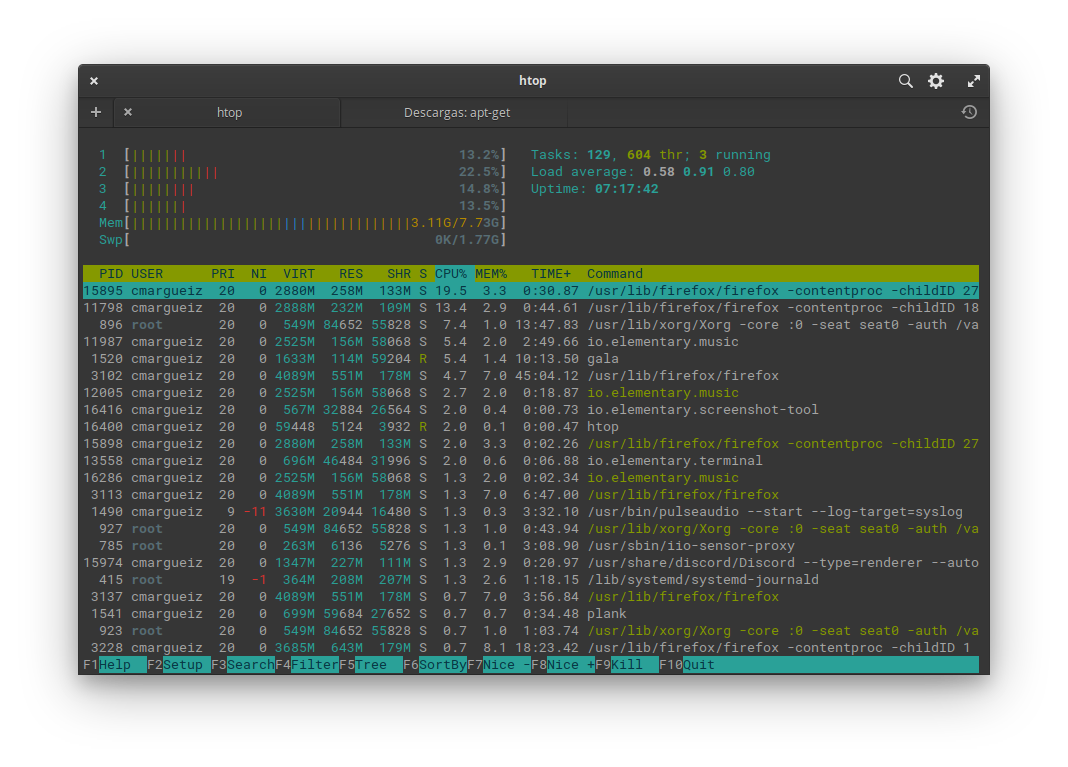
**Est.: Meda Margueiz, Christian Eduardo-MM17017**

Actividad I

Describa el funcionamiento de los siguientes comando y ejemplifique un escenario para su uso

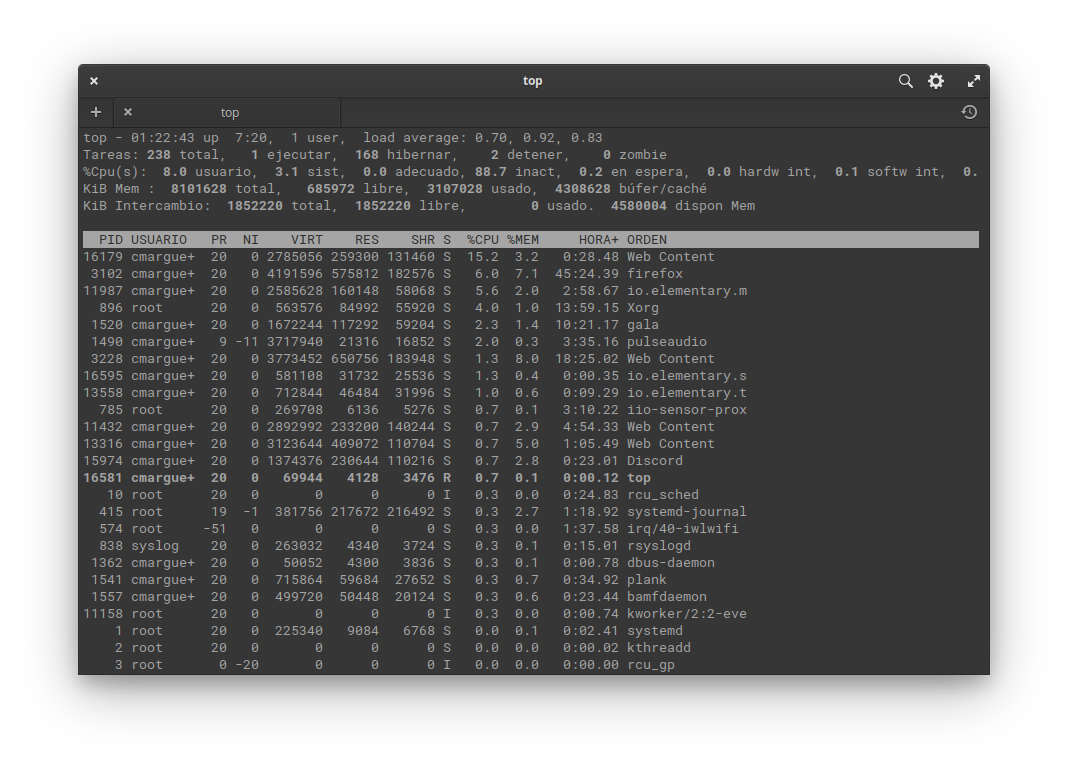
htop: administra interactivamente el sistema

$htop



top: Muestra los procesos de linux

$top



awk: es una herramienta de procesamiento de patrones en líneas de texto

Imprimir último campo de cada línea:

# awk '{ print $NF }' fichero

ps: informa instanatenamente los procesos actuales.

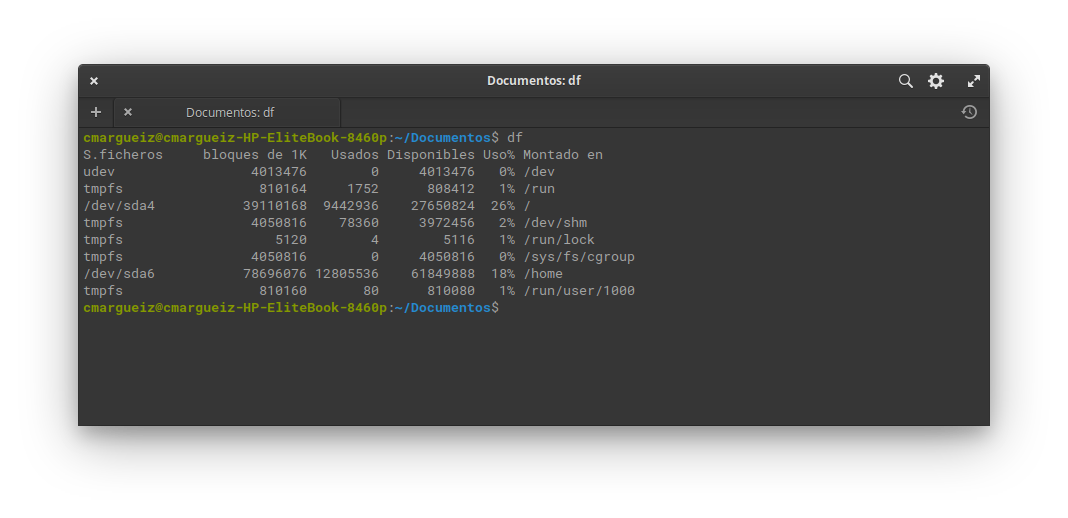
$ps

kill: es un comando que envía una señal de terminación

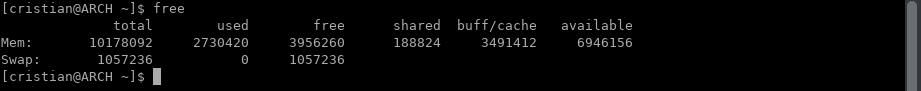
$kill oneko

killall: es que puedes matar cualquier proceso con solo el nombre del comando. Si más de un proceso está ejecutando el comando especificado, matará a todos.

#killall -v apache2

df: es una herramienta CLI del tipo Unix que nos permite conocer la cantidad de espacio libre y espacio utilizado por nuestro sistema de archivos en nuestras unidades de almacenamiento

free: Es un comando que puede en GNU/Linux resultarnos muy útil a la hora de entender el consumo de nuestra memoria



Actividad II

Explique el funcionamineto de los siguientes comandos.

Htop: muestra el eso de la memoria y los procesos que ocurren

top: Muestra los diferentes procesos del sistema linux

top -n 1: Especifica el número máximo de iteraciones, o cuadros, que top debería producir antes de finalizar en este caso es una iteracion.

ps -aux: Lista los procesos de todos los usuarios con información añadida

ps -aux | grep “usuario”: Lista los procesos de todos los usuarios con información añadida según el nombre del usuario.

killall -u “usuario” (si se usa como root, colgaria el sistema): Mata solo los procesos de los derechos del usuario especificado.

foo=”Hola”: Asigna la cadena “Hola” a la variable de entorno $foo

foo=”$foo Mundo”: Concatena la cadena de texto “ Mundo” al contenido de la variable foo

echo $foo: Imprime en consola “Hola mundo”

**Actividad III**

- Describa los tipos de rsyslog security levels con sus codigos, sus rsyslog y su severidad

|  |  |  |
| --- | --- | --- |
| **Codigo** | **rsyslog** | **severidad** |
| 0 | emerg, panic | Emergencia: el sistema no se puede usar |
| 1 | alert | Alerta: se deben tomar medidas de inmediato |
| 2 | crit | Crítico: condiciones críticas |
| 3 | err, error | Error: condiciones de error |
| 4 | warning, warn | Advertencia: condiciones de advertencia |
| 5 | notice | Aviso: condición normal pero significativa |
| 6 | info | Informativo: mensajes informativos |
| 7 | debug | Depuración: mensajes de nivel de depuración |

- Defina el funcionamiento de journalctl

Permite acceder y manipular los datos del registro de los logs del sistema, puedes ver todos los datos o especifcarlos y tambien decidir en que formato lo quieres como Json o otro

- Explique el funcionamiento de los siguientes comandos

**service rsyslog restart:**reinicia el servicio de rsyslog y aplica los cambios hechos en configuración si es que se hizo, pero interrumpiendo todas las conexiones establecidas en ese momento

**systemctl restart rsyslog.service:** reinicia el servicio de rsyslog (hace lo mismo que el comando anterior)

**sudo journalctl:** muestralos registros de los logs del sistema

**journalctl -r:** Nmuetra los registros de los logs del sistema en orden invertido, los primeros debajo, y los últimos encima.

- Describa que hacen las siguientes acciones cuando se están visualizando los logs del

sistema

**down arrow key, enter, e, or j**: muestra el siguiente logs de la lista subiendo en la pantalla uno por uno y desapareciendo el que esta al principio de la panalla

**up arrow key, y, or k:** sube en la lista haciendo que desapareca uno por uno los de abajo y que aparescan los que estaban arriban en la pantalla es decir los que estaban al principio de la lista

**space bar:** hace un salto de pagina en la lista de logs subiendo todos los que se mostraban en pantalla y mostrando uno nuevos que estaban mas abajo en la lista de logs

**b:** hace un salto de pagina en la lista de logs bajando todos los que se mostraban en pantalla y mostrando los que estaban arriba de los que se mostraban en pantalla

**/search term:** Busca hacia adelante desde la posicion actual para la cadena de terminos relacionados a la busqueda

**?search term:** Busca hacia atras desde la posicion actual para la cadena de terminos relacionados a la busqueda

**'<c>:** Regresa a una marca, donde <c> es la etiqueta de carácter individual para la marca

**q:** se sale de vista de los registros de logs

- ¿Qué comando debe de utilizar cuando se ven los journal log del sistema y desea

filtrarlos por un rango de fechas específicas?

sudo journalctl –since «YYYY-MM-DD HH:MM:SS» –until «YYYY-MM-DD HH:MM:SS»

- ¿Qué comando se puede ejecutar si deseo saber mediante los journal logs la lista de los

boots disponibles?

journalctl –list-boots (lista de todos los boot)

journalctl -b (para ver los log boot actuales)

- ¿Con cuál comando se pueden ver los mensajes del kernel?

journalctl -k

- Describa la funcion de los diferentes formatos presentados a continuación mientras se

observan los journal ogs del sistema

**short:** es el valor predeterminado y genera una salida que es casi idéntica al formato de los archivos clásicos de syslog

**verbose:** muestra los elementos de entrada completamente estructurados con todos los campos

**json:** formatea las entradas como estructuras de datos JSON, una por línea

**json-pretty:** formatea las entradas como estructuras de datos JSON, pero las formatea en varias líneas para que sean más legibles para los humanos

**Cat:** genera una salida muy concisa, que solo muestra el mensaje real de cada entrada de diario sin metadatos, ni siquiera una marca de tiempo

(nota para cambiar el formato se utiliza el siguiente comando journalctl -o formato a

usar)