

PowerShell

Dopo aver avviato sia la PowerShell che il prompt dei comandi eseguiamo i comandi “dir” e “ipconfig” in tutti e due i prompt. Come possiamo notare gli output di tutti e due i comandi sono simili.

```
Directory di C:\Users\andrw
02/12/2024 13:09 <DIR> .
01/05/2024 23:59 <DIR> ..
15/10/2024 11:44 6.48K .bash_history
30/09/2024 13:44 184 .gitconfig
21/10/2024 10:22 168 .packettracer
02/12/2024 13:09 .splunk
13/12/2024 02:43 <DIR> .VirtualBox
01/11/2024 19:12 <DIR> BrawlhallaReplays
02/10/2024 08:24 <DIR> Cisco Packet Tracer 8.0
01/05/2024 22:59 <DIR> Contacts
13/12/2024 15:38 <DIR> Desktop
08/11/2024 15:49 <DIR> Documents
02/10/2024 15:38 <DIR> Downloads
01/05/2024 22:59 <DIR> Favorites
01/05/2024 22:59 <DIR> Links
01/05/2024 22:59 <DIR> Music
01/05/2024 23:01 <DIR> OneDrive
02/10/2024 09:04 <DIR> Pictures
07/07/2024 16:41 <DIR> Saved Games
01/05/2024 23:16 <DIR> Searches
30/09/2024 22:22 <DIR> Videos
10/12/2024 15:12 <DIR> VirtualBox VMs
29/11/2024 04:07 73.72K VirtualKey.db
      4 File      80.56K byte
      19 Directory 57.25K.876.928 byte disponibili

C:\Users\andrw>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet 2:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::8dfb:4d3:7aec:5e22%5
    Indirizzo IPv4. . . . . : 192.168.56.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: station
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::65c4:8732:8b7c:5ec9%6
    Indirizzo IPv4. . . . . : 192.168.1.17
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1

C:\Users\andrw>
```

```
PS C:\Users\andrw> dir

Directory: C:\Users\andrw

Mode                LastWriteTime         Length Name
----                -
d-----          02/12/2024    13:09             .
d-----          13/12/2024    02:43             .VirtualBox
d-----          01/11/2024    19:12             BrawlhallaReplays
d-----          02/10/2024    09:24             Cisco Packet Tracer 8.0
d-----          01/05/2024    23:59             Contacts
d-----          13/12/2024    15:38             Desktop
d-----          08/11/2024    15:49             Documents
d-----          02/10/2024    15:38             Downloads
d-----          01/05/2024    23:59             Favorites
d-----          01/05/2024    23:59             Links
d-----          01/05/2024    23:59             Music
d-----          02/05/2024    09:01             OneDrive
d-----          02/10/2024    10:04             Pictures
d-----          07/07/2024    17:41             Saved Games
d-----          02/05/2024    00:16             Searches
d-----          30/09/2024    22:22             Videos
d-----          10/12/2024    15:12             VirtualBox VMs
-a-----          15/10/2024    12:44             648K .bash_history
-a-----          30/09/2024    14:44             184 .gitconfig
-a-----          21/10/2024    11:22             168 .packettracer
-a-----          29/11/2024    04:07             7372K VirtualKey.db

PS C:\Users\andrw> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet 2:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::8dfb:4d3:7aec:5e22%5
    Indirizzo IPv4. . . . . : 192.168.56.1
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . :

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: station
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::65c4:8732:8b7c:5ec9%6
    Indirizzo IPv4. . . . . : 192.168.1.17
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1
```

Per esplorare i comandi netstat eseguiamo il comando ”netstat -h” per vedere tutte le opzioni disponibili, ad esempio eseguendo il comando ”netstat -r” possiamo vedere la routing table con i routes attivi. Proviamo ad aprire PowerShell da amministratore e vediamo i protocolli TCP attivi con il comando ”netstat -abno”.

```
Amministratore: Windows PowerShell
Installa la versione più recente di PowerShell per nuove funzionalità e miglioramenti. https://aka.ms/PSWindows
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  1648
RpcSs
[svchost.exe]
TCP    0.0.0.0:445                0.0.0.0:0                  LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:3306               0.0.0.0:0                  LISTENING  6052
[mysqld.exe]
TCP    0.0.0.0:5040               0.0.0.0:0                  LISTENING  2224
CDPSvc
[svchost.exe]
TCP    0.0.0.0:7680               0.0.0.0:0                  LISTENING  1564
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:33060              0.0.0.0:0                  LISTENING  6052
[mysqld.exe]
TCP    0.0.0.0:49664              0.0.0.0:0                  LISTENING  1388
[Sistema]
TCP    0.0.0.0:49665              0.0.0.0:0                  LISTENING  1224
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:49666              0.0.0.0:0                  LISTENING  2228
Schedule
[svchost.exe]
TCP    0.0.0.0:49667              0.0.0.0:0                  LISTENING  2796
Eventlog
[svchost.exe]
TCP    0.0.0.0:49668              0.0.0.0:0                  LISTENING  4596
[spoolsv.exe]
TCP    0.0.0.0:49669              0.0.0.0:0                  LISTENING  1300
Impossibile ottenere informazioni sulla proprietà
TCP    0.0.0.0:54288              0.0.0.0:0                  LISTENING  4
Impossibile ottenere informazioni sulla proprietà
TCP    127.0.0.1:5354              0.0.0.0:0                  LISTENING  5092
[mDNSResponder.exe]
TCP    127.0.0.1:6463              0.0.0.0:0                  LISTENING  14740
[Discord.exe]
TCP    127.0.0.1:6463              127.0.0.1:53724            ESTABLISHED 14740
[Discord.exe]
TCP    127.0.0.1:9010              0.0.0.0:0                  LISTENING  15288
[lghub_agent.exe]
TCP    127.0.0.1:9010              127.0.0.1:53706            ESTABLISHED 15288
[lghub_agent.exe]
TCP    127.0.0.1:9080              0.0.0.0:0                  LISTENING  15288
[lghub_agent.exe]
TCP    127.0.0.1:9100              0.0.0.0:0                  LISTENING  2716
[lghub_updater.exe]
TCP    127.0.0.1:9100              127.0.0.1:53707            ESTABLISHED 2716
[lghub_updater.exe]
```

Possiamo usare la PowerShell anche per eseguire delle azioni sul pc, ad esempio svuotare il cestino.

```
PS C:\Users\andrm> 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:\Users\andrm> |
```