

**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 № М33091

Фисенко Никита Данилович

Рустамов Марк Самирович

Санкт-Петербург 2023

Цель работы:

Ознакомиться со встроенными средствами технического мониторинга, назначением и принципами работы Perfomance 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 -NoTypeInfoation -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 C:\Windows\system32\csrss.exe
388 csrss C:\Windows\system32\csrss.exe
1528 dfssvc C:\Windows\system32\dfssvc.exe
1716 dfssvc C:\Windows\system32\dfssvc.exe
2280 dllhost C:\Windows\system32\dllhost.exe
1568 dns C:\Windows\system32\dns.exe
768 dsm C:\Windows\system32\dsm.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_exe 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\Безмяный2.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>
```

processes.csv — Блокнот

```
1
File: ProcessName, Path, User, CPU, WorkingSet, StartTime
336, csrss, 2, 296875, 3698688, 17.11.2023 11:06:04
388, csrss, 2, 48625, 15835136, 17.11.2023 11:06:05
1528, dfssvc, C:\Windows\System32\dfssvc.exe, 0, 125, 13616000, 17.11.2023 12:06:40
1716, dfssvc, C:\Windows\System32\dfssvc.exe, 0, 815625, 5267456, 17.11.2023 12:06:41
2280, dllhost, C:\Windows\System32\dllhost.exe, 0, 4878336, 17.11.2023 12:06:59
1568, dns, C:\Windows\System32\dns.exe, 0, 78125, 6742448, 17.11.2023 12:06:40
768, dsm, C:\Windows\System32\dsm.exe, 0, 625, 43868160, 17.11.2023 11:06:17
2808, explorer, C:\Windows\Explorer.EXE, 3, 65625, 182252544, 17.11.2023 12:07:17
0, Idle, 0, 0, 0, 0, 0
1592, ismserv, C:\Windows\System32\ismserv.exe, 0, 815625, 4581584, 17.11.2023 12:06:41
488, lsass, C:\Windows\system32\lsass.exe, 1, 3125, 46534656, 17.11.2023 11:06:07
1488, Microsoft.ActiveDirectory.WebServices, C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe, 0, 78125, 41394376, 17.11.2023 12:06:36
2548, msdtc, C:\Windows\System32\msdtc.exe, 0, 815625, 6479872, 17.11.2023 12:08:56
1016, powershell_exe, C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe, 0, 65625, 168718336, 17.11.2023 12:07:44
2660, ServerManager, C:\Windows\system32\ServerManager.exe, 1, 6875, 77338384, 17.11.2023 12:07:26
480, services, 0, 296875, 80848640, 17.11.2023 11:06:06
224, smss, 0, 89375, 1864960, 17.11.2023 11:05:58
1464, spoolsv, C:\Windows\System32\spoolsv.exe, 0, 815625, 9121792, 17.11.2023 12:06:36
304, svchost, C:\Windows\system32\svchost.exe, 0, 125, 14262272, 17.11.2023 12:06:24
640, svchost, C:\Windows\system32\svchost.exe, 0, 189375, 9576448, 17.11.2023 11:06:16
684, svchost, C:\Windows\system32\svchost.exe, 0, 203125, 53858560, 17.11.2023 11:06:16
860, svchost, C:\Windows\System32\svchost.exe, 1, 515625, 17313792, 17.11.2023 12:06:20
888, svchost, C:\Windows\system32\svchost.exe, 4, 75, 13468416, 17.11.2023 12:06:21
912, svchost, C:\Windows\system32\svchost.exe, 0, 125, 18575872, 17.11.2023 12:06:21
936, svchost, C:\Windows\system32\svchost.exe, 0, 4587520, 17.11.2023 12:16:42
1000, svchost, C:\Windows\System32\svchost.exe, 0, 81325, 8441856, 17.11.2023 12:06:22
1100, svchost, C:\Windows\system32\svchost.exe, 0, 234375, 11476992, 17.11.2023 12:06:26
1556, svchost, C:\Windows\System32\svchost.exe, 0, 2744320, 17.11.2023 12:16:26
1608, svchost, C:\Windows\system32\svchost.exe, 0, 815625, 4689920, 17.11.2023 12:06:57
1616, svchost, C:\Windows\system32\svchost.exe, 0, 846875, 18137600, 17.11.2023 12:06:57
2704, svchost, C:\Windows\System32\svchost.exe, 0, 815625, 4546560, 17.11.2023 12:16:58
4, System, 0, 39375, 258048, 17.11.2023 11:05:58
1844, taskhost, C:\Windows\System32\taskhost.exe, 0, 69375, 12800000, 17.11.2023 12:16:26
2736, taskhostex, C:\Windows\system32\taskhostex.exe, 0, 815625, 8007680, 17.11.2023 12:07:16
3060, taskhostex, C:\Windows\system32\taskhostex.exe, 0, 63125, 4657152, 17.11.2023 12:16:26
1928, TiWorker, C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_6.3.9600.17709_none_fa7932f59afc2e40\TiWorker.exe, 27, 984375, 36646912, 17.11.2023 12:16:26
2596, TrustedInstaller, C:\Windows\servicing\TrustedInstaller.exe, 0, 265625, 4722688, 17.11.2023 12:16:26
792, VBoxService, C:\Windows\System32\VBoxService.exe, 0, 815625, 5181440, 17.11.2023 11:06:18
2844, VBoxTray, C:\Windows\system32\VBoxTray.exe, 0, 815625, 6481584, 17.11.2023 12:07:31
1408, vds, C:\Windows\system32\vds.exe, 0, 83125, 8327168, 17.11.2023 12:06:56
932, VSSVC, C:\Windows\system32\vssvc.exe, 0, 815625, 5697536, 17.11.2023 12:16:58
396, wininit, C:\Windows\system32\wininit.exe, 0, 815625, 3660928, 17.11.2023 11:06:09
424, winlogon, C:\Windows\system32\winlogon.exe, 0, 89375, 5976864, 17.11.2023 11:06:05
900, WmiPrvSE, C:\Windows\system32\wbem\wmiPrvse.exe, 0, 4658880, 17.11.2023 12:16:50
2312, WmiPrvSE, C:\Windows\system32\wbem\wmiPrvse.exe, 0, 815625, 5931808, 17.11.2023 12:07:00
```

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
```

