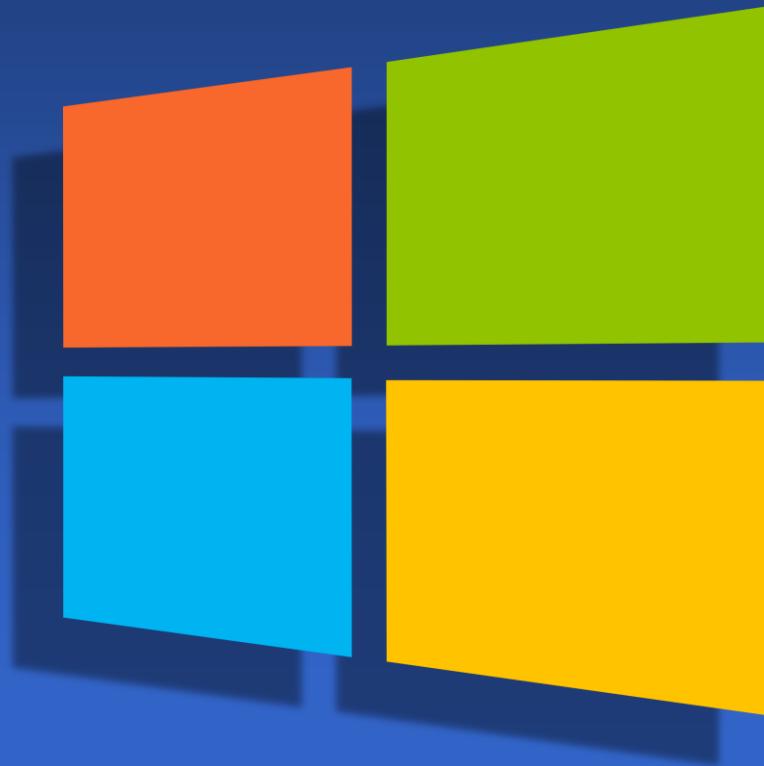


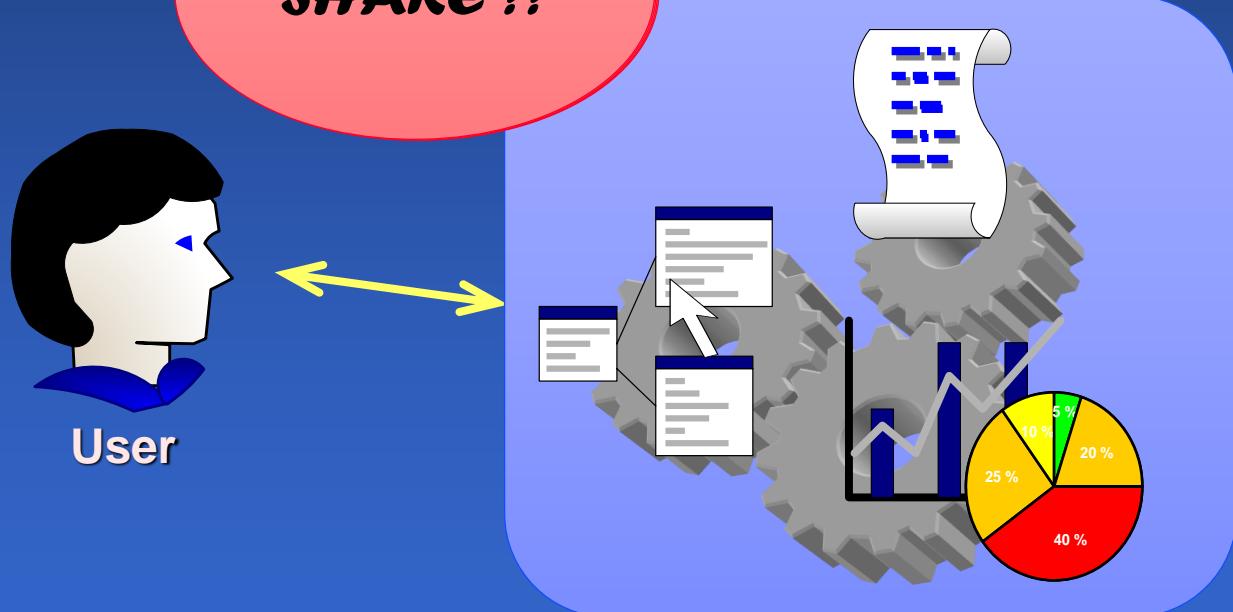
Use & Admin Windows Survival Kit – 4 RUNTIME



Windows Processes

Applications & Services

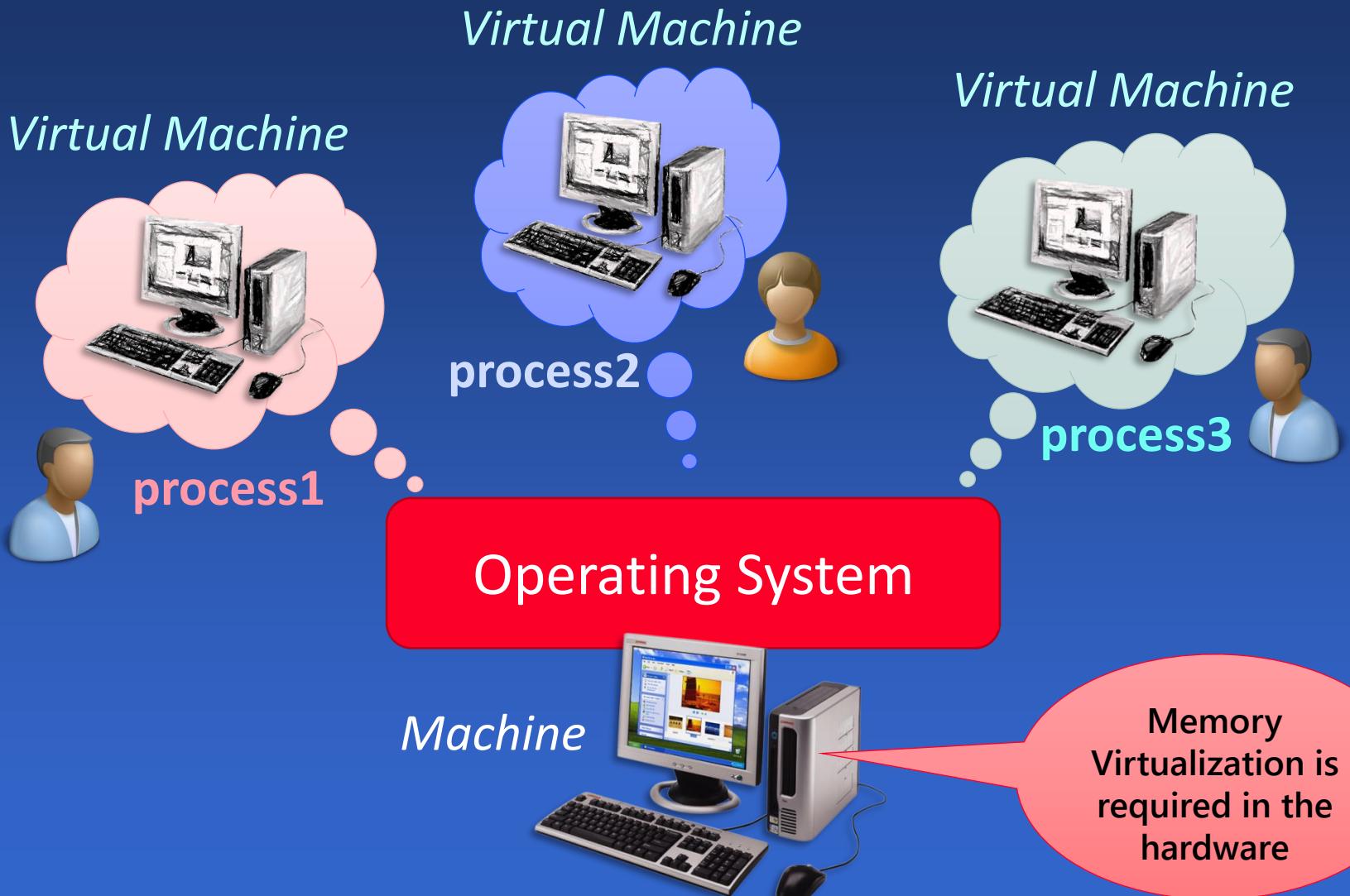
OS ?



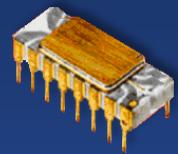
Hardware



Sharing the hardware



Role of the OS



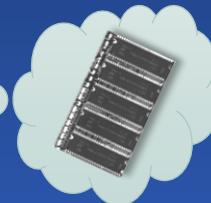
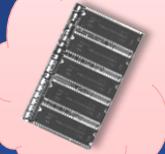
Virtual CPU

→ Schedule tasks



Virtual RAM

→ MMU



Virtual I/O

- File system
- Byte streams
- User interface

→ Driver management



OS Layers

SOFT



User environment

TTY shell

GUI shell

Developer environment

System API (LIBC, POSIX, Win32 ...)

OOP framework (JAVA, .NET ...)

Services

Virtualized I/O

Persistence → HDD, SSD, File System ...

IPC → pipes, sockets ...

Peripherals & Stacks → Serial, USB, Ethernet ...

