

UTILIZZO DI WINDOWS POWERSHELL

Obiettivi

l'obiettivo di questo report è quello di spiegare le basi dell'utilizzo di Windows PowerShell. L'esercizio si divide in 5 parti seguentemente elencate:

1. Accedere alla console di PowerShell
2. Esplorare i comandi di Prompt e di PowerShell
3. Esplorare cmdlets
4. Esplorare il comando netstat attraverso PowerShell
5. Svuotare il cestino attraverso l'utilizzo di PowerShell

1 - Accedere alla console di PowerShell e Prompt

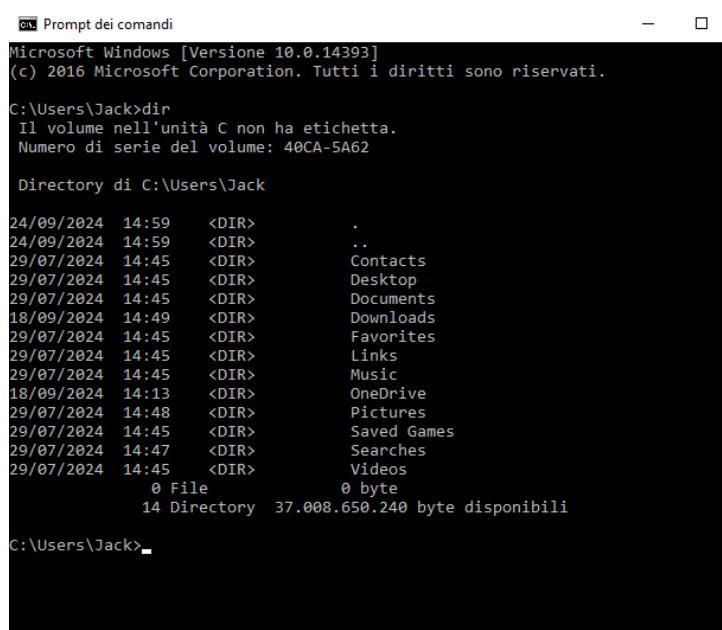
Per accedere alla console di PowerShell basta premere il tasto per il menù di Windows (o Start) e cercare nella barra di ricerca "PowerShell".

Analogamente per aprire il prompt dei comandi basta aprire il menù Windows e cercare "prompt dei comandi"

2 - Esplorare i comandi Prompt e i comandi Powershell

Proviamo con il comando "dir", questa è la risposta nelle due schermate:

Prompt dei comandi:



```
cs Prompt dei comandi
Microsoft Windows [Versione 10.0.14393]
(c) 2016 Microsoft Corporation. Tutti i diritti sono riservati.

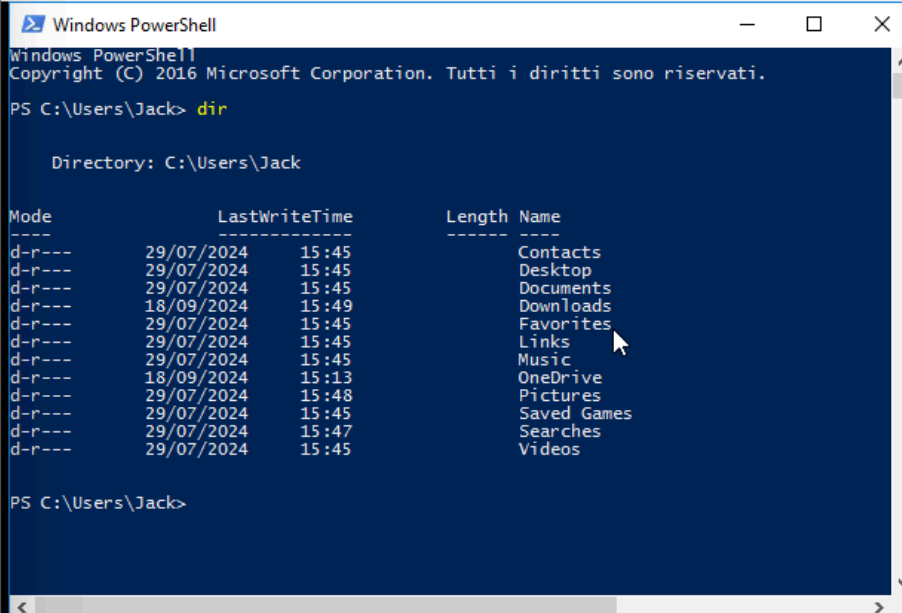
C:\Users\Jack>dir
Il volume nell'unità C non ha etichetta.
Numero di serie del volume: 40CA-5A62

Directory di C:\Users\Jack

24/09/2024 14:59 <DIR>      .
24/09/2024 14:59 <DIR>      ..
29/07/2024 14:45 <DIR>      Contacts
29/07/2024 14:45 <DIR>      Desktop
29/07/2024 14:45 <DIR>      Documents
18/09/2024 14:49 <DIR>      Downloads
29/07/2024 14:45 <DIR>      Favorites
29/07/2024 14:45 <DIR>      Links
29/07/2024 14:45 <DIR>      Music
18/09/2024 14:13 <DIR>      OneDrive
29/07/2024 14:48 <DIR>      Pictures
29/07/2024 14:45 <DIR>      Saved Games
29/07/2024 14:47 <DIR>      Searches
29/07/2024 14:45 <DIR>      Videos
                0 File             0 byte
                14 Directory  37.008.650.240 byte disponibili

C:\Users\Jack>
```

