Admins - Anomalie #3532

Le filesystem de la VM Drupal partie Mysql se remplit dangereusement

02/01/2019 15:08 - Frédéric Couchet

Statut:	Fermé	**Début:**	02/01/2019
Priorité:	Immédiate	**Echéance:**	
Assigné à:	Christian P. Momon	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Janvier 2019	**Temps passé:**	0.00 heure
Difficulté:	2 Facile		

Description

Salut,

ce mercredi 2 janvier 2019 matin le site www.april.org était down :

```
Erreur 50x - Le service demandé n'est pas accessible pour le moment
```

/var/lib/mysql était à 100%

Il y avait dans /var/lib/mysql/drupal6 deux fichiers watchdog-170409101709.BAK watchdog-181030225617.BAK qui prenaient 1,6 Go,
je les ai déplacé dans ~root. Mais je pense qu'on peut les supprimer, je
vous laisse juges.

/var/lib/mysql est ensuite à 58%.

Le site est de retour.

Mais vers 15h00 j'ai noté que /var/lib/mysql était à 89% avec notamment un fichier drupal6/watchdog.MYD de 1,2 Go.

Il faudrait voir si une config a été modifiée au niveau du Drupal qui générerait ce problème.

Ou alors c'est en lien avec https://agir.april.org/issues/1919.

Demandes liées:

Lié à Admins - Demande #6364: /var plein sur drupal6	**Résolu**	**27/02/2024**

Historique

#1 - 02/01/2019 17:16 - Christian P. Momon

A priori, un fichier watchdog de Mysql qui grandit est un signe d'activité du site web l'utilisant.

Dans les logs Apache, détection d'une IP qui floode un peu (1 000 000 de requêtes depuis hier) :

```
(April) root@drupal6:/var/log/apache2# zgrep -n 42.49.180.xx www.april.org.access.log |wc -l
227493
(April) root@drupal6:/var/log/apache2# zgrep -n 42.49.180.xx www.april.org.access.log.1 |wc -l
798642
(April) root@drupal6:/var/log/apache2# head -1 www.april.org.access.log www.april.org.access.log.1
==> www.april.org.access.log <==
109.234.x.x - - [02/Jan/2019:06:25:24 +0100] "GET /lav.xml HTTP/1.0" 200 664657 "-" "-"

==> www.april.org.access.log.1 <==
109.234.x.x - - [01/Jan/2019:06:25:28 +0100] "GET /lav.xml HTTP/1.0" 200 664657 "-" "-"
```

Les requêtes ne sont pas gentilles :

```
"GET /en/category/ HTTP/1.0" 404 22282 "https://www.april.org:443/" "uB8ZDnn6';select pg_sleep(3); --"
"GET /en/category/ HTTP/1.0" 404 22282 "https://www.april.org:443/" "CKZULjdk');select pg_sleep(6); --"
"GET /en/print/node HTTP/1.0" 200 6888 "https://www.april.org:443/" "Xz2SwCKV'));select pg_sleep(9); --"
"GET /en/category/ HTTP/1.0" 404 22282 "https://www.april.org:443/" "9QghF5Ig'));select pg_sleep(6); --"
"GET /en/print/node HTTP/1.0" 200 6888 "https://www.april.org:443/" "(select convert(int,CHAR(65)))"
```

```
"GET /en/category/themes/ HTTP/1.0" 404 18649 "https://www.april.org:443/" "(select(0)from(select(sleep(6)))v)
/*'+(select(0)from(select(sleep(6)))v)+'\"+(select(0)from(select(sleep(6)))v)
```

L'IP semble être utilisée en Chine :

```
whois 42.49.180.xx
[…]
inetnum:        42.48.0.0 - 42.49.255.255
netname:        UNICOM-HN
descr:          China Unicom HuNan province network
descr:          China Unicom
descr:          No.21,Jin-Rong Street,
descr:          Beijing 100033
country:        CN
```

Ban de l'IP sur la VM bastion dans */etc/nginx/sites-available/sites-enabled/www.april.org* :

```
location / {
    # Ban IP from cracker generating huge Mysql watchdog file (#3532).
    deny 42.49.180.18;

    proxy_pass http://172.16.0.7;
}
```

Constatation : le fichier watchdog de Mysql grandit 5 fois moins vite : passe de ~30Mo/h à ~5Mo/h.

À étudier :

- débannir l'ip ;
- consolider l'espace disque Mysql pour résister à de « plus » fortes sollicitations.

#2 - 02/01/2019 17:16 - Christian P. Momon

- Statut changé de Nouveau à En cours de traitement

#3 - 03/01/2019 10:16 - Quentin Gibeaux

À noter qu'on a eu un cas un peu similaire de spam (mais juste un crawl) le mois dernier : https://agir.april.org/issues/3524
J'avais bloqué directement via iptables sur bastion

#4 - 04/01/2019 11:30 - François Poulain

J'ai aussi réduit au minimum (100) le crappy log de drupal dans https://www.april.org/admin/settings/logging/dblog qui pourri la table watchdog. J'ai forcé le cron via https://www.april.org/admin/reports/status

#5 - 10/01/2019 11:51 - Quentin Gibeaux

- Assigné à mis à Christian P. Momon

#6 - 10/01/2019 11:52 - Quentin Gibeaux

- Version cible changé de Décembre 2018 à Janvier 2019

#7 - 10/01/2019 12:24 - Quentin Gibeaux

Débannir l'IP et vérifier si l'attaque continue

#8 - 12/01/2019 12:39 - Christian P. Momon

IP débannie et constat de l'absence de requête depuis cette IP.

#9 - 12/01/2019 12:39 - Christian P. Momon

- Statut changé de En cours de traitement à Résolu

#10 - 30/01/2019 21:29 - Quentin Gibeaux

- Statut changé de Résolu à Fermé

#11 - 27/02/2024 01:56 - Pierre-Louis Bonicoli

- Lié à Demande #6364: /var plein sur drupal6 ajouté