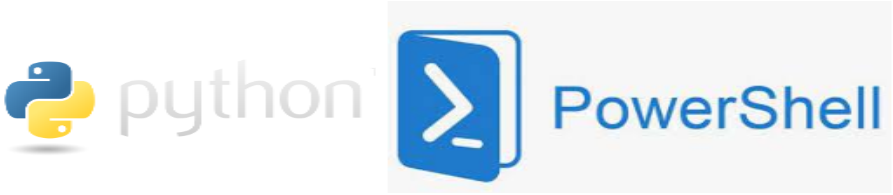

Full credit is given to the above companies including the OS that this PDF file was generated!

PowerShell Get-Help on command 'New-NetEventSession'

PS C:\Users\wahid> Get-Help New-NetEventSession

NAME

New-NetEventSession

SYNOPSIS

Creates a network event session.

SYNTAX

New-NetEventSession [-Name] <String> [-AsJob] [-CaptureMode {RealtimeRPC |

SaveToFile | RealtimeLocal}] [-CimSession <CimSession[]>] [-Confirm]

[-LocalFilePath <String>] [-MaxFileSize <UInt32>] [-MaxNumberOfBuffers <Byte>]

[-ThrottleLimit <Int32>] [-TraceBufferSize <UInt32>] [-WhatIf]

[<CommonParameters>]

DESCRIPTION

The New-NetEventSession cmdlet creates a network event session. A session

controls how the computer logs events and, optionally, network traffic, or

packets. Later, add network event providers to a session. A network event

provider logs events and network traffic as Event Tracing for Windows (ETW)

events. The session stores these events in an .etl file or provides them to an

application that displays them.

Assign a name for the session. Only one session can exist at a time. Remove an existing session by using the Remove-NetEventSession cmdlet. You can specify the maximum number of buffers in a session and the size of the trace buffer.

You can also specify whether to use an .etl file. If you use an .etl file, you can specify its location and maximum size. Instead of an .etl file, you can select a type of live display.

After you create a session, you can use the Set-NetEventSession cmdlet to modify the session settings. After you create a session, add one or more providers to it by using the Add-NetEventProvider cmdlet. Use the Start-NetEventSession and Stop-NetEventSession cmdlets to start and stop logging.

PARAMETERS

-AsJob [<SwitchParameter>]

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

-CaptureMode <CaptureModes>

Specifies a capture mode. The acceptable values for this parameter are:

- SaveToFile. Saves the capture to an .etl file. - RealtimeRPC. Connects remotely for a live event and packet capture. - RealtimeLocal. Connects locally for a live event and packet capture.

If you specify a value of SaveToFile, you can specify a location for the file by using the LocalFilePath parameter and specify a maximum file size by using the MaxFileSize parameter.

If you specify a value of RealtimeRPC or RealtimeLocal, the capture requires additional software, such as Microsoft Message Analyzer.

-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.

-LocalFilePath <String>

Specifies a file path. If you specify a value of SaveToFile for the CaptureMode parameter, the cmdlet saves the file to this location. Be sure that you can write to this location. If you do not specify this parameter, the cmdlet uses the default value of %LocalAppData%\Temp\NetTrace.etl.

-MaxFileSize <UInt32>

Specifies a maximum file size, in megabytes. If you specify a value of SaveToFile for the CaptureMode parameter, this value is the maximum size for the .etl file. Once the file reaches the maximum, the session continues to save events, and discards the oldest events to create space. A value of 0 means that there is no maximum. If you do not specify this parameter, the cmdlet uses a default value of 250.

-MaxNumberOfBuffers <Byte>

Specifies the maximum number of buffers used in a session. If the computer determines that the value restricts performance or the value is 0, the computer overrides the configuration to optimize trace performance. For more information, see EVENT_TRACE_PROPERTIES structure (https://msdn.microsoft.com/en-us/library/windows/desktop/aa363784(v=vs.85)in the Microsoft

Developer Network library.

-Name <String>

Specifies a name to assign to the session for event and packet capture.

-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.

-TraceBufferSize <UInt32>

Specifies the amount of memory, in kilobytes, for a buffer for event tracing. The maximum value is 1024. If the computer determines that the value restricts performance or the value is 0, the computer overrides the configuration to optimize trace performance. The ETW logger uses the size of physical memory to calculate the default value.

-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: Create a session ----------

PS C:\>New-NetEventSession -Name "Session38"

This command creates session named Session38. Use the Add-NetEventProvider cmdlet to add a provider for the session.

REMARKS

To see the examples, type: "get-help New-NetEventSession -examples".

For more information, type: "get-help New-NetEventSession -detailed".

For technical information, type: "get-help New-NetEventSession -full".

For online help, type: "get-help New-NetEventSession -online"