Gestion et Surveillance de Réseau

Gestion des journaux

Notions de base sur Syslog

Utilisation du protocole UDP, port 514

Les messages Syslog comportent deux attributs (outre le message proprement dit) :

Catégorie			Sévérité	
Auth	Security	|	Emergency	(0)
Authpriv	User	|	Alert	(1)
Console	Syslog	|	Critical	(2)
Cron	UUCP	|	Error	(3)
Daemon	Mail	|	Warning	(4)
Ftp	Ntp	|	Notice	(5)
Kern	News	|	Info	(6)
Lpr		|	Debug	(7)
Local0 ...Local7		|		

Gestion et supervision des journaux

- Stocker les journaux dans un lieu sûr où ils peuvent être facilement inspectés.
- Garder un œil sur les fichiers journaux.
- Ces fichiers contiennent des informations importantes :
  - Beaucoup de choses peuvent arriver et un contrôle doit être effectué.
  - Une fastidieuse, lorsqu'elle doit être faite manuellement.

Gestion et supervision des journaux

Sur vos routeurs et commutateurs

```
Sep  1 04:40:11.788 INDIA: %SEC-6-IPACCESSLOGP: list 100 denied tcp
79.210.84.154(2167) -> 169.223.192.85(6662), 1 packet

Sep  1 04:42:35.270 INDIA: %SYS-5-CONFIG_I: Configured from console
by pr on vty0 (203.200.80.75)

CI-3-TEMP: Overtemperature warning

Mar  1 00:05:51.443: %LINK-3-UPDOWN: Interface Serial1, changed
state to down
```

Ainsi que sur vos serveurs

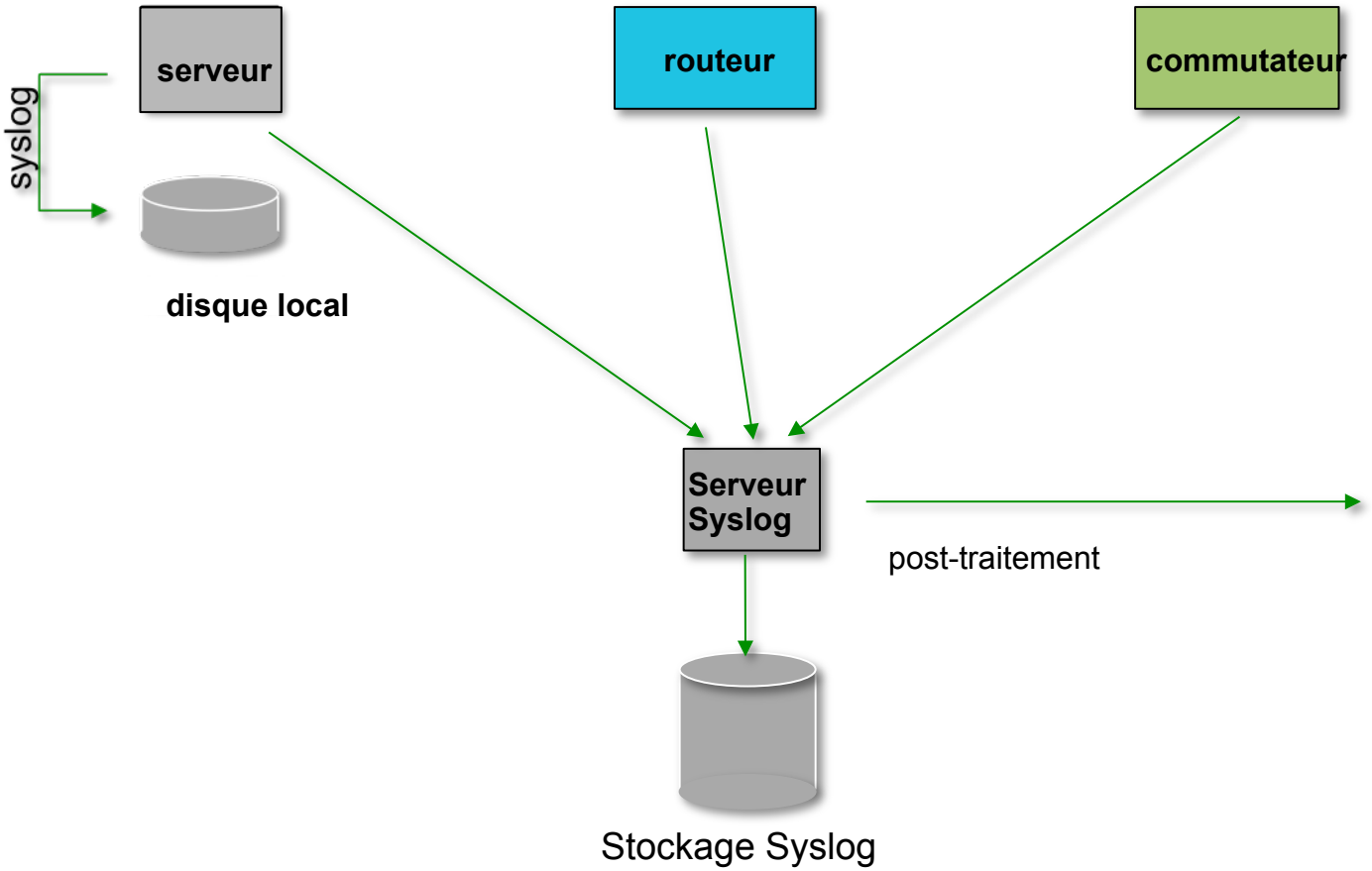
```
Aug 31 17:53:12 ubuntu nagios3: Caught SIGTERM, shutting down...

Aug 31 19:19:36 ubuntu sshd[16404]: Failed password for root from
169.223.1.130 port 2039 ssh2
```

