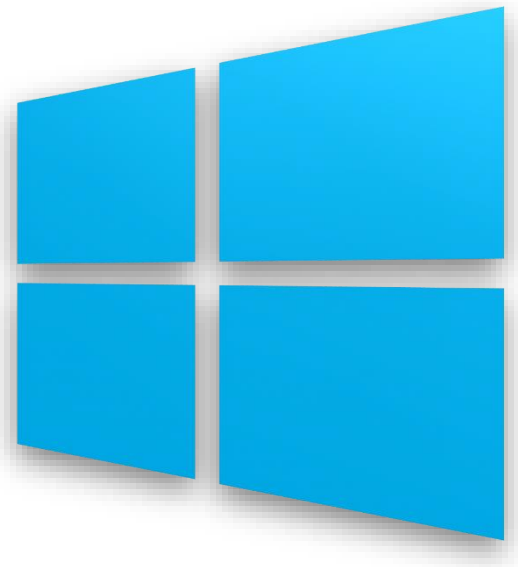
ИКОНОМИЧЕСКИ УНИВЕРСИТЕТ - ВАРНА

КАТЕДРА „ИНФОРМАТИКА”

Операционни системи

УПРАЖНЕНИЕ 9: НАБЛЮДАВАНЕ НА СИСТЕМАТА. УПРАВЛЕНИЕ НА ВИРТУАЛНАТА ПАМЕТ



Изготвил: гл. ас. д-р Радка Начева

ДАТА: 25 МАРТ 2019 Г.

УПРАЖНЕНИЕ 9: НАБЛЮДАВАНЕ НА СИСТЕМАТА. УПРАВЛЕНИЕ НА ВИРТУАЛНАТА ПАМЕТ

I. ЦЕЛ И ТЕМИ НА УПРАЖНЕНИЕТО

Целта на упражнението е да запознае студентите с инструментариума на ОС Windows за наблюдение на производителността на системата и управление на виртуалната памет.

Темите[1], засегнати в упражнението, са:

1. Способи за наблюдение на системата в ОС Windows - Event Viewer, Performance Monitor, Resource Monitor
2. Способи за управление на виртуалната памет

След изпълнение на предвидените задачи в упражнението студентите следва да придобият практически умения по проследяване на производителността на ОС Windows и на виртуалната памет.

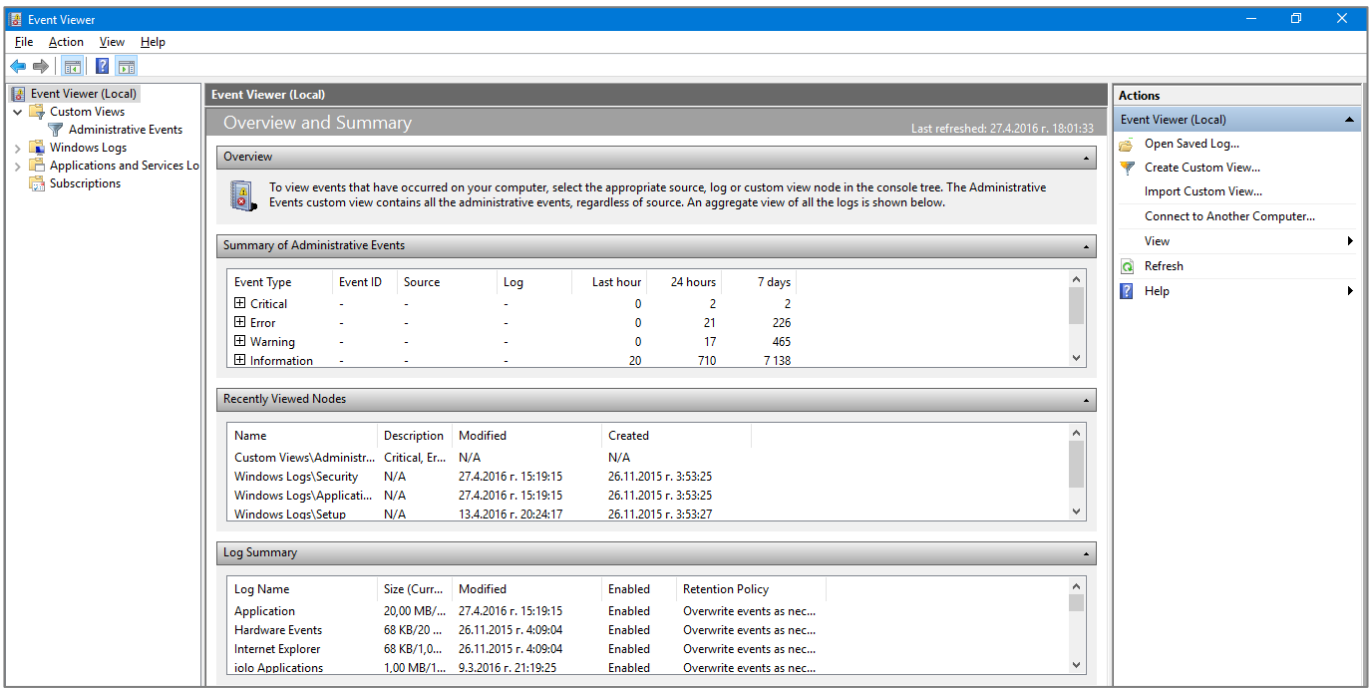
[1] ***Забележка**: Някои от поставените теми се разглеждат в теоретичната част на упражнението, а други – в практическата.*

II. ТЕОРЕТИЧНА ПОДГОТОВКА

1. Способи за наблюдение на системата в ОС Windows - Event Viewer, Performance Monitor, Resource Monitor

Event Viewer

Визуализаторът на събития (Event Viewer – Фиг. 1) или програмата за разглеждане на събития е инструмент, който показва подробна информация за важни събития (например, програми, които не се стартират правилно или актуализации, които се изтеглят автоматично) на компютъра. Програмата за разглеждане на събития може да е полезна при отстраняване на неизправности и грешки в Windows и други програми. Може да се използва само от потребители с администраторски права.

