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 'Save-EtwTraceSession'

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

NAME

   Save-EtwTraceSession

SYNOPSIS

   Saves the events collected by the ETW session to an .etl file.

SYNTAX

   Save-EtwTraceSession [-Name] <String> [-CimSession <CimSession>] [-Confirm] [-OutputFile <FileInfo>] [-OutputFolder

<DirectoryInfo>] [-Overwrite] [-Stop] [-WhatIf]

   [<CommonParameters>]

DESCRIPTION

   The Save-EtwTraceSession cmdlet saves the events collected by the ETW session to an .etl file.

PARAMETERS

  -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

  -Name <String>

    Specifies the name of the ETW session.

    Required?   true

    Position?   0

    Default value   None

    Accept pipeline input?   False

    Accept wildcard characters? false

  -OutputFile <FileInfo>

    Specifies the file to save the .etl file to for the ETW session.

    Required?   false

Position?   named

Default value   None

Accept pipeline input?   True (ByValue)

Accept wildcard characters? false

-OutputFolder <DirectoryInfo>

Specifies the folder to save the .etl file to for the ETW session.

When this parameter is set, the file name of the .etl will be selected automatically based on the session properties.

If the session is a buffering mode session, the file name will be the name of the session.

If the session is a file mode session, the file name will be the file name of the currently being written to.

To control the file name as well as the output folder, use the OutputFile parameter instead.

Required?   false

Position?   named

Default value   None

Accept pipeline input?   True (ByValue)

Accept wildcard characters? false

-Overwrite [<SwitchParameter>]

Controls whether an existing file should be overwritten by saving this session.

Required?   false

Position?   named

Default value   False

Accept pipeline input?   False

Accept wildcard characters? false

-Stop [<SwitchParameter>]

Controls whether the session should be stopped after the save is complete.   *Page 3/5*

Required?   false

    Position?   named

    Default value   False

    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

  System.IO.FileInfo, System.IO.DirectoryInfo

OUTPUTS

  System.IO.FileInfo, CIM_DataFile

    This cmdlet returns a System.IO.FileInfo object that represents a file on the local computer. The object is returned

when the current session is saved

    successfully to a file on the local machine.

This cmdlet returns a CIM_DataFile object when the current session is saved successfully to a file over a CIM session.

NOTES

RELATED LINKS

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

Get-EtwTraceSession

New-EtwTraceSession

Send-EtwTraceSession

Start-EtwTraceSession

Stop-EtwTraceSession

Update-EtwTraceSession