Lab 14A: Using Task Manager and Event Viewer

BETA MATERIALS for Microsoft Certified Trainer preparation purposes only

Objectives

After completing this lab, you will be able to:

- Monitor application performance by using Task Manager.
- Shut down applications by using Task Manager.
- Review computer activity by using Event Viewer.
- Manage event logs.
- Find information in event logs.

Lab Setup

To complete this lab, you need the following:

- Completed Lab 1C Upgrading Windows 98 to Windows XP Professional.
- A computer running Microsoft® Windows® XP Professional
- Lab files are located on the Student CD in the Labfiles folder. The required files are: App1-1.exe, App1-2.exe, App1-3.exe, App1-4.exe, App1-5.exe, Lab14.cmd, and Syslog.csv.

Estimated time to complete this lab: 45 minutes

Exercise 1
Monitoring Applications by Using Task Manager

Scenario

You are supporting computers running Windows XP Professional. One of the users that you support is complaining about her computer performance when she runs multiple applications. You need to find out which application is causing the problems so that you can take corrective action.

Goal

In this exercise, you will run several application on your computer and use Task Manager to determine which system resources that these running programs are using. You will then use Task Manager to stop a program.

<table>
<tr><th>Tasks</th><th>Detailed Steps</th></tr>
<tr><td><b>1.</b> Log on as Administrator with a password of <b>password</b>, and then run Lab14.cmd in the Labfiles\Mod14 folder.</td><td><b>a.</b> Log on as Administrator with a password of <b>password</b>.
<b>b.</b> Start <b>Lab14.cmd</b> located in \Labfiles\Mod14 located on the Student CD.
<i>This will start 4 applications App1-1 through App1-5 on your computer.</i></td></tr>
<tr><td><b>2.</b> Use Task Manager to determine which application is using the majority of system resources, and which system resources (memory, disk, processor) it is using.</td><td><b>a.</b> Press CTRL+ALT+DELETE, and then click <b>Task Manager</b>.
<b>b.</b> On the <b>Applications</b> tab, review the programs that are running.</td></tr>
<tr><td colspan="2">Does the list contain any operating system processes? Why or why not?
<b>No. The list contains no operating system process because the Applications tab lists only processes that are running in the current user’s security context.</b>
____
____
____
____</td></tr>
<tr><td><b>2.</b> <i>(continued)</i></td><td><b>c.</b> Click the <b>Performance</b> tab.</td></tr>
</table>

<table>
<tr><th>Tasks</th><th>Detailed Steps</th></tr>
<tr><td colspan="2">❓ Which system resources are used heavily?
<b>CPU usage is at or near 100 percent.</b></td></tr>
<tr><td><b>2.</b> <i>(continued)</i></td><td><b>d.</b> Click the <b>Processes</b> tab.</td></tr>
<tr><td colspan="2">❓ Which process is displaying the highest current CPU usage? Does this usage indicate a problem?
<b>App1-5 has the highest CPU usage. This usage could indicate a problem because this program’s CPU usage is preventing other programs from gaining processor time.</b></td></tr>
<tr><td><b>2.</b> <i>(continued)</i></td><td><b>e.</b> On the <b>View</b> menu, click <b>Select Columns</b>.
<b>f.</b> In the <b>Select Columns</b> dialog box, select the <b>CPU Time</b> check box, and then click <b>OK</b>.
<b>g.</b> Drag the border of the Windows Task Manager window down and to the right until you can see all columns and all rows.</td></tr>
<tr><td colspan="2">❓ Which process has used the most CPU time since your computer was started? Does this usage indicate a problem? Why or why not?
<b>The System Idle process has used the most CPU time. This usage does not indicate a problem, because the time that is displayed for the System Idle process indicates that the computer’s processor was not busy.</b></td></tr>
</table>

Tasks	Detailed Steps
3. Close the application that is using most of the CPU.	**a.** Right-click the process using the majority of CPU. *A Task Manager Warning message box appears. Read the message text. It tells you terminating a process may cause undesired results.* **b.** On the **Task Manager Warning** message box, click **No**. **c.** Click **Applications**, right-click the application that is using most of the CPU, and then click **End Task**. **d.** When the application is removed from the list, click **Performance**
What is the total CPU usage now? **Answers will vary, but should be about 4 percent**	
3. (*continued*)	**e.** Click **Applications**, and then close App1-1, App1-2, App1-3, App1-4, and then minimize Task Manager.

