Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет ИТМО»

Факультет информационных технологий и программирования

Администрирование в ОС Windows Server

Лабораторная работа №6

Работа со средствами мониторинга и диагностики в Windows.

Выполнили студенты группы № M33091

Фисенко Никита Данилович

Рустамов Марк Самирович

Санкт-Петербург 2023

Цель работы:

Ознакомиться со встроенными средствами технического мониторинга, назначением и принципами работы Prefomance Monitor. Получить навыки сбора и анализа данных, позволяющих оценивать производительность системы. Получить практические навыки поиска "узких мест" в производительности системы. Получить дополнительные навыки по управлению Windows Server, управлению процессами и журналами работы.

Артефакты:

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

```
$journalName = "ProcessMonitoringLog"
$journalExists = Get-EventLog -LogName Application -Source $journalName -
ErrorAction SilentlyContinue

if (-not $journalExists) {
    try {
        New-EventLog -LogName Application -Source $journalName -ErrorAction
Stop
        Write-Host "Журнал работы '$journalName' успешно создан."
    } catch {
        Write-Host "Ошибка при создании журнала: $_"
    }
} else {
    Write-Host "Журнал работы '$journalName' уже существует."
}
```

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

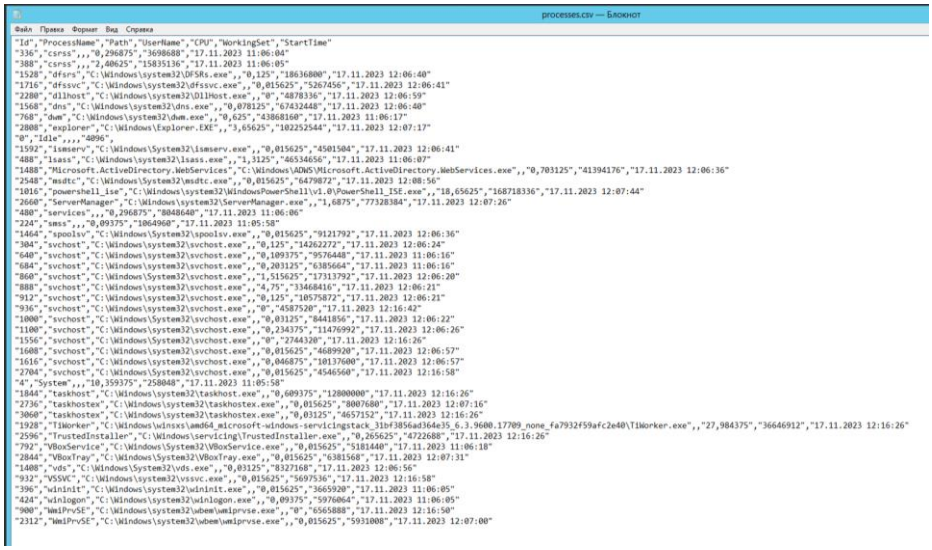
```
$processes = Get-Process | Select-Object Id, ProcessName, Path, UserName,
CPU, WorkingSet, StartTime

Write-Host "Список запущенных процессов:"
$processes | Format-Table -AutoSize

$csvFilePath = "C:\Users\Администратор\Desktop\processes.csv"

try {
    $processes | Export-Csv -Path $csvFilePath -NoTypeInformation -Force
    Write-Host "Данные успешно сохранены в CSV файл: $csvFilePath"

    $logMessage = "Данные о процессах успешно сохранены в CSV файл:
$csvFilePath"
    Write-EventLog -LogName Application -Source ProcessMonitoringLog -
EventId 1 -EntryType Information -Message $logMessage
}
catch {
    $errorMessage = "Ошибка при сохранении данных в CSV файл: $_"
    Write-Host $errorMessage
```

```
        Write-EventLog -LogName Application -Source ProcessMonitoringLog -
    EventId 2 -EntryType Error -Message $errorMessage
    }
```

Просмотр ProcessMonitoringLog:

```
$journalName = "ProcessMonitoringLog"

$events = Get-EventLog -LogName Application -Source $journalName -Newest 10

foreach ($event in $events) {
    Write-Host "Event ID: $($event.EventID)"
    Write-Host "Time Generated: $($event.TimeGenerated)"
    Write-Host "Message: $($event.Message)"
    Write-Host "-------------------------"
}
```

```
PS C:\Users\Администратор> C:\Users\Администратор\Desktop\processes.ps1
Список запущенных процессов:

  Id ProcessName                          Path
  -- -----------                          ----
 336 csrss
 388 csrss
1528 dfsrs                                C:\Windows\system32\DFSRs.exe
1716 dfssvc                               C:\Windows\system32\dfssvc.exe
2280 dllhost                              C:\Windows\system32\DllHost.exe
1568 dns                                  C:\Windows\system32\dns.exe
 768 dwm                                  C:\Windows\system32\dwm.exe
2808 explorer                             C:\Windows\Explorer.EXE
   0 Idle
1592 ismserv                              C:\Windows\System32\ismserv.exe
 488 lsass                                C:\Windows\system32\lsass.exe
1488 Microsoft.ActiveDirectory.WebServices C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe
2548 msdtc                                C:\Windows\System32\msdtc.exe
1016 powershell_ise                       C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe
2660 ServerManager                        C:\Windows\system32\ServerManager.exe
 480 services
 224 smss
1464 spoolsv                              C:\Windows\System32\spoolsv.exe
 304 svchost                              C:\Windows\system32\svchost.exe
 640 svchost                              C:\Windows\system32\svchost.exe
 684 svchost                              C:\Windows\system32\svchost.exe
 860 svchost                              C:\Windows\system32\svchost.exe
 888 svchost                              C:\Windows\system32\svchost.exe
 912 svchost                              C:\Windows\system32\svchost.exe
 936 svchost                              C:\Windows\system32\svchost.exe
1000 svchost                              C:\Windows\System32\svchost.exe
1100 svchost                              C:\Windows\system32\svchost.exe
1556 svchost                              C:\Windows\System32\svchost.exe
1608 svchost                              C:\Windows\system32\svchost.exe
1616 svchost                              C:\Windows\system32\svchost.exe
2704 svchost                              C:\Windows\System32\svchost.exe
   4 System
1844 taskhost                             C:\Windows\system32\taskhost.exe
2736 taskhostex                           C:\Windows\system32\taskhostex.exe
3060 taskhostex                           C:\Windows\system32\taskhostex.exe
1928 TiWorker                             C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17...
2596 TrustedInstaller                     C:\Windows\servicing\TrustedInstaller.exe
 792 VBoxService                          C:\Windows\System32\VBoxService.exe
2844 VBoxTray                             C:\Windows\System32\VBoxTray.exe
1408 vds                                  C:\Windows\System32\vds.exe
 932 VSSVC                                C:\Windows\system32\vssvc.exe
 396 wininit                              C:\Windows\system32\wininit.exe
 424 winlogon                             C:\Windows\system32\winlogon.exe
 900 WmiPrvSE                             C:\Windows\system32\wbem\wmiprvse.exe
2312 WmiPrvSE                             C:\Windows\system32\wbem\wmiprvse.exe


Данные успешно сохранены в CSV файл: C:\Users\Администратор\Desktop\processes.csv

PS C:\Users\Администратор> C:\Users\Администратор\Desktop\Безымянный2.ps1
Event ID: 1
Time Generated: 11/17/2023 12:17:41
Message: Данные о процессах успешно сохранены в CSV файл: C:\Users\Администратор\Desktop\processes.csv
-------------------------
Event ID: 1
Time Generated: 11/17/2023 12:15:32
Message: Тестовое событие.
-------------------------

PS C:\Users\Администратор>
```



