

Manual de instalación de rsyslog en Rocky Linux 9.4

Máximo Castro, Federico González, Santiago Hornos, Wenten Viere

Escuela Superior de Informática

Sistemas Operativos III

Profesor Walter Domínguez

20 de septiembre de 2024



Informática

CGHV INFORMÁTICA S.R.L.

Av. Gral Rivera 3729 bis, 11600 Montevideo, Departamento de Montevideo



ESI
Escuela Superior de Informática

Índice

Propósito	3
Servicio de centralización de logs utilizando Rsyslog	4
Referencias y anexos	6

Propósito

Este documento está destinado al profesor de Sistemas Operativos III, Walter Domínguez, de la Escuela Superior de Informática y explicará los pasos para instalar Nagios en una máquina virtual con Rocky Linux 9.4. Encontrará en los anexos la instalación previa de Rocky Linux 9.4, MySQL, Ansible y Nagios.

Servicio de centralización de logs utilizando Rsyslog

Utilizaremos los rsyslog para poder centralizar donde recibimos los logs para facilitar la administración, en nuestro caso utilizaremos la máquina virtual de rocky y un WSL con Ubuntu.

Primero debemos descargar e iniciar rsyslog con los siguientes comandos.

```
[root@localhost ~]# sudo dnf install -y rsyslog
Última comprobación de caducidad de metadatos hecha hace 0:40:49, el sáb 27 jul 2024 16:19:02.
El paquete rsyslog-8.2310.0-4.el9.x86_64 ya está instalado.
Dependencias resueltas.
Nada por hacer.
¡Listo!
[root@localhost ~]# sudo systemctl enable rsyslog
[root@localhost ~]# sudo systemctl start rsyslog
[root@localhost ~]# sudo systemctl status rsyslog
```

```
sudo dnf install -y rsyslog
```

```
sudo systemctl enable rsyslog
```

```
sudo systemctl start rsyslog
```

```
sudo systemctl status rsyslog
```

Luego debemos cambiar la configuración de rsyslog.

```
root@localhost ~]# sudo nano /etc/rsyslog.conf
```

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

Agregaremos estas 2 líneas con la ip de el ip al que enviaremos los logs.

```
#queue.saveonshutdown="on"      # save messages to disk on shutdown
#queue.type="LinkedList"        # run asynchronously
#action.resumeRetryCount="-1"   # infinite retries if host is down
# # Remote Logging (we use TCP for reliable delivery)
# # remote_host is: name/ip, e.g. 192.168.0.1, port optional e.g. 10514
#Target="remote_host" Port="XXX" Protocol="tcp")
*. * @172.17.62.187:514 # Para UDP
*. * @@172.17.62.187:514 # Para TCP
```

Ahora debemos instalar en nuestra otra máquina rsyslog y también acceder a las configuraciones de la misma manera.

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

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

# provides kernel logging support and enable non-kernel klog messag
```

Deberemos quitar los # en module e input para establecer esta máquina como la que recibirá los logs.

Ahora en la máquina que enviará los logs utilizaremos este comando para comprobar si está funcionando bien lo que configuramos.

```
[root@localhost ~]# logger "Mensaje para probar el funcionamiento desde el Rocky"
[root@localhost ~]#
```

Y finalmente utilizaremos el siguiente comando para ver si llegó el log.

```
maximo@DESKTOP-OG1FK9Q:~$ sudo tail -f /var/log/syslog
Jul 27 17:14:05 DESKTOP-OG1FK9Q systemd[1]: Stopping OpenBSD Secure Shell server...
Jul 27 17:14:05 DESKTOP-OG1FK9Q systemd[1]: ssh.service: Deactivated successfully.
Jul 27 17:14:05 DESKTOP-OG1FK9Q systemd[1]: Stopped OpenBSD Secure Shell server.
Jul 27 17:14:05 DESKTOP-OG1FK9Q systemd[1]: Starting OpenBSD Secure Shell server...
Jul 27 17:14:05 DESKTOP-OG1FK9Q systemd[1]: Started OpenBSD Secure Shell server.
Jul 27 17:14:05 DESKTOP-OG1FK9Q systemd[1]: Reloading.
Jul 27 17:14:05 DESKTOP-OG1FK9Q systemd[1]: Configuration file /run/systemd/system/netplan-ovs-cleanup.service
world-inaccessible. This has no effect as configuration data is accessible via APIs without restrictions. Pro
yway.
Jul 27 17:14:13 DESKTOP-OG1FK9Q systemd[1]: apt-daily-upgrade.service: Deactivated successfully.
Jul 27 17:14:13 DESKTOP-OG1FK9Q systemd[1]: Finished Daily apt upgrade and clean activities.
Jul 27 17:14:46 DESKTOP-OG1FK9Q kernel: [ 1020.322668] mini_init (176): drop_caches: 1
Jul 27 17:15:19 localhost root[128423]: Mensaje para probar el funcionamiento desde el Rocky
```

Referencias y anexos

Link a Github:

<https://github.com/CGHV-UTU/Proyecto2024>

Manual de instalación de Rocky Linux 9.4

 ANEXO: Manual de instalación de Rocky Linux 9.4

Manual de instalación de MySQL en Rocky Linux 9.4

 ANEXO: Manual de instalación de MySQL en Rocky Linux 9.4

Manual de instalación de Ansible en Rocky Linux 9.4

 ANEXO: Manual de instalación de Ansible en Rocky Linux 9.4

Manual de instalación de Nagios en Rocky Linux 9.4

 ANEXO: Manual de instalación de Nagios en Rocky Linux 9.4