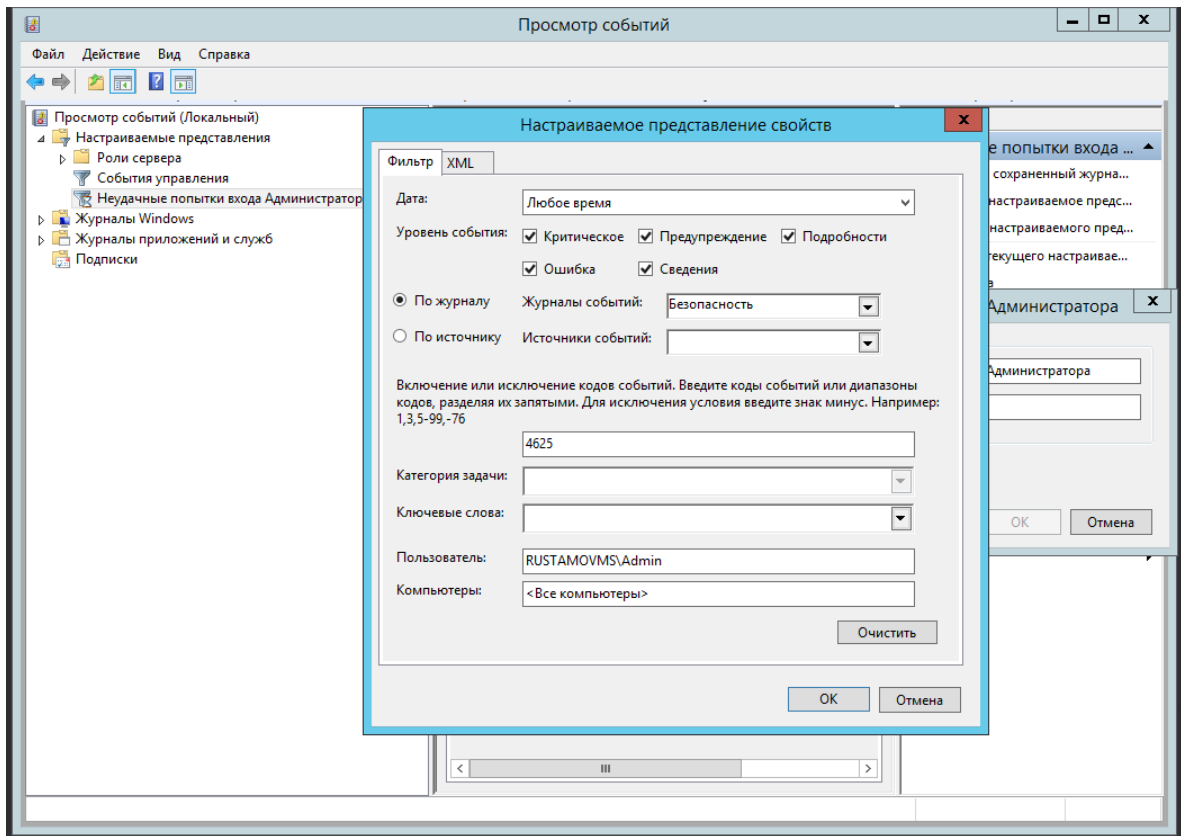
TaskPath	TaskName	State
\	MyTask	Ready

```
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
```

```
SystemInfo - Блокнот
Файл  Правка  Формат  Вид  Справка

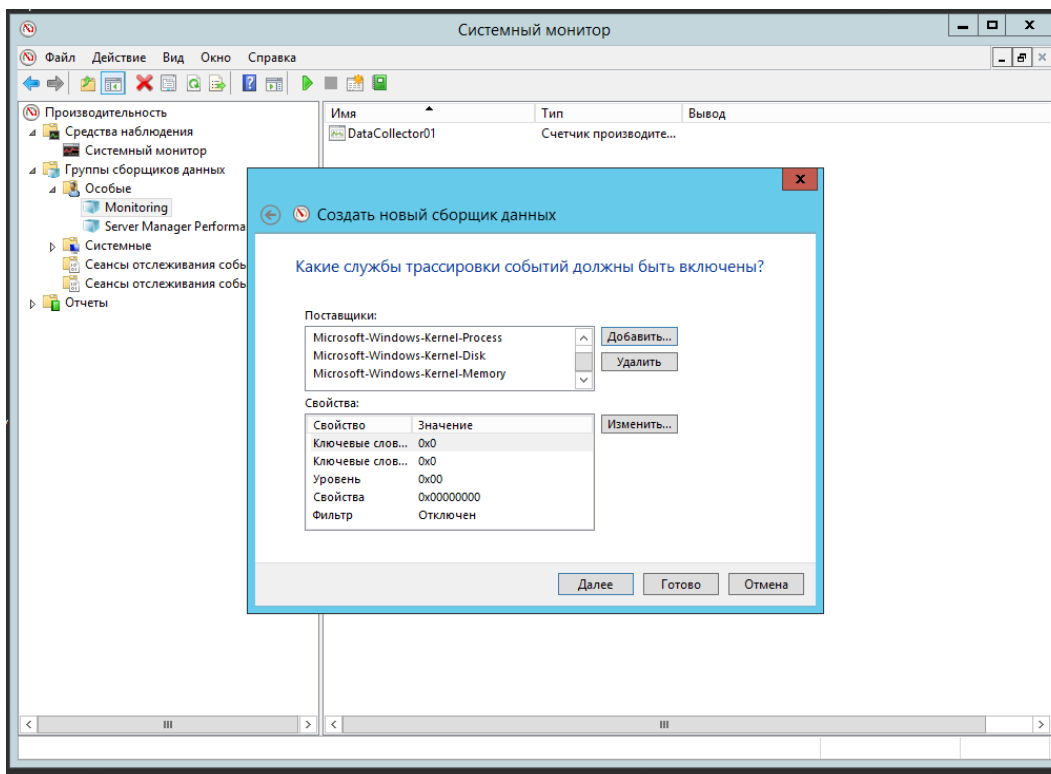
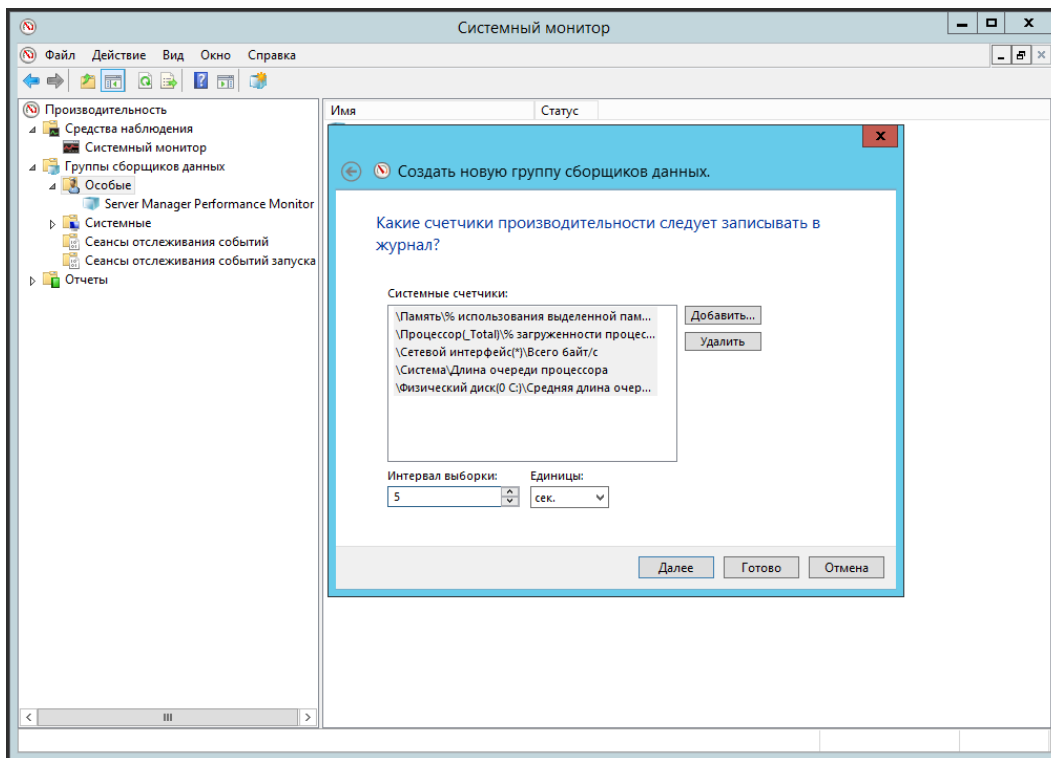
TimeCreated      Id Message
-----
17.11.2023 13:24:59 6005 Запущена служба журнала событий.
17.11.2023 13:24:50 6006 Служба журнала событий остановлена.
17.11.2023 13:23:21 6005 Запущена служба журнала событий.
