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

PowerShell Get-Help on command 'Set-NetEventPacketCaptureProvider'

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

NAME

Set-NetEventPacketCaptureProvider

SYNOPSIS

Modifies the configuration for a Remote Packet Capture provider.

SYNTAX

Set-NetEventPacketCaptureProvider [-AsJob] [-AssociatedCaptureTarget <CimInstance>] [-CaptureType {Physical | Switch | BothPhysicalAndSwitch}] [-CimSession <CimSession[]>] [-Confirm] [-EtherType <UInt16[]>] [-IpAddresses <String[]>] [-IpProtocols <Byte[]>] [-Level <Byte>] [-LinkLayerAddress <String[]>] [-MatchAllKeyword <UInt64>] [-MatchAnyKeyword <UInt64>] [-MultiLayer <Boolean>] [-PassThru] [-ThrottleLimit <Int32>] [-TruncationLength <UInt16>] [-VmCaptureDirection {Ingress | Egress | IngressAndEgress}] [-WhatIf] [<CommonParameters>]

Set-NetEventPacketCaptureProvider [-AsJob] [-AssociatedEventSession <CimInstance>] [-CaptureType {Physical | Switch | BothPhysicalAndSwitch}] [-CimSession <CimSession[]>] [-Confirm] [-EtherType <UInt16[]>] [-IpAddresses <String[]>] [-IpProtocols <Byte[]>] [-Level <Byte>] [-LinkLayerAddress

<String[]>] [-MatchAllKeyword <UInt64>] [-MatchAnyKeyword <UInt64>]
[-MultiLayer <Boolean>] [-PassThru] [-ThrottleLimit <Int32>]
[-TruncationLength <UInt16>] [-VmCaptureDirection {Ingress | Egress |
IngressAndEgress}] [-WhatIf] [<CommonParameters>]

Set-NetEventPacketCaptureProvider [-AsJob] [-CaptureType {Physical | Switch |
BothPhysicalAndSwitch}] [-CimSession <CimSession[]>] [-Confirm] [-EtherType
<UInt16[]>] -InputObject <CimInstance[]> [-IpAddresses <String[]>]
[-IpProtocols <Byte[]>] [-Level <Byte>] [-LinkLayerAddress <String[]>]
[-MatchAllKeyword <UInt64>] [-MatchAnyKeyword <UInt64>] [-MultiLayer
<Boolean>] [-PassThru] [-ThrottleLimit <Int32>] [-TruncationLength <UInt16>]
[-VmCaptureDirection {Ingress | Egress | IngressAndEgress}] [-WhatIf]
[<CommonParameters>]

Set-NetEventPacketCaptureProvider [[-SessionName] <String[]>] [-AsJob]
[-CaptureType {Physical | Switch | BothPhysicalAndSwitch}] [-CimSession
<CimSession[]>] [-Confirm] [-EtherType <UInt16[]>] [-IpAddresses <String[]>]
[-IpProtocols <Byte[]>] [-Level <Byte>] [-LinkLayerAddress <String[]>]
[-MatchAllKeyword <UInt64>] [-MatchAnyKeyword <UInt64>] [-MultiLayer
<Boolean>] [-PassThru] [-ThrottleLimit <Int32>] [-TruncationLength <UInt16>]
[-VmCaptureDirection {Ingress | Egress | IngressAndEgress}] [-WhatIf]
[<CommonParameters>]

DESCRIPTION

The Set-NetEventPacketCaptureProvider cmdlet modifies the configuration for a Remote Packet Capture provider.

PARAMETERS

-AsJob [<SwitchParameter>]

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

-AssociatedCaptureTarget <CimInstance>

Specifies the associated capture target as a CIM object. The capture target is one of the three following objects:

- MSFT_NetEventNetworkAdapter - MSFT_NetEventVmNetworkAdapter - MSFT_NetEventVmSwitch To obtain a capture target, use the Get-NetEventNetworkAdapter cmdlet, the Get-NetEventVmNetworkAdapter cmdlet, or the Get-NetEventVmSwitch cmdlet.

-AssociatedEventSession <CimInstance>

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

-CaptureType <CaptureType>

Specifies whether the packet capture is enabled for physical network adapters, virtual switches, or both. The acceptable values for this parameter are:

- Physical. Captures packets from physical network adapters. - Switch. Captures packets from the virtual machine switch(es) on Hyper-V hosts. - BothPhysicalAndSwitch. Captures packets from both the physical network adapters and the virtual machine switch(es).

-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.

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

-EtherType <UInt16[]>

Specifies an array of ether types. The most common ether types and their values are IPv4 (0800), IPv6 (86DD) and ARP (0806).

-InputObject <CimInstance[]>

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

-IpAddresses <String[]>

Specifies an array of IP addresses. The provider logs network traffic that matches the addresses that this cmdlet specifies. The provider joins multiple addresses by using logical OR.

-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.

-LinkLayerAddress <String[]>

Specifies an array of link layer, or Media Access Control (MAC), addresses. The packet capture provider logs network traffic that matches

this filter.

-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.

-MultiLayer <Boolean>

Indicates whether the capture should occur at various layers in the stack. By default, this parameter has a value of $False.

-PassThru [<SwitchParameter>]

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

-SessionName <String[]>

Specifies an array of names of sessions associated with packet capture providers.

-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.

-TruncationLength <UInt16>

Specifies the display length of each captured packet. The default size is

128 bytes.

-VmCaptureDirection <VmCaptureDirection>

Specifies the direction of network traffic for a virtual machine capture.

The acceptable values for this parameter are:

- Ingress. Network traffic from a virtual machine to a virtual switch. -

Egress. Network traffic from a virtual switch to a virtual machine.

-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: Modify a packet capture provider ---------

```
PS C:\>New-NetEventSession -SessionName "Session01"
PS C:\> Add-NetEventProvider -Name "Microsoft-Windows-TCPIP" -SessionName
"Session01"
PS C:\> Add-NetEventPacketCaptureProvider -SessionName "Session01"
PS C:\> Set-NetEventPacketCaptureProvider -SessionName "Session01"
-IpAddresses 182.168.0.1 -IpProtocol 6
```

This example modifies a packet capture provider.

The first command uses the New-NetEventSession cmdlet to create a new session

named Session01.

The second command uses the Add-NetEventProvider cmdlet to add a TCP/IP Net

provider to the session.

The third command uses the Add-NetEventPacketCaptureProvider cmdlet to add a packet capture provider to a session named Session01.

The fourth command modifies the packet capture provider settings.

REMARKS

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

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

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

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