

# **MONITORIZACIÓN DE SISTEMAS OPERATIVOS**

Raúl Arribas Redondo

ASO

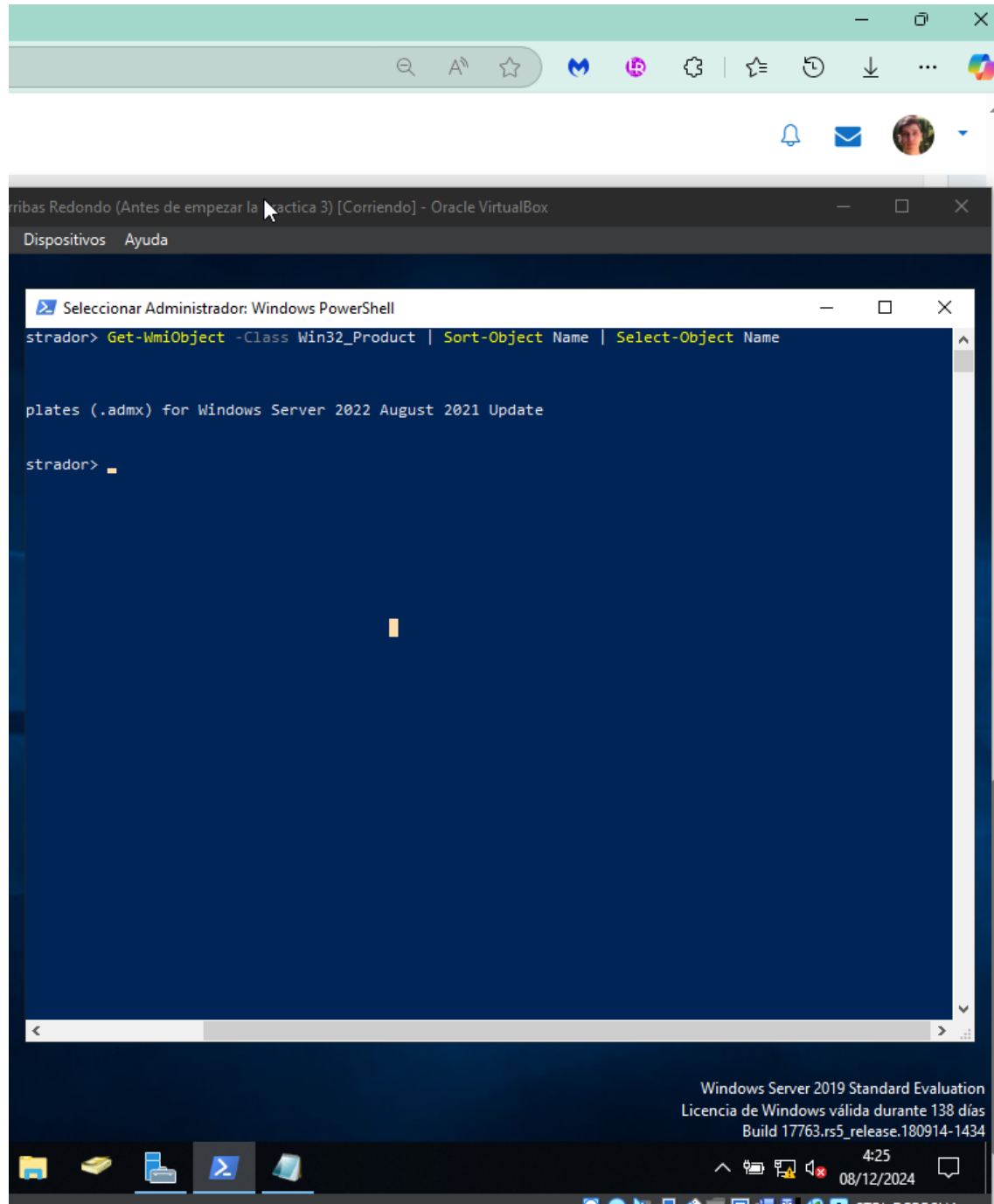
## Contenido

|     |                                                                                                     |    |
|-----|-----------------------------------------------------------------------------------------------------|----|
| 1   | Gestiona programas instalados en Windows Server .....                                               | 2  |
| 1.1 | Listado de los programas instalados en el sistema de forma ordenada desde Powershell .....          | 2  |
| 1.2 | Agrupar los programas cuyo nombre sea Microsoft desde Powershell .....                              | 3  |
| 1.3 | Instalar y desinstalar software adicional desde la terminal .....                                   | 4  |
| 2   | Apartado 2: Realizar un informe de rendimiento y fiabilidad de un servidor Windows Server .....     | 7  |
| 2.1 | Diagnóstico del sistema .....                                                                       | 7  |
| 2.2 | Análisis de procedimientos recomendados .....                                                       | 7  |
| 2.3 | Estudio de confiabilidad del sistema .....                                                          | 10 |
| 3   | Apartado 3: Crea tareas programadas para mejorar el rendimiento del sistema en Windows Server ..... | 12 |
| 3.1 | Alerta de rendimiento para uso elevado de la CPU .....                                              | 12 |
| 3.2 | Forzar el uso elevado de la CPU y localizar el evento .....                                         | 18 |
| 3.3 | Crear tarea asociada para detener servicios .....                                                   | 19 |
| 3.4 | Verificar que la tarea funciona correctamente .....                                                 | 21 |
| 4   | Apartado 4: Rendimiento en sistemas GNU/Linux .....                                                 | 24 |
| 4.1 | Instalar la herramienta SYSSTAT .....                                                               | 24 |
| 4.2 | Recopilar datos de rendimiento del sistema .....                                                    | 25 |
| 4.3 | Instalar herramienta gráfica para interpretar los datos .....                                       | 26 |
| 5   | Apartado 5: Administración del sistema GNU/Linux .....                                              | 29 |
| 5.1 | Listar los paquetes del sistema y buscar detalles del paquete cron .....                            | 29 |
| 5.2 | Crear tarea para copia de seguridad con rsync .....                                                 | 31 |
| 5.3 | Verificar registros del sistema para cron .....                                                     | 32 |
| 5.4 | Comprobar los logs .....                                                                            | 34 |
| 6   | Apartado 6: Monitorización de sistemas en red .....                                                 | 34 |
| 6.1 | Instalar un sistema de monitorización .....                                                         | 34 |
| 6.2 | Ejecutar tareas de monitorización .....                                                             | 36 |

## 1 Gestiona programas instalados en Windows Server

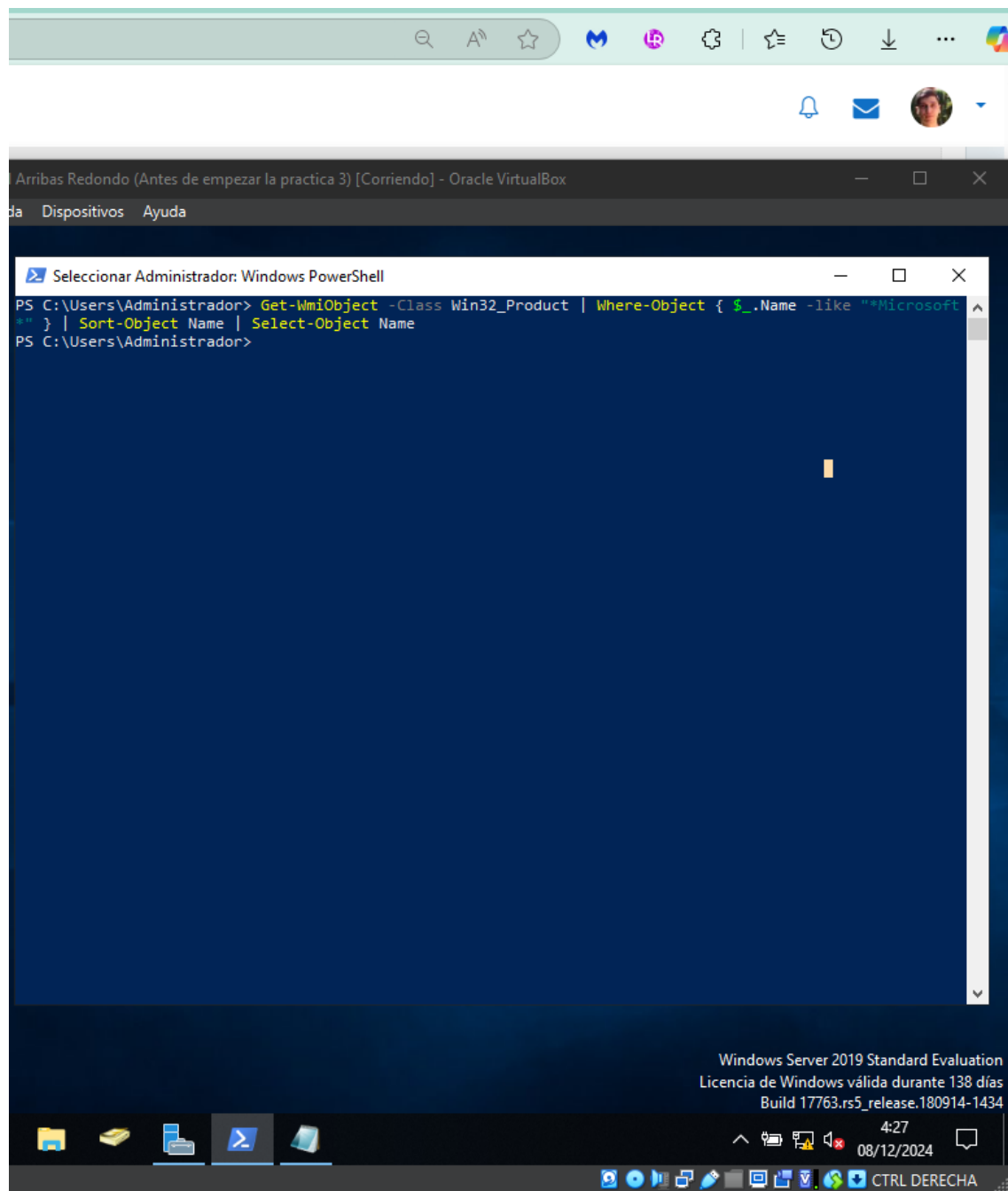
### 1.1 Listado de los programas instalados en el sistema de forma ordenada desde Powershell

**Get-WmiObject -Class Win32\_Product | Sort-Object Name | Select-Object Name**



## 1.2 Agrupar los programas cuyo nombre sea Microsoft desde Powershell

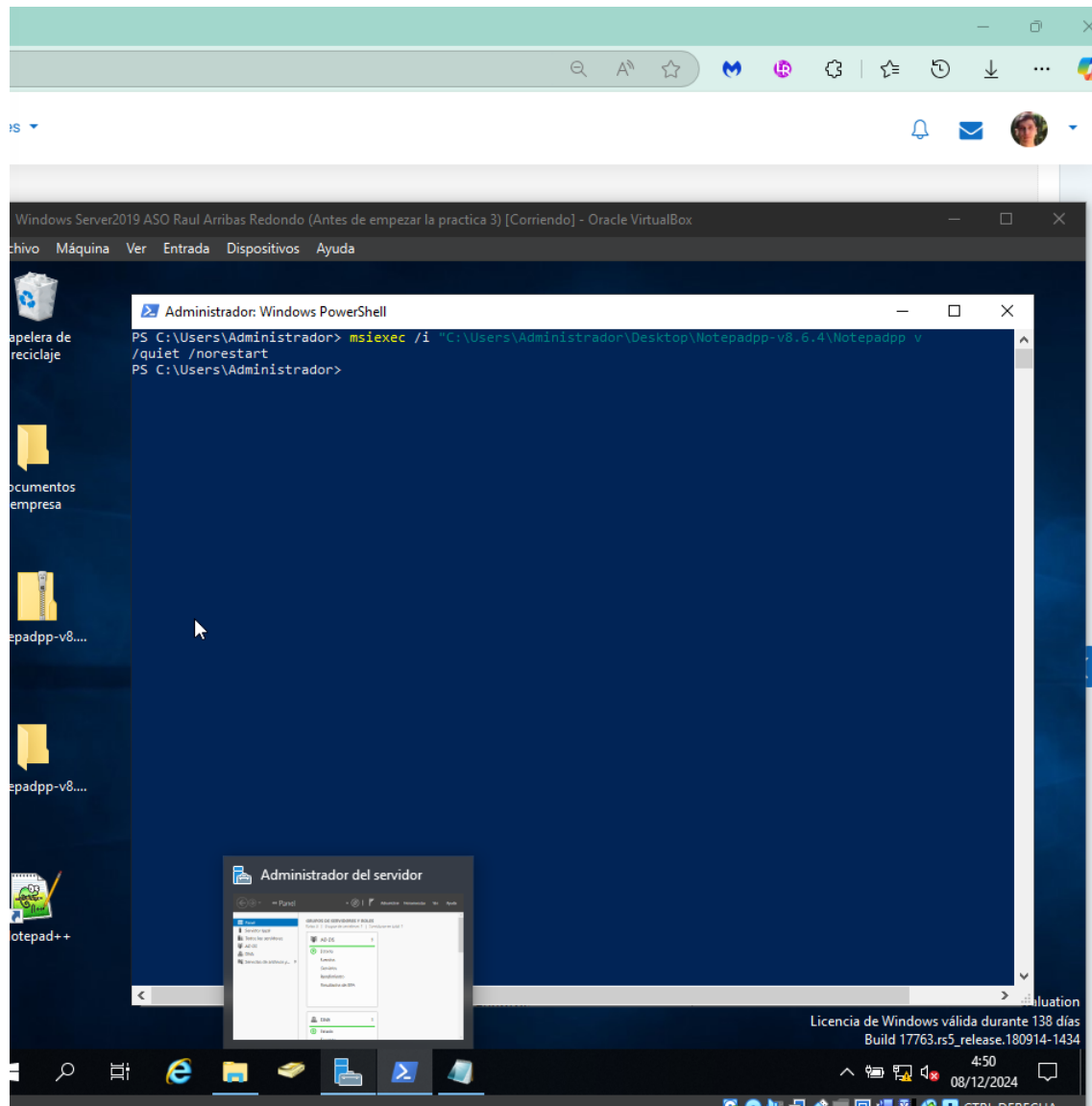
**Get-WmiObject -Class Win32\_Product | Where-Object { \$\_.Name -like "\*Microsoft\*" } | Sort-Object Name | Select-Object Name**



### 1.3 Instalar y desinstalar software adicional desde la terminal

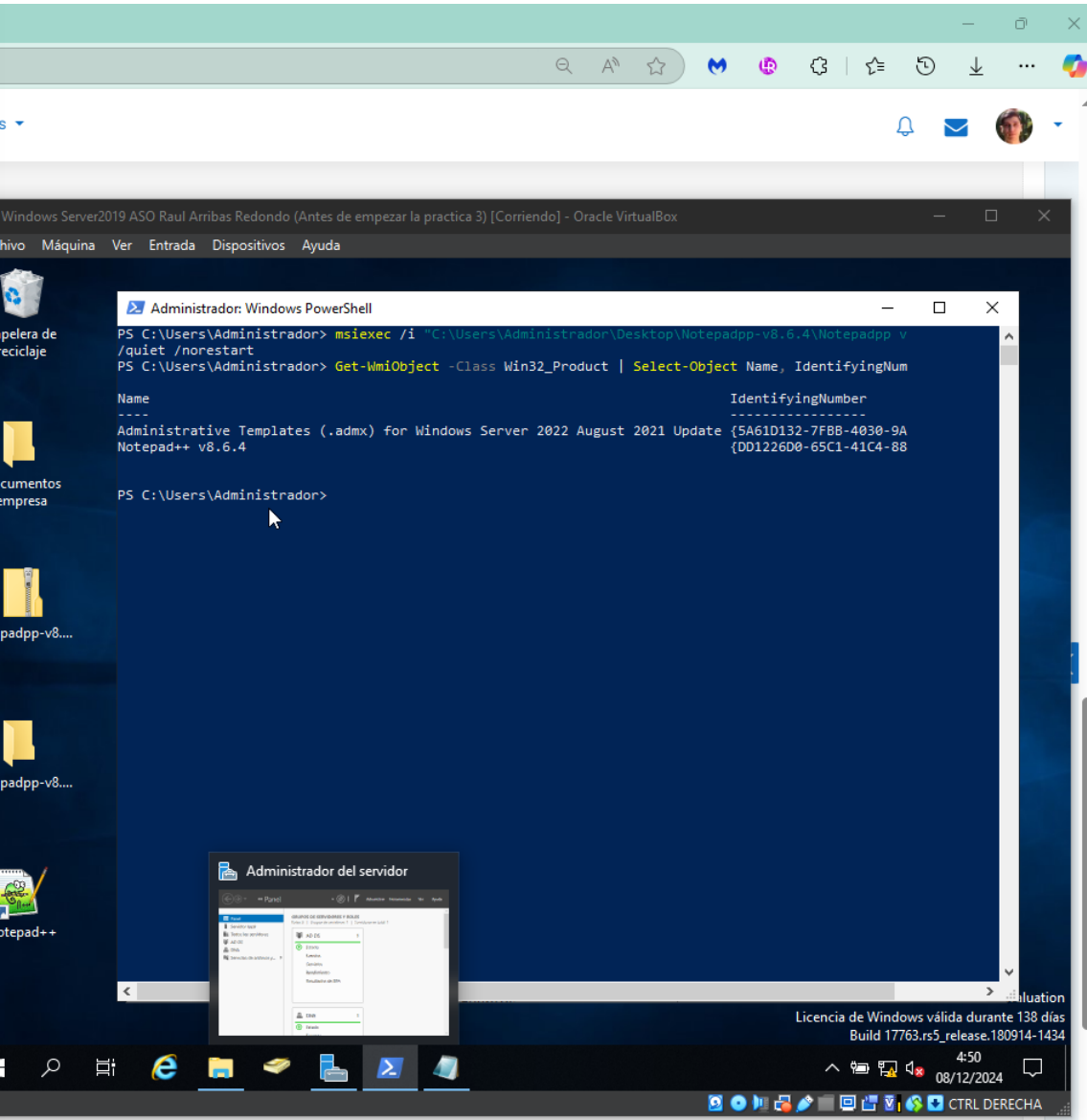
Para instalar aplicaciones:

**msiexec /i "ruta\_del\_archivo.msi" /quiet /norestart**

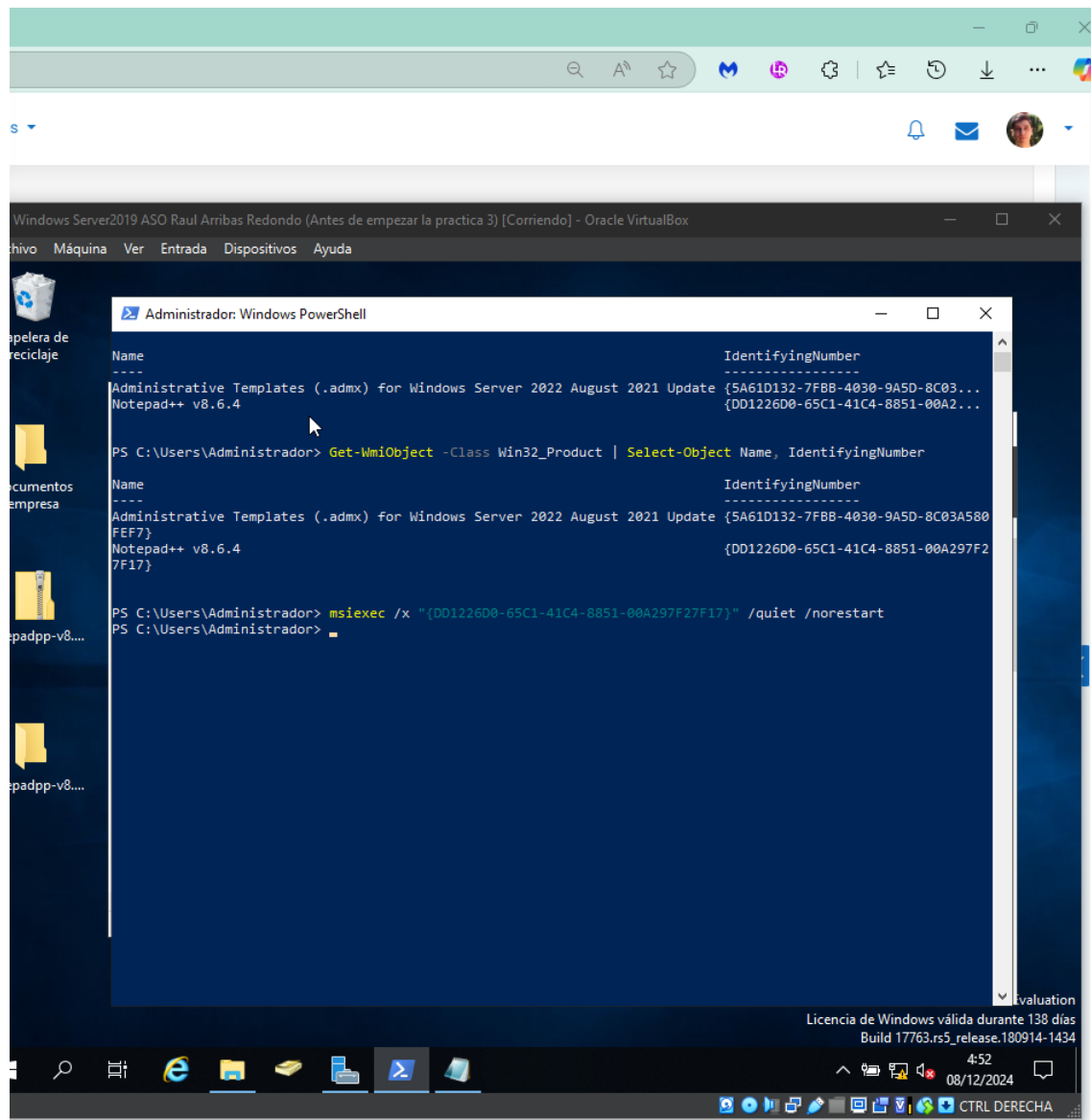


Para desinstalar aplicaciones:

**Get-WmiObject -Class Win32\_Product | Select-Object Name, IdentifyingNumber**



**msiexec /x "{PRODUCT-CODE}" /quiet /norestart**

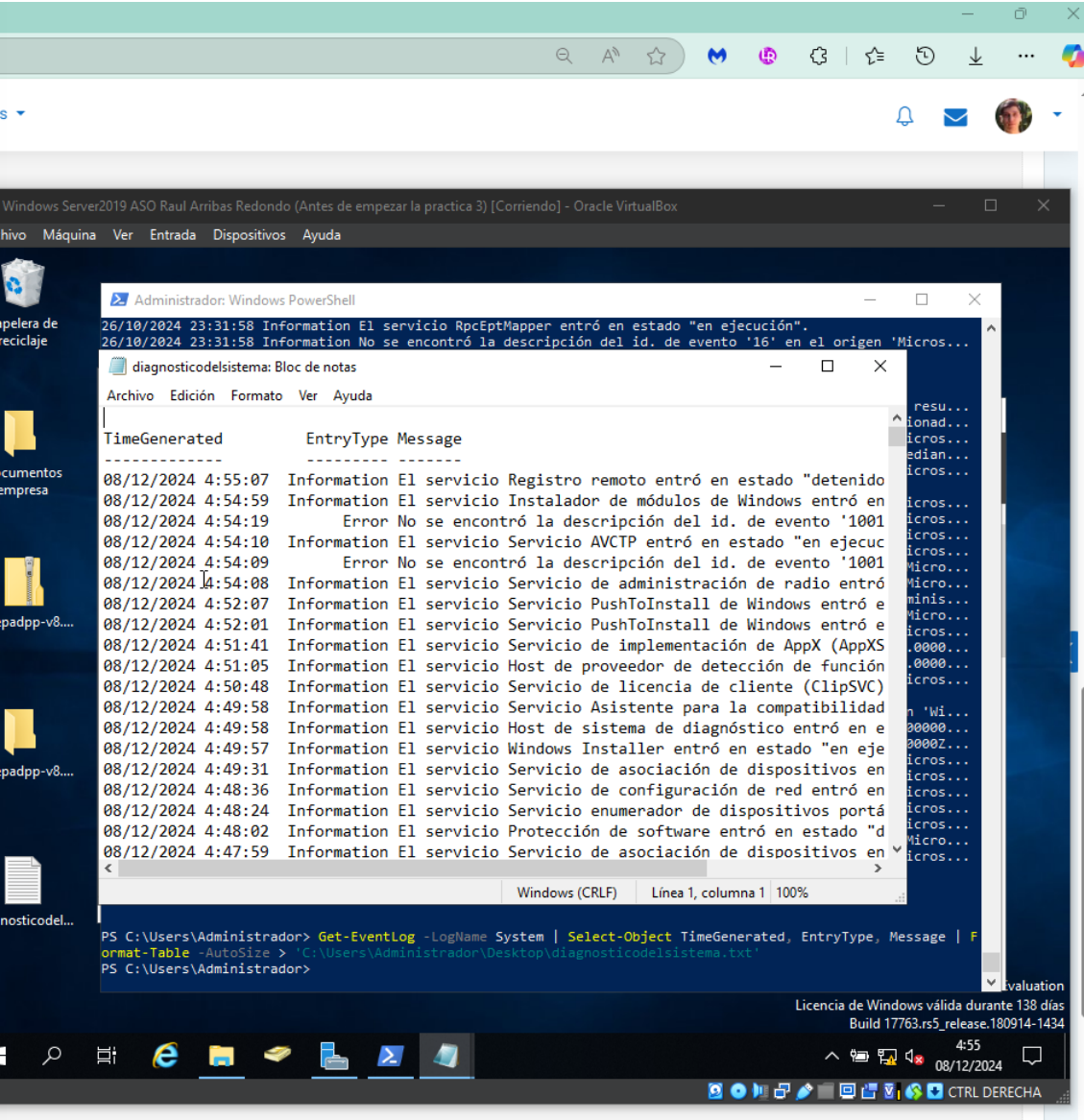


## 2 Apartado 2: Realizar un informe de rendimiento y fiabilidad de un servidor Windows Server

### 2.1 Diagnóstico del sistema

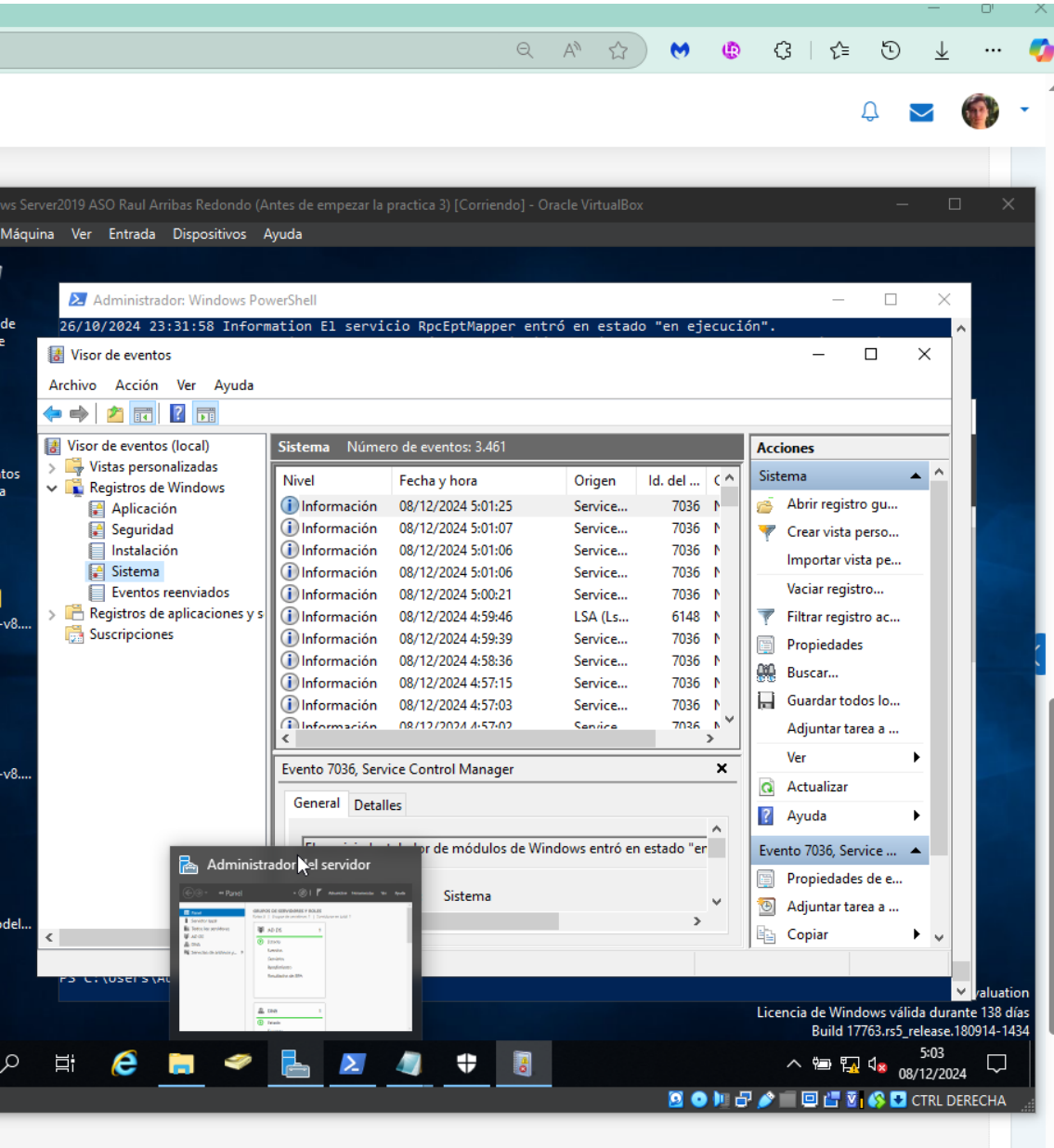
**Get-EventLog -LogName System | Select-Object TimeGenerated, EntryType, Message | Format-Table -AutoSize**

Hemos pasado la salida del comando al un documento txt para guardarlo.

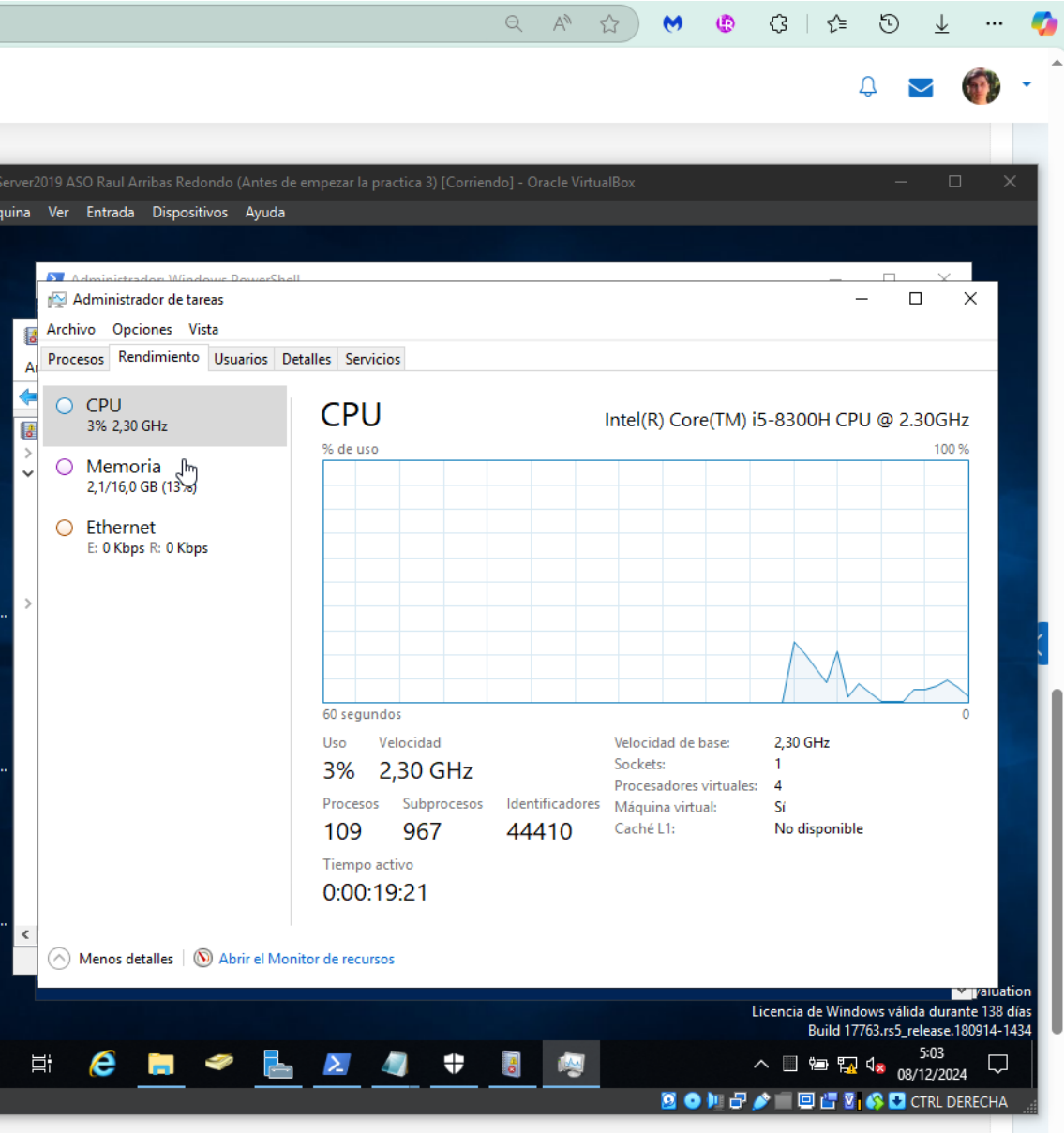


### 2.2 Análisis de procedimientos recomendados

Para hacer análisis vamos a utilizar la aplicaciones del Visor de Eventos:

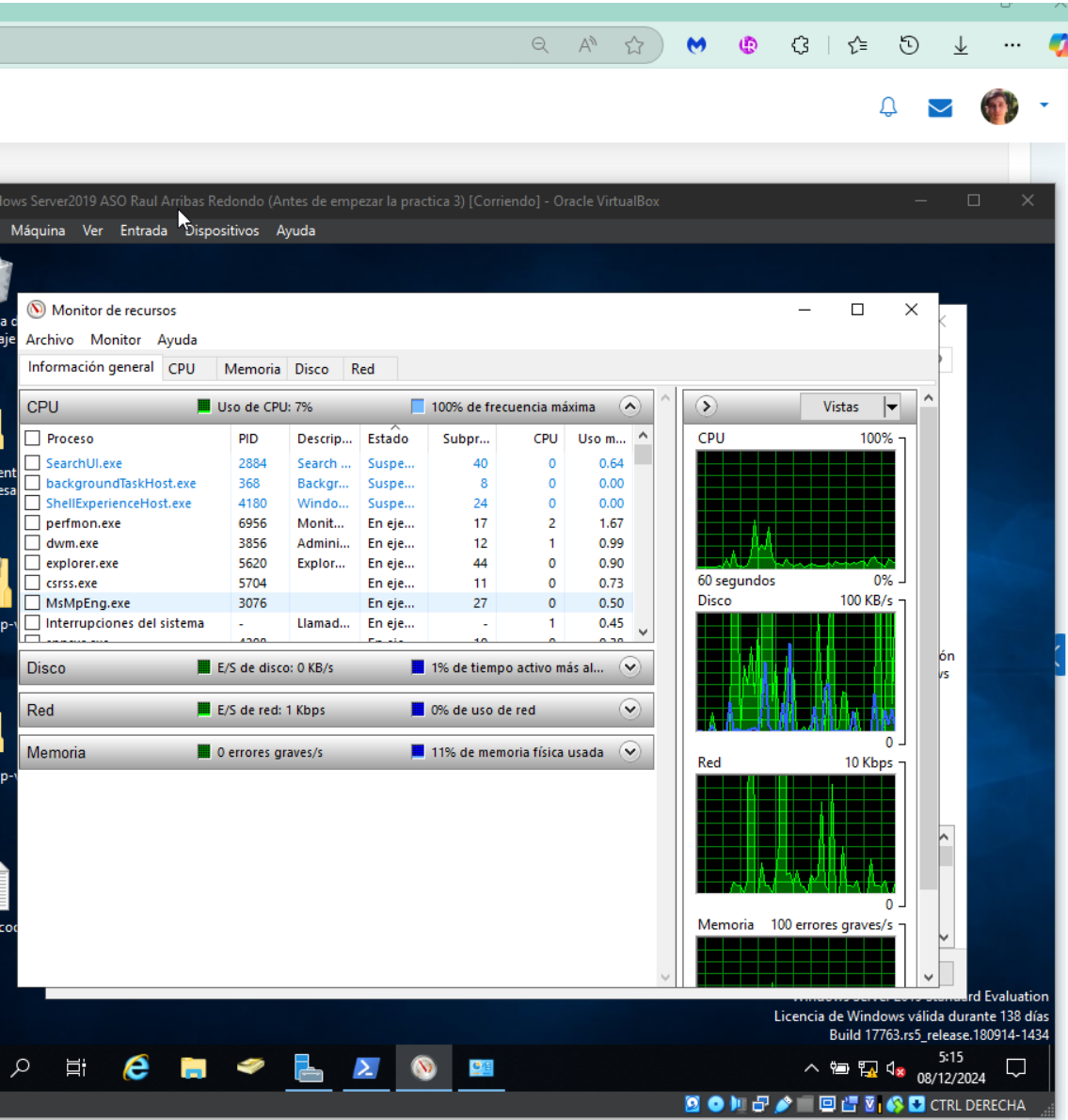


El administrador de tareas también nos puede dar información al respecto sobre el rendimiento de nuestra cpu, memoria ram y red:

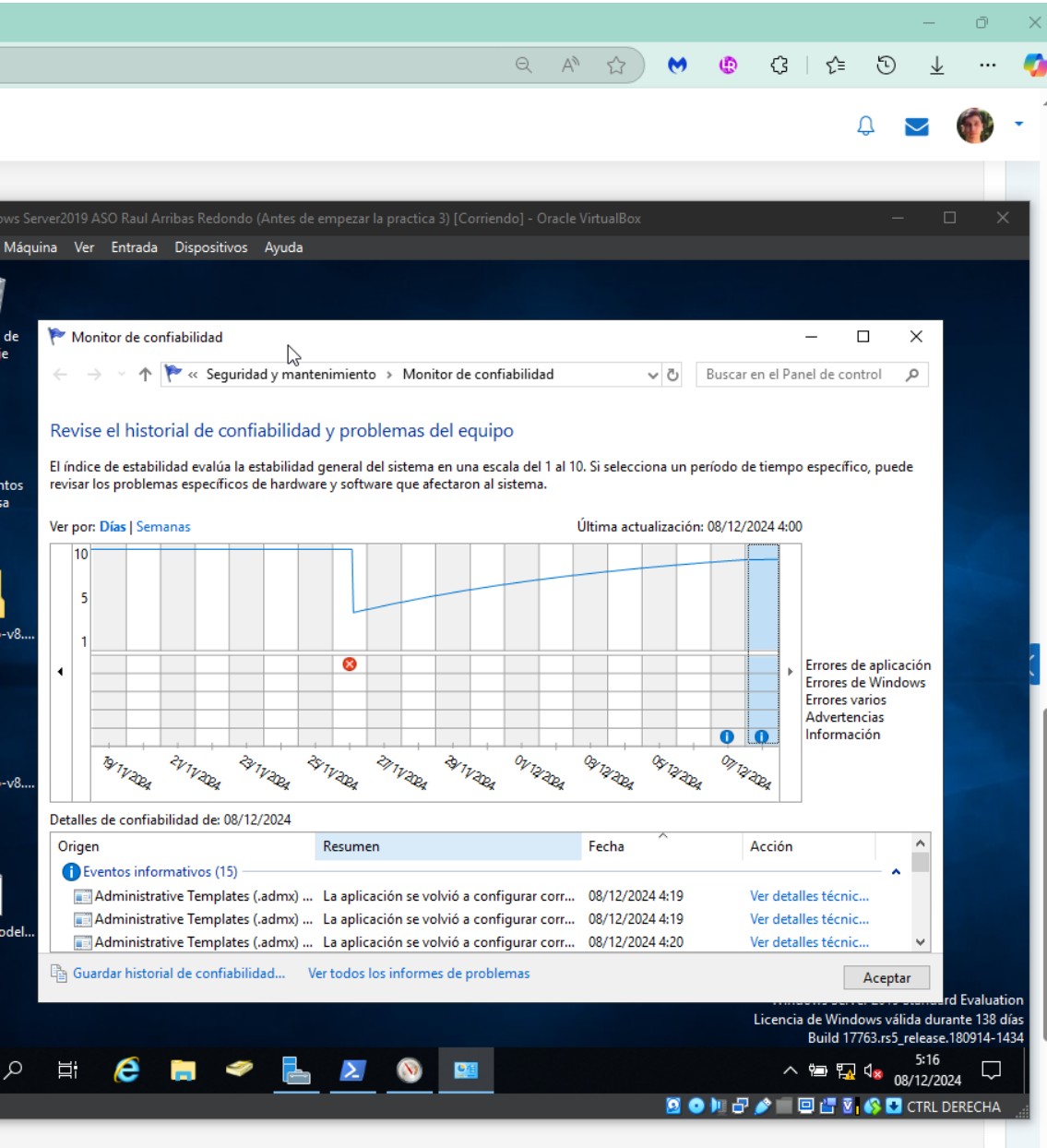


2.3 Estudio de confiabilidad del sistema

Tenemos el monitor de recursos



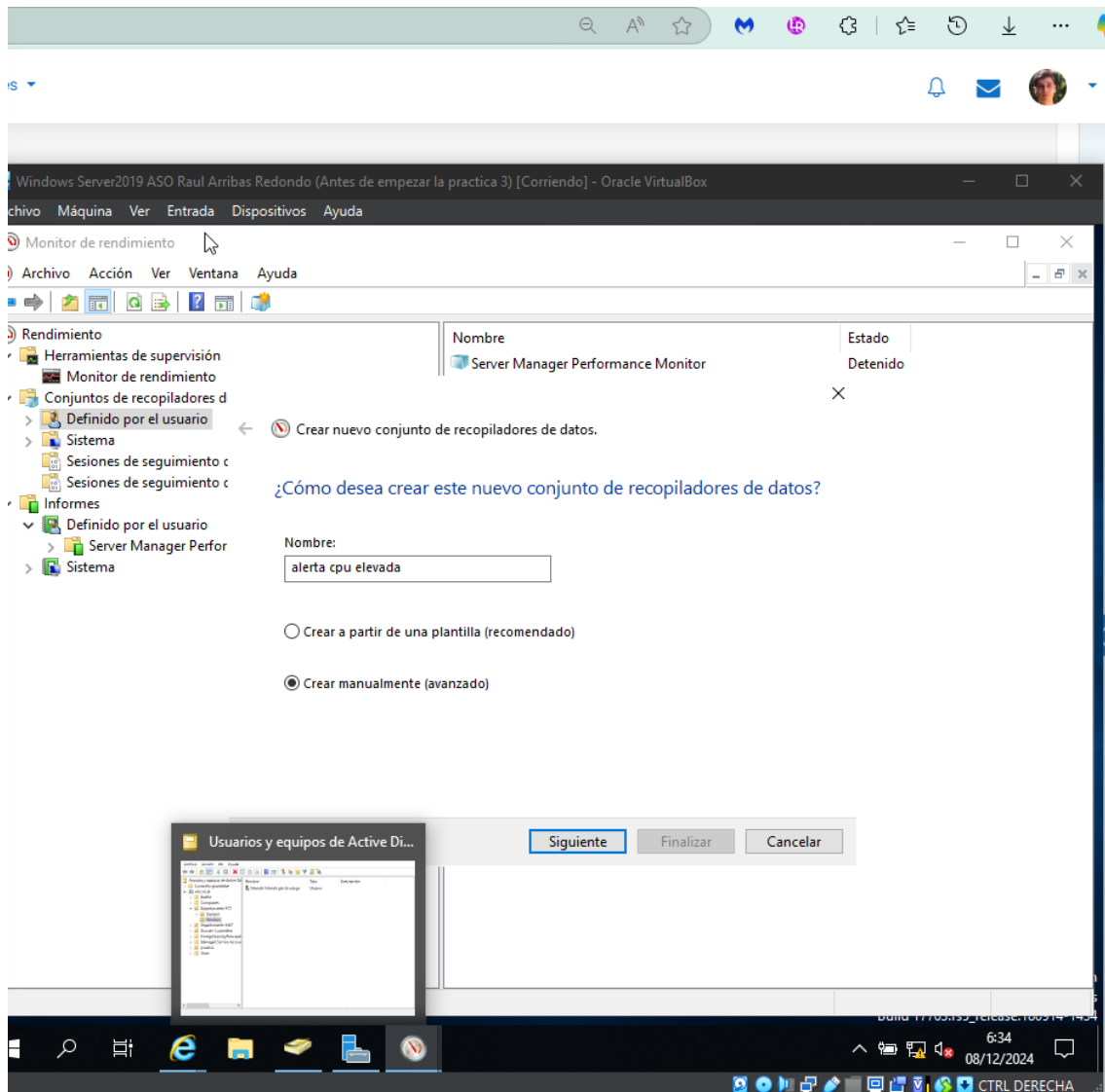
Tambien podemos abrir el Monitor de Confiabilidad, donde podemos ver l historial de los errores o apliaciones que hemos instalado en nuestro Windows Server.

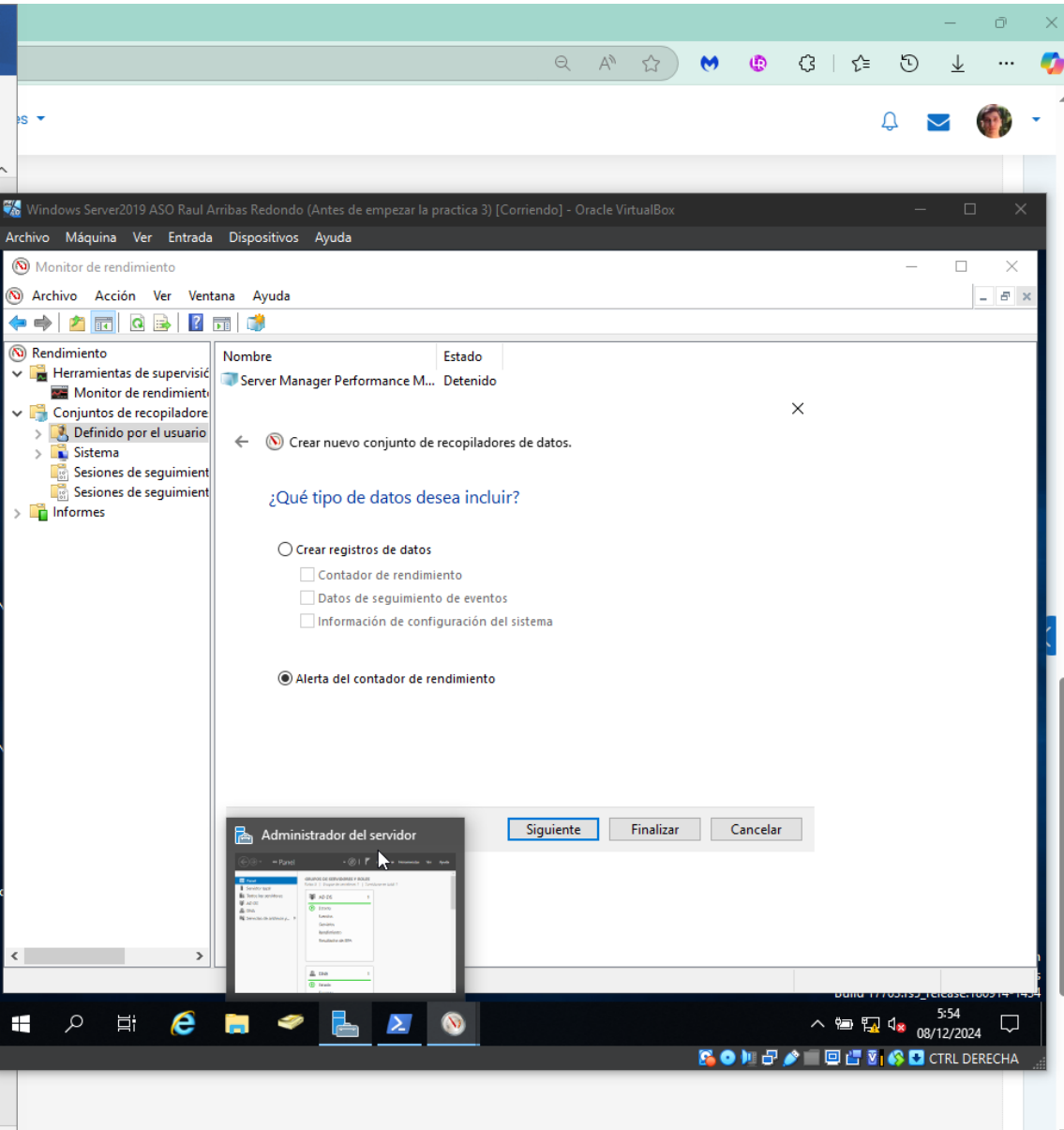


### 3 Apartado 3: Crea tareas programadas para mejorar el rendimiento del sistema en Windows Server

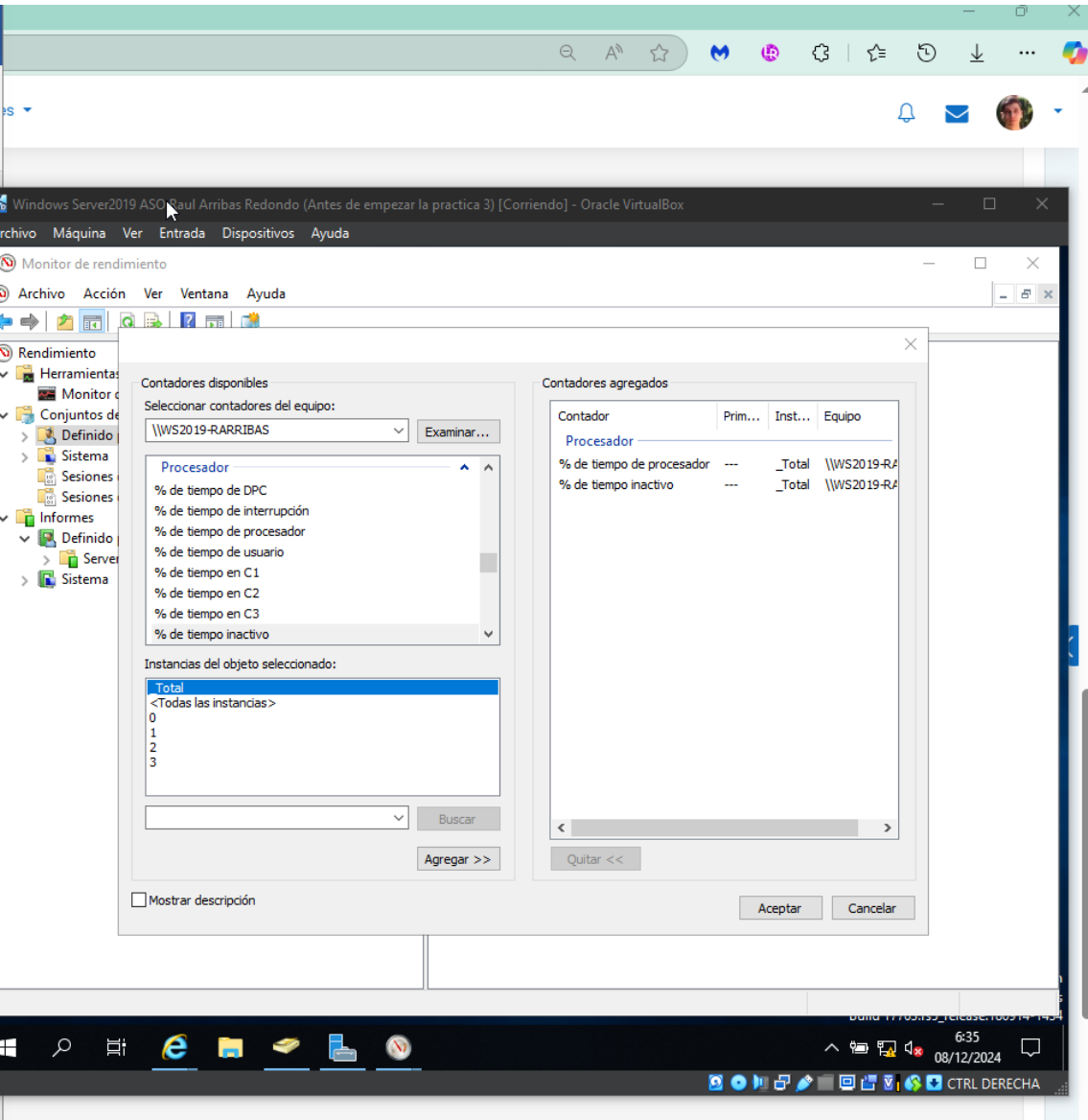
#### 3.1 Alerta de rendimiento para uso elevado de la CPU