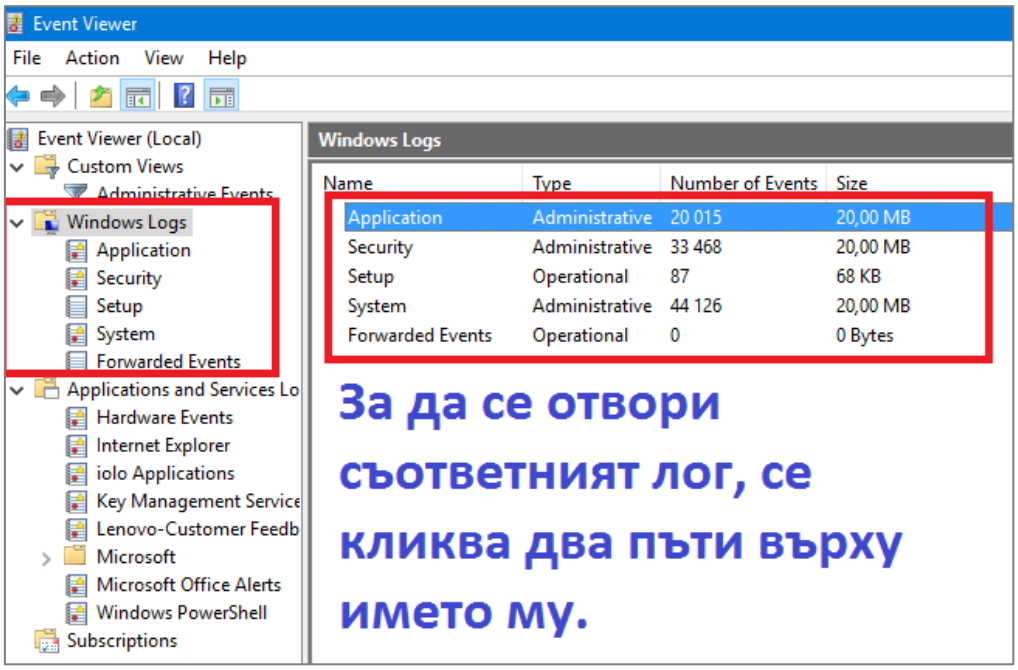


Фиг. 1. Визуализатор на събития на ОС Windows (Event Viewer)

Визуализаторът на събития записва информацията в няколко различни лог файла - регистри на събитията. Те са специални файлове, които записват по-важните събития на компютъра. Например, влизане в компютъра или възникване на грешка в програма. При възникването на тези събития Windows ги записва в регистрационен

файл, който може да се прочете с програмата за разглеждане на събития. Напредналите потребители могат да намерят данни в тези регистрационни файлове, които са им полезни за решаването на проблеми в Windows и други програми. Разделят се в две категории:

- *Регистрационни файлове на Windows (Windows Logs), които са (Фиг.2):*

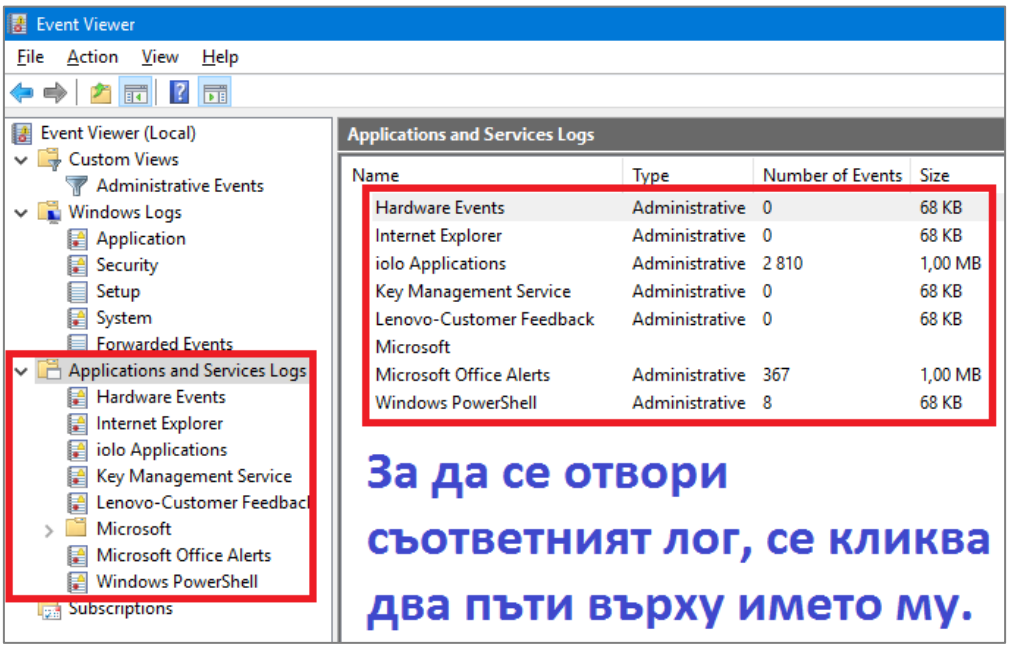


Фиг. 2. Windows Logs в Event Viewer

- **Събития с приложения (програми) - Application.** Събитията се класифицират като **грешки**, **предупреждения** и **информация**, в зависимост от сериозността на събитието. Грешката е важен проблем, напр. загуба на данни. Предупреждението е събитие, което не е задължително важно, но може да подскаже за евентуален проблем. Информацията описва успешната работа на програма, драйвер или услуга.
- **Събития, свързани със защитата - Security.** Тези събития се наричат **проверки** и се описват като успешни или неуспешни в зависимост от събитието, например дали даден потребител е влязъл успешно в Windows.

- **Събития за инсталиране - Setup.** Компютрите, които са домейн контролери имат допълнителни регистрационни файлове.
- **Системни събития - System.** Системните събития се регистрират от Windows и системните услуги на Windows и се класифицират като грешки, предупреждения или информация.
- **Препратени събития – Forwarded Events.** Тези събития са препратени към този регистрационен файл от други компютри.

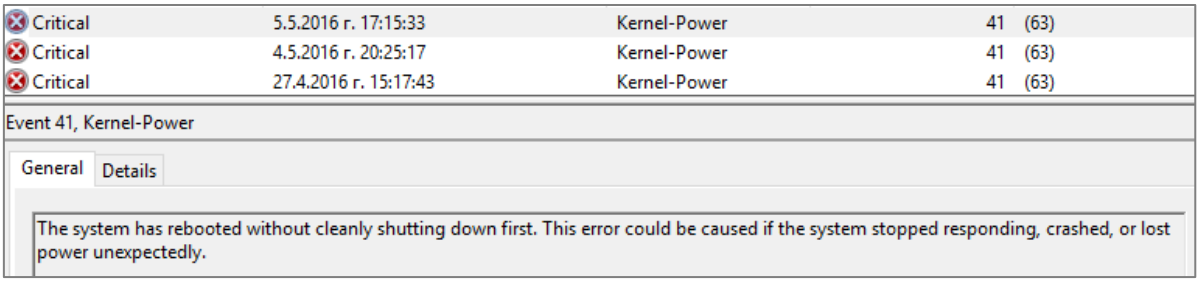
- *Регистрационни файлове за приложения и услуги (Applications and Services Logs – Фиг. 3)*, които включват отделни файлове за програмите, които работят на компютъра, както и подробни регистрационни файлове, които се отнасят за определени услуги на Windows. Например, Hardware Events, Internet Explorer и др.



