

Análisis Forense Informático

Rsyslog



Manual RSYSLOG

Autor: Pedro Manuel García Álvarez

Fecha: 12/02/2024

Índice

1.- Breve descripción de programa Rsyslog	3
2.- Instalación del paquete Rsyslog en el Servidor	5
3.- Configuración del servidor Rsyslog	6
4.- Instalar y configurar el cliente Rsyslog	8
5.- Verificamos los registros.....	9

Manual RSYSLOG

1.- Breve descripción de programa Rsyslog

Rsyslog (Remote System Logging) es una herramienta de software de syslog que permite la recopilación y el envío de registros de sistema a través de la red. Fue desarrollada originalmente por la empresa alemana Rsyslog GmbH y actualmente es mantenida por la comunidad de código abierto. Rsyslog es una herramienta muy versátil y potente que permite la recopilación de registros de sistema de diferentes fuentes, como servidores, dispositivos de red, sistemas embebidos, entre otros. Los registros recopilados pueden ser enviados a través de la red a un servidor centralizado, donde pueden ser almacenados, analizados y visualizados. Rsyslog admite diferentes protocolos de comunicación, como TCP, UDP, SSL/TLS y TCP sobre SSL/TLS. También admite diferentes formatos de registros, como RFC 5424, RFC 5427, RFC 6587, entre otros. Entre las características más destacadas de Rsyslog se encuentran:

- Recopilación de registros de sistema de diferentes fuentes, como servidores, dispositivos de red, sistemas embebidos, entre otros.
- Envío de registros recopilados a un servidor centralizado mediante diferentes protocolos de comunicación, como TCP, UDP, SSL/TLS y TCP sobre SSL/TLS.
- Admisión de diferentes formatos de registros, como RFC 5424, RFC 5427, RFC 6587, entre otros.
- Capacidad de filtrar y clasificar registros en función de diferentes criterios, como la fuente del registro, la fecha y hora del registro, el contenido del registro, entre otros.
- Integración con otros sistemas de monitoreo y gestión de registros, como Nagios, Splunk, Graylog, entre otros.
- Posibilidad de agregar funciones personalizadas mediante la creación de plugins y módulos de extensión.
- Interfaz de usuario gráfica para la configuración y monitoreo del sistema.
- Compatibilidad con diferentes sistemas operativos, como Linux, Unix, Windows, entre otros.

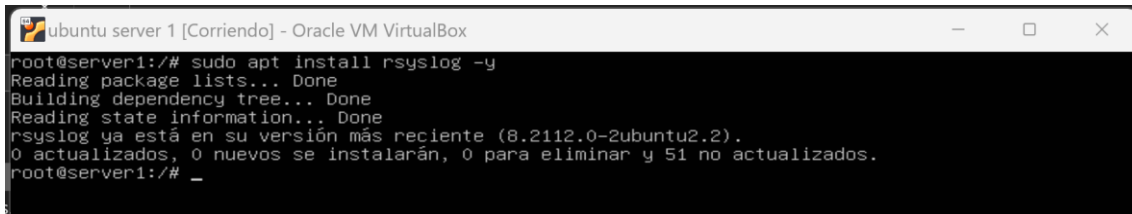
Rsyslog es una herramienta muy útil para la recopilación y el análisis de registros de sistema en entornos de red complejos. Permite la monitorización de servidores, dispositivos de red y sistemas embebidos de manera centralizada y eficiente, lo que facilita la detección y

resolución de problemas de seguridad y de rendimiento. Además, la capacidad de filtrar y clasificar registros en función de diferentes criterios permite una mayor eficiencia en la identificación de patrones y tendencias en los registros. En resumen, Rsyslog es una herramienta de syslog poderosa y versátil que permite la recopilación y el envío de registros de sistema a través de la red. Su capacidad de filtrar y clasificar registros, así como su integración con otros sistemas de monitoreo y gestión de registros, la convierten en una herramienta muy útil para la monitorización y el análisis de registros de sistema en entornos de red complejos.

2.- Instalación del paquete Rsyslog en el Servidor

Para instalar Rsyslog en Ubuntu 22.04 server, por defecto ya viene instalado.

