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

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

NAME

New-AzDataCollectionRule

SYNOPSIS

Create a data collection rule.

SYNTAX

New-AzDataCollectionRule -Name <String> -ResourceGroupName <String> [-SubscriptionId <String>] -Location <String> [-DataCollectionEndpointId <String>] [-DataFlow <IDataFlow[]>] [-DataSourceDataImportEventHubConsumerGroup <String>] [-DataSourceDataImportEventHubName <String>] [-DataSourceDataImportEventHubStream <String>] [-DataSourceExtension <IExtensionDataSource[]>] [-DataSourceIisLog <IIisLogsDataSource[]>] [-DataSourceLogFile <ILogFilesDataSource[]>] [-DataSourcePerformanceCounter <IPerfCounterDataSource[]>] [-DataSourcePlatformTelemetry <IPlatformTelemetryDataSource[]>] [-DataSourcePrometheusForwarder <IPrometheusForwarderDataSource[]>] [-DataSourceSyslog <ISyslogDataSource[]>] [-DataSourceWindowsEventLog <IWindowsEventLogDataSource[]>] [-DataSourceWindowsFirewallLog <IWindowsFirewallLogsDataSource[]>] [-Description <String>] [-DestinationAzureMonitorMetricName <String>] [-DestinationEventHub <IEventHubDestination[]>]

[-DestinationEventHubsDirect <IEventHubDirectDestination[]>] [-DestinationLogAnalytic <ILogAnalyticsDestination[]>] [-DestinationMonitoringAccount

<IMonitoringAccountDestination[]>] [-DestinationStorageAccount <IStorageBlobDestination[]>] [-DestinationStorageBlobsDirect <IStorageBlobDestination[]>]

[-DestinationStorageTablesDirect <IStorageTableDestination[]>] [-IdentityType <String>] [-Kind <String>] [-StreamDeclaration <Hashtable>] [-Tag <Hashtable>]

[-UserAssignedIdentity <Hashtable>] [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy

<Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

New-AzDataCollectionRule -Name <String> -ResourceGroupName <String> [-SubscriptionId <String>] -JsonFilePath <String> [-DefaultProfile <PSObject>] [-Break]

[-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials]

[-WhatIf] [-Confirm] [<CommonParameters>]

New-AzDataCollectionRule -Name <String> -ResourceGroupName <String> [-SubscriptionId <String>] -JsonString <String> [-DefaultProfile <PSObject>] [-Break]

[-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials]

[-WhatIf] [-Confirm] [<CommonParameters>]

DESCRIPTION

Create a data collection rule.

PARAMETERS

-Name <String>

The name of the data collection rule.

The name is case insensitive.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ResourceGroupName <String>

The name of the resource group.

The name is case insensitive.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-SubscriptionId <String>

The ID of the target subscription.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Location <String>

The geo-location where the resource lives.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DataCollectionEndpointId <String>

The resource ID of the data collection endpoint that this rule can be used with.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DataFlow <IDataFlow[]>

The specification of data flows.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DataSourceDataImportEventHubConsumerGroup <String>

Event Hub consumer group name

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DataSourceDataImportEventHubName <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

-DataSourceDataImportEventHubStream <String>

The stream to collect from EventHub

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DataSourceExtension <IExtensionDataSource[]>

The list of Azure VM extension data source configurations.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DataSourceIisLog <IIisLogsDataSource[]>

The list of IIS logs source configurations.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DataSourceLogFile <ILogFilesDataSource[]>

The list of Log files source configurations.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DataSourcePerformanceCounter <IPerfCounterDataSource[]>

The list of performance counter data source configurations.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DataSourcePlatformTelemetry <IPlatformTelemetryDataSource[]>

The list of platform telemetry configurations

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DataSourcePrometheusForwarder <IPrometheusForwarderDataSource[]>

The list of Prometheus forwarder data source configurations.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DataSourceSyslog <ISyslogDataSource[]>

The list of Syslog data source configurations.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DataSourceWindowsEventLog <IWindowsEventLogDataSource[]>

The list of Windows Event Log data source configurations.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DataSourceWindowsFirewallLog <IWindowsFirewallLogsDataSource[]>

The list of Windows Firewall logs source configurations.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Description <String>

Description of the data collection rule.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DestinationAzureMonitorMetricName <String>

A friendly name for the destination.

