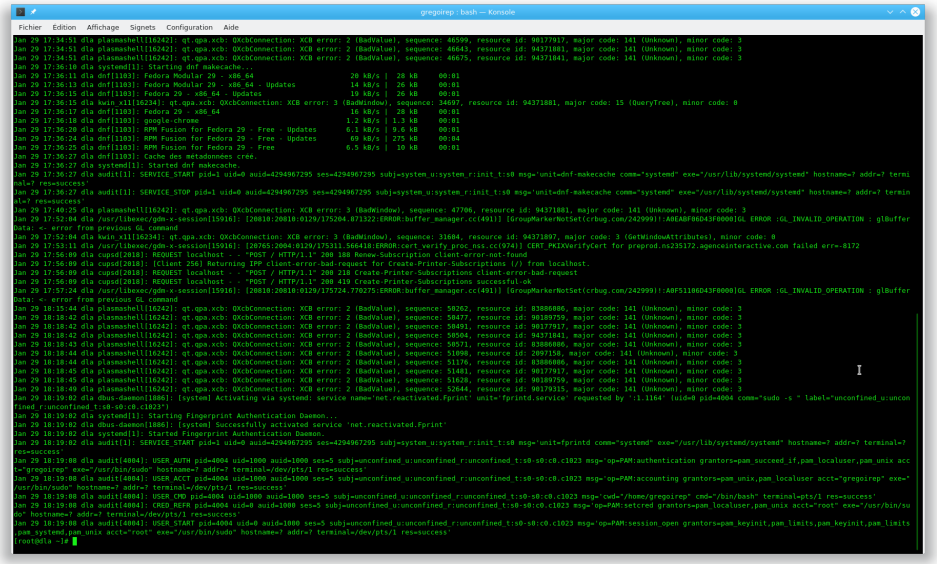

Gestion de logs

P. Grégoire

Date: 2023

Aperçu et Objectifs

Ce TP va vous faire découvrir le système de journaux (logs ou logfiles) de Linux et les outils qui permettent de les gérer en contrôlant à quel endroit et comment sont stockés ces journaux et le volume occupé sur les disques.

La bonne gestion de ces journaux est essentielle pour l'administration d'un cluster.

Quelques liens utiles

- systemd: http://www.freedesktop.org/wiki/Software/systemd
- journald: http://man7.org/linux/man-pages/man1/journalctl.1.html

Sommaire

4. Configuration du système de rotation de logs

Lancement des VMs

Exécutez la commande script pour enregistrer votre session de travail. Vous devrez m'envoyer ce fichier à la fin de la session.

Puis lancer votre machine virtuelle avec pcocc puis connectez vous sur cette machine avec la commande pcocc ssh et passer en root avec la commande sudo -s:

Vous voilà super-user root sur votre vm.

A la fin de la session, **quitter une à une les sessions par exit** : le sudo, puis votre login sur la vm0, puis la session pcocc, puis la session script.

La liste tp-log-client,tp-log-client donnée en paramètre de la commande pcocc indique que vous allez lancer deux vm : vm0 (tp-log-server) et vm1 (tp-log-client).

```
hpc01$ script -a -t=log0-$(id -un) trace-tp-log-vm0-$(id -un).txt

hpc01$ pcocc alloc  -c 3 tp-log-server,tp-log-client

salloc: Granted job allocation 9083

Configuring hosts... (done)

(pcocc/9083) [kevin.dummy@hpc01 ~]$ pcocc ssh vm0


[kevin.dummy@vm0 22:23:44]$ sudo -s

[root@vm0 22:23:20]#
```

Utilisation des commandes logger et journalctld

Utilisation de la commande logger

Lire la page de manuel de la commande **logger** et réaliser les actions suivantes.

1. Envoyer un message “OK file has been updated” avec la facility **user** et le level **info.**
2. Envoyer un message “Unable to write to file /tmp/foo” avec le tag foo, avec la facility **user** et le level **error**.
3. Envoyer un message “Where this msg will be sent ?” avec le tag « msg », avec la facility **local7** et le level **warning**, et le process id.
4. Vérifier avec la commande **tail** que les messages apparaissent dans les 3 dernières lignes du fichier de log **/var/log/messages**

Répondre aux questions de la section correspondante dans le questionnaire.

Utilisation de la commande journalctld

Lire la page de manuel de la commande **journalctl** et réaliser les actions suivantes.

1. Retrouver la liste des boots enregistrés dans le journal système
2. Lister les entrées du journal depuis le dernier boot
3. Lister les entrées du journal concernant le service crond
4. Lister les 10 dernières entrées du journal système
5. Lister uniquement les entrées du noyau dans le journal
6. Lister les entrées du journal de priorité **>** warning (c'est à dire err, crit, alert, emerg)
7. Lister les entrées du journal depuis le jour précédent à 13h30
8. Lister les entrées du journal avec le tag foo.
9. Lister les 10 dernières entrées du journal et celles qui suivront.

Répondre aux questions de la section correspondante dans le questionnaire.

Configuration de rsyslogd

Configuration locale de rsyslogd

Lire la page de manuel de **rsyslog et celle de son fichier de configuration**, en particulier le paragraphe **SELECTORS**.