17.11.2023 12:58:29 6005 Запущена служба журнала событий.
17.11.2023 12:58:16 6006 Служба журнала событий остановлена.
13.11.2023 13:27:20 6005 Запущена служба журнала событий.
13.11.2023 13:27:11 6006 Служба журнала событий остановлена.
13.11.2023 13:24:58 6005 Запущена служба журнала событий.
13.09.2023 14:08:28 6006 Служба журнала событий остановлена.
13.09.2023 14:04:10 6005 Запущена служба журнала событий.

Date            Title
-----
17.11.2023 13:23:57 Обновление механизма обнаружения угроз для Microsoft Defender Antivirus - KB2267602 (версия 1....
17.11.2023 12:59:36 Обновление механизма обнаружения угроз для Microsoft Defender Antivirus - KB2267602 (версия 1....
13.11.2023 13:25:49 Обновление механизма обнаружения угроз для Microsoft Defender Antivirus - KB2267602 (версия 1....
13.11.2023 13:25:07 Обновление механизма обнаружения угроз для Microsoft Defender Antivirus - KB2267602 (версия 1....

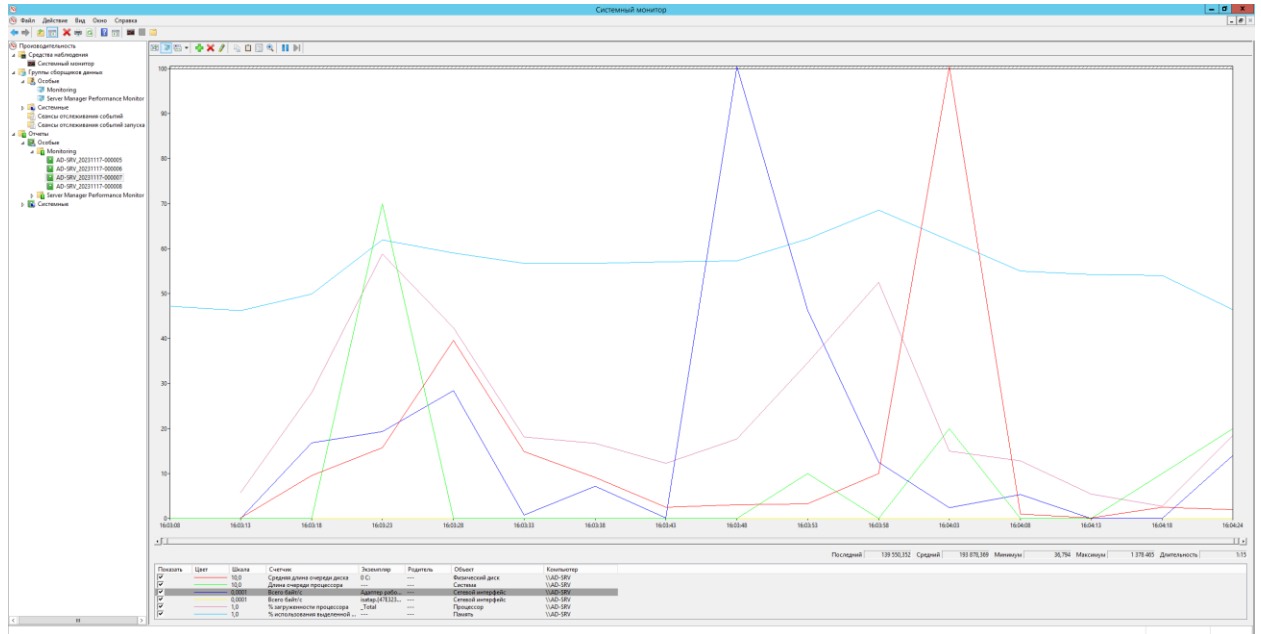
Errors: 2, Warnings: 6
```

