**Міністерство освіти та науки України**

**Київський національний торговельно - економічний університет**

**Факультет інформаційних технологій**

**Кафедра інженерії програмного забезпечення та кібербезпеки**

**ПРАКТИЧНА РОБОТА № 10**

**З ДИСЦИПЛІНИ**

**«Безпека інформаційних систем»**

**НА ТЕМУ:**

ПОЛІТИКИ БЕЗПЕКИ. АУДИТ ПОДІЙ БЕЗПЕКИ

**Виконала:** студентка ФІТ

Групи 4 курсу 3

Авєріна Наталія Ігорівна

**Викладач:** Лахно Валерiй Анатолiйович

Київ 2023

**Практична робота №10**

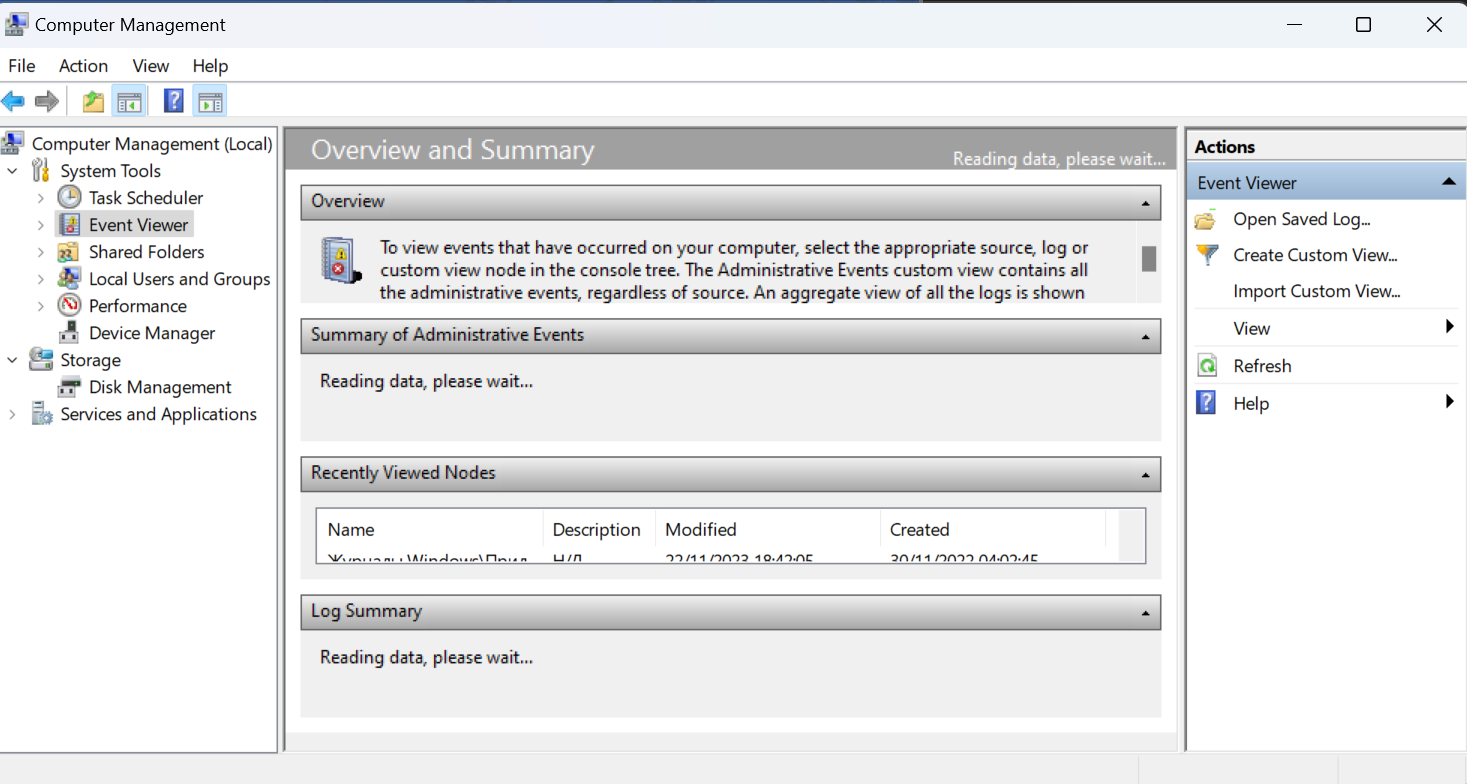
**Тема**: Політики безпеки. Аудит подій безпеки

