# **Module 12**

**Monitoring and Troubleshooting Windows Server 2019**

|  |
| --- |
| **At a Glance** |

#### Instructor’s Manual Table of Contents

* Overview
* Objectives
* Teaching Tips
* Quick Quizzes
* Class Discussion Topics
* Additional Projects
* Additional Resources
* Key Terms

|  |
| --- |
| Lecture Notes |

# **Overview**

In this module, your students learn to develop a basic troubleshooting strategy to solve problems step-by-step. The entire troubleshooting process is centered upon two golden rules: prioritizing problems and trying to solve the root of the problem. Next, your students learn how to successfully use the Windows Sever 2019 performance and monitoring tools to obtain detailed system and performance information that can be used to resolve a multitude of problem types. These tools include Task Manager, Resource Monitor, Performance Monitor, Data Collector Sets, Event Viewer, and Reliability Monitor. Finally, the five common categories of Windows Server 2019 problems are presented along with methodologies and testing techniques for resolving these issues. These common categories are hardware-related issues, performance-related issues, software-related issues, operating system-related issues, and network-related issues.

# **Module Objectives**

* Outline the process used to monitor and troubleshoot systems
* Use common monitoring and troubleshooting tools
* Troubleshoot common hardware, software, operating system, performance, and network problems

# **Teaching Tips**

**Monitoring and Troubleshooting Methodology**

1. Introduce this section by mentioning that after an administrator has successfully installed Windows Server 2019, configured and secured server roles, and documented settings, he or she must maintain the system’s integrity over time.
2. Refer to Figure 12-1 and mention that system integrity can be implemented by performing monitoring, proactive maintenance, and reactive maintenance.
3. Discuss what is meant by monitoring and note that it is one of a system administrator’s most time-consuming tasks. Define monitoring as the process of examining network connectivity, viewing log files, and running performance utilities periodically to identify problems and their causes.
4. Explain that proactive maintenance involves taking the required steps to minimize the chance of future problems as well as their impact. Provide some examples of proactive maintenance tasks a system administrator might perform. Emphasize that all proactive maintenance tasks should be documented for future reference.

1. Explain that reactive maintenance is used to correct problems when they arise during monitoring. Mention that when a problem is solved, it needs to be documented, and the system adjusted proactively to reduce the likelihood that the same problem will occur in the future. Note that documenting the solution to problems creates a template for action, allowing subsequent or similar problems to be remedied faster.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Take the time to explain the importance of taking baseline measurements and documenting all proactive maintenance efforts. Note that a baseline is a set of performance measurements taken during periods of normal system activity. When performance issues arise, an administrator can compare current performance measurements to those in the baseline. Values that have changed dramatically from the baseline can help the administrator pinpoint the source of the performance problem. |

1. Discuss the concept of creating and using troubleshooting procedures by explaining that reactive maintenance is further composed of many tasks known as troubleshooting procedures, which can be used to efficiently solve a problem in a systematic manner.
2. Refer to Figure 12-2 and review the basic steps an administrator might follow when following troubleshooting procedures.
3. Discuss the two golden rules of troubleshooting.

* Prioritize problems
* Try to solve the root of the problem

**Monitoring and Troubleshooting Tools**

1. Introduce this section by reminding your students that Server Manager and the Windows Admin Center can be used to monitor system events and performance.
2. List the addtional tools Windows Server 2019 includes that server administrators can use to obtain more detailed system and performance information.

* Task Manager
* Resource Monitor
* Performance Monitor
* Data Collector Sets
* Event Viewer
* Reliability Monitor

