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

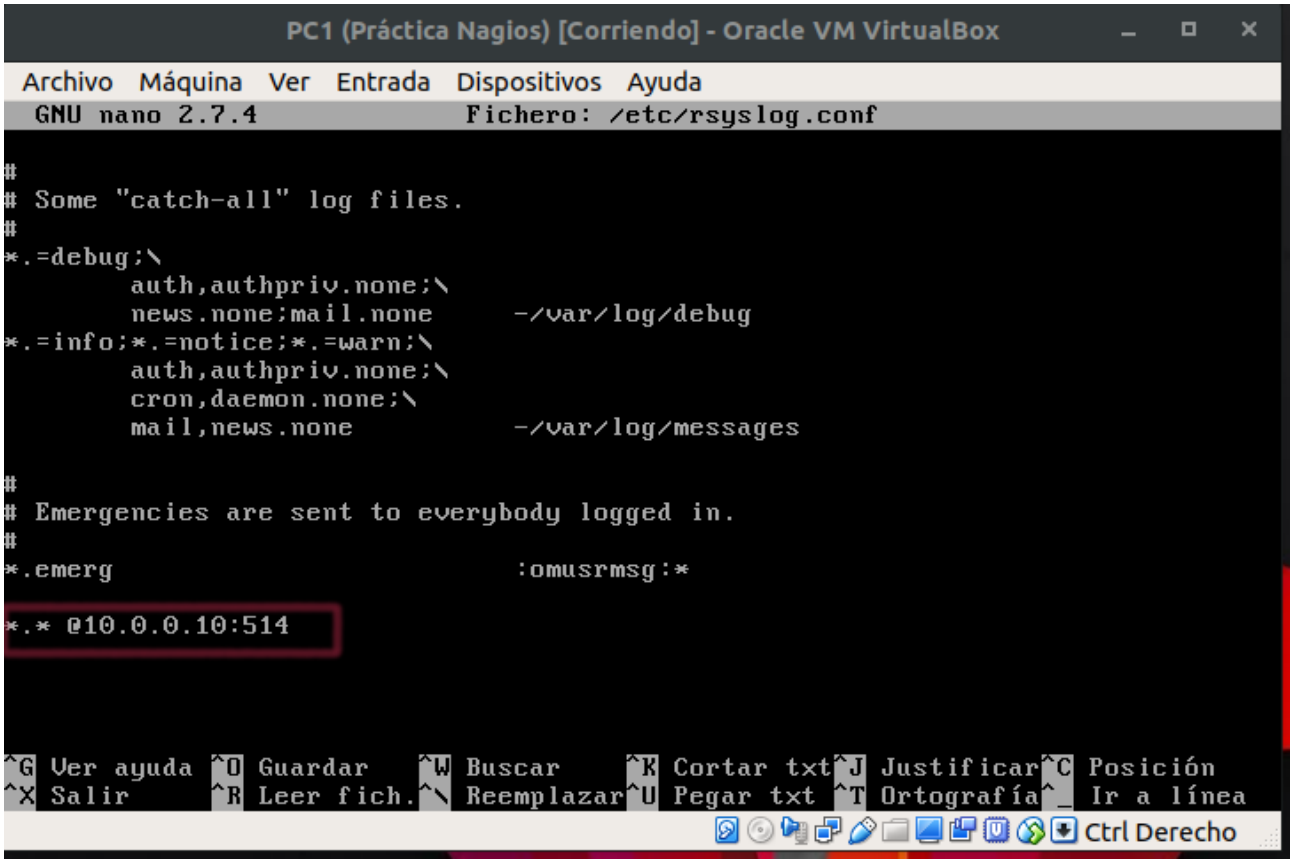
FECHA: 31/05/19

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?