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.

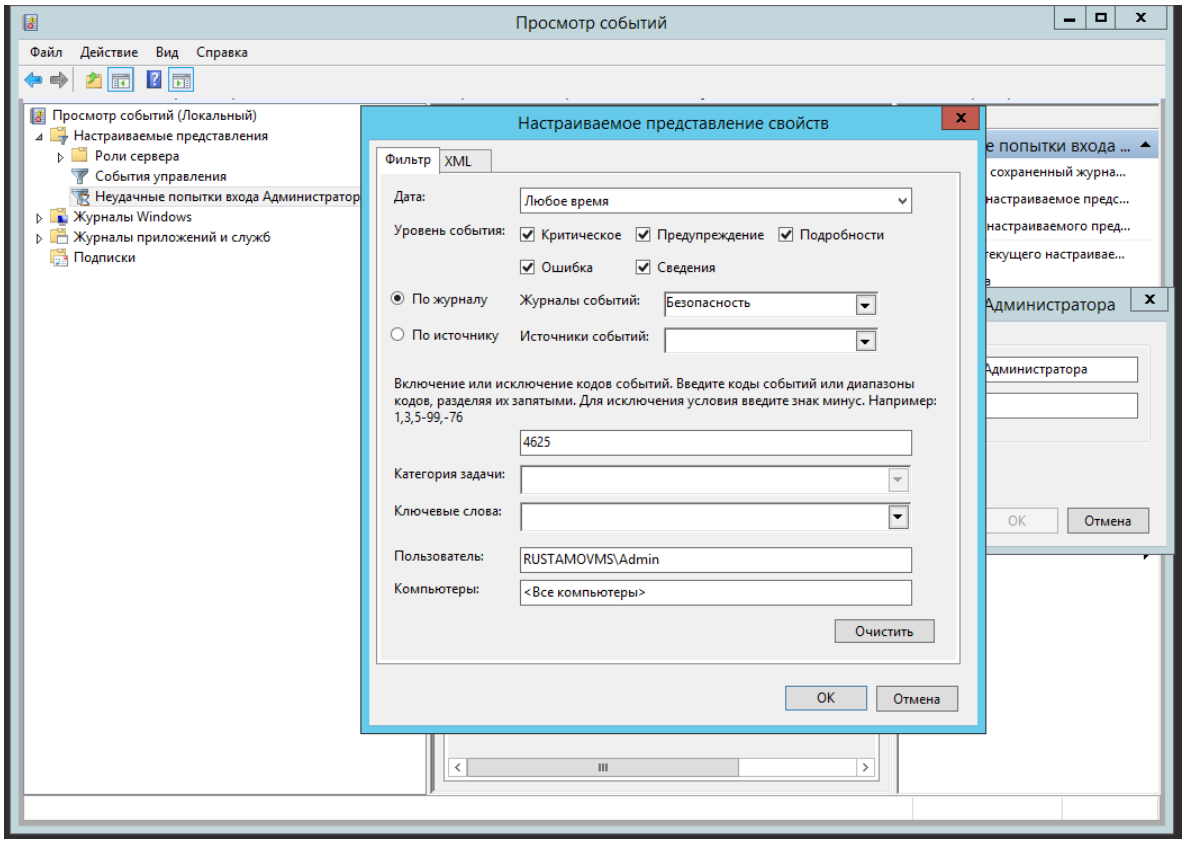
```
$ScriptPath = "C:\Users\Администратор\Desktop\processes.ps1"

$TaskName = "MyTask"
if (Get-ScheduledTask -TaskName $TaskName -ErrorAction
SilentlyContinue) {
    Write-Host "Задача с именем $TaskName уже существует."
} else {
    $Action = New-ScheduledTaskAction -Execute "powershell.exe" -
Argument "-NoProfile -ExecutionPolicy Bypass -File $ScriptPath"

    $Trigger = New-ScheduledTaskTrigger -Once -At ([DateTime]::Now) -
RepetitionInterval ([TimeSpan]::FromMinutes(3)) -RepetitionDuration
([TimeSpan]::MaxValue)

    Register-ScheduledTask -Action $Action -Trigger $Trigger -TaskName
$TaskName

    Write-Host "Задача успешно создана."
}
```

```
PS C:\Users\Администратор> C:\Users\Администратор\Desktop\planning.ps1

TaskPath                                 TaskName                 State
--------                                 --------                 -----
\                                        MyTask                   Ready
Задача успешно создана.
```

```
PS C:\Users\Администратор> C:\Users\Администратор\Desktop\Безымянный2.ps1
Event ID: 1
Time Generated: 11/17/2023 12:50:50
Message: Данные о процессах успешно сохранены в CSV файл: C:\Users\Администратор\Desktop\processes.csv
-----------------------
Event ID: 1
Time Generated: 11/17/2023 12:47:51
Message: Данные о процессах успешно сохранены в CSV файл: C:\Users\Администратор\Desktop\processes.csv
-----------------------
Event ID: 1
Time Generated: 11/17/2023 12:17:41
Message: Данные о процессах успешно сохранены в CSV файл: C:\Users\Администратор\Desktop\processes.csv
-----------------------
Event ID: 1
Time Generated: 11/17/2023 12:15:32
Message: Тестовое событие.
-----------------------

PS C:\Users\Администратор>
```

