Infra Chapril - Anomalie #3723

Les logs fail2bans ne sont jamais purgées

31/05/2019 02:04 - 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:	Sprint 2020 novembre		

Description

En investiguant une alerte de Chatonic à propos d'espace disque sur coon:/var (résolue par un apt-get clean), constat que le fichier /var/lib/fail2ban est énorme : 1,3 Go.

Or :

```
=(^-^)=root@coon:/var/lib/fail2ban# df -h /var/
Sys. de fichiers        Taille Utilisé Dispo Uti% Monté sur
/dev/mapper/vg_coon-var   3,9G    3,2G  480M  87% /var
```

Et :

```
===== maine.chapril.org =====
-rw------- 1 root root 1,2G mai   31 00:50 /var/lib/fail2ban/fail2ban.sqlite3
Connection to maine.chapril.org closed.
===== coon.chapril.org =====
-rw------- 1 root root 1,3G mai   31 00:50 /var/lib/fail2ban/fail2ban.sqlite3
```

Puisque la mission de Fail2ban agit sur de courtes périodes (de quelques minutes à quelques jours), les 1,3 Go de données utiles sont difficilement justifiables.

En regardant dans la base de données, on constate qu'il y a **1 560 462** logs de ban en base:

```
=(^-^)=root@maine:/var/lib/fail2ban# sqlite3 copy.sqlite3
SQLite version 3.16.2 2017-01-06 16:32:41
Enter ".help" for usage hints.
sqlite> select count(*) from bans;
1560462
```

Et que le plus ancien ban stocké date de la mise en place de la plateforme :

```
sqlite> select timeofban from bans order by timeofban asc limit 5;
1496480937
1496481650
1496482371
1496483093
1496483795
sqlite> ^Z
=(^-^)=root@maine:/var/lib/fail2ban# date -d @1496480937
samedi 3 juin 2017, 11:08:57 (UTC+0200)
```

Conclusion : les logs de Fail2ban ne sont pas purgées.

Pourtant, Fail2ban est configuré pour ne pas conserver le log d'un ban plus de 24 heures :

```
=(^-^)=root@maine:/var/lib/fail2ban# fail2ban-client get dbpurgeage
Current database purge age is:
`- 86400seconds
```

Il semble que la non purge automatique soit un phénomène répandu et normal :

- https://github.com/fail2ban/fail2ban/issues/1316#issuecomment-178796884 : « dbpurgeage currently does not affect (because no purge takes place at all, only in test cases currently)... »
- https://github.com/fail2ban/fail2ban/issues/1267#issuecomment-162590924 : « I've said already several times, purge will never called (only in test case): »

Pas trouvé d'infos de l'intégration dans Debian.

Questions :

- Y-a-t-il une utilité à conserver le log de tous les bans ?
- 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 02:18 - Christian P. Momon

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

#2 - 04/03/2020 18:47 - Christian P. Momon

- Projet changé de Chapril à Infra Chapril

#3 - 04/03/2020 21:44 - Romain H.

- Assigné à mis à Romain H.

#4 - 01/04/2020 16:50 - Romain H.

- Statut changé de Nouveau à En cours de traitement

#5 - 01/04/2020 17:50 - Christian P. Momon

- Version cible mis à Backlog

#6 - 29/11/2020 19:09 - Romain H.

- Statut changé de En cours de traitement à Résolu

- % réalisé changé de 0 à 100

J'ai rajouté la cron et le script dans sexy-chapril version 1.19.
J'ai mis à jour le paquet sur les VM.
Pour bastion l'historique était trop gros et faisait plein d'IO, j'ai reset la base sqlite3.

#7 - 02/12/2020 23:24 - Romain H.

- Statut changé de Résolu à Fermé

#8 - 03/12/2020 00:54 - Christian P. Momon

- Version cible changé de Backlog à Sprint 2020 novembre