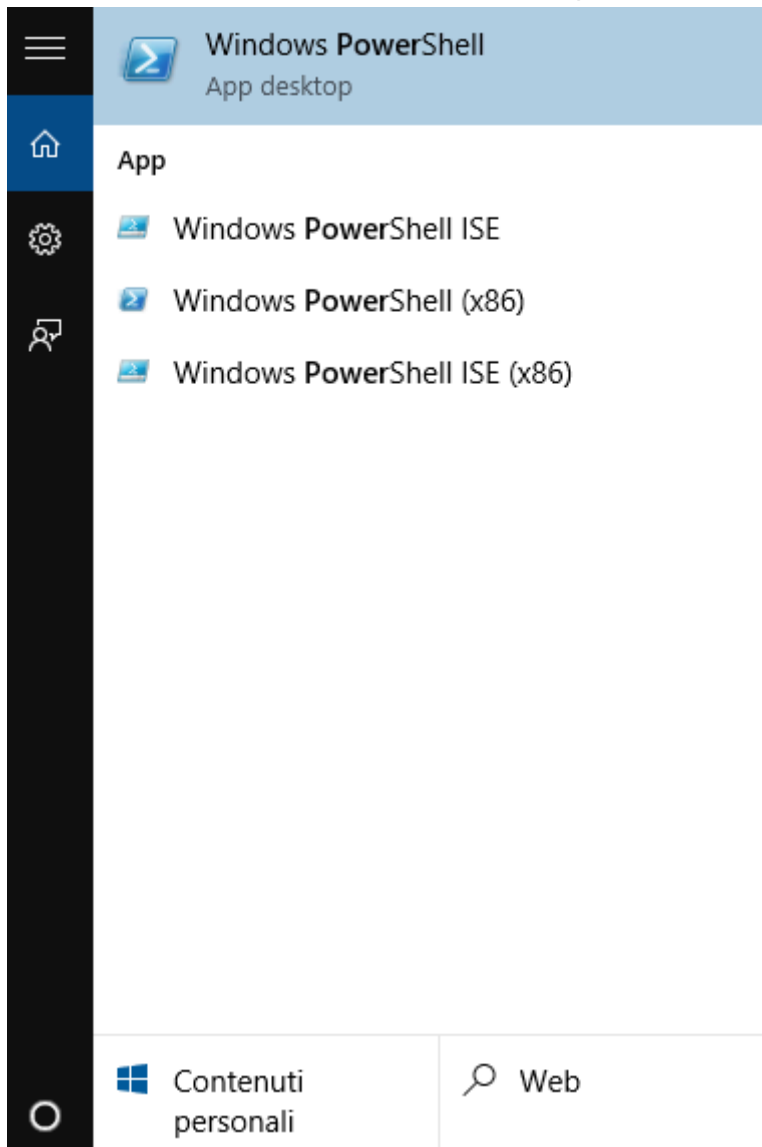


Esplorazione di PowerShell

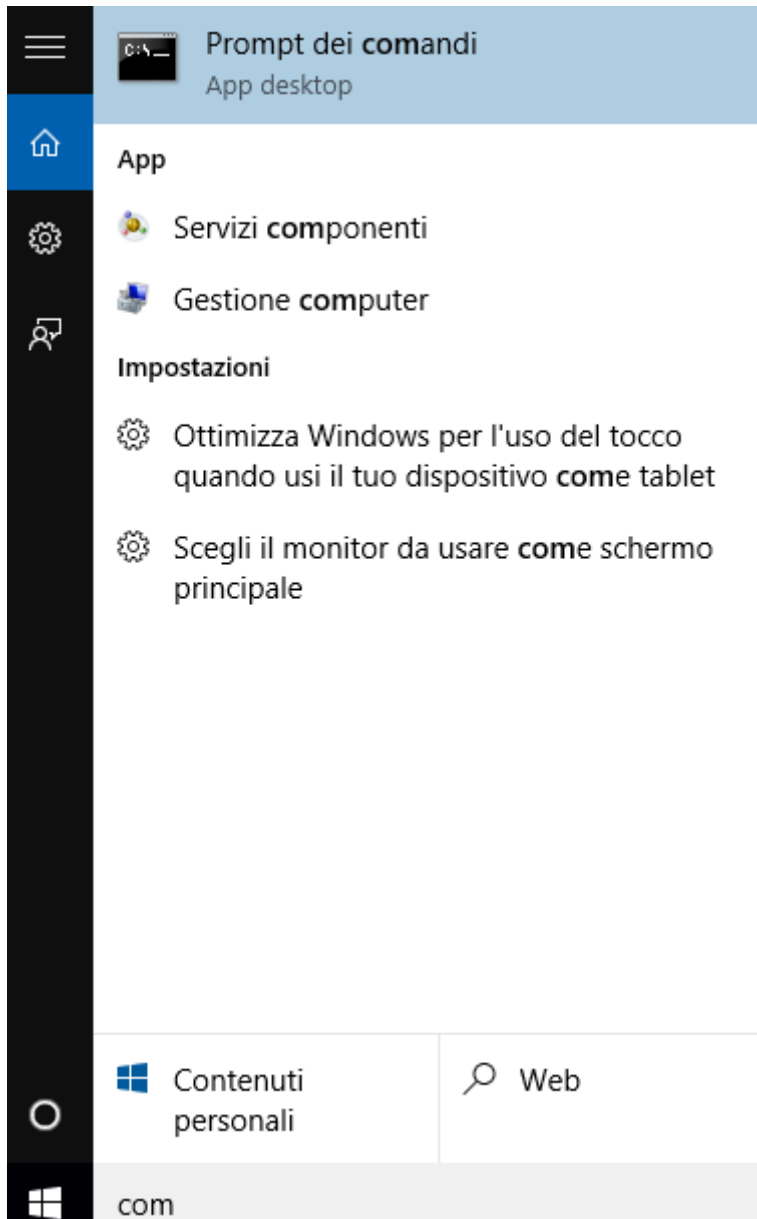
Esplorazione di PowerShell

Parte 1: Accesso alla Console di PowerShell

- Ho cliccato su Start e cercato **PowerShell** per avviare la console.



- Ho cliccato su Start e cercato **Command Prompt** per aprire il prompt dei comandi.



Parte 2: Esplorazione dei Comandi del Prompt dei Comandi e di PowerShell

1. Ho eseguito il comando `dir` in entrambe le console.
 - Entrambe hanno restituito un elenco di file e sottodirectory con informazioni come tipo, dimensione, data e ora dell'ultima modifica.

- In PowerShell, sono mostrati anche gli attributi/modi dei file.

2. Ho provato altri comandi comuni del prompt dei comandi, `cd` e `ipconfig`.

- I risultati sono stati simili in entrambe le console.

Parte 3: Esplorazione dei Cmdlet

1. Ho verificato quale cmdlet PowerShell corrisponda al comando dir digitando:

```
Get-Alias dir
```

- Il risultato ha mostrato che `dir` è un alias per `Get-ChildItem`.

