Gestion y Monitoreo de Redes
Usando Swatch por los Registros

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 "pc1-pcx-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
----

0. Haz un log in en su PC como el usuario sysadm
----

1. Vamos a mandar todo los mensajes de logging a un solo archivo
----

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

        Y al find del archivo agrega la siguiente linea:

```
destination everything {
  file("/var/log/everything"
    template("$DATE <$FACILITY.$PRIORITY> $HOST $MSG\n") template_escape(no)
  );
};
log { source(s_all); destination(everything); };
```

        Con esto tendremos todo los mensajes de logging llegando a un solo archivo
        y, asi, podemos hacer monitoreo de los mensajes mas facilmente usando
        Swatch.

        Ahora reinitializa Syslog:

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

2. Haz un escripto para automatizar el proceso de mantener nuestro archivo de logs
   a un tamano razonable

        $ sudo vi /etc/logrotate.d/everything

        En el archvo escriba:

```
/var/log/everything {
  daily
```

```
  copytruncate
  rotate 1
  postrotate
        /etc/init.d/swatch restart
  endscript
}
```

Graba el archivo y sale.

3. Instala Swatch

```
$ sudo apt-get install swatch
```

4. Crea el archivo de /etc/swatch.conf y agrega las siguiente reglas al archivo:

```
$ sudo vi /etc/swatch.conf

watchfor /PRIV_AUTH_PASS/
        mail=sysadm,subject=Mode de enable habilitado
        threshold type=limit,count=1,seconds=3600

watchfor /CONFIG_I/
        mail=sysadm,subject=Configuracion de enrutador
        threshold type=limit,count=1,seconds=3600

watchfor /LINK-3-UPDOWN/
        mail=sysadm,subject=Cambio del estado de link
        threshold type=limit,count=1,seconds=3600

watchfor /SSH/
        mail=sysadm,subject=Coneccion a traves SSH
        threshold type=limit,count=1,seconds=3600

watchfor /ssh/
        mail=sysadm,subject=Coneccion a traves ssh
        threshold type=limit,count=1,seconds=3600
```

5. Corre Swatch

```
$ sudo swatch -c /etc/swatch.conf --daemon
```

Verifica que Swatch esta corriendo:

```
$ ps ax | grep swatch
```

6. Conectate a su enrutador y haz algun cambio de configuracion

---

```
$ ssh cisco@rtrN                        [N es "1" a "9" dependiendo en su grupo]
```

```
Paswword: <clave dado por instructor>
rtrN> enable
Password: <clave dado por instrucotr>
rtrN# config terminal
rtrN(config)# int FastEthernet0/0
rtrN(config-int)# description Cambio de Description de FastEthernet0/0 por Swatch
rtrN(config-int)# ctrl-z
rtrN# write memory
rtrN# exit
```

7. Revisa que esta recibiendo correos al usuario sysadm desde Swatch usando mutt

---

```
$ sudo apt-get install mutt
$ su - sysadm
$ mutt -f /var/mail/sysadm
"q" para quitar de mutt
```

Si haya problemas con abrir correo haz esto:

```
$ sudo touch /var/mail/sysadm
$ sudo chown sysadm:mail /var/mail/sysadm
$ sudo chmod 664 /var/mail/sysadm
```

y, ahora intenta de nuevo asi:

```
$ mutt
```