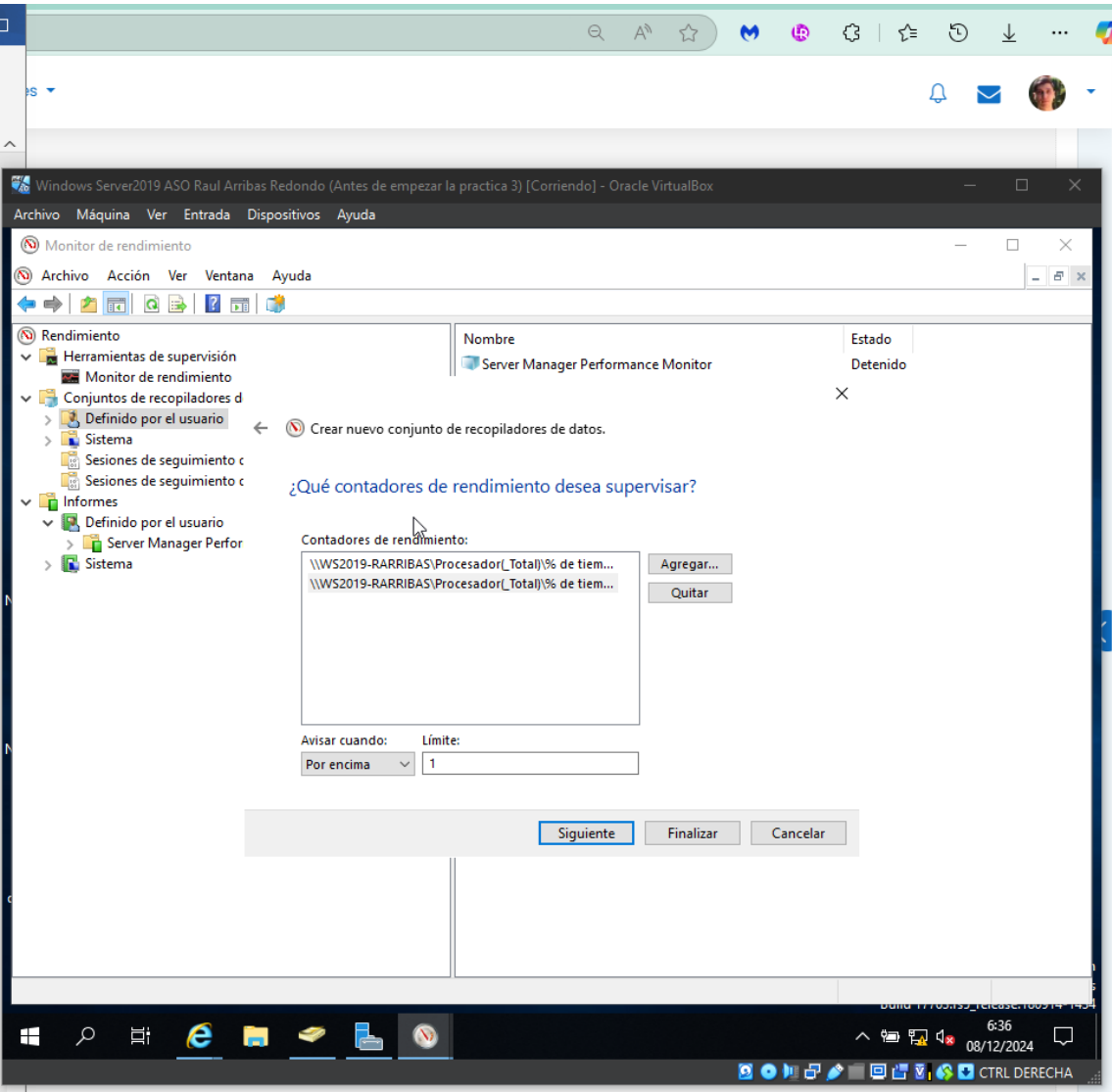
Abrimos el monitor de rendimiento → Conjunto de recopiladores → Definido por el usuario → Click derecho y Nuevo → Conjunto de recopiladores de datos

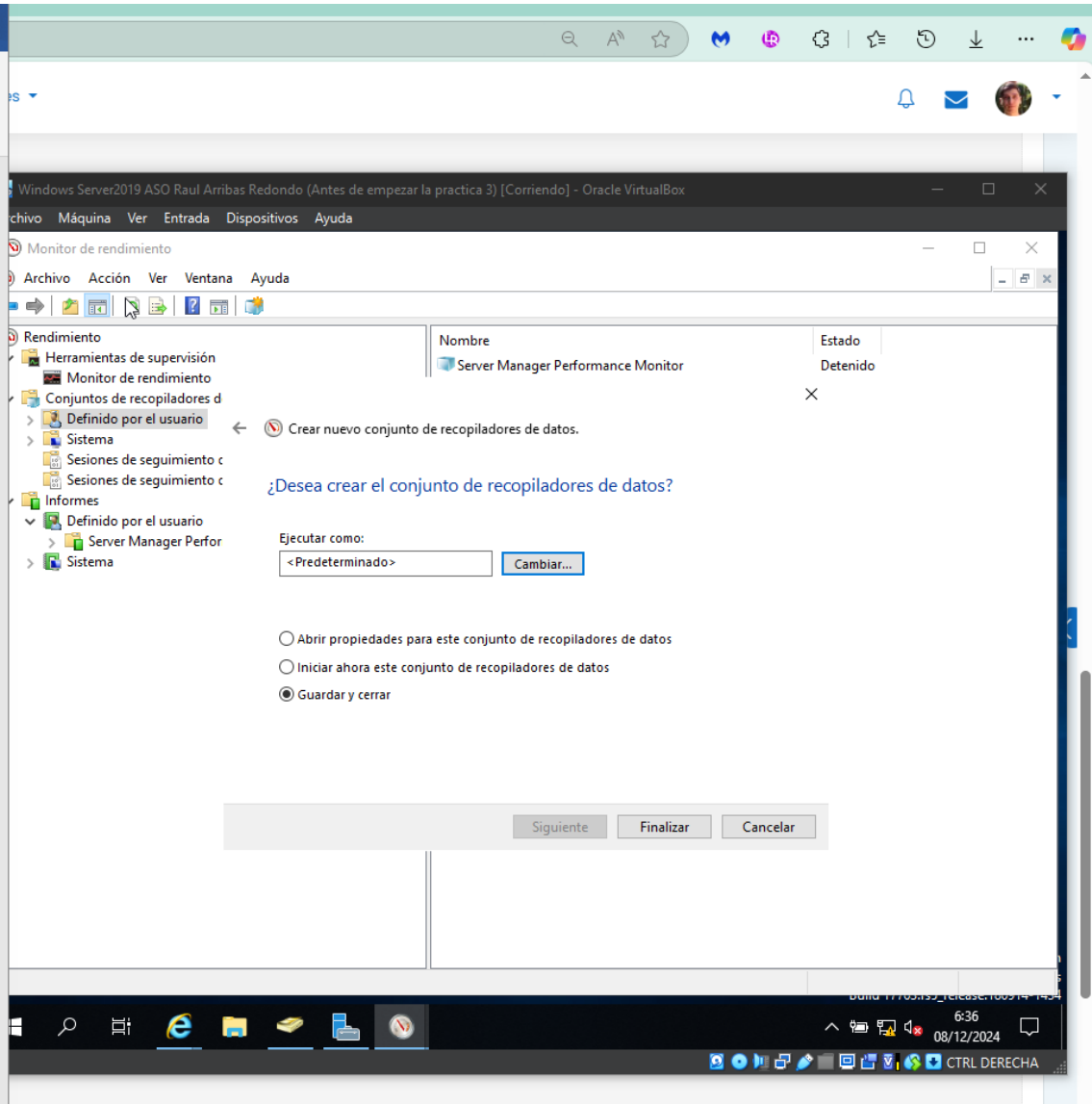




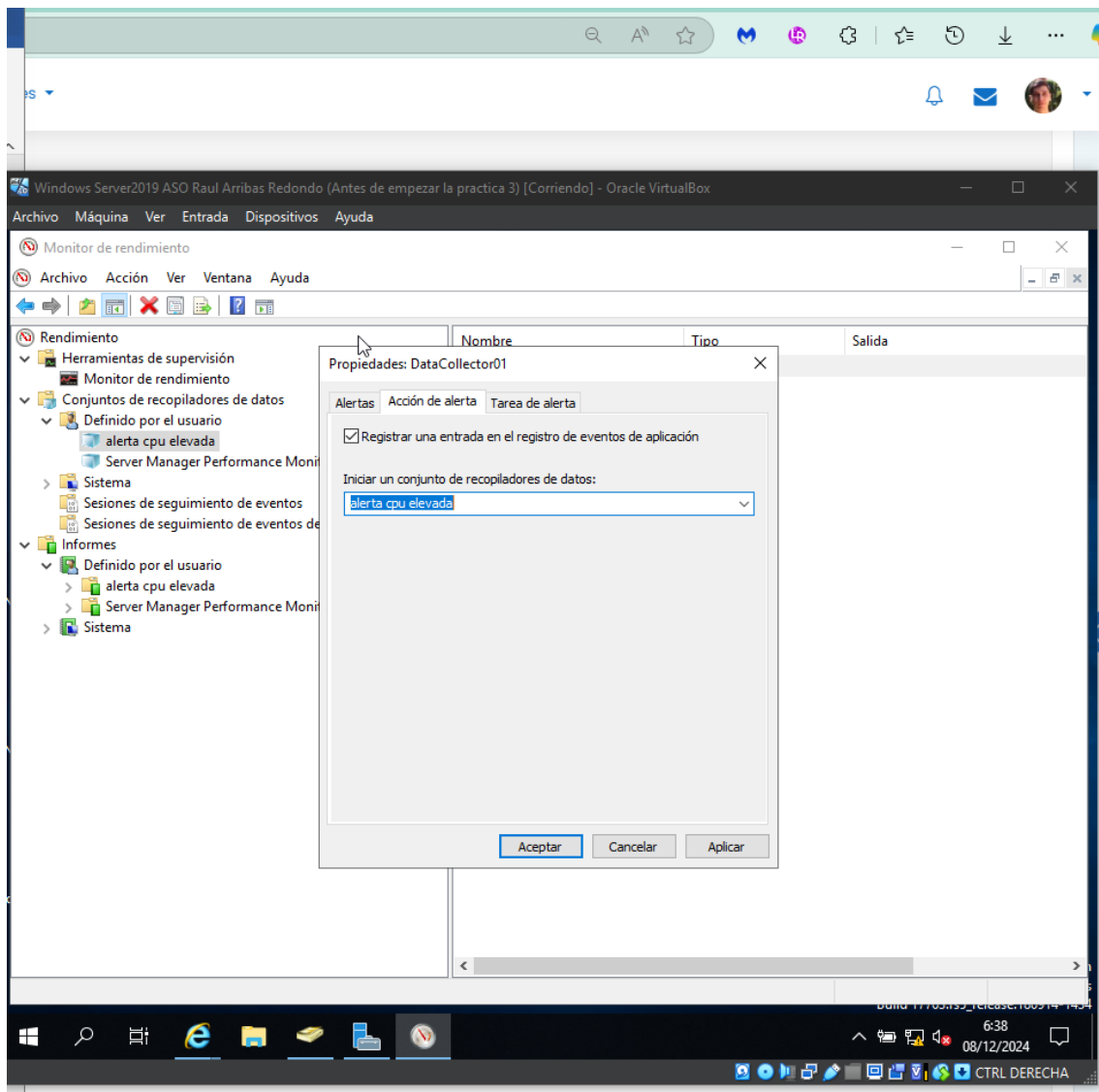
Agregamos el procesador:





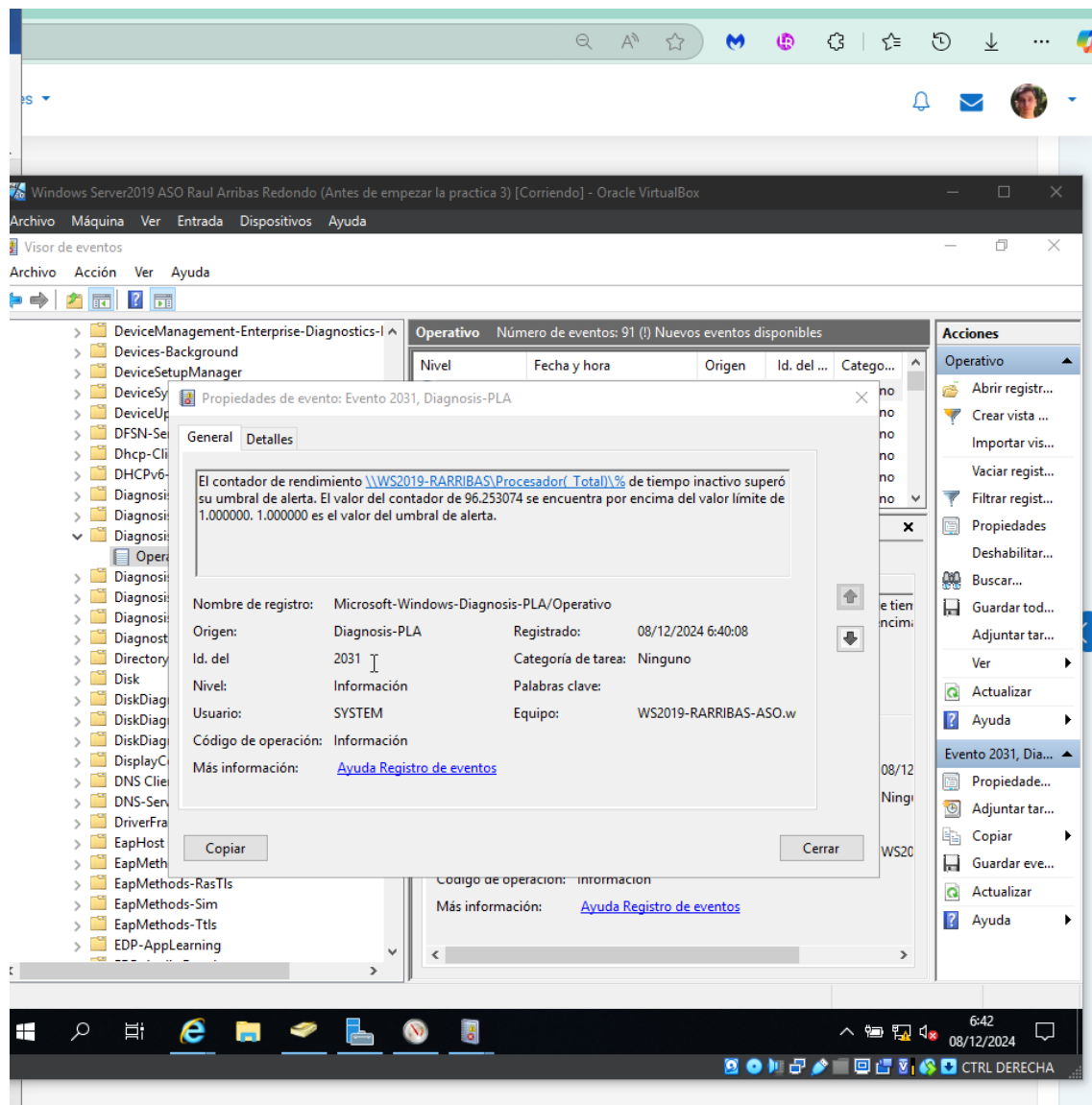


Abrimos la alerta que hemos creado y pinchamos en DataCollector01, propiedades:



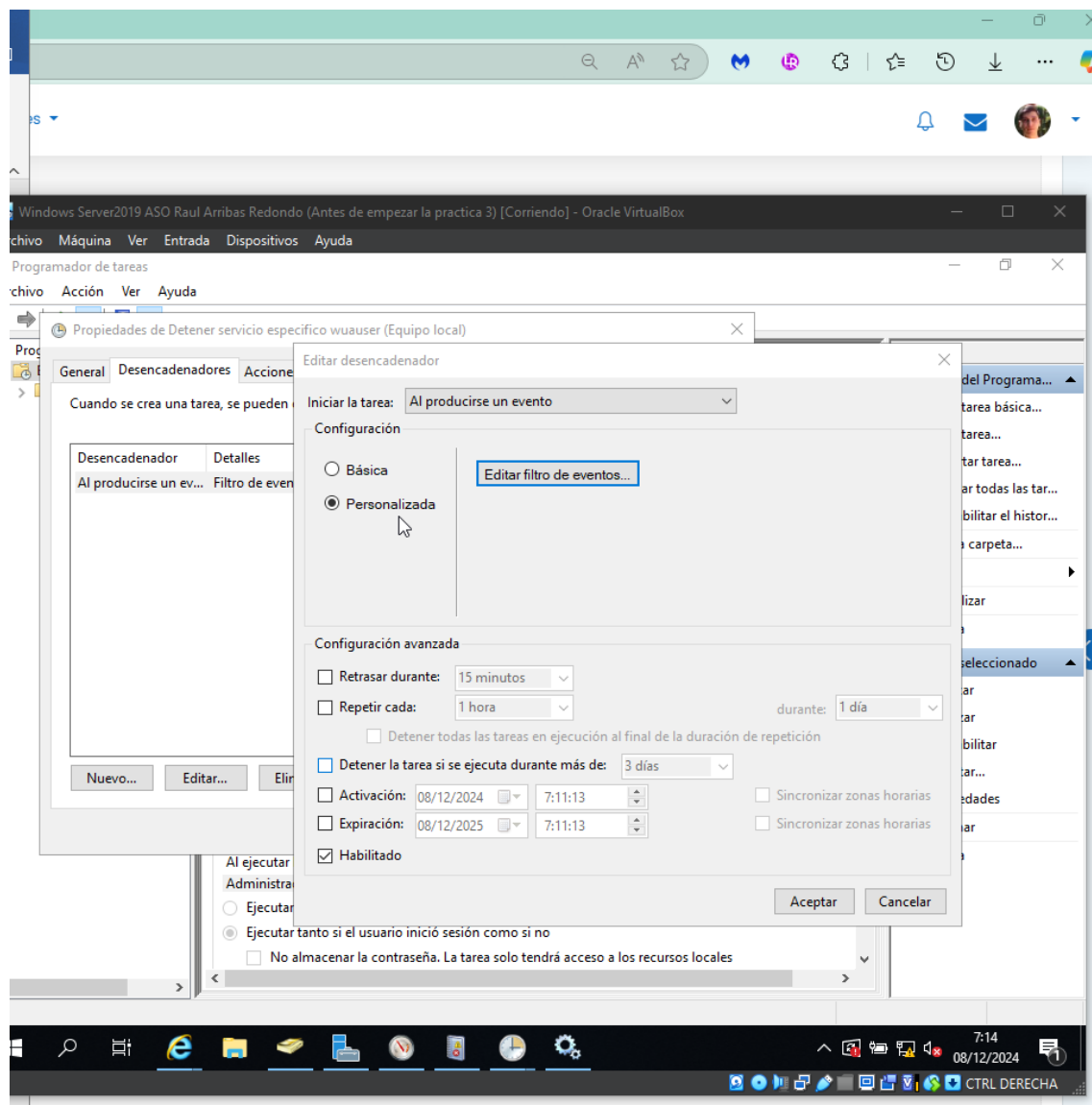
### 3.2 Forzar el uso elevado de la CPU y localizar el evento

