Whitelist dinámica de rspamd via email en Directadmin

Qué hace

Permite a cualquier usuario autenticado del servidor gestionar la whitelist de rspamd enviando un email. No requiere acceso al panel ni SSH.

Enviar un email a `whitelist@<cualquier-dominio-del-servidor>` con la acción en el asunto:

Asunto del email	Acción
`add ejemplo.com`	Añade el dominio completo ejemplo.com — todos los correos de @ejemplo.com pasan
`add user@ejemplo.com`	Añade solo esa dirección concreta — otros de @ejemplo.com siguen filtrados
`ejemplo.com`	Añade ejemplo.com (add implícito)
`del ejemplo.com`	Elimina ejemplo.com de la whitelist
`del user@ejemplo.com`	Elimina esa dirección de la whitelist
`remove ejemplo.com`	Igual que `del` (también `delete`, `rm`)
`list`	Responde con la whitelist completa actual

El sistema responde por email confirmando cada operación: dominio añadido, eliminado, ya existente, bloqueado, o error de formato.

El email debe enviarse desde un cliente de correo autenticado (Thunderbird, Outlook, webmail). Correos no autenticados son ignorados silenciosamente.

Dominios vs direcciones

El sistema distingue entre dos tipos de whitelist:

- **Dominio completo** (`add ejemplo.com`): todos los correos desde cualquier cuenta @ejemplo.com pasan sin penalización
- **Dirección concreta** (`add user@ejemplo.com`): solo los correos de esa cuenta pasan; el resto de @ejemplo.com sigue siendo evaluado normalmente

Esto es útil para proveedores masivos (Gmail, Outlook, Proton, etc.) donde no queremos whitelistear todo el dominio sino solo una cuenta concreta de confianza.

Restricciones de seguridad

- **Solo SMTP AUTH:** si el email no viene de un usuario autenticado del servidor, se descarta
- **Mass providers bloqueados como dominio:** no se puede whitelistear gmail.com, outlook.com, proton.me, etc. como dominio completo — pero SÍ se puede whitelistear una dirección concreta como `contacto@proton.me`
- **Límite:** máximo 500 entradas por servidor (dominios + direcciones combinados)
- **Validación estricta:** el dominio/email debe tener formato válido
- **Respuesta informativa:** el sistema responde indicando exactamente qué hizo o por qué rechazó la petición

Proveedores masivos bloqueados

gmail.com, googlemail.com, yahoo.com, yahoo.es, yahoo.fr, hotmail.com, hotmail.es, outlook.com, outlook.es, live.com, msn.com, aol.com, mail.ru, yandex.ru, yandex.com, protonmail.com, proton.me, icloud.com, me.com, mac.com, gmx.com, gmx.es, gmx.de, zoho.com, tutanota.com, tuta.com, tuta.io, fastmail.com, mail.com, email.com, web.de, freenet.de, t-online.de, libero.it, virgilio.it, laposte.net, free.fr, orange.fr, 163.com, 126.com, qq.com

Si se intenta añadir uno de estos como dominio, el sistema lo rechaza y sugiere usar la dirección completa (`add usuario@proveedor.com`).

Cómo funciona internamente

```
Email autenticado → whitelist@dominio.com
        ↓
Exim router (whitelist_pipe_router)
  · condición: $authenticated_id no vacío
  · domains = +local_domains (solo dominios hospedados)
        ↓
Exim transport → pipe a /usr/local/bin/rspamd_whitelist.sh
  · pasa AUTH_USER via variable de entorno
        ↓
Script: parsea Subject, valida, determina tipo (dominio/dirección)
        ↓
```

```
  Si dominio → /etc/rspamd/local.d/maps/whitelist_dynamic.map
  Si dirección → /etc/rspamd/local.d/maps/whitelist_dynamic_addr.map
        ↓
rspamd recarga automáticamente (~10 segundos)
        ↓
  Multimap WHITELIST_FROM_DYNAMIC (dominios, score -100.0)
  Multimap WHITELIST_ADDR_DYNAMIC (direcciones, score -100.0)
        ↓
Respuesta por email al usuario confirmando la operación
```

