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

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

NAME

New-AzOperationalInsightsCustomLogDataSource

SYNOPSIS

Defines a custom log collection policy.

SYNTAX

New-AzOperationalInsightsCustomLogDataSource [-ResourceGroupName] <System.String> [-WorkspaceName] <System.String> [-Name] <System.String> [-CustomLogRawJson] <System.String> [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Force] [-Confirm] [-WhatIf] [<CommonParameters>]

New-AzOperationalInsightsCustomLogDataSource [-Workspace] <Microsoft.Azure.Commands.OperationalInsights.Models.PSWorkspace> [-Name] <System.String> [-CustomLogRawJson] <System.String> [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Force] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The New-AzOperationalInsightsCustomLogDataSource cmdlet defines a custom log collection policy.

PARAMETERS

-CustomLogRawJson <System.String>

Specifies the custom collection policy as a raw JavaScript Object Notation (JSON) string.

Required? true

Position? 4

Default value None

Accept pipeline input? True (ByPropertyName)

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

-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.

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: Defines a custom log collection policy ------

$customLogRawJson =
'{"customLogName":"Validation_CL","description":"test","inputs":[{"location":{"fileSystemLocations":{"linuxFileTypeLogPaths"
:null,"windowsFileTypeL

ogPaths":["C:\\e2e\\Evan\\ArubaSECURITY*.log"]}},"recordDelimiter":{"regexDelimiter":{"pattern":"\\n","matchIndex":0}}}],"e
xtractions":[{"extractionName":"TimeGenera

ted","extractionType":"DateTime","extractionProperties":{"dateTimeExtraction":{"regex":"((\\d{2})|(\\d{4}))-([0-1]\\d)-(([0-3]\\d)|
(\\d))\\s((\\d)|([0-1]\\d)|(2[0-4]))
:[0-5][0-9]:[0-5][0-9]","joinStringRegex":null}}}]}'

New-AzOperationalInsightsCustomLogDataSource -ResourceGroupName rg-name -WorkspaceName workspace-name
-CustomLogRawJson $customLogRawJson -Name "MyCustomLog"

Name : MyCustomLog
ResourceGroupName : rg-name
WorkspaceName : workspace-name
ResourceId :
/subscriptions/sub-id/resourceGroups/rg-name/providers/Microsoft.OperationalInsights/workspaces/workspace-name/dataso

urces/MyCustomLog

Kind : CustomLog

Properties :

{"customLogName":"Validation_CL","description":"test","extractions":[{"extractionName":"TimeGenerated","extractionProperties":{"dateTimeExtraction"

:{"joinStringRegex":null,"regex":[{"m

atchIndex":0,"numberdGroup":null,"pattern":"((\\d{2})|(\\d{4}))-([0-1]\\d)-(([0-3]\\d)|(\\d))\\s((\\d)|([0-1]\\d)|(2[0-4])):[0-5][0-9]:[0-5][0-9]"}

],"formatString":null}},"extractionTy

pe":"DateTime"}],"inputs":[{"location":{"fileSystemLocations":{"linuxFileTypeLogPaths":null,"windowsFileTypeLogPaths":["C:\\e2e\\Evan\\ArubaSECURIT

Y*.log"]}},"recordDelimiter":{"rege

xDelimiter":{"matchIndex":0,"numberdGroup":null,"pattern":"\\n"}}}]}

The response recieved after defining a custom log collection policy

RELATED LINKS

Online Version:

https://learn.microsoft.com/powershell/module/az.operationalinsights/new-azoperationalinsightscustomlogdatasource

Disable-AzOperationalInsightsLinuxCustomLogCollection

Enable-AzOperationalInsightsLinuxCustomLogCollection