Tuning de rspamd en DirectAdmin — Guía post-instalación

Por qué hace falta

DirectAdmin instala rspamd via CustomBuild pero lo entrega **sin configuración operativa**:

- **Bayes:** backend SQLite (lento, sin concurrencia), `per_user=true` (cada usuario necesita 200+ muestras propias — inalcanzable en hosting compartido), sin autolearn, sin entrenamiento
- **Thresholds:** defaults muy permisivos (reject=15, add_header=6)
- **ESF (Easy Spam Fighter):** otorga -60 puntos acumulados a cualquier correo con SPF+DKIM+rDNS válidos — blinda spam reenviado via Google Groups
- **Sin phishing.conf:** OpenPhish desactivado por defecto desde rspamd 3.14.3
- **Sin url_suspect.conf:** patrones de URL ofuscada pueden generar falsos positivos en footers HTML

Resultado: rspamd funciona solo con reglas estáticas, Bayes nunca contribuye, y un spam con autenticación válida llega al INBOX.

Ficheros a crear

La receta completa son **8 ficheros** en `/etc/rspamd/local.d/` (que DA nunca toca) + 1 en ESF:

1. `/etc/rspamd/local.d/actions.conf` — Thresholds globales

```
# Thresholds globales rspamd
# reject = null → NUNCA rechazar correo (solo marcar)
# add_header = 5 → marca como spam a partir de score 5

reject = null;
```

```
add_header = 5;
rewrite_subject = 8;
greylist = null;
```

Decisión clave: `reject = null`. NUNCA rechazar correo por score rspamd en hosting compartido. El riesgo de rechazar un falso positivo legítimo es mayor que el coste de marcar. El usuario puede revisar su carpeta spam.

2. `/etc/rspamd/local.d/classifier-bayes.conf` — Bayes con Redis

```
# Bayes con Redis — obligatorio para rendimiento y concurrencia
# per_user = false: pool global, obligatorio para <50 usuarios

backend = "redis";
autolearn = true;

autolearn {
    spam_threshold = 8.0;
    ham_threshold = -1.0;
    min_balance = 0.9;
    min_learns = 100;
}

per_user = false;

# Conexión Redis — DA usa socket, NO localhost:6379
servers = "/var/lib/rspamd/.redis/redis.sock";
```

Trampas:

- **`per_user = false` es obligatorio** para servidores <50 usuarios. Con `per_user=true`, cada usuario necesita 100+ spam y 100+ ham propios — nunca se alcanza
- **Redis en DA no es el estándar.** El servicio se llama `redis-rspamd.service`, no `redis-server`. El socket está en `/var/lib/rspamd/.redis/redis.sock`
- **Verificar Redis:** `systemctl is-active redis-rspamd.service`

3. `/etc/rspamd/local.d/groups-override.conf` — Neutralizar MAILLIST

```
# Neutralizar símbolo MAILLIST — beneficia spam via Google Groups
symbols {
    "MAILLIST" {
        weight = 0.0;
        description = "Neutralized - mailing lists benefit spam forwarding";
    }
}
```

4. `/etc/rspamd/local.d/multimap.conf` — Penalizaciones y whitelists

```
# Penalizar mailing lists de dominios sospechosos
FOREIGN_MAILLIST {
    type = "header";
    header = "List-Id";
    map = "/etc/rspamd/local.d/maps/foreign_maillist_domains.map";
    regexp = true;
    score = 4.0;
    description = "Foreign mailing list domain in List-Id";
}

GOOGLE_GROUPS_FOREIGN {
    type = "header";
    header = "X-Beenthere";
    map = "/etc/rspamd/local.d/maps/foreign_maillist_domains.map";
    regexp = true;
    score = 3.0;
    description = "Google Groups with foreign domain in X-Beenthere";
}

# Whitelist de dominios confianza
WHITELIST_FROM {
    type = "from";
    filter = "email:domain";
    map = "/etc/rspamd/local.d/maps/whitelist_from.map";
    symbol = "WHITELIST_FROM_TRUSTED";
    score = -100.0;
    description = "Whitelisted trusted sender — domain match";
```

```
}
```

Trampas multimap:

- `filter = "email:domain"` **es OBLIGATORIO** para whitelists por dominio. Sin él, rspamd matchea la dirección completa contra el literal del mapa — nunca coincide
- **Dominios sin `@` en el mapa** — `castris.com`, NO `@castris.com`
- **NUNCA usar `prefilter=true` + `action="no action"` como whitelist** — no funciona de forma fiable. Usar `score = -100.0` es la forma correcta
- `regexp:///path` como protocolo de mapa no funciona — usar `map = "/path"; regexp = true;` como campos separados

5. `/etc/rspamd/local.d/maps/foreign_maillist_domains.map`

```
# Dominios de mailing lists sospechosos (regex)
/go1001000\.com/
/googlegroups\.com/
```

Añadir nuevos dominios según aparezcan en spam. rspamd recarga mapas automáticamente (~10s).

