Atelier - Anomalie #1841

Montée de charge à 142 sur la machine drupal6

21/12/2016 16:42 - Christian P. Momon

Statut:	Fermé	**Début:**	21/12/2016
Priorité:	Normale	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:		**Temps passé:**	0.00 heure

Description

Ce matin, sur le canal IRC :

```
05:33 <vivivi[6]> [00] drupal6:LOAD is CRITICAL: CRITICAL - load average: 142.48, 98.64, 44.84
05:34 <vivivi[6]> [01] bastion:Check Web libre-et-accessible.org is CRITICAL: CRITICAL - Socket ti
meout after 10 seconds
05:34 <vivivi[6]> [02] bastion:Check Secure Web libre-et-accessible.org is CRITICAL: CRITICAL - So
cket timeout after 10 seconds
05:35 * vivivi[6] s'appelle maintenant vivivi[3]
05:39 * vivivi[3] s'appelle maintenant vivivi[1]
05:39 <vivivi[1]> bastion:Check Web libre-et-accessible.org is OK: HTTP OK: Status line output mat
ched 200 - 5947 bytes in 0.184 second response time
05:39 <vivivi[1]> bastion:Check Secure Web libre-et-accessible.org is OK: HTTP OK: Status line out
put matched 200 - 5973 bytes in 0.184 second response time
06:03 <vivivi[1]> [03] drupal6:LOAD is WARNING: WARNING - load average: 0.17, 0.65, 8.44
06:13 <vivivi[1]> drupal6:LOAD is OK: OK - load average: 0.10, 0.23, 4.50
```

Avec QGull, en regardant les logs nginx pour le site april.org, on voit beaucoup de « /april?page=%2C1&membre= »:

```
208.89.210.30 - - [21/Dec/2016:05:33:32 +0100] "GET /april?page=2124&amp;membre=aphxxx HTTP/1.1" 2
00 9065 "https://www.april.org/april?page=%2C1&amp;membre=crexxx" "Mozilla/5.0 (Windows NT 10.0; W
OW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36"
93.127.147.151 - - [21/Dec/2016:05:33:32 +0100] "GET /april?page=99&amp;membre=ctoxxx HTTP/1.1" 20
0 10069 "https://www.april.org/april?page=%2C7&amp;membre=scrxxx" "Mozilla/5.0 (Windows NT 10.0; W
OW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36"
158.222.6.214 - - [21/Dec/2016:05:33:32 +0100] "GET /april?page=2124&amp;membre=lsaxxx HTTP/1.1" 2
00 9059 "http://www.fraifrai.net/index.php?post/2013/11/15/Gravity-%3A-non-mais...-non" "Mozilla/5
.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537
.36"
66.34.168.45 - - [21/Dec/2016:05:33:32 +0100] "GET /april?page=%2C5&amp;membre=aphxxx HTTP/1.1" 20
0 9996 "https://www.april.org/april?page=%2C1&amp;membre=ggrxxx" "Mozilla/5.0 (Windows NT 10.0; WO
W64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36"
104.203.245.104 - - [21/Dec/2016:05:33:33 +0100] "GET /april?page=2124&amp;membre=ctoxxx HTTP/1.1"
 200 9067 "https://www.april.org/april?page=2124&amp;membre=groxxx" "Mozilla/5.0 (Windows NT 10.0;
 WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36"
66.34.168.45 - - [21/Dec/2016:05:33:33 +0100] "GET /april?page=%2C4&amp;membre=aphxxx HTTP/1.1" 20
0 10002 "https://www.april.org/april?page=%2C3&amp;membre=fdexxx" "Mozilla/5.0 (Windows NT 10.0; W
OW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36"
```

Et les requêtes viennent de plusieurs IP différentes :

```
root@bastion:~/Cpm# grep "2016:05:3" www.april.org.access_log.1 | grep 'membre=' | cut -f 1 -d ' '
 | sort -n -k 1,1 -k 2,2 -k 3,3 -k 4,4 | uniq -c | sort -n -k 1,1 | tail
    190 5.157.15.20
    190 66.34.168.45
    193 5.157.15.107
    200 104.203.245.104
    200 208.89.210.30
    204 155.94.244.48
    204 93.127.147.151
    213 199.229.235.82
```

```
    213 204.44.83.97
    227 204.44.83.12
```

Difficile de conclure. Un bot visant un site Drupal ?

Ticket créé pour laisser une trace et donc fermé de suite.

Historique

#1 - 21/12/2016 17:04 - Christian P. Momon

- Description mis à jour