Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное образовательное учреждение высшего образования
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Отчет

по лабораторной работе №6

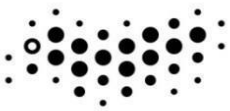
по дисциплине «**Администрирование Windows Server**»

Авторы: Юрпалов С. Н.

Кошкин М. С.

Факультет: ИТиП

Группа: М33051



УНИВЕРСИТЕТ ИТМО

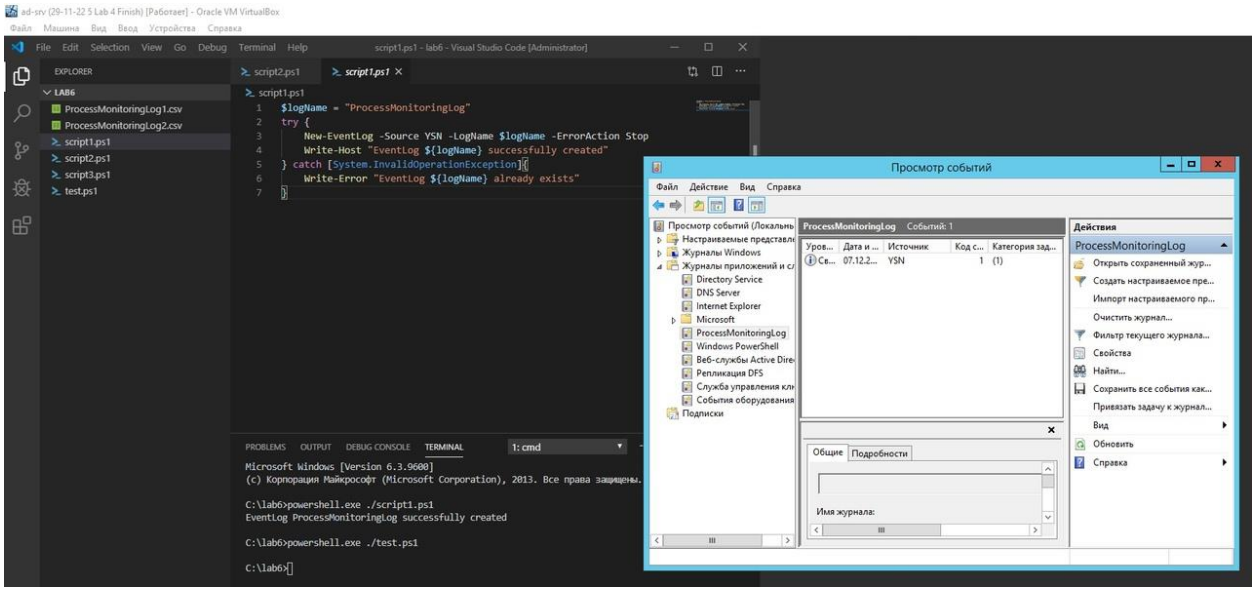
Санкт-Петербург 2022

Артефакты выполнения

1:

```powershell
$logName = "ProcessMonitoringLog"
try {
    New-EventLog -Source YSN -LogName $logName -ErrorAction Stop
    Write-Host "EventLog ${logName} successfully created"
} catch [System.InvalidOperationException]{
    Write-Error "EventLog ${logName} already exists"
}
```

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL

C:\lab6>powershell.exe ./script1.ps1
EventLog ProcessMonitoringLog successfully created

C:\lab6>
```



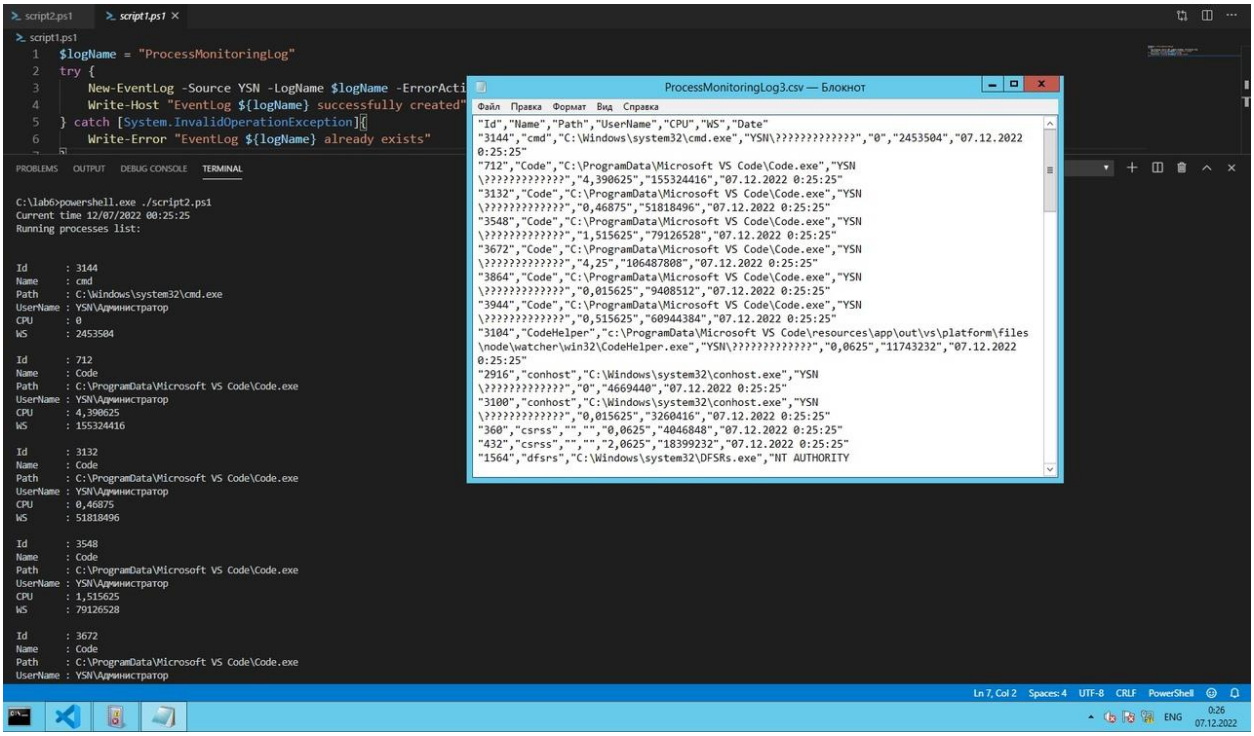
Remove-EventLog –LogName ProcessMonitoringLog

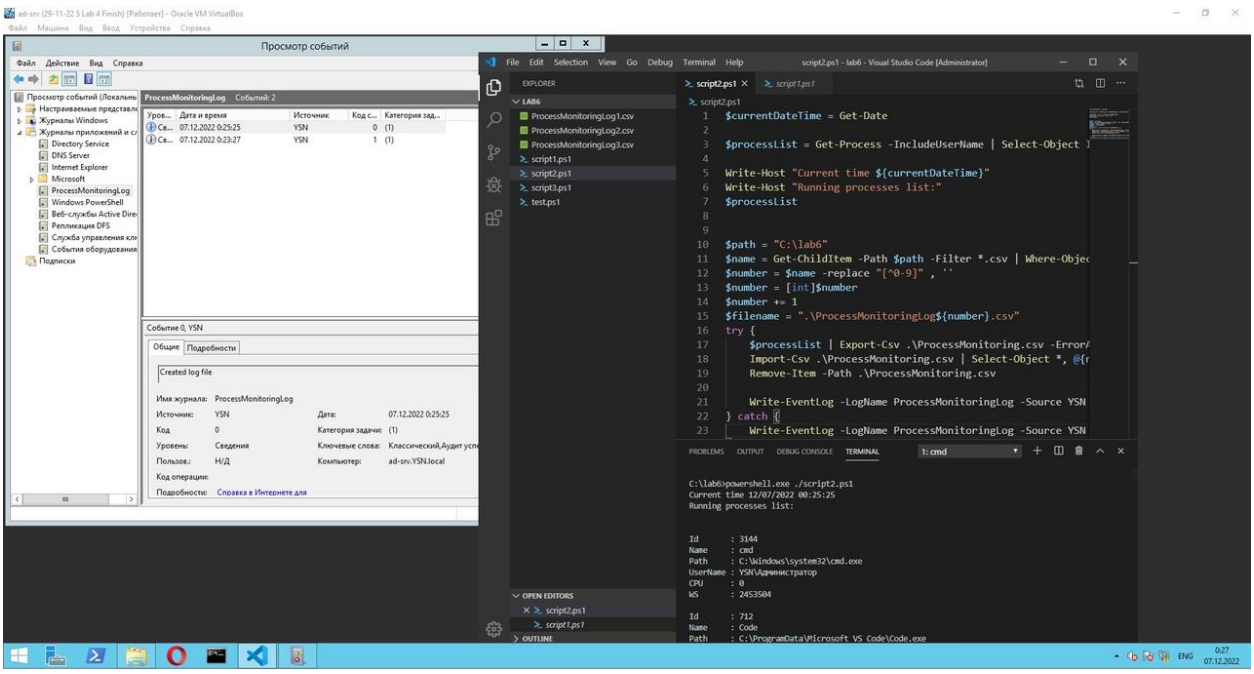
script2.ps1

```powershell
$currentDateTime = Get-Date

$processList = Get-Process -IncludeUserName | Select-Object ID, Name, Path, UserName, CPU, WS

Write-Host "Current time ${currentDateTime}"
Write-Host "Running processes list:"
$processList

$path = "C:\lab6"
try {
    $name = Get-ChildItem -Path $path -Filter *.csv | Where-Object {$_Name -match ${ProcessMonitoringLog[0-9]+}} | Select-Object Name -Last 1
    $number = $name -replace "[^0-9]" , ''
    $number = [int]$number
} catch {
    $number = 0
}

$number += 1
$filename = "C:\lab6\ProcessMonitoringLog${number}.csv"
try {
    $processList | Export-Csv .\ProcessMonitoring.csv -ErrorAction Stop
    Import-Csv .\ProcessMonitoring.csv | Select-Object *, @{n="Date";e={$currentDateTime}} | Export-Csv $filename -NoTypeInformation -ErrorAction Stop
    Remove-Item -Path .\ProcessMonitoring.csv

    Write-EventLog -LogName ProcessMonitoringLog -Source YSN -EventId 0 -EntryType SuccessAudit -Message "Created log file"
} catch {
    Write-EventLog -LogName ProcessMonitoringLog -Source YSN -EventId 1 -EntryType FailureAudit -Message "Failed to create log file"
}

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

```
C:\lab6>powershell.exe ./script2.ps1
Current time 12/07/2022 00:25:25
Running processes list:


Id       : 3144
Name     : cmd
Path     : C:\Windows\system32\cmd.exe
UserName : YSN\Администратор
CPU      : 0
WS       : 2453504

Id       : 712
Name     : Code
Path     : C:\ProgramData\Microsoft VS Code\Code.exe
UserName : YSN\Администратор
CPU      : 4,390625
WS       : 155324416

Id       : 3132
Name     : Code
Path     : C:\ProgramData\Microsoft VS Code\Code.exe
UserName : YSN\Администратор
CPU      : 0,46875
WS       : 51818496

Id       : 3548
Name     : Code
Path     : C:\ProgramData\Microsoft VS Code\Code.exe
UserName : YSN\Администратор
CPU      : 1,515625
WS       : 79126528

Id       : 3672
Name     : Code
Path     : C:\ProgramData\Microsoft VS Code\Code.exe
UserName : YSN\Администратор
```