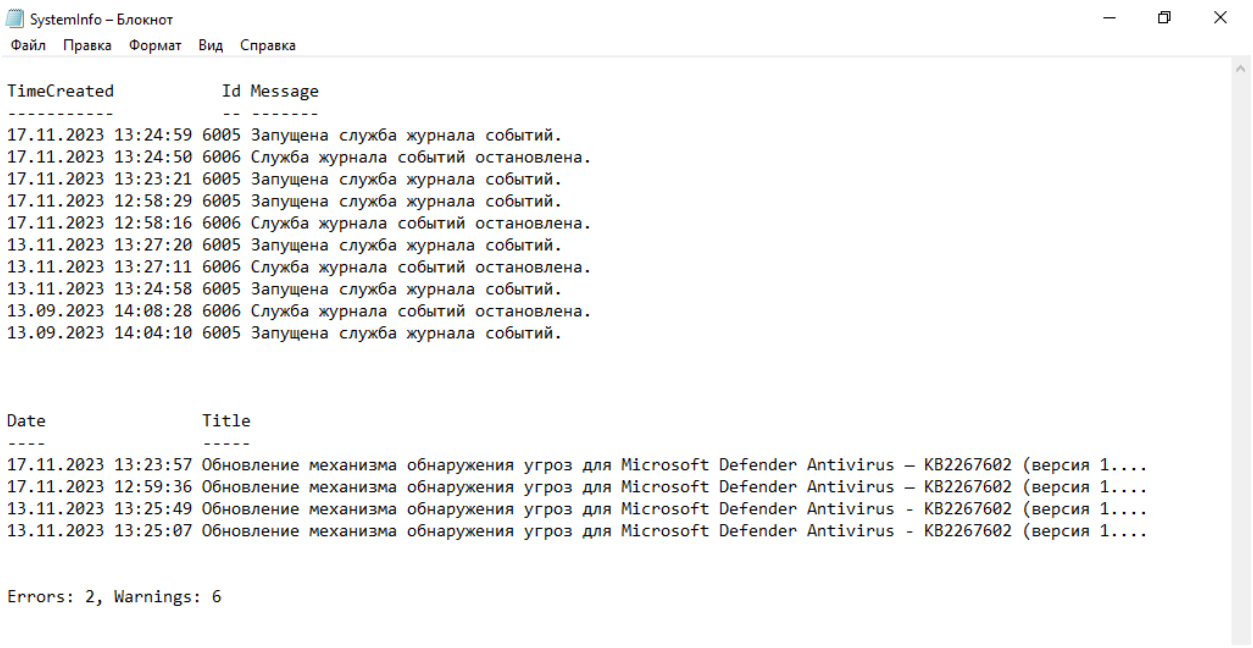
Часть 3. Работа с журналом событий.

1. Создайте настраиваемое представление журнала, позволяющее увидеть все неудачные попытки входа в ОС под именем Администратора.



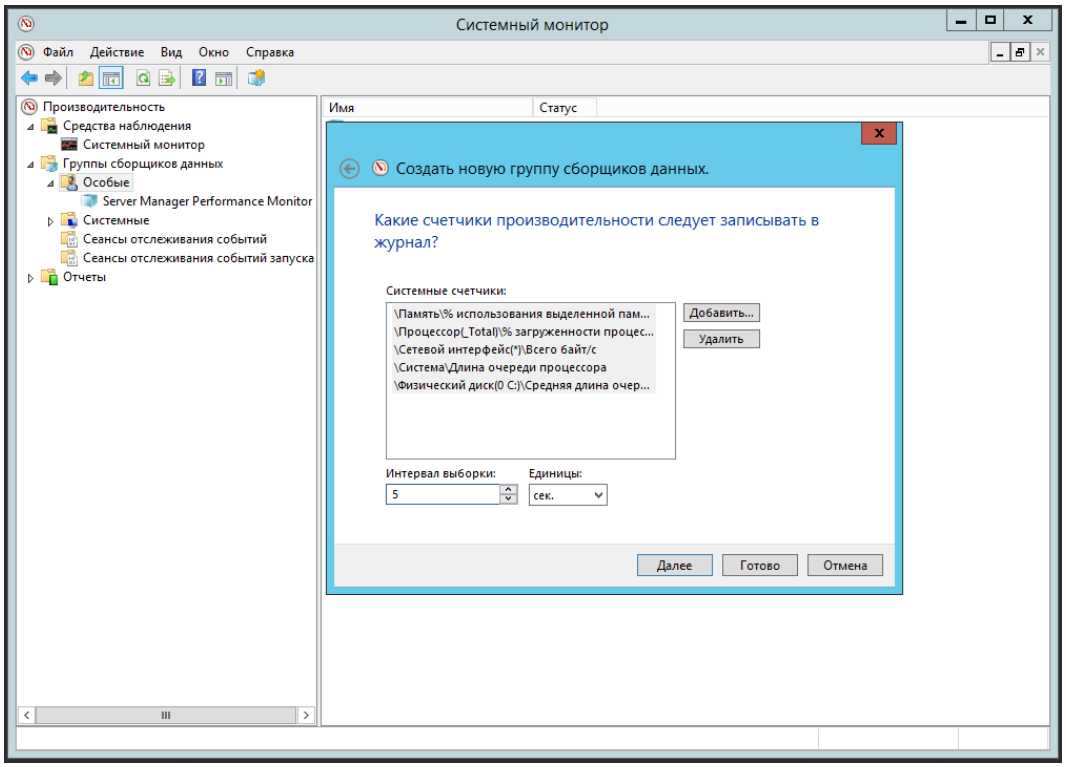
2. С помощью PowerShell напишите скрипт, который выводит в текстовый файл:
   a. время последних 10 включений компьютера,
   b. время 5 последних установок пакетов обновлений с указанием названий обновлений (например KB1299393),
   c. количество ошибок и количество предупреждений за последние 24 часа.

