



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 'Clear-EventLog'

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

NAME

Clear-EventLog

SYNOPSIS

Clears all entries from specified event logs on the local or remote computers.

SYNTAX

```
Clear-EventLog [-LogName] <System.String[]> [[-ComputerName]
<System.String[]>] [-Confirm] [-WhatIf] [<CommonParameters>]
```

DESCRIPTION

The `Clear-EventLog` cmdlet deletes all of the entries from the specified event logs on the local computer or on remote computers. To use `Clear-EventLog`, you must be a member of the Administrators group on the affected computer.

The cmdlets that contain the `EventLog` noun (the `EventLog` 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 the

``Get-WinEvent` cmdlet.`

PARAMETERS

`-ComputerName <System.String[]>`

Specifies a remote computer. The default is the local computer.

Type the NetBIOS name, an Internet Protocol (IP) address, or a 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 Windows 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 event logs. Enter the log name (the value of the `Log` property not the `LogDisplayName`) of one or more event logs, separated by commas. Wildcard characters are not permitted. This parameter is required.

> [!IMPORTANT] > This parameter is supposed to accept values from the pipeline by property name. However, there is > a bug that prevents this from working. You must pass a value using the parameter directly.

`-Confirm <System.Management.Automation.SwitchParameter>`

Prompts you for confirmation before running the cmdlet.

`-WhatIf <System.Management.Automation.SwitchParameter>`

Shows what would happen if the cmdlet runs. The cmdlet is not run.

`<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) (https://go.microsoft.com/fwlink/?LinkID=113216).

Example 1: Clear specific event log types from the local computer

```
Clear-EventLog "Windows PowerShell"
```

This command clears the entries from the Windows PowerShell event log on the local computer.

Example 2: Clear specific multiple log types from the local and remote computers

```
Clear-EventLog -LogName ODiag, OSession -ComputerName localhost, Server02
```

This command clears all of the entries in the Microsoft Office Diagnostics (ODiag) and Microsoft Office Sessions (OSession) logs on the local computer and the Server02 remote computer.

Example 3: Clear all logs on the specified computers then display the event log list

```
Clear-EventLog -LogName application, system -confirm
```

This command prompts you for confirmation before deleting the entries in the specified event logs.

Example 4: Clear all logs on the specified computers then display the event log list

```
function clear-all-event-logs ($computerName="localhost")
{
    $logs = Get-EventLog -ComputerName $computername -List | ForEach-Object
    {$_ .Log}
    $logs | ForEach-Object {Clear-EventLog -ComputerName $computername -LogName
    $_ }
```

```
Get-EventLog -ComputerName $computername -list
}
```

```
clear-all-event-logs -ComputerName Server01
```

Max(K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	0	Application
15,168	0	OverwriteAsNeeded	0	DFS Replication
512	7	OverwriteOlder	0	DxStudio
20,480	0	OverwriteAsNeeded	0	Hardware Events
512	7	OverwriteOlder	0	Internet Explorer
20,480	0	OverwriteAsNeeded	0	Key Management Service
16,384	0	OverwriteAsNeeded	0	Microsoft Office Diagnostics
16,384	0	OverwriteAsNeeded	0	Microsoft Office Sessions
30,016	0	OverwriteAsNeeded	1	Security
15,168	0	OverwriteAsNeeded	2	System
15,360	0	OverwriteAsNeeded	0	Windows PowerShell

This function clears all event logs on the specified computers and then displays the resulting event log list.

Notice that a few entries were added to the System and Security logs after the logs were cleared but before they were displayed.

REMARKS

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

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

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

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