

# FAQ Anti-SPAM

Voici quoi faire pour diagnostiquer votre serveur si vous recevez un taux de spams est anormalement élevé.

## Diagnostic

### rspamd ou SpamAssassin

DirectAdmin propose le choix entre SpamAssassin ou rspamd pour contrôler les spams qui entrent sur votre serveur.

Pour connaître quel logiciel vous utiliser, utilisez la commande suivante

```
grep -rn "spamd" /usr/local/directadmin/custombuild/options.conf
```

Exemple de résultat pour rspamd:

```
63:spamd=rspamd
```

Exemple de résultat pour SpamAssassin

```
63:spamd=spamassassin
```

### Est-ce que les headers sont présent?

Si oui, on sait que le message passe par le logiciel anti-spam. Si non, assurez-vous que le logiciel fonctionne.

Vous pouvez voir les headers des e-mail en visualisant la source du e-mail en question.

### Exemples de headers qu'on recherche:

rspamd:

```
X-Spam-Score: 5.5 (+++++)
X-Spam-Report: Action: add header
Symbol: HFILTER_HOSTNAME_UNKNOWN(2.50)
Symbol: ARC_NA(0.00)
Symbol: R_DKIM_ALLOW(-0.20)
Symbol: FROM_HAS_DN(0.00)
Symbol: TO_MATCH_ENVRCPT_ALL(0.00)
Symbol: HTML_SHORT_LINK_IMG_1(2.00)
Symbol: MIME_GOOD(-0.10)
Symbol: TO_DN_NONE(0.00)
```

```

Symbol: RCPT_COUNT_ONE(0.00)
Symbol: MANY_INVISIBLE_PARTS(0.05)
Symbol: R_SPF_ALLOW(-0.20)
Symbol: DKIM_TRACE(0.00)
Symbol: DMARC_POLICY_ALLOW(-0.50)
Symbol: RCVD_COUNT_ONE(0.00)
Symbol: RCVD_NO_TLS_LAST(0.10)
Symbol: FROM_EQ_ENVFROM(0.00)
Symbol: MIME_TRACE(0.00)
Symbol: SUBJECT_ENDS_QUESTION(1.00)
Symbol: ASN(0.00)
Symbol: MID_RHS_MATCH_FROM(0.00)
Symbol: R_PARTS_DIFFER(0.75)
Symbol: ONCE_RECEIVED(0.10)
Message-ID: qhJmIOy-mIE8-zHSAHdbOz-
KklxRdXUocBeadGqvfv0.fVxgg7PgZJ_ve1MUFR9foylBAGNxxvuCPfb4LMfeiIA@treeparking
.xyz

```

SpamAssassin:

Content analysis details: (4.5 points, 2.5 required)

pts	rule name	description
-1.9	BAYES_00	BODY: Bayes spam probability is 0 to 1% [score: 0.0013]
-0.0	SPF_HELO_PASS	SPF: HELO matches SPF record
2.0	PDS_OTHER_BAD_TLD	Untrustworthy TLDs [URI: disgracecycle.xyz (xyz)]
-0.0	SPF_PASS	SPF: sender matches SPF record
0.0	HTML_MESSAGE	BODY: HTML included in message
0.0	HTML_FONT_LOW_CONTRAST	BODY: HTML font color similar or identical to background
-0.1	DKIM_VALID_AU	Message has a valid DKIM or DK signature from author's domain
0.1	DKIM_SIGNED	Message has a DKIM or DK signature, not necessarily valid
-0.1	DKIM_VALID	Message has at least one valid DKIM or DK signature
-0.1	DKIM_VALID_EF	Message has a valid DKIM or DK signature from envelope-from domain
1.4	PYZOR_CHECK	Listed in Pyzor (https://pyzor.readthedocs.io/en/latest/)
0.5	FROM_SUSPICIOUS_NTLD	From abused NTLD
0.8	RDNS_NONE	Delivered to internal network by a host with no rDNS
1.5	FROM_FMBLA_NEWDOM	From domain was registered in last 7 days
0.0	FSL_BULK_SIG	Bulk signature with no Unsubscribe
0.4	FROM_SUSPICIOUS_NTLD_FP	From abused NTLD

```
X-Old-Subject: Get a FREE Reverse Mortgage Loan info kit in 2 minutes !
Subject: *****SPAM***** Get a FREE Reverse Mortgage Loan info kit in 2
minutes !
X-Spam-Status: Yes, score=4.5, +20 total spam score
SpamTally: Final spam score: -5
```

## URIBL\_BLOCKED

Si vous avez le message suivant dans les headers des e-mails, c'est que votre serveur anti-spam ne peut pas vérifier les RBL et liste de blocage.

