

# Tips de Directadmin

- [Como ejecutar tu acceso a mysql en un Directadmin sin usar root](#)
- [Desactivar el acceso público a PhpMyAdmin en Directadmin](#)
- [Tips rápidos de Directadmin](#)
- [ModSecurity en DirectAdmin](#)
- [DKIM, SPF y DMARC para el hostname de un servidor con Directadmin](#)
- [PHP en shell para usar wp cli en DirectAdmin](#)
- [Limpieza de mysql tras una migración: permisos de host antiguos](#)
- [Activar DKIM a todos los dominios de un servidor con Directadmin](#)
- [Mod Security. Desactivación global de reglas por path](#)
- [Reconstrucción del indice Full Text Search \(FTS\) en cuentas de correo :: Dovecot](#)
- [Cambio el doc root de un dominio en DirectAdmin](#)
- [Donde está la configuracion básica del servidor con Directadmin](#)
- [Cambios especificados en el php.ini disable\\_functions por dominio](#)
- [Git desde DirectAdmin Interface](#)
- [Como bloquear los Bad bots \(Bot basura\) usando ModeSecurity en Directadmin nueva](#)
- [Wordpress Manager de Directadmin y wp cli problemas de memoria](#)
- [Configurar PHP en un servidor con Directadmin](#)
- [Configuración de Smart Relay en DirectAdmin/Exim](#)
- [Redis: Rotura de WordPress por error de Redis en Directadmin](#)

# Como ejecutar tu acceso a mysql en un Directadmin sin usar root

## Introducción Mysql password en Directadmin

Muchos estamos habituados al uso de un `.my.cnf` en nuestro usuario para acceder como `root` a mysql.

En el caso de **Directadmin** la instalación por defecto no autroiza a root con el uso de sockets, si no que es una instalación personalizada, en la que el usuario que tiene privilegios globales se llama `da_admin` y tiene su contraseña guardada en `/usr/local/directadmin/conf/mysql.conf`

Si no queremos añadir otro usuario y conservar este sistema, podemos usar este comando (o generar un alias para usarlo ;-)

```
mysql -u da_admin -p$(grep 'passwd' /usr/local/directadmin/conf/mysql.conf | awk -F= '{print $2}')
```

## Alternativa .my.cnf

La otra es la de siempre, si confias en ella que en realidad es mas segura que pasar un password por un script, que es editar el fichero `/root/.my.cnf`

```
[client]
user=da_admin
password=PasswordObtenidodelFecijeroDeConfiguracion
```

“ En ese caso tendras que podres hacer `sudo mysql xxxx`

## 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](#).

# Desactivar el acceso público a PhpMyAdmin en Directadmin

## Introducción

Nunca me ha gustado tener phpMyAdmin activo en mis servidores, pero es algo inevitable. Lo usuarios no tiene porque saber acceder a mysql para hacer ciertas cosas, y además el 99% de los super tutoriales para hacer cosita estan basados en esa herramienta.

Pero eso sin, lo que no nunca permito es el acceso directamente. Al mnso que el phpMyAdmin goce de la capa de protección adicional de estar logeado en el cpanel.

Eso supone que si tienes un desarrollador web, que lo neccita y no le quieres dar acceso, un par de cosas:

- Un desarrollador de verdad, no necesita acceso a phpMyadmin
- Un desarrllador de verdad, no necesita acceso remoto via 3306 (puerto de mysql el cual tambien suelo capar) sino acceso SSH para acceder via tunel

“ Si de verdad necesitas trabajar como desarrllador sobre mysql te recomiendo usar [Mysql sobre SSH](#)

## Desactivar el acces público de phpMyAdmin en Directadmin

Versión en el momento de escribir el artículo: 1.666

[Quiero que todo el acceso a /phpMyAdmin sea accesible solo a través de DirectAdmin.](#)

```
da build set phpmyadmin_public no
```

```
da build phpmyadmin
```

# Inicio de sesión SignOn en PhpMyAdmin

[Inicio de sesión con un solo clic \(Single SignOn\) a PHPMyAdmin](#)

## 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](#).

# Tips rápidos de Directadmin

## Introducción

Algunas veces las cosas son difíciles por la confusión generada en la propia documentación de lo que usamos.

Y esto puede llevarnos a la desesperación.

Aquí te dejo trucos y si tienen modificación tras alguna nueva versión con su versión desde la cuál se comprobó. El documento se empezó en julio de 2024 con la [versión 1.6.6](#)

“ Lo pongo en inglés el tablero porque jamás uso el español como idioma en el software, ya que los mejores manuales y tutoriales esta en el idioma de **Sakespeare** ☹️.

Después de cualquier modificación que queramos que sea aplicada debemos hacer un restart de DirectAdmin `systemctl restart directadmin`

**Última actualización: 7/08/2024 18:00 GMT +2**

## Índice

- [Apuntes sobre Let's Encrypt For Services en la documentación oficial de DirectAdmin](#)
- [Actualizar la cuota de una cuenta de correo](#)
- [Cambia el email del admin](#)
- [Cambio del hostname](#)
- [Cambia valores de configuración de Directadmin en el shell](#)
- [Cloudflare para el tablero o panel de control Directadmin](#)
- [Composer en Directadmin](#)
- [Let's encrypt para dominios que han fallado](#)
- [Valores por usuario en el user.conf](#)

- [Webmail impresionation - OneClick](#)
- [directadmin license-expired](#)

# Apuntes sobre Let's Encrypt For Services en la documentación oficial de DirectAdmin

[Let's Encrypt For Services](#)

## Actualizar la cuota de una cuenta de correo

Muchas veces el usuario cambia o purga el contenido de sus cuentas de correo y los cambios no se ven reflejados inmediatamente en Directadmin.

Esto es frustrante para el usuario y para el técnico de soporte.

Las cuotas no son algo instantaneo, y se ejecutana cada cierto tiempo, y son globales, lo que hace que el tiempo es largo. Ademas de que generalmente esas cosas se hacen de noche y observando algunas pautas apara evitar sobrecargas.

Podemos actualizar los datos de un cliente con este comando de Devecot [doveadm quota recalc](#)

```
doveadm quota recalc -u user@domain.ltd
```

Después podemos verificar con:

```
doveadm quota get -u user@domain.ltd
```

Quota name	Type	Value	Limit	%
STORAGE	0	-		0
MESSAGE	0	-		0

## Cambia el email del admin

Vía rápida por SSH

Editando el fichero `/usr/local/directadmin/data/users/admin/user.conf` la variable `email=` y haciendo un restart de `directadmin`

```
systemctl restart directadmin
```

“ Igual tienes que revisar el CSF para las notificaciones

Vía tablero en `Dashboard > User Profile > General`

- [Change admin email?](#)

## Cambio del hostname y forzar certificado de hostname

En principio uno pensaría que con cambiar el **hostname** en el `Tablero > Admin > Server Manager > Administrator Settings > Server Settings` se producirían todas las acciones necesarias.

Pues no. Y además, si buscas, puede que lo encuentres a la primera pero puede que comiences un viaje a ninguna parte. [Hostname change does not work properly.](#)

Aquí te lo dejo mas formalito, y se entiende que `hostname -f` te resuelve el Hostname que tu quieres y tienes ya configurado para resuelva a tu servidor.

```
/usr/local/directadmin/scripts/letsencrypt.sh server_cert `hostname -f`
```

## Cambia valores de configuración de DirectAdmin en el shell

En la documentación tenemos [todos los valores de configuración de Directadmin](#) que puedes manejar en el shell.

Algunos de los son muchísimo más prácticos que ir buscando por su tablero de mandos.

Se cambian con:

```
da config-set variable value  
systemctl restart directadmin
```



O también con

```
/usr/local/directadmin/directadmin config-set variable value  
systemctl restart directadmin
```

Si quieres buscar alguno o un grupo por palabra que buenbo usar `grep`

```
cat /usr/local/directadmin/conf/directadmin.conf | grep dkim  
dkim=2
```

Hay variables que no funcionan con `da config-set` y hay que editarlas manualment.