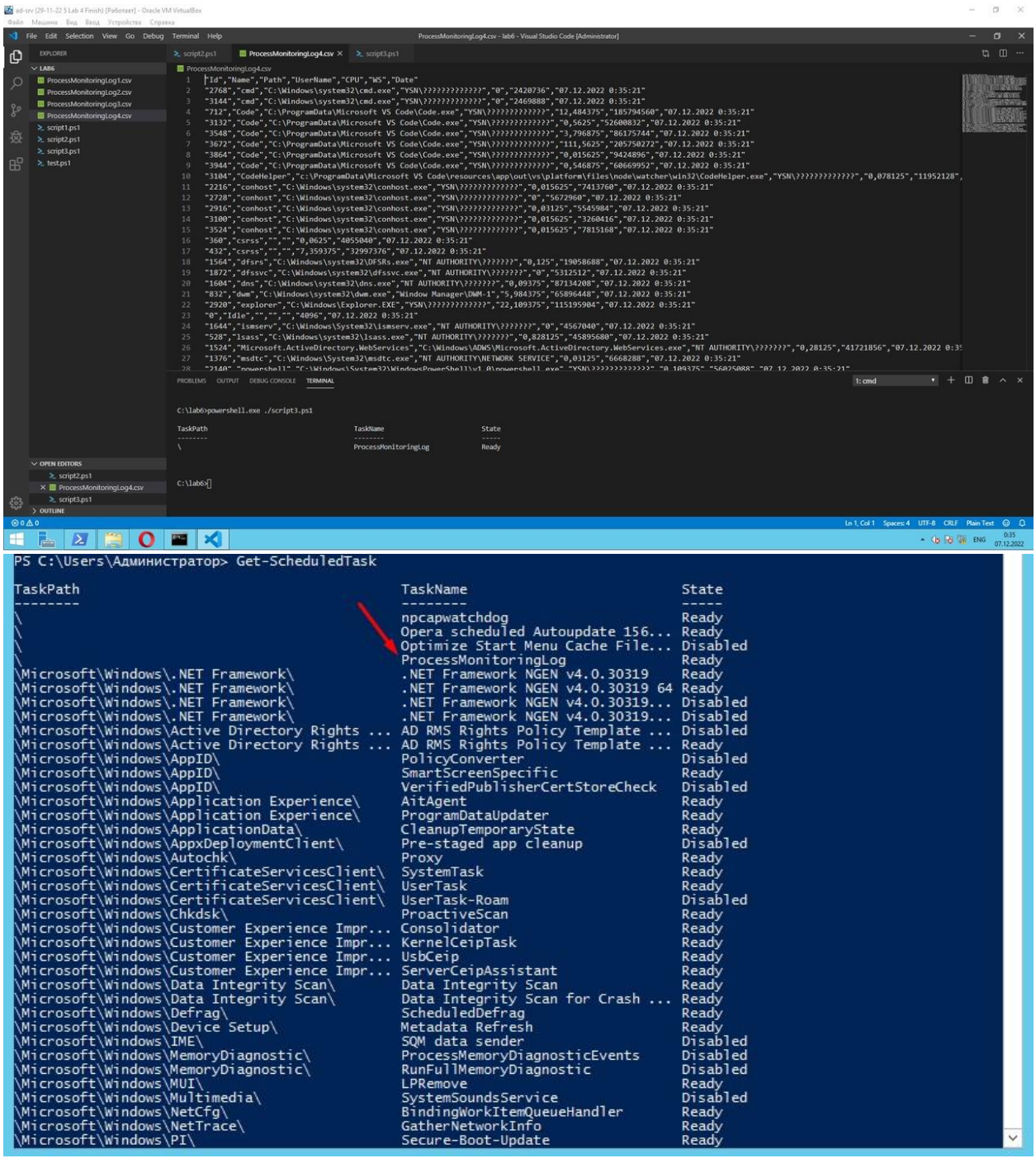




WS: размер рабочего множества процесса в килобайтах. Рабочий набор состоит из страниц памяти, на которые недавно ссылался процесс.

2:

```powershell
$taskName = "ProcessMonitoringLog"
$action = New-ScheduledTaskAction -Execute "powershell.exe" -Argument "-File C:\lab6\script2.ps1"

$repetitionInterval = New-TimeSpan -Minutes 3
$repetitionDuration = [timeSpan]::MaxValue
$taskTrigger = New-ScheduledTaskTrigger -Once -At (Get-Date).AddSeconds(5) -RepetitionInterval $repetitionInterval -RepetitionDuration $repetitionDuration


try{
    Register-ScheduledTask -TaskName $taskName -Action $action -Trigger $taskTrigger
} catch {
    Write-Error "Scheduled task is already exist"
}
```

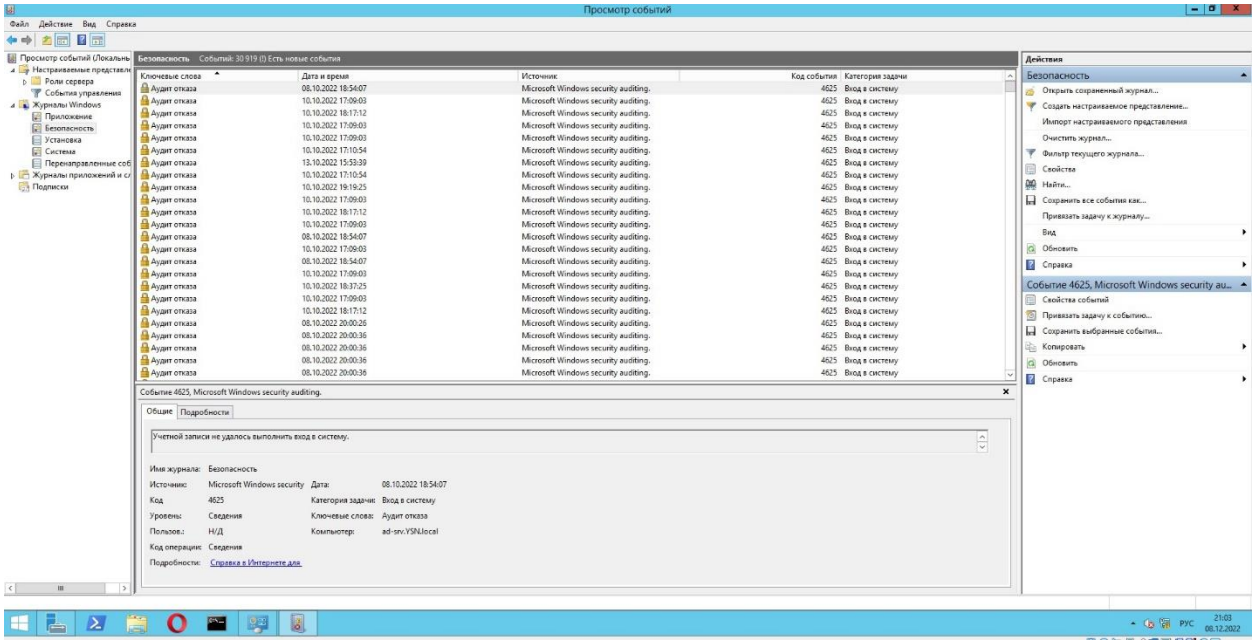


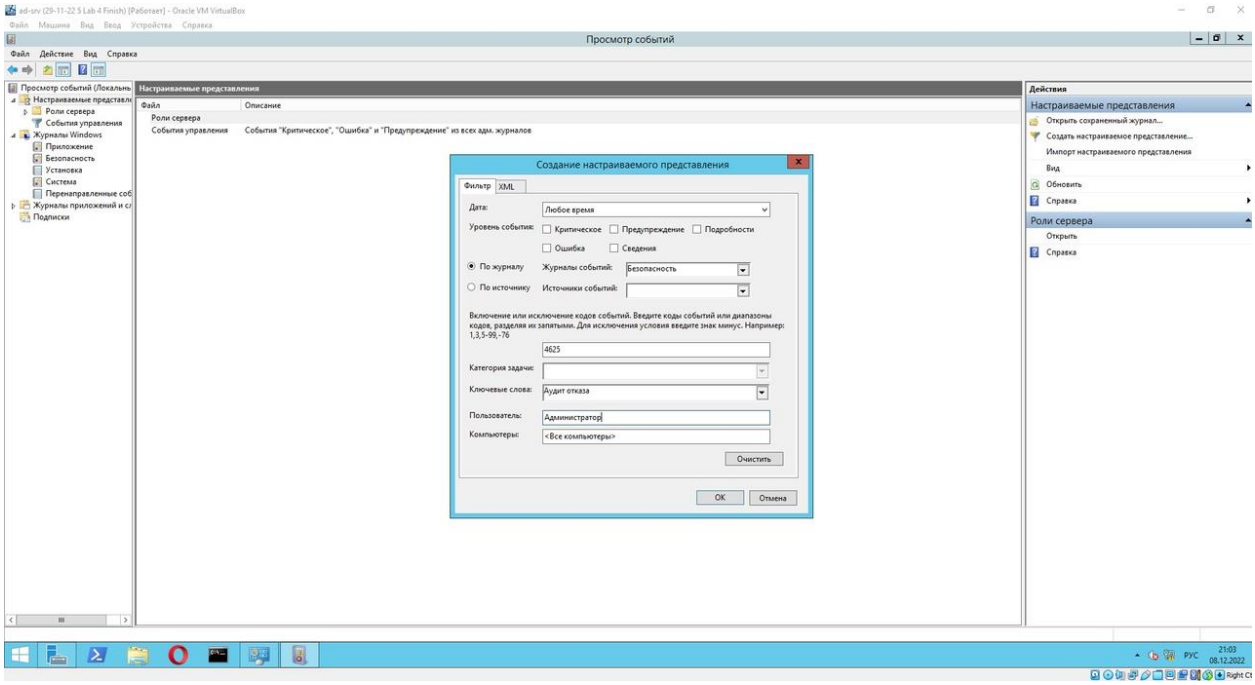

```
PS C:\Users\Администратор> Get-ScheduledTask

TaskPath                                 TaskName                          State
--------                                 --------                          -----
\                                        npcapwatchdog                     Ready
\                                        Opera scheduled Autoupdate 156... Ready
\                                        Optimize Start Menu Cache File... Disabled
\                                        ProcessMonitoringLog              Ready
\Microsoft\Windows\.NET Framework\       .NET Framework NGEN v4.0.30319    Ready
\Microsoft\Windows\.NET Framework\       .NET Framework NGEN v4.0.30319 64 Ready
\Microsoft\Windows\.NET Framework\       .NET Framework NGEN v4.0.30319... Disabled
\Microsoft\Windows\.NET Framework\       .NET Framework NGEN v4.0.30319... Disabled
\Microsoft\Windows\Active Directory Rights ... AD RMS Rights Policy Template ... Disabled
\Microsoft\Windows\Active Directory Rights ... AD RMS Rights Policy Template ... Ready
\Microsoft\Windows\AppID\                PolicyConverter                   Disabled
\Microsoft\Windows\AppID\                SmartScreenSpecific               Ready
\Microsoft\Windows\AppID\                VerifiedPublisherCertStoreCheck   Disabled
\Microsoft\Windows\Application Experience\ AitAgent                        Ready
\Microsoft\Windows\Application Experience\ ProgramDataUpdater              Ready
\Microsoft\Windows\ApplicationData\      CleanupTemporaryState             Ready
\Microsoft\Windows\AppxDeploymentClient\ Pre-staged app cleanup            Disabled
\Microsoft\Windows\Autochk\              Proxy                             Ready
\Microsoft\Windows\CertificateServicesClient\ SystemTask                   Ready
\Microsoft\Windows\CertificateServicesClient\ UserTask                     Ready
\Microsoft\Windows\CertificateServicesClient\ UserTask-Roam                Disabled
\Microsoft\Windows\Chkdsk\               ProactiveScan                     Ready
\Microsoft\Windows\Customer Experience Impr... Consolidator                Ready
\Microsoft\Windows\Customer Experience Impr... KernelCeipTask              Ready
\Microsoft\Windows\Customer Experience Impr... UsbCeip                     Ready
\Microsoft\Windows\Customer Experience Impr... ServerCeipAssistant         Ready
\Microsoft\Windows\Data Integrity Scan\  Data Integrity Scan               Ready
\Microsoft\Windows\Data Integrity Scan\  Data Integrity Scan for Crash ... Ready
\Microsoft\Windows\Defrag\               ScheduledDefrag                   Ready
\Microsoft\Windows\Device Setup\         Metadata Refresh                  Ready
\Microsoft\Windows\IME\                  SQM data sender                   Disabled
\Microsoft\Windows\MemoryDiagnostic\     ProcessMemoryDiagnosticEvents     Disabled
\Microsoft\Windows\MemoryDiagnostic\     RunFullMemoryDiagnostic           Disabled
\Microsoft\Windows\MUI\                  LPRemove                          Ready
\Microsoft\Windows\Multimedia\           SystemSoundsService               Disabled
\Microsoft\Windows\NetCfg\               BindingWorkItemQueueHandler       Ready
\Microsoft\Windows\NetTrace\             GatherNetworkInfo                 Ready
\Microsoft\Windows\PI\                   Secure-Boot-Update                Ready
```

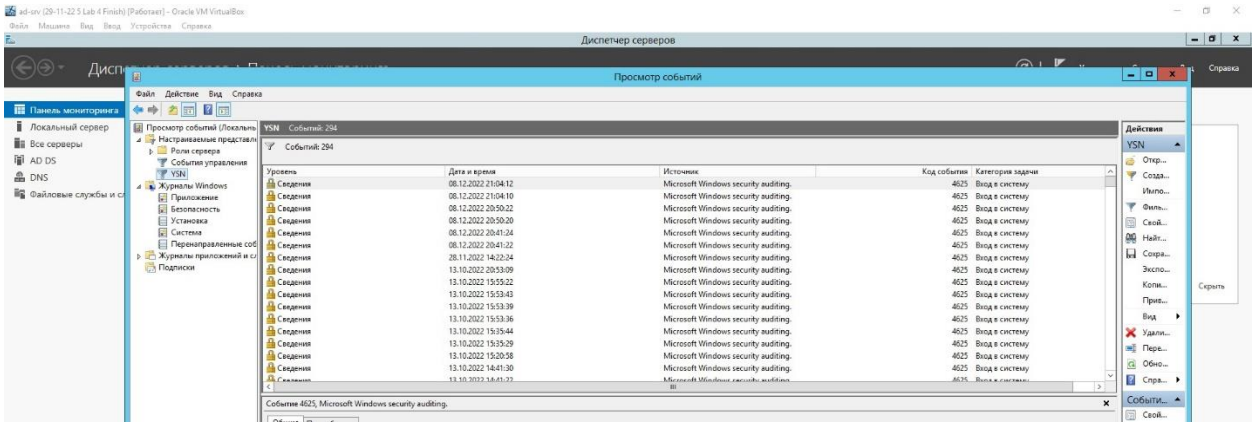
Unschedule-ScheduledTask –TaskName ProcessMonitoringLog

Стоит отметить, что запланированные таски по стандарту не будут выполняться, если питание идёт от батареи / ИБП. Если же задание было в том, чтобы запускать их и в этих случаях тоже, нам следовало бы добавить $taskSettings = New-ScheduledTaskSettingsSet -DontStopIfGoingOnBatteries –AllowStartIfOnBatteries, эту опцию, в свою очередь, к Register-ScheduledTask.

3:







4:

script4.ps1 test.ps1

```powershell
param (
    [string] $input_filename = $null
)

if (!$input_filename) {
    throw "You haven't entered a path!"
}

if (Test-Path -Path $input_filename -PathType Leaf) {
    throw "File with this name already exists"
}

Get-EventLog System | Where-Object {$_.EventID -contains "6009"} | Select -First 10 > $input_filename
Get-HotFix | Sort InstalledOn -Descending | Select-Object HotFixID, InstalledOn -First 5 >> $input_filename

$eventNames = Get-WinEvent -ListLog * | Where-Object {$_.LastWriteTime -GE (Get-Date).AddDays(-1)}

foreach ($name in $eventNames) {
    $name.LogName >> $input_filename
    Get-WinEvent -LogName $name.LogName | Group-Object -Property LevelDisplayName |
    Select-Object Name, Count | Sort-Object -Property Name | Select-Object -First 2 >> $input_filename
}
```

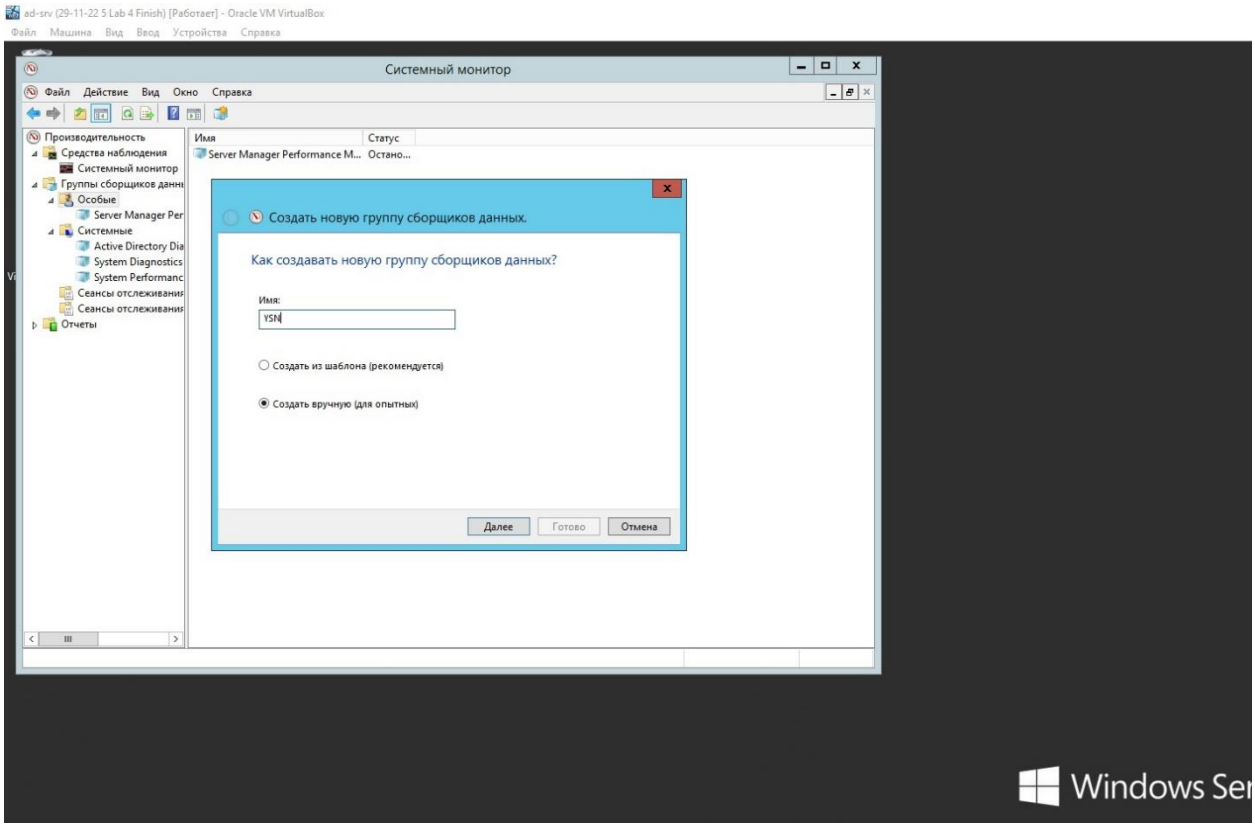
```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL

Microsoft Windows [Version 6.3.9600]
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.

C:\lab6>powershell.exe ./script4.ps1 c:\lab6\dump.txt

C:\lab6>
```

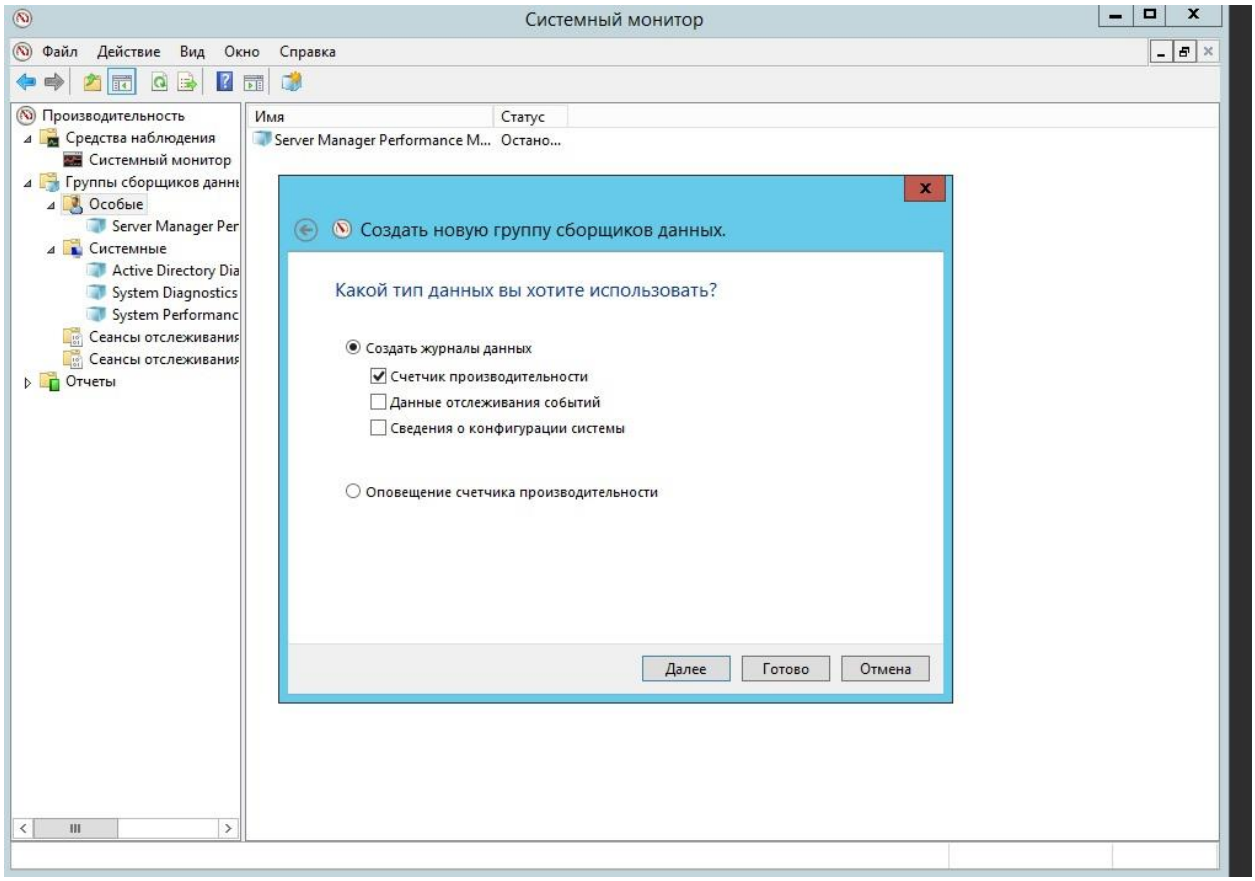
dump.txt — Блокнот

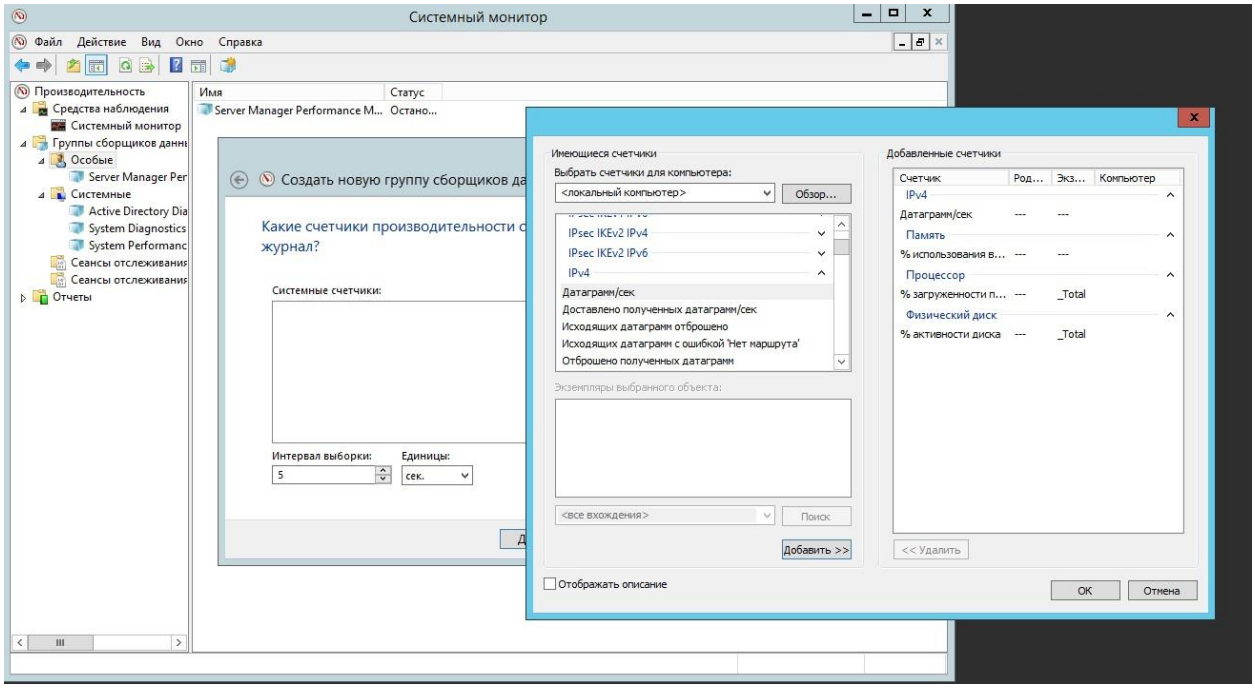
Файл Правка Формат Вид Справка

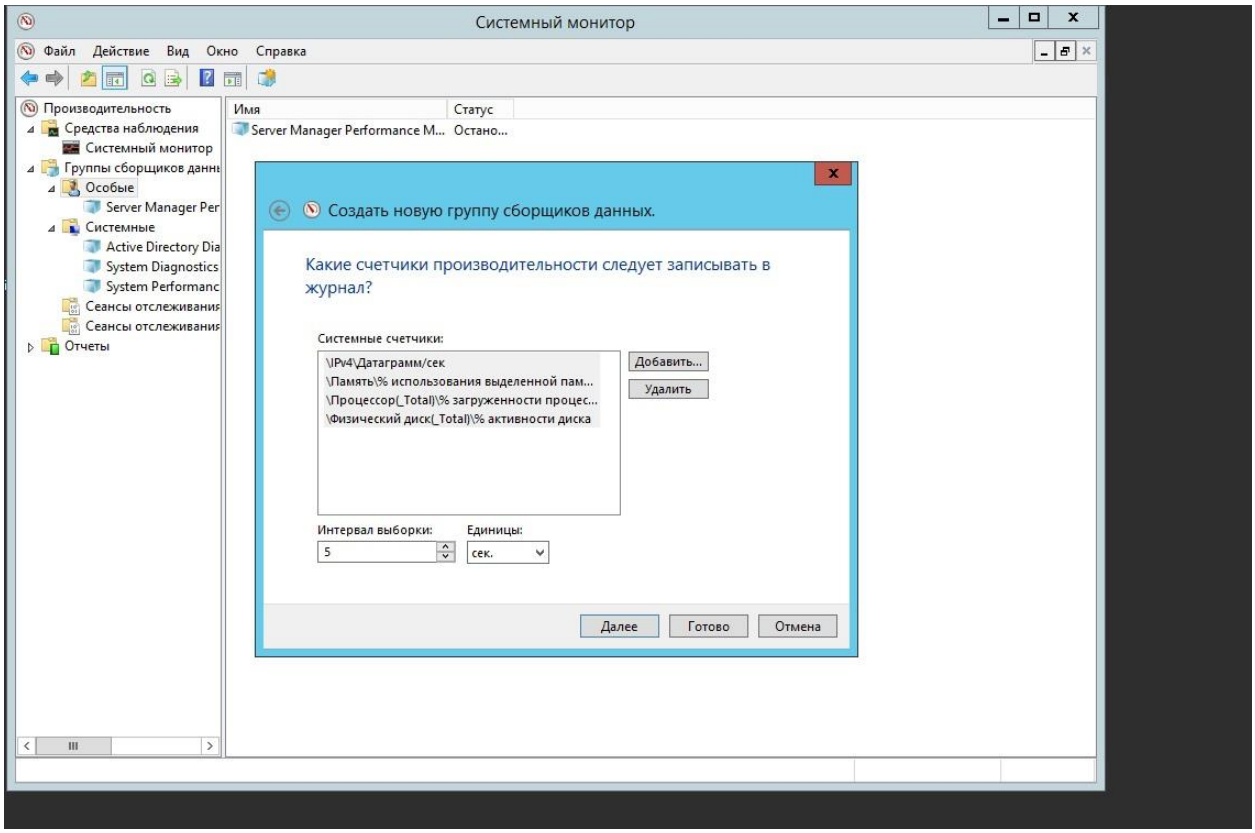
```
Index Time          EntryType   Source                 InstanceID Message
----- ----          ---------   ------                 ---------- -------
 6738 дек 08 21:00  Information EventLog              2147489657 Microsoft (R) Windows (R) 6.03. 9600  Multiprocessor Free.
 6585 дек 08 20:36  Information EventLog              2147489657 Microsoft (R) Windows (R) 6.03. 9600  Multiprocessor Free.
 6468 дек 07 12:15  Information EventLog              2147489657 Microsoft (R) Windows (R) 6.03. 9600  Multiprocessor Free.
 6330 дек 07 00:21  Information EventLog              2147489657 Microsoft (R) Windows (R) 6.03. 9600  Multiprocessor Free.
 6118 дек 06 22:30  Information EventLog              2147489657 Microsoft (R) Windows (R) 6.03. 9600  Multiprocessor Free.
 6007 ноя 29 15:44  Information EventLog              2147489657 Microsoft (R) Windows (R) 6.03. 9600  Multiprocessor Free.
 5908 ноя 29 15:40  Information EventLog              2147489657 Microsoft (R) Windows (R) 6.03. 9600  Multiprocessor Free.
 5765 ноя 29 14:11  Information EventLog              2147489657 Microsoft (R) Windows (R) 6.03. 9600  Multiprocessor Free.
 5609 ноя 28 18:00  Information EventLog              2147489657 Microsoft (R) Windows (R) 6.03. 9600  Multiprocessor Free.
 5475 ноя 28 17:12  Information EventLog              2147489657 Microsoft (R) Windows (R) 6.03. 9600  Multiprocessor Free.


HotFixID  InstalledOn
--------  -----------
KB2931358 21.11.2019 0:00:00
KB2931366 21.11.2019 0:00:00
KB2959977 21.11.2019 0:00:00
KB3173424 21.11.2019 0:00:00
KB2923528 21.11.2019 0:00:00

Active Directory Web Services

Name           Count
----           -----
Ошибка             1
Предупреждение     1

Application

Name      Count
----      -----
Сведения     10

DFS Replication

Name           Count
----           -----
Предупреждение     1
Сведения           9

Directory Service
```

5:

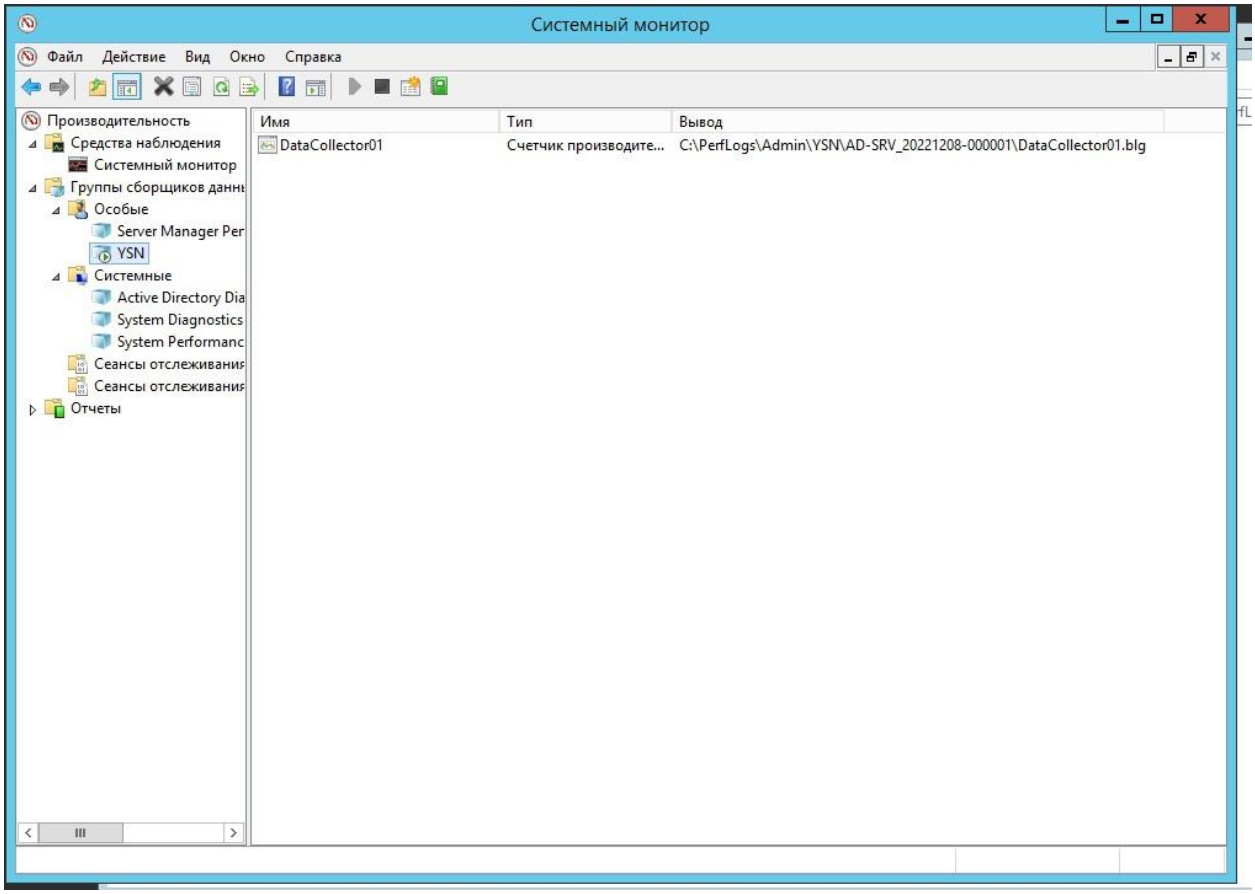

ad-srv (29-11-22 5 Lab 4 Finish) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Системный монитор
Файл Действие Вид Окно Справка
Производительность
Средства наблюдения
Системный монитор
Группы сборщиков данны
Особые
Server Manager Per
Системные
Active Directory Dia
System Diagnostics
System Performanc
Сеансы отслеживания
Сеансы отслеживания
Отчеты
Имя
Статус
Server Manager Performance M...
Остано...
Создать новую группу сборщиков данных.
Как создавать новую группу сборщиков данных?
Имя:
YSN
Создать из шаблона (рекомендуется)
Создать вручную (для опытных)
Далее
Готово
Отмена
Windows Ser

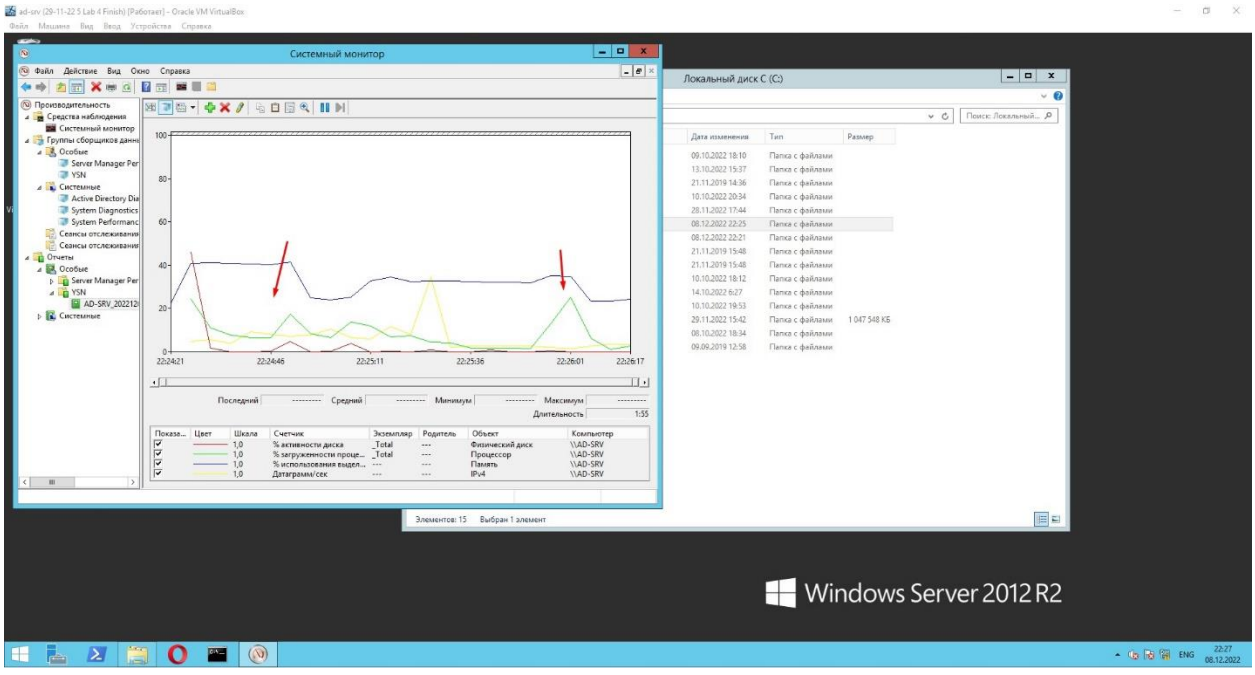

Системный монитор
Файл Действие Вид Окно Справка
Производительность
Средства наблюдения
Системный монитор
Группы сборщиков данны
Особые
Server Manager Per
Системные
Active Directory Dia
System Diagnostics
System Performanc
Сеансы отслеживания
Сеансы отслеживания
Отчеты
Имя
Статус
Server Manager Performance M...
Остано...
Создать новую группу сборщиков данных.
Какой тип данных вы хотите использовать?
Создать журналы данных
Счетчик производительности
Данные отслеживания событий
Сведения о конфигурации системы
Оповещение счетчика производительности
Далее
Готово
Отмена





