Monitorización de Procesos

Profa. Hazem Álvarez Rodríguez

Marzo/2022

¿Qué es Monitorización?

Es la mediación sistemática y planificada de indicadores de calidad; una actividad que tiene como objetivo identificar la existencia de situaciones problemáticas que hay que evaluar o sobre las que hay que intervenir [1].

- CentOS es una distribución del SO de código abierto Linux, basado en la distribución Red Hat Enterprise Linux, que opera de manera similar, y cuyo objetivo es ofrecer al usuario un software de "clase empresarial" gratuito. Se define como robusto, estable y fácil de instalar y utilizar [2].
  - Ubuntu es una distribución popular entre dispositivos inteligentes o servicios web, compatible con multitud de plataformas de Hardware, tiene un gran número de servicios web y servidores que funcionan con este[3].
- La terminal es una interfaz de gestión que permite, mediante órdenes escritas realizar todo tipo de operaciones, con unas pocas órdenes se pueden realizar operaciones de forma masiva [4].

Imagen recuperada de https://douglasbarahona.com/8-comandos-basicos-y-necesarios-para-monitorear-un-servidor-linux/

Contenido…

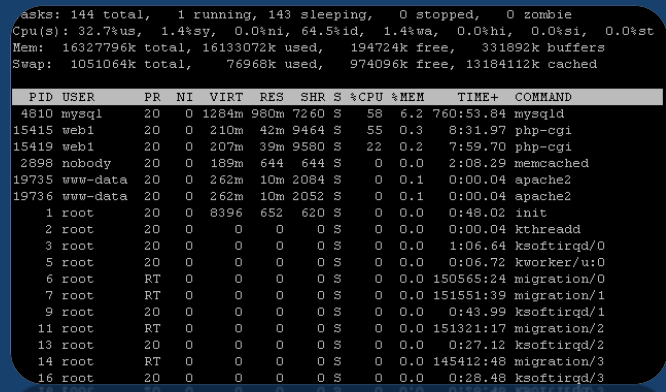
uptime	time	top	ps	vmstat
free	df	du	hdparm	w
mpstat	iostat			

Uptime, time & top…

- **uptime**, muestra la información de la carga del sistema, como la hora del sistema, el tiempo de marcha del sistema, la cantidad de usuarios conectados, y el valor medio de la carga.
- **time**, muestra el tiempo que tarda en ejecutar un comando en modo procesador, usuario y supervisor.
- **top**, parecido a un administrador de tareas, ya que muestra los procesos que se encuentran en ejecución; así como quien los ejecuto. Usado para identificar la memoria utilizada por los procesos, se actualiza con cada intervalo de tiempo y permite ser administrada. (*salir 'q', ayuda 'h'*)

Modificadores

- **top –d [time] o d:** especificar el intervalo de tiempo para refrescar datos
- **1:** muestra la información del procesador desglosada por cada CPU
- **n y Número:** muestra el número(definido) de procesos con más consumo
- **Z:** cambia el color
- **top –b:** vista por lotes.
- **top –u [user]:** filtra los procesos del usuario definido



Recuperado de https://www.servidoresadmin.com/comando-top-linux/ y

ps

- Visualiza las actividades de los procesos, con su identificador del proceso (PID), terminal asociado (TTY), tiempo de uso de CPU (TIME) y nombre del ejecutable (CMD) .

Modificadores

- **ps –e:** permite visualizar todos los procesos.
- **ps –u [user] o -u:** indica los procesos ejecutados por el usuario especificado.
- **ps –o [format]:** enmascara la información y tendrá el formato indicado.
- **-a** Lista los procesos de todos los usuarios
- **-x** Lista procesos de todas las terminales y usuarios
- **-aux** Lista los procesos de todos los usuarios con información añadida (destacamos más abajo).
- **–forest –** Muestra el listado procesos en un formato tipo árbol que permite ver como los procesos interactúan entre si, podría ser algo similar al comando ***pstree.***

```
$ ps aux
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.3   2844  1692 ?        Ss   18:13   0:01 /sbin/init
root           2  0.0  0.0      0     0 ?        S<   18:13   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        S<   18:13   0:00 [migration/0]
root           4  0.0  0.0      0     0 ?        S<   18:13   0:00 [ksoftirqd/0]
root           5  0.0  0.0      0     0 ?        S<   18:13   0:00 [watchdog/0]
root           6  0.0  0.0      0     0 ?        S<   18:13   0:00 [migration/1]
root           7  0.0  0.0      0     0 ?        S<   18:13   0:00 [ksoftirqd/1]
```

```
[CMBSC@localhost ~]$ ps
  PID TTY          TIME CMD
 4860 pts/0    00:00:00 bash
 5148 pts/0    00:00:00 ps
```

Recuperado de https://www.servidoresadmin.com/comando-top-linux/

vmstat

- Esta herramienta brinda un **informe sobre la memoria física y virtual (memory),** del intercambio entre memoria y disco (swap), las transferencias, interrupciones, cambios de contexto y uso del procesador (cpu), proceso conocido como *swapping*.

M o d i f i c a d o r e s

- **vmstat –a:** nos permite visualizar la memoria active e inactive.
- **vmstat –f:** muestra el número de tareas que se han creado desde que se arranca el sistema.
- **vmstat –d:** brinda estadísticas sobre el uso del disco.
- **vmstat *n*:** donde ***n*** intervalo de segundo entre informes,
- **vmstat -s** para mostrar cuántos eventos del sistema se produjeron desde la última vez que se inició el sistema.

```
[CMBSC@localhost ~]$ vmstat
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 2  0  32904 200112      0 303132    1   13   420    56  250  493  7  2 86  5  0
```

Recuperado de https://docs.oracle.com/cd/E38897_01/html/E23086/spmonitor-22.html

free

- Muestra la cantidad de **memoria libre y usada que tiene el sistema**. Por una parte muestra la memoria física y por otra la swap, también muestra la memoria caché y de buffer consumida por el Kernel.

M o d i f i c a d o r e s

- **free –s t:** la ejecución se realizará cada lapso de tiempo especificado.
- **c n, –count=n, r**efresca la información n veces y luego saldrá del programa
- **-t, –total,** muestra un resumen del total de memoria física y swap.
- **l, –lowhigh, m**uestra información detallada acerca de la utilización baja y alta de memoria.

```
$ free
             total       used       free     shared    buffers     cached
Mem:        514796     503800      10996          0       9208     184804
-/+ buffers/cache:     309788     205008
Swap:      1510036      38252    1471784
```

Recuperado de https://n9.cl/qy94

df

- Significa **Disk Filesystem** se usa para revisar el espacio/uso del disco duro. Muestra el almacenamiento/particiones disponibles y utilizados de los sistemas de archivos en el equipo, así como las unidades de disco montadas.

Al ejecutar el comando se muestran las columnas,

- ***Filesystem:*** *te brinda el nombre del sistema de archivos.*
- ***Size:*** *te indica el tamaño total de cada sistema de archivos.*
- ***Used:*** *muestra cuánto espacio está usando cada sistema de archivos.*
- ***Available:*** *muestra cuánto espacio disponible queda en el sistema de archivos.*
- ***Use%:*** *muestra el porcentaje del espacio que está siendo usado.*
- *Mounted On: nos dice el punto de montaje de un sistema de archivos*

```
cautvydas@support-2:~$ df -h
Filesystem            Size  Used Avail Use% Mounted on
udev                  7,8G     0  7,8G   0% /dev
tmpfs                 1,6G   10M  1,6G   1% /run
/dev/nvme0n1p1        219G  5,6G  202G   3% /
tmpfs                 7,8G  580M  7,3G   8% /dev/shm
tmpfs                 5,0M  4,0K  5,0M   1% /run/lock
tmpfs                 7,8G     0  7,8G   0% /sys/fs/cgroup
192.168.168.100:/home 100G   74G   27G  74% /home
tmpfs                 1,6G  4,0K  1,6G   1% /run/user/0
tmpfs                 1,6G  148K  1,6G   1% /run/user/5012
```

M o d i f i c a d o r e s :

- **df –h:** muestra las unidades legibles en el sistema.
- **df -i:** informa sobre la utilización de los nodos en el sistema.
- **df -m:** esta línea de comando se utiliza para mostrar la información del uso del sistema de archivos en MB.
- esta opción mostrará el tipo de sistema de archivos (aparecerá una nueva columna).

- **df –df -T:** ht /home: te permite ver información de un sistema de archivos específico en un formato legible (en este caso el sistema de archivos /home).

du

- Abreviación de **Disk Usage.** muestra los detalles sobre el uso del disco duro de los archivos y directorios en el ordenador o servidor Linux. Además, muestra la ruta de los mismos y requiere especificar qué carpeta o archivo quieres comprobar.

du /home/user/Desktop/

muestra el uso del disco de los archivos y las carpetas que están en el directorio Desktop (los subdirectorios se incluyen también).

M o d i f i c a d o r e s :

- **du -h:** indica los tamaños de los archivos en un formato más entendible (GB, MB, KB).
- **df -i:** informa sobre la utilización de los nodos en el sistema
- **du -h /home/user/Desktop/:** muestra información en un formato legible por humanos.
- **du -sh /home/user/Desktop/:** muestra el tamaño total de una carpeta especifica (en este caso, el directorio Desktop)
- **du -m /home/user/Desktop/:** proporciona los tamaños de carpetas y archivos en Megabytes (podemos usar -k para ver la información en Kilobytes).
- **du –all:** muestra el tamaño ocupado por todos los archivos.

```
[CMBSC@localhost ~]$ du
4       ./.mozilla/extensions/{ec8030f7-c20a-464f-9b0e-13a3a9e97384}
4       ./.mozilla/extensions
0       ./.mozilla/plugins
0       ./.mozilla/firefox/nbwh9qbe.default/gmp
4       ./.mozilla/firefox/nbwh9qbe.default/webapps
16      ./.mozilla/firefox/nbwh9qbe.default/bookmarkbackups
1272    ./.mozilla/firefox/nbwh9qbe.default/sessionstore-backups
4       ./.mozilla/firefox/nbwh9qbe.default/healthreport
4       ./.mozilla/firefox/nbwh9qbe.default/datareporting
1248    ./.mozilla/firefox/nbwh9qbe.default/gmp-gmpopenh264/1.5.3
1248    ./.mozilla/firefox/nbwh9qbe.default/gmp-gmpopenh264
28      ./.mozilla/firefox/nbwh9qbe.default/weave/changes
20      ./.mozilla/firefox/nbwh9qbe.default/weave/logs
52      ./.mozilla/firefox/nbwh9qbe.default/weave
1036    ./.mozilla/firefox/nbwh9qbe.default/extensions
```

Recuperado de https://n9.cl/qy944

Ordenar archivos

- Se reúnen los archivos y carpetas en Desktop en un formato legible usando el comando **du**
- Empleando pipe para enviar el resultado al comando **sort**, junto con la opción **-rn**

```
du -h /home/user/Desktop/ | sort –rn
```

Excluir por tamaño de archivo

- Para ver todos los archivos que superan un determinado tamaño. La manera más efectiva de hacerlo es usando el comando que se muestra a continuación:

```
du -h /home/user/Desktop | grep '^\s*[0-9\.]\+G'
```

- Donde **grep** permite buscar archivos basados en un patrón especificado. En este ejemplo, el script devolverá todos los archivos mayores a 1 GB. Si deseas seleccionar los datos de más de 1 MB, puedes sustituir la **G** por la **M**.

Excluir tipos de archivos

- Para excluir un formato de archivo concreto de los resultados de la búsqueda.

```
du -h /home/user/Desktop/ --exclude="*.txt"
```

El argumento **-exclude=».txt»** hace que el comando du muestre todos los formatos de archivo excepto los documentos **.txt.**

Recuperado de https://n9.cl/7fwpb

hdparm

- Facilita un listado de opciones que permite al usuario modificar los parámetros del disco duro de la computadora, como por ejemplo las dimensiones de las particiones del disco, también nos permite eliminar o crear particiones.
  - ✓ Ajustes relacionados con el disco de visualización** `hdparm /dev/sda`
  - `hdparm -g /dev/sda` ✓ Cilindro de disco duro, la cabeza, número de sector **
  - ✓ Evaluación de la eficiencia de leer el disco duro** `hdparm -t /dev/sda`

Modificadores:

- **hdparm –g:** muestra la geometría del disco según la tripleta (cilindros / cabezales / sectores).
- **hdparm -T:** indica la velocidad de lectura de memoria caché de entrada/salida del SO.
- **hdparm -t:** muestra la velocidad de lectura en sectores secuenciales que el disco es capaz de mantener.

***Ejecute como root*

Recuperado de https://n9.cl/ii2k5

```
root@abueno-laptop:/home/abueno# hdparm -g /dev/sda3

/dev/sda3:
 geometry     = 9729/255/63, sectors = 30298590, start = 108149580
```

w

Muestra información sobre los usuarios que están conectados al equipo, además indica los procesos correspondientes de cada uno, el parámetro JCPU revela el tiempo total de procesador usado por todos los procesos.

- Al ejecutarlo muestra los campos:
  - ***USUARIO/USER –*** *Nombre del usuario.*
  - ***TTY –*** *Tipo de terminal (depende del entorno).*
  - ***DE/FROM –*** *Si es posible imprime el hostname o la ip.*
  - ***LOGIN@ –*** *Tiempo de actividad de la sesión.*
  - ***IDLE –*** *Tiempo desde la última actividad.*
  - ***JCPU –*** *Tiempo de uso de los procesos sujetos al tty.*
  - ***PCPU –*** *Tiempo de uso del proceso actual sujeto al tty.*
  - ***WHAT –*** *Proceso que ejecuta el usuario en este momento (depende de PCPU).*

```
sololinux ~ # w
 18:10:44 up  2:44,  3 users,  load average: 0,86, 0,89, 0,91
USUARIO  TTY      DE               LOGIN@   IDLE   JCPU   PCPU WHAT
sergio   tty7     :0               15:27    2:43m  2:33   0.22s /sbin/upstart -
demo1    tty8     :1               17:39    2:43m  2.67s  0.15s /sbin/upstart -
demo2    tty9     :2               17:40    2:43m  3.28s  0.16s /sbin/upstart -
sololinux ~ # www.sololinux.es
```

Modificadores:

- **w –h:** no muestra el encabezado
- **w usuario**: permite especificar los datos de un usuario en particular.
- **w-s:** la salida es en formato corto. No se imprime el tiempo de inicio de sesión, JCPU ni tampoco el campo PCPU.
- **w –f**: imprimir el hostname o ip del usuario.
- **w –i:** imprimirá la ip del usuario y no el host.

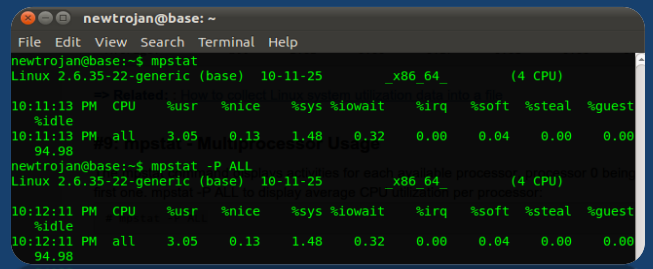
Recuperado de https://www.sololinux.es/como-usar-el-comando-w-con-ejemplos/

mpstat

- Muestra las actividades del o los procesadores (en caso de múltiples núcleos), contando desde cero 0 para el primer núcleo. También proporciona un promedio de las actividades de todos en conjunto. Además, este comando puede ser utilizado en sistemas multiprocesadores o SMP. El parámetro ***interval*** especifica la cantidad de tiempo en segundos entre cada reporte. Un valor de 0 indica que las estadísticas de los procesadores serán reportadas desde que arrancó el sistema.
- El parámetro ***count*** puede ser especificado en conjunto con interval si éste no es 0. El valor de ***count*** determina el número de reportes generados en el intervalo de segundos indicado. Si el parámetro interval se especifica sin count, el comando generará reportes continuamente hasta que lo paremos (***Ctrl+C)*.**
- Ver 5 reportes del primer núcleo a intervalos de 2 segundos `fraterneo@rainbow:~$ mpstat -P 0 2 5`
- Ver 3 reportes de todos los núcleos a intervalos de 3 segundos `fraterneo@rainbow:~$ mpstat -P ALL 3 3`

M o d i f i c a d o r e s :

- **mpstat -P cpu_number:** muestra las actividades de la CPU especificada
- mediante un número.
- **mpstat -P ALL:** indica las actividades de todas las CPU existentes.



Recuperado de https://n9.cl/idqxy

iostat

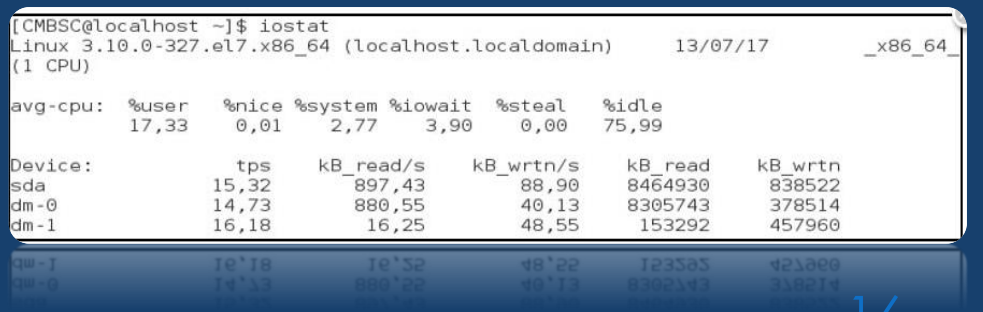
Se usa para monitorear la carga de entrada/salida (**I/O**) del dispositivo del sistema, normalmente el/los discos. La herramienta vigila el tiempo que los dispositivos están activos en relación con sus velocidades promedio de transferencia.

Genera informes muy útiles para detectar sobrecargas y poder equilibrar el I/O de los discos del sistema

- ***Iostat*** esta incluido en ***systat***, el cual es necesario instalar: sudo ***apt-get install sysstat***
- En Rhel, CentOS, Fedora y derivados: ***sudo yum install sysstat***

Modificadores:

- **Iostat -c:** muestra solo información de la CPU.
- **Iostat -d:** muestra solo información de los dispositivos.
- **Iostat -k:** utiliza Kilobytes por segundo para mostrar la información.
- **Iostat -m:** utiliza Megabytes por segundo para mostrar la información.
- **Iostat -p:** muestra detalles sobre las particiones existentes.



Recuperado de https://n9.cl/eo733

Fuentes de información

- [1] P. S. Hernández, «Qué, Cómo y Cuándo Monitorizar: Marco Conceptual y Guía Metodológica,» Murcia, 1997.
- [2] E. P. CentOS, «CentOS,» CentOs Legal, 2017. [En línea]. Available: https://www.centos.org/. [Último acceso: 01 08 2017].
- [3] Ubuntu, la distribución Gnu/Linux preferida por los usuarios para conectarse, recuperado de https://www.linuxadictos.com/ubuntu-la-distribucion-gnu-linux-preferida-por-los-usuarios-para-conectarse.html
- [3] J. G. d. Jalón, I. Aguinaga y A. Mora, Aprenda Linux Como si Estuviera en Primero, San Sebastián: Fcapra, 2000.
- Monitorización de procesos en Linux-UAEH, recuperado de https://n9.cl/a95dz

¿Cómo mostrar el ID del proceso en Linux?

- El comando kill te permite terminar un proceso utilizando un ID de proceso específico, también conocido como pid. Para mostrar un pid en Linux (***ps***)
- Listar todos los procesos disponibles y sus pid, parar listar sea más específica (***ps -ux | grep java***)
- Para mostrar todas las señales del comando Kill (***kill –l***)
- Para finalizar un proceso específico con un PID (***kill PID proceso***) en caso de no funcionar se puede utilizar ***kill [Señal_u_Opción] pid***
- Cancelar múltiples procesos ***kill -9 pid1 pid2 pid3***
- Pkill es una variación del comando kill. Con esta variación puedes especificar el nombre del proceso o un patrón para encontrar un proceso ***pkill chrome o pkill chr***
- Verificar los procesos coincidentes con un nombre parcial ***pgrep -l chr***
- Cancelar un proceso en Linux usando el comando Killall. La diferencia básica entre killall y kill es que killall puede terminar el proceso por nombre mientras el comando kill usa el pid. ***killall Chrome***
- killall se puede personalizar para finalizar procesos basados en marcas de tiempo. Para eliminar un proceso específico que se haya estado ejecutando durante menos de 40 minutos, puedes usar:

killall -y 40m [Nombre_de_proceso>]

Se pueden usar las opciones:

s – segundos, m – minutos, h – horas, d – días, w semanas, M – meses, y – años

Recuperado de https://n9.cl/n4cu9

Htop en Linux

Profa. Hazem Álvarez Rodríguez

Marzo/2021

Breve descripción…

La interfaz de usuario del programa htop está basada en ncurses. La representación de la información es realmente limpia. Con esta herramienta se puede filtrar, administrar y hacer otras cosas interesantes sobre los procesos en ejecución en nuestro sistema. Se trata de una gran herramienta para los administradores de sistemas Gnu/Linux.

Los ataques se aprovechan de las aplicaciones inutilizadas. Por lo que es recomendado deshabilitar demonios (servicios) que no sean utilizados.

Para revisar qué procesos están ejecutándose actualmente en el servidor, se puede utilizar **htop**:

- Para instalar htop, utilice: **apt-get install htop**
- Para ejecutar ejecute: htop

Fuentes

- https://ubunlog.com/htop-controlar-procesos-ubuntu/
- https://docs.bluehosting.cl/tutoriales/servidores/como-instalar-y-utilizar-la-herramienta-htop.html#:~:text=htop%20es%20una%20herramienta%20sumamente,usar%20sus%20identificadores%20(PIDs).

Gracias!!!