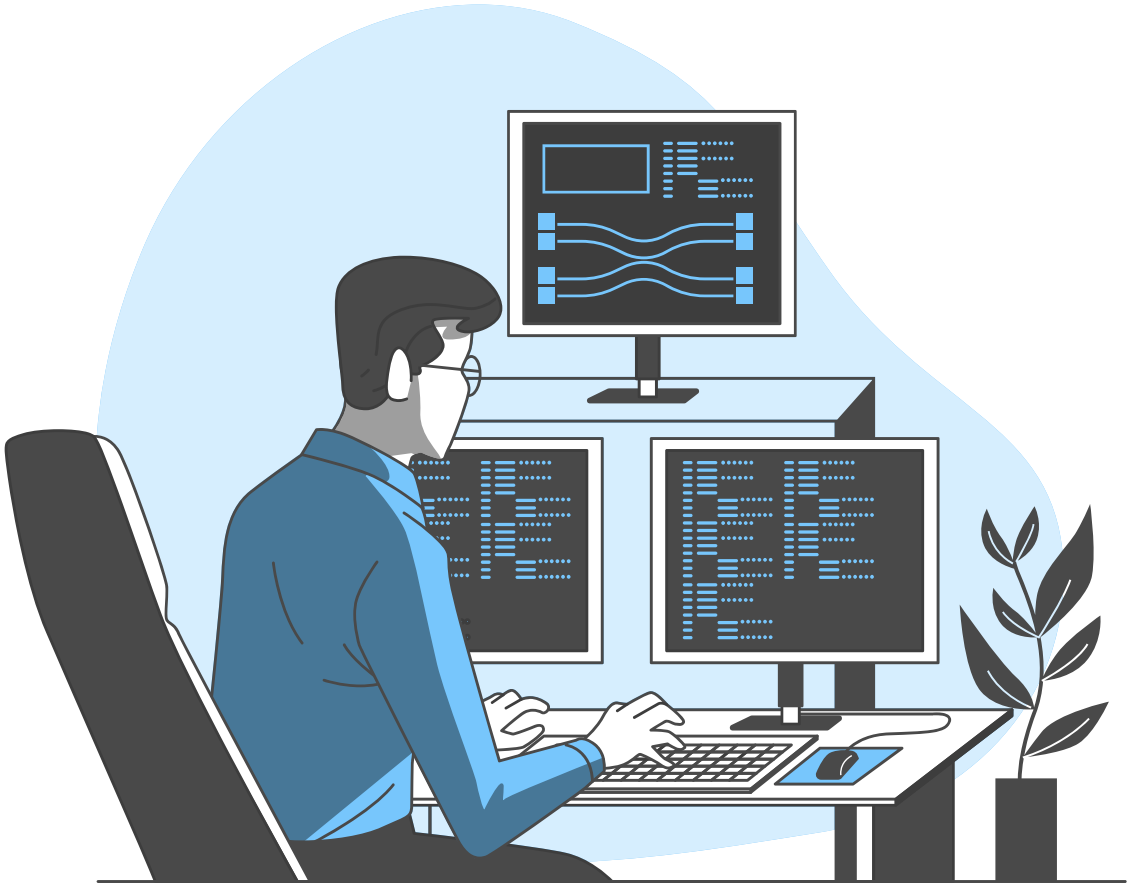


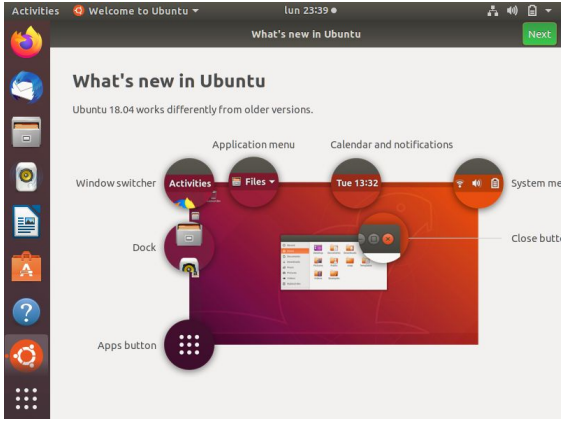
Industrias Oscorp

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@jserver:~$
jezraelj@jserver:~$ 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@jserver:~$
```

- Conexión de la segunda con la primer máquina

