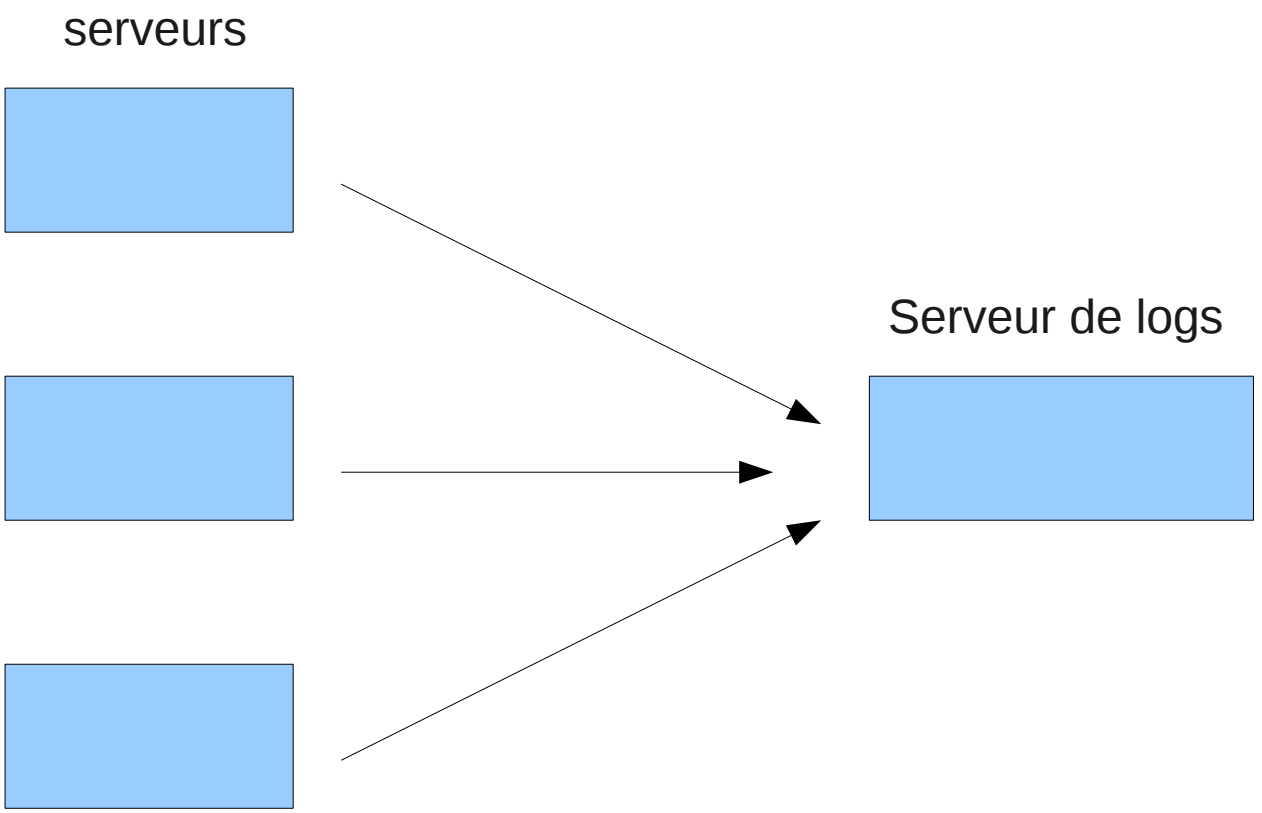
Laboratoire LIG

Présentation de la gestion des fichiers de log

Architecture générale



Les messages de log

Facility

- AUTHPRIV
- KERN
- MAIL, FTP, ...
- DAEMON
- LOCAL0
- ...

Level

- EMERG
- ALERT
- CRIT
- WARNING
- NOTICE
- ...

Tri des messages par syslogd

Fichier /etc/rsyslogd.conf

mail.info	/var/log/mail.info
mail.warn	/var/log/mail.warn
kern.*	/var/log/messages
*.debug	/var/log/debug
.	@tupi.imag.fr
.	@@tupi.imag.fr

Organisation sur la machine tupi

Choix :

- Utilisation de syslog-ng
- Destination : le directory /logarchive
- Un directory par mois de nom <annee>.<mois> (exemple : 2012.06 pour juin 2012)
- Des fichiers préfixés par la nom de la machine source

Configuration de syslog-ng

Fichier /etc/syslog-ng/syslog-ng.conf :

- source s_net { udp(); };
- filter f_auth { facility(auth, authpriv); };
- destination df_auth_net { file("/logarchive/$YEAR.$MONTH/$HOST.auth.log"); }
- log{

  source(s_net);

  filter(f_auth);

  destination(df_auth_net);

  };

Politique de gestion des logs

- Implémentée par un script déclenché par cron qui :
  - Compresse les fichiers qui ne sont pas du mois courant
  - Encrypte les fichiers de plus de 3 mois
  - Détruit les fichiers de plus de un an

Infrastructure de cryptage

- Contraintes : respect de la loi
  - pouvoir coder sans pouvoir décoder.
  - Conserver les informations permettant le décodage pour pouvoir les donner sur réquisition judiciaire.

Infrastructure de cryptage (2)

- Réalisation :
  - Choix de gnupg avec clé privée et clé publique
  - Le serveur de log crypte à l'aide de la clé publique
  - La clé privée a été copiée sur 2 clés USB confiées à des personnes n'étant pas des administrateurs système.

Quelques chiffres

- 77 serveurs loggés
- 1,3 Go d'espace disque consommé

Merci de votre attention