Gestion y Monitoreo de Redes
Usando syslog-ng

Notas:
------
* Comandos que empiezan con un "$" implica que deberia ejecutar el comando
  como un usuario general - no como root.
* Comandos que empiezan con un "#" implica que deberia trabajar como el usuario root.
* Comandos con lineas mas especificas (como "GW-RTR>" o "mysql>") implica que esta
  ejecutando el comando en un equipo remoto o dentro otro programa.
* Si una linea termina con un "\" esto indica que el comando sigue en la proxima
  linea y Ud. deberia tratar el comando si como fuera en una sola linea.

Ejercicios

Ejercicios Parte I
----

0. Haz un log in en su PC o abre una ventana de terminal como el usuario sysadmin.

1. Instalacion de syslog-ng (ya esta hecho en todo sus maquinas):

        $ sudo apt-get install syslog-ng

2. Abre /etc/syslog-ng/syslog-ng.conf

        $ sudo vi /etc/syslog-ng/syslog-ng.conf

Encuentra las lineas:

        # (this is equivalent to the "-r" syslogd flag)
        # udp();

y cambiarlas a:

        # (this is equivalent to the "-r" syslogd flag)
        udp();

Al fin del archivo agrega (usa copia y pegar!):

```
filter f_routers { facility(local5); };
log {
        source(s_all);
        filter(f_routers);
        destination(routers);
};
destination routers {
 file("/var/log/network/$YEAR/$MONTH/$DAY/$HOST-$YEAR-$MONTH-$DAY-$HOUR.log"
 owner(root) group(root) perm(0644) dir_perm(0755) create_dirs(yes)
 template("$YEAR $DATE $HOST $MSG\n"));
};
```

3. Crear el directorio /var/log/network

```
$ sudo  mkdir /var/log/network/
```

4. Reinitializa syslog-ng:

```
$ sudo /etc/init.d/syslog-ng restart
```

5. Ya hemos configurado los enrutadores para que mandan mensajes de syslog a su servidor:

Esto es que hicemos por el grupo 1:

```
rtr1> enable
rtr1# config terminal
rtr1(config)# logging 10.10.1.1
rtr1(config)# logging 10.10.1.2
rtr1(config)# logging 10.10.1.3
rtr1(config)# logging 10.10.1.4
rtr1(config)# logging facility local5
rtr1(config)# logging userinfo
rtr1(config)# exit
rtr1# write memory
rtr1# exit
```

No es necesary que Ud. haz algo.

6. En su PC revisa si hay mensajes bajo los directorios de /var/log/network
---

```
$ ls /var/log/network/2011/11/13/...            (ejemplo)
```

Si no hay nada haz un login a la enrutador de su grupo y corre un comando de configuracion, sale de enrutador y revisa los logs de nuevo. Por ejemplo:

```
$ ssh cisco@rtrN                        [N es "1" a "9" dependiendo en su grupo]
password: <clave dado por instructor>
rtrX> enable
password: <clave dado por instructor>
rtrX# conf t
rtrX(config)# int FastEthernet0/0
rtrX(config-if)# description Modulo Ethernet 0/0
rtrX(config-if)# ctrl-z
rtrX# wr mem
Building configuration...
[OK]
rtrX# exit

$ ls /var/log/network/2011/11/13/...                    (ejemplo)
$ more /var/log/network/2011/11/13/15.10.10.*           (ejemplo)

etc...
```