8 - Gestion des logs

M1 RÉSEAUX & TÉLÉCOMS

RT0701 : ADMINISTRATION SYSTÈME 1

OLIVIER FLAUZAC

UNIVERSITÉ
DE REIMS
CHAMPAGNE-ARDENNE

Contrôler et mémoriser

Contrôle d’exécution

Contrôler le fonctionnement du réseau

Collecter les paramètres d’exécution

Etudier les données collectées

Définir les seuils d’alerte

Etre alerté des dysfonctionnements

Contrôle

Ordinateurs

serveurs

- machines utilisateurs
- services (service d'authentification, service WEB ...)

Equipement réseau

- Routeur
- commutateurs

Périphériques réseau

- imprimante

Informations collectables

Informations d’accès

- accès à une page web
- accès d’un utilisateur
- accès à un service

Erreurs

- accès illégaux
- erreurs d’authentifications
- erreurs d’exécution

Gestion des informations

Détermination du comportement normal du système

- connaissance évaluée au préalable
- Apprentissage
- définition contextuelle du comportement

Définition des alertes et des seuils associés

Journalisation

Enregistrement des traces des opérations

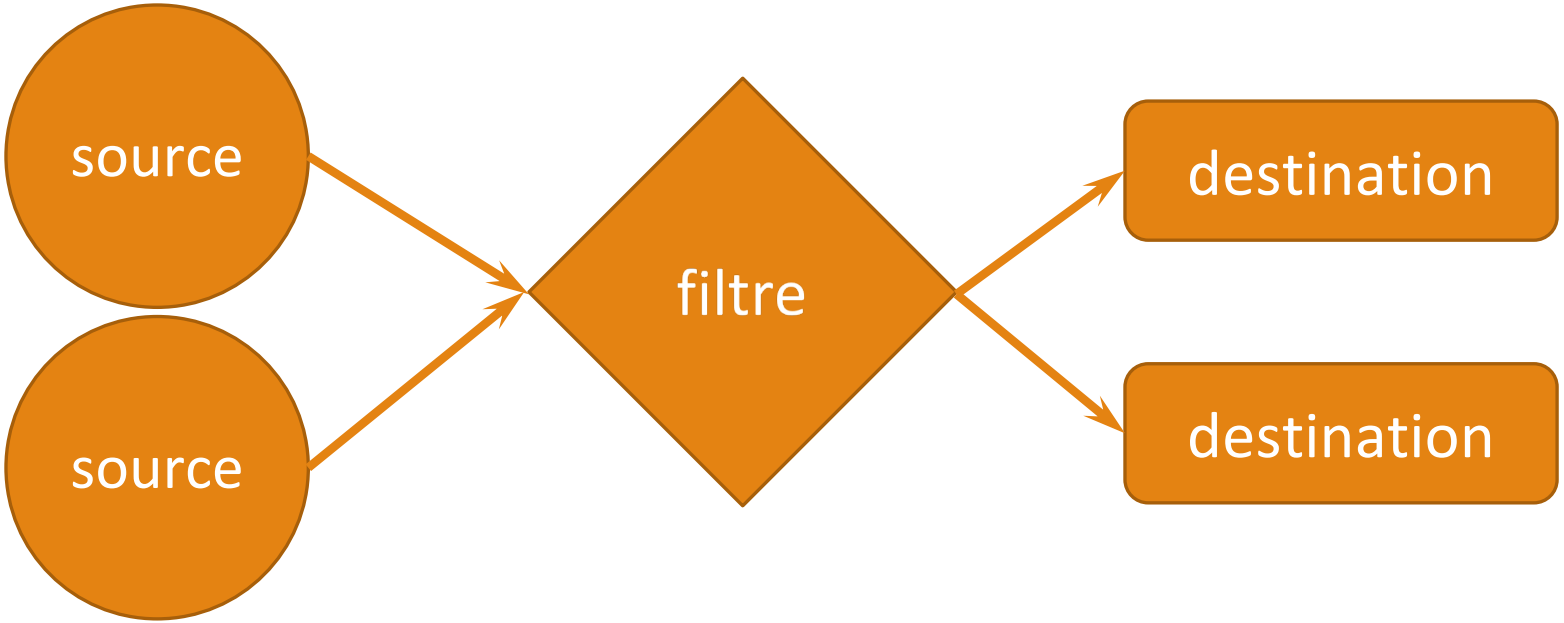
Sauvegarde des opérations

- en fonction du degré d'importance
- en fonction de la source

Localisation des fichiers

```
/var/log
```

Système de gestion de log



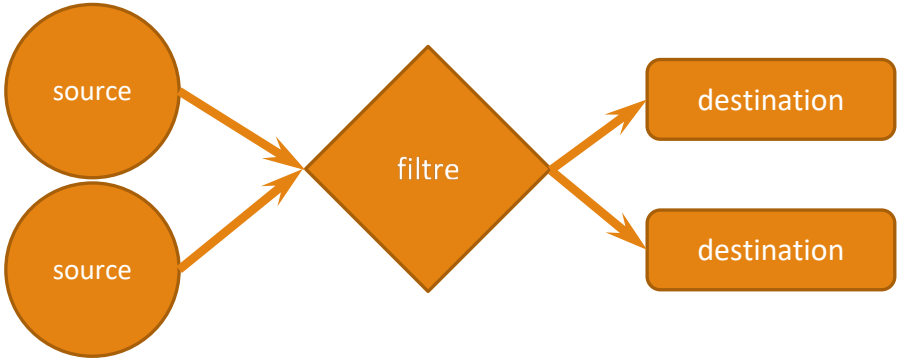
Système de gestion de log : Sources

Fichier

Flux réseau

Flux applicatif

Protocole standard



Système de gestion de log : traitement

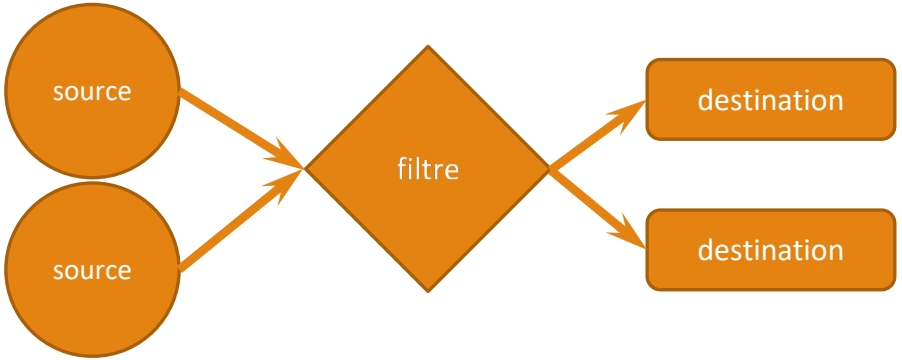
Filtrage

Criticité

Source

Destination

Message



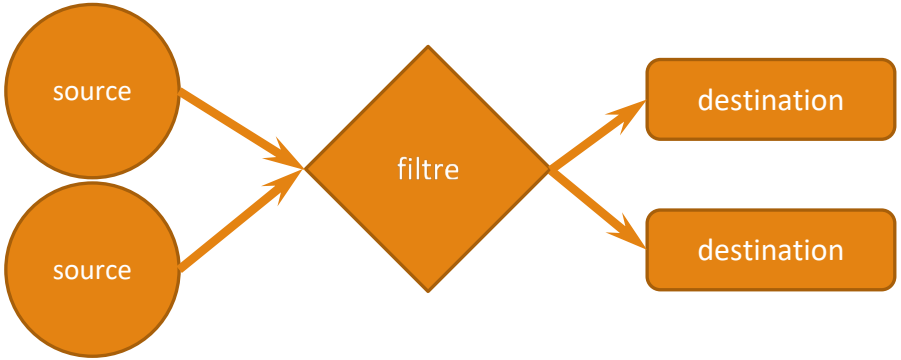
Système de gestion de log : destination

Fichier

Flux réseau

Flux applicatif
- BdD

Protocole standard



Système de log

Messages

Messages du noyau : `dmesg`

- messages mis en *buffer*
- diagnostique des chargements de noyau
  - au démarrage
  - à chaud (pilotes USB …)

