



FACULTAD CIENCIAS DEL HOMBRE Y LA NATURALEZA

CATEDRATICO(A): MANUEL FLORES VILLATORO

MATERIA: SISTEMA OPERATIVOS DE REDES

INTEGRANTES:

NO.	APELLIDOS	NOMBRES	CARNET	%
1	HERNANDES LOBO	XAVIER EDENILSON	HL01133112	100%
2	MOGE SANCHEZ	KEVIN EDGARDO	MS01133510	100%
3	GUEVARA PEREZ	ROBERTO ALONSO	GP01133096	100%

**TEMA DE INVESTIGACIÓN: MANUAL DE INSTALACION DE SISTEMA DE
ALMACENAMIENTO DE LOGS**

FECHA: SABADO 12 DE MAYO DEL 2018

MATERIALES Y MÉTODOS.

PREPARACIÓN DEL EQUIPO:

Para realizar el proyecto utilizamos 3 computadoras con un procesador amd a10 de 3,00 GHz, un disco duro de 1TB, 8GB de memoria RAM y una arquitectura de 64bits. Sobre este equipo me dispuse a instalar una distribución de Debían versión 9.1 y configuramos las ip de las maquinas con nuestra la red LAN.

- ✓ **Para el pc 1 utilizaremos la ip:** 192.168.1.40
- ✓ **Para el pc 2:** 192.168.1.50
- ✓ **Para el pc 3:** 192.168.1.60

```
servidor@Servidor: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@Servidor:/home/servidor# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:c6:18:f6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.40/24 brd 192.168.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fec6:18f6/64 scope link
        valid_lft forever preferred_lft forever
root@Servidor:/home/servidor#
```

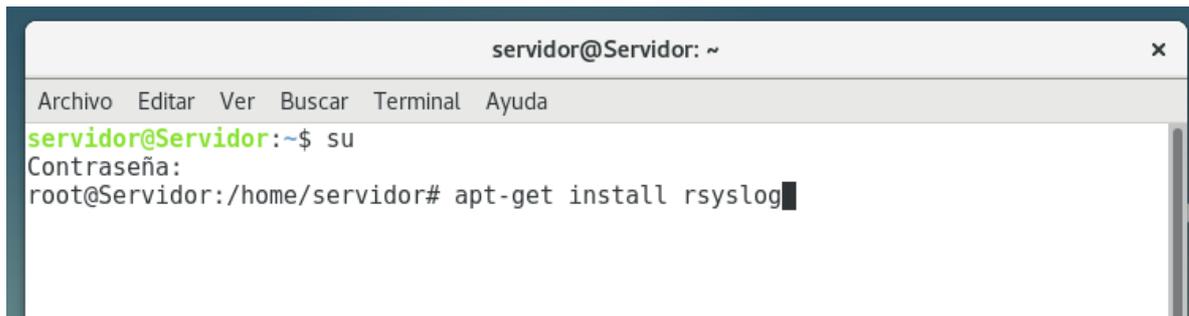
Ilustración 1 Configuración de ip.

IMAGEN 1: Configuración de la ip de la maquina 1 que servirá como el servidor centralizado de logs del sistema, le asignamos la ip: 192.168.1.40.

CONFIGURAR RSYSLOG COMO UN SERVIDOR:

El daemon (demonio) de Rsyslog se instala automáticamente en la mayoría de las distribuciones de Linux. Sin embargo, si Rsyslog no está instalado en su sistema, puede emitir uno de los siguientes comandos para instalar el servicio> necesitará privilegios de administrador para ejecutar los comandos.

En las distribuciones basadas en Debían:

A screenshot of a terminal window titled 'servidor@Servidor: ~'. The window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The terminal shows the user 'servidor@Servidor' at the prompt '~\$' typing 'su'. The prompt changes to 'root@Servidor:~/home/servidor#' and the user types 'apt-get install rsyslog'.

```
servidor@Servidor: ~
Archivo  Editar  Ver     Buscar  Terminal  Ayuda
servidor@Servidor:~$ su
Contraseña:
root@Servidor:~/home/servidor# apt-get install rsyslog
```

Ilustración 2 Instalación de rsyslog.

