Rapport sur Syslog

Préparé par :

M. CHRIYAA Mohamed Amine

Encadré par :

M. B. NASSEREDDINE

Sommaire

Introduction

Syslog est un utilitaire de journalisation de tous types de messages du système, qu'ils soient sans importance ou d'une importance critique.

Chaque message envoyé à **syslog** a deux labels :

- Le premier décrit la fonction de l'application qui l'a généré (**facility**).
  Ex : **Mail**.

- Le second décrit le degré de gravité du message.

L'enregistrement des événements système est géré par un logiciel **syslogd.**

I- Le fichier /etc/syslog.conf :

Les dossiers auxquels syslog écrit chaque type de message reçu est défini dans le fichier de configuration /etc/syslog.conf

Ce fichier consiste de 2 colonnes :

- La première :
  ->Liste des facilités et sévérités des messages à attendre.

- La seconde :

->L'emplacement où ils doivent être enregistrés

Exemple :

Par défaut, les messages d'**info** sont enregistrés dans **/var/log/messages** et les messages de **Mail** dans **/var/log/maillog.**

II- Les services/facilités supportés :

Pour les services supportés par syslog, on trouve les services suivants :

Service	Description
Auth	Authentification
Authpriv	Messages privés auth
Mail	Système de courrier
Kern	Le noyau
User	Process des utilisateurs
Daemon (Disk And Execution MONitor)	Démon système
Uucp	UUCP
Cron	Démon cron
Mark	Messages générés à intervalles réguliers
Local0-7	Huit niveaux de messages locaux
*****	Toutes les facilités sauf **mark**

III- Les degrés de gravité :

Les niveaux de gravité sont huit, on peut les classer comme suivant dans un ordre décroissant selon le degré de gravité la plus importante :

Degré de gravité	Mot-clé	Description
0	**Emerg**	Emergency : Urgence → Système inutilisable
1	**Alert**	Alerte : Action immédiate nécessaire
2	**Crit**	Critical : Condition critique
3	**Err**	Erreur
4	**Warning**	Avertissement
5	**Notice**	Notification
6	**Info**	Messages à titre d'information seulement
7	**Debug**	Messages de débogage

IV- Applications et exemples :

A partir du fichier syslog.conf de Redhat, on tire :

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

➔ Dans ce cas, tous les messages avec une gravité supérieure ou égale à « info » seront enregistrés dans le fichier /var/log/messages à l'exception des messages provenant des services Mail, cron ou auth.

Authpriv.* /var/log/secure
Mail.* -/var/log/maillog

➔ Tous les messages provenant du service authpriv sont loggés dans /var/log/secure.

➔ Tous les messages du service mail sont loggés dans le fichier /var/log/maillog. Mais, la diffèrence est que le « **-** » nous permet de dire au système de ne pas loggé les messages dès qu'ils arrivent mais de les laisser pour après. (caching mode)

*.emerg *

→ Tous les utilisateurs connectés reçoivent le message d'urgence

Enfin, quelques commandes pratiques :

- Activer les modifications, il faut redémarrer **syslog** en tapant cette commande en mode administrateur :

/etc/init.d/syslog restart

- Voir les nouveaux **logs** en temps réel :

Tail -f /var/log/messages
(même commande pour les autres fichiers de **log**)

- Voir les **logs** page par page :
  More /var/log/maillog

- Machine distante :

Syslogd permet l'envoi des messages à une autre machine utilisant aussi syslogd. Il suffir de taper :

***.crit @server** (envoie les messages critiques au serveur)

Cependant, avant on doit lancer **syslog** avec le paramètre **–r**.

- Liste d'utilisateurs :

On donne les logins :

*.info user1, user3

Conclusion :

L'archivage des événements s'avère très utile lors de la recherche des erreurs d'une application et aussi lors de l'administration d'un réseau.

L’utilitaire syslog est certes difficile à gérer mais facilité énormément la gestion du système.