**Module 9 – Monitoring and optimizing Windows 11**

**Module Overview**

It’s important to be able to monitor your users’ computers. Monitoring enables you to determine if the computers have problems, and if they’re optimized to provide the best platform for your users’ apps. Windows 11 includes a number of tools that enable you to monitor your devices to review events, and identify and resolve reliability and performance issues.

**Objectives**

After completing this module, you will be able to:

* Describe the available monitoring options in Windows 11.
* Manage workloads and computer resources to optimize performance.

Lesson 1

**Monitoring Windows 11**

Windows 11 provides numerous tools with which you can monitor the function and reliability of your computer. In this lesson, you’ll learn how to use these tools.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe Task Manager.
* View reliability history in Windows 11.
* Describe how to use Event Viewer to monitor Windows 11.
* Create event subscriptions.

**Using Task Manager**

Task Manager provides a good starting point for determining if your computer has problems. You can use Task Manager to identify performance issues, crashed apps, startup resource usage, and detailed information about running services and processes.

Open Task Manager by pressing CTRL+ALT+DEL on your keyboard, and then select **Task Manager**. Click More details to get the most useful feedback about your computer’s current state.

Task Manager provides the following tabs:

* **Processes**. Displays a list of apps and background processes. The **Status** column displays the state of the app or process. For example, UWP apps often display a green leaf symbol that indicates the app is suspended in the background. If an app is not working, it might display **Not Responding**. Also displayed are columns for CPU, Memory, Disk, Network, Power usage, and Power user trend. These columns provide relevant information about the computer’s use of those respective resources.
* **Performance**. Displays more detailed information about performance of apps and processes running on your computer. This tab also uses a graphical format for the output. CPU, Memory, Disk, and network are displayed (either Ethernet or WiFi). There’s also a link for the Resource Monitor tool. It’s worth considering that although this information is useful, it does represent a point in time snapshot of the current performance of the computer, and might not be indicative of typical performance characteristics.
* **App history**. Displays statistics relating to resource consumption for apps running over the last few days and weeks. This can help identify resource-hungry apps, and indicate the resource they use most.
* **Startup**. Displays the apps configured to start when the computer starts. These apps often reside in the corner overflow area of the taskbar. You can use the Startup tab to Enable or Disable the listed apps to help accelerate startup.
* **Users**. Displays resource consumption on a per-user basis. You also can expand the user view to see more detailed information about the specific processes that a user is running.
* **Details**. Lists all the running processes on a computer, providing data about process ID, Status, User name, CPU and memory consumption, Architecture, and a description. You can identify the processes related to a specific app by right-clicking an app on the **Processes** tab and selecting **Go** **to details**. On the Details tab, the appropriate processes are highlighted.
* **Services**. Displays a list of all the installed services in your computer. The process ID is displayed, along with the status (Running or Stopped). You can start or stop any listed services, as appropriate.

Although Task Manager is a good starting point to review running apps and processes, and the resources they’re consuming, Windows provides additional performance monitoring tools which we’ll explore in the next lesson.

**Using Reliability Monitor**

Reliability Monitor can provide an index of reliability for your computer. It gathers the necessary data and displays it graphically so that it’s easy to understand. To access Reliability Monitor, click **Start**, type **reliability** and then click **View reliability history**. Windows generates a reliability report.

The report consists of two parts:

* **System stability chart**. A graphical representation of the reliability index for the computer over the past days and weeks, depending on what you select. An index between 1 and 10 is displayed. The chart also provides data about detailed events that occurred on specific days in the following categories:
* Application failures
* Windows failures
* Miscellaneous failures
* Warnings
* Information
* **Reliability details**. Beneath the stability chart, the reliability details are displayed for the selected day. These details provide a list of the recorded events, and enable you to click links to review more information about the events.

Reliability Monitor tracks important events about the computer’s configuration, including the installation of apps, Windows updates, and driver installation. It can help you identify the reasons for reliability issues by tracking events that relate to:

* Application or operating system failures
* Driver issues
* Memory or hard disk problems

At the bottom of the Reliability Monitor display, you can access links that enable you to:

* **Save reliability history**. This is useful for subsequent analysis.
* **View all problem reports**. Provides a list of all problems that were reported to Microsoft.

Because Reliability Monitor displays historical data, it’s useful in determining whether a user has experienced a particular computer problem before. It can also help establish patterns in recorded events that might indicate an underlying problem.

**Reviewing events**

Windows collects data about events and stores that data in a collection of logs files. You can use the Event Viewer to review these logs.