2. Ho cercato online ulteriori informazioni sui cmdlet di PowerShell.

```
PS C:\Users\user> Get-Command
```

CommandType	Name	Version	Source
Alias	Add-ProvisionedAppxPackage	3.0	Dism
Alias	Apply-WindowsUnattend	3.0	Dism
Alias	Begin-WebCommitDelay	1.0.0.0	WebAdministration
Alias	Disable-PhysicalDiskIndication	2.0.0.0	Storage
Alias	Disable-StorageDiagnosticLog	2.0.0.0	Storage
Alias	Enable-PhysicalDiskIndication	2.0.0.0	Storage
Alias	Enable-StorageDiagnosticLog	2.0.0.0	Storage
Alias	End-WebCommitDelay	1.0.0.0	WebAdministration
Alias	Flush-Volume	2.0.0.0	Storage
Alias	Get-DiskSNV	2.0.0.0	Storage
Alias	Get-PhysicalDiskSNV	2.0.0.0	Storage
Alias	Get-ProvisionedAppxPackage	3.0	Dism
Alias	Get-StorageEnclosureSNV	2.0.0.0	Storage
Alias	Initialize-Volume	2.0.0.0	Storage
Alias	Move-SmbClient	2.0.0.0	SmbWitness
Alias	Remove-ProvisionedAppxPackage	3.0	Dism
Alias	Write-FileSystemCache	2.0.0.0	Storage
Function	A:		
Function	Add-BCDataCacheExtension	1.0.0.0	BranchCache
Function	Add-BitLockerKeyProtector	1.0.0.0	BitLocker
Function	Add-DnsClientNrptRule	1.0.0.0	DnsClient
Function	Add-DtcClusterTMMapping	1.0.0.0	MsDtc
Function	Add-EtwTraceProvider	1.0.0.0	EventTracingManagement
Function	Add-InitiatorIdToMaskingSet	2.0.0.0	Storage
Function	Add-MpPreference	1.0	Defender
Function	Add-NetEventNetworkAdapter	1.0.0.0	NetEventPacketCapture
Function	Add-NetEventPacketCaptureProvider	1.0.0.0	NetEventPacketCapture
Function	Add-NetEventProvider	1.0.0.0	NetEventPacketCapture
Function	Add-NetEventVmNetworkAdapter	1.0.0.0	NetEventPacketCapture
Function	Add-NetEventVmSwitch	1.0.0.0	NetEventPacketCapture
Function	Add-NetEventWFPCaptureProvider	1.0.0.0	NetEventPacketCapture
Function	Add-NetIPHttpsCertBinding	1.0.0.0	NetworkTransition
Function	Add-NetLbfoTeamMember	2.0.0.0	NetLbfo
Function	Add-NetLbfoTeamNic	2.0.0.0	NetLbfo
Function	Add-NetNatExternalAddress	1.0.0.0	NetNat
Function	Add-NetNatStaticMapping	1.0.0.0	NetNat
Function	Add-NetSwitchTeamMember	1.0.0.0	NetSwitchTeam
Function	Add-OdbcDsn	1.0.0.0	Wdac
Function	Add-PartitionAccessPath	2.0.0.0	Storage
Function	Add-PhysicalDisk	2.0.0.0	Storage

Comando che mostra tutti i comandi della PowerShell

3. Ho chiuso la finestra del Prompt dei Comandi.

Parte 4: Esplorazione del Comando `netstat` in PowerShell

1. Ho eseguito `netstat -h` per visualizzare le opzioni disponibili.

```
PS C:\Users\user> 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.

2. Ho eseguito `netstat -r` per visualizzare la tabella di routing attiva.

```

PS C:\Users\user> netstat -r
=====
Elenco interfacce
3...08 00 27 46 eb bf .....Intel(R) PRO/1000 MT Desktop Adapter
1.....Software Loopback Interface 1
5...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
4...00 00 00 00 00 00 00 e0 Microsoft Teredo Tunneling Adapter
=====