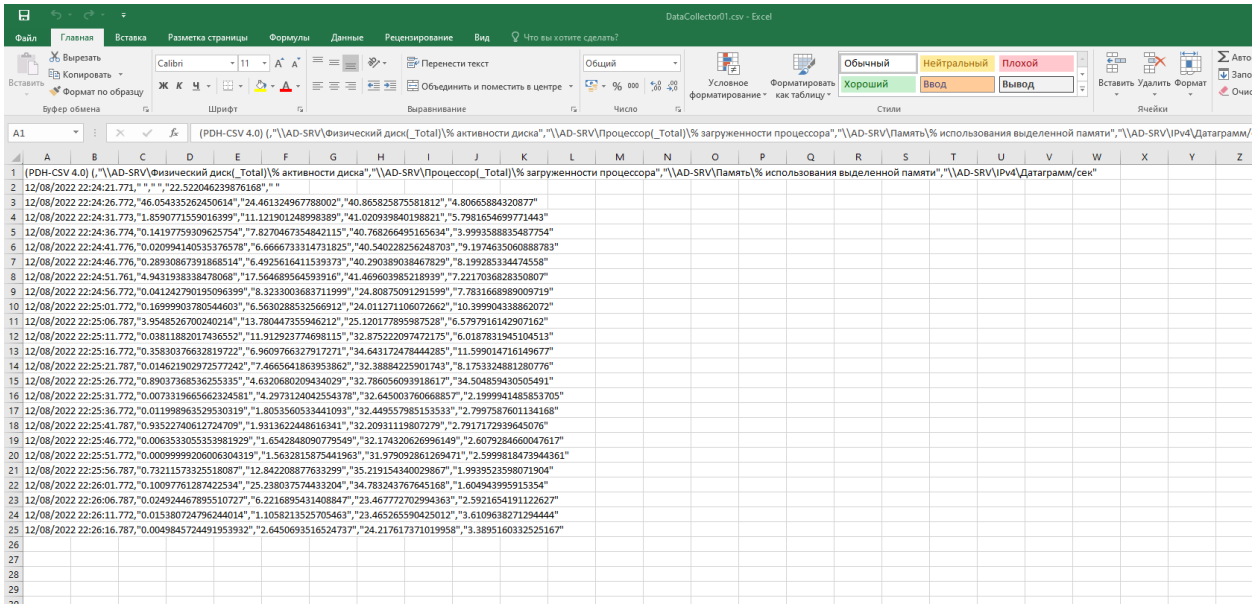
%SystemRoot%\PerfLogs\Admin\YSN



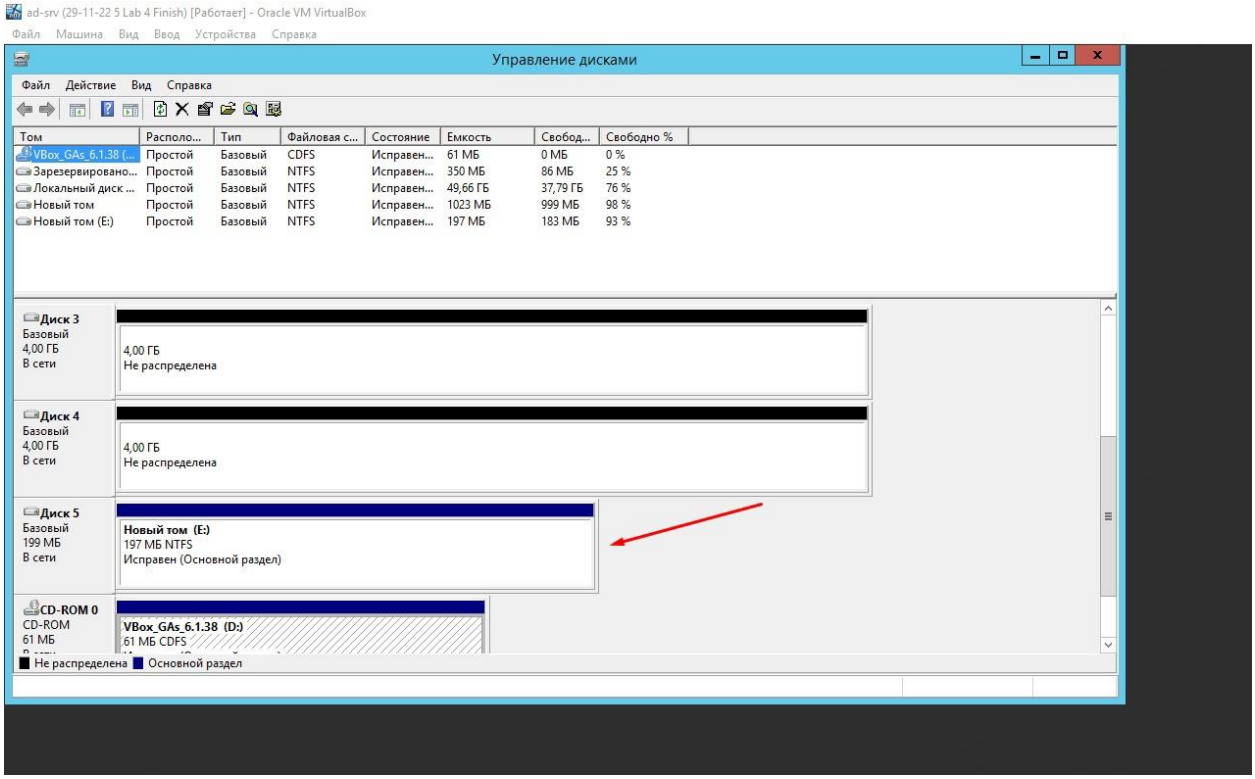


На месте 1 стрелки можно увидеть увеличение в использования ЦП и интернета – были включены 2 браузера Opera, Internet Explorer. На месте второй стрелки был выполнен script4.ps1 и открыть Visual Studio Code, можно увидеть спайк в использовании ЦП. Чтобы записать данные в таблицу воспользуемся cmd:

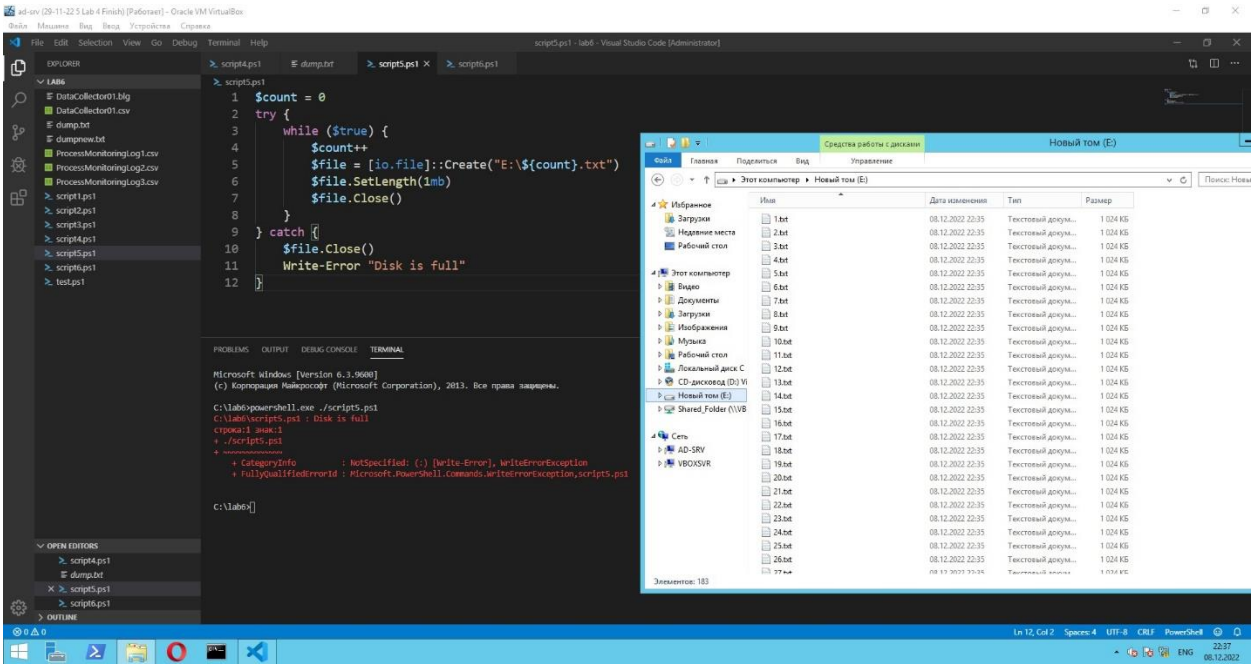
Relog DataCollector01.blg –f CSV -o DataCollector01.csv

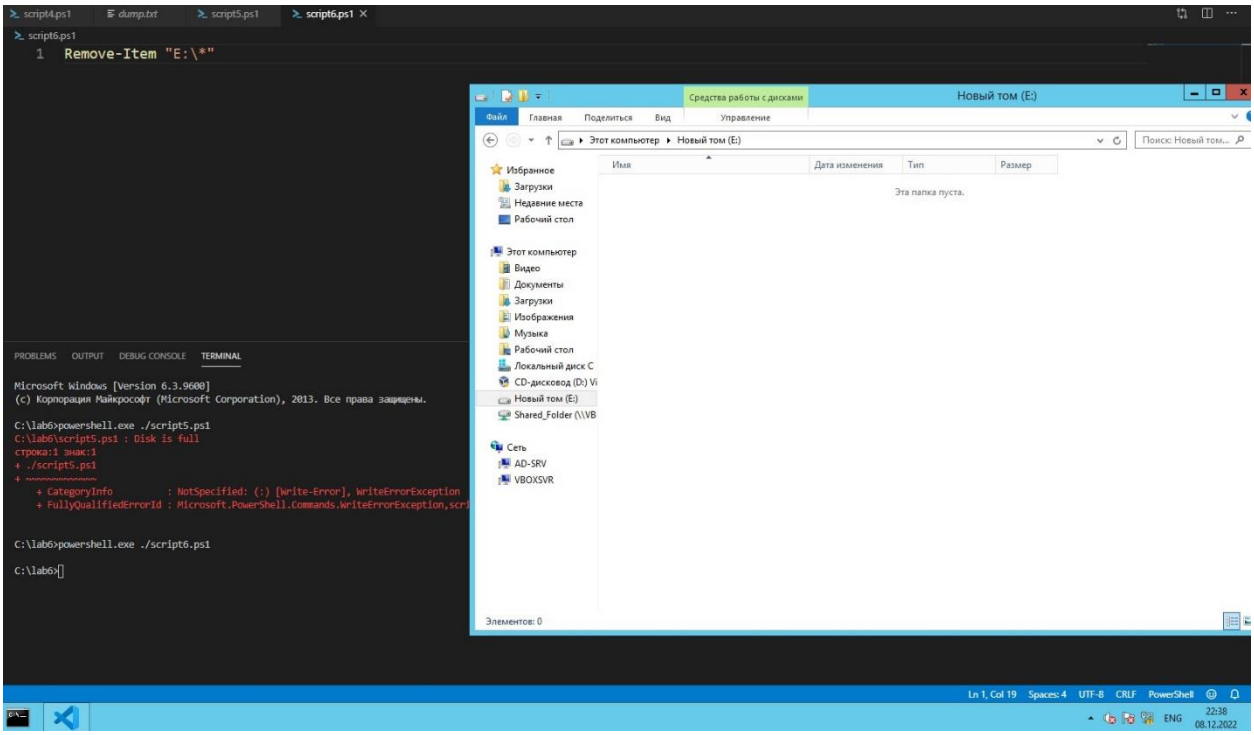

DataCollector01.csv - Excel
(PDH-CSV 4.0) (,"\\AD-SRV\Физический диск(_Total)\% активности диска","\\AD-SRV\Процессор(_Total)\% загруженности процессора","\\AD-SRV\Память\% использования выделенной памяти","\\AD-SRV\IPv4\Датаграмм/сек"
12/08/2022 22:24:21.771," "," ","22.522046239876168"," "
12/08/2022 22:24:26.772,"46.054335262450614","24.461324967788002","40.865825875581812","4.80665884320877"
12/08/2022 22:24:31.773,"1.8590771559016399","11.121901248998389","41.020939840198821","5.7981654699771443"
12/08/2022 22:24:36.774,"0.14197759309625754","7.827046735484211 5","40.768266495165634","3.9993588835487754"
12/08/2022 22:24:41.776,"0.020994140535376578","6.6666733314731825","40.540228256248703","9.1974635060888783"
12/08/2022 22:24:46.776,"0.28930867391868514","6.4925616411539373","40.290389038467829","8.1992853344745 58"
12/08/2022 22:24:51.761,"4.9431938338478068","17.564689564593916","41.469603985218939","7.2217036828350807"
12/08/2022 22:24:56.772,"0.041242790195096399","8.3233003683711999","24.80875091291599","7.7831668989009719"
12/08/2022 22:25:01.772,"0.16999903780544603","6.5630288532566912","24.011271106072662","10.399904338862072"
12/08/2022 22:25:06.787,"3.9548526700240214","13.780447355946212","25.120177895987528","6.5797916142907162"
12/08/2022 22:25:11.772,"0.038118820174365 52","11.912923774698115","32.875222097472175","6.0187831945104513"
12/08/2022 22:25:16.772,"0.35830376632819722","6.9609766327917271","34.643172478444285","11.599014716149677"
12/08/2022 22:25:21.787,"0.014621902972577242","7.4665641863953862","32.38884225901743","8.1753324881280776"
12/08/2022 22:25:26.772,"0.89037368536255335","4.6320680209434029","32.786056093918617","34.504859430505491"
12/08/2022 22:25:31.772,"0.0073319665662324581","4.2973124042554378","32.645003760668857","2.1999941485853705"
12/08/2022 22:25:36.772,"0.011998963529530319","1.8053560533441093","32.449557985153533","2.7997587601134168"
12/08/2022 22:25:41.787,"0.93522740612724709","1.9313622448616341","32.20931119807279","2.7917172939645076"
12/08/2022 22:25:46.772,"0.006353305535398 1929","1.6542848090779549","32.174320626996149","2.6079284660047617"
12/08/2022 22:25:51.772,"0.000999992060063043 19","1.5632815875441963","31.979092861269471","2.5999818473944361"
12/08/2022 22:25:56.787,"0.73211573325518087","12.842208877633299","35.219154340029867","1.9939523598071904"
12/08/2022 22:26:01.772,"0.10097761287422534","25.238037574433204","34.783243767645168","1.6049439959153 54"
12/08/2022 22:26:06.787,"0.024924467895510727","6.2216895431408847","23.467772702994363","2.5921654191122627"
12/08/2022 22:26:11.772,"0.015380724796244014","1.1058213525705463","23.465265590425012","3.6109638271294444"
12/08/2022 22:26:16.787,"0.004984572449195393 2","2.6450693516524737","24.217617371019958","3.3895160332525167"

6:


ad-srv (29-11-22 5 Lab 4 Finish) [Работает] - Oracle VM VirtualBox
Управление дисками
Том
Диск 3
Базовый
4,00 ГБ
В сети
4,00 ГБ
Не распределена
Диск 4
Диск 5
Новый том (E:)
197 МБ NTFS
Исправен (Основной раздел)
CD-ROM 0
VBox_GAs_6.1.38 (D:)
Не распределена
Основной раздел


script5.ps1
$count = 0
try {
while ($true) {
$count++
$file = [io.file]::Create("E:\${count}.txt")
$file.SetLength(1mb)
$file.Close()
}
} catch {
$file.Close()
Write-Error "Disk is full"
}





Ответы на вопросы

1. В журнале событий есть 3 основных раздела:
   Файл журнала приложений — для событий приложений и служб
   Файл журнала безопасности — для событий системы аудита
   Файл системного журнала — для событий драйверов устройств
   Стоит отметить, что при установке служб AS DS, DNS, модулей Powershell появляются соответствующие файлы журналов. Также, очевидно, там содержатся разделы, создаваемые пользователем – в них контент определяется создателем.