**Мета**: Навчитися працювати з журналом подій та вміти здійснювати аудит політик безпеки

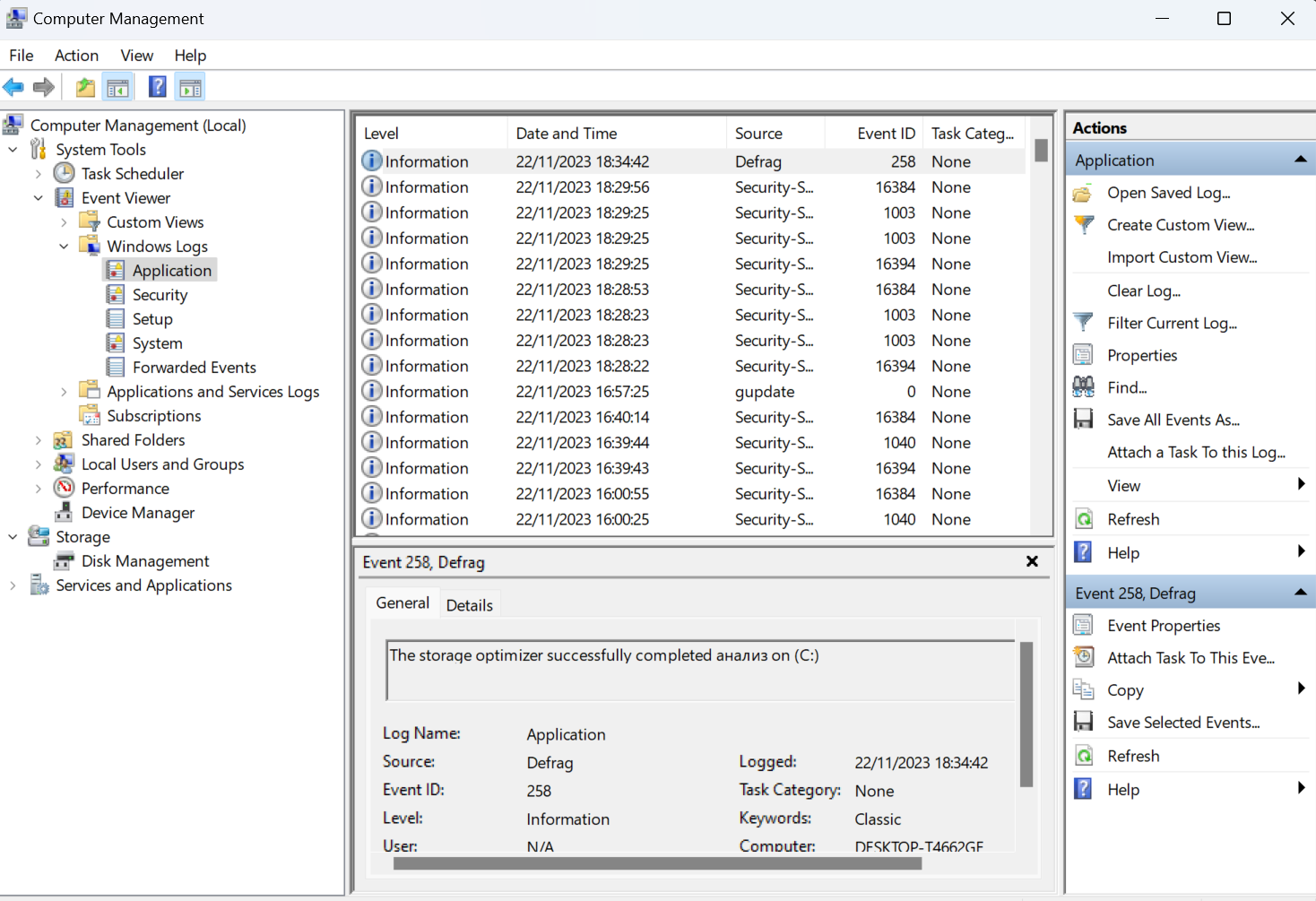
**Хід роботи:**

**Частина 1. Робота з журналами подій**

1. Перегляд подій
   1. Натикаємо на кнопку «Пуск» для відкриття меню, відкриваємо «Computer Management», зі списку компонентів панелі управління вибираємо «System tools» і зі списку адміністративних компонентів - «Event Viewer».

