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

PowerShell Get-Help on command 'Set-NetEventProvider'

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

NAME

Set-NetEventProvider

SYNOPSIS

Modifies settings for an ETW provider.

SYNTAX

Set-NetEventProvider [[-Level] <Byte>] [[-MatchAnyKeyword] <UInt64>]
[[-MatchAllKeyword] <UInt64>] [-AsJob] [-AssociatedCaptureTarget
<CimInstance>] [-CimSession <CimSession[]>] [-Confirm] [-PassThru]
[-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

Set-NetEventProvider [[-Level] <Byte>] [[-MatchAnyKeyword] <UInt64>]
[[-MatchAllKeyword] <UInt64>] [-AsJob] [-AssociatedEventSession <CimInstance>]
[-CimSession <CimSession[]>] [-Confirm] [-PassThru] [-ThrottleLimit <Int32>]
[-WhatIf] [<CommonParameters>]

Set-NetEventProvider [[-Level] <Byte>] [[-MatchAnyKeyword] <UInt64>]
[[-MatchAllKeyword] <UInt64>] [-AsJob] [-CimSession <CimSession[]>] [-Confirm]
-InputObject <CimInstance[]> [-PassThru] [-ThrottleLimit <Int32>] [-WhatIf]

[<CommonParameters>]

Set-NetEventProvider [[-Name] <String[]>] [[-Level] <Byte>]
[[-MatchAnyKeyword] <UInt64>] [[-MatchAllKeyword] <UInt64>] [-AsJob]
[-CimSession <CimSession[]>] [-Confirm] [-PassThru] [-ThrottleLimit <Int32>]
[-WhatIf] [<CommonParameters>]

DESCRIPTION

The Set-NetEventProvider cmdlet modifies settings for an Event Tracing for Windows (ETW) 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.

-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.

-InputObject <CimInstance[]>

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

-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. 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 CLR ETW Keywords and Levels (https://msdn.microsoft.com/en-us/library/ff357720.aspx)in the

Microsoft Developer Network library.

-Name <String[]>

Specifies an array of names that identify ETW providers.

-PassThru [<SwitchParameter>]

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

-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.

-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 an ETW provider ----------

PS C:\>New-NetEventSession -SessionName "Session01"
PS C:\> Add-NetEventProvider -Name "Microsoft-Windows-TCPIP" -SessionName "Session01"
PS C:\> Set-NetEventProvider -Name "Microsoft-Windows-TCPIP" -Level 3

This example modifies an ETW 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 provider named Microsoft-Windows-TCPIP to the session named Session01.

The third command modifies the logging level for the provider named Microsoft-Windows-TCPIP.

REMARKS

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

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

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

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