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

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DestinationEventHub <IEventHubDestination[]>

List of Event Hubs destinations.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DestinationEventHubsDirect <IEventHubDirectDestination[]>

List of Event Hubs Direct destinations.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DestinationLogAnalytic <ILogAnalyticsDestination[]>

List of Log Analytics destinations.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DestinationMonitoringAccount <IMonitoringAccountDestination[]>

List of monitoring account destinations.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DestinationStorageAccount <IStorageBlobDestination[]>

List of storage accounts destinations.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DestinationStorageBlobsDirect <IStorageBlobDestination[]>

List of Storage Blob Direct destinations.

To be used only for sending data directly to store from the agent.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DestinationStorageTablesDirect <IStorageTableDestination[]>

List of Storage Table Direct destinations.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-IdentityType <String>

Type of managed service identity (where both SystemAssigned and UserAssigned types are allowed).

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Kind <String>

The kind of the resource.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-StreamDeclaration <Hashtable>

Declaration of custom streams used in this rule.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Tag <Hashtable>

Resource tags.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-UserAssignedIdentity <Hashtable>

The set of user assigned identities associated with the resource.

The userAssignedIdentities dictionary keys will be ARM resource ids in the form:

'/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.ManagedIdentity/userAssignedIdentities/{identityName}.

The dictionary values can be empty objects ({}) in requests.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-JsonFilePath <String>

Path of Json file supplied to the Create operation

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-JsonString <String>

Json string supplied to the Create operation

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DefaultProfile <PSObject>

The DefaultProfile parameter is not functional.

Use the SubscriptionId parameter when available if executing the cmdlet against a different subscription.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Break [<SwitchParameter>]

Wait for .NET debugger to attach

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-HttpPipelineAppend <SendAsyncStep[]>

SendAsync Pipeline Steps to be appended to the front of the pipeline

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-HttpPipelinePrepend <SendAsyncStep[]>

SendAsync Pipeline Steps to be prepended to the front of the pipeline

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Proxy <Uri>

The URI for the proxy server to use

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyCredential <PSCredential>

Credentials for a proxy server to use for the remote call

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyUseDefaultCredentials [<SwitchParameter>]

Use the default credentials for the proxy

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-WhatIf [<SwitchParameter>]

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Confirm [<SwitchParameter>]

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.IDataCollectionRuleResource

NOTES

COMPLEX PARAMETER PROPERTIES

To create the parameters described below, construct a hash table containing the appropriate properties. For information on hash tables, run Get-Help about_Hash_Tables.

DATAFLOW <IDataFlow[]>: The specification of data flows.

[BuiltInTransform <String>]: The builtIn transform to transform stream data

[Destination <List<String>>]: List of destinations for this data flow.

[OutputStream <String>]: The output stream of the transform. Only required if the transform changes data to a different stream.

[Stream <List<String>>]: List of streams for this data flow.

[TransformKql <String>]: The KQL query to transform stream data.

DATASOURCEEXTENSION <IExtensionDataSource[]>: The list of Azure VM extension data source configurations.

ExtensionName <String>: The name of the VM extension.

[ExtensionSetting <IExtensionDataSourceExtensionSettings>]: The extension settings. The format is specific for particular extension.

[(Any) <Object>]: This indicates any property can be added to this object.

[InputDataSource <List<String>>]: The list of data sources this extension needs data from.

[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.

[Stream <List<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.

DATASOURCEIISLOG <IIisLogsDataSource[]>: The list of IIS logs source configurations.

Stream <List<String>>: IIS streams

[LogDirectory <List<String>>]: Absolute paths file location

[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.

DATASOURCELOGFILE <ILogFilesDataSource[]>: The list of Log files source configurations.

FilePattern <List<String>>: File Patterns where the log files are located

Stream <List<String>>: List of streams that this data source will be sent to. A stream indicates what schema will be used for this data source

[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.

[SettingTextRecordStartTimestampFormat <String>]: One of the supported timestamp formats

DATASOURCEPERFORMANCECOUNTER <IPerfCounterDataSource[]>: The list of performance counter data source configurations.

[CounterSpecifier <List<String>>]: A list of specifier names of the performance counters you want to collect. Use a wildcard (*) to collect a counter

for all instances. To get a list of performance counters on Windows, run the command 'typeperf'.

[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.

[SamplingFrequencyInSecond <Int32?>]: The number of seconds between consecutive counter measurements (samples).

[Stream <List<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.

DATASOURCEPLATFORMTELEMETRY <IPlatformTelemetryDataSource[]>: The list of platform telemetry configurations

Stream <List<String>>: List of platform telemetry streams to collect

[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.