**Task Manager**

1. Introduce this topic by reminding students that Task Manger can be used to view and manage processes.
2. Emphasize that Task Manager can be used to quickly analyze the performance of a system, and it is often the first tool that server administrators open when reacting to a performance problem.
3. Review some of the methods for opening Task Manager.
4. Explain that the Task Manager default view only displays a short list of processes started by the current user.
5. Refer to Figure 12-3 and illustrate how an administrator can view performance information in Task Manager. Explain that by default, the Performance tab displays hardware utilization information regarding the processor (CPU), including the number of processes, threads, and handles.
6. Define a thread as a unique sequence of instructions that is executed by a process. Discuss how threads and processes interact.
7. Define a handle as a resource (often a file) that is connected to a process. Mention that processes that use storage frequently often use a large number of handles.
8. Refer to Figure 12-3 and explain how an administrator can view memory utilization information by selecting Memory under the Performance tab in Task Manager.
9. Refer to Figure 12-4 to illustrate the memory utilization window after it is selected. Explain the different types of memory that can be reviewed, including committed memory, cached memory, paged pool memory, and non-paged pool memory.
10. Refer to Figure 12-5 to illustrate the network statistics that are displayed for an associated network interface. Mention that the send and receive values shown in Figure 12-5 will vary depending on the number of clients connected to the server and the amount of data that they are transferring. Emphasize that high sustained send and receive values could indicate a large number of connections transferring data, or a Distributed Denial of Service (DDoS) network attack that is flooding the server with traffic in an attempt to disrupt service.
11. Mention that high processor or memory utilization values can be the result of too many processes running on the system, but can also be caused by rogue processes and memory leaks.
12. Define rogue processes as processes that have encountered an error that forces them to use an unusually high amount of processor time.
13. Mention that memory leaks cause processes to enter a state that allows them to continually use more memory until the memory in the system is exhausted.
14. Refer to Figure 12-6 and explain how to identify rogue processes and memory leaks.
15. Explain how to end suspected rogue processes and those that are causing memory leaks.
16. Explain that an administrator can highlight the Users tab in Figure 12-6 to view a list of processes organized by the user that started them. Refer to Figure 12-7 to illustrate the results from this action.
17. Explain that an administrator can highlight the Details tab in Figure 12-6 to view more information for each process on the system. Refer to Figure 12-8 to illustrate the results from this action.
18. Note that in addition to showing the process ID (PID), status, user name, and CPU and memory utilization for each process, the Details tab shown in Figure 12-8 provides additional actions when an administrator right-clicks a process. Briefly review these actions.

* End process tree
* Set priority
* Set affinity
* Analyze wait chain
* UAC virtualization

1. Refer to Figure 12-9 to illustrate the list of services that results from highlighting the Services tab in Figure 12-8. Mention that most problems related to unresponsive services can be resolved by restarting the service, or starting it if it is stopped. Explain how to restart or start a service.

**Resource Monitor**

1. Introduce the Resource Monitor by explaining that it can be used when an administrator needs more information than Task Manager offers in order to troubleshoot a performance problem such as a process that is writing to a particular file.
2. Refer to Figure 12-10 to illustrate the Resource Monitor tool.
3. Review some of the methods for opening the Resource Monitor tool.
4. Explain that in addition to a graph showing CPU, disk, network, and memory utilization, the CPU section on the Overview tab of Resource Monitor displays a list of processes that an administrator can select to display the associated detailed storage, network, and memory information.
5. Discuss the contents in the other tabs shown in Figure 12-10, noting that they display specific information for each process selected in the CPU section of the Overview tab.

* The CPU tab displays related services and file handles.
* The Memory tab displays physical and virtual memory usage.
* The Disk tab displays the disks and files used.
* The Network tab displays network activity, TCP connections, and ports.

**Performance Monitor**

1. Introduce Performance Monitor by noting that it is Windows Server’s most comprehensive tool for collecting data on real-time system performance.
2. Explain that Performance Monitor allows an administrator to track how individual system resources are being used and how they are behaving under the current workload.
3. Review some of the methods for opening and starting the Performance Monitor tool.
4. Refer to Figure 12-11 to illustrate and explain the three performance information components in the Performance Monitor tool.

* Performance objects
* Performance counters
* Instances

1. Refer to Table 12-1 to illustrate some of the many different performance objects and counters that are available.
2. Refer to Figure 12-11 and Figure 12-12 to explain how to add a performance counter to Performance Monitor.
3. Note that it is often difficult to view the output of multiple performance counters in the default line graph view of Performance Monitor. Explain how to view the current performance counter values as a bar chart or a report.
4. Refer to Figure 12-13 to illustrate a report of the current performance counter values. Note that the report shown in Figure 12-13 is appropriate for creating a simple performance baseline, as it lists the values for each performance counter. Explain how to save the baseline report as a webpage.
5. Note that an administrator can click the Unfreeze Display icon in the webpage to view the current values of each performance counter interactively using the Performance Monitor.
6. Explain how to use the baseline report to identify the cause of the performance problems.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | The performance counter values an administrator obtains when taking a baseline on a system will vary from system to system, as they are largely dependent on the underlying hardware and software. As a result, an administrator should not interpret baseline performance counter values for a system. Instead, baseline performance counter values are only compared to current performance counter values to help locate the cause of a performance problem. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Any time an administrator adds software or hardware to a system, he or she should take a new baseline for that system. |