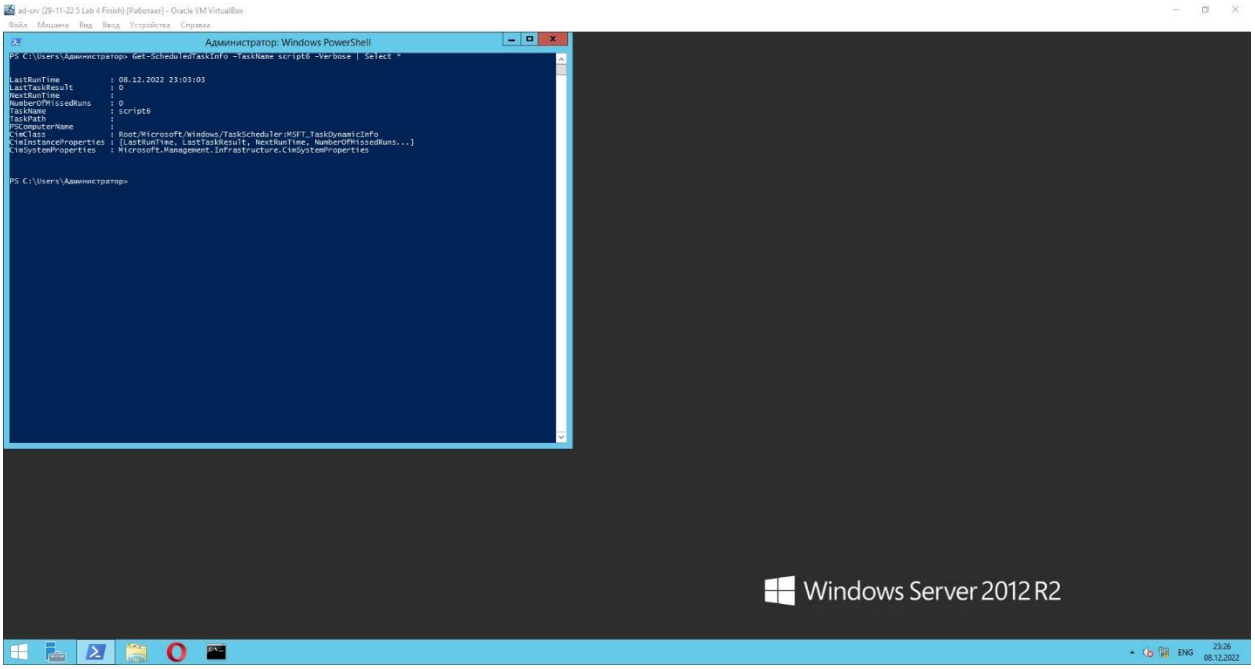
2. С функциональной точки зрения перенаправленное событие — это тип события, который может вызывать обработчики для нескольких прослушивателей в дереве элементов, а не только в источнике событий. Прослушиватель событий — это элемент, в котором подключен и вызывается обработчик событий. Источником события является элемент или объект, изначально вызвавшее событие. В разделе перенаправленные события хранятся логи о них. Данный вид событий используется, например, в ситуации, когда мы организовываем подписки на какие-либо события на сервере с клиентов.

3. По умолчанию файлы Просмотр событий используют расширение EVT и находятся в папке %SystemRoot%\System32\winevt\Logs. Имя файла журнала и сведения о расположении хранятся в реестре. Эти сведения можно изменить, чтобы изменить расположение файлов журнала по умолчанию.

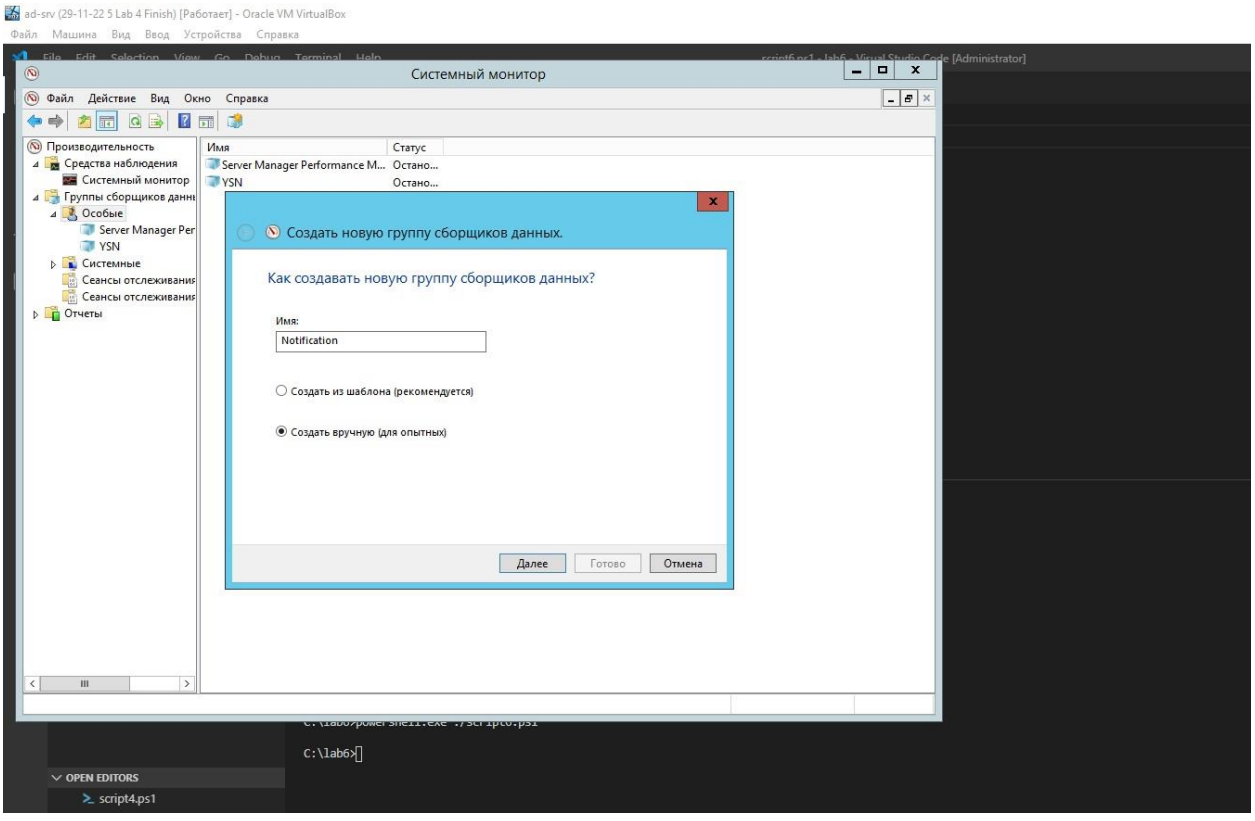
4. Чтобы узнать информацию о том, когда было подключено и настроено устройство, необходимо записи в логах с соответствующим id: “6416: Система распознала новое внешнее устройство.” – в каждой такой записи помимо прочей информации есть и дата, которая нам интересна, и Vendor ID, который нам известен. Про настройку аналогичную информацию можно найти в записях с id 6424S.

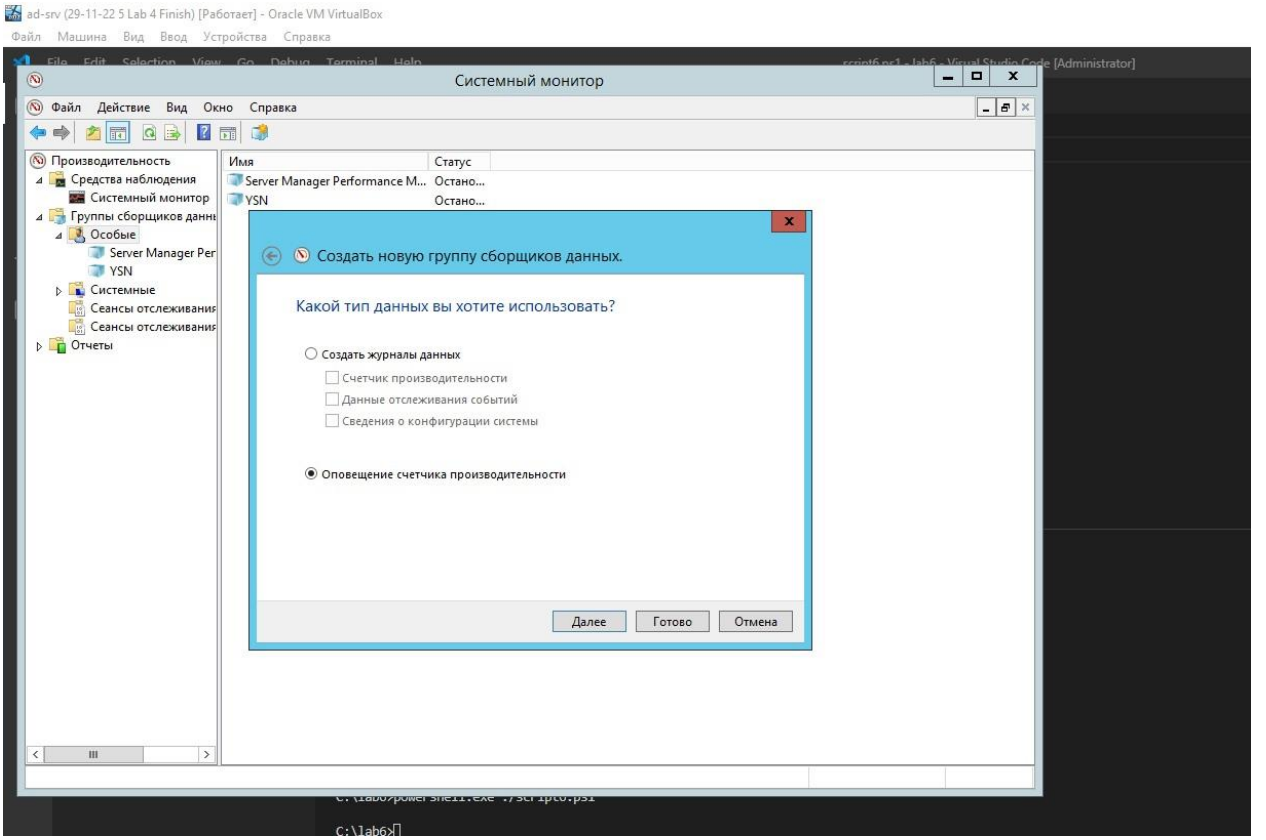
5. В задании 4 были выбраны параметры % активности диска, % загруженности процессова, % использования выделенной памяти, датаграмм/сек для контроля трафика. Эти параметры, на наш взгляд, являются довольно объективными для оценки нагрузки на систему для её соответствующих компонентов. Также они не подвержены сильным колебаниям и весьма репрезентативны на диаграммах подобно нашей, приведённой в артефакте 5. Также выбранный интервал замера в 5 секунд избавляет нас от проблемы случайных спайков, что только улучшает качество мониторинга.

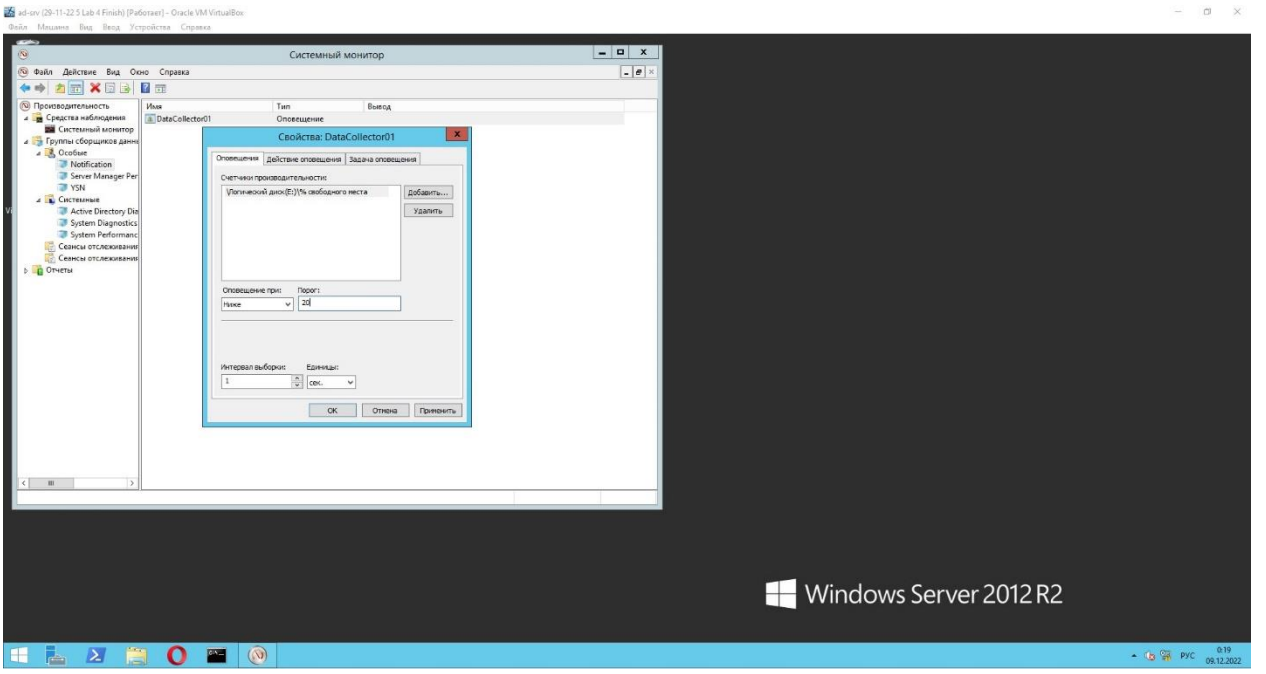
6. Get-ScheduledTaskInfo –TaskName script6 –Verbose | Select *