“ A veces es mucho más práctico conocer la variable que ir buscando por el tablero

## Cloudflare para el tablero o panel de control

Interesante usar el tablero en otro puerto (por imperativo de Cloudflare) pero muy interesante para evitar un buen porcentaje de bobos haciendo pruebas contra tu panel.

Habilita el modo Cloudflare en tu registro que apunta a tu máquina, y comienza a funciona por el puerto 2096

```
da config-set port 2096  
› systemctl restart directadmin
```

“ Si tras hacer el cambio, tu panel de control Directadmin hace **parpadeo** (blinking,) elimina en las **herramientas del desarrollador** (Webmaster Tools), todo lo que hay en **Almacenamiento** y vuelve a hacer login.

## Composer en Directadmin

Por defecto no esta instalado, **composer v2** en **Directadmin**

```
da build composer
```

# Let's Encrypt para dominios que han fallado al crearse (SSL)

A veces puede darse que falle la creación de los certificados de un dominio. Mejor que perder el tiempo en el tablero lo podemos solventar via terminal

```
domain=domain.tld  
/usr/local/directadmin/scripts/letsencrypt.sh request $domain 4096
```

1. Entendemos `domain.tld` como un fake que debemos sustituir.
2. El dominio ya resuelve de forma global a nuestra máquina.

[Let's Encrypt For Domains](#)

## Valores por usuario en el `user.conf`

Muchas veces es posible que deseemos no estar tan limitados a los valores globales o aplicados por cuestión de un plan, o de los valores del usuario en la administración. Incluso hay valores que no están reflejados en el panel de administración, como puede ser el caso de la limitación del número de correos por usuario.

En este caso, entra en funcionamiento el `override` o `sobrescritura` de los valores de configuración, que podemos ejecutar ya sea con la edición del fichero

`/usr/local/directadmin/data/users/<USER>/user.conf` o con el uso de la API.

## Cambio del `max_per_email_send_limit` por usuario

Un ejemplo es el de cambiar el valor máximo que limita el envío de correos por día, algo muy útil en el entorno de hosting para evitar entrar en listas de spam, ya sea porque han hackeado una cuenta, un script abierto sin protección, etc.

En este caso, para permitir a un usuario saltarse el límite para una cuenta en concreto (atención, él podrá aplicar esto a todas sus cuentas, y lo lamento, pero hay mucho espabilado, así que tendréis que tener un mecanismo de vigilancia de su uso).

El cambio de forma global autorizaría a todos los usuarios al uso del máximo, en todas las cuentas configuradas como máximo en ese valor. Sin embargo, si lo hacemos modificando el fichero

`/usr/local/directadmin/data/users/<USER>/user.conf` añadiendo `max_per_email_send_limit=VALUE` y haciendo un restart del servicio de **Directadmin**, el usuario podría en todas sus cuentas añadir dicho límite.

## Webmail impresionation o OneClick

Para administradores y resellers, se puede realizar un impersonation, o como llaman en Directadmin, OneClick, para que el administrador puede acceder al roundcube. Información adicional: [One-Click login to RoundCube](#)

```
da config-set one_click_webmail_login 1
systemctl restart directadmin
da build dovecot_conf
da build exim_conf
da build roundcube
```

“ Sobre la discusión de la legalidad de esta acción, muchos parecen olvidar que el hoster, ya en su contrato (si se hizo correctamente) es el responsable de la custodia de los datos, y por la naturaleza de sus credenciales, está habilitado a ver todo. Si bien no de forma directa, sí puede verlo desde el shell. Así pues, en ese contrato, de responsabilidad, queda implícito que existe un total acceso a los datos de los clientes, suscrito a la profesionalidad y la confidencialidad, limitándose esos accesos a los estrictamente necesarios, para el buen funcionamiento del servicio.

## directadmin license-expired

Aquí hablamos de un escenario, en el que en realidad el problema estaba relacionado con una sobre carga de tareas del **Directadmin** que se pueden ver con `journalctl -u directadmin`, pero esta página del manual de directadmin es muy interesante.

[License expired](#) sobre todo, por que encontraremos el comando para refrescar la licencia en [Permanent license error 'invalid license key'](#)

Así que en realidad, aquí tenemos información para muchas situaciones diferentes que afectan al sistema de licencia 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 se entrega, tal y como está, sin que ello implique ninguna obligación ni responsabilidad por parte de [Castris](#)

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

# ModSecurity en DirectAdmin

## Introducción

El uso de ModSecurity esta altamente recomendado. El software eactual, y mas con la proliferación de **expertos** en javascript o creadores de **temas** y **plugins** hacen más que necesaria una capa adicional de seguridad en la llamadas al servidor web.

## ModSecurity en Directadmin con owasp

En mi caso opto siempre por owasp.

[ModSecurity Documentación para Directadmin](#)

Algunos tips.

- Al principio es una pesadilla, pero lo mejor es no desactivar pro defecto. Es lo que hacen el 99% de los hosters que **no quieren lios** con sus clientes, pero luego sus clientes mueren una y otra vez de hackeos, inyecciones de código malicioso, y problemas de seguridad.
- Si alguna **regla** (rule ID) la tienes clara y documentada, puede desactivarla en el manager de ModSecurity que esta accesible en `/evo/admin/modsecurity`
- Esas reglas son globales, es decir las desactivas para todo el mundo, asi que ten muy claro que las desactivas por es necesario.

“ Muchas reglas son necesarias para determinado templates famosos, crm y plugins que son famosos, y pese a ello, una autentica verguenza de codificación. Queda en tú política el permitirlo de forma global o obligar al usuario a que el actualice sus reglas haciendose responsable de su seguridad.

## 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, SPF y DMARC para el hostname de un servidor con Directadmin

## Introducción

La importancia de tener al día y configurado un servidor y su **hostname** es crucial, para que el correo emitido por el servidor como tal (alertas, mensjaes al usuario, etc) y la fiabilidad del propio servidor es crucial.

Por el ello uno de los grandes olvidados es tener el SPF, DKIM, y DMARC para el `hostname`

## Proceso de creación de los reegistros SPF, DKIM y DMARC en un host con Directadmin

### Creación de la zona

Con indipendencia de si el hostname esta controlado por un dominio cuyo sistema de resolución es distinto al de la maquina, ya sea por DNS locales o por un cluster externo, o por un proveedor externo como Cloudflare, debemos crear una zona para el hostanme en el tablero.

### SPF

Si lo tienes correctamente configurado (te aconsejo que pases por la documentación [All Directadmin Conf Values](#) ya que si esta configurado el lo creara automaticamente



Si lo configuras tambien puedes modificar los valores por defecto, muy útil cuando tenemos servidores de correo de relay, etc.

Para ello además de la configuración hay que crear un fichero

```
/usr/local/directadmin/data/templates/custom/dns_txt.conf
```

```
|DOMAIN|.="v=spf1 a mx ip4:|SERVER_IP||EXTRA_SPF||SPF_IPV6| -all"
```

## DKIM

EL DKIM lo podremos crear ahora que ya existe la zona, con:

```
/usr/local/directadmin/scripts/dkim_create.sh `hostname -f`
```

Esto generará la entrada adecuada en el fichero de zona del hostname.

## DMARC

Procederemos a editar el fichero anterior `/usr/local/directadmin/data/templates/custom/dns_txt.conf` para **añadir** el registro `_dmarc`

```
_dmarc="v=DMARC1; p=none; sp=none;"
```

Ahora nuestro fichero tendrá algo así:

```
|DOMAIN|.="v=spf1 a mx ip4:|SERVER_IP||EXTRA_SPF||SPF_IPV6| -all"  
_dmarc="v=DMARC1; p=none; sp=none;"
```

“ NO es el alcance de este tutorial el explicar si usar o no usar **rua** en el registro, y lo que dice Google y lo que dice Microsoft.

