

Лабораторная работа 7

МОНИТОРИНГ СОБЫТИЙ И ПРОИЗВОДИТЕЛЬНОСТЬ СИСТЕМЫ

Цель лабораторной работы

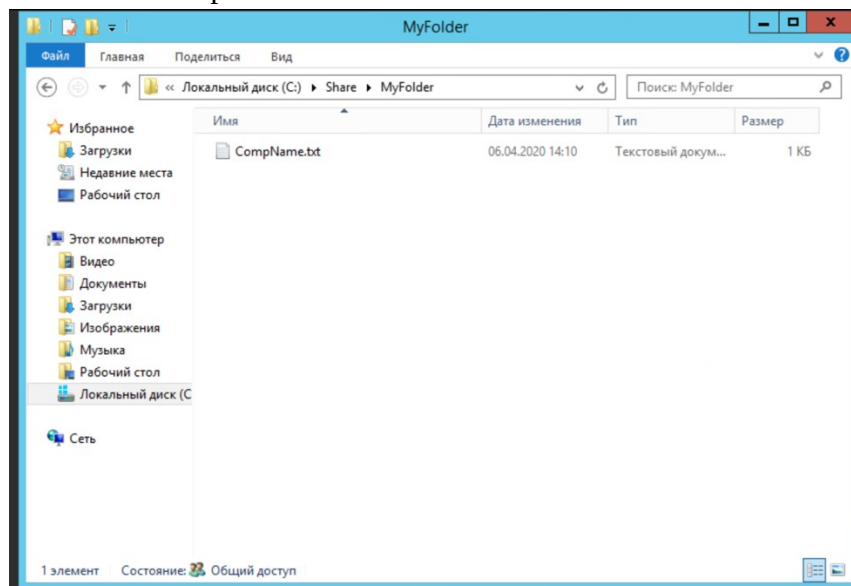
1. Изучить оснастку «Просмотр событий».
2. Ознакомиться с «Диспетчер задач».

Используемое программное обеспечение

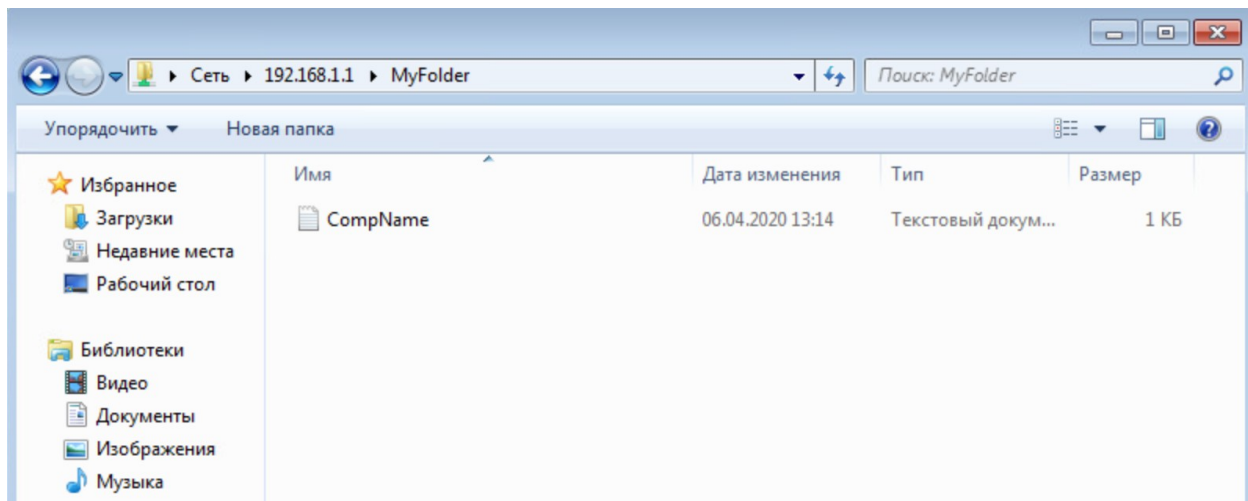
Для выполнения лабораторной работы используются ОС *Windows Server*.

