**Министерство науки и высшего образования Российской Федерации**

федеральное государственное автономное образовательное учреждение высшего образования

**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»**

**Отчет**

по лабораторной работе №4

по дисциплине «**Администрирование Windsows Server**»

Автор: Триголос Алексей Павлович,

Факультет: ФИТиП

Группа: M3204

Преподаватель: Шараева Кристина Витальевна

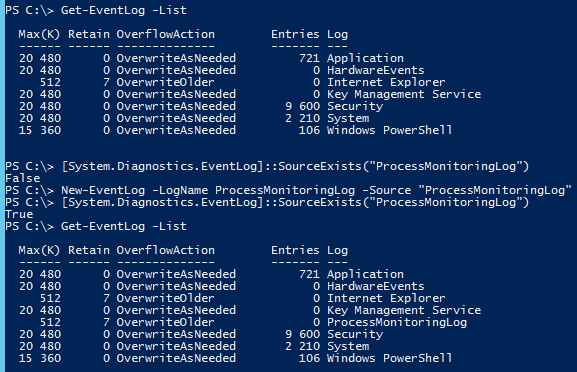
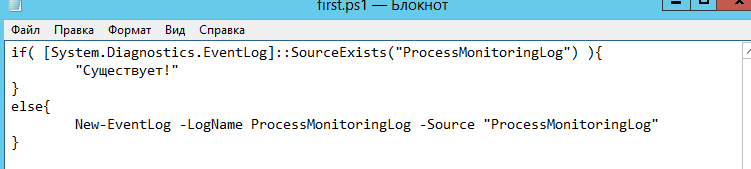


Санкт-Петербург 2021

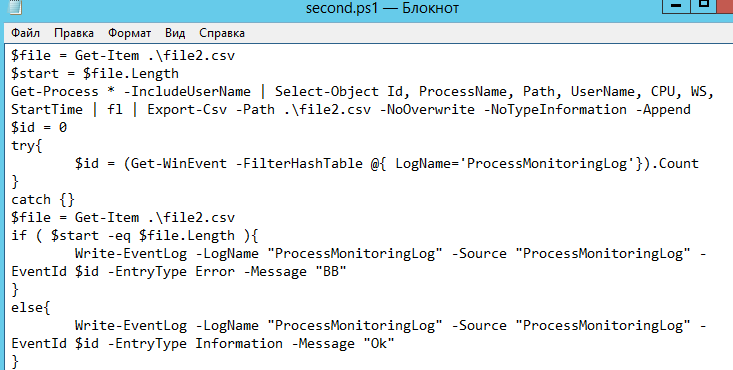
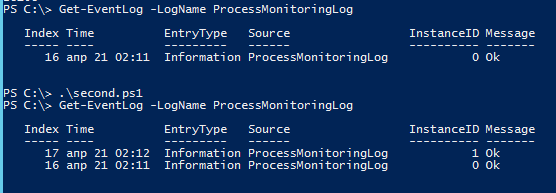
**Порядок выполнения работы:**

**Часть 1. Работа с процессами. Разработка скриптов.**

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

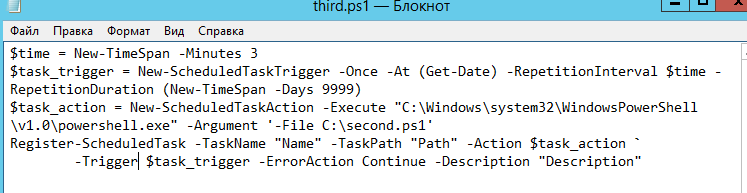
 

1. Напишите скрипт на PowerShell, который:
   1. при запуске выводит список запущенных процессов (PID, Имя процесса, Путь к исполняемому файлу, Пользователь процесса, Утилизация CPU, Занимаемая память, Время Получения данных).
   2. Записывает эти данные в CSV файл.
   3. При успешном сохранении данных пишет в журнал ProcessMonitoringLog сообщение об успехе, при ошибках сохранения – сообщение об ошибке.

