Windows PowerShell Get-Help on Cmdlet 'Add-NetEventProvider'

PS:\>Get-HELP Add-NetEventProvider -Full

NAME

Add-NetEventProvider

SYNOPSIS

Adds an ETW provider to a session.

SYNTAX

Add-NetEventProvider [-Name] <String> [-SessionName] <String> [[-Level] <Byte>] [[-MatchAnyKeyword] <UInt64>] [[-MatchAllKeyword] <UInt64>] [-AsJob] [-CimSession

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

DESCRIPTION

The Add-NetEventProvider cmdlet adds an Event Tracing for Windows (ETW) provider to a session.

PARAMETERS

-AsJob [<SwitchParameter>]

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

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-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.

Required? false

Position? 2

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-MatchAllKeyword <UInt64>

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

Required? false

Position? 4

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-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.

Required? false

Position? 3

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <String>

Specifies a name that identifies an ETW provider.

Required? true

Position? 0

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SessionName <String>

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

Required? true

Position? 1

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-WhatIf [<SwitchParameter>]

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

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

<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).

INPUTS

OUTPUTS

NOTES

--------- Example 1: Add an ETW provider to a session ---------

PS C:\>New-NetEventSession -SessionName "Session01"

PS C:\> Add-NetEventProvider -Name "Microsoft-Windows-TCPIP" -SessionName "Session01"

This example adds an ETW provider to a session.

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

The second command adds an ETW provider named Microsoft-Windows-TCPIP to the session named Session01.

RELATED LINKS

https://learn.microsoft.com/powershell/module/neteventpacketcapture/add-neteventprovider?view=windowsserver2022-ps&wt.mc_id=ps-gethelp

- Get-NetEventProvider
- New-NetEventSession
- Remove-NetEventProvider
- Set-NetEventProvider