

S11L2 - Esplorazione di Processi, Thread, Handle e Registro di Windows

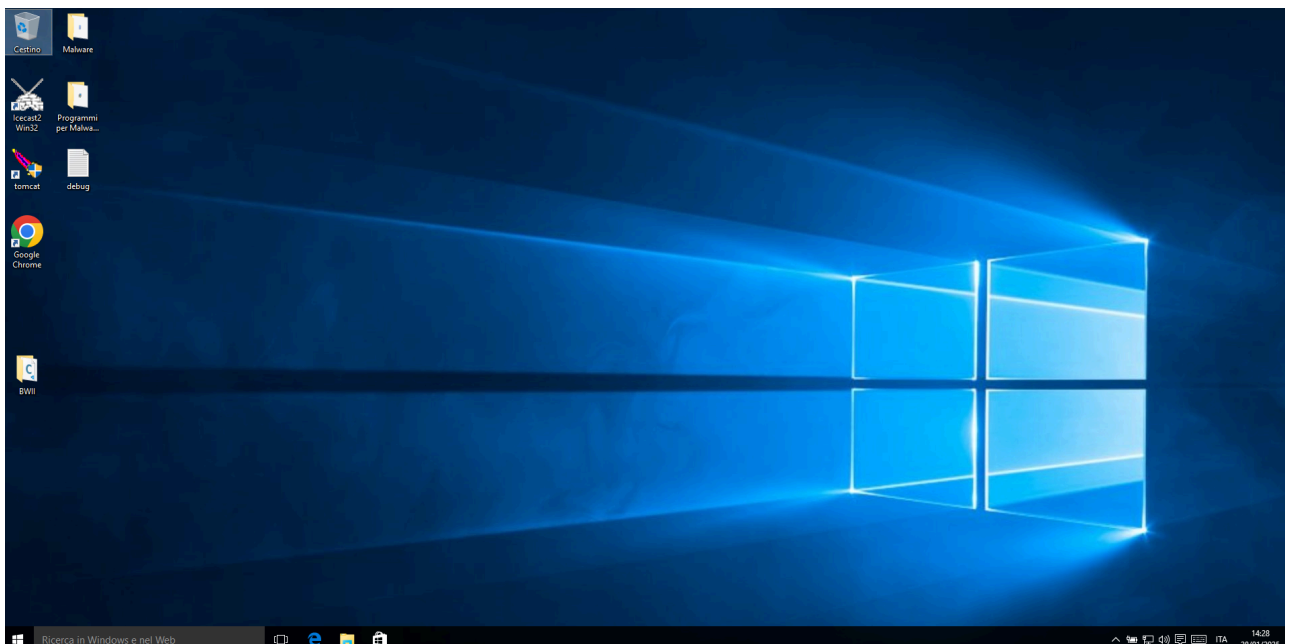
Esplorazione di Processi, Thread, Handle e Registro di Windows

1. Esplorazione di Processi, Thread e Handle con Process Explorer

Passaggi:

1. Avvio di Process Explorer:

- Ho avviato la macchina virtuale Windows 10.



- Ho scaricato la Sysinternals Suite (dato che non era già installata) da <https://learn.microsoft.com/sysinternals/>.

Microsoft utilizza i cookie opzionali per migliorare l'esperienza dell'utente sui nostri siti Web, ad esempio tramite connessioni ai social media, e per visualizzare annunci pubblicitari personalizzati in base alla sua attività online. Qualora l'utente rifiuti i cookie opzionali, saranno utilizzati solo i cookie necessari per fornirgli i servizi. La selezione può essere modificata facendo clic su "Gestisci i cookie" in fondo alla pagina. [Informazioni sulla privacy](#) [Cookie di terze parti](#)

Accetta Rifiuta Gestisci i cookie

Learn Rilevazione Documentazione del prodotto Linguaggi di sviluppo Argomenti

Sysinternals Download Community Risorse

Parti di questo argomento potrebbero essere state tradotte automaticamente o con l'intelligenza artificiale.

Filtra in base al titolo

Home

Download

Utilità file e dischi

Utilità di rete

Utilità di processo

Utilità di sicurezza

Informazioni sul sistema

Varie

Sysinternals Suite

Microsoft Store

Community

Risorse

Condizioni di Licenza software

Domande frequenti sulle licenze

Sysinternals

Articolo • 17/12/2024 • 11 contributori

In questo articolo

Sysinternals Live

Novità

Il sito Web di Sysinternals è stato creato nel 1996 da Mark Russinovich per ospitare le utilità di sistema avanzate e le informazioni tecniche. Le utility di Sysinternals sono a disposizione di professionisti IT e gli sviluppatori per gestire, risolvere i problemi e diagnosticare i sistemi e le applicazioni di Windows e Linux.

- Leggere la guida ufficiale agli strumenti Sysinternals, [Risoluzione dei problemi con gli strumenti Sysinternals di Windows](#)
- Per un feed dettagliato sugli aggiornamenti degli strumenti, consultare il [blog di Sysinternals](#)
- Guardare i video di aggiornamento su Sysinternals in YouTube di Mark

Risorse aggiuntive

Formazione

Modulo

Explore support and diagnostic tools - Training

This module introduces the tools for troubleshooting the Windows client operating system and provides guidance on how to use them.

Documentazione

Sysinternals Suite - Sysinternals

La risoluzione dei problemi di Windows Sysinternals è stata implementata in un'unica suite di strumenti.