Drivers

Memory

MMU → processus → protection

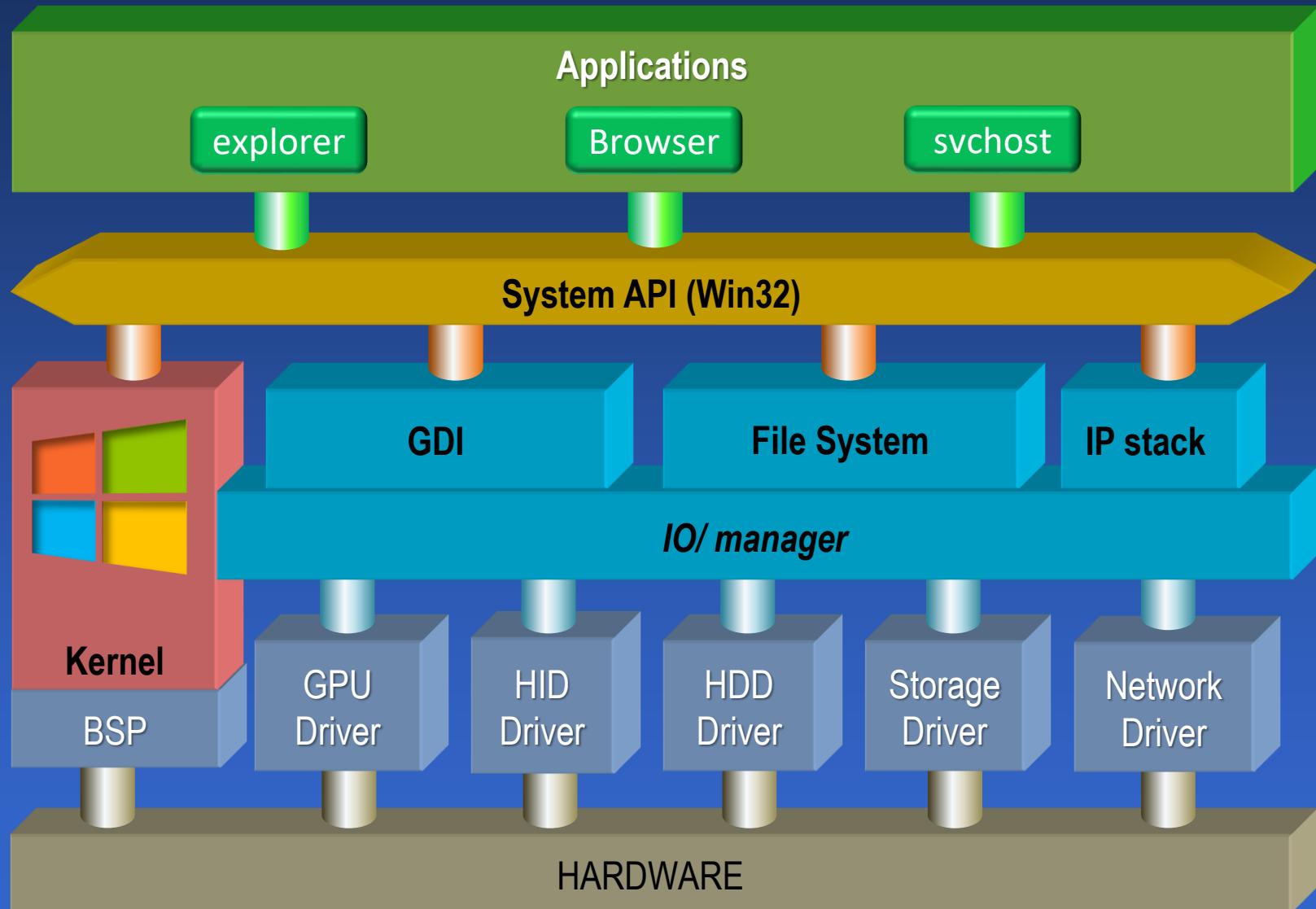
Execution

Scheduler → thread → synchronization

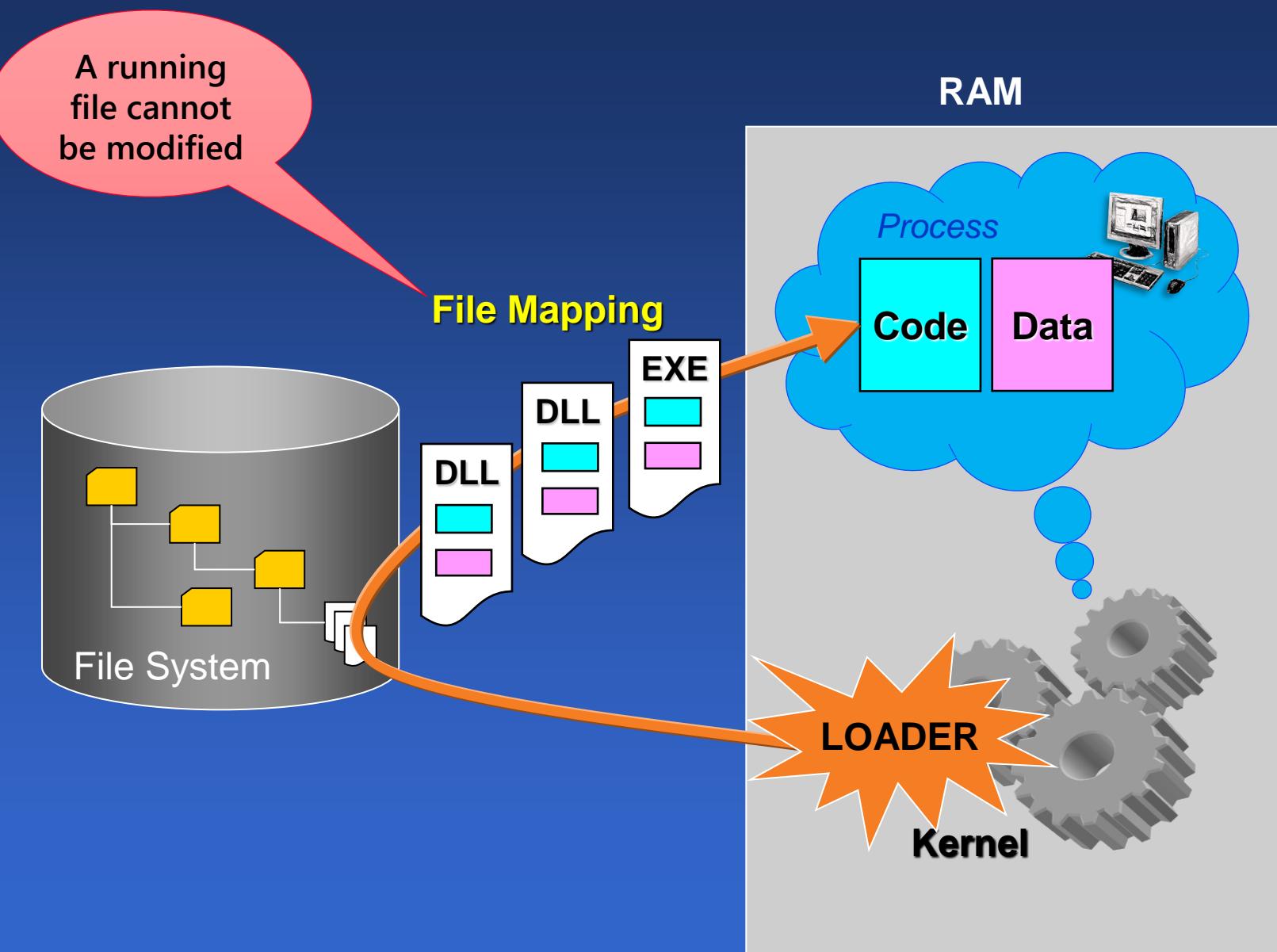
Kernel

HARD

OS logical organization



Executable files EXE & DLL



Module DLLs

◆ Explore NOTEPAD with ProcExp

Process Explorer - Sysinternals: www.sysinternals.com [LAN\tjoubert]

File Options View Process Find Users DLL Help

CSwitch Delta CPU Private By... Working Set PID Description Company Name

Process	CSwitch Delta	CPU	Private By...	Working Set	PID	Description	Company Name
notepad.exe		3 696 K	18 296 K	1216 Bloc-notes	1216	Bloc-notes	Microsoft Corpor
SmartAudio3.exe		< 0.01	76 716 K	64 068 K	12520	SmartAudio 3	Conexant System
Flow.exe		< 0.01	59 100 K	59 044 K	10004	Flow	Open Inno Sc
lsvhost		< 0.01	59 100 K	59 044 K	10004	lsvhost	Open Inno Sc

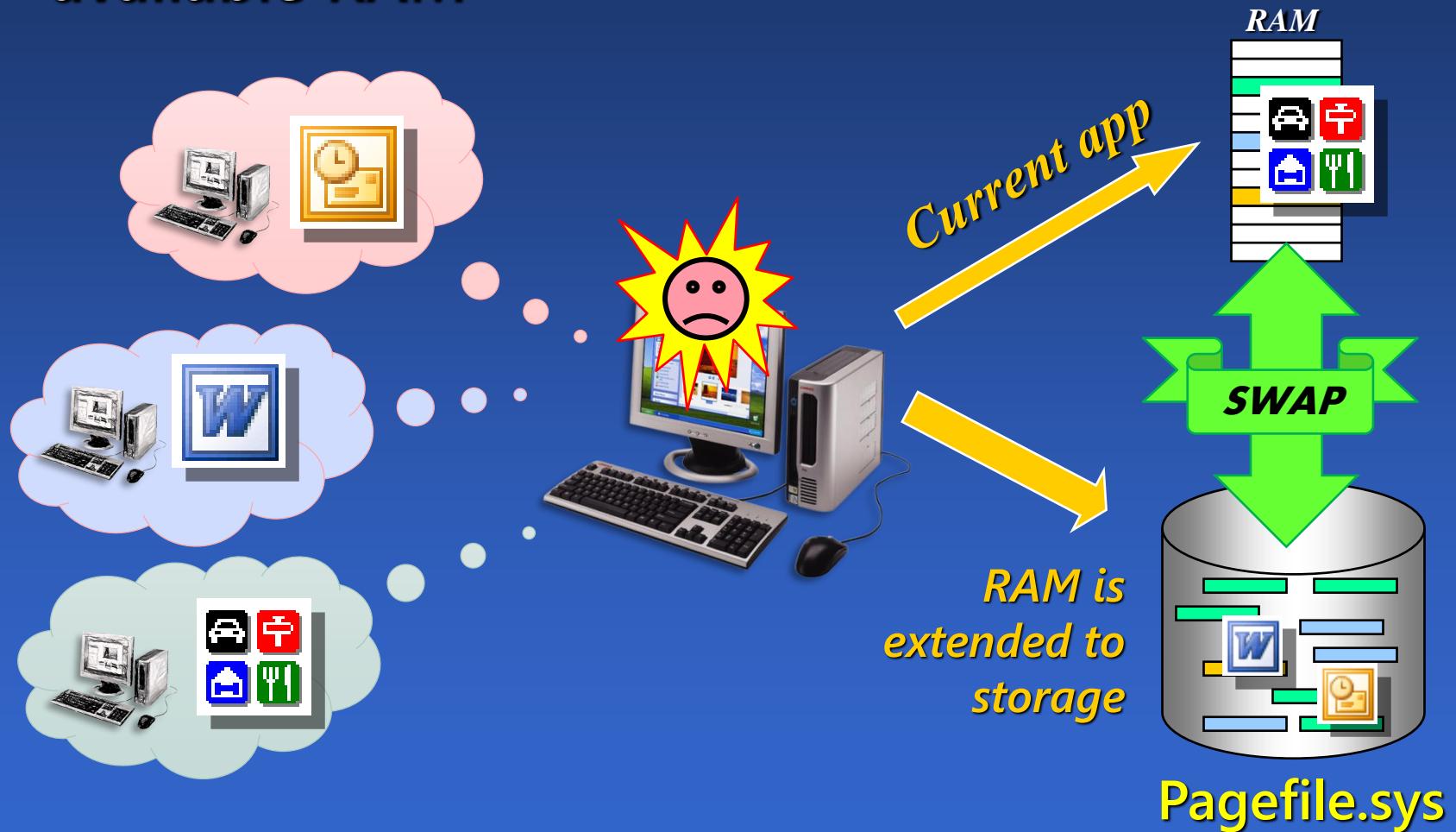
Handles DLLs Threads

Name	Description	Company Name	Path
{6AF0698E-D558-4F6E-9B3C-3...			C:\ProgramData\Microsoft\Windows\Caches\{6...
{AFBF9F1A-8EE8-4C77-AF34-C...			C:\Users\tjoubert.LAN\AppData\Local\Microsoft...
{DDF571F2-BE98-426D-8288-1...			C:\ProgramData\Microsoft\Windows\Caches\{D...
advapi32.dll	API avancées Windows 32	Microsoft Corporation	C:\Windows\System32\advapi32.dll
bcryptprimitives.dll	Windows Cryptographic Pri...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll
cfgmgr32.dll	Configuration Manager DLL	Microsoft Corporation	C:\Windows\System32\cfgmgr32.dll
clbcatq.dll	COM+ Configuration Catalog	Microsoft Corporation	C:\Windows\System32\clbcatq.dll
combase.dll	Microsoft COM pour Windo...	Microsoft Corporation	C:\Windows\System32\combase.dll
comctl32.dll	Bibliothèque de contrôles d...	Microsoft Corporation	C:\Windows\WinSxS\amd64_microsoft.windows...
comdlg32.dll	DLL commune de boîtes d...	Microsoft Corporation	C:\Windows\System32\comdlg32.dll
CoreMessaging.dll	Microsoft CoreMessaging Dll	Microsoft Corporation	C:\Windows\System32\CoreMessaging.dll
CoreUIComponents.dll	Microsoft Core UI Compon...	Microsoft Corporation	C:\Windows\System32\CoreUIComponents.dll
crostini_2.db			C:\ProgramData\Microsoft\Windows\Caches\cv

CPU Usage: 0.19% Commit Charge: 45.16% Processes: 216 Physical Usage: 46.62%

Virtual Memory & Swap

- ◆ Applications may use more memory than the available RAM



Swap parameters

À propos de

Support

Fabricant

Site Web

Paramètres associés

Paramètres de Bitlocker

Gestionnaire de périphériques

Bureau à distance

Protection du système

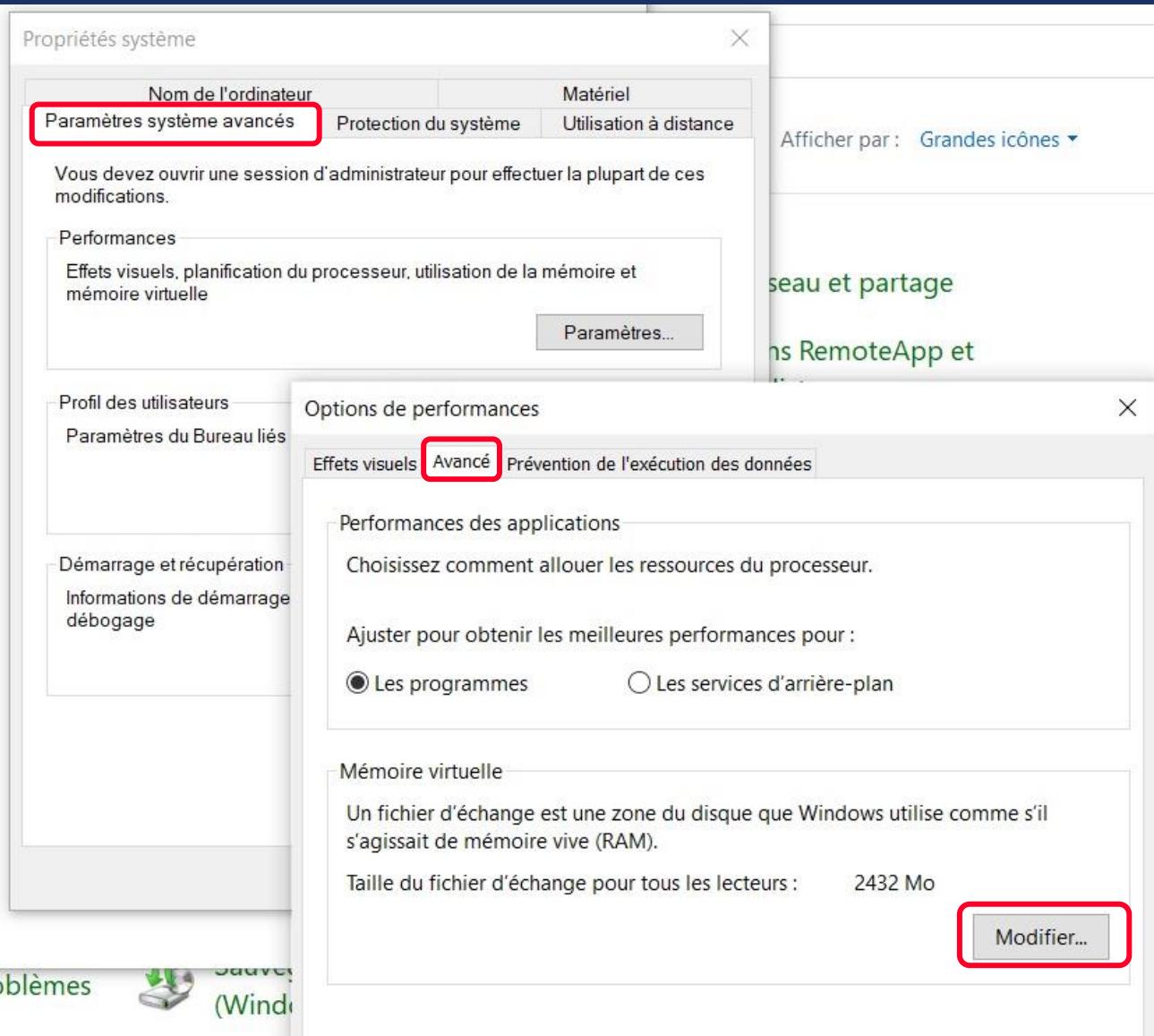
Paramètres avancés du système

Renommer ce PC (avancé)

Obtenir de l'aide

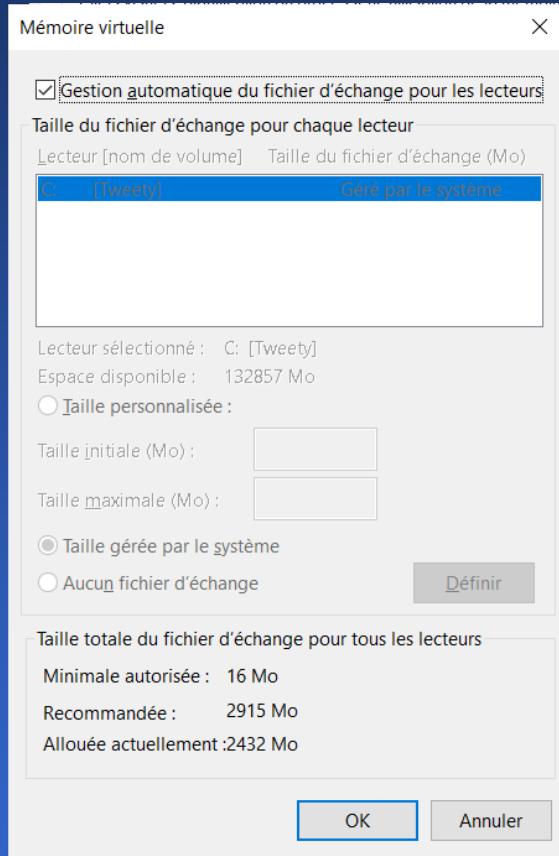
Résolution des problèmes

Sauvegarde (Windows)