Edición de la zona en el Tablero de Directadmin

# Proceso adicional si el sistema de DNS no es el del servidor

Si como suele ser habitual, el control de DNS del hostname no es una DNS local o del cluster deberemos abrir el fichero de zona, ya sea en el Tablero de Directadmin o en el shell, para copiar el contenido de estos registro de zona y copiar en la zona del dns que controla el dominio del

hostname.

## 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](#).



# PHP en shell para usar wp cli en DirectAdmin

## Introducción

En este caso y para facilitar las cosas a los usuarios de Directadmin, en el que como norma general se instalan distintas versiones de PHP y la principal del servidor puede ser incompatible con nuestras necesidades es mejor usar la que necesitamos.

“ Aunque este tip es para DirectAdmin, vale para cualquier distribución Linux o \*nix. adaptando el tip a tu SO

[PHP en shell para usar wp cli - Version cPanel](#)

## Ejemplo

```
wp core update && wp plugin upgrade --all && wp theme upgrade --all
Fatal error: __autoload() is no longer supported, use spl_autoload_register() instead in
/home/user/public_html/wiki.dominio.com/wp-includes/compat.php on line 502

php -v
PHP 7.2.34 (cli) (built: Mar 28 2023 21:20:00) ( NTS )
Copyright (c) 1997-2018 The PHP Group
Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies
    with the ionCube PHP Loader + ionCube24 v10.4.5, Copyright (c) 2002-2020, by ionCube Ltd.
    with Zend OPcache v7.2.34, Copyright (c) 1999-2018, by Zend Technologies
```

El usuario tiene una versión correcta en la que todavía no estaba declarada obsoleta la función `__autoload()`

Si estamos como usuario

```
$ which php
/usr/local/php74/bin/php
$ which wp
/usr/local/bin/wp
```

Ahora solo nos queda llamar al wp-cli de forma adecuada `74` es la versión que queremos usar `/usr/local/bin/wp` es el path de instalación global de la herramienta wp

```
/usr/local/php74/bin/php /usr/local/bin/wp core update
```

## Tip

Esto podemos añadirlo a nuestro fichero de configuración del shell usado.

Por ejemplo y para el caso de que tengamos mas de un sitio web con distintos requerimientos mejor usar este formato

```
wp74="/usr/local/php74/bin/php /usr/local/bin/wp"
wp82="/usr/local/php82/bin/php /usr/local/bin/wp"
```

## 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](#).

# Limpieza de mysql tras una migración: permisos de host antiguos

## Introducción

Cuando se realizan migraciones entre servidores, ya sea cPanel a Cpanel, cPAnel a Directamdin,, siempre quedan proquerías que hay que limpiar.

Una de ellas son las entradas en la tabla `user` de mysql/maridab en la que se conservan los hosts remotos de antiguos servidores.

He visto alguna vez cuando me han contratado para un mantenimiento de un servidor y un tuning, servidores con mas de 1000 usuarios mysql, y que llevaban arrastrando 4 o 5 hosts de distintos servidores, de migración en migración.

Luego, claro, mysql va lento.

“ Nota. No es precismanet la raíz del porblema, peoro cuando en el jardin dejas malas hierbas, al final caban poniendose feo.

## Revisión

Accedemos a nuestro mysql

```
> mysql
SELECT User, Host FROM mysql.user;
+-----+-----+
| User          | Host          |
+-----+-----+
| cdbtnet       | localhost    |
```

cdbtnet	old.server.com	
cdbtnet	old2.server.com	
...		

# Cramos el script

El escript se ejecuta pasandole un parámetro:

- El nombre del host a eliminar

## ATENCIÓN

ESTE COMO TODOS LOS COMANDOS DE ELIMINACION DEBE HACER LEYYENDOSE, ENTENDIENDOLO Y CON ... BACKUP

```
#!/bin/bash

# Verificar que se haya pasado un parámetro
if [ $# -eq 0 ]; then
    echo "Debe proporcionar un host para eliminar los usuarios. Uso: $0 <host>"
    exit 1
fi

# Guardar el parámetro proporcionado como el host a eliminar
delete_host=$1

# Variables de conexión a la base de datos
db_user="da_admin"
db_password=$(grep 'passwd' /usr/local/directadmin/conf/mysql.conf | awk -F= '{print $2}')
db_host="localhost" # Cambia si tu base de datos no está en localhost

# Comando para listar usuarios del host específico
list_users_command="SELECT user, host FROM mysql.user WHERE host='${delete_host}';"

# Conéctate a MySQL y obtiene la lista de usuarios
users=$(mysql -u "$db_user" -p"$db_password" -h "$db_host" -Bse "$list_users_command")

# Verificar si se obtuvieron usuarios
if [ -z "$users" ]; then
```

```

    echo "No se encontraron usuarios con host '$delete_host'."
    exit 0
fi

# Generar y ejecutar los comandos de eliminación de usuario
while IFS=$'\t' read -r user host; do
    if [ ! -z "$user" ] && [ ! -z "$host" ]; then
        drop_user_command="DROP USER '$user'@$host';"
        mysql_command="mysql -u \"$db_user\" -p\"$db_password\" -h \"$db_host\" -e \"$drop_user_command\""
        echo "Ejecutando: $drop_user_command"

        eval $mysql_command

        # Verificar si el comando se ejecutó correctamente
        if [ $? -ne 0 ]; then
            echo "Error al ejecutar: $drop_user_command"
        else
            echo "Usuario eliminado con éxito: $user@$host"
        fi
    fi
fi

done <<< "$users"

```

```

chmod +x nombre_script.sh
./nombre_script.sh 5.0.0.0
....
Ejecutando: DROP USER 'tblrmml_root'@'5.0.0.0';
Comando que se ejecutará: mysql -u "da_admin" -p"ElPaSsWoRd" -h "localhost" -e "DROP USER
'tblrmml_root'@'5.0.0.0';"
...

```

## 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](#).

# Activar DKIM a todos los dominios de un servidor con Directadmin

## Introducción

DKIM es pieza fundamental en el sistema actual de antispam, y sobre todo para garantizar que nuestro dominio y/o Ip no loleguen a ser considerados como SPAM.

## Configuracion DKIM global

Indicada en el manual, [directadmin.conf - #dkim](#) nos indica que la variable es `dkim`

Valor	Comentario
0	DKIM está deshabilitado por defecto para los nuevos dominios
1	DKIM está habilitado por defecto para los nuevos dominios
2	La funcionalidad de DKIM está habilitada, pero no es obligatoria para los nuevos dominios

Podemos editarlo manualmente o usar por ejemplo:

```
da config-set dkim 1
cd /usr/local/directadmin/custombuild
./build update
./build exim
./build eximconf
```

```
da build update
da build exem
da build exemconf
```

Esta configuración hará que todos los dominios futuros, se configuren con **DKIM**.

## Para dominios existentes

Es probable que en una migración o situación específica, el administrador desee poner el valor a **2** para poder realizar la migración sin añadir una capa de complejidad.

Bien, una vez asentado todo, o bien porque había dominios anteriores sin **DKIM**, procedemos:

“ Atención: Si hay ya dominios que no quieren tener **DKIM**, ya sea porque no saben como usar servicios exteriores de correo sin configurarlo correctamente o porque no se lo explicarón, se puede producir problemas con ellos. Tener en cuenta.

Habilitar la creación automática de registros **DKIM** no afecta a los dominios existentes. Tienes algunas opciones para agregar **DKIM** a los dominios antiguos una vez que has habilitado **DKIM** en el archivo `directadmin.conf`. Puedes hacerlo para cada dominio uno por uno o para todos los dominios existentes a la vez.