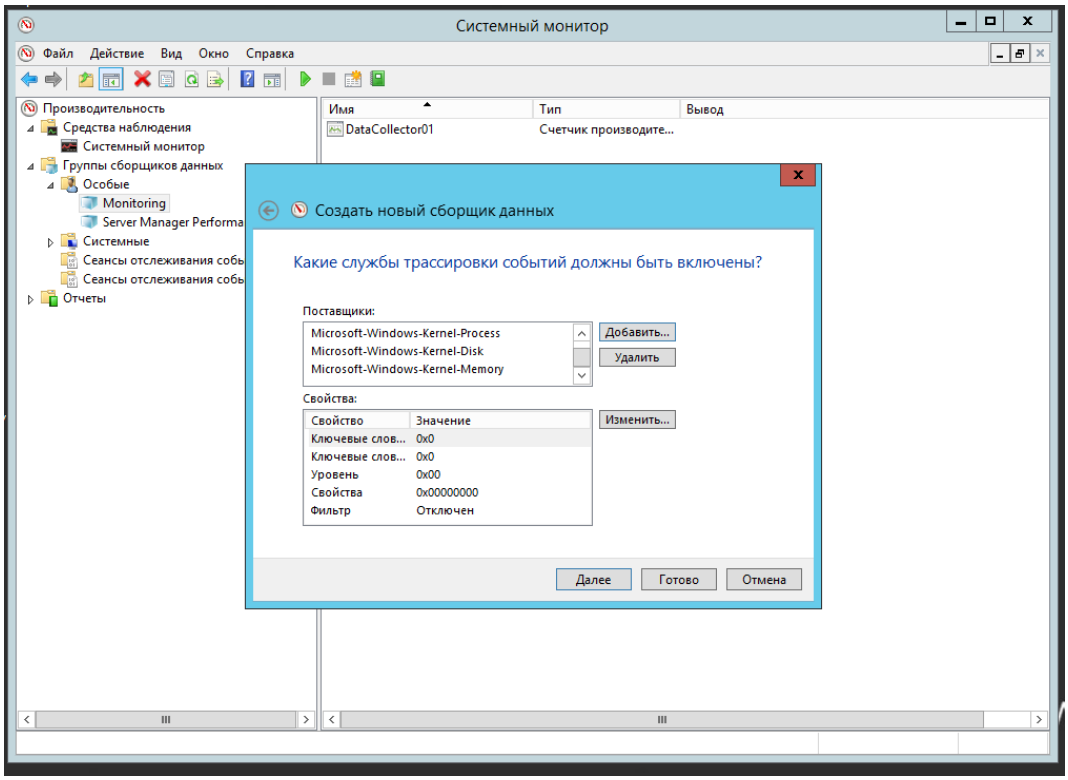
```
$bootEvents = Get-WinEvent -LogName System -FilterXPath
"*[System[(EventID=6005) or (EventID=6006)]]" -MaxEvents 10 | Sort-Object
TimeCreated -Descending
$bootEvents | Format-Table TimeCreated, Id, Message -AutoSize -Wrap | Out-
File -FilePath "C:\SystemInfo.txt" -Append

$updateHistory = Get-WUHistory -Last 5
$updateHistory | Format-Table Date, Title, UpdateID -AutoSize | Out-File -
FilePath "C:\SystemInfo.txt" -Append

$endTime = Get-Date
$startTime = $endTime.AddHours(-24)
$systemLogs = Get-WinEvent -LogName System -FilterXPath "*[System[(Level=2 or
Level=3) and TimeCreated[@SystemTime>='$($startTime.ToString("yyyy-MM-
ddTHH:mm:ss") )']]]"
$errorsAndWarnings = $systemLogs | Where-Object { $_.Level -eq 2 -or $_.Level
-eq 3 }

$errorCount = ($errorsAndWarnings | Where-Object { $_.Level -eq 2 }).Count
$warningCount = ($errorsAndWarnings | Where-Object { $_.Level -eq 3 }).Count

"Errors: $errorCount, Warnings: $warningCount" | Out-File -FilePath
"C:\SystemInfo.txt" -Append
```



