

# Cpanel & WHM

## Tips sobre problemas comunes

- [Problemas para acceder a Roundcube - Redirección login](#)
- [cPanel - Acceso al terminal \(shell\) via cPanel de usuario](#)
- [Problemas con el uso de redes mixtas en cPanel](#)
- [all hosts for 'example.es' have been failing for a long time \(and retry time not reached\)](#)
- [Como instalar Snapd en CentOS 7](#)
- [Instalar redis / phpredis con control de estado en cPanel](#)
- [Composer 1 y Composer 2 en la misma máquina cPanel](#)
- [Cambiar el public\\_html del dominio principal en cPanel](#)
- [Error con WP-CLI en el shell con cPanel - PHP Fatal error: Allowed memory size of bytes exhausted](#)
- [Database Error Connection Failed - RoundCube cPanel con error 500 o página blanca](#)
- [Webmail. Pagina en blanco o error 500.](#)
- [Análisis de procesos en PHP-FPM cPanel](#)
- [Servidor PowerDNS no arranca por error en named.conf](#)
- [Cómo añadir una entrada SPF a todos los dominios de un servidor cPanel](#)
- [Problemas con las renovaciones y altas de certificados AutoSSL cPanel \(powered by Sectigo\)](#)
- [Lista de includes en backups especiales de WHM/cPanel](#)
- [Conocer versiones usadas en php via API](#)
- [Jetbackup](#)
- [Api](#)
  - [Añadir DMARC a los dominios con WHM Cpanel API](#)
- [Smartroute para destinatarios que nos tienen baneados, en cPanel con Exim](#)
- [Exim. Eliminar la cola de correo \(un correo o todos\)](#)
- [DKIM para el propio nombre del host o correo del servidor](#)
- [Buscando accesos raros a una cuenta de correo en los logs de cPanel](#)
- [El usuario no ve lo correos en su programa o en webmail \(cPanel\)](#)

- [Rutas Específicas o smarthost complejo para Exim y cPanel](#)
- [MySQL: Error "No space left on device" en /tmp](#)
- [Bloqueo de Bad Bots en cPanel con ModSecurity usando el Sistema Vendor](#)

# Problemas para acceder a Roundcube - Redirección login

## Introducción

Algunas veces RoundCube no permite a los usuarios, incluidos los administradores, el acceso a su webmail.

## Síntomas

Muestra los síntomas de inicio de sesión fallidos o una redirección constante a la página de inicio de sesión si accede desde cPanel.

## Corrección

Debemos posicionarnos en la carpeta de usuario

```
cd /home/<user>/etc/dominio
```

## Recuperación de la copia de seguridad

Podemos restaurar a una versión anterior que hayamos obtenido de las copias de seguridad. Esta es la mejor opción ya que de esta forma no perderemos los datos que esa base de datos tuviera.

Restaurar la copia de seguridad de <correo\_pop>.rcube.db en cd /home/  
/etc/dominio/<correo\_pop>.rcube.db

## Reconstrucción del fichero de datos

- Cambie el nombre del archivo <correo\_pop>.rcube.db a <correo\_pop>.rcube.db.bak
- Cambie el nombre del fichero <correo\_pop>.rcube.db.<numero\_de\_marca> más reciente a <correo\_pop>.rcube.db

## Enlaces y agradecimientos

- [How-To Fix A Corrupted RoundCube SQLite Database](#)

## Palabras clave

roundcube, webmail, problemas de acceso a roundcube, roundcube redirecciona vuelve al login, no puedo logearme

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# cPanel - Acceso al terminal (shell) via cPanel de usuario

## Introducción

El acceso a SSH es algo necesario o cuando menos, mucho más eficaz para un usuario de hosting, que andar a golpes con el servidor FTP. Ciertamente es que muchos, por no decir casi todos los proveedores de alojamiento web, no permiten el acceso vía SSH al servidor.

Muchos aducen un problema de seguridad, cuando en realidad los problemas de seguridad son más importantes en otras áreas del sistema, mucho más descuidadas que permitir un acceso a la consola shell, la cual puede ser monitorizada y fiscalizada con eficacia, siempre que el administrador de los sistemas de la empresa, esté cualificado para trabajar con sistemas y no con paneles de control solamente

## Acceso a terminal (shell) para usuarios de cPanel

Si tu proveedor lo ha activado, desde cPanel puedes acceder al shell de tu cuenta para hacer múltiples operaciones: Visualizar en tiempo real los logs de error Editar ficheros de configuración o ficheros que necesitan cambios Verificar o cambiar permisos de ficheros y directorios Copias de seguridad de ficheros (rsync) o mysql ultra rápidas Creación de snapshots de tu sitio antes de hacer un upgrade

cPanel > Terminal

Por favor, cuando leas en internet que alguien te dice que necesitas permisos 777 ó 666, como norma general cierra la pestaña del navegador y busca ayuda en otro artículo. Suele ser la información de un #copypaster. (copiar y Pegar)

## Hosting con acceso a terminal o SSH

Si tu proveedor de hosting no te deja acceder vía SSH o no te da acceso al terminal, planteate un cambio. En castris te ofrecemos ambas posibilidades.

# Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Problemas con el uso de redes mixtas en cPanel

## Introducción

Alguna vez por necesidades o por estrategias de red o administración de sistemas, es necesario usar redes mixtas en un mismo servidor.

En mi caso uso dos redes para los VPS de cPanel por estrategia de migración en caliente usando una IP primaria que uso exclusivamente para el host, pero no para las cuentas shared (compartidas) o con ip propia, para las que uso una red diferenciada.

Si estas dos redes tienen una diferente máscara de red, cpanel a veces se hace un lío en su gestión de ips alias, `/etc/ips` asignando un gateway incorrecto, por lo que la comunicación entre servidores con el mismo concepto de red, es imposible, ya que las rutas no están bien definidas

Este artículo es única y exclusivamente a nivel de operaciones de red, para cPanel que tiene su propio sistema de ip alias, [Add a New IP Address](https://docs.cpanel.net/whm/ip-functions/add-a-new-ip-address/)

## Síntomas

Un de ellos es el correo ya que los dominios de ambos servidores, tiene definidos como servidor remoto la IP shared (red B) en lugar de la IP de la interfaz de red primaria (red A)

La red A es una red /26 y la red B es una /27

Comprobamos que la red no tiene acceso aunque si lo tenemos a la interfaz primaria

```
$ telnet IP.RED.X.B 25
Trying 178.32.236.135...
```

Visualizamos la ruta o el fichero de ips `/etc/ips`

```
IP.RED.X.B:255.255.255.0CTET0:178.32.236.GATEWAY
```

Si observamos la Ip del gateway es incorrecta, ya que en realidad por lo que sea cpanel ha calculado el gateway para la red de la primaria, por lo que la tabla de rutas que crea el sistema de cpanel al activar (levantar) la red con su servicio ipaliases es incorrecta para la comunicación entre estas IPs.

## Solución

Se trata de asignar de forma correcta en el fichero `/etc/ips` la ip adecuada a nuestra red B y reiniciar la red y el sistema de alias de cPanel

```
Mi consejo es que estas cosas siempre las hagas en un terminal multiplexado **(screen)**
```

```
service network restart && service ipaliases restart
```

## Enlaces

[How To Use Linux Screen](#)

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).



# all hosts for 'example.es' have been failing for a long time (and retry time not reached)

## Introducción

A veces ocurren [errores de comunicación](#) muy continuados entre nuestros servidor cpanel y otro servidor, y cuando lo arreglamos, y ya estamos en disposición de enviar correos de nuestro servidor al otro, ocurre que obtenemos ese error

```
all hosts for 'example.tld' have been failing for a long time (and retry time not reached)
```

También puede ocurrir que nuestro cliente reclame que el administrador del otro servidor indique que nuestro servidor le rechaza. Y el 99% de los casos en una empresa de hosting, el administrador remoto, insistirá y golpeará el teclado en vez de analizar el problema usando un simple telnet. Recuerdale este tip

## Prueba de trabajo

Primero verificaremos que la comunicación con el servidor de correo es correcta

```
telnet IP.XXX.XXX.XXX 25
Trying IP.XXX.XXX.XXX...
Connected to IP.XXX.XXX.XXX
Escape character is '^]'.
220-serXXXX.YYYYYYY.com ESMTP Exim 4.94.2 #2 Wed, 14 Jul 2021 11:10:24 +0200
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
```

Pero sigue dándonos el error nuestro servidor exim

```
all hosts for 'example.tld' have been failing for a long time (and retry time not reached)
```

# Solución

Debemos eliminar las entradas de la base de datos de exim para los reenvios, los rechazos y los servidor en espera

```
# /usr/sbin/exim_tidydb -t 0d /var/spool/exim retry > /dev/null
# /usr/sbin/exim_tidydb -t 0d /var/spool/exim reject > /dev/null
# /usr/sbin/exim_tidydb -t 0d /var/spool/exim wait-remote_smtp > /dev/null
# /scripts/restartsrv_exim
```

Tras estas acciones el problema debería quedar resuelto.

## Enlaces

[all hosts for domain.ca have been failing for a long time \(and retry time not reached\)](#)

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Como instalar Snapd en CentOs 7

## Introducción

Snapd es un sistema universal de gestión de paquetes creado por Canonical (Ubuntu), que usa un formato de archivo llamado snap que se monta como un sistema de archivos comprimidos basado en el formato [squashfs](#), montado dinámicamente en el sistema operativo host.

Sin embargo su instalación en centos 7 ó 8, no está exenta de problemas que requieren algún tip..

## Instalación

La instalación habitual de snap es sencilla, pero en CentOs se requiere la instalación del [repositorio EPEL](#).

Instalar snapd en Centos Install

Si por cualquier casual estás usando un servidor cPanel, instalar el repositorio EPEL, tiene sus peculiaridad en cPanel si no quieres tener problemas posteriores, entre ellas que deberías desactivar por defecto el repositorio epel. Consultar el artículo enlazado.

```
[root@centos7 ~]# yum --enablerepo=epel install -y snapd
```

...

Instalado:

```
  snapd.x86_64 0:2.51-1.el7
```

¡Listo!

Una vez instalado, el manejador de servicios systemd necesita activar el sistema de comunicación por sockets.

```
[root@centos7 ~]# systemctl enable --now snapd.socket
```

```
Created symlink from /etc/systemd/system/sockets.target.wants/snapd.socket to  
/usr/lib/systemd/system/snapd.socket.
```

Después para activar el soporte del snap clásico, deberemos crear el enlace simbólico entre

```
/var/lib/snapd/snap y /snap
```

```
[root@centos7 ~]# ln -s /var/lib/snapd/snap /snap
```

## Otros enlaces

- [Installing snap on CentOS](#)

## Especificaciones sobre root y sudo

En esta y otras muchas entradas de esta wiki, no se actúa como usuario, sobre todo cuando no se trata de cuestiones como compilar paquetes, programas, ya que mi preferencia es trabajar como root salvo cuando por cuestiones de seguridad como las anteriores descritas si lo aconsejen, por lo que las entradas no tiene el uso de `sudo`

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Instalar redis / phpredis con control de estado en cPanel

## Introducción

Redis es para mi una de las mejores soluciones básicas para el caché de aplicaciones y sobre todo para la gestión de colas es Redis. Es perfecto para Wordpress, Prestashop, Laravel, Symfony, e imprescindible para Magento.

