МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

Университет ИТМО

Факультет информационных технологий и программирования
Кафедра информационных систем

Практическая работа № **4**
Работа со средствами мониторинга и диагностики в Windows

Выполнили студенты группы **M32101**:
Рожновский Иван
Юрченко Владислав

САНКТ-ПЕТЕРБУРГ
2021

Вопросы:

1) Приложение – хранит важные события, связанные с конкретным приложением. Эти данные помогут системному администратору установить причину отказа той или иной программы.

Система – хранит события операционной системы или ее компонентов (например, неудачи при запусках служб или инициализации драйверов; общесистемные сообщения и прочие сообщения, относящиеся к системе в целом).

Безопасность – хранит события, связанные с безопасностью (такие как: вход/выход из системы, управление учётными записями, изменение разрешений и прав доступа к файлам и папкам).

Перенаправленных события — сюда по умолчанию сохраняются события, перенаправленные с других компьютеров сети.

Установка – события, связанные с инсталляцией обновлений Windows, дополнительных приложений.

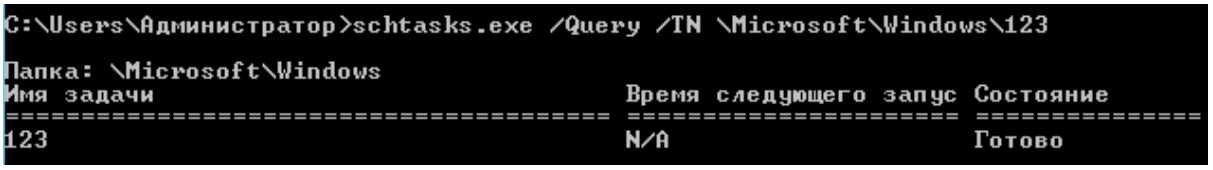
2) Указанные события, происходящие на исходных компьютерах, будут перенаправлены в журнал переадресованных событий, где вы сможете проанализировать их все с одного компьютера.

3) Файлы находятся в папке C:\Windows\System32\winevt\Logs с расширением .evtx.

4) Добавить новое представление соответствующему фильтеру.

5) Для “физического диска” мы выбрали — скорость чтения и записи на диск а также процент активности диска. Для сетевого адаптера выбрали — объем отправленных и полученных данных. Для процессора — его % загруженности. Для памяти — % ее использования. Данные параметры мы выбрали из-за того, что на наш взгляд они лучше всего дают представление об объеме использования данных частей компьютера.

6) Для подробных параметров можно добавить флаг /V, но винда очень некрасиво выводит результат.



7) Чтобы получить требуемый в задании результат требуется проделать неинтуитивные махинации с группами. Так, для оптимальной работы программе требуется запуск группы сборщика данных, в противном случае, она отказывалась работать.