Para habilitar **DKIM** para todos los dominios existentes después de configurar **DKIM** en **1** en el archivo `directadmin.conf`, puedes ejecutar el siguiente comando a través de **SSH** como el usuario `root`.

```
echo "action=rewrite&value=dkim" >> /usr/local/directadmin/data/task.queue; /usr/local/directadmin/dataskq
```

Para habilitar **DKIM** solo para dominios seleccionados uno por uno, utiliza ya sea la cola de tareas o el script `dkim_create.sh` proporcionado por DirectAdmin (reemplaza **DOMAIN.COM** con el dominio para el cual deseas habilitar **DKIM**).

```
/usr/local/directadmin/scripts/dkim_create.sh DOMAIN.TLD
```

o inmediatamente

```
echo "action=rewrite&value=dkim&domain=DOMAIN.COM&dns=yes" >>
/usr/local/directadmin/data/task.queue; /usr/local/directadmin/dataskq
```

Ambos comandos funcionan de la misma manera, con la excepción de que puedes tener el **DKIM** escrito inmediatamente con **dataskq** en comparación con dentro de un minuto utilizando el script `dkim_create.sh`.

# Deshabilitar DKIM por Usuario

## Cuando Está Habilitado o Permitido Globalmente

Esta función está diseñada para que **DKIM** esté habilitado o permitido globalmente, pero puedes deshabilitarlo a nivel de usuario.

Esto requiere que se establezca `dkim=1` o `dkim=2` en el archivo `directadmin.conf`.

La configuración de `1` habilitará **DKIM automáticamente** para todos los dominios bajo cada usuario, a menos que especifiques lo contrario en sus archivos `user.conf`.

La configuración de `2` les permitirá a los usuarios, habilitar **DKIM** por sí mismos, a menos que se especifique lo contrario en su archivo `user.conf`.

Ten en cuenta, que establecer `dkim=0` en el archivo `directadmin.conf` **deshabilita completamente DKIM** para todo el servidor y los archivos `user.conf` no se verificarán. Por lo tanto, si deseas que **DKIM** esté deshabilitado globalmente por defecto con la opción de habilitarlo solo para ciertos usuarios/dominios, configurar `dkim=2` en el archivo `directadmin.conf` es una mejor opción.

Cuando creas un usuario, se crea con un dominio predeterminado. Este dominio tendrá **DKIM** creado para el dominio por defecto debido a la configuración habilitada globalmente y la no existencia de un `user.conf` hasta que se cree la cuenta (no hay un `user.conf` para editar y deshabilitar **DKIM**).

Por lo tanto, se deberá eliminar manualmente **DKIM** para el dominio predeterminado si prefieres que no tenga un registro **DKIM**.

Aquí están los pasos para, primero eliminar el registro del dominio predeterminado y luego deshabilitar la creación automática de registros DKIM para los dominios subsiguientes bajo ese usuario.

Para eliminar los registros del dominio predeterminado, elimina el registro **TXT** `x._domainkey` de `/var/named/DOMAIN.TLD.db` y luego elimina las claves.



```
rm -f /etc/virtual/DOMAIN.COM/dkim.public.key
rm -f /etc/virtual/DOMAIN.COM/dkim.private.key
```

Ahora, edita el `user.conf` para que no se habiliten registros *\*DKIM* para los dominios que se creen posteriormente bajo el usuario. El `user.conf` se puede editar a través de **SSH** como el usuario root y el archivo se encuentra aquí (donde USERNAME representa el nombre de usuario del usuario que estás editando),

```
/usr/local/directadmin/data/users/USERNAME/user.conf
```

Esto permite que la configuración de **DKIM** de ese usuario particular anule la configuración de **DKIM** habilitada globalmente establecida en el archivo `directadmin.conf`, evitando así que se creen registros **DKIM** para los dominios de ese usuario en adelante.

Reinicia DirectAdmin después de hacer los cambios.

```
systemctl restart directadmin
```

## Deshabilitar DKIM a Nivel de Dominio

Esta es esencialmente la misma función que la característica a nivel de usuario, con la excepción de que editarías el archivo de configuración del dominio ubicado en

```
/usr/local/directadmin/data/users/USERNAME/domains/DOMAIN.TLD.conf
```

, en su lugar.

No es necesario editar el archivo `user.conf` del usuario para controlar **DKIM** a nivel de dominio.

Si un determinado dominio utiliza tanto un DNS remoto como un servidor de correo remoto, es posible que desees deshabilitar DKIM para este dominio en particular en lugar de para todos los dominios del usuario. Aquí es donde esta función es útil.

“ En realidad no es necesaria esta dudosa práctica usada, cuando el usuario final o la otra empresa que le ofrece servicios de correo, no le da las putas adecuadas) La gran mayoría de los sevricios de correo externo, si dan la información necesaria para crear y mantener un registro **DKIM** para cada servicios de correo, basandonos en el registro **selector** pero su complejidad y la falta de conocimientos llevan a un salida incorrecta. Pero este es otro tema del que hablaremos en otro post, en fechas próximas.

Reinicia DirectAdmin después de hacer cambios en el archivo DOMAIN.TLD.conf:

```
systemctl restart directadmin
```

# Cambiar el Selector Predeterminado

DirectAdmin utiliza `x` como el selector predeterminado. Para cambiar el selector, necesitarás actualizar el archivo `directadmin.conf` con el selector deseado. Los siguientes ejemplos cambian el selector a `default`:

```
/usr/local/directadmin/directadmin set dkim_selector default restart
```

Necesitarás reconstruir la configuración de Exim de la siguiente manera:

```
/usr/local/directadmin/custombuild/build exim_conf
```

Confirma que el selector fue cambiado en el archivo `/etc/exim.dkim.conf`:

```
> grep -i selector /etc/exim.dkim.conf  
dkim_selector = x
```

Ahora, cualquier registro DKIM creado nuevo utilizará tu selector especificado. Ten en cuenta que necesitarás eliminar y recrear los registros DKIM antiguos que utilicen el selector antiguo si deseas que usen el nuevo selector.

## Conclusión

Ya hemos revisado el procedimiento paso a paso para habilitar DKIM con el panel de control DirectAdmin. Podemos decir, que el registro **DNS DKIM** es esencial para un servicio de correo electrónico más fluido y para la autenticación de correos electrónicos.

## 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](#).

# Mod Security. Desactivación global de reglas por path

## Introducción

Una vez más, con el tema de Mod Security, compruebo que el 99% de los administradores de sistemas, sigue la misma pauta de siempre, la salida hacia adelante más fácil, deshabilitando todo.

Soy cabezón, y no he basado mi seguridad en mis máquinas, en abrir la puerta menoscabando la seguridad perimetral.

Tengo cliente a los que llevo sus servicios, que son incapaces de aguantar en firme, con las normas y reglas de seguridad que trato de imponerles, pese a que eso suponga un aumento de costes en horas para limpiar problemas derivados de los **mini hackeos**

## Escenario

En el caso que me llevó a este tema, estaba implicado [DirectAdmin](#) y el webmail [RoundCube](#) en una situación algo especial.

Con las cuentas de sistema `usuario` usadas como cuenta de correo, RoundCube recibía una serie de errores al lanzarse prohibiciones vía Mod Security.

“ Connection Error (Failed to reach the server)! !Error de conexión fallo al intentar alcanzar el servidor)!

“ Cuando teneos problemas con RoundCube como con muchas aplicaciones web, insisto a mis clientes que observen las webmaster tools del navegador y/o al menos las cabeceras de respuesta (406) más allá de los mensajes tipo **Alert** de las aplicaciones.

Al final, localizando las reglas afectadas por RoundCube a nivel hostname, salieron a la palestra las siguiente reglas afectadas:

- 911100
- 932260
- 920340
- 932235
- 941100
- 941130
- 941160
- 941170
- 949110
- 980130

Todas ellas, con Paranoia Level 1, [ModSecurity :: Concepto Paranoia Level](#)

Uy... que cosas. EL **PR 1** es básicamente el nivel con menor número de falsos positivos, y muchas de estas rules, ofrecen una protección extraordinaria a muchos de los errores más comunes de los "programadores" de javascript.

