

# Gestión de Registros Parte 2: Tenshi

## Gestión de Redes

### Contents

0.1	Notas . . . . .	1
<b>1</b>	<b>Ejercicio</b>	<b>1</b>
1.1	Actualice la configuración de rsyslog . . . . .	2
1.2	Rotación de archivos de registro . . . . .	2
1.3	Instalar tenshi . . . . .	3
1.4	Configurar tenshi . . . . .	3
1.5	Comprobación de tenshi . . . . .	4
1.6	Opcional: Añadir una regla adicional a Tenshi . . . . .	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

Asegúrese de que sus enrutadores están configurados para enviar registros a su PC (ejercicio anterior)

## 1.1 Actualice la configuración de rsyslog

Si no lo ha hecho ya, ingrese en su máquina virtual y conviértase en root:

```
$ sudo bash
#
```

Configure rsyslog para guardar todos los registros en un archivo para fines de monitorización.

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

... y encuentre la línea

```
local0.*    -?RouterLogs
```

... y agregue la siguiente línea inmediatamente después:

```
local0.*    /var/log/network/everything
```

(pero antes de la línea que dice ‘& ~’). O sea que debe terminar siendo esto:

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

Esto hará que todos los mensajes con “facility local0” vayan a un mismo archivo, de manera que podamos usar un programa que monitoree los mensajes.

Asegúrese de grabar y salir del editor.

Reinicie syslog para que recargue la configuración:

```
# service rsyslog restart
```

## 1.2 Rotación de archivos de registro

Cree un script automático para truncar el archivo de registros de manera que no se vuelva demasiado grande (COPIAR y PEGAR):

```
# editor /etc/logrotate.d/everything

/var/log/network/everything {
    daily
    copytruncate
    rotate 1
    postrotate
        /etc/init.d/tenshi restart
    endscript
}
```

Grabe y salga.

### 1.3 Instalar tenshi

```
# apt-get install tenshi
```

### 1.4 Configurar tenshi

Configure tenshi para enviarle alarmas cuando los enrutadores sean configurados (COPIAR Y PEGAR):

```
# editor /etc/tenshi/includes-available/network

set logfile /var/log/network/everything
set queue network_alarms tenshi@localhost sysadm@localhost [*/1 * * * *] Log check

group_host rtr
network_alarms SYS-5-CONFIG_I
network_alarms PRIV_AUTH_PASS
network_alarms LINK
group_end
```

Grabe y salga.

Cree un enlace simbólico para que tenshi recargue el archivo nuevo (COPIAR Y PEGAR):

```
# ln -s /etc/tenshi/includes-available/network /etc/tenshi/includes-active
```

Finalmente, reinicie tenshi:

```
# service tenshi restart
```

## 1.5 Comprobación de tenshi

Ingresa en su enrutador, y ejecute algunos comandos de configuración (vea el ejemplo):

```
$ ssh cisco@rtrX
rtrX> enable
Password: <password>
rtrX# config terminal
rtrX(config)# int FastEthernet0/0
rtrX(config-if)# description Cambiando la descripcion para Tenshi
rtrX(config-if)# ctrl-z
rtrX# write memory
```

No salga del enrutador todavía. Tal como en el ejercicio anterior de rsyslog, pruebe a bajar y subir una interfaz loopback: Don't exit from the router yet. Just as in the previous rsyslog exercises, attempt to shutdown / no shutdown loopback interface:

```
rtrX# conf t
rtrX(config)# interface Loopback 999
rtrX(config-if)# shutdown
```

espere unos segundos

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

Grabe y salga:

```
rtrX(config-if)# ctrl-z                (same as exit, exit twice)
rtrX# write memory
rtr1# exit
```

Verifique que está recibiendo e-mails de Tenshi en el buzón de sysadmin. Puede comprobar resto rápidamente mirando al directorio de correo:

```
$ ls -l /var/mail
```

Debe ser usuario sysadmin (no root). Puede abrir una sesión nueva en su máquina virtual, o puede salir de la shell de root (exit), y escribir:

```
$ mutt
```

Baje con el cursor para seleccionar un mensaje de “tenshi@localhost”, luego oprima **ENTER** para verlo, y **q** para salir del mensaje, y luego **q** de nuevo para salir de mutt.

Si no están llegando los correos, revise lo siguiente:

- Están llegando registros al archivo `/var/log/network/everything`?

```
$ tail /var/log/network/everything
```

- En estos registros se muestran nombres de nodo como ‘rtr5’? Recuerde que la manera en que hemos configurado Tenshi, sólo busca mensajes cuyos nombres de nodo concuerden con el patrón ‘rtr’.
- Revise la configuración de tenshi. Reinicie tenshi si la cambia.
- Si todavía está atascado pregunte a su instructor, o a un compañero.

## 1.6 Opcional: Añadir una regla adicional a Tenshi

Pruebe a ver si puede agregar una regla a Tenshi de manera que se envíe un e-mail si alguien introduce incorrectamente la clave de “enable” en el enrutador.

Pistas:

- “PRIV\_AUTH\_FAIL” es el tipo de mensaje de IOS (Cisco) en tales casos.
- Para probar que funciona su nueva regla, ingrese en el enrutador, escriba “enable”, y escriba una clave incorrecta.
- Nota: Tenshi revisa el archivo `/var/log/network/everything` una vez por minuto, así que puede que tenga que esperar un minuto antes de que llegue el mensaje de e-mail.

FIN.