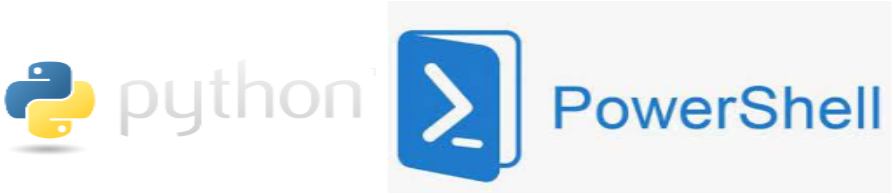

Full credit is given to the above companies including the OS that this PDF file was generated!

PowerShell Get-Help on command 'Add-EtwTraceProvider'

PS C:\Users\wahid> Get-Help Add-EtwTraceProvider

NAME

Add-EtwTraceProvider

SYNOPSIS

Adds an ETW trace provider to an ETW trace session or AutoLogger session configuration.

SYNTAX

Add-EtwTraceProvider [-Guid] <String> [-AsJob] -AutologgerName <String> [-CimSession <CimSession[]>] [-Confirm] [-Level <Byte>] [-MatchAllKeyword <UInt64>] [-MatchAnyKeyword <UInt64>] [-Property <UInt32>] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

Add-EtwTraceProvider [-Guid] <String> [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Level <Byte>] [-MatchAllKeyword <UInt64>] [-MatchAnyKeyword <UInt64>] [-Property <UInt32>] -SessionName <String> [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Add-EtwTraceProvider cmdlet adds an Event Tracing for Windows (ETW) trace provider to a specified ETW trace session or AutoLogger session configuration with the specified parameters.

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).

-AutologgerName <String>

Specifies the name of the target AutoLogger session.

-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.

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

-Guid <String>

Specifies the provider ID.

-Level <Byte>

Specifies the maximum event level for which to enable for collection.

For more information, see EnableTraceEx2 function (https://msdn.microsoft.com/en-us/library/windows/desktop/dd392305.aspx)on MSDN.

-MatchAllKeyword <UInt64>

Specifies a bitmask of keywords an event must match in order to be logged to the session.

An event must match every keyword set by this parameter. Most of the time, the MatchAnyKeyword parameter is more suitable.

For more information, see EnableTraceEx2 function (https://msdn.microsoft.com/en-us/library/windows/desktop/dd392305.aspx)on MSDN.

-MatchAnyKeyword <UInt64>

Specifies a bitmask of keywords an event must match in order to be logged to the session.

An event must match at least one keyword set by this parameter.

For more information, see EnableTraceEx2 function (https://msdn.microsoft.com/en-us/library/windows/desktop/dd392305.aspx)on MSDN.

-Property <UInt32>

Specifies the Enable property to use for events logged from this provider to the session.

For more information, see Configuring and Starting an AutoLogger Session (https://msdn.microsoft.com/en-us/library/windows/desktop/aa363687.aspx).

-SessionName <String>

Specifies the name of the target ETW session.

-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 zero 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.

-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).

Example 1: Add an ETW trace provider to an AutoLogger configuration

```
PS C:\> Add-EtwTraceProvider -Guid "{5EEFEBDB-E90C-423A-8ABF-0241E7C5B87D}"
-AutologgerName "WFP-IPsec Trace"
SessionName     :
AutologgerName  : WFP-IPsec Trace
Guid            : {5EEFEBDB-E90C-423A-8ABF-0241E7C5B87D}
Level           : 0
MatchAnyKeyword : 0x0
```

MatchAllKeyword : 0x0

Property : 0

This command adds the ETW trace provider that has the specified GUID to an

AutoLogger configuration named WFP-IPsec Trace.

---- Example 2: Add an ETW trace provider to an ETW session ----

PS C:\> Add-EtwTraceProvider -Guid "{5EEFEBDB-E90C-423A-8ABF-0241E7C5B87D}"

-SessionName "VMM"

SessionName : VMM

AutologgerName :

Guid : {5EEFEBDB-E90C-423A-8ABF-0241E7C5B87D}

Level : 0

MatchAnyKeyword : 0x0

MatchAllKeyword : 0x0

Property : 0

This command adds the ETW trace provider that has the specified GUID to an

session named VMM.

REMARKS

To see the examples, type: "get-help Add-EtwTraceProvider -examples".

For more information, type: "get-help Add-EtwTraceProvider -detailed".

For technical information, type: "get-help Add-EtwTraceProvider -full".

For online help, type: "get-help Add-EtwTraceProvider -online"