Así que las soluciones que se presentan en, StackOverFlow, el foro de DirectAdmin, y otras muchas, no me convencían, porque se trata de atajos (workaround) que llevan a la desactivación de la regla de forma global, o en su defecto, no cumplen con la documentación de Mod Security o de DirectAdmin.

## Solución (Actualizado 8/01/2025)

Al final vi el método antiguo (me llama mas la atención que el nuevo) ofrecido por Directadmin y que usamos en [Como bloquear los Bad bots \(Bot basura\) usando ModeSecurity en Directadmin nueva](#) que es mas manejable y programable.

# /usr/local/directadmin/custombuild/custom/modsecurity/conf/

Hay que crear este path como repositorio de los ficheros especificos que creemos para el manejo de ModSecuirty sin miedo a que se eliminen.

```
mkdir -p /usr/local/directadmin/custombuild/custom/modsecurity/conf/
```

# Fichero de exclusiones

En mi caso uso `/usr/local/directadmin/custombuild/custom/modsecurity/conf/01_REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf`, pero como es una precarga, le asigno numeros bajos como 00, 01, 02 con el fin de que sean los primeros en cargar.

Tenemos un ejemplo de como tratar el tema en el fichero `/etc/modsecurity.d/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf.example`

```
cp /etc/modsecurity.d/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf.example
/usr/local/directadmin/custombuild/custom/modsecurity/conf/01_REQUEST-900-EXCLUSION-RULES-BEFORE-
CRS.conf
```

Una vez creado, o modificado, **SIEMPRE** debemos verificar primero (si usamos nginx o apache+nginx) que no hay ningun problema, con. Para ello escribimos la rule en el fichero real, `/etc/modsecurity.d/01_REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf` (copiar y pegar)

```
nginx -t
```

Una vez verificado, procedemos a reconstruir los ficheros de configuracion con:

```
> da build modsecurity_rules
Installing OWASP Core Rule Set for ModSecurity...
download_cached: using cached '/usr/local/directadmin/custombuild/cache/owasp-modsecurity-crs-4.9.0.tar.gz'
file
Copying custom ModSecurity rules to /etc/modsecurity.d/...
Installation of ModSecurity Rule Set has been finished.
```

Después reconstruimos la configuración.

```
> da build rewrite_confs
cp: cannot remove '/etc/httpd/conf/extra/httpd-directoryindex.conf': Operation not permitted
2025/01/08 17:15:27 info executing task          task=action=rewrite&value=ips
2025/01/08 17:15:27 info finished task          duration=10.262712ms task=action=rewrite&value=ips
Using 5.135.93.75 for your server IP
Copying custom ModSecurity rules to /etc/modsecurity.d/...
Restarting apache.
Installing OWASP Core Rule Set for ModSecurity...
download_cached: using cached '/usr/local/directadmin/custombuild/cache/owasp-modsecurity-crs-4.9.0.tar.gz'
file
Copying custom ModSecurity rules to /etc/modsecurity.d/...
```

Installation of ModSecurity Rule Set has been finished.

2025/01/08 17:15:31 info executing task task=action=rewrite&value=ips

2025/01/08 17:15:31 info finished task duration=7.557145ms task=action=rewrite&value=ips

Using 5.135.93.75 for your server IP

Using 5.135.93.75 for your server IP

Copying custom ModSecurity rules to /etc/modsecurity.d/...

2025/01/08 17:15:34 info executing task task=action=rewrite&value=nginx

2025/01/08 17:15:40 info finished task duration=6.360399294s task=action=rewrite&value=nginx

Restarting nginx.

Ya podriamos hacer pruebas.

## Ejemplos

```
SecRule REQUEST_FILENAME "@beginsWith /roundcube" \
    "id:1001,\
    phase:2,\
    pass,\
    nolog,\
    ctl:ruleRemoveById=911100,\
    ctl:ruleRemoveById=932260,\
    ctl:ruleRemoveById=920340,\
    ctl:ruleRemoveById=932235,\
    ctl:ruleRemoveById=941100,\
    ctl:ruleRemoveById=941130,\
    ctl:ruleRemoveById=941160,\
    ctl:ruleRemoveById=941170,\
    ctl:ruleRemoveById=949110,\
    ctl:ruleRemoveById=980130"
```

## Idea y apuntes

- [ModSecurity Rules: Global or for Hostname?](#)
- [How do I skip certain rules for parameter in a path in ModSecurity?](#)

### 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](#).



# Reconstrucción del índice Full Text Search (FTS) en cuentas de correo :: Dovecot

## Introducción

A veces ocurre que la correspondencia entre el tamaño en disco de una cuenta de correo usando los medios reales como son `du` no se corresponde con lo que DirectAdmin nos muestra en el panel de usuario para dicha cuenta de correo.

Esto suele ocurrir tras una eliminación de correo muy intensa en la que por cuestiones de espacio el usuario quiere ver liberada su cuenta por estar cerca de excederse o haberse excedido ya. También puede ocurrir que sea un problema que requiere de una reconstrucción forzada.

Esos índices de búsqueda pueden ser gigantes, del orden de varios GB.

## doveadm-fts(1) -

[Manipulate the Full Text Search \(FTS\) index](#)

Basicamente podemos hacer lo siguiente:

```
## Cuenta E-mail
> doveadm fts rescan -u jmvarela@omnicon.es

## Usuario y todas sus cuentas
> doveadm fts rescan -u USERNAME
```

También podemos usar un script para usarlo como mantenimiento de estos índices.

## rescan\_fts.sh

## Cremos el fichero

```
#!/bin/bash

# Directorio que contiene los usuarios
USER_DIR="/usr/local/directadmin/data/users"

# Iterar sobre cada usuario (directorio)
for user in "$USER_DIR"/*; do
    # Verificar si el item es un directorio
    if [ -d "$user" ]; then
        # Obtener el nombre del usuario
        username=$(basename "$user")
        echo "Ejecutando doveadm fts rescane para el usuario: $username"
        # Ejecutar el comando doveadm fts rescane
        doveadm fts rescane -u "$username"
    fi
done
```

## Damos permiso y ejecutamos

```
chmod +xrescan_fts.sh
./rescan_fts.sh
```

## 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](#).

# Cambio el doc root de un dominio en DirectAdmin

## Doc root, public, public\_html

El software moderno desde hace años, evita la publicación del software en el mismo area publica o expuesta a internet. Por seguridad, por ordenación, el codigo usa el contenido en distintas carpetas dejando a una carpeta el destino de exposición al publico.

Este puede ser `public` como en el caso de Laravel, u otros distintos segun el framework.

Esto suele ser un problema para los hosters porque sus paneles de control usand el de toda la vida, `public_html`

En el camino, mucho se aventuran a enlace simbolicos, redirecciones. Y todo eso es muy bonito pero al final altera, no solo la realidad de la instalación sino un posible cambio de servidor, de paradigma de sistema, etc.

## Cambiar el DOC ROOT en Directadmin

Si bien es sencillo, a veces parece que los manuales son algo espesos, y si encima tenemos un for de mas de 20 años de antigüedad, sin pruning, pues acabas por volverte loco con los cambios en el tiempo.

En la actualidad es bien sencillo.

### (Admin) Custom HTTPD Configurations

`evo/admin/custom-httpd`

Seleccionar el dominio (o subdominio entendiendose como entidad configurada como dominio independiente)

Después, deberemos modificar la configuracion de `httpd.conf` `nginx.conf.proxy`

Custom Httpd Configurations

En cada uno de ellas veremos un boton con la palabra **Customize**

## Customize HTTPD

Que la hacer click nos mostrará la caja de exto donde introducir nuestros cambios.