Ficheros involucrados

Fichero	Propósito	Persistencia
`/usr/local/bin/rspamd_whitelist.sh`	Script principal	Manual (no gestionado por DA)
`/etc/exim.routers.pre.conf`	Router Exim custom	Sobrevive `rewrite_confs` (include en template DA)
`/etc/exim.transports.pre.conf`	Transport Exim custom	Sobrevive `rewrite_confs` (include en template DA)
`/etc/rspamd/local.d/multimap.conf`	Definición de los símbolos WHITELIST_*_DYNAMIC	`local.d/` = override oficial de rspamd
`/etc/rspamd/local.d/maps/whitelist_dynamic.map`	Lista de dominios (uno por línea)	Fichero de datos, no config
`/etc/rspamd/local.d/maps/whitelist_dynamic_addr.map`	Lista de direcciones exactas (una por línea)	Fichero de datos, no config
`/var/log/rspamd_whitelist.log`	Log de operaciones	Fichero de log

Persistencia ante rebuilds de DA

Los ficheros `.pre.conf` son puntos de extensión del template de Exim en DirectAdmin. El template fuente (`custombuild/configure/exim/exim.conf`) contiene:

```
.include_if_exists /etc/exim.routers.pre.conf     # línea 519
.include_if_exists /etc/exim.transports.pre.conf   # línea 773
```

Estas directivas `.include_if_exists` están en el template, no solo en el fichero generado. Esto significa que:

- `build rewrite_confs` regenera `/etc/exim.conf` pero **no toca** los `.pre.conf`
- `build exim_conf` idem

- `build exim` (rebuild completo del binario) idem

Los ficheros `.pre.conf` son del usuario, no de DA. Son el único mecanismo ligero para añadir routers y transports custom sin mantener una copia completa de exim.conf.

Para rspamd, `local.d/` es el mecanismo oficial de override. DA no gestiona estos ficheros.

Instalación en un servidor nuevo

Prerequisitos

- DirectAdmin con Exim y rspamd
- rspamd con multimap configurado (al menos `local.d/multimap.conf` existente)

Pasos

1. Script:

```
# Subir rspamd_whitelist.sh al servidor
scp rspamd_whitelist.sh root@servidor:/usr/local/bin/
chmod +x /usr/local/bin/rspamd_whitelist.sh
```

2. Map files y log:

```
# Map de dominios
touch /etc/rspamd/local.d/maps/whitelist_dynamic.map
chown root:mail /etc/rspamd/local.d/maps/whitelist_dynamic.map
chmod 664 /etc/rspamd/local.d/maps/whitelist_dynamic.map

# Map de direcciones
touch /etc/rspamd/local.d/maps/whitelist_dynamic_addr.map
chown root:mail /etc/rspamd/local.d/maps/whitelist_dynamic_addr.map
chmod 664 /etc/rspamd/local.d/maps/whitelist_dynamic_addr.map

# Log
touch /var/log/rspamd_whitelist.log
chown mail:mail /var/log/rspamd_whitelist.log
chmod 644 /var/log/rspamd_whitelist.log
```

3. Exim router (prepend a `/etc/exim.routers.pre.conf` — ANTES de cualquier otro router):

```
# Dynamic whitelist via email
whitelist_pipe_router:
  driver = accept
  local_parts = whitelist
  domains = +local_domains
  condition = ${if !eq{$authenticated_id}{}}
  transport = whitelist_pipe_transport
```

4. Exim transport (crear o añadir a `/etc/exim.transports.pre.conf`):

```
# Dynamic whitelist pipe transport
whitelist_pipe_transport:
  driver = pipe
  command = /usr/local/bin/rspamd_whitelist.sh
  user = mail
  environment = AUTH_USER=$authenticated_id
```