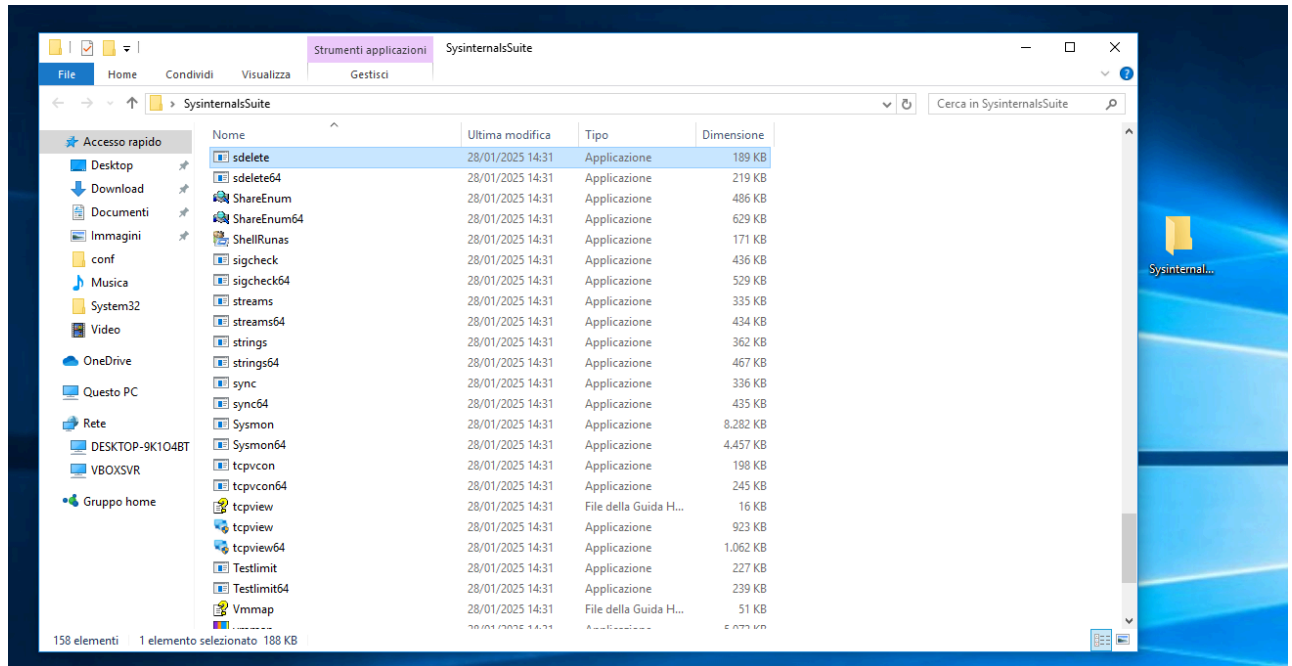
Utilità Sysinternals - Sysinternals

Valutare e scoprire come installare, distribuire e gestire Windows con le utilità Sysinternals.