Windows PowerShell:



```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Tutti i diritti sono riservati.

PS C:\Users\Jack> dir

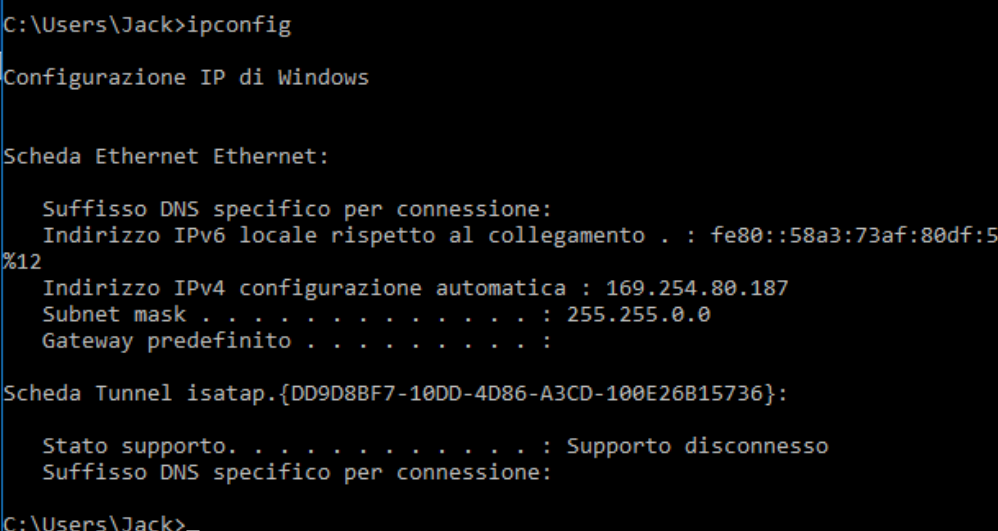
Directory: C:\Users\Jack

Mode                LastWriteTime         Length Name
----                -
d-r---          29/07/2024   15:45             Contacts
d-r---          29/07/2024   15:45             Desktop
d-r---          29/07/2024   15:45             Documents
d-r---          18/09/2024   15:49             Downloads
d-r---          29/07/2024   15:45             Favorites
d-r---          29/07/2024   15:45             Links
d-r---          29/07/2024   15:45             Music
d-r---          18/09/2024   15:13             OneDrive
d-r---          29/07/2024   15:48             Pictures
d-r---          29/07/2024   15:45             Saved Games
d-r---          29/07/2024   15:47             Searches
d-r---          29/07/2024   15:45             Videos

PS C:\Users\Jack>
```

Come visto ci sono lievissime differenze nelle due schermate. Proviamo adesso con un altro comando, come ad esempio “**ipconfig**”:

Prompt dei Comandi:



```
C:\Users\Jack>ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:


    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::58a3:73af:80df:5%12
    Indirizzo IPv4 configurazione automatica : 169.254.80.187
    Subnet mask . . . . . : 255.255.0.0
    Gateway predefinito . . . . . :

Scheda Tunnel isatap.{DD9D8BF7-10DD-4D86-A3CD-100E26B15736}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

C:\Users\Jack>
```

Windows Powershell:



```
PS C:\Users\Jack> ipconfig

Configurazione IP di Windows

Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione:
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::58a3:73af:80df:50bb%12
    Indirizzo IPv4 configurazione automatica : 169.254.80.187
    Subnet mask . . . . . : 255.255.0.0
    Gateway predefinito . . . . . :

Scheda Tunnel isatap.{DD9D8BF7-10DD-4D86-A3CD-100E26B15736}:

    Stato supporto. . . . . : Supporto disconnesso
    Suffisso DNS specifico per connessione:

PS C:\Users\Jack>
```

Come è possibile notare, entrambe le schermate presentano un aspetto molto simile tra di loro.

3 - Esplorare cmdlets

I comandi di PowerShell, chiamati cmdlets, sono costruiti in modo da avere un aspetto del tipo *verbo-sostantivo*. Ad esempio il cmdlet del tipo *Get-Command* incluso in PowerShell viene usato per ottenere tutti i cmdlet registrati nella shell dei comandi. Il verbo identifica l'azione eseguita dal cmdlet e il sostantivo identifica la risorsa in cui il cmdlet esegue l'azione. Andiamo a provare il comando “**Get-Alias** dir” e vediamo che succede:

```
PS C:\Users\Jack> Get-Alias dir

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

4 - Esplorare il comando netstat usando PowerShell

Come detto, proviamo a vedere il comando “**netstat -h**”, in modo da vedere un ventaglio di opzioni che possiamo utilizzare con questo comando:

```
PS C:\Users\Jack> netstat -h

Visualizza statistiche relative ai protocolli e alle
connessioni di rete TCP/IP correnti.

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

-a          Visualizza tutte le connessioni e le porte di ascolto.
-b          Visualizza il file eseguibile utilizzato per la creazione
           di ogni connessione o porta di ascolto. Alcuni file
           eseguibili conosciuti includono più componenti indipendenti.
           In tali casi viene visualizzata la sequenza dei componenti
           utilizzati per la creazione della connessione o porta di
           ascolto e il nome del file eseguibile viene visualizzato
           in fondo, tra parentesi quadre ([]). Nella parte superiore
           è indicato il componente chiamato e così via, fino al
           raggiungimento di TCP/IP. Se si utilizza questa opzione,
           l'esecuzione del comando può richiedere molto tempo e
           riuscirà solo se si dispone di autorizzazioni sufficienti.
-e          Visualizza le statistiche Ethernet. Può essere utilizzata
           insieme all'opzione -s.
-f          Visualizza i nomi di dominio completi (FQDN, Fully Qualified
           Domain Name) per gli indirizzi esterni.
-n          Visualizza indirizzi e numeri di porta in forma numerica.
-o          Visualizza l'ID del processo proprietario associato a ogni
           connessione.
-p proto    Visualizza le connessioni relative al protocollo specificato
           da "proto", che può essere TCP, UDP, TCPv6 o UDPv6.
           Se utilizzato insieme all'opzione -s per le statistiche per
           protocollo, "proto" può essere: IP, IPv6, ICMP, ICMPv6, TCP,
           TCPv6, UDP o UDPv6.
-q          Visualizza tutte le connessioni, le porte di ascolto e le porte
           TCP non di ascolto associate. Le porte non di ascolto associate
           possono essere associate o meno a una connessione attiva.
-r          Visualizza la tabella di routing.
-s          Visualizza le statistiche per protocollo. Per impostazione
           predefinita, vengono visualizzate le statistiche per IP,
           IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP e UDPv6. Per specificare
           un sottoinsieme dei valori predefiniti, è possibile
           utilizzare l'opzione -p.
-t          Visualizza lo stato di offload della connessione corrente.
-x          Visualizza le connessioni, i listener e gli endpoint
           condivisi.
-y          Visualizza il modello di connessione TCP per tutte le
           connessioni. Non può essere utilizzata in combinazione con le
           altre opzioni.
interval   Ripete la visualizzazione delle statistiche selezionate,
           con una pausa di un numero di secondi pari a "interval"
           dopo ogni visualizzazione. Per interrompere la ripetizione
           della visualizzazione delle statistiche, premere CTRL+C.
           Se questa opzione viene omessa, le informazioni di
           configurazione correnti verranno visualizzate una volta sola.
```

Come possibile notare, ci sono veramente tante opzioni. Tra queste ne scegliamo una da eseguire, come ad esempio “**netstat -r**”, che come leggiamo “visualizza la tabella di routing”:

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

=====
Elenco interfacce
12...08 00 27 34 65 71 .....Intel(R) PRO/1000 MT Desktop Adapter
1 .....Software Loopback Interface 1
17...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
=====

IPv4 Tabella route
=====
Route attive:
  Indirizzo rete      Mask      Gateway      Interfaccia Metrica
  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
  169.254.0.0         255.255.0.0 On-link      169.254.80.187 281
  169.254.80.187      255.255.255.255 On-link      169.254.80.187 281
  169.254.255.255     255.255.255.255 On-link      169.254.80.187 281
  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      169.254.80.187 281
  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      169.254.80.187 281
=====
Route permanenti:
  Nessuna

IPv6 Tabella route
=====
Route attive:
  Interf Metrica Rete Destinazione      Gateway
  1      331  ::1/128      On-link
  12     281  fe80::/64     On-link
  12     281  fe80::58a3:73af:80df:50bb/128 On-link
  1      331  ff00::/8     On-link
  12     281  ff00::/8     On-link
=====
Route permanenti:
  Nessuna
PS C:\Users\Jack>
```

5 - Svuotare il cestino con PowerShell

I comandi in PowerShell possono anche aiutare molto nella gestione di grandi reti di computer.

Possono infatti semplificare operazioni che di norma richiederebbero un grandissimo numero di passaggi riducendole a pochi comandi.

Possono anche compiere operazioni come svuotare il cestino, e lo faremo utilizzando il comando “**clear-recyclebin**”. Il sistema ci chiederà se vogliamo definitivamente eliminare i files ed una volta inviato il comando “S”, il cestino sarà definitivamente svuotato.

```
PS C:\Users\Jack> 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\Jack>
```