Computer Security

Computer security is the discipline that is responsible for analyzing, planning and protecting an organization's assets related to computer systems.

Asset is a resource with a certain value for an organization, it can be data, equipment and/or services.

- Identify the assets
- Classify assets
- Identify threats
- Mitigate risks

- Confidentiality, Integrity and Availability.
- “Security is not a product, it is a process”

  Bruce Schneier
- There is no such thing as 100% security

Systems hardening

- Defense in Depth: Security layers must be applied, if a barrier is breached, the system will not be compromised.
- Minimum Exposure: System must use only components necessary for its designed function.
- Minimum Assigned Privilege: Assigned privileges must be strictly necessary to perform the assigned task.

Security Risks

- Malware: Malicious software, viruses, worms, trojans, rootkits, keyloggers, backdoor, spam, phishing, spear phishing, hijacking, ransomware.

- Other Risks: Theft of credentials, leak of confidential data, theft of data or equipment, legal, loss of credibility or image.

Good practices

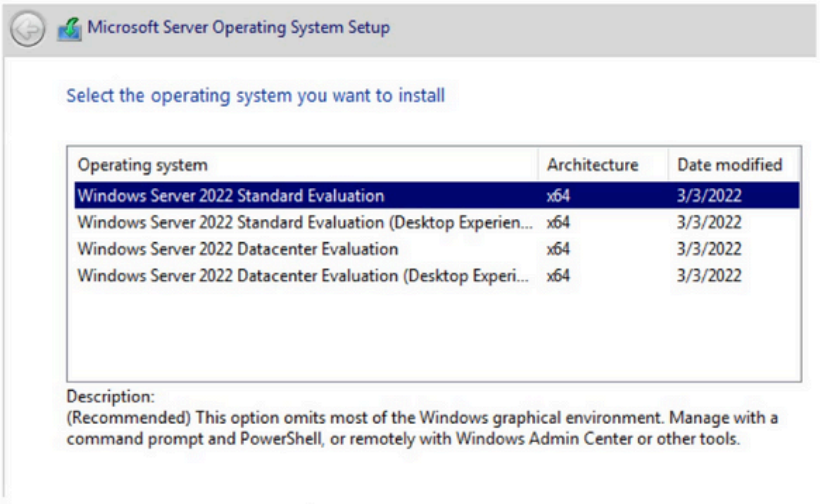
- Design an Update application policy.
- Apply the principle of Least Privilege.
- Use appropriate user accounts for each task.
- Restrict the use of Privileged accounts.
- Design a physical access control plan.

Microsoft Windows Server
https://www.microsoft.com/en-us/windows-server

Windows Server Evaluation Center
https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022

