Système de gestion de logs

Philippe GRÉGOIRE

Plan

Définition

- Fichiers journaux contiennent des messages relatifs
  - Au système,
  - Aux services,
  - Aux applications

Utilité

- Enregistrement des événements importants
  - Informations sur le fonctionnement
  - Chronologie des événements
- Analyse des problèmes
  - Pendant qu'ils se produisent
  - Plusieurs jours après

Format

- Généralement enregistrés sous forme de texte.
- Les formats des messages sont variés
  - Le plus souvent horodatés – mais pas toujours avec les mêmes conventions
  - Une même information peut être présentée sous des formes différentes selon la source.

Emplacement / Volumes

- Sous Linux, généralement sous le répertoire /var.
- Un sous-répertoire si plusieurs fichiers de logs
  - Créé par le paquet (rpm) du logiciel
- Volumes variables selon
  - L'utilisation du service / de l'application.
  - Des événements extérieurs.
  - La verbosité de la source :info, error, debug1, … debug9.
    - Configurable dans le fichier de conf ou
    - En paramètre de commande
    - Dynamique (kill -USR1 <procid>

Différentes log Linux

- /var/log/boot.log*
- /var/log/cron*
- /var/log/dmesg*
- /var/log/lastlog*
- /var/log/messages*
- /var/log/secure*
- /var/log/audit/audit.log*
- # dmesg

Gestion des fichiers de logs

- Espace disque /var limité
  - Nécessite d'une politique de gestion
- Politique de découpage des logs selon certains critères
  - Taille
  - Date
- Politique de rétention des logs
  - Archivage
    - Déplacement dans un autre espace de stockage.
  - Rotation :
    - Conservation d'un nombre limité de fichiers.
  - Critères de volumes, de durée de conservation

Gestion des journaux : Logrotate

- Pour chaque journal une politique spécifique :
  - Critères de temps :
    - Toutes les heures (hourly)
    - Tous les jours (daily),
    - toutes les semaines (weekly),
    - Tous les mois (monthly)
    - Tous les ans (yearly)
  - Critères de taille :
    - Maxsize, minsize, size
  - Actions
    - Compression, Troncation, Renommage, …
  - Nombre de fichiers conservés

Journal Système

- Service de collecte des journaux système : journald
- Création structurée et indexée de journaux
- Collecte via
  - L'interface Kernel log messge kmesg
  - Fonction syslog (3) de la bibliothèque standard
  - stdout/stderr des services systèmes
  - API native systemd sd_journal_print(4)
  - Système d'audit.
- Stockage non persistant dans /run/log/journal
- Configuration dans /etc/systemd/journald.conf
- Directive ForwardToSyslog=yes pour renvoi à Syslog
- Man page : systemd-journald.service (8)

Utilisation du journal Système

- Afficher les messages du démarrage courant (message du noyau lors du boot)
  - journalctl -b
- Afficher les messages du démarrage ayant la priorité err ou supérieure
  - journalctl -b -p err
- Afficher les messages ayant trait à l'unit (service) nginx
  - journalctl -u nginx
- Afficher les messages d'erreur ayant trait au service nginx
  - journalctl -p err -u nginx
- Afficher les 10 derniers messages et ceux qui viendront ensuite
  - journalctl -f
  - tail -f /var/log/messages
- Afficher les messages tagés dnsmasq-dhcp
  - journalctl -t dnsmasq-dhcp

Envoi d'un message vers rsyslog : API

- Man 3 syslog

```
SYSLOG(3)                  Linux Programmer's Manual                  SYSLOG(3)

NAME
       closelog, openlog, syslog, vsyslog - send messages to the system logger

SYNOPSIS
       #include <syslog.h>

       void openlog(const char *ident, int option, int facility);
       void syslog(int priority, const char *format, ...);
       void closelog(void);

       #include <stdarg.h>

       void vsyslog(int priority, const char *format, va_list ap);
```

Envoi d'un message vers rsyslog : API

- Priorité : <catégorie>.<niveau>

Catégorie	Description
auth	Messages de sécurité et d'authentification.
authpriv	Messages de sécurité et d'authentification.
cron	Messages de *crontab* et de *at*.
deamon	Messages systèmes générés par le démon.
ftp	Messages du serveur ftp.
kern	Messages du noyau.
lpr	Messages du serveur d'impression.
mail	Messages du serveur de messagerie.
news	Messages du serveur de news.
syslog	Messages de *syslog*.
user	Messages générés par le programme en cours d'un utilisateur.
uucp	Messages UUCP.

Niveau		Description
7	debug	Messages de débogage.
6	info	Messages d'information.
5	notice	Messages d'information un peu plus importants.
4	warning	Messages d'avertissement.
3	err	Message d'erreur.
2	crit	Situation critique.
1	alert	Situation critique nécessitant une intervention immédiate.
0	emerg	Système inutilisable.