Exercise 2
Adjusting Base Priorities

In this exercise, you will adjust base priorities on running processes.

Scenario

You are supporting computers running Windows XP Professional. One of the users that you support is complaining about his computer's performance when he runs multiple applications. You want to adjust base priorities on some of the applications that are running to see if the computer performance improves.

Tasks	Detailed steps
1. You will start multiple instances of App1-5.	**a.** In Windows Explorer, open the \Labfiles\Mod14 folder, and then double-click **App1-5.exe** to start the application. **b.** Repeat step a two more times, as you want to run three instances of App1-5.exe.
⚠ **Important:** By running three instances of App 1-5, the computer may be very slow to respond. Therefore, you do not need to click multiple times. Click once, and then wait for the computer to respond.	
1. (*continued*)	**c.** Restore **Task Manager**. **d.** In **Windows Task Manager**, click **Processes**. *The three instances of App1-5 should be using approximately 98 percent of the CPU.* **e.** Right-click one of the instances of **App 1-5**, click **Set Priority**, and then click **BelowNormal**. **f.** When the **Task Manager Warning** message appears, click **Yes**. *The CPU usage will drop to zero with an occasional jump to less then 5 percent, the other two instances will total approximately 98 percent e.* **g.** Right-click one of the other instances of **App 1-5**, click **Set Priority**, and then click **BelowNormal**. **h.** When the **Task Manager Warning** message appears, click **Yes**. *Now the two instances of App 1-5 are using less then 5 percent CPU each and the third instance is using between 93 percent and 97 percent.* **i.** Right-click one of the two instances of **App 1-5** with low priority, click **Set Priority**, and then click **AboveNormal**. **j.** When the **Task Manager Warning** message appears, click **Yes**. *This time, the instance of App 1-5 with a priority above normal is using approximately 90 to 95 percent of the CPU, while the instances with normal priority and below normal priority are both at 0 occasionally jumping to about 5 percent.* **k.** Click the instance of **App 1-5** with an above normal priority, and then click **End Process**.

Tasks	Detailed steps
1. (*continued*)	**l.** When the **Task Manager Warning** message appears, click **Yes**. *Now the instance of App 1-5 with a normal priority is running mostly in the mid 90 percent range and the instance with a below normal priority is at zero, and occasionally jumps to approximately 5 percent.* **m.** Close both instances of App 1-5 that are running. **n.** Close Task Manager.

Exercise 3
Reviewing Computer Activities by Using Event Viewer

Scenario

To ensure that your computer is running without problems, you regularly use Event Viewer to review system activity during the last week. Also, your organization's security policy requires you to review and archive your computer's system logs weekly.

Goal

In this exercise, you will review the Windows XP Professional log files, configure log file archiving, and archive a log file.

Tasks	Detailed Steps
1. Use Event Viewer to determine the last time that your computer was started.	**a.** Click **Start**, right-click **My Computer**, and then click **Manage**. **b.** In Computer Management, expand **Event Viewer**. **c.** In the console tree, click **System Log**. **d.** In the details pane, find the most recent event with **Eventlog** as its source, and then double-click the event.
ℹ **Note:** Windows XP Professional automatically starts the event log service each time that the computer starts. The time that the event log service started is the approximate time that your computer started.	
1. *(continued)*	**e.** Click **OK** to close the **Event Properties** dialog box. **f.** Review the types of events in each of the event logs. **g.** Do not close Event Viewer.

Exercise 4
Archiving the Application Log

Scenario

One of the computers that you support has been experiencing problems. You want to start with a clean event log, but you want to keep the existing event log.

Goal

In this exercise, you will archive your computer's application log.

