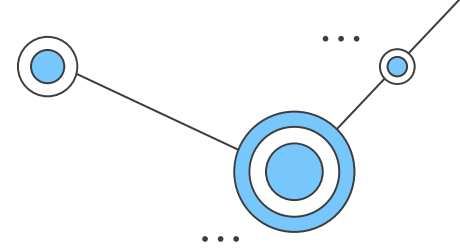


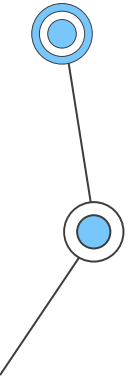


Industrias Oscorp

Sebastián Fernández Hernández
Jezrael Rachid Hernández Jiménez
Fabian Alberto Sandi Corrales
Daniel Fabricio Villalobos Huertas



¿EN QUE CONSISTE?

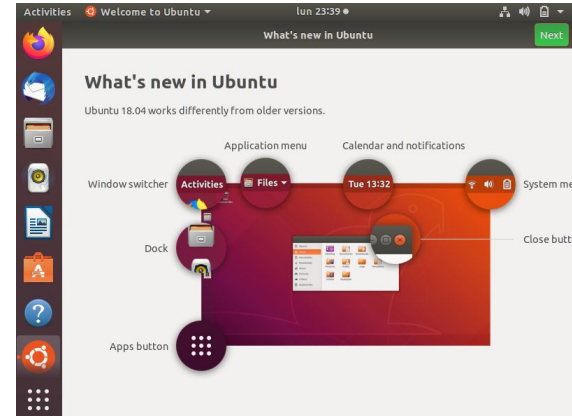


Sistema Operativo utilizado



- Ubuntu Server

- Ubuntu Desktop



Conexión entre ellas

```
jezraelj@jsserver:~$  
jezraelj@jsserver:~$ ping 198.168.56.100  
PING 198.168.56.100 (198.168.56.100) 56(84) bytes of data.  
64 bytes from 198.168.56.100: icmp_seq=1 ttl=64 time=1.22 ms  
64 bytes from 198.168.56.100: icmp_seq=2 ttl=64 time=1.09 ms  
64 bytes from 198.168.56.100: icmp_seq=3 ttl=64 time=0.932 ms  
64 bytes from 198.168.56.100: icmp_seq=4 ttl=64 time=0.790 ms  
64 bytes from 198.168.56.100: icmp_seq=5 ttl=64 time=0.944 ms  
64 bytes from 198.168.56.100: icmp_seq=6 ttl=64 time=0.919 ms  
64 bytes from 198.168.56.100: icmp_seq=7 ttl=64 time=1.26 ms  
^C  
--- 198.168.56.100 ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 6009ms  
rtt min/avg/max/mdev = 0.790/1.021/1.257/0.159 ms  
jezraelj@jsserver:~$
```

```
jezraelj@jsserver:~$  
jezraelj@jsserver:~$ ping 198.168.56.102  
PING 198.168.56.102 (198.168.56.102) 56(84) bytes of data.  
64 bytes from 198.168.56.102: icmp_seq=1 ttl=64 time=0.602 ms  
64 bytes from 198.168.56.102: icmp_seq=2 ttl=64 time=1.05 ms  
64 bytes from 198.168.56.102: icmp_seq=3 ttl=64 time=1.01 ms  
64 bytes from 198.168.56.102: icmp_seq=4 ttl=64 time=0.838 ms  
64 bytes from 198.168.56.102: icmp_seq=5 ttl=64 time=0.602 ms  
64 bytes from 198.168.56.102: icmp_seq=6 ttl=64 time=0.774 ms  
^C  
--- 198.168.56.102 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5007ms  
rtt min/avg/max/mdev = 0.602/0.812/1.051/0.176 ms  
jezraelj@jsserver:~$
```

- Conexión de la segunda con la primer máquina

- Conexión de la segunda con la tercer máquina

Conexión a internet

```
jezraelj@jserver:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=66.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=65.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=64.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=113 time=66.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=113 time=63.1 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=113 time=64.1 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=113 time=63.4 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=113 time=63.3 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=113 time=63.7 ms
^C
--- 8.8.8.8 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8013ms
rtt min/avg/max/mdev = 63.065/64.458/66.729/1.269 ms
jezraelj@jserver:~$
```

- Conexión a internet por DNS pública de google

Conexión con el host

```
jezraelj@jsrver:~$ ping 192.168.56.1
PING 192.168.56.1 (192.168.56.1) 56(84) bytes of data.
64 bytes from 192.168.56.1: icmp_seq=1 ttl=127 time=0.918 ms
64 bytes from 192.168.56.1: icmp_seq=2 ttl=127 time=1.74 ms
64 bytes from 192.168.56.1: icmp_seq=3 ttl=127 time=1.67 ms
64 bytes from 192.168.56.1: icmp_seq=4 ttl=127 time=1.98 ms
64 bytes from 192.168.56.1: icmp_seq=5 ttl=127 time=1.42 ms
64 bytes from 192.168.56.1: icmp_seq=6 ttl=127 time=0.936 ms
64 bytes from 192.168.56.1: icmp_seq=7 ttl=127 time=1.69 ms
64 bytes from 192.168.56.1: icmp_seq=8 ttl=127 time=1.62 ms
64 bytes from 192.168.56.1: icmp_seq=9 ttl=127 time=1.73 ms
```

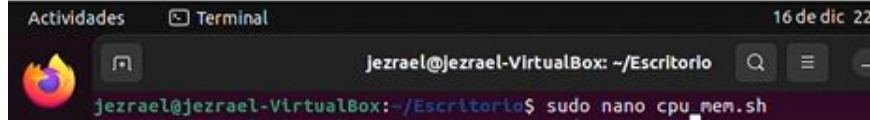
- Conexión con el host, terminación en 1



Tareas programadas:

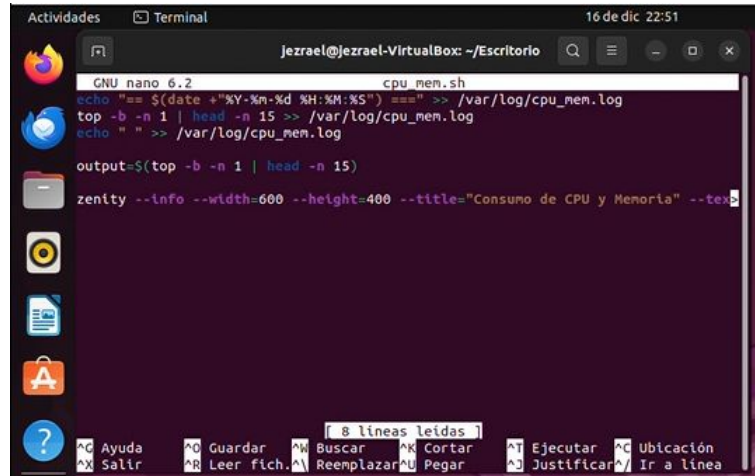
...

Capturar el consumo de CPU y memoria del sistema operativo y determinar cuáles son los procesos con más consumo. (Calendario: Todos los días, cada hora)



```
Actividades Terminal 16 de dic 22:51
Jezrael@Jezrael-VirtualBox: ~/Escritorio
Jezrael@Jezrael-VirtualBox:~/Escritorio$ sudo nano cpu_mem.sh
```

Archivos editables nano(nano debido a facilidad)



```
Actividades Terminal 16 de dic 22:51
Jezrael@Jezrael-VirtualBox: ~/Escritorio
GNU nano 6.2 cpu_mem.sh
echo "==" $(date +"%Y-%m-%d %H:%M:%S") ==> /var/log/cpu_mem.log
top -b -n 1 | head -n 15 >> /var/log/cpu_mem.log
echo " " >> /var/log/cpu_mem.log

output=$(top -b -n 1 | head -n 15)
zenity --info --width=600 --height=400 --title="Consumo de CPU y Memoria" --text=

8 líneas leídas
Ayuda Guardar Buscar Cortar Ejecutar Ubicación
Salir Leer fich. Reemplazar Pegar Justificar Ir a línea
```

Código que captura el consumo de CPU/Memoria

Capturar la lista de procesos activos en el sistema (Calendario: Todos los días, a las 8am y 8pm)

```
jezrael@jezrael-VirtualBox:~/Escritorio$ sudo nano active_processes.sh
```

Comando de acceso

```
GNU nano 6.2 active_processes.sh
echo "=== $(date +"%Y-%m-%d %H:%M:%S") ===" >> /var/log/active_processes.log
ps -aux >> /var/log/active_processes.log
echo " " >> /var/log/active_processes.log

output=$(ps aux --sort=-%mem | head -n 15 | awk '{printf "%-8s %-8s %-8s %s\n",
zenity --info --width=600 --height=400 --text="Procesos activos: $output"
```

Código que captura procesos activos del sistema

Capturar la utilización actual de todos los Filesystems presentes en el sistema (Calendario: Todos los días, cada 2 horas)

```
jezrael@jezrael-VirtualBox:~/Escritorio$ sudo nano filesystems.sh
```

Comando de acceso

```
GNU nano 6.2 filesystems.sh
echo "=== $(date +"%Y-%m-%d %H:%M:%S") ===" >> /var/log/filesystems.log
df -h >> /var/log/filesystems.log
echo " " >> /var/log/filesystems.log

output=$(df -h)

zenity --info --width=600 --height=400 --text="Utilizacion de filesystems: $out"
```

Código de captura utilización de filesystem

Captura de las últimas entradas de los siguientes logs de sistema (Calendario: Todos los días, cada hora):

```
jezrael@jezrael-VirtualBox:~/Escritorio$ sudo nano logs_capture.sh
```

Comando de acceso

...

Logs de Sistema

```
echo "=== Syslog ===" >> /var/log/system_logs.log  
sudo journalctl --since "1 hour ago" >> /var/log/system_logs.log  
echo " " >> /var/log/system_logs.log
```

Código de logs del sistema

...

Logs de Autorización o seguridad

```
echo "=== Authorization Logs ===" >> /var/log/system_logs.log  
sudo journalctl -u sshd --since "1 hour ago" >> /var/log/system_logs.log  
echo " " >> /var/log/system_logs.log
```

Código de autorización de logs

...

Logs del kernel

```
echo "=== Kernel Logs ===" >> /var/log/system_logs.log  
sudo journalctl -k --since "1 hour ago" >> /var/log/system_logs.log  
echo " " >> /var/log/system_logs.log
```

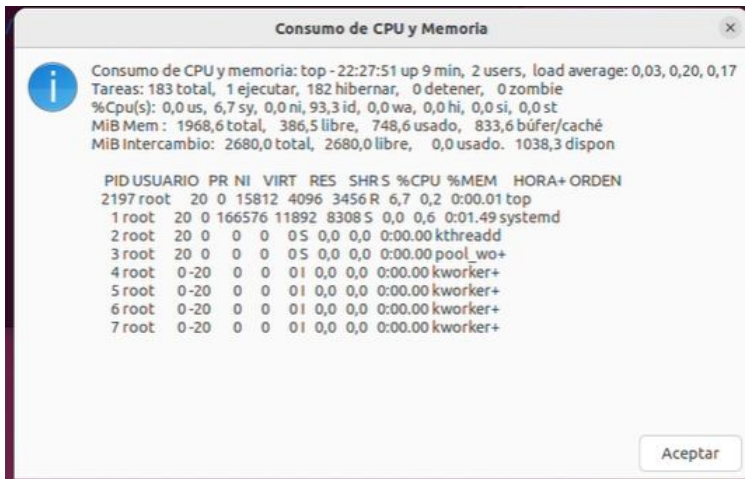
Código de autorización del kernel

...

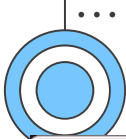
capacidad de ser ejecutadas ad-hoc

```
jezrael@jezrael-VirtualBox: ~/Escritorio$ sudo ./cpu_mem.sh
jezrael@jezrael-VirtualBox: ~/Escritorio$ sudo ./active_processes.sh
jezrael@jezrael-VirtualBox: ~/Escritorio$ sudo ./filesystems.sh
jezrael@jezrael-VirtualBox: ~/Escritorio$ sudo ./logs_capture.sh
```

- Comandos para presentar cada tarea programada ad-hoc



- Tarea capturar CPU y Memoria (ad-hoc)



capacidad de ser ejecutadas ad-hoc

```
Información
Procesos activos: USER PID %CPU COMMAND
jezrael 1458 3.8 /usr/bin/gnome-shell
jezrael 2131 0.4 /usr/libexec/gsd-xsettings
jezrael 1851 0.2 gjs
jezrael 1673 0.1 /usr/libexec/evolution-data-server/evolution-alarm-notify
jezrael 2128 0.2 /usr/bin/Xwayland
jezrael 2092 1.0 /usr/libexec/gnome-terminal-server
root 716 0.1 /usr/bin/python3
jezrael 1454 0.0 /usr/libexec/goa-daemon
root 658 0.3 /usr/lib/snapd/snapd
jezrael 1558 0.0 /usr/libexec/evolution-calendar-factory
jezrael 1913 0.0 update-notifier
jezrael 1696 0.5 /usr/libexec/ibus-extension-gtk3
jezrael 1816 0.0 /usr/libexec/xdg-desktop-portal-gnome
jezrael 2087 0.1 /usr/bin/gnome-terminal.real
```

