**Министерство науки и высшего образования Российской Федерации**

федеральное государственное автономное образовательное учреждение высшего образования

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**Лабораторная работа №4**

«Работа со средствами мониторинга и диагностики в Windows»

по дисциплине «**Администрирование ОС Windows Server**»

**Авторы:**

Сарипов Денис Рустамович

Золотарёва Анастасия Кирилловна

**Факультет:** ИТиП

**Группа:** M3206

**Преподаватель:**

Береснеев Артём Дмитриевич



Санкт-Петербург  
2021

Ход работы:  
1.1 Напишите скрипт, который создает Журнал Работы с именем «ProcessMonitoringLog». Если журнал существует, то выводится сообщение об этом.

Изображение выглядит как текст

Автоматически созданное описание

1.2a Напишите скрипт на PowerShell, который:

при запуске выводит список запущенных процессов (PID, Имя процесса, Путь к исполняемому файлу, Пользователь процесса, Утилизация CPU, Занимаемая память, Время Получения данных).

Изображение выглядит как текст

Автоматически созданное описание

1.2b Записывает эти данные в CSV файл

Изображение выглядит как текст

Автоматически созданное описание

1.2c При успешном сохранении данных пишет в журнал ProcessMonitoringLog сообщение об успехе, при ошибках сохранения – сообщение об ошибке.

Изображение выглядит как текст

Автоматически созданное описание

2.1 С помощью PowerShell добавьте автоматический запуск скрипта из Части 1. п.2 в планировщике заданий Windows (Task Scheduler), так чтобы, но запускался каждые 3 минуты, даже тогда, когда питание идет не от батареи или ИБП.

2.2 Убедитесь в работоспособности решения.

Изображение выглядит как текст

Автоматически созданное описание

3.1 Ознакомитесь с журналом событий.

Ознакомился

3.2 Создайте настраиваемое представление журнала,

позволяющее увидеть все неудачные попытки входа в ОС под именем Администратора.

Изображение выглядит как текст

Автоматически созданное описание

3.3a С помощью PowerShell напишите скрипт, который выводит в текстовый файл:

время последних 10 включений компьютера,

Изображение выглядит как текст

Автоматически созданное описание

3.3b время 5 последних установок пакетов обновлений с указанием названий обновлений (например KB1299393),

Изображение выглядит как текст

Автоматически созданное описание

3.3c количество ошибок и количество предупреждений за последние 24 часа.

Изображение выглядит как текст, табло

Автоматически созданное описание

4.1 создать в программе Performance Monitor Группу Сборщиков

Данных, которая будет содержать:  
a. Счетчик Производительности записи которого позволят

сравнить загрузку аппаратного обеспечения платформы. Счетчики для этого следует выбрать самостоятельно, но они должны отражать использование памяти, дисковой подсистемы, процессора и сети.

b. Периодичность журнала установить в 5 секунд.

Изображение выглядит как текст

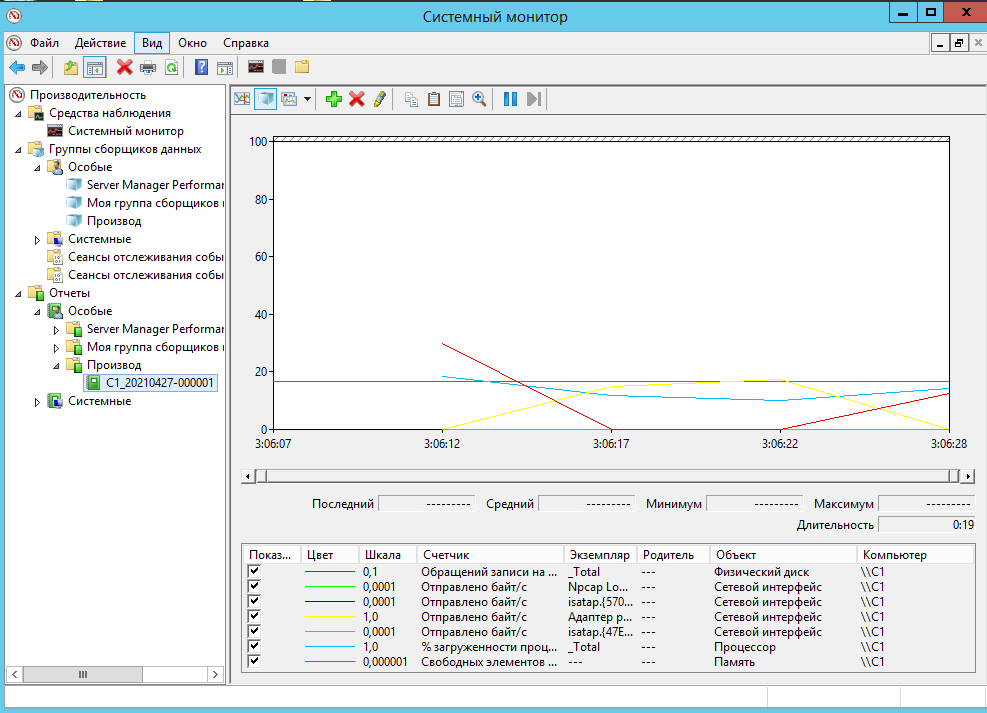
Автоматически созданное описание

4.1c Сборщик данных отслеживания событий, фиксирующий события ядра Windows.

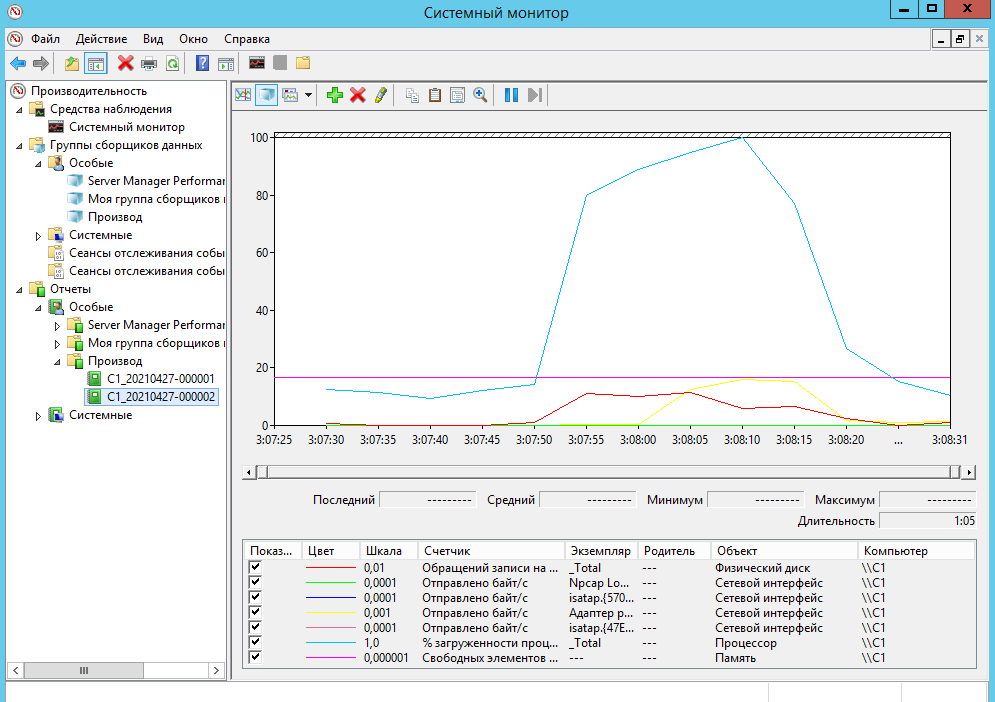
Изображение выглядит как текст

Автоматически созданное описание

4.2 before:



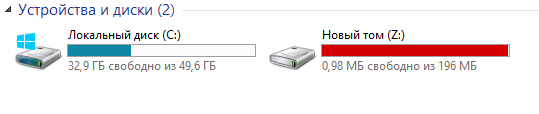
4.2 after:



4.3 С помощью механизма отчетов дайте первичный анализ загрузки в обоих случаях.

С помощью механизма отчётов видим, что нагрузка на систему увеличилась.

5.1 Добавьте в виртуальную машину еще один жесткий диск объемом 200 Мб. Включите виртуальную машину и создайте на новом диске раздел.



5.2 Создайте скрипит, который постепенно заполняет новый логический диск файлами размером до 1 Мб.

Изображение выглядит как текст

Автоматически созданное описание

5.3 Создайте скрипит, очищающий новый диск.

Изображение выглядит как текст

Автоматически созданное описание

Вопросы:  
1) Назначение каждого из журнала событий:

- Apllication – содержит события и ошибки приложений

- Security – записи, связанные с аудитами

- System – события ос и сервисов

- Setup – инсталяции обновлений windows

2) Перенаправленные события удобны при определении шаблонов элементов управления или использования страниц либо контейнеров макетаа

3) Путь до журналов событий Windows: %SystemRoot%\System32\Winevt\Logs\<раздел>

4) Как с помощью графической оснастки журнала событий установить по известному VID коду, когда было подключено и астроено устройство?   
Знаем, что существует файл “setupapi.dev.log” в котором по нужному vid коду можно найти интересующее нас устройство

5) Почему были выбраны конкретные счетчики в Части 4 п.1?

Обоснуйте выбор.

Память – свободных элементов записи таблицы, чтобы контролировать используемость памяти в данный момент  
Процессор-загруженность процессора – чтобы контролировать, насколько больше нагрузки стало на процессор

Сетевой интерфейс – получено байт, чтобы контролировать работу с веб ресурсами

Физический диск – обращение записи, чтобы контролировать работу жестких дисков

6) Как получить на консоль подробные параметры запланированного задания с помощью утилиты schtasks.exe? Проиллюстрируйте ответ на примере задания из части 5.

В утилите schtasks.exe есть флаг /Query, который как раз может задать запрос на получение информации о конкретном плане.

7) Опишите ваши выводы по пункту 5. Части 5.

Оповещения у системного монитора срабатывают не всегда, так как опрос работает лишь каждые n секунд(в нашем случае 5), поэтому и нет гарантий срабатывания.