**Data Collector Sets**

1. Introduce the Data Collector Sets tool by explaining that it is suitable for creating baselines that span a period of time, or for analyzing trends that can be used to proactively identify performance problems before they impact the system.
2. Refer to Figure 12-14 to illustrate the Data Collector Sets tool in the Performance MMC snap-in.
3. Explain that using the Data Collector Sets tool, an administrator can create a data collector set to collect and log data from performance counters, event trace providers, or system configuration information in the Windows Registry.
4. Describe event trace providers as Windows components that report detailed information about the Windows kernel and system applications.
5. Describe the data collector set configuration known as a performance counter alert. Explain that it monitors a performance counter and logs the associated data only when the performance counter exceeds or falls below a certain value.
6. Refer to Figures 12-15 through 12-21 and explain how to create a data collector set to log data.
7. Explain that the process used to create a performance counter alert is almost identical to the process used to create a data collector set for collecting and logging data. Point out that if an administrator selects Performance Counter Alert in Figure 12-16 and clicks Next, he or she is prompted to specify performance counters and the associated alert values. Refer to Figure 12-22 to illustrate these values.
8. Explain that in Figure 12-22, an administrator is prompted to configure the same data collector set options that were shown in Figure 12-21. After an administrator clicks Finish in Figure 12-21, he or she can manage the performance counter alert as they would any other data collector set.
9. Mention that after an administrator stops a data collector set, he or she can view the data that has been collected.
10. Refer to Figure 12-23 and explain that to view the data collected from performance counters, an administrator can expand the User Defined folder under the Reports folder and select the appropriate report under the folder for the data collector set.
11. Review the naming conventions for each report and folder.
12. Refer to Figure 12-24 to illustrate how to view the contents of a folder.

**Event Viewer**

1. Introduce this topic by explaining that when troubleshooting problems that affect a particular system component, service, or application, an administrator can often obtain details regarding the nature of the problem by examining event information stored in event logs.
2. Refer to Figure 12-25 and explain that an administrator can user the Event Viewer tool to view event logs and the events they contain.
3. Review some of the ways to start Event Viewer.
4. Refer to Figure 12-25 again and review the five standard Windows event logs available under the Windows Logs folder in the Event Viewer navigation pane.

* Application stores events from software applications on the system.
* Security stores auditing events, such as a successful or failed attempt to access a file.
* Setup stores events from the installation of server roles and features.
* System stores operating system-related events, including service startup, hardware errors, and events related to authorization and authentication.
* Forwarded Events stores events that were obtained from computers on the network using an event subscription. Note that to create an event subscription, an administrator can right-click the Subscriptions folder in Figure 12-25 and click Create Subscription.

1. Explain how Windows limits the number of events recorded in the Application and System event logs. Discuss where these additional logs are located.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | To accommodate new events, the oldest events in an event log are deleted automatically when the event log reaches its size limit. To modify this behavior, or to increase the size limit for an event log, an administrator can highlight the event log in the navigation pane of Event Viewer and click Properties in the Actions pane. |

1. Note that each event displayed in Event Viewer contains a level that indicates the type or severity of the event. Review the six different event levels that are available.

* Information
* Warning
* Error
* Critical
* Audit Success
* Audit Failure

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | To search for the next occurrence of a certain event in an event log, an administrator can click Find from the Actions pane in Event Viewer and specify an event ID or keyword. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | When searching for events related to a problem that affects a system or software component, it is often easier to display the associated event log in Event Viewer, reproduce the problem, and then view the most recent events that were added to the event log. |

1. Point out that a single event log may contain thousands of different events that are unrelated to the problem that an administrator is attempting to resolve.
2. Mention that to limit the events displayed for the System event log shown in Figure 12-25, an administrator can click Filter Current Log in the Actions pane and specify the appropriate criteria.
3. Explain that for recurring problems, or to display events from multiple event logs, an administrator should create a custom view that is saved under the Custom Views folder in the navigation pane for future use.
4. Refer to Figure 12-25 and Figure 12-26 to illustrate how to create a custom view.