**What can you do with Event Viewer?**

By using Event Viewer, you can:

* **Review multiple logs**. Filter for specific events across several or all logs, making it easy to investigate issues and troubleshoot problems that might generate events that are logged in several logs.
* **Create customized views**. Filter to narrow searches to only certain events. For example, filtering by Event level, Logged time and date, event source or event ID, and other properties. Being able to filter enables you to focus on what’s important.
* **Configure scheduled tasks**. You can attach tasks to a log to enable you to automate responses to events. This is possible because Event Viewer is integrated with Task Scheduler.
* **Create and manage event subscriptions**. Enables you to create subscriptions from other computers’ logs, filter these subscribed logs for specific events, and review them in a single location – the Forwarded Events log.

Event Viewer provides categorized lists of essential Windows log events, and stores them in one of several logs files:

* Application
* Security
* Setup
* System

There are also log groupings for individual installed apps and specific Windows components. These are displayed beneath the **Applications and Services Logs** node, and include:

* Hardware Events
* Microsoft Office Alerts
* Windows PowerShell

There’s a **Microsoft** folder which contains a **Windows** subfolder. Diagnostic and operational logs are accessible here for installed services and apps.

An individual event provides detailed information about:

* The type of event that occurred
* When the event occurred
* The source of the event
* Technical detailed information about the event

These details can help assist in troubleshooting the event.

**Overview of the logs**

Event Viewer tracks information in multiple logs. These logs provide detailed information that includes:

* A description of the event.
* An event ID number.
* The component or subsystem that generated the event.
* Information, Warning, or Error status.
* The time of the occurrence.
* The user’s name which is associated with an event.
* The computer on which the event occurred.
* A link to Microsoft documentation for more information about the event.

The following table describes the available logs accessible in Event Viewer.

|  |  |
| --- | --- |
| Built-in Windows log | Description |
| Application | Contains errors, warnings, and informational events that relate to the operation of apps. |
| Security | Displays the results of auditing, if enabled. Audit events are displayed as either successful or failed, depending on the event. |
| Setup | Contains events that relate to app setup. |
| System | Displays general events that are logged by components and services Events are classified as error, warning, or information. |
| Forwarded Events | Stores and displays events collected from remote computers. |

**Managing logs**

You can clear the logs if you need to, but you’ll need to sign in as a local administrator. You can also configure logs by using Group Policy. Open the Group Policy Management Editor for your selected GPO, and then navigate to **Computer Configuration / Policies / Administrative Templates / Windows Components / Event Log Service**.

For each log, you can define:

* Log file location.
* Maximum log file size.
* Automatic backup options.
* Log permissions.
* Behavior that occurs when the log is full.

**Creating an event subscription**

It can be tiresome to have to connect to multiple computers and review their Event Logs. However, Event Viewer enables you to create an event subscription to help mitigate this problem.

Event Viewer enables you to collect copies of events from multiple remote computers, and then store them locally.

To specify which events to collect, create an event subscription.

After your subscription is active and Windows is collecting events, you can review and manage these forwarded events just as you would any other locally stored events.

To use the event-collecting feature, configure the forwarding (source), and the collecting computers.

The event-collecting functionality depends on the Windows Remote Management (WinRM) service and the Windows Event Collector service (Wecsvc).

Both of these services must be running on computers that are participating in the forwarding and collecting process.

**Enabling subscriptions**

To enable subscriptions, perform the following steps:

1. On each forwarding, or source, computer, enable Windows Remote Management. Run the following command at an elevated command prompt:

* winrm quickconfig

1. On the collector computer, enable the Windows Event Collector service. Run the following command at an elevated command prompt:

* wecutil qc

1. Finally, add the computer account of the collector computer to the local **Event Log Readers** group on each of the forwarding (source) computers.

**Demonstration: Reviewing resource usage**

Lesson 2

**Optimizing Windows 11 performance**

It’s important that your users get the best experience from using their computers. A significant part of element is performance. You must ensure that your users’ computers are configured with sufficient resources to meet the demands of the workloads they run on those computers. Windows 11 provides a collection of tools with which you can identify performance problems, and then take action.

**Lesson Objectives**

After completing this lesson, you will be able to:

* Describe the key hardware resources in PCs.
* Use the available performance monitoring tools.

**Understanding computer resources**

Poor or degraded computer system performance is a common source of user complaints. Sometimes this is because the original specification of a user’s computer is insufficient to meet the needs of the intended workloads. But sometimes, it’s due to a lack of resources to meet an unexpected increase in workload.

A typical Windows 11 workstation should be configured with:

* A modern i5 processor with two or more cores (or better)
* No less than 8 GB of memory
* A primary disk subsystem using SSD
* A fast network interface card (NIC)

Although the minimum requirements are lower, these are sensible hardware resource levels for typical office workloads, such as multiple tabs open in Microsoft Edge, Outlook, Word, and possibly Microsoft Teams running concurrently.

Even with this recommendation, from time-to-time, a user will complain about poor responsiveness. It will be your job to figure out what the problem is. Let’s define some terms.

Performance is a measure of how quickly a computer completes requested app and system-related tasks. Performance problems occur when available resources are insufficient for the requested tasks. Factors that influence computer performance include:

* Slow hard disks.
* Insufficient memory available.
* Insufficient processor capacity and speed.
* Insufficient NIC bandwidth.
* Excessive resource consumption by individual apps.
* Component faults.
* Device driver issues.

**What are the four key resources?**

The four main hardware resources that you should monitor in a Windows computer are:

* **Memory**. For a Windows computer, memory is usually the most critical resource. If you don’t have enough, the computer runs slowly. If you have insufficient memory, the virtual memory manager in Windows pages to the hard disk. This paging slows the computer down significantly. Conversely, if you have more than you need, your computer uses the excess to perform disk caching, which means that the disk is less likely to be a performance issue.
* **Disk**. Older HDDs should be avoided; their moving parts limit their performance. Using SSDs makes a significant difference to startup times and other disk intensive tasks. Always avoid paging, as this is very disk intensive. As mentioned above, paging is caused by insufficient working memory at a given moment.

The relationship between insufficient memory, and imposed workload on the disk caused by paging, means that memory and disk are the two critical resources in most client computers.

* **Processor**. A modern two core processor shouldn’t create any bottlenecks in workstation performance for typical office tasks. But demanding workloads do require high-end processors.
* **Network interface**. Of the four key resources, this is the least significant. Modern NICs support high speeds, even over WiFi connections. However, issues with network configuration, or infrastructure components (such as routing) can slow things down; but that’s not related to the network interface in your computer.

Although not considered a core component, the graphics adapter can have a big impact on performance, particularly with graphics-intensive apps. If your users are likely to run graphically demanding apps, ensure you choose computers with a high-performance graphics adapter, and one that doesn’t use system memory (i.e. shared memory). Let’s review these resources in more detail.

**What’s a bottleneck?**

A performance bottleneck happens when your computer can’t service the current requests for a specific resource. The resource might be memory, disk, processor, or network interface.

If you use performance monitoring tools regularly, and compare the results to a baseline and to historical data, you can identify performance bottlenecks, perhaps before they begin to affect your users.

A baseline is a measured responsiveness under a known load.

After you’ve identified a bottleneck, you must decide how to remove it. There are two fundamental options:

* **Reduce workload**. Reduce the number of apps running on the computer. If that’s not possible, then consider replacing the computer with one that has sufficient resource, and repurposing the old computer for a user with less demanding apps.
* **Add more resources**. Some computers enable you to add more resource, such as memory. Changing older HDDs for SSDs is a pretty easy fix, and makes a big difference in performance, especially for disk intensive tasks. However, most computers don’t enable you to add additional processor capacity.

**Using performance monitoring tools**

A good starting point for measuring performance is to know what good performance, or at least typical performance, looks like. Sometimes, this doesn’t need to be measured; after all, you probably have a pretty good idea, based on experience, about how long it should take to complete a computing task. For example, maybe your computer starts up in the morning from cold and displays the sign in screen in 10 seconds. Then one day, it takes two minutes to boot. You know something’s wrong right away.

**What’s a baseline?**

However, since we’re thinking here about your users’ computers, you might need to generate a measurable baseline. Windows provides the necessary tools for measuring performance, and you can easily use those to create your baseline. Thereafter, when experiencing a performance-related problem, compare what you measure during the problem with what you measured in the baseline scenario. That should point you at the bottlenecked resource.

Baselines help you:

* Evaluate your computer’s workload.
* Monitor system resources.
* Identify changes and trends in resource use.
* Test configuration changes.
* Diagnose problems.

**Performance monitoring tools**

Windows 11 provides a range of tools you can use to measure performance.

**Task Manager**

You can use the Performance tab in Task Manager to review performance in your Windows computer. The Performance tab displays details about: Processor, memory, physical disk, network, and graphics subsystem performance.

