Gestión de Red
Gestión de Registros (logs)

Network Startup Resource Center
www.nsrc.org

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
  - 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: servidor de registros.
- Todos los dispositivos de red y los servidores Unix/Linux se pueden monitorizar usando alguna versión de *syslog* (usaremos `syslog-ng` o `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.

Conceptos básicos de Syslog

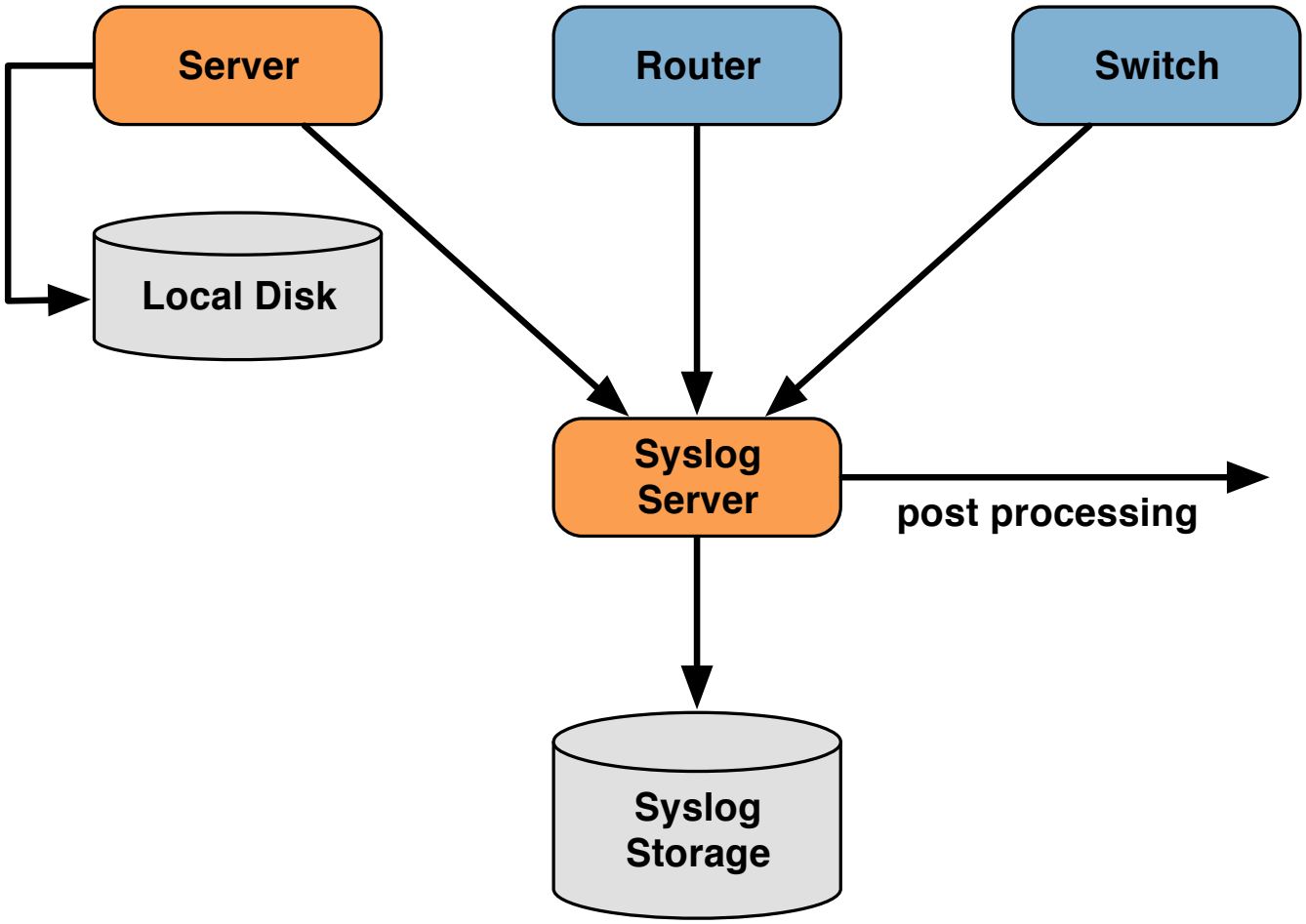
Usa el protocolo UDP, puerto 514

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

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				

Además existe el concepto de ”Priority” que es el resultado de la combinación de ”facility” y ”level”. Ver http://en.wikipedia.org/wiki/Syslog#Priority.

Registro Centralizado



Configurar Registro Centralizado

Hardware Cisco

- Como mínimo:

```
logging host1 host2 host3
```

Nodos Unix y Linux

- En syslogd.conf, o en rsyslog.conf, añadir:

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

- Reiniciar syslogd, rsyslog o syslog-ng

Otros equipos tienen opciones similares

- Opciones para controlar *facility* y *level*

Recibiendo mensajes – syslog-ng

- Identifique el facility que su equipo usará para enviar los mensajes.
- Reconfigure *syslog-ng para escuchar en la red**
  - En Ubuntu actualizar `/etc/syslog-ng/syslog-ng.conf`
- Crear el siguiente fichero*

```
/etc/syslog-ng/conf.d/10-network.conf
```

- Crear una nueva carpeta para los mensajes:

```
# mkdir /var/log/network
```

- Reiniciar el servicio *syslog-ng*:

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

*Más detalles en los ejercicios

Si se usa rsyslog

- *rsyslog* se incluye por defecto en Ubuntu (pero preferimos syslog-ng). Tiene una configuración algo distinta – también hay laboratorios de esto:
- Actualice `/etc/rsyslog`
- Cree el siguiente fichero

```
/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 el servicio rsyslog

```
# service rsyslog restart
```

Agrupación de registros

- U• 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 que quiera eliminar:

```
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 para no llenar tu correo

Ejemplo Configuración 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
```

Para aprender más de Syslog

- **RFC 3164:** *BSD Syslog Protocol*
  http://tools.ietf.org/html/rfc3164
- **RFC 5426:** Transmission of Syslog Messages over UDP
  http://tools.ietf.org/html/rfc5426
- Transmission of syslog messages over UDP draft-ietf-syslog-transport-udp-00
  http://tools.ietf.org/html/draft-ietf-syslog-transport-udp-00
- Wikipedia Syslog Entry
  http://tools.ietf.org/html/rfc3164
- Cisco Press: *An Overview of the Syslog Protocol*
  http://www.ciscopress.com/articles/article.asp?p=426638

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?