IMAGEN 2: Se puede visualizar el comando para instalar Rsyslog

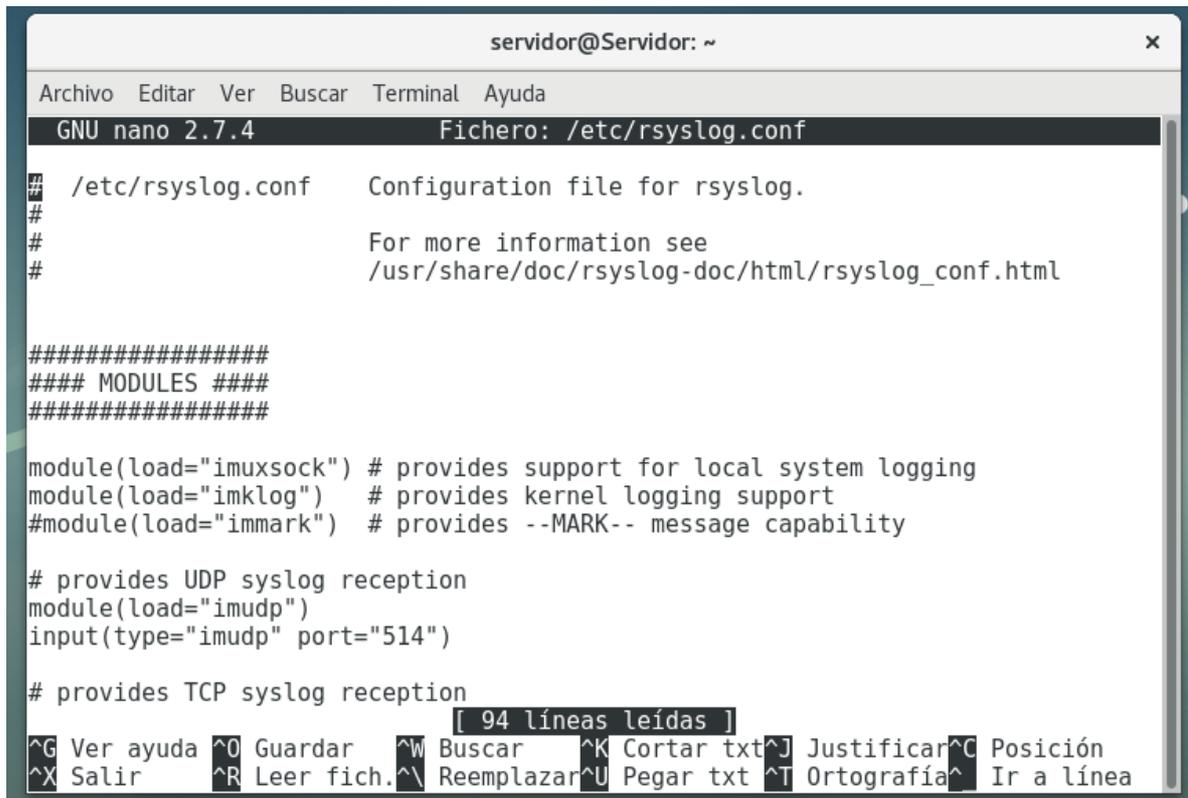
Luego Para configurar un programa rsyslog para que se ejecute en modo servidor, edite el archivo de configuración principal en /etc/rsyslog.conf. En este archivo realice los siguientes cambios como se muestra en la muestra siguiente.

Ubique y descomente eliminando el hashtag (#) las siguientes líneas para permitir la recepción de mensajes de registro UDP en el puerto 514. Por defecto, el puerto UDP es utilizado por syslog para enviar y recibir mensajes.

- ❖ #module (load = "imudp")
- ❖ #input (type = "imudp" port = "514")

Haz lo mismo para las siguientes dos líneas:

- ❖ #module (load = "imtcp")
- ❖ #input (type = "imtcp" puerto = "514")



```
servidor@Servidor: ~
Archivo Editar Ver Buscar Terminal Ayuda
GNU nano 2.7.4 Fichero: /etc/rsyslog.conf
## /etc/rsyslog.conf Configuration file for rsyslog.
#
# For more information see
# /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html
#####
#### MODULES ####
#####
module(load="imuxsock") # provides support for local system logging
module(load="imklog") # provides kernel logging support
#module(load="imark") # provides --MARK-- message capability
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")
# provides TCP syslog reception
[ 94 líneas leídas ]
^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
```

Ilustración 3 Editando el archivo `/etc/rsyslog.conf`

IMAGEN 3: Editamos el archivo `/etc/rsyslog.conf` desmarcando recepción de mensajes de registro UDP en el puerto 514.

