

Utilizzo di Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

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

PS C:\Users\User> dir

Directory: C:\Users\User

Mode                LastWriteTime         Length Name
----                -
d-r---           08/09/2024    23:19             3D Objects
d-r---           08/09/2024    23:19             Contacts
d-r---           08/09/2024    23:19             Desktop
d-r---           08/09/2024    23:19             Documents
d-r---           08/09/2024    23:19             Downloads
d-r---           08/09/2024    23:19             Favorites
d-r---           08/09/2024    23:19             Links
d-r---           08/09/2024    23:19             Music
d-r---           25/10/2024    10:25             OneDrive
d-r---           08/09/2024    23:22             Pictures
d-r---           08/09/2024    23:19             Saved Games
d-r---           08/09/2024    23:21             Searches
d-r---           08/09/2024    23:19             Videos

PS C:\Users\User>
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

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

PS C:\Users\User> dir

Directory: C:\Users\User

Mode                LastWriteTime         Length Name
----                -
d-r---            08/09/2024    23:19             3D Objects
d-r---            08/09/2024    23:19             Contacts
d-r---            08/09/2024    23:19             Desktop
d-r---            08/09/2024    23:19             Documents
d-r---            08/09/2024    23:19             Downloads
d-r---            08/09/2024    23:19             Favorites
d-r---            08/09/2024    23:19             Links
d-r---            08/09/2024    23:19             Music
d-r---            25/10/2024    10:25             OneDrive
d-r---            08/09/2024    23:22             Pictures
d-r---            08/09/2024    23:19             Saved Games
d-r---            08/09/2024    23:21             Searches
d-r---            08/09/2024    23:19             Videos

PS C:\Users\User> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: station
    Indirizzo IPv6 . . . . . : fd00::f1b3:4604:1737:425e
    Indirizzo IPv6 temporaneo. . . . . : fd00::59dc:43bb:11bf:cb28
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::7de5:ce64:b266:fed3%5
    Indirizzo IPv4. . . . . : 10.0.2.15
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : fe80::2%5
                                   10.0.2.2

PS C:\Users\User>
```

```
Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: station
    Indirizzo IPv6 . . . . . : fd00::f1b3:4604:1737:425e
    Indirizzo IPv6 temporaneo. . . . . : fd00::59dc:43bb:11bf:cb28
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::7de5:ce64:b266:fed3%5
    Indirizzo IPv4. . . . . : 10.0.2.15
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : fe80::2%5
                                   10.0.2.2

PS C:\Users\User> Get-Alias dir

CommandType      Name
-----
Alias             dir -> Get-ChildItem
```

```
PS C:\Users\User> 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, TCPv6 o UDPv6. Se usato con-s opzione per la visualizzazione delle statistiche per protocollo, Proto può essere qualsiasi: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP o UDPv6.
 - q 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 associato a una connessione attiva.
 - r Visualizza la tabella di routing.
 - s Visualizza le statistiche per protocollo. Per impostazione predefinita, le statistiche vengono visualizzata per IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6; l'opzione-p può essere utilizzata per specificare un sottoinsieme del valore predefinito.
 - t Visualizza lo stato corrente di offload della connessione.
 - x 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 omissso, netstat stamperà il informazioni di configurazione una volta.

```
PS C:\Users\User>
```

```
Windows PowerShell

tra ogni schermo. Premere CTRL+C per interrompere la rivisualizzazione
Statistiche. Se viene omissso, netstat stamperà il
informazioni di configurazione una volta.

PS C:\Users\User> netstat -r
=====
Elenco interfacce
5...08 00 27 96 c2 10 .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
=====

IPv4 Tabella route
=====
Route attive:
Indirizzo rete      Mask      Gateway    Interfaccia Metrica
0.0.0.0             0.0.0.0    10.0.2.2   10.0.2.15    25
10.0.2.0            255.255.255.0    On-link    10.0.2.15    281
10.0.2.15           255.255.255.255    On-link    10.0.2.15    281
10.0.2.255          255.255.255.255    On-link    10.0.2.15    281
127.0.0.0            255.0.0.0    On-link    127.0.0.1    331
127.0.0.1           255.255.255.255    On-link    127.0.0.1    331
127.255.255.255     255.255.255.255    On-link    127.0.0.1    331
224.0.0.0            240.0.0.0    On-link    127.0.0.1    331
224.0.0.0            240.0.0.0    On-link    10.0.2.15    281
255.255.255.255     255.255.255.255    On-link    127.0.0.1    331
255.255.255.255     255.255.255.255    On-link    10.0.2.15    281
=====
Route permanenti:
Nessuna

IPv6 Tabella route
=====
Route attive:
Interf Metrica Rete Destinazione Gateway
5      281 ::/0             fe80::2
1      331 ::1/128           On-link
5      281 fd00::/64         On-link
5      281 fd00::59dc:43bb:11bf:cb28/128
On-link
5      281 fd00::f1b3:4604:1737:425e/128
On-link
5      281 fe80::/64         On-link
5      281 fe80::7de5:ce64:b266:fed3/128
On-link
1      331 ff00::/8           On-link
5      281 ff00::/8           On-link
=====
Route permanenti:
Nessuna
PS C:\Users\User>
```


Windows PowerShell

Amministratore: Windows PowerShell

Statistiche. Se viene omissa, netstat stamperà il informazioni di configurazione una volta.

PS C:\Users\User> netstat -r

Elenco interfacce

5...08 00 27 96 c2 10Intel(R) PRO/1000 MT Desktop Adapter

1.....Software Loopback Interface 1

IPv4 Tabella route

Route attive:

Indirizzo rete	Mask	Gateway	Interfaccia	Metrica
0.0.0.0	0.0.0.0	10.0.2.2	10.0.2.15	25
10.0.2.0	255.255.255.0	On-link	10.0.2.15	281
10.0.2.15	255.255.255.255	On-link	10.0.2.15	281
10.0.2.255	255.255.255.255	On-link	10.0.2.15	281
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
127.0.0.1	255.255.255.255	On-link	127.0.0.1	331
127.255.255.255	255.255.255.255	On-link	127.0.0.1	331
224.0.0.0	240.0.0.0	On-link	10.0.2.15	281
255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
255.255.255.255	255.255.255.255	On-link	10.0.2.15	281

Route permanenti:
Nessuna

IPv6 Tabella route

Route attive:

Interf	Metрика	Rete	Destinazione	Gateway
5	281	:::/0		fe80::2
1	331	::1/128		On-link
5	281	fd00::/64		On-link
5	281	fd00::59dc:43bb:11bf:c28/128		On-link
5	281	fd00::f1b3:4604:1737:425e/128		On-link
5	281	fe80::/64		On-link
5	281	fe80::7de5:ce64:b266:fed3/128		On-link
1	331	ff00::/8		On-link
5	281	ff00::/8		On-link

Route permanenti:
Nessuna

PS C:\Users\User>

Windows PowerShell

Amministratore: Windows PowerShell

Windows PowerShell

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

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

PS C:\Windows\system32> netstat -abno

Connessioni attive

Proto	Indirizzo locale	Indirizzo esterno	Stato	PID	
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	1020	
RpcSs					
[svchost.exe]	TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
Impossibile ottenere informazioni sulla proprietà	TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING	4624
CDPSvc					
[svchost.exe]	TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING	532
Impossibile ottenere informazioni sulla proprietà	TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	772
[lsass.exe]	TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	584
Impossibile ottenere informazioni sulla proprietà	TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1408
EventLog					
[svchost.exe]	TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1260
Schedule					
[svchost.exe]	TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	2764
[spoolsv.exe]	TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	704
Impossibile ottenere informazioni sulla proprietà	TCP	10.0.2.15:139	0.0.0.0:0	LISTENING	4
Impossibile ottenere informazioni sulla proprietà	TCP	10.0.2.15:49685	91.81.130.151:80	CLOSE_WAIT	5280
[wwahost.exe]	TCP	10.0.2.15:49686	192.229.221.95:80	CLOSE_WAIT	5280
[wwahost.exe]	TCP	10.0.2.15:49687	104.104.52.105:443	CLOSE_WAIT	5280
[wwahost.exe]	TCP	10.0.2.15:49688	104.104.52.105:443	CLOSE_WAIT	5280
[wwahost.exe]	TCP	10.0.2.15:49689	104.104.52.105:443	CLOSE_WAIT	5280
[wwahost.exe]	TCP	10.0.2.15:49690	104.104.52.105:443	CLOSE_WAIT	5280
[wwahost.exe]	TCP	10.0.2.15:49691	104.104.52.105:443	CLOSE_WAIT	5280

Proprietà - svchost

Generale

Firme digitali

Sicurezza

Dettagli

Versioni precedenti

svchost

Tipo di file: Applicazione (exe)

Descrizione: Processo host per servizi di Windows

Percorso: C:\Windows\System32

Dimensioni: 54,0 KB (57.320 byte)

Dimensioni su disco: 56,0 KB (57.344 byte)

Data creazione: venerdì 5 maggio 2023, 14:22:19

Ultima modifica: venerdì 5 maggio 2023, 14:22:19

Ultimo accesso: Oggi 25 ottobre 2024, 11 minuti fa

Attributi: ☐ Sola lettura ☐ Nascondo

OK

Annulla

Applica

Gestione attività

File

Opzioni

Visualizza

Processi

Prestazioni

Cronologia applicazioni

Avvio

Utenti

Dettagli

Servizi

Nome	PID	Stato	Nome utente	CPU	Memoria (workin...	Virtualizzazione cont...
svchost.exe	7740	In esecuzione	SYSTEM	00	1.776 K	Non consentito
svchost.exe	7688	In esecuzione	SERVIZIO LOCALE	00	1.860 K	Non consentito
svchost.exe	7672	In esecuzione	SYSTEM	00	2.580 K	Non consentito
msedge.exe	7604	In esecuzione	User	00	19.528 K	Disabilitato
conhost.exe	7472	In esecuzione	User	00	3.584 K	Disabilitato
svchost.exe	7464	In esecuzione	SERVIZIO LOCALE	00	2.464 K	Non consentito
svchost.exe	7268	In esecuzione	SYSTEM	00	5.252 K	Non consentito
powershell.exe	7240	In esecuzione	User	00	54.072 K	Disabilitato
svchost.exe	7224	In esecuzione	SERVIZIO LOCALE	00	1.512 K	Non consentito
msedge.exe	7148	In esecuzione	User	00	42.128 K	Disabilitato
RuntimeBroker.exe	7112	In esecuzione	User	00	700 K	Disabilitato
SearchApp.exe	7036	Sospeso	User	00	0 K	Disabilitato
svchost.exe	6956	In esecuzione	SERVIZIO DI RETE	00	2.844 K	Non consentito
SearchIndexer.exe	6940	In esecuzione	SYSTEM	00	10.068 K	Non consentito
RuntimeBroker.exe	6868	In esecuzione	User	00	4.576 K	Disabilitato
dllhost.exe	6664	In esecuzione	User	00	2.208 K	Disabilitato
WinStore.App.exe	6628	Sospeso	User	00	0 K	Disabilitato
svchost.exe	6500	In esecuzione	SYSTEM	00	11.492 K	Non consentito
SearchFilterHost.exe	6376	In esecuzione	SYSTEM	00	1.020 K	Non consentito
RuntimeBroker.exe	6240	In esecuzione	User	00	8.440 K	Disabilitato
TiWorker.exe	6220	In esecuzione	SYSTEM	00	2.620 K	Non consentito
svchost.exe	6108	In esecuzione	User	00	1.592 K	Disabilitato
svchost.exe	6072	In esecuzione	SYSTEM	00	1.576 K	Non consentito

PS C:\Windows\system32> clear-recyclebin

Conferma

Eseguire l'operazione?

Esecuzione dell'operazione "Clear-RecycleBin" sulla destinazione "Tutto il contenuto del Cestino".

[S] Sì [T] Sì a tutti [N] No [U] No a tutti [O] Sospendi [?] Guida

(il valore predefinito è "S"):s

PS C:\Windows\system32>