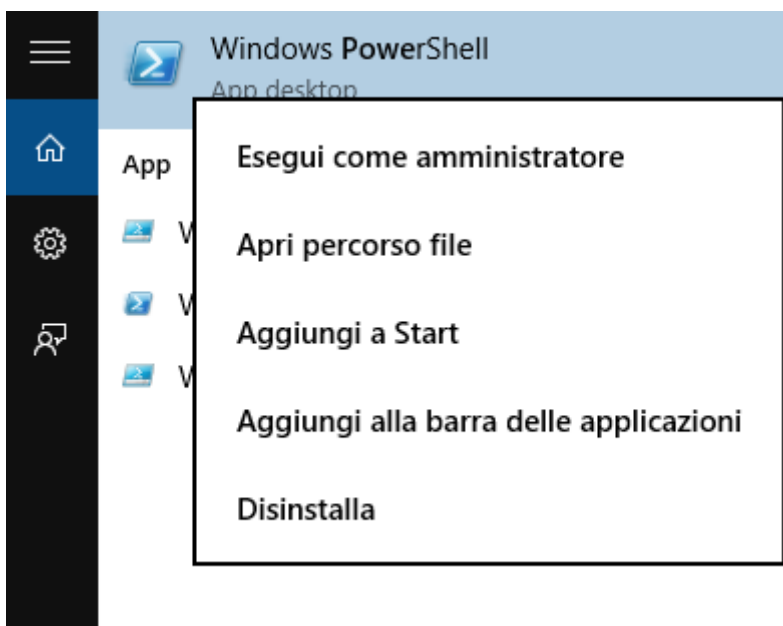
IPv4 Tabella route
=====
Route attive:
  Indirizzo rete      Mask      Gateway      Interfaccia Metrica
  0.0.0.0             0.0.0.0    10.0.2.2     10.0.2.15    10
  10.0.2.0            255.255.255.0 On-link      10.0.2.15    266
  10.0.2.15           255.255.255.255 On-link      10.0.2.15    266
  10.0.2.255          255.255.255.255 On-link      10.0.2.15    266
  127.0.0.0           255.0.0.0   On-link      127.0.0.1    306
  127.0.0.1           255.255.255.255 On-link      127.0.0.1    306
  127.255.255.255     255.255.255.255 On-link      127.0.0.1    306
  224.0.0.0           240.0.0.0   On-link      127.0.0.1    306
  224.0.0.0           240.0.0.0   On-link      10.0.2.15    266
  255.255.255.255     255.255.255.255 On-link      127.0.0.1    306
  255.255.255.255     255.255.255.255 On-link      10.0.2.15    266
=====