**Часть 2. Планирование периодического выполнения.**

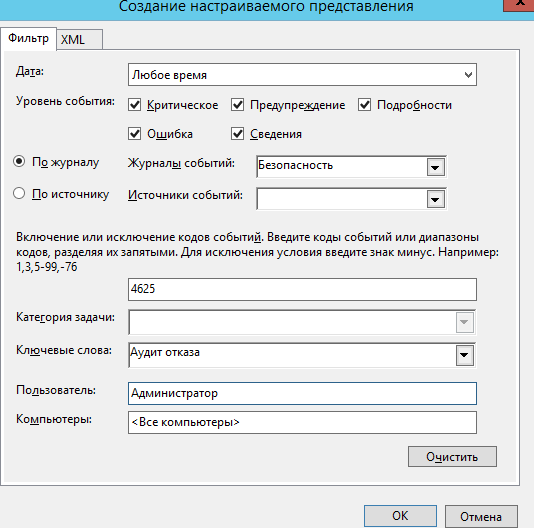
1. С помощью PowerShell добавьте автоматический запуск скрипта из Части 1. п.2 в планировщике заданий Windows (Task Scheduler), так чтобы, но запускался каждые 3 минуты, даже тогда, когда питание идет не от батареи или ИБП.



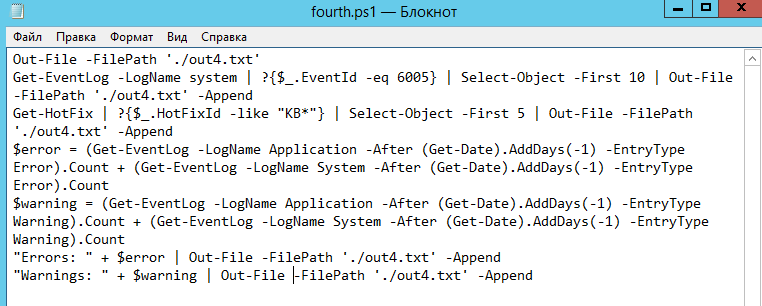
1. Убедитесь в работоспособности решения.

**Часть 3. Работа с журналом событий.**

1. Ознакомитесь с журналом событий.
2. Создайте настраиваемое представление журнала, позволяющее увидеть все неудачные попытки входа в ОС под именем Администратора.

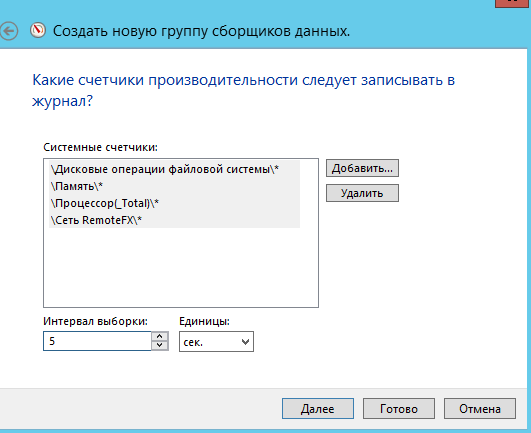


1. С помощью PowerShell напишите скрипт, который выводит в текстовый файл:
2. время последних 10 включений компьютера,
3. время 5 последних установок пакетов обновлений с указанием названий обновлений (например KB1299393),
4. количество ошибок и количество предупреждений за последние 24 часа.