- `sudo apt install Rsyslog -y`

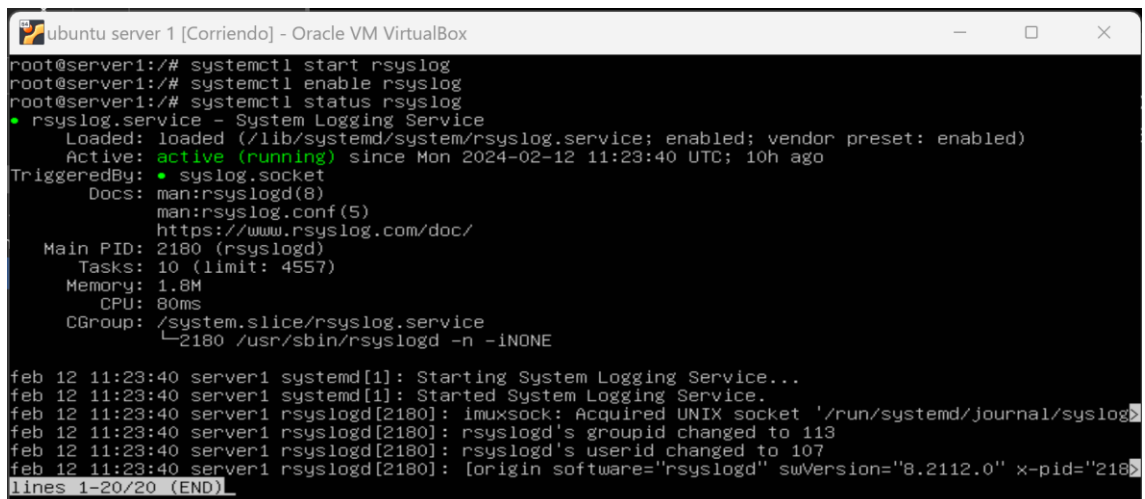


```
ubuntu server 1 [Corriendo] - Oracle VM VirtualBox
root@server1:~# sudo apt install rsyslog -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
rsyslog ya está en su versión más reciente (8.2112.0-2ubuntu2.2).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 51 no actualizados.
root@server1:~# _
```

Una vez instalada la aplicación, iniciaremos el servicio Rsyslog y lo habilitaremos para comenzar a reiniciar el sistema. Para ello, abriremos la terminal y ejecutaremos los siguientes comandos:

- `sudo systemctl start rsyslog` - Este comando inicia el servicio Rsyslog.
- `sudo systemctl enable rsyslog` - Este comando habilita el servicio Rsyslog para que se inicie automáticamente cada vez que se reinicie el sistema.
- `sudo systemctl status Rsyslog` - Este comando es para verificar el estado del servicio Rsyslog en el sistema y para diagnosticar posibles problemas con el servicio.

Una vez habilitado el servicio, el sistema estará listo para reiniciar y comenzar a recopilar los registros de sistema en el archivo de registro designado.



```
ubuntu server 1 [Corriendo] - Oracle VM VirtualBox
root@server1:~# systemctl start rsyslog
root@server1:~# systemctl enable rsyslog
root@server1:~# systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2024-02-12 11:23:40 UTC; 10h ago
     TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
    Main PID: 2180 (rsyslogd)
      Tasks: 10 (limit: 4557)
     Memory: 1.8M
        CPU: 80ms
    CGroup: /system.slice/rsyslog.service
            └─2180 /usr/sbin/rsyslogd -n -iNONE

feb 12 11:23:40 server1 systemd[1]: Starting System Logging Service...
feb 12 11:23:40 server1 systemd[1]: Started System Logging Service.
feb 12 11:23:40 server1 rsyslogd[2180]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog'
feb 12 11:23:40 server1 rsyslogd[2180]: rsyslogd's groupid changed to 113
feb 12 11:23:40 server1 rsyslogd[2180]: rsyslogd's userid changed to 107
feb 12 11:23:40 server1 rsyslogd[2180]: [origin software="rsyslogd" swVersion="8.2112.0" x-pid="2180"]
lines 1-20/20 (END)
```