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.

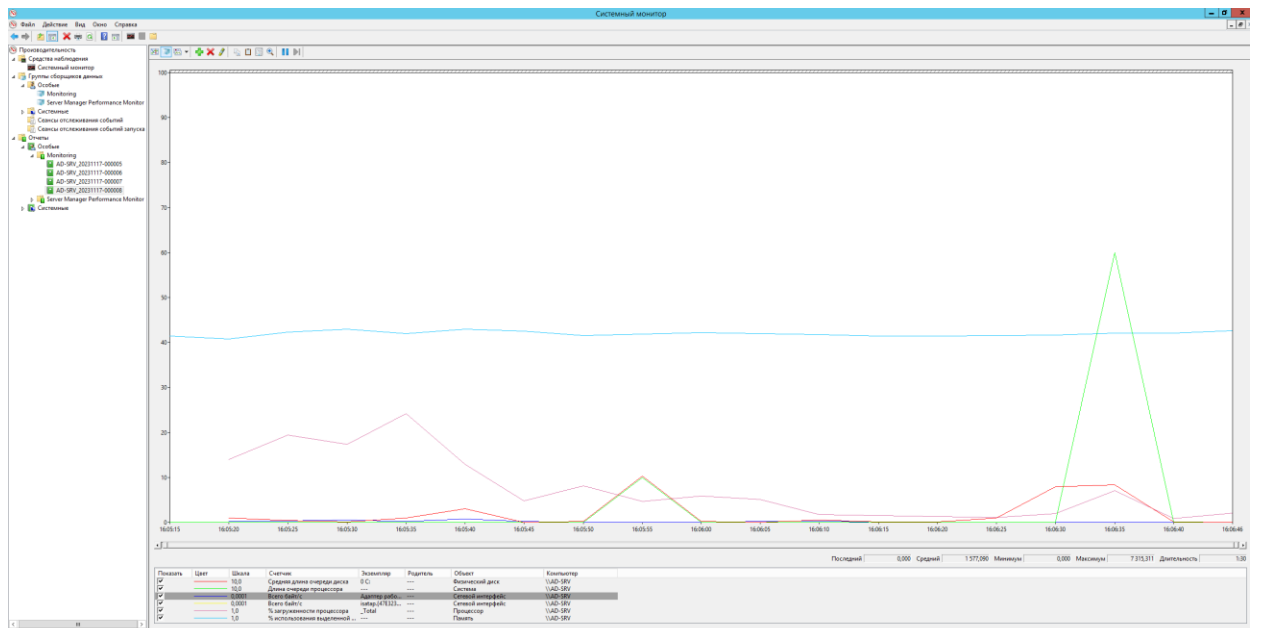


opera + explorer



Для браузеров характерно использование сети, памяти, процессора.

