Syslog

- syslogd: daemon chargé de gérer les journaux d'une machine
  - journaux: /var/log/*.log (en général)
- peut gérer les journaux d'hôtes distants
  - option « -r » à positionner explicitement
  - rfc 3164: BSD Syslog protocol
  - udp port 514
  - supporté par de nombreux type d'équipement réseau: un standard incontournable

Syslog est un système de gestion des journaux utilisé sur les systèmes unix. Il apporte deux choses vitales: 1) décharger les programmeurs de la gestion des journaux et 2) permettre à l'administrateur de contrôler l'ensemble des journaux au travers d'un outil et d'un fichier de configuration unique.

syslog permet de gérer les entrées de journaux en fonction de leur type et de leur niveau d'urgence. Il est capable de sauvegarder les entrées dans des fichiers (situés souvent dans /var/log), sur la console d'utilisateurs connectés mais aussi de les envoyer via réseau à une machine distante. Le protocole utilisé pour l'envoi distant est décrit dans la RFC 3164. Le transfert se fait en udp sur le port 514.

Ce mode de fonctionnement distant est utilisé par de nombreux matériels réseau (commutateur, coupe-feu, routeurs, ...) et constitue de nos jour un standard incontournable. syslog est couramment utilisé pour centraliser tous les journaux d'un parc. Il existe des services syslog pour windows (cf ntsyslog).

Pour activer la réception des évenements distants sur la machine cible, il faut utiliser le commutateur « -r » de syslogd.

Le signal HUP (1) oblige syslogd à fermer ses fichiers journaux et à relire son fichier de configuration. Il est utilisé pour permettre un déplacement des journaux : 1) déplacer le journal (l'inoeud ne change pas donc syslog continu d'écrire dedans) 2) killall -HUP syslogd

A noter, certaines versions anciennes de syslogd n'étaient capables d'utiliser que des fichiers journaux existants. Si un journal configuré dans syslogd.conf n'existait pas sur disque, il n'était pas créé et les événements n'étaient pas journalisés.

Syslog

- sécurité:
  - pas d'authentification, de filtrage des sources,
  - pas de chiffrement des informations
  - udp: non connecté, pas d'assurance de délivrance

Sécurité:

syslog n'a pas été pensé pour fonctionner dans un environnement agressif. Il est facile à abuser, à inonder avec de fausses alertes, ...:

- les hôtes distants pouvant envoyer des événements via réseau ne sont pas authehtifiés: syslogd est donc vulnérables à l'usurpation (spoofing). En cas de compromission d'un poste sur le réseau, il faut être très méfiant vis vis des entrées concernant ce poste mais aussi de celles concernant les autres postes.
- les informations circulent en clair sur le réseau et peuvent donc être sniffées
- syslog s'appuie sur udp qui est en mode non connecté sans garantie de délivrance: certains paquets peuvent être perdus. Un attaquant peut tenter d'augmenter le pourcentage de pertes de paquets pour diminuer le nombre d'événements récus par le syslog distant. Certains syslog réccents ou outils équivalents sont capables de travailler en tcp.

Syslog

- gestion des journaux:
  - gaffe classique: un disque plein à cause de journaux accumulés
  - outils de gestion des journaux : logrotate, newsyslog, ...: compresser, déplacer, effacer, ...

gestion des journaux:

Les journaux sont des fichiers dans lesquels l'information s'accumule. Il est nécesaire de gérer les journaux de façon à éviter qu'ils finissent par remplir le système de fichiers où ils sont. Cette gestion doit répondre à deux contraintes contradictoires : 1) Taille: supprimer des informations quand la taille devient trop importante et 2) durée: garder les information un temps minimal pour permettre leur analyse éventuelle.

Les politiques usuelles s'appuie sur des rotations à intervalle régulier avec une conservation des fichiers un temps donné. Par exemple: rotation tous les soirs et conservation des fichiers 5 jours au plus.

Une telle politique, fonction uniquement du temps n'est pas en mesure de réagir à une augmentation subite du volume des journaux due à un problème où à une attaque. Elle doit donc être complétée par des mesures liées à la taille des journaux permettant à l'administrateur d'être informé et de réagir à temps pour éviter 1) une perte des événements et 2) un blocage de la machine à cause du remplissage du système de fichier correspondant.

De nos jours, la rotation des journaux n'est plus gérée par des scripts écrit par l'administrateur système mais par des outils comme logrotate (Linux debian sarge), newsyslog (FreeBSD), ...

Syslog

- analyse des journaux:
  - pour détecter un problème et/ou en déterminer les causes **après coup**
  - pour alerter d'un problème **en cours**
  - des rapport d'analyse de journaux trop long ne sont pas (plus) lus. Il faut :
    - réagir rapidement aux choses graves
    - extraire les informations pertinentes de la masse d'information
  - Deux types d'outils
    - outils d'analyse de journaux: logcheck, logsurfer, swatch, sec, ...
    - via un ids: système de détection d'intrusion

Les journaux contiennent une masse d'événements anodins dans lesquels il va falloir détecter les entrées pertinentes. Extraire les événements dignes d'intérêt est une tâche difficile qui doit répondre à deux contraintes opposées : 1) ne pas laisser passer des choses apparemment anodines mais pouvant se révéler importantes(=> rapports plus gros) et 2) avoir des rapports **courts** et synthétiques pour limiter le temps de lecture.

Comme ces deux contraintes sont impossibles à satisfaire, il est usuel d'avoir des rapports synthétiques courts (et donc incomplets) permettant de surveiller les points vitaux.

