Лабораторна робота №8

Моніторинг системних ресурсів та керування ними

Мета: освоїти основи роботи з адміністративними інструментами для моніторингу та керування системними ресурсами у Windows (на прикладі Windows 10).

Інструменти: Windows 10, встановлена на фізичний комп’ютер, або віртуальна машина з Windows 10.

Завдання лабораторної роботи

*Ця лабораторна робота пов’язана з курсом **ITE 8 (розділ 11)**.*

Виконайте ***лабораторну роботу 11.3.1.11 “Monitor and Manage System Resources” (адаптовані версії роботи розміщена у додатку 8.1).***

Вимоги до звіту

Звіт має містити: тему, мету, скриншоти з Windows, на яких показано хід виконання завдань лабораторної роботи, відповіді на запитання лабораторної роботи 11.3.1.11 “Monitor and Manage System Resources”.

Завдання до лабораторної роботи 11.3.1.11 розміщене у *додатку 8.1* (україномовна та англомовна адаптовані версії).

Додаток 8.1

Адаптовані версії лабораторної роботи
11.3.1.11 “Monitor and Manage System Resources”
(курс IT Essentials 8)

[Українською]

Лабораторна робота - Моніторинг системних ресурсів та керування ними

Вступ

У цій лабораторній роботі ви будете використовувати адміністративні інструменти для моніторингу та керування системними ресурсами.

Рекомендоване обладнання

ПК з Windows з доступом в Інтернет

Інструкції

Частина 1: Перегляд подій (Event Viewer)

У цій частині "Безпека у Windows" використовується для дослідження Переглядача подій, коли стан служби змінюється. Безпека у Windows - це вбудований компонент захисту від шкідливих програм в Windows.

Крок 1: Перевірка роботи Захисника Windows.

Примітка: Для роботи Безпека у Windows на комп'ютері необхідно видалити антивірусні або антишпигунські програми**.**

Увійдіть у Windows з обліковим записом адміністратора.

Щоб визначити, чи зупинена служба Безпека у Windows, натисніть **Пуск**, знайдіть **Безпека у Windows**.

У Windows 10 натисніть **Захист від вірусів і загроз**. Прокрутіть вниз до **Настройки захисту від вірусів і загроз**. Натисніть **Керування параметрами**. Під заголовком «Захист у реальному часу» переконайтеся, що перемикач **Увімкнуто**.

У Windows 8.1 у вкладці **Головна** переконайтеся, що захист в режимі реального часу включений. Якщо Безпека у Windows не відкривається, перейдіть в **Настройки** натисніть **Оновлення та захист**> знайдіть **Безпека у Windows**. Натисніть **Увімкнути зараз** для захисту від програм-шпигунів і небажаних програм (важливо) і захисту від вірусів (важливо).

У Windows 7 ви отримаєте повідомлення: **Ця програма відключена** у вікні Windows Defender. Натисніть **Натиснути тут, щоб включити** у вікні, а потім натисніть **Закрити**, щоб продовжити.

Залиште Захисник Windows відкритим.

Крок 2: Вивчення консолі «Служби».

> **Примітка**: Хоча більшістю служб Windows можна керувати через консоль «Служби», в Windows 10 і 8.1 неможливо зупинити **Безпека у Windows** з **консолі** Служби Windows**.**

Натисніть **Пуск**> пошук **Панель керування**. В панелі керування в поданні дрібних піктограм натисніть **Адміністрування**> **Керування комп'ютером.** У вікні **Керування комп'ютером** розкрийте **Служби та застосунки** і виберіть **Служби**.

Прокрутіть у вікні Керування комп'ютером в розділі Служби, щоб знайти **Служба мережевої перевірки Антивірусу для Захисника Windows** (Windows 10) або **Служба захисника Windows** (Windows 8.1) або **Захисник Windows** (Windows 7).

Запитання:

Який стан служби?

Запишіть тут свою відповідь.

Додайте до звіту **скриншот вікна оснащення Служби** так, щоб було видно знайдену службу та її стан.

Закрийте вікно **Керування комп'ютером**. Поверніться назад до Windows Defender і вимкніть його.

У Windows 10 натисніть **Захист від вірусів і загроз**. Прокрутіть вниз до **Настройки захисту від вірусів і загроз**. Натисніть **Керування параметрами**. У розділі Захист у реальному часі натисніть перемикач, щоб вимкнути його. Натисніть **Так** аби дозволити цій програмі робити зміни на вашому пристрої.

У Windows 8.1 на вкладці **Параметри** виберіть вкладку **Параметри**. На вкладці Параметри виберіть **Адміністратор.** Натисніть **Увімкнути цей додаток** для виключення Захисника Windows. Натисніть **Зберегти зміни** для виключення Захисника Windows. Натисніть **Закрити** у спливаючому вікні, як необхідно.

У Windows 7 натисніть **Налаштування.** Натисніть **Параметри.** У вікні «Параметри» виберіть **Адміністратор**> натисніть **Використовувати цю програму.** Натисніть **Зберегти** для зупинки Захисника Windows. Натисніть **Закрити** для продовження, коли з'явиться попередження про те, що ви виключаєте його.

Поверніться в «Служби». (**Панель керування** в поданні з дрібними піктограмами > **Адміністрування** > **Служби**). Натисніть **Дія** > **Оновити.**

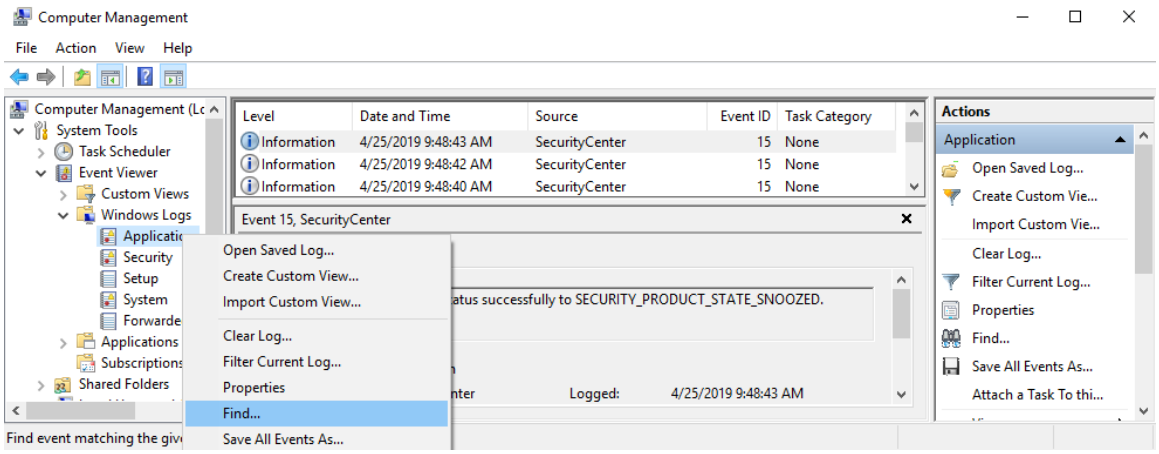
Знайдіть **Служба мережевої перевірки Антивірусу для Захисника Windows** (Windows 10) або **Служба захисника Windows** (Windows 8.1) або **Захисник Windows** (Windows 7). Запишіть стан Безпека у Windows.

Запишіть тут свою відповідь.

Додайте до звіту **скриншот вікна оснащення Служби** так, щоб було видно знайдену службу та її стан.

Перейдіть в Перегляд подій (Event Viewer). У вікні Керування комп'ютером розкрийте **Системні інструменти** > **Перегляд подій (Event Viewer)** > виберіть **Журнали Windows (Windows Logs)**> виберіть **Застосунок (Application)** (Windows 10), виберіть **Система** (Windows 8.1 і 7).

