BIOS

The BIOS (Basic Input-Output System) is the software built into a chip on the motherboard, which locates and recognizes all the devices necessary to load the operating system.

Protection measures:

- Protect the BIOS with a password.
- Do not allow booting from a CD or USB Device.
- Physical Security, someone with access to the equipment could reset the BIOS by removing the battery and returning the configuration to its original values, although in more modern devices it would be more complicated because they store the configuration in an EEPROM memory.
- Manufacturer BIOS passwords.
  https://www.cgsecurity.org/wiki/CmosPwd

Bypass BIOS passwords

Some tools allow you to manage BIOS passwords from the operating system, one of the most popular is Cmospwd, it requires execution privileges because it requires the installation of a service.

http://www.cgsecurity.org/wiki/CmosPwd

```
C:\>ioperm.exe –i
C:\>net Start ioperm
C:\>Cmospwd_win
     1 – Kill cmos
     2 – Kill cmos 8try to keep date and time)
     0 – Abort
C:\> Ioperm -u
```

Hard drive password

Modern BIOS allow to protect access to the hard drive using a password, some brands call it DriveLock or ATA Password, this password does not encrypt the hard drive, it prevents access by compatible systems at the driver level, non-compatible systems do not they will recognize the disk.

Code injection

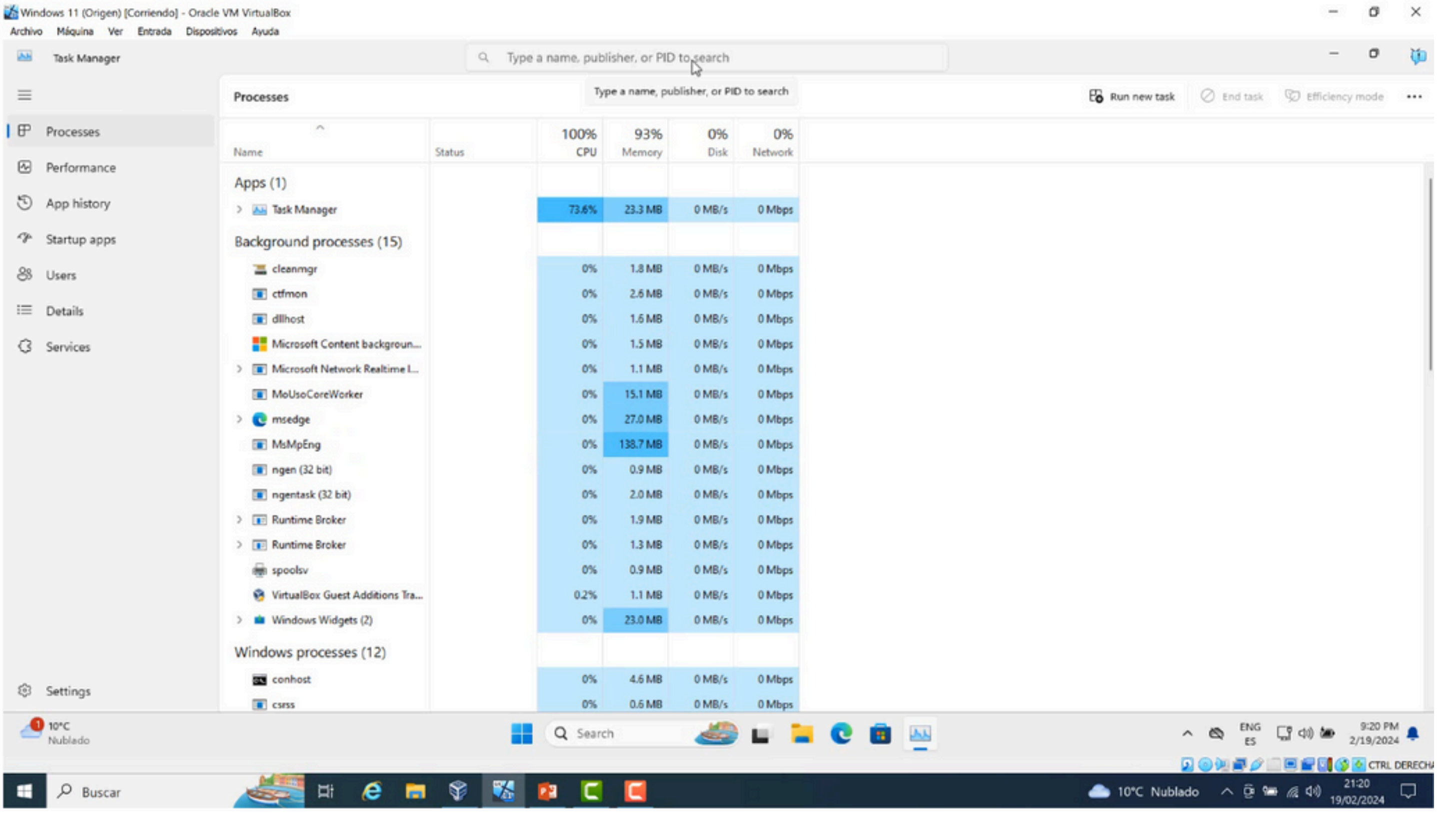
The hardware includes a technology capable of marking memory pages as “non-executable” to prevent code injection. The name of this technology varies depending on the manufacturer: NX, XN, XD, DEP or Enhanced Virus Protection.

The operating system must recognize this processor technology to be able to use it, in Windows it has been used since Windows XP SP2, in addition in Windows there is the possibility of activating DEP by software, although it is a different protection that controls the safe handling of exceptions.

The software must be compiled to take advantage of DEP, to test if an executable can use this technology it is necessary to inspect its PE headers. Use PEStudio, PETools or ExplorerSuite.

http://www.winitor.net/
http://www.ntcore.com

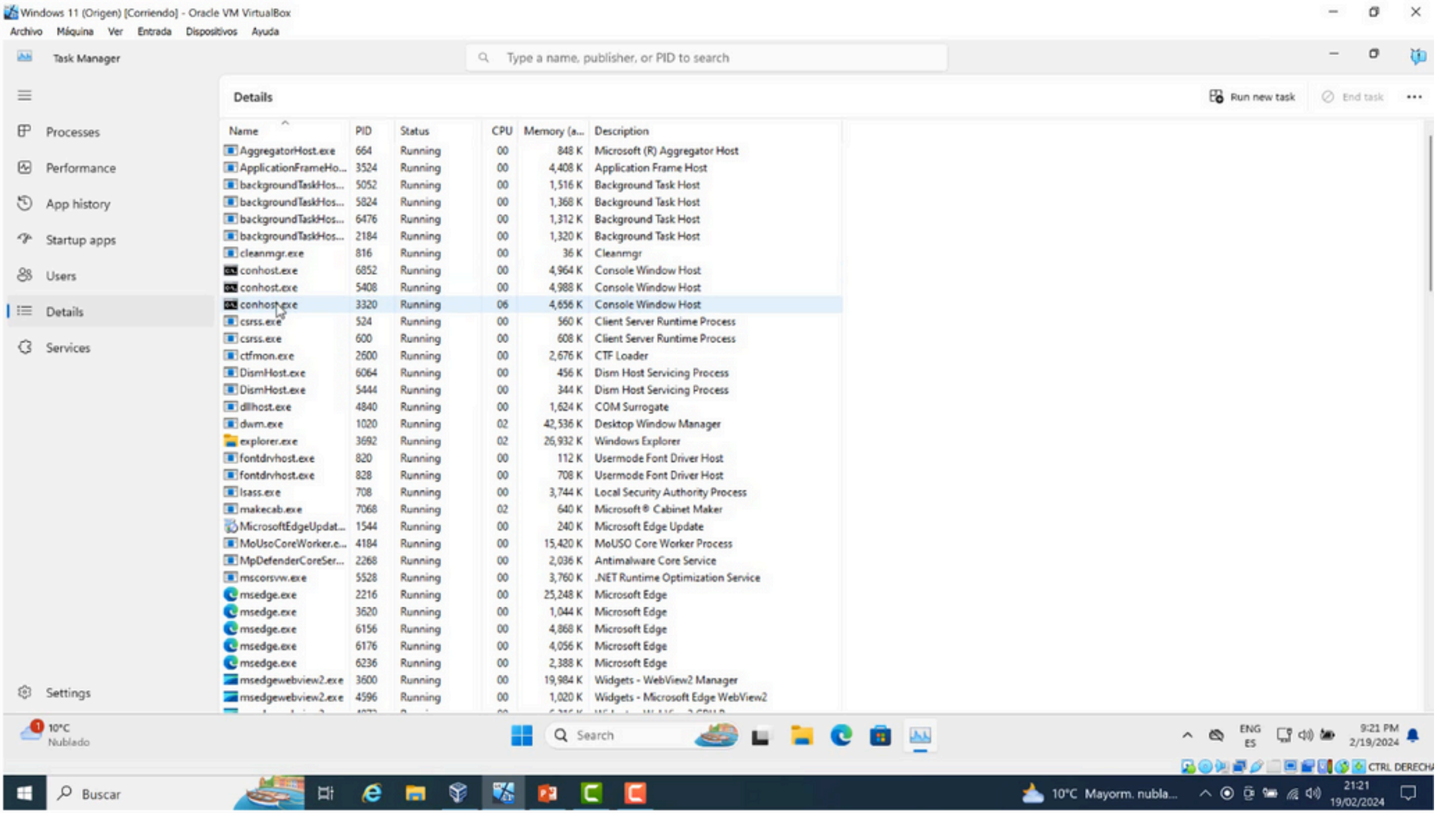
The task manager also shows us if DEP is activated in a process.



Processes

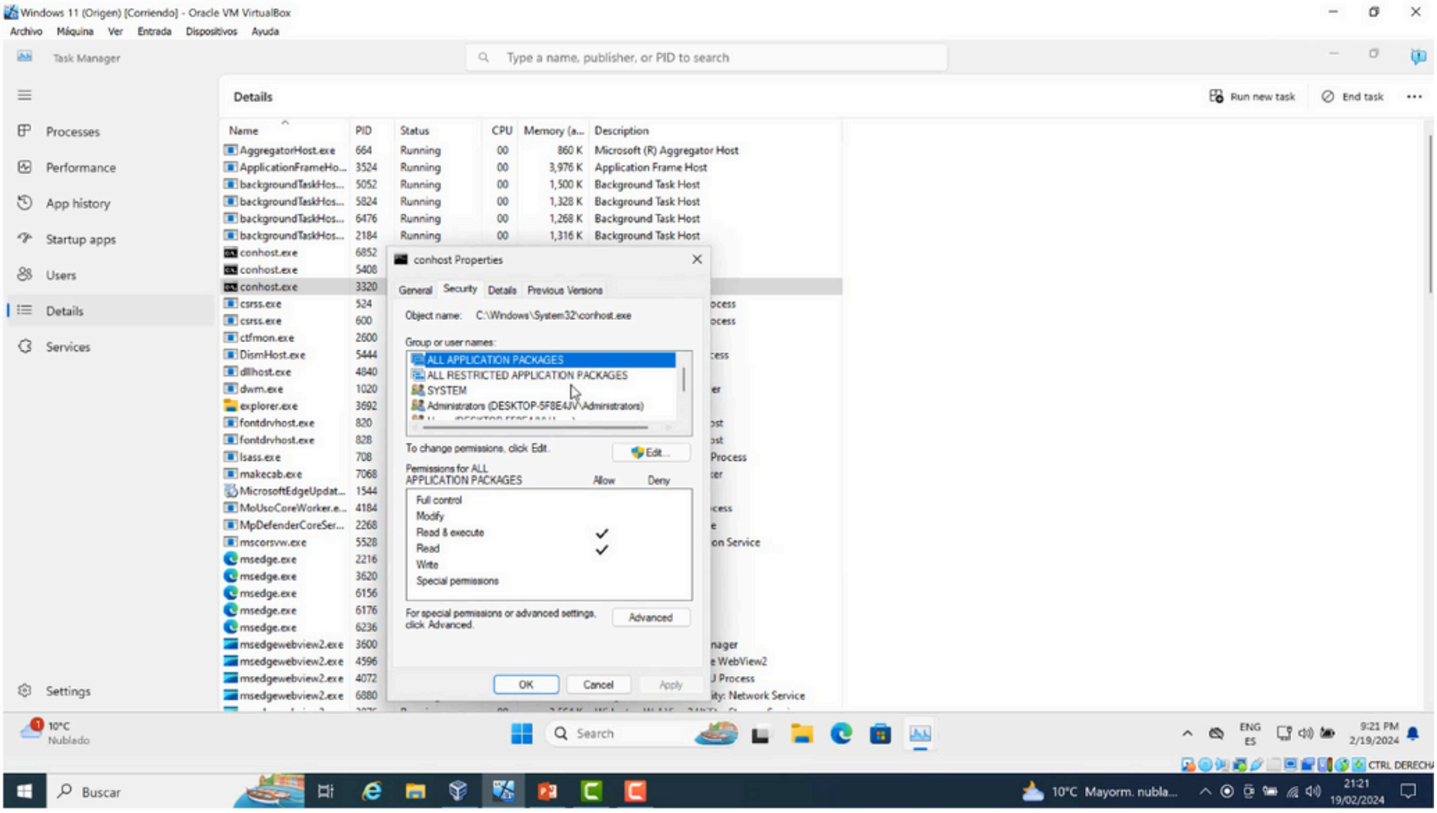
Type a name, publisher, or PID to search

Name	Status	100% CPU	93% Memory	0% Disk	0% Network
Apps (1)					
Task Manager		73.6%	23.3 MB	0 MB/s	0 Mbps
Background processes (15)					
cleanmgr		0%	1.8 MB	0 MB/s	0 Mbps
ctfmon		0%	2.6 MB	0 MB/s	0 Mbps
dllhost		0%	1.6 MB	0 MB/s	0 Mbps
Microsoft Content backgroun...		0%	1.5 MB	0 MB/s	0 Mbps
Microsoft Network Realtime I...		0%	1.1 MB	0 MB/s	0 Mbps
MoUsoCoreWorker		0%	15.1 MB	0 MB/s	0 Mbps
msedge		0%	27.0 MB	0 MB/s	0 Mbps
MsMpEng		0%	138.7 MB	0 MB/s	0 Mbps
ngen (32 bit)		0%	0.9 MB	0 MB/s	0 Mbps
ngentask (32 bit)		0%	2.0 MB	0 MB/s	0 Mbps
Runtime Broker		0%	1.9 MB	0 MB/s	0 Mbps
Runtime Broker		0%	1.3 MB	0 MB/s	0 Mbps
spoolsv		0%	0.9 MB	0 MB/s	0 Mbps
VirtualBox Guest Additions Tra...		0.2%	1.1 MB	0 MB/s	0 Mbps
Windows Widgets (2)		0%	23.0 MB	0 MB/s	0 Mbps
Windows processes (12)					
conhost		0%	4.6 MB	0 MB/s	0 Mbps
csrss		0%	0.6 MB	0 MB/s	0 Mbps



Details

Name	PID	Status	CPU	Memory (a...	Description
AggregatorHost.exe	664	Running	00	848 K	Microsoft (R) Aggregator Host
ApplicationFrameHo...	3524	Running	00	4,408 K	Application Frame Host
backgroundTaskHos...	5052	Running	00	1,516 K	Background Task Host
backgroundTaskHos...	5824	Running	00	1,368 K	Background Task Host
backgroundTaskHos...	6476	Running	00	1,312 K	Background Task Host
backgroundTaskHos...	2184	Running	00	1,320 K	Background Task Host
cleanmgr.exe	816	Running	00	36 K	Cleanmgr
conhost.exe	6852	Running	00	4,964 K	Console Window Host
conhost.exe	5408	Running	00	4,988 K	Console Window Host
conhost.exe	3320	Running	06	4,656 K	Console Window Host
csrss.exe	524	Running	00	560 K	Client Server Runtime Process
csrss.exe	600	Running	00	608 K	Client Server Runtime Process
ctfmon.exe	2600	Running	00	2,676 K	CTF Loader
DismHost.exe	6064	Running	00	456 K	Dism Host Servicing Process
DismHost.exe	5444	Running	00	344 K	Dism Host Servicing Process
dllhost.exe	4840	Running	00	1,624 K	COM Surrogate
dwm.exe	1020	Running	02	42,536 K	Desktop Window Manager
explorer.exe	3692	Running	02	26,932 K	Windows Explorer
fontdrvhost.exe	820	Running	00	112 K	Usermode Font Driver Host
fontdrvhost.exe	828	Running	00	708 K	Usermode Font Driver Host
lsass.exe	708	Running	00	3,744 K	Local Security Authority Process
makecab.exe	7068	Running	02	640 K	Microsoft® Cabinet Maker
MicrosoftEdgeUpdat...	1544	Running	00	240 K	Microsoft Edge Update
MoUsoCoreWorker.e...	4184	Running	00	15,420 K	MoUSO Core Worker Process
MpDefenderCoreSer...	2268	Running	00	2,036 K	Antimalware Core Service
mscorsvw.exe	5528	Running	00	3,760 K	.NET Runtime Optimization Service
msedge.exe	2216	Running	00	25,248 K	Microsoft Edge
msedge.exe	3620	Running	00	1,044 K	Microsoft Edge
msedge.exe	6156	Running	00	4,868 K	Microsoft Edge
msedge.exe	6176	Running	00	4,056 K	Microsoft Edge
msedge.exe	6236	Running	00	2,388 K	Microsoft Edge
msedgewebview2.exe	3600	Running	00	19,984 K	Widgets - WebView2 Manager
msedgewebview2.exe	4596	Running	00	1,020 K	Widgets - Microsoft Edge WebView2



Details

Name	PID	Status	CPU	Memory (a...	Description
AggregatorHost.exe	664	Running	00	860 K	Microsoft (R) Aggregator Host
ApplicationFrameHo...	3524	Running	00	3,976 K	Application Frame Host
backgroundTaskHos...	5052	Running	00	1,500 K	Background Task Host
backgroundTaskHos...	5824	Running	00	1,328 K	Background Task Host
backgroundTaskHos...	6476	Running	00	1,268 K	Background Task Host
backgroundTaskHos...	2184	Running	00	1,316 K	Background Task Host
conhost.exe	6852				
conhost.exe	5408				
conhost.exe	3320				
csrss.exe	524				
csrss.exe	600				
ctfmon.exe	2600				
DismHost.exe	5444				
dllhost.exe	4840				
dwm.exe	1020				
explorer.exe	3692				
fontdrvhost.exe	820				
fontdrvhost.exe	828				
lsass.exe	708				
makecab.exe	7068				
MicrosoftEdgeUpdat...	1544				
MoUsoCoreWorker.e...	4184				
MpDefenderCoreSer...	2268				
mscorsvw.exe	5528				
msedge.exe	2216				
msedge.exe	3620				
msedge.exe	6156				
msedge.exe	6176				
msedge.exe	6236				
msedgewebview2.exe	3600				
msedgewebview2.exe	4596				
msedgewebview2.exe	4072				
msedgewebview2.exe	6880				

conhost Properties

General | Security | Details | Previous Versions

Object name: C:\Windows\System32\conhost.exe

Group or user names:

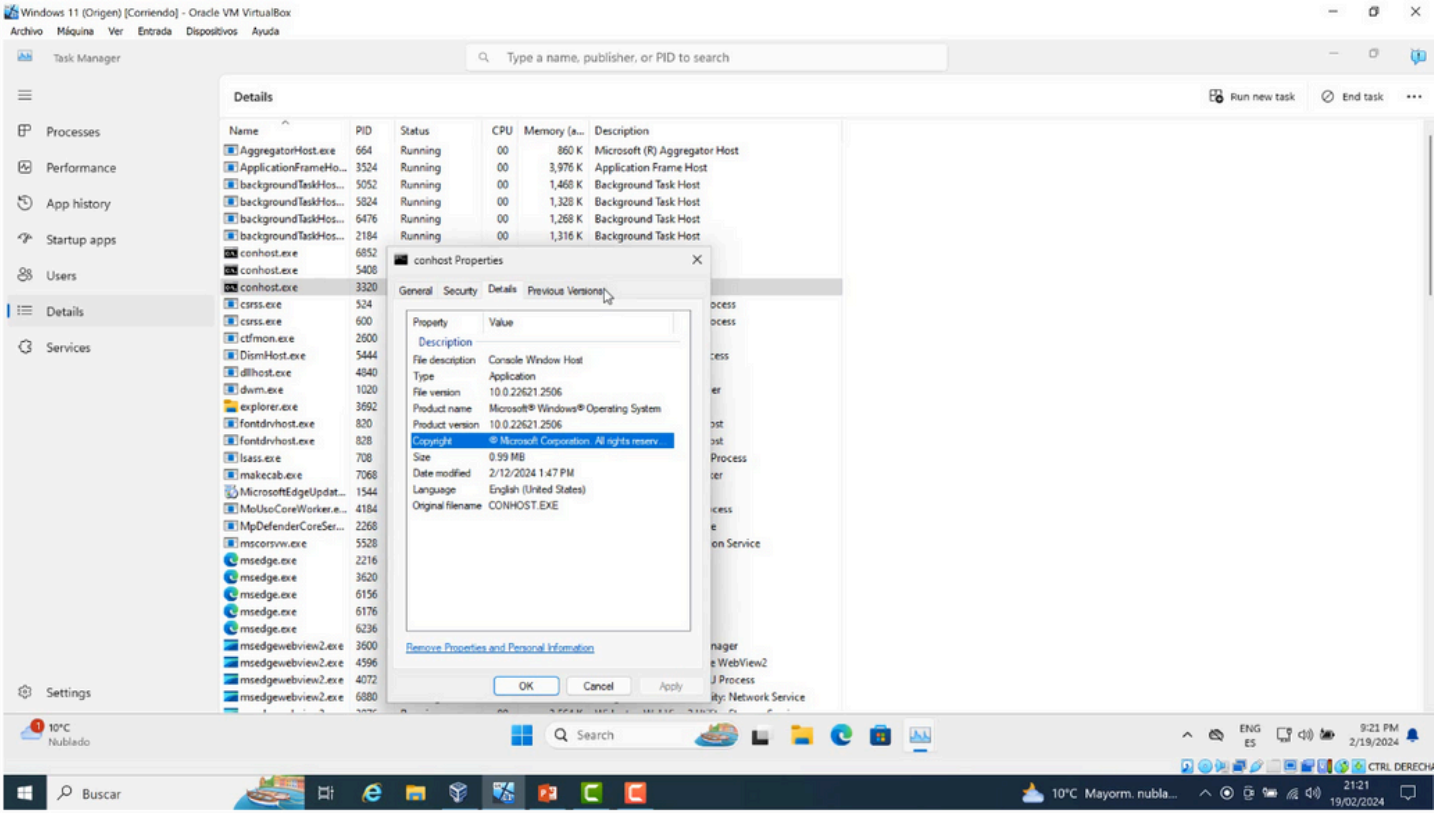
- ALL APPLICATION PACKAGES
- ALL RESTRICTED APPLICATION PACKAGES
- SYSTEM
- Administrators (DESKTOP-5F8E4JV\Administrators)

To change permissions, click Edit. [Edit...]

Permissions for ALL APPLICATION PACKAGES	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write		
Special permissions		

For special permissions or advanced settings, click Advanced. [Advanced]

[OK] [Cancel] [Apply]



Details

Name	PID	Status	CPU	Memory (a...	Description
AggregatorHost.exe	664	Running	00	860 K	Microsoft (R) Aggregator Host
ApplicationFrameHo...	3524	Running	00	3,976 K	Application Frame Host
backgroundTaskHos...	5052	Running	00	1,468 K	Background Task Host
backgroundTaskHos...	5824	Running	00	1,328 K	Background Task Host
backgroundTaskHos...	6476	Running	00	1,268 K	Background Task Host
backgroundTaskHos...	2184	Running	00	1,316 K	Background Task Host
conhost.exe	6852				
conhost.exe	5408				
conhost.exe	3320				
csrss.exe	524				
csrss.exe	600				
ctfmon.exe	2600				
DismHost.exe	5444				
dllhost.exe	4840				
dwm.exe	1020				
explorer.exe	3692				
fontdrvhost.exe	820				
fontdrvhost.exe	828				
lsass.exe	708				
makecab.exe	7068				
MicrosoftEdgeUpdat...	1544				
MoUsoCoreWorker.e...	4184				
MpDefenderCoreSer...	2268				
mscorsvw.exe	5528				
msedge.exe	2216				
msedge.exe	3620				
msedge.exe	6156				
msedge.exe	6176				
msedge.exe	6236				
msedgewebview2.exe	3600				
msedgewebview2.exe	4596				
msedgewebview2.exe	4072				
msedgewebview2.exe	6880				

