# ARQUITECTURA Y SISTEMAS OPERATIVOS

# TRABAJO PRÁCTICO: GESTIÓN DE SERVICIOS EN LOS SISTEMAS OPERATIVOS

## SUSSINI PATRICIO

# 1- Preparativos

# Entorno de trabajo:

Me encuentro usando una computadora fisica con windows 10, que corre una VM en virtualbox con una distro de Lubuntu.

#### **Herramientas Necesarias:**

Cuento con todas las herramientas instaladas en mi entorno de trabajo.

# **Configuracion:**

Tengo la totalidad de los servicios basicos por defecto corriendo en ambos setups. Salvo windows update en la fisica

2- Tareas

## **Exploración en Windows:**

- Listar servicios activos por defecto: **Powershell** 

```
PS C:\Users\paddy> Get-Service | Where-Object {$_.Status -eq "Running"}
Status
         Name
                               DisplayName
Running AdAppMgrSvc Autodesk Desktop App Service
Running AdskLicensingSe... Autodesk Desktop Licensing Service
Running AMD Crash Defen... AMD Crash Defender Service
Running AMD External Ev... AMD External Events Utility
Running Appinfo Application Information
Running AppXSvc AppX Deployment Service (App
                              AppX Deployment Service (AppXSVC)
Running asComSvc
                              ASUS Com Service
Running AsusFanControlS... AsusFanControlService
Running AudioEndpointBu... Windows Audio Endpoint Builder
Running Audiosrv
                              Windows Audio
Running Autodesk Access... Autodesk Access Service Host
Running BFE
                              Base Filtering Engine
Running BrokerInfrastru... Background Tasks Infrastructure Ser...
Running BTAGService Bluetooth Audio Gateway Service
Running BthAvctpSvc AVCTP service
Running bthserv
                              Bluetooth Support Service
Running camsvc
                             Capability Access Manager Service
Running CaptureService_... CaptureService_b5029
Running cbdhsvc_b5029 Clipboard User Service_b5029
Running CDPSvc Connected Devices Platform Service
Running CDPUserSvc_b5029 Connected Devices Platform User Ser...
Running ClickToRunSvc Microsoft Office Click-to-Run Service
Running CoreMessagingRe... CoreMessaging
                              Cryptographic Services
Running CryptSvc
Running DcomLaunch
                              DCOM Server Process Launcher
Running DeviceAssociati... Device Association Service
Running DeviceInstall Device Install Service
Running Dhcp
                              DHCP Client
Running DiagTrack
                             Connected User Experiences and Tele...
Running DispBrokerDeskt... Display Policy Service
Running Dnscache
                              DNS Client
Running DPS
                             Diagnostic Policy Service
                             Data Sharing Service
Running DsSvc
Running DusmSvc
                            Data Usage
Running EFS
                             Encrypting File System (EFS)
Running EventLog
                             Windows Event Log
Running EventLog Windows Event Log
Running EventSystem COM+ Event System
Running FlexNet Licensi... FlexNet Licensing Service
Running FontCache
                              Windows Font Cache Service
                             Gaming Services
Running GamingServices
Running GamingServicesNet Gaming Services
Running hidsery
                               Human Interface Device Service
Running IKEEXT
                               IKE and AuthIP IPsec Keying Modules
Running InputMapper Cer... InputMapper Cerberus Whitelister
```

