
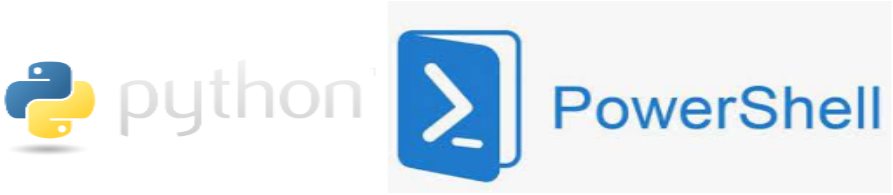


*Full credit is given to the above companies including the OS that this PDF file was generated!*

***PowerShell Get-Help on command 'New-WinEvent'***

***PS C:\Users\wahid> Get-Help New-WinEvent***

NAME

New-WinEvent

SYNOPSIS

Creates a new Windows event for the specified event provider.

SYNTAX

New-WinEvent [-ProviderName] <System.String> [-Id] <System.Int32> [[-Payload] <System.Object[]>] [-Version <System.Byte>] [<CommonParameters>]

DESCRIPTION

The `New-WinEvent` cmdlet creates an Event Tracing for Windows (ETW) event for an event provider. You can use this cmdlet to add events to ETW channels from PowerShell.

PARAMETERS

-Id <System.Int32>

Specifies an event Id that is registered in the event provider.

-Payload <System.Object[]>

The payload is an array of values passed as positional arguments to the event template. The values are inserted into the template to construct the message for the event. Events can have multiple template versions that use different formats.

If the values in the payload do not match the types in the template, the event is logged but the payload contains an error.

-ProviderName <System.String>

Specifies the event provider that writes the event to an event log, such as "Microsoft-Windows-PowerShell". An ETW event provider is a logical entity that writes events to ETW sessions.

-Version <System.Byte>

Specifies the version number of the event. PowerShell converts the number to the required Byte type. The value specifies the version of the event when different versions of the same event are defined.

<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).

---------- Example 1 - Create a new event ----------

New-WinEvent -ProviderName Microsoft-Windows-PowerShell -Id 45090 -Payload @("Workflow", "Running")

This command uses the `New-WinEvent` cmdlet to create event 45090 for the Microsoft-Windows-PowerShell provider.

---------- Example 2 - Get the template for an event ----------

```
(Get-WinEvent -ListProvider Microsoft-Windows-GroupPolicy).Events |
Where-Object Id -eq 8007

Id          : 8007
Version     : 0
LogLink     : System.Diagnostics.Eventing.Reader.EventLogLink
Level       : System.Diagnostics.Eventing.Reader.EventLevel
Opcode      : System.Diagnostics.Eventing.Reader.EventOpcode
Task        : System.Diagnostics.Eventing.Reader.EventTask
Keywords    : {}
Template    : <template
xmlns="http://schemas.microsoft.com/win/2004/08/events">
              <data name="PolicyElaspedTimeInSeconds" inType="win:UInt32"
outType="xs:unsignedInt"/>
              <data name="ErrorCode" inType="win:UInt32"
outType="win:HexInt32"/>
              <data name="PrincipalSamName" inType="win:UnicodeString"
outType="xs:string"/>
              <data name="IsMachine" inType="win:Boolean"
outType="xs:boolean"/>
              <data name="IsConnectivityFailure" inType="win:Boolean"
outType="xs:boolean"/>
            </template>

Description : Completed periodic policy processing for user %3 in %1 seconds.

Id          : 8007
Version     : 1
LogLink     : System.Diagnostics.Eventing.Reader.EventLogLink
Level       : System.Diagnostics.Eventing.Reader.EventLevel
Opcode      : System.Diagnostics.Eventing.Reader.EventOpcode
```

```
Task        : System.Diagnostics.Eventing.Reader.EventTask
Keywords    : {}
Template    : <template
xmlns="http://schemas.microsoft.com/win/2004/08/events">
              <data name="PolicyElaspedTimeInSeconds" inType="win:UInt32"
outType="xs:unsignedInt"/>
              <data name="ErrorCode" inType="win:UInt32"
outType="win:HexInt32"/>
              <data name="PrincipalSamName" inType="win:UnicodeString"
outType="xs:string"/>
              <data name="IsMachine" inType="win:UInt32"
outType="xs:unsignedInt"/>
              <data name="IsConnectivityFailure" inType="win:Boolean"
outType="xs:boolean"/>
            </template>

Description : Completed periodic policy processing for user %3 in %1 seconds.

The Description property contains the message that gets written to the event
log. The `%3` and `%1` value are placeholders for the values passed into the
template. The `%3` string is replace with the value passed to the
PrincipalSamName field. The `%1` string is replaced withe value passed to the
PolicyElaspedTimeInSeconds field.
-- Example 3 - Create a new event using a versioned template --

$Payload = @(300, [uint32]'0x8001011f', $env:USERNAME, 0, 1)
New-WinEvent -ProviderName Microsoft-Windows-GroupPolicy -Id 8007 -Version 1
-Payload $Payload
Get-winEvent -ProviderName Microsoft-Windows-GroupPolicy -MaxEvents 1

ProviderName: Microsoft-Windows-GroupPolicy

TimeCreated             Id LevelDisplayName Message
```

```
-----------          -- ---------------- -------
5/4/2022 8:40:24 AM  8007 Information      Completed periodic policy
processing for user User1 in 300 seconds
```

If the values in the payload do not match the types in the template, the event is logged but the payload contains an error.

REMARKS

To see the examples, type: "get-help New-WinEvent -examples".

For more information, type: "get-help New-WinEvent -detailed".

For technical information, type: "get-help New-WinEvent -full".

For online help, type: "get-help New-WinEvent -online"