# Windows 11 System Monitoring and Services Management Lab

Objective:
Learn to use Event Viewer to monitor system events, manage services to understand their impact, and configure System Tools to monitor and record system usage.

## Part 1: Event Viewer - Monitor Windows Defender Service Changes

Objective: Use Event Viewer to observe changes in the Windows Defender service status.

1. Open Event Viewer:
  - Press Win + X and select Event Viewer, or search for "Event Viewer" in the Windows search bar.

2. Navigate to Windows Defender Events:
  - In Event Viewer, expand Applications and Services Logs > Microsoft > Windows > Windows Defender.
  - Select Operational to see a log of events related to Windows Defender.

3. Start and Stop Windows Defender Service:
  - Open Settings > Privacy & Security > Windows Security > Virus & threat protection.
  - In Virus & threat protection settings, toggle off Real-time protection (you may need administrative privileges to do this).
  - Wait a few moments, then toggle Real-time protection back on.

4. Observe Changes in Event Viewer:
  - Return to Event Viewer and refresh the Windows Defender Operational log.
  - Look for entries related to the service status change, noting the timestamp and event details.

Practice Questions:
  - What types of events does Windows Defender log in Event Viewer?
  - How can monitoring Event Viewer help identify security-related issues with Windows Defender?

## Part 2: Explore the Impact of Services - Print Spooler Service

Objective: Disable the Print Spooler service to observe its impact on system functionality.

1. Open Services Manager:

- Press Win + R, type services.msc, and press Enter.

2. Locate and Stop the Print Spooler Service:
- In the Services window, scroll down to find Print Spooler.
- Right-click on Print Spooler and select Stop. This action will disable the service responsible for managing print jobs.

3. Observe System Changes:
- Go to Settings > Bluetooth & devices > Printers & scanners.
- You should see that printers and scanners are no longer listed or accessible. Attempting to print will result in an error, as the Print Spooler service is required for printing functionality.

4. Restart the Print Spooler Service:
- Return to the Services window, right-click on Print Spooler, and select Start.
- Verify that printers and scanners are now available in Printers & scanners settings.

Practice Questions:
- Why is the Print Spooler service important in a networked or shared environment?
- What other system functionalities could be impacted by stopping critical services?

## Part 3: Monitor and Record System Usage with System Tools

Objective: Use System Tools in Windows to monitor and record system resource usage, gaining insights into performance and resource demands.

1. Open Performance Monitor:
- Press Win + R, type perfmon, and press Enter to open Performance Monitor.

2. Configure Resource Monitoring:
- In Performance Monitor, expand Monitoring Tools and select Performance Monitor.
- Click the + icon to add performance counters. Choose counters such as Processor (_Total), Memory, Disk, and Network Adapter to monitor resource usage.
- Click Add >> for each counter, then click OK to begin monitoring these metrics in real-time.

3. Record System Performance Over Time:
- In Performance Monitor, right-click on Performance Monitor in the left pane and select New > Data Collector Set.
- Name the data collector set (e.g., “System Usage Monitor”) and select Create manually (Advanced), then click Next.
- Choose Performance counter and add the counters you configured earlier. Click Next and

choose a destination to save the log file.
  - Click Finish to start recording system usage data.

4. Review Collected Data:
  - Allow the data collector set to run for a period (e.g., 10 minutes) to gather performance data.
  - In Performance Monitor, navigate to the saved log location, right-click on the log file, and select View to review the recorded data and observe resource usage patterns.

Practice Questions:
  - How can monitoring system performance over time help in diagnosing system bottlenecks?
  - In what scenarios would resource monitoring be particularly useful?

## Final Questions

1. Compare and contrast using Event Viewer and Performance Monitor for system monitoring. What are the advantages of each tool?
2. Describe a scenario where stopping a service could help troubleshoot system issues, and a scenario where stopping a service might create problems.
3. How does monitoring and recording system performance provide insights into application and resource management?