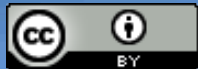




## Gestión de Red

# Gestión de Registros (logs)



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

# Conceptos Básicos de Syslog

## Usa el protocolo UDP, puerto 514

Los mensajes de Syslog tienen dos atributos (además del mensaje en sí):

### Facility

Auth	Security
Authpriv	User
Console	Syslog
Cron	UUCP
Daemon	Mail
Ftp	Ntp
Kern	News
Lpr	
Local0 ...Local7	

### Level

Emergency	(0)
Alert	(1)
Critical	(2)
Error	(3)
Warning	(4)
Notice	(5)
Info	(6)
Debug	(7)

# Gestión y Monitorización de Registros

- Mantenga sus registros en un lugar seguro donde puedan ser consultados fácilmente.
- Observe sus registros.
  - Contienen información importante:
    - Muchas cosas ocurren y alguien tiene que ponerles atención.
    - No es práctico hacer esto manualmente

# Gestión y Monitorización de Registros

## En sus enrutadores y switches

```
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 en sus servidores

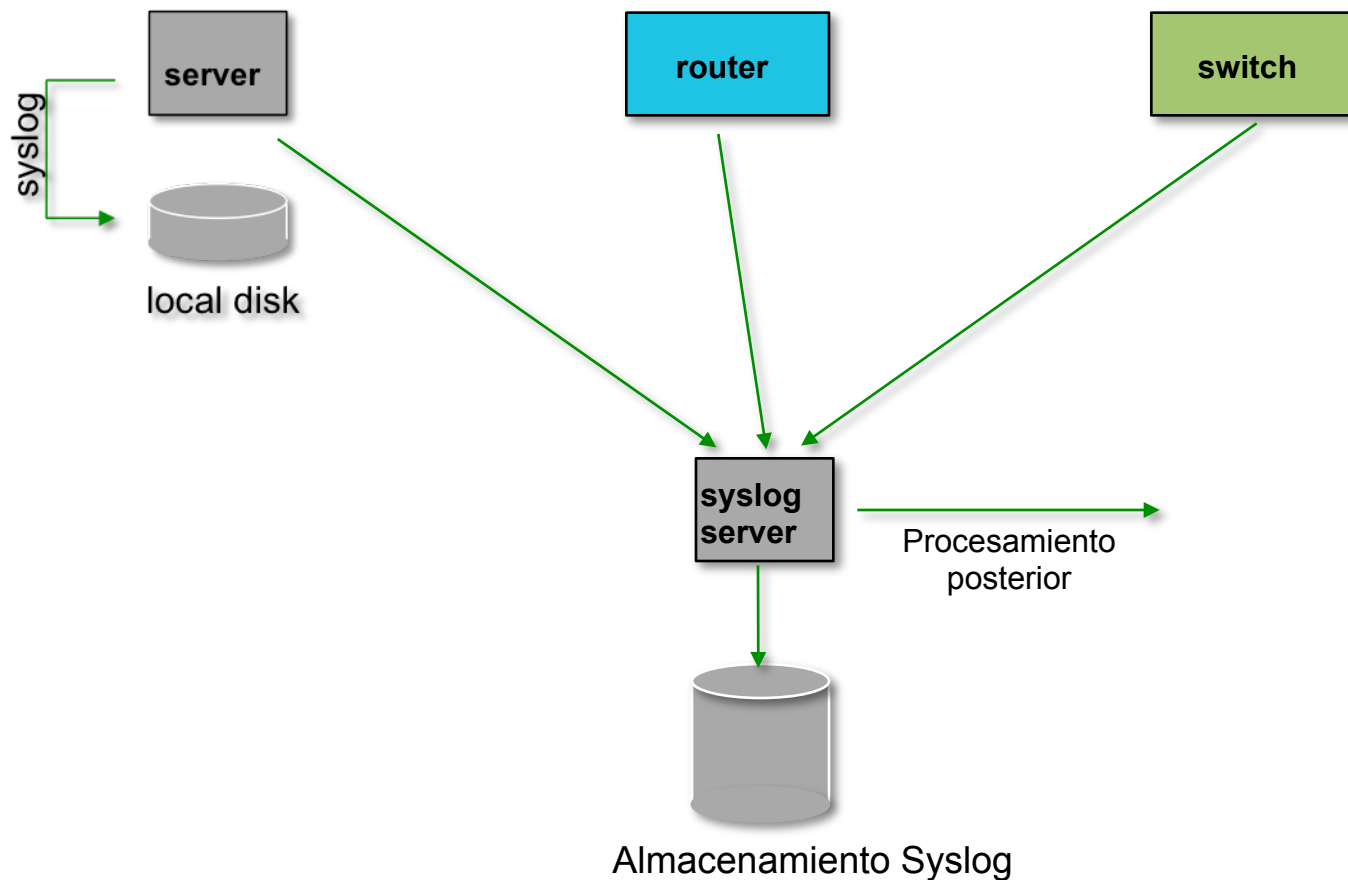
```
Aug 31 17:53:12 ubuntu nagios3: Caught SIGTERM, shutting down...
```

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

# Gestión de Registros

- Centralice y consolide sus archivos de registros
- Envíe todos los mensajes de todos sus dispositivos a un único nodo: *el servidor de registros*.
- Todos los dispositivos de red y los servidores Unix/Linux se pueden monitorizar usando alguna versión de *syslog* (usaremos `rsyslog` en este taller).
- Windows también puede usar syslog con herramientas adicionales.
- Guarde una copia de sus registros localmente, pero también envíelos a un repositorio central.

# Centralización de registros



# Configuración para enviar registros fuera del sistema

## Equipos de Cisco

- Como mínimo:

```
logging ip.of.logging.host
```

## Unix y Linux

- En syslogd.conf, r en rsyslog.conf:

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

- Reiniciar syslogd o rsyslogd

## Otros equipos tienen opciones similares

- Opciones para controlar *facility* y *level*

# Cómo recibir mensajes Syslog

- Identifique el *facility* que su equipo usará para enviar los mensajes.
- Reconfigure *rsyslog* para escuchar en la red\*
  - En Ubuntu actualice `/etc/rsyslog`
- Cree el siguiente archivo y actualice\*  
`/etc/rsyslog.d/30-routerlogs.conf`
- Cree una nueva carpeta para los mensajes y actualice los permisos:  

```
# mkdir /var/log/network  
# chown syslog:adm /var/log/network
```
- Reinicie *rsyslog*:  

```
# service rsyslog restart
```

\*más detalles en los ejercicios

# Agrupación de registros

- Por medio de *facility* y *level* se pueden agrupar los registros por categoría en archivos separados
- Con software como *rsyslog* se puede agrupar por nodo, fecha, etc. automáticamente en directorios separados
- Puede usar *grep* para revisar los registros.
- Puede usar herramientas UNIX típicas para agrupar y filtrar registros:

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

- Puede hacerse esto automáticamente?

# Tenshi

- Herramienta flexible para monitorizar los registros
- Los mensajes se clasifican en colas, usando expresiones regulares
- Cada cola puede configurarse para enviar un e-mail resumiendo los registros dentro de una ventana de tiempo
  - Ej. Envíame todos los mensajes que cumplan este criterio en un solo e-mail, cada 5 minutos

# Configuración de 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
```

# Referencias y enlaces

## **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/>

# Preguntas?

?