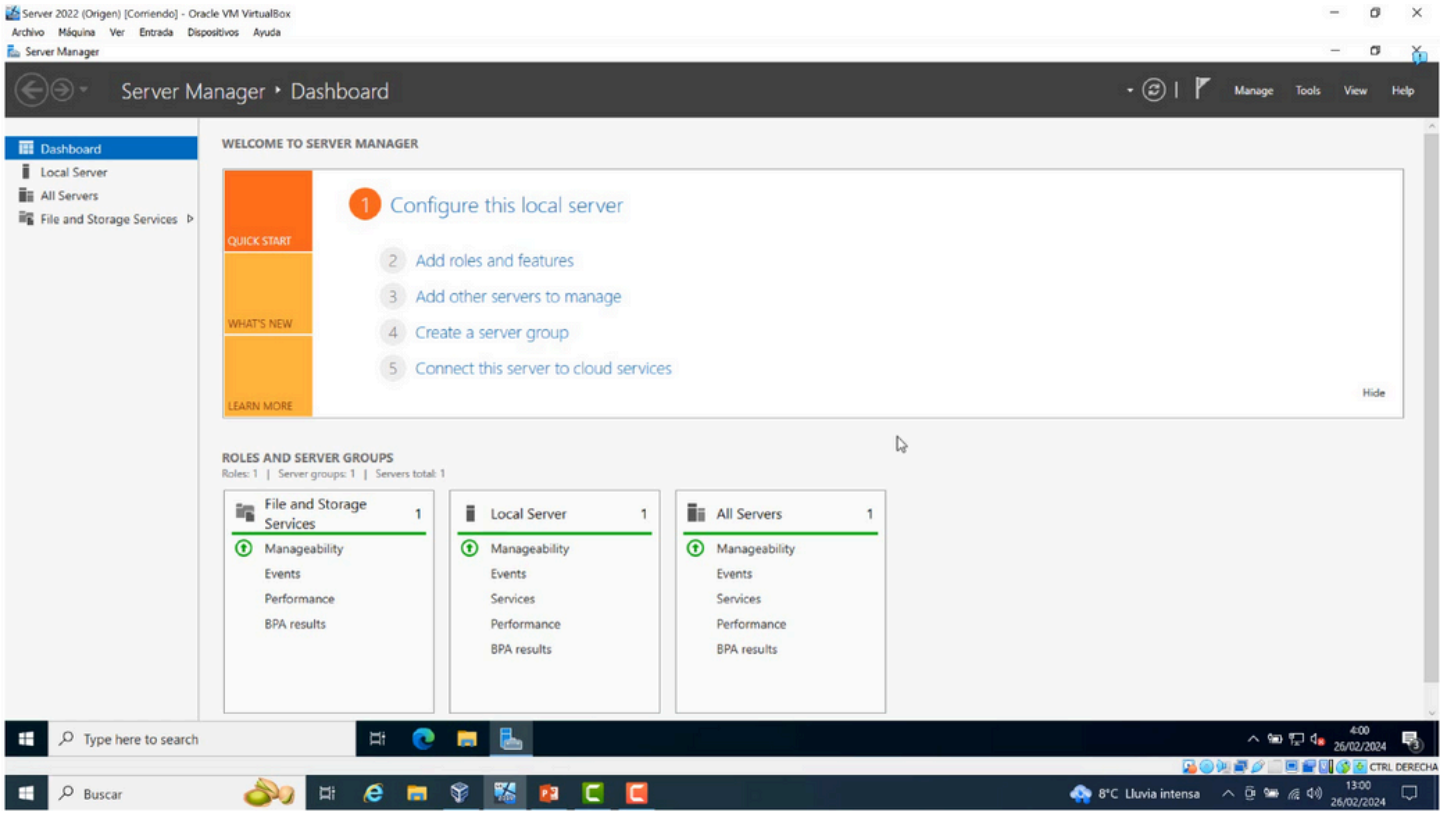
Getting started with Windows Server

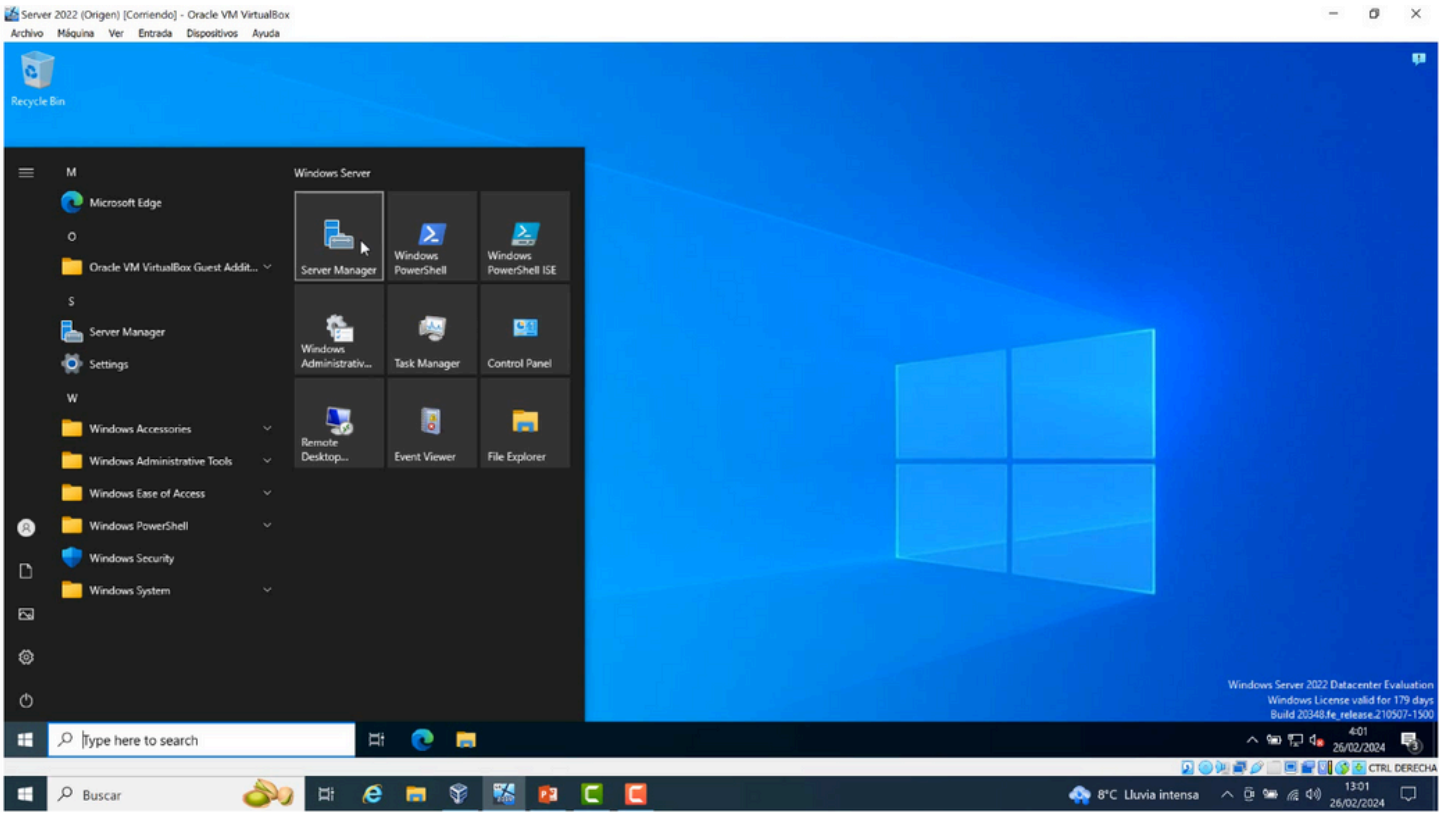
- Getting started with Windows Server
- What version to install?
  - Desktop Experience