Route permanenti:
Nessuna

IPv6 Tabella route
=====
Route attive:
  Interf Metrica Rete Destinazione Gateway
  3 266 ::/0 fe80::2
  1 306 ::1/128 On-link
  4 306 2001::/32 On-link
  4 306 2001:0:2851:782c:2c6d:354c:b0ce:1545/128 On-link
  3 266 fd00::/64 On-link
  3 266 fd00::59c9:ffd0:48:462c/128 On-link
  3 266 fd00::e56c:42cd:32d0:24a5/128 On-link
  3 266 fe80::/64 On-link
  4 306 fe80::/64 On-link
  4 306 fe80::2c6d:354c:b0ce:1545/128 On-link
  3 266 fe80::59c9:ffd0:48:462c/128 On-link
  1 306 ff00::/8 On-link
  3 266 ff00::/8 On-link
  4 306 ff00::/8 On-link
=====

```

3. Ho aperto una seconda istanza di PowerShell con privilegi elevati (Esegui come amministratore).



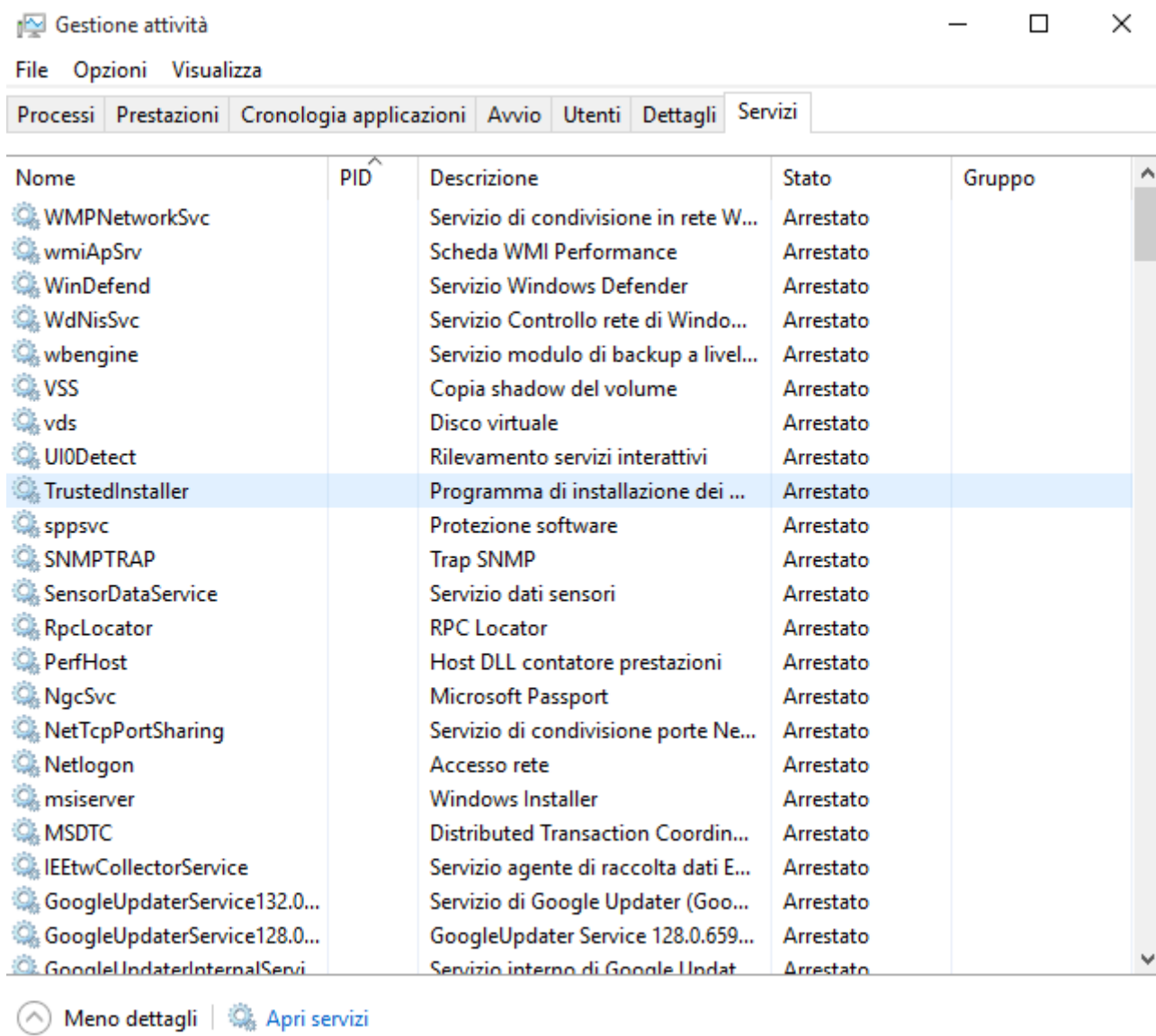
4. Ho eseguito `netstat -abno` per visualizzare le connessioni TCP attive e i processi associati.