## Customize configuration

Aqui usando varmiables podemos adecuar a lo que queramos nuestros path. Ejemplo de abajo me sirve a mi porque se trata de una migracion que no queria complicar.

```
|?DOCROOT=`HOME`/domains/`DOMAIN`/public_html/public|
```

El resultado de eso sera que tras reconstruir la configuracion del `doc root` será

```
/home/user/domains/subdomain.domain.tld/public_html/public
```

De esta forma el proyecto estará en el `public_html`, pero solo estará expuesta la carpeta `public`

## da build rewrite\_confs

Siemrpe, cuando terminemos deberamos reconstruir los ficheros de configruación, lo cual se hace con el comando `da build rewrite_confs` o bien en el botón de

Custom HTTPD Configuration :: `da build rewrite_confs`

## 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](#).

# Donde está la configuración básica del servidor con Directadmin

## Directadmin configuración interna

Directadmin es más sencillo que otros paneles de control y te ayuda a localizar donde están las configuraciones que despliega en el servidor.

Directadmin, compila y configura el software de servidor, como Web (Apache, Nginx,...) Correo (Imap, exim,...) desde dos puntos claves:

## Software de servicio

```
/usr/local/directadmin/custombuild/options.conf
```

## Directadmin (interno)

```
/usr/local/directadmin/conf/directadmin.conf
```

Con estos ficheros podremos trabajar cosas como templates, clones, etc.

“ Esta entrada es una entrada rápida, de conocimiento básico.

## 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 se entrega, tal y como está, sin que ello implique ninguna obligación ni responsabilidad por parte de [Castris](#)

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

# Cambios especificados en el php.ini disable\_functions por dominio

## Cambiar individualmente en un dominio disable\_functions

Un escenario muy común en sistemas, es la salida hacia adelante obviando los problemas que puede causar nuestra decisión.

Un caso común es el quitar las protecciones de forma global a través de el proceso general del servidor, en lugar de buscar una solución individual, para el caso concreto.

En el caso de Directadmin, si tenemos la opción [secure\\_php](#) esta añadirá a la configuración del php del servidor

```
disable_functions =  
exec,system,passthru,shell_exec,proc_close,proc_open,dl,popen,show_source,posix_kill,posix_mkfifo,posix_getp  
wuid,posix_setpgid,posix_setsid,posix_setuid,posix_setgid,posix_seteuid,posix_setegid,posix_uname  
mysqli.allow_local_infile = Off  
expose_php = Off  
register_globals = Off
```

Existe el camino fácil, que es ir quitando las funciones que molestan a nuestros clientes, [How to customize the disable functions list](#) y existe otro camino, que es desahabilitar al que nuestro cliente necesita, si esto es totalmente necesario, ya sea por un tiempo limitado, o de forma definitiva.

## Opciones de php.ini por dominio

[Opciones por dominio](#) nos ayuda a esto último ya que tratar de modificar `disable_functions` via `.user_ini` aunque este autorizado, no funcionará para modificar esa clave.

- Lo primero es buscar el path de nuestra instalación para nuestro Directadmin y nuestra distro.

En mi caso esta en `/usr/local/phpXX/lib/php.conf.d`

Así que, siguiendo el manual, introducido el path y el dominio o subdominio del que quiero tal corrección, el nos lo dará.

En nuestro caso el cliente tenía algunos despliegues con Laravel que necesitaban `shell_exec` por lo que lo eliminamos del fichero **ini** personalizado,

```
/usr/local/php83/lib/php.conf.d/30-subdomain.full.tld.ini
```

```
disable_functions =  
exec,system,passthru,proc_close,proc_open,dl,popen,show_source,posix_kill,posix_mkfifo,posix_get  
puid,posix_setpgid,posix_setsid,posix_setuid,posix_setgid,posix_seteuid,posix_setegid,posix_una  
me
```

Después simplemente tenemos que hacer un rebuild de la función de seguridad.

da build secure\_php

##### 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](https://castris.com)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](https://intranet.castris.com/store/soporte-profesional).



# Git desde DirectAdmin Interface

## Git desde DirectAdmin Interface

Jamás le aconsejaría a nadie usar el Git a través de un interface visual de este tipo, pero a veces por cuestiones de seguridad, metodologías y otras cuestiones, e las que el acceso a SSH esta restringido, puede ser el último recurso.

Aun así, no imagino una jefe de proyectos lidiando con un interface de esta naturaleza en la que por hacer fácil la cosa, el final se hace difícil.

En primer lugar es imperativo leer la documentación, (Git manager feature)[<https://docs.directadmin.com/other-hosting-services/git/general.html>]

Aquí tendremos una idea general de lo que nos espera.

- El proyecto como root estará en el path que indiquemos
- La configuración no esta en el root de nuestro proyecto, sino en `/home/USER/domains/DOMAIN/name.git` lo cual tendremos que recordarlo, si como es bine seguro, algún día deberemos lidiar con Git para arreglar o realizar operaciones más complejas que un simple **click** para hacer el equivalente a un **git pull**

Es importante la parte final, (Technical)[<https://docs.directadmin.com/other-hosting-services/git/general.html#technical>] donde veréis la información sobre como ejecutar `git` usando comando y las opciones a escribir para entenderlo mejor.

To desde luego, no le aconsejo a ningún desarrollador o jefe de proyecto, el uso de esta interface. Menos si no tiene acceso a `root` ya que la BD con los datos del git estará ubicada en `/usr/local/directadmin/data/users/USER/user.db` y las complejidades de uso no merecen la pena, a cambio de negarse a usar el terminal.

## Nota

En estos tiempos, es muy sistémico, la falta de conocimientos de sistemas. Hemos llegado a un punto de especialización y de venta de supuestos sistemas amigables, que en realidad no lo son. Desconocer el uso de SSH, de los comandos básicos de git, de el como de aquellas cosas que

operan en nuestro espacio profesional, es un serio handicap para la industria. Parece que aquí llego también el paradigma del **conocimiento mínimo** o lo que es lo mismo la **falta de formación profesional adecuada**

## 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 bloquear los Bad bots (Bot basura) usando ModeSecurity en Directadmin nueva

## Introducción BadBots

El término "bot" se utiliza frecuentemente en internet y se refiere a un programa informático que automatiza acciones o tareas en la red. Aunque un bot no es inherentemente bueno o malo, puede clasificarse en alguna de estas dos categorías, dependiendo de si se utiliza con buenas o malas intenciones.

## Bots Buenos

Se llama "bot bueno" a aquel que realiza tareas útiles o beneficiosas que no perjudican la experiencia del usuario en internet. Hay muchos bots que se consideran buenos, por ejemplo:

- Bots de Motores de Búsqueda: A menudo conocidos como rastreadores web o arañas, son operados por grandes motores de búsqueda como Google o Bing.
- Bots de Monitoreo de Sitios: Estos bots supervisan métricas de páginas web, como el seguimiento de enlaces o caídas del sistema, y pueden alertar a los usuarios sobre cambios importantes o tiempos de inactividad. Son utilizados por sitios como UptimeRobot o Cloudflare.
- Bots de Feed: Estos bots recorren internet en busca de contenido para añadir a los feeds de noticias de diversas plataformas, y son gestionados por sitios de agregación o redes sociales.
- Bots de Asistentes Personales: Aunque estos programas son más avanzados que un bot típico, siguen siendo considerados bots. Son programas informáticos que buscan datos en internet que coincidan con una búsqueda, y son operados por empresas como Apple (Siri) o Google (Alexa).

# Bots Malos

Por otro lado, se refiere como "bot malo" a aquellos que realizan actos maliciosos, roban datos o causan daños en servidores, redes o sitios web. Pueden ser empleados para llevar a cabo ataques de denegación de servicio distribuido (DDoS) o para escanear servidores, redes o páginas web en busca de vulnerabilidades que puedan comprometer estos sistemas.

