TP N°2a Journaux (logs)

Lancer votre cluster virtuel à 2 nœuds avec pcocc puis connectez vous sur la première machine **vm0** et passer en root avec la commande sudo :

$ script trace-tp2A-vm0
$ pcocc alloc -c 3 mycentos74-tp2:2
(pcocc/3443) [guestX@hpc01 ~]$ **pcocc ssh vm0**
Last login: Sun Jan 28 17:41:54 2018 from hpc01.c-hpc.pedago.ensiie.fr
[guestX@vm0 ~]$ [guestX@vm0 ~]$ **sudo bash**
[root@vm0 guestX]#

A la fin de la session, **quitter une à une les sessions par exit** (vm0, script, login hpc)
Envoyer moi immédiatement par mail à philippe.gregoire@cea.fr ce fichier rempli.
Merci de rajouter votre nom de famille dans le nom du fichier.
Vous devez ensuite terminer seul ce travail et me le rendre par mail 7 jours après par mail.

Partie A : Utilisation de la commande logger

Lire la man page de la commande **logger** et réaliser les actions suivantes. Remplir la grille de réponses avec la commande.

1. Envoyer un message « hello world » avec la facility **user** et le level **info.**
2. Envoyer un message « bad luck i am dead » avec le tag « foo », avec la facility **user** et le level **error**.
3. Vérifier avec la commande **tail** que les messages apparaissent dans les 5 derneires lignes du fichier de log **/var/log/messages**

Partie B : Utilisation de journalctl

1. Exécuter la commande journalctl pour obtenir les messages depuis le dernier boot
2. Exécuter la commande journalctl pour obtenir les 5 dernières lignes du journal.
3. Exécuter la commande journalctl pour obtenir les messages taggés foo
4. Exécuter la commande journalctl pour obtenir les messages de priorité > warning
5. Exécuter la commande journalctl pour obtenir les messages depuis le jour précédent à 13 h30
6. Exécuter la commande journalctl pour obtenir les 10 derniers messages et attendre les suivants. A partir d'une autre fenêtre, envoyer un message avec la commande **logger**.. Vérifier que les messages apparaissant dans la première fenêtre. Arrêter la commande avec <Ctrl-c>.
7. Quelle commande journalctl permet d'obtenir uniquement les messages du noyau ?

Partie C : Configuration simple de rsyslog

Rsyslogd est un démon qui permet de collecter les journaux (logs) de différentes sources, de faire un tri pour les envoyer à d'autres démons rsyslogd sur d'autres machines ou de les écrire dans différents fichiers ou dans des bases de données.

Lancer la machine vm-<mylogin>-logsrv. Connecter vous. Éditer le fichier de configuration **/etc/rsyslog.conf** pour le passer en revue.

Pour répondre aux questions suivantes, aidez-vous de la man page **rsyslog.conf**, en particulier le paragraphe **SELECTORS**.

1. Quelle règle permet d'envoyer des messages dans le fichier /var/log/messages ?
2. Quelle facilité est utilisée par les messages de boot ?
3. Quels sont les sources qui alimentent le démon rsyslog ? Donner le nom des modules correspondants.
4. Quelle directive permet d'inclure des fichiers de configuration ? Pourquoi la directive est avant la section *### RULES* ?
5. En écrivant un fichier **/etc/rsyslog.d/local2.conf,** faire en sorte que le démon rsyslogd écrive touls les messages de catégorie **local2** et niveaux ≥ à warning dans le fichier **/var/log/local2-warning-and-more**.
6. Relancer le service **rsyslog** et tester la configuration avec la commande **logger** sur les différents niveaux et vérifier que les messages sont bien triés. Donner les commandes et les fichiers en résultats.
7. Lire la page de manuel de **rsyslog.conf**, spécialement la partie **Property-Based Filters**. Dans un fichier **/etc/rsyslog.d/appli1.conf**, écrire une règle de filtrage nouvelle syntaxe avec des accolades et **stop** pour que tous les messages taggés **appli1** sur la facilité **level2** 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.
8. Les fichiers dans **/etc/rsyslog.d/** sont traités par ordre alphabétique. Que se passe t-il si on renomme le fichier **/etc/rsyslog.d/appli1.conf** en **/etc/rsyslog.d/ze_appli1.conf.**