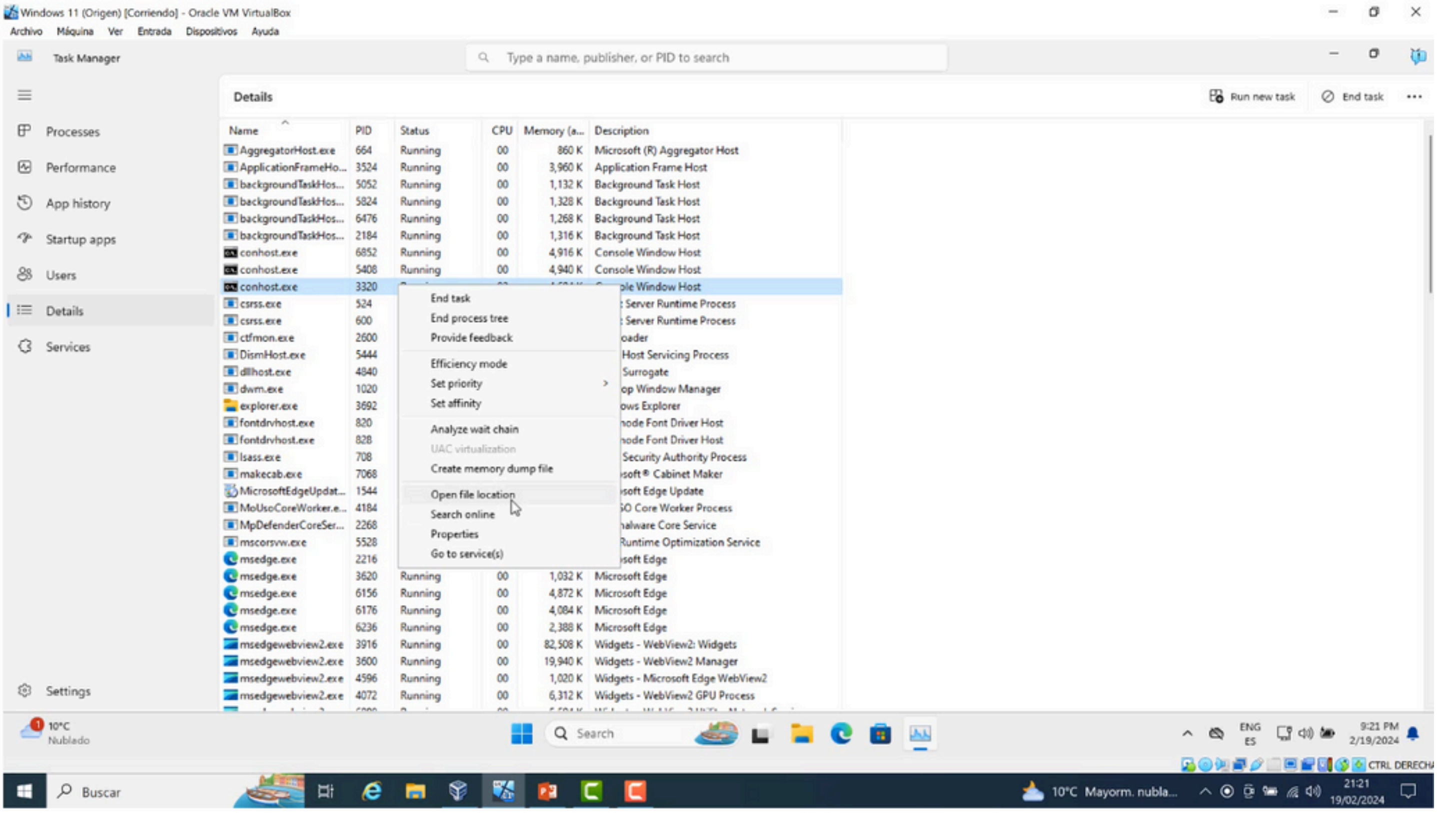
conhost Properties

General | Security | Details | Previous Versions

Property	Value
Description	
File description	Console Window Host
Type	Application
File version	10.0.22621.2506
Product name	Microsoft® Windows® Operating System
Product version	10.0.22621.2506
Copyright	© Microsoft Corporation. All rights reserv...
Size	0.99 MB
Date modified	2/12/2024 1:47 PM
Language	English (United States)
Original filename	CONHOST.EXE

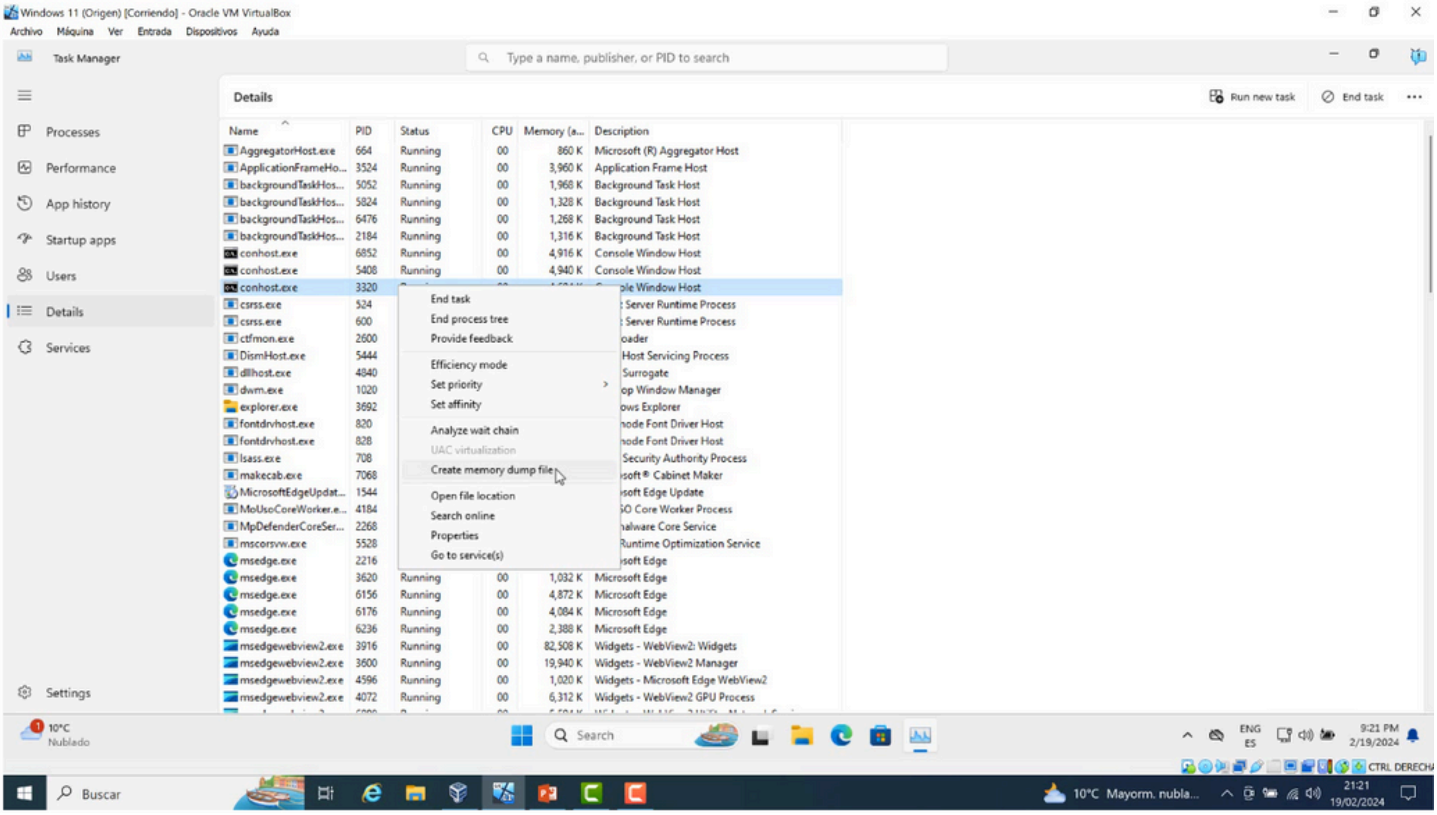
Remove Properties and Personal Information

