



python



PowerShell

FPDF Library
PDF generator

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

PowerShell Get-Help on command 'New-EventLog'

PS C:\Users\wahid> Get-Help New-EventLog

NAME

New-EventLog

SYNOPSIS

Creates a new event log and a new event source on a local or remote computer.

SYNTAX

```
New-EventLog [-LogName] <System.String> [-Source] <System.String[]>  
[[-ComputerName] <System.String[]>] [-CategoryResourceFile <System.String>]  
[-MessageResourceFile <System.String>] [-ParameterResourceFile  
<System.String>] [<CommonParameters>]
```

DESCRIPTION

This cmdlet creates a new classic event log on a local or remote computer. It can also register an event source that writes to the new log or to an existing log.

The cmdlets that contain the `EventLog` noun (the Event log cmdlets) work only on classic event logs. To get events from logs that use the Windows Event Log

technology in Windows Vista and later versions of Windows, use ``Get-WinEvent``.

PARAMETERS

`-CategoryResourceFile <System.String>`

Specifies the path to the file that contains category strings for the source events. This file is also known as the Category Message File.

The file must be present on the computer on which the event log is being created. This parameter does not create or move files.

`-ComputerName <System.String[]>`

Creates the new event logs on the specified computers. The default is the local computer.

The NetBIOS name, IP address, or fully qualified domain name of a remote computer. To specify the local computer, type the computer name, a dot (``.``), or ``localhost``.

This parameter does not rely on PowerShell remoting. You can use the `ComputerName` parameter of ``Get-EventLog`` even if your computer is not configured to run remote commands.

`-LogName <System.String>`

Specifies the name of the event log.

If the log does not exist, ``New-EventLog`` creates the log and uses this value for the `Log` and `LogDisplayName` properties of the new event log. If the log exists, ``New-EventLog`` registers a new source for the event log.

`-MessageResourceFile <System.String>`

Specifies the path to the file that contains message formatting strings for the source events. This file is also known as the Event Message File.

The file must be present on the computer on which the event log is being created. This parameter does not create or move files.

`-ParameterResourceFile <System.String>`

Specifies the path to the file that contains strings used for parameter substitutions in event descriptions. This file is also known as the Parameter Message File.

The file must be present on the computer on which the event log is being created. This parameter does not create or move files.

`-Source <System.String[]>`

Specifies the names of the event log sources, such as application programs that write to the event log. This parameter is required.

`<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 log -----

```
New-EventLog -source TestApp -LogName TestLog -MessageResourceFile
C:\Test\TestApp.dll
```

---- Example 2 - add a new event source to an existing log ----

```
$file = "C:\Program Files\TestApps\NewTestApp.dll"
New-EventLog -ComputerName Server01 -Source NewTestApp -LogName Application
-MessageResourceFile $file -CategoryResourceFile $file
```

The command requires that the `NewTestApp.dll` file is located on the Server01 computer.

REMARKS

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

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

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

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