Manual de Uso: Script de Búsqueda de Patrones en Logs

Descripción

Este script en Bash permite buscar patrones específicos dentro del archivo de logs del sistema (/var/log/syslog). Utiliza grep para la búsqueda, awk para formatear la salida y sed para resaltar ciertos elementos con colores.

Uso del Script

1. Configuración y Ejecución

1. Otórgale permisos de ejecución:

   chmod +x log_search.sh

2. Ejecútalo con el siguiente comando:

   ./log_search.sh

3. Se te pedirá ingresar el patrón que deseas buscar dentro del archivo de logs.
4. El script mostrará los resultados en la terminal con el siguiente formato:
   - **La fecha del log aparecerá en color verde.**
   - **El patrón buscado se resaltará en color rojo.**
   - **Los errores serán convertidos a mayúsculas usando sed.**

Explicación Técnica y Función de los Comandos

grep --color=always -i "$PATTERN" "$LOG_FILE"

- grep: Busca patrones dentro de archivos de texto.
- --color=always: Resalta las coincidencias encontradas en color.
- -i: Ignora mayúsculas y minúsculas en la búsqueda.
- "$PATTERN": Es el patrón que el usuario ingresa para buscar.
- "$LOG_FILE": Especifica el archivo de logs donde se realizará la búsqueda.

awk '{print "\033[1;32mFecha: "$1, $2, $3 "\033[0m - Mensaje: " substr($0, index($0,$4))}'

- awk: Procesa y formatea el texto de salida.
- "\033[1;32mFecha: "$1, $2, $3 "\033[0m": Colorea la fecha en verde.
- substr($0, index($0,$4)): Extrae el mensaje del log omitiendo la fecha y otros datos iniciales.

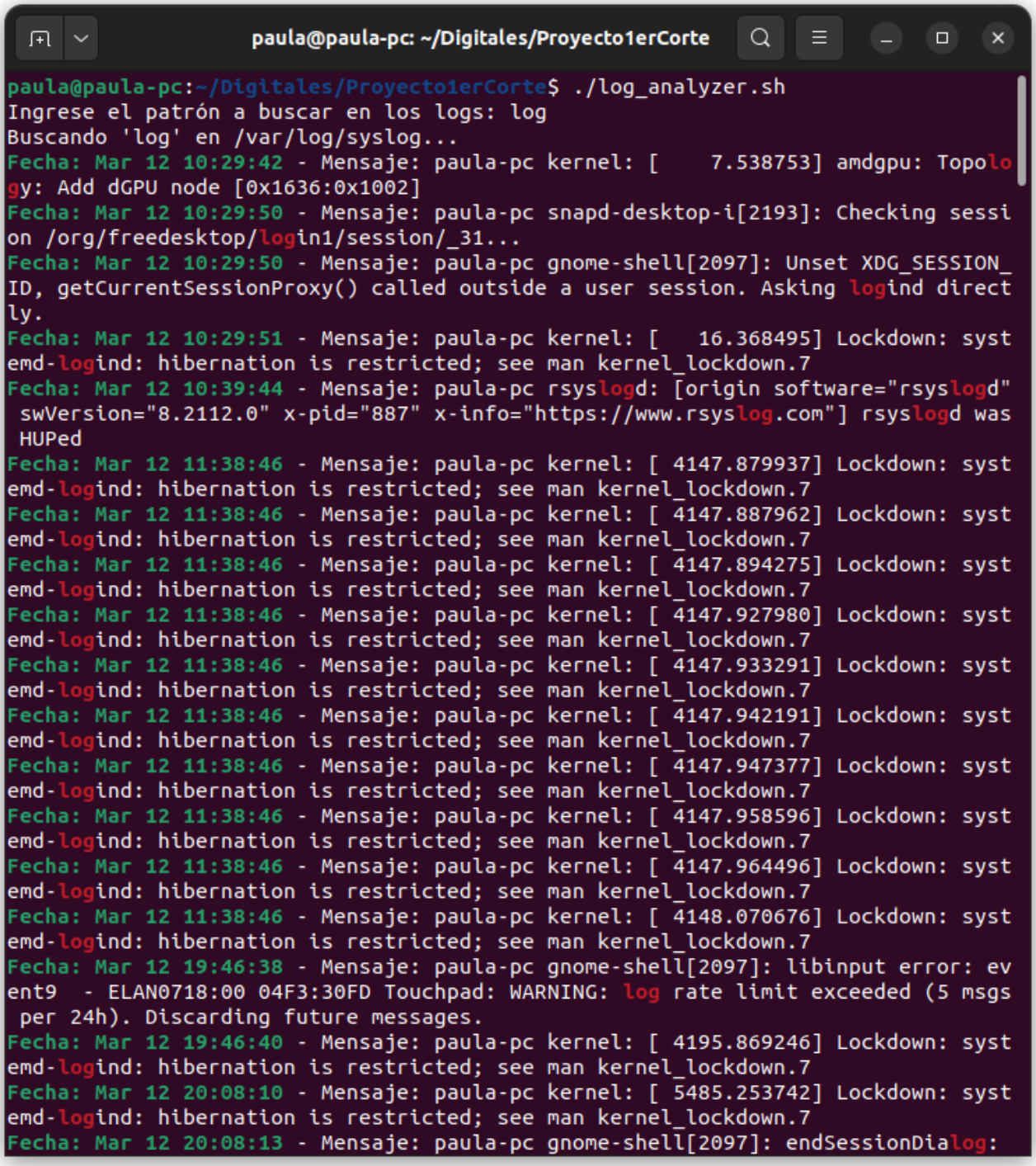
Notas Adicionales

- Se recomienda ejecutar el script como superusuario (sudo) si el archivo de logs tiene restricciones de lectura.
- Si deseas buscar en otro archivo de logs, puedes modificar la variable LOG_FILE en el script.
- Puedes redirigir la salida a un archivo con:

  ./log_search.sh > resultado.log

Script

```
#!/bin/bash

# Pedir al usuario el patrón a buscar
read -p "Ingrese el patrón a buscar en los logs: " PATTERN

# Definir el archivo de logs a analizar
LOG_FILE="/var/log/syslog"

# Verificar si el archivo de log existe
if [[ ! -f "$LOG_FILE" ]]; then
    echo "El archivo de log $LOG_FILE no existe. Saliendo..."
    exit 1
fi

# Buscar el patrón en el log y resaltar con color
echo "Buscando '$PATTERN' en $LOG_FILE..."
grep --color=always -i "$PATTERN" "$LOG_FILE" | awk '{print "\033[1;32mFecha: "$1, $2, $3 "\033[0m -
Mensaje: " substr($0, index($0,$4))}'

# Mensaje final
echo "Búsqueda completada."
```


paula@paula-pc: ~/Digitales/Proyecto1erCorte
paula@paula-pc:~/Digitales/Proyecto1erCorte$ ./log_analyzer.sh
Ingrese el patrón a buscar en los logs: log
Buscando 'log' en /var/log/syslog...
Fecha: Mar 12 10:29:42 - Mensaje: paula-pc kernel: [7.538753] amdgpu: Topology: Add dGPU node [0x1636:0x1002]
Fecha: Mar 12 10:29:50 - Mensaje: paula-pc snapd-desktop-i[2193]: Checking session /org/freedesktop/login1/session/_31...
Fecha: Mar 12 10:29:50 - Mensaje: paula-pc gnome-shell[2097]: Unset XDG_SESSION_ID, getCurrentSessionProxy() called outside a user session. Asking logind directly.
Fecha: Mar 12 10:29:51 - Mensaje: paula-pc kernel: [16.368495] Lockdown: systemd-logind: hibernation is restricted; see man kernel_lockdown.7
Fecha: Mar 12 10:39:44 - Mensaje: paula-pc rsyslogd: [origin software="rsyslogd" swVersion="8.2112.0" x-pid="887" x-info="https://www.rsyslog.com"] rsyslogd was HUPed
Fecha: Mar 12 11:38:46 - Mensaje: paula-pc kernel: [4147.879937] Lockdown: systemd-logind: hibernation is restricted; see man kernel_lockdown.7
Fecha: Mar 12 11:38:46 - Mensaje: paula-pc kernel: [4147.887962] Lockdown: systemd-logind: hibernation is restricted; see man kernel_lockdown.7
Fecha: Mar 12 11:38:46 - Mensaje: paula-pc kernel: [4147.894275] Lockdown: systemd-logind: hibernation is restricted; see man kernel_lockdown.7
Fecha: Mar 12 11:38:46 - Mensaje: paula-pc kernel: [4147.927980] Lockdown: systemd-logind: hibernation is restricted; see man kernel_lockdown.7
Fecha: Mar 12 11:38:46 - Mensaje: paula-pc kernel: [4147.933291] Lockdown: systemd-logind: hibernation is restricted; see man kernel_lockdown.7
Fecha: Mar 12 11:38:46 - Mensaje: paula-pc kernel: [4147.942191] Lockdown: systemd-logind: hibernation is restricted; see man kernel_lockdown.7
Fecha: Mar 12 11:38:46 - Mensaje: paula-pc kernel: [4147.947377] Lockdown: systemd-logind: hibernation is restricted; see man kernel_lockdown.7
Fecha: Mar 12 11:38:46 - Mensaje: paula-pc kernel: [4147.958596] Lockdown: systemd-logind: hibernation is restricted; see man kernel_lockdown.7
Fecha: Mar 12 11:38:46 - Mensaje: paula-pc kernel: [4147.964496] Lockdown: systemd-logind: hibernation is restricted; see man kernel_lockdown.7
Fecha: Mar 12 11:38:46 - Mensaje: paula-pc kernel: [4148.070676] Lockdown: systemd-logind: hibernation is restricted; see man kernel_lockdown.7
Fecha: Mar 12 19:46:38 - Mensaje: paula-pc gnome-shell[2097]: libinput error: event9 - ELAN0718:00 04F3:30FD Touchpad: WARNING: log rate limit exceeded (5 msgs per 24h). Discarding future messages.
Fecha: Mar 12 19:46:40 - Mensaje: paula-pc kernel: [4195.869246] Lockdown: systemd-logind: hibernation is restricted; see man kernel_lockdown.7
Fecha: Mar 12 20:08:10 - Mensaje: paula-pc kernel: [5485.253742] Lockdown: systemd-logind: hibernation is restricted; see man kernel_lockdown.7
Fecha: Mar 12 20:08:13 - Mensaje: paula-pc gnome-shell[2097]: endSessionDialog: