

LESSON 5.3

98-365 Windows Server Administration Fundamentals

# Understand Logs and Alerts

## LESSON 5.3

### 98-365 Windows Server Administration Fundamentals

## Lesson Overview

In this lesson, you will learn:

- Managing performance logs
- Creating performance alerts

## LESSON 5.3

### 98-365 Windows Server Administration Fundamentals

## **Anticipatory Set**

- What is a benefit of performance and reliability monitoring?

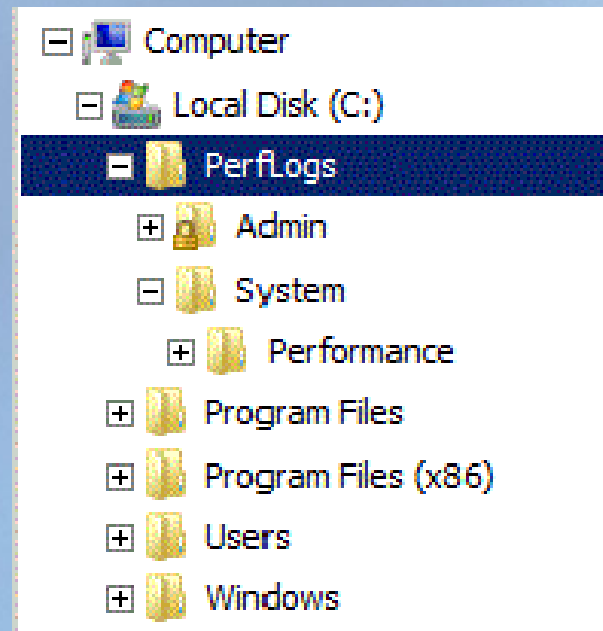
## LESSON 5.3

### 98-365 Windows Server Administration Fundamentals

# Managing Performance Logs

The default location for performance logs is:

<system drive>:\PerfLogs





## **Managing Performance Logs (continued)**

Administrators can manage log files several ways:

- Open existing log files in Performance Monitor
- Compare multiple log files in Performance Monitor

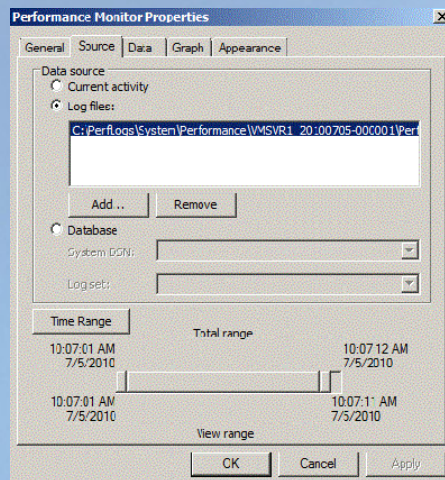
## LESSON 5.3

### 98-365 Windows Server Administration Fundamentals

# Managing Performance Logs (continued)

## Open Existing log files in Performance Monitor

- In the Windows® Performance Monitor navigation pane, expand Monitoring Tools and click Performance Monitor.
- In the console pane toolbar, click the **View Log Data** button. The Performance Monitor properties page will open at the Source tab.
- In the Data Source section, select **Log files** and click **Add**.



## Managing Performance Logs (continued)

### Compare multiple log files in Performance Monitor

1. Click **Start**, click in the **Start Search** box, type **perfmon /sys /comp**, and press Enter. Performance Monitor will open in stand-alone mode with comparison enabled.

**You can use overlay only when Performance Monitor is running in stand-alone mode with comparison enabled.**

2. To create a view you will use as a base to compare against, open logs or a data source and add counters from the logs or data source to the Performance Monitor display.
3. When you have finished creating your base view, repeat step 1 to open another instance of Performance Monitor running in stand-alone mode with comparison enabled.

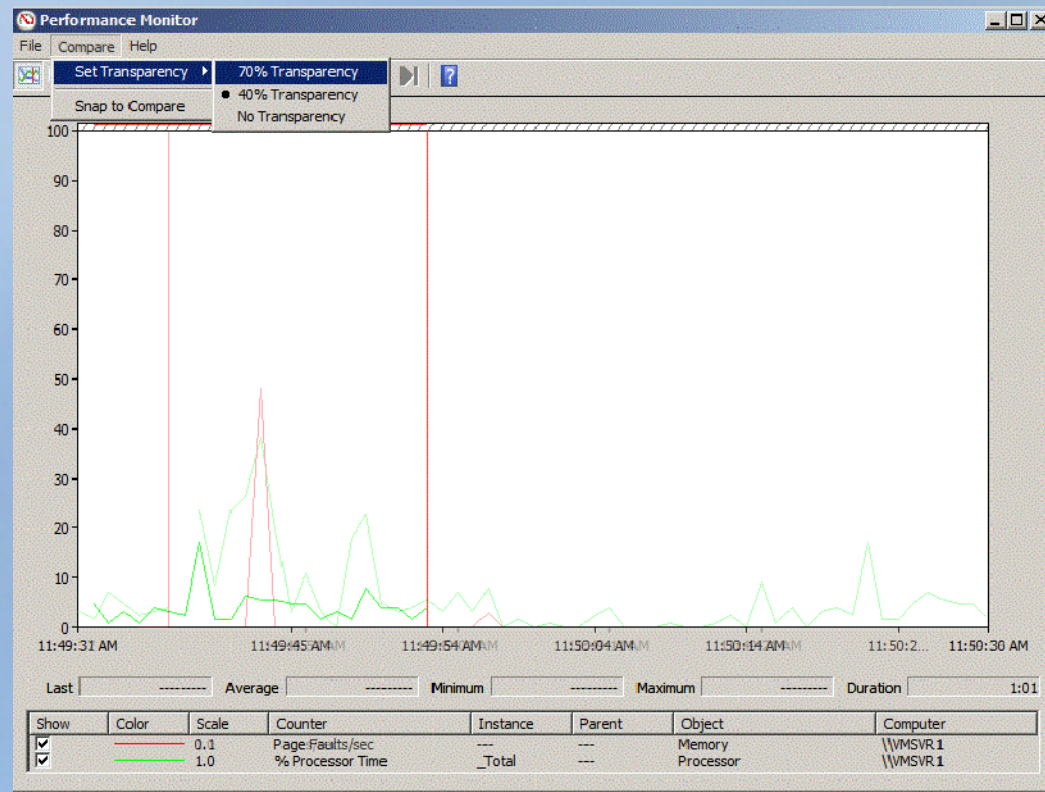


## LESSON 5.3

### 98-365 Windows Server Administration Fundamentals

# Managing Performance Logs (continue)

Compare multiple log files in Performance Monitor



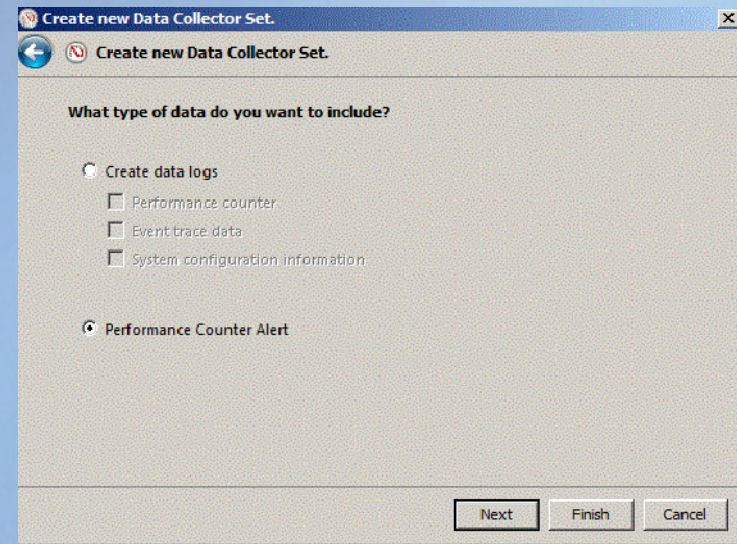
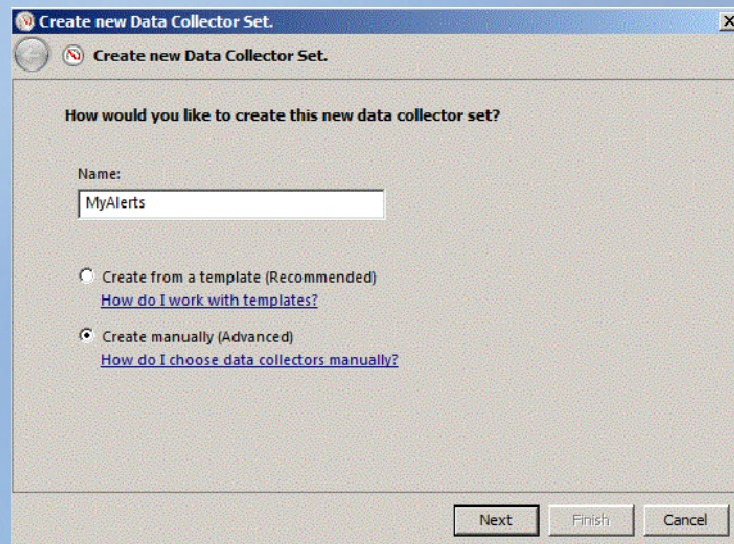


## LESSON 5.3

### 98-365 Windows Server Administration Fundamentals

# Creating Performance Alerts

- You can create a custom Data Collector Set containing performance counters and configure alert activities based on the performance counters exceeding or dropping below limits you define.
- After creating the Data Collector Set, you must configure the actions the system will take when the alert criteria are met.