En este doc te explico en pocos pasos cómo instalar Redis para tus aplicaciones web en un entorno de cPanel CentOS.

## Instalación redis en CentOS (cPanel)

Debemos instalar epel, y al ser un sistema con el intrusivo panel de control cPanel deberemos deshabilitar el repositorio, so pena de tener problemas en el futuro.

Cuando nos pregunte pecl por las opciones es recomendable usar **igbinary** y la compresión **lzf**

```
# yum install epel-release
# grep -q '^enabled' /etc/yum.repos.d/epel.repo && sed -i 's/^enabled.*/enabled=0/'
/etc/yum.repos.d/epel.repo || echo 'enable=0' >> /etc/yum.repos.d/epel.repo
# yum install --enablerepo=epel redis
# systemctl enable redis
# systemctl start redis
# /opt/cpanel/ea-php80/root/usr/bin/pecl install igbinary igbinary-devel redis # ea-php80 para
php 8.0, Deberás repetir para cada versión php instalada
/opt/cpanel/ea-php80/root/usr/bin/pecl install igbinary igbinary-devel redis
Ignoring installed package pecl/igbinary
Ignoring installed package pecl/igbinary
WARNING: channel "pecl.php.net" has updated its protocols, use "pecl channel-update
pecl.php.net" to update
downloading redis-5.3.4.tgz ...
Starting to download redis-5.3.4.tgz (268,154 bytes)
.....done: 268,154 bytes
```

```
29 source files, building
running: phpize
Configuring for:
PHP Api Version:      20200930
Zend Module Api No:   20200930
Zend Extension Api No: 420200930
enable igbinary serializer support? [no] : yes
enable lzf compression support? [no] : yes
enable zstd compression support? [no] : no
```

## Script de control de estado

Como norma general, **Redis** en un entorno fuerte con memoria abundante y de calidad (ECC) no suele tener ningún problema. En caso de no estar trabajando en un entorno HA (High Availability) mediante un cluster de redis, es más que bueno y necesario tener un monitor que controle la salud de nuestro servicio.

```
#!/bin/sh

active=$(redis-cli ping) # redis sin contraseña
# Si usamos protección por contraseña
# active=$(redis-cli -a
+S62tFFXqTXhAQ1Y2X1PxUQNJASHSHSHFu4aS5iBZiCQfCz4wp6hrpCc62vNLLKXE3LPsJxBIgM6 ping)
hostname=$(hostname -f)

if [ "$active" != "PONG" ]; then
    echo "Redis ${hostname} down" | mail -s "Redis ${hostname} down" monitor@myemail.com
    systemctl restart redis
fi
```

Damos permisos de ejecución 700 y añadimos al crontab de root

```
* * * * * /usr/local/bin/redischeck.sh > /dev/null 2>&1
```

## Tips sobre la configuración

**WARNING: The TCP backlog setting of 511 cannot be enforced because /proc/sys/net/core/somaxconn is set to the lower value of 128**

Editar el fichero `chmod +x /etc/rc.d/rc.local`

```
# Añadir  
sysctl -w net.core.somaxconn=65535
```

Ejecutar

```
chmod +x /etc/rc.d/rc.local
```

**WARNING overcommit\_memory is set to 0!**

```
nano /etc/sysctl.conf  
vm.overcommit_memory = 1
```

**WARNING you have Transparent Huge Pages (THP) support enabled in your kernel**

```
echo never > /sys/kernel/mm/transparent_hugepage/enabled
```

Editar tambien `/etc/rc.d/rc.local`

```
echo never > /sys/kernel/mm/transparent_hugepage/enabled
```

## Redis 6.2 con control ACL

### Editado 2023-05-10

La version actual ya no es la 6.2. He optado por ir a la última estable.

```
yum install systemd-devel
cd /usr/local/src
# https://redis.io/download
wget https://download.redis.io/redis-stable.tar.gz
tar xvfz redis-stable.tar.gz
cd redis-stable
make
make test
make install
groupadd redis
adduser --system -g redis --no-create-home redis
mkdir -p /var/lib/redis
chown redis: /var/lib/redis
chmod 770 /var/lib/redis
mkdir /etc/redis
cp /usr/local/src/redis-stable/redis.conf /etc/redis/
mkdir /var/run/redis
chown redis: /var/run/redis
```

Editamos el fichero de configuracion

```
supervised systemd
unixsocket /var/run/redis/redis.sock
unixsocketperm 770
port 0
```

Creamos el fichero system /etc/systemd/system/redis.service

```
[Unit]
Description=Redis Data Store
After=network.target
[Service]
User=redis
Group=redis
ExecStart=/usr/local/bin/redis-server /etc/redis/redis.conf
ExecStop=/usr/local/bin/redis-cli shutdown
Restart=always
[Install]
WantedBy=multi-user.target
```



Activamos y arrancamos

```
systemctl enable redis  
systemctl start redis  
systemctl status redis
```

# Notas sobre Ubuntu

Los cambios a realizar para la configuración del sistema se realizan en el fichero `/etc/sysctl.conf`

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Introducción

# Instalar la versión de composer 1 junto a composer 2

# Use composer1

```
$ composer1 -v
```

```
 / /  / _ \ _ ` _ \ _ \ _ \ _ / _ \ _ /
 / _ / / / / / / / / / / / / / ( _ ) _ / /
 \ _ / \ _ / / / / / . _ / \ _ / \ _ / /
      / _ /
```

Composer version 1.10.23 2021-10-05 09:44:27

Usage:

command [options] [arguments]

# Notas de seguridad

No incluye la verificación del hash md5 del archivo descargado, lo cual es a elección del administrador.

# Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Cambiar el public\_html del dominio principal en cPanel

## Introducción

Aunque todo se puede hacer vía .htaccess, no soy partidario de esto. Estoy más acostumbrado a Nginx, y por otro lado cuanto menos se complique .htaccess mejor será la respuesta FRT (First Time Response) mejor.

Así que prefiero adecuar el sitio a un formato via configuración de Apache. Pero cPanel es un panel altamente intrusivo que te obliga a respetar sus formas, más con Apache.

## Modificación de los ficheros userdata del usuario y dominio

/var/cpanel/userdata/usuario/dominio.principal.tld

```
---
customlog:
-
  format: combined
  target: /etc/apache2/logs/domlogs/dominio.principal.tld
-
  format: "\"%{s}t %I .\\n%{s}t %O .\"
  target: /etc/apache2/logs/domlogs/dominio.principal.tld-bytes_log
documentroot: /home/usuario/public_html/public
group: usuario
hascgi: 0
homedir: /home/usuario
ip: 87.98.230.68
owner: root
```

```
phpopenbasedirprotect: 1
port: 80
scriptalias:
-
  path: /home/usuario/public_html/public/cgi-bin
  url: /cgi-bin/
serveradmin: webmaster@dominio.principal.tld
serveralias: mail.dominio.principal.tld www.dominio.principal.tld
servername: dominio.principal.tld
usecanonicalname: 'Off'
user: usuario
```

## dominio.principal.tld\_SSL

```
---
documentroot: /home/usuario/public_html
group: usuario
hascgi: 0
homedir: /home/usuario
ip: 87.98.230.68
ipv6: ~
owner: root
phpopenbasedirprotect: ~
port: 443
secruleengineoff: ~
serveradmin: webmaster@dominio.principal.tld
serveralias: mail.dominio.principal.tld www.dominio.principal.tld
servername: dominio.principal.tld
ssl: 1
usecanonicalname: 'Off'
user: usuario
userdirprotect: ''
```

## Eliminar los ficheros de caché

```
rm -vf /var/cpanel/userdata/username/*.cache
```

# Actualizar Apache via WHM

```
# /scripts/updateuserdatacache
```

```
# /scripts/rebuildhttpdconf
```

## Modificación de PHP-FPM

Si usamos php-fpm, que es lo mejor para un hosting, hay que hacer un paso más que es modificar el path en php-fpm para el usuario editando el fichero `/var/cpanel/userdata/USER/DOMAIN.php-fpm.yaml`

```
php_admin_value_doc_root: { name: 'php_admin_value[doc_root]', value:  
/home/USER/NEW/DOCUMENT/ROOT }
```

Una vez modificado (imagino que habrás sustituido **USER**, **DOMAIN** y **NEW/DOCUMENT/ROOT** por sus valores adecuados hay que reconstruir los ficheros de php-fpm y hacer un restart de php-fpm

```
/scripts/php_fpm_config --rebuild  
/scripts/restartsrv_apache_php_fpm
```

## Enlaces

- [How to change the document root for a cPanel account](#)
- [How to update the PHP-FPM document root for the primary domain](#)

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Error con WP-CLI en el shell con cPanel - PHP Fatal error: Allowed memory size of bytes exhausted

## Escenario

Intentas instalar o ejecutar con wp-cli una instalación y te das de bruces con un problema de memoria, y lo único que se les ocurre a los “expertos” de cpqanel es replicar que cambies la memoria en tu panel, cuando la cuestión es el PHP en modo cli, y no en modo PHP-FPM.

## Log del error

```
[12-May-2022 06:07:40 UTC] PHP Fatal error: Allowed memory size of 67108864 bytes exhausted (tried to allocate 36864 bytes) in phar:///usr/local/bin/wp/vendor/wp-cli/wp-cli/php/WP_CLI/Extractor.php on line 100
```

Tienes una solución.

## Editar el comando

```
$ php -d memory_limit=512M "$(which wp)" core download --locale=es_ES
Downloading WordPress 5.9.3 (es_ES)...
md5 hash verified: b7e70ab7cd8749ae5f5a5a3c63772117
Success: WordPress downloaded.
```

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias

de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).



# Database Error Connection Failed - RoundCube cPanel con error 500 o página blanca

A veces un sólo usuario de una cuenta cpanel tiene un problema con el acceso a su Roundcube, teniendo un error 500 y al hacer reload un mensaje con **Database Error Connectio Failed**

Una de las posibles causas es la corrupción del fichero **.rcube.db** de la cuenta de correo afectada.

## Solución

Mover el fichero y dejar que Roundcube regenere el fichero.

```
mv /home/<user>/etc/<dominio.tld>/<cuenta_correo>.rcube.db  
/home/<user>/etc/<dominio.tld>/<cuenta_correo>.rcube.db.bak2
```

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como esta, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Webmail. Pagina en blanco o error 500.

## Introducción

Muchos de los problemas derivados de webmail de cPanel vienen de la mano de corrupciones de los ficheros **sqlite** que tiene como uso ser la base de datos de cada cuenta.

No siempre, pero este es un buen punto de partida.

- [How-To FiX a Corrupted Royudcube SQLite Database](#)

## Remover el fichero dañado

- /home/<cpanel\_user>/etc//

# Análisis de procesos en PHP-FPM cPanel

## Introducción

Lo de PHP-FPM a veces es mas complejo de lo que parece. Funciona bien pero da quebraderos de cabeza. El post original es muy bueno para trabajar con el.