**Reliability Monitor**

1. Introduce this topic by explaining that the Reliability Monitor can indicate event trends over a period of time in order to proactively identify system stability or performance problems.
2. Review some of the ways to start the Reliability Monitor.
3. Refer to Figure 12-27 to illustrate the Reliability Monitor. Discuss and explain some of the indicators shown in the figure.

**Quick Quiz 1**

1. Which term refers to a set of performance measurements taken during periods of normal system activity?
   1. event subscription
   2. data collection set
   3. baseline
   4. event

Answer: c. baseline

1. Which term refers to a unique sequence of instructions that is executed by a process?
2. data collector set
3. event
4. handle
5. thread

Answer: d. thread

1. Which tool is Windows Server’s most comprehensive tool for collecting data on real-time system performance?
   1. Resource Monitor
   2. Performance Monitor
   3. Task Manager
   4. Data Collector Sets

Answer: b. Performance Manager

1. Of the five standard Windows event logs that are available under the Windows Logs folder in the Event Viewer navigation pane, which log stores events that were obtained from computers on the network using an event subscription?
   1. Setup
   2. Security
   3. System
   4. Forwarded Events

Answer: d. Forwarded Events

**Resolving Common System Problems**

1. Open this topic by emphasizing that most Windows Server 2019 problems can be divided into five categories: hardware-related, performance-related, software-related, operating system-related, and network-related.

**Hardware-Related Problems**

1. Introduce this topic by mentioning that failure of hardware components is common in environments where servers are continually under heavy load.
2. Note that a hardware component may fail entirely, preventing the system from using it.
3. Note that a process called jabbering might occur—that is, hardware components may fail intermittently, or malfunction by sending large amounts of information to the processor when not in use. Emphasize that jabbering can slow down a processor and the rest of the Windows system.
4. Explain how an administrator can detect jabbering.
5. Explain why hard disks and SSDs are the most common hardware components to fail.
6. Discuss the various ways data on a failed hard disk or SSD can be recovered, considering whether or not fault tolerant devices are being used, whether or not the failed storage device contains the system or boot partition, and whether or not a backup of the data exists.

**Performance-Related Problems**

1. Introduce this topic by explaining that performance problems occur when the software on a system requires more hardware resources than are currently available.
2. Explain that resolving performance problems often involves reducing the amount of software that is run on a system or adding additional hardware resources.
3. Emphasize that first, an administrator should examine the services running on a system and remove or disable any unnecessary ones to prevent them from consuming system resources.
4. Explain how to stop an unnecessary service, and refer to Figure 12-28 to illustrate how to prevent a service from starting again at boot time.
5. Second, if the performance information shown by Task Manager or Resource Monitor indicates that necessary processes are consuming too many resources on a system, or current performance counters for hardware components vary greatly from their baseline values, an administrator can adjust the number of processes competing for hardware resources to resolve the performance problem. As an example, if other systems in the organization are underutilized, an administrator can move some applications and server roles to those systems to provide adequate resources for existing applications and sever roles.
6. Third, explain that performance problems can be remedied by altering the hardware. As an example, mention that upgrading or adding another processor allows the Windows system to execute processes faster and reduce the number of processes running concurrently on the processor.
7. As another example, define bus mastering as allowing devices to perform processing tasks that are normally performed by the processor. Explain that an organization can upgrade hardware components to include bus mastering and reduce the amount of processing the processor must perform. This in turn increases system speed.
8. Discuss how adding physical memory to the computer increases system speed because it gives processes more working space in memory and reduces the use of the paging file.
9. Fourth, explain how replacing slower hard disk drives with faster ones or SSDs improves the performance of programs that require frequent access to filesystems.

**Software-Related Problems**

1. Introduce this topic by explaining the many ways software-related problems can occur. Specifically mention that processes can fail because of missing dependencies, incorrect configuration settings, software bugs, or conflicting applications. Additionally, note that restrictive file permissions, incorrect file ownership, and missing environment variables may also prevent a process from accessing files needed for the process to run properly.
2. Mention that a failed process may generate a memory leak or become a rogue process that an administrator can identify and remove using Task Manager.
3. Emphasize and explain why another important area to review is the Application event log.
4. Discuss the importance of being able to understand and use the Event Viewer to look for events related to the software problem or an event description that identifies the specific cause of the failure.