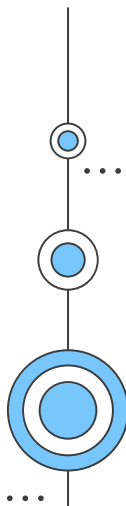
- Tarea capturar procesos activos(ad-hoc)

```
Logs del sistema
=== Authorization Logs === Dec 17 22:28:28 jezrael-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)
Dec 17 22:28:28 jezrael-VirtualBox sudo: root: TTY=pts/1; PWD=/home/jezrael/Escritorio; USER=root; COMMAND=/usr/bin/journalctl -u sshd -since '1 hour ago'
Dec 17 22:28:28 jezrael-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by jezrael(uid=0)
Dec 17 22:28:28 jezrael-VirtualBox sudo: root: TTY=pts/1; PWD=/home/jezrael/Escritorio; USER=root; COMMAND=/usr/bin/journalctl -k -since '1 hour ago'
Dec 17 22:28:28 jezrael-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by jezrael(uid=0)
Dec 17 22:28:28 jezrael-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
Dec 17 22:28:28 jezrael-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by jezrael(uid=0)
Dec 17 22:28:28 jezrael-VirtualBox sudo: pam_unix(sudo:session): session opened for user root(uid=0) by jezrael(uid=0)
Dec 17 22:28:28 jezrael-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
Dec 17 22:28:28 jezrael-VirtualBox sudo: pam_unix(sudo:session): session closed for user root
Dec 17 22:26:44 jezrael-VirtualBox gnome-shell[2133]: The XKEYBOARD keymap compiler (xkbcomp) reports:
Dec 17 22:26:44 jezrael-VirtualBox gnome-shell[2133]: > Warning: Unsupported maximum keycode 708, clipping.
Dec 17 22:26:44 jezrael-VirtualBox gnome-shell[2133]: > X11 cannot support keycodes above 255.
Dec 17 22:26:44 jezrael-VirtualBox gnome-shell[2133]: > Errors from xkbcomp are not fatal to the X server
Dec 17 22:26:44 jezrael-VirtualBox systemd[1283]: Started GNOME XSettings service.
Dec 17 22:26:44 jezrael-VirtualBox systemd[1283]: Reached target GNOME session X11 services.
Dec 17 22:26:44 jezrael-VirtualBox gnome-shell[1458]: ATK Bridge is disabled but a11y has already been enabled.
Dec 17 22:27:37 jezrael-VirtualBox crontab[2185]: (root) BEGIN EDIT (root)
Dec 17 22:27:43 jezrael-VirtualBox crontab[2185]: (root) END EDIT (root)
```

- Tarea programada logs del sistema(ad-hoc)

```
Información
Utilizacion de filesystems: S.ficheros Tamaño Usados Disp Uso% Montado en
tmpfs 197M 1,5M 196M 1% /run
/dev/sda3 24G 15G 8,7G 62% /
tmpfs 985M 0 985M 0% /dev/shm
tmpfs 5,0M 4,0K 5,0M 1% /run/lock
/dev/sda2 512M 6,1M 506M 2% /boot/efi
tmpfs 197M 100K 197M 1% /run/user/1000
```

- Tarea capturar file systems(ad-hoc)



Cron y Glances

```
jezrael@jezrael-VirtualBox:~/Escritorio$ sudo crontab -e
```

Comando de acceso a cron

```
0 * * * * DISPLAY=:0 /home/jezrael/cpu_mem.sh
0 8,20 * * * * DISPLAY=:0 /home/jezrael/active_processes.sh
0 */2 * * * * DISPLAY=:0 /home/jezrael/filesystems.sh
0 * * * * DISPLAY=:0 /home/jezrael/logs_capture.sh
```

- Código cron

```
jezrael-VirtualBox (Ubuntu 22.04 64bit / Linux 6.8.0-45-generic) Uptime: 0:10:41
```

CPU	[9.3%]	user	5.0%	total	1.92G	total	2.62G	1 min:	0.08
MEM	[48.2%]	system	1.0%	used	949M	used	0	5 min:	0.19
SWAP	[0.0%]	lowait	0.0%	free	1019M	free	2.62G	15 min:	0.17

NETWORK	Rx/s	Tx/s	TASKS 178 (419 thr), 1 run, 133 slp, 44 oth						
enp0s3	0b	0b							
enp0s8	920b	1Kb							
lo	2Kb	2Kb							

DefaultGateway		5ms							

DISK I/O	R/s	W/s							
sda	0	51K	0.0	3.4	1851	jezrael	6	0	S gjs /usr/s
sda1	0	0	0.0	3.4	1673	jezrael	6	0	S evolution-
sda2	0	0	0.0	3.3	2128	jezrael	1	0	S Xwayland :
sda3	0	0	0.0	2.4	716	root	1	0	S python3 /u
sr0	0	51K	0.0	2.0	1454	jezrael	4	0	S goa-daemon
	0	0	0.0	1.6	658	root	8	0	S snapd
			0.0	1.6	1558	jezrael	9	0	S evolution-
			0.0	1.5	1913	jezrael	4	0	S update-not

FILE SYS	Used	Total							
/ (sda3)	14.0G	23.9G							
2024-12-17 22:29:18 CST9G									

- Glances como forma grafica

Comprobación de funcionamiento

...