Partie D : Configuration de rsyslog en mode forward

Dans un cluster, on peut désirer concentrer tous les fichiers journaux de tous les nœuds vers une seule machine pour faciliter 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**). Puis exécuter les commandes suivantes :

hpc01$ script trace-tp2B-vm1

hpc01$ pcocc ssh vm1

vm1$ sudo bash

A partir de ce moment, vous disposez de 2 connections sur le cluster, une sur la machine **NTP server vm0**, l'autre sur la machine **NTP client vm1**. Faites attention où vous devez entrer les commandes !

1. Installer la commande lsof sur les machines **vm0 et vm1**.
2. Sur la machine **vm1,** configurer le service rsyslog pour qu'il accepte des messages entrants en TCP sur le port 514. Relancer le service. Vérifier par lsof et pidof que le démon a bien un socket TCP port 514.
3. Sur la machine **vm0, c**onfigurer le service rsyslog pour qu'il envoie tous les messages vers le service rsyslog de la machine vm0. Relancer le service. Vérifier par lsof et pidof que le démon a bien un socket TCP port 514.
4. Quel problème risque de se poser si on redirige dans un cluster toutes les messages de logs de tous les nœuds vers un seul serveur ?

Partie E: Rotation de logs

Lire la page de manuel de logrotate. Logrotate se configura via le fichier /etc/logrotate.conf et les fichiers déposés dans le répertoire **/etc/logrotate.d** lors de l'installation de paquets rpm.

1. Comment logrotate est il exécuté ? Que faut-il modifier pour pourvoir effectuer des rotations de logs toutes les heures ?
2. Lire le fichier de configuration. Quelles sont les options définies par défaut ?
3. Modifier la configuration de logrotate pour que les fichiers /var/log/local2* soient compressés minsiwe 20K, rotation sur 8 jours.
4. Modifier la configuration de logrotate pour que ce fichier soit compressé et archivé des qu'il atteint 10 Ko, que le démon soit averti, que 6 fichiers de journaux archivés soient conservés

1.

Question	Commande	Résultat
A-1	# logger -p user.info "hello world"	
A-2	# logger -p user.error -t foo "bad luck i am dead"	
A-3	# tail -n5 /var/log/messages	Feb 19 15:15:46 vm0 systemd: Started Update UTMP about System Runlevel Changes. Feb 19 15:15:46 vm0 systemd: Startup finished in 1.127s (kernel) + 1.638s (initrd) + 1min 7.421s (userspace) = 1min 10.188s. Feb 19 15:17:37 vm0 guest11: hello world Feb 19 15:18:05 vm0 guest11: user.info hello world Feb 19 15:20:31 vm0 foo: bad luck i am dead

Question	Commande	Résultat
B-1	# journalctl -b	
B-2	# journalctl -n5	
B-3	# journalctl -t foo	# journalctl -t foo -- Logs begin at lun. 2018-02-19 15:14:37 UTC, end at lun. 2018-02-19 15:20:31 UTC. -- févr. 19 15:20:31 vm0.pcocc foo[7535]: bad luck i am dead
B-4	# journalctl -p 5..7	
B-5	# journalctl -S "2018-02-18 13:30"	
B-6	# journalctl -n10 -f	
B-7	# journalctl -k	

Question	Commande	Résultat
C-1	*.info;mail.none;authpriv.none;cron.none /var/log/messages	
C-2	local7	
C-3	imuxsock, imjournal	
C-4	$IncludeConfig /etc/rsyslog.d/*.conf Cette directive est placée avant la section RULES de façon à être prioritaire sur les modifications éventuelles de l'utilisateur.	
C-5	local2.warning /var/log/local2-warning-and-more	
C-6		
C-7		
C-8		

Question	Commande	Résultat
D-1		
D-2		
D-3		
D-4		

Question	Commande	Résultat
E-1		
E-2		
E-3		
E-4		