STUDENT ACTIVITY 6.4_KEY: UNDERSTAND TROUBLESHOOTING METHODOLOGY

MTA Course: 98-365 Windows Server® Administration Fundamentals
Topic: Understand Troubleshooting Methodology
File name: WinServerFund_SA_6.4_Key

Lesson Objective

6.4: Understand troubleshooting methodology. *This objective may include but is not limited to:* processes; procedures; best practices; systematic vs. specific approach; perfmon; Event Viewer; Resource Monitor; Information Technology Infrastructure Library; central logging; event filtering; default logs

Resources, software, and additional files needed for this lesson

- Windows® Server 2008® R2
- Internet access

Directions to the student

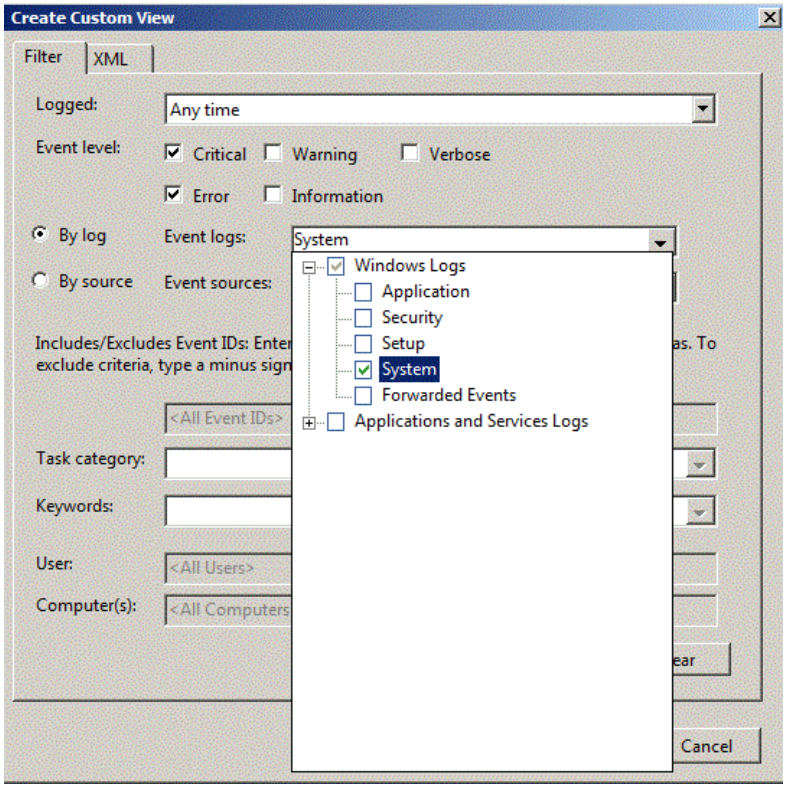
Complete the following activity. Have your instructor verify upon completion.

Content

Creating a Custom Filter in Event Viewer

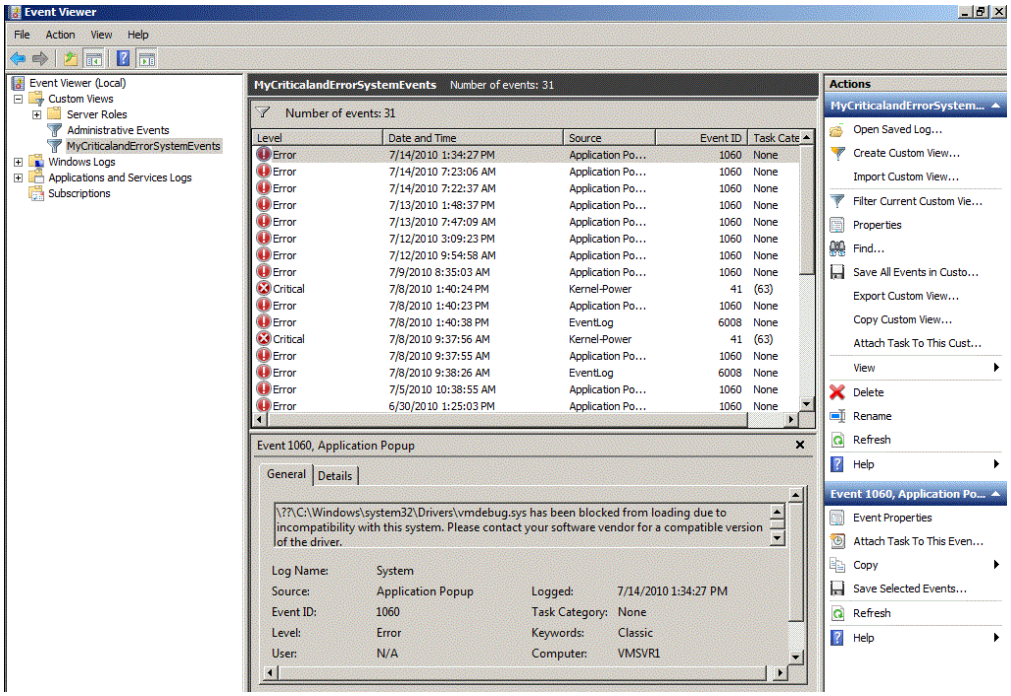
1. Log on to Windows Server 2008 R2 as Administrator.
2. Click **Start→All Programs→Administrator Tools** and click on **Event Viewer**.
3. Right-click on **Custom Views** and select **Create Custom View**.
4. In the Event level section, select **Critical** and **Error**.