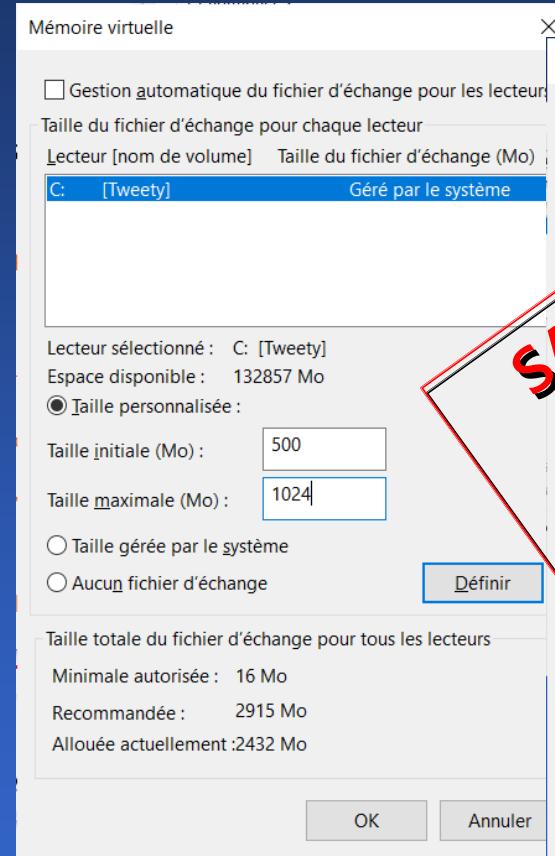


Swap options

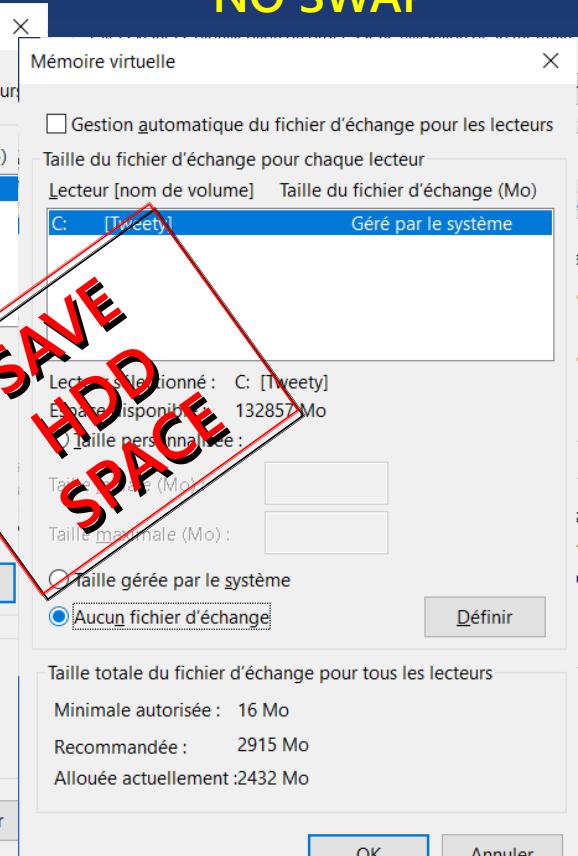
AUTO SWAP (default)



DEDICATED SWAP



NO SWAP



SAVE
HDD
SPACE

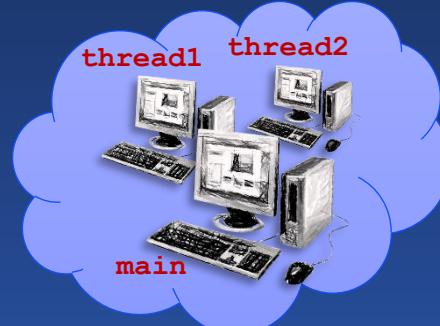
Reboot is required

Next step = Threads

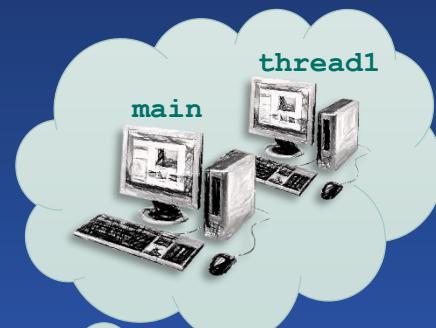
Virtual Machines



Virtual Machines



Virtual Machines



Operating System

Machine



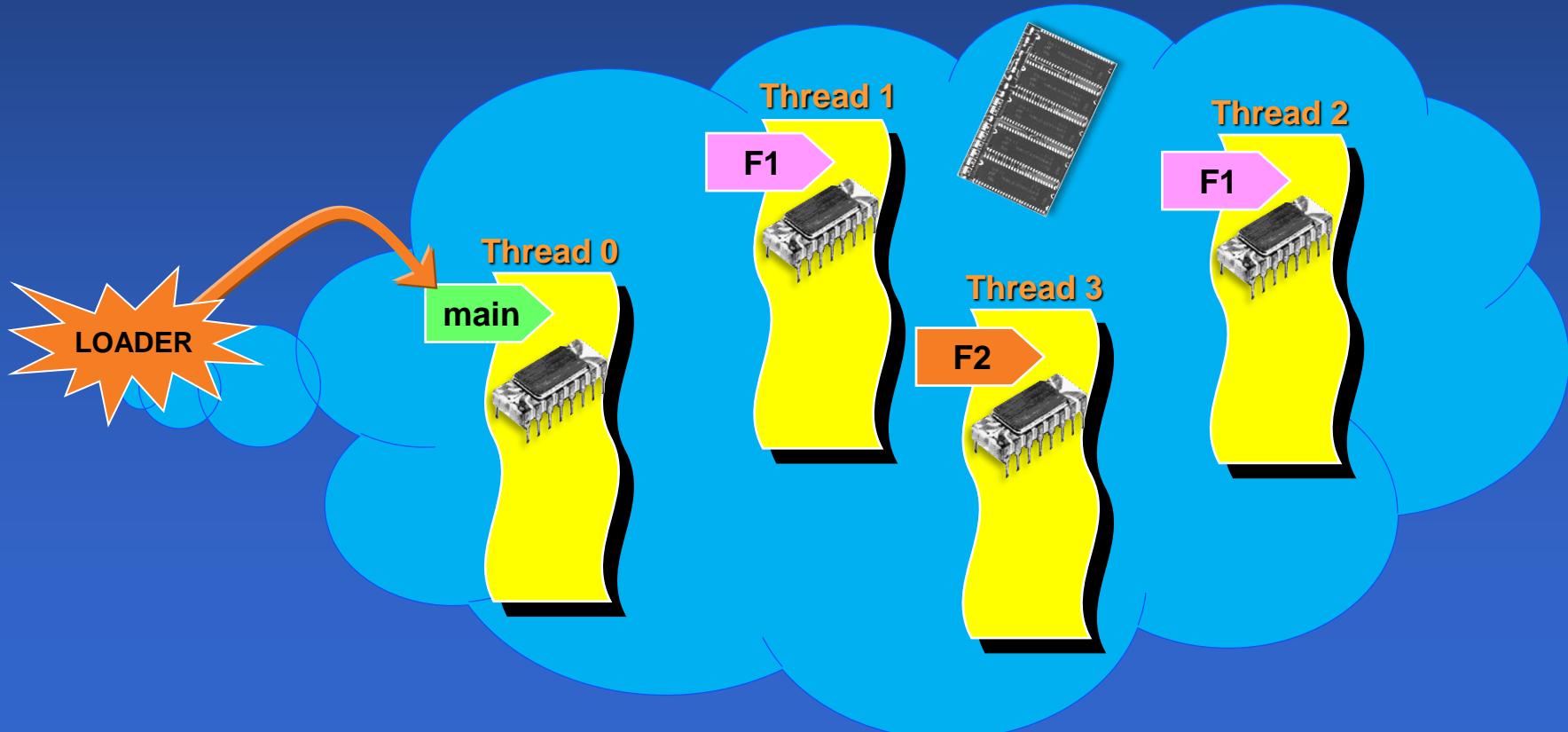
Threads share
the process
memory

Thread
scheduling

Multi-threading

- ◆ Applications may have several threads

- Thread0 runs the **main**
- Others Threads run dedicated code
- Each thread has its own STACK
- All threads share the same memory space (BSS, HEAP)



Module Threads

◆ Explore NOTEPAD with ProcExp

Process Explorer - Sysinternals: www.sysinternals.com [LAN\tjoubert]

File Options View Process Find Users Thread Help

Process CSwitch Delta CPU Private By... Working Set PID Description Company Name

Process	CSwitch Delta	CPU	Private By...	Working Set	PID	Description	Company Name
notepad.exe		3 432 K	18 324 K	1216 Bloc-notes	1216	Bloc-notes	Microsoft Corpor
SmartAudio3.exe	14	< 0.01	76 716 K	64 068 K	12520	SmartAudio 3	Conexant System
Flow.exe							
taskhost.exe							

Handles DLLs Threads

Stack Module Terminate

State	Wait Reason	TID	User Ti...	Kernel T...	CPU	CPU Ti...	Start Time	Start Address	Base ...	Dyn
Waiting	WrUserReq...	6188	00:00:00	00:00:00		00:00:00	01/05/23 18...	NOTEPAD.EXE+0x...	8	
Waiting	WrQueue	22420	00:00:00	00:00:00		00:00:00	01/05/23 18...	ntdll.dll!TpReleaseC...	8	
Waiting	WrQueue	2404	00:00:00	00:00:00		00:00:00	01/05/23 18...	ntdll.dll!TpReleaseC...	8	
Waiting	WrQueue	20148	00:00:00	00:00:00		00:00:00	01/05/23 18...	ntdll.dll!TpReleaseC...	8	

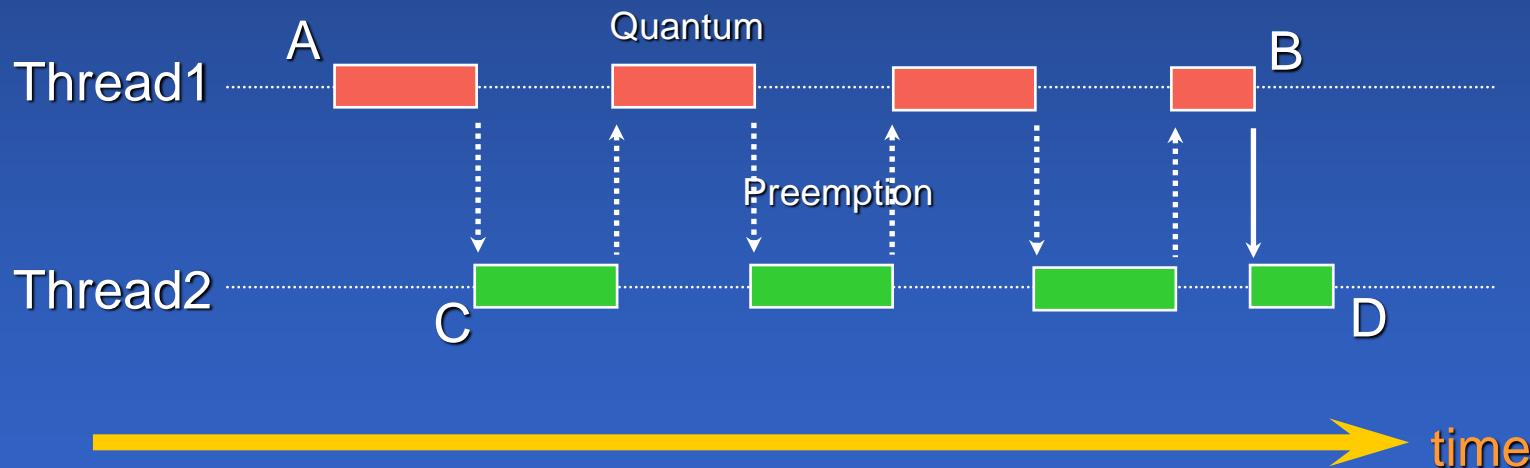
CPU Usage: 0.96% Commit Charge: 45.10% Processes: 215 Physical Usage: 46.54%

CPU distribution



Windows is a preemptive OS

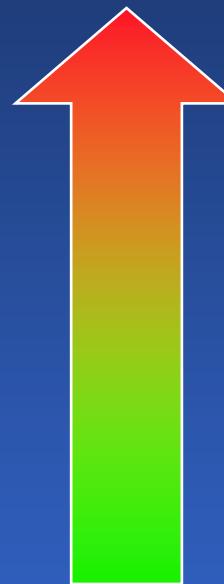
- The highest priority thread always runs
- Two threads with equal priorities run in "quantums"
- Two threads may run in parallel in case of multicore



Process priorities

- ◆ Windows has 6 priority levels for processes

- REAL TIME
- HIGH
- ABOVE_NORMAL
- NORMAL
- BELOW_NORMAL
- IDLE



Change a process priority

The screenshot shows the Windows Task Manager interface. A context menu is open for the process "EXCEL.EXE" (PID: 13476). The menu includes options like "Fin de tâche", "Terminer l'arborescence du processus", "Fournir des commentaires", "Définir la priorité" (which is highlighted with a red box), "Définir l'affinité", "Analyser la chaîne d'attente", "Déboguer", "Virtualisation du contrôle de compte d'utilisateur", "Créer un fichier de vidage", "Ouvrir l'emplacement du fichier", "Recherche en ligne", "Propriétés", and "Accéder aux services". A secondary dropdown menu titled "Temps réel" is open, listing priority levels: "Haute" (highlighted with a red box), "Supérieure à la normale", "Normale" (selected and highlighted with a blue dot), "Inférieure à la normale", and "Basse". The main task list shows other processes like "explorer.", "FileCoAu", "Flow.exe", "fontdrv", "HelpPan", "IGCC.exe", "IGCCTray", "igfxCUIS", "igfxEMN", "IntelAud", "IntelCpH", "Interrupt", "jhi_service", "jusched.exe", "LMS.exe", "LockApp.exe", "Lsalso.exe", and "lspk.exe". The "Details" tab is selected at the top.