**Operating System-Related Problems**

1. Introduce this topic by explaining that the Windows operating system can also encounter problems that prevent it from running properly.
2. Explain that some problems result in a system crash. Mention that if the system crashes, the system administrator should first ensure that he or she has the latest critical updates for the software on their system. Next, the administrator should examine the contents of the System event log in Event Viewer at the time of the system crash to identify possible causes and solutions.
3. Explain that some problems result in boot errors. Explain that if the system fails to boot following a crash, an administrator can access the Advanced Boot Options menu at boot time to remedy the problem. Describe how to enable the Advanced Boot Options menu.
4. Refer to Figure 12-29 and Figure 12-30 to illustrate the Windows Boot Manager screen the Advanced Boot Options menu screen.
5. Refer to Table 12-2 for a list of Advanced Boot Options menu options and their meanings.

**Network-Related Problems**

1. List the most common types of network issues that server administrators encounter.

* Network connectivity
* Service access
* Network latency

1. Explain that if a user is unable to connect to other computers on the network from a Windows Server 2019 system, there are several items to investigate.
2. First, mention that an administrator should determine whether the associated network interface has a valid IP configuration and is connected properly to the LAN. Explain how to run the ipconfig /all command at a Windows PowerShell or Command Prompt window to view the IP configuration of each network interface on the system. If a network interface uses DHCP to obtain IP settings, also ensure that the DHCP server is available on the network and has not exhausted its range of IP addresses.
3. Second, mention that an administrator should test connectivity to the IP address of the network interface. Explain how to use the ping *IPaddress* command at a Command Prompt window, or the Test-NetConnection *IPaddress* command in Windows PowerShell, to perform this test. Emphasize that if an administrator does not receive a successful response, then the device driver for his or her network interface has experienced a failure that can be solved by rebooting the system.
4. Third, mention that an administrator should test connectivity to an IP address on the same LAN as the network interface. Explain how to use the ping or Test-NetConnection command to perform this check. If an administrator is unable to connect to other computers on his or her LAN, the administrator may need to reboot the network switch.
5. Fourth, mention that after testing local LAN access, an administrator should test connectivity to an IP address on another LAN, or a public IP address on the Internet, using the ping or Test-NetConnection command. If the administrator is unable to connect to computers outside of their LAN, he or she may not have the correct default gateway configured on their network interface, or a router between their computer and the target IP address has failed, contains incorrect configuration, or is experiencing high load. Mention that an administrator can supply the target IP address as an argument to the tracert or Test-NetConnection –TraceRoute command to determine which router is the source of the problem.
6. Fifth, mention that if an administrator can access both local and remote LANs from his or her system by IP address, then the issue is likely due to name resolution. Test connectivity to the FQDN of a computer on network (e.g., using the ping *FQDN* or Test-NetConnection *FQDN* command). Explain that if connectivity to the computer’s FQDN fails, then an administrator must ensure that their network interface lists the correct DNS server for name resolution, and that the DNS server is available on the network. If the DNS server is unavailable, an administrator can specify an alternate DNS server in their network interface configuration to obtain network connectivity.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | When using ping or Test-NetConnection, it is best to choose a target computer that does not have a firewall enabled. Firewalls often block ICMP, preventing these commands from receiving a successful response. In this case, an administrator can determine whether the target computer was contacted successfully by looking for the target computer’s IP address in the MAC address cache on their computer. An administrator can use the arp -a command to display the MAC address cache. |