6. `/etc/rspamd/local.d/maps/whitelist_from.map`

```
# Dominios de confianza (uno por línea, sin @)
castris.com
aichadigital.es
tabratino.com
```

7. `/etc/rspamd/local.d/phishing.conf` — Activar OpenPhish

```
# OpenPhish desactivado por defecto desde rspamd 3.14.3
# Activar explícitamente para detección de phishing
openphish_enabled = true;
```

8. `/etc/rspamd/local.d/url_suspect.conf` — Desactivar word_dot

```
# El patrón word_dot genera falsos positivos en footers HTML
# (ej: "reservados. skyp" → URL_OBFUSCATED_TEXT score 9.0)
# Afecta correos WHMCS, PHPMailer, cualquier footer con "frase. Dominio"
checks {
    obfuscated_text {
        patterns_enabled {
            word_dot = false;
        }
    }
}
```

Contexto: `URL_OBFUSCATED_TEXT` es un prefilter con score 5.0 hardcoded en `url_suspect.lua`. Ni `groups-override.conf` ni `override.d/` pueden cambiar el peso. La única solución es desactivar el patrón causante.

9. `/etc/exim.easy_spam_fighter/variables.conf.custom` — Reducir scores ESF

```
# Reducir scores ESF de -60 acumulado a -15
# El default blinda spam con autenticación válida (SPF+DKIM+rDNS = -60)
EASY_SPF_PASS == -5
EASY_DKIM_PASS == -5
EASY_FORWARD_CONFIRMED_RDNS == -5

# No rechazar correo por score ESF (nunca)
EASY_HIGH_SCORE_DROP == 9999

# Escanear correos hasta 15MB (default 200K omite adjuntos)
EASY_SPAMASSASSIN_MAX_SIZE == 15M
```

```
# Penalizaciones reducidas (evitar falsos positivos por forwarding)
EASY_DKIM_FAIL == 0
EASY_NO_REVERSE_IP == 30
EASY_SPF_FAIL == 50
EASY_SPF_SOFT_FAIL == 10
```

Trampas ESF:

- **Usar `==` para redefinir macros**, no `=`. Con `=` simple, Exim falla: "macro already defined (use ==)"
- **`variables.conf.custom` se incluye via `.include_if_exists`** al final de `variables.conf`. DA regenera `variables.conf` pero NUNCA toca el `.custom`

DNS resolvers — CRÍTICO para servidores de correo

rspamd consulta listas de reputación (Spamhaus ZEN, SURBL, URIBL) via DNS. Si el resolver está bloqueado, todas estas listas devuelven "not found" y el spam pasa sin penalización.

Resolvers válidos para DNSBL:

Resolver	IP	Spamhaus
Verisign	64.6.64.6	
Neustar	199.85.126.10	
Neustar Ultra	156.154.70.2	

NUNCA usar en servidores de correo:

Resolver	IP	Spamhaus
Google	8.8.8.8	Bloqueado
Cloudflare	1.1.1.1	Bloqueado
Quad9	9.9.9.9	Bloqueado
OVH	213.186.33.99	Bloqueado

Verificación:

```
# Debe devolver 127.0.0.2, 127.0.0.4 o 127.0.0.10
dig +short 2.0.0.127.zen.spamhaus.org
```

```
# Si devuelve NXDOMAIN o 127.255.255.254 → resolver bloqueado
```

Síntomas de DNSBL ciegas en rspamd: símbolos `DBL_BLOCKED_OPENRESOLVER`, `URIBL_BLOCKED`, `SURBL_BLOCKED` en las cabeceras X-Spamd-Result.

Cambiar DNS en Ubuntu (netplan):

```
# Editar /etc/netplan/*.yaml → nameservers: [64.6.64.6, 199.85.126.10, 156.154.70.2]
netplan apply
systemctl restart systemd-networkd
systemctl restart systemd-resolved
# Verificar: dig +short 2.0.0.127.zen.spamhaus.org
```

Atención: `netplan apply` puede no aplicar DNS — requiere reiniciar `systemd-networkd` y `systemd-resolved` por separado.