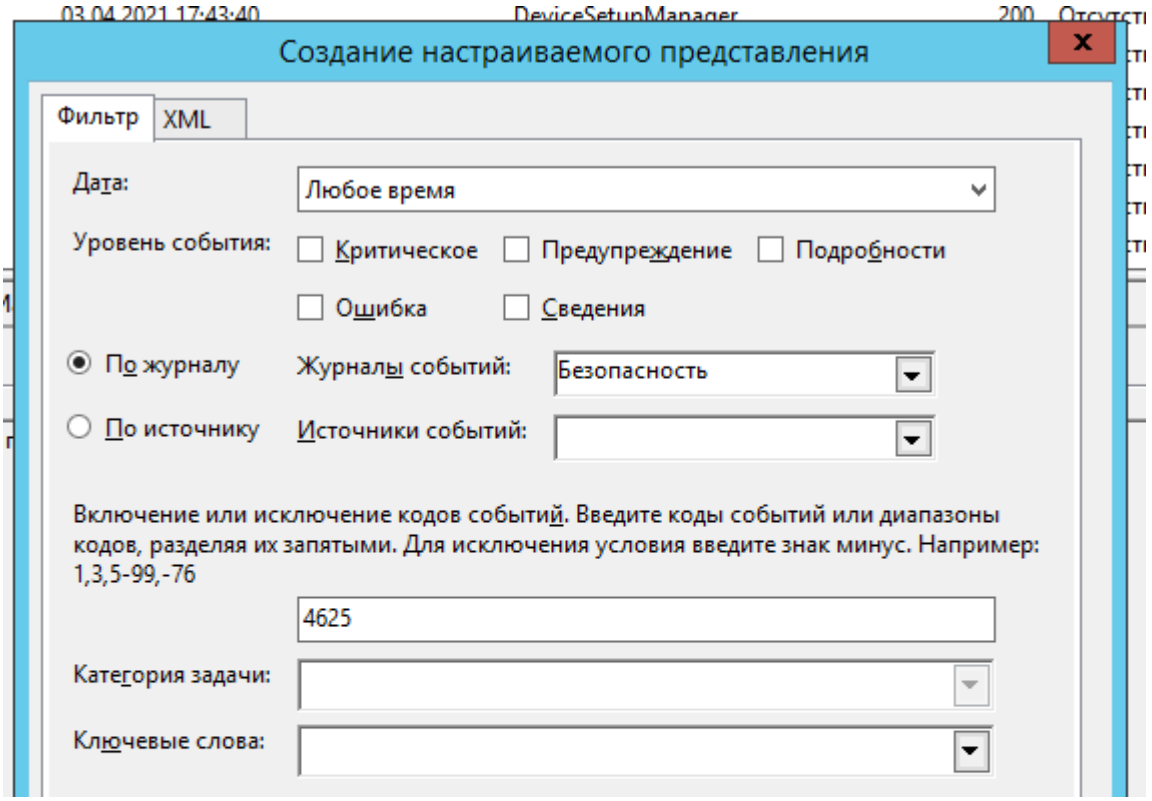
Артефакты:

1. ```
   try {
         New-EventLog -LogName ProcessMonitoringLog -Source Test
   }
   catch {
         Write-Host "Event log with this name already exists"
   }
   ```

```
try {
      Get-Process -IncludeUserName | Select-Object Id,
ProcessName, Path, Username, CPU, WS, @{Name="Date";
Expression={Get-Date}} | Export-Csv "C:\abc.csv"
      Write-EventLog -LogName "ProcessMonitoringLog" -Source
Test -EventId 1 -EntryType SuccessAudit -Message "Process info
file was created successfully"
}
catch {
      Write-EventLog -LogName "ProcessMonitoringLog" -Source
Test -EventId 2 -EntryType FailureAudit -Message "Process info
file was not created"
}
```

2. ```
   $act = New-ScheduledTaskAction -Execute "powershell.exe"
   -Argument "C:\processes.ps1"
   $trigger = New-ScheduledTaskTrigger -Once -At (Get-Date)
   -RepetitionInterval (New-TimeSpan -Minutes 3)
   -RepetitionDuration ([System.TimeSpan]::MaxValue)
   $settings = New-ScheduledTaskSettingsSet
   -DontStopIfGoingOnBatteries -AllowStartIfOnBatteries

   Register-ScheduledTask -TaskName "Process monitoring" -Action
   $act -Trigger $trigger -Settings $settings
   ```

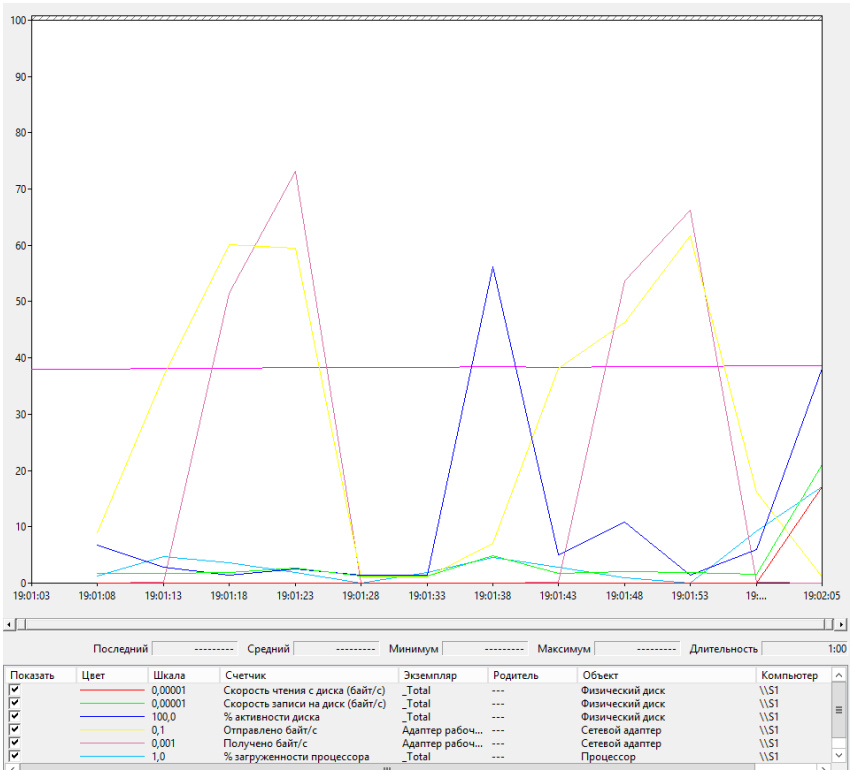
3. 

