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

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

NAME

   Update-EtwTraceSession

SYNOPSIS

   Modifies an existing ETW session.

SYNTAX

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

     -InputObject <CimInstance[]> [-LocalFilePath <String>] [-LogFileMode <UInt32>] [-MaximumBuffers <UInt32>] [-MaximumFileSize <UInt32>] [-PassThru] [-ThrottleLimit

   <Int32>] [-WhatIf] [<CommonParameters>]

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

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

   [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Update-EtwTraceSession cmdlet modifies an existing Event Tracing for Windows (ETW) 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

-InputObject <CimInstance[]>

Specifies the input to this cmdlet. You can use this parameter, or you can pipe the input to this cmdlet.

Required?   true

Position?   named

Default value   None

Accept pipeline input?   True (ByValue)

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.

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

-Name <String[]>

Specifies the name of the ETW session.

Required?   true

Position?   0

Default value   None

Accept pipeline input?   True (ByPropertyName)

Accept wildcard characters? false

-PassThru [<SwitchParameter>]

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

Required?   false

Position?   named

Default value   False

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

RELATED LINKS

Online Version:

https://learn.microsoft.com/powershell/module/eventtracingmanagement/update-etwtracesession?view=windowsserver2022

-ps&wt.mc_id=ps-gethelp

Get-EtwTraceSession

New-EtwTraceSession

Save-EtwTraceSession

Send-EtwTraceSession

Start-EtwTraceSession

Stop-EtwTraceSession