Gestion des journaux

- Centralisez et consolidez vos fichiers journaux.
- Acheminez tous les fichiers journaux de vos routeurs, commutateurs et serveurs vers un nœud unique – *serveur de journaux*.
- Tous les équipements réseau et serveurs UNIX/ Linux peuvent être gérés avec une version de *syslog* (on utilise `syslog-ng` ou `rsyslog` pour cet atelier)
- Windows peut également utiliser syslog avec des outils supplémentaires.
- Enregistrez vos fichiers journaux en local ainsi que sur un serveur de journaux central.

Journalisation centralisée



Configurer une journalisation centralisée

Équipement Cisco

- Le minimum:

```
logging IP.du.log.host
```

Nœuds Unix et Linux

- Modifiez /etc/syslog.conf, en ajoutant :

```
*.*          @ip.of.log.host
```

- Redémarrez syslogd, rsyslog ou syslog-ng

D'autres équipements présentent des options similaires

- Options de contrôle *facility* et *level*

Réception de messages - syslog-ng

- Identifiez le *facility* sur laquelle l'équipement émetteur enverra ses messages.
- Reconfigurez *syslog-ng* pour écouter au réseau*
  - Sous Ubuntu, changer `/etc/syslog-ng/syslog-ng.conf`
- Créer le fichier suivant*

  `/etc/syslog-ng/conf.d/10-network.conf`
- Créer un nouveau répertoire pour les logs:

  ```
  # mkdir /var/log/network
  ```
- Redémarrer le service *syslog-ng* :

  ```
  # service syslog-ng restart
  ```

Si on utilise rsyslog

- *rsyslog* est inclus par défaut dans Ubuntu (mais nous préférons syslog-ng). La configuration est un peu différente, mais nous avons des labos pour:
- Mettre à jour `/etc/rsyslog`
- Créer le fichier suivant

  `/etc/rsyslog.d/30-routerlogs.conf`
- Créer un nouveau répertoire pour les logs et mettre à jour les permissions:

```
# mkdir /var/log/network
# chown syslog:adm /var/log/network
```

- Redémarrer le service *rsyslog*:

```
# service rsyslog restart
```

Tri des journaux

- A l'aide des attributs *facility* et *level*, vous pouvez trier les journaux par catégories dans différents fichiers.
- Avec un logiciel tel que *syslog-ng* vous pouvez effectuer des tris automatiques par machine, date... dans différents répertoires.
- Vous pouvez utiliser *grep* pour examiner les journaux.
- Vous pouvez utiliser les outils UNIX classiques pour trier et éliminer les éléments désirés :

```
egrep -v '(list 100 denied|logging rate-limited)' mylogfile
```

- Ces procédures peuvent-elles être automatisées ?

Tenshi

- Outil simple et flexible pour la supervision
- Messages triés en files (queues), avec des expression rationnelles
- Chaque file peut être configuré pour qu'un mail de synthèse soit envoyé pendant un intervalle de temps donnée
  - C'est à dire: indiquer à Tenshi de vous envoyer un mail de synthèse avec tous les messages syslogs qui répondent aux critères, mais une fois toutes les 5 minutes, pour éviter de remplir votre boite à lettres.

Exemple de configuration Tenshi

```
set uid tenshi
set gid tenshi

set logfile /log/dhcp

set sleep 5
set limit 800
set pager_limit 2
set mailserver localhost
set subject tenshi report
set hidepid on

set queue dhcpd tenshi@localhost sysadmin@noc.localdomain [*/10 * * * *]

group ^dhcpd:
dhcpd ^dhcpd: .+no free leases
dhcpd ^dhcpd: .+wrong network
group_end
```

Références et liens

Rsyslog

http://www.rsyslog.com/

SyslogNG

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

Windows Log to Syslog

http://code.google.com/p/eventlog-to-syslog/

http://www.intersectalliance.com/projects/index.html

Tenshi

http://www.inversepath.com/tenshi.html

Other software

http://sourceforge.net/projects/swatch/

http://www.crypt.gen.nz/logsurfer

http://simple-evcorr.sourceforge.net/

Questions ?