Etat des accès : `lastlog`

- utilisateurs / info de connexion

Fichiers de logs

Log du noyau

Log systèmes

Log de serveurs

- Apache
  - `/var/log/apache2`
  - access.log ; error.log
- apt (gestionnaire de package)
  - `/var/log/apt`
  - history.log
  - term.log

Centralisation de logs

Exploitation du protocole syslog

Fonctionnement général

- collecte des informations
- filtre des informations
- émission des résultats

Solutions existantes :

- protocole syslog
- rsyslog syslog-ng

Protocole syslog

Protocole assurant

- la collecte des informations (client) auprès des services
- la centralisation et la gestion des fichiers (serveur)

Exploitation du protocole UDP

- port 514

Définition du format d'enregistrement

```
date nom_hôte service[level] identifiant message
```

Niveau de gravité (level)

0	Emerg (emergency) : système inutilisable
1	Alert : intervention immédiate requise
2	Crit (critical) : erreur critique pour le système
3	Err (Error) : erreur de fonctionnement
4	Warning : avertissement
5	Notice : événement normal signalé
6	Info (informational) : pour information seulement
7	Debug : message de mise au point

Sources standard (facility)

0	kernel
1	user-level
2	mail system
3	system daemons
4	security/authorization
5	syslogd
6	printer
7	network news
8	UUCP

9	clock daemon
10	security/authorization
11	FTP
12	NTP
13	log audit
14	log alert
15	clock daemon
16 - 23	local use 0,7

Syslog-NG

Syslog-ng

Gestion/centralisation des logs

Collecte des messages émis

Filtrage selon différentes stratégies

Emission du log vers différentes destinations

Installation du package syslog-ng

Configuration

Répertoire de configuration

- `/etc/syslog-ng`

Gestion des drivers (modules)

- Sources
- destinations

Gestion des règles de log

Gestion des sources

Origine des messages à enregistrer

Depuis

- un fichier (file)
- un flux réseau (tcp / udp)
- une socket UNIX (unix-stream / unix-dgram)
- des information syslog (internal)

Format des sources

```
source <ident> { source-driver(params);
                 source-driver(params);
                 ...};
```

Sources : exemple

```
source s_src { unix-dgram("/dev/log");
               internal();
               file("/proc/kmsg" program_override("kernel"));
};
```

Gestion des destinations

Destination des messages

Vers

- un fichier (file)
- les logs d'une machine distante (udp / tcp)
- la console d'un utilisateur (usertty)
- socket unix (unix-stream / unix-dgram)

Format des destinations

```
destination <ident> { destination-driver(params);
                      destination-driver(params);
                      ...};
```

Destinations : exemple

```
destination d_auth { file("/var/log/auth.log"); };
destination d_cron { file("/var/log/cron.log"); };
destination d_syslog { file("/var/log/syslog"); };
destination d_console { usertty("root"); };
```

Destinations : propriétés

```
destination df_auth {
    file("/var/log/$YEAR/$MONTH/$DAY/auth.log");
    owner("root")
    group("adm")
    perm(0600)
    create_dirs(yes));
};
```

Gestion des filtres

Aiguillage des log :

1. identification des log
2. affectation à une destination

Politiques de log

- service / programme d'origine (program)
- criticité des informations (level)
- expression régulière (match)
- source (host)
- Sources standards (facility) (cron, lpr, mail, syslog ...)
- autres filtres (filter)

Format des filtres

```
filtre <ident> { filtre-driver(params);
                 filtre-driver(params);...
               };
```

