

Finding Needles: Better Event Log Management with PowerShell

Jeff Hicks
Learning Architect

Level: Intermediate

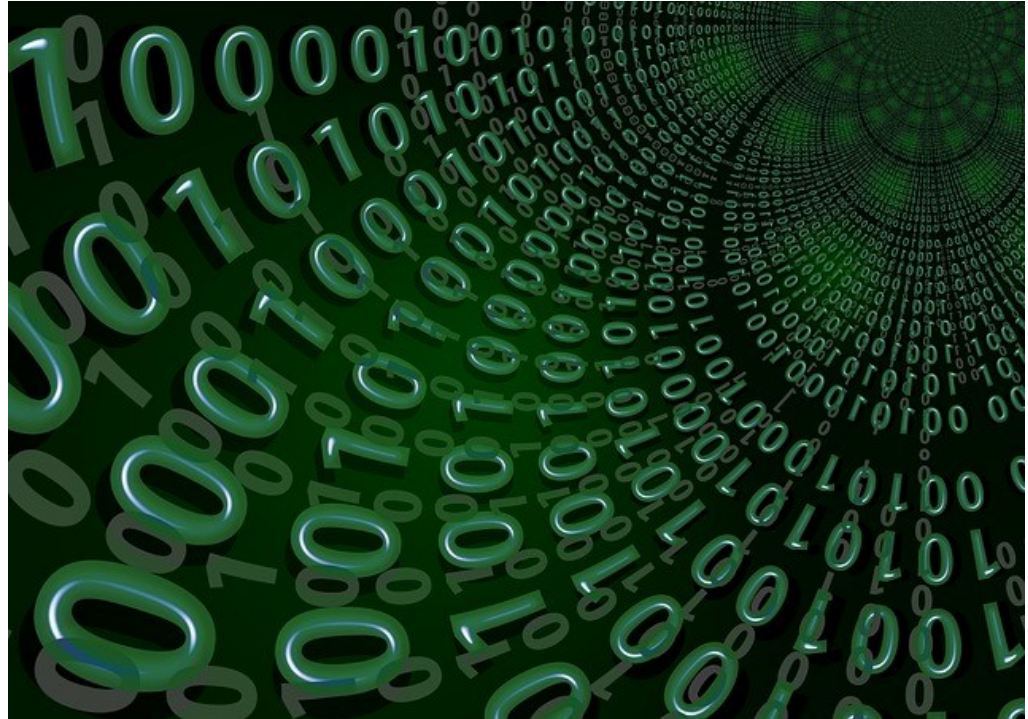
PS C:\> whoami

- Veteran IT Pro
- Microsoft MVP
- Author
- Teacher
- <https://jdhitsolutions.github.io>



Eternal Event Logs

- Event log management is critical
 - Security
 - Availability
 - Configuration
 - Performance
- Use management tools where available
- Build your own with PowerShell





Legacy Management

```
PS C:\> Get-Eventlog system -EntryType Error -Newest 10
```

Index	Time	EntryType	Source	InstanceID	Message
----	----	-----	-----	-----	-----
4230	Oct 08 07:19	Error	Microsoft-Windows...	1129	The processing of Group Policy failed because o...
4223	Oct 08 07:19	Error	Microsoft-Windows...	1129	The processing of Group Policy failed because o...
4220	Oct 08 07:19	Error	NETLOGON	5719	This computer was not able to set up a secure s...
4173	Oct 08 07:19	Error	EventLog	2147489656	The previous system shutdown at 6:24:40 AM on ...
3566	Sep 28 00:22	Error	Service Control M...	3221232506	The OpenSSH SSH Server service terminated unexp...
3537	Sep 27 12:51	Error	Microsoft-Windows...	20	Installation Failure: Windows failed to install...
3532	Sep 27 12:47	Error	Microsoft-Windows...	20	Installation Failure: Windows failed to install...
3441	Sep 27 12:35	Error	Microsoft-Windows...	1129	The processing of Group Policy failed because o...
3436	Sep 27 12:35	Error	Microsoft-Windows...	1129	The processing of Group Policy failed because o...
3433	Sep 27 12:35	Error	NETLOGON	5719	This computer was not able to set up a secure s...

Get-EventLog

- Limited to classic event logs
- Uses legacy protocols
- Not an option in PowerShell 7
- Consider it deprecated
 - Win32_NTEventLogFile



NAME

Get-WinEvent

SYNOPSIS

Gets events from event logs and event tracing log files on local and remote computers.

SYNTAX

```
Get-WinEvent [[-LogName] <System.String[]>] [-ComputerName <System.String>] [-Credential  
<System.Management.Automation.PSCredential>] [-FilterXPath <System.String>] [-Force] [-MaxEvents <System.Int64>]  
[-Oldest] [<CommonParameters>]
```

```
Get-WinEvent [-ListLog] <System.String[]> [-ComputerName <System.String>] [-Credential  
<System.Management.Automation.PSCredential>] [-Force] [<CommonParameters>]
```

```
Get-WinEvent [-ListProvider] <System.String[]> [-ComputerName <System.String>] [-Credential  
<System.Management.Automation.PSCredential>] [<CommonParameters>]
```

```
Get-WinEvent [-ProviderName] <System.String[]> [-ComputerName <System.String>] [-Credential  
<System.Management.Automation.PSCredential>] [-FilterXPath <System.String>] [-Force] [-MaxEvents <System.Int64>]  
[-Oldest] [<CommonParameters>]
```

```
Get-WinEvent [-FilterHashtable] <System.Collections.Hashtable[]> [-ComputerName <System.String>] [-Credential  
<System.Management.Automation.PSCredential>] [-Force] [-MaxEvents <System.Int64>] [-Oldest] [<CommonParameters>]
```

```
Get-WinEvent [-FilterXml] <System.Xml.XmlDocument> [-ComputerName <System.String>] [-Credential  
<System.Management.Automation.PSCredential>] [-MaxEvents <System.Int64>] [-Oldest] [<CommonParameters>]
```

```
Get-WinEvent [-Path] <System.String[]> [-Credential <System.Management.Automation.PSCredential>] [-FilterXPath  
<System.String>] [-MaxEvents <System.Int64>] [-Oldest] [<CommonParameters>]
```



Show Me

Session Survey

- Your feedback is very important to us
- Please take a moment to complete the session survey found in the mobile app
- Use the QR code or search for “Converge360 Events” in your app store
- Find this session on the Agenda tab
- Click “Session Evaluation”
- Thank you!



Questions and Answers