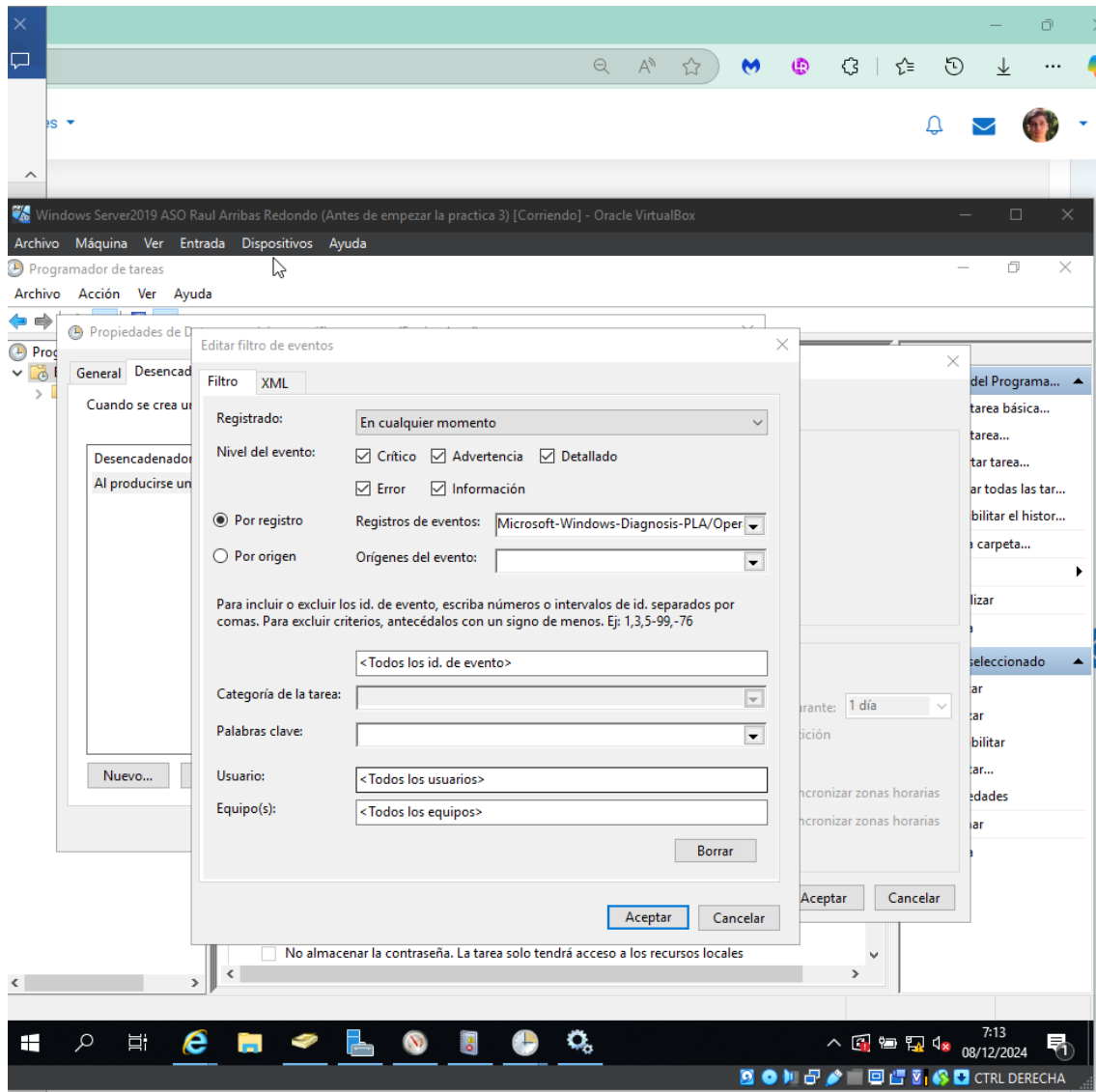
En el visor de eventos Registro de Aplicaciones y servicios → Microsoft → Windows → Diagnostic-PLA → Operativo



### 3.3 Crear tarea asociada para detener servicios

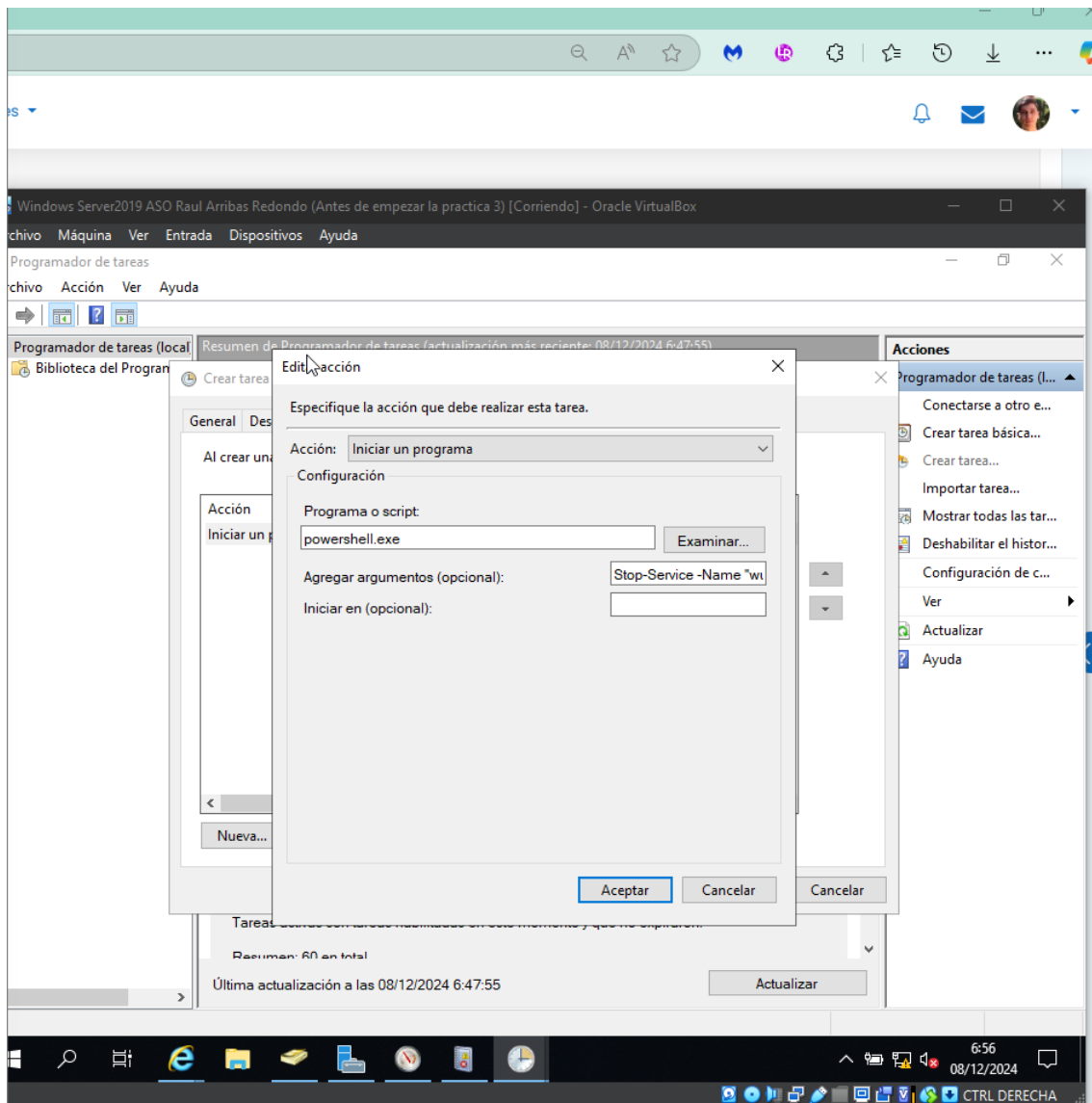
Abrimos el programador de tareas, creamos nueva tarea y ponemos lo siguiente:





Como hemos puesto anteriormente que el procesador tiene que pasar del 1% para que se ejecute la tarea, tenemos que comprobar que se ha ejecutado correctamente, y que el servicio de wuauser está detenido:

Nos vamos a la pestaña de acciones y escribimos lo siguiente:



powershell.exe

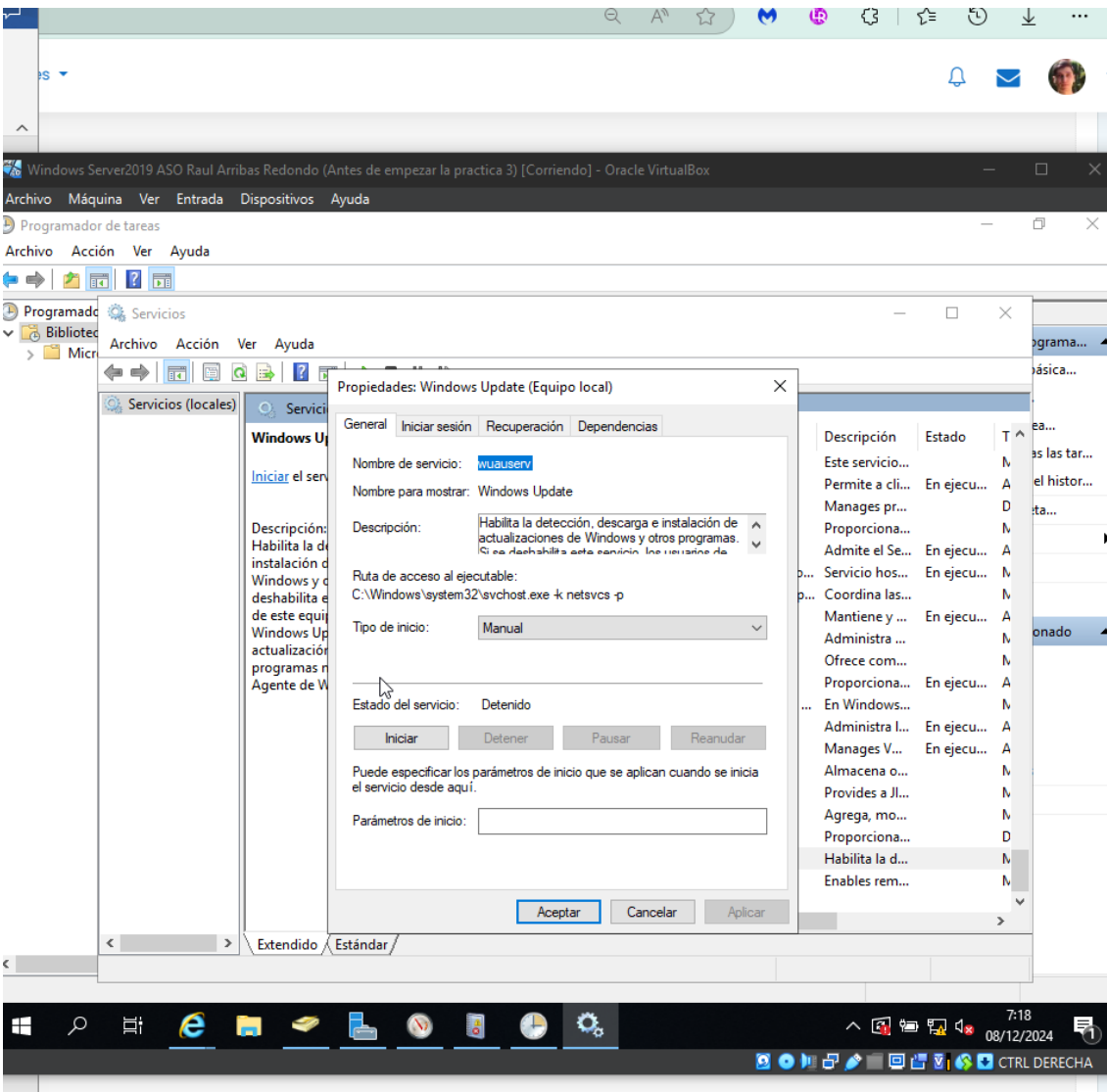
Stop-Service -Name "wuau servicing"

### 3.4 Verificar que la tarea funciona correctamente

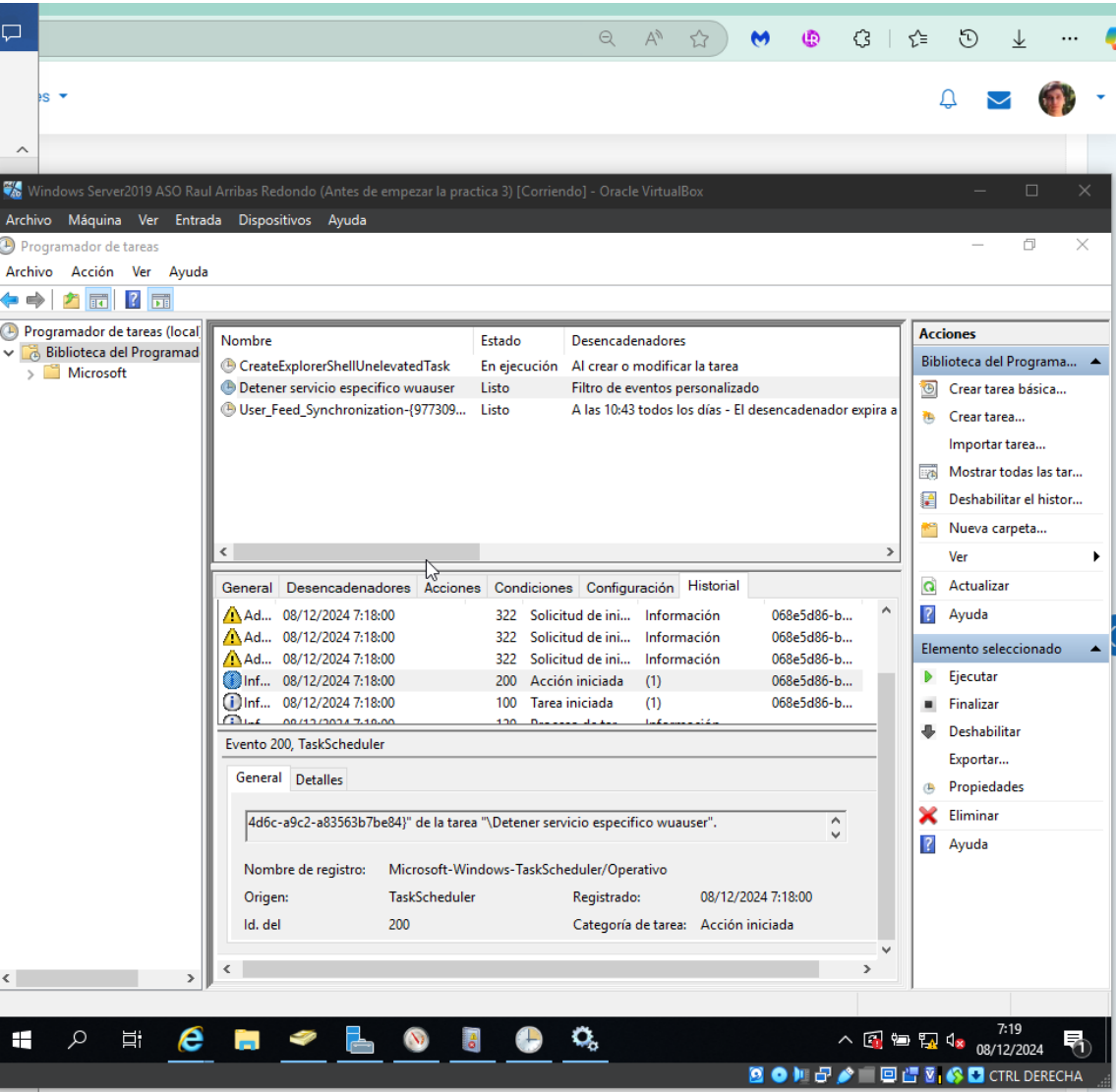
Iniciamos la alerta cpu elevada que creamos anteriormente en el monitor de rendimiento.

