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

PowerShell Get-Help on command 'Add-NetEventPacketCaptureProvider'

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

NAME

Add-NetEventPacketCaptureProvider

SYNOPSIS

Adds a Remote Packet Capture provider.

SYNTAX

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

DESCRIPTION

The Add-NetEventPacketCaptureProvider cmdlet adds a Remote Packet Capture
provider. You can only use one packet capture provider at a time and you must

remove an existing provider before you use this cmdlet to add a new provider.
To remove an existing Remote Packet Capture provider, use the
Remove-NetEventPacketCaptureProvider cmdlet.

PARAMETERS

-AsJob [<SwitchParameter>]

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

-CaptureType <CaptureType>

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

-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. Set the MatchAnyKeyword parameter value to 0 (zero) to match all keywords.

-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. For more information, see EnableTraceEx2 function (https://msdn.microsoft.com/en-us/library/windows/desktop/dd392305(v=vs.85))in the Microsoft Developer Network library.

-MultiLayer <Boolean>

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

-SessionName <String>

Specifies the name of the session associated with the packet capture provider.

-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: Add a packet capture provider ----------

```
PS C:\>New-NetEventSession -Name "Session01"
PS C:\> Add-NetEventProvider -Name "Microsoft-Windows-TCPIP" -SessionName
"Session01"
PS C:\> Add-NetEventPacketCaptureProvider -SessionName "Session01"
```

This example adds a Remote Packet Capture provider to a session.

The first command uses the New-NetEventSession cmdlet to create a new session named Session01.

The second command adds a provider named Microsoft-Windows-TCPIP to the session named Session01 by using the Add-NetEventProvider cmdlet.

The third command adds a packet capture provider to the session.

REMARKS

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

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

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

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