# Лабораторна робота - Моніторинг і керування системними ресурсами

## 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**.**

a. Увійдіть у Windows з обліковим записом адміністратора.

b. 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. c.

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**.**

a. 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**.

b. 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?

***Включений***

c. 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.

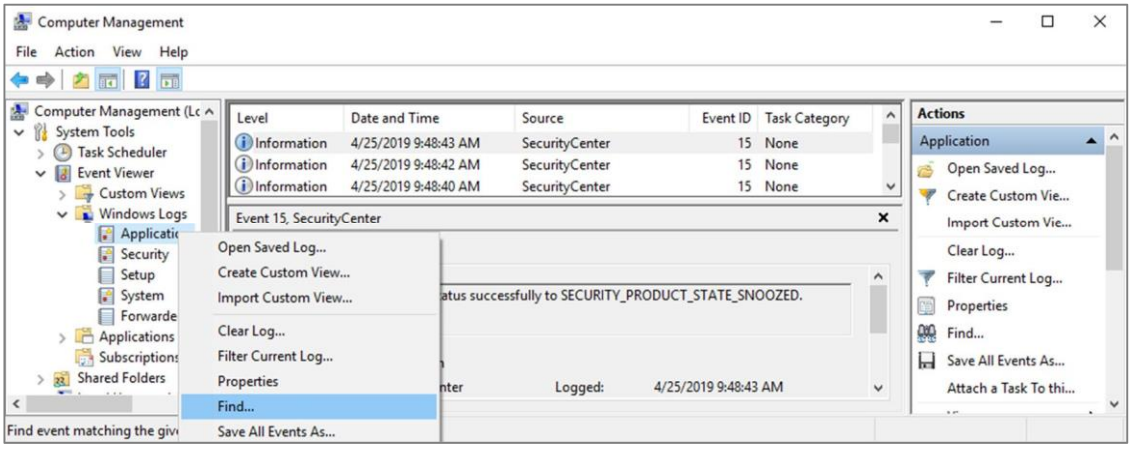
d. Поверніться в «Служби». (**Панель керування** в поданні з дрібними піктограмами > **Адміністрування** > **Служби**). Натисніть **Дія** > **Оновити.**

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.

***Вимкнено.***

e. 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).

f. 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?

***Security Center.***

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

h. 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

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

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

*HP LaserJet Professional M1132 MFP.*

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

### Крок 2: Зупинка диспетчера друку

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

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

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

Запитання:

Яке повідомлення ви отримали? Як би ви це виправили?

*З'явилося вікно з помилкою, яке закликає встановити принтер, інакше настроювання сторінки і друку неможливе. Додав би знову принтер.*

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

### Крок 3: Перезапуск диспетчера друку

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

b. 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.

a. 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?

*Intel (R) Dynamic Application Loader Host Interface server*

*IP Helper*

*Win HTTP Web Proxy Auto-Discovery Service*

*Служба списку мереж*

*Network Location Awareness.*

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

Запитання:

Чому важливо проявляти обережність при керуванні службами?

***Відключення однієї служби може призвести до відключення інших служб. У висновку деякі операції стануть недоступними і не будуть виконуватися. Слід запам'ятати які служби ми вимикаємо.***

c. 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.

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

b. 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)**.

c. 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**.

d. 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.

e. 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**.

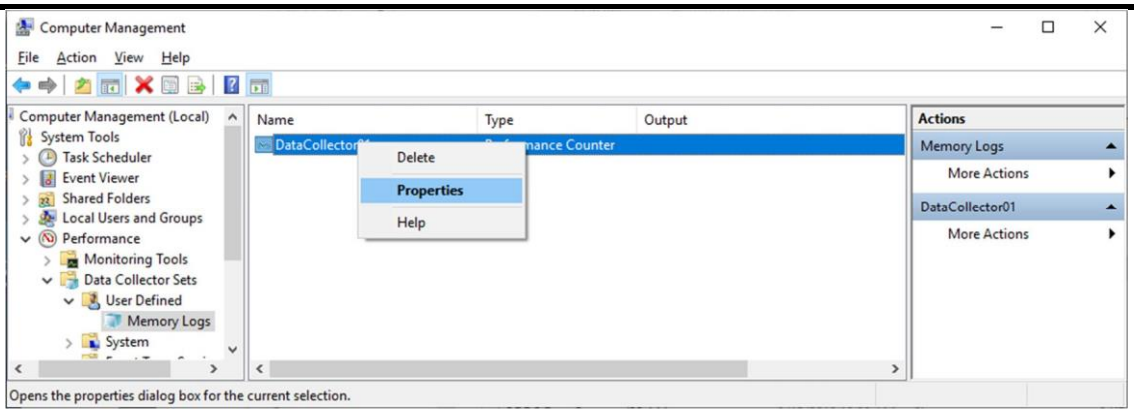
f. Встановіть в поле **Інтервал вибірки (Sample interval)**: значення **4** секунди. Натисніть **Далі**, щоб продовжити.

g. 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.

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

### Крок 2: Форматування групи збирачів даних

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




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

c. Відкрийте вкладку **File**.

Запитання:

Який повний шлях до файлу в прикладі?

***C:\PerfLogs\DESKTOP-DVG90E6_20221128-000001\DataCollector01.csv.***

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

## Крок 3: Збір і перегляд даних.

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

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

c. 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.

d. 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?

***Точний час в який відбувся збір логів (16:40:08.937).***

e. Закрийте файл DataCollector01.csv.

## Крок 4: Видалення

a. 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.

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

c. Закрийте всі відкриті вікна.