



python



PowerShell

FPDF Library
PDF generator

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

PowerShell Get-Help on command 'Set-NetEventVFPPProvider'

PS C:\Users\wahid> Get-Help Set-NetEventVFPPProvider

NAME

Set-NetEventVFPPProvider

SYNOPSIS

Modifies a VFP provider for network events.

SYNTAX

```
Set-NetEventVFPPProvider [[-Level] <Byte>] [[-MatchAnyKeyword] <UInt64>]
[[-MatchAllKeyword] <UInt64>] [[-DestinationMACAddresses] <String[]>]
[[-SourceMACAddresses] <String[]>] [[-VLANIds] <UInt16[]>] [[-TenantIds]
<UInt32[]>] [[-GREKeys] <UInt32[]>] [[-SourceIPAddresses] <String[]>]
[[-DestinationIPAddresses] <String[]>] [[-IPProtocols] <Byte[]>] [[-TCPPorts]
<UInt16[]>] [[-UDPPorts] <UInt16[]>] [[-VFPFlowDirection] {Inbound | Outbound
| InboundAndOutbound}] [[-SwitchName] <String>] [[-PortIds] <UInt32[]>]
[-AsJob] [-AssociatedEventSession <CimInstance>] [-CimSession <CimSession[]>]
[-PassThru] [-ThrottleLimit <Int32>] [-Confirm] [-WhatIf] [<CommonParameters>]
```

```
Set-NetEventVFPPProvider [[-Level] <Byte>] [[-MatchAnyKeyword] <UInt64>]
[[-MatchAllKeyword] <UInt64>] [[-DestinationMACAddresses] <String[]>]
[[-SourceMACAddresses] <String[]>] [[-VLANIds] <UInt16[]>] [[-TenantIds]
```

```
<UInt32[]> [[-GREKeys] <UInt32[]>] [[-SourceIPAddresses] <String[]>]
[[ -DestinationIPAddresses] <String[]>] [[-IPProtocols] <Byte[]>] [[-TCPPorts]
<UInt16[]>] [[-UDPPorts] <UInt16[]>] [[-VFPFlowDirection] {Inbound | Outbound
| InboundAndOutbound}] [[-SwitchName] <String>] [[-PortIds] <UInt32[]>]
[-AsJob] [-CimSession <CimSession[]>] -InputObject <CimInstance[]> [-PassThru]
[-ThrottleLimit <Int32>] [-Confirm] [-WhatIf] [<CommonParameters>]
```

```
Set-NetEventVFPPProvider [[-SessionName] <String[]>] [[-Level] <Byte>]
[[ -MatchAnyKeyword] <UInt64>] [[-MatchAllKeyword] <UInt64>]
[[ -DestinationMACAddresses] <String[]>] [[-SourceMACAddresses] <String[]>]
[[ -VLANIds] <UInt16[]>] [[-TenantIds] <UInt32[]>] [[-GREKeys] <UInt32[]>]
[[ -SourceIPAddresses] <String[]>] [[-DestinationIPAddresses] <String[]>]
[[ -IPProtocols] <Byte[]>] [[-TCPPorts] <UInt16[]>] [[-UDPPorts] <UInt16[]>]
[[ -VFPFlowDirection] {Inbound | Outbound | InboundAndOutbound}] [[-SwitchName]
<String>] [[-PortIds] <UInt32[]>] [-AsJob] [-CimSession <CimSession[]>]
[-PassThru] [-ThrottleLimit <Int32>] [-Confirm] [-WhatIf] [<CommonParameters>]
```

DESCRIPTION

The Set-NetEventVFPPProvider cmdlet modifies 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.

-AssociatedEventSession <CimInstance>

Specifies the associated network event session, as a CIM object. To obtain the network event session, use the Get-NetEventSession cmdlet.

-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.

`-InputObject <CimInstance[]>`

Specifies the input object that is used in a pipeline command.

`-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.

`-MatchAllKeyword <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.

`-PassThru [<SwitchParameter>]`

Returns an object representing the item with which you are working. By default, this cmdlet does not generate any output.

`-PortIds <UInt32[]>`

Specifies port numbers.

`-SessionName <String[]>`

Specifies the name of the session that is associated with the `NetEventVFPPProvider`. 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 PowerShell 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 <VFPFlowDirection>

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

----- Example 1: Modify a VFP provider -----

```
New-NetEventSession -Name "Session01"  
Add-NetEventVFPPProvider -SessionName "Session01"  
Set-NetEventVFPPProvider -SessionName "Session01" -SourceIPAddresses  
182.168.0.1 -IPProtocols 6
```

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.

The third command modifies the VFP provider with the specified source IP address and IP protocol.

REMARKS

To see the examples, type: "get-help Set-NetEventVFPPProvider -examples".

For more information, type: "get-help Set-NetEventVFPPProvider -detailed".

For technical information, type: "get-help Set-NetEventVFPPProvider -full".

For online help, type: "get-help Set-NetEventVFPPProvider -online"