Admins - Anomalie #4218

Problème de swap sur la vm mail

25/01/2020 09:39 - Christian P. Momon

Statut:	Fermé	**Début:**	25/01/2020
Priorité:	Normale	**Echéance:**	
Assigné à:	Romain H.	**% réalisé:**	100%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Mai 2020	**Temps passé:**	0.00 heure
Difficulté:	2 Facile		

Description

La supervision informe que :

```
Mail       SWAP WARNING - 32% free (301 MB out of 951 MB)
```

Vérification :

```
(April) root@mail:~# free -m
              total        used        free      shared  buff/cache   available
Mem:           1994         721         166          20        1107        1073
Swap:           951         650         301
(April) root@mail:~# psswap |head
clamd 2408 580852 kB
systemd-journal 247 42472 kB
postgrey --pidf722 16976 kB
opendkim 672 7008 kB
amavis-mc 807 3708 kB
icinga2 563 3596 kB
systemd-udevd 264 1584 kB
freshclam 441 1412 kB
icinga2 721 1296 kB
nginx 574 1192 kB
```

Ce n'est pas la première fois. Que faire ?

- augmenter la RAM : mais elle est déjà à 2 Go ;
- limiter clamd : trouver un paramètre de configuration permettant de limiter l'usage de la RAM ;
- autre ?

Historique

#1 - 25/01/2020 09:40 - Christian P. Momon

- Description mis à jour

#2 - 25/01/2020 09:45 - Christian P. Momon

En attendant, mesure curative manuelle :

```
(April) root@mail:~# free -m
              total        used        free      shared  buff/cache   available
Mem:           1994         721         166          20        1107        1073
Swap:           951         650         301
(April) root@mail:~# systemctl restart clamav-daemon.service
(April) root@mail:~# free -m
              total        used        free      shared  buff/cache   available
Mem:           1994         641         239          19        1114        1154
Swap:           951          84         867

(April) root@mail:~# swapoff -a && swapon -a
(April) root@mail:~# free -m
```

```
              total        used        free      shared  buff/cache   available
Mem:           1994        1276          74          20         643         520
Swap:           951           0         951
```

#3 - 26/01/2020 11:36 - Christian P. Momon

- Statut changé de Nouveau à En cours de traitement

- Assigné à mis à Christian P. Momon

Au bout d'un jour, ça recommence :

```
(April) root@mail:/etc/clamav[master$]# free -m
              total        used        free      shared  buff/cache   available
Mem:           1994         537         326          20        1130        1257
Swap:           951         820         131
(April) root@mail:/etc/clamav[master$]# psswap |head
clamd 4586 732784 kB
systemd-journal 247 44408 kB
/usr/sbin/amavi 22086 20080 kB
postgrey --pidf722 16204 kB
/usr/sbin/amavi 12346 12168 kB
/usr/sbin/amavi 12388 12160 kB
opendkim 672 5560 kB
icinga2 563 3592 kB
amavis-mc 807 3324 kB
icinga2 721 1280 kB
```

#4 - 29/01/2020 21:27 - Quentin Gibeaux

- Assigné à changé de Christian P. Momon à Romain H.

- Version cible changé de Janvier 2020 à Février 2020

#5 - 26/02/2020 22:33 - Quentin Gibeaux

- Version cible changé de Février 2020 à Mars 2020

#6 - 06/03/2020 23:52 - Christian P. Momon

Situation du 06/03/2020 vers 23h43 :

```
23:41 < vivivi[5]> [04] mail:SWAP is CRITICAL: SWAP CRITICAL - 2% free (9 MB out of 951 MB)

(April) root@mail:~# psswap |head
clamd 10283 756196 kB
/usr/sbin/amavi 7168 89912 kB
systemd-journal 246 64296 kB
/usr/sbin/amavi 10508 53268 kB
/usr/sbin/amavi 10513 49880 kB
postgrey --pidf781 16916 kB
opendkim 616 11264 kB

(April) root@mail:~# free -m
              total        used        free      shared  buff/cache   available
Mem:           1994         588         353          20        1052        1208
Swap:           951         941          10
```

A priori, tout est dans les buffers…

Situation après un clearswap :

```
(April) root@mail:~# free -m
              total        used        free      shared  buff/cache   available
Mem:           1994        1378         162          14         453         428
Swap:           951          74         877
```

#7 - 25/03/2020 22:04 - Quentin Gibeaux

- Version cible changé de Mars 2020 à Avril 2020

#8 - 29/04/2020 22:13 - Quentin Gibeaux

- Version cible changé de Avril 2020 à Mai 2020

#9 - 01/05/2020 13:03 - Romain H.