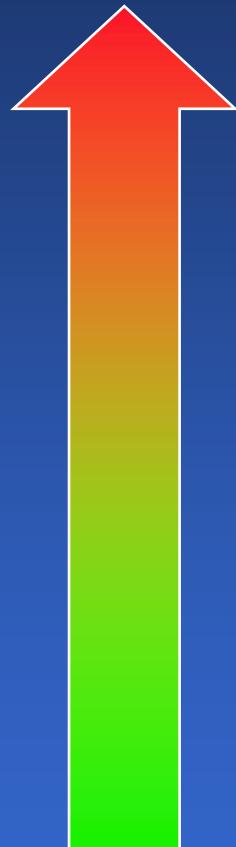
Nom	PID	Statut	Nom d'utili...	Proc...	Mémoire (p...)	Virtualisation d...
EXCEL.EXE	13476	En cours d'exécution	tjoubert	00	35 828 Ko	Désactivé
explorer.		Fin de tâche	tjoubert	00	91 852 Ko	Désactivé
FileCoAu		Terminer l'arborescence du processus	tjoubert	00	3 736 Ko	Désactivé
Flow.exe		Fournir des commentaires	tjoubert	00	8 720 Ko	Désactivé
fontdrv		Définir la priorité	Temps réel		80 Ko	Désactivé
HelpPan		Définir l'affinité	Haute		1 072 Ko	Désactivé
IGCC.exe		Analyser la chaîne d'attente	Supérieure à la normale		1 904 Ko	Désactivé
IGCCTray		Déboguer	Normale		3 608 Ko	Désactivé
igfxCUIS		Virtualisation du contrôle de compte d'utilisateur	Inférieure à la normale		944 Ko	Non autorisé
igfxEMN		Créer un fichier de vidage	Basse		1 700 Ko	Désactivé
IntelAud		Ouvrir l'emplacement du fichier	Système	00	2 948 Ko	Non autorisé
IntelCpH		Recherche en ligne	Système	00	368 Ko	Non autorisé
Interrupt		Propriétés	Système	03	0 Ko	
jhi_service		Accéder aux services	Système	00	328 Ko	Non autorisé
jusched.exe			tjoubert	00	1 112 Ko	Désactivé
LMS.exe	4784	En cours d'exécution	Système	00	888 Ko	Non autorisé
LockApp.exe	5040	Interrompu	tjoubert	00	0 Ko	Désactivé
Lsalso.exe	1012	En cours d'exécution	Système	00	404 Ko	Non autorisé
lspk.exe	nc	En cours d'autorisation	Système	00	7 616 Ko	Non autorisé

Moins de détails Fin de tâche

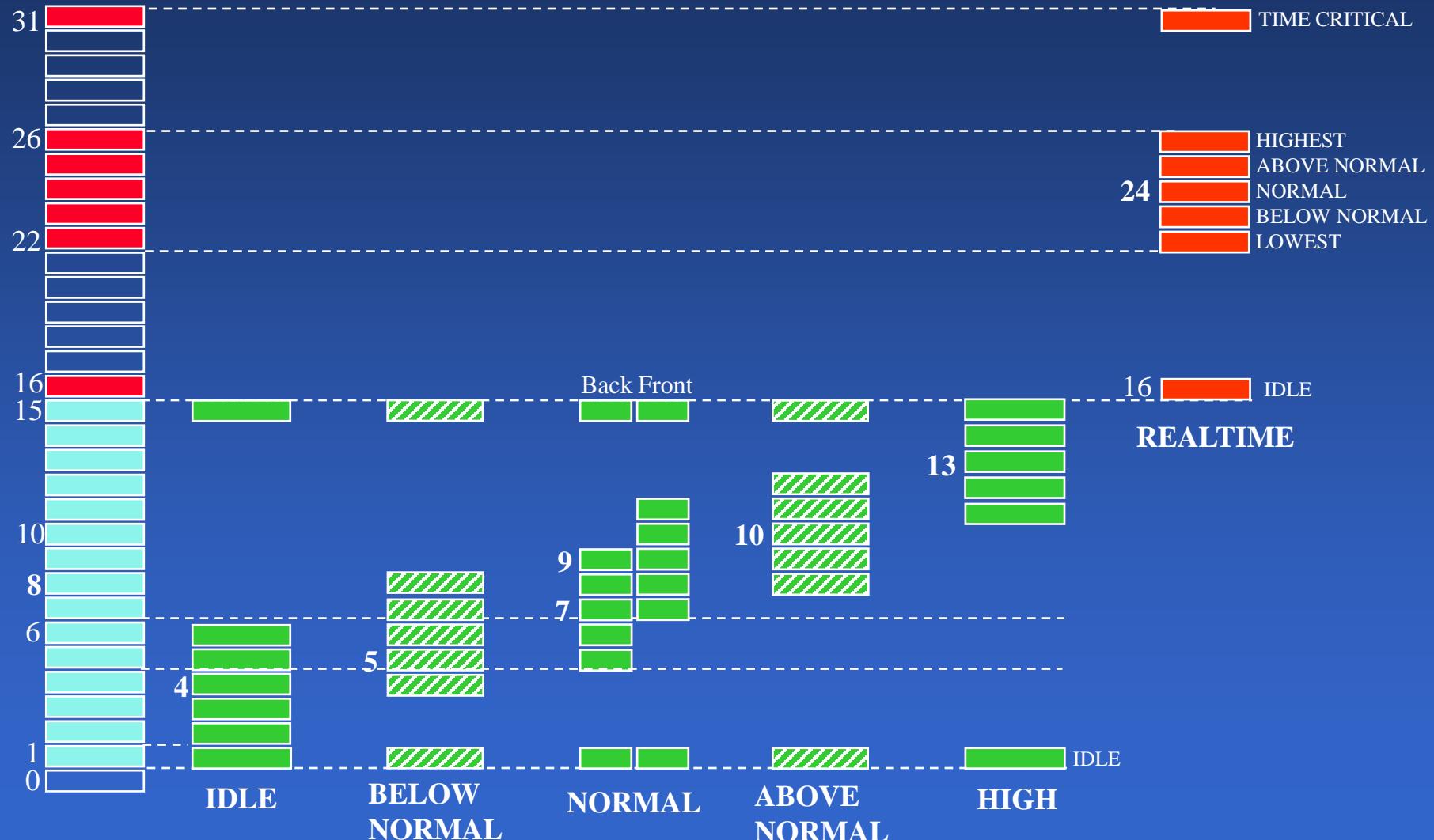
Thread priorities

◆ Windows has 7 priority levels for threads

- THREAD_PRIORITY_TIME_CRITICAL (15 or 31)
- THREAD_PRIORITY_HIGHEST (+2)
- THREAD_PRIORITY_ABOVE_NORMAL (+1)
- THREAD_PRIORITY_NORMAL (default)
- THREAD_PRIORITY_BELOW_NORMAL (-1)
- THREAD_PRIORITY_LOWEST (-2)
- THREAD_PRIORITY_IDLE (1 or 16)