En los últimos años, hemos visto que los bots maliciosos se han convertido en un problema significativo tanto para los administradores de servidores como para los dueños de sitios web. Estos bots suelen dirigirse a un servidor o página web, realizando miles de solicitudes y recopilando grandes cantidades de datos en un tiempo muy corto.

Su práctica, su diseño, y su falta de ética son un problema para muchos sitios, sus administradores y los administradores de sistemas.

## Técnicas de bloqueo

Hay algunas técnicas de bloqueo como el uso de .htaccess a través de formulas como la expuesta en [Bad Bots y la pesadilla del tráfico. Htaccess en Apache 2.4](#):

```
# Start Bad Bot Prevention
<IfModule mod_setenvif.c>
# SetEnvIfNoCase User-Agent ^$ bad_bot
SetEnvIfNoCase User-Agent "^12soso.*" bad_bot
SetEnvIfNoCase User-Agent "^192.comAgent.*" bad_bot
SetEnvIfNoCase User-Agent "^1Noonbot.*" bad_bot
...
<Limit GET POST PUT>
    Order Allow,Deny
    Allow from all
    Deny from env=bad_bot
</Limit>
</IfModule>
```

Pero esto es una pesadilla a nivel administrador de sistemas, donde cada uno pone su lista.

Para mi, la mejor es el uso de ModSecurity y como ya me dedico prioritariamente a Directadmin lo dejaré aquí más claro.

# Bad Bots bloqueados en Directadmin con ModSecurity

Para usar este método tenemos que hacerlo de manera que no se sobre escriba la configuración cuando se actualiza Directadmin, Apache o Nginx

## Crear el directorio si no existe

```
cd /usr/local/directadmin/custombuild  
mkdir -p custom/modsecurity/conf
```

## Crear 00\_bad\_bots\_conf

```
nano /usr/local/directadmin/custombuild/custom/modsecurity/conf/00_bad_bots.conf
```

### Contenido

```
# BLOCK BAD BOTS  
SecRule REQUEST_HEADERS:User-Agent "@pmFromFile bad_bot_list.txt"  
"phase:2,t:none,t:lowercase,log,deny,severity:2,status:406,id:1100000,msg:'Custom WAF Rules: WEB  
CRAWLER/BAD BOT'"
```

⚠ Atención a la rule ID, para que no choque con otra rules si tenias con anterioridad alguna adicional en otro sistema, o tienes un sistema para controlar las rules tuyas. Aquí usaremos `1100000`

## Crear bad\_bot\_list.txt

Esta lista puedes actualizarla con la lista [Apache Ultimate Bad Bot](#)

El fichero a usar es `https://raw.githubusercontent.com/mitchellkrogza/apache-ultimate-bad-bot-blocker/master/_generator_lists/bad-user-agents-htaccess.list`

```
wget -O /usr/local/directadmin/custombuild/custom/modsecurity/conf/bad_bot_list.txt  
https://raw.githubusercontent.com/mitchellkrogza/apache-ultimate-bad-bot-blocker/master/_generator_lists/bad-  
user-agents-htaccess.list
```

O con curl

```
curl -o /usr/local/directadmin/custombuild/custom/modsecurity/conf/bad_bot_list.txt
https://raw.githubusercontent.com/mitchellkrogza/apache-ultimate-bad-bot-blocker/master/_generator_lists/bad-
user-agents-htaccess.list
```

También puedes crear una estrategia, para usando dicha lista eliminar o añadir los tuyos propios, cuando se actualice.

## Actualización

```
da build modsecurity_rules
da build rewrite_confs
```

## Verificación

Puedes verificar que esta correcto con el siguiente comando, que te mostrará que lo usado se copio en el lugar apropiado.

```
ls -la /etc/modsecurity.d/*bad*
-rw-r--r-- 1 root root 199 Jan 4 09:24 /etc/modsecurity.d/00_bad_bots.conf
-rw-r--r-- 1 root root 5534 Jan 4 09:26 /etc/modsecurity.d/bad_bot_list.txt
```

## Testing

```
curl -A "AiHitBot" https://example.com
<html>
<head><title>406 Not Acceptable</title></head>
<body>
<center><h1>406 Not Acceptable</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

```
curl -A "aihitbot" https://example.com
<html>
<head><title>406 Not Acceptable</title></head>
<body>
<center><h1>406 Not Acceptable</h1></center>
<hr><center>nginx</center>
</body>
</html>
```

Reemplaza example.com con un dominio del servidor ☐☐

Deberas obtener un **406 Not Acceptable** como respuesta

## Agradecimientos

- [How to Block Bad Bots using ModSecurity with 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](#).

# Wordpress Manager de Directadmin y wp cli problemas de memoria

## PHP Fatal error: Allowed memory size of 134217728 bytes exhausted

Un cliente reporto que estaba usando la herramienta **Wordpress Manager** de **Directadmin** y cuando instaló le salió un error de memoria

```
PHP Fatal error: Allowed memory size of 134217728 bytes exhausted (tried to allocate 47526080 bytes) in
/home/miusuairoes/domains/midominio.es/public_html/wp-includes/class-wpdb.php on line 2320 Fatal error:
Allowed memory size of 134217728 bytes exhausted (tried to allocate 47526080 bytes) in
/home/miusuairoes/domains/midominio.es/public_html/wp-includes/class-wpdb.php on line 2320 PHP Fatal error:
Allowed memory size of 134217728 bytes exhausted (tried to allocate 47526080 bytes) in
/home/miusuairoes/domains/midominio.es/public_html/wp-includes/class-wpdb.php on line 2320 Fatal error:
Allowed memory size of 134217728 bytes exhausted (tried to allocate 47526080 bytes) in
/home/miusuairoes/domains/midominio.es/public_html/wp-
includes/class-wpdb.php on line 2320
```

Error de memoria Wordpress Manager Directadmin

Que raro. El cliente trabaja ya con la modificación de `memory_limit` segun el método de Directadmin, y era verificable con un `phpinfo();`

## Prueba en shell



Para ver el tema más cerca, me fui al shell.

```
> wp
```

```
PHP Fatal error: Allowed memory size of 134217728 bytes exhausted (tried to allocate 47526080 bytes) in  
/home/unilanges/domains/MYDOMAIN.ES/public_html/wp-includes/class-wpdb.php on line 2320
```

```
Fatal error: Allowed memory size of 134217728 bytes exhausted (tried to allocate 47526080 bytes) in  
/home/unilanges/domains/MYDOMAIN.ES/public_html/wp-includes/class-wpdb.php on line 2320
```

```
PHP Fatal error: Allowed memory size of 134217728 bytes exhausted (tried to allocate 47526080 bytes) in  
/home/unilanges/domains/MYDOMAIN.ES/public_html/wp-includes/class-wpdb.php on line 2320
```

```
Fatal error: Allowed memory size of 134217728 bytes exhausted (tried to allocate 47526080 bytes) in  
/home/unilanges/domains/MYDOMAIN.ES/public_html/wp-includes/class-wpdb.php on line 2320
```

Y claro no quedo otra:

```
> php -i | grep memory
```

```
memory_limit => 128M => 128M
```

```
Collecting memory statistics => No
```

```
opcache.memory_consumption => 128 => 128
```

```
opcache.preferred_memory_model => no value => no value
```

```
opcache.protect_memory => Off => Off
```

Como es **Directadmin**, su compilación trata el tema de una manera particular, y no encontré el como modificar el cli, para el cliente de php.

Así que conociendo el tema, la cuestión era probar lo más sencillo del mundo. Modificar el `wp-config.php`

