

Monitoring Events and Troubleshooting



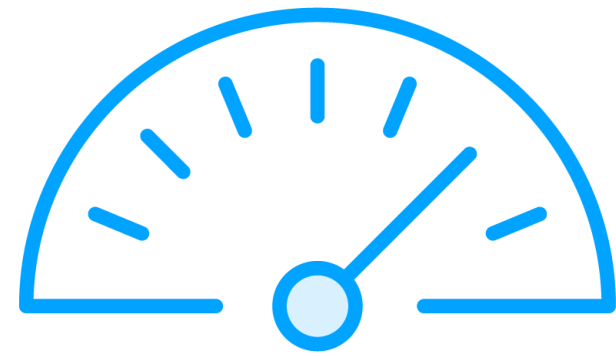
Adam Bertram

6x Microsoft MVP

adamtheautomator.com Twitter/X: @adbertram



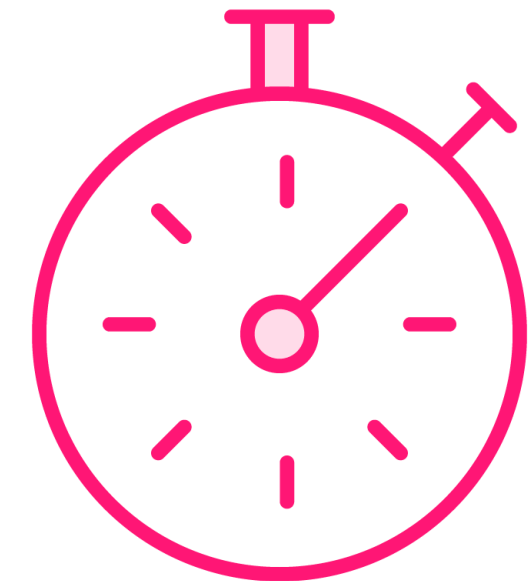
Real-time Server Health Monitoring



**Monitor performance
counters**



Analyze event logs



Identify issues quickly



CPU Monitoring in Action



Performance issues with a critical application

Sluggish response on a set schedule

Let's investigate the CPU utilization



Key Server Performance Metrics



CPU load trends



Available memory and swap utilization



Disk I/O operations



Network throughput



Collecting Server Performance Metrics



Collecting CPU utilization metrics

Retrieving available memory data

Monitoring disk latency counters

Tracking network traffic stats



Monitoring File System Activity with WMI Events



Create a WMI event filter to watch for changes in a specific directory.

Use Register-CimIndicationEvent to listen for these changes.

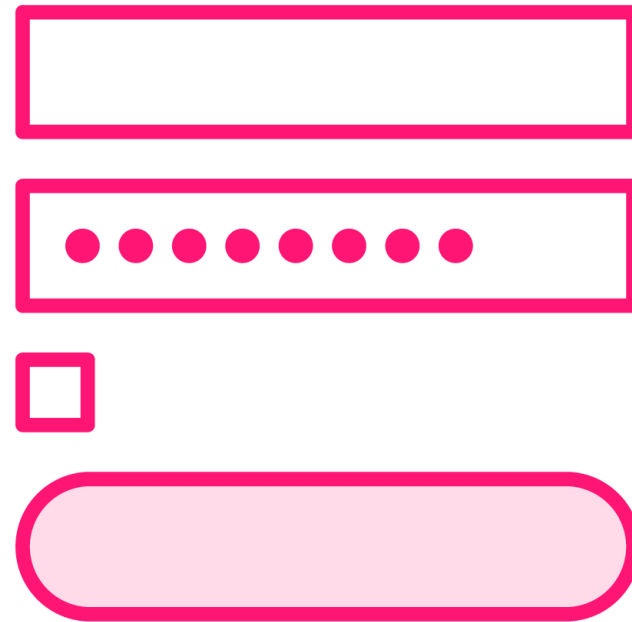
Write an action script block that logs the details of any file system change to a log file.