[How to review PHP-FPM processes per account](#)

## Ver procesos de un usuario

```
cPusername=user_cpanel
ps -f -U $cPusername |grep "[p]hp-fpm"
ps -f -U $cPusername |grep "[p]hp-fpm"
mysite      3353 15248  2 09:28 ?          00:00:00 php-fpm: pool mysite_net
mysite      26746 15248  4 09:25 ?          00:00:08 php-fpm: pool mysite_net
mysite      27163 15248  3 09:26 ?          00:00:05 php-fpm: pool mysite_net
```

## Contarlos

```
ps -f -U $cPusername|grep -c "[p]hp-fpm"
3
```

## Ver los procesos de todas las cuentas

```
for user in `cat /etc/trueuserdomains|awk '{print $2}'`;
do printf "User $user PHP-FPM processes:\n\n";
ps -f -U $user -u $user|grep "[p]hp-fpm";done
```

## Contarlos

```
for user in `cat /etc/trueuserdomains|awk '{print $2}'`;
do printf "User $user PHP-FPM processes:  ";
```

```
ps -f -U $user -u $user|grep -c "[p]hp-fpm";done
```

# Links

Otro documtno muy interante es [PHP-FPM Performance Tuning Basics](#)

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Servidor PowerDNS no arranca por error en named.conf

## Introducción

PowerDNS es una solución bastante aceptable como servidor DNS para entornos empresariales. Su uso por parte de cpanel no está exento de problemas. Uno de ellos es que se produzca una avería en el fichero `/etc/named.conf` lo cual irremediablemente, dejará apagado nuestro dns y un montón de líneas en el log, confirmando el desastre.

```
Sep  3 01:00:11 stark pdns_server: PowerDNS Authoritative Server 4.4.1 (C) 2001-2020
PowerDNS.COM BV
Sep  3 01:00:11 stark pdns_server: Using 64-bits mode. Built using gcc 4.8.2 20140120 (Red Hat
4.8.2-16) on Oct 25 2021 16:52:08 by root@bh-centos-7.dev.cpanel.net.
Sep  3 01:00:11 stark pdns_server: PowerDNS comes with ABSOLUTELY NO WARRANTY. This is free
software, and you are welcome to redistribute it according to the terms of the GPL version 2.
Sep  3 01:00:11 stark pdns_server: [webserver] Listening for HTTP requests on 127.0.0.1:953
Sep  3 01:00:11 stark pdns_server: Creating backend connection for TCP
Sep  3 01:00:11 stark systemd: Started PowerDNS Authoritative Server.
Sep  3 01:00:11 stark pdns_server: Error parsing bind configuration: Error in bind
configuration '/etc/named.conf' on line 5634: syntax error
Sep  3 01:00:11 stark pdns_server: Caught an exception instantiating a backend: Error in bind
configuration '/etc/named.conf' on line 5634: syntax error
Sep  3 01:00:11 stark pdns_server: Cleaning up
Sep  3 01:00:11 stark pdns_server: TCP server is unable to launch backends - will try again
when questions come in: Error in bind configuration '/etc/named.conf' on line 5634: syntax
error
Sep  3 01:00:11 stark pdns_server: Only asked for 1 backend thread - operating unthreaded
Sep  3 01:00:11 stark pdns_server: Error parsing bind configuration: Error in bind
configuration '/etc/named.conf' on line 5634: syntax error
Sep  3 01:00:11 stark pdns_server: Caught an exception instantiating a backend: Error in bind
configuration '/etc/named.conf' on line 5634: syntax error
Sep  3 01:00:11 stark pdns_server: Cleaning up
Sep  3 01:00:11 stark pdns_server: Distributor caught fatal exception: Error in bind
configuration '/etc/named.conf' on line 5634: syntax error
```

```
Sep  3 01:00:11 stark systemd: pdns.service: main process exited, code=exited,
status=1/FAILURE
Sep  3 01:00:11 stark systemd: Unit pdns.service entered failed state.
Sep  3 01:00:11 stark systemd: pdns.service failed.
```

# Solución

En el caso de nuestros servidores o los de algunos clientes, en los que usamos una estructura maestro y secundarios en distintas redes, lo necesario será usar el propio script de reparación de cPanel.

“ Aun así en entorno como miles de entradas DNS (zonas) es más que aconsejable hacer copias regulares (con intensidad adecuada a los cambios en su estructura) por si este script fallará, dada la sensibilidad de los servidores de nombres basados en named, con su fichero de configuración.

```
mv /etc/named.conf /etc/named.conf.bak
/usr/local/cpanel/scripts/rebulddnsconfig
/scripts/restartsrv_named
```

# Más información

[DNS Functions :: WHM/cPanel](#) [PowerDNS :: Documentacion](#)

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Cómo añadir una entrada SPF a todos los dominios de un servidor cPanel

## Introducción

Cualquiera que tenga la administración de un servidor con **cPanel**, habrá sufrido en algún momento la dictadura de **Microsoft** con su patético y cruel sistema de **anti-spam**, denominado **SNDS (Smart Network Data Service)**.

La entrada de una IP de un servidor de correo en este dichoso sistema, es la antesala de un montón de problemas, comenzando por la poca ética y corresponsabilidad de Microsoft con los administradores de sistemas.

Desde hace años, la mejor salida pasa por tener preparados microservidores con un servidor de correo (recomiendo Postfix) configurados para hacer de **smarthost** de tal forma que en caso de alcanzar en el punto rojo con el SNDS de Microsoft, podamos sacar el correo a través de dicho smarthost, mientras luchamos contra el gigante y su penoso soporte entre pares.

## Despliegue

cPanel tiene esta opción desde hace años integrada en su panel WHM, e incluye una marca (checkbox) para añadir la entrada a las **zonas DNS**, pero esta nunca me funcionó bien ni es la adecuada a mis necesidades.

Esta actualización es necesaria, ya que de lo contrario cualquier servidor de correo que tenga configurado meridianamente bien su sistema de correo y antispam, rechazará el correo porque las entradas DNS de los dominios, (sobre todo si está DKIM activado) no contendrán respuesta adecuada sobre la IP del smarthost.

Es imperativo añadir la **IP** o el **hostname** del servidor **smarthost**.

Configuracion Exim :: Smarthost

# Script para añadir la entrada SPF a todos los dominios del servidor

## Comando para añadir un FQDN

```
cat /etc/localdomains | xargs -n 1 /scripts/whoowns | sort | uniq | egrep -v '^$' | xargs -n 1  
-I account sh -c 'echo Installing for account...;/usr/local/cpanel/bin/spf_installer account  
include:_smart.domain.tld echo Done.'
```

## Comando para añadir una IP

```
cat /etc/localdomains | xargs -n 1 /scripts/whoowns | sort | uniq | egrep -v '^$' | xargs -n 1  
-I account sh -c 'echo Installing for account...;  
/usr/local/cpanel/bin/spf_installer account +ip4:192.88.99.21; echo Done.'
```

## Enlaces

- [Microsoft \(Hotmail y otros\): como defenderse de sus listas negras con JMRP y SNDS de microsoft](#)
- [Hotmail – outlook: error ... since part of their network is on our block list](#)
- [How to add an SPF entry to all domains on the server](#)

## Otro tip para todos las cuentas

[How to add an SPF entry to all domains on the server](#)

## Añade un hostname

```
cat /etc/localdomains | xargs -n 1 /scripts/whoowns | sort | uniq | egrep -v '^$' | xargs -n 1  
-I account sh -c 'echo Installing for account...; /usr/local/cpanel/bin/spf_installer account  
include:example.domain.tld; echo Done.'
```

## Añade una ip

```
cat /etc/localdomains | xargs -n 1 /scripts/whoowns | sort | uniq | egrep -v '^$' | xargs -n 1  
-I account sh -c 'echo Installing for account...; /usr/local/cpanel/bin/spf_installer account  
+ip4:192.88.99.21; echo Done.'
```

## Quieres añadir mas de una ip?



```
cat /etc/localdomains | xargs -n 1 /scripts/whoowns | sort | uniq | egrep -v '^$' | xargs -n 1  
-I account sh -c 'echo Installing for account...; /usr/local/cpanel/bin/spf_installer account  
'+ip4:192.0.2.0/24,-ip4:203.0.113.5,+ip6:2001:db8:1a34::/64'; echo Done.'
```

## Help del comando

```
/usr/local/cpanel/bin/spf_installer --help
```

```
Usage: /usr/local/cpanel/bin/spf_installer <user> [policy [is-complete [overwrite  
[preserve]]]]
```

Installs an SPF policy in TXT records for the given user's domains.

Note: The following will be prepended to the policy: +a +mx +ip4:<main-IP>.

### Options:

<user>            User whose domains will receive the SPF record.

<policy>

Comma delimited list of SPF mechanisms to include in the policy, e.g:

'+ip4:192.0.2.0/24,-ip4:203.0.113.5,+ip6:2001:db8:1a34::/64'.

Default: ""

<is-complete>

Indicates whether the policy represents a complete record, that is, whether it should terminate with "-all". Use "1" to indicate that it is; otherwise, use "0". Default: "0"

<overwrite>

Indicates whether all SPF records should be overwritten for the user. If not, only select records will be replaced; see Overwrite. Use "1" to indicate that it should; otherwise, use "0". Default: "0"

<preserve>

Indicates that existing mechanisms should be retained from the current SPF record for the domain. Use "1" to indicate that they should be kept; otherwise, use "0". Default: "0"

Overwrite

When this script is run, the zone file for the domain is inspected and the first SPF record that is found (generally, the main domain) is recorded. Any other subdomains that have an identical SPF record to this one are replaced. If <overwrite> is "1", then all SPF records, regardless of whether their content matches the first record, are replaced.

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Problemas con las renovaciones y altas de certificados AutoSSL cPanel (powered by Sectigo)

## Detección de problemas con certificados Free SSL de cPanel

Son sencillos, ya que ni altas de nuevos dominio o subdominios, ni renovaciones funcionan muchas de las veces, pese a que si buscamos en los logs, encontramos que el trabajo fue puesto en cola por estar en un estado “DEFECTIVO” el actual certificado (sin él, caducado, etc).

La cuestión es clara desde hace unos meses (Agosto de 2022) y ha ido a peor. Sectigo no está por la labor, y el nivel de producción de sus cola gratuitas es muy deficitario para la demanda que tiene. Como resultado miles de certificados no se renuevan en tiempo y forma, y los nuevos ya ni siquiera entran en el juego.

## Solución: el cambio de proveedor

La solución más adecuada es el cambio de proveedor a Let 's Encrypt aunque tiene algunas peculiaridades como que los certificados del hostname no los genera. Pero creo que quien tiene un servidor dedicado, bien puede gastar unos pocos euros por tener su certificado de pago.

## Como cambiar en WHM el proveedor de certificados gratuitos a Let's Encrypt

Acceder como root al terminal ssh (podemos hacerlo desde WHM si está activado) Ejecutar `/usr/local/cpanel/scripts/install_lets_encrypt_autossl_provider` Volver al navegador a nuestra entrada WHM y navegar a Manage AutoSSL > AutoSSL Providers, seleccionando **Let's Encrypt™** Aceptar los **Términos de Servicio** Salvar

Esto ya sería suficiente. Si tienes pendientes certificados puedes ganar tiempo ejecutando la herramienta para comprobar a todos los usuarios.

# Diferencias

Deberías leer el documento [The Let's Encrypt Plugin](#)

“ This plugin does not generate hostname certificates for your system's services. It only generates SSL certificates for your cPanel accounts. For more information, read our Manage AutoSSL documentation.

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Lista de includes en backups especiales de WHM/cPanel

## Introducción

Los backups de cPanel no son precisamente lo mejor para un administrador. Esta bien para lo justo. Si tienes un sistema, propio o otro que te permita añadir o crear backups de directorios o ficheros especiales esta bien tener la lista a mano. Yop me guardo estos, por si acaso.