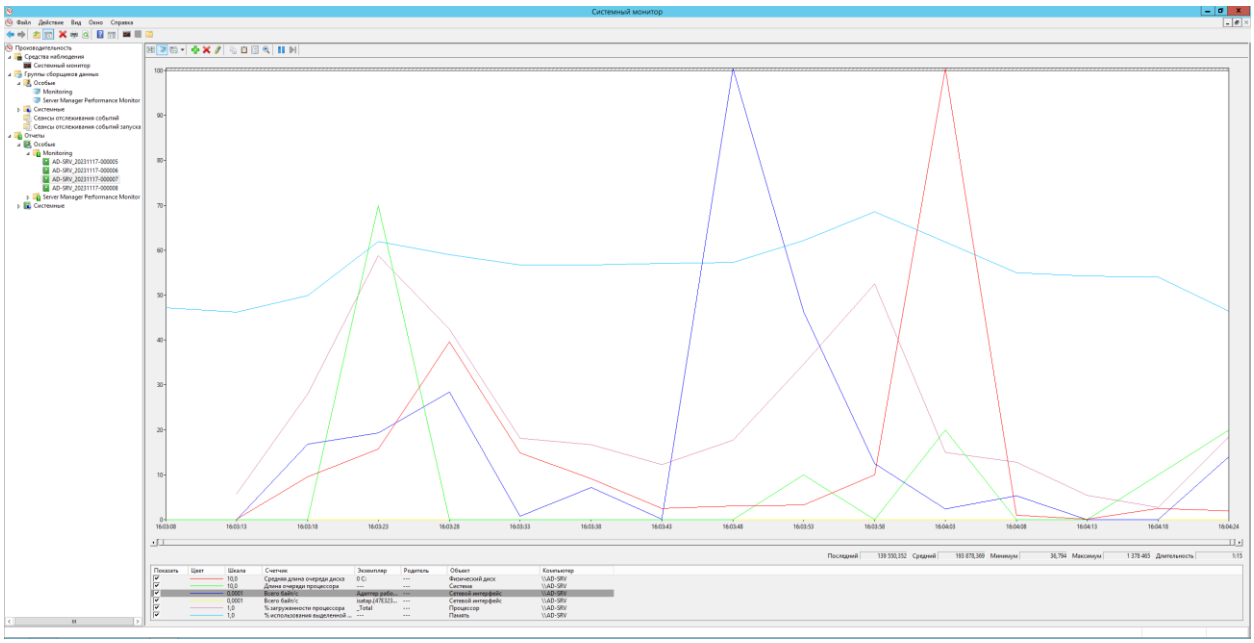
Часть 4. Сбор и анализ данных

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


Системный монитор
Файл Действие Вид Окно Справка
Производительность
Средства наблюдения
Системный монитор
Группы сборщиков данных
Особые
Server Manager Performance Monitor
Системные
Сеансы отслеживания событий
Сеансы отслеживания событий запуска
Отчеты
Имя
Статус
Создать новую группу сборщиков данных.
Какие счетчики производительности следует записывать в журнал?
Системные счетчики:
\Память\% использования выделенной пам...
\Процессор(_Total)\% загруженности процес...
\Сетевой интерфейс(*)\Всего байт/с
\Система\Длина очереди процессора
\Физический диск(0 C:)\Средняя длина очер...
Добавить...
Удалить
Интервал выборки:
5
Единицы:
сек.
Далее
Готово
Отмена

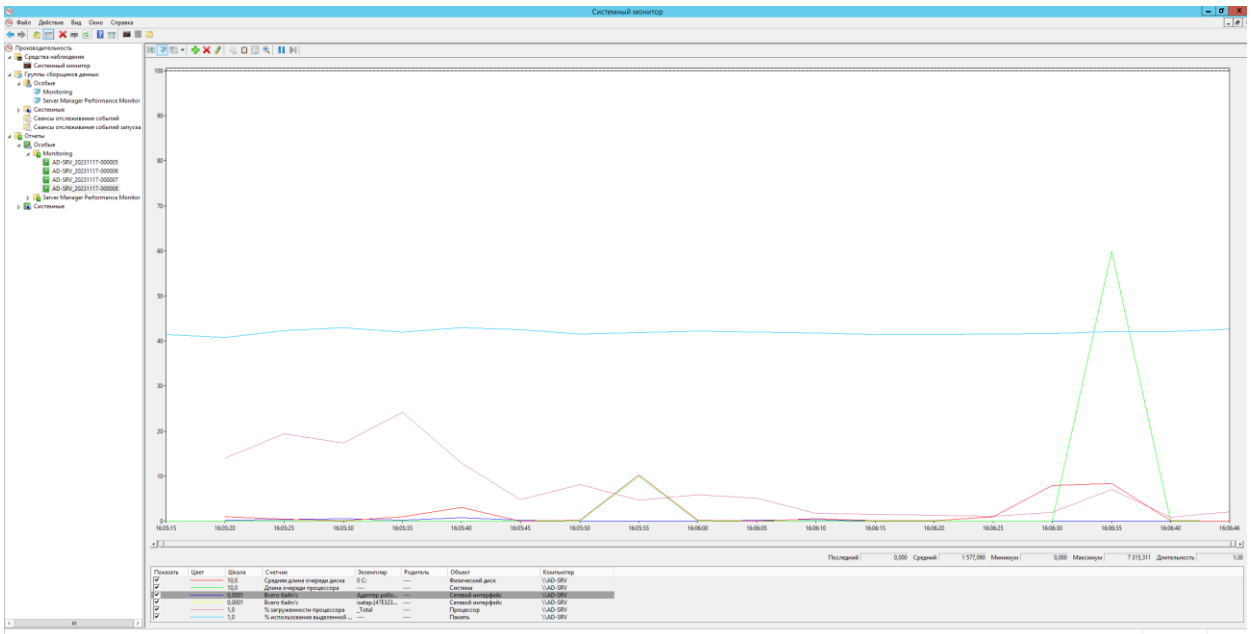

Системный монитор
Файл Действие Вид Окно Справка
Производительность
Средства наблюдения
Системный монитор
Группы сборщиков данных
Особые
Monitoring
Server Manager Performa
Системные
Отчеты
Имя
Тип
Вывод
DataCollector01
Счетчик производите...
Создать новый сборщик данных
Какие службы трассировки событий должны быть включены?
Поставщики:
Microsoft-Windows-Kernel-Process
Microsoft-Windows-Kernel-Disk
Microsoft-Windows-Kernel-Memory
Добавить...
Удалить
Свойства:
Свойство
Значение
Ключевые слов... 0x0
Ключевые слов... 0x0
Уровень 0x00
Свойства 0x00000000
Фильтр Отключен
Изменить...
Далее
Готово
Отмена

opera + explorer



Для браузеров характерно использование сети, оперативной памяти, процессора.