Фиг. 3. Applications and Services Logs в Event Viewer

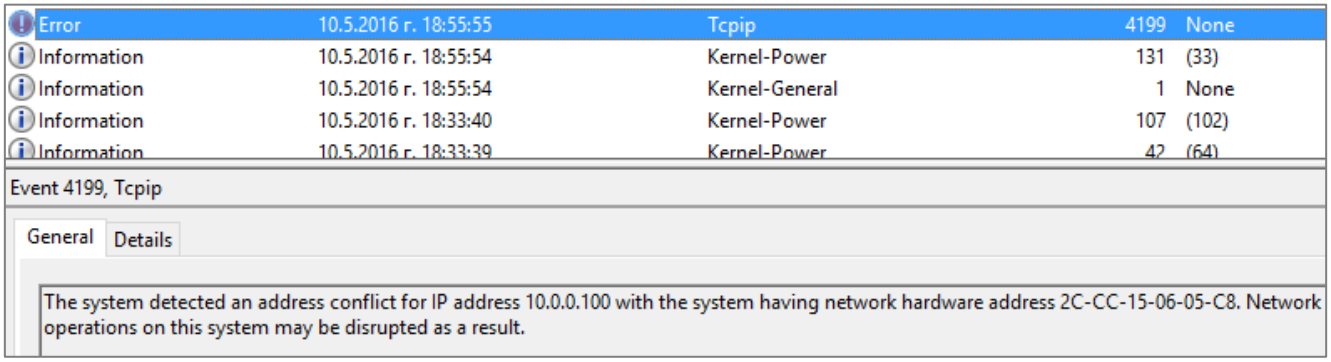
В логовете се записват събития, които могат да бъдат няколко вида:

- **Критични събития (Critical)** – появяват се с червен индикатор със знак „x“, който дава информация за настъпил критичен проблем със системата. Вж. Фиг. 4.



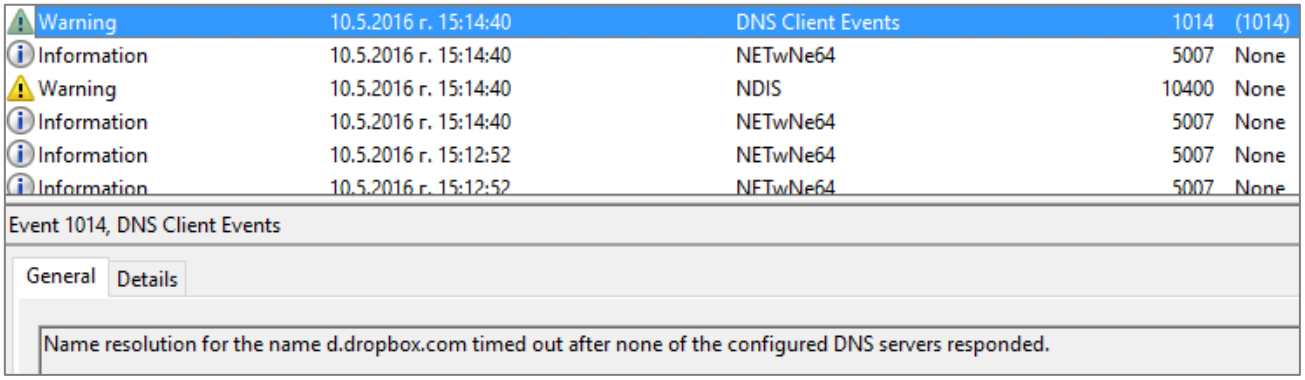
Фиг. 4. Изглед на критично събитие в Event Viewer

- **Грешки (Errors)** – появяват се с червен индикатор с удивителен знак, който е знак за появил се проблем, като например, загуба на данни. Вж. Фиг. 5.



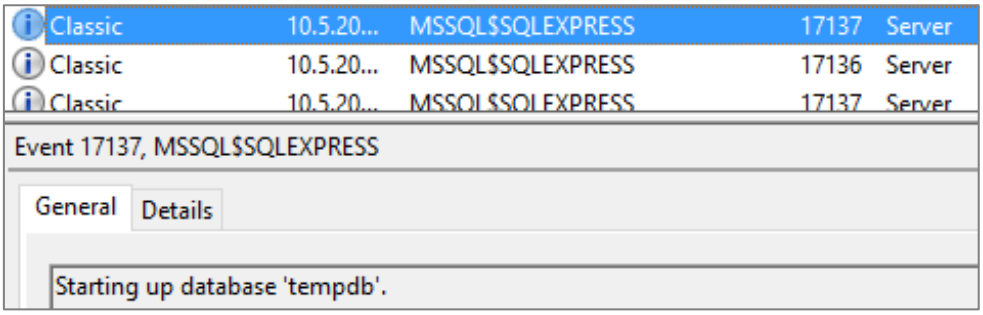
Фиг. 5. Изглед на грешка в Event Viewer

- **Предупреждения (Warnings)** – появяват се с жълт индикатор, който е знак за предупреждение за проблем, който не влияе на работата на съответната програма. Служи и като предизвестие за бъдещи проблеми. Вж. Фиг. 6.



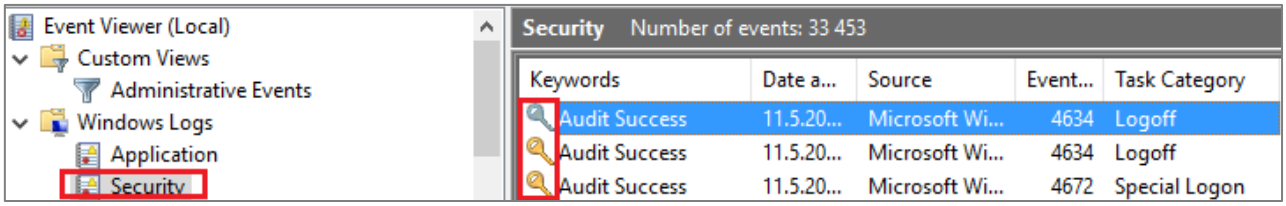
Фиг. 6. Изглед на предупреждение в Event Viewer

- **Информация (Information)** – появяват се с бял индикатор, който е дава информация за успешното изпълнение на операции на програма, драйвер или услуга. Вж. Фиг. 7.



Фиг. 7. Изглед на информационно съобщение в Event Viewer

Забележка: *Дневникът на сигурността (Security log) не използва горните нива на събития, а по-скоро използва одити на сигурността (Фиг. 8).*



Фиг. 8. Security log в Event Viewer

Регистрите на събития съдържат хиляди събития и намирането на необходимата информация понякога може да бъде трудно. При условие, че знаете какво търсите, винаги можете да използвате опциите за филтриране и така да игнорирате цялата ненужна информация. Това става от меню **Action -> Filter Current Log**. Същата операция може да се извърши и от контекстното меню на лога (десен бутон върху името на лога –> Filter Current Log).

