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 controler 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=spamassasssin
```

Est-ce que les headers sont présent?

Si oui, le message est scanner correctement 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: qhJmI0y-mIE8-zHSAHdbOz-
KklxRdXUocBeaDGqvfvo.fVxgg7PgzJ_velMUFR9foy1BAGNxxvuCPfb4LMfeiIA@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
```