Microsoft

LESSON 6.4

98-365 Windows Server Administration Fundamentals

Understand Troubleshooting Methodology

LESSON 6.4

98-365 Windows Server Administration Fundamentals

Lesson Overview

In this lesson, you will learn about:

- Troubleshooting procedures
- Event Viewer
- Logging
- Resource Monitor

Anticipatory Set

If the workstation service failed to start, where would this event be recorded?

Troubleshooting Procedures

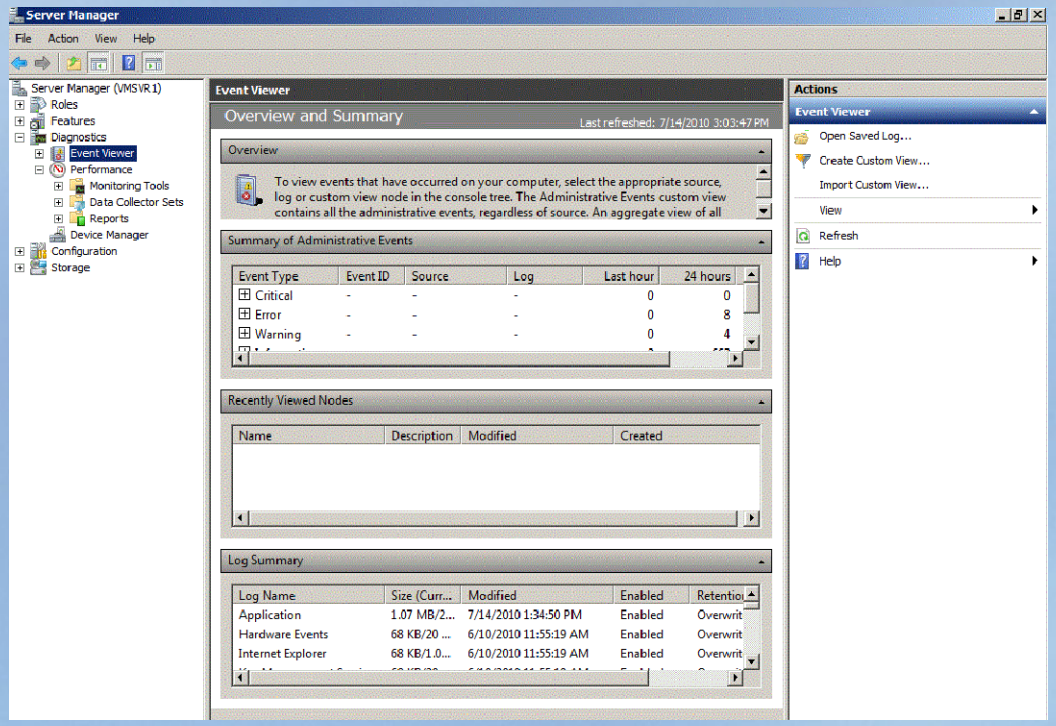
- Determine whether the problem is systemic or specific
  - Systemic—An approach used when there is more than one resource experiencing problems
    - Virus outbreak can affect several systems on a single network.
      - Solution: Isolate the network and clean affected machines.
  - Specific—An approach used when a problem has been isolated to a single system and related to a process, program or hardware. All other systems remain unaffected.
    - A system has a disk failure. This does not affect any other systems on the network.
      - Solution: Replace the failed disk.

LESSON 6.4

98-365 Windows Server Administration Fundamentals

Troubleshooting Procedures (continued)

Event Viewer is the first tool to be used to determine the time and type of problem that a machine may be having.



Event Viewer

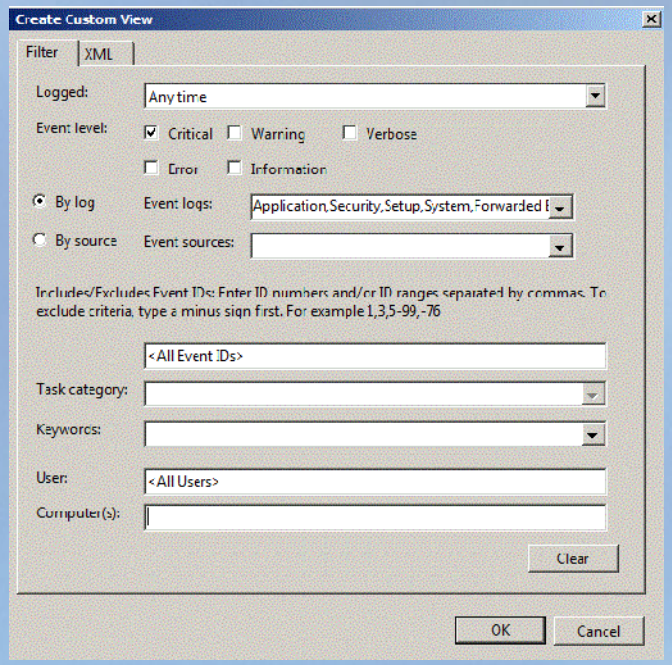
- Event Viewer has three default logs:
  1. Application—Contains events logged by applications or programs
  2. Security—Records events such as valid and invalid logon attempts, as well as events related to resource use such as creating, opening, or deleting files or other objects. An administrator can specify what events are recorded in the security log.
  3. System—Contains events logged by Windows® system components that are predetermined by Windows
- Other log files found in event viewer, if the computer is a Domain Controller:
  - Directory Service—Contains events logged by the Windows directory service
  - File Replication Service—Contains events logged by the Windows File Replication service
  - DNS Server—Contains events logged by the Windows DNS service such as events that resolve DNS names to Internet protocol (IP) addresses

