Gestion de Redes
NSRC-UNAN León

Gestion de Logs

Gestion de Logs y Monitoreo

Que es gestion de logs y monitoreo?

- Matienendo sus logs en un lugar seguro donde se puede estar inspeccionado facilmente.
- Vigilando los archivos de logs
- Tienen datos importantes…
  - Muchas cosas pasen y alguien tiene que revisarlos.
  - No es practico hacer esto manualmente.

Gestion de Logs y Monitoreo

En sus enrutadores y conmutadores:

```
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
```

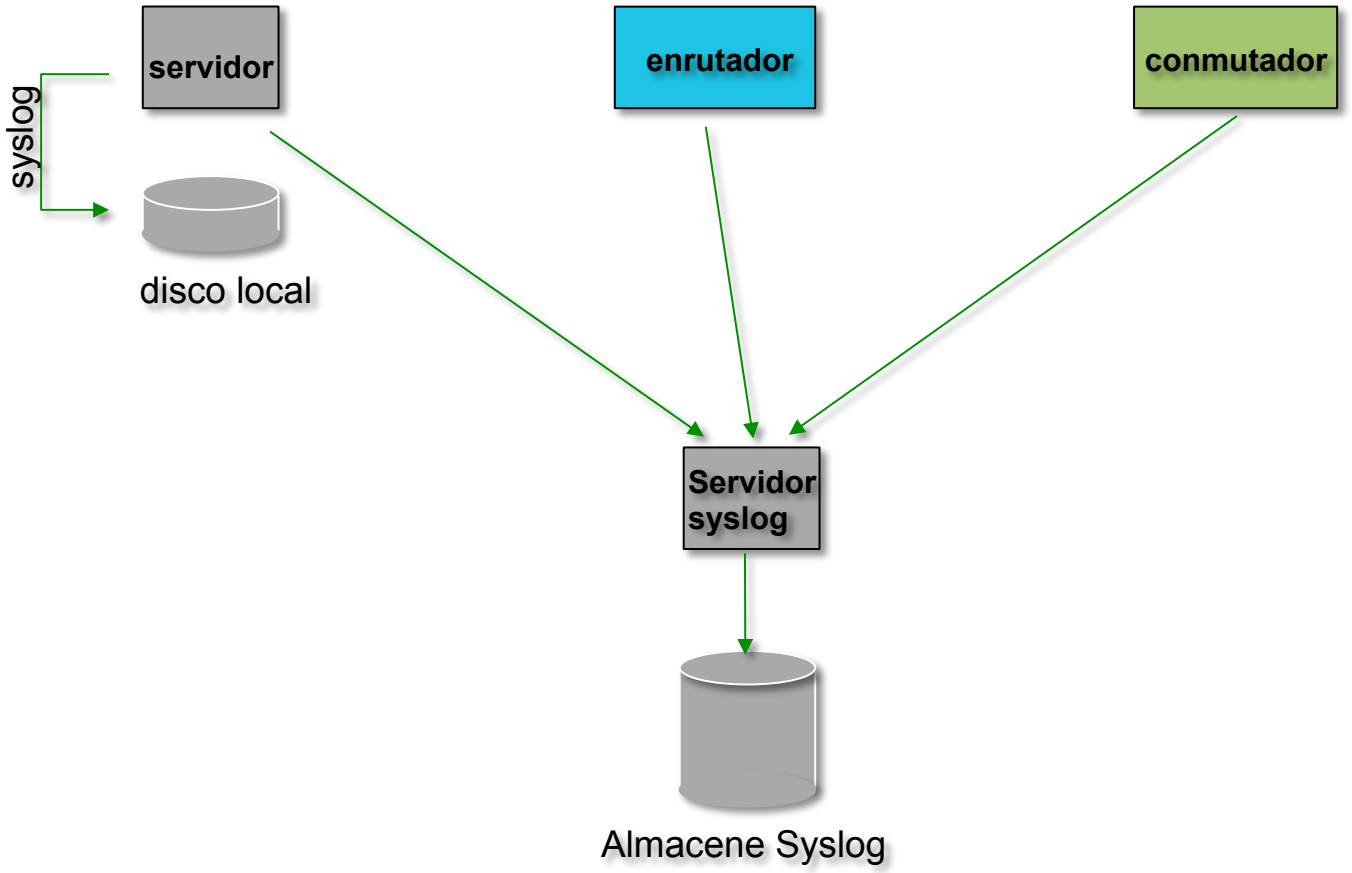
Y, los servidores:

```
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 de Logs

- Centralizar y consolidar los archivos de log
- Manda todo los mensajes de sus enrutadores, conmutadores y servidores a un solo nodo – *un servidor de logs*.
- Todo los mensajes de equipos de Red y de servidores de UNIX y Linux se lo hace a traves `syslog`.
- Windows puede usar syslog tambien usando herramientas extras.
- Graba los logs localmente, pero tambien a un servidor central de logs.

Logging Centralizado



Configurando Logging Centralizado

Equipos Cisco

- Minimo:
  - logging ip.de.host.de.logs

Nodos de Unix y Linux

- En /etc/syslog.conf, agrega:

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

- Reinitializa syslogd

Otros equipos tiene opciones similares

- Opciones para controlar *`facility`* y *`level`*

Recibiendo los Mensages

- Identifica la *`facility`* que el nodo o dispositivo de SENDING va a mandar sus mensajes.
- Reconfigurar *syslogd* escuchar a la Red.
  - Ubuntu: agrega "`-r`" a `/etc/defaults/syslogd`
- Agrega una entrada a *syslogd* a donde se va a escribir los mensajes:

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

- Crea el archivo:

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

- Reinitializa *syslogd*

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

Los Basicos de Syslog

Usa protocolo UDP, puerto 514

- Los mensages de syslog tienen dos atributos (mas que el mensaje mismo):

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			

Agrupando Logs

- Usando *`facility`* y *`level`*, agrupa por categoria en archivos distintos.
- Con software como *syslog-ng*, agrupa por nodo, fecha, etc. en forma automatica en directorios diferentes.
- Usa *grep* para revisar los logs.
- Usa herramientas tipicas de UNIX para agrupar y eliminar las cosas que quiere filtrar:

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

- Hay forma de hacer esto automaticamente?

SWATCH

Simple Log Watcher

- Escrito en Perl
- Hace monitorea de los logs buscando patrones usando expresiones regulares.
- Ejecutar una accion especifica si se encuentra un patron.
- Puede ser cualquier patron y cualquier accion.
- Definir los patrones es el parte dificil.

Configuracion de Muestra

```
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
```

Que son? Que significa?

Referencias

http://www.loganalysis.org/

Syslog NG

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

Windows Event Log a Syslog:

- https://engineering.purdue.edu/ECN/Resources/Documents/UNIX/evtsys

SWATCH log watcher

- http://swatch.sourceforge.net/
- http://www.loganalysis.org/sections/signatures/log-swatch-skendrick.txt
- http://www.loganalysis.org/
- http://sourceforge.net/docman/display_doc.php?docid=5332&group_id=25401

Referencias

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/

Preguntas?

?