The problem with Task Manager’s Performance tab is it just displays a rolling point-in-time chart. This is useful in some situations, but not for analysis, and certainly not for comparison to a baseline.

**Resource Monitor**

Resource Monitor also provides a snapshot of system performance, but with considerably more detail about the processes and services generating the load. The four core resources are displayed in four active charts on the Overview tab: CPU, Disk, Network, and Memory. You can easily review these charts for indications about resourcing problems. There is also a separate tab for each resource that enables you to take a closer look at the specific resource and its current workload.

**Performance Monitor**

Performance Monitor is a Microsoft Management Console (MMC) snap-in that you can use to obtain system performance information. You can use this tool to analyze the performance effect that applications and services have on your computer. You also can use it to obtain an overview of system performance or collect detailed information for troubleshooting.

Performance Monitor includes the following components:

* **Monitoring Tools**. Provides a real-time chart of selected resources. Due to the real-time nature of the display, this is less useful than either of the other components.
* **Data Collector Sets**. Enables you to create a custom set of performance counters, event traces, and system configuration data. You can define what you want to measure, how frequently, and for how long. Data Collector Sets are ideal to establish baselines, and to capture performance data for comparison with baselines.
* **Reports**. For each Data Collector Set you generate, there is a corresponding Reports node with the same name. You can review the reports in text or graphical form, depending on your needs.

**Using data collector sets**

In Performance Monitor, under the Data Collector Sets, select the User Defined node to create your own data collector sets. You can choose which objects and counters you want to include for monitoring. To help you choose the appropriate objects and counters, you can use templates, including:

* **Basic**. Enables you to create a basic data collector set. You can add your own counters, and choose appropriate scheduling for your set.
* **System Diagnostics**. Selects objects and counters that focus on the status of hardware resources, system response time, and processes, plus system information and configuration data. The resultant report provides guidance on how you might improve the computer’s performance.
* **System Performance**. Generates reports on the status of local hardware resources, system response times, and processes.
* **WDAC Diagnostics**. Enables you to trace debug information for Windows Data Access Components.

**What objects and counters should you add?**

Performance Monitor, Data Collector Sets, and Reports are based on *objects* and *counters*, and sometimes *instances*. An *object* is like a resource. It might indeed be Memory, or Processor. But there are also some esoteric objects you can include.

Each object consists of *counters*. These are measurable elements of the object. For example, the %Disk Time counter of the Physical Disk object. When creating your data collector set, you can add whole objects, and gather all their counters, or just add specific counters.

Finally, some objects can have multiple *instances*. For example, a computer with two hard disks has two Physical Disk objects, each with their own set of counters. For some objects, it’s worth considering which instance of an object is suffering a bottleneck. Physical Disks are a good example. By knowing which disk is bottlenecked, you can determine which app or component on that disk is the problem.

When considering which instances to add, you can select **\_Total**, **<All instances>**, or specific instances. You should probably use the \_Total instance as this aggregates the workload across all instances.

The following table describes common objects and counters that identify key resource usage and bottlenecks.

|  |  |
| --- | --- |
| Object\counter | Description |
| PhysicalDisk\% Disk Time | The percentage of elapsed time that the selected disk drive was busy servicing read or write requests. This should be less than 85%. Higher than that, coupled with Avg. Disk Queue Length > 2 indicates a disk bottleneck. |
| PhysicalDisk\Avg. Disk Queue Length | The average number of both read and write requests that were queued for the selected disk during the sample interval. |
| Memory\Pages per Second | The rate at which pages are read from or written to disk to resolve hard page faults. This counter is a primary indicator of the kinds of faults that cause system-wide delays. |
| Processor\% Processor Time | The percentage of elapsed time that the processor spends to execute a non-Idle thread. This should be less than 85%. If it’s higher, and System\Processor Queue Length is excessive, it suggests a processor bottleneck. |
| System\Processor Queue Length | The number of threads in the processor queue. |
| Network Interface\Bytes Total/Sec | The rate at which bytes are sent and received over each network adapter, including framing characters. |
| Network Interface\Output Queue Length | The length of the output packet queue (in packets). There is network saturation if the value is more than 2. |

**Demonstration: Creating a data collector set**

**Lab: Monitoring and optimizing performance**

**Question:**In the lab, you worked with several performance monitoring tools. How would you gather performance data over a period for comparison with a baseline?

**Module Review and Takeaways**

Review Questions

**Question:**What are the four core resources in a Windows 11 computer, and which is likely the most important of the four?

**Question:**Which tools could you consider using to troubleshoot reliability issues in Windows 11?