Consulter son fichier de configuration :

1. Retrouver la règle permet d'envoyer des messages dans le fichier /var/log/messages.
2. Quelle facilité est utilisée par les messages de boot ?
3. Retrouver les sources qui alimentent le démon rsyslog.
4. Quelle directive permet d'inclure des fichiers de configuration ? En écrivant un fichier **/etc/rsyslog.d/local2.conf,** faire en sorte que le démon rsyslogd écrive tous les messages de catégorie **local2** et niveaux **≥** à warning dans le fichier **/var/log/local2-warning-and-more**.
5. Relancer le service **rsyslog** , vérifier son état et tester la configuration avec la commande **logger** sur les différents niveaux et vérifier que les messages sont bien triés.
6. Lire la page de manuel de **rsyslog.conf**, spécialement la partie Expression**-Based Filters**. Vous pouvez consulter aussi :

   https://www.rsyslog.com/doc/v8-stable/configuration/filters.html

   https://www.rsyslog.com/doc/v8-stable/rainerscript/control_structures.html

   https://www.rsyslog.com/doc/master/configuration/actions.html#discard-stop

   Dans un fichier **/etc/rsyslog.d/appli1.conf**, écrire une règle de filtrage en utilisant la nouvelle syntaxe (expression-based filters) avec des accolades et **stop** pour que tous les messages taggés **appli1** sur la facilité **local2** soient envoyés dans le fichier **/var/log/local2-all** . Tester et montrer que les messages vont bien dans ce fichier et uniquement dans celui-là.

Centralisation des journaux

Dans un cluster, on désire concentrer tous les fichiers journaux de tous les nœuds vers une seule machine pour faciliter la consultation et l'analyse ou pour des raisons d'espace disque sur les nœuds (ex nœuds sans disque!)

Ouvrez une nouvelle connexion sur le cluster hpc pour travailler sur la seconde machine de votre cluster virtuel (**vm1**) :

```
[kevin.dummy@hpc01 ~]$ script -a -t=log1-$(id -un) trace-tp-log-vm1-$(id -un).txt
Le script a débuté, le fichier est trace-tp-log-vm1-kevin.dummy.txt
[kevin.dummy@hpc01 ~]$ pcocc ssh vm1
Last login: Thu Feb 14 20:00:04 2019 from 192.168.1.21
[kevin.dummy@vm1 20:41:42]$ sudo -s
[root@vm1 20:43:02]#
```

A partir de ce moment, vous disposez de 2 connexions sur le cluster, une sur le nœud **vm0**, et l'autre sur le nœud **vm1**. Faites attention où vous entrez les commandes !

Lisez le paragraphe "**Remote machine"** de la page de manuel de rsyslog.conf.

Sur la machine **vm0 :**

- Configurer le service rsyslog pour qu'il accepte des messages entrants en TCP sur le port 514.
- Relancer le service et vérifier son état
- Récupérer avec la commande **pidof** le PID du démon rsyslogd
- Vérifier avec la commande **lsof -p <pid> -P** -que le démon écoute bien sur un socket TCP port 514.
- Avec la commande **ip a** , repérer l'adresse IP de la carte eth0 de la vm0

Sur la machine **vm1 :**

- Configurer le service rsyslog pour qu'il envoie tous les messages vers le service rsyslog de la machine vm0 en utilisant l'adresse IP eth0 de la vm0.
- Relancer le service.
- Récupérer avec la commande **pidof** le PID du démon rsyslogd
- Vérifier avec la commande **lsof -p <pid> -P** -que le démon a bien établi une connexion TCP port 514.
- Avec la commande "**logger -i -t qux hello i am your sister vm**" , envoyer plusieurs messages et vérifier que ces messages arrivent bien dans le fichier /var/log/messages sur la vm0.

Répondre aux questions de la section correspondante dans le questionnaire.

Rotation des logs

Lire la page de manuel de la commande logrotate.

La commande logrotate se configure via le fichier /etc/logrotate.conf et les fichiers déposés dans le répertoire **/etc/logrotate.d** par l'installation de paquets rpm.

La commande logrotate est exécutée une fois par jour par le démon crond via le script /etc/cron.daily/logrotate

Lire le fichier de configuration.

Répondre aux questions de la section correspondante dans le questionnaire.

Une fois ce travail terminé, terminer par la commande **history** puis sortez des différentes sessions et envoyez moi les 2 fichiers de trace trace-tp-log-vm0-your-name.txt et trace-tp-log-vm1-your-name.txt accompagnés des deux fichiers de timing log[01]-your-name.

```
[root@vm0 01:40:30]# history
.....
[root@vm0 01:50:01]# exit
exit
[kevin.dummy@vm0 01:40:33]$ exit
déconnexion
Connection to hpc04 closed.
(pcocc/9091) [kevin.dummy@hpc01 ~]$ exit
exit
Terminating the cluster...
[kevin.dummy@hpc01 ~]$ exit
exit
Script terminé, le fichier est trace-tp-log-vm0-kevin.dummy.txt
```