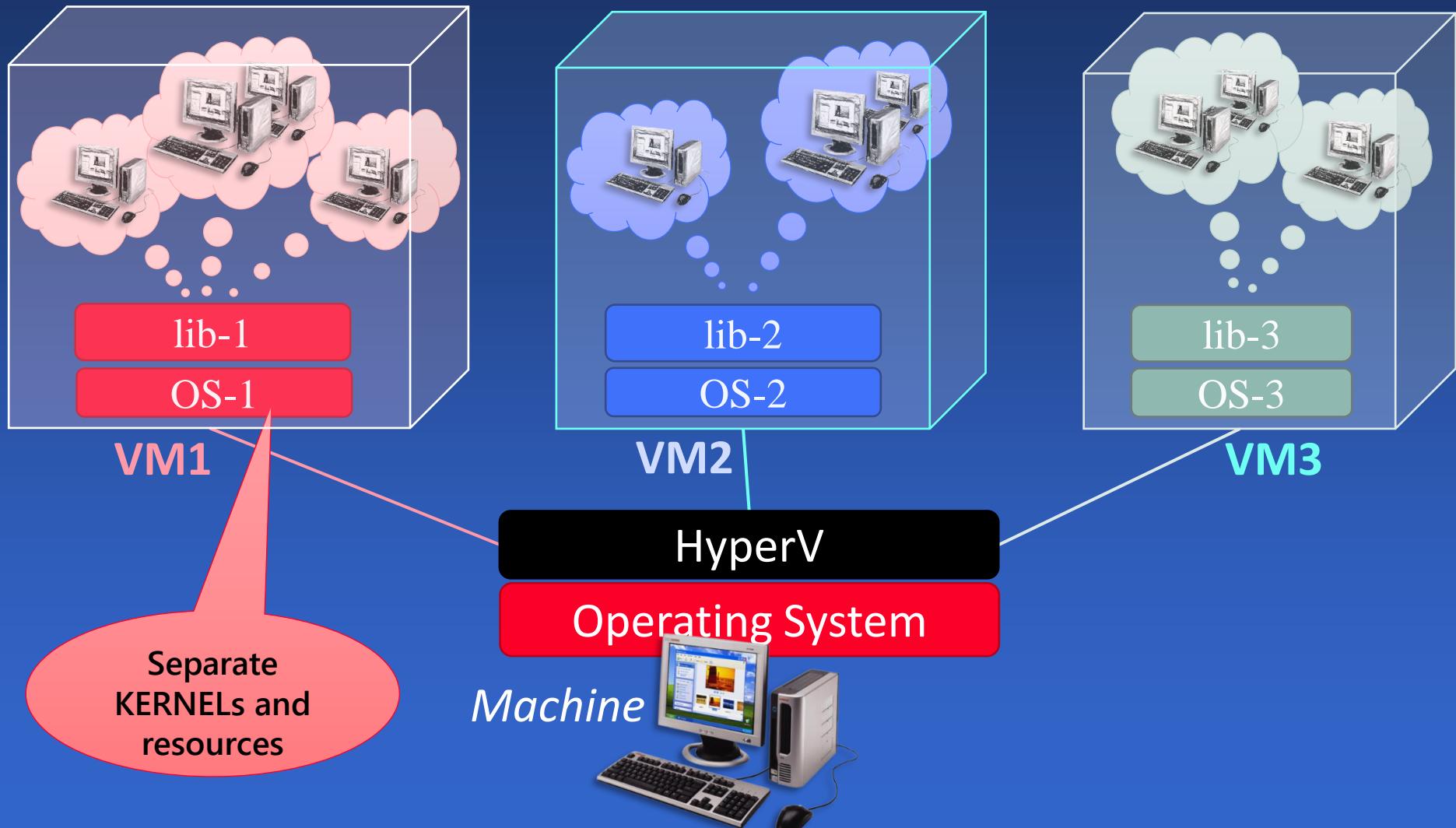
Runtime priority map



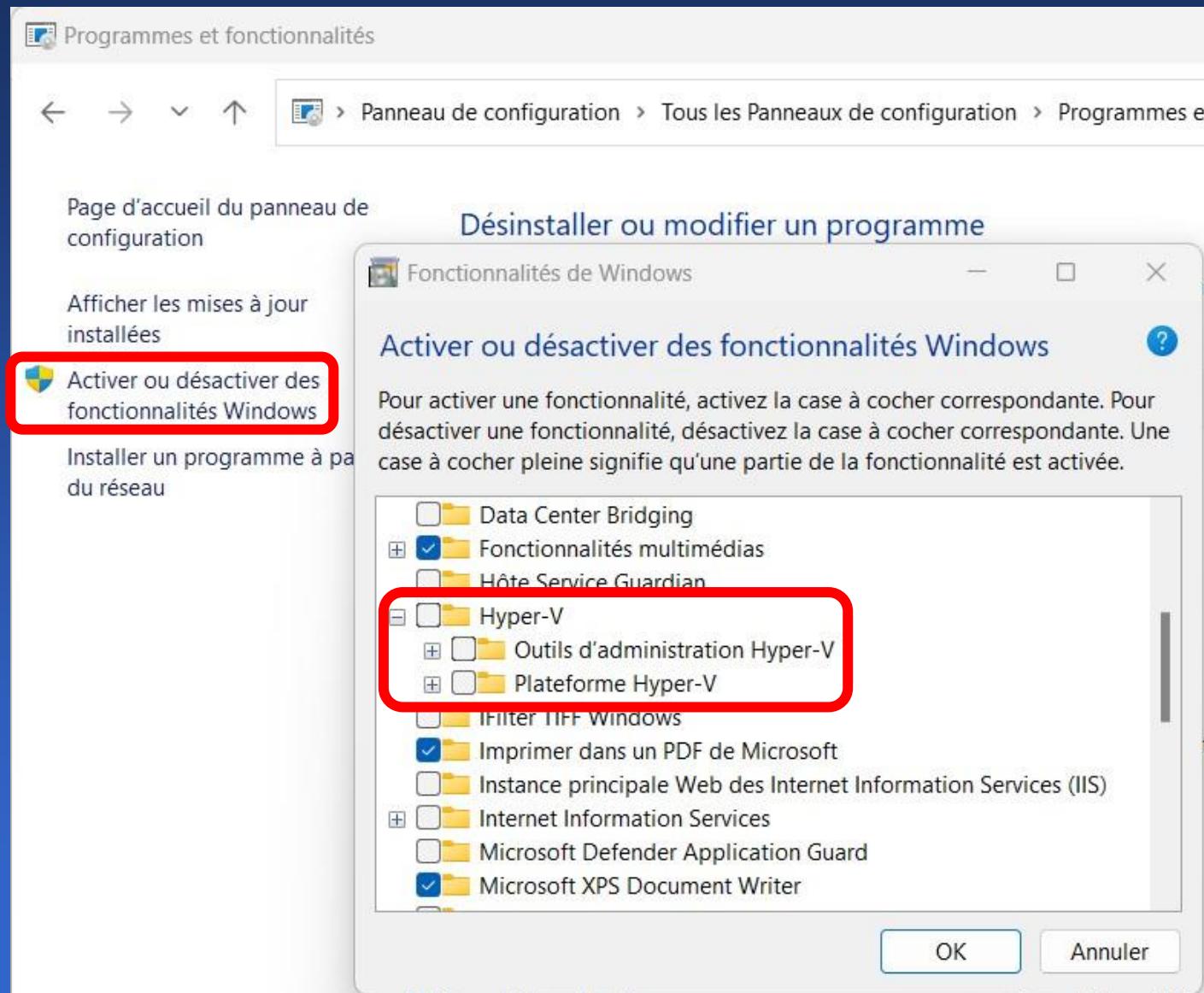
Beyond Processes

Hypervisor

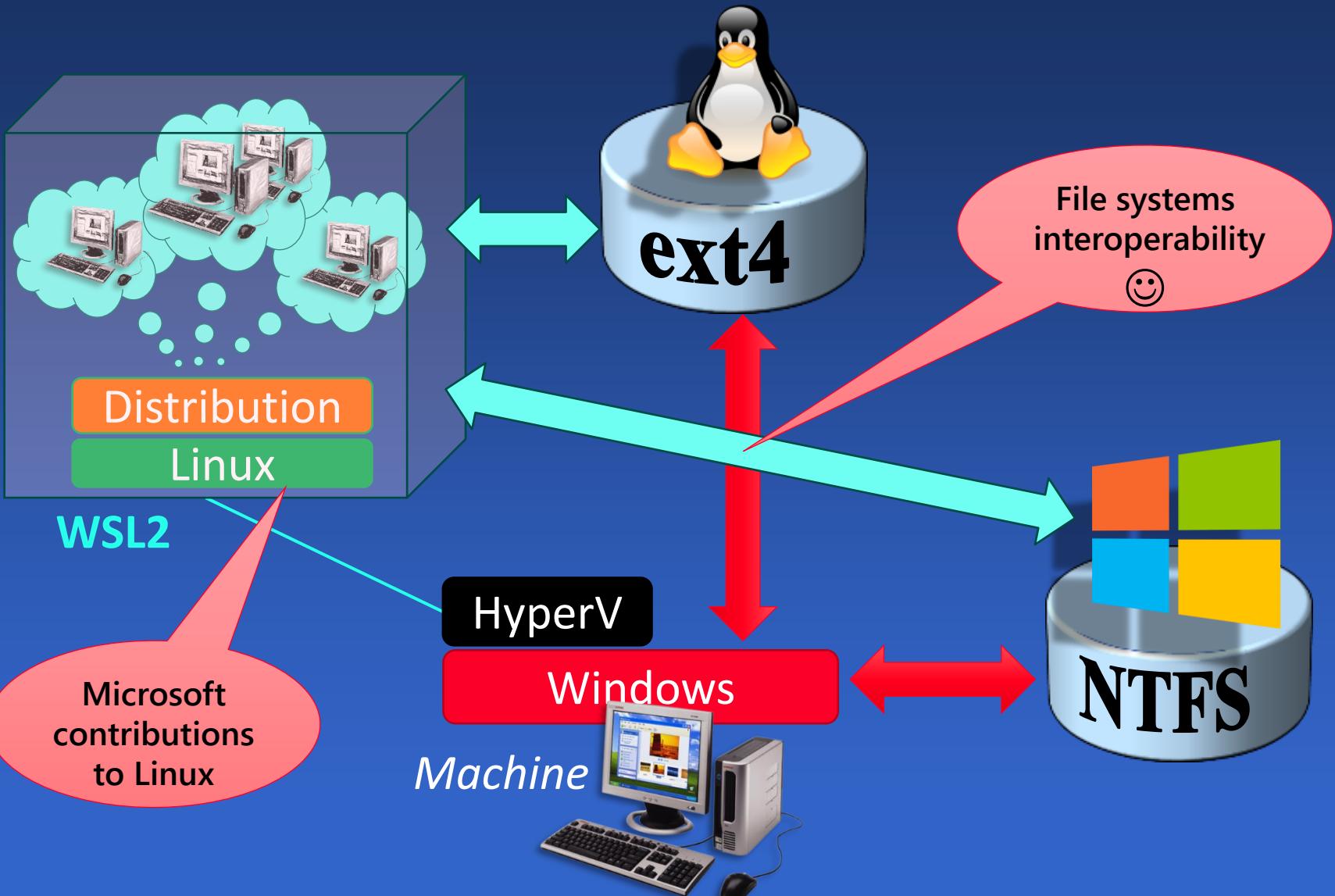
Many OSes = HyperV



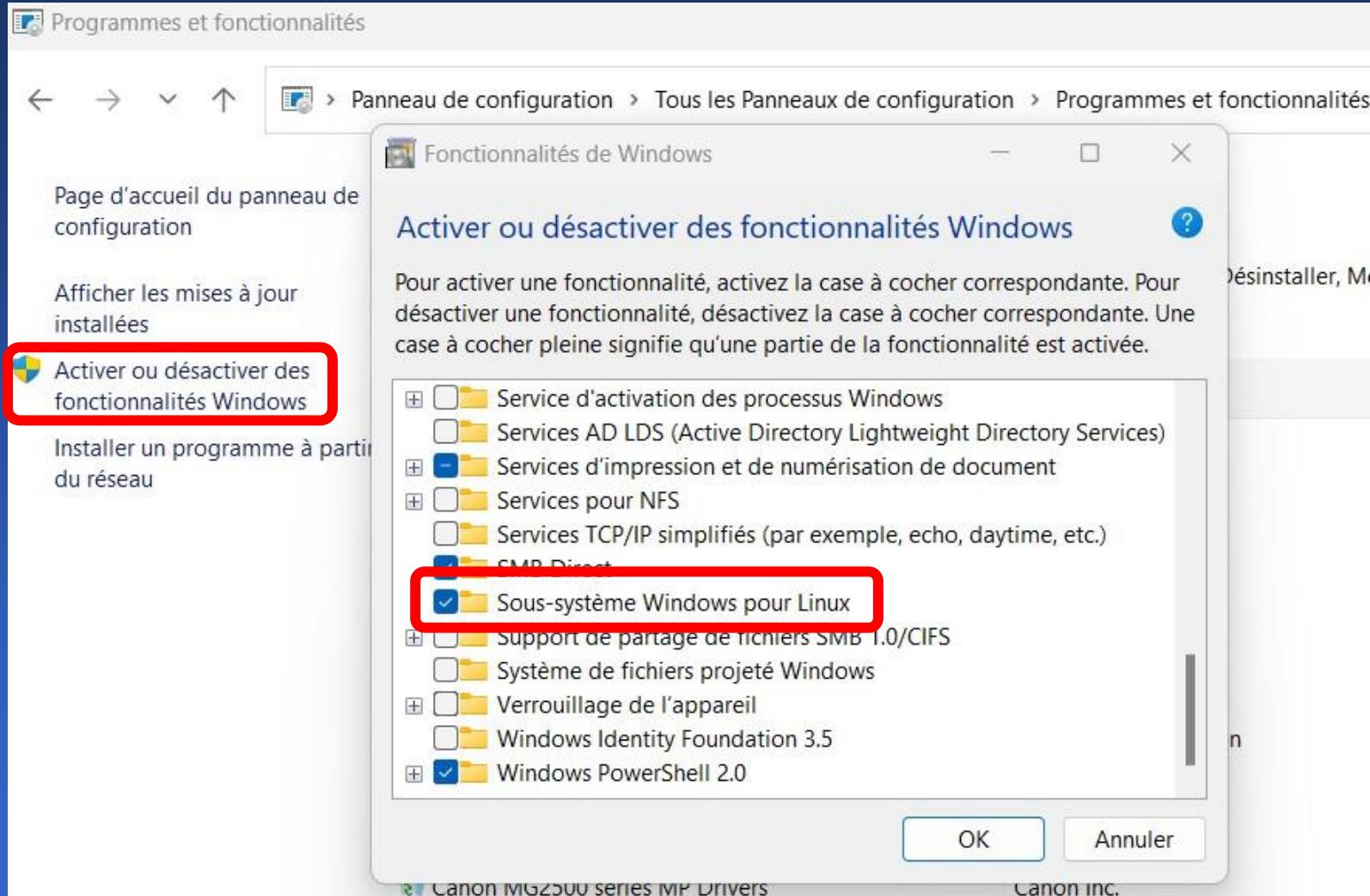
Activate HyperV in Control Panel



A native HyperV VM = WSL2



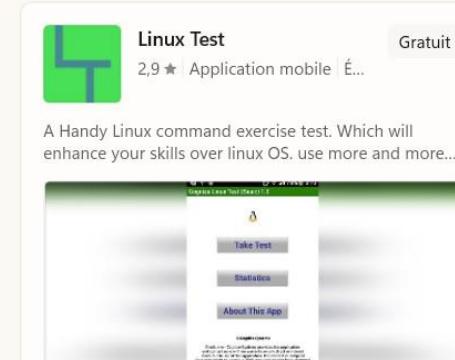
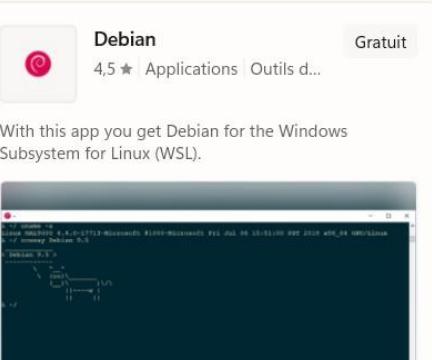
Activate WSL2 in control panel



Install a distribution

◆ Native WSL2 is limited to the Kernel

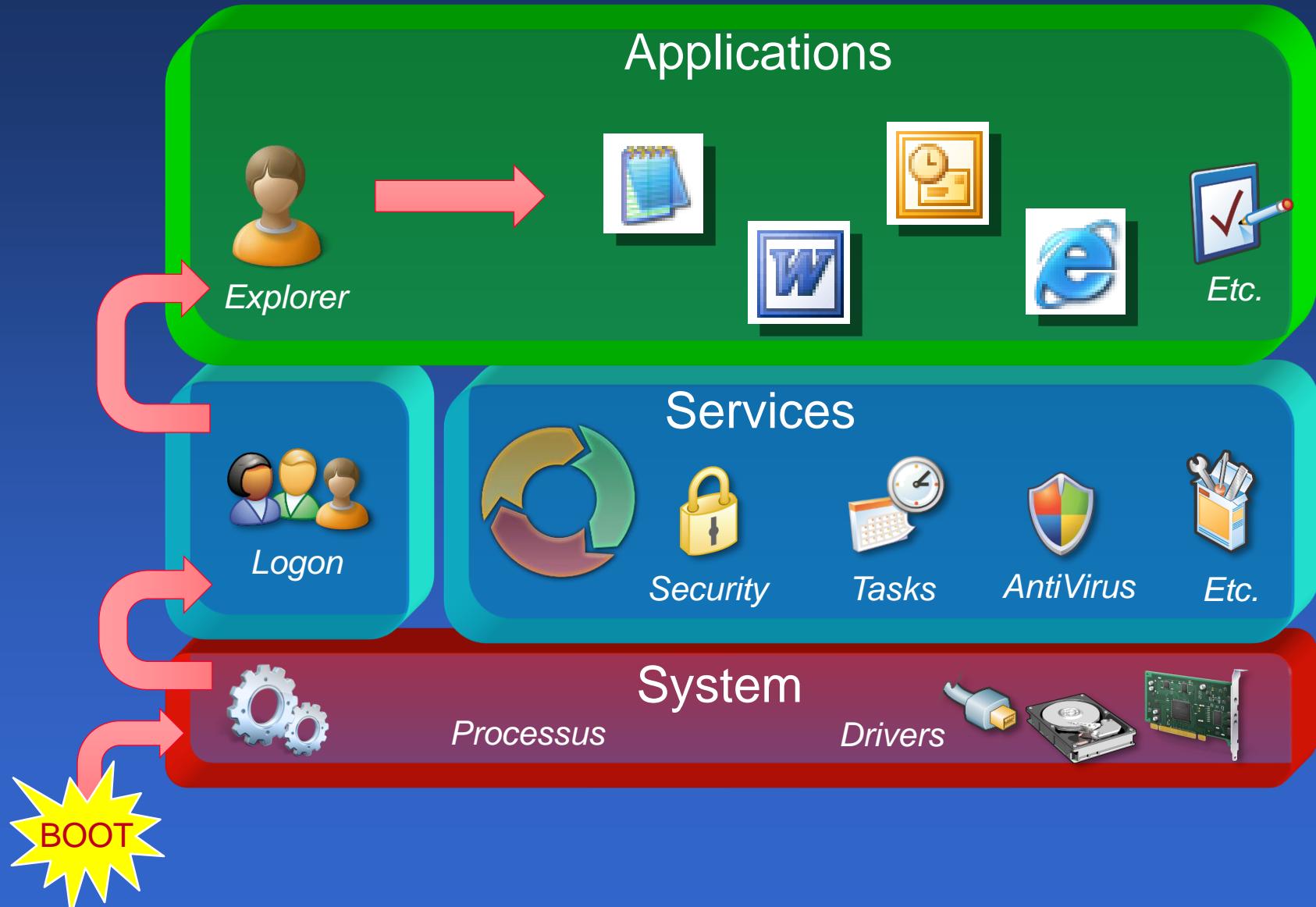
- Complete system services are in a “distribution”
- Many flavors available in the Windows Store



Windows Services

Background activities

Software layers



Services processus

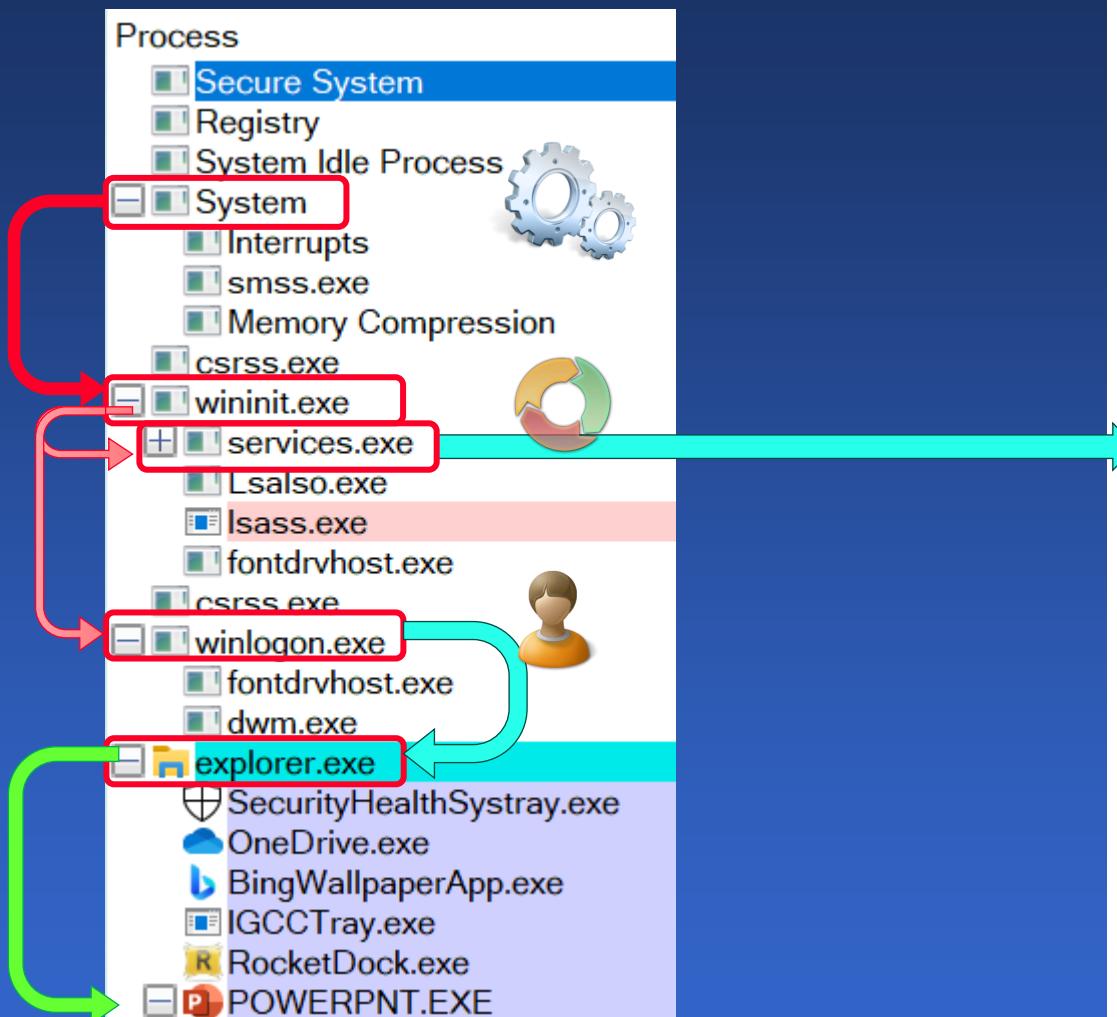
- ◆ Run before logon
 - Use system identities