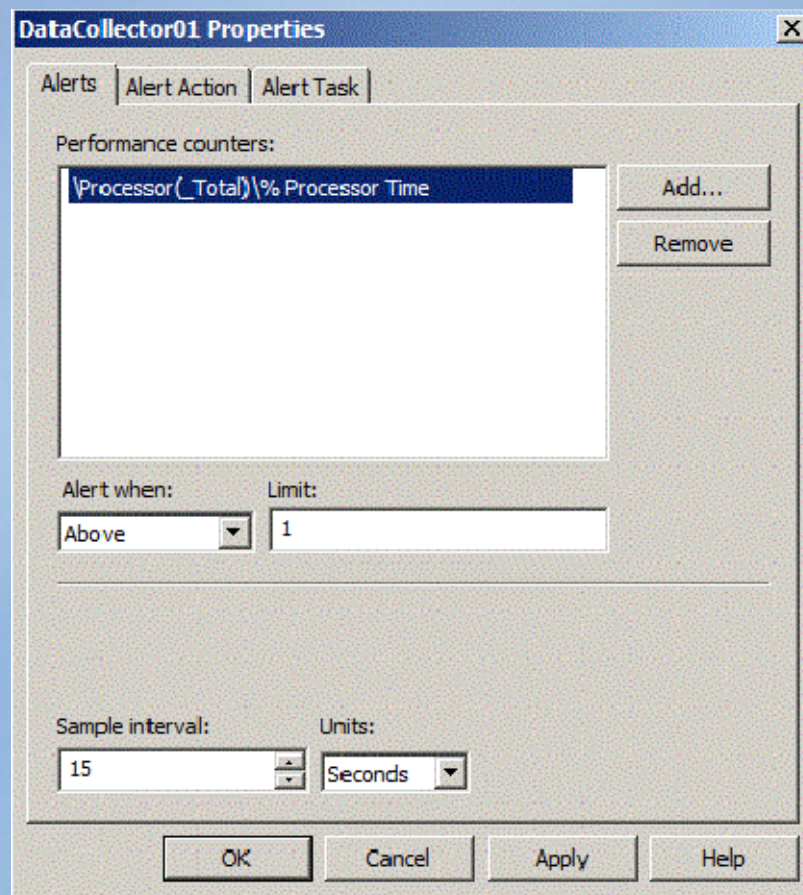




## LESSON 5.3

### 98-365 Windows Server Administration Fundamentals

# Creating Performance Alerts (continued)



The 'DataCollector01 Properties' dialog box is shown with the 'Alerts' tab selected. The 'Performance counters' list contains the entry '\Processor(\_Total)\% Processor Time'. To the right of this list are 'Add...' and 'Remove' buttons. Below the list, the 'Alert when:' dropdown is set to 'Above' and the 'Limit:' text box contains the value '1'. At the bottom, the 'Sample interval:' is set to '15' and the 'Units:' dropdown is set to 'Seconds'. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom of the dialog.

**DataCollector01 Properties**

Alerts | Alert Action | Alert Task

Performance counters:

\Processor(\_Total)\% Processor Time