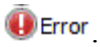
5. Select the By log section, click the drop down, expand **Windows Logs**, select **System** (see below) and then click **OK**.



6. In the Save Filter to Custom View screen, provide a name of **MyCriticalandErrorSystemEvents** and click **OK**.

7. Your results should look similar to the following (see below):

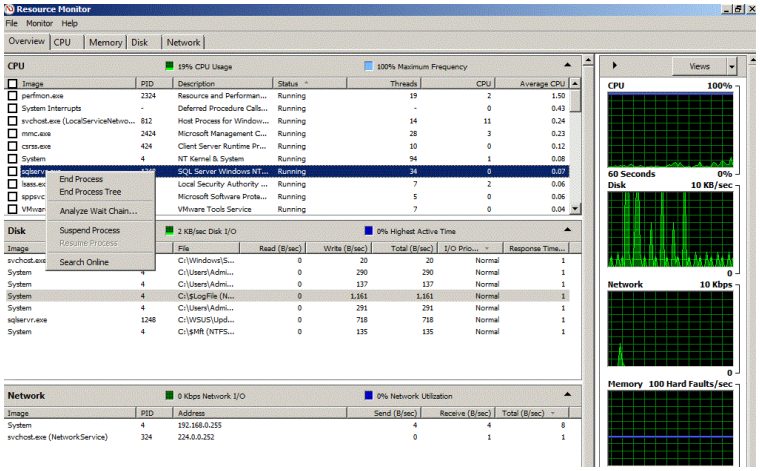


8. Double-click on a event with a level of Error 

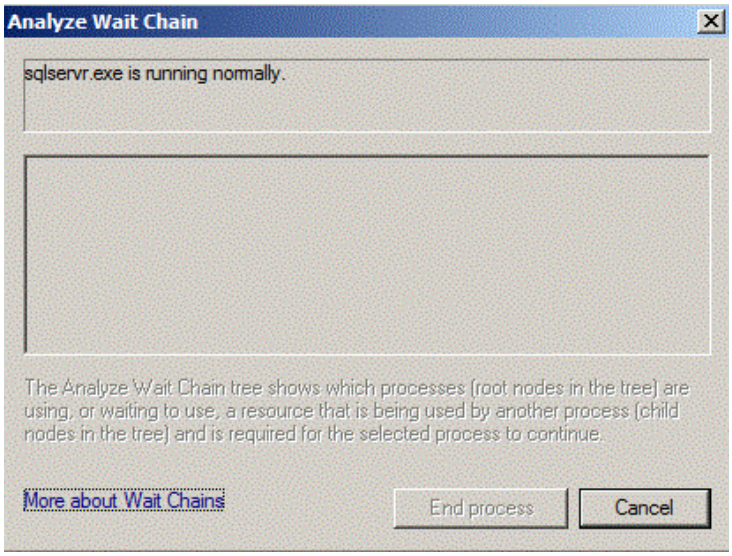
.
9. List the information related to that error:
   a. Log name: Answers will vary_____
   b. Source: Answers will vary_____
   c. Event ID: Answers will vary_____
   d. Level: Answers will vary_____
   e. Logged: Answers will vary_____
   f. User: Answers will vary_____
10. Using this information, open Internet Explorer® and perform a search for those items to find a reasonable solution. Items that you should be focused on are:
    a. Source
    b. Event ID
11. Have your instructor verify your search upon completion.
12. If your results are relevant, proceed with the recommendations provided by those results to correct the error.
13. Close all windows and programs.

