
SUSSINI PATRICIO

1- Preparativos

Entorno de trabajo:

Me encuentro usando una computadora física 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 física.

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 (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
Running CryptSvc        Cryptographic Services
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
Running DsSvc          Data Sharing Service
Running DusmSvc        Data Usage
Running EFS            Encrypting File System (EFS)
Running EventLog       Windows Event Log
Running EventSystem     COM+ Event System
Running FlexNet Licensi... FlexNet Licensing Service
Running FontCache       Windows Font Cache Service
Running GamingServices  Gaming Services
Running GamingServicesNet Gaming Services
Running hidserv        Human Interface Device Service
Running IKEEXT          IKE and AuthIP IPsec Keying Modules
Running InputMapper Cer... InputMapper Cerberus Whitelister
```

- [illegible]

- ```
PS C:\Users\paddy> Get-Service -Name VBoxSDS | Format-List *

Name : VBoxSDS
RequiredServices : {RPCSS}
CanPauseAndContinue : False
CanShutdown : False
CanStop : True
DisplayName : VirtualBox system service
DependentServices : {}
MachineName : .
ServiceName : VBoxSDS
ServicesDependedOn : {RPCSS}
ServiceHandle : SafeServiceHandle
Status : Running
ServiceType : Win32OwnProcess
StartType : Manual
Site :
Container :
```

- Inspecciono configuraciones con PowerShell

```
Administrator: Windows PowerShell

PS C:\Users\paddy> Get-WmiObject Win32_Service | Select-Object Name, StartMode, State
```

| Name                         | StartMode | State   |
|------------------------------|-----------|---------|
| AdAppMgrSvc                  | Auto      | Running |
| AdskLicensingService         | Auto      | Running |
| AJRouter                     | Manual    | Stopped |
| ALG                          | Manual    | Stopped |
| AMD Crash Defender Service   | Auto      | Running |
| AMD External Events Utility  | Auto      | Running |
| AppIDSvc                     | Manual    | Stopped |
| Appinfo                      | Manual    | Running |
| AppMgmt                      | Manual    | Stopped |
| AppReadiness                 | 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                     | Manual    | Stopped |
| BDESVC                       | Manual    | Stopped |
| BEService                    | Manual    | Stopped |
| BFE                          | Auto      | Running |
| BITS                         | Manual    | Stopped |
| BrokerInfrastructure         | Auto      | Running |
| BTAGService                  | Manual    | Running |
| BthAvctpSvc                  | Manual    | Running |
| bthserv                      | Manual    | Running |
| camsvc                       | Manual    | Running |
| CDPSvc                       | Auto      | Running |
| CertPropSvc                  | Manual    | Stopped |
| ClickToRunSvc                | Auto      | Running |
| ClipSVC                      | Manual    | Stopped |
| cloudidsvc                   | Manual    | Stopped |
| COMSysApp                    | Manual    | Stopped |
| CoreMessagingRegistrar       | Auto      | Running |
| CryptSvc                     | Auto      | Running |
| CscService                   | Manual    | Stopped |
| DcomLaunch                   | Auto      | Running |
| dcsvc                        | Manual    | Stopped |
| defragsvc                    | Manual    | Stopped |
| DeviceAssociationService     | Auto      | Running |
| DeviceInstall                | Manual    | Running |
| DevQueryBroker               | Manual    | Stopped |

- Análisis logs de eventos relacionados: *Usa Get-EventLog*

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". It displays a list of system events. The events are listed in a table-like format with columns for ID, date, time, level, source, and description. The events include various File System Filter events (e.g., 'npsvcrtig', 'UCPD', 'FileCrypt', 'WdFilter', 'Wof', 'FileInfo') and EventLog events (e.g., 'The system uptime is 10 seconds', 'The Event log service was started', 'Microsoft (R) Windows (R) 10.00.19045 Multipr...').

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

### Exploración en Linux:

- Listar servicios activo por defecto:

A screenshot of a Linux terminal window titled "missetup@lmissetup-virtualbox: ~". The terminal shows the output of the command `systemctl`. The output is a table with columns: UNIT, LOAD, ACTIVE, SUB, and D. The units listed include `proc-sys-fs-binfmt_misc.automount`, `sys-devices-pci0000:00-0000:00:01.1-ata2-host1-target1:0:0-1:0:0:0-block-sr0.device`, `sys-devices-pci0000:00-0000:00:03.0-net-enp0s3.device`, `sys-devices-pci0000:00-0000:00:05.0-sound-card0-controlC0.device`, `sys-devices-pci0000:00-0000:00:0d.0-ata3-host2-target2:0:0-2:0:0:0-block-sda-sda1.device`, `sys-devices-pci0000:00-0000:00:0d.0-ata3-host2-target2:0:0-2:0:0:0-block-sda.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.0-tty-ttyS0.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.1-tty-ttyS1.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.10-tty-ttyS10.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.11-tty-ttyS11.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.12-tty-ttyS12.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.13-tty-ttyS13.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.14-tty-ttyS14.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.15-tty-ttyS15.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.16-tty-ttyS16.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.17-tty-ttyS17.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.18-tty-ttyS18.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.19-tty-ttyS19.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.2-tty-ttyS2.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.20-tty-ttyS20.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.21-tty-ttyS21.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.22-tty-ttyS22.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.23-tty-ttyS23.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.24-tty-ttyS24.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.25-tty-ttyS25.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.26-tty-ttyS26.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.27-tty-ttyS27.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.28-tty-ttyS28.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.29-tty-ttyS29.device`, `sys-devices-platform-serial8250-serial8250:0-serial8250:0.3-tty-ttyS3.device`, and `sys-devices-platform-serial8250-serial8250:0-serial8250:0.30-tty-ttyS30.device`. The status for all units is "loaded" and "active", and the sub-state is "plugged".

- Listado de servicios en estado “running”:

```
misetup@lmetisup-virtualbox: ~$ systemctl list-units --type=service --state=running
```

| UNIT                           | LOAD   | ACTIVE | SUB     | DESCRIPTION                                                   |
|--------------------------------|--------|--------|---------|---------------------------------------------------------------|
| accounts-daemon.service        | loaded | active | running | Accounts Service                                              |
| avahi-daemon.service           | loaded | active | running | Avahi mDNS/DNS-SD Stack                                       |
| cron.service                   | loaded | active | running | Regular background program processing daemon                  |
| cups-browsed.service           | loaded | active | running | Make remote CUPS printers available locally                   |
| cups.service                   | loaded | active | running | CUPS Scheduler                                                |
| dbus.service                   | loaded | active | running | D-Bus System Message Bus                                      |
| kerneloops.service             | loaded | active | running | Tool to automatically collect and submit kernel crash signatu |
| ModemManager.service           | loaded | active | running | Modem Manager                                                 |
| NetworkManager.service         | loaded | active | running | Network Manager                                               |
| polkit.service                 | loaded | active | running | Authorization Manager                                         |
| rsyslog.service                | loaded | active | running | System Logging Service                                        |
| rtkit-daemon.service           | loaded | active | running | RealtimeKit Scheduling Policy Service                         |
| sddm.service                   | loaded | active | running | Simple Desktop Display Manager                                |
| switcheroo-control.service     | loaded | active | running | Switcheroo Control Proxy service                              |
| systemd-journald.service       | loaded | active | running | Journal Service                                               |
| systemd-logind.service         | loaded | active | running | User Login Management                                         |
| systemd-resolved.service       | loaded | active | running | Network Name Resolution                                       |
| systemd-timesyncd.service      | loaded | active | running | Network Time Synchronization                                  |
| systemd-udev.service           | loaded | active | running | Rule-based Manager for Device Events and Files                |
| udisks2.service                | loaded | active | running | Disk Manager                                                  |
| unattended-upgrades.service    | loaded | active | running | Unattended Upgrades Shutdown                                  |
| upower.service                 | loaded | active | running | Daemon for power management                                   |
| user@1000.service              | loaded | active | running | User Manager for UID 1000                                     |
| virtualbox-guest-utils.service | loaded | active | running | Virtualbox guest utils                                        |
| wpa_supplicant.service         | loaded | active | running | WPA supplicant                                                |

Legend: LOAD → Reflects whether the unit definition was properly loaded.  
ACTIVE → The high-level unit activation state, i.e. generalization of SUB.  
SUB → The low-level unit activation state, values depend on unit type.

25 loaded units listed.

- Filtrar servicios habilitados al inicio:

```
misetup@lmisetup-virtualbox: ~$ systemctl list-unit-files --type=service | grep enabled
accounts-daemon.service enabled enabled
alsa-utils.service masked enabled
anacron.service enabled enabled
apparmor.service enabled enabled
apport.service enabled enabled
avahi-daemon.service enabled enabled
blk-availability.service enabled enabled
blueman-mechanism.service enabled enabled
bluetooth.service enabled enabled
cloud-init.service disabled enabled
console-setup.service enabled enabled
cron.service enabled enabled
cryptdisks-early.service masked enabled
cryptdisks.service masked enabled
cups-browsed.service enabled enabled
cups.service enabled enabled
dmesg.service enabled enabled
e2scrub_reap.service enabled enabled
getty@.service enabled enabled
gpu-manager.service enabled enabled
grub-common.service enabled enabled
grub-initrd-fallback.service enabled enabled
hwclock.service masked enabled
kerneloops.service enabled enabled
keyboard-setup.service enabled enabled
lm-sensors.service enabled enabled
lvm2-monitor.service enabled enabled
ModemManager.service enabled enabled
netplan-ovs-cleanup.service enabled-runtime enabled
networkd-dispatcher.service enabled enabled
NetworkManager-dispatcher.service enabled enabled
NetworkManager-wait-online.service enabled enabled
```

- 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: AMD AuthenticAMD
abr 24 16:35:08 lmisetup-virtualbox kernel: Hygon HygonGenuine
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: [Firmware Bug]: TSC doesn't count with P0 frequency!
abr 24 16:35:08 lmisetup-virtualbox kernel: BIOS-provided physical RAM map:
abr 24 16:35:08 lmisetup-virtualbox kernel: BIOS-e820: [mem 0x0000000000000000-0x0000000000009fbff] usable
abr 24 16:35:08 lmisetup-virtualbox kernel: BIOS-e820: [mem 0x0000000000009fc00-0x0000000000009ffff] reserved
abr 24 16:35:08 lmisetup-virtualbox kernel: BIOS-e820: [mem 0x000000000000f0000-0x000000000000ffffff] reserved
abr 24 16:35:08 lmisetup-virtualbox kernel: BIOS-e820: [mem 0x00000000000100000-0x000000000000dffff] usable
abr 24 16:35:08 lmisetup-virtualbox kernel: BIOS-e820: [mem 0x00000000000dfff0000-0x00000000000dffffff] ACPI data
abr 24 16:35:08 lmisetup-virtualbox kernel: BIOS-e820: [mem 0x000000000fec00000-0x000000000fec00fff] reserved
abr 24 16:35:08 lmisetup-virtualbox kernel: BIOS-e820: [mem 0x000000000fae00000-0x000000000fae00fff] reserved
abr 24 16:35:08 lmisetup-virtualbox kernel: BIOS-e820: [mem 0x000000000ffc00000-0x000000000ffffff] reserved
abr 24 16:35:08 lmisetup-virtualbox kernel: BIOS-e820: [mem 0x00000000100000000-0x0000000010ffffff] usable
abr 24 16:35:08 lmisetup-virtualbox kernel: NX (Execute Disable) protection: active
abr 24 16:35:08 lmisetup-virtualbox kernel: APIC: Static calls initialized
abr 24 16:35:08 lmisetup-virtualbox kernel: SMBIOS 2.5 present.
abr 24 16:35:08 lmisetup-virtualbox kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
abr 24 16:35:08 lmisetup-virtualbox kernel: Hypervisor detected: KVM
abr 24 16:35:08 lmisetup-virtualbox kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
abr 24 16:35:08 lmisetup-virtualbox kernel: kvm-clock: using sched offset of 4372566704 cycles
abr 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
abr 24 16:35:08 lmisetup-virtualbox kernel: e820: update [mem 0x000000000-0x00000fff] usable ==> reserved
abr 24 16:35:08 lmisetup-virtualbox kernel: e820: remove [mem 0x000a00000-0x000ffff] usable
```

### 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 automáticamente OnStartup
- La gestión está centralizada en un administrador, diferente para cada entorno claro.
- No requieren interacción del usuario para su funcionamiento ni tienen interfaz gráfica.

#### 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 terminal 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. Afectación en Windows:

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

#### Linux:

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

#### C. Tipos de evento de Servicios en Windows:

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

#### Tipos de evento de Daemons en Linux:

- Mensajes de sistema
- Errores
- Advertencias
- Debug

#### Diferencias Principales:

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

#### D. Windows:

- Sufre más 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 daemons 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 automatización avanzada.

**Complicaciones en Linux:**

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