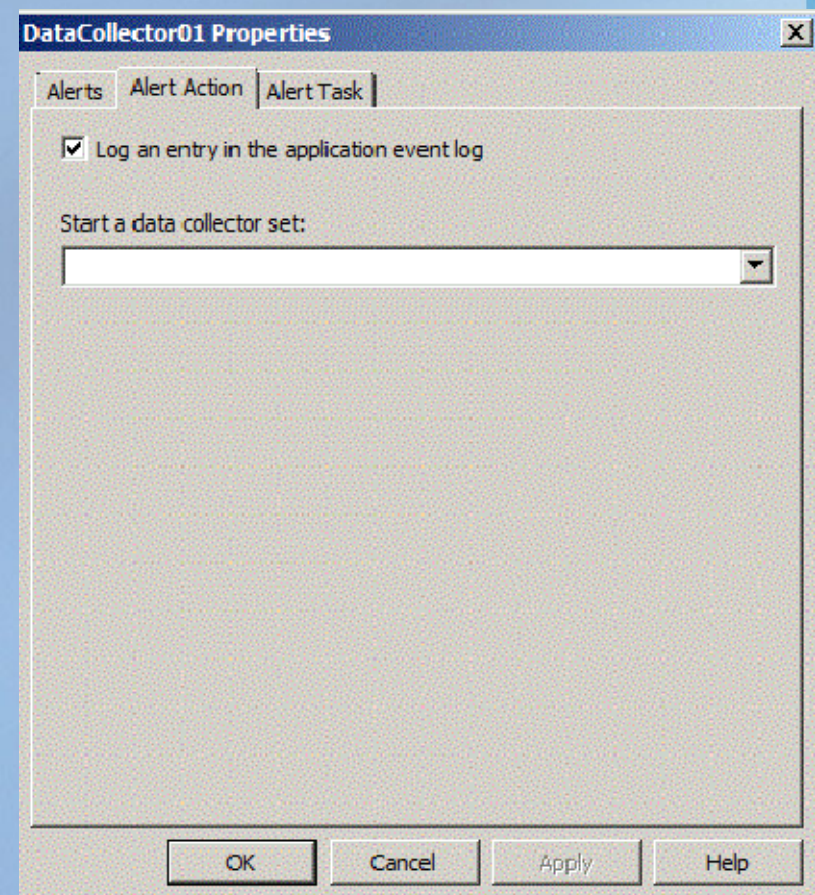
Add...

Remove

Alert when: Above Limit: 1

Sample interval: 15 Units: Seconds

OK Cancel Apply Help



The 'DataCollector01 Properties' dialog box is shown with the 'Alert Action' tab selected. The 'Log an entry in the application event log' checkbox is checked. Below this, the 'Start a data collector set:' dropdown menu is empty. The 'OK', 'Cancel', 'Apply', and 'Help' buttons are at the bottom of the dialog.

**DataCollector01 Properties**

Alerts | Alert Action | Alert Task

☒ Log an entry in the application event log

Start a data collector set:

OK Cancel Apply Help

## Lesson Review

- What is the default location for performance log files?
- What is the event log file that alerts can be written to?
- What type of data collector set must be created in order to configure performance alerts?