CENTRALISER SES LOGS AVEC SYSLOG-NG

Formation A3IMP

DR12 - CNRS

Janvier 2008

Julien Charpin

CENTRALISER SES LOGS AVEC SYSLOG-NG

- Introduction (possibilités, installation, principes généraux, ...)
- Configuration serveur
- Configuration client(s)
- Exemple de Frontend : PHP-Syslog-ng

CENTRALISER SES LOGS AVEC SYSLOG-NG

- Présentation de syslog-ng (possibilités, installation, principes, ...)
- Configuration serveur
- Configuration client(s)
- Exemple de Frontend : PHP-Syslog-ng

CENTRALISER SES LOGS AVEC SYSLOG-NG

- Gestionnaire de journaux systèmes de nouvelle génération (**ng = new generation**), capable (entre autres) :
  - de filtrer les messages en utilisant les expressions régulières
  - d'envoyer/recevoir les logs sur le réseau via UDP ou TCP
  - Compatible IPV6

CENTRALISER SES LOGS AVEC SYSLOG-NG

- **Disponible :**
  - Sur la plupart des distributions sous forme de paquet (Debian, Red Hat, Mandriva ...)
  - En téléchargement (format **tar.gz**) sur SOURCEFORGE (http://sourceforge.net/projects/php-syslog-ng/) ou chez BALABIT (http://www.balabit.com/downloads/files/syslog-ng/sources/stable/)
- **Configuration :**
  - /etc/syslog-ng/syslog-ng.conf

CENTRALISER SES LOGS AVEC SYSLOG-NG

- **Les options de syslog-ng**

  Syslog-ng a un certain nombre d'options permettant de définir le comportement vis à vis du DNS, du format de timestamp ...

  On les définit dans le fichier /etc/syslog-ng/syslog-ng.conf :

```
...
use_dns(no);
create_dir(yes);
perm(0640);
...
```

CENTRALISER SES LOGS AVEC SYSLOG-NG

- **Principe de fonctionnement**
  - la configuration repose sur la définition, le nommage et le paramétrage d'objets globaux, qui sont :
    - **source** -> Où et comment syslog-ng reçoit-il ses messages de logs ?
    - **destination** -> Où et comment le message de log est-il envoyé ?
    - **filter** -> les messages ne seront envoyés vers la destination définie que s'ils "matchent" les règles de filtrage définies.
    - **log** -> définit ce qui se passe pour chaque message de log reçu.

CENTRALISER SES LOGS AVEC SYSLOG-NG

- **Déclaration des objets** :

```
type  identifier { parameters };
```

  - 1er champ : type d'objet (*source, destination, filter, log*)
  - 2ème champ : identifiant de l'objet (s_source1, d_network, f_filterdemo1, ...)

CENTRALISER SES LOGS AVEC SYSLOG-NG

- **Déclaration des objets (suite)** :
  - 3ème champ : paramètres des objets (obligatoires et optionnels) avec notamment :
    - les **drivers** propres au type d'objet **source** et **destination** :
      - **source** : *internal(), unix-stream(), udp(), tcp(), udp6(), tcp6() ...*
      - **destination** : *file(), unix-stream(), tcp(), udp(), tcp6(), fifo(), pipe() ...*

CENTRALISER SES LOGS AVEC SYSLOG-NG

- **Déclaration des objets (suite)** :
  - 3ème champ : paramètres des objets (obligatoires et optionnels) avec notamment :
    - Exemple d'utilisation des **drivers** :

```
source s_demo {
    internal();
    unix-stream("/dev/log");
    udp(ip(10.1.2.3) port(514));
    };
```

CENTRALISER SES LOGS AVEC SYSLOG-NG

- **Déclaration des objets (suite)** :
  - 3ème champ : paramètres des objets (obligatoires et optionnels) avec notamment :
    - les **expressions** (propres au type **filter**) construites à partir de :
      - **fonctions** pré-définies : *host(regexp), match(regexp), program(regexp), facility, level(emerg, alert, err ...) ...*
      - **parenthèses**
      - **des opérateurs booléens** : *and, or, not*

CENTRALISER SES LOGS AVEC SYSLOG-NG

- **Déclaration des objets (suite)** :
  - 3ème champ : paramètres des objets (obligatoires et optionnels) avec notamment :
    - exemple d'utilisation des **expressions** :

```
filter f_demofilter1 {
   host("host1") and match("deny"); };

filter f_demoregexp {
   host("system.*1") and match("deny"); };
```

CENTRALISER SES LOGS AVEC SYSLOG-NG

- **Déclaration des objets (suite)** :
  - 3ème champ : paramètres des objets (obligatoires et optionnels) avec notamment :
    - les **flags** (propres au type *log*) permettent de modifier le fonctionnement type d'écriture de logs :
      - **final** : ne pas envoyer le message à une autre destination
      - **flow-control** : arrêter de lire le message provenant de cette source si la destination ne peut pas les accepter
      - ...

CENTRALISER SES LOGS AVEC SYSLOG-NG

- **Déclaration des objets (suite)** :
  - 3ème champ : paramètres des objets (obligatoires et optionnels) avec notamment :
    - Exemple d'utilisation des **flags** :

```
log {
    source(s_localhost);
    destination(d_tcp);
    flags(flow-control); };
```

CENTRALISER SES LOGS AVEC SYSLOG-NG

- **Déclaration des objets (suite)** :
  - 3ème champ : paramètres des objets (obligatoires et optionnels) avec notamment :
    - les **Macros** : peuvent être utilisées notamment, pour construire des noms de fichiers de destination de logs.
      - HOST : le nom de la machine d'où provient le message
      - MONTH : le mois où le message a été envoyé
      - DAY : le jour où le message a été envoyé
      - ...

CENTRALISER SES LOGS AVEC SYSLOG-NG

- Présentation de syslog-ng (possibilités, installation, principes, ...)
- Configuration serveur
- Configuration client(s)
- Exemple de Frontend : PHP-Syslog-ng

CENTRALISER SES LOGS AVEC SYSLOG-NG

- Définir les **sources** de syslog-ng

```
...
source s_all {
   internal();
   unix-stream("/dev/log");
   file("proc_kmsg" log_prefix("kernel: "));
   udp();
   udp(10.2.3.4);
   tcp(port(54230));
   tcp(ip(10.2.3.4) port(54230));
};
...
```

CENTRALISER SES LOGS AVEC SYSLOG-NG

- Définir les **destinations** :

```
#quelques destinations classiques
destination d_auth { file("/var/log/auth.log"); };
destination d_syslog { file("/var/log/syslog"); };
destination d_cron { file("/var/log/cron"); };

#Récupérer les logs du reseau et les trier
destination d_network {
file("/var/log/syslog/$YEAR.$MONTH.$DAY/$HOST/reseau.l
  og");
};
```

CENTRALISER SES LOGS AVEC SYSLOG-NG

- Créer des **filtres** :

```
...
filter f_auth { facility(auth, authpriv); };
filter f_syslog { not facility(auth, authpriv); };
filter f_messages {
   level(info, notice, warn)
      and not facility(auth, authpriv, cron,
       daemon, mail, news);
};
...
```

CENTRALISER SES LOGS AVEC SYSLOG-NG

- finalement créer les traitements de logs en mélangeant tout ça :

```
log {
    source(s_all);
    filter(f_auth);
    destination(d_auth); };

log {
    source(s_network);
    destination(d_network); };
```

CENTRALISER SES LOGS AVEC SYSLOG-NG

- Présentation de syslog-ng (possibilités, installation, principes, ...)
- Configuration serveur
- Configuration client(s)
- Exemple de Frontend : PHP-Syslog-ng