Envoi d'un message : commande

- Commande logger : man 1 logger

```
LOGGER(1)                          User Commands                          LOGGER(1)

NAME
       logger - a shell command interface to the syslog(3) system log module

SYNOPSIS
       logger [options] [message]

DESCRIPTION
       logger  makes entries in the system log.  It provides a shell command
       interface to the syslog(3) system log module.
```

```
[root@dlat pgregoire]# logger -p user.notice -t devenv -i "cant find any compi
ler"
[root@dlat pgregoire]# tail -1 /var/log/messages
Dec  3 23:05:14 dlat devenv[30281]: cant find any compiler
[root@dlat pgregoire]#
```

Rsyslog

- Démon de gestion des messages
- Ecoute sur un port Unix local ou Remote
- Applique des regles de filtrage
- im == Input Module
- om == Output module
- mm == Message Modification Module
- sm == String Generator Module
- pm == Parser Module

rsyslog

Analyse de journaux

- Sur une machine
  - Identifier la date des premiers symptomes
  - Rechercher les erreurs dans le journal de l'application :
    - Stdout/stderr d'un job
    - Fichier de logs du service
  - Rechercher d'autres erreurs au même moment ou antérieurement dans d'autres composants
  - Grep -i 'error|fail|abort|dump|segv|unable|timeout' /var/log/….
- L'erreur peut venir d'un incident sur d'autres serveurs :
  - Dns,
  - Ldap,
  - Kerberos,
  - Slurm,
  - Nfs,
  - Lustre

Analyse de journaux

- Sur une machine
  - Identifier la date des premiers symptomes
  - Rechercher les erreurs dans le journal de l'application :
    - Stdout/stderr d'un job
    - Fichier de logs du service
  - Rechercher d'autres erreurs au même moment ou antérieurement dans d'autres composants
  - Grep -i 'error|fail|abort|dump|segv|unable|timeout' /var/log/….
- L'erreur peut venir d'un incident sur d'autres serveurs
- Comment identifier l’origine d'un problème pour une application s’exécutant sur des milliers de nœuds et faisant appel à des dizaines de serveurs (Dns, Ldap, Kerberos, Slurm, Nfs, Lustre)

Analyse de journaux

- Sur une machine :
  - Pas simple !
- Sur un cluster :
  - Comment identifier l’origine d'un problème pour une application s’exécutant sur des milliers de nœuds et faisant appel à des dizaines de serveurs (Dns, Ldap, Kerberos, Slurm, Nfs, Lustre)
- Nécessité de centraliser les journaux
- Nécessité d'outils puissants d'analyse
- Intérêt de corréler avec la métrologie

ELK

- ElasticSearch
- Logstash
- Kibana

Logstash

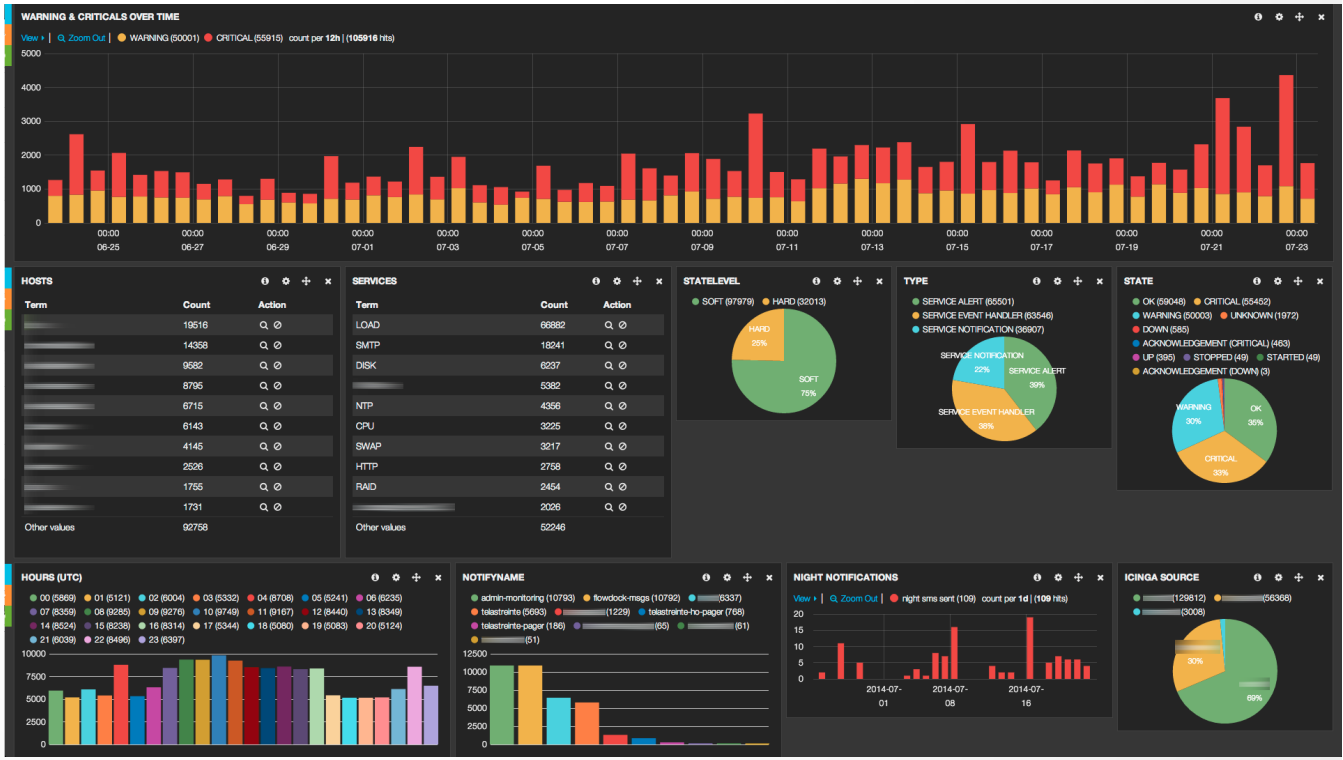
- Accepte des logs de différents formats en entrée
- Filtre (regex)
- Renvoit des messages reformatés sous différéntes formes

ElasticSearch

- Serveur de recherche distribué
- Open source
- Très rapide
- Développé en Java
- Scalable

ElasticSearch

- Interface graphique
- Création de tableaux de bords



Questions ?

?