```
jezraelj@jserver:~$
jezraelj@jserver:~$ 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@jserver:~$
```

- 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

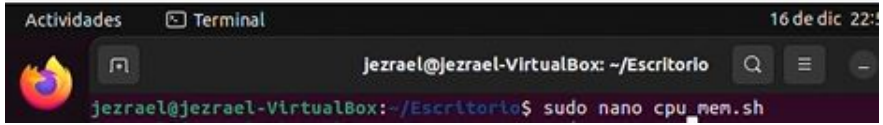
Conexión con el host

```
jezraelj@jserver:~$ 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
```

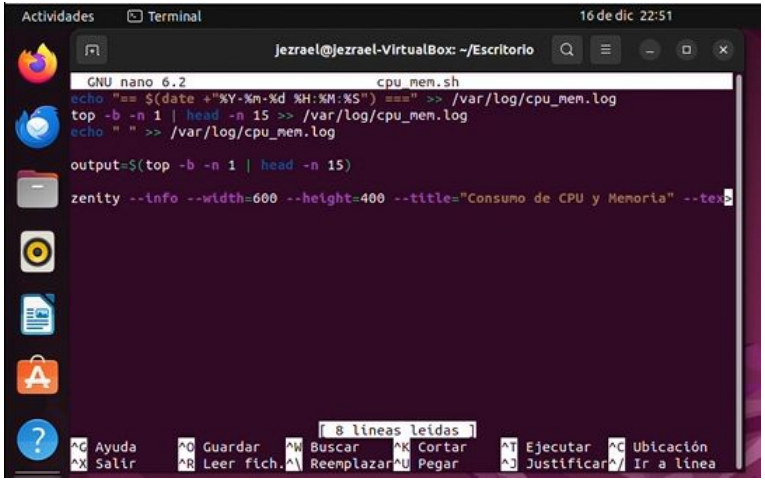
- Conexion con el host, terminación en 1

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)



Archivos editables nano(nano debido a facilidad)



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

                                [ 8 líneas leídas ]
^G Ayuda    ^O Guardar   ^W Buscar   ^K Cortar    ^T Ejecutar  ^C Ubicación
```