Deux types d'outils sont disponibles pour aider à l'analyse des journaux:

- des outils d'analyse de journaux comme logcheck, swatch, logsurfer, ... qui se contente de sélectionner des lignes en fonction de critères configurables. SEC est un outil plus évolué qui permet de définir des critères embrassant plusieurs événements. Ces outils sont relativement simples à configurer mais ils ne sont capables de faire des liens entre des opérations différentes apparemment anodine mais dont l'ensemble constitue par exemple une attaque. Exemple classique: scan de port et cartographie préludant un attaque.
- les systèmes de détection d'intrusion: l'analyse des journaux est l'un des multiples sources d'informations à partir de laquelle travaillent ces outils. Ils ont le défaut d'être plus lourds à déployer et, surtout, dans un soucis d'exhaustivité, de fournir des rapports longs comme un jour sans pain qui finissent par ne plus être lus faute de temps.

Quelque soit la solution utilisée, elle doit garantir que les trois types de messages suivants sont signalés à l'administrateur :

- messages relatifs à la sécurité
- messages qui indiquent que les disques sont remplis
- message qui arrivent plusieurs fois

syslog-ng:

- configuration plus souple
- classement des messages par leur contenu, par l'hôte d'origine
- meilleure redirection des messages sur le réseau
- possibilité de chroot
- peut utiliser UDP et TCP
- chiffrement et authentification du trafic réseau
- portable
- export des journaux vers un sgbd

configuration: syslog.conf

- facilité.niveau<tab>action
- facilité: type de service source

Action
fichier
terminal
pipe |
@machineDistante
utilisateur1,utilisateur2,..
*

Niveau	
emerg (panic)	Situations de panique.
alert	Situations urgentes.
crit	Situations critiques.
err (error)	Erreurs.
warning (warn)	Messages de WARNING.
notice	Messages divers.
info	Messages d'informations.
debug	Débogage.

Facilités	
kern	Le noyau.
user	Process des utilisateurs.
mail	Système de courrier.
daemon	Démons systèmes.
auth	Authentification.
lpr	Système de spooling d'imprimante.
news	Usenet.
uucp	UUCP.
cron	Démon cron.
mark	Messages générés à intervals réguliers.
local0-7	Huit niveaux de messages locaux.
syslog	Messages internes à syslogd.
authpriv	Messages privés auth.
*	Toutes les facilités sauf mark.

syslog.conf a un format simple :

- les lignes vides et les lignes contenant le caractère # sont ignorées
- les autres sont de la forme: selecteur <tabulation> action

La fait d'utiliser des espaces au lieu de tabulation est une erreur classique qui rend le fichier invalide pour certains syslog. C'est une erreur facile à faire via un copier/coller.

Le sélecteur est soit un sélecteur seul, soit une liste de sélecteur séparés par des point virgules

un sélecteur seul est de la forme facilité.niveau. La facitlité indique l'entité qui a émis l'événement. Tout événement correspondant à la facilité et ayant **un niveau supérieur ou égal** à celui indiqué entraînera l'exécution de l'action correspondante. Une facilité peut être remplacé par une liste de facilités séparées par des virgules. * (tout) remplace facilité ou niveau.

La virgule dans une liste de sélecteur correspond à un OU logique (il suffit de vérifier l'un des sélecteurs pour que l'action soit effectuée). Il y a une seule exception: si le niveau est none, tout événement correspondant au à la facilité associé ne déclenchera pas l'action, indépendamment du reste du sélecteur.

La majeure partie des syslog récents offrent des extensions et notamment la possibilité d'utiliser le signe égal pour désigner les évéments dont le niveau est égal au niveau indiqué (et non plus supérieur ou égal).
Exemple: mail.=debug <tabulation> /var/log/mail.debug

Exemple d'extrait de syslog.conf (FreeBSD) :

```
*.err;kern.debug;auth.notice;mail.crit          /dev/console
*.notice;kern.debug;lpr.info;mail.crit;news.err /var/log/messages
security.*                                      /var/log/security
auth.info;authpriv.info                         /var/log/auth.log
cron.*                                          /var/log/cron
*.emerg                                         *
```

Syslog : demo

- lister le syslog d'un système existant
- lister un journal de /var/log, montrer les entrées "MARK" insérées par syslogd
- tester son comportement avec la commande logger
  - logger -p mail.crit "boîte au lettre en feu :-) »
  - logger -p news.err "pas de nouvelles, bonne nouvelle"
  - comparer l'effet avec le contenu de syslog.conf et notamment que le message est stocké si son niveau est supérieur ou égal à celui de la règle
- le modifier en y insérant une entrée
- tester l'entrée insérée avec logger

Bibliographie sur la supervision et sur syslog

- « unix, guide de l'administrateur » de Nemeth, Snyder & Al, Campus press
- « MISC No 22 » (revue): superviser sa sécurité
- Ntsyslog: http://ntsyslog.sourceforge.net/

Comme souvent, le livre de Nemeth, Snyder et Al est une bonne présentation tant des concepts liés à syslog que des détails pratiques importants tirés de leur expérience de terrain. Le chapitre consacré à syslog est bon point d'entrée.

Misc 22: un numéro de la revue MISC (sécurité) consacré à la supervision. Un ensemble assez riche d'articles qui présente les tenants et les aboutissants de tout ce qui est supervision.

NTSyslog: permet d'envoyer les événements des journaux windows NT, 2000 et + à un syslog distant.