Servidor RSYLOG

Propósito: Redirigir los mensajes de syslog de un equipo a un servidor de rsyslog que los almacene. Centralizar la recuperación de mensajes de sistema en un solo host.

Escenario: dos equipos con rsyslog 1) envía sus mensajes a otro host. 2) adecúa su configuración para recibir los logs de otros equipos.

Ejemplo ficheros de configuración (añadir esta info modificando las direcciones IP)

```
1] #vi /etc/rsyslog.conf

(...) agregar esta línea

###############

#### RULES ####

###############

*.* action(type="omfwd" target="172.16.1.97" port="514"
protocol="tcp")

2] #vi /etc/rsyslog.conf

(...) agregar o descomentar esta línea

# Provides TCP syslog reception

# for parameters see http://www.rsyslog.com/doc/imtcp.html

module(load="imtcp") # needs to be done just once

input(type="imtcp" port="514")

$template entradaRemota, "/var/log/remote/%HOSTNAME%".log

*.* ?entradaRemota

3] Reiniciar los servicios

# systemctl restart rsyslog


OJOOOO!!!!!!!! Atención con el firewall.

Truco (en Redhat) firewall-cmd --add-port=514/tcp
```