Windows PowerShell Get-Help on Cmdlet 'New-AzWindowsEventLogDataSourceObject'

PS:\>Get-HELP New-AzWindowsEventLogDataSourceObject -Full

NAME

New-AzWindowsEventLogDataSourceObject

SYNOPSIS

Create an in-memory object for WindowsEventLogDataSource.

SYNTAX

New-AzWindowsEventLogDataSourceObject [-Name <String>] [-Stream <String[]>] [-XPathQuery <String[]>] [<CommonParameters>]

DESCRIPTION

Create an in-memory object for WindowsEventLogDataSource.

PARAMETERS

-Name <String>

A friendly name for the data source.

This name should be unique across all data sources (regardless of type) within the data collection rule.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Stream <String[]>

List of streams that this data source will be sent to.

A stream indicates what schema will be used for this data and usually what table in Log Analytics the data will be sent to.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-XPathQuery <String[]>

A list of Windows Event Log queries in XPATH format.

Required? false

Position? named

Default value

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

Microsoft.Azure.PowerShell.Cmdlets.Monitor.DataCollection.Models.WindowsEventLogDataSource

---------- EXAMPLE 1 ----------

PS C:\>New-AzWindowsEventLogDataSourceObject -Name cloudSecurityTeamEvents -Stream Microsoft-WindowsEvent -XPathQuery "Security!"

---------- EXAMPLE 2 ----------

PS C:\>New-AzWindowsEventLogDataSourceObject -Name appTeam1AppEvents -Stream Microsoft-WindowsEvent -XPathQuery "System![System[(Level = 1 or Level = 2 or Level = 3)]]","Application!*[System[(Level = 1 or Level = 2 or Level = 3)]]"

RELATED LINKS

https://learn.microsoft.com/powershell/module/Az.Monitor/new-azwindowseventlogdatasourceobject