

Using Windows PowerShell

Iniziamo aprendo una finestra di PowerShell e una di Prompt dei comandi, diamo il comando `dir` e confrontiamo, gli output sono simili, powershell mostra anche i permessi:

Prompt dei comandi

Microsoft Windows [Versione 10.0.19045.3803]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\User>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: F812-46F0

Directory di C:\Users\User

14/10/2024 18:46 <DIR> .
14/10/2024 18:46 <DIR> ..
14/10/2024 10:30 <DIR> .splunk
29/07/2024 15:49 <DIR> 3D Objects
29/07/2024 15:49 <DIR> Contacts
22/10/2024 14:31 <DIR> Desktop
29/07/2024 15:49 <DIR> Documents
24/10/2024 10:15 <DIR> Downloads
29/07/2024 15:49 <DIR> Favorites
29/07/2024 15:49 <DIR> Links
29/07/2024 15:49 <DIR> Music
24/08/2024 20:47 <DIR> OneDrive
29/07/2024 15:51 <DIR> Pictures
29/07/2024 15:49 <DIR> Saved Games
29/07/2024 15:49 <DIR> Searches
29/07/2024 15:49 <DIR> Videos
0 File 0 byte
16 Directory 25.302.151.168 byte disponibili

C:\Users\User>

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----- 14/10/2024 10:30 .splunk
d-r--- 29/07/2024 15:49 3D Objects
d-r--- 29/07/2024 15:49 Contacts
d-r--- 22/10/2024 14:31 Desktop
d-r--- 29/07/2024 15:49 Documents
d-r--- 24/10/2024 10:15 Downloads
d-r--- 29/07/2024 15:49 Favorites
d-r--- 29/07/2024 15:49 Links
d-r--- 29/07/2024 15:49 Music
d-r--- 24/08/2024 20:47 OneDrive
d-r--- 29/07/2024 15:51 Pictures
d-r--- 29/07/2024 15:49 Saved Games
d-r--- 29/07/2024 15:49 Searches
d-r--- 29/07/2024 15:49 Videos

PS C:\Users\User>

Proviamo con altri comandi come `ping` `cd` e `ipconfig`:

Prompt dei comandi

C:\Users\User>ping rickastley.co.uk

Esecuzione di Ping rickastley.co.uk [217.160.0.132] con 32 byte di dati:
Risposta da 217.160.0.132: byte=32 durata=28ms TTL=52
Risposta da 217.160.0.132: byte=32 durata=39ms TTL=52
Risposta da 217.160.0.132: byte=32 durata=27ms TTL=52
Risposta da 217.160.0.132: byte=32 durata=28ms TTL=52

Statistiche Ping per 217.160.0.132:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 27ms, Massimo = 39ms, Medio = 30ms

Windows PowerShell

PS C:\Users\User> ping rickastley.co.uk

Esecuzione di Ping rickastley.co.uk [217.160.0.132] con 32 byte di dati:
Risposta da 217.160.0.132: byte=32 durata=27ms TTL=52
Risposta da 217.160.0.132: byte=32 durata=27ms TTL=52
Risposta da 217.160.0.132: byte=32 durata=26ms TTL=52
Risposta da 217.160.0.132: byte=32 durata=39ms TTL=52

Statistiche Ping per 217.160.0.132:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 26ms, Massimo = 39ms, Medio = 29ms
PS C:\Users\User>

```

C:\Users\User>cd
C:\Users\User

C:\Users\User>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::f9e6:ad14:cb60:b4f9%3
    Indirizzo IPv4. . . . . : 10.0.2.15
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 10.0.2.2

C:\Users\User>

```

 Windows PowerShell

```

PS C:\Users\User> cd
PS C:\Users\User> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::f9e6:ad14:cb60:b4f9%3
    Indirizzo IPv4. . . . . : 10.0.2.15
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 10.0.2.2
PS C:\Users\User>

```

Otteniamo lo stesso output.