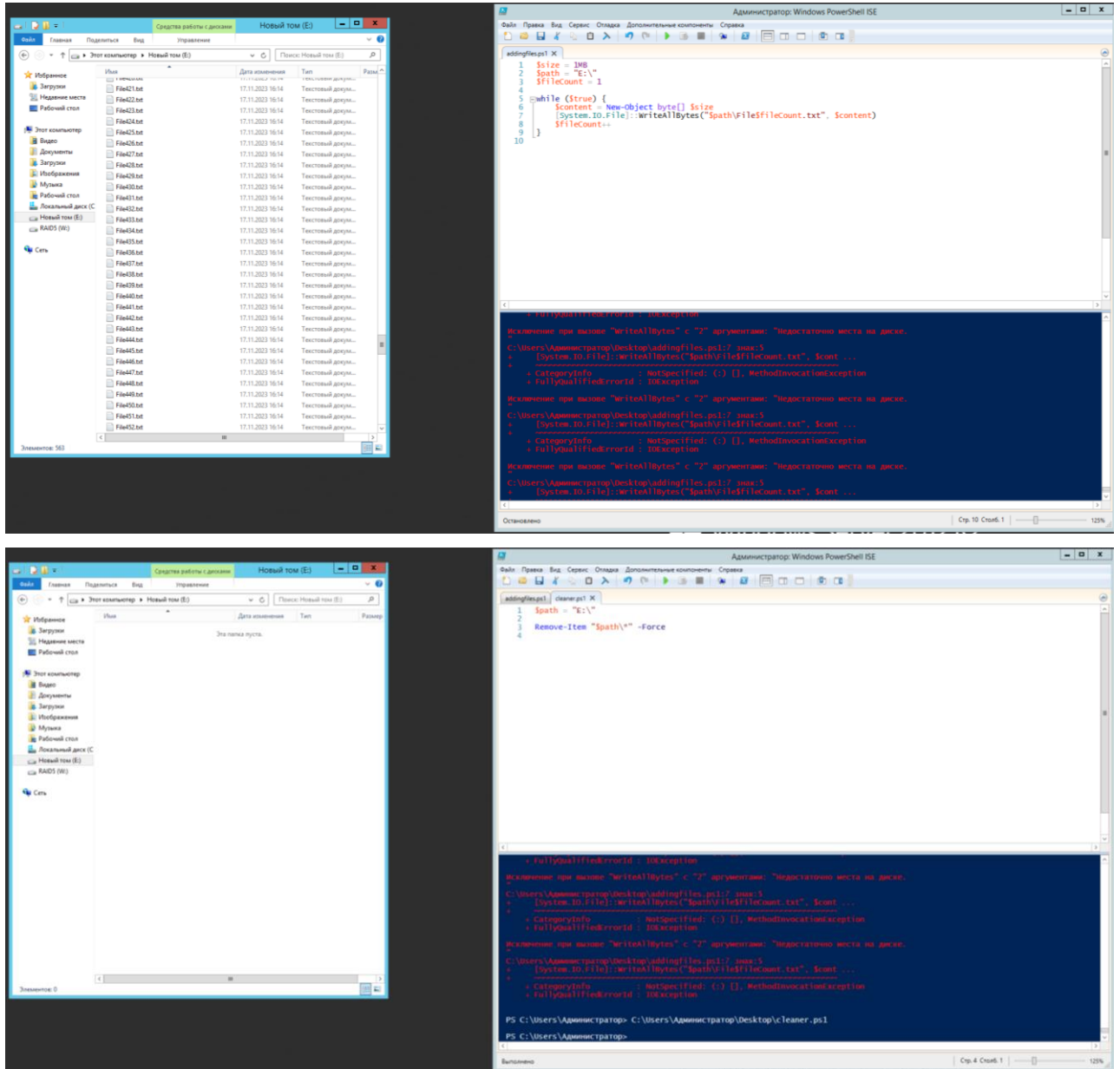
vs code + notepad



Для текстовых редакторов характерно использование памяти.

