108.2 Logs del sistema - Ejercicios

Nota: Estos ejercicios implican visualizar y manipular archivos de log. Algunos directorios de log requieren privilegios de superusuario (`sudo`). Realízalos en un entorno de prueba (VM).

Ejercicio 8.2.1: Explorando el Directorio de Logs Tradicional (`/var/log`)

- **Objetivo:** Identificar los archivos de log comunes en `/var/log/`.
- **Requisitos:** Acceso a la línea de comandos.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Lista el contenido de `/var/log/`:** Ejecuta `ls -l /var/log/`. Observa los diferentes archivos y directorios. Identifica los archivos principales (ej: `syslog`, `messages`, `auth.log`, `secure`, `kern.log`).
    3. **Identifica los archivos rotados:** Verás archivos con extensiones numéricas (`.1`, `.2.gz`) o de fecha, que son versiones antiguas gestionadas por `logrotate`.
    4. **Visualiza el contenido de un archivo de log (ej: syslog o messages):** Ejecuta `sudo less /var/log/syslog` (Debian) o `sudo less /var/log/messages` (Red Hat). Desplázate y observa el formato de las líneas (marca de tiempo, nombre del host, nombre del servicio/proceso, mensaje). Presiona `q` para salir.
    5. **Visualiza un archivo de log de autenticación/seguridad:** Ejecuta `sudo less /var/log/auth.log` (Debian) o `sudo less /var/log/secure` (Red Hat). Busca intentos de conexión SSH, acciones con sudo, etc.
    6. **Visualiza el buffer de mensajes del kernel:** Ejecuta `dmesg`. Esto muestra mensajes del kernel capturados durante el arranque y la ejecución. La mayoría de estos mensajes también se registran en `/var/log/kern.log` o en el journald.

Ejercicio 8.2.2: Leyendo Logs en Tiempo Real (`tail -f`)

- **Objetivo:** Monitorizar archivos de log a medida que se escriben nuevos mensajes.
- **Requisitos:** Privilegios de superusuario (`sudo`) para algunos logs.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Monitoriza el log general del sistema:** Ejecuta `sudo tail -f /var/log/syslog` (Debian) o `sudo tail -f /var/log/messages` (Red Hat).
    3. **En otra terminal (o presionando Ctrl+Z y luego `bg` en la primera terminal):** Ejecuta un comando que genere mensajes de log, como intentar iniciar sesión con una contraseña incorrecta (en otra TTY o ventana) o reiniciar un servicio (ej: `sudo systemctl restart sshd`).
    4. **Observa cómo los nuevos mensajes aparecen en la terminal que ejecuta `tail -f`.**
    5. **Detén `tail -f`:** Presiona `Ctrl+C` en la terminal donde se ejecuta `tail -f`.

6. **Monitoriza el log de autenticación:** Ejecuta `sudo tail -f /var/log/auth.log` (Debian) o `sudo tail -f /var/log/secure` (Red Hat). Intenta acceder con `sudo` o `su` en otra terminal y observa los mensajes.

Ejercicio 8.2.3: Usando `journalctl` para Ver y Filtrar Logs (Sistemas con Systemd)

- **Objetivo:** Interactuar con el sistema de registro journald.
- **Requisitos:** Tu distribución debe usar `systemd`.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Muestra todos los logs del journal (paginado):** Ejecuta `journalctl`. Es el equivalente moderno a ver todos los logs tradicionales juntos. Presiona `q` para salir.
    3. **Muestra los logs en tiempo real:** Ejecuta `journalctl -f`. Genera actividad en otra terminal y observa los nuevos mensajes. Presiona `Ctrl+C` para detener.
    4. **Muestra solo los logs del arranque actual:** Ejecuta `journalctl -b`.
    5. **Muestra los logs del arranque anterior:** Ejecuta `journalctl -b -1`.
    6. **Muestra solo los logs del kernel:** Ejecuta `journalctl -k`. Compara con la salida de `dmesg`.
    7. **Muestra logs de un servicio específico (ej: SSH):** Ejecuta `journalctl -u ssh.service`.
    8. **Muestra logs con una prioridad mínima de "error" o superior:** Ejecuta `journalctl -p err`.
    9. **Combina filtros (ej: logs de kernel de la última hora con prioridad info o superior):** Ejecuta `journalctl -k -p info --since "1 hour ago"`.
    10. **Muestra logs de un usuario específico por UID (ej: tu usuario):** Identifica tu UID con `id -u`. Ejecuta `journalctl _UID=<tu_uid>`.

Ejercicio 8.2.4: Añadiendo una Entrada al Log con `logger`

- **Objetivo:** Escribir un mensaje personalizado en el sistema de logs.
- **Requisitos:** Acceso a la línea de comandos.
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Añade un mensaje simple al log:** Ejecuta `logger "Este es un mensaje de prueba desde mi terminal."`.
    3. **Verifica que el mensaje llegó al log (usando `journalctl`):** Ejecuta `journalctl | grep "Este es un mensaje de prueba"`.
    4. **Verifica que el mensaje llegó al log (usando archivos tradicionales):** Ejecuta `sudo cat /var/log/syslog` (Debian) o `sudo cat /var/log/messages` (Red Hat) y busca el mensaje. Si usas `tail -f` en otra terminal mientras ejecutas `logger`, lo verás aparecer.

Ejercicio 8.2.5: Explorando la Configuración de Rotación de Logs (`logrotate`)

- **Objetivo:** Ver cómo está configurada la rotación de logs.
- **Requisitos:** Privilegios de superusuario (`sudo`).
- **Desarrollo Paso a Paso:**
    1. Abre una terminal.
    2. **Visualiza el archivo de configuración principal de logrotate:** Ejecuta `sudo less /etc/logrotate.conf`. Lee los comentarios y las directivas globales (ej: frecuencia predeterminada, número de versiones a mantener).
    3. **Navega al directorio de configuración de servicios específicos:** Ejecuta `ls -l /etc/logrotate.d/`. Verás archivos para Apache, Nginx, gestores de paquetes, servicios del sistema, etc.
    4. **Visualiza el contenido de un archivo de configuración de un servicio (ej: sshd):** Ejecuta `sudo less /etc/logrotate.d/sshd` (o el nombre de otro servicio que tengas instalado). Observa cómo se definen reglas específicas (qué archivo(s) rotar, frecuencia, opciones).