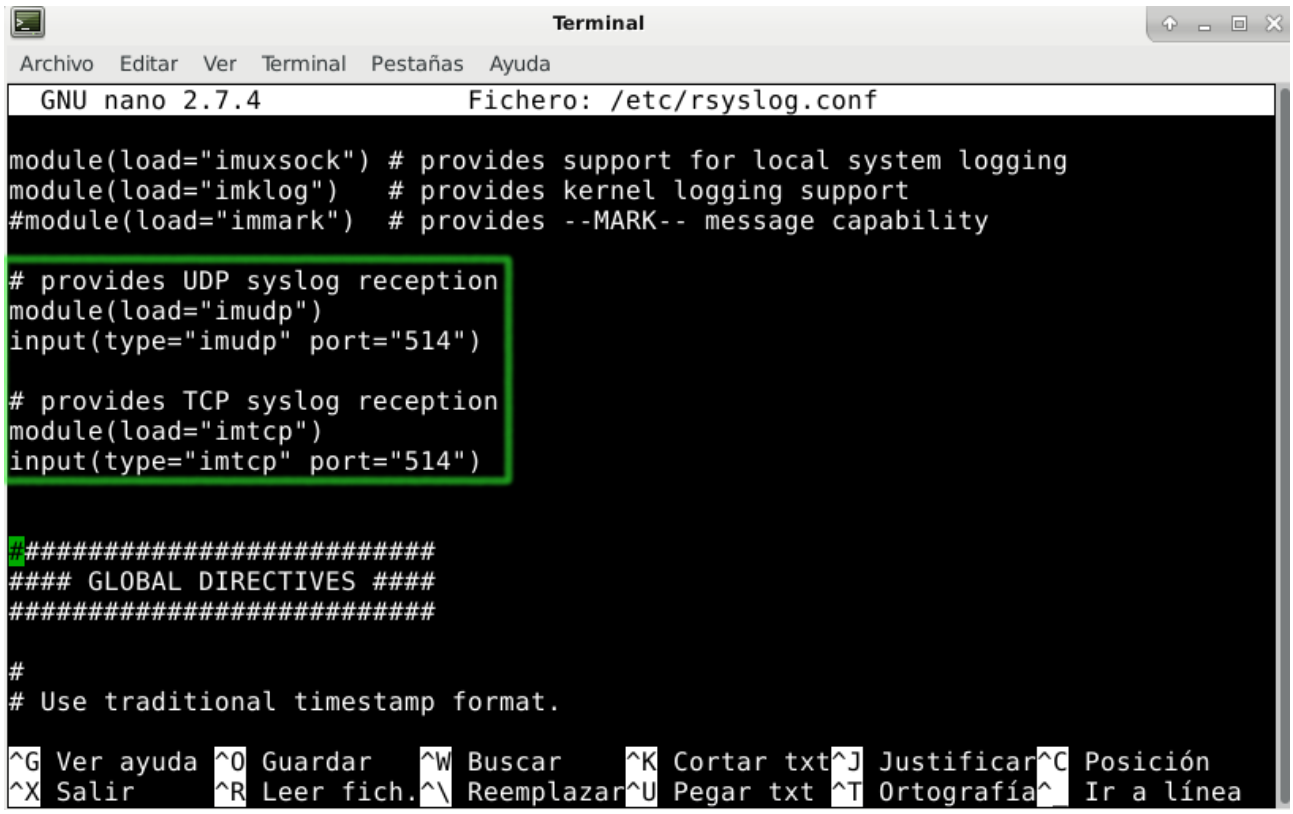
R= En el fichero de configuración del cliente solo es necesario añadir solamente una línea:



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

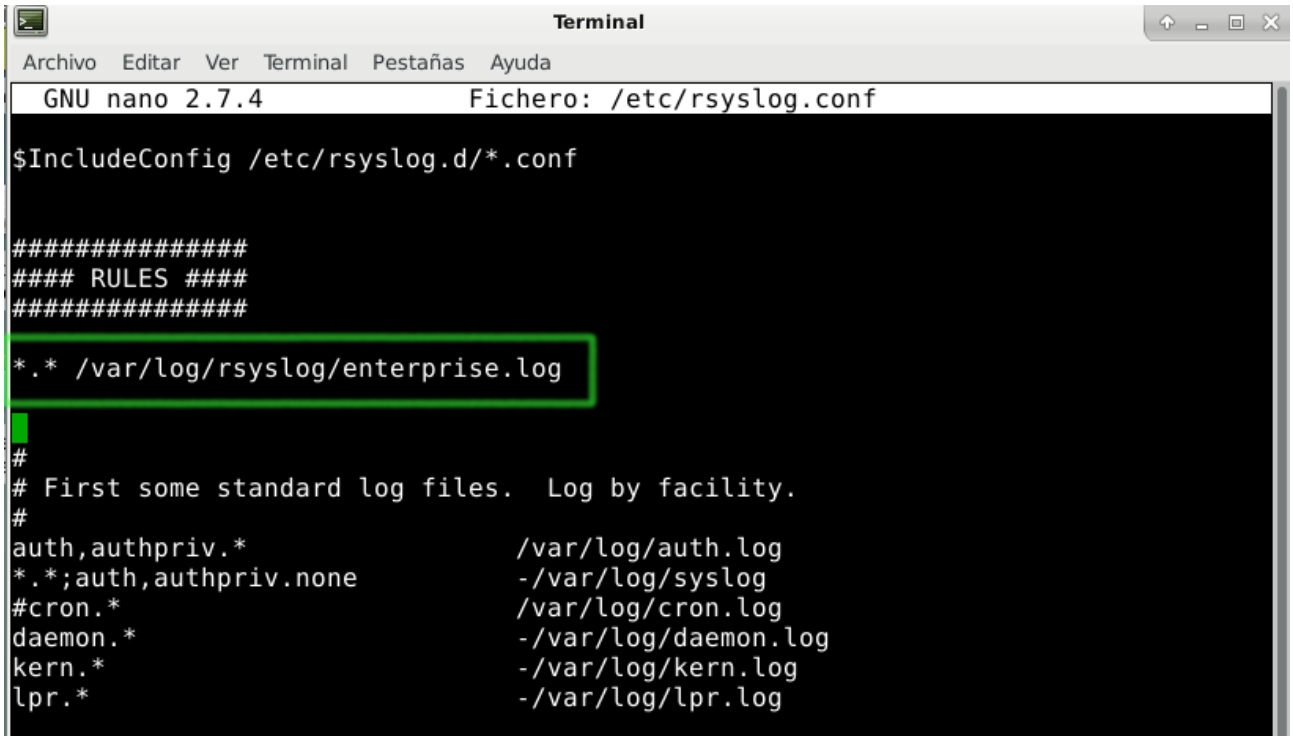
¿Qué cambios ha realizado en la configuración del servidor? ¿Cómo ha verificado su funcionamiento correcto?