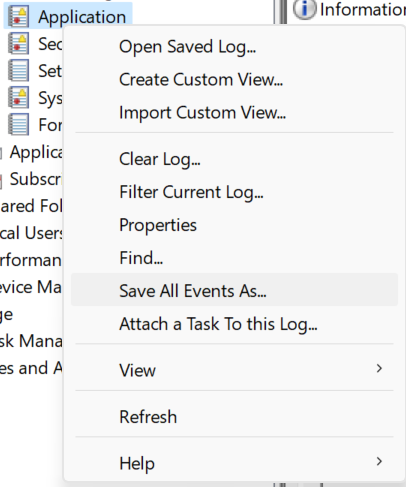


* 1. В «Event Viewer» обираємо «Windows logs», далі «Applications».



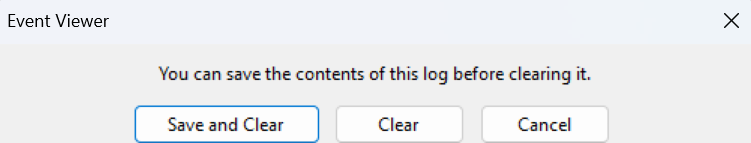
Панель «Область перегляду» показує основні дані про події на вкладці «Загальні», а додаткові специфічні дані - на вкладці «Подробиці». Включити і вимкнути цю панель можна, вибравши меню «Вид», а потім команду «Область перегляду».

* 1. Зберігаємо журнал. Для цього обираємо потрібний журнал подій, натискаємо правою кнопкою миші та обираємо команду «Save All Events As…».

