Windows PowerShell Get-Help on Cmdlet 'Set-EtwTraceProvider'

PS:\>Get-HELP Set-EtwTraceProvider -Full

NAME

Set-EtwTraceProvider

SYNOPSIS

Modifies a provider's enablement settings in an ETW or AutoLogger session.

SYNTAX

Set-EtwTraceProvider [[-Guid] <String[]>] [-AsJob] [-AutologgerName <String[]>] [-CimSession <CimSession[]>] [-Confirm] [-Level <Byte>] [-MatchAllKeyword <UInt64>]

[-MatchAnyKeyword <UInt64>] [-PassThru] [-Property <UInt32>] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

Set-EtwTraceProvider [[-Guid] <String[]>] [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Level <Byte>] [-MatchAllKeyword <UInt64>] [-MatchAnyKeyword <UInt64>]

[-PassThru] [-Property <UInt32>] [-SessionName <String[]>] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

Set-EtwTraceProvider [-AsJob] [-CimSession <CimSession[]>] [-Confirm] -InputObject <CimInstance[]> [-Level <Byte>] [-MatchAllKeyword <UInt64>] [-MatchAnyKeyword

<UInt64>] [-PassThru] [-Property <UInt32>] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Set-EtwTraceProvider cmdlet modifies a provider's enablement settings in an Event Tracing for Windows (ETW) or AutoLogger 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

-AutologgerName <String[]>

Specifies the name of the target AutoLogger session.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

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

-Guid <String[]>

Specifies the provider ID.

Required? false
Position? 0
Default value None
Accept pipeline input? True (ByPropertyName)
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

-Level <Byte>

Specifies the maximum event level to enable for a collection.

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

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-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 about keywords, see EnableTraceEx2 function (https://msdn.microsoft.com/en-us/library/windows/desktop/dd392305.aspx)for

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-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 about keywords, see EnableTraceEx2 function (https://msdn.microsoft.com/en-us/library/windows/desktop/dd392305.aspx).

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PassThru [<SwitchParameter>]

Indicates that this cmdlet returns an object that represents the item on which it operates. By default, this cmdlet does not generate any output.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Property <UInt32>

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

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

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SessionName <String[]>

Specifies the name of the target ETW session.

Required? false

Position? named

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

---------- Example 1: Modify an ETW trace provider ----------

PS C:\> set-EtwTraceProvider -Guid "{106B464A-8043-46B1-8CB8-E92A0CD7A560}" -AutologgerName "WFP-IPsec Trace" -Level 2

SessionName :

AutologgerName : WFP-IPsec Trace

Guid : {106B464A-8043-46B1-8CB8-E92A0CD7A560}

Level : 2

MatchAnyKeyword : 0xFFFFFFFF

MatchAllKeyword : 0x0

Property :

This command modifies the ETW trace provider that has the specified GUID. That provider is associated with a specified AutoLogger configuration named WFP-IPsec Trace.

The command sets the Level to have a value of 2, TRACE_LEVEL_ERROR.

RELATED LINKS

Online Version:

https://learn.microsoft.com/powershell/module/eventtracingmanagement/set-etwtraceprovider?view=windowsserver2022-ps&wt.mc_id=ps-gethelp

Configuring and Starting an AutoLogger Session https://msdn.microsoft.com/library/windows/desktop/aa363687.aspx

Configuring and Starting an Event Tracing Session https://msdn.microsoft.com/library/windows/desktop/aa363688.aspx

Add-EtwTraceProvider

Get-EtwTraceProvider

Remove-EtwTraceProvider