Use Windows Resource Monitor to Analyze a Process

1. Authenticate to your Windows Server 2008 R2 as Administrator.
2. Click **Start**→ click in **Search programs and files** and type **resmon.exe** and press Enter.
3. Click the **Overview** tab.
4. Right-click on any process under the Image column and select **Analyze Wait Chain…** (see below).



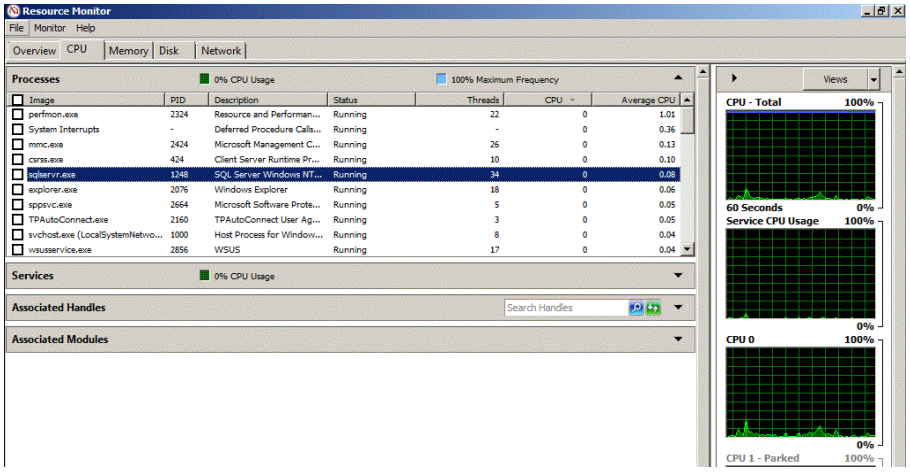
5. If everything is functioning properly, you should receive the results similar to the following (see below):



6. Close all windows and programs.

Use Resource Monitor to Identify Top CPU Resource Consumers

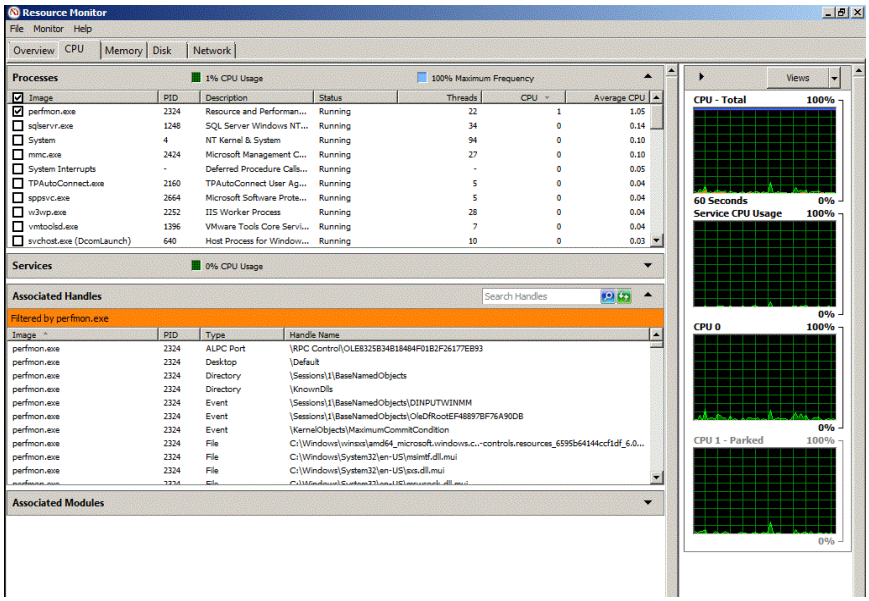
1. Authenticate to your Windows Server 2008 R2 as Administrator.
2. Click **Start**→ click in Search programs and files and type **resmon.exe** and press Enter.
3. Click the **CPU** tab.
4. In the Processes section, click the **CPU column** to sort by CPU resource consumption (see below).



5. Close all windows and programs.

Use Resource Monitor to Identify the Process That is Using a File

1. Log on to Windows Server 2008 R2 as Administrator.
2. Click **Start→** click in **Search programs and files** and type **resmon.exe** and press Enter**.**
3. Click the **CPU** tab.
4. Click an image's checkbox, e.g., perfmon.exe, to filter.
5. Click the title bar of **Associated Handles** to expand the table.
6. The results should display all the files that the selected process has opened (see below).



7. Have your instructor verify upon completion.