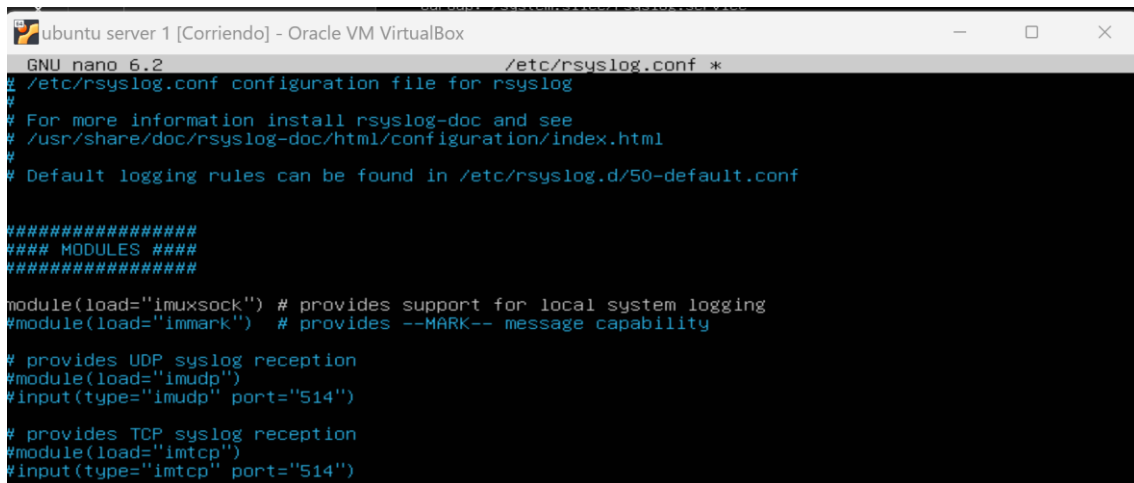
3.- Configuración del servidor Rsyslog

Tenemos que configurar el servidor Rsyslog para que corra en modo servidor. Tenemos que editar el archivo:

```
sudo nano /etc/rsyslog.conf
```

Tenemos que quitar el comentario de las líneas siguientes:

```
#module(load="imudp")
#input(type="imudp" port="514")
#module(load="imtcp")
#input(type="imtcp" port="514")
```



The screenshot shows a terminal window titled 'ubuntu server 1 [Corriendo] - Oracle VM VirtualBox'. Inside, the nano text editor is open editing '/etc/rsyslog.conf'. The visible content includes the top of the file with comments about configuration and logging rules, followed by a section of modules. The lines to be uncommented are: `#module(load="imudp")`, `#input(type="imudp" port="514")`, `#module(load="imtcp")`, and `#input(type="imtcp" port="514")`. The terminal background is black with green and white text.

Y a continuación tenemos que añadir la siguiente línea:

```
$template      RemInputLogs,      "/var/log/remotelogs/%FROMHOST-IP%/%PROGRAMNAME%.log"
*.? ?RemInputLogs
```

```
ubuntu server 1 [Corriendo] - Oracle VM VirtualBox
GNU nano 6.2 /etc/rsyslog.conf *
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf

#####
#### MODULES ####
#####

module(load="imuxsock") # provides support for local system logging
#module(load="imark") # 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")

$template RemInputLogs, "/var/log/REMOTELOGS/%FROMHOST-IP%/%PROGRAMNAME%.log"
*. * ?RemInputLogs
```

El archivo al final quedaría de esta manera y al final verificamos si esta activado bien el Rsyslog.

```
# systemctl restart rsyslog
# systemctl status Rsyslog
```

```
ubuntu server 1 [Corriendo] - Oracle VM VirtualBox
root@server1:/# systemctl restart rsyslog
root@server1:/# systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2024-02-12 21:52:47 UTC; 4s ago
     TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
    Main PID: 2489 (rsyslogd)
      Tasks: 10 (limit: 4557)
     Memory: 1.5M
        CPU: 11ms
    CGroup: /system.slice/rsyslog.service
            └─2489 /usr/sbin/rsyslogd -n -iNONE

feb 12 21:52:47 server1 systemd[1]: Starting System Logging Service...
feb 12 21:52:47 server1 rsyslogd[2489]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog'
feb 12 21:52:47 server1 rsyslogd[2489]: rsyslogd's groupid changed to 113
feb 12 21:52:47 server1 systemd[1]: Started System Logging Service.
feb 12 21:52:47 server1 rsyslogd[2489]: rsyslogd's userid changed to 107
feb 12 21:52:47 server1 rsyslogd[2489]: [origin software="rsyslogd" swVersion="8.2112.0" x-pid="2489"]
lines 1-20/20 (END)
```

Con el siguiente comando podemos verificar si esta los puerto escuchando con este comando:

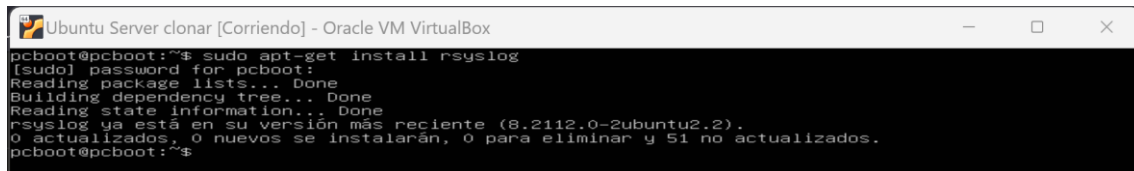
```
# ss -antpl | grep 514
```

```
ubuntu server 1 [Corriendo] - Oracle VM VirtualBox
root@server1:/# ss -antpl | grep 514
LISTEN 0      25          0.0.0.0:*    users:((("rsyslogd",pid=2489,fd=7))
LISTEN 0      25          [::]:*     users:((("rsyslogd",pid=2489,fd=8))
root@server1:/#
```

