

Es.1 PowerShell

Relazione sull'utilizzo di PowerShell



Tag:

#powershell

#comandi

#networking

#windows

Introduzione

PowerShell è un potente strumento di automazione della riga di comando e scripting progettato da Microsoft, utile per l'amministrazione e la gestione di ambienti Windows. In questa relazione, sono stati eseguiti diversi comandi tramite PowerShell e il prompt dei comandi per esaminare la configurazione del sistema, le interfacce di rete, la tabella di routing e le connessioni attive, oltre alla gestione del cestino.

Comandi eseguiti e risultati

1. Comando `dir` (Get-ChildItem)

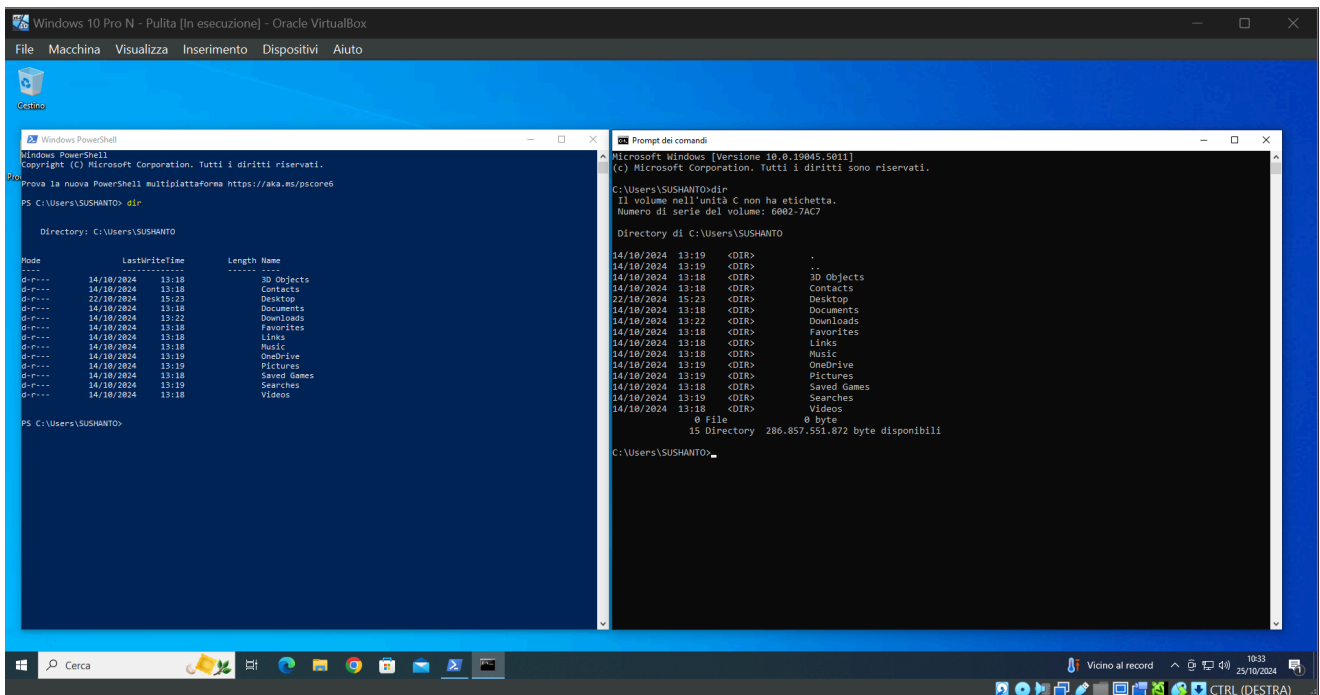
- Eseguito per visualizzare la lista delle directory e dei file nella cartella dell'utente.
- Risultato: Elenco delle directory principali, come "Documents", "Downloads", "Pictures", ecc.



Tag:

#directory

#file

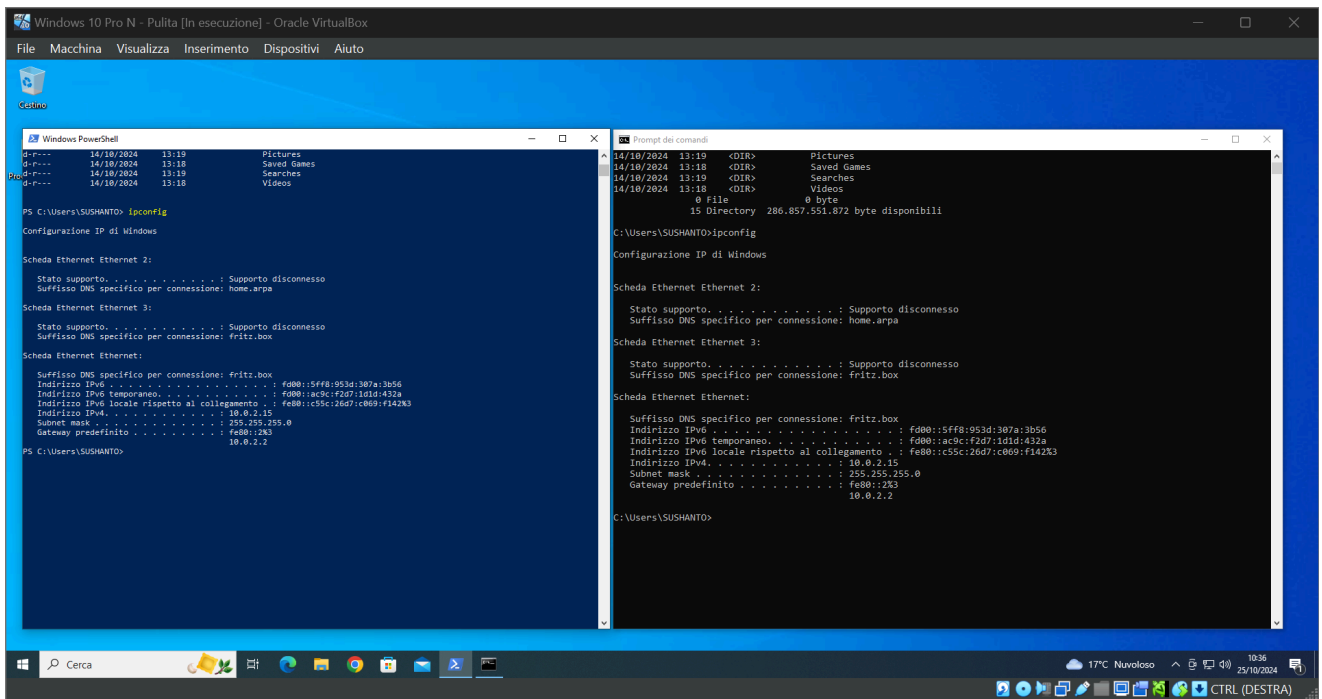


2. Comando ipconfig

- Utilizzato per visualizzare la configurazione IP delle schede di rete.
- Risultato: Le schede Ethernet 2 e 3 risultano disconnesse, mentre la scheda Ethernet principale è collegata, con un indirizzo IPv4 (10.0.2.15), un gateway predefinito (10.0.2.2) e indirizzi IPv6 assegnati.



Tag: #ipconfig #networking

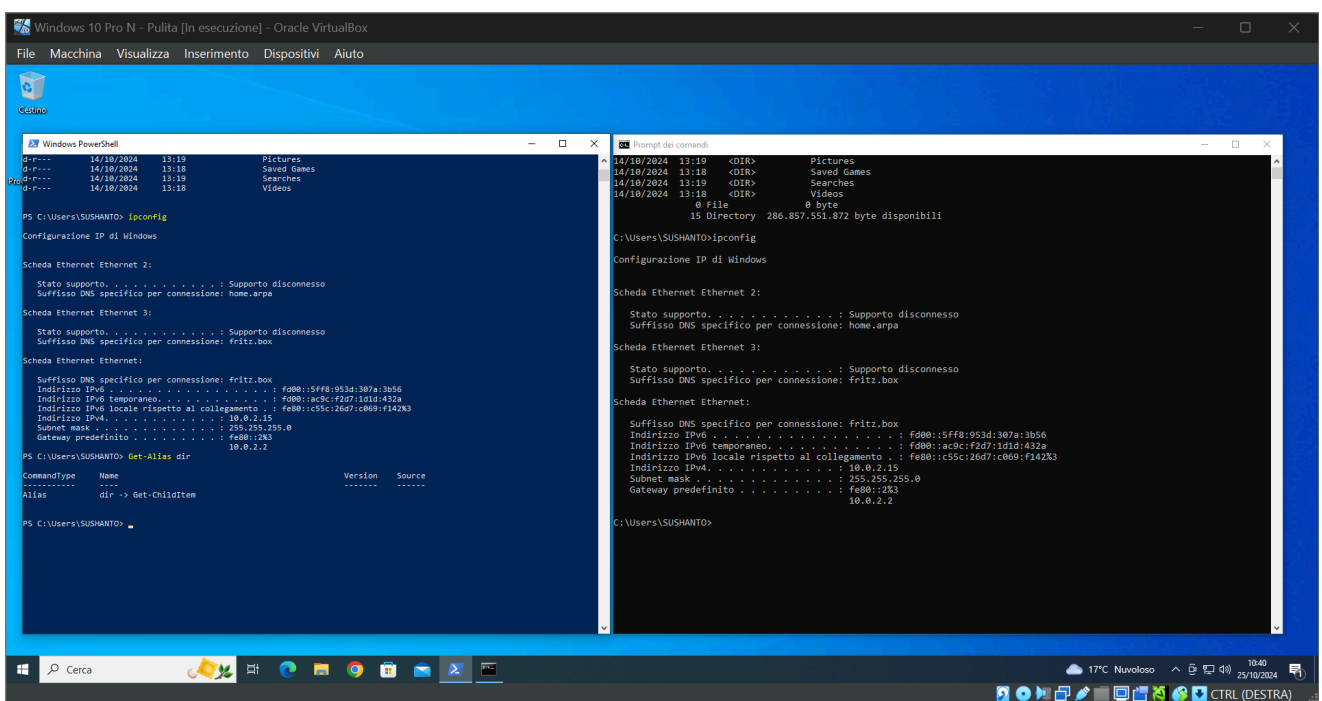


3. Comando Get-Alias

- Eseguito per verificare l'alias associato al comando `dir`, che punta a `Get-ChildItem`.
- Risultato: L'alias `dir` è associato al comando `Get-ChildItem`.



Tag: [#alias](#) [#comandi](#)



4. Comando netstat -h

- Fornisce una guida sui parametri disponibili per il comando `netstat`, utile per monitorare le connessioni di rete attive e le statistiche.
- Risultato: Mostra i dettagli sulle opzioni di `netstat`, come visualizzare tutte le connessioni (`-a`), l'elenco delle porte in ascolto (`-b`), e la tabella di routing (`-r`).



Tag: [#netstat](#) [#networking](#)

```
Windows 10 Pro N - Pulita [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

Windows PowerShell
CommandType Name Version Source
-----
Alias dir -> Get-Childitem

PS C:\Users\SUSHANTO> netstat -h

Visualizza le statistiche del protocollo e le connessioni di rete TCP/IP correnti.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [interval]

-a Visualizza tutte le connessioni e le porte di ascolto.
-b Visualizza l'eseguibile coinvolto nella creazione di ogni connessione o
  porta di ascolto. In alcuni casi, host di eseguibili noti
  più componenti indipendenti e in questi casi il
  sequenza di componenti coinvolti nella creazione della connessione
  o la porta in ascolto. In questo caso, l'eseguibile
  il nome è in [] nella parte inferiore, in alto è il componente che ha chiamato,
  e così via fino al raggiungimento di TCP/IP. Si noti che questa opzione
  può richiedere molto tempo e avrà esito negativo, a meno che non siano sufficienti
  autorizzazioni.
-e Visualizza le statistiche Ethernet. È possibile combinare
  opzione.
-f Visualizza nomi di dominio completi (FQDN) per stranieri
  indirizzi.
-n Visualizza indirizzi e numeri di porta in formato numerico.
-o Visualizza l'ID del processo proprietario associato a ogni connessione.
-p proto Mostra le connessioni per il protocollo specificato da proto; proto
  può essere qualsiasi: TCP, UDP, ICMPv6 o UDPv6. Se usato con
  opzione per la visualizzazione delle statistiche per protocollo, Proto può essere qualsiasi:
  IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
  Visualizza tutte le connessioni, le porte di ascolto e i binding
  non in ascolto di porte TCP. Le porte di nonlistening associate possono o meno essere
  essere associate a una connessione attiva.
-r Visualizza la tabella di routing. Per impostazione predefinita, le statistiche vengono
  visualizzate per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6;
  l'opzione-p può essere utilizzata per specificare un sottoinsieme del valore predefinito.
-s Visualizza lo stato corrente di origine della connessione.
-t Visualizza connessioni NetworkDirect, listener e condivisi
  endpoint.
-y Visualizza il modello di connessione TCP per tutte le connessioni.
  Non può essere combinato con le altre opzioni.
intervallo Rivisualizza le statistiche selezionate, la sospensione dell'intervallo di secondi
  tra ogni schermo. Premere CTRL+C per interrompere la rivisualizzazione
  Statistiche. Se viene omesso, netstat stamperà il
  informazioni di configurazione una volta.

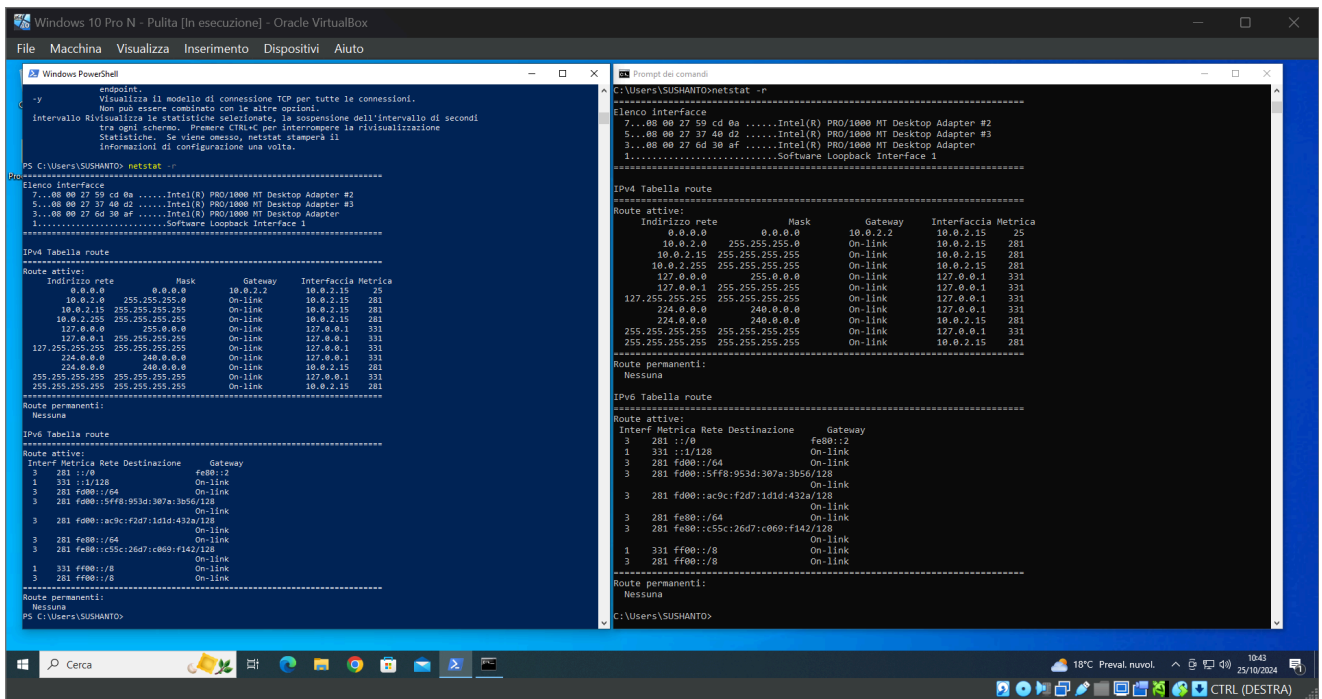
PS C:\Users\SUSHANTO>
```

5. Comando netstat -r

- Visualizza la tabella di routing IPv4 e IPv6 del sistema.
- Risultato: Mostra le rotte attive e permanenti per gli indirizzi IPv4 e IPv6, con dettagli su maschere di sottorete, gateway e metriche di interfaccia.



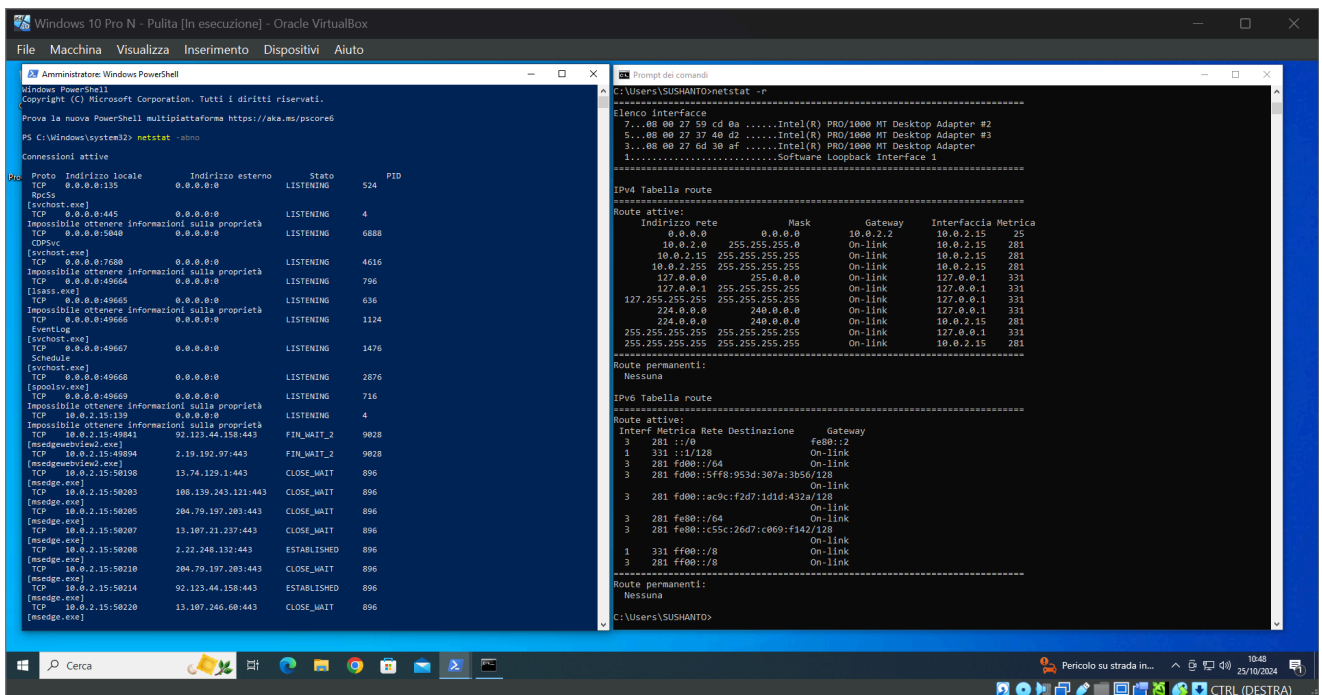
Tag: [#routing](#) [#ipv4](#) [#ipv6](#)



6. Comando netstat -abno

- Utilizzato per elencare tutte le connessioni attive con il PID associato, mostrando anche gli indirizzi di rete locali ed esterni.
- Risultato: Elenco dettagliato delle connessioni di rete attive, con informazioni sullo stato (es. LISTENING) e i PID (es. 524).

Tag: [#connessioni](#) [#processi](#)



7. Verifica PID 524

- Tramite il Task Manager, si è verificato che il processo associato al PID 524 è `svchost.exe`, il servizio di rete in ascolto sulla porta 135.

Tag: #pid #processi

Windows 10 Pro N - Pulita [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

Selezione Amministratore Windows PowerShell

Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Prova la nuova PowerShell multiplatforma https://aka.ms/pscore6

PS C:\Windows\system32> netstat -sno

Connessioni attive

Proto	Indirizzo locale	Indirizzo esterno	Stato	PID
TCP	0.0.0.0:3335	0.0.0.0:0	LISTENING	524
Rpcss				
[svchost.exe]				
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	6888
CDPSvc				
[svchost.exe]				
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING	4616
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	796
[lsass.exe]				
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	636
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	1124
Eventlog				
[svchost.exe]				
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1476
Schedule				
[svchost.exe]				
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	2876
[spoolsv.exe]				
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	716
Impossibile ottenere informazioni sulla proprietà				
TCP	10.0.2.15:119	0.0.0.0:0	LISTENING	4
Impossibile ottenere informazioni sulla proprietà				
TCP	10.0.2.15:49841	92.123.44.158:443	FIN_WAIT_2	9028
[msedge.exe]				
TCP	10.0.2.15:49894	2.19.192.97:443	FIN_WAIT_2	9028
[msedge.exe]				
TCP	10.0.2.15:50198	13.74.129.1:443	CLOSE_WAIT	896
[msedge.exe]				
TCP	10.0.2.15:50203	188.139.243.121:443	CLOSE_WAIT	896
[msedge.exe]				
TCP	10.0.2.15:50205	204.79.197.203:443	CLOSE_WAIT	896
[msedge.exe]				
TCP	10.0.2.15:50207	13.107.21.237:443	CLOSE_WAIT	896
[msedge.exe]				
TCP	10.0.2.15:50208	2.22.248.132:443	ESTABLISHED	896
[msedge.exe]				
TCP	10.0.2.15:50210	204.79.197.203:443	CLOSE_WAIT	896
[msedge.exe]				
TCP	10.0.2.15:50214	92.123.44.158:443	ESTABLISHED	896
[msedge.exe]				
TCP	10.0.2.15:50220	13.107.246.60:443	CLOSE_WAIT	896
[msedge.exe]				

Gestione attività

Processi Prestazioni Cronologia applicazioni Avvio Utenti Dettagli Servizi

Nome	PID	Stato	Nome utente	CPU	Memoria	Virtualizzazio...
Interrup sistema	-	In esecuzione	SYSTEM	00	0 K	
Processo di inattiva...	0	In esecuzione	SYSTEM	97	8 K	
System	4	In esecuzione	SYSTEM	01	20 K	
Registry	124	In esecuzione	SYSTEM	00	3.032 K	Non consentito
smss.exe	452	In esecuzione	SYSTEM	00	244 K	Non consentito
svchost.exe	504	In esecuzione	SYSTEM	00	1.304 K	Non consentito
svchost.exe	524	In esecuzione	SERVIZIO DI RETE	00	7.044 K	Non consentito
csrss.exe	556	In esecuzione	SYSTEM	00	868 K	Non consentito
wininit.exe	636	In esecuzione	SYSTEM	00	884 K	Non consentito
csrss.exe	644	In esecuzione	SYSTEM	00	1.124 K	Non consentito
services.exe	716	In esecuzione	SYSTEM	00	4.272 K	Non consentito
winlogon.exe	744	In esecuzione	SYSTEM	00	1.404 K	Non consentito
lsass.exe	796	In esecuzione	SYSTEM	00	5.840 K	Non consentito
svchost.exe	888	In esecuzione	SERVIZIO LOCALE	00	3.024 K	Non consentito
msedge.exe	896	In esecuzione	SLSHANTD	00	6.700 K	Disabilitato
svchost.exe	920	In esecuzione	SYSTEM	00	7.664 K	Non consentito
fontdrvhost.exe	956	In esecuzione	UMFD-0	00	1.092 K	Disabilitato
svchost.exe	1040	In esecuzione	SYSTEM	00	1.200 K	Non consentito
svchost.exe	1058	In esecuzione	SERVIZIO LOCALE	00	872 K	Non consentito
OneDrive.exe	1092	In esecuzione	SLSHANTD	00	32.168 K	Disabilitato
svchost.exe	1124	In esecuzione	SERVIZIO LOCALE	00	10.324 K	Non consentito
svchost.exe	1148	In esecuzione	SYSTEM	00	1.480 K	Non consentito
svchost.exe	1156	In esecuzione	SERVIZIO LOCALE	00	1.664 K	Non consentito
dmv.exe	1232	In esecuzione	DWM-1	01	24.420 K	Disabilitato
svchost.exe	1260	In esecuzione	SERVIZIO LOCALE	00	4.504 K	Non consentito
svchost.exe	1348	In esecuzione	SERVIZIO LOCALE	00	1.928 K	Non consentito
svchost.exe	1384	In esecuzione	SERVIZIO LOCALE	00	1.928 K	Non consentito
svchost.exe	1476	In esecuzione	SYSTEM	00	4.808 K	Non consentito
svchost.exe	1488	In esecuzione	SYSTEM	00	1.700 K	Non consentito
svchost.exe	1596	In esecuzione	SERVIZIO DI RETE	00	2.412 K	Non consentito
svchost.exe	1624	In esecuzione	SYSTEM	00	1.384 K	Non consentito
svchost.exe	1768	In esecuzione	SERVIZIO LOCALE	00	1.108 K	Non consentito
VBoxService.exe	1796	In esecuzione	SYSTEM	00	1.516 K	Non consentito
svchost.exe	1832	In esecuzione	SERVIZIO LOCALE	00	2.384 K	Non consentito
svchost.exe	1908	In esecuzione	SERVIZIO LOCALE	00	18.454 K	Non consentito