```
PS C:\Users\user> netstat -abno

Connessioni attive

Proto Indirizzo locale Indirizzo esterno Stato PID
TCP 0.0.0.0:7 0.0.0.0:0 LISTENING 2840
```

5. Ho aperto il Task Manager, ordinato i processi per PID, e identificato un processo specifico.



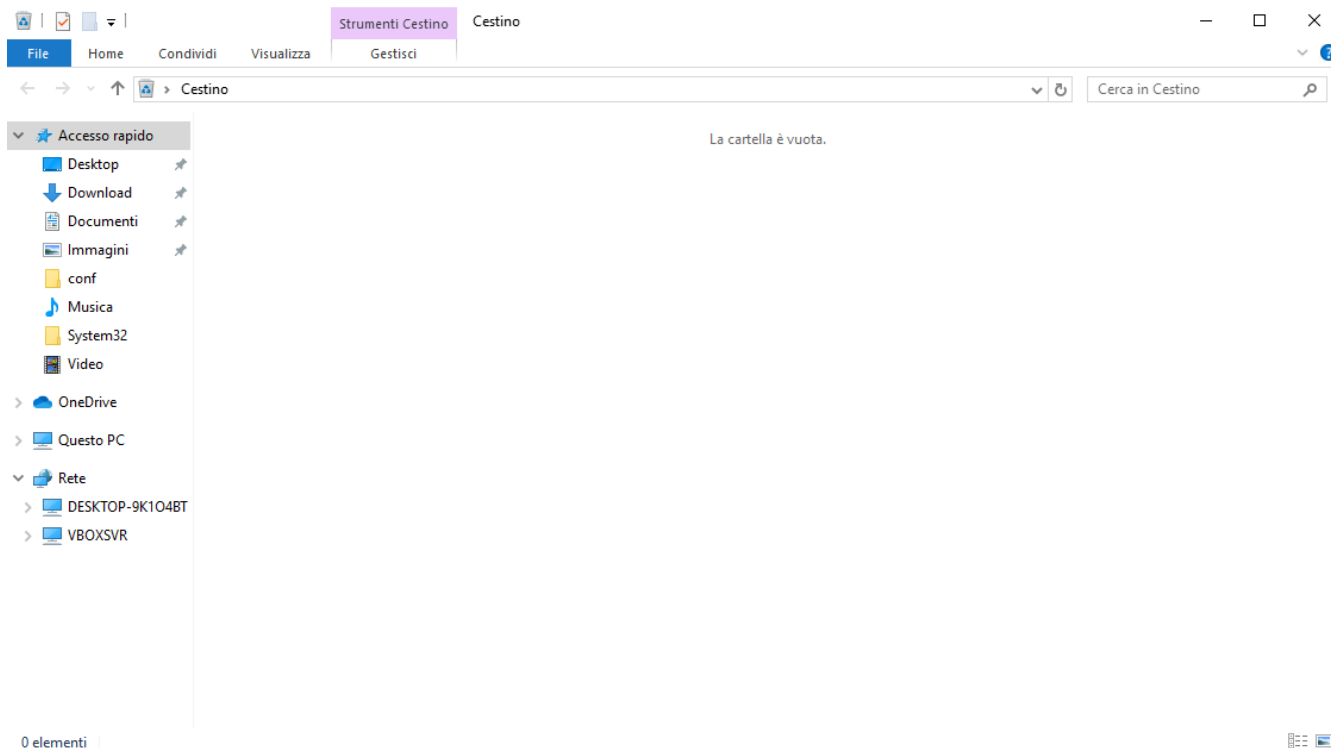
6. Ho fatto clic con il tasto destro sul processo e aperto la finestra Proprietà per ulteriori dettagli.

TCPSVCS.EXE	2840	In esecuzione	SERVIZIO L...	00	228 K	TCP/IP Services App...
tomcat7.exe	3040	In esecuzione	SYSTEM	00	64.044 K	Commons Daemon ...
unsecapp.exe	1924	In esecuzione	SYSTEM	00	480 K	Sink to receive asyn...
VBoxService.exe	240	In esecuzione	SYSTEM	00	772 K	VirtualBox Guest Ad...
