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

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

NAME

New-AzOperationalInsightsWindowsEventDataSource

SYNOPSIS

Collects event logs from computers that run the Windows operating system.

SYNTAX

New-AzOperationalInsightsWindowsEventDataSource [-ResourceGroupName] <System.String> [-WorkspaceName] <System.String> [-Name] <System.String> [-EventLogName] <System.String> [-CollectErrors] [-CollectInformation] [-CollectWarnings] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Force] [-Confirm] [-WhatIf] [<CommonParameters>]

New-AzOperationalInsightsWindowsEventDataSource [-Workspace] <Microsoft.Azure.Commands.OperationalInsights.Models.PSWorkspace> [-Name] <System.String> [-EventLogName] <System.String> [-CollectErrors] [-CollectInformation] [-CollectWarnings] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Force] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The New-AzOperationalInsightsWindowsEventDataSource cmdlet adds a data source that collects Windows event logs from connected computers that run the Windows operating

system in Azure Operational Insights.

PARAMETERS

-CollectErrors <System.Management.Automation.SwitchParameter>

Indicates that Operational Insights collects error messages.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-CollectInformation <System.Management.Automation.SwitchParameter>

Indicates that Operational Insights collects information messages.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-CollectWarnings <System.Management.Automation.SwitchParameter>

Indicates that Operational Insights collects warning messages.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>

The credentials, account, tenant, and subscription used for communication with azure

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-EventLogName <System.String>

Specifies the name of the event log.

Required? true

Position? 4

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Force <System.Management.Automation.SwitchParameter>

Forces the command to run without asking for user confirmation.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Name <System.String>

Specifies a name for the data source. The name is not exposed in the Azure Portal and any string can be used as long as it is unique.

Required? true

Position? 3

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ResourceGroupName <System.String>

Specifies the name of a resource group that contains computers.

Required? true

Position? 1

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Workspace <Microsoft.Azure.Commands.OperationalInsights.Models.PSWorkspace>

Specifies a workspace in which this cmdlet operates.

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-WorkspaceName <System.String>

Specifies the name of a workspace in which this cmdlet operates.

Required? true

Position? 2

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Confirm <System.Management.Automation.SwitchParameter>

Prompts you for confirmation before running the cmdlet.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-WhatIf <System.Management.Automation.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

Microsoft.Azure.Commands.OperationalInsights.Models.PSWorkspace

System.String

OUTPUTS

Microsoft.Azure.Commands.OperationalInsights.Models.PSDataSource

NOTES

------ Example 1: Create system Windows event data source ------

```
$EventLogNames       = @()
$EventLogNames      += 'Directory Service'
$EventLogNames      += 'Microsoft-Windows-EventCollector/Operational'
$EventLogNames      += 'System'
$ResourceGroupName   = 'MyResourceGroup'
$WorkspaceName       = 'MyWorkspaceName'

$Count = 0
foreach ($EventLogName in $EventLogNames) {
    $Count++
    $null = New-AzOperationalInsightsWindowsEventDataSource `
    -ResourceGroupName $ResourceGroupName `
    -WorkspaceName $WorkspaceName `
    -Name "Windows-event-$($Count)" `
    -EventLogName $EventLogName `
    -CollectErrors `
    -CollectWarnings `
    -CollectInformation
}

Get-AzOperationalInsightsDataSource `
  -ResourceGroupName $ResourceGroupName `
```

```
    -WorkspaceName $WorkspaceName `
    -Kind 'WindowsEvent'
```

Adds a data source that collects Windows event logs from connected computers that run the Windows operating system in Azure Operational Insights.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.operationalinsights/new-azoperationalinsightswindowseventdatasource