Programme
Opérations de registre avancées

Gestion des journaux

Gestion et supervision des journaux

- Qu'entend-on par gestion et supervision des journaux ?
- Il s'agit de stocker les journaux en lieu sûr tout en pouvant facilement les inspecter avec des outils.
- Gardez un oeil sur vos fichiers journaux.
- Ces fichiers fournissent des indications importantes...
  - il se passe beaucoup de choses, et quelqu'un doit garder l'oeil ouvert...
  - pas très pratique manuellement !

Gestion et supervision des journaux (suite)

- Sur les routeurs et les 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 les serveurs

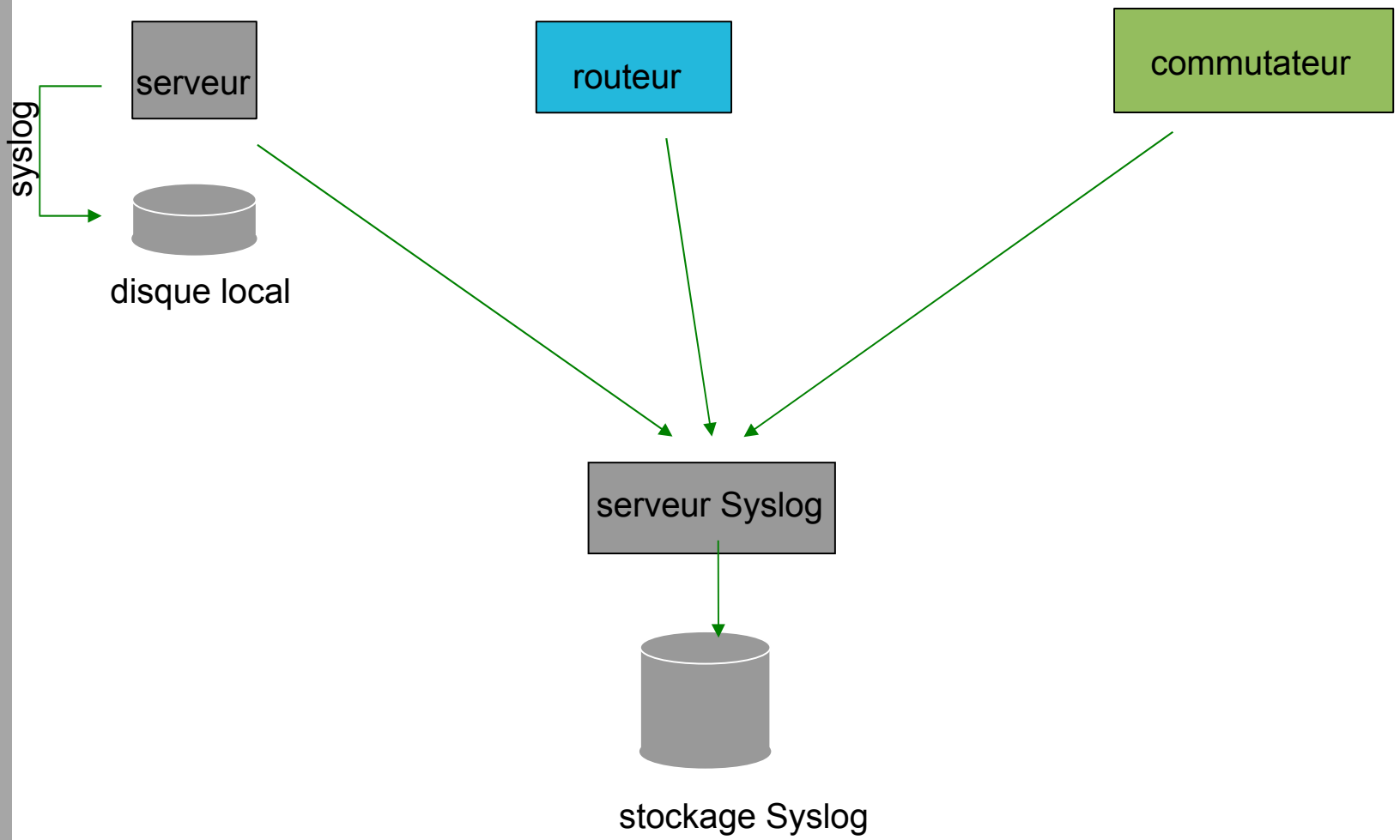
  Aug 31 17:53:12 ubuntu nagios3: Caught SIGTERM, shutting down...

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

Gestion des journaux

- Vous devez tout d'abord centraliser et consolider vos fichiers journaux.
- Consignez dans un fichier journal tous les messages des routeurs, commutateurs et serveurs sur une machine unique – un serveur de journaux.
- Tous les enregistements issus des équipements réseau et serveurs UNIX sont réalisés avec syslog.
- Windows peut être configuré pour utliliser également syslog avec certains outils.
- Entregistrez vos fichiers journaux localement ainsi que sur le serveur central.

Journalisation centralisée



Configuration pour une journalisation centralisée

- **Equipement Cisco**
  - A minima :
    - Ip de l'hôte de connexion

- **Hôte UNIX**
  - Modifiez /etc/syslog.conf, en ajoutant :

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

  - Relancez syslogd.

- **D'autres équipements présentent des options de contrôle similaires**
  - options *facility* (installation) et *level* (niveau).

Réception des messages

- Identifiez l'installation sur laquelle l'hôte ou l'équipement émetteur enverra ses messages.
- Reconfigurez syslogd pour écouter le réseau (sous Ubuntu/Debian : ajoutez "-r" dans /etc/defaults/syslogd
- Ajoutez dans syslogd une entrée indiquant où écrire les messages :

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

- Créez le fichier :

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

- Redémarrez syslogd

```
/etc/init.d/sysklogd restart
```

Notions de base sur Syslog

- Protocole UDP, port 514
- Les messages Syslog comportent deux attributs (outre le message proprement dit) :

Facility			Level	
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		|		

Tri des journaux

- En partant des attributs facility et level, triez par catégories dans les différents fichiers.
- Recourez à des outils tels que syslog-ng pour effectuer des tris automatiques par hôte, date... dans différents répertoires.
- Repérez-vous avec grep à travers les différents journaux.
- Recourez aux outils UNIX classiques pour trier et éliminer les éléments superflus :

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

  - Ces procédures peuvent-elles être automatisées ?

SWATCH

- Simple Log Watcher
  - Écrit en Perl
  - Supervise les fichiers journaux, recherche des ”motifs” (expressions régulières) à appliquer aux journaux
  - Effectue une action donnée lorsqu’un motif est identifié.

Exemple de configuration

```
ignore /things to ignore/

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
```

Références

- http://www.loganalysis.org/
- Syslog NG
  - http://www.balabit.com/network-security/syslog-ng/
- Journal d'événements Windows dans Syslog
  - https://engineering.purdue.edu/ECN/Resources/Documents/UNIX/evt
- Supervision de journaux avec SWATCH
  - http://swatch.sourceforge.net/
  - http://www.loganalysis.org/sections/signatures/log-swatch-skendrick.t
  - http://www.loganalysis.org/
  - http://sourceforge.net/docman/display_doc.php?docid=5332&group_i

Références

- http://www.crypt.gen.nz/logsurfer/
- http://sial.org/howto/logging/swatch/
- http://www.occam.com/sa/CentralizedLogging2009.pdf
- http://ristov.users.sourceforge.net/slct/

Des questions ?

?