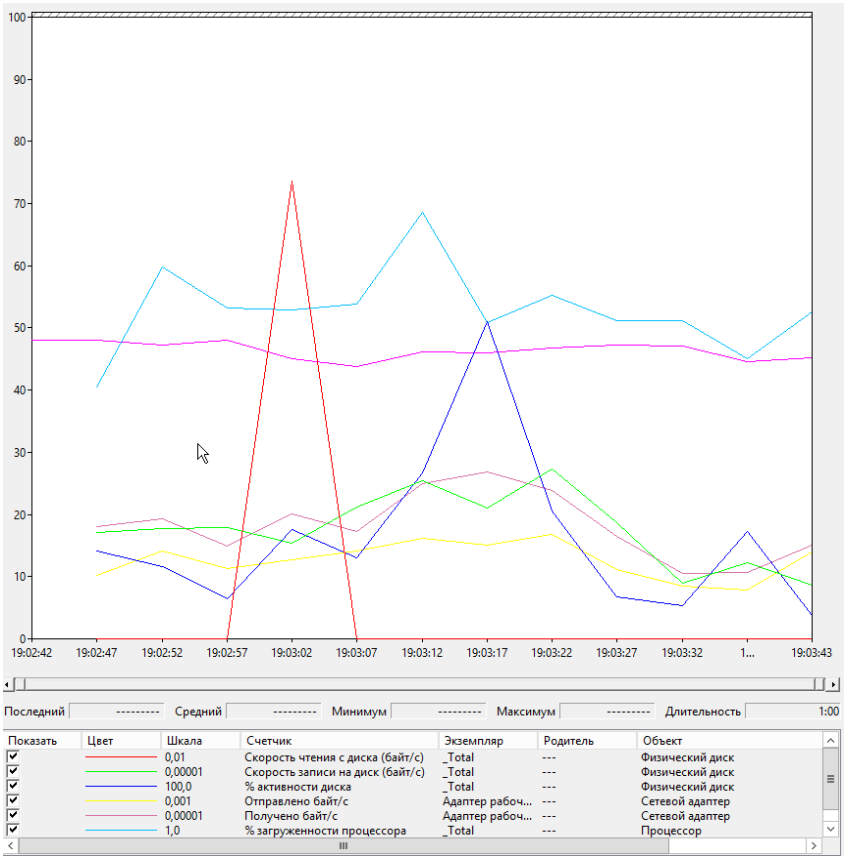
4. `Get-EventLog -LogName "System" -Newest 10 -InstanceId 12`

   `Get-SilWindowsUpdate | Sort-Object -Property InstallDate | Select -First 5`

   `@(Get-EventLog -list | %{Get-EventLog -LogName $_.Log -EntryType @("Error", "Warning") -After (Get-Date).AddDays(-1) -ErrorAction Ignore}).Count`

5.





6.
```
$i = 0
while (1) {
    $i = $i + 1
```

```
    Copy-Item -Path "C:\1.jpg" -Destination "E:\$i"
    Start-Sleep -Milliseconds 100
}
-------------
Remove-Item -Path "E:\*"
```