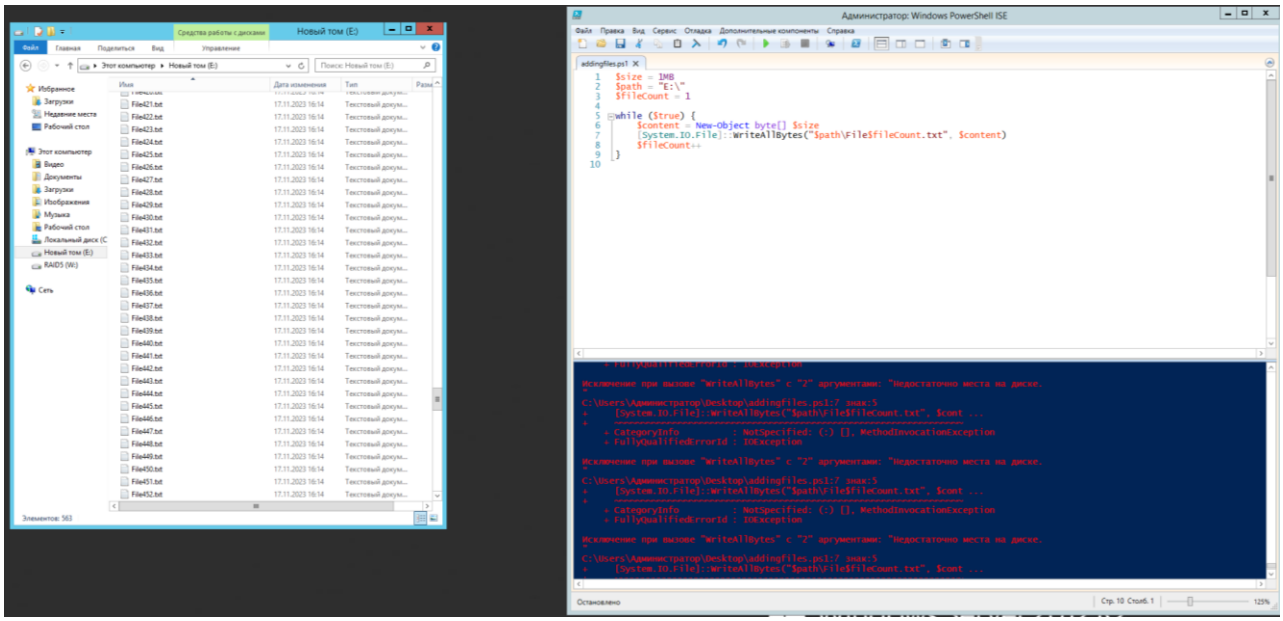
vs code + notepad

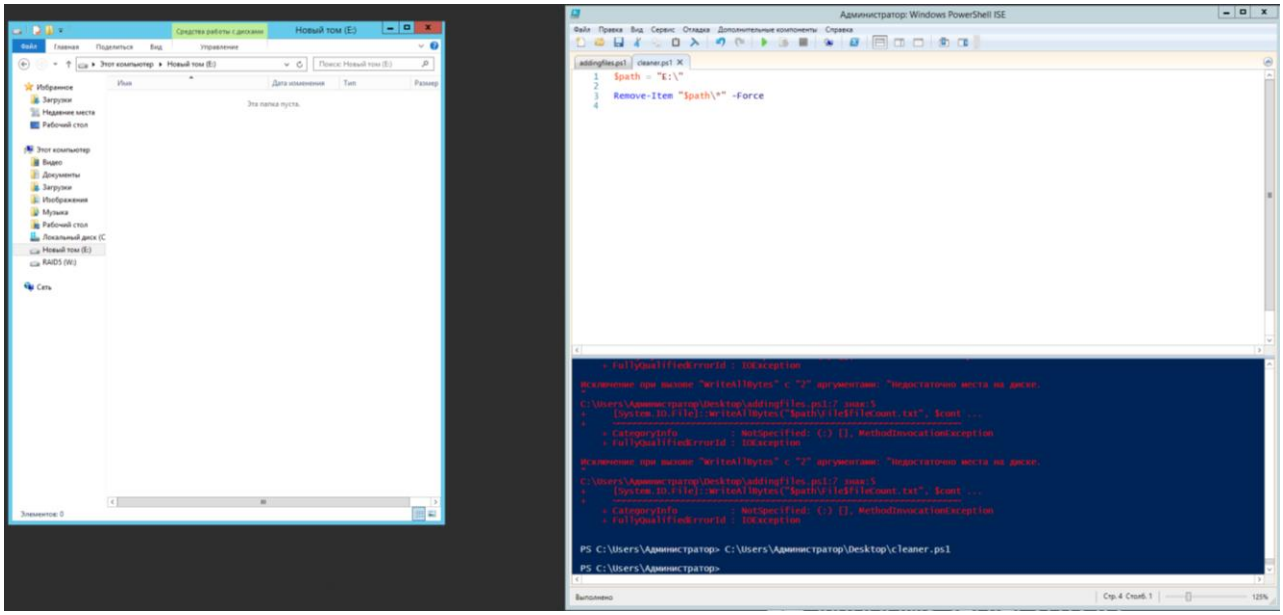


Для текстовых редакторов характерно использование оперативной памяти.

Часть 5. Автоматизация реакции системы на ее состояние

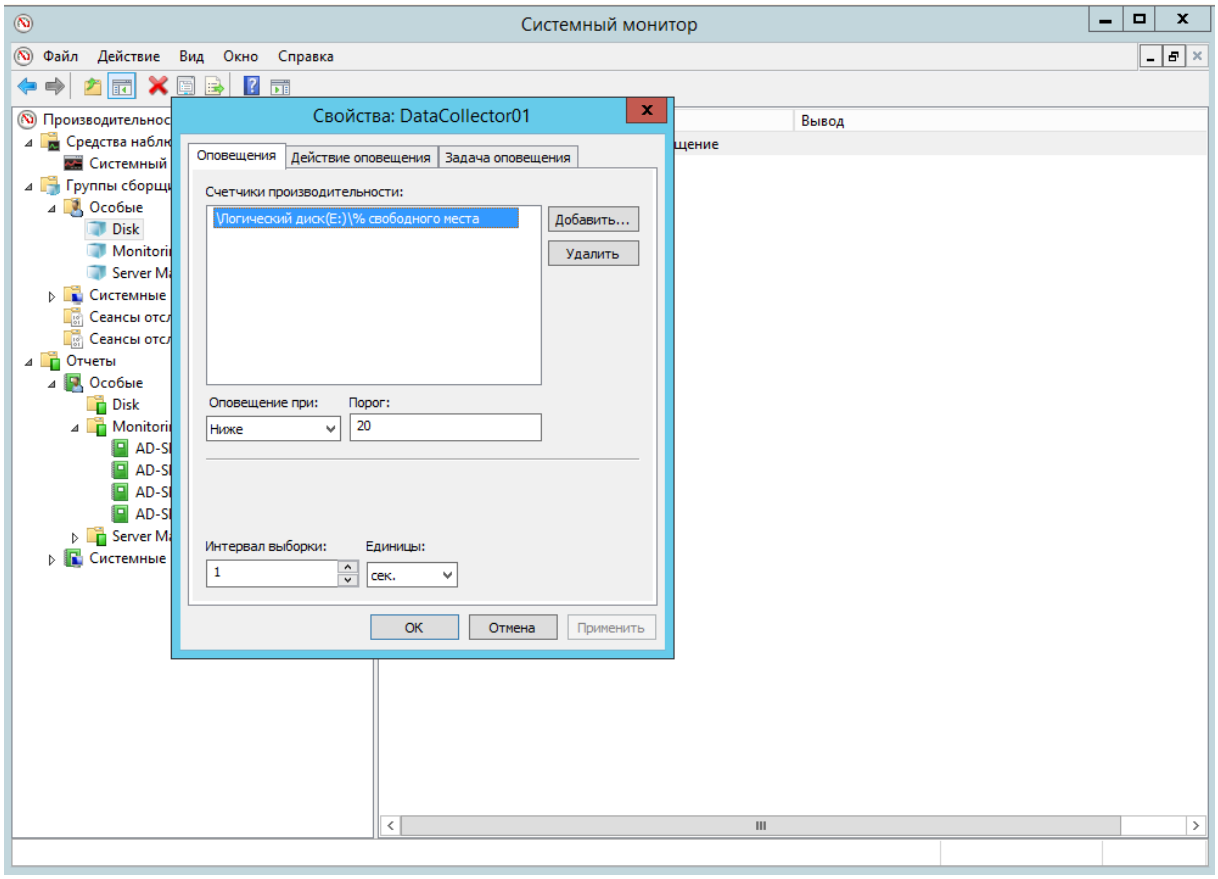
1) Создайте скрипит, который постепенно заполняет новый логический диск файлами размером до 1 Мб.
2) Создайте скрипит, очищающий новый диск.