Abrimos services.msc y comprobamos si el servicio de Windows update está inactivo:

## Monitorización de Sistemas Operativos



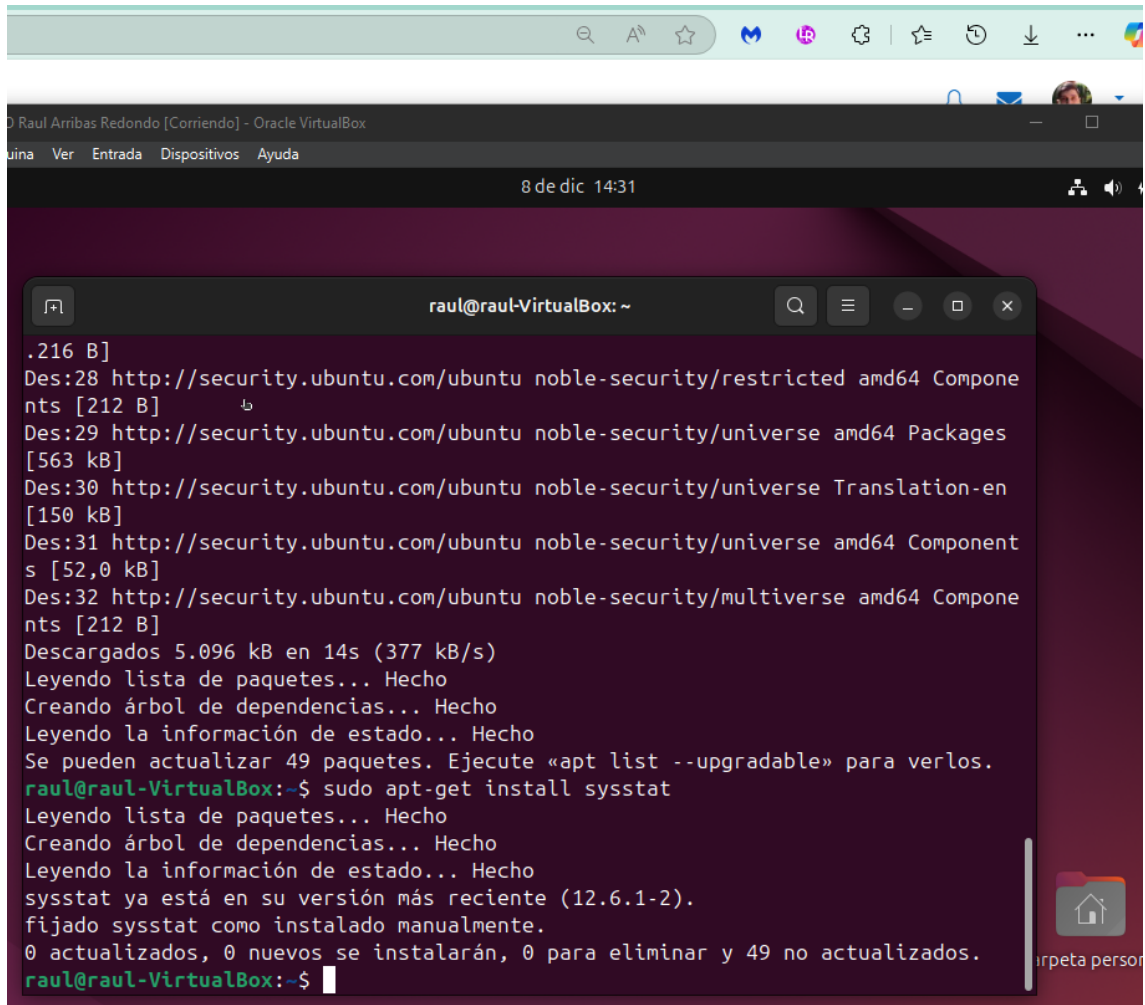
Como vemos la tarea se ha ejecutado correctamente y ha parado el servicio de Windows update.



## 4 Apartado 4: Rendimiento en sistemas GNU/Linux

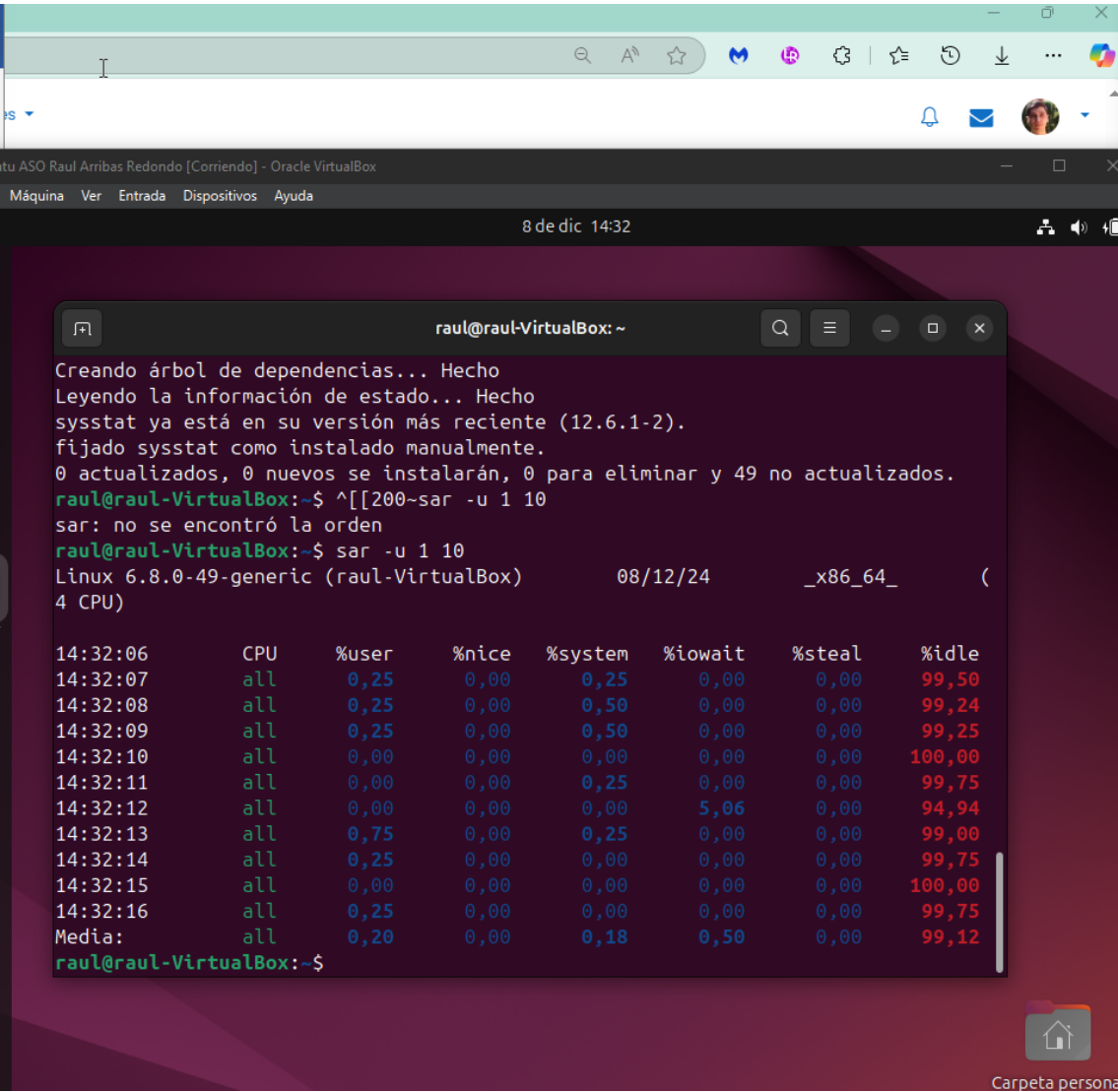
### 4.1 Instalar la herramienta SYSSTAT

**sudo apt-get install sysstat**



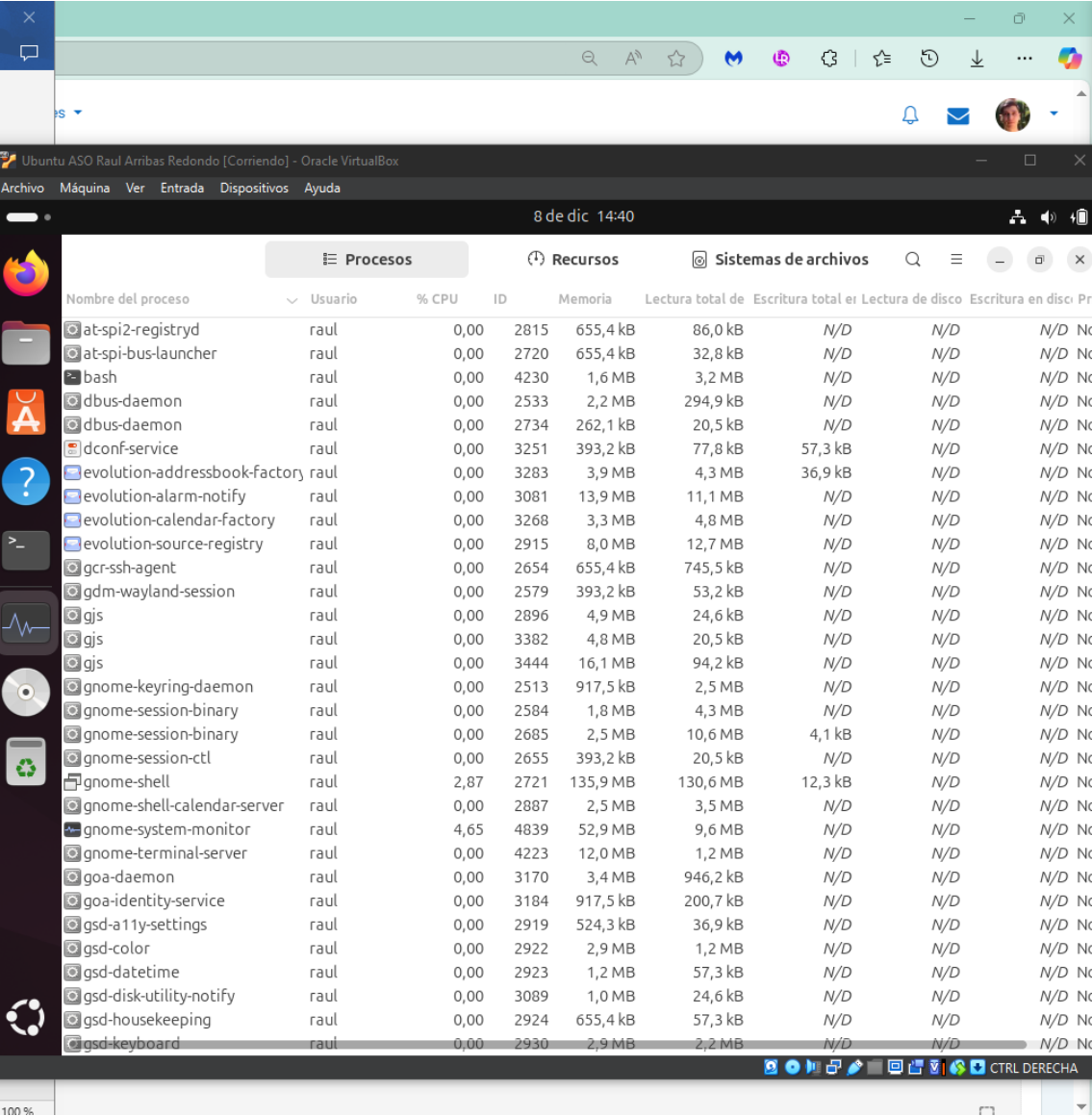
```
raul@raul-VirtualBox: ~  
.216 B]  
Des:28 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Compone  
nts [212 B]  
Des:29 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages  
[563 kB]  
Des:30 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en  
[150 kB]  
Des:31 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Component  
s [52,0 kB]  
Des:32 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Compone  
nts [212 B]  
Descargados 5.096 kB en 14s (377 kB/s)  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
Se pueden actualizar 49 paquetes. Ejecute «apt list --upgradable» para verlos.  
raul@raul-VirtualBox:~$ sudo apt-get install sysstat  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias... Hecho  
Leyendo la información de estado... Hecho  
sysstat ya está en su versión más reciente (12.6.1-2).  
fijado sysstat como instalado manualmente.  
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 49 no actualizados.  
raul@raul-VirtualBox:~$
```

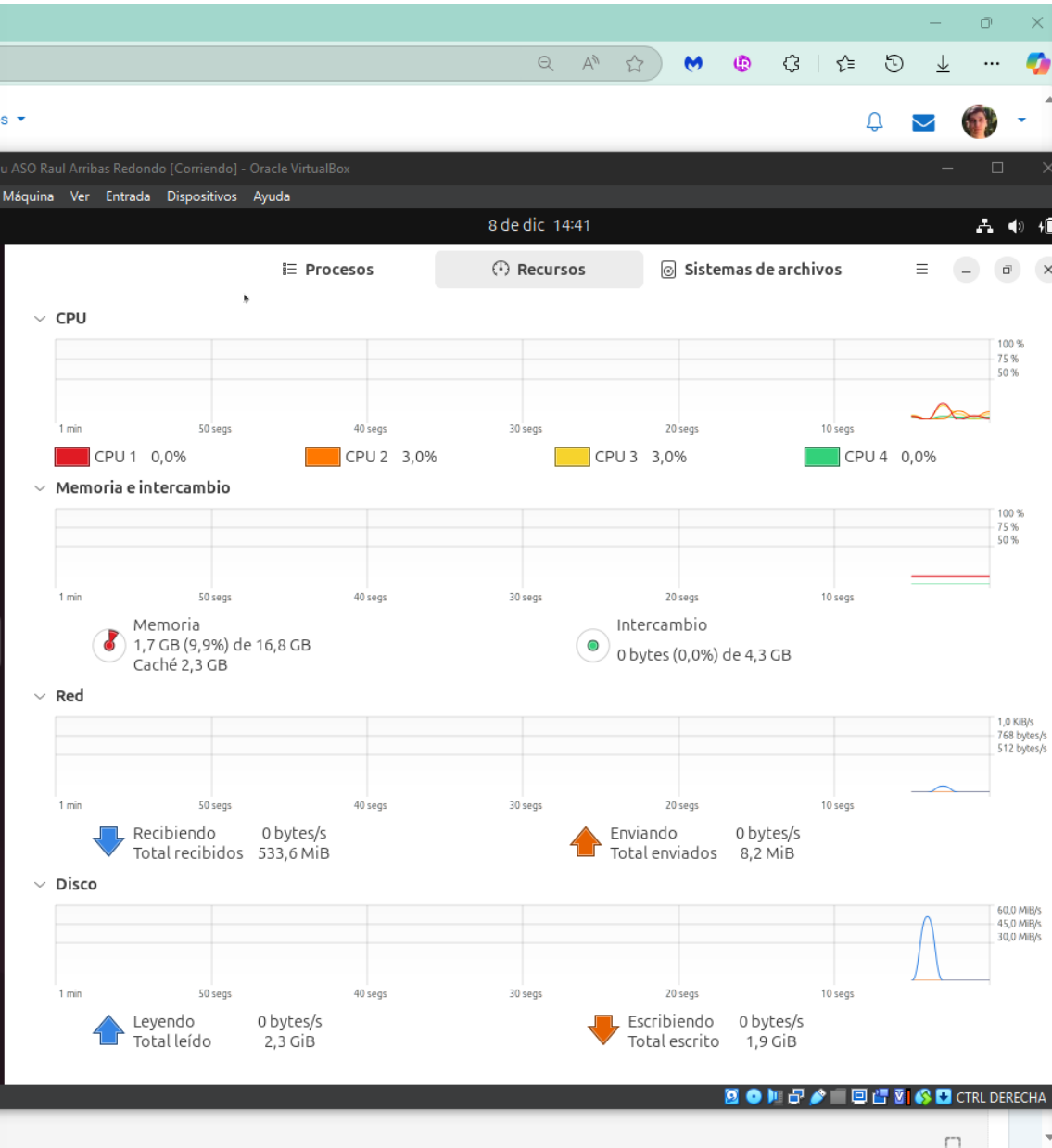
4.2 Recopilar datos de rendimiento del sistema