Usiamo il comando Get-Alias dir

```

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

```

CommandType	Name	Version	Source
Alias	dir -> Get-ChildItem		

Sappiamo ora che dir esegue il comando Get-ChildItem

Eseguiamo ora netstat -h e otteniamo la lista dei comandi disponibili

```
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.
```

Con netstat -r otteniamo la tabella di routing:

```
PS C:\Users\User> netstat -r

=====
Elenco interfacce
 3...08 00 27 d3 1a 68 .....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     127.0.0.1     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     127.0.0.1     127.0.0.1    331
  224.0.0.0               240.0.0.0     10.0.2.15     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
  1      331 ::1/128      On-link
  3      281 fe80::/64    On-link
  3      281 fe80::f9e6:ad14:cb60:b4f9/128
                                On-link
  1      331 ff00::/8      On-link
  3      281 ff00::/8      On-link
=====
Route permanenti:
 Nessuna
```

Il nostro gateway è 10.0.2.2

Apriamo un secondo powershell con i privilegi da amministratore e lanciamo il comando netstat -abno

 Seleziona Amministratore: Windows PowerShell

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	956
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	5056
CDPSvc				
[svchost.exe]				
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING	4
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING	5836
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:8000	0.0.0.0:0	LISTENING	3044
[splunkd.exe]				
TCP	0.0.0.0:8089	0.0.0.0:0	LISTENING	3044
[splunkd.exe]				
TCP	0.0.0.0:8191	0.0.0.0:0	LISTENING	8036
[mongod.exe]				
TCP	0.0.0.0:9997	0.0.0.0:0	LISTENING	3044
[splunkd.exe]				
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING	716
[lsass.exe]				
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING	544
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:49666	0.0.0.0:0	LISTENING	1216
EventLog				
[svchost.exe]				
TCP	0.0.0.0:49667	0.0.0.0:0	LISTENING	1212
Schedule				
[svchost.exe]				
TCP	0.0.0.0:49668	0.0.0.0:0	LISTENING	2536
[spoolsv.exe]				
TCP	0.0.0.0:49669	0.0.0.0:0	LISTENING	692
Impossibile ottenere informazioni sulla proprietà				
TCP	0.0.0.0:49670	0.0.0.0:0	LISTENING	2768
PolicyAgent				
[svchost.exe]				
TCP	10.0.2.15:139	0.0.0.0:0	LISTENING	4
Impossibile ottenere informazioni sulla proprietà				

Otteniamo tutte le connessioni TCP attive

Ora apriamo il task manager, sotto dettagli cerchiamo il PID corrispondente al primo della nostra lista:

Connessioni attive

Proto	Indirizzo locale	Indirizzo esterno	Stato	PID
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	956
RpcSs				
[svchost.exe]				
TCP	0.0.0.0:445			
Impossibile ottenere informazioni				
TCP	0.0.0.0:5040			
CDPSvc				
[svchost.exe]				
TCP	0.0.0.0:5357			
Impossibile ottenere informazioni				
TCP	0.0.0.0:7680			
Impossibile ottenere informazioni				
TCP	0.0.0.0:8000			
[splunkd.exe]				
TCP	0.0.0.0:8089			
[splunkd.exe]				
TCP	0.0.0.0:8191			

Gestione attività

File Opzioni Visualizza


Processi Prestazioni Cronologia applicazioni Avvio Utenti Dettagli Servizi

Nome	PID	Stato	Nome utente
svchost.exe	832	In esecuzione	SYSTEM
svchost.exe	956	In esecuzione	SERVIZIO ...
svchost.exe	1000	In esecuzione	SYSTEM
svchost.exe	1064	In esecuzione	SYSTEM
svchost.exe	1140	In esecuzione	SERVIZIO L...
svchost.exe	1212	In esecuzione	SYSTEM

Tasto destro e apriamo le proprietà:

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: 54,1 KB (55.456 byte)

