

Windows 11 Advanced System Monitoring and Troubleshooting Lab

Objective:

Learn to monitor, troubleshoot, and manage Windows 11 systems using Task Manager, Event Viewer, Reliability Monitor, Diagnostics and Recovery Toolset, Steps Recorder, and Microsoft Management Console (MMC).

Task 1: Task Manager - Monitor and Manage Processes

Objective: Use Task Manager to monitor system performance, view running processes, and manage applications.

1. Open Task Manager:

- Right-click on the Taskbar and select Task Manager, or press Ctrl + Shift + Esc.

2. Monitor Processes:

- In the Processes tab, observe the list of active applications and background processes.
- Click on a column header (like CPU or Memory) to sort processes by resource usage.

Identify processes using high CPU, memory, or disk resources.

3. Manage Applications:

- Select an application and click End Task to terminate it.
- Right-click on a process and select Go to details to view more detailed information or

Open file location to access the executable file.

4. Check Performance:

- Navigate to the Performance tab to monitor real-time usage of CPU, memory, disk, and network.

- Click each resource (e.g., CPU) to view detailed graphs and metrics.

Practice Questions:

- How can Task Manager help identify resource-hungry applications?
- What types of processes should not be terminated, and why?

Task 2: Event Viewer - Identify System Problems

Objective: Use Event Viewer to identify and diagnose system issues by reviewing system logs.

1. Open Event Viewer:

- Press Win + X and select Event Viewer, or type "Event Viewer" into the Windows search bar.

2. Navigate System Logs:

- In the left pane, expand Windows Logs and click on System to see events related to the operating system.
- Review entries, looking for Error and Warning entries that may indicate system problems.

3. Filter Events:

- Right-click on the System log and select Filter Current Log.
- Set the Event level to Error and Warning to display critical events only, then click OK.

4. Examine Event Details:

- Click on any event to view detailed information about the issue in the General and Details tabs.

Practice Questions:

- What are some common types of system errors you might find in Event Viewer?
- How can Event Viewer help troubleshoot recurring system issues?

Task 3: Reliability Monitor - Track System Stability

Objective: Use Reliability Monitor to track system stability and view historical system events.

1. Open Reliability Monitor:

- Go to Control Panel > System and Security > Security and Maintenance > Maintenance > View reliability history.

2. Review Stability Chart:

- The Reliability Monitor displays a stability chart with a timeline of events. Look for red X's or yellow triangles indicating critical errors or warnings.

3. View Event Details:

- Click on any day with events to view specific issues. Events include Application Failures, Windows Failures, and Miscellaneous Failures.
- Select an event and review the summary to understand the issue.

4. Generate a Reliability Report:

- Click View all problem reports to generate a full list of recent issues and crashes, making it easier to identify patterns over time.

Practice Questions:

- How does Reliability Monitor differ from Event Viewer?
- How can tracking stability over time be helpful in identifying hardware or software issues?

Task 4: Diagnostics and Recovery Toolset - Troubleshoot and Recover from Issues

Objective: Use Diagnostics and Recovery Toolset (DaRT) to troubleshoot and recover from serious system issues.

Note: Microsoft DaRT is part of the Microsoft Desktop Optimization Pack (MDOP) and may need to be installed separately.

1. Open Diagnostics and Recovery Toolset:

- Boot into DaRT by restarting your computer and booting from the DaRT recovery media (e.g., a USB drive with DaRT installed).

2. Use Recovery Tools:

- In the DaRT menu, explore recovery tools like System File Repair, Disk Commander, File Restore, Registry Editor, and Crash Analyzer.
- Use System File Repair to fix corrupted system files, or Disk Commander to repair disk issues.

3. Recover Lost Files:

- Use File Restore to recover accidentally deleted files if needed.

4. Analyze System Crashes:

- Open Crash Analyzer to analyze crash dump files and determine the cause of system crashes.

Practice Questions:

- How does DaRT enhance system recovery options compared to Windows' built-in tools?
- What types of system issues would prompt you to use DaRT?

Task 5: Steps Recorder - Record Steps to Reproduce a Problem

Objective: Use Steps Recorder to document steps leading to a problem, useful for troubleshooting and support.

1. Open Steps Recorder:

- Press Win + R, type psr, and press Enter.

2. Record Steps:

- Click Start Record and perform the actions that lead to the problem.
- Steps Recorder will capture screenshots and descriptions of each action. Click Stop Record when done.

3. Save the Recording:

- Review the recording in Steps Recorder.
- Click Save, name the file, and save it as a ZIP file for easy sharing with support staff.

Practice Questions:

- How can using Steps Recorder improve support interactions?
- In what situations would recording steps be particularly useful?

Task 6: Microsoft Management Console (MMC) - Manage System Settings and Resources

Objective: Use Microsoft Management Console (MMC) to access and manage various system settings and resources in one interface.

1. Open Microsoft Management Console:

- Press Win + R, type mmc, and press Enter.

2. Add Snap-ins:

- In the MMC window, go to File > Add/Remove Snap-in...
- Select snap-ins like Device Manager, Event Viewer, Services, and Performance Monitor. Click Add > OK to include them in the console.

3. Explore Snap-ins:

- Use Device Manager to check hardware status, Services to manage background services, and Performance Monitor to analyze system performance.

4. Save Custom Console:

- Go to File > Save As... and save your custom console for easy access to your chosen management tools.

Practice Questions:

- What are the advantages of using MMC to manage system resources?
- How can MMC improve efficiency when managing multiple system settings?

Final Questions

1. Compare Task Manager, Event Viewer, and Reliability Monitor in terms of functionality and use cases.
2. How does using MMC with custom snap-ins simplify system administration tasks?
3. Describe a scenario where DaRT would be necessary, compared to other recovery tools.