Събитията имат заглавие и описание. Вж. Таблица 1.

Таблица 1

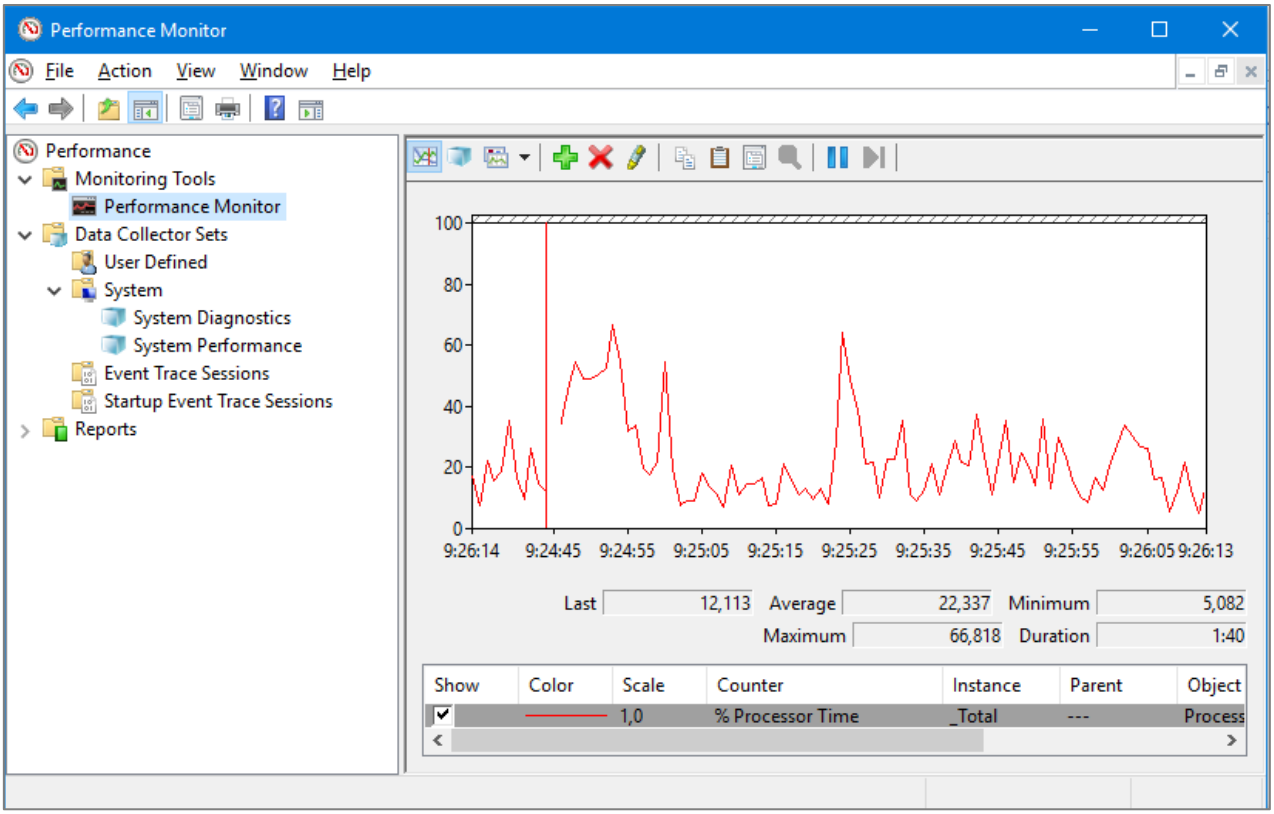
Включена информация за събития

Вид информация	Описание
Дата (Date)	Дата, на която е настъпило събитието (dd.mm.yyyy)[2]
Време (Time)	Време, по което е настъпило събитието (hh:mm:ss)[3]
Потребител (User)	Потребителят, който е бил логнат в системата, при настъпване на събитието. Посочено е потребителското име.
Компютър (Computer)	Компютърът, на който е настъпило събитието. Посочено е името на компютъра (Computer Name).
Номер на събитието (Event ID)	Уникалният номер, който идентифицира типа на събитието.
Източник (Source)	Източникът (инициаторът) на събитието. Може да е приложение или системен компонент.
Тип (Type)	Категорията (типа) на събитието (Информация, Предупреждение, Грешка, Критично събитие, Успешен или Неуспешен одит – последните две важат само за Security Log)

Performance Monitor

Това е инструмент на ОС Windows, който се използва за наблюдение на производителността на компютърната система. Чрез него може да се наблюдава хардуерната производителност в реално време, но същевременно се съхранява и история. Стартира се чрез perfmon.exe. Вж. Фиг. 9.

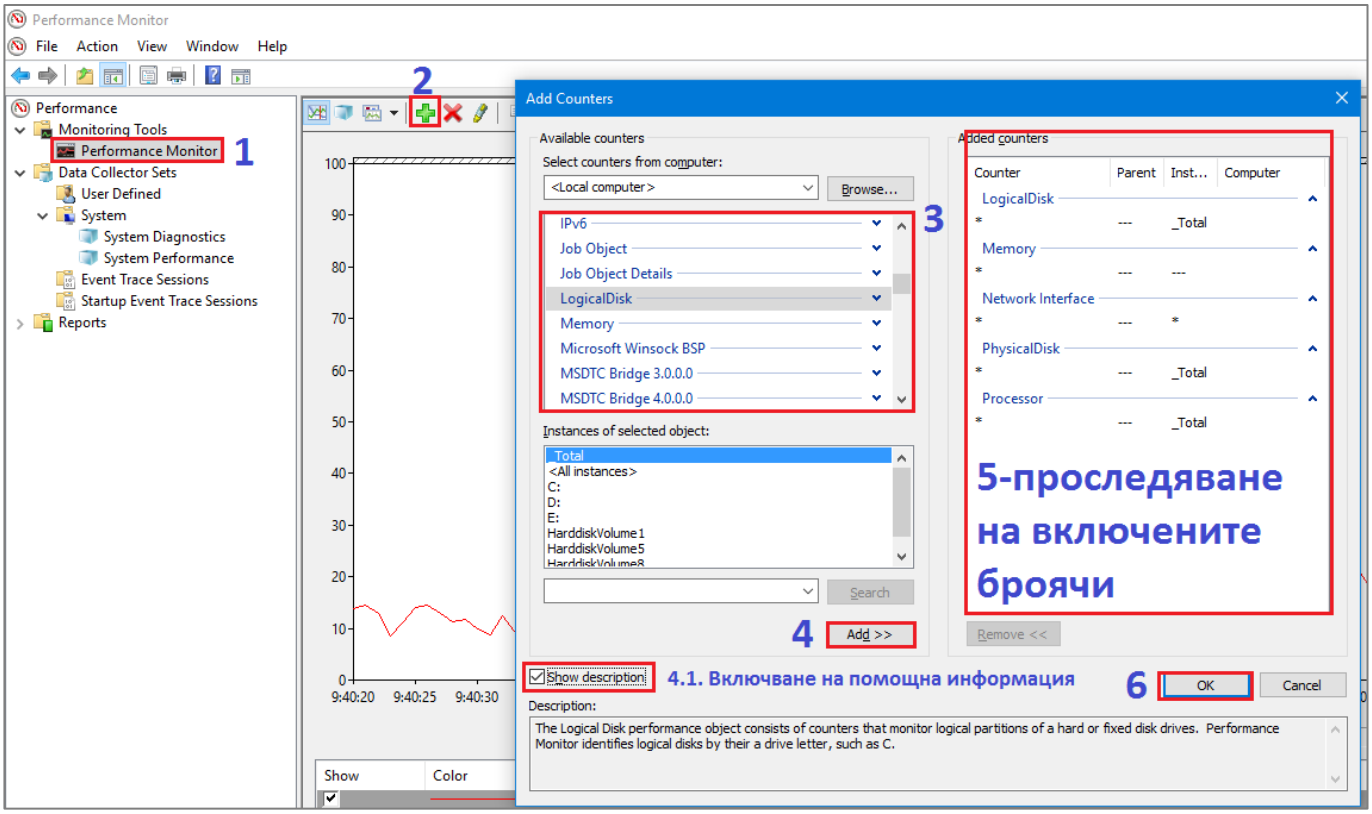
[2] Форматът зависи от регионалните настройки.
[3] Форматът зависи от регионалните настройки.



Фиг. 9. Performance Monitor

Инструментът работи с т. нар. „броячи за ефективност“ (performance counters), които представляват измервания на това как нещо (хардуерен компонент, компонент на операционната система или приложение) се представя в даден момент. Например, може да се измери времето, което процесорът прекарва в отговор на исканията на системата, работата на BIOS, на харддиска и т.н.

Потребителят може да добавя собствени броячи с цел персонализирано наблюдение на критични компоненти на софтуерната и хардуерната система. Вж. Фиг. 10.

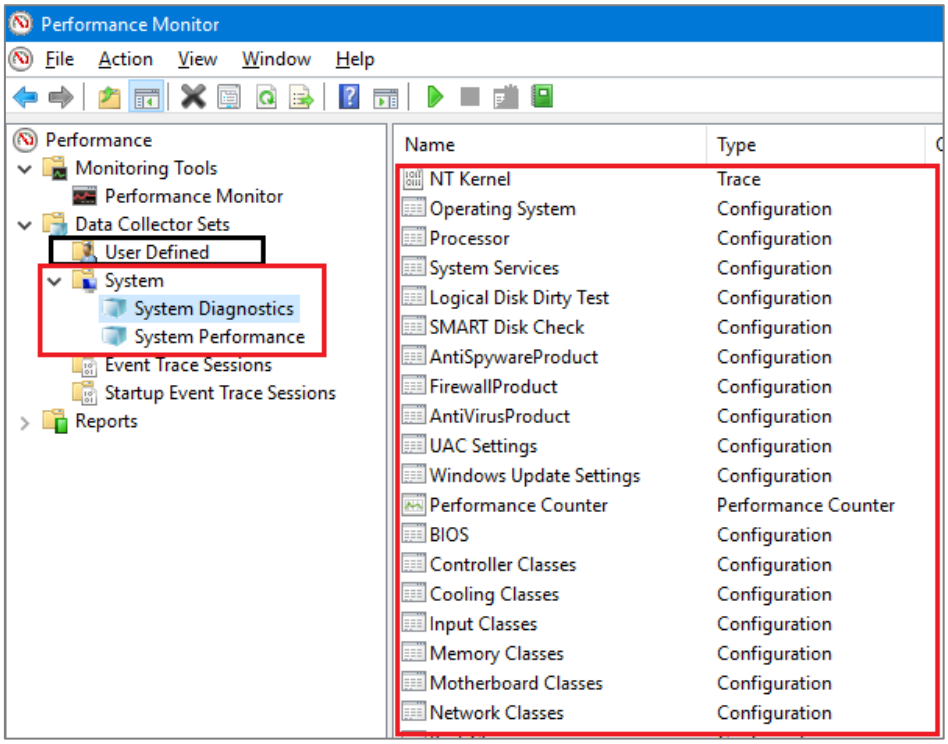


Фиг. 10. Performance Monitor – персонализирано наблюдение

От менюто с инструменти могат да се извършват допълнителни операции, като:

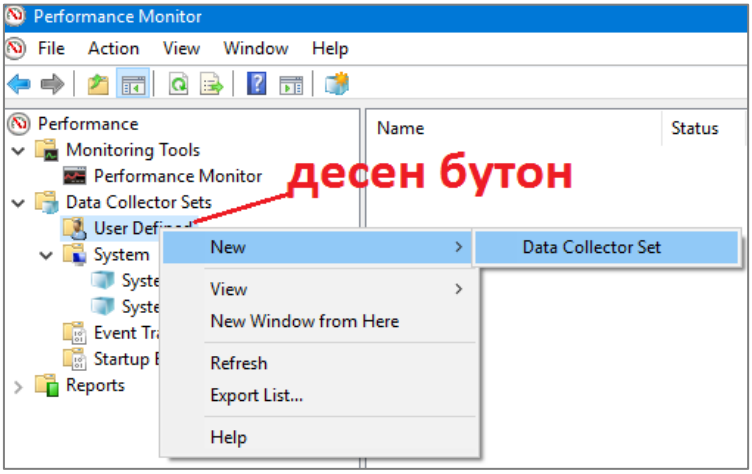
- Преглед на данните в лога (View Log Data) – Ctrl+L;
- Промяна на изгледа на графиката (Change graph type) – Ctrl+G;
- Изтриване на брояч (Delete key) – за да се изтрие брояч, първо трябва да се маркира. За по-голямо удобство, може да се премине в изглед Report.
- Копиране на свойства на брояч (Copy properties) - Ctrl+C;
- Разглеждане на свойствата на изгледа (Properties) – Ctrl+Q. Може да се добавят / премахват броячи, да се променя цвета на брояча, с който той се идентифицира в графиката и т.н.
- Спиране на наблюдението (Freeze Display)- Ctrl+F;
- Възстановяване на наблюдението (Unfreeze Display)- Ctrl+F.

Друга възможност на инструмента е свързана с управление на наборите от данни, които могат да се наблюдават (Data Collector Sets). Те могат да са потребителски дефинирани (User Defined) и системни (System). Вж. Фиг. 11.

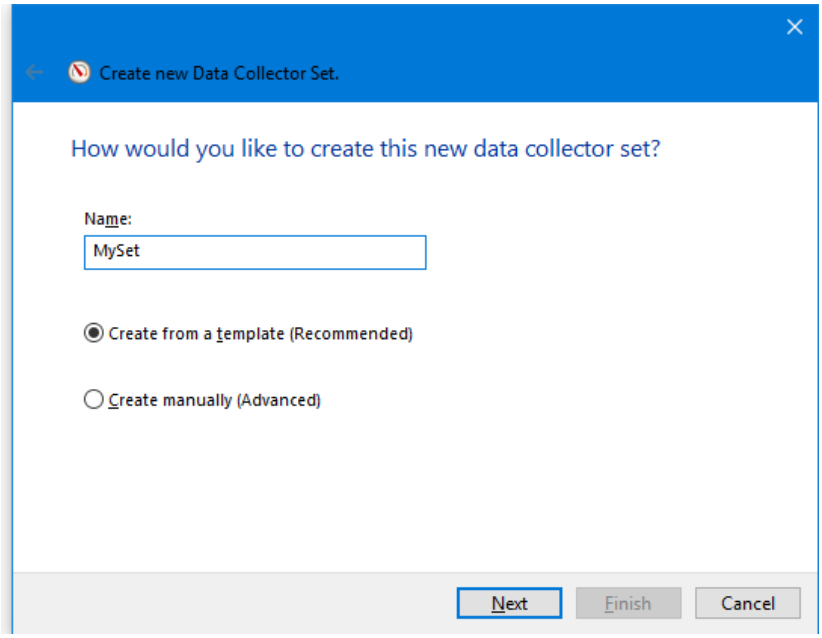


Фиг. 11. Performance Monitor - Data Collector Sets

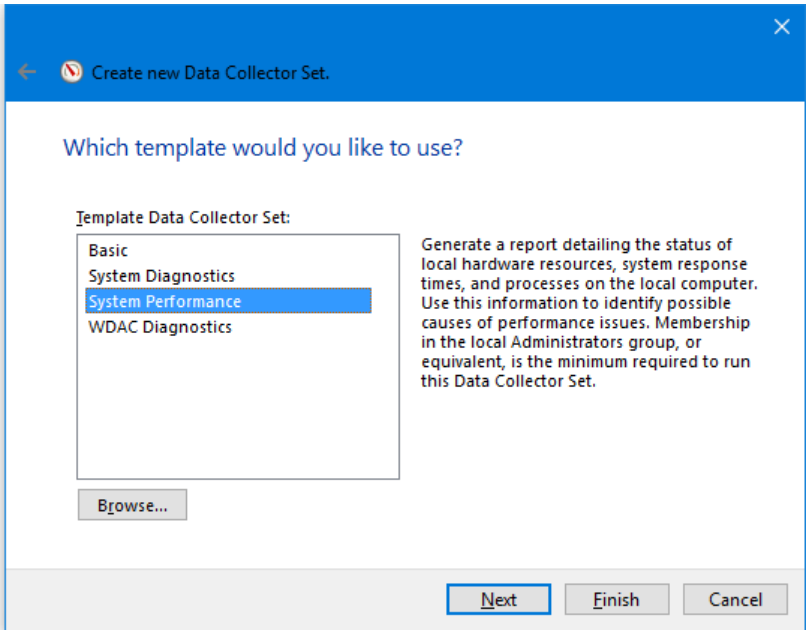
За създаване на нов потребителски набор от данни проследете фигури от 12 до



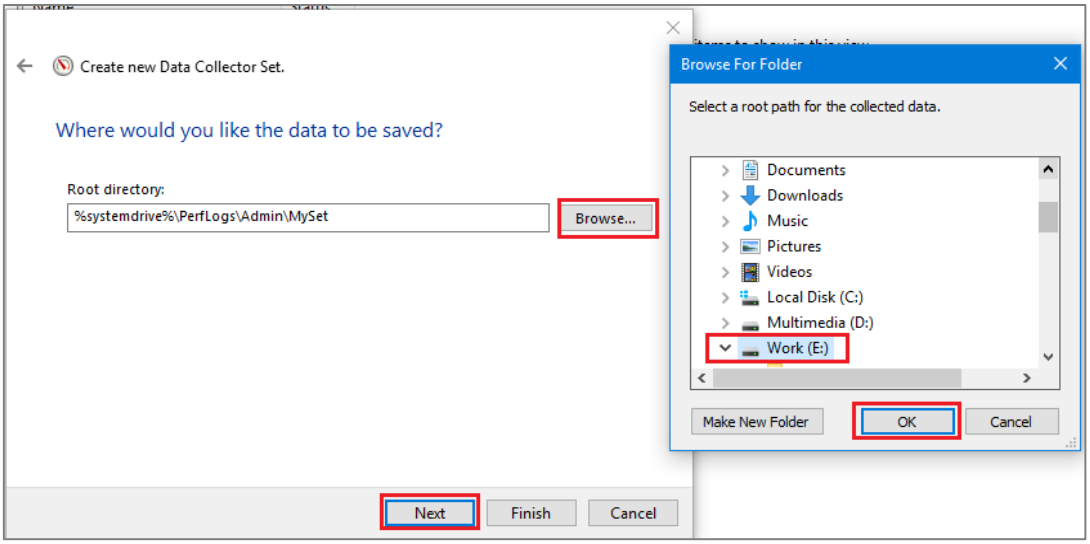
Фиг. 12. Performance Monitor – Потребителски дефиниран набор от данни - 1



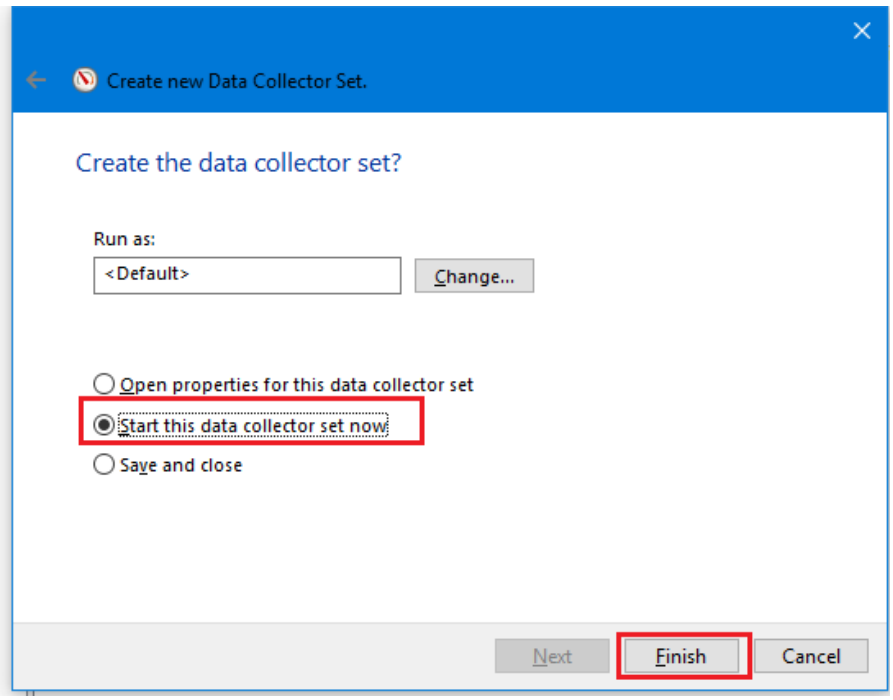
Фиг. 13. Performance Monitor – Потребителски дефиниран набор от данни - 2