Clamav bloque bien quelques menaces même si elles ne sont pas nombreuses.
Depuis le 23 février il y a eu 16 blocages :

Nom de la signature	Nombre de mail
Email.Phishing.VOF1-6331187-0	1
Email.Phishing.VOF2-6338307-1	1
Win.Trojan.Ponystealer-7648176-0	1
Win.Packed.Razy-7486442-0	1
Pdf.Dropper.Agent-7598556-0	1
Heuristics.Phishing.Email.SpoofedDomain	1
Xls.Dropper.Agent-7586492-0	1
Win.Virus.Tainp-1	7
Win.Dropper.Smdd-6956905-0	2

Amavis dans sa configuration liste d'autres antivirus mais aucun ne semble plus adapté :

antivirus	avis
Sophie	semble mort
Sophos	pas libre
OpenAntiVirus	semble mort
Trophie	semble mort
AVG Ani-Virus	pas libre
F-Prot	pas libre
DrWebD	pas libre
KasperskyLab	pas libre
CentralCommand Vexira	semble mort
Avira AntiVir	pas libre
Command Antivirus	semble mort
Symantec	pas libre
F-Secure	pas libre
Avast	pas libre
CAI eTrust Antivirus	semble mort
MkS_Vir	pas libre
ESET NOD32	pas libre
Norman Virus Control	mort (racheté par AVG)
Panda CommandLineSecure	pas libre
GeCAD RAV Antivirus	mort (racheté par Microsoft)
NAI McAfee	pas libre
VirusBuster	mort (racheté par Sophos)
CyberSoft VFind	pas libre
Ikarus Antivirus	pas libre
BitDefender	pas libre
ArcaVir	pas libre
File::scan	semble plus mis à jour et pas vraiment efficace

Le passage à Rspamd pourrait simplifier la configuration mais je ne pense pas qu'il réduira la consommation en mémoire comme il faut tout de même un Antivirus derrière. La doc sur https://rspamd.com/doc/modules/antivirus.html semble indiquer que le choix naturel est aussi Clamav.

L'occupation en mémoire de clamavd semble être lié à la taille de la base de signature qu'il utilise. Je n'ai pas trouvé de version officielle d'une base qui pourrait être plus légère avec un jeu de signature plus restreint.

Le passage en mode lancement à la demande (clamscan) plutôt que démon pourrait permettre d'éviter une occupation permanente de la mémoire. Mais vu la quantité de mail que nous recevons, les lancements répétés pourraient avoir un impact encore plus négatif sur les performances.

#10 - 01/05/2020 15:07 - Romain H.

Aujourd'hui Clamav analyse les mails qui vont vers les adresses mails internes et pour les redirections. Pour les adresses redirigées, les adresses cibles ont certainement déjà un système antivirus plus fiable que notre Clamav. Pour les adresses internes, les quelques menaces bloquées par Clamav ne semble pas vraiment nous concerner.

Vu le peu de chose que nous apporte Clamav et notre manque de RAM disponible, nous allons tester de le désactiver pendant 1 mois pour voir comment se comporte le serveur.

#11 - 01/05/2020 16:37 - Romain H.

Ajout dans /etc/amavis/conf.d/50-user de :

```
# Disable Clamav (#4218)
@bypass_virus_checks_maps = (1);
```

Désactivation des deux services clamav :

```
systemctl stop clamav-freshclam
systemctl stop clamav-daemon
systemctl disable clamav-freshclam
systemctl disable clamav-daemon
```

Désactivation des services ClamAV et Amavis sur admin dans /etc/icinga2/zones.d/master/cluster/mail.conf.
Désactivation des services ClamAV et Amavis sur galanga dans /etc/icinga/objects/hosts/cluster-vms/mail.cfg.
Le service Clamav vérifiait la bonne mise à jour de Clamav et Amavis envoyait un email EICAR pour tester le bon fonctionnement du blocage de Clamav.

#12 - 23/05/2020 21:10 - Romain H.

- Fichier april_vm_mail_swap.png ajouté

- Statut changé de En cours de traitement à Résolu

- % réalisé changé de 0 à 100

Depuis la modification il y a toujours au moins 800 Mo de swap disponible et pas d'alerte icinga.
Il y a une augmentation au début mais ça se stabilise, ça me semble être le comportement normal.

#13 - 27/05/2020 22:30 - Quentin Gibeaux

- Statut changé de Résolu à Fermé

Fichiers

april_vm_mail_swap.png	103 ko	23/05/2020	Romain H.