Gestion des filtres : exemple

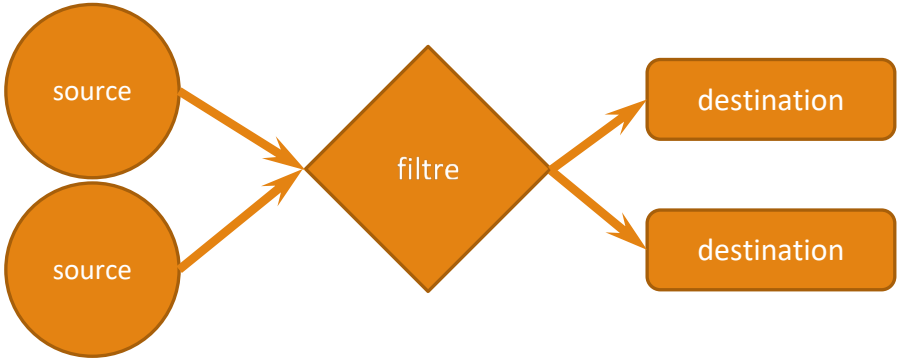
```
filter f_cron { facility(cron); };
filter f_daemon { facility(daemon); };
filter f_kern { facility(kern); };

filter f_debug { level(debug); };

filter f_cron { facility(cron) and not filter(f_debug);
};
```

Règles de log

Création de triplets

Association

- source ; filtre ; destination

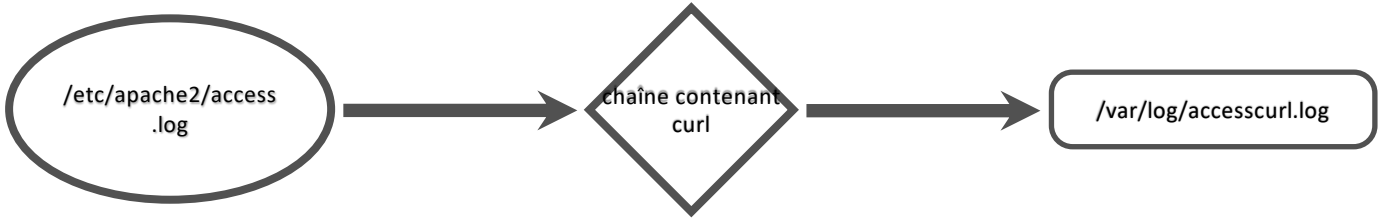


Format des règles de log

```
log { source(...);
      filter(...);
      destination(...);
     };
```

Exemple

Création de log des accès avec curl à apache



Exemple /etc/syslog-ng/syslog-ng.com

Gestion de la source

```
Source s_src file("/var/log/apache2/access.log");
```

Gestion de la destination

```
destination d_curl { file("/var/log/accescurl.log");};
```

Gestion du filtre

```
filter f_apache{match("curl");};
```

Règle du log

```
log { source(s_src);
      filter(f_apache);
      destination(d_curl); };
```

logger

-i log du PID

-p pri : (source) et criticité

```
logger -i -p user.notice je logue ici
```

```
Jan 14 13:05:39 OliDeb olivier[5277]: je logue ici
```

Gestion des fichiers

Gestion des fichiers

Explosion de la taille des fichiers

- serveur WEB d'un vendeur en ligne

Difficultés à visualiser les logs

Utilisation d'une solution de gestion des fichiers de logs

logrotate

Solution de rotation de log

Sauvegarde / archivage automatique

Evite l’explosion de la taille des fichiers

Permet de simplifier la lecture

Fonctionnement

Lancé périodiquement par le *cron*

Applique des règles par serveur

- syslog-ng
- Apache
- …

`/etc/logrotate.d`

Définition de règles

Définition du fichier ou des fichiers à traiter

```
/var/log/*.log{ ... }
/var/log/auth.log{ ... }
```

Définition de la «rotation»

```
weekly
```

Définition du nombre de log gardés

```
rotate 4
```

Etat des fichiers créés

```
Create
```

Gestion des fichiers

```
compress
```

Exemple rotation des logs apache

```
/var/log/apache2/*.log {
        weekly
        missingok
        rotate 52
        compress
        delaycompress
        notifempty
        create 640 root adm
        sharedscripts
        postrotate
                /etc/init.d/apache2 reload > /dev/null
        endscript
        prerotate
                if [ -d /etc/logrotate.d/httpd-prerotate ]; then \
                        run-parts /etc/logrotate.d/httpd-prerotate; \
                fi; \
        endscript
}
```

hebdomadaire

pas d'erreur sur un fichier absent

52 log mémorisés

compression des fichiers

compression après copie

pas d'archivage de fichier vide

création des fichiers de log

exécution de script

- Avant
- Après