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

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

NAME

Send-EtwTraceSession

SYNOPSIS

Sends the log file of the specified ETW session to a destination.

SYNTAX

Send-EtwTraceSession [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-DeleteAfterSend] -DestinationFolder <String> -InputObject <CimInstance[]> [-ThrottleLimit

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

Send-EtwTraceSession [-Name] <String[]> [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-DeleteAfterSend] -DestinationFolder <String> [-ThrottleLimit <Int32>]

[-WhatIf] [<CommonParameters>]

DESCRIPTION

The Send-EtwTraceSession cmdlet sends the log file of the specified Event Tracing for Windows (ETW) session to a destination.

For file mode ETW sessions, the session will be updated to write to a new file and the previous file will be copied to the specified destination.

For buffering mode ETW sessions, the session will be flushed to the specified destination.

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

-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

-DeleteAfterSend [<SwitchParameter>]

Deletes the original file that the ETW session was writing to after the file has been copied to the destination.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-DestinationFolder <String>

Specifies the destination for the output .etl file.

If the ETW session is a buffering mode session, this parameter must be a full file path rather than a folder.

Required? true

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

-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

-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

* The return values consist of a Win32 error code and a value returned by the cmdlet. The codes have the following meanings:

- 0: Success . New file created. Existing file copied to the destination folder. Existing file deleted, if specified. - 1: CreateNewFileFailed . Operation halts

at this point if a new file is not created. - 2: CopyFileFailed . New file created. - 3: DeleteOldFileFailed . New file created. Existing file copied to the

destination folder.

--------- Example 1: Send a trace session to a folder ---------

PS C:\> Send-EtwTraceSession -Name "WFP-IPsec Trace" -DestinationFolder "\\server1\traces\"

-DeleteExistingFileAfterSend

This command sends an ETW trace session named WFP-IPsec Trace to the destination folder \\server17\traces\. The command deletes the local copy of the original trace

after it is successfully copied.

RELATED LINKS

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

Get-EtwTraceSession

New-EtwTraceSession

Save-EtwTraceSession

Start-EtwTraceSession

Stop-EtwTraceSession

Update-EtwTraceSession