CENTRALISER SES LOGS AVEC SYSLOG-NG

- **Client Linux** (2 possibilités)
  - **Syslog** "classique" **:**

    Configurer pour la redirection des logs (**514/UDP**) avec par exemple la ligne suivante dans **/etc/syslog.conf** :

```
...
#Redirection vers loghost
*.*                                @10.1.2.3
auth,authpriv.*                 -/var/log/syslog
*.*;auth,authpriv.none          -/var/log/syslog
...
```

CENTRALISER SES LOGS AVEC SYSLOG-NG

- **Client Linux** (suite)
  - **syslog-ng :**
    - Définir une **destination**

```
destination d_network { tcp("target_host"
  port("54230"); };
destination d_network { udp("target_host"); };
```

    - Définir (éventuellement) un **filtre**
    - Définir le traitement du message de log

```
log {
   source(s_all);
   destination(d_network); };
```

CENTRALISER SES LOGS AVEC SYSLOG-NG

- **Client Windows** :
  - **Observateur d'évènements** -> *Impossible*
  - **Snare** (Open Source) d'**Interselect Alliance** -> Redirection vers Syslog ou Syslog-ng
    - Clients NT/2000/XP/2003
    - Spécification du **serveur** et du **port** via l'interface web d'administration sur port 6161

CENTRALISER SES LOGS AVEC SYSLOG-NG

- Exemple :

```
Wed Jan 30 15:10:33 2008        593     Security
  charpin.j       User    Success Audit   PORT-JULIEN
  Suivi détaillé          Un processus est terminé :
  Id. du processus : 864    Nom du fichier image :
  C:\WINDOWS\system32\cmd.exe    Utilisateur : charpin.j
    Domaine : PORT-JULIEN    Id. d'ouv. de session :
  (0x0,0x21AEDA)        0

Jan 30 15:10:39 139.124.2.9 MSWinEventLog       1
  Application     2       Wed Jan 30 15:10:31 2008
  108     SNARE   Unknown User    N/A     Information
  PORT-JULIEN     None            The service was
  stopped.        0
```

CENTRALISER SES LOGS AVEC SYSLOG-NG

- Présentation de syslog-ng (possibilités, installation, principes, ...)
- Configuration serveur
- Configuration client(s)
- Exemple de Frontend : PHP-Syslog-ng

CENTRALISER SES LOGS AVEC SYSLOG-NG

- Téléchargement : **http://code.google.com/p/php-syslog-ng/downloads/list**
- Version : **php-syslog-ng-2.9.4**
- Nécessite MySQL5 et PHP4/5

CENTRALISER SES LOGS AVEC SYSLOG-NG

- Installation
  - tar.gz -> Apache(2)
  - Créer un site virtuel dans Apache ou configurer Apache pour avoir **http://loghost/php-syslog-ng/**

CENTRALISER SES LOGS AVEC SYSLOG-NG

- Configuration
  - Se connecter sur **http://localhost/php-syslog-ng/install**
    - Crée une base de données "syslog" avec les comptes utilisateurs adéquats
    - paramètre le site (mot de passe admin, ...)
  - Installer Scripts fournis dans crontab
  - Créer une **destination** et **log** spécifiques dans syslog-ng.conf

CENTRALISER SES LOGS AVEC SYSLOG-NG


```
destination d_mysql {

    program("/usr/bin/mysql -usyslogadmin -psyslogadmin
      syslog"

    template("INSERT INTO logs (host, facility, priority,
      level, tag, datetime, program, msg)

    VALUES ( '$HOST', $FACILITY, '$PRIORITY', '$LEVEL',
      '$TAG', '$YEAR-MONTH-$DAY' $HOUR:$MIN:$SEC',
      '$PROGRAM', '$MSG');\n")

    template-escape(yes));

}

...

log {source(s_network); destination(d_mysql); };

...
```

CENTRALISER SES LOGS AVEC SYSLOG-NG

- Démo ...