Eso es todo lo que hay en la configuración en el servidor. Guarde y cierre ese archivo. Reinicie rsyslog con el comando:



```
servidor@Servidor: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@Servidor:/home/servidor# /etc/init.d/rsyslog restart
[ ok ] Restarting rsyslog (via systemctl): rsyslog.service.
root@Servidor:/home/servidor#
```

Ilustración 4 Reinicio de rsyslog

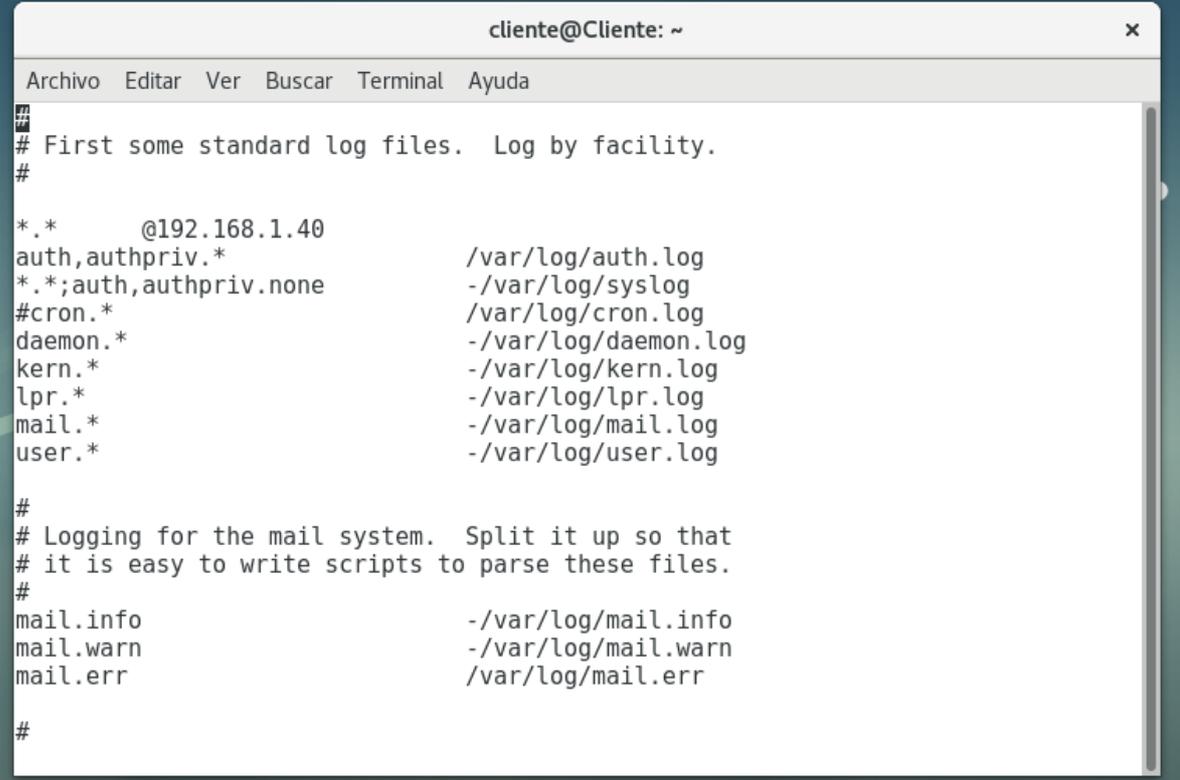
IMAGEN 5: comando para reiniciar Rsyslog

CONFIGURACIÓN DE LOS CLIENTE:

Ahora vamos a configurar los clientes para que envíen sus registros al servidor centralizado. Para hacer esto, primero abra el archivo de configuración con el comando `sudo nano /etc/rsyslog.conf`. Desplácese hasta la parte inferior de ese archivo y agregue la línea:

```
*.* @192.168.1.40
```

Esta línea permite que el servicio Rsyslog envíe todos los registros internos a un servidor Rsyslog distante en el puerto UDP 514.

