



Gestion et Surveillance de Réseau

Gestion des journaux



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license
(<http://creativecommons.org/licenses/by-nc/3.0/>)

Notions de base sur Syslog

Utilisation du protocole UDP, port 514

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

<u>Facility</u>		<u>Level</u>
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

Qu'entend-on par 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 opération délicate et 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

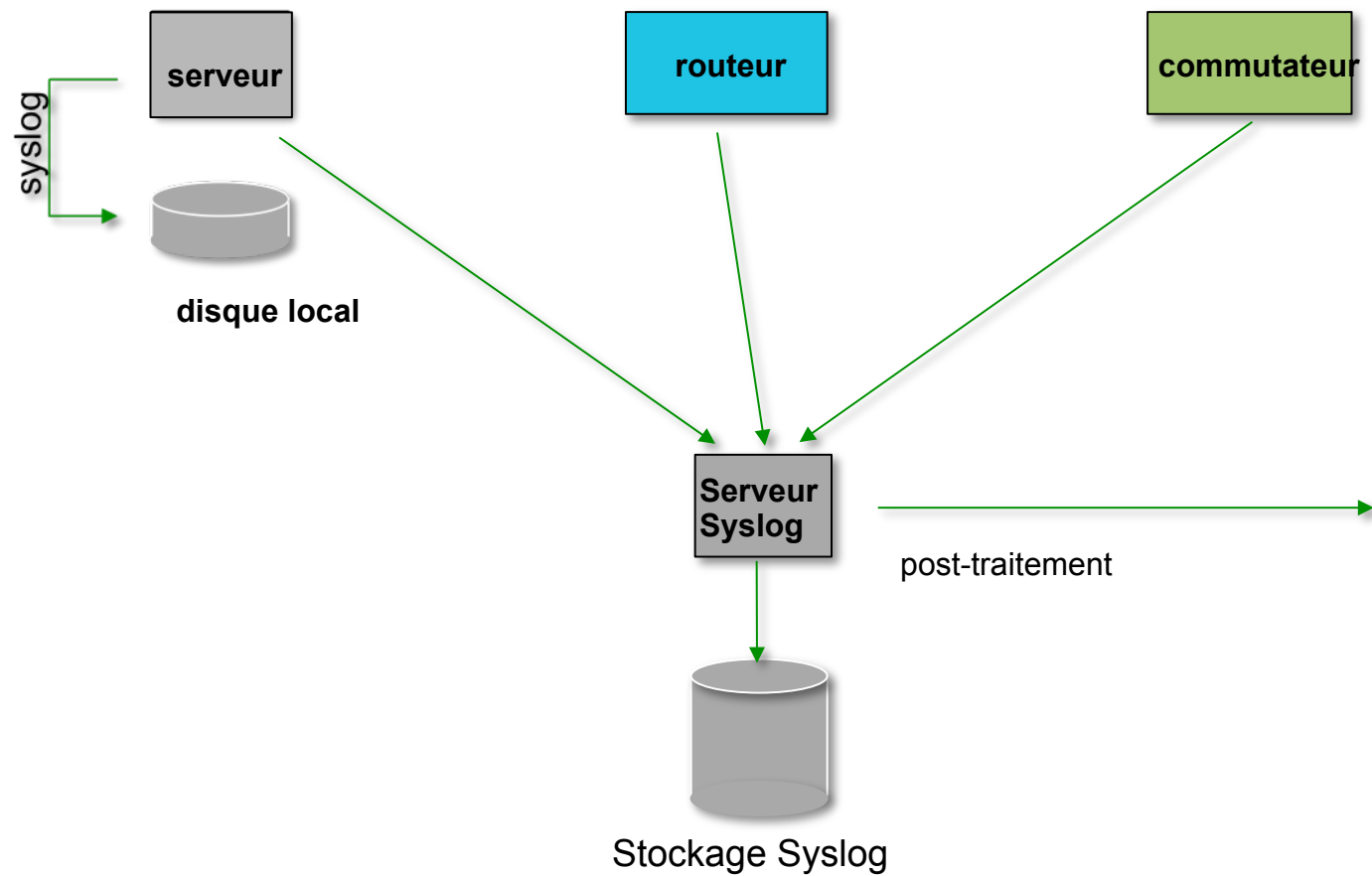
```
Aug 31 17:53:12 ubuntu nagios3: Caught SIGTERM, shutting down...
```

```
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 stockés avec une version de *syslog*.
- 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

- A minima :
 - Ip de l'hôte de connexion

Nœuds Unix et Linux

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

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

- Redémarrez syslogd

D'autres équipements présentent des options similaires

- Options de contrôle *facility* et *level*

Réception de messages syslog

- Identifiez *l'installation* sur laquelle l'équipement émetteur enverra ses messages.
- Reconfigurez *syslogd* pour écouter le réseau.
 - Sous Ubuntu : ajoutez "-r" dans `/etc/default/syslogd`
 - (Les versions récentes utilisent `rsyslog`)
- Ajoutez dans *syslodg* une entrée indiquant où écrire les messages :

```
local7.*                /var/log/routers
```

- Créez le fichier

```
touch /var/log/routers
```

- Redémarrez *syslogd*

```
/etc/init.d/syslogd 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 ?

SWATCH

Simple Log Watcher

- Écrit en Perl
- Supervise les journaux en recherchant des motifs à l'aide d'expressions régulières
- Effectue une action spécifique en cas de détection d'un motif
- Tous les motifs et actions sont possibles.
- Définir les motifs est la partie la plus difficile.

Exemple de configuration

```
ignore /éléments à ignorer/  
  
watchfor /NATIVE_VLAN_MISMATCH/  
    mail=root,subject=VLAN problem  
    threshold type=limit,count=1,seconds=3600  
  
watchfor /CONFIG_I/  
    mail=root,subject=Router config  
    threshold type=limit,count=1,seconds=3600
```

Quels sont ces éléments ? Quelle est leur signification ?

Références & liens

SyslogNG

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

Rsyslog

<http://www.rsyslog.com/>

Journal d'événements Windows dans Syslog

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

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

Supervision de journaux avec SWATCH

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

Autres logiciels

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

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

Exemples de configurations

SWATCH : <http://www.campin.net/swatchrc>

SEC :

<http://www.brandanhutchinson.com/>

[Simple_Event_Coordinator_\(SEC\).html](http://www.brandanhutchinson.com/Simple_Event_Coordinator_(SEC).html)

Questions ?

?