Фиг. 14. Performance Monitor – Потребителски дефиниран набор от данни - 3

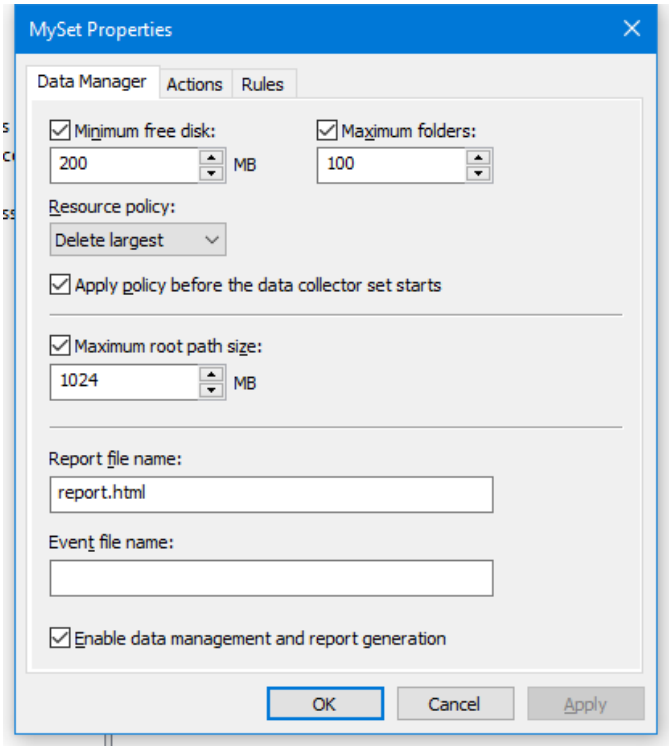


Фиг. 15. Performance Monitor – Потребителски дефиниран набор от данни - 4



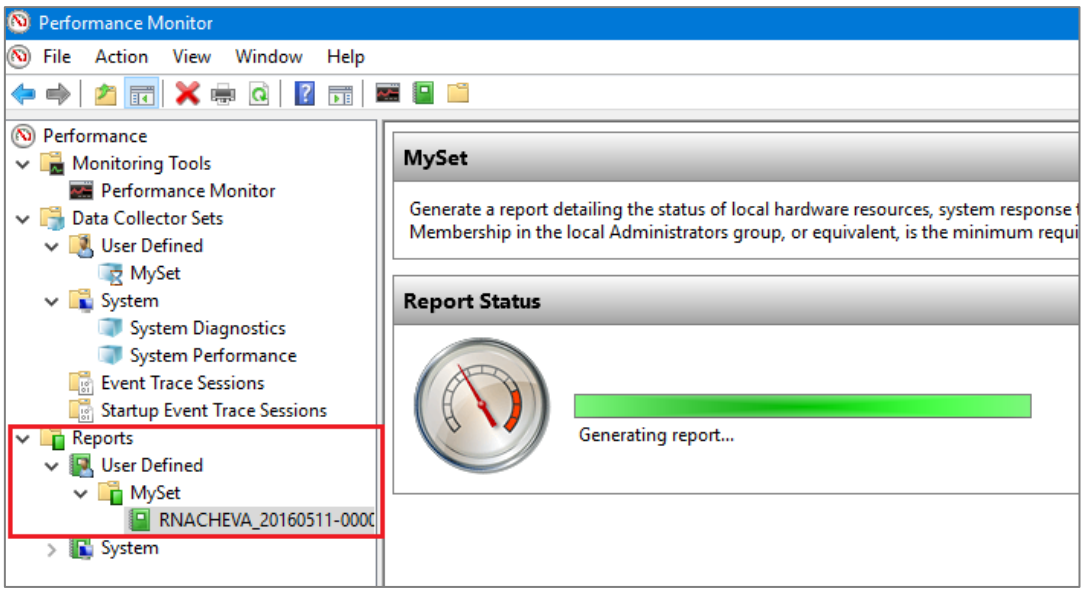
Фиг. 16. Performance Monitor – Потребителски дефиниран набор от данни - 5

От контекстното меню на новия потребителски набор могат да се регулират неговите настройки – Data Manager. Вж. Фиг. 17.



Фиг. 17. Performance Monitor – Настройки на потребителски дефиниран набор от данни

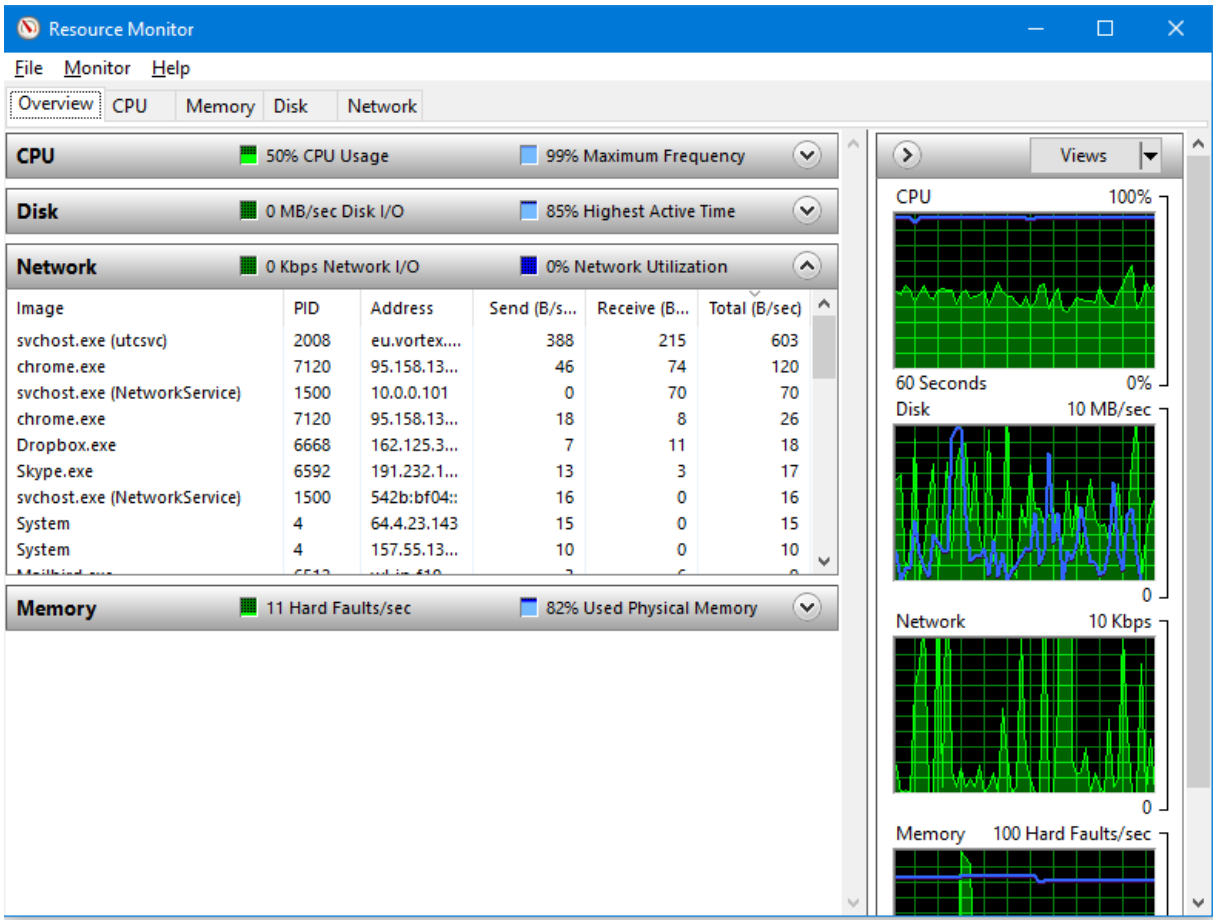
След създаване на новия набор от данни се генерира и потребителски отчет – Фиг. 18.