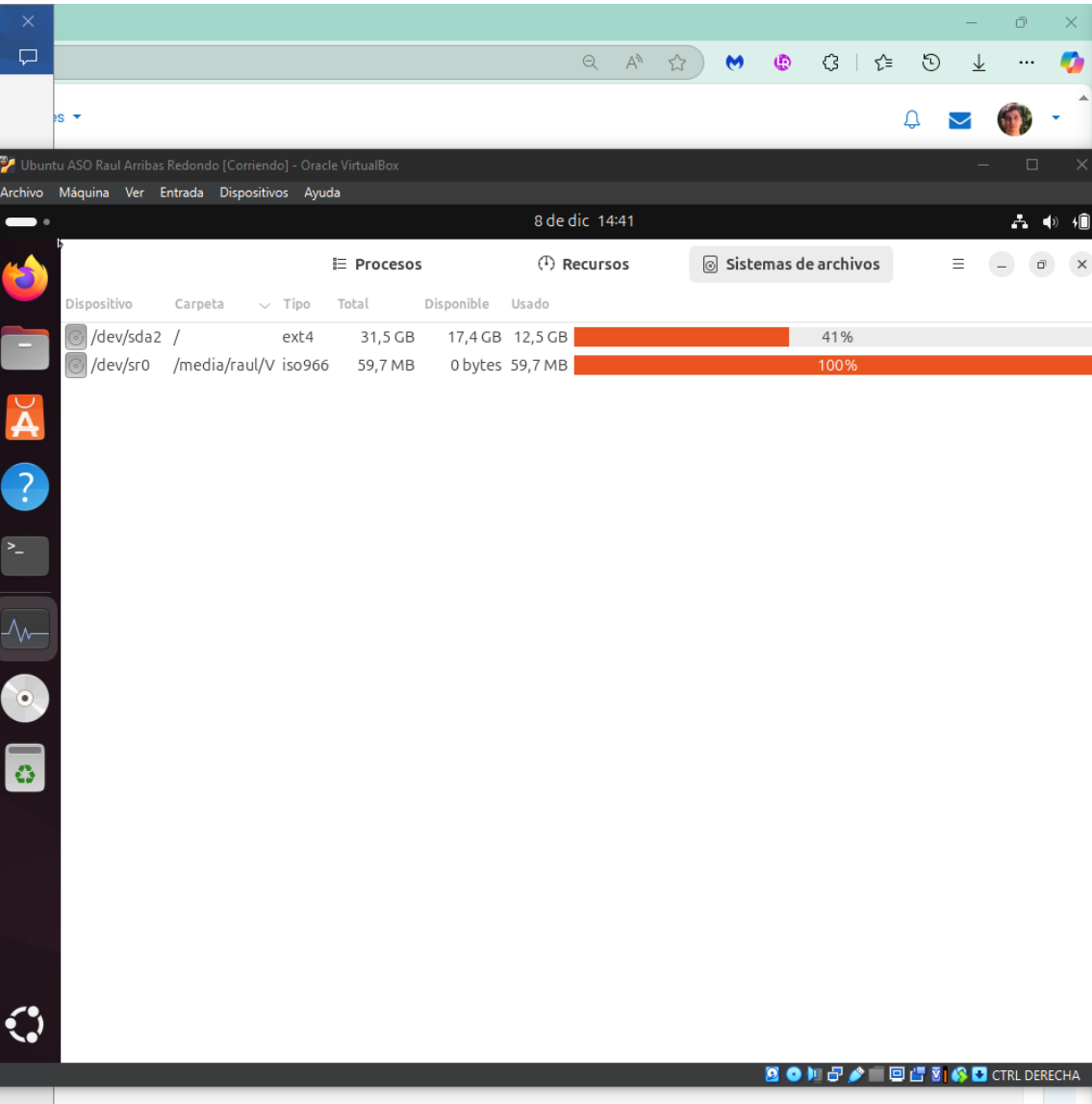


4.3 Instalar herramienta gráfica para interpretar los datos

`sudo apt-get install gnome-system-monitor`





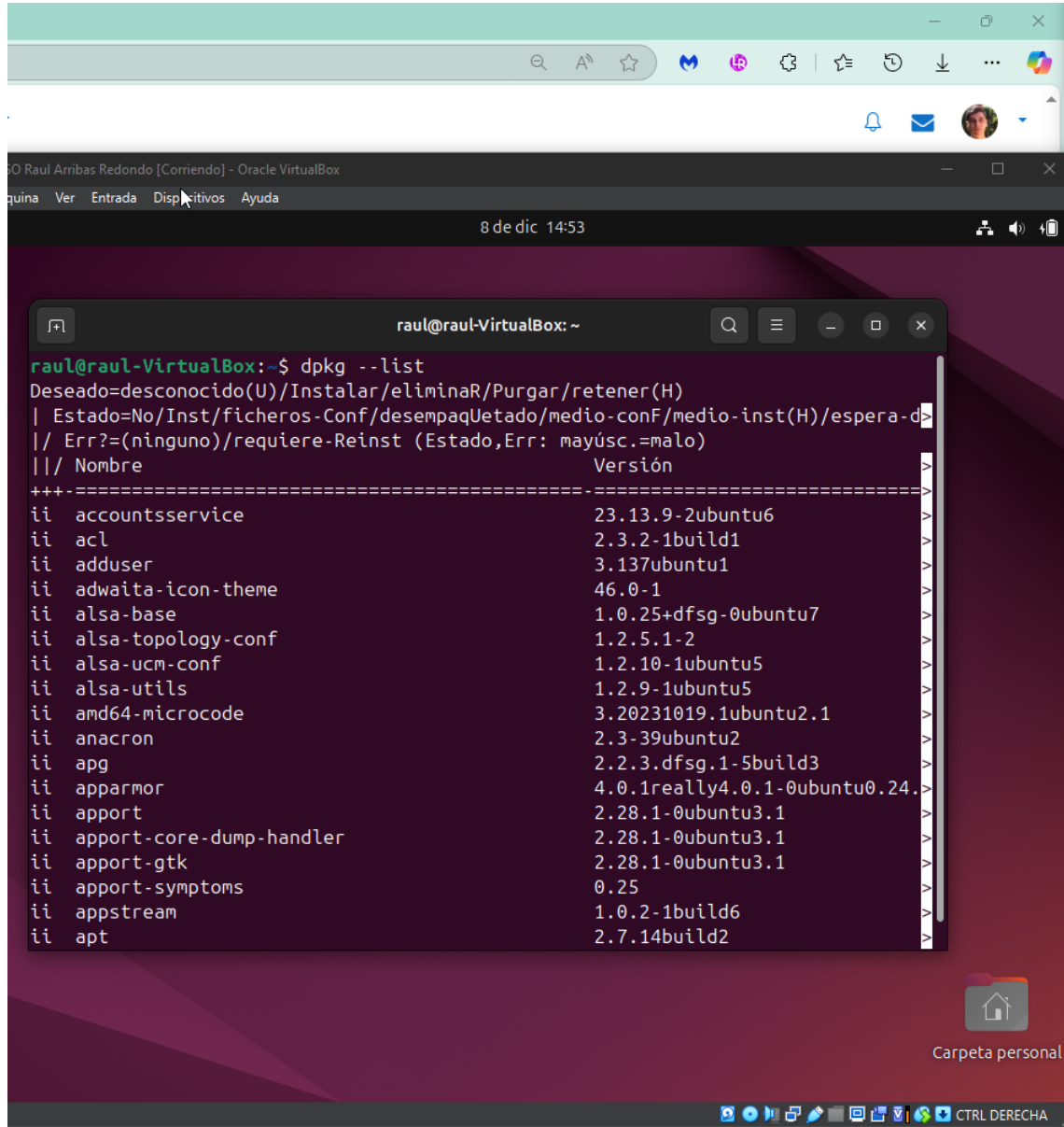


## 5 Apartado 5: Administración del sistema GNU/Linux

### 5.1 Listar los paquetes del sistema y buscar detalles del paquete cron

Listar los paquetes del sistema:

`dpkg --list`

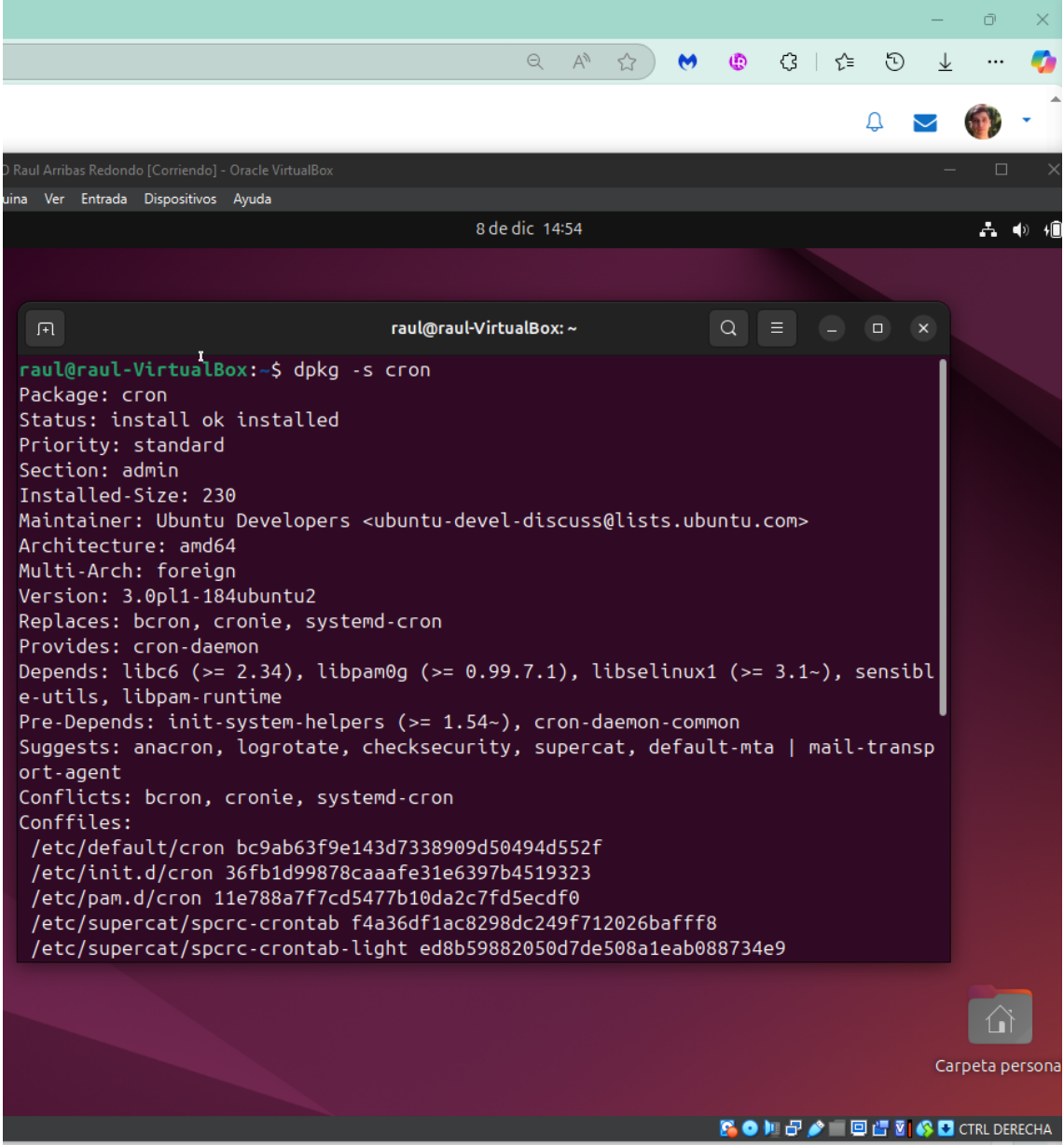


```

raul@raul-VirtualBox:~$ dpkg --list
Deseado=desconocido(U)/Instalar/eliminar/Purgar/retener(H)
| Estado=No/Inst/ficheros-Conf/desempaquetado/medio-conf/medio-inst(H)/espera-d
|/ Err?=(ninguno)/requiere-Reinst (Estado,Err: mayúsc.=malo)
|// Nombre                               Versión
+++-----+-----+-----+-----+-----+-----+-----+-----+-----+
ii accountsservice                       23.13.9-2ubuntu6
ii acl                                   2.3.2-1build1
ii adduser                               3.137ubuntu1
ii adwaita-icon-theme                    46.0-1
ii alsa-base                             1.0.25+dfsg-0ubuntu7
ii alsa-topology-conf                    1.2.5.1-2
ii alsa-ucm-conf                         1.2.10-1ubuntu5
ii alsa-utils                            1.2.9-1ubuntu5
ii amd64-microcode                       3.20231019.1ubuntu2.1
ii anacron                               2.3-39ubuntu2
ii apg                                   2.2.3.dfsg.1-5build3
ii apparmor                              4.0.1really4.0.1-0ubuntu0.24.
ii apport                                2.28.1-0ubuntu3.1
ii apport-core-dump-handler              2.28.1-0ubuntu3.1
ii apport-gtk                            2.28.1-0ubuntu3.1
ii apport-symptoms                       0.25
ii appstream                             1.0.2-1build6
ii apt                                    2.7.14build2
  
```

Buscar detalles del paquete cron:

`dpkg -s cron`



The screenshot shows a terminal window titled 'raul@raul-VirtualBox: ~' running the command `dpkg -s cron`. The output displays the following details for the 'cron' package:

```
raul@raul-VirtualBox:~$ dpkg -s cron
Package: cron
Status: install ok installed
Priority: standard
Section: admin
Installed-Size: 230
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Architecture: amd64
Multi-Arch: foreign
Version: 3.0pl1-184ubuntu2
Replaces: bcron, cronie, systemd-cron
Provides: cron-daemon
Depends: libc6 (>= 2.34), libpam0g (>= 0.99.7.1), libselinux1 (>= 3.1~), sensible-utils, libpam-runtime
Pre-Depends: init-system-helpers (>= 1.54~), cron-daemon-common
Suggests: anacron, logrotate, checksecurity, supercat, default-mta | mail-transfer-agent
Conflicts: bcron, cronie, systemd-cron
Conffiles:
 /etc/default/cron bc9ab63f9e143d7338909d50494d552f
 /etc/init.d/cron 36fb1d99878caaafe31e6397b4519323
 /etc/pam.d/cron 11e788a7f7cd5477b10da2c7fd5ecdf0
 /etc/supercat/spcrc-crontab f4a36df1ac8298dc249f712026bafff8
 /etc/supercat/spcrc-crontab-light ed8b59882050d7de508a1eab088734e9
```

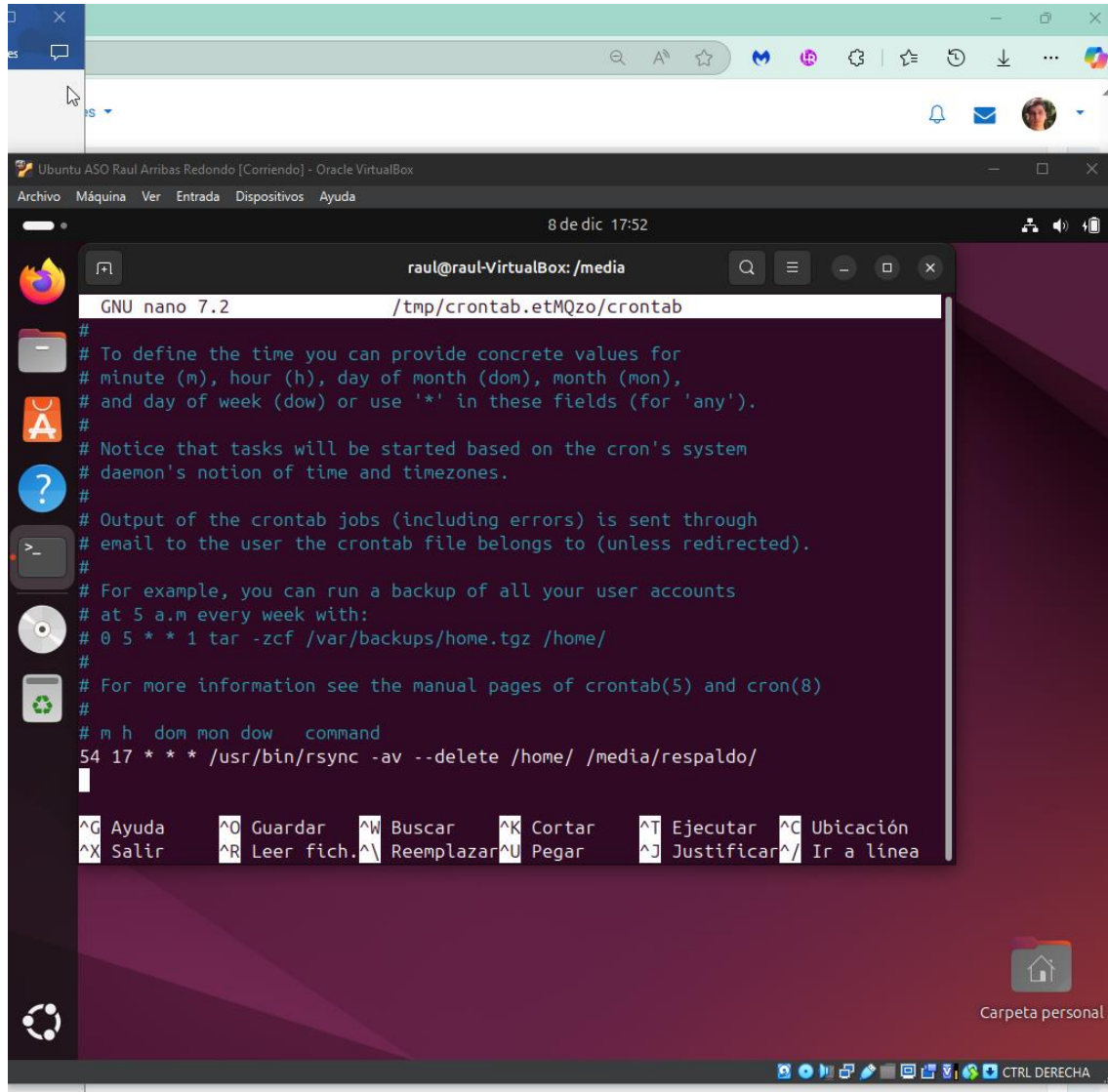
## 5.2 Crear tarea para copia de seguridad con rsync

Editamos el archivo de Cron:

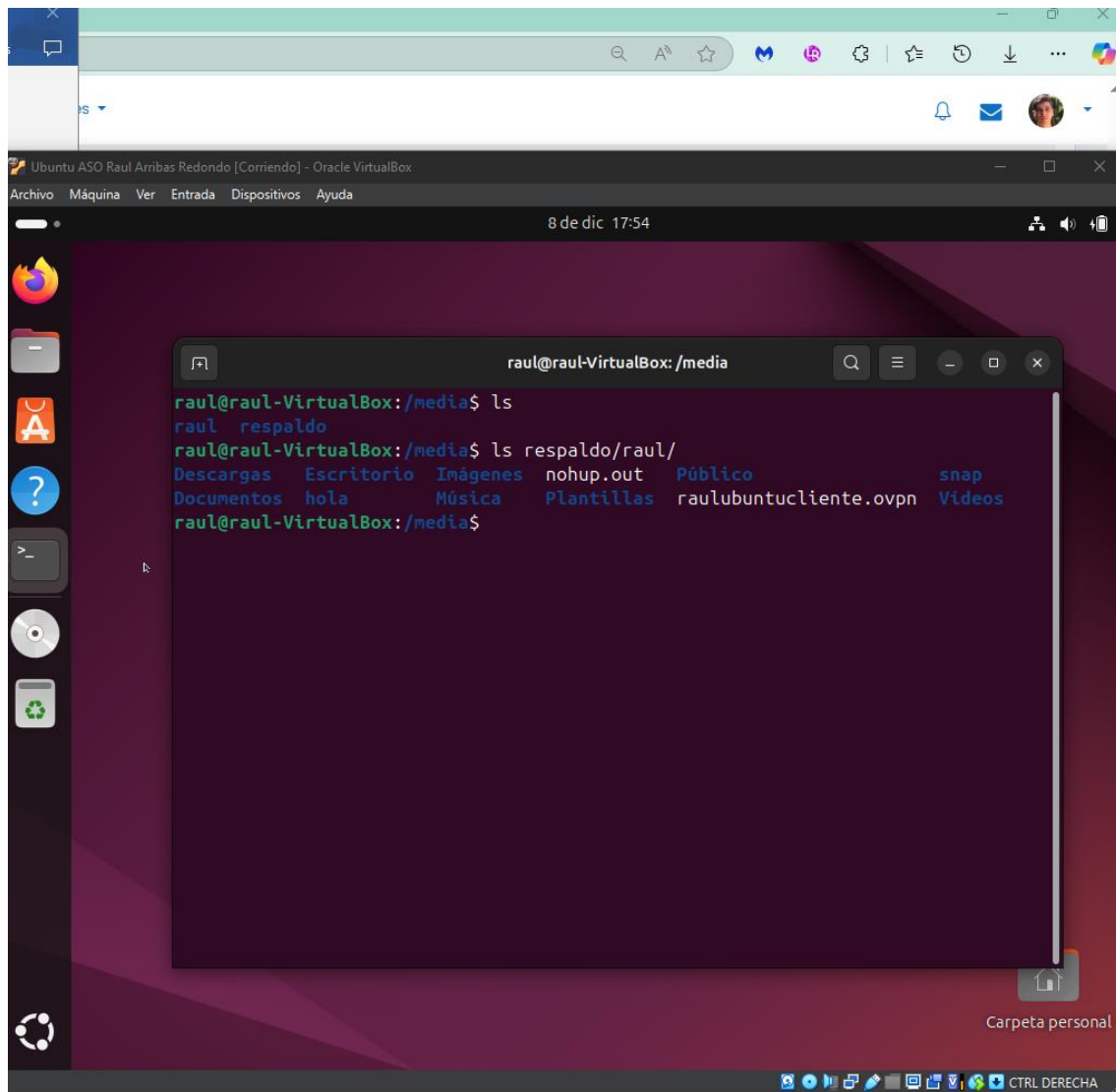
Sudo crontab -e

Añadimos la siguiente línea al archivo:

```
54 17 * * * /usr/bin/rsync -av --delete /home/ /media/respaldo/
```