В панелі Застосунок (Application) або Система ви можете знайти найостанніші події, пов'язані з Безпека у Windows. Натисніть правою кнопкою миші по потрібному журналі виберіть **Знайти(Find)**. Введіть **defender** для пошуку записів, пов'язаних з Безпека у Windows.



На вкладці Загальні (General), що вказано як Джерело (Source) події? Який рівень вираженості?

Запишіть тут свою відповідь.

Додайте до звіту **скриншот вікна оснащення Event Viewer** так, щоб було видно джерело події та рівень вираженості.

Поверніться назад до Безпека у Windows і ввімкніть його. Закрийте Безпека у Windows.

Перейдіть в Перегляд подій (Event Viewer), щоб переглянути найостанніші записи подій, пов'язані з Безпека у Windows.

Частина 2: Вивчення впливу служб.

У цій частині ви зупините службу **Диспетчер друку (Print Spooler)**, щоб вивчити вплив на систему. Диспетчер друку відповідає за керування завданнями принтера і взаємодію з принтером. Якщо ця служба відключена, друк стане неможливим і не буде видно свої принтери.

Крок 1: Перевірка служби друку

Відкрийте **Блокнот**. Натисніть **Пуск** і знайдіть **Блокнот**.

У **Блокнот**, натисніть **Файл** > **Друк**. Запишіть вказаний нижче принтер. **Примітка**: Вам не потрібно встановлювати фізичний принтер.

Напишіть тут свою відповідь.

Додайте до звіту **скриншот вікна друку** так, щоб було видно цей принтер.

Натисніть **Скасувати** щоб вийти з діалогового вікна принтера.

Крок 2: Зупинка диспетчера друку

Відкрийте консоль Служби (Services). (Панель управління> Адміністрування> Services).

Натисніть правою кнопкою миші **Диспетчер друку** та виберіть **Зупинити (Stop)**.

Перейдіть до **Блокнот**. Виконайте спробу друку.

Запитання:

Яке повідомлення ви отримали? Як би ви це виправили?

Запишіть тут свою відповідь.

Додайте до звіту **скриншот вікна повідомлення**, яке ви одержали.

Натисніть **OK** або **Ні** у вікні повідомлення та натисніть **Скасувати** для виходу з вікна друку.

Крок 3: Перезапуск диспетчера друку

Перейдіть до консолі **Служби (Services)** і перезапустіть диспетчер друку. Натисніть правою кнопкою миші **Диспетчер друку (Print Spooler)** та виберіть **Запустити (Start)**.

Переконайтеся в тому, що можете друкувати.

Крок 4: Вивчення служби DHCP клієнт (DHCP Client)

Служба DHCP клієнт реєструє і оновлює IP-адреси і записи DNS для ПК. Якщо ця служба зупинена, ПК не отримуватиме динамічну IP-адресу і оновлення DNS.

В консолі Служби знайдіть **DHCP клієнт (DHCP Client)**. Натисніть правою кнопкою миші на **DHCP Client** і виберіть **Зупинити (Stop)**.

Запитання:

Коли DHCP клієнт зупиняється, які інші служби також будуть зупинені?

Напишіть тут свою відповідь.

Додайте до звіту **скриншот вікна оснащення Служби** так, щоб було видно виконані там дії.

Натисніть **Ні (No)** у вікні **Зупинити інші служби (Stop Other Services)**.

Запитання:

Чому важливо проявляти обережність при керуванні службами?

Запишіть тут свою відповідь.

Перевірте **DHCP Client**, чи він ще запущений.

Частина 3: Відстеження та запис використання системи за допомогою панелі Адміністрування

Ви налаштуєте розширені функції Адміністрування та будете контролювати використання системних ресурсів комп’ютера.

Крок 1: Створення нового набору збирача даних.

Перейдіть до Панелі керування> натисніть Адміністрування> натисніть Керування комп'ютером > розгорніть Системні інструменти.

