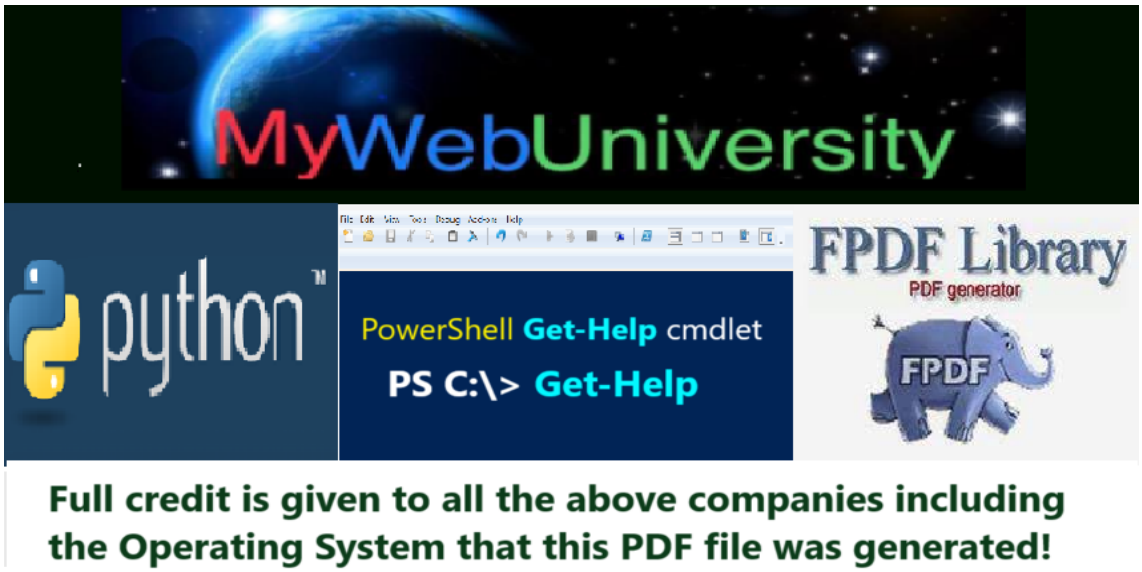

Windows PowerShell Get-Help on Cmdlet 'Get-AzActivityLog'

PS:\>Get-HELP Get-AzActivityLog -Full

NAME

Get-AzActivityLog

SYNOPSIS

Retrieve Activity Log events.

SYNTAX

Get-AzActivityLog [-CorrelationId] <System.String> [-Caller <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-DetailedOutput] [-EndTime <System.Nullable`1[System.DateTime]>] [-MaxRecord <System.Int32>] [-StartTime <System.Nullable`1[System.DateTime]>] [-Status <System.String>] [<CommonParameters>]

Get-AzActivityLog [-ResourceGroupName] <System.String> [-Caller <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-DetailedOutput] [-EndTime <System.Nullable`1[System.DateTime]>] [-MaxRecord <System.Int32>] [-StartTime <System.Nullable`1[System.DateTime]>] [-Status <System.String>] [<CommonParameters>]

Get-AzActivityLog [-ResourceId] <System.String> [-Caller <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-DetailedOutput] [-EndTime <System.Nullable`1[System.DateTime]>] [-MaxRecord <System.Int32>] [-StartTime <System.Nullable`1[System.DateTime]>] [-Status <System.String>] [<CommonParameters>]

Get-AzActivityLog [-ResourceProvider] <System.String> [-Caller <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-DetailedOutput] [-EndTime <System.Nullable`1[System.DateTime]>] [-MaxRecord <System.Int32>] [-StartTime <System.Nullable`1[System.DateTime]>] [-Status <System.String>] [<CommonParameters>]

DESCRIPTION

The Get-AzActivityLog cmdlet retrieve Activity Log events. The events can be associated with the current subscription ID, correlation ID, resource group, resource ID,
or resource provider.

PARAMETERS

-Caller <System.String>

The caller of the events to fetch

Required? false
Position? named
Default value None
Accept pipeline input? True (ByPropertyName)
Accept wildcard characters? false

-CorrelationId <System.String>

The CorrelationId

Required? true

Position? 0

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

-DetailedOutput <System.Management.Automation.SwitchParameter>

Return object with all the details of the events (the default is to return only some attributes, i.e. no detail)

Required? false

Position? named

Default value False

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-EndTime <System.Nullable`1[System.DateTime]>

The endTime of the query

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-MaxRecord <System.Int32>

The maximum number of records to fetch. Alias: MaxRecords, MaxEvents

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ResourceGroupName <System.String>

The resource group name

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ResourceId <System.String>

The ResourceId

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ResourceProvider <System.String>

The ResourceProvider name

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-StartTime <System.Nullable`1[System.DateTime]>

The startTime of the query

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Status <System.String>

The status of the events to fetch

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

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

System.Nullable`1[[System.DateTime, System.Private.CoreLib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=7cec85d7bea7798e]]

System.String

System.Management.Automation.SwitchParameter

System.Int32

OUTPUTS

Microsoft.Azure.Commands.Insights.OutputClasses.PSEventData

NOTES

-------- Example 1: Get an event log by subscription ID --------

Get-AzActivityLog

This command lists at most 1000 events associated with the user's subscription ID that took place 7 days from the current date/time.

Example 2: Get an event log by subscription ID with a maximum number of events

Get-AzActivityLog -MaxRecord 100

This command lists at most 100 events associated with the user's subscription ID that took place 7 days from the current date/time.

Example 3: Get an event log by subscription ID with a start time.

Get-AzActivityLog -StartTime 2017-06-01T10:30

This command lists at most 1000 events associated with the user's subscription ID that took place on or after 2017-06-01T10:30 local time if that date/time is not

older than 90 days from the current date/time.

Example 4: Get an event log by subscription ID with a start time and end time.

Get-AzActivityLog -StartTime 2017-04-01T10:30 -EndTime 2017-04-14T11:30

This command lists at most 1000 of the events associated with the user's subscription ID that took place on or after 2017-04-01T10:30 local time, and before

2017-04-14T11:30 local time if the whole date/time range is not older than 90 days from the current date/time, i.e.: the retention period.

-------- Example 5: Get an event log by correlation ID --------

Get-AzActivityLog -CorrelationId "60c694d0-e46f-4c12-bed1-9b7aef541c23"

This command lists at most 1000 events associated with the specified correlation ID that took place 7 days from the current date/time. NOTE : this is usually only one

event.

Example 6: Get an event log by correlation ID with a maximum number of events

Get-AzActivityLog -CorrelationId "60c694d0-e46f-4c12-bed1-9b7aef541c23" -MaxRecord 100

This command lists at most 100 events associated with the specified correlation ID that took place 7 days from the current date/time. NOTE : this is usually only one

event.

- Example 7: Get an event log by correlation ID and start time -

Get-AzActivityLog -CorrelationId "60c694d0-e46f-4c12-bed1-9b7aef541c23" -StartTime 2017-05-22T04:30:00

This command lists at most 1000 events associated with the specified correlation ID that took place on or after 2017-05-22T04:30:00 local time if the start time is

not older than 90 days from the current date/time. NOTE : this is usually only one event.

Example 8: Get an event log by correlation ID with start time and end time

Get-AzActivityLog -CorrelationId "60c694d0-e46f-4c12-bed1-9b7aef541c23" -StartTime 2017-04-15T04:30:00 -EndTime 2017-04-25T12:30:00

This command lists at most 1000 events associated with the specified correlation ID that took place on or after 2017-04-15T04:30 local time, but before

2017-04-25T12:30 local time if the whole date/time range is not older than 90 days from the current date/time, i.e.: the retention period.

------- Example 9: Get an event log for a resource group -------

Get-AzActivityLog -ResourceGroupName "Contoso-Web-CentralUS"

This command lists at most 1000 the events associated with the specified resource group that took place 7 days from the current date/time.

Example 10: Get an event log for a resource group with a maximum number of events

Get-AzActivityLog -ResourceGroup "Contoso-Web-CentralUS" -MaxRecord 100

This command lists at most 100 events associated with the specified resource group that took place 7 days from the current date/time.