## Lista de directorios y ficheros a incluir en un backup cPanel

```
/etc/apache2/conf/httpd.conf
/etc/dovecot/sni.conf
/etc/exim.conf
/etc/exim.conf.local
/etc/exim.conf.localopts
/etc/fstab
/etc/group
/etc/ips
/etc/localdomains
/etc/mailips
/etc/manualmx
/etc/master.passwd
/etc/my.cnf
/etc/named.conf
/etc/namedb/named.conf
/etc/passwd
/etc/proftpd.conf
/etc/pure-ftpd.conf
/etc/rc.conf
/etc/remotedomains
/etc/reservedipreasons
/etc/reservedips
```

```
/etc/rndc.conf
/etc/secondarymx
/etc/senderverifybypasshosts
/etc/spammeripblocks
/etc/cpanel_exim_system_filter
/etc/global_spamassassin_enable
/etc/spammers
/etc/shadow
/etc/wwwacct.conf
/root
/var/cpanel/greylist/conf
/var/cpanel/greylist/greylist.sqlite
/var/cpanel/mysql/remote_profiles/profiles.json
/etc/ips.remotemail
/etc/ips.remotedns
/etc/valiases
/etc/vdomainaliases
/etc/vfilters
/etc/proftpd
/usr/local/cpanel/3rdparty/mailman
/var/spool/cron
/etc/cpanel
/etc/mail
/etc/namedb
/var/lib/rpm
/var/lib/named/chroot/var/named/master
/var/named
/var/cpanel
/var/cron/tabs
/var/spool/fcron
/var/log/bandwidth
/usr/share/ssl
/etc/pki/tls/certs
/etc/ssl
/var/ssl
/var/cpanel/users
```

“ Ojo, esta es una lista recomendada, no completa.

# Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Conocer versiones usadas en php via API

## Introducción

A veces necesitamos saber que sitios web estan usando una versión determinada de PHP. He visto algunos que pretenden que hagas estos con un find buscando en los .htaccess de todo el servidor. ¡Que barbaridad!!!

## whmapi

En el shell como root, y ya esta

```
whmapi1 php_get_vhosts_by_version version=ea-php56

---
data:
  vhosts: []

metadata:
  command: php_get_vhosts_by_version
  reason: OK
  result: 1
  version: 1
> whmapi1 php_get_vhosts_by_version version=ea-php55

---
data:
  vhosts:
    - formacion.fuentesdecarions.org

metadata:
  command: php_get_vhosts_by_version
  reason: OK
  result: 1
  version: 1
```



Recuerda que `whmap11` tiene la posibilidad de formatear la salida `--output=[json|jsonpretty|xml|yaml]`

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Jetbackup

Las cosas del sistema Jetbackup

# Api

La API de cpanel es potente, pero su documentación aunque va mejorando, sigue siendo un poco difícil de encontrar

# Añadir DMARC a los dominios con WHM Cpanel API

## Introducción

Básicamente se trata de añadir un registro a la zona dns de un dominio

Ya sé que se puede hacer via WHM, pero... imagínate que tienes que hacerlo en TODOS, o una buena parte de los dominios del servidor?

Bien, ese es el caso.

“ El tip presentado adolece de uno de los problemas más absurdos de la API, en el tema de los DNS. No tiene un control de lo que haces, y por tanto si existe el registro que creas, crea otro. En el caso de los **\_dmarc** es una duplicidad, y aunque no es un error estricto ya se trata de un problema. No es el alcance de este tip0, el incluir la operativa para buscar un registro en una zona dns, si existe eliminar, y después continuar con la inserción actualizada. ;-)

## Operativa

El comando en el shell es `whmapi1 addzonerecord`

Parámetro	tipo	Descripción	Valor	Ejemplo
domain	string	Nombre de la zona dns	El nombre del dominio (sin www, por favor)	example.com
name	string	Nombre del registro	_dmarc	_dmarc
class	string	La clase de registro	IN	IN

Parámetro	tipo	Descripción	Valor	Ejemplo
ttl	integer	Es el TTL del registro. Desde hace un tiempo para evitar problemas con el validador de zonas DNS de cPanel, debe ser el mismo en todos los registros	TTL representado en segundos	1800
type	string	Tipo de registro	TXT	TXT
txtdata	text	Al ser un TXT requiere le texto del registro DMARC entre comillas	"v=DMARC1;p=quarantine;sp=quarantine;adkim=s;aspf=s;pct=100;fo=0;rf=afrr;ri=86400;rua=mailto:dmarc@example.com;ruf=mailto:dmarc@example.com"	

## Ejemplo

```
[root@b ~]# whmapil addzonerecord domain=example.com name=_dmarc class=IN ttl=1800 type=TXT
txtdata="v=DMARC1;p=quarantine;sp=quarantine;adkim=s;aspf=s;pct=100;fo=0;rf=afrr;ri=86400;rua=
mailto:dmarc@example.com;ruf=mailto:dmarc@example.com"
```

“ Se recomienda la lectura del artículo enlazado para entender las posibilidades

## Enlaces

[Dmarc, protección frente al phishing, scam, spoofing en cPanel](#)

### Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Smarteroute para destinatarios que nos tienen baneados, en cPanel con Exim

## NOTA IMPORTANTE

Este artículo se mantiene, pero es más moderno y mejor estructurado, el artículo [Configuración de Smart Relay en cPanel/Exim](#)

## Introducción

Algunas veces, como administradores de sistemas en servidores compartidos, nos encontramos con un destino que nos tiene baneados, bien por sistemas internos o por el uso de listas negras de dudosa reputación, como es el caso de la **@policia.es** que usa un sistema antispam, algo restrictivo y cuyo canales de comunicación a nivel **abuse@**, **postmaster@** es nulo.

La mejor forma es usar un smarthost, para sacar nuestro correo por él. Pero el método habitual de cPanel, nos redirige todo el correo por el smart, y es algo que no queremos, salvo en contadas ocasiones.

Smarthost :: Exim :: cPanel

## Smarthost por destinatario

Debemos modificar la configuración de **exim**, usando el Advanced Editor

## Backup

Importante como siempre, guardar un backup rápido

Exim:: backup

## Advanced Editor

En la sección **ROUTERSTART**

```
policia_smarthost_router:
  driver = manualroute
  transport = policia_smarthost_transport
  route_list = policia.es <smart_host_Fqdn_or_ip>
```

cPanel :: Exim :: Advanced Editor :: Routerstart Section

En la sección **TRANSPORTSTART**

```
policia_smarthost_transport:
  driver = smtp
  hosts_require_tls = *
```

Exim :: Advanced Editor :: TransportStart Section

Con esta configuración, que podemos extender a múltiples destinados y múltiples emisores si queremos aumentar el juego de posibilidad, todo el correo del servidor dirigido a **@policia.es** será enrutado al smarthost, evitando así su insufrible antispam, mientras tratamos de comunicarnos con sus técnicos.

El resto del correo saldrá por nuestro servidor SMTP.

“ Si el dominio tiene protección (que debería [SPF](#), [DMARC](#), deberás actualizar el registro SPF para que permita también el relay desde la ip del smarthost.

## Enlaces interesantes

- [Configure Exim to use a Smarthos](#)
- [Forward certain domain emails to Smart Host](#) Algo antiguo pero útil
- [How to send email from different domains using different smarthosts](#)
- [Help with smarthost setup for using smarthost only for certain domain recipients](#) con varios enlaces organizados.

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#) Si necesitas soporte profesional puedes contratar

con Castris [soporte profesional](#).



# Exim. Eliminar la cola de correo (un correo o todos)

## Exim eliminar la cola de correo: ¿Cómo hacerlo fácilmente?

¿Buscas cómo eliminar la cola de correo en Exim?

Exim es un agente de transferencia de correo (MTA) que puede utilizarse como alternativa a Sendmail en sistemas Unix. Es el usado por cPanel entre otros.

La función principal de un MTA es recibir mensajes de diferentes fuentes y entregarlos a sus destinos correspondientes.

## Análisis rápido de la cola de correo en Exim

Un servidor de correo, recibe correos electrónicos entrantes y los reenvía a clientes/usuarios de correo.

Exim puede aceptar mensajes de hosts remotos utilizando SMTP sobre TCP/IP, así como de procesos locales.

## La cola de correo en Exim

### Imprimir la lista de mensjaes en cola

```
exim -bp
```

### Mostrar el número de correos en cola

Para mostrar el número de correos electrónicos en la cola, utilizamos el comando:

```
exim -bpc
```

## Contar emails de un usuario

Para contar los correos electrónicos de un remitente en particular, utilizamos el comando:

```
exim -bp|grep "<"|grep $userName|wc -l
```

## Contar correos usando exiqgrep

```
exiqgrep -cr $recipientAddress
```

## Otra alternativa con Exim para contra emails

```
exim -bp|grep $recipientAddress|wc -l
```

# Eliminación de correos en la cola de Exim

A veces es necesario (spam, error de envío, ...) eliminar correos de la cola

## Eliminar TODOS los correos de la cola de Exim

```
exim -bp|grep "<"|awk {'print $3'}|xargs exim -Mrm
```

o su alterntiva

```
exim -bp | awk '/^ *[0-9]+[mhd]/{print "exim -Mrm " $3}' | bash
```

En este método, el comando 'exim -bp' se utiliza para obtener el ID del mensaje de la cola de correo de Exim.

Luego, eliminamos el correo correspondiente de la cola utilizando el comando 'exim -Mrm' como argumento.

También utilizamos el comando 'exiqgrep' para eliminar la cola de correo.

```
exiqgrep -i | xargs exim -Mrm
```

Además, para eliminar un mensaje específico de la cola, utilizamos el siguiente comando:

```
exim -Mrm {ID-del-mensaje}
```

De manera similar, para eliminar todos los correos electrónicos de un usuario específico de la cola, utilizamos el siguiente comando:

Editado y corregido 16/09/2024 ~~exiqgrep -i -f \$usuario | xargs exim -Mrm~~

```
exiqgrep -i -f "$userName" | xargs -n1 exim -Mrm
```

También, para eliminar todos los mensajes congelados, utilizamos los siguientes comandos:

```
exiqgrep -z -i | xargs exim -Mrm
```

Con estos comandos, podemos realizar diferentes operaciones de eliminación en la cola de correo de Exim para nuestros clientes.

## Conclusión

En resumen, hemos revisado cómo verificar la cola de correo utilizando comandos de Exim. Sin embargo dejame que te diga que hay plugin muy bueno para la gestion de colas de Exim en cpanel, como puede ser [ConfigServer Mail Queues - cmq](#)

### Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# DKIM para el propio nombre del host o correo del servidor

## DKIM for main server hostname

### Introducción

Se detecta que en determinados casos (se suponía arreglado hace uno 5 años) cPanel no crea la entrada adecuada en el registro DNS de un hostname que coincide con el dominio principal de un servidor VPS.

Si este dominio tiene DKIM activado (que debería) los email enviados por cPanel (como nobody) fallarán si el receptor tiene en u servidor habilitado el DKMI fail.

### Solución

Crear o añadir al fichero `/var/cpanel/users/nobody`

```
DNS=hostname.domain.com
```

“ hostname.domain.com es claro que hay que sustituirlo por el real.