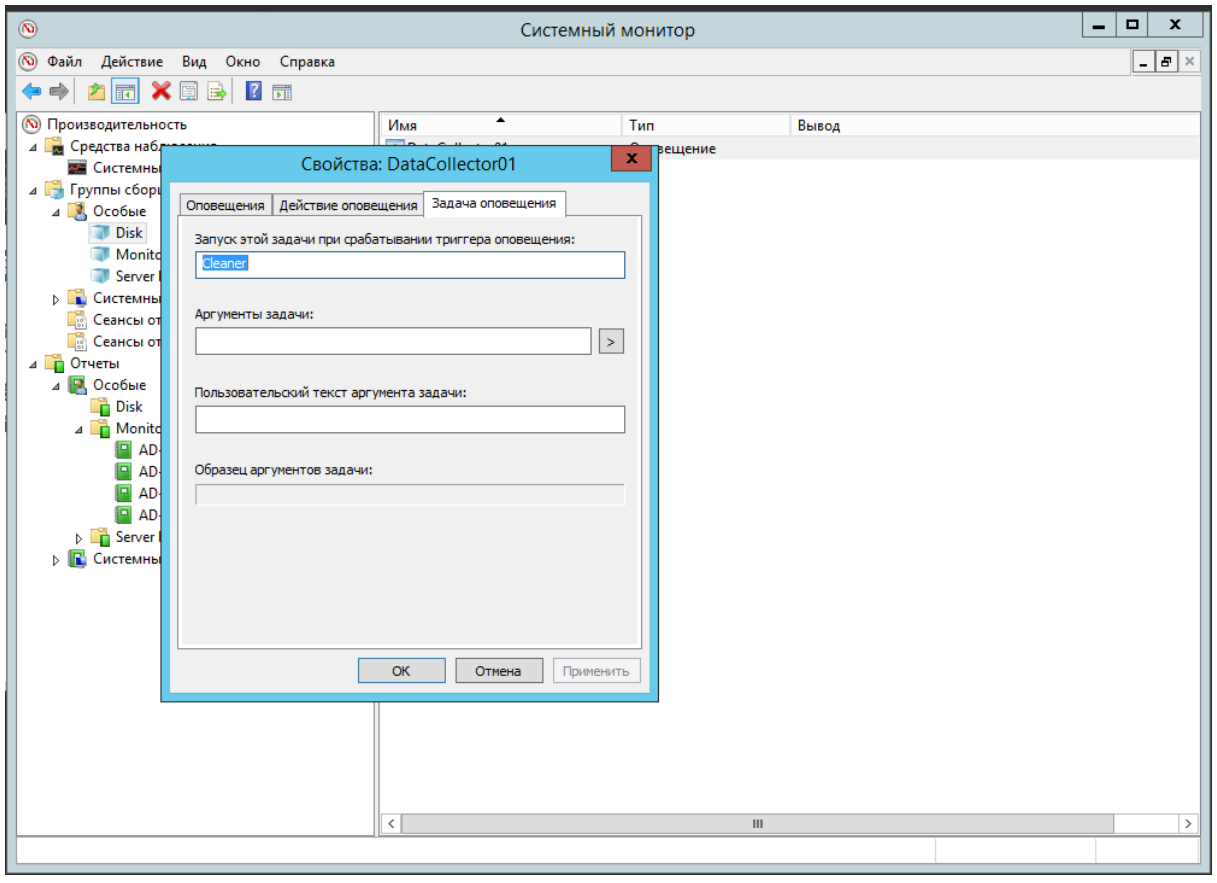




3) В Performance Monitor создайте новую Группу Сборщиков Данных с Оповещением счетчика производительности, который, срабатывает в случае, если осталось менее 20% свободного места на новом разделе и выводящее предупреждение в журнал событий и запускающее скрипт из п.3.

