

Sistema Syslog

- 1)¿Para qué sirve guardar logs?
- 2)¿Qué tipo de servicios que manejan logs conocen?
- 3)¿se puede centralizar los logs?¿Como?

Archivos Syslog

- 1)¿Dónde está el archivo de configuración?
- 2)¿Cómo reinicio el sistema de logs?
- 3)¿Dónde están los archivos de logs?
- 4)Enunciar los archivos de logs esenciales del sistema y su uso.

Configurando syslog.conf

- 1)¿Qué es un facility? Enumerar y explicar cada uno
- 2)¿Que es un priority? Enumerar y explicar cada uno
- 3)¿Cómo genero una regla en el archivo de configuración para que todos los tipos de errores se redireccionen a /dev/tty2?
- 4)Generar una regla para que todos los priorities del facility de users se redireccionen a /var/log/mio.log , salvo los del tipo debug
- 5)Generar una regla para que todos los facilities salvo el de user y mail envíen todos los priorities superiores a warn al archivo /var/log/mio2.log
- 6)Reiniciar el servicio para que tenga efecto.
- 7)Forzar a escribir un error en algún facility.priority con el comando adecuado.

Detectando Errores

- 1)¿Con qué comando se puede ver los últimos usuarios conectados?
- 2)Encontrar todos los errores de logueo.

Rotacion de logs

- 1)¿En qué directorio se encuentran los archivos de rotación?
- 2)Con qué comando puedo forzar la rotación de logs.
- 3)Crear un archivo de rotación, para que rote en 4 generaciones y se comprima.