Y entonces ejecutar `/usr/local/cpanel/bin/dkim_keys_install nobody`

### Notas

Ahora que la empresa propietaria de cPanel sigue subiendo los precios, y ya no da soporte a las licencias compradas a **sus revendedores** y que estos se hacen los locos, cada día es más importante tener una base de conocimiento, frente a los mil problemas que este panel tiene.

### Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún

obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Buscando accesos raros a una cuenta de correo en los logs de cPanel

## Introducción

Algunas veces se hace necesario revisar los logs para investigar problemas reportados en tickets de "no me llegan los correos".

Muchas veces son filtros de correo mal implementados, pero otras veces son signos de que la cuenta está hackeada.

Una cosa que no entienden los usuarios es que un exploit que permita acceso al atacante para inyectar un mini shell o una utilidad de administración de archivos, le da al atacante acceso a ciertas cosas de su cuenta.

Así que haremos uso intensivo de `grep`, `awk` y otros comandos de shell.

## Busqueda de accesos en el correo

```
{ grep -Ei "login:" /var/log/maillog | awk '{print $1 " " $2 " " $3 " " $10 " " $8 }' | sed 's/rip=//g;s/,//g' && grep -Ei "\[webmaild\]" /usr/local/cpanel/logs/session_log* | awk '{print $1 " " $2 " " $6 " " $8}' | cut -d"[" -f 2 | sort | uniq && grep -Ei "\[webmaild\]" /usr/local/cpanel/logs/login_log* | awk '{print $1 " " $2 " " $6 " " $8}' | cut -d"[" -f 2 | sort | uniq; }
```

```
2024-07-02 21:21:44 213.194.xxx.220 paqui@dfsdfsdfsdf.com
2024-07-02 21:57:51 213.194.xxx.220 info@sdfsdfsdfsdf.com
2024-07-02 22:49:56 216.147.xxx.79 reservas@sdfsefsfdd.com
2024-07-02 23:21:27 213.194.xxx.220 info@sdfsdfsdfsdf.com
2024-07-03 03:07:18 35.173.xxx.157 ignacio@sdfsdfsdfsdf.es
2024-07-03 05:50:35 80.30.xxx.100 educacion@sdfsdfs.sdfsdfsdfss.org
```

### Version por cuenta especifica

```
cuenta="usuario@dominio.com"
```

```
{  
  grep -Ei "login:" /var/log/maillog | grep "$cuenta" | awk '{print $1 " " $2 " " $3 " " $10 "  
  " $8}' | sed 's/rip=//g;s/,//g'  
  grep -Ei "\[webmaild\]" /usr/local/cpanel/logs/session_log* | grep "$cuenta" | awk '{print  
$1 " " $2 " " $6 " " $8}' | cut -d"[" -f 2 | sort | uniq  
  grep -Ei "\[webmaild\]" /usr/local/cpanel/logs/login_log* | grep "$cuenta" | awk '{print $1  
  " " $2 " " $6 " " $8}' | cut -d"[" -f 2 | sort | uniq  
}
```

```
2024-06-26 08:51:11 213.194.xxx.220 usuario@dominio.com  
2024-07-01 22:39:16 213.194.xxx.220 usuario@dominio.com  
2024-07-02 12:06:21 31.221.xxx.87 usuario@dominio.com  
2024-07-02 14:08:57 213.194.xxx.220 usuario@dominio.com  
2024-07-02 14:17:08 213.194.xxx.220 usuario@dominio.com
```

# Agradecimientos

A Ehsan Dowlatshah en [How To List Email Login History?](#) por la idea.

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# El usuario no ve los correos en su programa o en webmail (cPanel)

## Introducción

Esto suele pasar más veces de lo deseado en cPanel, y pone muy nerviosos a los clientes.

El cliente acude a su programa y no ve ningún correo o le faltan correos en sus carpetas. Usa IMAP, por supuesto.

Se trata de una rotura de los índices de **Dovecot** que es el gestor IMAP usado en cPanel.

## Solución cPanel

Se trata de clarear o reindexar los índices de las cuentas de correos del usuario.

cPanel pone un script para esta cuestión.

```
/scripts/remove_dovecot_index_files --user cpaneluser
```

## Otra cuestión

Puede ser necesario también eliminar los ficheros `dovecot-uid*` en la mayoría de los casos, aunque prefiero hacerlo sólo si falla el primero en alguna cuenta particular.

```
cd /home/CPANELUSER/mail/USERDOMAIN.TLD/ACCOUNT/  
/scripts/remove_dovecot_index_files --user cpaneluser  
/bin/rm -f ./dovecot-uid*
```

## Explicación del script

Con la explicación también obtienes posibilidades para hacer esto en otro sistema que no tenga cPanel o no tenga panel de control, pero si **Dovecot**

## Remover los ficheros index



```
#dovecot.index*  
#dovecot.index.cache*  
#dovecot.index.log*  
find "$maildir" -type f -regex '.*dovecot\.index(\.cache|\.log(\.[0-9]+)?)?' -exec rm -f {} +
```

## Otros

En un servidor sin cPanel tambien puedes usar

```
doveadm index -u usuario@example.com
```

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Rutas Específicas o smarthost complejo para Exim y cPanel

## Configuración de Smart Relay en cPanel/Exim

### Smarthosts

A veces, lidiar con Microsoft, Yahoo y toda la gama de Big Tech dedicadas al correo es una misión imposible. Son los eternos enemigos de las empresas de servicios de hosting, por muchas razones, una de ellas es la cultura de "con ellos no tengo problemas".

- Excepto cuando un correo se pierde y no hay soporte.
- Excepto cuando alguien borra los correos y no hay soporte.
- Excepto cuando tu **ex** (socio, pareja, ...) secuestra la cuenta de tu empresa.
- Excepto cuando tienes un problema y **no hay soporte**.

El caso que nos ocupa es la modificación de [Exim](#) para cPanel, siguiendo sus especificaciones para construir una red de smarthosts para clientes con problemas.

“ Aunque está dedicada a cPanel y sus peculiaridades, es fácilmente trasladable a [Directadmin](#).

“ Editado el día 21/05/2025 Cambios debidos a la aparición de problemas por `message has lines too long for transport`. Tras revisarlo y dada la dificultad de testing se cambia de óptica en la configuración.

### Funcionamiento en cPanel

cPanel utiliza un script (`/usr/local/cpanel/3rdparty/bin/perl/buildeximconf`) que:

1. Lee el archivo `/etc/exim_cpanel/exim.conf.local`
2. Procesa todos los includes y configuraciones
3. Genera un nuevo `/etc/exim.conf` con toda la configuración consolidada
4. Verifica la sintaxis antes de aplicar los cambios
5. Si hay errores, mantiene la configuración anterior

Por esto es importante realizar los cambios en el editor de configuración de Exim en la pestaña **Avanzado** de WHM, ya que esto asegura que:

- La sintaxis es correcta
- Los includes se procesan adecuadamente
- La configuración es validada antes de aplicarse

# Introducción

cPanel utiliza un enfoque modular y eficiente para la configuración de smart relay, permitiendo definir rutas específicas por dominio y rutas por defecto, mientras mantiene la capacidad de excluir ciertos remitentes del enrutamiento inteligente. La configuración se divide en varios archivos dentro del directorio `/etc/exim_cpanel/`.

## Estructura de Archivos

### 1. Configuración Principal (`/etc/exim_cpanel/exim.conf.local`)

Para implementar los cambios en la configuración de Exim, hay dos métodos:

#### Método 1: A través de WHM (Recomendado)

1. Acceder a WHM
2. Ir a "Service Configuration" > "Exim Configuration Manager"
3. Seleccionar la pestaña "Advanced Editor"
4. Localizar la sección `ROUTERSTART` y añadir la configuración de abajo

```
.include_if_exists /etc/exim/routers.pre.conf
```

5. Localizar la sección `TRANSPORTSTART` y añadir la configuración de abajo

```
remote_smtp_dkim:  
  driver = smtp
```

```

hosts_require_tls = *
interface = ${if
exists{/etc/mailips}${lookup{$sender_address_domain}lsearch*/etc/mailips}{$value}{}}{}}
helo_data = ${if
exists{/etc/mailhelo}${lookup{$sender_address_domain}lsearch*/etc/mailhelo}{$value}{$primary
_hostname}}}{$primary_hostname}}
dkim_domain = ${perl{get_dkim_domain}}
dkim_selector = default
dkim_private_key = /var/cpanel/domain_keys/private/${dkim_domain}
dkim_canon = relaxed
message_linelength_limit = 998

```

6. Guardar los cambios

7. WHM ejecutará automáticamente la validación y reconstrucción de la configuración

## Método 2: Línea de comandos (Para administradores avanzados)

1. Editar directamente el archivo añadiendo los mismos datos en las mismas secciones como en el ejemplo de abajo:

```

vi /etc/exim_cpanel/exim.conf.local
@ROUTERSTART@
.include_if_exists /etc/exim/routers.pre.conf
@TRANSPORTEND@

@TRANSPORTMIDDLE@

@TRANSPORTSTART@
remote_smtp_dkim:
    driver = smtp
    hosts_require_tls = *
    interface = ${if
exists{/etc/mailips}${lookup{$sender_address_domain}lsearch*/etc/mailips}{$value}{}}{}}
    helo_data = ${if
exists{/etc/mailhelo}${lookup{$sender_address_domain}lsearch*/etc/mailhelo}{$value}{$primary
_hostname}}}{$primary_hostname}}
    dkim_domain = ${perl{get_dkim_domain}}
    dkim_selector = default
    dkim_private_key = /var/cpanel/domain_keys/private/${dkim_domain}
    dkim_canon = relaxed
    message_linelength_limit = 998

```

## 2. Ejecutar el script de reconstrucción:

```
/usr/local/cpanel/scripts/buildeximconf
```

4. Si hay errores, el script los mostrará y mantendrá la configuración anterior
5. Si todo es correcto, verás el mensaje: "Configuration file passes test! New configuration file was installed."

“ **IMPORTANTE:** El script `buildeximconf` no solo recompila la configuración, también:

- Verifica la sintaxis
- Actualiza la configuración DKIM
- Actualiza los permisos necesarios
- Reinicia los servicios relacionados si es necesario

## 2. Router Smart Routes ( `/etc/exim_cpanel/routers.pre.conf`)

Define el router para el enrutamiento inteligente:

```
smart_routes_router:
  driver = manualroute
  domains = !+local_domains
  transport = remote_smtp_dkim
  condition = ${if exists{/etc/exim/skip_smart_senders}\
    ${lookup{$sender_address_domain}nwildlsearch{/etc/exim/skip_smart_senders}{no}{yes}}\
    {yes}}
  route_list = *
  ${lookup{$domain}nwildlsearch{/etc/exim/smart_routes.txt}{$value}${lookup{*}nwildlsearch{/etc
/exim/smart_routes.txt}{$value}{}}}
  hosts_randomize = true
```

## 3. Smart Routes ( `/etc/exim_cpanel/smart_routes.txt`)

Archivo principal de rutas que combina rutas específicas y la ruta por defecto:

```
gmail.com: hetzner-xer08.domain.tld:hetzner-xer06.domain.tld:hetzner-xer01.domain.tld:hetzner-
xer02.domain.tld:hetzner-xer04.domain.tld
hotmail.com: hetzner-xer06.domain.tld:hetzner-xer07.domain.tld
hotmail.es: hetzner-xer06.domain.tld:hetzner-xer07.domain.tld
outlook.com: hetzner-xer06.domain.tld:hetzner-xer07.domain.tld
outlook.es: hetzner-xer06.domain.tld:hetzner-xer07.domain.tld
live.com: hetzner-xer06.domain.tld:hetzner-xer07.domain.tld
yahoo.com: hetzner-xer02.domain.tld:hetzner-xer03.domain.tld
yahoo.es: hetzner-xer02.domain.tld:hetzner-xer03.domain.tld

# Rutas específicas para dominios institucionales
policia.es: hetzner-xer11.domain.tld:hetzner-xer06.domain.tld

# Rutas específicas para clientes
amenabarobrasyproyectos.com: hetzner-xer01.domain.tld:hetzner-xer07.domain.tld

# Ruta por defecto para todos los demás dominios. Es necesario el wildcard
*: hetzner-xer11.domain.tld:hetzner-xer01.domain.tld:hetzner-xer06.domain.tld
```

“ el `#` funciona como comentario, por lo que se puede usar para activar o desactivar una ruta para un dominio particular

“ la existencia de `*` es necesaria. He realizado otras configuraciones más complejas, para evitarlo pero al final, siempre aparecen muchos problemas, para los que no tengo tiempo actualmente. Con esta, puedo garantizar el funcionamiento de todos los correos a dominios externos.

