Tool #2: Log Investigator

Adam Bertram
Microsoft MVP

adamtheautomator.com Twitter: @adbertram

Tool Overview

Troubleshooting

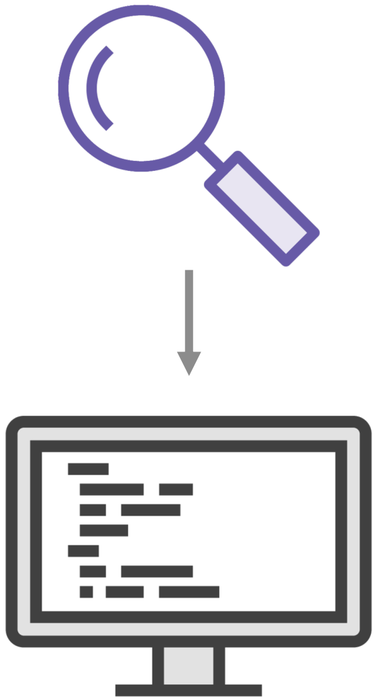
Prerequisites

PowerShell v7+

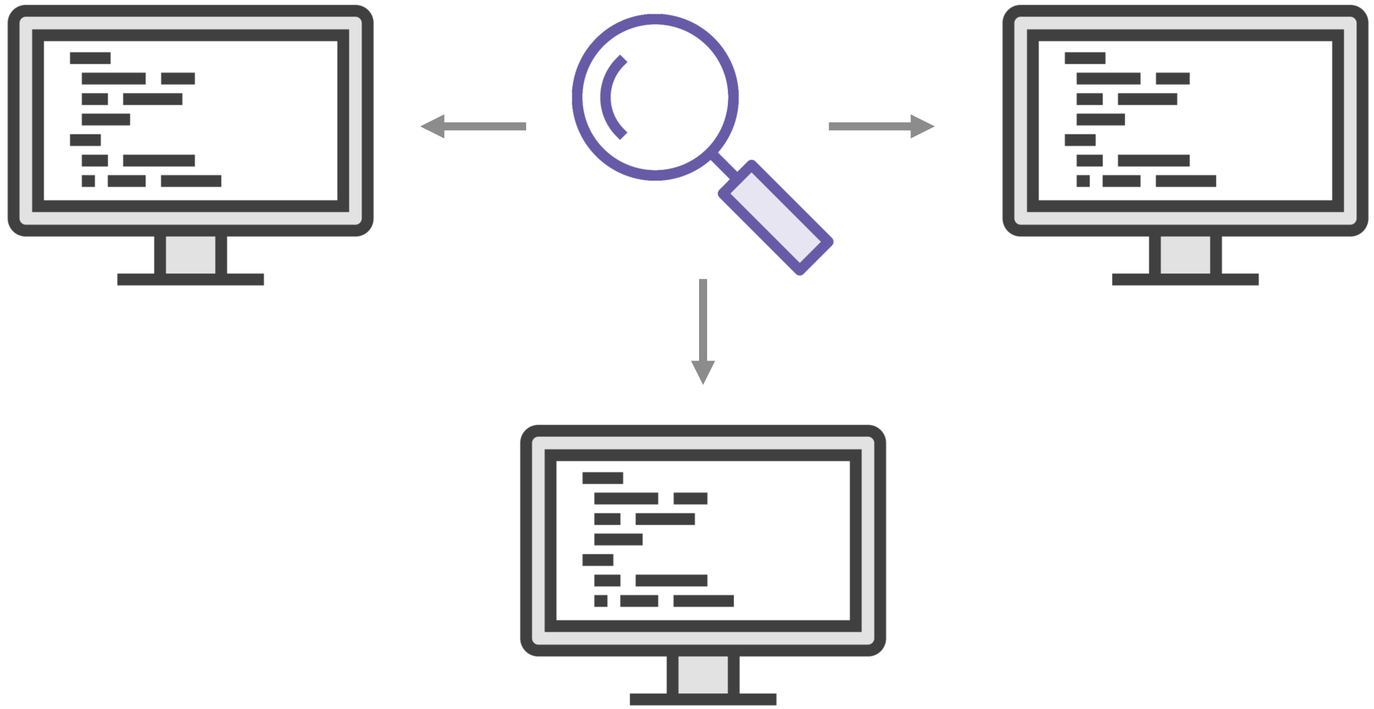
Administrative privileges

Interrogating Windows Event Logs

Get-EventLog cmdlet



Log Investigator tool



Interrogating Text Logs

Text logs

Search for log files that were last written to within the specified time period

Name	Last Modified ▼
########.log	########
########.log	########
########.log	########
########.log	########
########.log	########
########.log	########
########.log	########

Building the Tool Set

Scripts → Functions

Reusability

Functions → Module

Takeaways

Get-EventLog cmdlet is more common than the Get-WinEvent cmdlet

Get-WinEvent has a drastic performance improvement over Get-EventLog

Summary

Created the Log Investigator tool

Scan Multiple Log sources

Get Logs within a specified timeframe