5. rspamd multimap (añadir a `/etc/rspamd/local.d/multimap.conf`):

```
WHITELIST_FROM_DYNAMIC {
    type = "from";
    filter = "email:domain";
    map = "/etc/rspamd/local.d/maps/whitelist_dynamic.map";
    symbol = "WHITELIST_FROM_DYNAMIC";
    score = -100.0;
    description = "Dynamic whitelist — added via email by authenticated users";
}

WHITELIST_ADDR_DYNAMIC {
    type = "from";
    filter = "email:addr";
    map = "/etc/rspamd/local.d/maps/whitelist_dynamic_addr.map";
    symbol = "WHITELIST_ADDR_DYNAMIC";
    score = -100.0;
    description = "Dynamic whitelist (address) — specific sender addresses added via email";
}
```

6. Verificar y reiniciar:

```
exim -bV                    # Syntax check Exim
rspamadm configtest         # Syntax check rspamd
systemctl restart exim
systemctl restart rspamd
systemctl is-active exim rspamd
```

Verificación

```
# Comprobar que el router es el primero
exim -bP router_list | head -5

# Comprobar que rspamd carga los símbolos
rspamadm configdump multimap | grep -A3 "WHITELIST.*DYNAMIC"

# Test de routing (debe resolver al pipe transport)
exim -bt whitelist@undominiodel.servidor
```

Operaciones de mantenimiento

Ver whitelist actual:

```
echo "=== Dominios ===" && cat /etc/rspamd/local.d/maps/whitelist_dynamic.map
echo "=== Direcciones ===" && cat /etc/rspamd/local.d/maps/whitelist_dynamic_addr.map
```

Ver log de operaciones:

```
cat /var/log/rspamd_whitelist.log
```

Añadir/eliminar manualmente:

```
# Añadir dominio
echo "dominio.com" >> /etc/rspamd/local.d/maps/whitelist_dynamic.map

# Añadir dirección
echo "user@dominio.com" >> /etc/rspamd/local.d/maps/whitelist_dynamic_addr.map

# Eliminar (dominios)
sed -i '/^dominio\.com$/d' /etc/rspamd/local.d/maps/whitelist_dynamic.map
```

```
# Eliminar (direcciones)
sed -i '/^user@dominio\.com$/d' /etc/rspamd/local.d/maps/whitelist_dynamic_addr.map
```

rspamd recarga el map file automáticamente en ~10 segundos.

Vaciar whitelist:

```
> /etc/rspamd/local.d/maps/whitelist_dynamic.map
> /etc/rspamd/local.d/maps/whitelist_dynamic_addr.map
```

Trampas conocidas

- **Lock file:** NO usar `/var/lock/` ni `/run/lock/` — están montados con `noexec` y bash no puede abrir file descriptors ahí. El script usa el LOG file como target de `flock` (advisory lock, no interfiere con appends)
- **Permisos map files:** deben ser `root:mail 664`. Si se crean como root durante tests, el transport Exim (que corre como `user = mail`) no podrá escribir. Verificar con `ls -la /etc/rspamd/local.d/maps/whitelist_dynamic*.map`
- **El directorio `/etc/rspamd/local.d/maps/` es `root:root 755`:** mail no puede crear ficheros nuevos ahí. El script escribe directamente al map file (que sí tiene permiso de grupo). La operación `del` usa redirección en memoria en vez de fichero temporal
- **Tests manuales como root:** crean lock/map/log files con ownership `root:root`. Tras tests manuales, verificar y corregir permisos: `chown root:mail /etc/rspamd/local.d/maps/whitelist_dynamic*.map`

Servidores desplegados

Servidor	Fecha	Estado
kvm456	2026-03-11	Activo, probado (v3: dominios + direcciones + respuesta email)
srv120	2026-03-11	Activo
srv121	2026-03-11	Activo
dar	2026-03-11	Activo

No aplica: titrit (no recibe correo), amazzal (no recibe correo)

Revision #3
Created 2026-03-10 05:39:47 UTC by Abkrim
Updated 2026-03-11 06:07:24 UTC by Abkrim