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



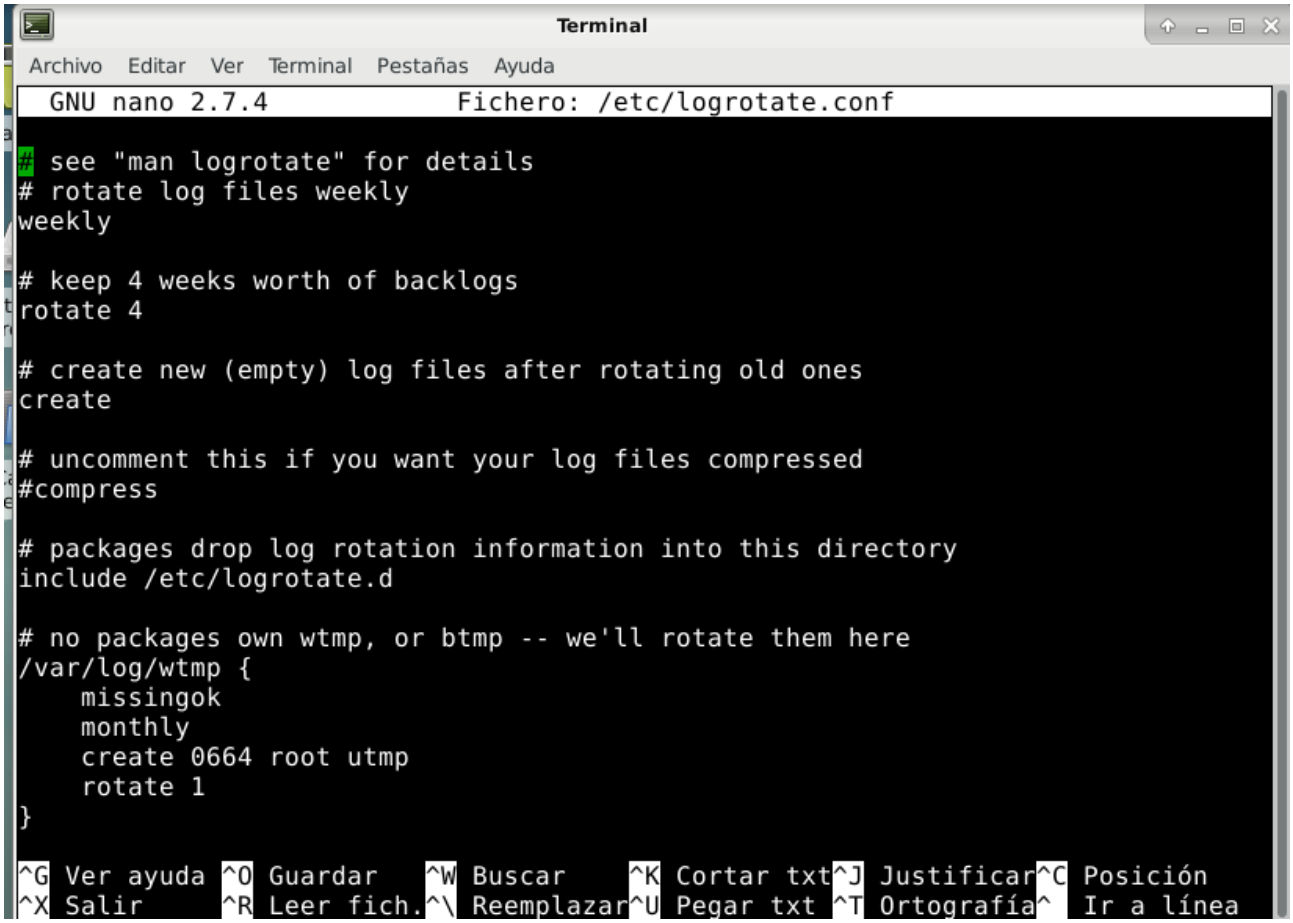
Esto lo que nos permite es poner a nuestro servidor a escuchar en el puerto 514 tanto para TCP como UDP.

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



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?



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.