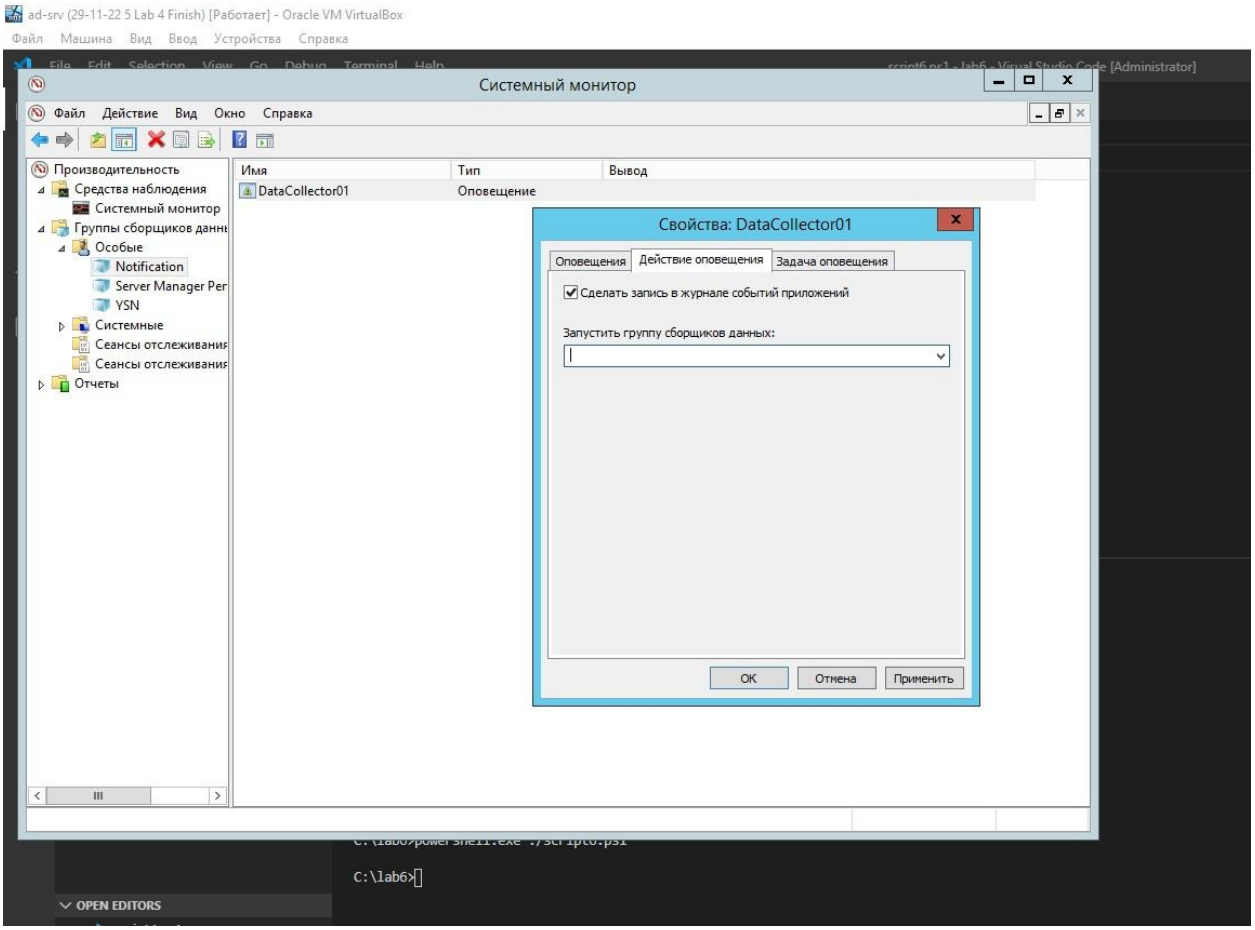


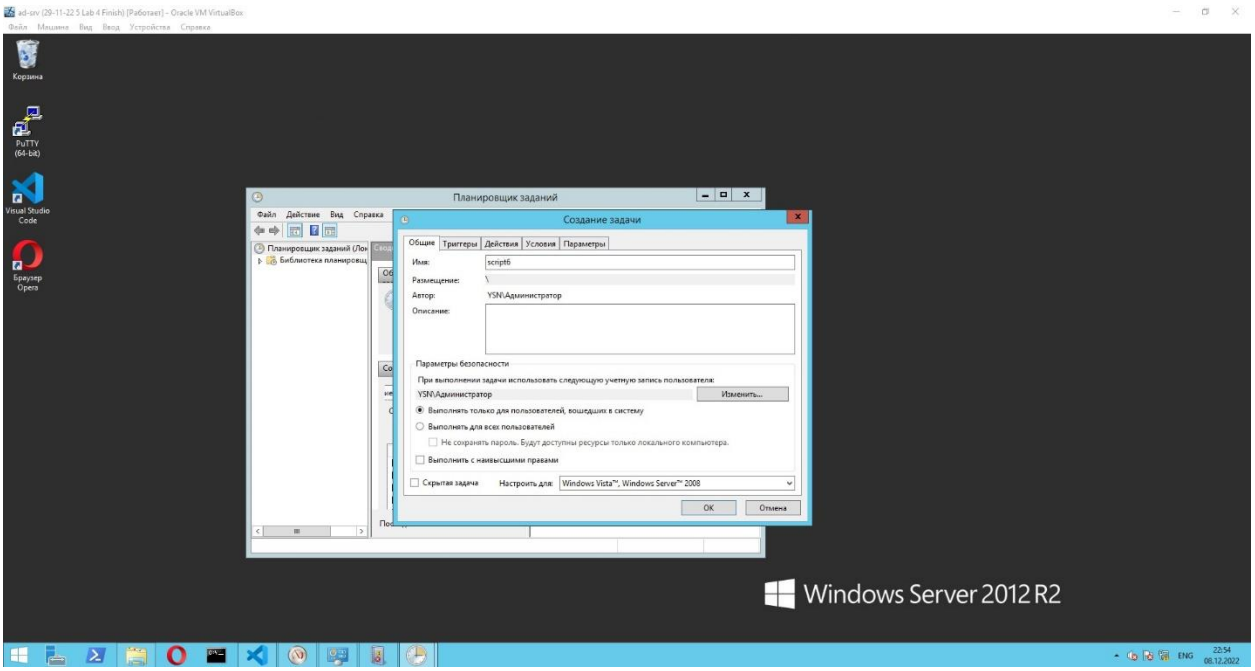
7.

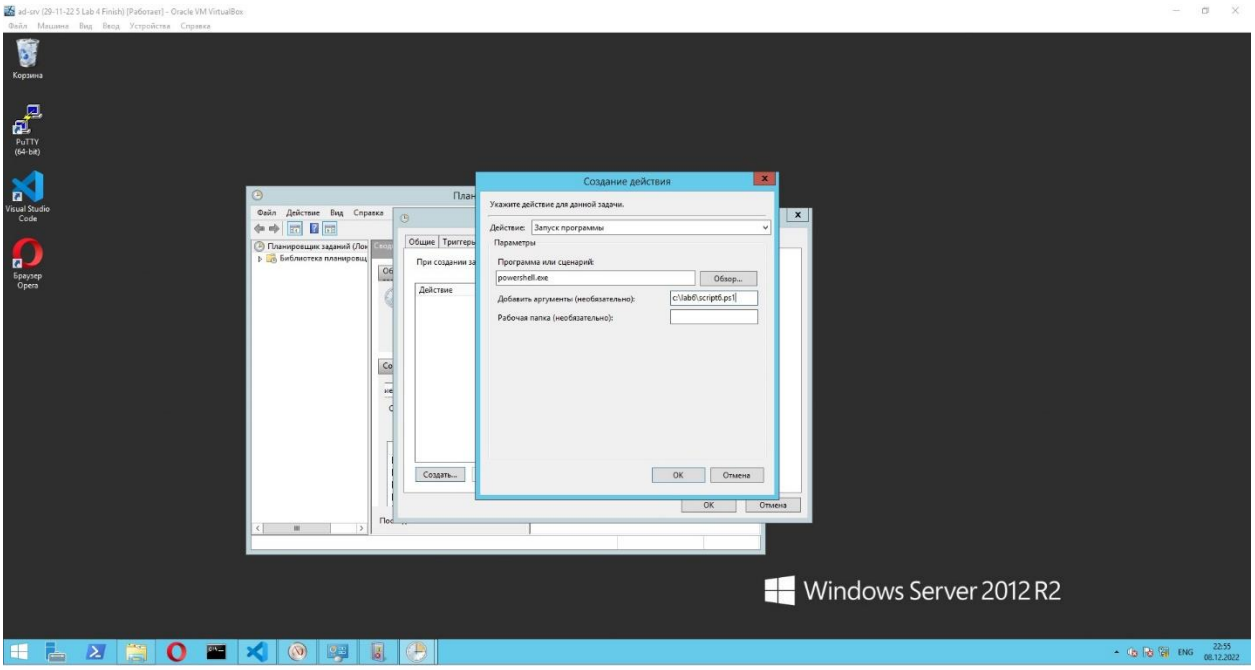


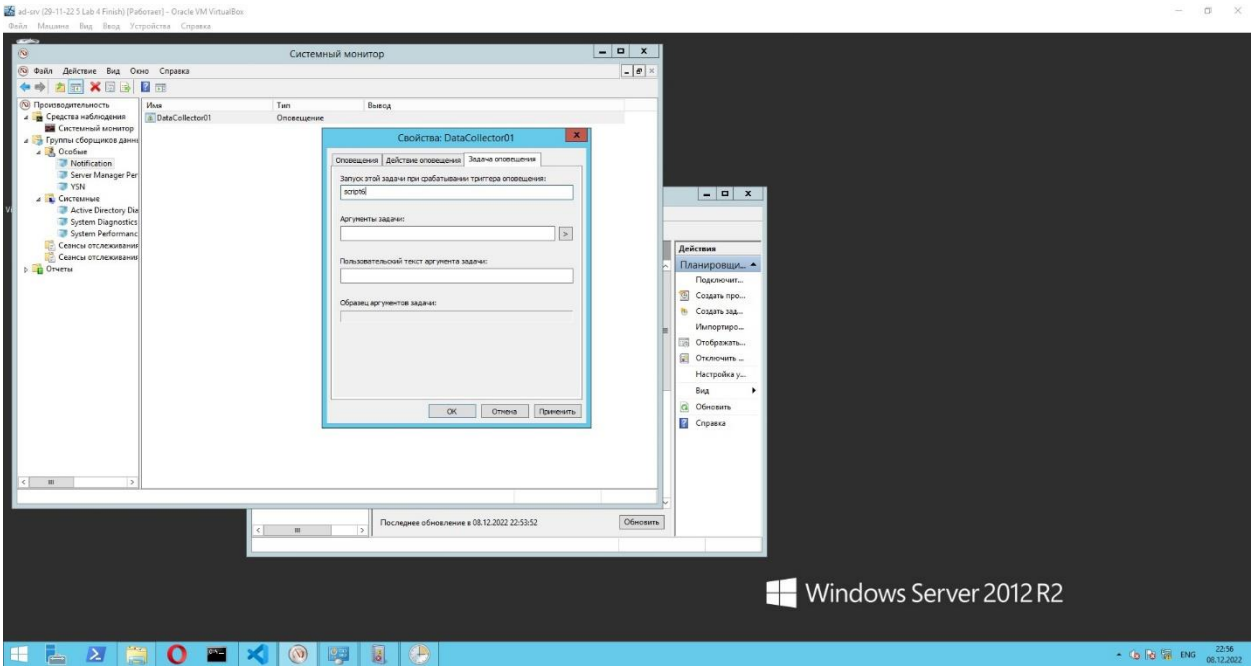

ad-srv (29-11-22 5 Lab 4 Finish) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Системный монитор
Файл Действие Вид Окно Справка
Производительность
Средства наблюдения
Системный монитор
Группы сборщиков данны
Особые
Server Manager Per
YSN
Системные
Сеансы отслеживания
Сеансы отслеживания
Отчеты
Имя
Статус
Server Manager Performance M...
Остано...
YSN
Остано...
Создать новую группу сборщиков данных.
Какой тип данных вы хотите использовать?
Создать журналы данных
Счетчик производительности
Данные отслеживания событий
Сведения о конфигурации системы
Оповещение счетчика производительности
Далее
Готово
Отмена
C:\lab6>powershell.exe ./script6.ps1
C:\lab6>