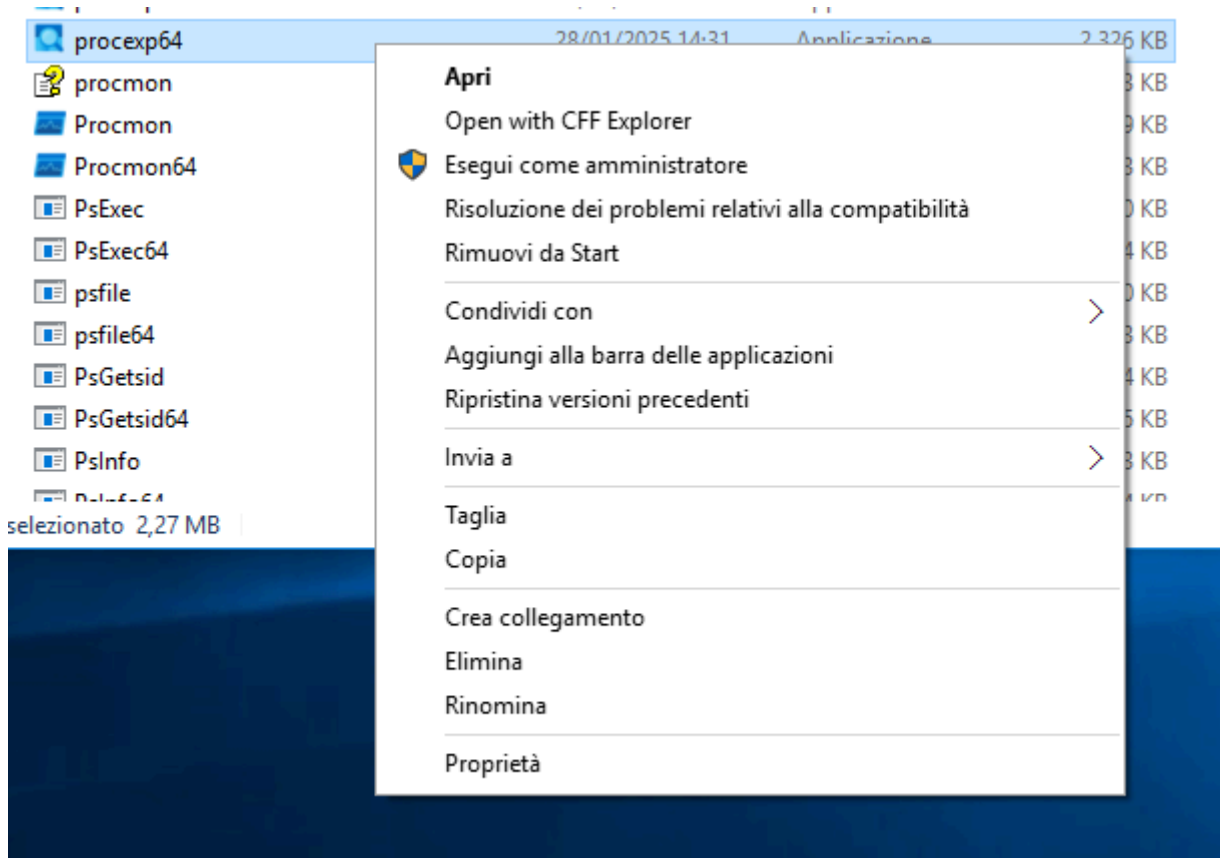
Community Sysinternals - Sysinternals

Informazioni e collegamenti della community di Windows Sysinternals

- Ho estratto il file .zip



- Ho eseguito Process Explorer con privilegi di amministratore.



2. Esplorazione dei Processi:

- Ho analizzato l'elenco dei processi attivi.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	92.15	0 K	4 K	0		
System	< 0.01	228 K	22.304 K	4		
Interrupts	0.78	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		336 K	936 K	272		
csrss.exe	< 0.01	1.200 K	3.412 K	348		
wininit.exe		836 K	4.248 K	428		
services.exe		2.640 K	6.188 K	544		
svchost.exe	< 0.01	5.160 K	14.832 K	632	Processo host per servizi di ...	Microsoft Corporation
unsecapp.exe		1.084 K	5.820 K	1976	Sink to receive asynchronou...	Microsoft Corporation
WmiPrivSE.exe	< 0.01	4.404 K	12.312 K	2360	WMI Provider Host	Microsoft Corporation
WmiPrivSE.exe	< 0.01	3.000 K	8.612 K	2252	WMI Provider Host	Microsoft Corporation
RuntimeBroker.exe		4.112 K	19.920 K	3752	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Susp...	12.080 K	26.424 K	3712	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	32.112 K	46.256 K	4920	Search and Cortana applicati...	Microsoft Corporation
ApplicationFrameHost.exe		3.516 K	17.788 K	3116	Application Frame Host	Microsoft Corporation
SppExtComObj.Exe		1.468 K	7.044 K	5040	KMS Connection Broker	Microsoft Corporation
svchost.exe	< 0.01	3.484 K	8.744 K	688	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	< 0.01	19.356 K	36.364 K	880	Processo host per servizi di ...	Microsoft Corporation
sihost.exe		4.136 K	18.164 K	3216	Shell Infrastructure Host	Microsoft Corporation
taskhostw.exe	< 0.01	5.012 K	12.908 K	3276	Processo host per attività di ...	Microsoft Corporation
svchost.exe		9.352 K	18.580 K	888	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		5.372 K	14.008 K	932	Processo host per servizi di ...	Microsoft Corporation
svchost.exe	0.78	18.468 K	23.804 K	1008	Processo host per servizi di ...	Microsoft Corporation
audiodg.exe		6.020 K	8.200 K	2724		
svchost.exe		8.732 K	21.400 K	288	Processo host per servizi di ...	Microsoft Corporation
VBoxService.exe	< 0.01	1.820 K	4.900 K	340	VirtualBox Guest Additions S...	Oracle and/or its affiliates
svchost.exe	< 0.01	36.144 K	46.512 K	540	Processo host per servizi di ...	Microsoft Corporation
WmsSvc.exe		4.812 K	12.916 K	1296	WmsService	Microsoft Corporation
WmsSessionAgent.exe				3248	Wms Session Agent	Microsoft Corporation
WmsSelfHealingSvc.exe				1304	WmsRepairService	Microsoft Corporation
spoolsv.exe				1504	Applicazione sottosistema sp...	Microsoft Corporation
svchost.exe		3.024 K	6.884 K	1584	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		5.672 K	16.744 K	1632	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		936 K	3.532 K	1640	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		3.756 K	9.628 K	1984	Processo host per servizi di ...	Microsoft Corporation
mqsvc.exe		2.656 K	6.892 K	1256	Message Queuing Service	Microsoft Corporation
snmp.exe	< 0.01	2.656 K	6.892 K	1628	Servizio SNMP	Microsoft Corporation
pg_ctl.exe		1.684 K	5.944 K	1684	pg_ctl - starts/stops/restarts ...	PostgreSQL Global Develo...
postgres.exe		3.332 K	12.172 K	2380	PostgreSQL Server	PostgreSQL Global Develo...
conhost.exe	< 0.01	10.124 K	7.756 K	2412	Console Window Host	Microsoft Corporation
postgres.exe		2.508 K	3.780 K	2592	PostgreSQL Server	PostgreSQL Global Develo...
postgres.exe		2.556 K	4.052 K	2728	PostgreSQL Server	PostgreSQL Global Develo...
postgres.exe		2.552 K	4.160 K	2736	PostgreSQL Server	PostgreSQL Global Develo...
postgres.exe		2.560 K	3.988 K	2744	PostgreSQL Server	PostgreSQL Global Develo...
postgres.exe		3.792 K	5.004 K	2752	PostgreSQL Server	PostgreSQL Global Develo...
postgres.exe		2.484 K	4.020 K	2760	PostgreSQL Server	PostgreSQL Global Develo...
TCPVCS.EXE		832 K	3.872 K	1936	TCP/IP Services Application	Microsoft Corporation