Розгорніть **Продуктивність (Performance)**> розгорніть **Набори колектора даних (Data Collector Sets)**> на панелі ліворуч натисніть правою кнопкою миші **Визначено користувачем (User Defined)**> виберіть **Створити (New)** > натисніть **Набір колектора даних (Data Collector Set)**.

У вікні **Створити новий набір збирача даних (Create new Data Collector Set)** введіть **Memory Logs** в поле Ім'я (Name). Виберіть перемикач **Створити вручну (розширений) (Create manually (Advanced))** та натисніть **Далі**.

У розділі Який тип даних ви хочете включити? (What type of data do you want to include?), виберіть Лічильник ефективності (Performance counter) та натисніть кнопку Далі.

Відкриється екран **Які лічильники продуктивності ви хочете додати? (Which performance counters would you like to log?)**. Вікно, натисніть **Додати (Add)**. У списку доступних лічильників знайдіть і розгорніть **Пам'ять (Memory)**. Виберіть **Доступні Мбайт (Available MBytes) > Додати (Add)** та натисніть **OK**.

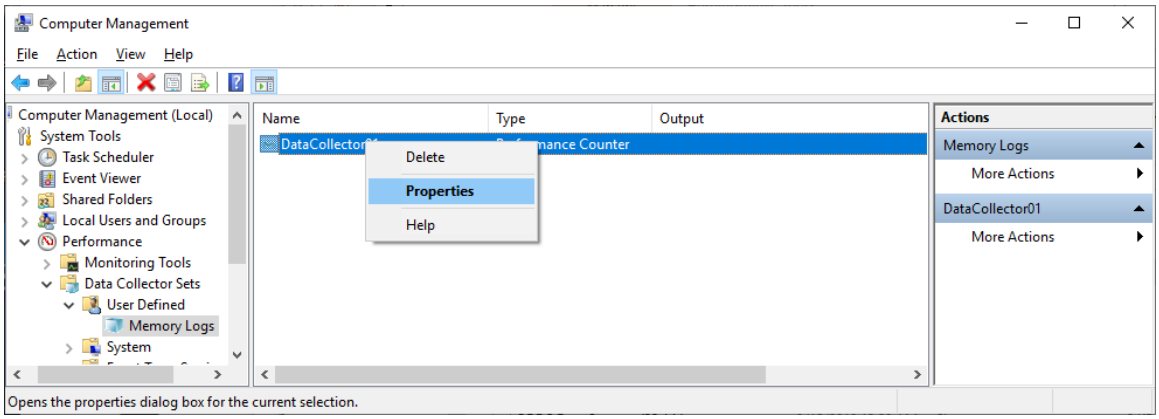
Встановіть в поле **Інтервал вибірки (Sample interval)**: значення **4** секунди. Натисніть **Далі**, щоб продовжити.

У розділі Де ви хочете зберігати дані? (Where would you like the data to be saved?) У вікні, натисніть Browse. Виберіть Локальний диск (C:) і виберіть теку PerfLogs. Натисніть OK, щоб продовжити.

Перевірте, чи відображено правильний шлях кореневого каталогу (C:\PerfLogs), і натисніть **Завершити** щоб продовжити.

Крок 2: Форматування групи збирачів даних

Розгорніть **Визначені користувачем (User Defined)** і виберіть **Memory Logs** на лівій панелі. Натисніть правою кнопкою миші **Data Collector01** та виберіть **Властивості**.



У вікні Властивості DataCollector01 змініть поле Формат журналу: на **3 поділом комами (Comma Separated)**.

Відкрийте вкладку **File**.

Запитання:

> Який повний шлях до файлу в прикладі?
>
> ***Напишіть тут свою відповідь.***
>
> **Додайте** до звіту **скриншоти основних етапів налаштування нової групи збирачів даних**.

Натисніть **OK** щоб закрити вікно Властивості (Properties).

Крок 3: Збір і перегляд даних.

Виберіть **Memory Logs** в лівій панелі вікна **Керування комп'ютером**. Натисніть правою кнопкою миші **Memory Logs** і виберіть **Пуск (Start)**.

Щоб комп'ютер примусово використовував частину доступної пам'яті, відкрийте і закрийте браузер.

Натисніть правою кнопкою миші **Memory Logs** і виберіть **Стоп (Stop)**, щоб завершити збір даних.

Перейдіть до **Локальний диск (C:)\PerfLogs**. Натисніть кнопку **Продовжити** у попереджувальних повідомленнях Windows.

Відкрийте папку, яка була створена для зберігання журналу пам'яті. Натисніть кнопку **Продовжити** у попереджувальних повідомленнях. Відкрийте файл **DataCollector01.csv.**

Виберіть **Блокнот** або іншу програму, яка може читати файли, розділені комами (.csv), щоб відкрити файл, якщо Windows не може відкрити файл, відображається файлове повідомлення.

Запитання:

Що показано в найдальшому стовпці праворуч?

Запишіть тут свою відповідь.

Додайте до звіту **скриншот вікна оснащення Memory Logs** так, щоб було видно виконані вами дії.

Закрийте файл DataCollector01.csv.

Крок 4: Видалення

Перейдіть у вікно **Керування комп'ютером**. Виберіть **Продуктивність (Performance)**> натисніть**Групи збирачів даних (Data Collection Sets)**> натисніть **Визначені користувачем (User Defined)**. Натисніть правою кнопкою миші **Memory Logs** і виберіть **Видалити**. Натисніть **Так**, щоб підтвердити видалення.

Перейдіть до теки **Локальний диск C: > PerfLogs**. Видаліть збережену теку журналів пам'яті (теку з DataCollector01.csv), створену в цій лабораторній роботі.

Закрийте всі відкриті вікна.

[In English]

Lab - Monitor and Manage System Resources

Introduction

In this lab, you will use administrative tools to monitor and manage system resources.

Recommended Equipment

A computer running Windows with internet access

Instructions

Part 1: Event Viewer

In this part, Windows Defender is used to explore the Event Viewer when the status of a service changes. Windows Defender is the built-in anti-malware component in Windows.

Step 1: Verify Windows Defender is running.

Note: Some antivirus or antispyware programs must be uninstalled on the computer for Windows Security to work.

Log on to Windows as an administrator.

To determine if Windows Defender service is stopped, click **Start**, search for **Windows Security**.

Click **Virus & threat protection**. Scroll down to the **Virus & threat protection settings**. Click **Manage settings**.

Under the Real-time protection heading, verify that it is **On**. Keep the Windows Security window open.

Step 2: Explore the Services console.

Right-click **Start** > click **Computer Management**. In the **Computer Management** window, select **Services and Applications** > **Services**.

Scroll down to **Windows Defender Antivirus Network Inspection Service**.

Question:

What is the status of the service?

Type your answers here.

Add a **screenshot of the Services snap-in** window to your report so that the located service and its status are visible.

Keep the **Computer Management** window open.

Navigate back to Windows Security. Turn off **Real-time Protection** by clicking the slider to turn it off. Click **Yes** to allow this app to make changes to the device.

Navigate back to **Services**. Click **Action** > click **Refresh**.

Look for **Windows Defender Antivirus Network Inspection**.

Record the Windows Defender status.

Type your answers here.

Add a **screenshot of the Services snap-in** window to your report so that the located service and its status are visible.

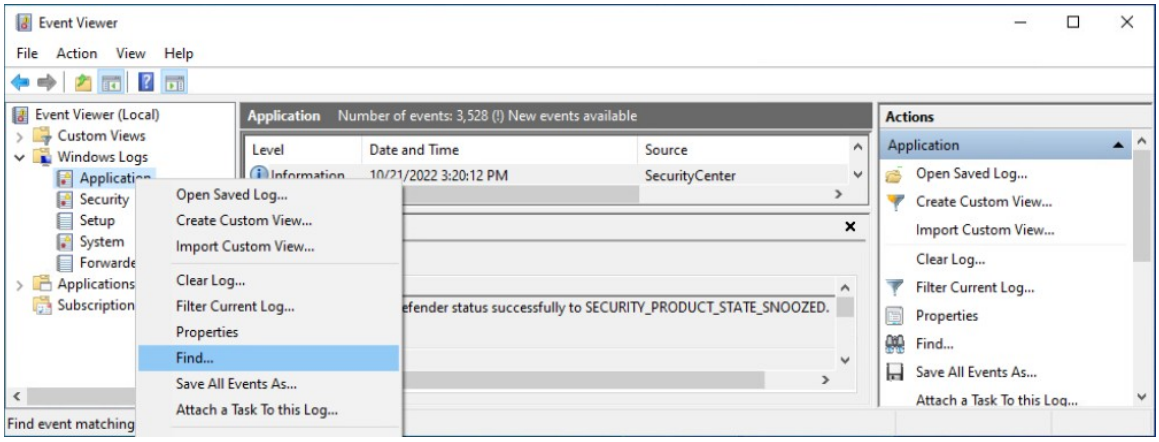
Close the **Computer Management** window.

Step 3: Explore the Event Viewer.

Navigate to the Event Viewer. Right-click **Start** > select **Event Viewer**.

Expand **Windows Logs** > select **Application**.

In the Application pane, you can find the most recent events related to Windows Defender. Right-click **Application** > select **Find**. Enter **defender** to search Windows Defender related entries and click **Find Next**.



Questions:

In the General tab, what is listed as the Source of the event? What is the severity level?

Type your answers here.

Add a **screenshot of the Event Viewer snap-in** window to your report so that the source and severety level are visible.

What is the status of Windows Defender?

Type your answers here.

Navigate to Windows Security and re-enable Real-time protection. Close Windows Security window.

Navigate to the Event Viewer to review the most recent event entries that are related to Windows Defender. Close the Event Viewer window when done.

Part 2: Explore the Impact of Services.

In this part, you will stop **Print Spooler** service to explore the impact in the system. The print spooler is responsible for managing the printer jobs and handling the interaction with the printer. With this service turned off, you will not be able to print or see your printers.

Step 1: Verify printing service

Open **Notepad**. Click **Start** and search for **Notepad**.

In **Notepad**, click **File** > **Print**. Record a listed printer below. **Note**: You do not need to install a physical printer.

Type your answers here.

Add a **screenshot of the Print window** to your report so that the printer is visible.

Click **Cancel** to exit the print dialog. Leave Notepad open.

Step 2: Stop print spooler.

Right-click **Start** > select **Computer Management**. Expand **Services and Applications** > select **Services** to open the Services console.

Right-click **Print Spooler** and select **Stop**.

Navigate to **Notepad**. Attempt to print.

Question:

What message did you receive? How would you fix this?

Type your answers here.

Add a **screenshot of the message window** you received to the report.

Click **No** in the message window and click **Cancel** to exit the Print window.

Step 3: Restart print spooler

Navigate to the **Services** console and restart the print spooler. Right-click **Print Spooler** and select **Start**.

Verify that you can print and close Notepad.

Step 4: Explore DHCP Client service

The DHCP Client service registers and updates the IP addresses and DNS records for the PC. If this service is stopped, the PC will not receive a dynamic IP address and DNS updates.

In the Services console, search for **DHCP Client**. Right-click **DHCP Client** and select **Stop**.

Question:

When DHCP Client stops, what other services will also be stopped?

Type your answers here.

Add a **screenshot of the Services snap-in window** to your report so that the actions performed there are visible.

Click **No** in the **Stop Other Services** window.

Question:

Why is it important to exercise care when managing services?

Type your answers here.

Verify that **DHCP Client** is still running.

Part 3: Monitor and Record System Usage with System Tools

You will configure System Tools features and monitor the usage of system resources of the computer.

Step 1: Create a new data collector set.

Right-click **Start**. > select **Computer Management** > expand **System Tools**.

Expand **Performance** > expand **Data Collector Sets**.

In the left pane, right-click **User Defined** > select **New** > click **Data Collector Set**.

In the **Create new Data Collector Set** window, type **Memory Logs** in the Name field. Select the **Create manually (Advanced)** and click **Next** to continue.

In the **What type of data do you want to include?** window, select **Performance counter** and click **Next**.

In the **Which performance counters would you like to log?** Window, click **Add**. From the list of available counters, locate and expand **Memory**. Select **Available MBytes** > **Add** and click **OK** to continue.

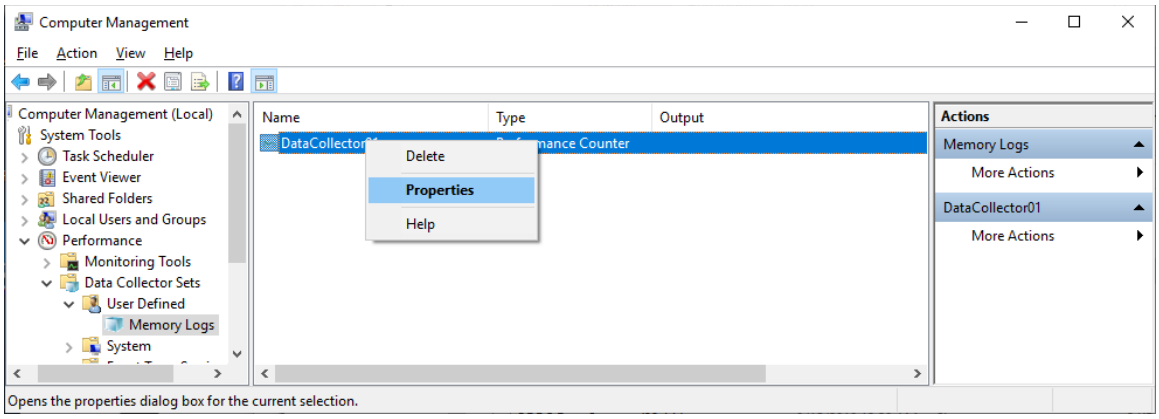
Set the **Sample interval**: field to **4** seconds. Click **Next** to continue.

In the **Where would you like the data to be saved?** Window, click **Browse**. Select **Local Disk (C:)** > **PerfLogs**. Click **OK** to continue.

Verify the correct root directory path is displayed (C:\PerfLogs) and click **Finish** to continue.

Step 2: Format the data collector set.

Expand **User Defined** and select **Memory Logs** in the left pane. Right-click **Data Collector01** and right-click **Properties**.



In DataCollector01 Properties window, change the Log format: field to **Comma Separated**.

Click the **File** tab.

Question:

What is the full path name to the example file name?

Type your answers here.

Add **screenshots of the main steps** in setting up the new data collector set to the report.

Click **OK** to continue to close the Properties window.

Step 3: Collect and view the data.

To start data collection, right-click **Memory Logs** and select **Start**.

To force the computer to use some of the available memory, open and close a browser.

Right-click **Memory Logs** and select **Stop** to stop the data collection set.

Navigate to **Local Disk (C:)\PerfLogs**. Click **Continue** in the Windows warning messages.

Open the folder that was created to store the memory log. Click **Continue** on the Windows warning messages.

Open the **DataCollector01.csv** file. Select **Notepad** or another program that can read comma-separated files (.csv) to open the file if Windows cannot open the file message is displayed.

Question:

What does the column farthest to the right show?

Type your answers here.

Add a **screenshot of the Memory Logs snap-in window** to the report so that the actions you performed are visible.

Close the DataCollector01.csv file.

Step 4: Clean up

Navigate to the **Computer Management** window. Right-click **Memory Logs** and select **Delete**. Click **Yes** to confirm the deletion.

Navigate to the **Local Drive C:** > **PerfLogs** folder. Delete the stored memory logs folder (folder with the DataCollector01.csv) created from this lab.

Close all opened windows.