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

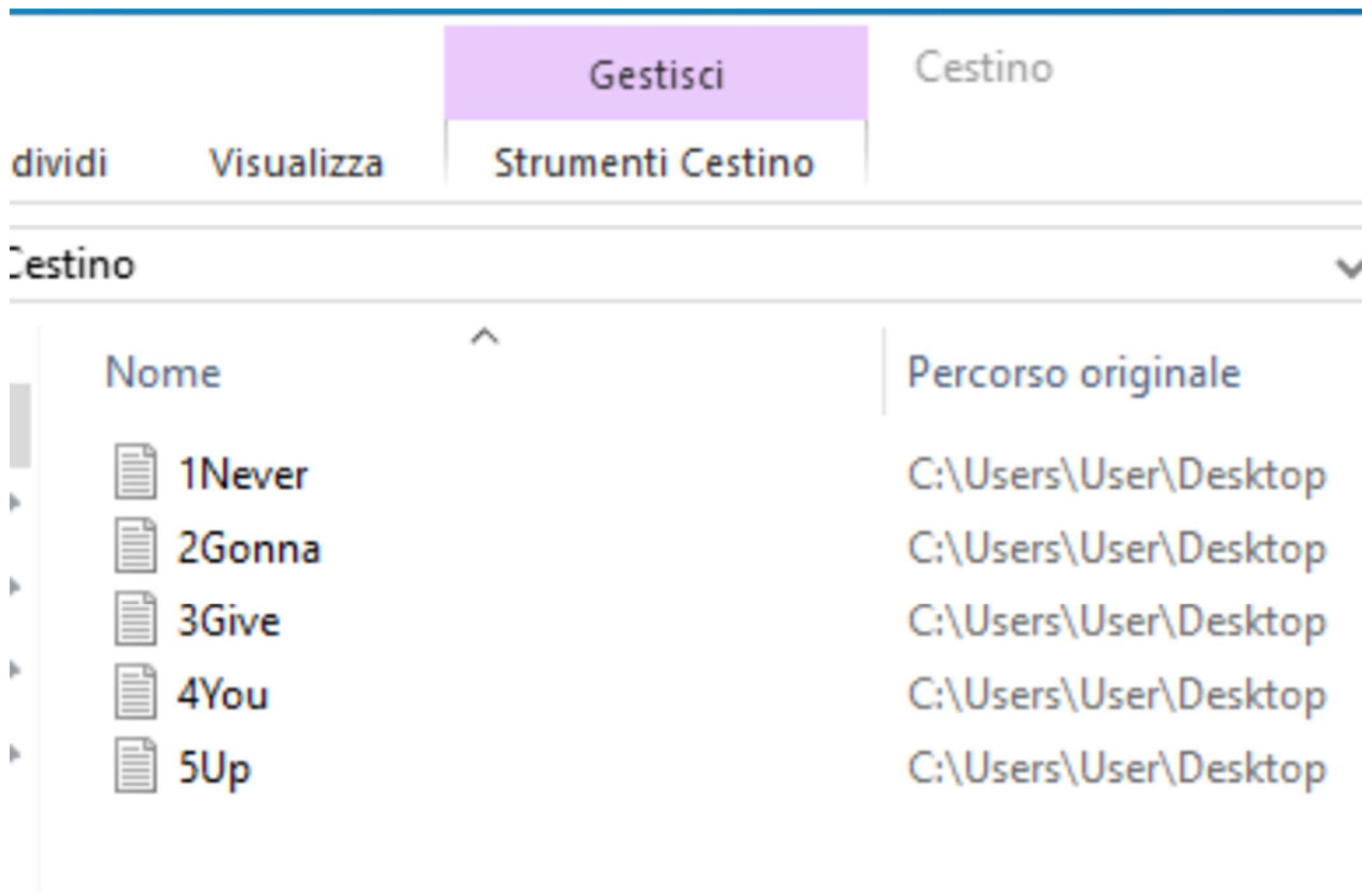
Data creazione: lunedì 4 dicembre 2023, 03:46:50

Ultima modifica: lunedì 4 dicembre 2023, 03:46:50

Ultimo accesso: Oggi 25 ottobre 2024, 30 minuti fa

Attributi: ☐ Sola lettura ☐ Nascosto

Ora inseriamo dei file nel cestino e proviamo a cancellarli con i comandi in PowerShell:



Usiamo il comando clear-recyclebin:

