

TRABAJO PRÁCTICO

Gestion de servicios en los sistemas operativos

Alumno: Ignacio Figueroa

Tecnicatura Universitaria en Programación – UTN

Materia: AySO

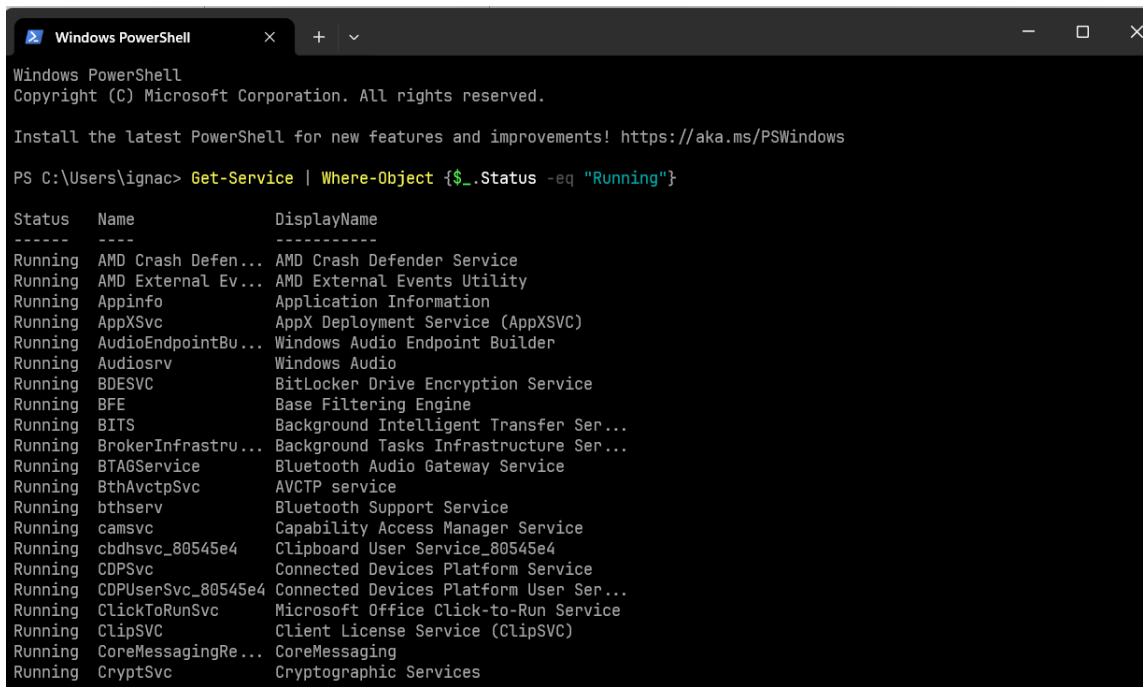
Comisión: 7

Introducción

Este trabajo práctico busca comparar y analizar los servicios activos por defecto en Windows y los daemons en Linux, así como su influencia en los logs de eventos de cada sistema operativo. Este trabajo práctico busca comparar y analizar los servicios activos por defecto en Windows y los daemons en Linux, así como su influencia en los logs de eventos de cada sistema operativo. Se utilizarán comandos nativos de cada sistema, PowerShell en Windows y asistentes de línea de comandos en Linux para realizar esta exploración. Este trabajo práctico busca comparar y analizar los servicios activos por defecto en Windows y los daemons en Linux, así como su influencia en los logs de eventos de cada sistema operativo. Se utilizarán comandos nativos de cada sistema, PowerShell en Windows y asistentes de línea de comandos en Linux para realizar esta exploración.

Desarrollo

Usar PowerShell para listar todos los servicios que están **ejecutándose**



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\ignac> Get-Service | Where-Object {$_.Status -eq "Running"}

Status Name                DisplayName
-----
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 AudioEndpointBu... Windows Audio Endpoint Builder
Running Audiosrv         Windows Audio
Running BDESVC           BitLocker Drive Encryption Service
Running BFE              Base Filtering Engine
Running BITS             Background Intelligent Transfer Ser...
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 cbdhsvc_80545e4   Clipboard User Service_80545e4
Running CDPsvc           Connected Devices Platform Service
Running CDPUserSvc_80545e4 Connected Devices Platform User Ser...
Running ClickToRunSvc     Microsoft Office Click-to-Run Service
Running ClipSVC           Client License Service (ClipSVC)
Running CoreMessagingRe... CoreMessaging
Running CryptSvc          Cryptographic Services
```

En PowerShell, para obtener detalles de un servicio (por ejemplo, "wuauserv"):

```
Windows PowerShell
PS C:\Users\ignac> Get-Service -Name wuauserv | Format-List *

Name                : wuauserv
RequiredServices    : {rpcss}
CanPauseAndContinue : False
CanShutdown         : False
CanStop             : True
DisplayName         : Windows Update
DependentServices   : {}
MachineName         : .
ServiceName         : wuauserv
ServicesDependedOn  : {rpcss}
ServiceHandle       :
Status              : Running
ServiceType         : Win32OwnProcess, Win32ShareProcess
StartType           : Manual
Site                :
Container           :
```

Para inspeccionar configuraciones (inicio automático, estado, usuario, etc.):

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

Name                StartMode State
-----
ALG                  Manual   Stopped
AMD Crash Defender Service Auto     Running
AMD External Events Utility Auto     Running
AppIDSvc             Manual   Stopped
Appinfo              Manual   Running
AppReadiness         Manual   Stopped
AppXSvc              Manual   Running
ApxSvc               Manual   Stopped
AudioEndpointBuilder Auto     Running
Audiosrv             Auto     Running
autotimesvc          Manual   Stopped
AxInstSV             Manual   Stopped
BDESVC               Manual   Running
BFE                  Auto     Running
BITS                 Auto     Running
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   Running
com.docker.service   Manual   Stopped
COMSysApp            Manual   Stopped
```

Analizar los eventos relacionados en PowerShell, para ver eventos del sistema:

```
Windows PowerShell
PS C:\Users\ignac> Get-EventLog -LogName System -EntryType Information, Warning, Error
```

Index	Time	EntryType	Source	InstanceID	Message
32667	Jun 11 18:48	Information	Microsoft-Windows...	19	Installation Successful: Windows successfully i...
32666	Jun 11 18:46	Information	Microsoft-Windows...	16	The description for Event ID '16' in Source 'Mi...
32665	Jun 11 18:46	Information	Microsoft-Windows...	16	The description for Event ID '16' in Source 'Mi...
32664	Jun 11 18:46	Information	Microsoft-Windows...	16	The description for Event ID '16' in Source 'Mi...
32663	Jun 11 18:40	Information	Microsoft-Windows...	19	Installation Successful: Windows successfully i...
32662	Jun 11 18:40	Information	Microsoft-Windows...	19	Installation Successful: Windows successfully i...
32661	Jun 11 18:40	Information	Microsoft-Windows...	19	Installation Successful: Windows successfully i...
32660	Jun 11 18:40	Information	Microsoft-Windows...	16	The description for Event ID '16' in Source 'Mi...
32659	Jun 11 18:40	Information	Microsoft-Windows...	16	The description for Event ID '16' in Source 'Mi...
32658	Jun 11 18:40	Information	Microsoft-Windows...	16	The description for Event ID '16' in Source 'Mi...
32657	Jun 11 18:40	Information	Microsoft-Windows...	44	Windows Update started downloading an update.
32656	Jun 11 18:40	Information	Microsoft-Windows...	44	Windows Update started downloading an update.
32655	Jun 11 18:40	Information	Microsoft-Windows...	44	Windows Update started downloading an update.
32654	Jun 11 18:40	Information	Microsoft-Windows...	43	Installation Started: Windows has started insta...
32653	Jun 11 18:38	Information	Service Control M...	1073748864	The start type of the Windows Modules Installer...
32652	Jun 11 18:38	Error	Microsoft-Windows...	20	Installation Failure: Windows failed to install...
32651	Jun 11 18:38	Information	Microsoft-Windows...	16	The description for Event ID '16' in Source 'Mi...
32650	Jun 11 18:38	Information	Microsoft-Windows...	44	Windows Update started downloading an update.
32649	Jun 11 18:38	Information	Microsoft-Windows...	16	The description for Event ID '16' in Source 'Mi...
32648	Jun 11 18:37	Information	Microsoft-Windows...	43	Installation Started: Windows has started insta...
32647	Jun 11 18:37	Information	Microsoft-Windows...	16	The description for Event ID '16' in Source 'Mi...
32646	Jun 11 18:36	Information	Microsoft-Windows...	19	Installation Successful: Windows successfully i...
32645	Jun 11 18:36	Information	Microsoft-Windows...	44	Windows Update started downloading an update.
32644	Jun 11 18:36	Information	Microsoft-Windows...	43	Installation Started: Windows has started insta...
32643	Jun 11 18:36	Information	Microsoft-Windows...	44	Windows Update started downloading an update.
32642	Jun 11 18:36	Information	Microsoft-Windows...	44	Windows Update started downloading an update.

