

# Gestión de Registros Parte I: rsyslog

## Gestión de Redes

### Contents

0.1	Notas . . . . .	1
<b>1</b>	<b>Ejercicio</b>	<b>1</b>
1.1	Configurar el enrutador para enviar registros syslog . . . . .	2
1.2	Configurar rsyslog . . . . .	3
1.3	Comprobación de syslog . . . . .	4
1.4	Resolver problemas con rsyslog . . . . .	5

### 0.1 Notas

- Los comandos precedidos por “\$” implican que debe ejecutar el comando como usuario genérico - no como root
- Los comandos precedidos por “#” implican que debería estar trabajando como usuario root.
- Los comandos con inicios de línea más específicos como “RTR-GW>” o “mysql>” indican que debe ejecutar los comandos en un equipo remoto, o dentro de otro programa

## 1 Ejercicio

Los enrutadores son capaces de enviar mensajes syslog a múltiples destinos. Por lo tanto debemos configurar el enrutador para enviar registros a cada una de las PCs en un grupo.

## 1.1 Configurar el enrutador para enviar registros syslog

Configure el enrutador virtual para que envíe mensajes syslog a todas las PCs de su grupo.

Cada persona en su grupo debería ingresar al enrutador del grupo y hacer lo siguiente (asumiendo que ya ha ingresado a su máquina virtual).

```
$ ssh cisco@rtrX
rtrX> enable
rtrX# config terminal

rtrX(config)# logging 10.10.X.Y
```

... sustituya X.Y por la IP de su PC (grupo + número, ej. pc2 = 10.10.1.2).

```
rtrX(config)# logging facility local0
rtrX(config)# logging userinfo
rtrX(config)# exit
rtrX# write memory
rtrX# exit
```

Ahora ejecute `show logging` para ver en resumen la configuración de envío de registros.

```
rtrX# show logging
```

Los otros participantes en su grupo estarán haciendo la misma cosa, por lo tanto no se sorprenda al ver otros destinos además del suyo en la salida del comando anterior. Oprima la barra espaciadora para visualizar todo el texto.

Salga del enrutador:

```
rtrX# exit
```

Eso es todo. El enrutador debería estar enviando paquetes UDP SYSLOG a su PC en el puerto 514.

Para verificar esto, ingrese en su PC como usuario `sysadmin` (si no lo ha hecho ya) y haga lo siguiente:

```
$ sudo bash
# apt-get install tcpdump          (puede que ya esté instalado)
# tcpdump -s0 -n -i eth0 udp port 514
```

Luego, una persona del grupo debe ingresar de nuevo al enrutador y hacer lo siguiente:

```
$ ssh cisco@rtrX
rtrX> enable
rtrX# config terminal
rtrX(config)# exit
rtrX> exit
```

El `tcpdump` producirá una salida en su PC. Algo como lo siguiente:

```
11:20:24.942289 10.10.1.254.63515 > 10.10.1.1.514: SYSLOG local0.notice, length: 110
11:20:24.944376 10.10.1.254.53407 > 10.10.1.1.514: SYSLOG local0.notice, length: 102
```

Luego de ver esto, presione Ctrl-C para salir de `tcpdump`.

Nota: `tcpdump` también podría mostrar el *contenido* de los mensajes syslog si usara el parámetro `-v` en la línea de comandos. Para aprender más sobre `tcpdump` puede escribir “man `tcpdump`”.

Ahora puede configurar el programa de manejo de registros en su PC para recibir esta información y guardarla en un conjunto de archivos.

## 1.2 Configurar rsyslog

Si no lo está, ingrese en su máquina virtual y conviértase en el usuario `root`.

Edite el archivo `/etc/rsyslog.conf`:

```
# editor /etc/rsyslog.conf
```

... y encuentre y des-comente las siguientes líneas (quite los “#”)

```
#$ModLoad imudp
#$UDPServerRun 514
```

change to:

```
$ModLoad imudp
$UDPServerRun 514
```

Luego cambie esta línea:

```
$PrivDropToGroup syslog
```

```
a:
```

```
$PrivDropToGroup adm
```

Grabe y salga.

Ahora, cree un archivo nuevo:

```
# editor /etc/rsyslog.d/30-routerlogs.conf
```

... y ponga lo siguiente (COPIAR/PEGAR!):

```
$template RouterLogs, "/var/log/network/%$YEAR%/%$MONTH%/%$DAY%/%HOSTNAME%-%$HOUR%.log"
local0.* -?RouterLogs
& ~
```

Grabe y salga, y luego:

```
# mkdir /var/log/network
# chown syslog:adm /var/log/network
```

Reinicie rsyslog:

```
# service rsyslog restart
```

### 1.3 Comprobación de syslog

Para asegurarse de enviar mensajes, ingrese de nuevo al enrutador y ejecute algunos comandos de configuración, y luego salga:

```
$ ssh cisco@rtrX
rtrX> enable
rtrX# config terminal
rtrX(config)# exit
rtrX> exit
```

No olvide salir del enrutador cuando termine. Si mucha gente ingresa en el enrutador sin hacer logout, entonces otros no pueden entrar.

En su PC, vea si los mensajes están empezando a aparecer como `/var/log/network/<año>/<mes>/<día>/`

```
$ cd /var/log/network
$ ls
$ cd 2012
$ ls
```

... esto le mostrará el directorio para el mes ... haga cd a este directorio

```
$ ls
... repita para el siguiente nivel (día del mes)
$ ls
```

Luego, use el programa ‘tail’ para mirar el final de los archivos en este directorio. Los nombres son dinámicos, basados en el nombre del origen, así que use el archivo que vea. Será algo como esto:

```
$ ls
rtr8-16.log
$ tail rtr8-16.log
... se muestran mensajes de registro ...
```

## 1.4 Resolver problemas con rsyslog

Si no aparece ningún archivo bajo la carpeta `/var/log/network`, entonces puede probar otro comando en el enrutador para generar mensajes de registro. Específicamente, el comando para bajar y subir una interfaz:

```
$ ssh cisco@rtrX
rtrX> enable
rtrX# conf t
rtrX(config)# interface Loopback 999
rtrX(config-if)# shutdown
```

Espere unos segundos

```
rtrX(config-if)# no shutdown
```

Luego salga y grabe la configuración (“write mem”):

```
rtrX(config-if)# exit
rtrX(config)# exit
rtrX# write memory
rtr1# exit
```

Mire si hay registros en `/var/log/network`

```
# cd /var/log/network
# ls
...siga la cascada de directorios
```

Aún no tiene registros?

Pruebe con el siguiente comando para enviar un mensaje de prueba localmente:

```
# logger -p local0.info "Hello World\!"
```

Si todavía no se ha creado un archivo bajo `/var/log/network`, revise si su configuración tiene errores. No olvide reiniciar rsyslog cada vez que haga un cambio en la configuración.

Qué otros comandos se le ocurren que podría ejecutar en el enrutador que puedan generar mensajes de registro? (TENGA CUIDADO!). Podría intentar ingresando al enrutador y escribiendo una clave incorrecta para “enable”.

No olvide ejecutar el comando “ls” en su directorio de registros para ver si se ha creado un archivo nuevo.

FIN.