- Listar servicios activos por defecto: Command Prompt

```
Select Administrator: Command Prompt
C:\Users\paddy>sc query | findstr "RUNNING"
        STATE
                                 RUNNING
                            : 4
        STATE
                                 RUNNING
                            : 4
        STATE
                                 RUNNING
        STATE
                                 RUNNING
        STATE
                            : 4
                                 RUNNING
                            : 4
        STATE
                                 RUNNING
        STATE
                           : 4
                                 RUNNING
        STATE
                            : 4
                                 RUNNING
        STATE
                                 RUNNING
        STATE
                            : 4
                                 RUNNING
                            : 4
        STATE
                                 RUNNING
        STATE
                            : 4 RUNNING
        STATE
                                 RUNNING
        STATE
                                 RUNNING
        STATE
                                 RUNNING
        STATE
                            : 4
                                 RUNNING
        STATE
                                 RUNNING
        STATE
                                 RUNNING
        STATE
                            : 4
                                 RUNNING
        STATE
                                 RUNNING
        STATE
                            : 4
                                 RUNNING
                           : 4
        STATE
                                 RUNNING
        STATE
                            : 4
                                 RUNNING
                            : 4
        STATE
                                 RUNNING
        STATE
                                 RUNNING
        STATE
                            : 4
                                 RUNNING
        STATE
                                 RUNNING
        STATE
                              4
                                 RUNNING
```

- Examinar parámetros de los servicios: Virtual Box

```
PS C:\Users\paddy> Get-Service -Name VBoxSDS_ Format-List
Name
                  : VBoxSDS
RequiredServices
                 : {RPCSS}
CanPauseAndContinue : False
             : False
CanShutdown
CanStop
                 : True
DisplayName
                 : VirtualBox system service
DependentServices : {}
MachineName : .
ServiceName
                 : VBoxSDS
ServicesDependedOn : {RPCSS}
ServiceHandle : SafeServiceHandle
Status
                 : Running
                 : Win32OwnProcess
ServiceType
StartType
                 : Manual
Site
Container
```

- Inspecciono configuraciones con PowerShell

DcomLaunch

defragsvc

DeviceInstall

DevQueryBroker

DeviceAssociationService

dcsvc

#### Administrator: Windows PowerShell PS C:\Users\paddy> Get-WmiObject Win32\_Service | Select-Object Name, StartMode, State Name StartMode State Running AdAppMgrSvc Auto AdskLicensingService AJRouter Auto Running Manual Stopped ALG Manual Stopped AMD Crash Defender Service Running Auto AMD External Events Utility Auto Running AppIDSvc Manual Stopped Appinfo Manual Running AppMgmt AppReadiness Stopped Manual Manual Stopped AppVClient Disabled Stopped AppXSvc Manual Running asComSvc Auto Running AssignedAccessManagerSvc Manual Stopped AsusFanControlService Auto Running AudioEndpointBuilder Auto Running Audiosrv Auto Running Autodesk Access Service Host Auto Running autotimesvc Manual Stopped AxInstSV BDESVC Stopped Manual Manual Stopped BEService Manual Stopped BFE Auto Running BITS Stopped Manual BrokerInfrastructure Auto Running BTAGService Manual Running BthAvctpSvc Manual Running bthserv Running Manual camsvc CDPSvc Manual Running Auto Running CertPropSvc Manual Stopped ClickToRunSvc ClipSVC Running Auto Stopped Manual cloudidsvc Manual Stopped COMSysApp Manual Stopped CoreMessagingRegistrar Running Auto CryptSvc CscService Running Auto Manual Stopped

