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

Windows PowerShell Get-Help on Cmdlet 'New-EtwTraceSession'

PS:\>Get-HELP New-EtwTraceSession -Full

NAME

New-EtwTraceSession

SYNOPSIS

Creates an ETW trace session.

SYNTAX

New-EtwTraceSession [-Name] <String> [-AsJob] [-BufferSize <UInt32>] [-CimSession <CimSession[]>] [-ClockType {Performance | System | Cycle}] [-Confirm] [-FlushTimer

<UInt32>] [-LocalFilePath <String>] [-LogFileMode <UInt32>] [-MaximumBuffers <UInt32>] [-MaximumFileSize <UInt32>] [-MinimumBuffers <UInt32>] [-ThrottleLimit <Int32>]

[-WhatIf] [<CommonParameters>]

DESCRIPTION

The Start-EtwTraceSession cmdlet replaces this cmdlet as the recommended method of starting an ETW session. It provides an easier way to specify common LogFileMode

settings and other parameters.

The New-EtwTraceSession cmdlet creates an Event Trace for Windows (ETW) trace session.

PARAMETERS

-AsJob [<SwitchParameter>]

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

The cmdlet immediately returns an object that represents the job and then displays the command prompt. You can continue to work in the session while the job

completes. To manage the job, use the `*-Job` cmdlets. To get the job results, use the Receive-Job (https://go.microsoft.com/fwlink/?LinkID=113372)cmdlet.

For more information about Windows PowerShell background jobs, see about_Jobs (https://go.microsoft.com/fwlink/?LinkID=113251).

Required?   false

Position?   named

Default value   False

Accept pipeline input?   False

Accept wildcard characters? false

-BufferSize <UInt32>

Specifies the ETW session buffer size, in kilobytes.

Required?   false

Position?   named

Default value   None

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
```

-ClockType <ClockType>

Specifies the type of timestamp that will be used for each event logged to this ETW session.

This is an advanced session configuration option, and it is not recommended that this parameter be set.

For more information, see the description of the ClientContext field in the topic WNODE_HEADER structure (https://msdn.microsoft.com/en-us/library/windows/desktop/aa364160.aspx)for a description of the different clock types available.

```
        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
```

-FlushTimer <UInt32>

When set, all active buffers in the session will be flushed at this interval, in seconds.

This is an advanced session configuration option, and it is not recommended that this parameter be set.

If it is not set, the ETW will select an appropriate default based on the LogFileMode.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-LocalFilePath <String>

Specifies the full path to the file the ETW session should write to. For non-buffering mode sessions only.

When creating a new-file file mode session, the file path must contain a %d in the file name.

Do not use this parameter if the session is configured as a buffering mode session. Use Save-EtwTraceSession to save a buffering mode session to disk instead.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-LogFileMode <UInt32>

Specifies the ETW session logging mode. The value is a bitmask of the ETW logging mode constants. For valid values, see Logging Mode Constants

(https://msdn.microsoft.com/library/windows/desktop/aa364080.aspx).

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-MaximumBuffers <UInt32>

Specifies the maximum number of buffers the ETW session should use.

The ETW session will use a maximum of (BufferSize * MaximumBuffers) kilobytes of memory. Depending on the specified LogFileMode this may be pageable or non-paged memory.

If the session is losing events because the buffers cannot be flushed quickly enough to keep up with the incoming event rate, try increasing this value.

Configuring a session to use too many buffers may affect system performance.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-MaximumFileSize <UInt32>

Specifies the maximum file size for the output .etl file to grow to, in megabytes.

The parameter must be set for a circular, new-file, or sequential file mode ETW session.

For circular sessions, once the file reaches this size the oldest buffers will be overwritten by the new buffers.

For new-file sessions, once the file reaches this size a new file will be created and all new events will be written to that file.

For sequential file sessions, once the file reaches this size the session will stop.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-MinimumBuffers <UInt32>

Specifies the minimum number of buffers the ETW session should use.

The ETW session will use a minimum of (BufferSize * MinimumBuffers) kilobytes of memory. Depending on the specified LogFileMode this may be pageable or non-paged

memory.

If the session is losing events because the buffers cannot be flushed quick enough to keep up with the incoming event rate, try increasing this value.

Configuring a session to use too many buffers may affect system performance.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-Name <String>

Specifies the name of the new ETW trace session.

Required?	true
Position?	0
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: Create an ETW trace session ------------

```
PS C:\> New-EtwTraceSession -Name "NetCfgTrace" -MaximumBuffers 24
```

This command creates an ETW trace session named NetCfgTrace that has a value of 24 for the MaximumBuffers parameter.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/eventtracingmanagement/new-etwtracesession?view=windowsserver2022-ps&wt.mc_id=ps-gethelp

Get-EtwTraceSession

Save-EtwTraceSession

Send-EtwTraceSession

Start-EtwTraceSession

Stop-EtwTraceSession

Update-EtwTraceSession