- Ho identificato i processi principali (ad esempio `explorer.exe`, `svchost.exe`).

svchost.exe	3.12	8.212 K	21.176 K	288	Processo host per servizi di ...	Microsoft Corporation
explorer.exe	< 0.01	38.352 K	106.096 K	3632	Esplora risorse	Microsoft Corporation

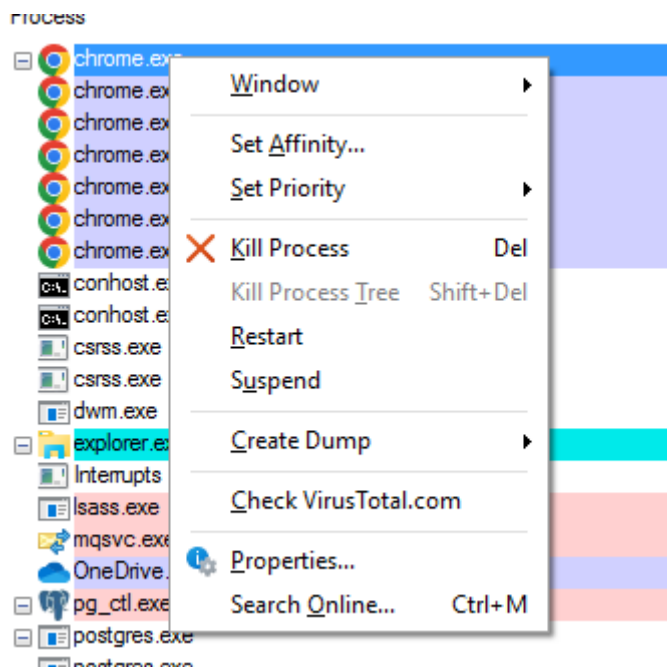
- Per ogni processo, ho osservato:

- **PID (Process ID)**
- Utilizzo della CPU e della memoria
- Percorso eseguibile.

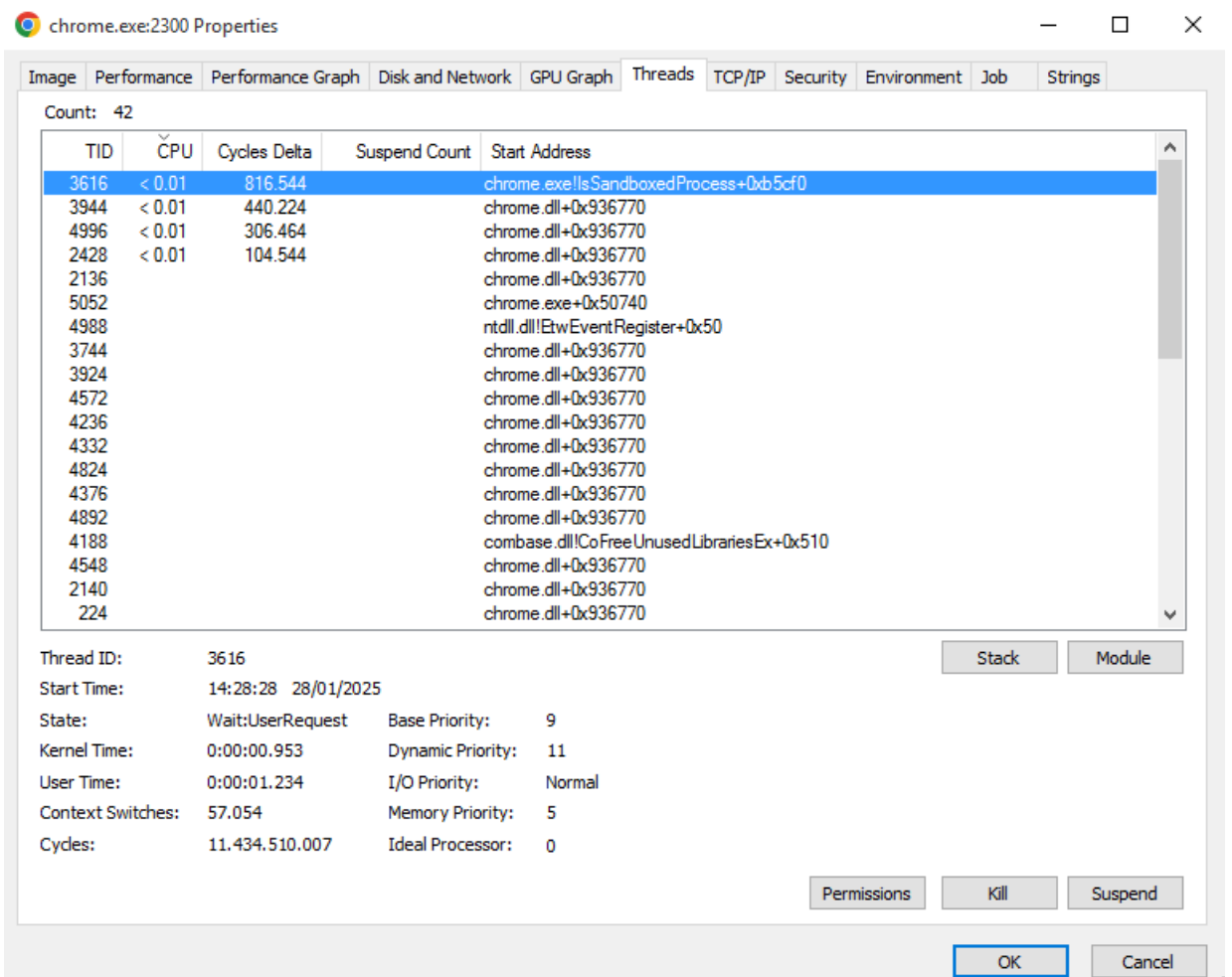
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
chrome.exe	< 0.01	47.404 K	129.188 K	2300	Google Chrome	Google LLC

