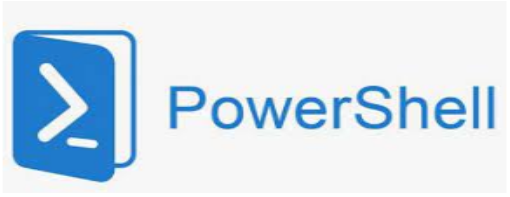

Full credit is given to the above companies including the OS that this PDF file was generated!

PowerShell Get-Help on command 'Start-EtwTraceSession'

PS C:\Users\wahid> Get-Help Start-EtwTraceSession

NAME

Start-EtwTraceSession

SYNOPSIS

Starts an ETW session with the specified name and settings.

SYNTAX

Start-EtwTraceSession [-Name] <String> [-BufferSize <UInt32>] [-CimSession <CimSession>] [-ClockType {Performance | System | Cycle}] [-Compress] [-Confirm] [-FileMode {File | Buffering | Sequential | Circular}] [-FlushTimer <UInt32>] [-LocalFilePath <String>] [-LogFileMode <UInt32>] [-MaximumBuffers <UInt32>] [-MaximumFileSize <UInt32>] [-MinimumBuffers <UInt32>] [-NonPaged] [-RealTime] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Start-EtwTraceSession cmdlet starts an ETW session with the specified name and settings.

PARAMETERS

-BufferSize <UInt32>

Specifies the Event Tracing for Windows (ETW) session buffer size, in kilobytes.

-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.

-ClockType <String>

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.

-Compress [<SwitchParameter>]

Controls whether ETW should compress the saved buffers as they are filled. Enabling this parameter sets the EVENT_TRACE_COMPRESSED_MODE bit in the LogFileMode parameter.

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

-FileMode <String>

Specifies how events received by the session should be saved. FileMode provides named values for common logging mode constants, and setting it will affect the value of LogFileMode that is passed to ETW when the session is created.

If you specify this parameter do not specify any file or buffering mode bits in the LogFileMode parameter.

For more information about available modes, see Logging Mode Constants (https://msdn.microsoft.com/en-us/library/windows/desktop/aa364080.aspx)in MSDN.

-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 .

-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.

-LogFileMode <UInt32>

Specifies the ETW session logging mode. The value is a bitmask of the ETW logging mode constants.

For more information, see Logging Mode Constants (https://msdn.microsoft.com/en-us/library/windows/desktop/aa364080.aspx)in MSDN.

-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 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.

-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.

-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.

-Name <String>

Specifies the name of the ETW trace session.

-NonPaged [<SwitchParameter>]

Controls whether ETW should use memory from the non-paged pool for the session buffers. Enabling this parameter clears the EVENT_TRACE_USE_PAGED_MEMORY bit in the LogFileMode parameter.

Using memory from the non-paged pool for the session buffers is only required if any of the events that will be sent to the session are logged from the kernel or a driver at high a dispatch level. This parameter should not be set otherwise.

Allocating too much memory from the non-paged pool can seriously degrade

system performance.

-RealTime [<SwitchParameter>]

Controls whether ETW should allow real-time consumers to connect to the session. Enabling this parameter sets the EVENT_TRACE_REAL_TIME_MODE bit in the LogFileMode parameter.

-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).

REMARKS

To see the examples, type: "get-help Start-EtwTraceSession -examples".

For more information, type: "get-help Start-EtwTraceSession -detailed".

For technical information, type: "get-help Start-EtwTraceSession -full".

For online help, type: "get-help Start-EtwTraceSession -online"