Auto

Manual

Manual

Auto

Manual

Manua1

Running

Stopped

Stopped

Running

Running

Stopped

Analizo logs de eventos relacionados: Uso Get-EventLog

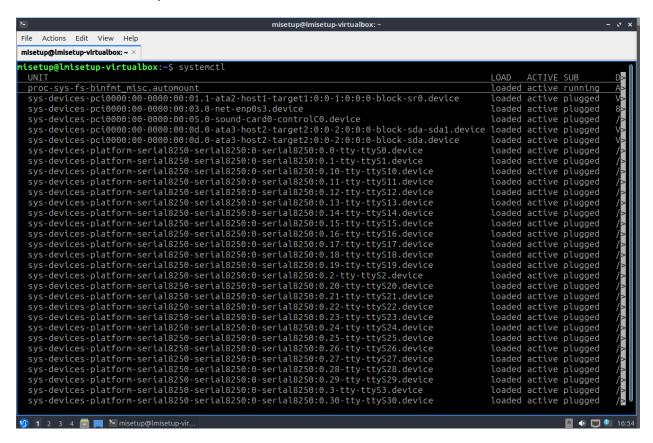
```
Administrator: Windows PowerShell
                                                                                6 File System Filter 'npsvctrig' (10.0, 2025-01-0...
6 File System Filter 'UCPD' (10.0, 1985-02-13T20:...
6 File System Filter 'FileCrypt' (10.0, 2002-03-0...
98 The description for Event ID '98' in Source 'Mi...
98 The description for Event ID '98' in Source 'Mi...
6 File System Filter 'WdFilter' (10.0, 2042-01-14...
6 File System Filter 'Wof' (10.0, 2090-03-16T15:5...
6 File System Filter 'FileInfo' (10.0, 2062-12-23...
2147489651 The system uptime is 10 seconds.
2147489657 Microsoft (R) Windows (R) 10.00. 19045 Multipr...
2147489656 The previous system shutdown at 3:46:57 PM on f...
                              Information Microsoft-Windows...
 150511 Aug 27 16:22
 150510 Aug 27 16:22
                              Information Microsoft-Windows...
 150509 Aug 27 16:22
                              Information Microsoft-Windows...
 150508 Aug 27 16:22
                              Information Microsoft-Windows...
 150507 Aug 27 16:22
                              Information Microsoft-Windows...
150506 Aug 27 16:22
150505 Aug 27 16:22
                              Information Microsoft-Windows...
                              Information Microsoft-Windows...
                              Information Microsoft-Windows...
 150504 Aug 27 16:22
 150503 Aug 27 16:22
                              Information EventLog
 150502 Aug 27 16:22
                              Information EventLog
 150501 Aug 27 16:22
                              Information EventLog
                                                                                2147489656 The previous system shutdown at 3:46:57 PM on [...
 150500 Aug 27 16:22
                              Error
                                               EventLog
 150499 Aug 27 16:22
                              Information Microsoft-Windows...
                                                                                            16 The iommu fault reporting has been initialized.
                                                                                            20 The description for Event ID '20' in Source 'Mi...
30 The description for Event ID '30' in Source 'Mi...
 150498 Aug 27 16:22
                              Information Microsoft-Windows...
 150497 Aug 27 16:22
150496 Aug 27 16:22
                              Information Microsoft-Windows...
                                                                                            27 The description for Event ID '27' in Source 'Mi...
                              Information Microsoft-Windows...
150495 Aug 27 16:22
150494 Aug 27 16:22
                                                                                            25 The description for Event ID '25' in Source 'Mi...
                              Information Microsoft-Windows...
                                                                                          238 The description for Event ID '238' in Source 'M...
                              Information Microsoft-Windows...
                                                                                           20 The description for Event ID '20' in Source 'Mi...
32 The description for Event ID '32' in Source 'Mi...
 150493 Aug 27 16:22
                              Information Microsoft-Windows...
 150492 Aug 27 16:22
                              Information Microsoft-Windows...
 150491 Aug 27 16:22
                              Information Microsoft-Windows...
                                                                                            18 The description for Event ID
                                                                                                                                         '18' in Source 'Mi...
                                                                                          153 The description for Event ID '153' in Source 'M...

12 The description for Event ID '12' in Source 'Mi...
 150490 Aug 27 16:22
                               Information Microsoft-Windows...
 150489 Aug
                27 16:22
                              Information Microsoft-Windows...
 150488 Aug 27 15:27
                              Information Service Control M...
                                                                                1073748869 A service was installed in the system...
                                                                                2147549186 Bluetooth HID device either went out of range
                27 15:27
 150487 Aug
                              Warning
                                                HidBth
```