1. Emphasize that if clients are unable to contact a particular service running on the server from across the network, an administrator should start troubleshooting at the server itself.
2. First, use Task Manager to determine if the network service is running, and start the service if necessary. Point out that if the network service fails to start, then the administrator should check the associated event in the System event log to determine why the service failed to start, searching the description online if necessary. Review some of the reasons a service may be prevented from starting successfully.
3. Second, determine if the service is listening on the correct port number using the netstat -a command at a Command Prompt window, or the Get-NetTCPConnection and Get-NetUDPEndpoint commands in Windows PowerShell. Explain that if the network service is configured to listen to a non-standard port number, then client programs will also need to specify the non-standard port number for a connection to be successful.
4. Third, explain that an administrator should attempt to interact with the network service locally to see if it is responding to requests on the correct port number. Demonstrate how to do this using a local Web server listening on Port 80.
5. Fourth, if the network service is responding to requests, explain that an administrator should attempt to access the network service from the local computer using an appropriate client program.
6. Fifth, mention that an administrator should attempt to access the service from another computer on the network by connecting to the service by IP address. Emphasize that if an administrator is able to access a service locally, but is unable to access the same service from across a network by IP address, then a firewall on the server or network is likely preventing the access. Explain how to remedy the issue, by allowing the protocol name or port number in the appropriate firewall configuration.
7. Sixth, mention that an administrator should attempt to access the service from another computer on the network by connecting to the service using the FQDN. If the administrator can access the service from another computer by IP address but not by FQDN, then name resolution is the issue. Refer to Figure 12-31 and review the items to check to correct this issue.
8. Introduce the concept of network latency by explaining that sometimes, a network is properly configured, but the time it takes for services to respond to network requests is very high or users receive occasional timeout errors when attempting to connect to a service.
9. Explain that network latency can occur when a network is saturated with traffic or has limited bandwidth.
10. Explain that to determine if a particular service or application is saturating the network, an administrator can examine the traffic that is passing to and from their network interface using a third-party packet sniffer program.
11. Mention that an administrator can also test the network latency between their computer and other computers on the network to identify bandwidth problems.
12. Explain how to test the latency (in milliseconds) to a target computer by IP address, by using the pathping *IPaddress* command at a Command Prompt window, or the Test-NetConnection –InformationLevel Detailed *IPaddress* command in Windows PowerShell.
13. Note that in some cases, network latency can be caused by firewall devices that are restricting network throughput, or by a malfunctioning network interface, switch, or router that is dropping IP packets instead of processing them. Point out that rebooting the affected device often remedies the problem.
14. Finally, if network latency affects a single computer, then an application on that computer is probably sending or receiving a large amount of data on the network interface. Explain that by using Resource Monitor to list the top processes accessing the network an administrator can often identify which process is causing the problem.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Many third-party packet sniffer programs are available. Wireshark is a free packet sniffer program that an administrator can download from: <https://www.wireshark.org>. |

**Quick Quiz 2**

1. Which term refers to hardware components failing intermittently, or malfunctioning by sending large amounts of information to the processor when not in use?
   1. packet sniffing
   2. jabbering
   3. memory leak
   4. network latency

Answer: b. jabbering

1. Which term refers to allowing a device to perform processing tasks that are normally performed by the processor?
   1. bus mastering
   2. jabbering
   3. monitoring
   4. sniffing

Answer: a. bus mastering

1. When restarting a Windows Server 2019 system and reaching the Windows Boot Manager screen, which key would an administrator press to access the Advanced Boot Options menu?
   1. F1
   2. F2
   3. F6
   4. F8

Answer: c. F8

1. Which term refers to the problem of long response times or timeout errors when users attempt to connect to a service, even though the network is configured properly?
   1. page fault
   2. network latency
   3. memory leak
   4. Distributed Denial of Service (DDoS)

Answer: b. network latency

# **Class Discussion Topics**

1. What can you do when booting in Safe Mode?
2. What are the main benefits of using event logs?

# **Additional Projects**

1. Ask your students to read the netstat command help page at <https://www.computerhope.com/netstat.htm> and write a report explaining how to use the *netstat* command.
2. Ask your students to read the following article on packet sniffing: <https://www.dnsstuff.com/packet-sniffers>. Have each student briefly summarize important characteristics of a packet sniffing program. Next, have each student select a packet sniffer from the examples in the article, and continue with their report by summarizing how the packet sniffer they selected works and the advantages it provides.

# **Additional Resources**

1. The Story of the PING Program

<https://ftp.arl.army.mil/~mike/ping.html>

1. netstat

<https://en.wikipedia.org/wiki/Netstat>

1. ipconfig  
   (the syntax and options for using the ipconfig diagnostic ttility for network connections)

<https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig>

1. Event Viewer

<http://en.wikipedia.org/wiki/Event_Viewer>

1. Performance Tuning Network Adapters

<https://docs.microsoft.com/en-us/windows-server/networking/technologies/network-subsystem/net-sub-performance-tuning-nics>