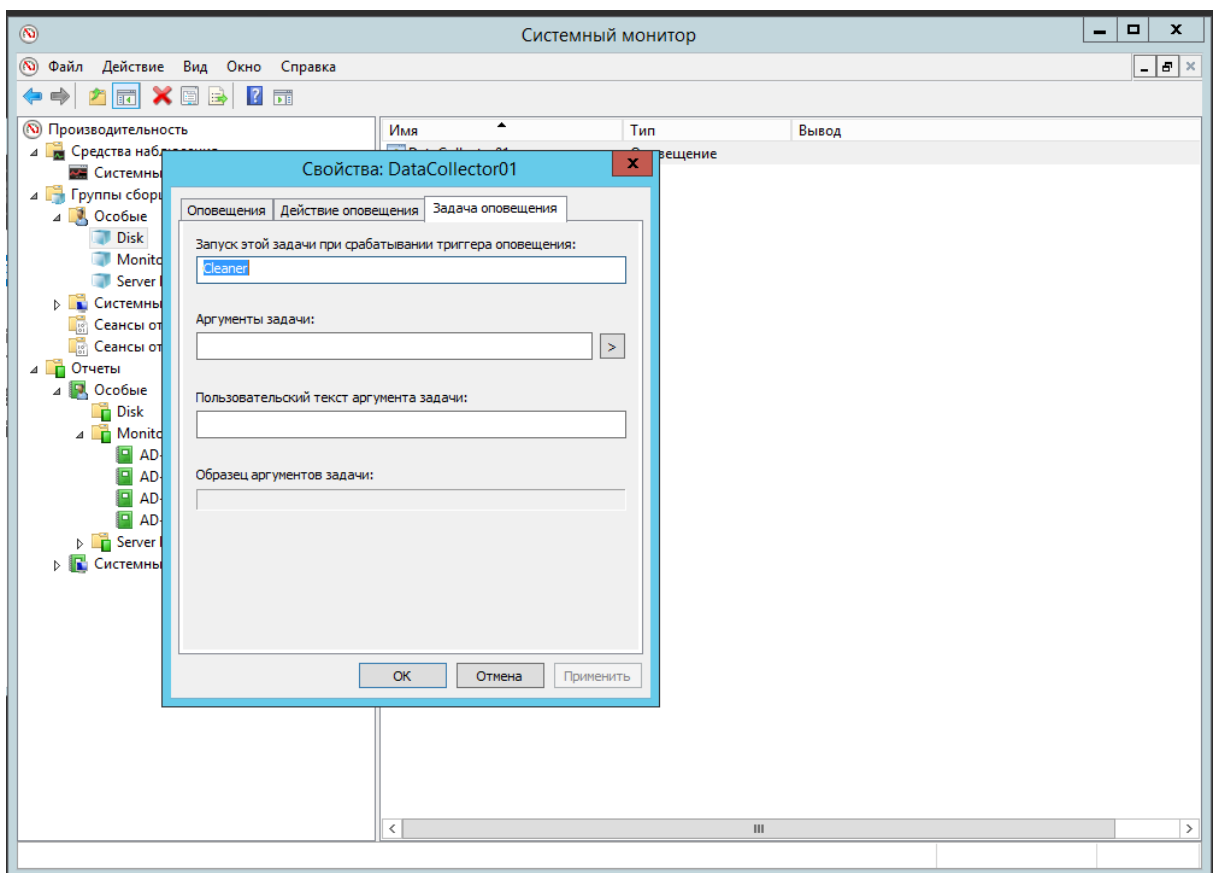
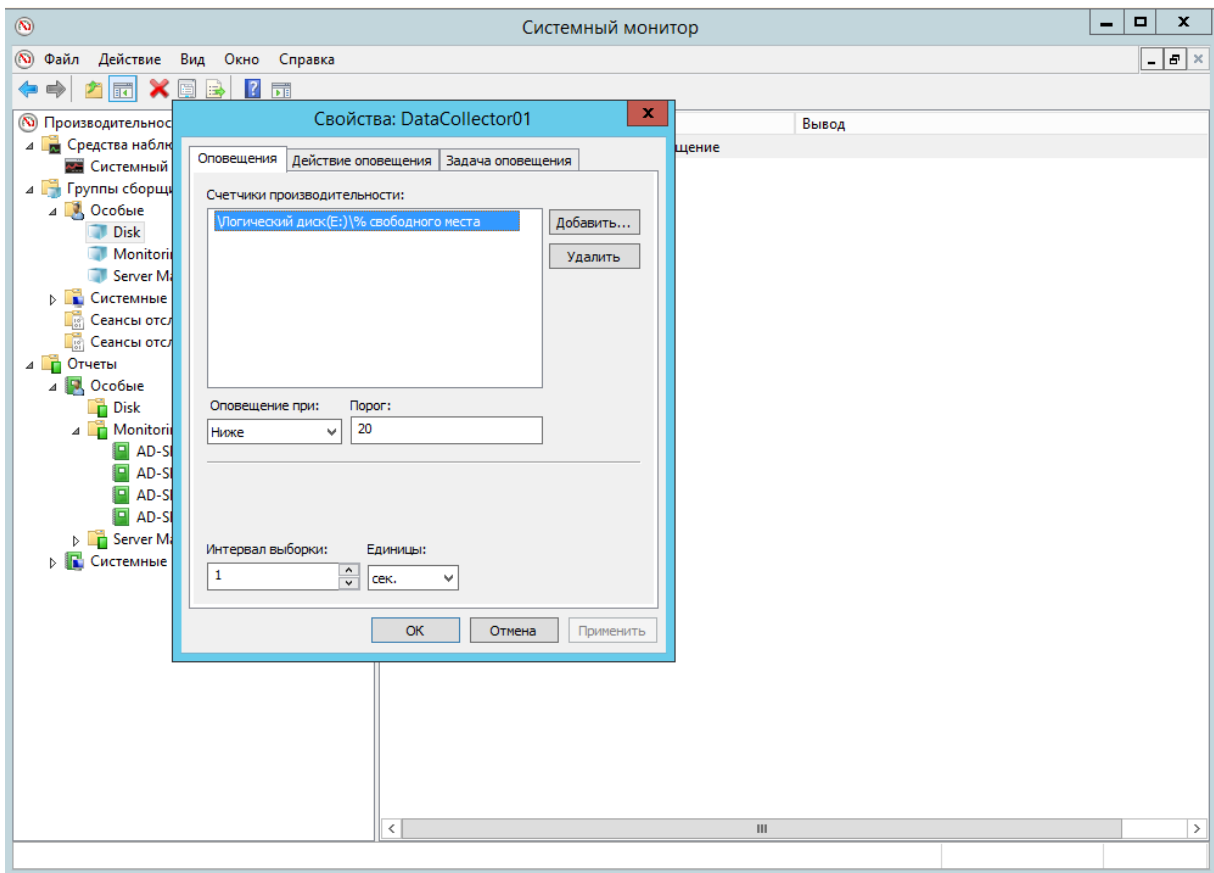
Часть 5. Автоматизация реакции системы на ее состояние