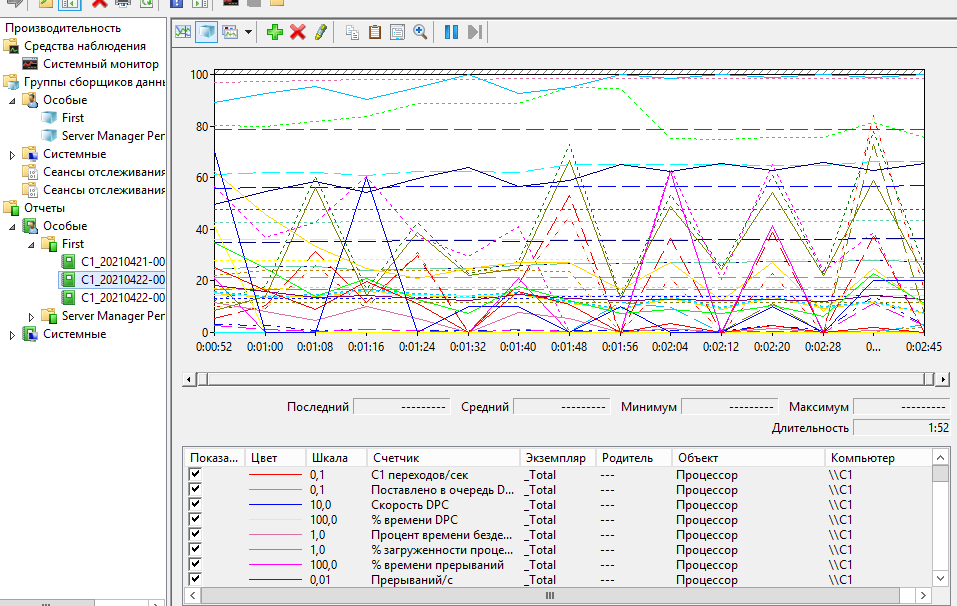
**Часть 4. Сбор и анализ данных**

1. создать в программе Performance Monitor Группу Сборщиков Данных, которая будет содержать:
   1. 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.
   2. Периодичность журнала установить в 5 секунд.
   3. Сборщик данных отслеживания событий, фиксирующий события ядра Windows.

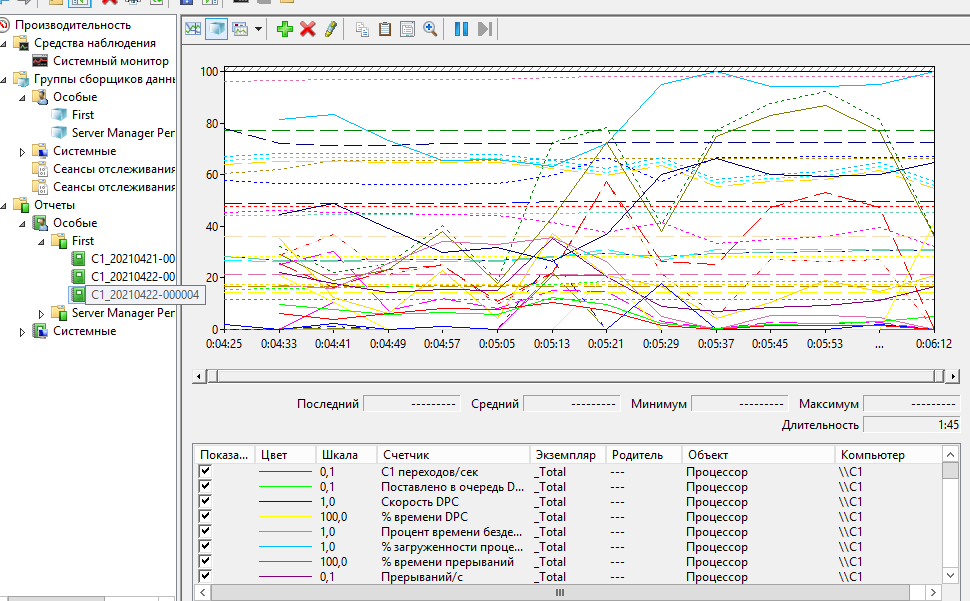


1. С помощью Группы Сборщиков Данных сравните загрузку системы в двух разных ситуациях. Это может быть загрузка при использовании разных приложений одного типа (2 антивируса, 2 браузера, 2 СУБД, 2 кодека и т. п.), наборы разных программ (MS Word + MS Excel и MS Excel + MS Access и т.п.) или одно и тоже приложение при разной его конфигурации.
2. С помощью механизма отчетов дайте первичный анализ загрузки в обоих случаях.
3. С помощью электронных таблиц или других средств анализа данных представите данные о загрузке в виде графиков.

Открыто несколько блокнотов, powershell’ов, браузеров и других приложений:

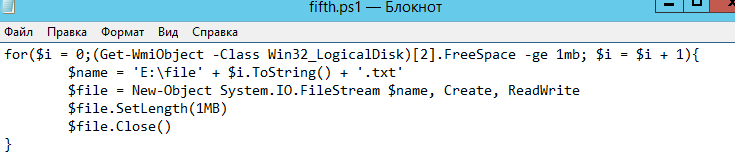


Запущен только системный монитор:

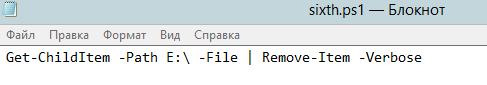


**Часть 5. Автоматизация реакции системы на ее состояние**

1. Добавьте в виртуальную машину еще один жесткий диск объемом 200 Мб. Включите виртуальную машину и создайте на новом диске раздел.
2. Создайте скрипит, который постепенно заполняет новый логический диск файлами размером до 1 Мб.



