Syslog

Généralités

Syslog est un protocole définissant un service de journaux d'événements. C'est aussi le nom du format qui permet ces échanges.

Installation

Syslog

Syslog est présent sur toutes les distributions Linux on n'a pas besoin de l'installer. Il réceptionne les messages dans /var/log/messages. Son nom est syslogd.

Syslog-ng

Si on veut installer un serveur syslog alors on installe syslog-ng qui va se charger de supprimer syslogd. Récupérer le paquetage sur le site de rpm.pbone. Je ne l'ai pas trouvé sur le site de dag-wieers. http://rpm.pbone.net/

Récupérer le rpm de syslog-ng en fonction de l'architecture du système et la version de la Red Hat.

```
wget http://...el4.rf.i386.rpm
```

L'installer avec la commande suivante.

```
rpm -ivh syslog-ng...el4.rpm
```

Il y a peut-être des dépendances à installer. Les récupérer sur le site et les installer avant de

PHPsyslog-ng

A faire.

Configuration

Documentation

Site officiel : http://www.balabit.com/network-security/syslog-ng/

Configuration cliente (syslog)

Pour configurer un client syslog afin qu'il s'intègre dans une infrastructure syslog-ng, il faut modifier le fichier de configuration suivant.

Emplacement	Fonction
/etc/syslog.conf	Fichier de configuration client de syslog.

Ajouter la ligne en gras qui spécifie d'envoyer les messages sur le serveur dont l'adresse IP est spécifiée.

```
*.info;mail.none;authpriv.none;cron.none                /var/log/messages
*.info;mail.none;authpriv.none;cron.none                @172.25.30.10
```

ou

```
*.info;mail.none;authpriv.none;cron.none                @srv-syslog.admin
```

Redémarrer le service syslogd.

```
service syslog restart
```

Se connecter sur l'interface PHPsyslog-ng : https://srv-syslog.domaine.local/ L'adresse IP du serveur doit apparaître dans la liste et les logs doivent être accessibles.

La configuration est terminée pour ajouter un serveur à une infrastructure syslog-ng en place.