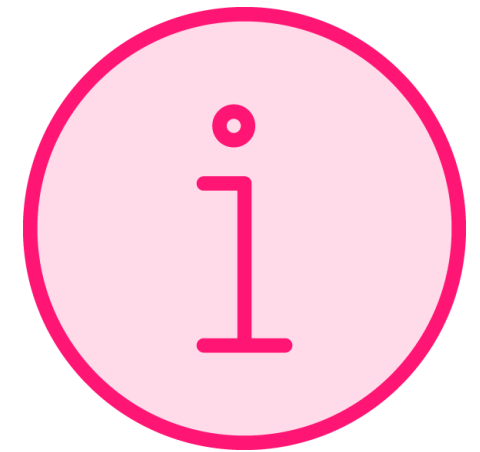
Event Logs for Server Monitoring



**Application crashes or
timeouts in IIS sites**



**Logon failures for
disabled AD accounts**



**System resource
exhaustion events**



Auditing Failed Logons

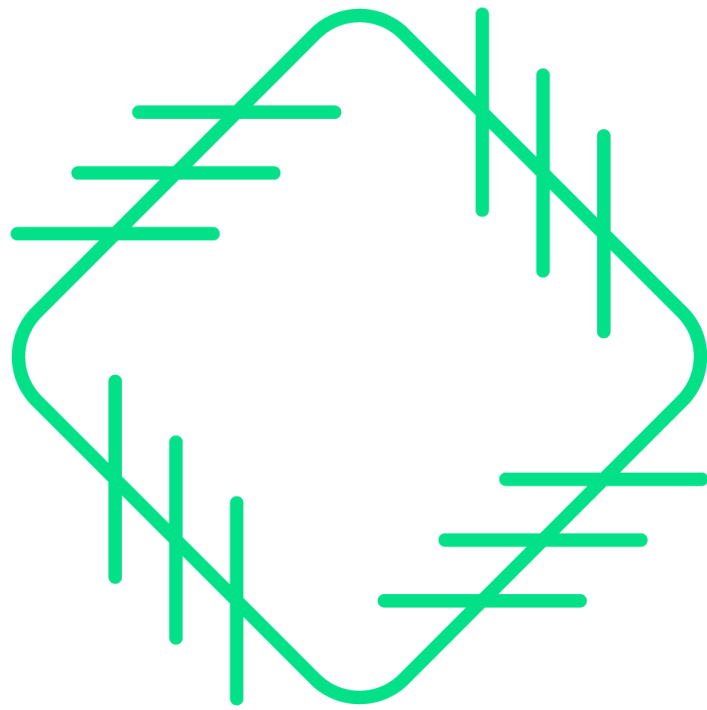


Failed login attempts

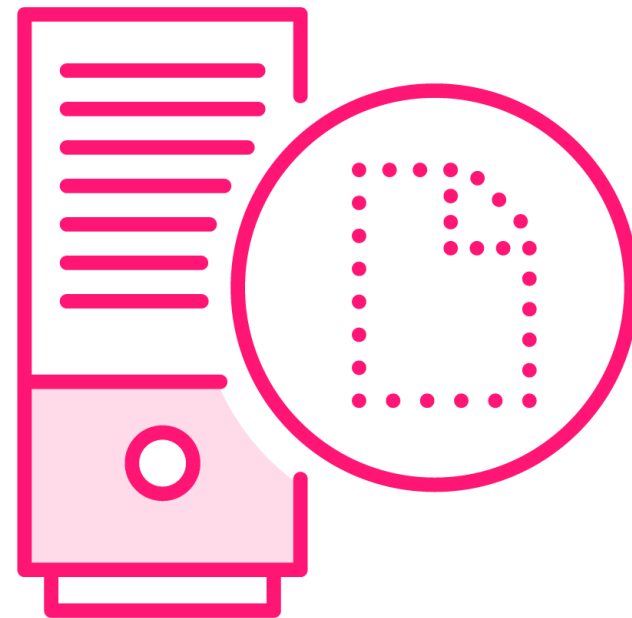
Let's do some inspecting



Resetting Update Components

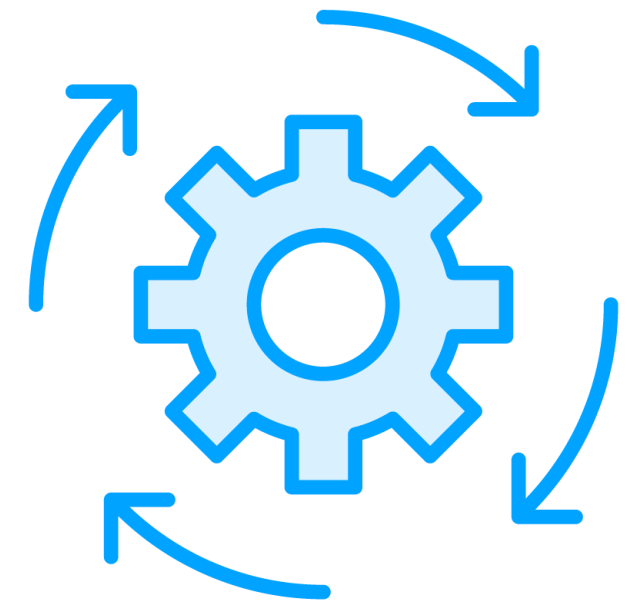


When and Why



Steps

Clear the cache
Reset services
Trigger new scan



PSWindowsUpdate



Troubleshooting Failed Updates



Identify failed updates

Determine failure reasons

Reset components with PSWindowsUpdate