Entrenamiento masivo de Bayes

Sin entrenamiento, Bayes no contribuye al scoring (necesita mínimo 200 muestras de cada clase).

```
# SPAM — desde carpetas spam de todos los usuarios
# IMPORTANTE: usar SIEMPRE controller socket, NO worker 11333
find /home/*/Maildir/.INBOX.spam/cur/ -type f 2>/dev/null | head -500 | \
  xargs -I{} rspamc --connect /var/run/rspamd/rspamd_controller.sock learn_spam {}

find /home/*/Maildir/.Junk/cur/ -type f 2>/dev/null | head -500 | \
  xargs -I{} rspamc --connect /var/run/rspamd/rspamd_controller.sock learn_spam {}

# HAM — desde INBOX y Sent de todos los usuarios
find /home/*/Maildir/cur/ -type f 2>/dev/null | head -500 | \
  xargs -I{} rspamc --connect /var/run/rspamd/rspamd_controller.sock learn_ham {}

find /home/*/Maildir/.Sent/cur/ -type f 2>/dev/null | head -500 | \
  xargs -I{} rspamc --connect /var/run/rspamd/rspamd_controller.sock learn_ham {}
```

Trampas rspamc:

- `rspamc learn_spam` **contra el worker (puerto 11333)** da "HTTP 500 invalid command". HAY QUE usar el controller socket

- `rspamc stat` **contra puerto default (11333)** da "Connection refused" en DA — usar siempre: `rspamc --connect /var/run/rspamd/rspamd_controller.sock stat`
- `redis-server` / `redis` no existen como servicio en DA — es `redis-rspamd.service`
- `exim -bP macro` (singular) no existe — el comando es `exim -bP macros` (plural)

Verificación post-training:

```
rspamc --connect /var/run/rspamd/rspamd_controller.sock stat | grep -E "learned|messages"
# Debe mostrar >200 spam y >200 ham
```

Procedimiento de aplicación

Pre-checks

```
systemctl is-active rspamd
systemctl is-active redis-rspamd.service
ls -la /etc/rspamd/local.d/
cat /etc/exim.easy_spam_fighter/variables.conf.custom 2>/dev/null || echo "NO EXISTE"
# Contar correos disponibles para training
find /home/*/Maildir/.INBOX.spam/cur/ -type f 2>/dev/null | wc -l
find /home/*/Maildir/.Junk/cur/ -type f 2>/dev/null | wc -l
```

Orden

1. `mkdir -p /etc/rspamd/local.d/maps`
2. Crear los 8 ficheros rspamd (secciones 1-8 arriba)
3. `rspamadm configtest` — verificar sintaxis
4. `systemctl reload rspamd`
5. Crear/actualizar `variables.conf.custom` (sección 9)
6. `exim -bV` — verificar sintaxis Exim
7. `systemctl restart exim`
8. Entrenamiento masivo de Bayes
9. Verificar: `rspamc stat`, enviar correo de prueba

Verificación post-aplicación

```
# rspamd
systemctl is-active rspamd
```

```
rspamadm configtest
rspamc --connect /var/run/rspamd/rspamd_controller.sock stat

# Exim
systemctl is-active exim
exim -bP macros | grep -E "EASY_(SPF|DKIM|FORWARD)"
# Debe mostrar -5 en cada macro

# Test correo: enviar email y verificar cabeceras X-Spamd-Result
```

Rollback

Todos los ficheros son independientes. Para revertir cualquier cambio, borrar el fichero y `systemctl reload rspamd`:

```
# Rollback total rspamd
rm -f /etc/rspamd/local.d/actions.conf
rm -f /etc/rspamd/local.d/classifier-bayes.conf
rm -f /etc/rspamd/local.d/groups-override.conf
rm -f /etc/rspamd/local.d/multimap.conf
rm -f /etc/rspamd/local.d/phishing.conf
rm -f /etc/rspamd/local.d/url_suspect.conf
rm -rf /etc/rspamd/local.d/maps/
systemctl reload rspamd
```

Para ESF, editar `variables.conf.custom` y eliminar las líneas añadidas, luego `systemctl restart exim`.

Servidores aplicados

Servidor	Fecha	Bayes (spam/ham)	Estado
kvm456	2026-03-04	1.035 / 873	Completo
dar	2026-03-04 (alineado 2026-03-23)	Trained	Completo
srv120	2026-03-07	567 / 448	Completo
srv121	2026-03-07	158 / 1.597	Autolearn activo (spam bajo)

Ficheros que DA gestiona — NO TOCAR

Fichero	Motivo
`/etc/rspamd/users.d/<user>.conf`	Settings per-user generados por DA
`/etc/rspamd/directadmin-users.conf`	Config global usuarios DA
`/etc/exim.easy_spam_fighter/variables.conf`	Macros ESF (el `.custom` SÍ es seguro)
`/etc/rspamd/local.d/dkim_signing.conf`	Puede ser gestionado por DA

Revision #1
Created 2026-03-24 17:31:40 UTC by Abkrim
Updated 2026-03-24 17:31:40 UTC by Abkrim