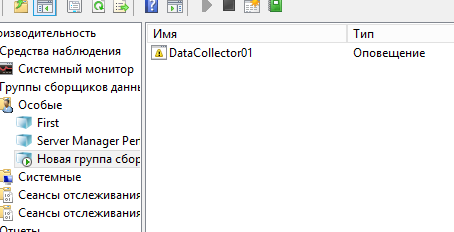
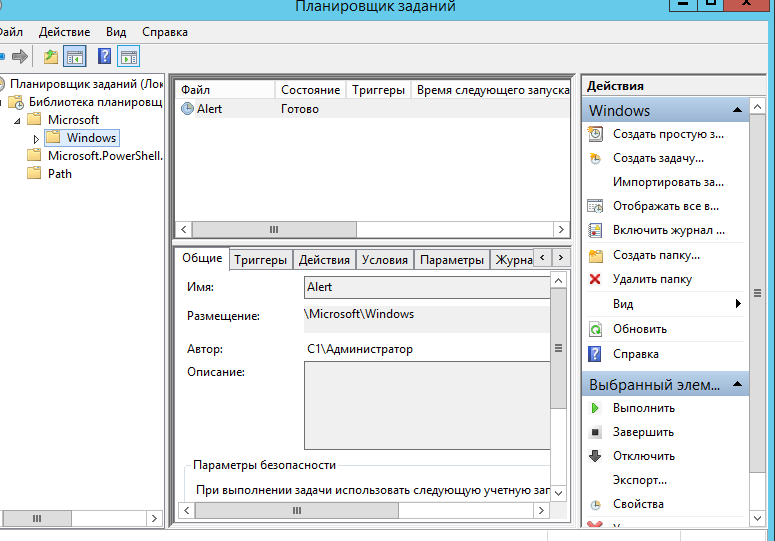
1. Создайте скрипит, очищающий новый диск.



1. В Performance Monitor создайте новую Группу Сборщиков Данных с Оповещением счетчика производительности, который, срабатывает в случае, если осталось менее 20% свободного места на новом разделе и выводящее предупреждение в журнал событий и запускающее сприт из п.3.

Разработчики Performance Monitor предполагают, что нужно в Планировщике заданий создать задание, выполняющее скрипт из п. 3 и указать имя этого задания в настройках Сборщика данных отслеживания событий.

1. Проверьте срабатывание оповещений. Вероятно, вы обнаружите неожиданное поведение системы. Попробуйте выяснить причину, заменяя используемые счетчики.

Вопросы:

1. В чем назначение каждого из разделов журнала событий?

Разграничение журнала по источникам.

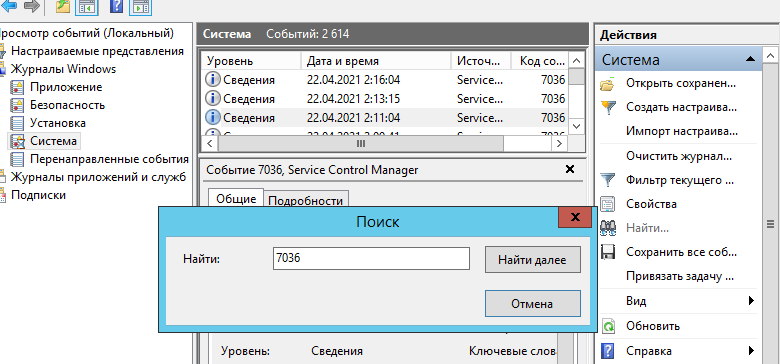
1. Зачем нужен раздел Перенаправленные события?

Используется для отображений событий на удалённых компьютерах.

1. Где находится журналы событий Windows в виде файлов?

C:\Windows\System32\winevt\Logs\

1. Как с помощью графической оснастки журнала событий установить по известному VID коду, когда было подключено и настроено устройство?



1. Почему были выбраны конкретные счетчики в Части 4 п.1? Обоснуйте выбор.

Выбрал их по той причине, что мне показалось выбрать эти конкретные счетчики верным.

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