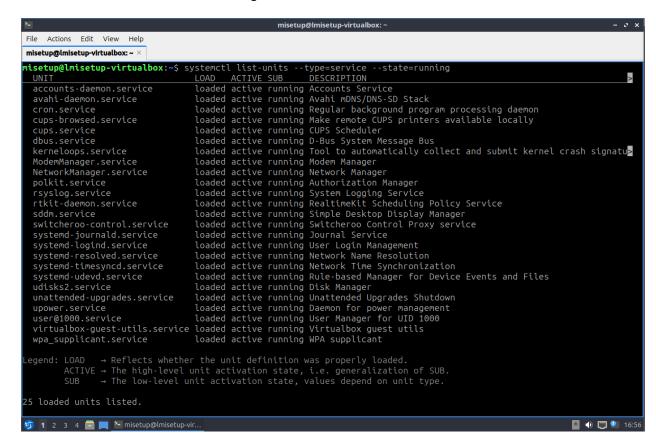
Tengo una instalación de Windows 10 que tiene aproximadamente 5 años de uso diario. Por ende tengo muchísimos logs. No los ha mostrado todos.

#### **Exploracion en Linux:**

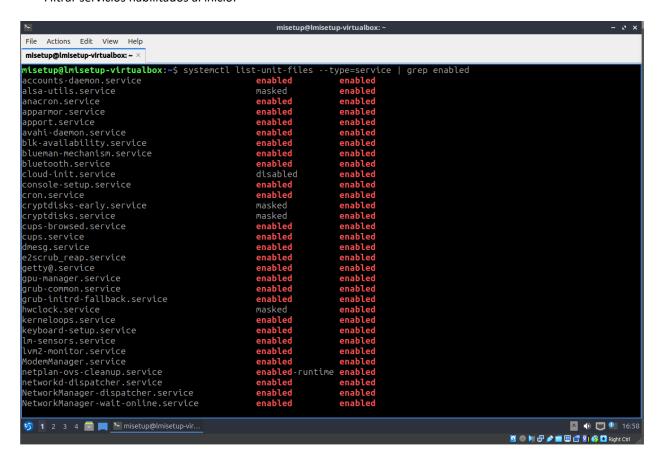
Listar servicios activo por defecto:



- Listado de servicios en estado "running":



- Filtrar servicios habilitados al inicio:



- Examinar parámetros de los daemons:

Inspecciono el servicio de Keyboard:

```
misetup@lmisetup-virtualbox:~$ systemctl show keyboard-setup.service
Type=oneshot
ExitType=main
Restart=no
RestartMode=normal
NotifyAccess=none
RestartUSec=100ms
RestartSteps=0
RestartMaxDelayUSec=infinity
RestartUSecNext=100ms
TimeoutStartUSec=infinity
TimeoutStopUSec=1min 30s
TimeoutAbortUSec=1min 30s
TimeoutStartFailureMode=terminate
TimeoutStopFailureMode=terminate
RuntimeMaxUSec=infinity
RuntimeRandomizedExtraUSec=0
WatchdogUSec=0
WatchdogTimestampMonotonic=0
RootDirectoryStartOnly=no
RemainAfterExit=yes
GuessMainPID=yes
MainPID=0
ControlPID=0
FileDescriptorStoreMax=0
NFileDescriptorStore=0
FileDescriptorStorePreserve=restart
StatusErrno=0
Result=success
ReloadResult=success
CleanResult=success
```

Ver detalles de configuración:

misetup@lmisetup-virtualbox:~\$ cat /etc/systemd/system/keyboard-setup.service
cat: /etc/systemd/system/keyboard-setup.service: No such file or directory

No pude ver los detalles de configuracion.

- Analizar los logs de eventos relacionados:

```
misetup@lmisetup-virtualbox:~$ journalctl
abr 24 16:35:08 lmisetup-virtualbox kernel: Linux version 6.8.0-58-generic (buildd@lcy02-amd64-040) (x86_64-linux-gn-
abr 24 16:35:08 lmisetup-virtualbox kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-6.8.0-58-generic root=UUID=0cf148-
abr 24 16:35:08 lmisetup-virtualbox kernel: KERNEL supported cpus:
abr 24 16:35:08 lmisetup-virtualbox kernel: Intel GenuineIntel
abr 24 16:35:08 lmisetup-virtualbox kernel:
abr 24 16:35:08 lmisetup-virtualbox kernel:
                                                         Centaur CentaurHauls
abr 24 16:35:08 lmisetup-virtualbox kernel:
                                                         zhaoxin Shanghai
 abr 24 16:35:08 lmisetup-virtualbox kernel: Hypervisor detected: KVM
                    lmisetup-virtualbox kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
     24 16:35:08
 abr 24 16:35:08 lmisetup-virtualbox kernel: kvm-clock: using sched offset of 4372566704 cycles
    24 16:35:08 lmisetup-virtualbox kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4df
 abr 24 16:35:08 lmisetup-virtualbox kernel: tsc: Detected 3593.254 MHz processor
    24 16:35:08 lmisetup-virtualbox kernel: e820: update [mem 0x00000000-0x0000fff] usable ==> reserved 24 16:35:08 lmisetup-virtualbox kernel: e820: remove [mem 0x000a0000-0x000fffff] usable
👣 1 2 3 4 🛅 💹 🗠 misetup@lmisetup-vir...
                                                                                                                                     17:06
```

# 3- Resultados Esperados

Se han agregado capturas de pantalla de los resultados obtenidos al ver cada servicio, log y configuración tanto en linux como en windows.

# 4- Preguntas de análisis

## A. Dentro de sus similitudes encontramos que:

- Ambos funcionan en segundo plano como procesos para proporcionar funcionalidades clave para el sistema operativo o aplicaciones.
- Se inician automaticamente OnStartup
- La gestion esta centralizada en un administrador, diferente para cada entorno claro.
- No requieren interaccion del usuario para su funcionamiento ni tienen interfaz grafica.

#### Dentro de sus diferencias encontramos:

- Su sistema de gestión difiere, Windows tiene un GUI con Services.msc y Linux solo puede ser accedido mediante la teminal utilizando el comando.
- Se configuran de forma diferente, con Windows vemos el registro de eventos y en Linux tenemos el Journal
- Se definen diferente. Sus dependencias.

#### B. Afectacion en Windows:

- Se ven en el visor de eventos. En las secciones Aplication y en System

#### Linux:

- Se ve en el Journal. Es importante la redireccion de salida para no perder los logs.

# C. Tipos de evento de Servicios en Windows:

- Evento de inicio o detencion
- Errores
- Advertencias
- Eventos personalizados

## Tipos de evento de Daemons en Linux:

- Mensajes de sistema
- Errores
- Advertencias
- Debug

#### **Diferencias Principales:**

- Window usa eventos estructurados y Linux usa logs de texto plano o binarios.

#### D. Windows:

- Sufre mas por exceso de servicios automáticos y bloatware, como OneDrive, Copilot o Update. El arranque se vuelve lento y consume recursos.

#### Linux:

- Maneja mejor la carga, pero tener deamons mal optimizados puede afectar fuertemente al rendimiento.

## E. Complicaciones en Windows:

- La configuración de los servicios depende del Registry, lo que complica su migración o respaldo.
- Los servicios suelen ejecutarse como SYSTEM o cuentas de dominio, generando verdaderos riesgos de seguridad si no se administran bien.
- Bloqueos y reinicios obligatorios. Muchos cambios requieren obligatoriamente que se reinicie el sistema operativo, afectando la confiabilidad.
- Fuerte dependencia en GUI. Limita la automatizacion avanzada.

## **Complicaciones en Linux:**

- Fragilidad en sus dependencias ya que los daemons pueden fallar si otro servicio o recurso no esta disponible.
- Multiples sistemas de inicio dependiendo de la distro que se utilice, lo que fragmenta el soporte y el conocimiento.
- Los logs estan descentralizados, puede dificultar su mantenimiento centralizado.
- Problemas y riesgos de seguridad si un daemon se ejecta como ROOT.