

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA

UNAN-León



FACULTAD DE CIENCIAS Y TECNOLOGÍA

DEPARTAMENTO DE COMPUTACIÓN

INGENIERÍA EN TELEMÁTICA

COMPONENTE: Gestión de Red.

DOCENTE: Wilmer Matamoroz

TEMA: Configuración de un servidor Syslog remoto

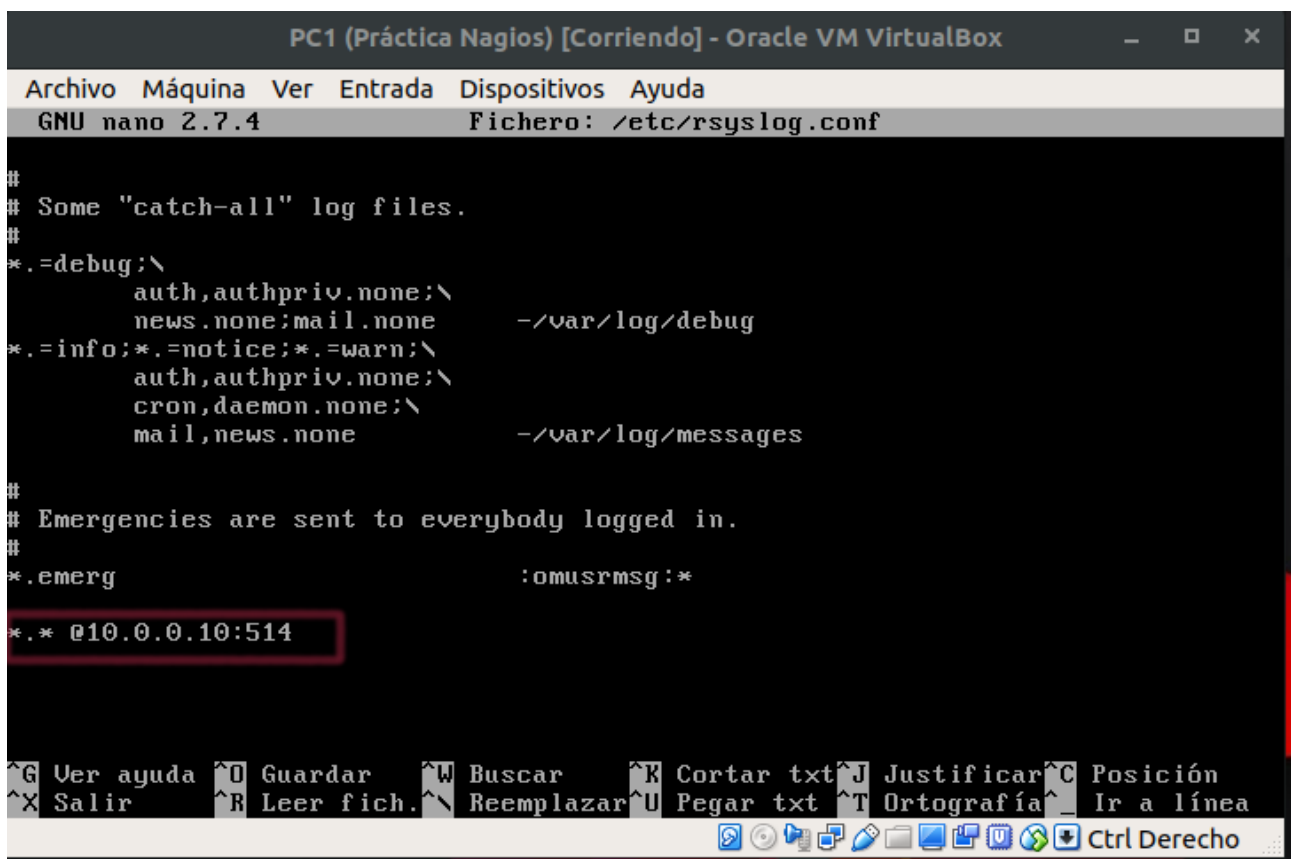
FECHA: 31/05/19

INTEGRANTE: Jonathan Eduardo Ochoa Velasquez 15-01898-0

¡A la libertad por la Universidad!

¿Qué cambios ha realizado en el fichero de configuración del cliente de rsyslog.conf?