- ◆ Run in the background
 - Cannot display windows of any type
 - Print in a system log (event viewer)
 - May display icons in the **SYSTRAY**



- ◆ Are controlled by the logged user
 - START
 - STOP
 - PAUSE

Process hierarchy



services.exe
svchost.exe
dllhost.exe
StartMenuExperienceHo...
RuntimeBroker.exe
RuntimeBroker.exe
TextInputHost.exe
dllhost.exe
RuntimeBroker.exe
IGCC.exe
ApplicationFrameHost.exe
FileCoAuth.exe
ShellExperienceHost.exe
UserOOBEBroker.exe
SDXHelper.exe
LockApp.exe
RuntimeBroker.exe
dllhost.exe
RuntimeBroker.exe
SearchApp.exe
CalculatorApp.exe
RuntimeBroker.exe
PhoneExperienceHost.exe
DataExchangeHost.exe
HelpPane.exe
SystemSettings.exe
Microsoft.Photos.exe
RuntimeBroker.exe
smartscreen.exe
WUDFHost.exe
svchost.exe
svchost.exe

Services in the Task Manager

Gestionnaire des tâches

Fichier Options Affichage

Processus	Performance	Historique des applications	Démarrage	Utilisateurs	Détails	Services	
Nom	PID	Description				Statut	Groupe
AarSvc		Agent Activation Runtime				Arrêté	AarSvcGroup
AarSvc_267c38		Agent Activation Runtime_267c38				Arrêté	AarSvcGroup
AESMService	21428	Intel® SGX AESM				En cours d'exéc...	
AJRouter		Service de routeur AllJoyn				Arrêté	LocalServiceNe...
ALG		Service de la passerelle de la couche Application				Arrêté	
AppIDSvc		Identité de l'application				Arrêté	LocalServiceNe...
Appinfo	10356	Informations d'application				En cours d'exéc...	netsvcs
AppMgmt	17472	Gestion d'applications				En cours d'exéc...	netsvcs
AppReadiness		Préparation des applications				Arrêté	AppReadiness
AppVClient		Microsoft App-V Client				Arrêté	
AppXSvc		Service de déploiement AppX (AppXSVC)				Arrêté	wsappx
AssignedAccessManagerSvc		Service AssignedAccessManager				Arrêté	AssignedAcces...
AudioEndpointBuilder	2200	Génération de points de terminaison du service Audio Windows				En cours d'exéc...	LocalSystemNe...
Audiosrv		Démarrer				En cours d'exéc...	LocalServiceNe...
autetimesvc		Arrêter				Arrêté	autoTimeSvc
AxInstSV		Redémarrer				Arrêté	AxInstSVGroup
BcastDVRUserService		Ouvrir les services				Arrêté	BcastDVRUserS...
BcastDVRUserService_267c38		Recherche en ligne				Arrêté	BcastDVRUserS...
DDPSVC		Accéder aux détails				Arrêté	notavice

Démarrer

Arrêter

Redémarrer

Ouvrir les services

Recherche en ligne

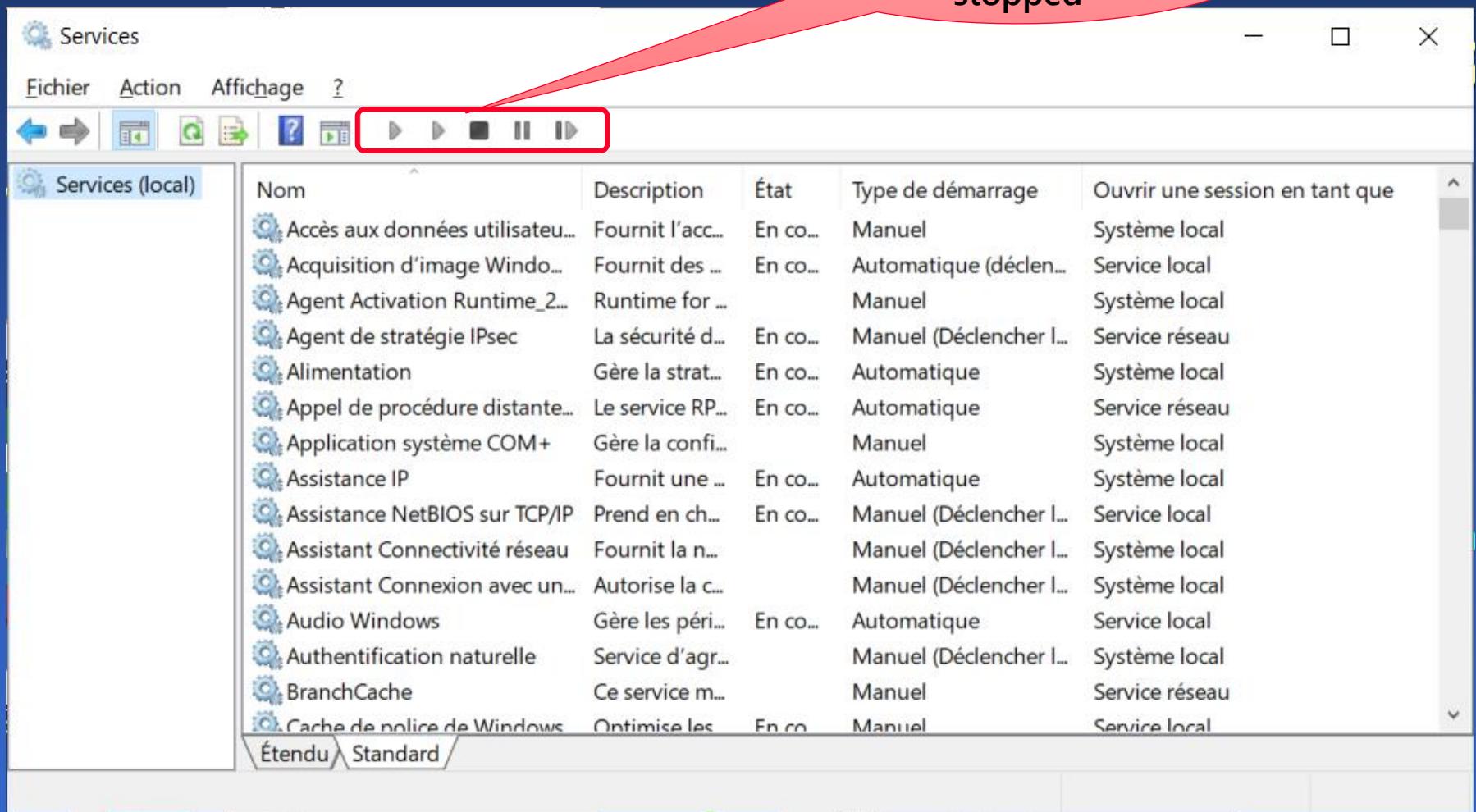
Accéder aux détails

Moins de détails | Ouvrir les services

Services console

Windows + R « services.msc »

A Service may be started, paused or stopped



Services in the registry

HKLM/SYSTEM/CurrentControlSet/Services

The screenshot shows the Windows Registry Editor window with the following details:

Titre : Éditeur du Registre

Menu : Fichier, Edition, Affichage, Favoris, ?

Adresse : Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RpcSs

Tableau des propriétés :

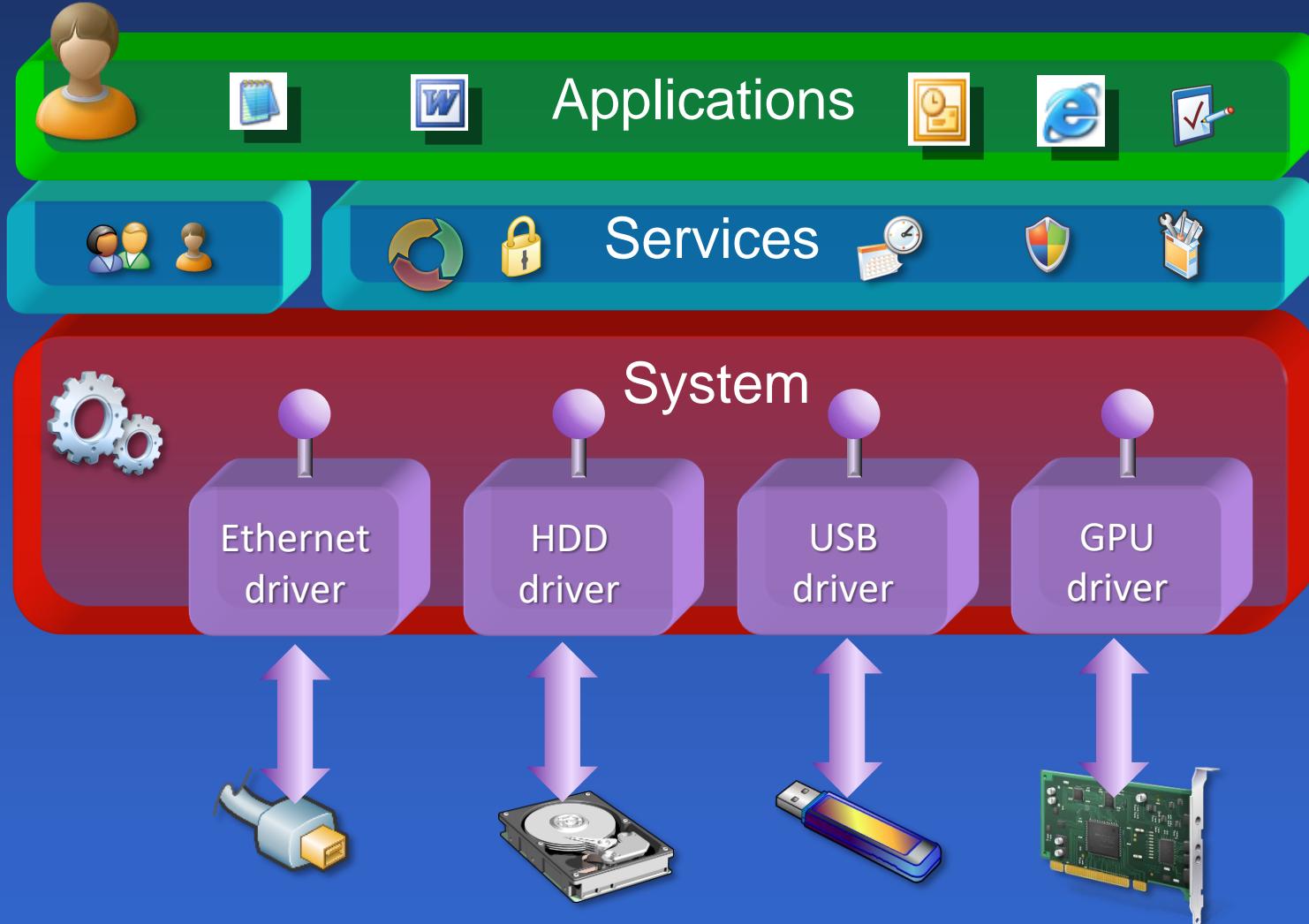
Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
DependOnService	REG_MULTI_SZ	RpcEptMapper DcomLaunch
Description	REG_SZ	@combase.dll,-5011
DisplayName	REG_SZ	@combase.dll,-5010
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 02 0...
Group	REG_SZ	COM Infrastructure
ImagePath	REG_EXPAND...	%SystemRoot%\system32\svchost.exe -k rpcss -p
MitigationFlags	REG_DWORD	0x00000001 (1)
ObjectName	REG_SZ	NT AUTHORITY\NetworkService
RequiredPrivileges	REG_MULTI_SZ	SeChangeNotifyPrivilege SeCreateGlobalPrivilege SeImpersonate...
ServiceSidType	REG_DWORD	0x00000001 (1)
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000020 (32)

Un élément de la liste est encadré en rouge et pointé par une flèche rouge vers un cercle rouge contenant le texte "Start mode".