## 4. Exclusiones de Smart Routing (`/etc/exim_cpanel/skip_smart_senders`)

Define qué remitentes deben usar el routing estándar de Exim:

```
# Excluir solo el hostname completo del smart routing
servidor02.domain.tld

# Excluir algun dominio emisor en particular
```

# Diferencias con DirectAdmin

Puedes consultar como [Configuración de Smart Relay en DirectAdmin/Exim](#)

## 1. Estructura de Configuración

- DirectAdmin: Utiliza un único archivo con un router y un transporte
- cPanel: Sistema modular con includes condicionales

## 2. Granularidad

- DirectAdmin: Una configuración global para todos los dominios
- cPanel: Permite configurar rutas específicas y exclusiones

## 3. Flexibilidad

- DirectAdmin: Configuración más directa pero menos flexible
- cPanel: Sistema modular que permite activar/desactivar componentes

## 4. Balanceo de Carga

- DirectAdmin: Usa `hosts_randomize` para balanceo aleatorio
- cPanel: Balanceo implícito mediante lista de servidores por dominio

# Funcionamiento

## 1. Proceso de Enrutamiento

- Primero verifica si el remitente debe ser excluido (`skip_smart_senders`)
- Si no está excluido, busca una ruta específica para el dominio destino
- Si no encuentra ruta específica, usa la ruta por defecto (\*)

## 2. Redundancia y Balanceo

- Múltiples servidores pueden especificarse para cada ruta
- Balanceo mediante `hosts_randomize`
- Failover implícito al siguiente servidor en la lista

## 3. Exclusiones

- Sistema simple pero efectivo para excluir remitentes específicos
- Útil para correos del sistema y casos especiales

# Ventajas del Enfoque Modular

## 1. Control Granular

- Exclusión selectiva de remitentes
- Rutas específicas por dominio
- Ruta por defecto como fallback

## 2. **Mantenimiento Simple**

- Archivos independientes para cada función
- Cambios no requieren modificar la configuración principal de Exim
- Fácil activar/desactivar funcionalidades

## 3. **Robustez**

- Sistema de fallback en múltiples niveles
- Configuración a prueba de fallos
- Fácil diagnóstico y debugging

# Notas de Implementación

1. Los archivos deben tener permisos adecuados
2. El hostname en skip\_smart\_senders debe ser el FQDN exacto
3. Los cambios en las rutas no requieren reinicio del servicio
4. El orden de los servidores determina la prioridad de uso

Esta implementación ofrece mayor flexibilidad y control granular sobre el enrutamiento del correo saliente, aunque requiere más mantenimiento que la solución más simple de DirectAdmin.

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).



# MySQL: Error "No space left on device" en /tmp

## Síntomas del problema

Los usuarios reportan errores similares a estos en cPanel, phpMyAdmin y otras aplicaciones:

```
Can't create/write to file '/tmp/#sql_911_0.MAI' (Errcode: 28 "No space left on device")
Se experimentó un error mientras se obtenían los datos: Can't create/write to file
'/tmp/#sql_1234_0.MAI'
```

## Diagnóstico paso a paso

### Verificar espacio en disco

```
df -h

Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1        20G   8.5G   10G   46% /
tmpfs            2.0G   144K   2.0G    1% /tmp
```

Salida para indicar que todo es normal

### Verificar inodos (la causa real)

```
df -i

Filesystem      Inodes   IUsed   IFree IUse% Mounted on
/dev/sda1      1310720  145230 1165490   11% /
tmpfs           524288   524271     17  100% /tmp
```

**Observación:** La salida indica el agotamiento al 100% de los inodos.

### Identificar los archivos problemáticos

Al intentar listar `/tmp` con `ls`, obtendremos:

```
ls /tmp
-bash: /bin/ls: Argument list too long
```

Por eso utilizamos `find`:

```
find /tmp -maxdepth 1 -name 'sess*' | wc -l
```

Resultado atípico: `288789` (cientos de miles de archivos)

## Causa raíz

Acumulación masiva de archivos de sesión PHP (`sess_*`) que no se eliminan automáticamente, causando agotamiento de inodos en `/tmp`.

## Solución inmediata

```
find /tmp -maxdepth 1 -type f -name 'sess*' -delete
```

**¿Por qué usar find?** Porque `rm sess*` falla con "Argument list too long" cuando hay miles de archivos.

## Prevención

## Configuración automática de limpieza

Añadir al crontab de root:

```
# Limpieza diaria de archivos temporales antiguos (>24h)
0 3 * * * find /tmp -type f -name "sess_*" -mtime +1 -delete >/dev/null 2>&1
```

## Script para aplicar cambios PHP en todas las versiones de cPanel

**Contexto:** En cPanel cada versión PHP tiene su propio archivo de configuración:

```
/opt/cpanel/ea-php81/root/etc/php.ini
/opt/cpanel/ea-php82/root/etc/php.ini
/opt/cpanel/ea-php83/root/etc/php.ini
```

## Script automático para todas las versiones:

```
#!/bin/bash
# fix_php_gc_all_versions.sh
# Script para corregir configuración de garbage collector en todas las versiones PHP de cPanel

echo "=== Corrigiendo configuración PHP Garbage Collector ==="
echo "Fecha: $(date)"
echo

# Buscar todas las versiones de PHP instaladas de forma eficiente
PHP_VERSIONS=$(find /opt/cpanel -maxdepth 1 -name "ea-php*" -type d | grep -E "ea-php[0-9]+" |
sort -V)

if [ -z "$PHP_VERSIONS" ]; then
    echo "❌ No se encontraron versiones de PHP en cPanel (/opt/cpanel/ea-php*)"
    exit 1
fi

echo "Versiones de PHP encontradas:"
echo "$PHP_VERSIONS" | sed 's/.*ea-php/- PHP /' | sed 's/$//'
echo

for php_dir in $PHP_VERSIONS; do
    php_ini="$php_dir/root/etc/php.ini"
    version=$(basename "$php_dir" | sed 's/ea-php//')

    echo "--- Procesando PHP $version ---"

    if [ ! -f "$php_ini" ]; then
        echo "⚠️ No existe: $php_ini"
        continue
    fi

    # Crear backup
    cp "$php_ini" "$php_ini.backup.$(date +%Y%m%d_%H%M%S)"
```

```

echo "📁 Backup creado"

# Mostrar configuración actual
current_prob=$(grep -E "^session\.gc_probability\s*=" "$php_ini" | cut -d=' ' -f2 | tr -d '
')
current_div=$(grep -E "^session\.gc_divisor\s*=" "$php_ini" | cut -d=' ' -f2 | tr -d ' ')

echo "   Configuración actual: gc_probability=$current_prob, gc_divisor=$current_div"

# Aplicar cambios
sed -i 's/^session\.gc_probability\s*=.*\/session.gc_probability = 1/' "$php_ini"
sed -i 's/^session\.gc_divisor\s*=.*\/session.gc_divisor = 1000/' "$php_ini"

# Verificar cambios
new_prob=$(grep -E "^session\.gc_probability\s*=" "$php_ini" | cut -d=' ' -f2 | tr -d ' ')
new_div=$(grep -E "^session\.gc_divisor\s*=" "$php_ini" | cut -d=' ' -f2 | tr -d ' ')

echo "   Nueva configuración: gc_probability=$new_prob, gc_divisor=$new_div"
echo "   🔄 PHP $version actualizado"
echo
done

echo "=== Resumen ==="
echo "🔄 Cambios aplicados a todas las versiones PHP"
echo "⚠️ Los cambios se aplicarán en nuevas sesiones PHP"
echo

# Comando de verificación
echo "Verificar cambios:"
echo "grep -E 'session\.gc_(probability|divisor)' /opt/cpanel/ea-php*/root/etc/php.ini"

```

**Version actualizada** del script se mantiene en [Git Lab Castris - Utilidades](#)

### Uso del script:

```

chmod +x fix_php_gc_all_versions.sh
./fix_php_gc_all_versions.sh

```

# Análisis de la configuración PHP problemática

## Configuración actual encontrada en servidores cPanel:

```
session.gc_probability = 0      ; ▲ PROBLEMA: Numerador en 0
session.gc_divisor = 0          ; ▲ PROBLEMA: Denominador en 0
session.gc_maxlifetime = 1440  ; ☐ Correcto: 24 minutos (1440 segundos)
```

**Explicación del problema:** El garbage collector de PHP funciona con esta fórmula:

- Probabilidad de limpieza =  $gc\_probability / gc\_divisor$

Con la configuración actual:  $0 / 0 = \text{indefinido}$  → **Garbage collector completamente desactivado**

## Qué significa cada parámetro:

- `gc_probability`: Numerador de la probabilidad (cuántas veces de cada X)
- `gc_divisor`: Denominador de la probabilidad (el total X)
- `gc_maxlifetime`: Tiempo en segundos después del cual una sesión se considera "basura"

## Ejemplos de probabilidades:

- $1/100 = 1\%$  → 1 de cada 100 peticiones ejecuta limpieza
- $1/1000 = 0.1\%$  → 1 de cada 1000 peticiones ejecuta limpieza
- $0/0 = \text{desactivado}$  → Nunca se ejecuta limpieza automática

# Configuración PHP corregida

## Para servidores de producción (recomendado):

```
session.gc_probability = 1      ; Cambiar de 0 a 1
session.gc_divisor = 1000       ; Cambiar de 0 a 1000 (0.1% probabilidad)
session.gc_maxlifetime = 1440   ; Mantener actual
```

## Para servidores de desarrollo/bajo tráfico:

```
session.gc_probability = 1      ; Cambiar de 0 a 1
session.gc_divisor = 100        ; Cambiar de 0 a 100 (1% probabilidad)
session.gc_maxlifetime = 1440   ; Mantener actual
```

## Justificación de los valores:

- **Producción (1/1000):** Menor impacto en rendimiento, suficiente con alto tráfico
- **Desarrollo (1/100):** Mayor frecuencia de limpieza necesaria con poco tráfico