[OK] [Cancel] [Apply]



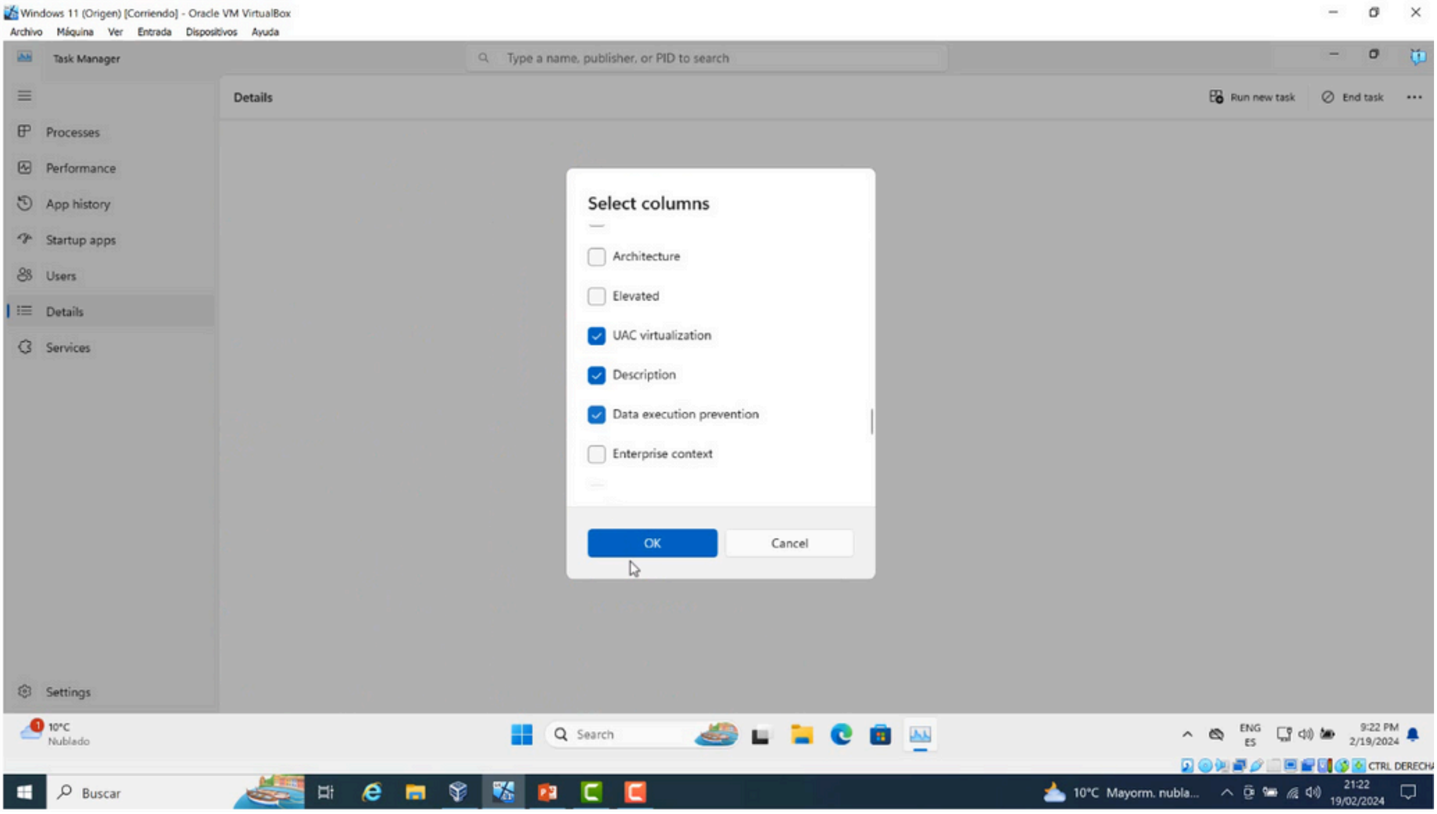
Details

Name	PID	Status	CPU	Memory (a...	Description
AggregatorHost.exe	664	Running	00	860 K	Microsoft (R) Aggregator Host
ApplicationFrameHo...	3524	Running	00	3,960 K	Application Frame Host
backgroundTaskHos...	5052	Running	00	1,132 K	Background Task Host
backgroundTaskHos...	5824	Running	00	1,328 K	Background Task Host
backgroundTaskHos...	6476	Running	00	1,268 K	Background Task Host
backgroundTaskHos...	2184	Running	00	1,316 K	Background Task Host
conhost.exe	6852	Running	00	4,916 K	Console Window Host
conhost.exe	5408	Running	00	4,940 K	Console Window Host
conhost.exe	3320				ole Window Host
csrss.exe	524				: Server Runtime Process
csrss.exe	600				: Server Runtime Process
ctfmon.exe	2600				oader
DismHost.exe	5444				Host Servicing Process
dllhost.exe	4840				Surrogate
dwm.exe	1020				op Window Manager
explorer.exe	3692				ows Explorer
fontdrvhost.exe	820				node Font Driver Host
fontdrvhost.exe	828				node Font Driver Host
lsass.exe	708				Security Authority Process
makecab.exe	7068				soft® Cabinet Maker
MicrosoftEdgeUpdat...	1544				soft Edge Update
MoUsoCoreWorker.e...	4184				SO Core Worker Process
MpDefenderCoreSer...	2268				alware Core Service
mscorsvw.exe	5528				Runtime Optimization Service
msedge.exe	2216				soft Edge
msedge.exe	3620	Running	00	1,032 K	Microsoft Edge
msedge.exe	6156	Running	00	4,872 K	Microsoft Edge
msedge.exe	6176	Running	00	4,084 K	Microsoft Edge
msedge.exe	6236	Running	00	2,388 K	Microsoft Edge
msedgewebview2.exe	3916	Running	00	82,508 K	Widgets - WebView2: Widgets
msedgewebview2.exe	3600	Running	00	19,940 K	Widgets - WebView2 Manager
msedgewebview2.exe	4596	Running	00	1,020 K	Widgets - Microsoft Edge WebView2
msedgewebview2.exe	4072	Running	00	6,312 K	Widgets - WebView2 GPU Process



Details

Name	PID	Status	CPU	Memory (a...	Description
AggregatorHost.exe	664	Running	00	860 K	Microsoft (R) Aggregator Host
ApplicationFrameHo...	3524	Running	00	3,960 K	Application Frame Host