Event Viewer (continued)

- Event Viewer event types:
  - Error—a significant problem, such as loss of data or loss of functionality.
  - Warning—might not be significant, but may indicate a possible future problem.
  - Information—describes the successful operation of an application, driver, or service.
  - Success Audit—an audited security access attempt that succeeds.
  - Failure Audit—an audited security access attempt that fails.
- The Event Log service starts automatically when you start Windows. All users can view application and system logs. Only administrators can gain access to security logs.

Event Viewer (continued)

- Event Filtering—can filter events based on a set of rules to determine which events in the log would be visible.
- Custom Views—saved filters that you intend on using again.



Logging

Windows primary log locations

1. Event Viewer logs
   - %systemroot%\system32\winevt\logs\<log file>.evtx
2. Microsoft® firewall logs
   - %systemroot%\system32\logfiles\firewall\firewall.log

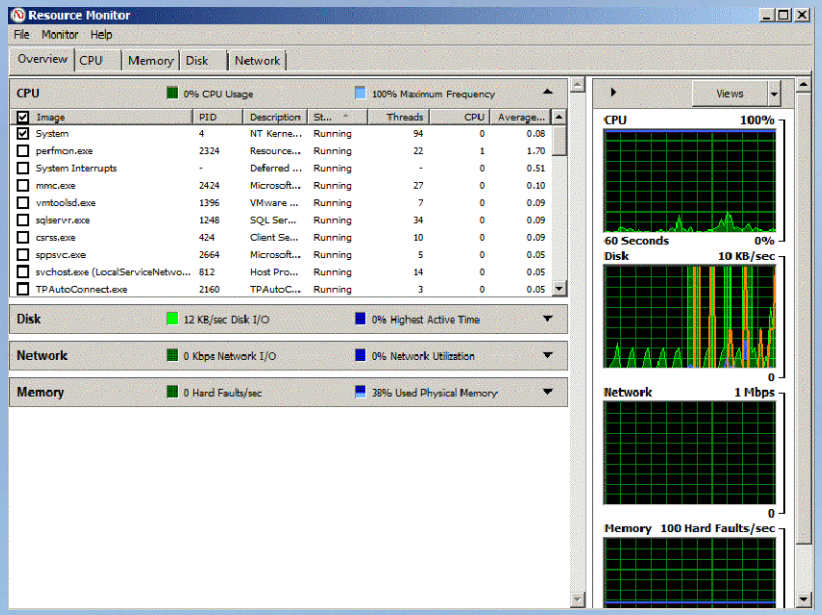
Most applications create their own log files upon installation.

LESSON 6.4

98-365 Windows Server Administration Fundamentals

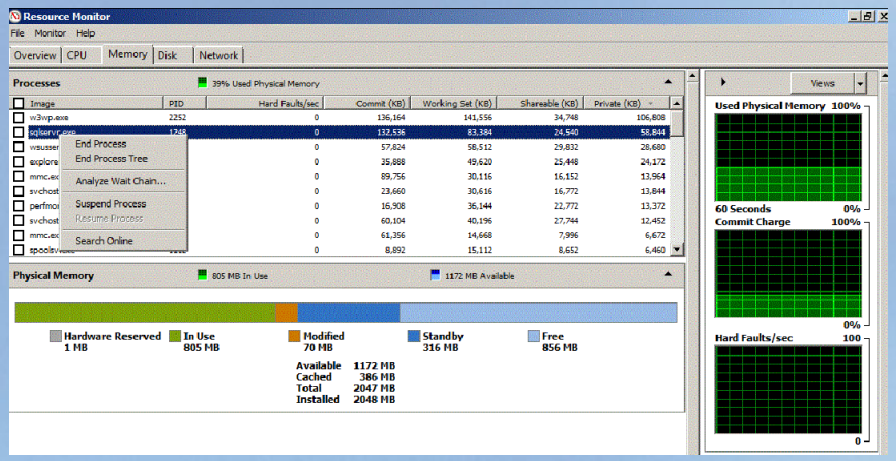
Resource Monitor

- A system tool that allows you to view information about the use of hardware (CPU, memory, disk, and network) and software (file handles and modules) resources in real time.
- You can filter the results according to specific processes or services that you want to monitor.



Resource Monitor (continued)

- Allows you to view all processes and either selectively end a single process or the entire process tree. You can also temporarily suspend a process.
- Allows you to view a process wait chain, and to end processes that are preventing a program from working properly.
- A process that is not responding will appear as a red entry in the CPU table of the Overview tab, and in the Process table of the CPU tab.



LESSON 6.4

98-365 Windows Server Administration Fundamentals

Lesson Review

- What are the three default event logs found in Windows Event Viewer?
- What is the default location for the event logs?
- What is the difference between systemic and specific troubleshooting?