PowerShell Get-Help on command 'Limit-EventLog'

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

NAME

Limit-EventLog

SYNOPSIS

Sets the event log properties that limit the size of the event log and the age

of its entries.

SYNTAX

Limit-EventLog [-LogName] <System.String[]> [-ComputerName <System.String[]>]

[-MaximumSize <System.Int64>] [-OverflowAction {OverwriteOlder |

OverwriteAsNeeded | DoNotOverwrite}] [-RetentionDays <System.Int32>]

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

DESCRIPTION

The `Limit-EventLog` cmdlet sets the maximum size of a classic event log, how

long each event must be retained, and what happens when the log reaches its

maximum size. You can use it to limit the event logs on local or remote

computers.

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 `Get-WinEvent`.

PARAMETERS

  -ComputerName <System.String[]>

    Specifies remote computers. The default is the local computer.

    Type the NetBIOS name, an Internet Protocol (IP) address, or a fully qualified domain name (FQDN) 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 `Limit-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.

  -MaximumSize <System.Int64>

    Specifies the maximum size of the event logs in bytes. Enter a value between 64 kilobytes (KB) and 4 gigabytes (GB). The value must be divisible by 64 KB (65536).

    This parameter specifies the value of the MaximumKilobytes property of the System.Diagnostics.EventLog object that represents a classic event log.

  -OverflowAction <System.Diagnostics.OverflowAction>

    Specifies what happens when the event log reaches its maximum size.

The acceptable values for this parameter are:

- `DoNotOverwrite`: Existing entries are retained and new entries are discarded.

- `OverwriteAsNeeded`: Each new entry overwrites the oldest entry.

- `OverwriteOlder`: New events overwrite events older than the value specified by the MinimumRetentionDays property. If there are no events older than specified by the MinimumRetentionDays property value, new events are discarded.

This parameter specifies the value of the OverflowAction property of the System.Diagnostics.EventLog object that represents a classic event log.

-RetentionDays <System.Int32>
  Specifies the minimum number of days that an event must remain in the event log.

  This parameter specifies the value of the MinimumRetentionDays property of the System.Diagnostics.EventLog object that represents a classic event log.

-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).

--------- Example 1: Increase the size of an event log ---------

Limit-EventLog -LogName "Windows PowerShell" -MaximumSize 20KB

This command increases the maximum size of the Windows PowerShell event log on the local computer to 20480 bytes (20 KB).

--- Example 2: Retain an event log for a specified duration ---

Limit-EventLog -LogName Security -ComputerName "Server01", "Server02"
-RetentionDays 7

This command ensures that events in the Security log on the Server01 and Server02 computers are retained for at least 7 days.

--- Example 3: Change the overflow action of all event logs ---

$Logs = Get-EventLog -List | ForEach {$_.log}
Limit-EventLog -OverflowAction OverwriteOlder -LogName $Logs
Get-EventLog -List

Max(K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteOlder	3,412	Application
512	0	OverwriteOlder	0	DFS Replication
512	0	OverwriteOlder	17	DxStudio
10,240	7	OverwriteOlder	0	HardwareEvents
512	0	OverwriteOlder	0	Internet Explorer
512	0	OverwriteOlder	0	Key Management Service
16,384	0	OverwriteOlder	4	ODiag
16,384	0	OverwriteOlder	389	OSession Security
15,168	0	OverwriteOlder	19,360	System
15,360	0	OverwriteOlder	15,828	Windows PowerShell

This example changes the overflow action of all event logs on the local computer to OverwriteOlder.

The first command gets the log names of all of the logs on the local computer. The second command sets the overflow action. The third command displays the results.

REMARKS

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

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

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

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