Фиг. 18. Performance Monitor – Потребителски отчет

Resource Monitor

Това е инструмент на Windows, чрез който могат да се наблюдават процесора, паметта, диска и мрежата. Стартира се чрез resmon.exe. Вж. Фиг. 19. Инструментът може да се използва като алтернатива на Task Manager -> Performance, която дава по-детайлна информация.

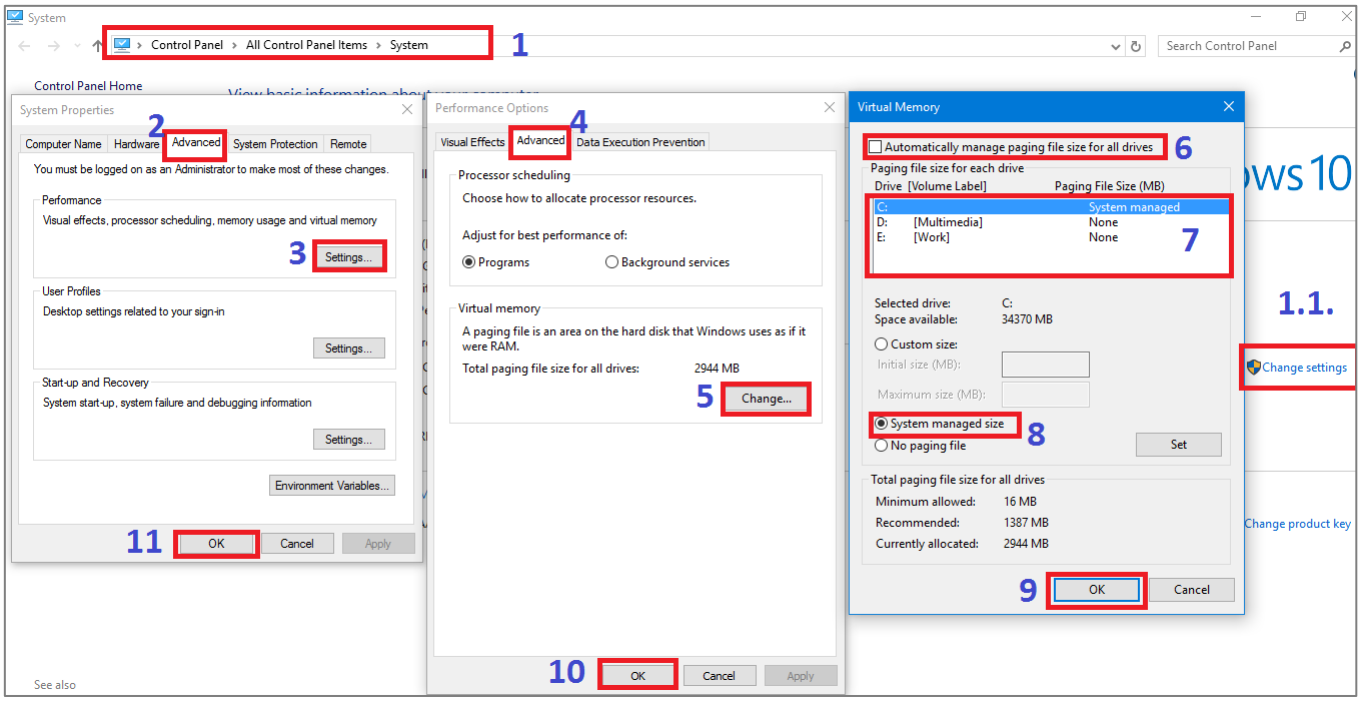


Фиг. 19. Resource Monitor

За всеки от включените за наблюдение инструменти могат да се наблюдават различни параметри. За целта прегледайте табовете с имената на компонентите. Вж. Следния урок: http://bit.ly/1On1BqH .

2. Способи за управление на виртуалната памет

За управление на виртуалната памет проследете Фиг. 20.



Фиг. 20. Управление на виртуалната памет

Често срещани грешки, свързани с виртуалната памет, са PAGE_FAULT_IN_NONPAGED_AREA или KERNEL_DATA_INPAGE_ERROR Blue Screen of Death (BSOD). Те изискват, обикновено, ръчна промяна на големината на Pagefile.

III. ВЪПРОСИ ЗА САМОПРОВЕРКА

1. Какво представлява виртуалната памет и как се управлява в ОС Windows?

2. Какви способи за наблюдение на работата на системата познавате в ОС Windows? Разяснете предназначението на всеки от тях.

IV. ОБОБЩЕНИЯ И ДОПЪЛНИТЕЛНА ЛИТЕРАТУРА

Запомнете, че:

- *Event Viewer* дава възможност за преглед на лог файлове, съдържащи важна информация за настъпили събития в системата.

- *Performance Monitor* дава възможност за преглед на потребителски дефинирана информация в реално време, включително и за съхраняване на наблюдението за определен период от време (поддържа лог файлове).

- *Resource Monitor* е алтернатива на Task Manager, която съдържа по-подробна информация за текущата работа на машината.

Допълнителна литература:

1. List of Microsoft Windows components
2. Windows 10 TechCenter