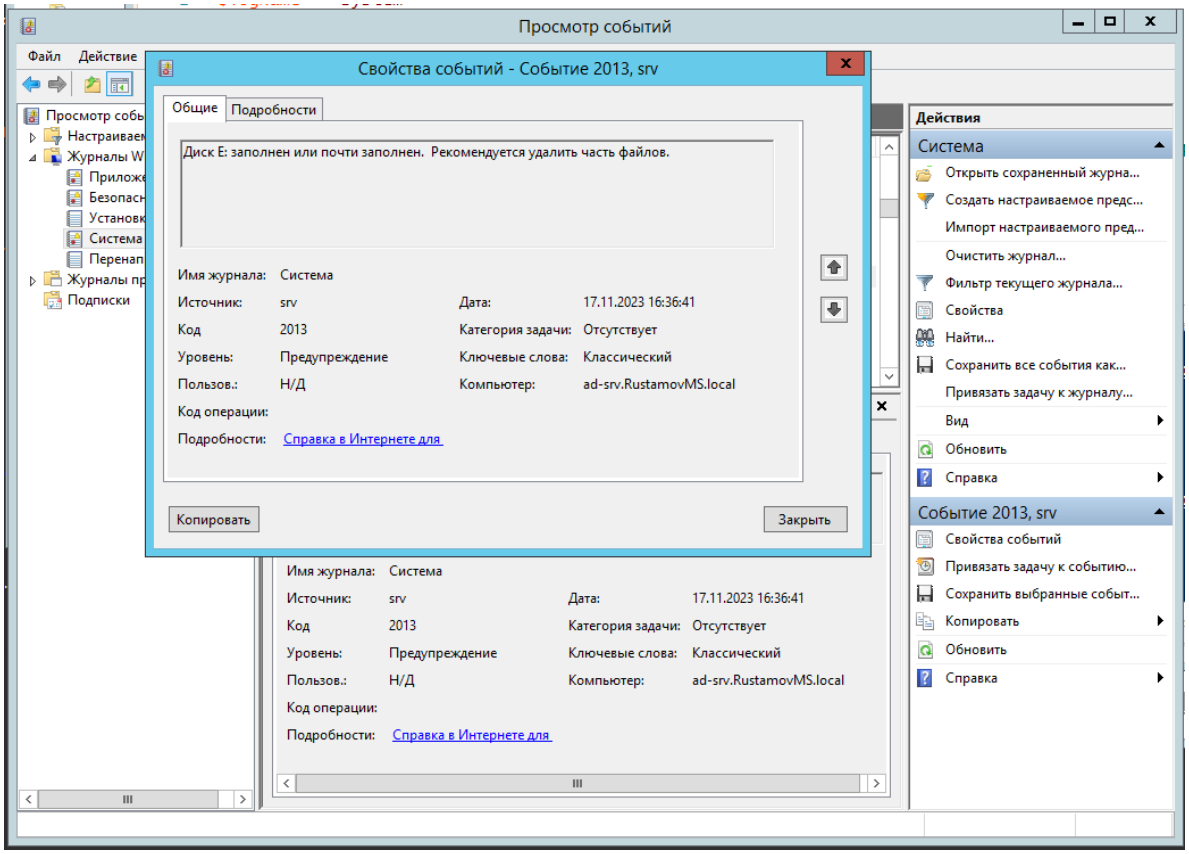
   Разработчики Performance Monitor предполагают, что нужно в Планировщике заданий создать задание, выполняющее скрипт из п. 3 и указать имя этого задания в настройках Сборщика данных отслеживания событий.


Системный монитор
Файл Действие Вид Окно Справка
Свойства: DataCollector01
Оповещения
Действие оповещения
Задача оповещения
Счетчики производительности:
\Логический диск(E:)\% свободного места
Добавить...
Удалить
Оповещение при:
Порог:
Ниже
20
Интервал выборки:
Единицы:
1
сек.
OK
Отмена
Применить
Производительность
Средства наблюдения
Системный монитор
Группы сборщиков данных
Особые
Disk
Monitoring
Server Manager
Системные
Сеансы отслеживания
Отчеты
Имя
Тип
Вывод


Системный монитор
Файл Действие Вид Окно Справка
Свойства: DataCollector01
Оповещения
Действие оповещения
Задача оповещения
Запуск этой задачи при срабатывании триггера оповещения:
Cleaner
Аргументы задачи:
Пользовательский текст аргумента задачи:
Образец аргументов задачи:
OK
Отмена
Применить
Производительность
Имя
Тип
Вывод

```powershell
$action = New-ScheduledTaskAction -Execute 'powershell.exe' -Argument 'C:\Users\Администратор\Desktop\cleaner.ps1'
$trigger = New-ScheduledTaskTrigger -AtStartup

Register-ScheduledTask -Action $action -Trigger $trigger -TaskName 'Cleaner'

```

```
PS C:\Users\Администратор> C:\Users\Администратор\Desktop\Безымянный6.ps1

TaskPath                                 TaskName                 State
--------                                 --------                 -----
\                                        Cleaner                  Ready
```



При запуске скрипта диск все время отчищается благодаря задаче Cleaner, и все время на диске свободно будет 35мб, что примерно 80%.

Ответы на вопросы:

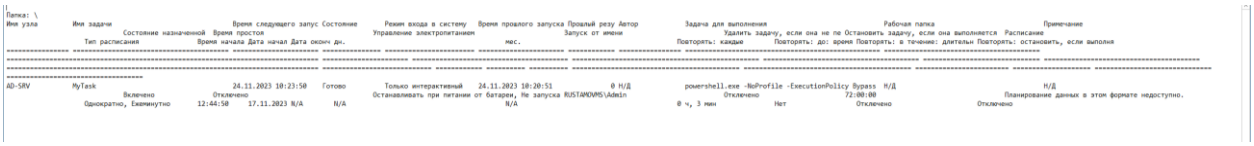
1) В чем назначение каждого из разделов журнала событий?
    - Приложение: Здесь записываются события, связанные с работой приложений.
    - Безопасность: В этом разделе регистрируются события безопасности, такие как вход в систему или неудачные попытки входа.
    - Система: Фиксирует события, касающиеся работы операционной системы и системных компонентов.
2) Зачем нужен раздел Перенаправленные события?
    - Этот раздел содержит события, перенаправленные из других журналов на этот. Используется для централизованного анализа событий с разных источников.
3) Где находится журналы событий Windows в виде файлов?

   Файлы журналов событий хранятся в папке %SystemRoot%\System32\Winevt\Logs.
4) Как с помощью графической оснастки журнала событий установить по известному VID коду, когда было подключено и настроено устройство?

   В Windows Device Manager выбрать устройство, затем свойства устройства, перейти на вкладку "Драйвер" и найти VID (Vendor ID) код в разделе "Идентификатор оборудования". Затем в журнале событий найти события с этим VID кодом.
5) Почему были выбраны конкретные счетчики в Части 4 п.1? Обоснуйте выбор.

   Память, дисковая подсистема, процессор и сеть являются ключевыми компонентами системы, влияющими на ее производительность.
6) Как получить на консоль подробные параметры запланированного задания с помощью утилиты schtasks.exe? Проиллюстрируйте ответ на примере задания из части 5.

schtasks /query /v /tn "Имя_задания"



Вывод: в результате работы были изучены встроенные средства технического мониторинга, назначением и принципами работы Prefomance Monitor. Получены навыки сбора и анализа данных, позволяющих оценивать производительность системы. Получены практические навыки поиска "узких мест" в производительности системы. Получены дополнительные навыки по управлению Windows Server, управлению процессами и журналами работы.