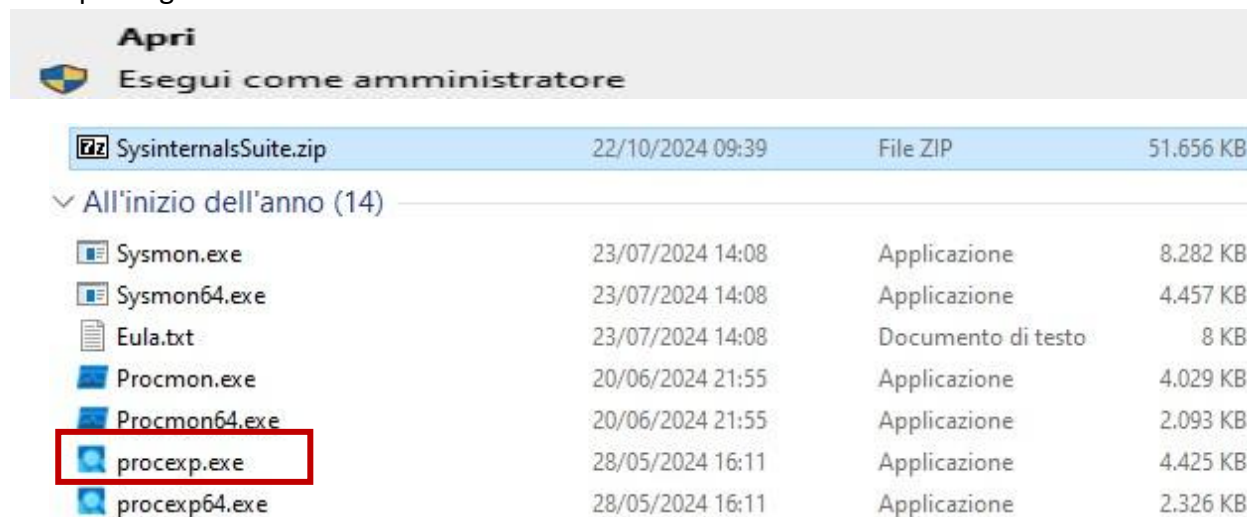


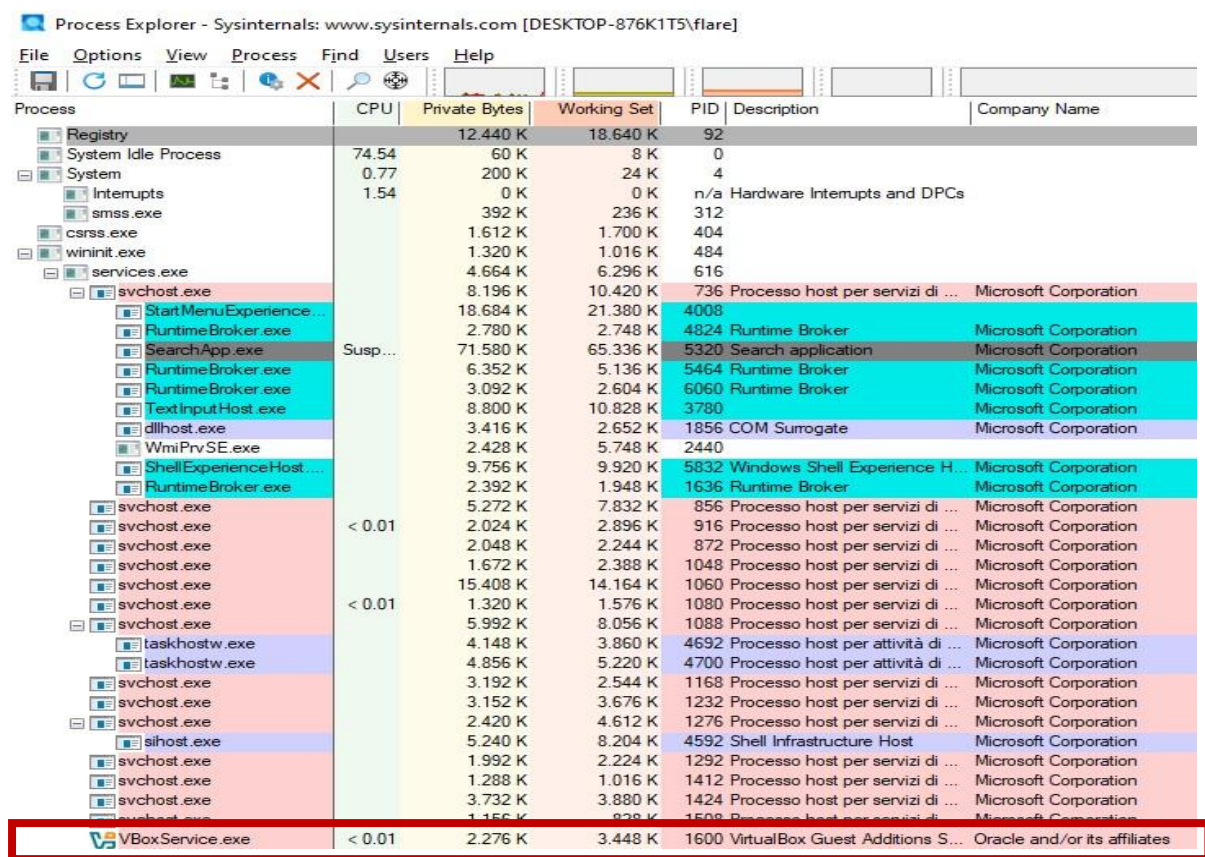
Relazione Processi – Threads – Handle e Registro di Windows

Nella seguente immagine dopo aver scaricato **SysinternalsSuite.zip** sulla macchina Windows, estraggo i file zippati, e come da immagine seguente, ho vari programmi (exe), eseguibili.

Il programma che utilizzerò per svolgere le operazioni richieste è **procexp.exe**, che devo eseguire con i privilegi **amministratore**



Nel passaggio successivo, dopo aver estratto i file dalla cartella **SysinternalsSuite.zip**, clicco sul file eseguibile **procexp.exe**, dove vedrò i vari processi in corso del mio sistema operativo



Dopo aver individuato il file da analizzare nella lista dei processi, in questo caso, **VboxService.exe**, come già illustrato in precedenza, con il tasto destro, clicco su **Properties**, in cui vedo il **Path** (**percorsi del programma**), e nello specifico, nelle prossime immagini e passaggi, lavorerò sulla parte evidenziata in rosso, ma ora vado nella scheda **Threads**, per visualizzare sia il **TID**, che identifica l'**ID del processo** ed il tempo della **CPU** che impiega, utilizza ogni **Threads**

VS

VBoxService.exe:1500 Properties

GPU Graph

Services

Threads

TCP/IP

Security

Environment

Strings

Image

Performance

Performance Graph

Disk and Network

Image File

VS

VirtualBox Guest Additions Service

Version: 7.1.2.14945

Build Time: Thu Sep 26 15:46:48 2024

Path:

C:\Windows\System32\VBoxService.exe

Explore

Command line:

C:\Windows\System32\VBoxService.exe

Current directory:

C:\Windows\System32\

Autostart Location:

HKLM\System\CurrentControlSet\Services\VBoxService

Explore

Parent: services.exe(624)

User: NT AUTHORITY\SYSTEM

Started: 09:32:57 22/10/2024 Image: 64-bit

Comment:

VirusTotal:

Submit

Data Execution Prevention (DEP) Status: Enabled (permanent)

Address Space Load Randomization: Enabled (permanent)Disabled

Control Flow Guard: Enabled

Enterprise Context: N/A

Stack Protection: Disabled

Verify

Bring to Front

Kill Process

OK

Cancel

TID

CPU

1632

< 0.01

1724

< 0.01

1644

< 0.01

1668

1628

6700

1688

1392

1504

1576

1608

1708

VS

VBoxService.exe:1500 Properties

Image

Performance

Performance Graph

Disk and Network

GPU Graph

Services

Threads

TCP/IP

Security

Environment

Strings

Count: 12

TID	CPU	Cycles Delta	Suspend Count	Service	Start Address
1724	< 0.01	729.307		VBoxService	VBoxService.exe+0x23f80
1392	< 0.01	357.050		VBoxService	ntdll.dll!TpReleaseCleanu...
1668	< 0.01	85.433		VBoxService	VBoxService.exe+0x23f80
1632				VBoxService	VBoxService.exe+0x23f80
1628				VBoxService	VBoxService.exe+0x23f80
1644				VBoxService	VBoxService.exe+0x23f80
1504				VBoxService	VBoxService.exe+0x15a0
1576				VBoxService	sechost.dll!WaitServiceSt...
1608				VBoxService	VBoxService.exe+0x23f80
1688				VBoxService	VBoxService.exe+0x23f80
1708				VBoxService	VBoxService.exe+0x23f80
1452				VBoxService	ntdll.dll!TpReleaseCleanu...

Thread ID: 1504

Stack

Module

Start Time: 09:32:57 22/10/2024

State: Wait:UserRequest

Base Priority: 8

Kernel Time: 0:00:00.000

Dynamic Priority: 8

User Time: 0:00:00.000

I/O Priority: Normal

Context Switches: 57

Memory Priority: 5

Cycles: 41.840.081

Ideal Processor: 1

Permissions

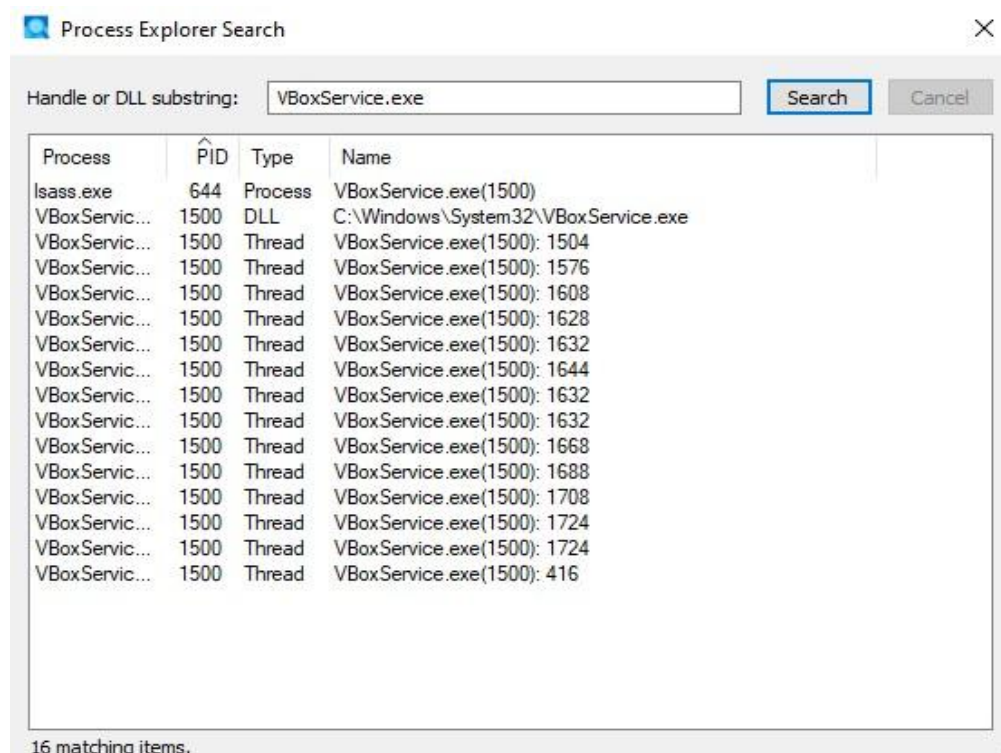
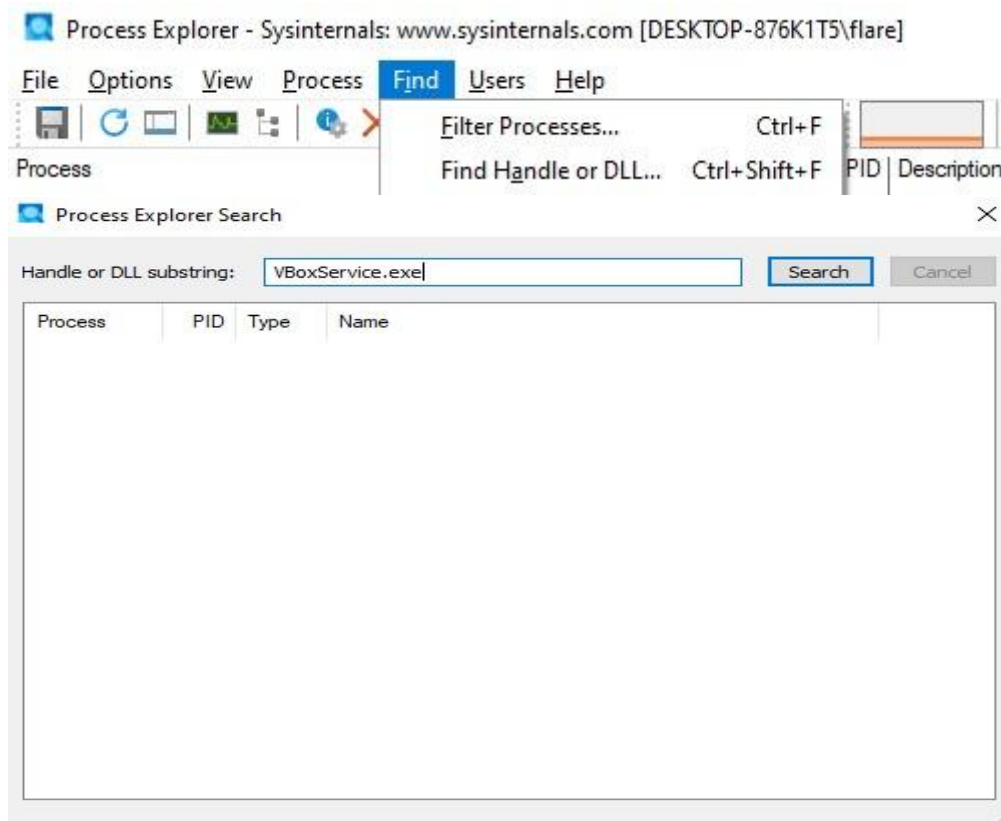
Kill

Suspend

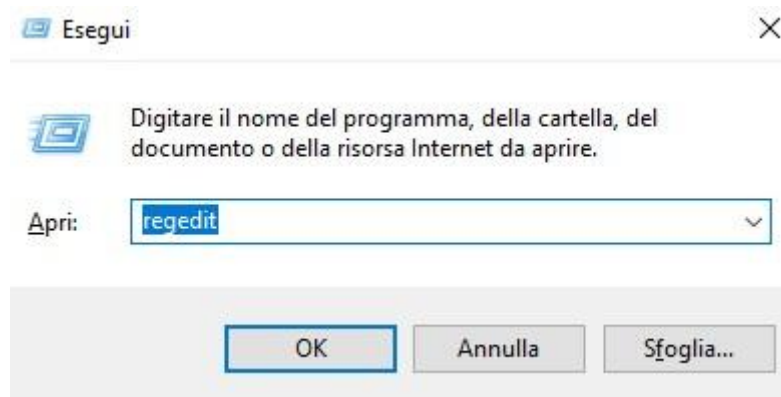
OK

Cancel

Nel passaggio illustrato di seguito, sempre, all'interno del programma **procexp.exe**, vado in alto a sinistra sulla scheda **Find**, e clicco su **Handle or DLL (Dynamic Link Libraries)**, dove posso cercare il programma specifico che voglio modificare o visualizzare, in questo caso e come illustrato e descritto in precedenza, **VBoxService.exe**, per aprire in modalità rapida la scheda **Find**, all'interno di **procexp.exe**, posso utilizzare il comando e combinazione di tasti **Ctrl + F**:



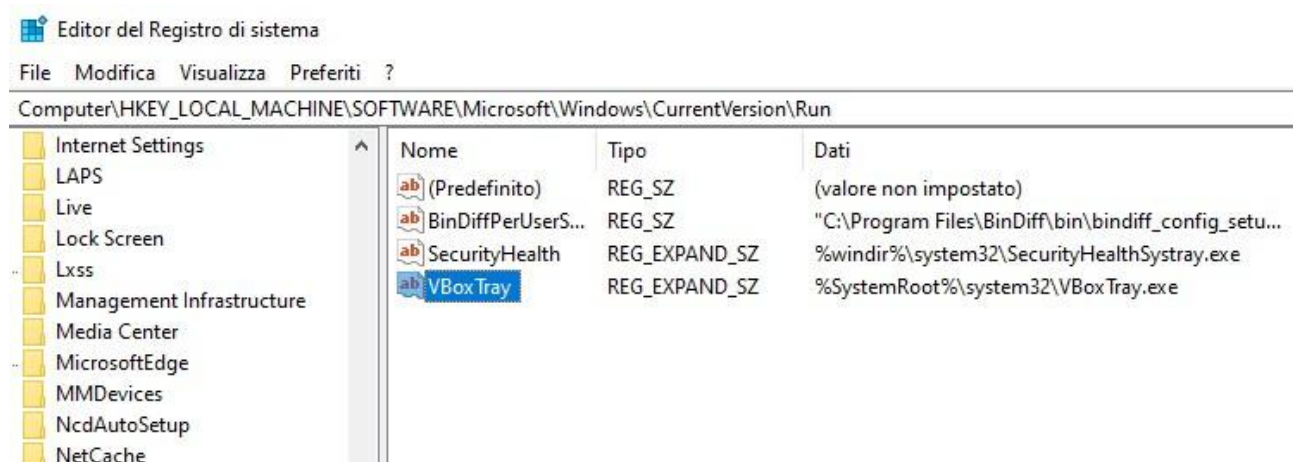
Nel prossimo passaggio con la combinazione tasti **Windows + R**, scrivo all'interno della stringa di ricerca **regedit (Editor del Registro di Sistema di Windows)**, nel quale posso andare a modificare o configurare le impostazioni del mio Sistema Operativo (Windows):



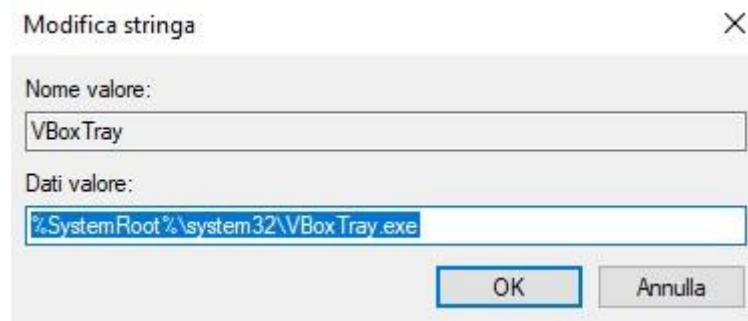
Nella prossima immagine e passaggio, all'interno dell'Editor del Registro di Sistema, in alto, posso notare il percorso:

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

- ❖ **HKEY_LOCAL_MACHINE:** è la radice del Registro di Windows, contenente le informazioni per le configurazioni, applicabili all'interno del computer e relative configurazioni anche per gli Users
- ❖ **SOFTWARE\Microsoft\Windows\CurrentVersion\Run:** è la chiave che identifica il file o i file che si avviano nella fase di avvio del Sistema Operativo (Windows)

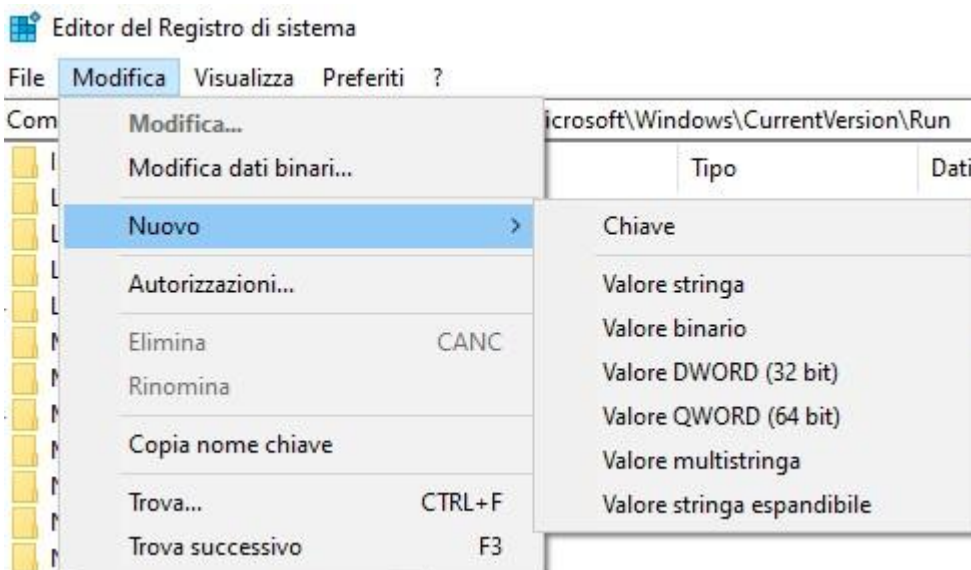


Dopo aver individuato nell'Editor del Registro di Sistema di Windows, VBoxTray clicco due volte sul file **VBoxTray**, per visualizzare il valore del programma, in fase di avvio di Windows:

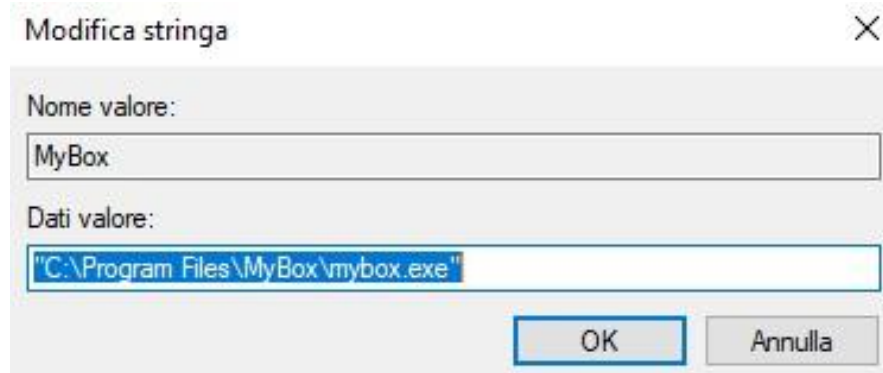


Dopo che ho visualizzato il percorso di **VboxTray** e verificato che il programma si avvia all'avvio della macchina Windows, ho cliccato su **Modifica**, successivamente su **Nuovo** e poi **Valore stringa** in cui ho creato u nuovo valore (exe), chiamato **MyBox** che si avvierà durante l'avvio di Windows, nella stringa Dati valore, come da immagine seguente, il percorso del programma è:

- **C:\Program Files\MyBox\mybox.exe**



Dopo aver creato il programma e dato un nome al valore **MyBox**, clicco su **OK** e per rendere le modifiche e configurazioni, eseguibili, all'avvio di Windows, riavvio la macchina



Dopo aver riavviato la macchina Windows, torno sull'Editor del Registro di Sistema di Windows e controllo se il valore configurato e programma, che si avviano all'avvio di Windows:

Nome	Tipo	Dati
(Predefinito)	REG_SZ	(valore non impostato)
BinDiffPerUserS...	REG_SZ	"C:\Program Files\BinDiff\bin\bindiff_config_setu...
MyBox	REG_SZ	"C:\Program Files\MyBox\mybox.exe"
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
VBox Tray	REG_EXPAND_SZ	%SystemRoot%\system32\VBox Tray.exe

Per verificare che **MyBox** si avii correttamente, all'avvio di Windows, verifico il tutto, con il comando **Ctrl + Shift + Esc**, che aprirà il **Task Manager**, nella scheda **Avvio**, verifico che il programma **MyBox**, si sia avviato:

Gestione attività

File Opzioni Visualizza

Processi Prestazioni Cronologia applicazioni **Avvio** Utenti Dettagli Servizi

Nome	Stato	10% CPU	26% Memoria	33% Disco	0% Rete	Consumo elet...	Tendenza con...
Applicazioni (1)							
Gestione attività		1,9%	16,8 MB	0 MB/s	0 Mbps	Molto basso	Molto basso
Processi in background (18)							
Applicazione sottosistema spo...		0%	3,8 MB	0 MB/s	0 Mbps	Molto basso	Molto basso
Caricatore CTF		0%	2,9 MB	0 MB/s	0 Mbps	Molto basso	Molto basso
Cerca		0%	0 MB	0 MB/s	0 Mbps	Molto basso	Molto basso
Host esperienza shell di Windows		0%	7,1 MB	0 MB/s	0 Mbps	Molto basso	Molto basso
Microsoft Windows Search Inde...		0%	5,1 MB	0 MB/s	0 Mbps	Molto basso	Molto basso
Processo host per attività di Win...		0%	1,9 MB	0 MB/s	0 Mbps	Molto basso	Molto basso
Runtime Broker		0%	2,6 MB	0 MB/s	0 Mbps	Molto basso	Molto basso
Runtime Broker		0%	2,5 MB	0 MB/s	0 Mbps	Molto basso	Molto basso
Runtime Broker		0%	3,6 MB	0 MB/s	0 Mbps	Molto basso	Molto basso
Runtime Broker		0%	1,6 MB	0 MB/s	0 Mbps	Molto basso	Molto basso

Meno dettagli Termina attività

Gestione attività

File Opzioni Visualizza

Processi Prestazioni Cronologia applicazioni **Avvio** Utenti Dettagli Servizi

Ultima durata BIOS: secondi: 0.0

Nome	Autore	Stato	Impatto di avvio
bindiff_config_setup.exe		Abilitato	Non misurata
Mybox		Abilitato	Non misurata
Sysinternals Screen Magnifier	Sysinternals - www.sysin...	Abilitato	Non misurata
VirtualBox Guest Additions T...	Oracle and/or its affiliates	Abilitato	Media
Windows Security notificati...	Microsoft Corporation	Disabilitato	Media