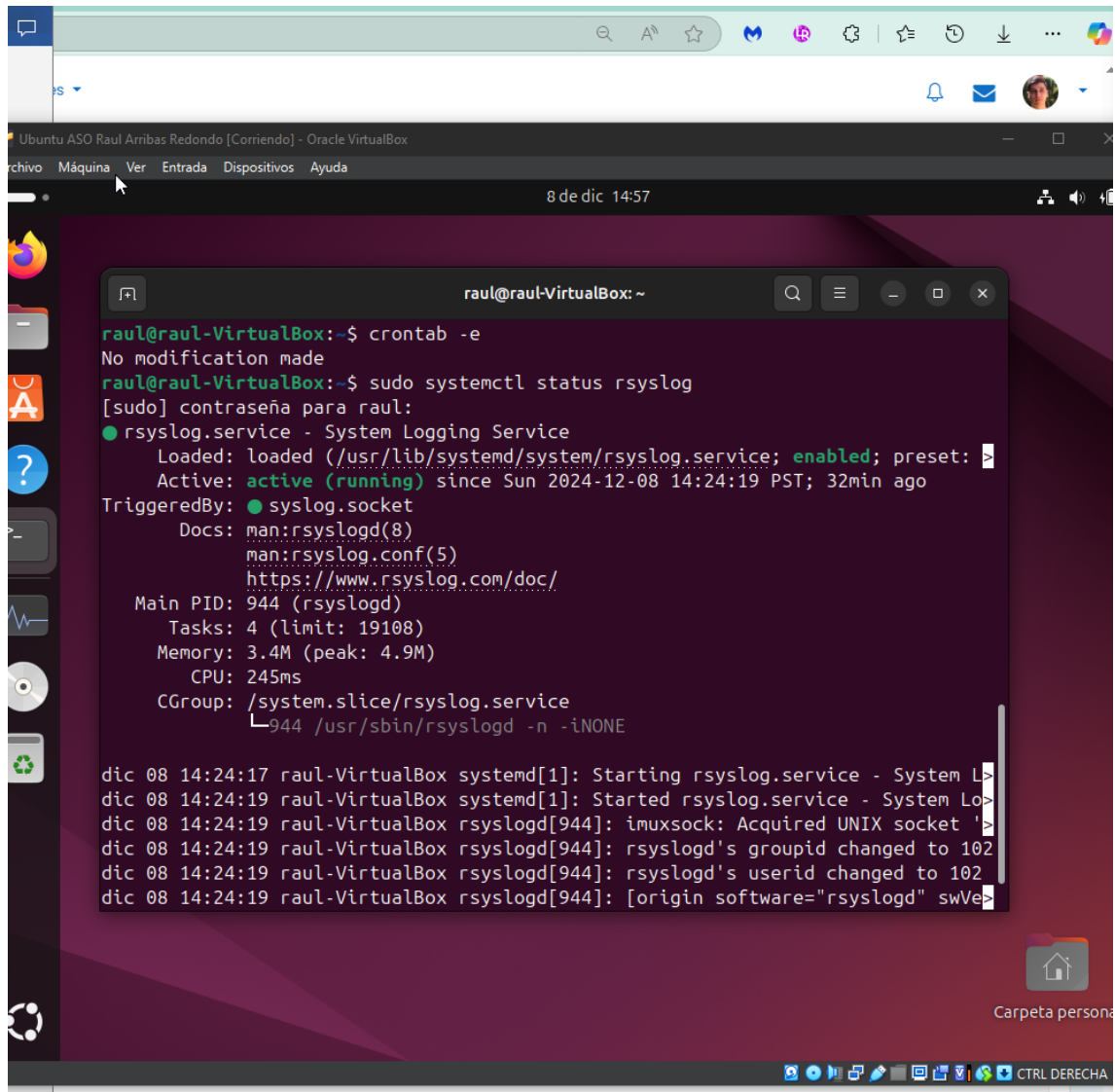


Vemos que nos ha generado la carpeta de raul en la ruta que hemos indicado en el cron.



### 5.3 Verificar registros del sistema para cron

`sudo systemctl status Rsyslog`



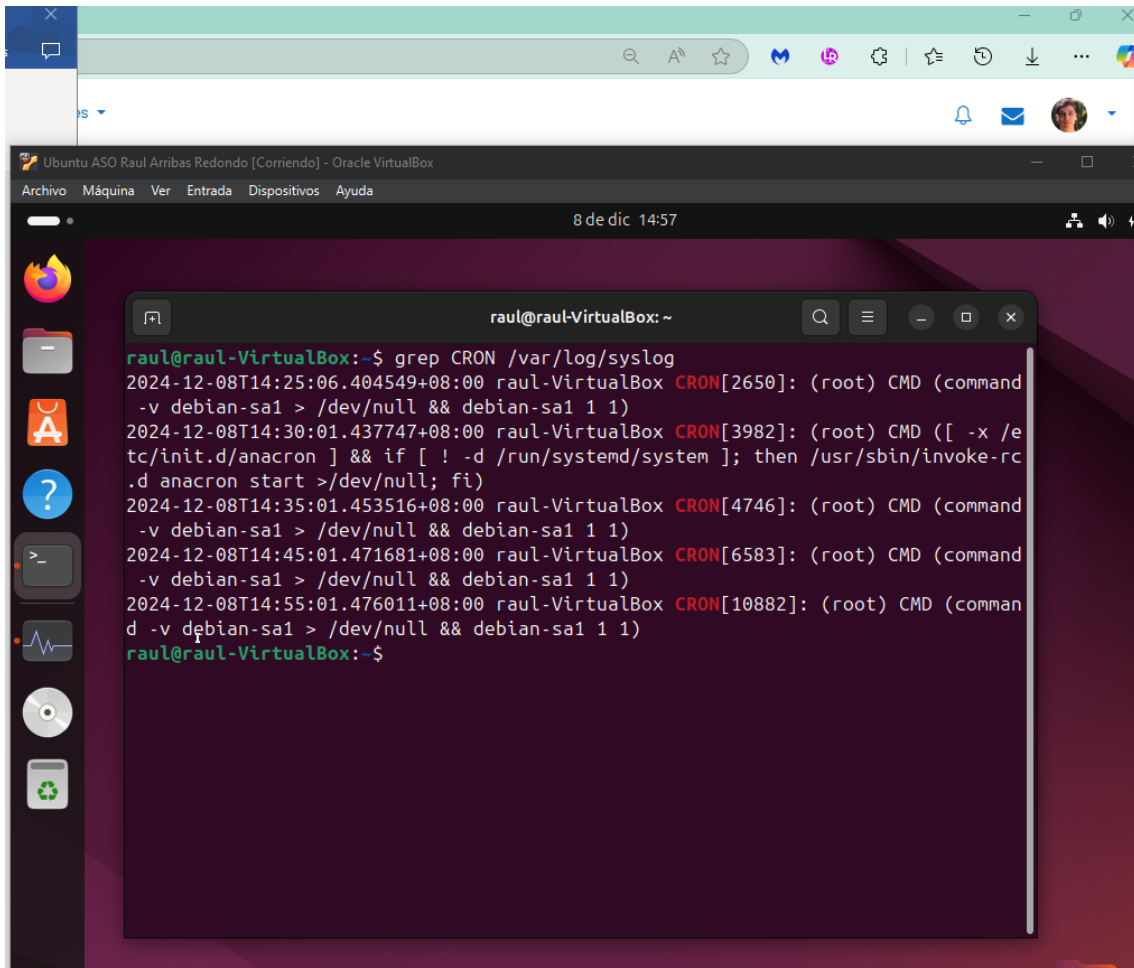
The screenshot shows a terminal window titled "raul@raul-VirtualBox: ~" running commands to check the status of the rsyslog service. The terminal output shows that the service is active and running. The terminal window is open on a desktop environment with a dark purple background. The desktop has a sidebar on the left with icons for applications like Firefox, LibreOffice, and a help icon. The top of the window shows the Oracle VM VirtualBox title bar with the name "Ubuntu ASO Raul Arribas Redondo [Corriendo] - Oracle VirtualBox" and a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". The system clock shows "8 de dic 14:57".

```
raul@raul-VirtualBox:~$ crontab -e
No modification made
raul@raul-VirtualBox:~$ sudo systemctl status rsyslog
[sudo] contraseña para raul:
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset:
   Active: active (running) since Sun 2024-12-08 14:24:19 PST; 32min ago
   TriggeredBy: ● syslog.socket
     Docs: man:rsyslogd(8)
           man:rsyslog.conf(5)
           https://www.rsyslog.com/doc/
    Main PID: 944 (rsyslogd)
      Tasks: 4 (limit: 19108)
     Memory: 3.4M (peak: 4.9M)
        CPU: 245ms
    CGroup: /system.slice/rsyslog.service
            └─944 /usr/sbin/rsyslogd -n -iNONE

dic 08 14:24:17 raul-VirtualBox systemd[1]: Starting rsyslog.service - System L>
dic 08 14:24:19 raul-VirtualBox systemd[1]: Started rsyslog.service - System Lo>
dic 08 14:24:19 raul-VirtualBox rsyslogd[944]: imuxsock: Acquired UNIX socket '>
dic 08 14:24:19 raul-VirtualBox rsyslogd[944]: rsyslogd's groupid changed to 102
dic 08 14:24:19 raul-VirtualBox rsyslogd[944]: rsyslogd's userid changed to 102
dic 08 14:24:19 raul-VirtualBox rsyslogd[944]: [origin software="rsyslogd" swVe>
```

## 5.4 Comprobar los logs

grep CRON /var/log/syslog



```
raul@raul-VirtualBox: ~  
raul@raul-VirtualBox:~$ grep CRON /var/log/syslog  
2024-12-08T14:25:06.404549+08:00 raul-VirtualBox CRON[2650]: (root) CMD (command  
-v debian-sa1 > /dev/null && debian-sa1 1 1)  
2024-12-08T14:30:01.437747+08:00 raul-VirtualBox CRON[3982]: (root) CMD ([ -x /e  
tc/init.d/anacron ] && if [ ! -d /run/systemd/system ]; then /usr/sbin/invoke-rc  
.d anacron start >/dev/null; fi)  
2024-12-08T14:35:01.453516+08:00 raul-VirtualBox CRON[4746]: (root) CMD (command  
-v debian-sa1 > /dev/null && debian-sa1 1 1)  
2024-12-08T14:45:01.471681+08:00 raul-VirtualBox CRON[6583]: (root) CMD (command  
-v debian-sa1 > /dev/null && debian-sa1 1 1)  
2024-12-08T14:55:01.476011+08:00 raul-VirtualBox CRON[10882]: (root) CMD (command  
-v debian-sa1 > /dev/null && debian-sa1 1 1)  
raul@raul-VirtualBox:~$
```

## 6 Apartado 6: Monitorización de sistemas en red

### 6.1 Instalar un sistema de monitorización

Descargamos los paquetes necesarios para instalar Nagios Core:

```
sudo apt install wget unzip vim curl gcc openssl build-essential libgd-dev libssl-dev  
libapache2-mod-php php-gd php apache2
```

```
sudo apt install -y apache2 php libapache2-mod-php build-essential libgd-dev
```

Descargamos la última version desde la pagina oficial:

```
wget https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.5.8.tar.gz
```

Extraemos y ejecutamos:

```
tar -xvzf nagios-4.x.x.tar.gz
```

```
cd nagios-4.x.x
```

```
./configure
```

```
make all
```

```
sudo make install
```

```
sudo make install-commandmode
```

```
sudo make install-init
```

Configuramos Nagios:

```
sudo make install-webconf
```

```
sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

```
sudo a2enmod rewrite cgi
```

```
sudo systemctl restart apache2
```

6.2 Ejecutar tareas de monitorización

Entramos en la web

Localhost/nagios

Y dentro de Services, podemos ver que el servicio ssh que hemos parado está como critico

The screenshot shows the Nagios web interface in a browser window. The address bar shows 'localhost/nagios/'. The interface includes a sidebar with navigation links like 'General', 'Current Status', 'Problems', 'Reports', and 'System'. The main content area displays 'Current Network Status', 'Host Status Totals', 'Service Status Totals', and a detailed table of 'Service Status Details For All Hosts'. In this table, the 'SSH' service is marked as 'CRITICAL'.

| Host      | Service         | Status   | Last Check          | Duration      | Attempt | Status Information                                                   |
|-----------|-----------------|----------|---------------------|---------------|---------|----------------------------------------------------------------------|
| localhost | Current Load    | OK       | 12-08-2024 18:58:01 | 0d 0h 14m 13s | 1/4     | OK - load average: 0.35, 0.50, 0.56                                  |
|           | Current Users   | OK       | 12-08-2024 18:58:39 | 0d 0h 13m 35s | 1/4     | USERS OK - 2 users currently logged in                               |
|           | HTTP            | OK       | 12-08-2024 18:59:16 | 0d 0h 12m 58s | 1/4     | HTTP OK: HTTP/1.1 200 OK - 10945 bytes in 0.001 second response time |
|           | PING            | OK       | 12-08-2024 18:59:54 | 0d 0h 12m 20s | 1/4     | PING OK - Packet loss = 0%, RTA = 0.04 ms                            |
|           | Root Partition  | OK       | 12-08-2024 19:00:31 | 0d 0h 11m 43s | 1/4     | DISK OK - free space: / 8572 MiB (30,06% inode=88%):                 |
|           | SSH             | CRITICAL | 12-08-2024 19:02:09 | 0d 0h 0m 5s   | 1/4     | connect to address 127.0.0.1 and port 22: Conexión rehusada          |
|           | Swap Usage      | OK       | 12-08-2024 19:01:46 | 0d 0h 10m 28s | 1/4     | SWAP OK - 100% free (4095 MB out of 4095 MB)                         |
|           | Total Processes | OK       | 12-08-2024 18:57:24 | 0d 0h 9m 50s  | 1/4     | PROCS OK: 59 processes with STATE = RSZDT                            |

Si lo activamos de nuevo ya nos salo como OK

ASO Raul Arribas Redondo [Corriendo] - Oracle VirtualBox

ArchivoMáquinaVerEntradaDispositivosAyuda

8 de dic 19:04

Nagios: localhost

localhost/nagios/

# Nagios®

General

Home

Documentation

Current Status

Tactical Overview

Map

Hosts

Services

Host Groups

Summary

Grid

Service Groups

Summary

Grid

Problems

Services (Unhandled)

Hosts (Unhandled)

Network Outages

Quick Search:

Reports

Availability

Trends

Alerts

History

Summary

Histogram

Notifications

Event Log

System

Comments

Downtime

Process Info

Performance Info

Current Network Status

Last Updated: Sun Dec 8 19:04:21 PST 2024

Updated every 90 seconds

Nagios® Core™ 4.5.6 - www.nagios.org

Logged in as raul

View History For all hosts

View Notifications For All Hosts

View Host Status Detail For All Hosts

Host Status Totals

UpDownUnreachablePending

1000

All ProblemsAll Types

01

Service Status Totals

OkWarningUnknownCriticalPending

8000

All ProblemsAll Types

08

Display Filters:

Host Status Types: All

Host Properties: Any

Service Status Types: Ok

Service Properties: Any

Limit Results: 100

| Host      | Service         | Status | Last Check          | Duration      | Attempt | Status Information                                                   |
|-----------|-----------------|--------|---------------------|---------------|---------|----------------------------------------------------------------------|
| localhost | Current Load    | OK     | 12-08-2024 19:03:01 | 0d 0h 16m 20s | 1/4     | OK - load average: 0.91, 0.66, 0.60                                  |
|           | Current Users   | OK     | 12-08-2024 19:03:39 | 0d 0h 15m 42s | 1/4     | USERS OK - 2 users currently logged in                               |
|           | HTTP            | OK     | 12-08-2024 19:04:16 | 0d 0h 15m 5s  | 1/4     | HTTP OK: HTTP/1.1 200 OK - 10945 bytes in 0,001 second response time |
|           | PING            | OK     | 12-08-2024 18:59:54 | 0d 0h 14m 27s | 1/4     | PING OK - Packet loss = 0%, RTA = 0.04 ms                            |
|           | Root Partition  | OK     | 12-08-2024 19:00:31 | 0d 0h 13m 50s | 1/4     | DISK OK - free space: / 8572 MiB (30,06% inode=88%):                 |
|           | SSH             | OK     | 12-08-2024 19:04:09 | 0d 0h 0m 12s  | 1/4     | SSH OK - OpenSSH_9.6p1 Ubuntu-3ubuntu13.5 (protocol 2.0)             |
|           | Swap Usage      | OK     | 12-08-2024 19:01:46 | 0d 0h 12m 35s | 1/4     | SWAP OK - 100% free (4095 MB out of 4095 MB)                         |
|           | Total Processes | OK     | 12-08-2024 19:02:24 | 0d 0h 11m 57s | 1/4     | PROCS OK: 59 processes with STATE = RSZDT                            |

Results 1 - 8 of 8 Matching Services

Page Tour