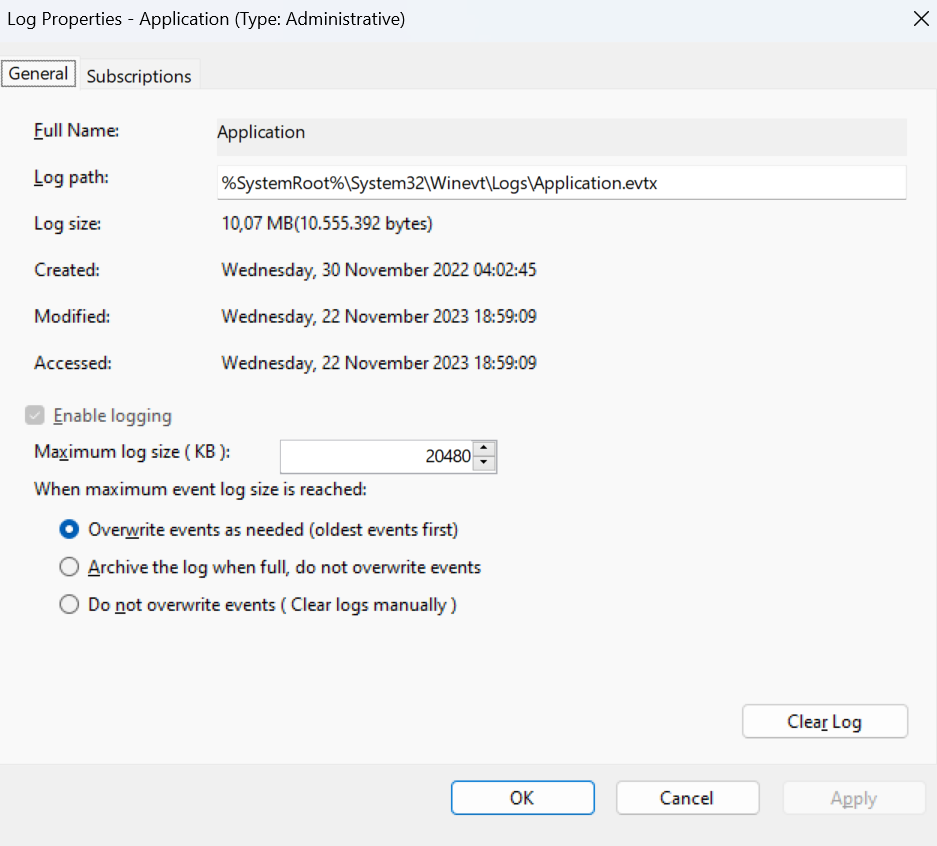


* 1. Далі у вікні обираємо папку, в яку необхідно зберегти файл.

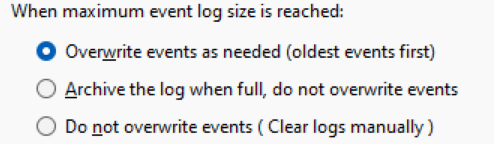
1. Очистка журналу подій
   1. У дереві консолі обираємо журнал подій, який потрібно очистити. Натискаємо правою кнопкою миші та обираємо команду «Clear log…». Далі можна або очистити журнал, або заархівувати його в тому випадку, якщо це не було зроблено раніше.



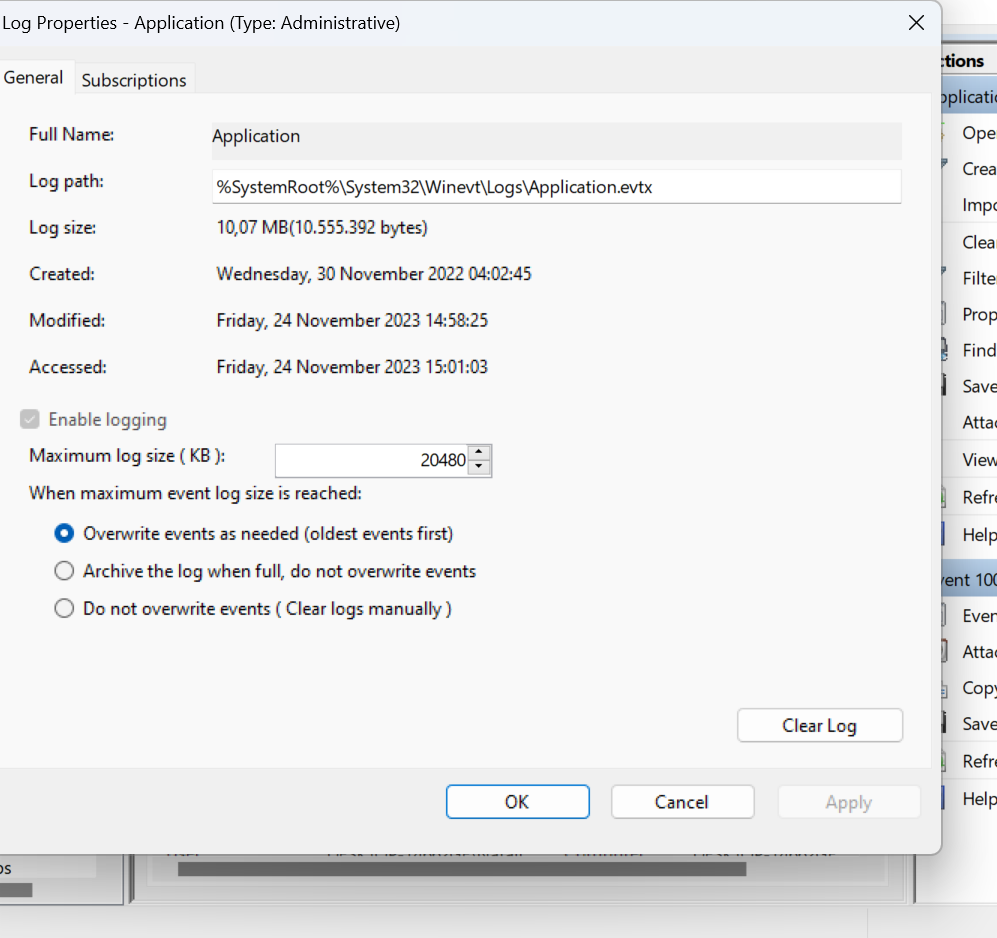
1. Встановлення максимального розміру журналу
   1. У дереві консолі обираємо журнал подій, для якого слід змінити розмір. Обираємо команду «Properties». В полі «Maximum log size (KB)» вписуємо потрібне значення.



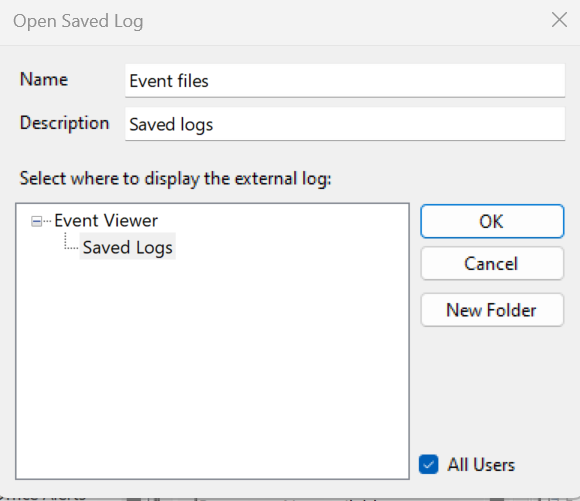
1. Політика збереження журналів
   1. Переходимо у властивості журналу та на вкладці «General» в розділі «When maximum event log size is reached» обираємо необіхідний параметр та натискаємо кнопку ОК.



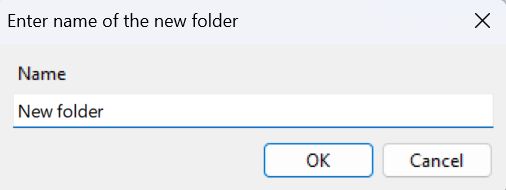
1. Активація аналітичного і налагоджувального журналу
   1. У дереві консолі знаходимо і обираємо аналітичний або оцінний журнал, який необхідно активувати;
   2. Обираємо команду «Properties» з меню «Actions» або з контекстного меню вибраного аналітичного або отладочного журналу;
   3. На вкладці «General» встановлюємо прапорець на опції «Enable logging».



1. Відкриття та закриття збереженого журналу
   1. Обираємо команду «Open saved log» в меню «Actions» або з контекстного меню в дереві консолі;
   2. У діалоговому вікні, пересуваючись по дереву каталогів, відкриваємо папку, яка містить потрібний файл.
   3. У діалозі «Open saved logs», в поле «Name» вводимо нове ім'я, яке буде використовуватися для журналу в дереві консолі. В поле «Desription» вводимо опис журналу.



* 1. Для створення папки, в якій буде розташований збережений журнал, натискаємо на кнопку «New folder». В поле «Name» вводимо ім'я папки, в якій буде перебувати відкритий журнал, а потім натискаємо кнопку «ОК».

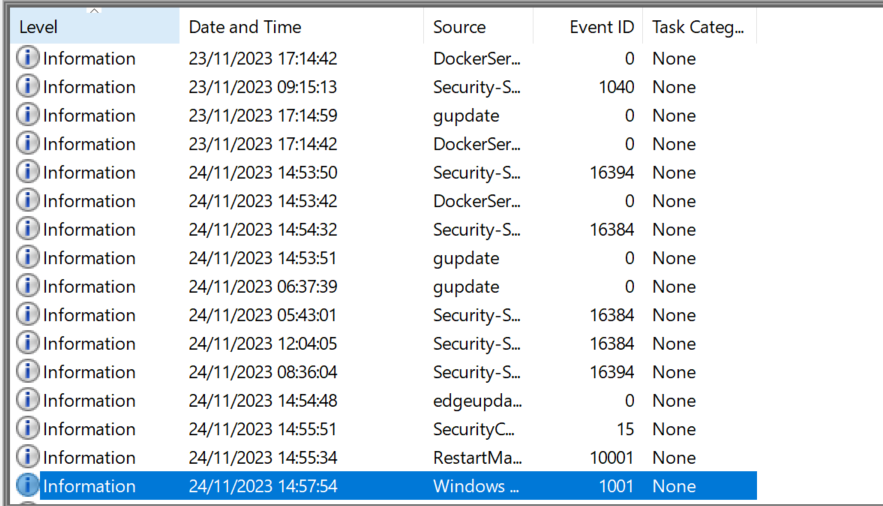


* 1. Для того щоб відкритий журнал подій став недоступним для інших користувачів комп'ютера, ми можемо зняти прапорець «All users».