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

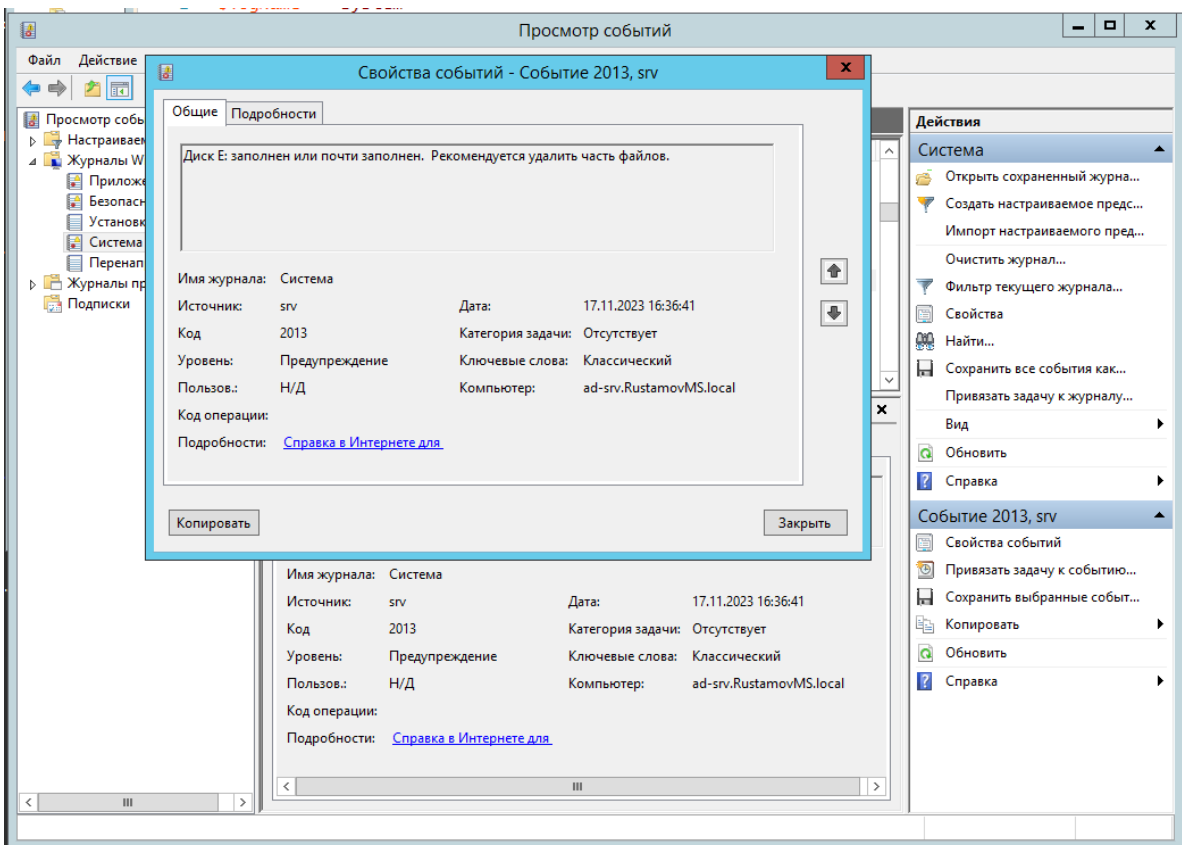
Разработчики Performance Monitor предполагают, что нужно в Планировщике заданий создать задание, выполняющее скрипт из п. 3 и указать имя этого задания в настройках Сборщика данных отслеживания событий.



```
1 $action = New-ScheduledTaskAction -Execute 'powershell.exe' -Argument 'C:\Users\Администратор\Desktop\cleaner.ps1'
2 $trigger = New-ScheduledTaskTrigger -AtStartup
3
4 Register-ScheduledTask -Action $action -Trigger $trigger -TaskName 'Cleaner'
5
```

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

TaskPath	TaskName	State
\	Cleaner	Ready



При запуске скрипта диск все время очищается 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 находятся журналы событий Windows в виде файлов?

Обычно, 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.
- 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 Performance 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.