R= En el fichero de configuración del cliente solo es necesario añadir solamente una línea:



```
PC1 (Práctica Nagios) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
GNU nano 2.7.4      Fichero: /etc/rsyslog.conf

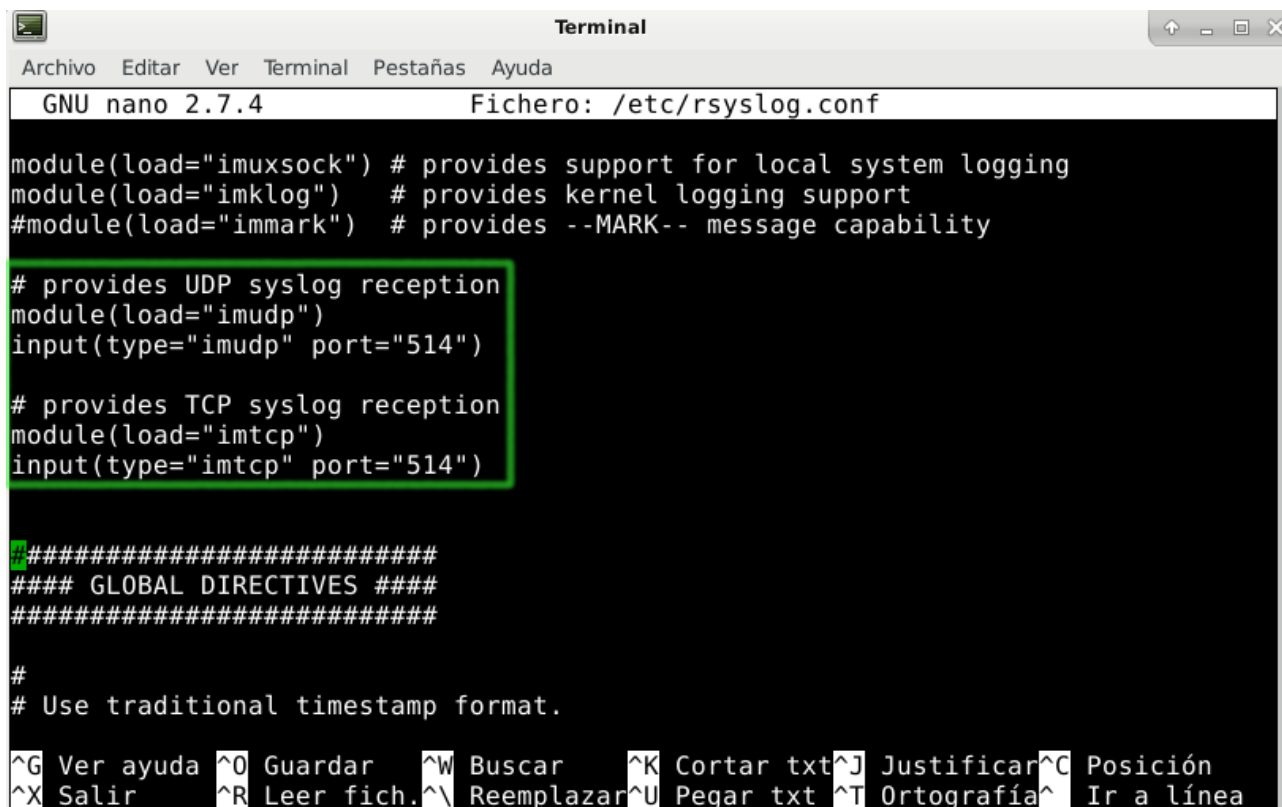
#
# Some "catch-all" log files.
#
*.=debug;\
    auth,authpriv.none;\
    news.none;mail.none      -/var/log/debug
*.=info;*.=notice;*.=warn;\
    auth,authpriv.none;\
    cron,daemon.none;\
    mail,news.none          -/var/log/messages
#
# Emergencies are sent to everybody logged in.
#
*.emerg                     :omusrmsg:*

*.* @10.0.0.10:514
```

Esta línea lo que indica es que todos los mensajes (de todo tipo) que se generen serán enviados al servidor rsyslog que configuramos, el cual tiene la ip 10.0.0.10

¿Qué cambios ha realizado en la configuración del servidor? ¿Cómo ha verificado su funcionamiento correcto?