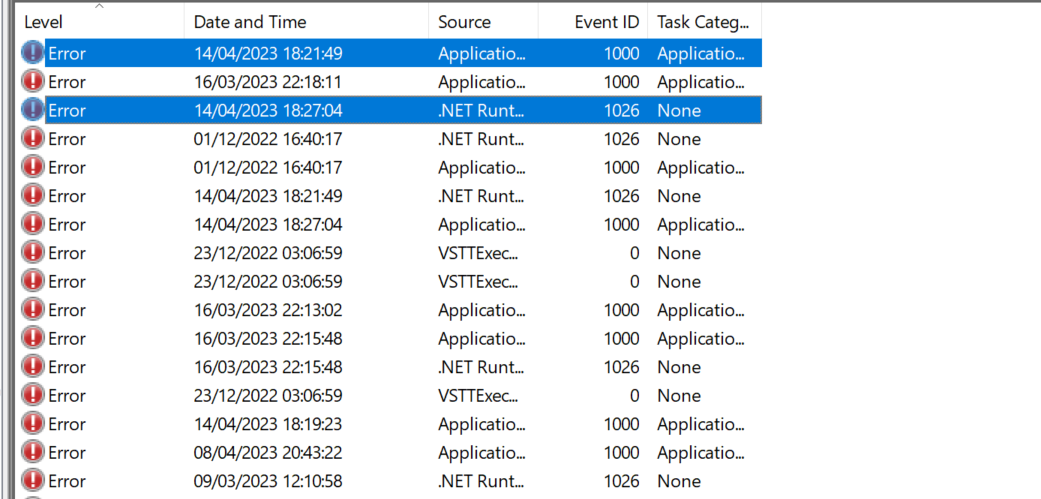


* 1. Для того щоб видалити відкритий журнал з дерева подій, виконуємо такі дії:
     + У дереві консолі обираємо журнал, який слід видалити;
     + Обираємо команду «Delete» з меню «Actions» або з контекстного меню вибраного журналу;
     + У діалозі «Event viewer» натискаємо на кнопку «Yes».

1. Індивідуальне завдання
   1. Відкриваємо журнал подій в ОС та сортуємо події по «Level».



* 1. Розглянемо значення коду події 2-х перших подій що мають різні коди подій. У мене це будуть події з кодами 1000 i 1026:
     + 1000:
       - Source: Application Error
       - Event ID: 1000
       - Level: Error - 2 (позначає, що виникла проблема, яка може вплинути на функції, зовнішні по відношенню до додатка або компоненту, що викликав подію)
       - User: DESKTOP-T4662GE\Natali
       - EventRecordID: 6734
       - Log Name: Application
       - Keywords: 0x8000000000000000
       - Computer: DESKTOP-T4662GE
       - Logged: 14/04/2023 18:21:49
       - ProcessID: 13704
       - ThreadID: 20868
     + 1026:
       - Source: .NET Runtime
       - Event ID: 1026
       - Level: Error - 2 (позначає, що виникла проблема, яка може вплинути на функції, зовнішні по відношенню до додатка або компоненту, що викликав подію)
       - User: DESKTOP-T4662GE\Natali
       - EventRecordID: 6737
       - Log Name: Application
       - Keywords: 0x8000000000000000
       - Computer: DESKTOP-T4662GE
       - Logged: 14/04/2023 18:27:04
       - ProcessID: 16272
       - ThreadID: 0