# Monitoreo de inodos

Script para alertas:

```
#!/bin/bash
#
# check_tmp_inodes.sh
# Checks the inode usage on /tmp and sends an alert if it exceeds a threshold.
#

# Ensure the script stops if any command fails
set -euo pipefail

# --- CONFIGURATION ---
# Path to the main configuration file
# Check repo for crons/.check_tmp_inodes.cfg file demo
# Not edit this file, copy the crons/.check_tmp_inodes.cfg file to /root/.check_tmp_inodes.cfg
CONFIG_FILE="/root/.check_tmp_inodes.cfg"

# --- FUNCTIONS ---

# Function to log errors and exit
# Usage: error_exit "Error message"
error_exit() {
    echo "ERROR: $1" >&2
    exit 1
}

# --- MAIN SCRIPT ---

# 1. Check if the configuration file exists and load it
if [ ! -f "$CONFIG_FILE" ]; then
    error_exit "Configuration file not found at $CONFIG_FILE"
fi
```

```

# Load variables from the configuration file
# shellcheck source=/dev/null
source "$CONFIG_FILE"

# 2. Verify that the necessary variables are defined
if [ -z "${EMAIL_TO-}" ] || [ -z "${THRESHOLD-}" ]; then
    error_exit "EMAIL_TO and THRESHOLD variables must be defined in $CONFIG_FILE"
fi

# 3. Get the current inode usage
# 'tail -n1' is used to be more robust on systems where 'df' might have more than 2 lines
USAGE=$(df -i /tmp | tail -n1 | awk '{print $5}' | sed 's/%//')

if ! [[ "$USAGE" =~ ^[0-9]+$ ]]; then
    error_exit "Could not retrieve a numeric value for inode usage. Got: '$USAGE'"
fi

# 4. Compare usage with the threshold and send an alert if necessary
echo "INFO: Current inode usage on /tmp: ${USAGE}% (Alert threshold: >${THRESHOLD}%)"

if [ "$USAGE" -gt "$THRESHOLD" ]; then
    # Build the message body
    HOSTNAME=$(hostname -f)
    BODY="ALERT on server: $HOSTNAME

Inode usage in the /tmp directory has exceeded the ${THRESHOLD}% threshold.

Current usage: ${USAGE}%

It is recommended to check the contents of /tmp to free up inode space.
"
    # Send the email
    echo "$BODY" | mail -s "$EMAIL_SUBJECT" "$EMAIL_TO"

    echo "ALERT: Threshold exceeded. Notification email sent to $EMAIL_TO."
else
    echo "INFO: Inode usage is within normal limits."
fi

exit 0

```

# Configuración de directorios temporales seguros

## Problema con la configuración actual

- `/home/user/tmp` → enlace simbólico a `/tmp` (cPanel)
- Todos los usuarios comparten el mismo espacio de inodos

## Solución recomendada

Configurar directorios temporales individuales:

```
// En configuración PHP por usuario
session.save_path = "/home/USERNAME/temporal"
upload_tmp_dir = "/home/USERNAME/temporal"
```

## Monitoreo continuo

## Comando para verificar estado actual

```
echo "Espacio: $(df -h /tmp | awk 'NR==2 {print $5}')"
echo "Inodos: $(df -i /tmp | awk 'NR==2 {print $5}')"
echo "Archivos sess: $(find /tmp -maxdepth 1 -name 'sess*' 2>/dev/null | wc -l)"
```

## Señales de alerta temprana

- Uso de inodos > 80% en `/tmp`
- Más de 10,000 archivos `sess_*`
- Quejas de usuarios sobre lentitud en aplicaciones web

---

**Severidad:** Crítica - Afecta disponibilidad de MySQL y aplicaciones web

**Impacto:** Todos los usuarios del servidor

**Tiempo de resolución:** 2-5 minutos con la solución inmediata



## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

# Bloqueo de Bad Bots en cPanel con ModSecurity usando el Sistema Vendor

## Introducción

Los **bad bots** representan una amenaza significativa para los **servidores web**, realizando miles de solicitudes no autorizadas que pueden comprometer la seguridad y el rendimiento del servidor. Este documento describe la implementación de un sistema automatizado de bloqueo de bad bots en cPanel utilizando **ModSecurity** y el sistema vendor nativo.

A diferencia de las soluciones tradicionales basadas en `.htaccess` que requieren mantenimiento manual y pueden generar inconsistencias entre diferentes servidores, esta solución aprovecha el sistema vendor de cPanel para automatizar completamente la gestión de reglas ModSecurity y actualizaciones de listas de bad bots.

## Diferencias con DirectAdmin

Mientras que en DirectAdmin se requiere configuración manual en el directorio

`/usr/local/directadmin/custombuild/custom/modsecurity/conf/`, cPanel ofrece un **sistema vendor** integrado que permite:

- Instalación automática de reglas ModSecurity
- Actualizaciones automáticas de configuraciones
- Gestión centralizada sin intervención manual
- Integración nativa con el sistema de gestión de cPanel

## Descripción del Sistema Castris ModSecurity

### Instalador one-click

Como root de un sistema con cPanel ejecutar:

```
curl -sSL https://gitlab.castris.com/root/utilidades/-
/raw/main/cpanel/castris_mod_security/install_castris_badbots.sh | bash
Castris Bad Bots ModSecurity Installer
=====

2025-07-05 06:56:34 - Starting Castris Bad Bots installation...
2025-07-05 06:56:34 - cPanel version detected: 11.110.0.68
SUCCESS: ModSecurity is available and loaded
2025-07-05 06:56:34 - SUCCESS: ModSecurity is available and loaded
2025-07-05 06:56:34 - Downloading Castris Bad Bots files from GitLab...
2025-07-05 06:56:34 - Downloading bot_list_management/update_badbot_list.sh...
SUCCESS: Downloaded bot_list_management/update_badbot_list.sh
2025-07-05 06:56:34 - SUCCESS: Downloaded bot_list_management/update_badbot_list.sh
2025-07-05 06:56:34 - Downloading bot_list_management/install_cron.sh...
SUCCESS: Downloaded bot_list_management/install_cron.sh
2025-07-05 06:56:34 - SUCCESS: Downloaded bot_list_management/install_cron.sh
2025-07-05 06:56:34 - Downloading bot_list_management/castris_badbots_list.txt...
SUCCESS: Downloaded bot_list_management/castris_badbots_list.txt
2025-07-05 06:56:34 - SUCCESS: Downloaded bot_list_management/castris_badbots_list.txt
SUCCESS: All files downloaded successfully
2025-07-05 06:56:34 - SUCCESS: All files downloaded successfully
2025-07-05 06:56:34 - Installing Castris Bad Bots cPanel vendor...
info [modsec_vendor] You have added the vendor "Castris".

[castris] Castris
  archive_url | https://gitlab.castris.com/root/utilidades/-
/raw/main/cpanel/castris_mod_security/vendor_package/castris-badbots-v1.0.0.zip
  description | Castris Bad Bots ModSecurity Blocker
  dist_md5 | bcf790fd90f757cd2ad780b76418dba5
  dist_sha512 |
39593fa919723094ff4fe86725f956a334465c1a029bfff2621cc354c83c579c152ce645b3e88841a1d56a0b39e39a
8c3dd814754d03b8aac162e329d4691db3
  distribution | castris-badbots-01
  enabled | 1
  inst_dist | castris-badbots-01
  installed | 1
  installed_from | https://gitlab.castris.com/root/utilidades/-
/raw/main/cpanel/castris_mod_security/vendor_package/meta_castris.yaml
  is_pkg |
meta_vendor_cache_file | /var/cpanel/modsec_vendors/meta_castris.cache
```

```
meta_yaml_file | /var/cpanel/modsec_vendors/meta_castris.yaml
               | name | Castris
               | path | /etc/apache2/conf.d/modsec_vendor_configs/castris
progress_bar |
report_url |
supported_versions | (3)
               | vendor_id | castris
               | vendor_url | https://castris.com
```

SUCCESS: Vendor added successfully

2025-07-05 06:56:35 - SUCCESS: Vendor added successfully

info [modsec\_vendor] You have enabled the vendor "castris".

SUCCESS: Vendor enabled successfully

2025-07-05 06:56:35 - SUCCESS: Vendor enabled successfully

2025-07-05 06:56:35 - Installing bot list management system...

2025-07-05 06:56:35 - Starting Castris Bad Bots cron installation...

SUCCESS: Update script found and executable

2025-07-05 06:56:35 - SUCCESS: Update script found and executable

2025-07-05 06:56:35 - Installing weekly cron job for bad bots list update...

SUCCESS: Cron job installed: /etc/cron.d/castris-badbot-update

2025-07-05 06:56:35 - SUCCESS: Cron job installed: /etc/cron.d/castris-badbot-update

2025-07-05 06:56:35 - Restarting cron service...

SUCCESS: Cron service restarted

2025-07-05 06:56:35 - SUCCESS: Cron service restarted

2025-07-05 06:56:35 - Testing cron installation...

WARNING: Cron syntax test failed (this might be normal on some systems)

2025-07-05 06:56:35 - WARNING: Cron syntax test failed (this might be normal on some systems)

SUCCESS: Cron installation test passed

2025-07-05 06:56:35 - SUCCESS: Cron installation test passed

2025-07-05 06:56:35 - Running initial bad bots list update...

2025-07-05 06:56:35 - Starting Castris Bad Bots List update...

2025-07-05 06:56:35 - Downloading new bad bots list from:

[https://raw.githubusercontent.com/mitchellkrogza/apache-ultimate-bad-bot-blocker/master/\\_generator\\_lists/bad-user-agents-htaccess.list](https://raw.githubusercontent.com/mitchellkrogza/apache-ultimate-bad-bot-blocker/master/_generator_lists/bad-user-agents-htaccess.list)

SUCCESS: Downloaded from primary URL

2025-07-05 06:56:36 - SUCCESS: Downloaded from primary URL

SUCCESS: New bad bots list installed

2025-07-05 06:56:36 - SUCCESS: New bad bots list installed

2025-07-05 06:56:36 - New list contains 515 entries

```
2025-07-05 06:56:36 - Testing Apache configuration...
SUCCESS: Apache configuration test passed
2025-07-05 06:56:36 - SUCCESS: Apache configuration test passed
2025-07-05 06:56:36 - Reloading Apache configuration...
SUCCESS: Apache configuration reloaded
2025-07-05 06:56:38 - SUCCESS: Apache configuration reloaded
2025-07-05 06:56:38 - Statistics:
2025-07-05 06:56:38 - - Previous list: 0 entries
2025-07-05 06:56:38 - - New list: 515 entries
2025-07-05 06:56:38 - - Change: 515 entries
SUCCESS: Bad bots list update completed successfully
2025-07-05 06:56:38 - SUCCESS: Bad bots list update completed successfully
SUCCESS: Initial update completed successfully
2025-07-05 06:56:38 - SUCCESS: Initial update completed successfully
```

```
=====
Castris Bad Bots Cron Installation
=====
```

Installation completed successfully!

#### Configuration:

- Update script: /usr/local/bin/castris/update\_badbot\_list.sh
- Cron file: /etc/cron.d/castris-badbot-update
- Log file: /var/log/castris\_cron\_install.log
- Schedule: Every Sunday at 2:00 AM

#### Manual commands:

- Run update now: /usr/local/bin/castris/update\_badbot\_list.sh
- Check cron logs: tail -f /var/log/castris\_badbot\_update.log
- Remove cron: rm -f /etc/cron.d/castris-badbot-update && systemctl restart cron

The bad bots list will be automatically updated weekly.