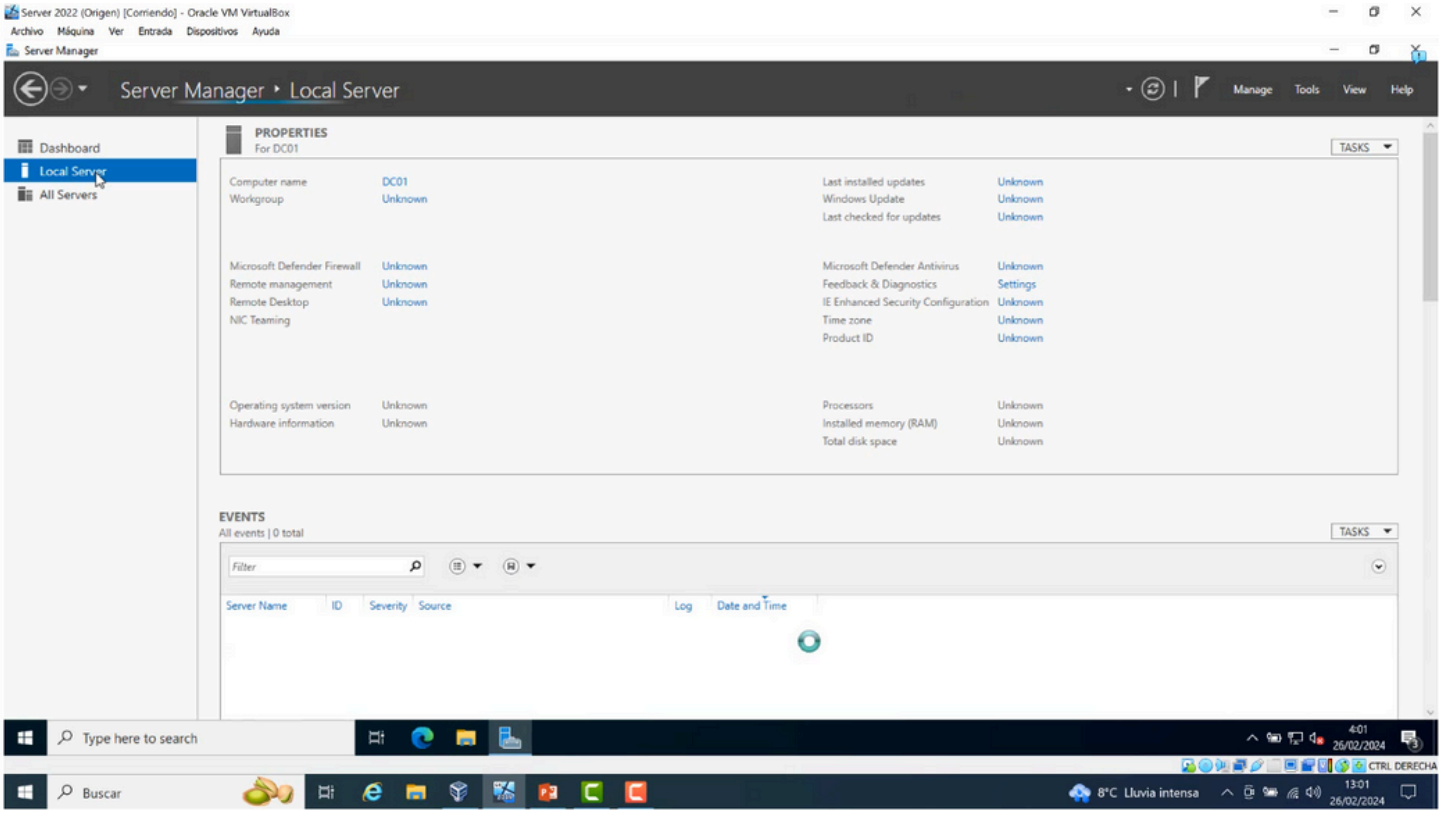


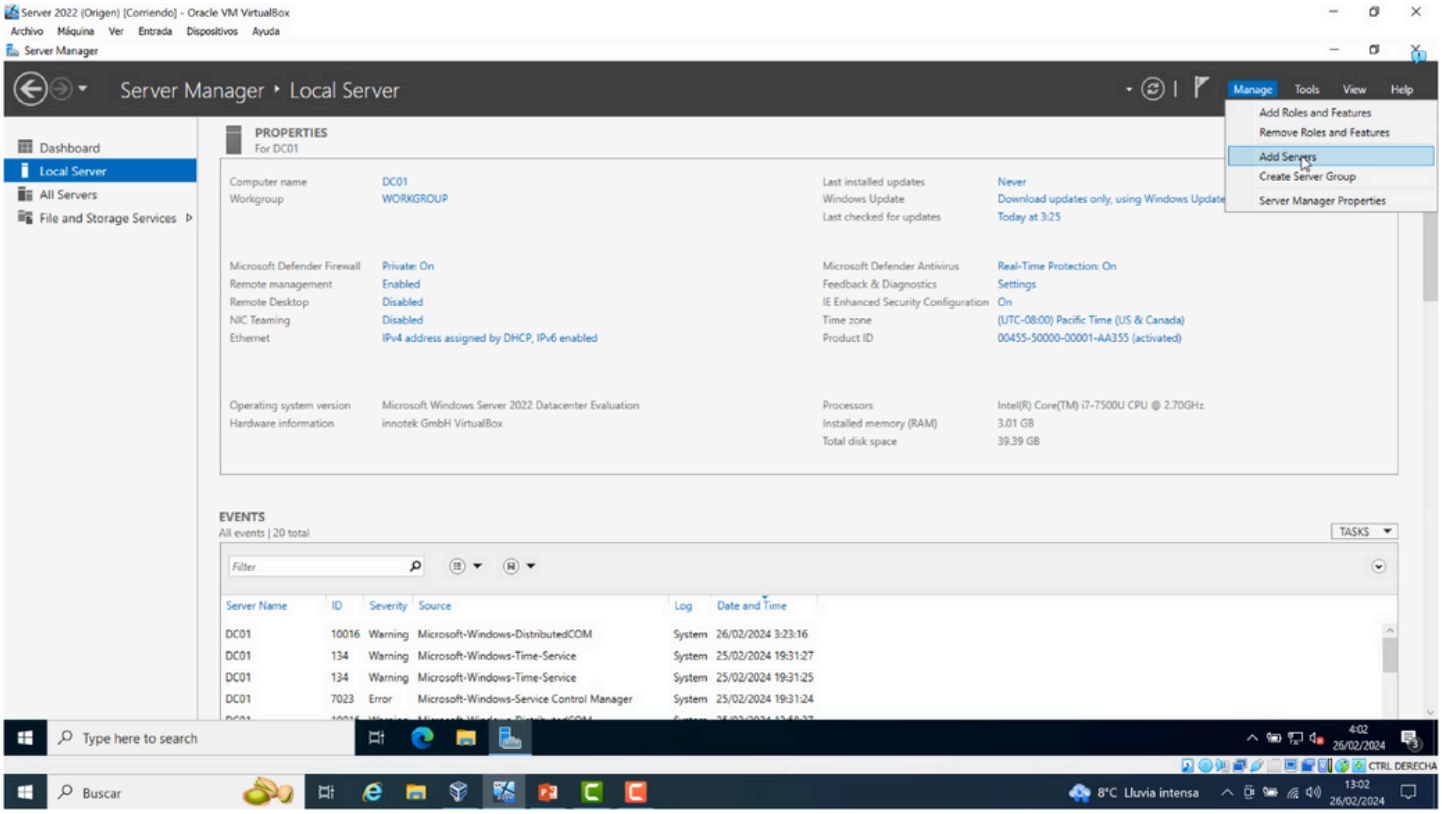
Pictures own elaboration

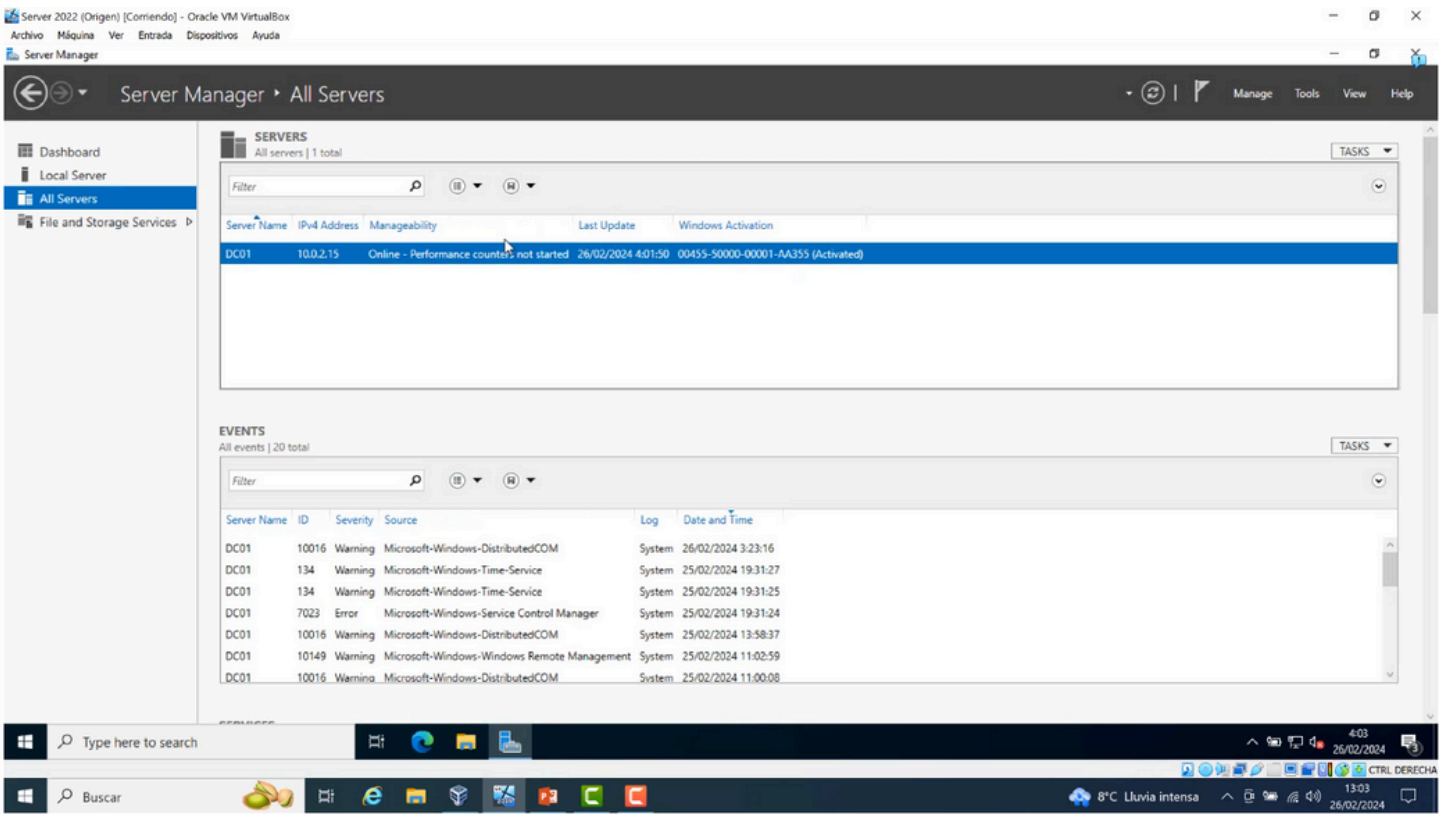
Singularity Hackers 0xWORD My Public Inbox




Server 2022 (Origen) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Recycle Bin
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer
Microsoft Edge
Oracle VM VirtualBox Guest Addit...
Server Manager
Settings
Windows Accessories
Windows Administrative Tools
Windows Ease of Access
Windows PowerShell
Windows Security
Windows System
Type here to search
Windows Server 2022 Datacenter Evaluation
Windows License valid for 179 days
Build 20348.fe_release.210507-1500
4:01
26/02/2024
CTRL DERECHA
Buscar
8°C Lluvia intensa
13:01
26/02/2024


Server 2022 (Origen) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Server Manager
Server Manager • Local Server
Manage Tools View Help
Dashboard
Local Server
All Servers
PROPERTIES
For DC01
TASKS
Computer name DC01
Workgroup Unknown
Last installed updates Unknown
Windows Update Unknown
Last checked for updates Unknown
Microsoft Defender Firewall Unknown
Remote management Unknown
Remote Desktop Unknown
NIC Teaming
Microsoft Defender Antivirus Unknown
Feedback & Diagnostics Settings
IE Enhanced Security Configuration Unknown
Time zone Unknown
Product ID Unknown
Operating system version Unknown
Hardware information Unknown
Processors Unknown
Installed memory (RAM) Unknown
Total disk space Unknown
EVENTS
All events | 0 total
TASKS
Filter
Server Name ID Severity Source Log Date and Time
Type here to search
4:01
26/02/2024
CTRL DERECHA
Buscar
8°C Lluvia intensa
13:01
26/02/2024


Server 2022 (Origen) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Server Manager
Server Manager • Local Server
Manage Tools View Help
Add Roles and Features
Remove Roles and Features
Add Servers
Create Server Group
Server Manager Properties
Dashboard
Local Server
All Servers
File and Storage Services
PROPERTIES
For DC01
Computer name DC01
Workgroup WORKGROUP
Last installed updates Never
Windows Update Download updates only, using Windows Update
Last checked for updates Today at 3:25
Microsoft Defender Firewall Private: On
Remote management Enabled
Remote Desktop Disabled
NIC Teaming Disabled
Ethernet IPv4 address assigned by DHCP, IPv6 enabled
Microsoft Defender Antivirus Real-Time Protection: On
Feedback & Diagnostics Settings
IE Enhanced Security Configuration On
Time zone (UTC-08:00) Pacific Time (US & Canada)
Product ID 00455-50000-00001-AA355 (activated)
Operating system version Microsoft Windows Server 2022 Datacenter Evaluation
Hardware information innotek GmbH VirtualBox
Processors Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz
Installed memory (RAM) 3.01 GB
Total disk space 39.39 GB
EVENTS
All events | 20 total
TASKS
Filter
Server Name ID Severity Source Log Date and Time
DC01 10016 Warning Microsoft-Windows-DistributedCOM System 26/02/2024 3:23:16
DC01 134 Warning Microsoft-Windows-Time-Service System 25/02/2024 19:31:27
DC01 134 Warning Microsoft-Windows-Time-Service System 25/02/2024 19:31:25
DC01 7023 Error Microsoft-Windows-Service Control Manager System 25/02/2024 19:31:24
Type here to search
4:02
26/02/2024
CTRL DERECHA
Buscar
8°C Lluvia intensa
13:02
26/02/2024


Server 2022 (Origen) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Server Manager
Server Manager • All Servers
Manage Tools View Help
Dashboard
Local Server
All Servers
File and Storage Services
SERVERS
All servers | 1 total
TASKS
Filter
Server Name IPv4 Address Manageability Last Update Windows Activation
DC01 10.0.2.15 Online - Performance counters not started 26/02/2024 4:01:50 00455-50000-00001-AA355 (Activated)
EVENTS
All events | 20 total
TASKS
Filter
Server Name ID Severity Source Log Date and Time
DC01 10016 Warning Microsoft-Windows-DistributedCOM System 26/02/2024 3:23:16
DC01 134 Warning Microsoft-Windows-Time-Service System 25/02/2024 19:31:27
DC01 134 Warning Microsoft-Windows-Time-Service System 25/02/2024 19:31:25
DC01 7023 Error Microsoft-Windows-Service Control Manager System 25/02/2024 19:31:24
DC01 10016 Warning Microsoft-Windows-DistributedCOM System 25/02/2024 13:58:37
DC01 10149 Warning Microsoft-Windows-Windows Remote Management System 25/02/2024 11:02:59
DC01 10016 Warning Microsoft-Windows-DistributedCOM System 25/02/2024 11:00:08
Type here to search
4:03
26/02/2024
CTRL DERECHA
Buscar
8°C Lluvia intensa
13:03
26/02/2024

Conclusions

It is important to plan computer security processes as something dynamic, with constant reviews and the application of improvements over time, identifying the organization's assets and the risks associated with these elements.