backgroundTaskHos...	5052	Running	00	1,968 K	Background Task Host
backgroundTaskHos...	5824	Running	00	1,328 K	Background Task Host
backgroundTaskHos...	6476	Running	00	1,268 K	Background Task Host
backgroundTaskHos...	2184	Running	00	1,316 K	Background Task Host
conhost.exe	6852	Running	00	4,916 K	Console Window Host
conhost.exe	5408	Running	00	4,940 K	Console Window Host
conhost.exe	3320				ole Window Host
csrss.exe	524				: Server Runtime Process
csrss.exe	600				: Server Runtime Process
ctfmon.exe	2600				oader
DismHost.exe	5444				Host Servicing Process
dllhost.exe	4840				Surrogate
dwm.exe	1020				op Window Manager
explorer.exe	3692				ows Explorer
fontdrvhost.exe	820				node Font Driver Host
fontdrvhost.exe	828				node Font Driver Host
lsass.exe	708				Security Authority Process
makecab.exe	7068				soft® Cabinet Maker
MicrosoftEdgeUpdat...	1544				soft Edge Update
MoUsoCoreWorker.e...	4184				SO Core Worker Process
MpDefenderCoreSer...	2268				alware Core Service
mscorsvw.exe	5528				Runtime Optimization Service
msedge.exe	2216				soft Edge
msedge.exe	3620	Running	00	1,032 K	Microsoft Edge
msedge.exe	6156	Running	00	4,872 K	Microsoft Edge
msedge.exe	6176	Running	00	4,084 K	Microsoft Edge
msedge.exe	6236	Running	00	2,388 K	Microsoft Edge
msedgewebview2.exe	3916	Running	00	82,508 K	Widgets - WebView2: Widgets
msedgewebview2.exe	3600	Running	00	19,940 K	Widgets - WebView2 Manager
msedgewebview2.exe	4596	Running	00	1,020 K	Widgets - Microsoft Edge WebView2
msedgewebview2.exe	4072	Running	00	6,312 K	Widgets - WebView2 GPU Process



Select columns

☐ Architecture

☐ Elevated

☑ UAC virtualization

☑ Description

☑ Data execution prevention

☐ Enterprise context

OK Cancel

Other BIOS options

- Set system access password.
- Configure the boot order.
- Anti-theft service (according to manufacturer).
- TPM (Trusted Platform Module) Advantages of the cryptographic chip.
- BitLocker.
- Unnecessary options (Wake of LAN, etc.).

Singularity Hackers 0xWORD My Public® Inbox