Windows Drivers

Hardware control

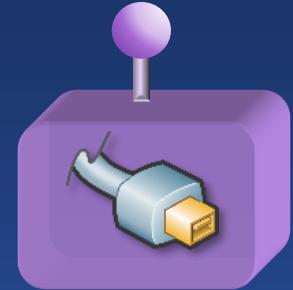
Low level Software layers



Windows Drivers

◆ Plug-in Kernel modules

- Dynamic link modules (*DLL structure*)
- Loaded by the Kernel (*.SYS extension*)
- Run at Kernel level (*Intel ring 0 = privileged*)



◆ OEM software

- Link with Kernel libraries
- Dedicated IDE (Win DDK)
- Third party kernel module may be a Threat
 - **BUGS** → MS driver certification process
 - **VIRUS** → MS driver signing process



Drivers in Proceexp

Process Explorer - Sysinternals: www.sysinternals.com [LAN\tjoubert]

File Options View Process Find Users DLL Help

CSwitch Delta CPU Private By... Working Set PID Description

System Interrupts Handles DLLs Threads

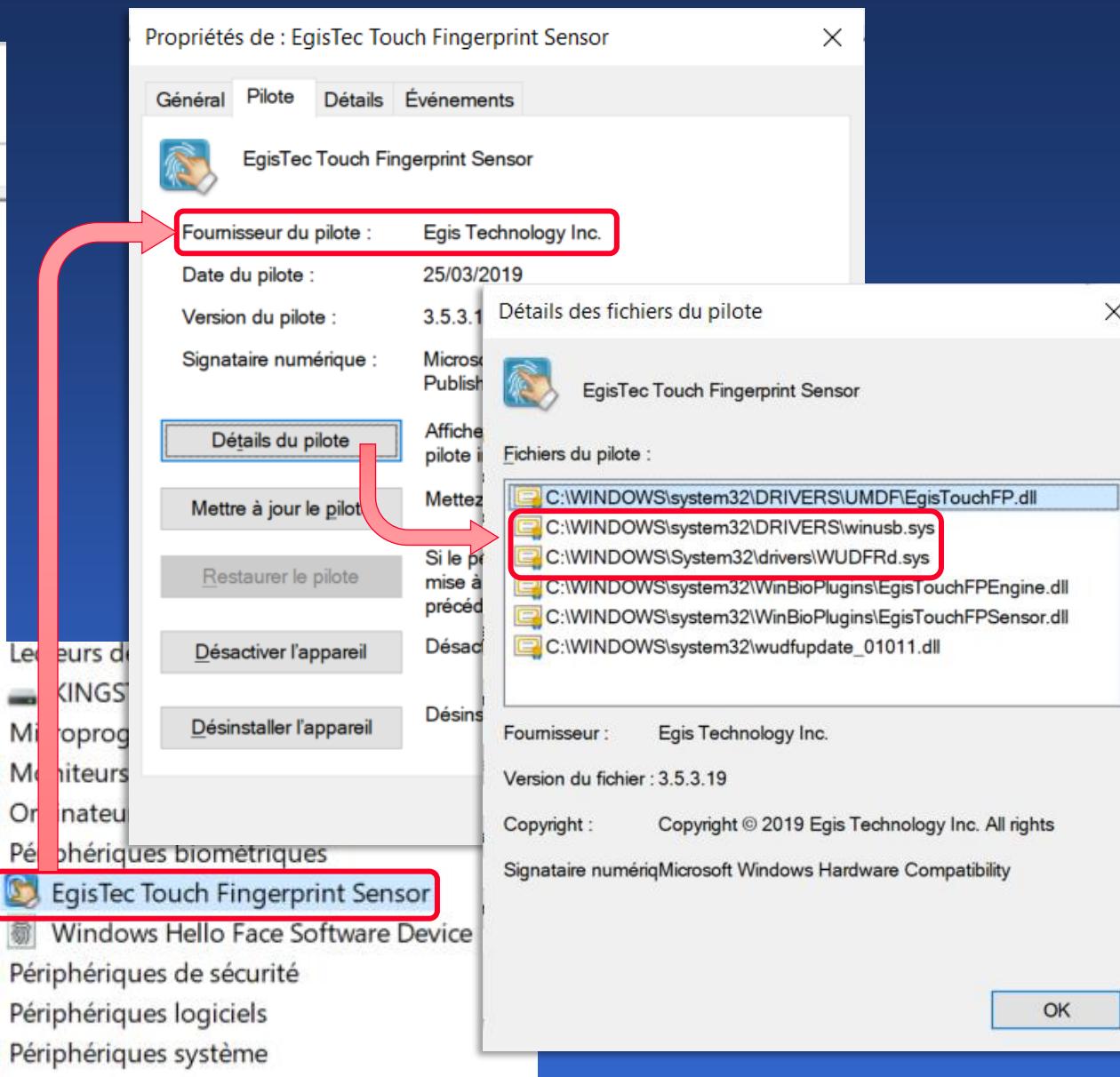
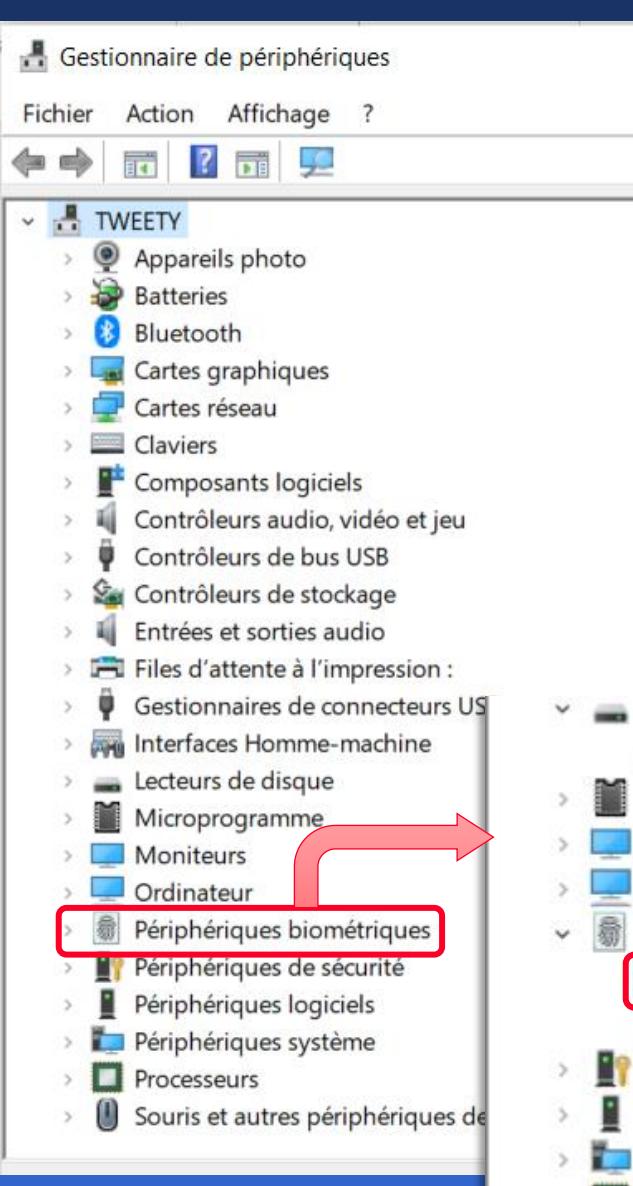
Name	Description	Company Name	Path
AcerAirplaneModeController	AcerAirplaneModeController	Acer Incorporated	C:\WINDOWS\System32\drivers\AcerAirplaneModeController.sys
CHDRT64ISST.sys	Definition Audio...	Conexant Systems I...	C:\WINDOWS\system32\drivers\CHDRT64ISST.sys
dptf_acpi.sys	Dynamic Tuning A...	Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\dptf_acpi.inf...
dptf_cpu.sys	Dynamic Tuning C...	Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\dptf_cpu.inf...
esif_lf.sys	Dynamic Tuning M...	Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\dptf_cpu.inf...
gna.sys	Intel gna device driver	Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\gna.inf_am...
HidEventFilter.sys	Intel(R) HID Event Filter	Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\hideventfilt...
iaLPSS2_GPIO2_ICL.sys	Intel(R) Serial IO GPIO Driv...	Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\ialpss2_gpi...
iaLPSS2_I2C_ICL.sys	Intel(R) Serial IO I2C Driver...	Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\ialpss2_i2c...
iaLPSS2_SPI_ICL.sys	Intel(R) Serial IO SPI Driver...	Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\ialpss2_spi...
iaLPSS2_UART2_ICL.sys	Intel(R) Serial IO UART Dri...	Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\ialpss2_uar...
iaStorAC.sys	Intel(R) Rapid Storage Tec...	Intel Corporation	C:\WINDOWS\System32\drivers\iaStorAC.sys
ibtusb.sys	Intel(R) Wireless Bluetooth...	Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\ibtusb.inf_a...
igdkmdn64.sys	Intel Graphics Kernel Mode...	Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\iigd_dch.inf...
Netwtw10.sys	Intel® Wireless WiFi Link D...	Intel Corporation	C:\WINDOWS\System32\drivers\Netwtw10.sys
TbtBusDrv.sys	Thunderbolt(TM) Bus Driver	Intel Corporation	C:\WINDOWS\System32\drivers\TbtBusDrv.sys
TeeDriverW10x64.sys	Intel(R) Management Engin...	Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\heci.inf_am...
IntcAudioBus.sys	Intel® Smart Sound Techno...	Intel(R) Corporatio...	C:\WINDOWS\System32\DriverStore\FileRepository\intcaudiobu...
IntcDAud.sys	Intel(R) Display Audio Driver	Intel(R) Corporatio...	C:\WINDOWS\System32\DriverStore\FileRepository\intcdaud.inf...
IntcDMic.sys	Intel® Smart Sound Techno...	Intel(R) Corporatio...	C:\WINDOWS\System32\DriverStore\FileRepository\intcdmic.inf...

CPU Usage: 1.31% Commit Charge: 54.55% Processes: 226 Physical Usage: 46.28%

Loaded kernel DLLs

OEMs

drivers in Computer Management



Drivers in the Registry

HKLM/SYSTEM/CurrentControlSet/Services

The screenshot shows the Windows Registry Editor window. The title bar reads "Éditeur du Registre". The menu bar includes "Fichier", "Edition", "Affichage", "Favoris", and "?". The main pane displays the registry key "Ordinateur\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ACPI". The left pane shows a tree view of subkeys: AarSvc, AarSvc_267c38, AcerAirplaneModeController, ACPI (selected), Enum, Parameters, AcpiDev, acpiex, acpipagr, AcpiPmi, acpitime, Acx01000, ADOVMPackage, ADP80XX, ads, AESMService, AFD, afunix, ahcache. The right pane is a table with columns "Nom", "Type", and "Données". It lists several registry entries for the ACPI service, with "ImagePath" highlighted by a red rectangle. The table data is as follows:

Nom	Type	Données
(par défaut)	REG_SZ	(valeur non définie)
DisplayName	REG_SZ	@acpi.inf,%ACPI.SvcDesc%;Microsoft ACPI Driver
ErrorControl	REG_DWORD	0x00000003 (3)
Group	REG_SZ	Core
ImagePath	REG_EXPAND...	System32\drivers\ACPI.sys
Owners	REG_MULTI_SZ	acpi.inf
Start	REG_DWORD	0x00000000 (0)
Tag	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000001 (1)

Drivers in Autoruns

Autoruns - Sysinternals: www.sysinternals.com

File Search Entry Options Category Help

Quick Filter

Applinit Known DLLs WinLogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Office

Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks

Autoruns Entry	Description	Publisher	Image Path	Timestamp
HKLM\System\CurrentControlSet\Services				Sun Jan 8 10:26:19
<input checked="" type="checkbox"/> AcerAirplaneModeController	Acer Airplane Mode Controller: AcerAirplaneMo...	(Verified) Acer Incorporated	C:\WINDOWS\System32\drivers\AcerAirplaneModeController...	Tue May 12 22:29:
<input checked="" type="checkbox"/> CnxtHdAudService	Synaptics UAA Function Driver for High Definitio...	(Verified) Synaptics Incorpor...	C:\WINDOWS\system32\drivers\CHDRT64ISST.sys	Wed Feb 24 17:43:
<input checked="" type="checkbox"/> dg_ssudbus	SAMSUNG Mobile USB Composite Device Dri...	(Verified) Samsung Electron...	C:\WINDOWS\system32\DRIVERS\ssudbus2.sys	Fri Sep 30 06:23:56
<input checked="" type="checkbox"/> dptf_acpi	dptf_acpi: Intel(R) Dynamic Tuning ACPI Partici...	(Verified) Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\dptf_acpi...	Tue Mar 24 14:49:4
<input checked="" type="checkbox"/> dptf_cpu	dptf_cpu: Intel(R) Dynamic Tuning CPU Particip...	(Verified) Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\dptf_cpu...	Tue Mar 24 14:49:4
<input checked="" type="checkbox"/> esif_if	esif_if: Intel(R) Dynamic Tuning Manager Partici...	(Verified) Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\dptf_cpu...	Tue Mar 24 14:49:5
<input checked="" type="checkbox"/> FTDIBUS	USB Serial Converter Driver: D2XX Driver	(Verified) Future Technology...	C:\WINDOWS\system32\drivers\ftdibus.sys	Thu Jul 8 08:55:30
<input checked="" type="checkbox"/> FTSER2K	USB Serial Port Driver: D2XX Serial Device Dri...	(Verified) Future Technology...	C:\WINDOWS\system32\drivers\ftser2k.sys	Thu Jul 8 08:55:34
<input checked="" type="checkbox"/> HidEventFilter	Intel(R) HID Event Filter: Intel(R) HID Event Filter	(Verified) Intel(R) Software	C:\WINDOWS\System32\DriverStore\FileRepository\hideventfi...	Thu Apr 18 22:56:4:
<input checked="" type="checkbox"/> iaLPSS2_GPIO2	Intel(R) Serial IO GPIO Driver v2: Intel(R) Serial...	(Verified) Intel(R) Embedde...	C:\WINDOWS\System32\DriverStore\FileRepository\ialpss2_g...	Tue May 7 19:59:1
<input checked="" type="checkbox"/> iaLPSS2 GPIO2 ICL	Intel(R) Serial IO GPIO Driver v2: Intel(R) Serial...	(Verified) Intel Corporation	C:\WINDOWS\System32\DriverStore\FileRepository\ialpss2_g...	Tue Apr 28 00:18:1

 CnxtHdAudService Size: 2 199 K
Synaptics UAA Function Driver for Hig Time: Wed Feb 24 17:43:38 2021
(Verified) Synaptics Incorporated Version: 9.0.282.0
C:\WINDOWS\system32\drivers\CHDRT64ISST.sys