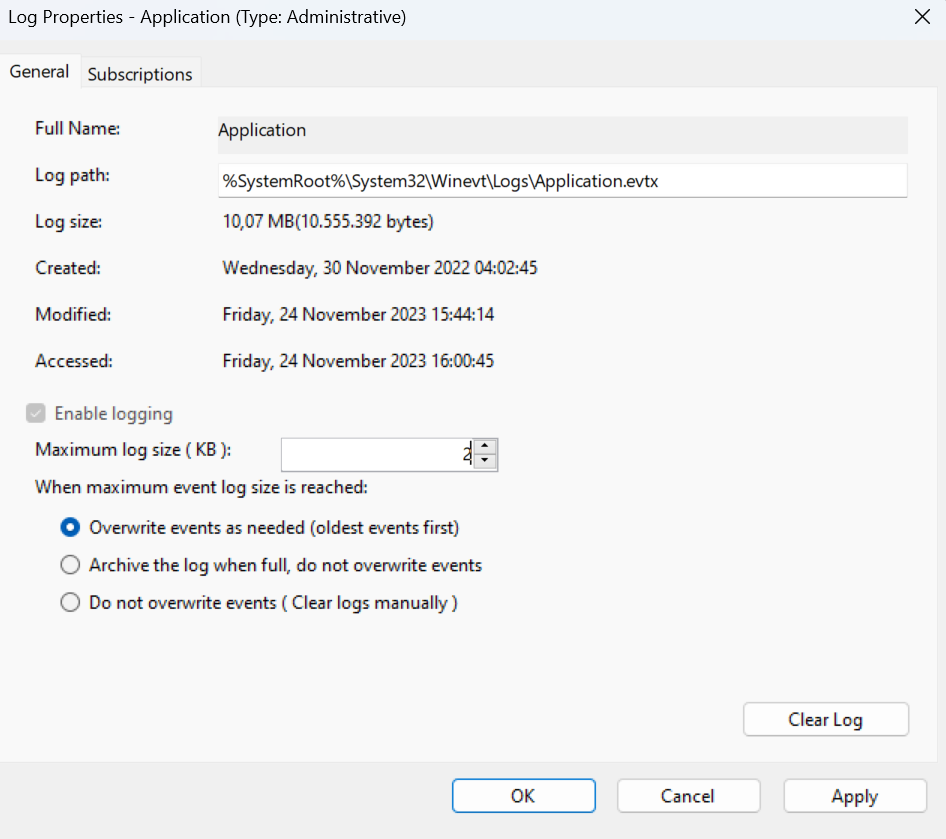


* 1. Розглянемо 3 події, з кодами, які закінчуються на номер індивідуального варіанту починаючи з 0 для 1-го варіанту по модулю 10.
     + 100:
       - Source: Bonjour Service
       - Event ID: 100
       - Level: Error - 2 (позначає, що виникла проблема, яка може вплинути на функції, зовнішні по відношенню до додатка або компоненту, що викликав подію)
       - User: DESKTOP-T4662GE\Natali
       - EventRecordID: 3781
       - Log Name: Application
       - Keywords: Classic
       - Computer: DESKTOP-T4662GE
       - Logged: 19/02/2023 17:12:14
       - ProcessID: 3684
       - ThreadID: 0
     + 0:
       - Source: VSTTExecution
       - Event ID: 0
       - Level: Error - 2 (позначає, що виникла проблема, яка може вплинути на функції, зовнішні по відношенню до додатка або компоненту, що викликав подію)
       - User: DESKTOP-T4662GE\Natali
       - EventRecordID: 11672
       - Log Name: Application
       - Keywords: Classic
       - Computer: DESKTOP-T4662GE
       - Logged: 05/10/2023 20:22:19
       - ProcessID: 0
       - ThreadID: 0
     + 10010:
       - Source: RestartManager
       - Event ID: 0
       - Level: Warning - 3
       - User: СИСТЕМА
       - EventRecordID: 3718
       - Log Name: Application
       - Keywords: 0x8000000000000000
       - Computer: DESKTOP-T4662GE
       - Logged: 18/02/2023 22:11:15
       - ProcessID: 17252
       - ThreadID: 7364





* 1. Встановлюємо максимальний розмір журналу, який описаний на 12 сторінці зі значенням яке вираховується 2^(2\*n-вар) КБ = 2^2 = 4 КБ



Висновок: під час виконання лабораторної роботи ми навчилися стежити за журналами подій та аналізувати інформацію, що міститься в цих журналах.