Cerca

FTSE mib +0.04%

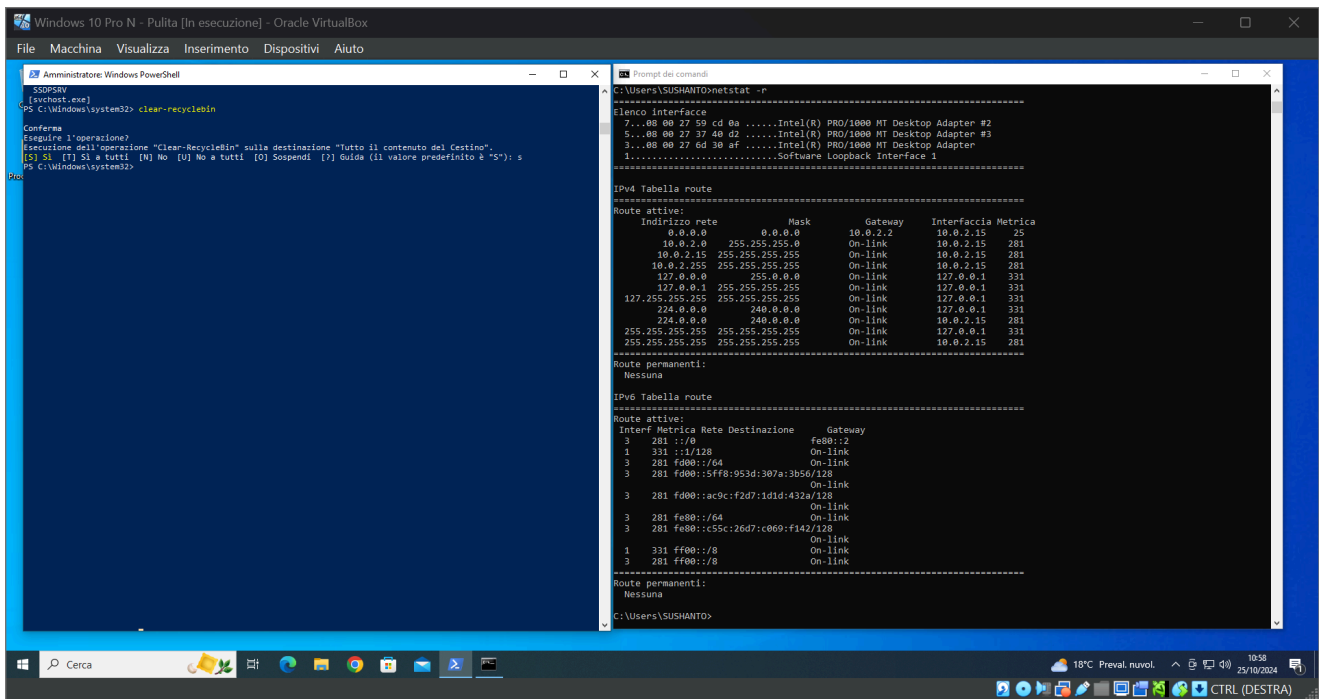
10:55 25/10/2024

CTRL (DESTRA)

8. Comando `clear-recyclebin`

- Utilizzato per svuotare il cestino tramite PowerShell.
- Risultato: Conferma dell'esecuzione e pulizia del contenuto del cestino.

Tag: #cestino #gestioneFile



Chiavi:

[powershell, comandi, networking, windows, netstat, ipconfig]