DATASOURCEPROMETHEUSFORWARDER <IPrometheusForwarderDataSource[]>: The list of Prometheus forwarder data source configurations.

[LabelIncludeFilter <IPrometheusForwarderDataSourceLabelIncludeFilter>]: The list of label inclusion filters in the form of label "name-value" pairs.

Currently only one label is supported: 'microsoft_metrics_include_label'. Label values are matched case-insensitively.

[(Any) <String>]: This indicates any property can be added to this object.

[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.

[Stream <List<String>>]: List of streams that this data source will be sent to.

DATASOURCESYSLOG <ISyslogDataSource[]>: The list of Syslog data source configurations.

[FacilityName <List<String>>]: The list of facility names.

[LogLevel <List<String>>]: The log levels to collect.

[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.

[Stream <List<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.

DATASOURCEWINDOWSEVENTLOG <IWindowsEventLogDataSource[]>: The list of Windows Event Log data source configurations.

[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.

[Stream <List<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.

[XPathQuery <List<String>>]: A list of Windows Event Log queries in XPATH format.

DATASOURCEWINDOWSFIREWALLLOG <IWindowsFirewallLogsDataSource[]>: The list of Windows Firewall logs source configurations.

Stream <List<String>>: Firewall logs streams

[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.

DESTINATIONEVENTHUB <IEventHubDestination[]>: List of Event Hubs destinations.

[EventHubResourceId <String>]: The resource ID of the event hub.

[Name <String>]: A friendly name for the destination. This name should be unique across all destinations (regardless of type) within the data collection

rule.

DESTINATIONEVENTHUBSDIRECT <IEventHubDirectDestination[]>: List of Event Hubs Direct destinations.

[EventHubResourceId <String>]: The resource ID of the event hub.

[Name <String>]: A friendly name for the destination. This name should be unique across all destinations (regardless of type) within the data collection

rule.

DESTINATIONLOGANALYTIC <ILogAnalyticsDestination[]>: List of Log Analytics destinations.

[Name <String>]: A friendly name for the destination. This name should be unique across all destinations (regardless of type) within the data collection

rule.

[WorkspaceResourceId <String>]: The resource ID of the Log Analytics workspace.

DESTINATIONMONITORINGACCOUNT <IMonitoringAccountDestination[]>: List of monitoring account destinations.

[AccountResourceId <String>]: The resource ID of the monitoring account.

[Name <String>]: A friendly name for the destination. This name should be unique across all destinations (regardless of type) within the data collection rule.

DESTINATIONSTORAGEACCOUNT <IStorageBlobDestination[]>: List of storage accounts destinations.

[ContainerName <String>]: The container name of the Storage Blob.

[Name <String>]: A friendly name for the destination. This name should be unique across all destinations (regardless of type) within the data collection rule.

[StorageAccountResourceId <String>]: The resource ID of the storage account.

DESTINATIONSTORAGEBLOBSDIRECT <IStorageBlobDestination[]>: List of Storage Blob Direct destinations. To be used only for sending data directly to store from the agent.

[ContainerName <String>]: The container name of the Storage Blob.

[Name <String>]: A friendly name for the destination. This name should be unique across all destinations (regardless of type) within the data collection rule.

[StorageAccountResourceId <String>]: The resource ID of the storage account.

DESTINATIONSTORAGETABLESDIRECT <IStorageTableDestination[]>: List of Storage Table Direct destinations.

[Name <String>]: A friendly name for the destination. This name should be unique across all destinations (regardless of type) within the data collection rule.

[StorageAccountResourceId <String>]: The resource ID of the storage account.

[TableName <String>]: The name of the Storage Table.

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

PS C:\>New-AzDataCollectionRule -Name myCollectionRule1 -ResourceGroupName AMCS-TEST -JsonFilePath .\test\jsonfile\ruleTest1.json

```
# Note: content of .\test\jsonfile\ruleTest1.json
# {
#     "location": "eastus",
#     "properties": {
#         "dataSources": {
#             "performanceCounters": [
#             {
#                 "streams": [
#                     "Microsoft-InsightsMetrics"
#                 ],
#                 "samplingFrequencyInSeconds": 60,
#                 "counterSpecifiers": [
#                     "\\Processor(_Total)\\% Processor Time"
#                 ],
#                 "name": "perfCounter01"
#             },
#             {
#                 "name": "cloudTeamCoreCounters",
#                 "streams": [
#                   "Microsoft-Perf"
#                 ],
#                 "samplingFrequencyInSeconds": 15,
#                 "counterSpecifiers": [
#                   "\\Processor(_Total)\\% Processor Time",
#                   "\\Memory\\Committed Bytes",
#                   "\\LogicalDisk(_Total)\\Free Megabytes",
#                   "\\PhysicalDisk(_Total)\\Avg. Disk Queue Length"
#                 ]
#               }
#             ]
#         },
#         "destinations": {
#             "azureMonitorMetrics": {
```

```
#             "name": "azureMonitorMetrics-default"
#           }
#       },
#       "dataFlows": [
#           {
#               "streams": [
#                   "Microsoft-InsightsMetrics"
#           ],
#               "destinations": [
#                   "azureMonitorMetrics-default"
#           ]
#           }
#       ]
#   }
# }
```

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

```
PS C:\>$dataflow = New-AzDataFlowObject -Stream Microsoft-InsightsMetrics -Destination azureMonitorMetrics-default

            $windowsEvent = 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)]]"
    $performanceCounter1 = New-AzPerfCounterDataSourceObject -CounterSpecifier "\\Processor(_Total)\\% Processor
Time","\\Memory\\Committed
          Bytes","\\LogicalDisk(_Total)\\Free Megabytes","\\PhysicalDisk(_Total)\\Avg. Disk Queue Length" -Name
cloudTeamCoreCounters -SamplingFrequencyInSecond 15 -Stream
Microsoft-Perf
    $performanceCounter2 = New-AzPerfCounterDataSourceObject -CounterSpecifier "\\Process(_Total)\\Thread Count"
-Name appTeamExtraCounters -SamplingFrequencyInSecond 30
```

-Stream Microsoft-Perf

New-AzDataCollectionRule -Name myCollectionRule1 -ResourceGroupName AMCS-TEST -Location eastus -DataFlow $dataflow -DataSourcePerformanceCounter

$performanceCounter1,$performanceCounter2 -DataSourceWindowsEventLog $windowsEvent -DestinationAzureMonitorMetricName "azureMonitorMetrics-default"

---------- EXAMPLE 3 ----------

PS C:\>$dataflow2 = New-AzDataFlowObject -Stream Microsoft-Perf,Microsoft-Syslog -Destination centralWorkspace

$performanceCounter3 = New-AzPerfCounterDataSourceObject -CounterSpecifier "\\Processor(_Total)\\% Processor Time","\\Memory\\Committed

Bytes","\\LogicalDisk(_Total)\\Free Megabytes","\\PhysicalDisk(_Total)\\Avg. Disk Queue Length" -Name cloudTeamCoreCounters -SamplingFrequencyInSecond 15 -Stream

Microsoft-Perf

$performanceCounter4 = New-AzPerfCounterDataSourceObject -CounterSpecifier "\\Process(_Total)\\Thread Count" -Name appTeamExtraCounters -SamplingFrequencyInSecond 30

-Stream Microsoft-Perf

$windowsEvent1 = New-AzWindowsEventLogDataSourceObject -Name cloudSecurityTeamEvents -Stream Microsoft-WindowsEvent -XPathQuery "Security!*"

$windowsEvent2 = 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)]]"

$logAnalytics = New-AzLogAnalyticsDestinationObject -Name centralWorkspace -WorkspaceResourceId

/subscriptions/9e223dbe-3399-4e19-88eb-0975f02ac87f/resourcegroups/amcs-test/providers/microsoft.operationalinsights/workspaces/amcs-logtest-ws

$cronlog = New-AzSyslogDataSourceObject -FacilityName cron -LogLevel Debug,Critical,Emergency -Name cronSyslog -Stream Microsoft-Syslog

$syslog = New-AzSyslogDataSourceObject -FacilityName syslog -LogLevel Alert,Critical,Emergency -Name syslogBase

-Stream Microsoft-Syslog

New-AzDataCollectionRule -Name myCollectionRule2 -ResourceGroupName AMCS-TEST -Location eastus -DataFlow $dataflow2 -DataSourcePerformanceCounter

$performanceCounter3,$performanceCounter4 -DataSourceWindowsEventLog $windowsEvent1,$windowsEvent2 -DestinationLogAnalytic $logAnalytics -DataSourceSyslog

$cronlog,$syslog

RELATED LINKS

https://learn.microsoft.com/powershell/module/az.monitor/new-azdatacollectionrule