4.- Instalar y configurar el cliente Rsyslog

Instalar el programa Rsyslog en el cliente con el comando siguiente:

```
sudo apt-get install rsyslog
```

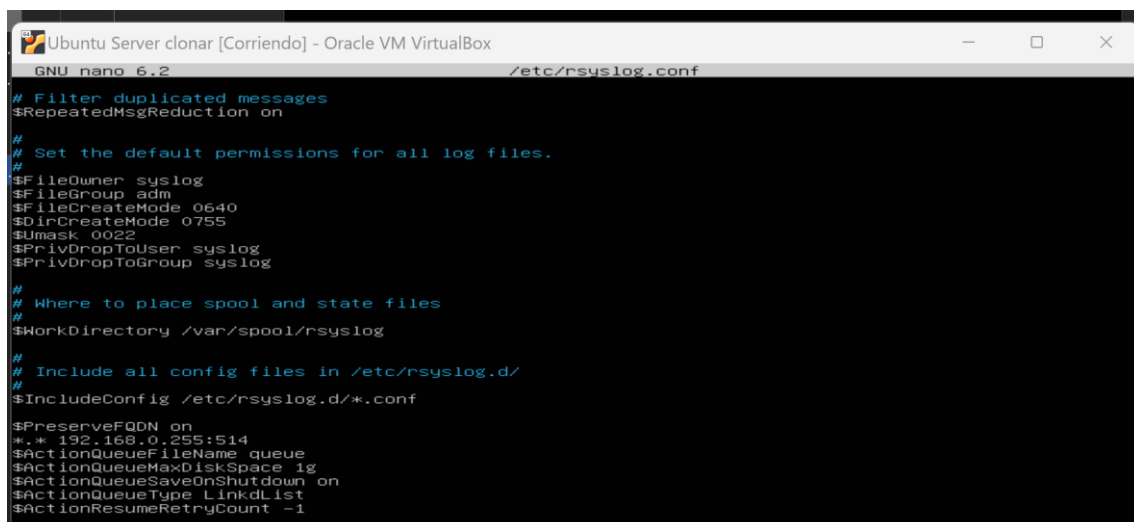


```
pcboot@pcboot:~$ sudo apt-get install rsyslog
[sudo] password for pcboot:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
rsyslog ya está en su versión más reciente (8.2112.0-2ubuntu2.2).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 51 no actualizados.
pcboot@pcboot:~$
```

Ahora lo que tenemos que hacer es editar el fichero Rsyslog.conf con el comando siguiente y añadimos al final del fichero las siguientes líneas:

```
sudo nano /etc/Rsyslog.conf
```

```
$PreserveFQDN on
*. * @@rsyslog-server-ip:514
$ActionQueueFileName queue
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
```



```
GNU nano 6.2 /etc/rsyslog.conf
# Filter duplicated messages
$RepeatedMsgReduction on
#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog
#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog
#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
#
$PreserveFQDN on
*. * 192.168.0.255:514
$ActionQueueFileName queue
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
```


Verificamos log con el comando siguiente:

`ls -l /var/log/`

```

Ubuntu Server clonar [Corriendo] - Oracle VM VirtualBox
$ActionQueueFileName queue
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkdList
$ActionResumeRetryCount -1

pcboot@pcboot:~$ ls -l /var/log/
total 2872
-rw-r--r-- 1 root root 34877 feb 8 20:36 alternatives.log
drwxr-xr-x 2 root root 4096 feb 8 20:36 apt
-rw-r--r-- 1 syslog adm 13478 feb 12 22:18 auth.log
-rw-r--r-- 1 root root 64549 ago 10 2023 bootstrap.log
-rw-rw-r-- 1 root utmp 1920 feb 12 21:34 btmp
-rw-r--r-- 1 syslog adm 377122 feb 12 21:34 cloud-init.log
-rw-r--r-- 1 root adm 18720 feb 12 21:34 cloud-init-output.log
drwxr-xr-x 2 root root 4096 ago 2 2023 dist-upgrade
-rw-r--r-- 1 root adm 48752 feb 12 21:34 dmesg
-rw-r--r-- 1 root adm 46822 feb 12 11:05 dmesg.0
-rw-r--r-- 1 root adm 14644 feb 8 21:14 dmesg.1.gz
-rw-r--r-- 1 root adm 14806 feb 8 20:53 dmesg.2.gz
-rw-r--r-- 1 root adm 14706 feb 8 20:44 dmesg.3.gz
-rw-r--r-- 1 root adm 15031 feb 8 20:35 dmesg.4.gz
-rw-r--r-- 1 root root 604380 feb 8 20:36 dpkg.log
-rw-r--r-- 1 root root 32032 feb 8 20:35 faillog
drwxr-xr-x 4 root adm 4096 feb 8 20:36 installer
drwxr-sr-x+ 3 root systemd-journal 4096 feb 8 20:35 journal
-rw-r--r-- 1 syslog adm 342401 feb 12 21:34 kern.log
drwxr-xr-x 2 landscape landscape 4096 feb 8 20:38 landscape
-rw-rw-r-- 1 root utmp 292292 feb 12 21:34 lastlog
drwx----- 2 root root 4096 ago 10 2023 private
-rw-r--r-- 1 syslog adm 1216708 feb 12 22:18 syslog
-rw-r--r-- 1 root root 2896 feb 12 11:43 ubuntu-advantage.log
drwxr-xr-x 2 root adm 4096 feb 8 20:35 unattended-upgrades
-rw-rw-r-- 1 root utmp 12672 feb 12 21:34 wtmp
pcboot@pcboot:~$

```

Ahora ejecutamos el comando `systemctl restart rsyslog`.

```

Ubuntu Server clonar [Corriendo] - Oracle VM VirtualBox
pcboot@pcboot:~$ systemctl restart rsyslog
==== AUTHENTICATING FOR org.freedesktop.systemd1.ManageUnits ====
Authentication is required to restart 'rsyslog.service'.
Authenticating as: pcboot
Password:
==== AUTHENTICATION COMPLETE ====
pcboot@pcboot:~$

```

5.- Verificamos los registros.

Ahora vamos al servidor Rsyslog y verificamos los registros recibidos desde el cliente con el siguiente comando:

`ls /var/log/remotelogs/127.0.0.1`

```

ubuntu server 1 [Corriendo] - Oracle VM VirtualBox
root@server1:~# ls /var/log/remotelogs/127.0.0.1
alternatives.log  apt  dmesg  installer  lastlog  syslog
auth.log          cloud-init.log  dmesg.0  journal  private  ubuntu-advantage.log
bootstrap.log     cloud-init-output.log  dpkg.log  kern.log  remotelogs  unattended-upgrades
pcboot@server1:~$ dist-upgrade  faillog  landscape  REMOTELOGS  wtmp
root@server1:~#

```

Índice Alfabético

A		Interfaz..... 3
Admisión..... 3		
análisis..... 3		
C		L
Capacidad..... 3		líneas..... 6, 8
características..... 3		LinkedList..... 8
código..... 3		Logging..... 3
comandos..... 5		
comentario..... 6		M
Compatibilidad..... 3		Manual..... 1, 3
complejos..... 3		módulos..... 3
comunicación..... 3		monitoreo..... 3, 4
comunidad..... 3		monitorización..... 3
configuración..... 3		
corra..... 6		N
creación..... 3		Nagios..... 3
criterios..... 3, 4		
D		P
descripción..... 2, 3		paquete..... 2, 5
detección..... 3		patrones..... 4
E		Permite..... 3
eficiencia..... 4		poderosa..... 4
empresa..... 3		Posibilidad..... 3
entornos..... 3		problemas..... 4, 5
envío..... 3, 4		programa..... 2, 3, 8
extensión..... 3		protocolos..... 3
F		
formatos..... 3		R
G		recopilación..... 3
GmbH..... 3		red..... 3
gráfica..... 3		registros..... 2, 3, 5, 9
H		RemInputLogs..... 6
herramienta..... 3		Remote..... 3
hora..... 3		rendimiento..... 4
I		resolución..... 4
identificación..... 4		RSYSLOG..... 1, 3
Instalación..... 2, 5		
Integración..... 3		S
		seguridad..... 4
		servicio..... 5
		sistema..... 3, 5
		sistemas..... 3
		software..... 3
		SSL/TLS..... 3
		status..... 5, 7
		System..... 3

T	usuario	3
TCP		3
tendencias.....		4
U		
Ubuntu		5
	V	
	Verificamos	2, 9