Preguntas de análisis:

A. ¿Qué similitudes y diferencias existen entre los servicios de Windows y los daemons de Linux en cuanto a funcionamiento y parámetros?

- Los servicios en Windows y los daemons en Linux son procesos que corren en segundo plano para mantener funcionando el sistema y sus aplicaciones. Ambos pueden configurarse para que se inicien automáticamente y se gestionan para asegurar que estén activos cuando se necesitan. La diferencia principal está en cómo se manejan: Windows usa un administrador de servicios centralizado y guarda la configuración en el registro del sistema, mientras que Linux usa systemd o init y las configuraciones están en archivos de texto que se pueden editar fácilmente. Además, Linux suele asignar permisos específicos a los daemons para mayor seguridad, y Windows controla esto a través de cuentas de servicio. En cuanto al registro de eventos, Windows centraliza todo en el Event Log, y Linux usa archivos de log o journalctl para monitorear lo que pasa con los daemons. En resumen, funcionan parecido, pero cada sistema tiene su forma particular de configurarlos y controlarlos.

B. ¿Cómo afecta la configuración de un servicio o daemon en los logs de eventos de cada sistema operativo?

- La configuración de un servicio o daemon influye directamente en los logs de eventos de ambos sistemas operativos porque determina qué información se registra y cómo se muestra. En Windows, si un servicio está configurado para generar eventos detallados, estos aparecerán en el Event Log con distintos niveles de severidad como información, advertencia o error, facilitando el seguimiento y diagnóstico. En Linux, la configuración del daemon puede especificar qué mensajes enviar al sistema de logs (journalctl o archivos en /var/log), incluyendo niveles como debug, info o error, lo que afecta la cantidad y tipo de información disponible para el análisis. Por lo tanto, una configuración más completa o detallada produce registros más útiles, mientras que una configuración limitada puede dificultar la identificación de problemas.

C. ¿Qué tipos de eventos generan los servicios en Windows frente a los daemons en Linux?

- Los servicios en Windows generan eventos que suelen clasificarse en categorías como información, advertencia y error, y estos eventos se registran en el Event Log del sistema, facilitando el monitoreo y la detección de problemas. En cambio, los daemons en Linux generan mensajes de log que pueden incluir niveles similares, como debug, info, warning y error, y se almacenan en archivos de registro o en el journal de systemd. Aunque ambos sistemas registran eventos para informar sobre el estado y posibles fallos, Windows tiende a usar una estructura más formal y centralizada, mientras que Linux ofrece una forma más flexible y distribuida de manejar los logs.

D. ¿Cómo influyen los parámetros de inicio automático en el rendimiento general del sistema en ambos casos?

- Los parámetros de inicio automático afectan el rendimiento general del sistema porque determinan qué servicios o daemons se ejecutan desde el arranque. Si hay muchos servicios configurados para iniciarse automáticamente, esto puede ralentizar el tiempo de arranque y consumir recursos como memoria y CPU durante el funcionamiento normal. En Windows, un exceso de servicios automáticos puede hacer que el sistema tarde más en estar listo para usar, mientras que en Linux, aunque el sistema suele ser más eficiente en este aspecto, también puede verse afectado si hay demasiados daemons arrancando al inicio. Por eso, en ambos sistemas es importante configurar solo los servicios necesarios para mantener un buen equilibrio entre funcionalidad y rendimiento.

E. ¿Qué desafíos surgen al administrar servicios en cada sistema operativo?

- Al administrar servicios en Windows, uno de los desafíos principales es manejar la gran cantidad de servicios preinstalados que pueden ser difíciles de identificar y configurar correctamente sin afectar la estabilidad del sistema. Además, la dependencia del registro y de herramientas gráficas puede complicar la automatización. En Linux, aunque la administración suele ser más flexible gracias a archivos de configuración y comandos en consola, puede ser un reto para usuarios menos experimentados entender las diferentes herramientas (systemd, init) y cómo afectan las dependencias entre daemons. En ambos casos, garantizar la seguridad, evitar conflictos entre servicios y mantener un rendimiento óptimo son desafíos comunes.