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
```

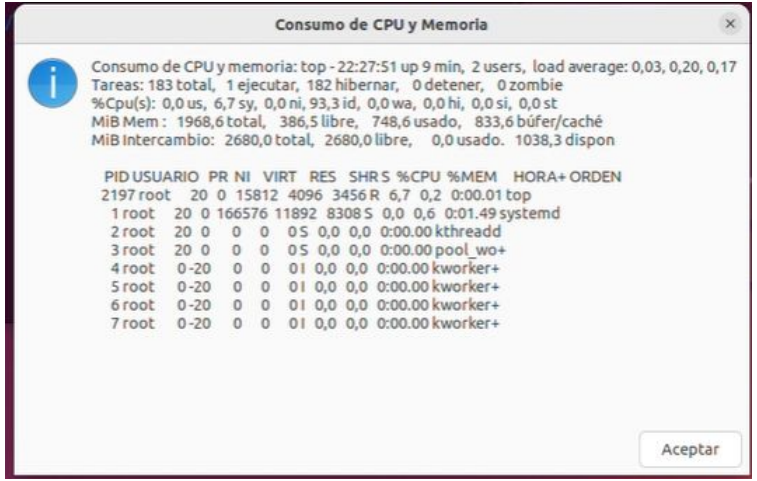
-

Código de autorización del kernel

capacidad de ser ejecutadas ad-hoc

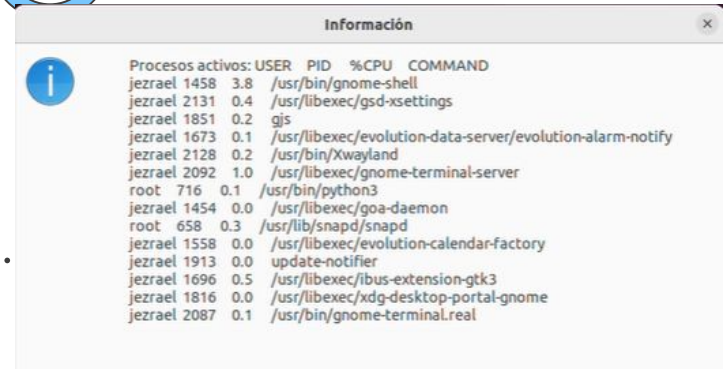
```
jezrael@jezrael-VirtualBox:~/Escritorio$ sudo ./cpu_mem.sh
jezrael@jezrael-VirtualBox:~/Escritorio$ sudo ./active_processes.sh
jezrael@jezrael-VirtualBox:~/Escritorio$ sudo ./filesystems.sh
jezrael@jezrael-VirtualBox:~/Escritorio$ sudo ./logs_capture.sh
```

- Comandos para presentar cada tarea programada ad-hoc



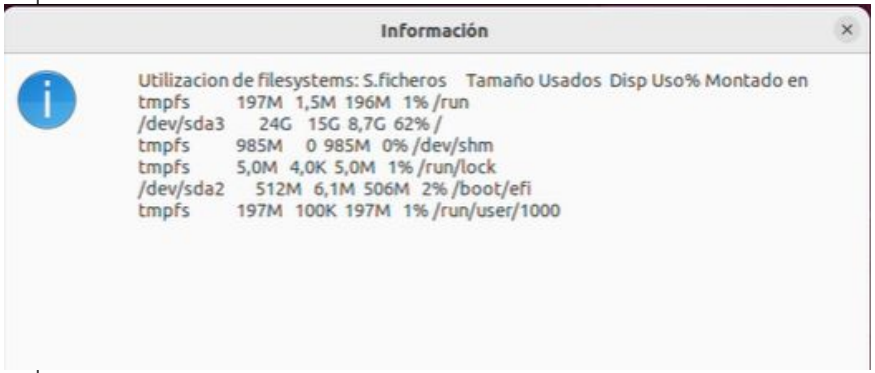
- Tarea capturar CPU y Memoria (ad-hoc)

capacidad de ser ejecutadas ad-hoc



- Tarea capturar procesos activos(ad-hoc)

- Tarea programada logs del sistema(ad-hoc)



- 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%   MEM     48.2%   SWAP      0.0%   LOAD     1-core
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%]   iowait    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   CPU%  MEM%      PID USER       THR  NI S
lo             2Kb    2Kb   >6.9   2.5     2251 jezrael    2     0 R python3 /u
                             1.8   16.4     1458 jezrael   11     0 S gnome-shel
DefaultGateway        5ms    0.5   2.6     2092 jezrael    4     0 S gnome-term
                             0.0   4.1     2131 jezrael    4     0 S gsd-xsetti
DISK I/O      R/s    W/s     0.0   3.4     1851 jezrael    6     0 S gjs /usr/s
sda             0    51K     0.0   3.4     1673 jezrael    6     0 S evolution-
sda1            0      0     0.0   3.3     2128 jezrael    1     0 S Xwayland :
sda2            0      0     0.0   2.4      716 root       1     0 S python3 /u
sda3            0    51K     0.0   2.0     1454 jezrael    4     0 S goa-daemon
sr0             0      0     0.0   1.6      658 root       8     0 S snapd
                             0.0   1.6     1558 jezrael    9     0 S evolution-
FILE SYS      Used  Total   0.0   1.5     1913 jezrael    4     0 S update-not
/ (sda3)     14.0G  23.9G
2024-12-17 22:29:18 CST9G
```

- Glances como forma grafica

Comprobación de funcionamiento