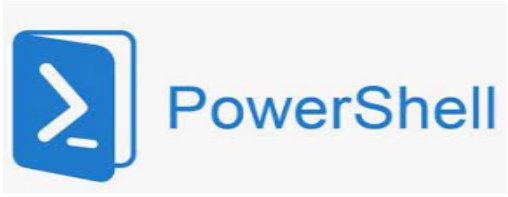

Full credit is given to the above companies including the OS that this PDF file was generated!

PowerShell Get-Help on command 'Add-NetEventVFPProvider'

PS C:\Users\wahid> Get-Help Add-NetEventVFPProvider

NAME

Add-NetEventVFPProvider

SYNOPSIS

Creates a VFP provider for network events.

SYNTAX

Add-NetEventVFPProvider [-SessionName] <String> [[-Level] <Byte>]

[[-DestinationIPAddresses] <String[]>] [[-IPProtocols] <Byte[]>] [[-TCPPorts]

<UInt16[]>] [[-UDPPorts] <UInt16[]>] [[-VFPFlowDirection] <UInt32>]

[[-SwitchName] <String>] [[-PortIds] <UInt32[]>] [[-MatchAnyKeyword] <UInt64>]

[[-MatchAllKeywords] <UInt64>] [[-DestinationMACAddresses] <String[]>]

[[-SourceMACAddresses] <String[]>] [[-VLANIds] <UInt16[]>] [[-TenantIds]

<UInt32[]>] [[-GREKeys] <UInt32[]>] [[-SourceIPAddresses] <String[]>] [-AsJob]

[-CimSession <CimSession[]>] [-ThrottleLimit <Int32>] [-Confirm] [-WhatIf]

[<CommonParameters>]

DESCRIPTION

The Add-NetEventVFPProvider cmdlet creates a Virtual Filtering Platform (VFP)

provider for network events.

PARAMETERS

-AsJob [<SwitchParameter>]

Runs the cmdlet as a background job. Use this parameter to run commands that take a long time to complete.

-CimSession <CimSession[]>

Runs the cmdlet in a remote session or on a remote computer. Enter a computer name or a session object, such as the output of a New-CimSession (https://go.microsoft.com/fwlink/p/?LinkId=227967) or [Get-CimSession](https://go.microsoft.com/fwlink/p/?LinkId=227966)cmdlet. The default is the current session on the local computer.

-DestinationIPAddresses <String[]>

Specifies destination IP addresses.

-DestinationMACAddresses <String[]>

Specifies destination MAC addresses.

-GREKeys <UInt32[]>

Specifies Generic Routing Encapsulation (GRE) keys.

-IPProtocols <Byte[]>

Specifies an array of one or more IP protocols, such as TCP or UDP, on which to filter. The packet capture provider logs network traffic that matches this filter.

-Level <Byte>

Specifies the level of Event Tracing for Windows (ETW) events for the provider. Use the level of detail for the event to filter the events that are logged. The default value for this parameter is 0x4. The acceptable

values for this parameter are:

- 0x5. Verbose - 0x4. Informational - 0x3. Warning - 0x2. Error - 0x1. Critical - 0x0. LogAlways

The provider must log the event if the value of the event is less than or equal to the value of this parameter.

-MatchAllKeywords <UInt64>

Specifies a bitmask that restricts the events that the provider logs.

-MatchAnyKeyword <UInt64>

Specifies keywords as a set of hexadecimal values. Keywords are flags that you can combine to generate values. Use a set of hexadecimal values of the keywords instead of the keyword names, and apply a filter to write ETW events for keyword matches.

-PortIds <UInt32[]>

Specifies port numbers.

-SessionName <String>

Specifies the name of the session that is associated with the NetEventVFPProvider . This parameter has the same value as the Name parameter for the New-NetEventSession cmdlet.

-SourceIPAddresses <String[]>

Specifies source IP addresses.

-SourceMACAddresses <String[]>

Specifies source MAC addresses.

-SwitchName <String>

Specifies the switch for this VFW provider.

-TCPPorts <UInt16[]>

Specifies an array of TCP ports. The provider filters and logs network traffic that matches the ports that this parameter specifies. The provider joins multiple port numbers with logical OR.

-TenantIds <UInt32[]>

Specifies tenant IDs.

-ThrottleLimit <Int32>

Specifies the maximum number of concurrent operations that can be established to run the cmdlet. If this parameter is omitted or a value of `0` is entered, then Windows PowerShellr calculates an optimum throttle limit for the cmdlet based on the number of CIM cmdlets that are running on the computer. The throttle limit applies only to the current cmdlet, not to the session or to the computer.

-UDPPorts <UInt16[]>

Specifies an array of UDP ports. The provider filters for and logs network traffic that matches the ports that this parameter specifies. The provider joins multiple port numbers with logical ORs.

-VFPFlowDirection <UInt32>

Specifies the WFP flow direction.

-VLANIds <UInt16[]>

Specifies virtual local area network IDs.

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

-WhatIf [<SwitchParameter>]

Shows what would happen if the cmdlet runs. The cmdlet is not run.

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug,

ErrorAction, ErrorVariable, WarningAction, WarningVariable,

OutBuffer, PipelineVariable, and OutVariable. For more information, see

about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

---------- Example 1: Add a VFP provider ----------

```
New-NetEventSession -Name "Session01"
Add-NetEventVFPProvider -SessionName "Session01"
```

This example adds a VFP provider.

The first command creates a network event session named `Session01` by using

the New-NetEventSession cmdlet.

The second command creates a VFP provider for the specified session.

REMARKS

To see the examples, type: "get-help Add-NetEventVFPProvider -examples".

For more information, type: "get-help Add-NetEventVFPProvider -detailed".

For technical information, type: "get-help Add-NetEventVFPProvider -full".

For online help, type: "get-help Add-NetEventVFPProvider -online"