R= En el servidor lo que hemos realizado es descomentar unas líneas en el fichero rsyslog.conf:



```
GNU nano 2.7.4 Fichero: /etc/rsyslog.conf

module(load="imuxsock") # provides support for local system logging
module(load="imklog") # provides kernel logging support
#module(load="immark") # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

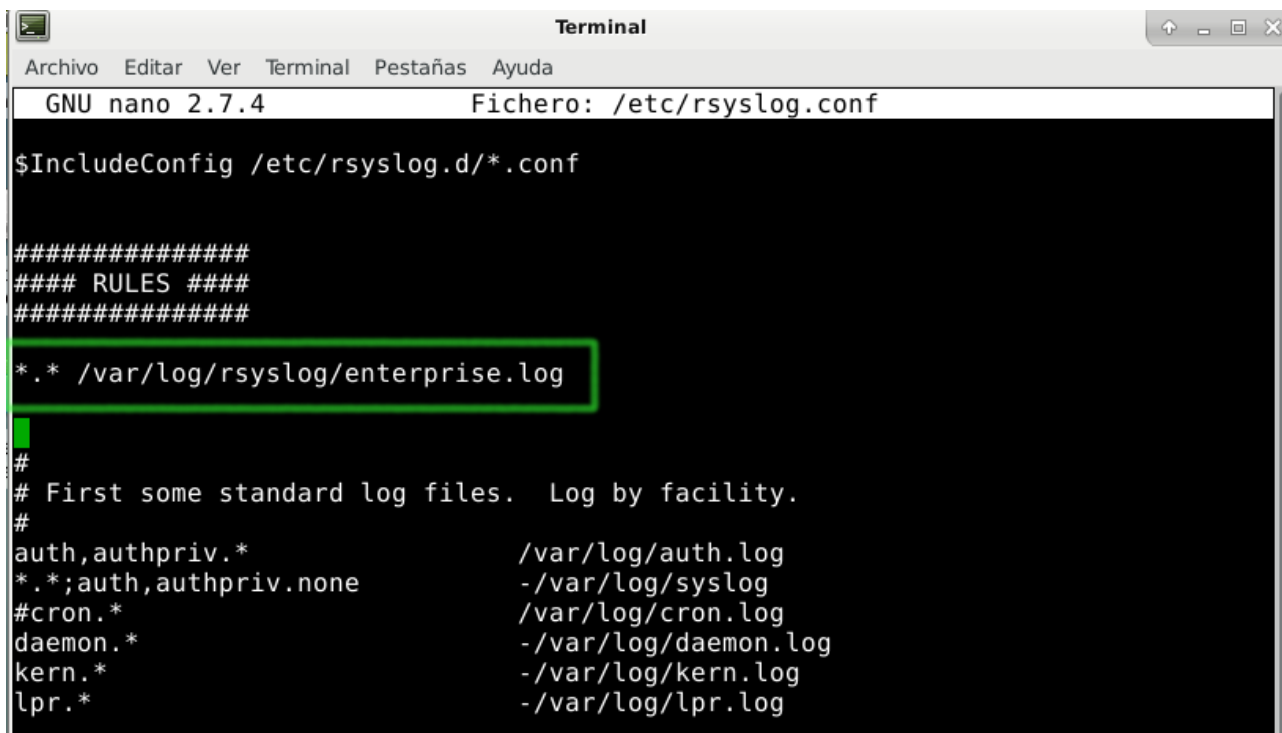
#####
#### GLOBAL DIRECTIVES ####
#####

#
# Use traditional timestamp format.

^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar txt ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar txt ^T Ortografía ^_ Ir a línea
```

Esto lo que nos permite es poner a nuestro servidor a escuchar en el puerto 514 tanto para TCP como UDP.

Lo otro que hay que hacer es agregar los tipos de mensajes que vamos a recibir:



```
GNU nano 2.7.4 Fichero: /etc/rsyslog.conf

$IncludeConfig /etc/rsyslog.d/*.conf

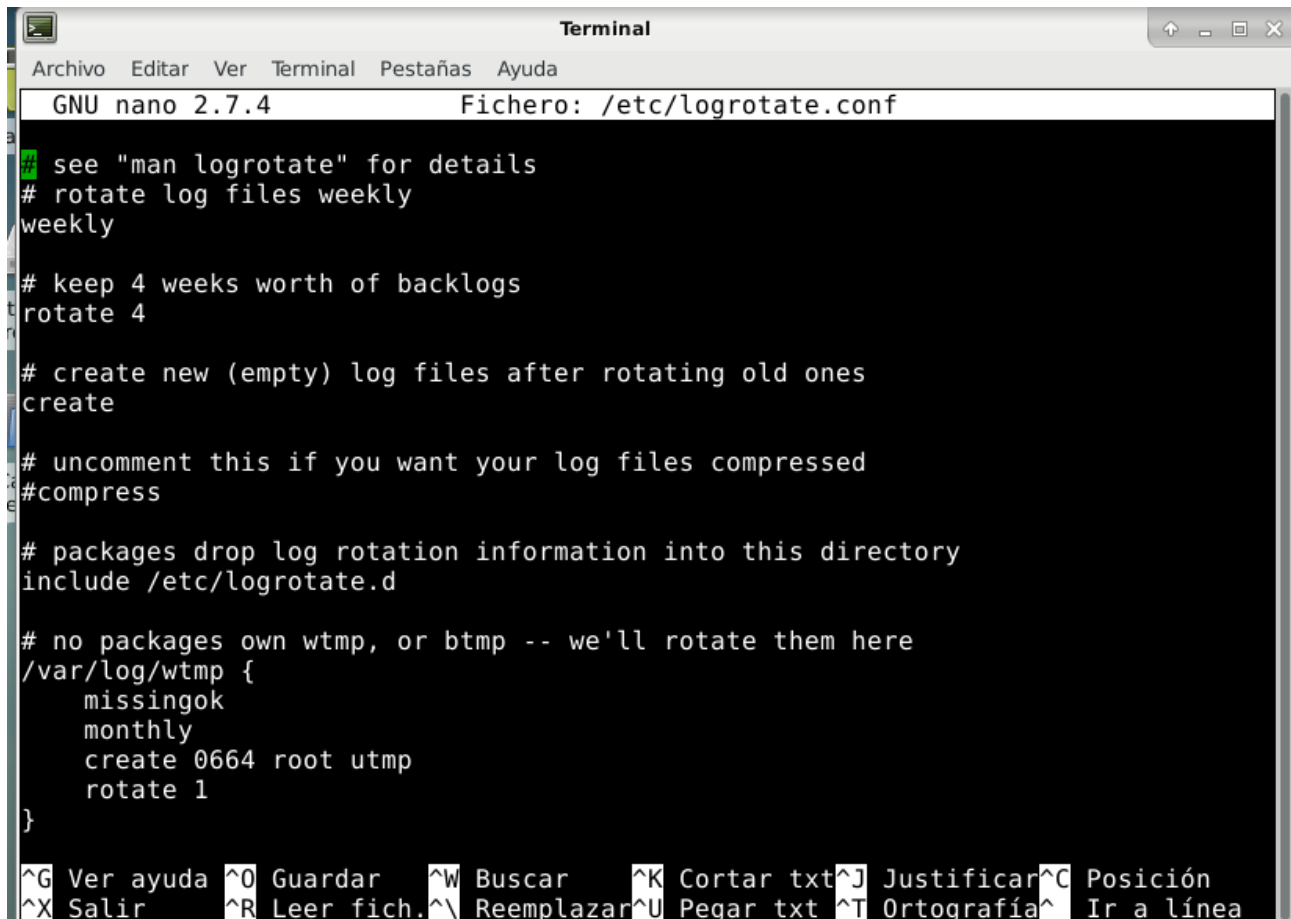
#####
#### RULES ####
#####

*.* /var/log/rsyslog/enterprise.log

#
# First some standard log files. Log by facility.
#
auth,authpriv.* /var/log/auth.log
*.*;auth,authpriv.none -/var/log/syslog
#cron.* /var/log/cron.log
daemon.* -/var/log/daemon.log
kern.* -/var/log/kern.log
lpr.* -/var/log/lpr.log
```

Esta línea lo que hace es registrar todos los mensajes de todos los dispositivos y guardar los datos en el fichero enterprise.log

¿Cómo están configurados los ficheros de syslog en logrotate.conf?



The screenshot shows a terminal window titled "Terminal" with a menu bar (Archivo, Editar, Ver, Terminal, Pestañas, Ayuda) and a status bar (GNU nano 2.7.4, Fichero: /etc/logrotate.conf). The file content is as follows:

```
see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}
```

At the bottom, a status bar shows keyboard shortcuts: ^G Ver ayuda, ^O Guardar, ^W Buscar, ^K Cortar txt, ^J Justificar, ^C Posición, ^X Salir, ^R Leer fich., ^\ Reemplazar, ^U Pegar txt, ^T Ortografía, ^ Ir a línea.

R= La configuración que los archivos de registro crecerán a lo largo de un mes, y una vez que se inicie un nuevo mes, logrotate los eliminará. Esto para evitar tener un archivo demasiado grande.

¿Qué ventajas aporta syslog-ng? ¿Indique alguna otra aplicación describiendo sus ventajas?

- Filtrado de mensajes basado en su contenido, no solo en categorías y prioridades
- Se pueden encadenar varios filtros
- Sistema más sofisticado de entrada/salida, incluyendo el envío mediante TCP y subprocesos.

Otra aplicación es **rsyslog** (The Rocket-fast Syslog Server), una de las ventajas que esta aplicación tiene es que es multihilo, tiene un hilo para aceptar los mensajes que llegan y otro hilo para guardarlos a disco, esto garantiza una mayor eficiencia, no solamente escribe mensajes a ficheros de texto y terminales, sino también a una amplia selección de base de datos.