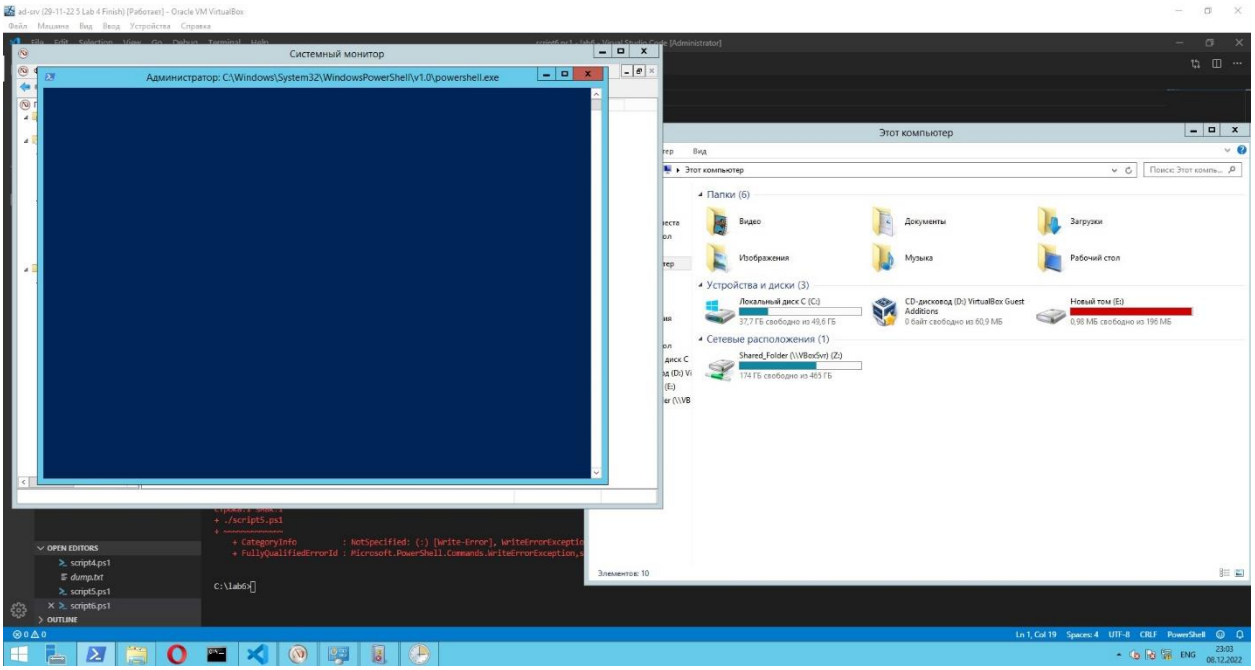

Системный монитор
Свойства: DataCollector01
Windows Server 2012 R2

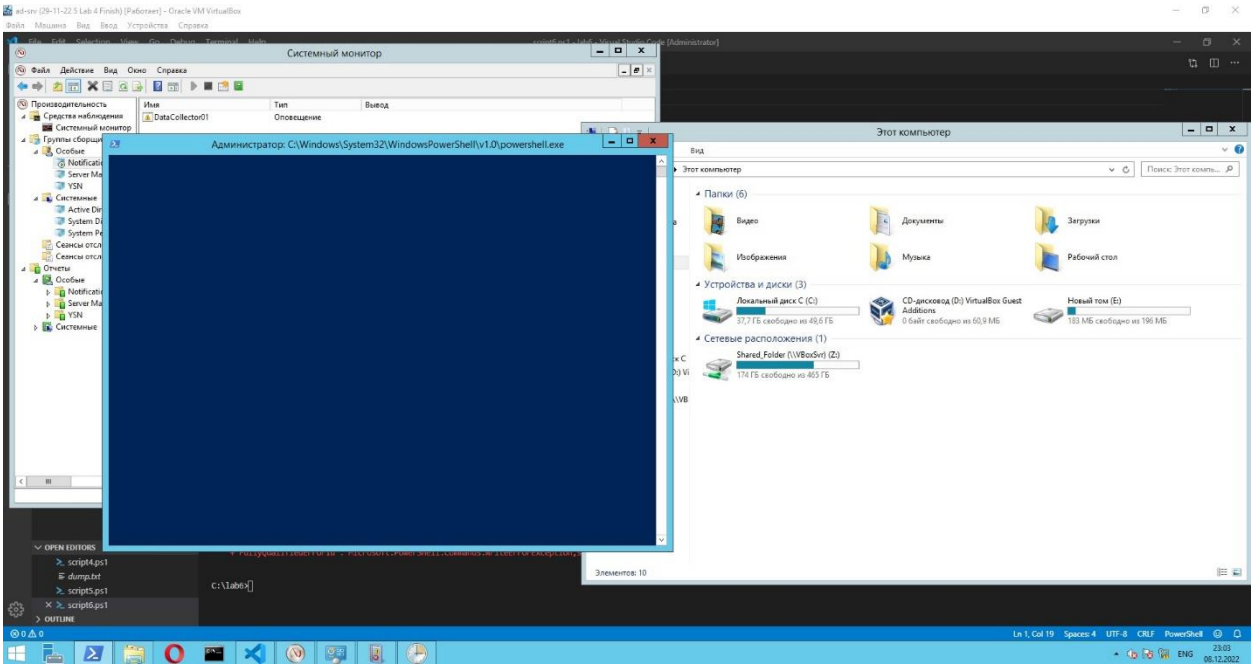

ad-srv (29-11-22 5 Lab 4 Finish) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Системный монитор
Файл Действие Вид Окно Справка
Производительность
Средства наблюдения
Системный монитор
Группы сборщиков данн
Особые
Notification
Server Manager Per
YSN
Системные
Сеансы отслеживания
Сеансы отслеживания
Отчеты
Имя
Тип
Вывод
DataCollector01
Оповещение
Свойства: DataCollector01
Оповещения
Действие оповещения
Задача оповещения
Сделать запись в журнале событий приложений
Запустить группу сборщиков данных:
OK
Отмена
Применить
C:\lab6>
OPEN EDITORS

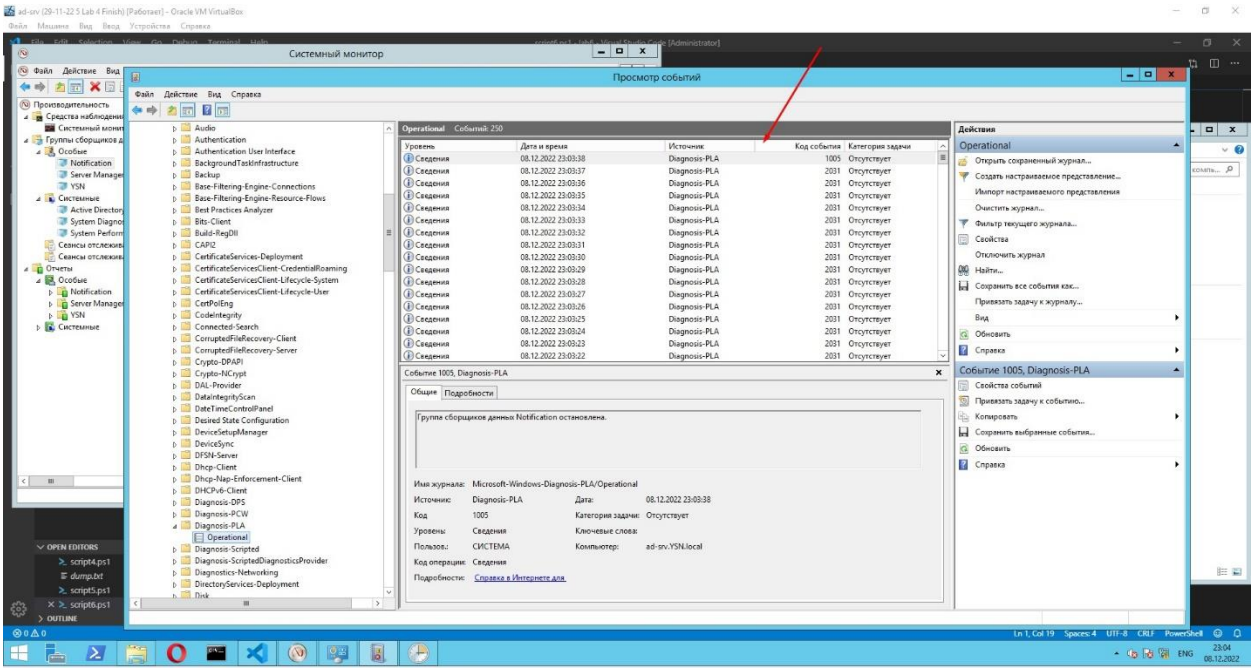

Корзина
PuTTY (64-bit)
Visual Studio Code
Браузер Opera
Планировщик заданий
Создание задачи
Общие
Триггеры
Действия
Условия
Параметры
Имя:
script6
Автор:
YSN\Администратор
Описание:
Параметры безопасности
Изменить...
Выполнять только для пользователей, вошедших в систему
Выполнять для всех пользователей
Выполнять с наивысшими правами
Скрытая задача
Настроить для:
Windows Server 2012 R2
ENG


Создание действия
Укажите действие для данной задачи.
Действие: Запуск программы
Параметры
Программа или сценарий:
powershell.exe
Обзор...
Добавить аргументы (необязательно):
c:\lab8\script6.ps1
Рабочая папка (необязательно):
OK
Отмена
Windows Server 2012 R2

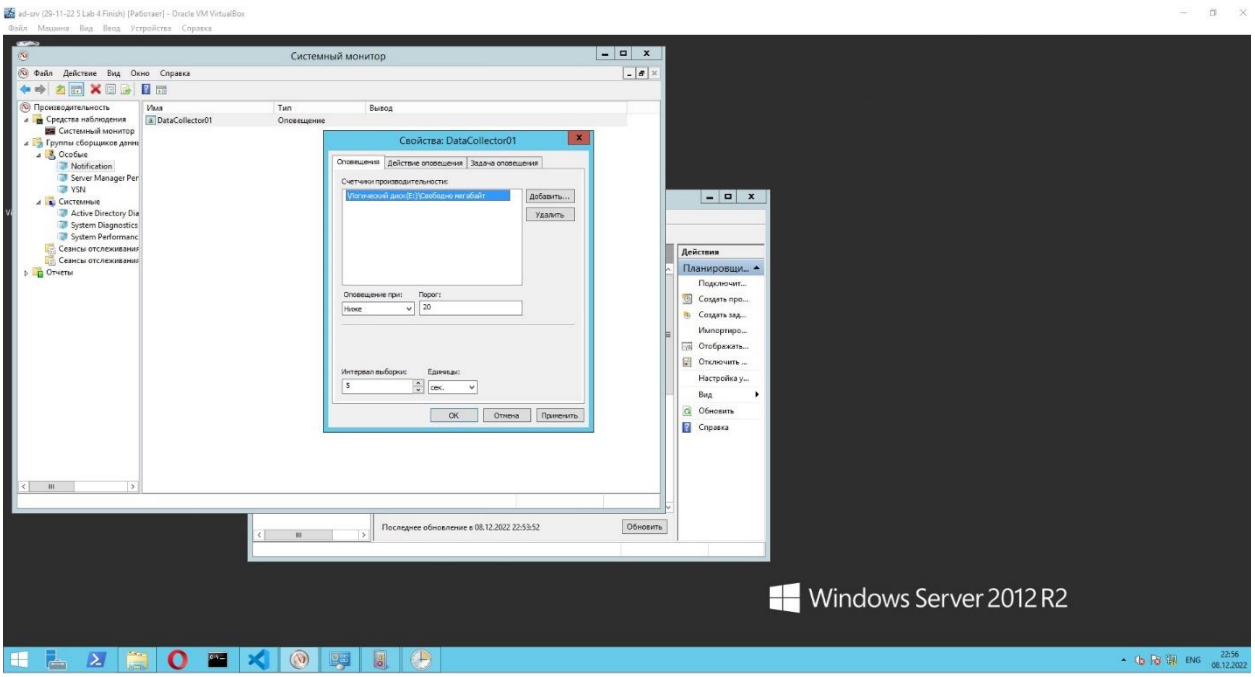

Системный монитор
Свойства: DataCollector01
Оповещения
Действие оповещения
Задача оповещения
Запуск этой задачи при срабатывании триггера оповещения:
script6
Аргументы задачи:
Пользовательский текст аргумента задачи:
Образец аргументов задачи:
OK
Отмена
Применить
Windows Server 2012 R2


Системный монитор
Администратор: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Этот компьютер
Папки (6)
Видео
Документы
Загрузки
Изображения
Музыка
Рабочий стол
Устройства и диски (3)
Локальный диск C (C:)
CD-дисковод (D:) VirtualBox Guest Additions
Новый том (E:)
Сетевые расположения (1)
Shared_Folder (\\VBoxSvr) (Z:)
OPEN EDITORS
script4.ps1
dump.txt
script5.ps1
script6.ps1
OUTLINE
C:\lab6>


Системный монитор
Администратор: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Этот компьютер
Папки (6)
Видео
Документы
Загрузки
Изображения
Музыка
Рабочий стол
Устройства и диски (3)
Локальный диск C (C:)
CD-дисковод (D:) VirtualBox Guest Additions
Новый том (E:)
Сетевые расположения (1)
Shared_Folder (\\VBoxSvr) (Z:)
OPEN EDITORS
script4.ps1
dump.txt
script5.ps1
script6.ps1
OUTLINE
C:\lab6>



Замеченная девиация в поведении – даже после очистки диска с помощью script6 продолжает запускать его и оставлять заметку в логах.



Даёт тот же результат.