Check the logs for update status and statistics.

```
SUCCESS: Castris Bad Bots cron installation completed
2025-07-05 06:56:38 - SUCCESS: Castris Bad Bots cron installation completed
SUCCESS: Bot list management system installed
2025-07-05 06:56:38 - SUCCESS: Bot list management system installed
2025-07-05 06:56:38 - Testing installation...
SUCCESS: Apache configuration test passed
```

2025-07-05 06:56:38 - SUCCESS: Apache configuration test passed

SUCCESS: Vendor installation verified

2025-07-05 06:56:38 - SUCCESS: Vendor installation verified

=====  
Castris Bad Bots Installation Complete!  
=====

- cPanel ModSecurity vendor installed
- Bot list management system installed
- Apache configuration validated

#### TESTING:

Test the installation with:

```
curl -H 'User-Agent: BadBot' http://yourserver.com/
```

(Should return 406 Not Acceptable)

#### MANAGEMENT:

- Update bot list: /usr/local/bin/castris/update\_badbot\_list.sh
- Check vendor: /scripts/modsec\_vendor list
- Disable vendor: /scripts/modsec\_vendor disable castris
- Remove vendor: /scripts/modsec\_vendor remove castris

#### LOGS:

- Installation: /var/log/castris\_badbots\_install.log
- Bot updates: /var/log/castris\_badbot\_update.log
- ModSecurity: /usr/local/apache/logs/modsec\_audit.log

The system will automatically update bad bots lists weekly.

Check cron with: cat /etc/cron.d/castris-badbot-update

SUCCESS: Installation completed successfully!

2025-07-05 06:56:38 - SUCCESS: Installation completed successfully!

“ Abajo esta la descripción técnica de todo el trabajo, y en mi [Gitlab el resto](#) Es público.

## Arquitectura del Paquete

El sistema está compuesto por tres componentes principales:

## 1. Vendor Package

- `meta_castris.yaml`: Configuración del vendor que define las URLs de descarga y metadatos
- `00_castris_badbots.conf`: Reglas ModSecurity optimizadas con IDs únicos (1090901-1090905)
- `castris-badbots-v1.0.0.zip`: Paquete ZIP que cPanel descarga automáticamente

## 2. Bot List Management

- `update_badbot_list.sh`: Script de actualización semanal de listas
- `install_cron.sh`: Instalador automatizado del cron
- `castris_badbots_list.txt`: Lista inicial de bad bots conocidos

## 3. Instalador Automático

- `install_castris_badbots.sh`: Script principal que orquesta toda la instalación
- `pre_install_setup.sh`: Script de verificación de prerequisites (opcional)

# Funcionamiento del Sistema Vendor

El sistema vendor de cPanel permite que las reglas ModSecurity se gestionen automáticamente:

1. **Descarga Automática:** cPanel descarga el ZIP desde la URL especificada en `meta_castris.yaml`
2. **Inyección de Reglas:** Las reglas se instalan automáticamente en `/etc/apache2/conf.d/modsec_vendor_configs/castris/`
3. **Actualización Transparente:** Los cambios se aplican sin intervención manual
4. **Persistencia:** Las configuraciones sobreviven a actualizaciones de cPanel

# Reglas ModSecurity Implementadas

**ID 1090901:** Bloqueo principal basado en User-Agent

- Utiliza `@pmFromFile` para comparar contra la lista de bad bots
- Respuesta HTTP 406 (Not Acceptable)
- Logging completo para monitoreo

**ID 1090902:** Bloqueo de User-Agent vacío

- Detecta solicitudes sin User-Agent
- Protección contra herramientas automatizadas básicas

**ID 1090903:** Detección de patrones sospechosos

- Identifica comportamientos anómalos en headers
- Análisis de patrones de solicitudes sospechosas

#### **ID 1090904:** Rate limiting avanzado

- Límite de 100 solicitudes por hora por IP
- Prevención de ataques de fuerza bruta

#### **ID 1090905:** Inicialización de contadores

- Gestión de estado para rate limiting
- Optimización de memoria y rendimiento

# Proceso de Instalación

## Instalación Automática

El script `install_castris_badbots.sh` realiza las siguientes operaciones:

### 1. Verificación de Prerrequisitos

- Comprueba que cPanel esté instalado y funcionando
- Verifica que ModSecurity esté habilitado
- Valida permisos de administrador

### 2. Descarga de Componentes

- Descarga únicamente los archivos necesarios desde GitLab
- Verifica integridad mediante checksums
- Maneja fallos de conectividad con URLs de respaldo

### 3. Instalación del Vendor

```
/scripts/modsec_vendor add https://gitlab.castris.com/root/utilidades/-  
/raw/main/cpanel/castris_mod_security/vendor_package/meta_castris.yaml  
/scripts/modsec_vendor enable castris
```

### 4. Configuración de Actualizaciones

- Instala cron para actualizaciones semanales (domingos 2:00 AM)
- Configura logs de actualización en `/var/log/castris_badbot_update.log`
- Establece URLs primarias y de respaldo para listas

### 5. Validación del Sistema

- Prueba reglas con User-Agents conocidos
- Verifica logs de ModSecurity
- Confirma respuestas HTTP correctas

### 6. Limpieza

- Elimina archivos temporales de instalación
- Optimiza configuraciones de Apache



- Reinicia servicios solo si es necesario

# Gestión de Listas de Bad Bots

El sistema mantiene actualizadas las listas de bad bots mediante:

## Fuentes de Datos

- **Primaria:** `https://download.castris.com/badbots/castris_badbots_list.txt`
- **Respaldo:** GitHub Apache Ultimate Bad Bot Blocker

## Actualización Automática

- Ejecución semanal vía cron
- Respaldo automático de listas anteriores
- Logging detallado de cambios y estadísticas
- Reinicio automático de Apache solo cuando es necesario

## Gestión de Fallos

- Fallback automático a URLs de respaldo
- Conservación de listas anteriores en caso de fallo
- Alertas en logs para problemas de conectividad

# Archivos de Configuración

## Estructura en el Servidor

```
/etc/apache2/conf.d/modsec_vendor_configs/castris/
├─ 00_castris_badbots.conf          # Reglas ModSecurity

/usr/local/apache/conf/modsec2/
├─ castris_badbots_list.txt         # Lista activa de bad bots
├─ castris_badbots_list.txt.backup  # Respaldo de la lista anterior

/etc/cron.d/
├─ castris-badbot-update            # Cron de actualización semanal

/var/log/
├─ castris_badbot_update.log        # Logs de actualizaciones
```

# Configuración del Cron

```
# Actualización semanal domingos 2:00 AM
0 2 * * 0 root /usr/local/bin/castris/update_badbot_list.sh >>
/var/log/castris_badbot_update.log 2>&1
```

## Monitoreo y Validación

### Testing del Sistema

```
# Estos comandos DEBEN devolver 406 Not Acceptable
curl -H 'User-Agent: BadBot' http://yourserver.com/
curl -H 'User-Agent: nikto' http://yourserver.com/
curl -H 'User-Agent: wget' http://yourserver.com/

# Este comando DEBE funcionar normalmente (200 OK)
curl -H 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36'
http://yourserver.com/
```

## Análisis de Logs

```
# Ver bloqueos en tiempo real
tail -f /usr/local/apache/logs/modsec_audit.log | grep 1090901

# Estadísticas de bloqueos
grep "1090901" /usr/local/apache/logs/modsec_audit.log | wc -l

# Top bots bloqueados
grep "1090901" /usr/local/apache/logs/modsec_audit.log | \
grep -o 'User-Agent: [^"]*' | sort | uniq -c | sort -nr | head -10
```

## Monitoreo de Actualizaciones

```
# Logs de actualización de listas
tail -f /var/log/castris_badbot_update.log
```

```
# Verificar última actualización  
grep "Statistics:" /var/log/castris_badbot_update.log | tail -5
```

# Consideraciones de Seguridad

## Ventajas del Sistema

- **Automatización Completa:** Sin intervención manual requerida
- **Actualizaciones Regulares:** Listas actualizadas semanalmente
- **Persistencia:** Configuraciones que sobreviven a actualizaciones del sistema
- **Monitoreo:** Logging detallado para análisis forense
- **Fallback:** Múltiples fuentes de datos para alta disponibilidad

## Precauciones

- **Falsos Positivos:** Monitorear que no se bloquee tráfico legítimo
- **Impacto en Rendimiento:** Las reglas son optimizadas pero requieren monitoreo
- **Conectividad:** Dependencia de URLs externas para actualizaciones
- **Logs:** Gestión del crecimiento de archivos de log

# Mantenimiento y Solución de Problemas

## Verificación de Estado

```
# Verificar vendor habilitado  
/scripts/modsec_vendor list  
  
# Verificar ModSecurity cargado  
httpd -M | grep security2  
  
# Verificar archivos de configuración  
ls -la /etc/apache2/conf.d/modsec_vendor_configs/castris/
```

## Solución de Problemas Comunes

## Apache no inicia

```
# Verificar sintaxis de configuración
httpd -t

# Revisar logs de error
tail -f /usr/local/apache/logs/error_log
```

## Reglas no funcionan

```
# Verificar lista existe
ls -la /usr/local/apache/conf/modsec2/castris_badbots_list.txt

# Verificar permisos
chmod 644 /usr/local/apache/conf/modsec2/castris_badbots_list.txt
```

## Actualizaciones fallan

```
# Ejecutar actualización manual con debug
bash -x /usr/local/bin/castris/update_badbot_list.sh

# Verificar conectividad
curl -I https://download.castris.com/badbots/castris_badbots_list.txt
```

# Desinstalación Completa

```
# Deshabilitar y remover vendor
/scripts/modsec_vendor disable castris
/scripts/modsec_vendor remove castris

# Eliminar cron
rm -f /etc/cron.d/castris-badbot-update
systemctl restart cron

# Limpiar archivos
rm -rf /usr/local/bin/castris
rm -f /usr/local/apache/conf/modsec2/castris_badbots_list.txt*
rm -f /var/log/castris_*.log
```

```
# Reiniciar Apache
systemctl restart httpd
```

# Conclusiones

Este sistema representa una evolución significativa en la gestión de bad bots para cPanel, ofreciendo automatización completa y mantenimiento mínimo. La integración con el sistema vendor nativo de cPanel garantiza persistencia y compatibilidad a largo plazo, mientras que las actualizaciones automáticas de listas mantienen la protección actualizada contra nuevas amenazas.

La implementación de reglas ModSecurity optimizadas con IDs únicos evita conflictos con otras configuraciones, y el sistema de monitoreo integral permite análisis detallado del tráfico bloqueado y la efectividad del sistema.

# Recursos Adicionales

- **Código fuente:** [https://gitlab.castris.com/root/utilidades/-/tree/main/cpanel/castris\\_mod\\_security](https://gitlab.castris.com/root/utilidades/-/tree/main/cpanel/castris_mod_security)
- **Documentación técnica:** Incluida en el README.md del repositorio
- **Soporte:** <https://castris.com>
- **Lista de bad bots:** Basada en Apache Ultimate Bad Bot Blocker

# Disclaimer

Esta herramienta se proporciona tal como está para propósitos de seguridad. Los administradores son responsables de probar y validar la configuración en su entorno antes del despliegue en producción. Se recomienda revisar el código fuente antes de ejecutar scripts de instalación automática.

## Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).