**Key Terms**

* **Advanced Boot Options** The Advanced Boot Options screen lets you start Windows in advanced troubleshooting modes. You can access the menu by turning on your computer and pressing the F8 key before Windows starts.
* **baseline** A baseline documents normal activity. You can use Performance Monitor or data collector sets to create baselines that can be used to identify possible causes of performance problems.
* **bus mastering** Allowing a device to perform processing tasks that are normally performed by the processor.
* **cached memory** A hardware or software component that stores data so that future requests for that data can be served faster; the data stored in a cache might be the result of an earlier computation or a copy of data stored elsewhere.
* **committed memory** Virtual memory from the paging file that applications have requested.
* **custom view** A type of filtered event that is saved under the Custom Views folder in the Event Viewer’s navigation pane for future use.
* **data collector set** An entity created by the Data Collector Set tool that collects and logs data from performance counters, event trace providers, or system configuration information in the Windows Registry.
* **Data Collector Sets** A Windows Server 2019 tool used for creating baselines that span a period of time, or for analyzing trends that can be used to proactively identify performance problems before they impact the system.
* **Distributed Denial of Service (DDoS)** A malicious attempt to disrupt normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.
* **dump file** A file used to help the developer team in your organization identify and fix a program logic problem.
* **event log** Files that contain details regarding the nature of problems.
* **event subscription** A registration indicating that a particular event is significant to a particular system and specifying the processing to perform when the triggering event occurs. A Forwarded Events log stores events that were obtained from computers on the network using an event subscription.
* **event trace provider** Windows component that reports detailed information about the Windows kernel and system applications.
* **Event Viewer** A tool used to view event logs and the events they contain.
* **handle** A resource (often a file) that is connected to a process.
* **instance** A component of the Performance Monitor tool that represents a specific hardware device or software component. For example, if your system has two network interfaces, you can choose to monitor the first network interface only (the first instance).
* **jabbering** A process where hardware components may fail intermittently, or malfunction by sending large amounts of information to the processor when not in use.
* **memory leak** A type of error where processes enter a state that allows them to continually use more memory until the memory in the system is exhausted.
* **monitoring** One of a system administrator’s most time-consuming tasks; it involves examining network connectivity, viewing log files, and running performance utilities periodically to identify problems and their causes.
* **network latency** The time it takes for data or a request to go from the source to the destination. Latency in networks is measured in milliseconds. The closer your latency is to zero, the better.
* **non-paged pool** The amount of kernel and device driver memory that must stay in physical memory. This type of memory cannot be offloaded onto the disk.
* **packet sniffer** A computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. Packet capture is the process of intercepting and logging traffic.
* **page fault** A type of exception raised by computer hardware when a running program accesses a memory page that is not currently mapped by the memory management unit into the virtual address space of a process.
* **paged pool** The amount of kernel and device driver memory that CAN spill over from physical memory into the slow page file (source).
* **performance counter** A component of the Performance Monitor tool that represents the components of a performance object that monitor a specific type of event.
* **performance counter alert** A data collector set configuration created when a data collector set monitors a performance counter and logs the associated data only when the performance counter exceeds or falls below a certain value.
* **Performance Monitor** A tool that allows a system administrator to monitor real-time system performance and create simple baselines.
* **performance object** A component of the Performance Monitor tool that represents the areas of the system that can be monitored. Common examples of performance objects include Processor, Memory, Physical Disk, Logical Disk (for volumes), and Network Interface.
* **PerfView** A CPU and memory performance-analysis tool.
* **proactive maintenance** Taking the required steps to minimize the chance of future problems as well as their impact. Performing regular system backups, monitoring available storage, creating baselines, and analyzing performance trends to identify problems before they occur are examples of proactive maintenance.
* **process** A series of interrelated tasks that, together, transform inputs into a given output.
* **reactive maintenance** Maintenance used to correct problems when they arise during monitoring.
* **Reliability Monitor** A type of monitor that indicates event trends over a period of time in order to proactively identify system stability or performance problems.
* **Resource Monitor** Used to display the specific hardware resources used by processes on the system.
* **rogue process** Process that has encountered an error that forces it to use an unusually high amount of processor time.
* **Safe Mode** An advanced boot option that boots the system without network connectivity using the minimum configuration of devices and drivers. You can enter Safe Mode to access files and programs that allow you to resolve an issue that prevents the system from booting.
* **Task Manager** Used to quickly analyze the performance of a system, as well as identify and stop rogue processes and memory leaks.
* **thread** A unique sequence of instructions that is executed by a process.
* **troubleshooting procedure** A series of many tasks which can be used to efficiently solve a problem in a systematic manner.
* **Wireshark** A free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.