Assurez-vous d'avoir les bonnes informations dans le fichier `/etc/resolv.conf`

```
URIBL_BLOCKED      ADMINISTRATOR NOTICE: The query to URIBL was blocked.
                   See
http://wiki.apache.org/spamassassin/DnsBlocklists#dnsbl-block
                   for more information.
```

## Vérification / modification du fichier `/etc/resolv.conf`

```
nano /etc/resolv.conf
```

```
nameserver 127.0.0.1
```

## Est-ce que le serveur anti-spam fonctionne?

Si vous n'avez pas de headers, vous pouvez vérifier que le serveur anti-spam fonctionne avec la commande suivante:

```
ps aux | grep spam
```

Exemple de résultat pour `rspamd` qui fonctionne:

```
_rspamd  7957  0.0  0.3 433724 98256 ?        Ss   Apr16   0:05 rspamd:
main process; 0.1 msg/sec, 0.1 msg/sec spam, 0.0 msg/sec ham
root     9325  0.0  0.0 110700   892 pts/0    R+   12:17   0:00 grep --
color=auto spam
_rspamd  13916  0.0  0.2 433724 94596 ?        S    Apr16   0:01 rspamd:
rspamd_proxy process (/var/run/rspamd/rspamd_proxy.sock mode=0600
owner=_rspamd)
_rspamd  13917  0.0  0.3 434504 100832 ?       S    Apr16   0:09 rspamd:
controller process (/var/run/rspamd/rspamd_controller.sock mode=0600
owner=_rspamd)
_rspamd  13918  0.0  0.3 435456 104540 ?       S    Apr16   0:04 rspamd:
normal process (localhost:11333)
_rspamd  13919  0.0  0.3 434876 102072 ?       S    Apr16   0:04 rspamd:
normal process (localhost:11333)
```

```

_rspamd 13920 0.0 0.3 435456 104640 ? S Apr16 0:04 rspamd:
normal process (localhost:11333)
_rspamd 13921 0.0 0.3 436288 104972 ? S Apr16 0:04 rspamd:
normal process (localhost:11333)
_rspamd 13922 0.0 0.2 433724 90556 ? S Apr16 0:00 rspamd:
hs_helper process
root 28294 0.0 0.2 312588 81248 ? Ss 03:46 0:06
/usr/bin/perl -T -w /usr/bin/spamd --pidfile /var/run/spamd.pid -d -c -m 15
--ipv4
root 28300 0.0 0.2 325384 93816 ? S 03:46 0:04 spamd child
root 28301 0.0 0.2 312588 78016 ? S 03:46 0:00 spamd child

```

Exemple de résultat pour SpamAssassin qui fonctionne:

```

root 2751 0.0 0.9 305084 77712 ? Ss 12:55 0:01
/usr/bin/perl -T -w /usr/bin/spamd --pidfile /var/run/spamd.pid -d -c -m 15
--ipv4
root 3959 0.1 0.9 306352 78140 ? S 12:55 0:02 spamd child
root 3961 0.0 0.9 306184 77832 ? S 12:55 0:00 spamd child

```

Si aucun résultat essayer de partir les serveurs et vérifier que ceux-ci fonctionne

rspamd:

```
systemctl start rspamd
```

spamassassin:

```
systemctl start spamassassin
```

### Le serveur rspamd/spamassassin fonctionne mais je n'ai pas de headers

- Voir à réinstaller et reconfigurer votre serveur anti-spam
  - Installation de rspamd
  - Installation de SpamAssassin
- Assurez-vous que tous les [ports sont ouvert sur votre firewall](#)

From:  
<https://wiki.proletaire.net/> - **Wiki**

Permanent link:  
[https://wiki.proletaire.net/email/spam/faq\\_anti\\_spam?rev=1587148661](https://wiki.proletaire.net/email/spam/faq_anti_spam?rev=1587148661)

Last update: **2020/04/17 18:37**

