STUDENT ACTIVITY 5.3: UNDERSTAND LOGS AND ALERTS

MTA Course: 98-365 Windows Server® Administration Fundamentals
Topic: Understand Logs and Alerts
File name: WinServerFund_SA_5.3

Lesson Objective

5.3: Understand logs and alerts. *This objective may include but is not limited to*: purpose of performance logs and alerts.

Resources, software, and additional files needed for this lesson

- Windows® Server 2008® R2 or Windows 7®
- Performance logs from WinServerFund_SA_5.2

Directions to the student

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

Content

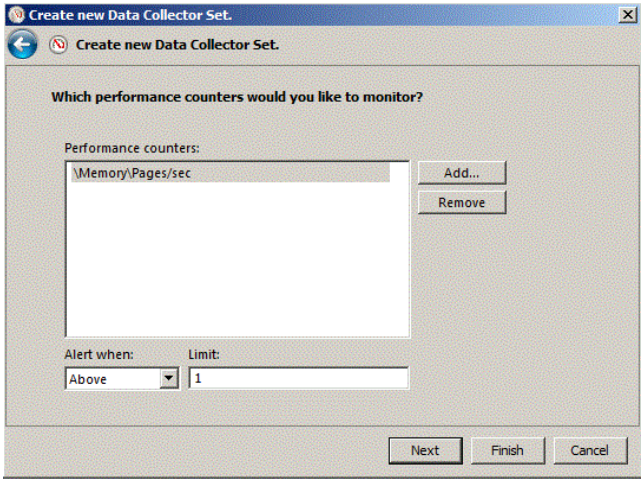
Comparing Multiple Log Files in Performance Monitor

1. Log onto your Windows Server 2008 R2 as Administrator.
2. Click **Start**, click in the **Search programs and files** box, type **perfmon /sys /comp**, and press Enter. Performance Monitor will open in stand-alone mode with comparison enabled.
   Note: You can only use overlay when Performance Monitor is running in stand-alone mode with comparison enabled.
3. Open logs (from WinServerFun_SA_5.2) or a data source and add counters from the logs or data source to the Performance Monitor display.
4. When you have finished creating your base view, repeat step 2 to open another instance of Performance Monitor running in stand-alone mode with comparison enabled.

5. To create a view you will use to compare to your base, open logs or a data source and add counters from the logs or data source to the second Performance Monitor display.
6. In the Performance Monitor window that you want to compare to your base, on the Compare menu, point to **Set Transparency** and select either 70% Transparency or 40% Transparency.
7. In the Performance Monitor window you want to compare to your base, on the Compare menu, click **Snap to Compare**. The active Performance Monitor window will automatically align itself with the other Performance Monitor window.
8. Have your instructor verify your log comparison upon completion.

Create a Data Collector Set to Monitor Performance Counters

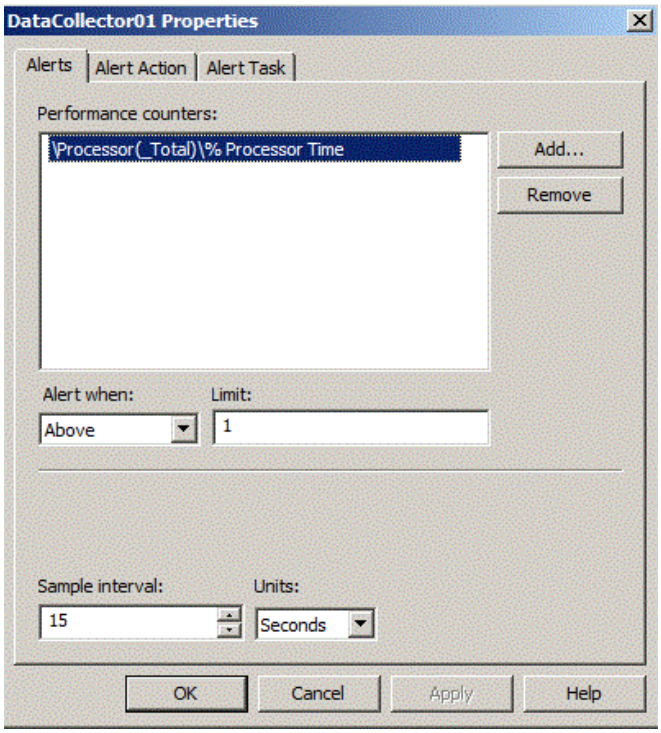
1. Log onto your Windows Server 2008 R2 as Administrator.
2. Launch Performance Monitor by clicking **Start→All Programs→Administrative Tools→Performance Monitor**.
3. In the Windows Performance Monitor navigation pane, expand **Data Collector Sets**, right-click **User Defined**, point to **New**, and click **Data Collector Set**. The Create new Data Collector Set Wizard starts.
4. Enter a name for your Data Collector Set called MyAlerts.
5. Select the **Create manually** option and click **Next**.
6. Select the **Performance Counter Alert** option and click **Next**.
7. Define alerts based on the values of performance counters you have selected.
8. From the list of Performance counters, select the counter to monitor and trigger an alert. Click **Add** to open the **Add Counters** dialog box. Add **Memory\Pages/sec** counter. When you are finished adding counters, click **OK** to return to the wizard (see below). Click **Next**.



9. From the **Alert when** drop-down, choose whether to alert when the performance counter value is above or below the limit of 2.
10. In the **Limit** box, enter the threshold value of 2.
11. When you are finished defining alerts, click **Next** to continue configuration.
12. After clicking **Next**, you can configure the Data Collector Set to run as a particular user. Click the **Change** button to enter the user name and password for a different user than the default listed.
13. Click **Finish** to return to Windows Performance Monitor.
14. To start the Data Collector Set immediately right-click on **MyAlerts** and select **Start this data collector set now**.

Configure Alert Actions

1. Log onto your Windows Server 2008 R2 as Administrator.
2. Launch Performance Monitor by clicking **Start→All Programs→Administrative Tools→Performance Monitor**.
3. Expand Data Collector Sets, expand User Defined, and click the name of the Data Collector Set, **MyAlerts**, with performance counter alerts.
4. In the console pane, right-click the name of a Data Collector whose type is Alert and click **Properties** (see below).



5. On the Data Collector Properties page, click the **Alerts** tab. The data collector's alerts already configured should appear.
6. Click the **Alert Action** tab to choose to write an entry to the event log Applications and Services Logs/Microsoft/Windows/Diagnosis-PLA/Operational when the alert criteria are met. You can also start a Data Collector Set when the alert criteria are met.
7. Click the **Alert Task** tab to choose a Windows Management Interface (WMI) task and arguments to run when the alert criteria are met.
8. Have your instructor verify that you have created your alert.