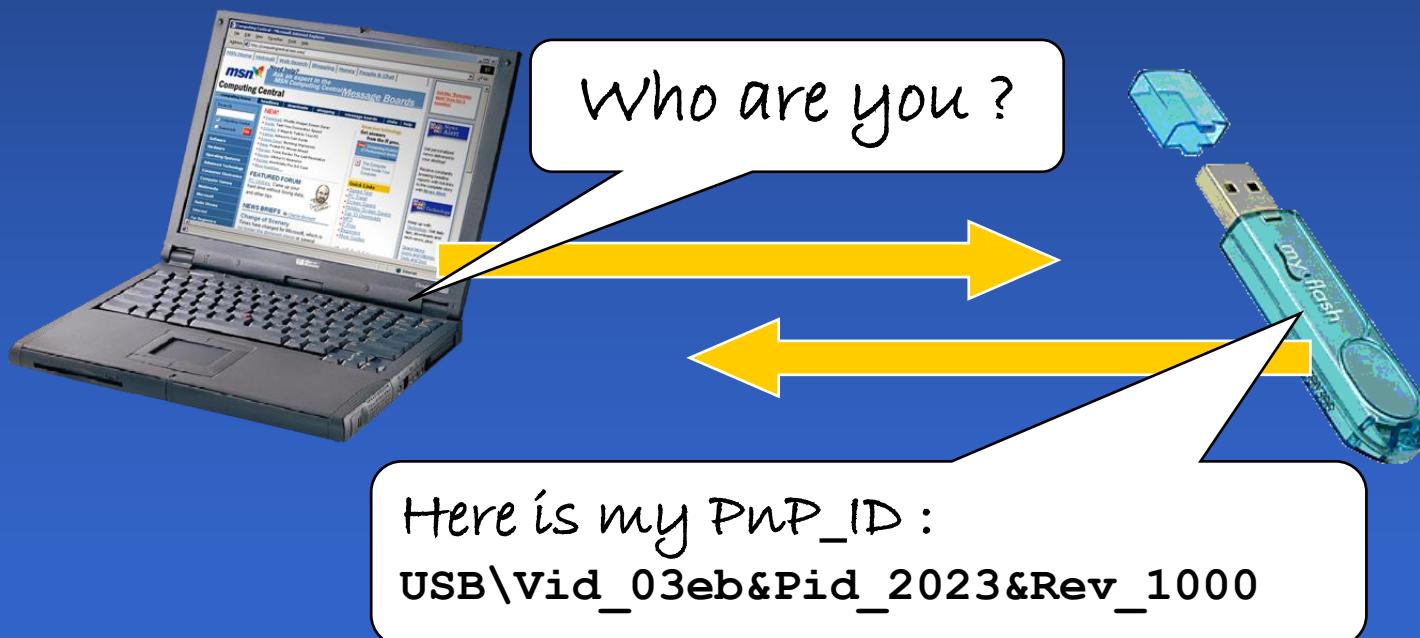
Ready

Hardware unique IDs

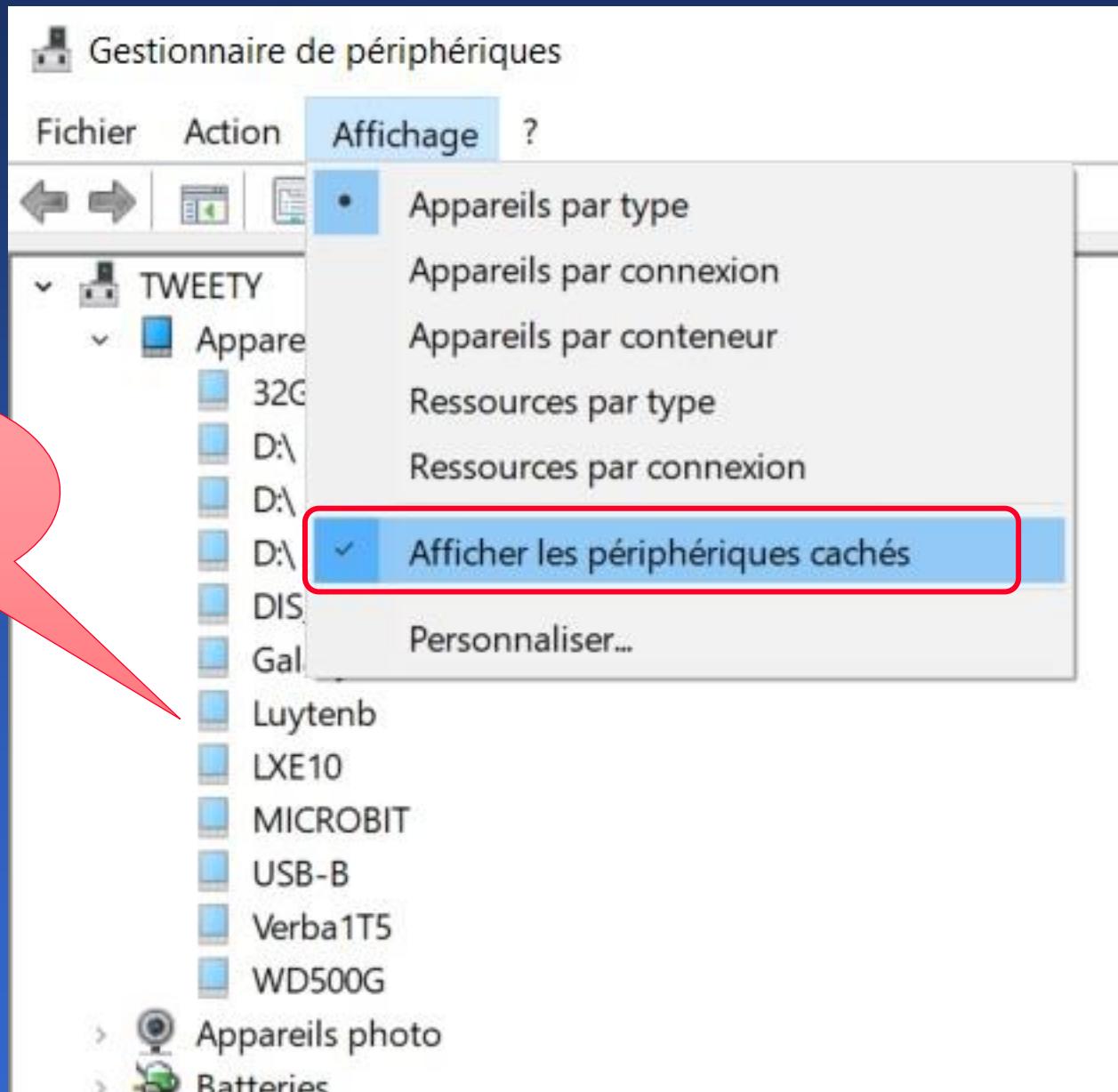
◆ Hardware query

- Fixed devices (PCI ...) in **HKLM/HARDWARE**
- Runtime Query protocol for Plug&Play devices

◆ Each device type has a **UNIQUE ID**



Known Plug&Play devices



Driver update & Install sources

◆ Microsoft official repository

- Contains WindowsUpdate & OEM Drivers
- MSFT certified OEM drivers
 - Bug free
 - Valid signature
- **This MUST always be your first try**



◆ OEM official Web repository

- Installers (setup.exe, etc.)
- Driver packages (.zip files)
- **This is only a second choice... for « weak » OEMs**

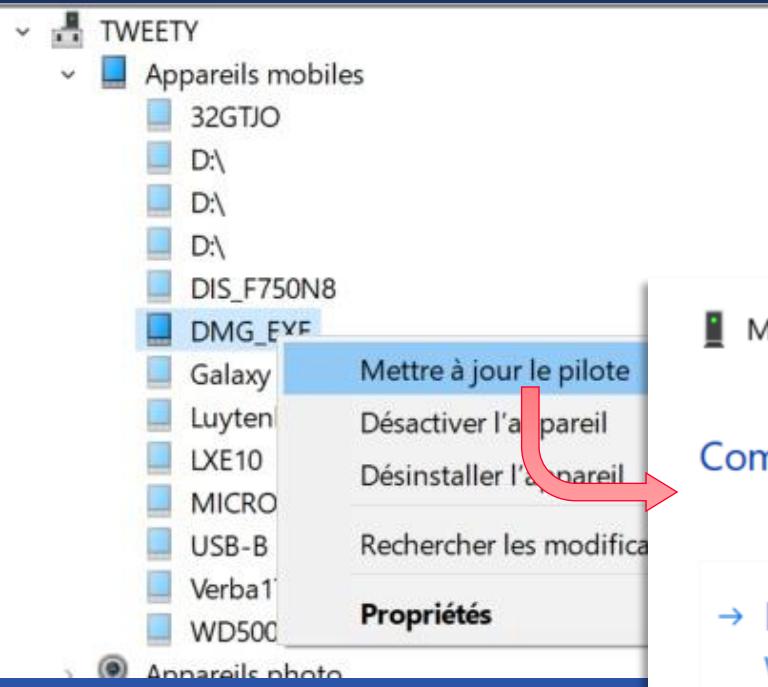


◆ Drivers HoneyPots (*top Search results*)

- Malware, Spamware Inc.
- Keep away - **unless you REALLY know what you do!**



Driver manual installation



■ Mettre à jour les pilotes - DMG_EXF



Microsoft
Official

Comment voulez-vous rechercher les pilotes ?

→ Rechercher automatiquement les pilotes

Windows recherche sur votre ordinateur le meilleur pilote disponible et l'installe sur votre appareil.

→ Parcourir mon poste de travail pour rechercher des pilotes

Localisez et installez un pilote manuellement.



Potential
road to HELL

Install an OEM driver

Mettre à jour les pilotes - DMG_EXE

Rechercher des pilotes sur votre ordinateur

Rechercher les pilotes à cet emplacement :

`C:\elisme\BigPixel\Software\USB_Driver\Windows-CH340-Driver`

Inclure les sous-dossiers

→ Choisir parmi une liste de pilotes disponibles sur mon ordinateur
Cette liste affichera les pilotes disponibles compatibles avec l'appareil ainsi que tous ceux dans la même catégorie que l'appareil.

Local folder containing the driver files



Re-use an existing driver

Files of an OEM Driver

◆ OEM installation script → **.inf**

- Go to **/Windows/inf**
- **Manufacturer** section = **Hardware_ID**

```
%USB\VID_1194&PID_0004.DeviceDesc%=FB11USB.Dev, USB\VID_1194&PID_0004
```

- **AddReg** section = Registry actions
- **CopyFiles** section = Files copy

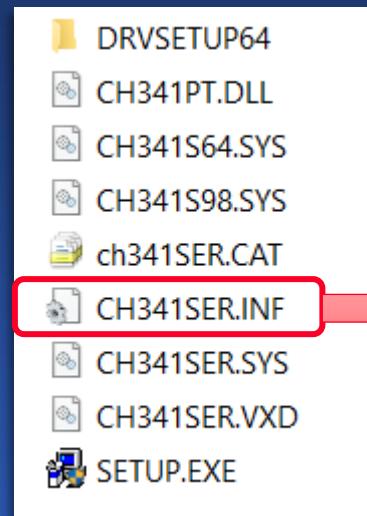
◆ Kernel DLL → **.sys**

- Go to **/Windows/System32/drivers**

◆ User code → **.exe, .dll, .cpl**

- Go to **/Windows/System32**

Example of OEM driver

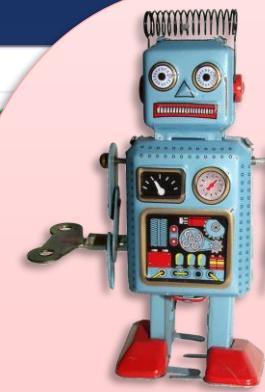


```
; CH341SER.INF
; Driver for CH341 (USB=>SERIAL chip)
; WDM&VXD for Windows 98/Me/2000/XP/7/8/10
; Copyright (C) W.ch 2001-2014
;

[Version]
Signature = "$Chicago$"
Class = Ports
ClassGuid = {4D36E978-E325-11CE-BFC1-00AA0000309D}
Provider = %WinChipHead%
DriverVer = 08/08/2014, 3.4.2014.0
CatalogFile = CH341SER.CAT

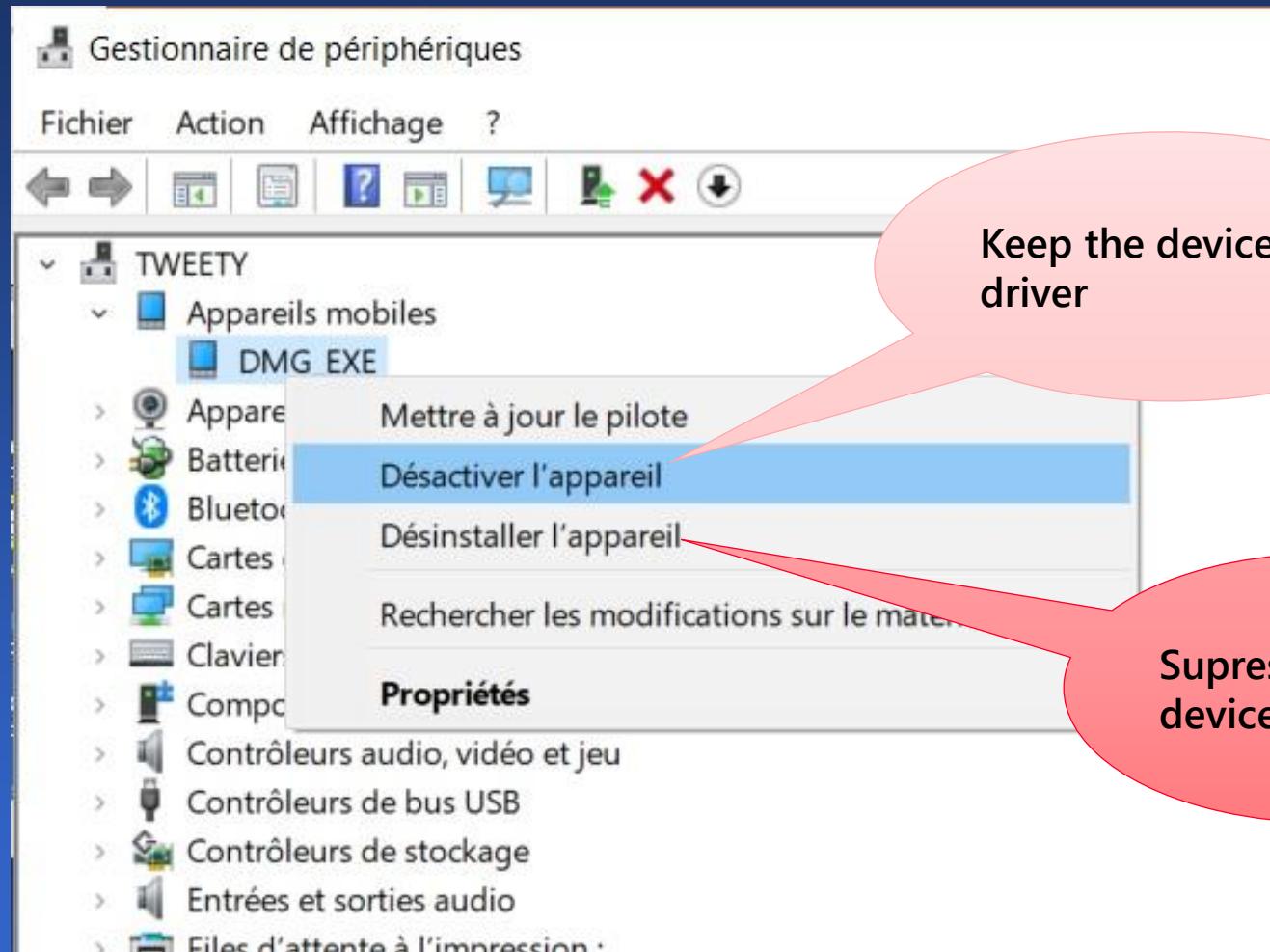
[ControlFlags]
ExcludeFromSelect = USB\VID_1A86&PID_7523
ExcludeFromSelect = USB\VID_1A86&PID_5523
ExcludeFromSelect = USB\VID_4348&PID_5523
ExcludeFromSelect = USB\VID_4348&PID_5523&REV_0250
ExcludeFromSelect = USBSERPORT\SER5523
ExcludeFromSelect = CH341PORT\SER5523

[Manufacturer]
%WinChipHead% = WinChipHead,NT,NTamd64,NTia64
```



OEM P&P IDs

Device control



Keep the device driver



Supress the device driver