```
define( 'WP_MEMORY_LIMIT', '256M');
```

Y voila. Ya no sale el error, y ya podemos usar el `wp-cli` en el shell. Ambas dos cosas solucionadas.

## Notas

Directadmin tiene muchas herramientas de ayuda, pero sigo pensando que el panel debería ser más orientado a sistemas, que ayudas al usuario.

Un gestor de Wordpress me parece un mal camino, como el del [git](#).

Pero esto es una opinión.

## 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](#).

# Configurar PHP en un servidor con Directadmin

Antes de acudir a medidas como el uso de `php.ini` o `.user.ini` debemos saber que **Directadmin** en modo usuario pone a disposición una entrada para poder configurar nuestro PHP, en aquellos servidor que así lo tiene posibilitado y usan PHP-FPM como es el caso de [Castris](#)

## Pasos

El proceso lógico, que además sirve para otras habilidades del panel, es el que se describe mas abajo.

1. Usar el buscador si no conocemos la ubicación del sitio para la acción a realizar

Panel principal y Buscador de menu

3. Realizar una busqueda corta, de tipo generalista

Buscador - búsqueda parcial

4. Realizar los cambios

Configuración PHP

- Selección del sitio web
- Cambios a de versión PHP
- Cambios posibles a realizar de uno en uno y cada un con sus valores predefinidos
  - `display_errors`
  - `error_reporting`
  - `file_uploads`
  - `include_path`
  - `log_errors`
  - `mail.force_extra_parameters`
  - `max_execution_time`
  - `max_file_uploads`
  - `max_input_time`
  - `max_input_vars`
  - `memory_limit`

- post\_max\_size
- register\_globals
- session.gc\_maxlifetime
- short\_open\_tag
- upload\_max\_filesize
- zlib.output\_compression

## 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](#).

# Configuración de Smart Relay en DirectAdmin/Exim

## Introducción al smart relay para Directadmin con Exim

DirectAdmin proporciona un mecanismo de inclusión de archivos para personalizar la configuración de Exim sin perder los cambios en actualizaciones posteriores. Para la configuración de smart relay, se utilizan dos archivos de inclusión específicos que se cargan en diferentes secciones del archivo principal `exim.conf`.

## Ubicación de las Inclusiones

En el archivo principal de configuración de Exim (`/etc/exim.conf`), encontramos dos inclusiones importantes:

1. Para los transportes:

```
begin transports
.include_if_exists /etc/exim.transports.pre.conf
```

2. Para los routers:

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

## Archivos de Configuración

# 1. Transport Configuration ( `/etc/exim_directadmin/exim.transports.pre.conf` )

Este archivo define cómo se realizará el envío de correo al smart host:

```
spamgateway_smarthost_transport:  
  driver = smtp  
  hosts_require_tls = *  
  .include_if_exists /etc/exim.dkim.conf
```

Desglose de la configuración:

- `driver = smtp`: Utiliza el protocolo SMTP estándar para el envío
- `hosts_require_tls = *`: Fuerza el uso de TLS para todas las conexiones
- Incluye la configuración DKIM para asegurar que los correos salientes sean firmados correctamente

# 2. Router Configuration ( `/etc/exim_directadmin/exim.routers.pre.conf` )

Este archivo define las reglas de enrutamiento para el correo saliente:

```
spamgateway_smarthost_router:  
  driver = manualroute  
  domains = ! +local_domains  
  ignore_target_hosts = 127.0.0.0/8  
  condition = "${perl{check_limits}}"  
  transport = spamgateway_smarthost_transport  
  route_list = * smart02.domain.tld:hetzner-smart01.domain.tld  
  hosts_randomize = true
```

Desglose de la configuración:

- `driver = manualroute`: Define un enrutamiento manual para los correos
- `domains = ! +local_domains`: Aplica solo a dominios que no son locales
- `ignore_target_hosts = 127.0.0.0/8`: Evita el envío a direcciones locales
- `condition = "${perl{check_limits}}"`: Verifica límites de envío mediante una función Perl
- `transport = spamgateway_smarthost_transport`: Utiliza el transporte definido anteriormente

- `route_list`: Define los smart hosts disponibles
- `hosts_randomize = true`: Habilita el balanceo de carga aleatorio entre los smart hosts

# Funcionamiento

Con esta configuración:

1. Todo el correo saliente (excepto para dominios locales) se enviará a través de los smart hosts configurados
2. El sistema alternará aleatoriamente entre los smart hosts disponibles ( `smart02.domain.tld` y `hetzner-smart01.domain.tld` )
3. Si un smart host falla, el sistema intentará automáticamente con el otro
4. Las conexiones se realizan con TLS
5. Los correos mantienen la firma DKIM gracias a la inclusión de la configuración DKIM en el transporte

# Notas Importantes

1. La configuración mantiene la firma DKIM en los correos reenviados
2. El balanceo de carga entre smart hosts proporciona redundancia y distribución de carga
3. La configuración se mantiene incluso después de actualizaciones de DirectAdmin o Exim
4. Los cambios se realizan en archivos separados, lo que facilita el mantenimiento y la depuración

# Verificación

Para verificar que la configuración está funcionando correctamente, puedes:

1. Revisar los logs de Exim para confirmar el uso alternado de los smart hosts
2. Verificar que los correos salientes mantienen la firma DKIM
3. Comprobar que el sistema cambia automáticamente al host alternativo si uno falla

## 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 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](#).



# Redis: Rotura de WordPress por error de Redis en Directadmin

## Escenario

- Sitio WordPress configurado con Redis Object Cache.
- El sitio deja de funcionar mostrando el mensaje *Error Establishing a Redis Connection*

Al ejecutar `systemctl`, se observa que:

- `redis-server` (Redis principal) está activo.
- `redis-rspamd` y `redis@user_a` están fallando.

## Análisis

Buscamos informacion sobre el estado del servicio

```
systemctl | grep redis
```

● redis-rspamd.service	loaded failed failed	Multi-user redis persistent key-value database
redis-server.service	loaded active running	Advanced key-value store
redis@user.service	loaded active running	Multi-user redis persistent key-value database
system-redis.slice	loaded active active	Slice /system/redis

## Diagnóstico

Los registros del sistema (`journalctl`) muestran:

```
cat /var/log/syslog| grep -i redis
```

...

```
2025-05-29T06:35:57.647681+02:00 dar redis-server[1064]: 1064:M 29 May 2025 06:35:57.647 * Server initialized
```

```
2025-05-29T06:35:57.648969+02:00 dar redis-server[1064]: 1064:M 29 May 2025 06:35:57.648 # Can't handle RDB format version 12
```

```
2025-05-29T06:35:57.649027+02:00 dar redis-server[1064]: 1064:M 29 May 2025 06:35:57.648 # Fatal error loading the DB, check server logs. Exiting.
```

...

“ Can't handle RDB format version 12 Fatal error loading the DB, check server logs. Exiting.

Esto indica que Redis no puede leer el archivo de base de datos dump.rdb. Las causas habituales son:

1. El archivo fue generado por una versión de Redis diferente (por ejemplo, tras un downgrade de versión en una actualización de DirectAdmin).
2. El archivo se ha corrompido, posiblemente tras un reinicio forzado o caída del sistema.

## Solución

### Previa para liberar al wordpress del problema

Deberas eliminar el fichero de wordpress `object-cache.php`

```
rm -f /home/USER/domains/DOMAIN.TLD/public_html/wp-content/object-cache.php
```

### Eliminar los archivos dump.rdb afectados para forzar su regeneración limpia:

```
rm -f /var/lib/respamd/.redis/db/dump.rdb  
rm -f /home/USER/.redis/db/dump.rdb
```

## Reiniciar los servicios Redis afectados:

```
systemctl restart redis-respamd  
systemctl restart redis@USER
```

## Consideraciones

- Esta operación elimina los datos almacenados en caché, pero no afecta a los datos persistentes del sitio WordPress.
- Redis volverá a crear los datos necesarios durante el uso normal del sistema.
- Si Redis estaba siendo utilizado para sesiones, estadísticas u otras funciones de estado, esa información se perderá.

## Verificación

Si no conoces la ubicación del archivo `dump.rdb`, puedes buscarlo con:

```
locate dump.rdb
```

“ Es necesario tener mlocate o plocate instalado y la base de datos actualizada con updatedb.

## 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 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](#).