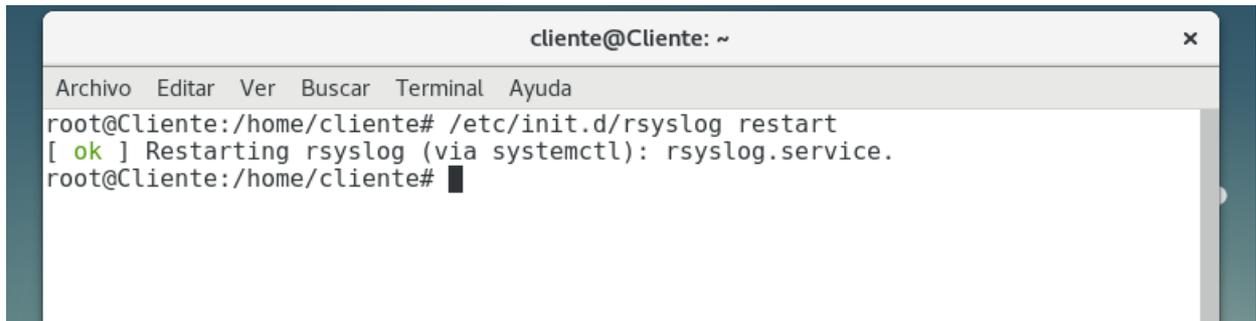


```
cliente@Cliente: ~
Archivo Editar Ver Buscar Terminal Ayuda
# First some standard log files.  Log by facility.
#
*.* @192.168.1.40
auth,authpriv.* /var/log/auth.log
*.*;auth,authpriv.none -/var/log/syslog
#cron.* /var/log/cron.log
daemon.* -/var/log/daemon.log
kern.* -/var/log/kern.log
lpr.* -/var/log/lpr.log
mail.* -/var/log/mail.log
user.* -/var/log/user.log
#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info -/var/log/mail.info
mail.warn -/var/log/mail.warn
mail.err /var/log/mail.err
#
```

Ilustración 5 Agregando el archivo Rsyslog

IMAGEN 6: En el archivo `/etc/rsyslog.conf` se agrega `*.* @` seguido se coloca la ip del servidor centralizado donde se enviarán los logs de los clientes.

Después reiniciamos Rsyslog para validar los cambios realizados:

A terminal window titled 'cliente@Cliente: ~' with a menu bar containing 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The terminal shows the command '/etc/init.d/rsyslog restart' being executed. The output is '[ok] Restarting rsyslog (via systemctl): rsyslog.service.' followed by a new prompt 'root@Cliente:/home/cliente#'.

```
cliente@Cliente: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@Cliente:/home/cliente# /etc/init.d/rsyslog restart
[ ok ] Restarting rsyslog (via systemctl): rsyslog.service.
root@Cliente:/home/cliente#
```

