Admins - Anomalie #3724

Les logs fail2bans ne sont jamais purgées

31/05/2019 02:15 - Christian P. Momon

Statut:	Fermé	**Début:**	31/05/2019
Priorité:	Normale	**Echéance:**	
Assigné à:	Romain H.	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Février 2020	**Temps passé:**	0.00 heure
Difficulté:	2 Facile		

Description

Détecté sur le Chapril avec des fichiers fail2ban.sqlite3 de 1,3 Go : #3723.

État pour le SI de l'April :

```
===== virola.april.org =====
-rw------- 1 root root 706M May 31 00:08 /var/lib/fail2ban/fail2ban.sqlite3
===== calamus.april.org =====
-rw------- 1 root root 257M May 31 00:08 /var/lib/fail2ban/fail2ban.sqlite3
===== galanga.april.org =====
-rw------- 1 root root 269M May 31 02:08 /var/lib/fail2ban/fail2ban.sqlite3
===== galanga.april.org =====
-rw------- 1 root root 812M mai   31 02:10 /var/lib/fail2ban/fail2ban.sqlite3
```

Les lignes de bans ne sont jamais purgées dans la base de données.

Questions :

- Y-a-t-il une utilité à conserver le log de tous les bans ?
- Est-ce grave si le fichier grossit indéfiniment ?
- Purge automatique ou purge manuelle ?
- Ajout d'une sonde pour détecter une taille excessive de la base Fail2ban ? À partir de quelle taille la jugée excessive ?

Historique

#1 - 31/05/2019 02:17 - Christian P. Momon

- Sujet changé de Les logs fail2bans ne sont jamais purgés à Les logs fail2bans ne sont jamais purgées

#2 - 29/01/2020 18:32 - Christian P. Momon

- Statut changé de Nouveau à Confirmé

- Version cible changé de Backlog à Janvier 2020

Le phénomène est à nouveau devenu gênant aujourd'hui, notamment sur virola.
Action de QGuLL :

```
18:06 < QGuLL>  3614  Wed 29 Jan 2020 01:47:27 PM UTC /usr/bin/sqlite3  -echo fail2ban.sqlite3  "delete FROM b
ans where timeofban < strftime('%s','now','-30 day'); SELECT changes(); vacuum"
18:09 < QGuLL> j'ai fais que la commande sql
18:10 < QGuLL> j'ai stoppé fail2ban
18:10 < QGuLL> j'ai lancé le sqlite
18:10 < QGuLL> le fs était hs
18:10 < QGuLL> la charge montait sur toute l'infra
18:10 < QGuLL> j'ai fait ctrl-c
18:10 < QGuLL> j'ai mv
18:10 < QGuLL> j'ai fait start fail2ban, il a refait un sqlite vierge
18:10 < QGuLL> et là à 18h j'ai rm le mv que j'avais laissé de côté
```

Comme indiqué sur le gestionnaire de ticket du projet officiel :

```
I've said already several times, purge will never called (only in test case):
```

Donc sur tout le SI, il faut mettre en place :

- un script ;
- un cron ;
- et une sonde (qui vérifie le cron et l'âge maxi des entrées de la base).

#3 - 29/01/2020 22:25 - Quentin Gibeaux

- Assigné à mis à Romain H.

#4 - 29/01/2020 22:25 - Quentin Gibeaux

- Version cible changé de Janvier 2020 à Février 2020

#5 - 22/02/2020 14:55 - Romain H.

- Statut changé de Confirmé à En cours de traitement

#6 - 23/02/2020 20:48 - Romain H.

- Statut changé de En cours de traitement à Résolu

- % réalisé changé de 0 à 100

J'ai ajouté la cron et la supervision sur :

- bastion
- mail
- virola
- calamus
- galanga
- guarana

La cron supprime les entrées >= 30 jours, tous les matins à 6h30.
La supervision surveille qu'il n'y a pas d'entrée >= 31 jours.

Comme la DB est accessible uniquement par root, j'ai rajouté une configuration à *sudo* pour permettre à l'utilisateur *nagios* d'exécuter le script.

Les DB de *calamus* , *galanga* et *guarana* étaient trop grosses pour permettre l'exécution du script sans faire beaucoup d'I/O, j'ai réinitialisé la DB.

#7 - 26/02/2020 22:17 - Quentin Gibeaux

- Statut changé de Résolu à Fermé