Tasks	Detailed Steps
1. Save the Application Log file as ***yyyy-mm-dd*.evt** (where *yyyy* is the current year, *mm* is the current month, and *dd* is the current date) in the Mod14 folder, and then clear the Application Log.	**a.** In Event Viewer, in the console tree, click **Application Log**. **b.** On the **Action** menu, click **Save Log File As**. **c.** In the **Save "Application " As** dialog box, beside the **Save in** drop down list, click **Create New Folder** icon (if you are not sure which icon this is let the cursor sit on the icon for a few seconds). Name the new folder **Mod14**. **d.** Double-click the **Mod14** folder. **e.** In the **File name** box, type ***yyyy-mm-dd*.evt** (where *yyyy* is the current year, *mm* is the current month, and *dd* is the current day), and then click **Save**. **f.** On the **Action** menu, click **Clear all Events**. **g.** In the **Event Viewer** message, click **No** to clear the events without saving them.

Exercise 5
Searching for Specific Events in a Saved Event Log File

Scenario

One of the computers that you support cannot detect network resources. While troubleshooting the problem, you determine that the computer does not have an IP address assigned by the DHCP service. You want to view the event logs for any warnings or errors that may show what is causing the problem.

Goal

In this exercise, you will filter for specific events and search the System Log for instances of problems with DHCP.

Tasks	Detailed Steps
1. Open the saved security log file, \Labfiles\Mod14\Lab14.evt, and then view the first entries.	**a.** In the console tree, right-click **Event Viewer (Local)**, and then click **Open Log File**. **b.** In the **Open** dialog box, in the **Look in** box, open the \Labfiles\Mod14 folder if necessary, and then click **Lab14.evt**. **c.** In the **Log Type** box, click **System**, and then click **Open**. **d.** Double-click the first event in the log. **e.** Click the down arrow to move to, view the information in the next event.
❓ Is examining each event the most efficient way to look for specific events? **No. Because of the high number of events that will appear in the logs, you will need some way to filter out the events that do not concern you during the present search.**	
1. *(continued)*	**f.** Click **Cancel** to close the **Event Properties** dialog box.
2. Filter the log entries so that only failure events appear, and then sort the entries by category.	**a.** In the console tree, right-click **Saved System Log**, point to **View**, and then click **Filter**. **b.** In the **Saved System Log Properties** dialog box, under **Event types**, clear all of the check boxes except for the **Warning** and **Error** check boxes. **c.** In **Event source** select **DHCP**, and then click **OK**. **d.** Double-click the first DHCP entry.

Tasks	Detailed Steps
❓	Based on the information in the description section of the event, why does the computer not have a DHCP address? **The Computer automatically configured an IP address.**
2. *(continued)*	**e.** Click **OK** to close the **Event Properties** dialog box.

Exercise 6
Saving a Security Log File in an Alternate File Format

Scenario

You want to save the system log information in a comma-delimited text file, so that you can import the information into Microsoft Excel for further analysis.

Goal

In this exercise, you will save the previously saved system log file as a comma-delimited text file.

Tasks	Detailed Steps
1. Save the Lab14.evt security log in comma-delimited format as \Labfiles\Mod14\Seclog.csv, and then use Notepad to view this file.	**a.** In the console tree, right-click **Saved System Log**, and then click **Save Log File As**. **b.** In the **Save "Saved System Log" As** dialog box, \Mod14 folder if necessary, and then in the **File name** box, type **Syslog** **c.** In the **Save as type** box, click **CSV (Comma delimited) (*.csv)**, and then click **Save**. **d.** Close Event Viewer. **e.** Click **Start**, click **All Programs**, click **Accessories**, and then click **Notepad**. **f.** From the **File** menu, click **Open**, double-click Lab14. **g.** In **File of types**, select **All Files**, and then double-click **Syslog**. **h.** Maximize Notepad. **i.** On the **Edit** menu, click **Find**. **j.** In the **Find what** box, type **DHCP** and then click **Find Next**. **k.** In the **Find** dialog box, click **Cancel**. *You just found the DHCP Error in the CSV file that you were viewing in the event log. You could import this data to a Microsoft Excel spreadsheet or Microsoft Access database.* **l.** Close Notepad, and then log off.