Ilustración 6 Reinicio de Rsyslog

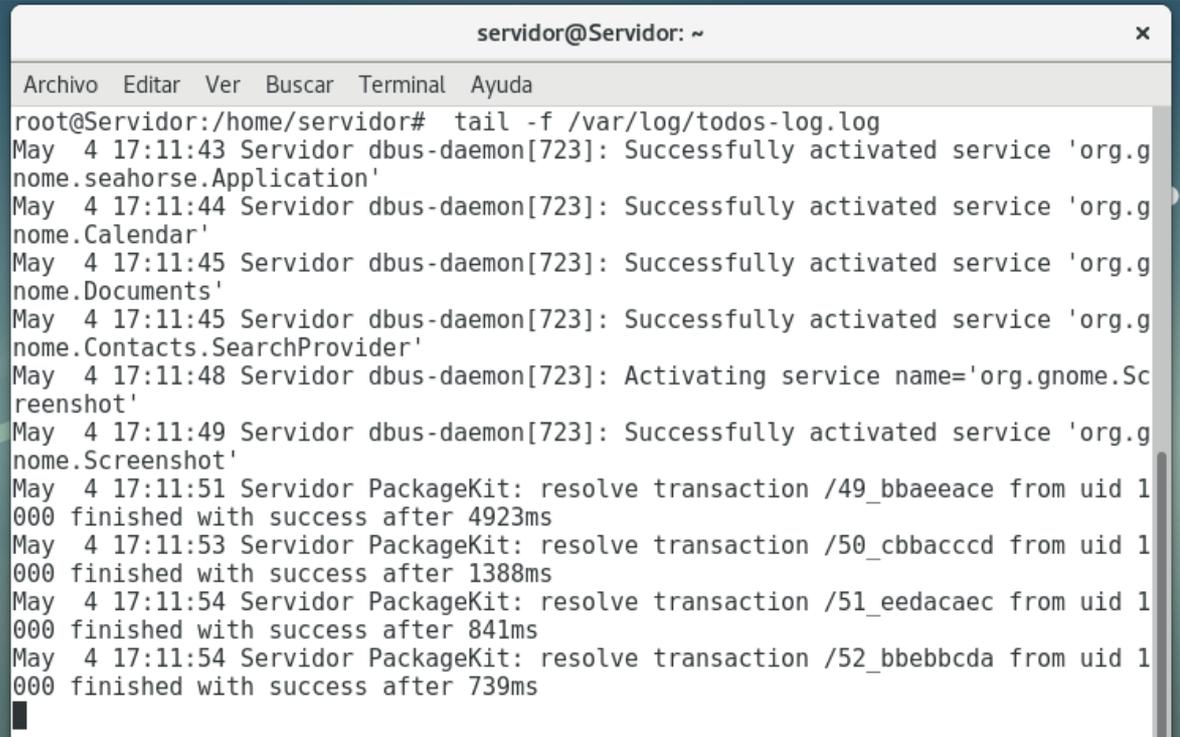
IMAGEN 7: Reinicio.

Con el mismo procedimiento podemos configurar más clientes para enviar los logs a un servidor centralizado.

RESULTADOS:

VISUALIZACIÓN DE LOS LOGS.

En este punto, los clientes rsyslog están enviando sus entradas de archivo de registro a su servidor. Si abre uno de los archivos en /va /log/todos-log.log, verá entradas que comienzan con el nombre de host de las máquinas cliente.

A screenshot of a terminal window titled 'servidor@Servidor: ~'. The terminal shows the command 'tail -f /var/log/todos-log.log' being executed. The output consists of several log entries from May 4, 2011, at 17:11:43 to 17:11:54. The entries include messages from 'dbus-daemon[723]' about activating services like 'org.gnome.seahorse.Application', 'org.gnome.Calendar', 'org.gnome.Documents', 'org.gnome.Contacts.SearchProvider', and 'org.gnome.Screenshot'. There are also messages from 'PackageKit' regarding transaction resolutions for various package IDs, all finished with success after a few hundred milliseconds.

```
servidor@Servidor: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@Servidor:/home/servidor# tail -f /var/log/todos-log.log
May  4 17:11:43 Servidor dbus-daemon[723]: Successfully activated service 'org.gnome.seahorse.Application'
May  4 17:11:44 Servidor dbus-daemon[723]: Successfully activated service 'org.gnome.Calendar'
May  4 17:11:45 Servidor dbus-daemon[723]: Successfully activated service 'org.gnome.Documents'
May  4 17:11:45 Servidor dbus-daemon[723]: Successfully activated service 'org.gnome.Contacts.SearchProvider'
May  4 17:11:48 Servidor dbus-daemon[723]: Activating service name='org.gnome.Screenshot'
May  4 17:11:49 Servidor dbus-daemon[723]: Successfully activated service 'org.gnome.Screenshot'
May  4 17:11:51 Servidor PackageKit: resolve transaction /49_bbaeeace from uid 1000 finished with success after 4923ms
May  4 17:11:53 Servidor PackageKit: resolve transaction /50_cbbacccd from uid 1000 finished with success after 1388ms
May  4 17:11:54 Servidor PackageKit: resolve transaction /51_eedacaec from uid 1000 finished with success after 841ms
May  4 17:11:54 Servidor PackageKit: resolve transaction /52_bbebbcda from uid 1000 finished with success after 739ms
```

Ilustración 7 Visualización de registros

IMAGEN 8: Visualización de registros

Archivos de registro hechos más manejables ya no tiene que acceder de forma remota a cada uno de sus servidores Linux para leer los archivos de registro. En su lugar, inicie sesión en ese servidor centralizado y vea sus entradas de registro, para cada cliente Linux configurado, en una ubicación conveniente. Esos archivos de registro son más manejables.