Example 11: Get an event log for a resource group by start time

Get-AzActivityLog -ResourceGroup "Contoso-Web-CentralUS" -StartTime 2017-05-22T04:30:00

This command lists at most 1000 events associated with the specified resource group that took place on or after 2017-05-22T04:30:00 local time if the start time is
not older than 90 days from the current date/time.

Example 12: Get an event log for a resource group with a start time and end time

Get-AzActivityLog -ResourceGroup "Contoso-Web-CentralUS" -StartTime 2017-04-15T04:30 -EndTime 2017-04-25T12:30

This command lists at most 1000 events associated with the specified resource group that took place on or after 2017-04-15T04:30 local time, but before
2017-04-25T12:30 local time if the whole date/time range is not older than 90 days from the current date/time, i.e.: the retention period.

--------- Example 13: Get an event log by resource ID ---------

Get-AzActivityLog -ResourceId "/subscriptions/623d50f1-4fa8-4e46-a967-a9214aed43ab/ResourceGroups/Contoso-Web-CentralUS/providers/Microsoft.Web/ServerFarms/Contoso1"

This command lists at most 1000 events associated with the specified resource ID that took place 7 days from the current date/time.

Example 14: Get an event log by resource ID with a maximum number of events

```
Get-AzActivityLog -ResourceId "/subscriptions/623d50f1-4fa8-4e46-a967-a9214aed43ab/ResourceGroups/Contoso-Web-CentralUS/providers/Microsoft.Web/ServerFarms/Contoso1"
-MaxRecord 100
```

This command lists at most 100 events associated with the specified resource ID that took place 7 days from the current date/time.

Example 15: Get an event log by resource ID with a start time

```
Get-AzActivityLog -ResourceId "/subscriptions/623d50f1-4fa8-4e46-a967-a9214aed43ab/ResourceGroups/Contoso-Web-CentralUS/providers/Microsoft.Web/ServerFarms/Contoso1"
-StartTime 2017-05-22T04:30
```

This command lists at most 1000 events associated with the specified resource ID that took place on or after 2017-05-22T04:30:00 local time if the start time is not
older than 90 days from the current date/time.

Example 16: Get an event log by resource ID with a start time and end time

```
Get-AzActivityLog -ResourceId "/subscriptions/623d50f1-4fa8-4e46-a967-a9214aed43ab/ResourceGroups/Contoso-Web-CentralUS/providers/Microsoft.Web/ServerFarms/Contoso1"
```

-StartTime 2017-04-15T04:30 -EndTime 2017-04-25T12:30

This command lists at most 1000 events associated with the specified resource ID that took place on or after 2017-04-15T04:30 local time, but before 2017-04-25T12:30

local time if the whole date/time range is not older than 90 days from the current date/time, i.e.: the retention period.

------ Example 17: Get an event log by resource provider ------

Get-AzActivityLog -ResourceProvider "Microsoft.Web"

This command lists at most 1000 events associated with the specified resource provider that took place 7 days from the current date/time.

Example 18: Get an event log by resource provider with a maximum number of events

Get-AzActivityLog -ResourceProvider "Microsoft.Web" -MaxRecord 100

This command lists at most 100 events associated with the specified resource provider that took place 7 days from the current date/time.

Example 19: Get an event log by resource provider with a start time

Get-AzActivityLog -ResourceProvider "Microsoft.Web" -StartTime 2017-05-22T04:30

This command lists at most 1000 events associated with the specified resource provider that took place on or after 2017-05-22T04:30:00 local time if the start time

is not older than 90 days from the current date/time.

Example 20: Get an event log by resource provider with a start time and end time

```
Get-AzActivityLog -ResourceProvider "Microsoft.Web" -StartTime 2017-04-15T04:30 -EndTime 2017-04-25T12:30
```

This command lists at most 1000 events associated with the specified resource provider that took place on or after 2017-04-15T04:30 local time, but before

2017-04-25T12:30 local time if the whole date/time range is not older than 90 days from the current date/time, i.e.: the retention period.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.monitor/get-azactivitylog