VBoxTray.exe	3788	In esecuzione	user	00	720 K	VirtualBox Guest Ad...
wininit.exe	428	In esecuzione	SYSTEM	00	256 K	Applicazione di avvi...
winlogon.exe	504	In esecuzione	SYSTEM	00	396 K	Applicazione Access...

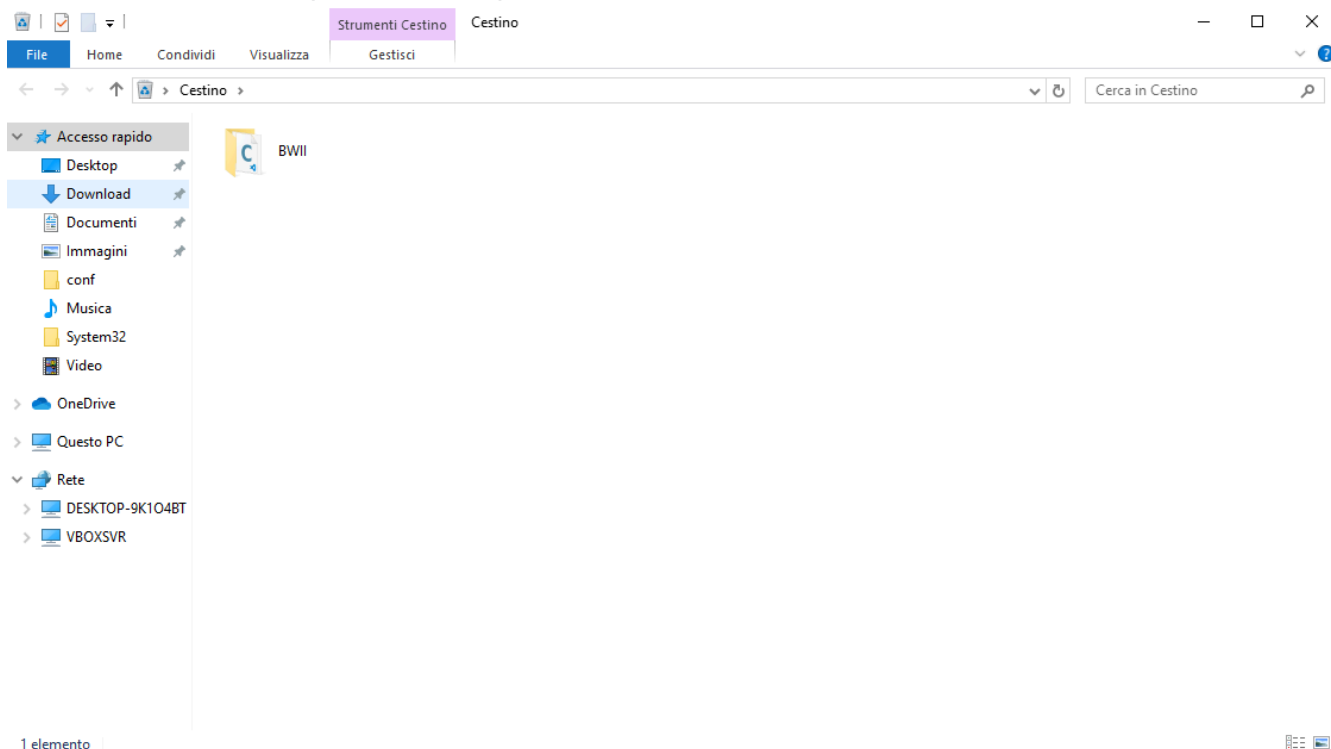
- Il processo con PID 3040 era tomcat7.exe.

Parte 5: Svuotamento del Cestino con PowerShell

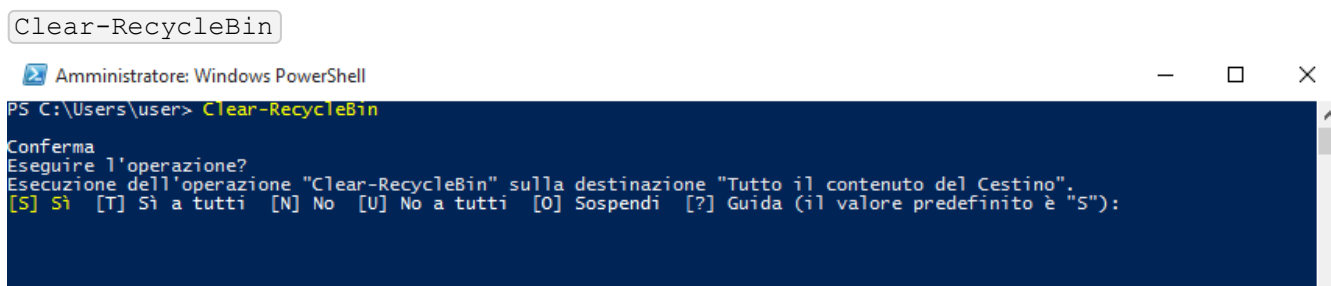
1. Ho aperto il Cestino per verificare la presenza di file eliminabili.



2. Ho creato alcuni file di prova e li ho spostati nel Cestino.



3. Ho eseguito il comando:



- Ho confermato l'operazione digitando **S**.

```
PS C:\Users\user> 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_
```

- Tutti i file nel Cestino sono stati eliminati definitivamente.