3. Esplorazione dei Thread:

- Ho fatto clic destro su un processo (ad esempio `chrome.exe`, se aperto) e selezionato Properties.



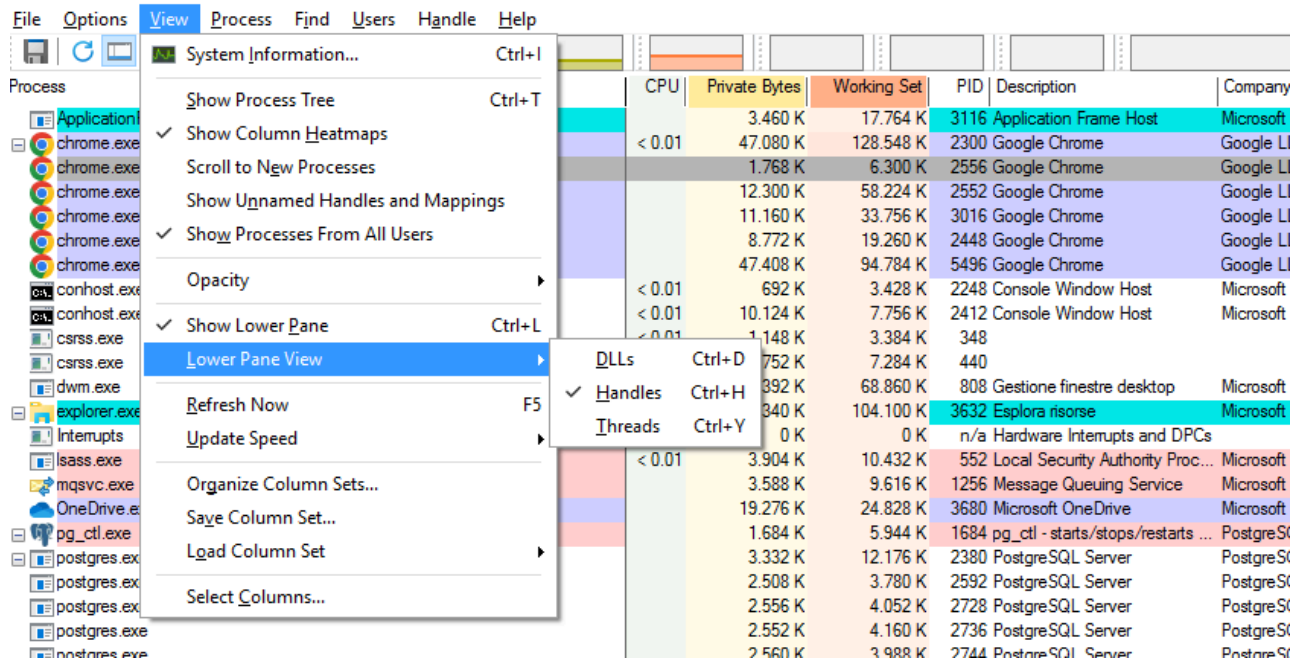
- Nella scheda **Threads**, ho:
 - Identificato i thread attivi.
 - Annotato il loro stato e i moduli associati.



4. Esplorazione degli Handle:

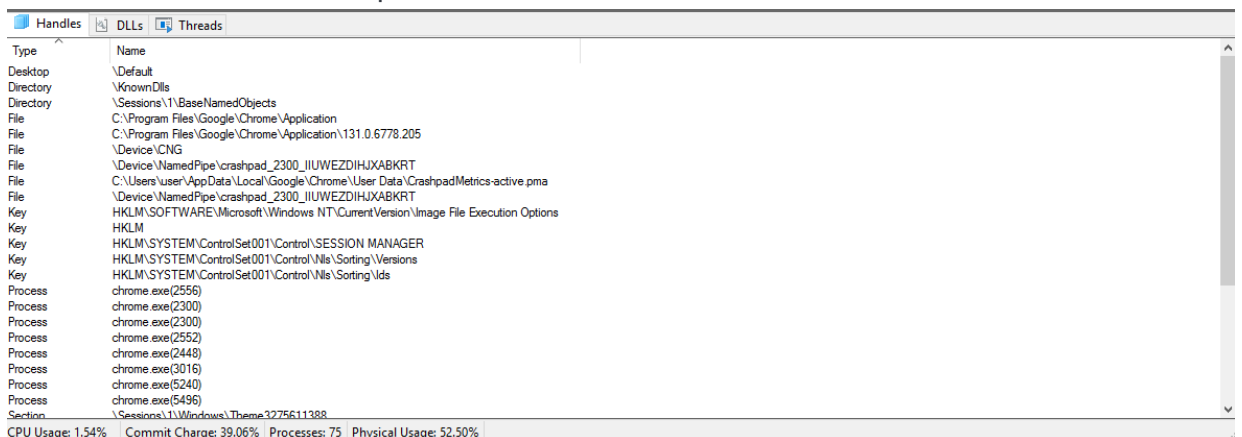
- Sono tornato su **Sysinternals Suite**.

- Nella scheda **View** ho abilitato la visualizzazione degli **Handles** da **Lower Pane View**



- Poi ho:

- Identificato le risorse aperte (file, chiavi di registro, ecc.).
- Notato eventuali handle sospetti o non necessari.

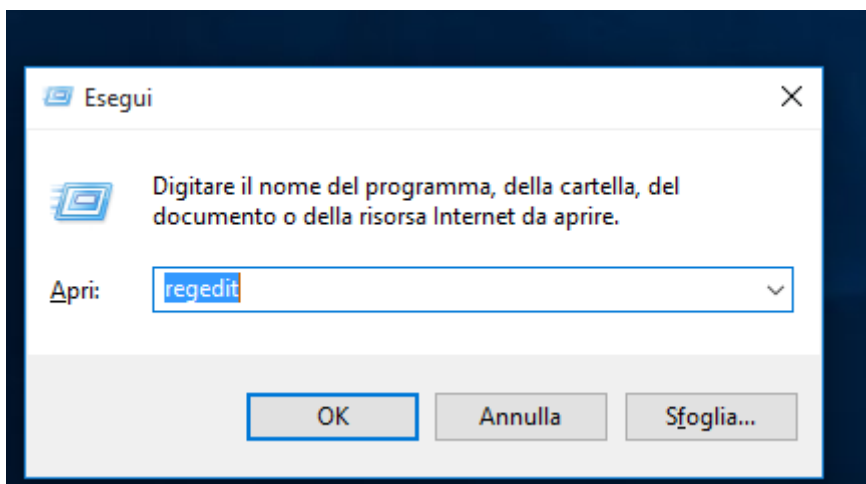


2. Modifica di un'Impostazione nel Registro di Windows

Passaggi:

1. Accesso al Registro di Windows:

- Nella macchina **Windows 10**, ho aperto il **Registry Editor** premendo **Win + R**, digitando **regedit** e premendo Invio.



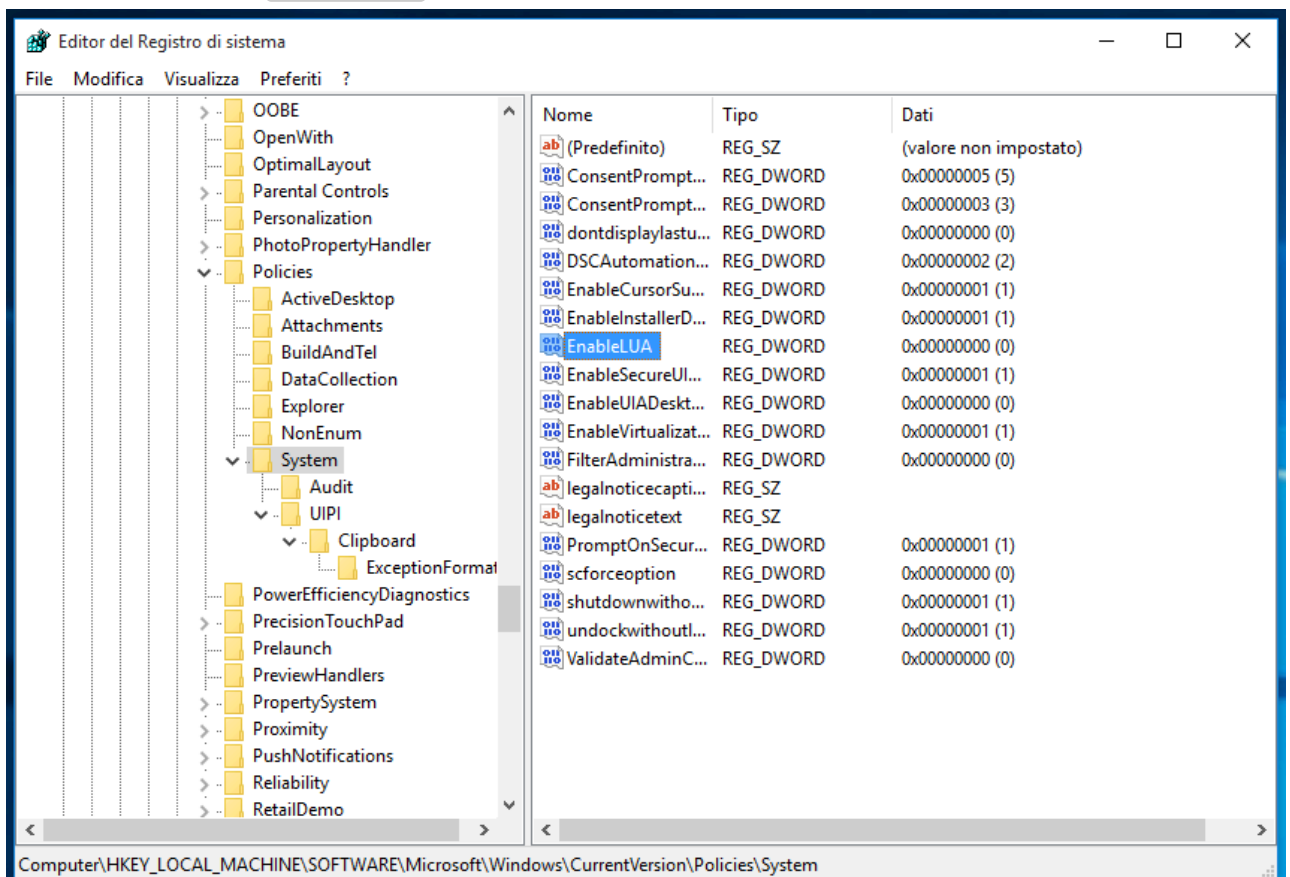
2. Individuazione della Chiave da Modificare:

- Ho navigato fino alla chiave:

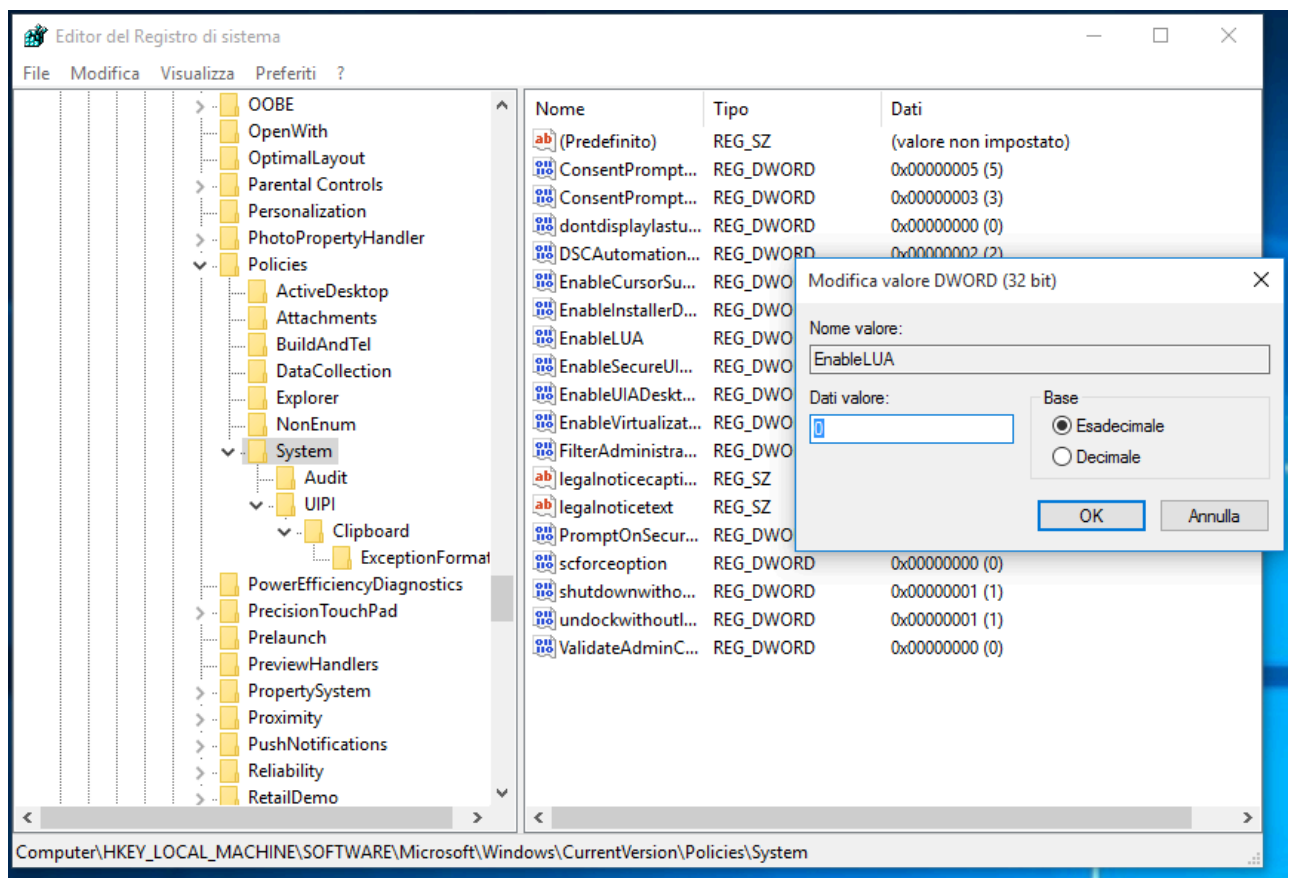
```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
```

3. Modifica dell'Impostazione:

- Ho trovato il valore `EnableLUA` (controllando che esistesse).



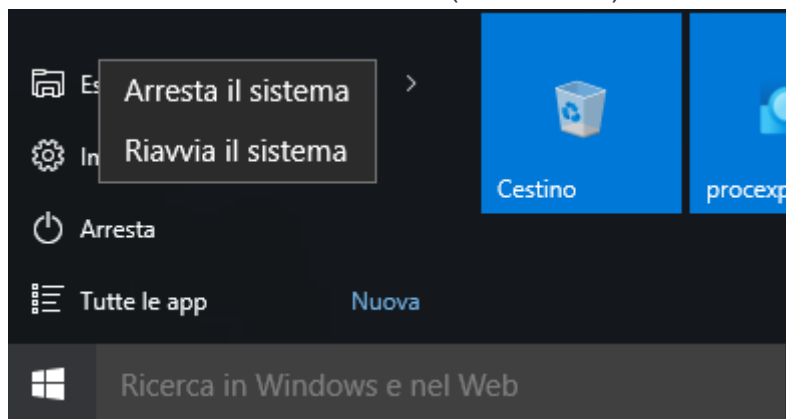
- Ho modificato il valore da `1` (abilitato) a `0` (disabilitato) per disabilitare il Controllo dell'Account Utente (UAC).



- Ho cliccato su OK per salvare la modifica.

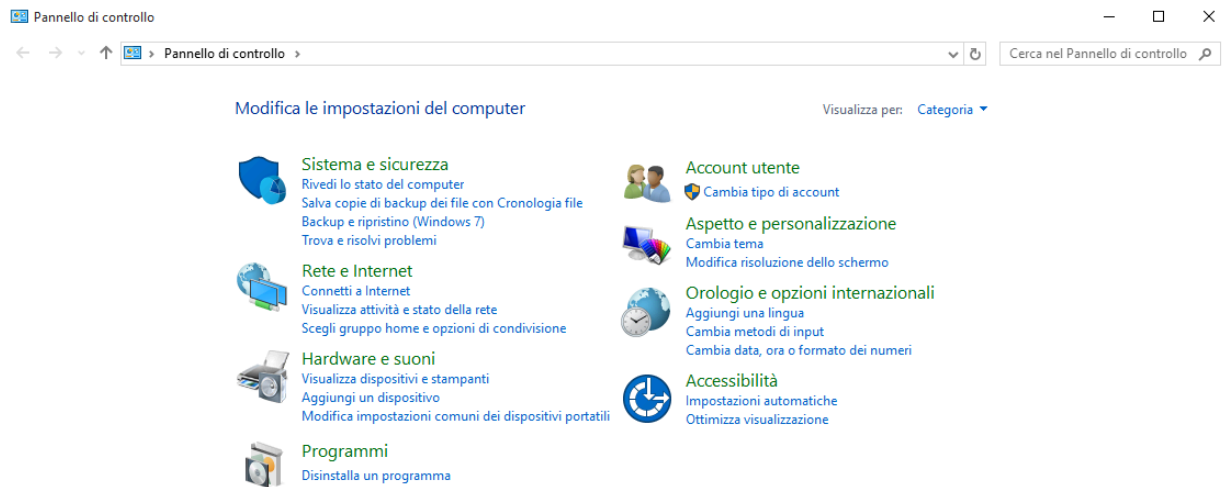
4. Verifica dell'Effetto della Modifica:

- Ho riavviato la macchina virtuale (se richiesto).

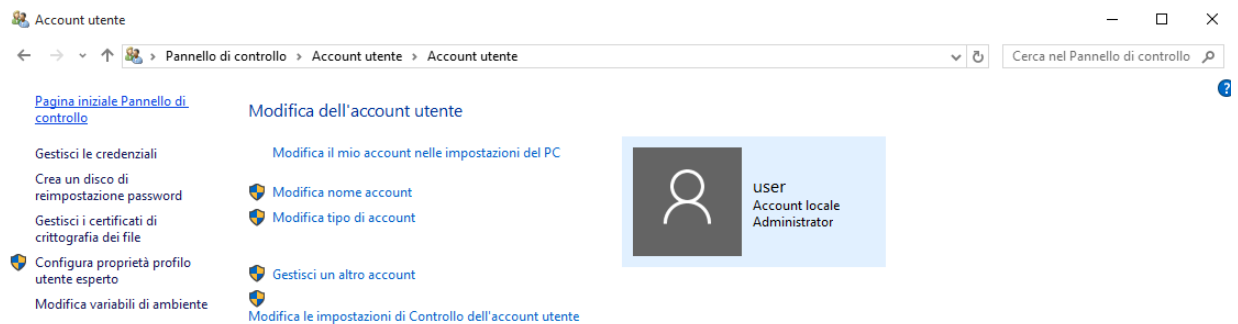


- Ho verificato che l'UAC fosse stato disabilitato (nel Pannello di controllo):.

- Ho aperto il **Pannello di controllo**.



- Sono andata su **Account utente > Modifica le impostazioni di Controllo dell'account utente**.



- Ho verificato che la barra fosse completamente abbassata su **Non notificare mai**, confermando che l'UAC era disabilitato.

Scegliere i casi in cui si desidera ricevere le notifiche per le modifiche apportate al computer

Controllo dell'account utente consente di impedire a programmi potenzialmente dannosi di apportare modifiche al computer.

[Ulteriori informazioni sulle impostazioni di Controllo dell'account utente](#)

Notifica sempre



Non notificare mai

Non notificare mai all'utente quando:

- Un'app tenta di installare software o di eseguire modifiche nel computer
- L'utente modifica le impostazioni di Windows



Per applicare questa impostazione, fare clic su OK per riavviare il PC.

OK

Annulla

Nota: Al termine, ho ripristinato il valore originale (1) per motivi di sicurezza.