Порядок выполнения работы

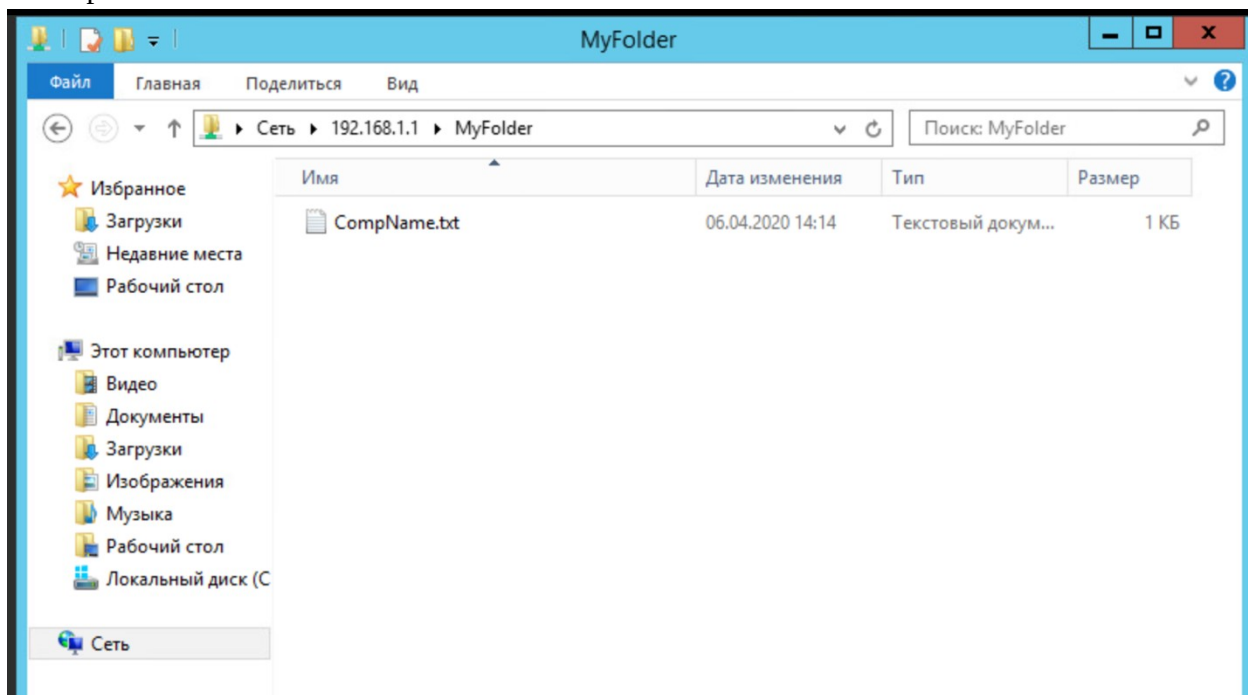
1. Войдите на *Windows Server*, в папке «Share» создайте папку «MyFolder» и разместите в ней документ с именем CompName.txt, содержащий сведения об IP-адресе и имени компьютера.



2. Откройте общий доступ к папке «MyFolder» для пользователей «Администратор» и «Student».
3. На *Windows Client* войдите пользователем «Student», перейдите в общую папку «MyFolder» и откройте файл «CompName.txt»



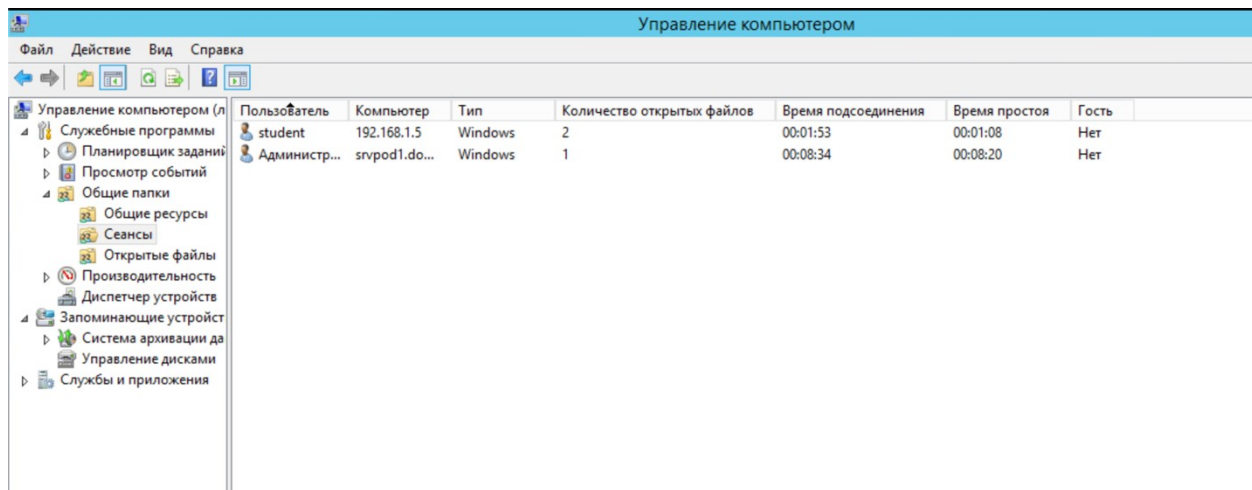
4. На Windows Server перейдите в общую папку «MyFolder» и откройте файл «CompName.txt».



5. Перейдите на Windows Server и откройте оснастку «Управление компьютером» («Диспетчер серверов» → «Средства» → «Управление компьютером»).
6. Разверните раздел «Общие ресурсы». Здесь перечислены все опубликованные (общие) ресурсы вашего компьютера.

	Общий ресурс	Путь к папке	Тип	Количество клиентских подключений	Описание
Управление компьютером (л)					
Служебные программы	admin	C:\Share\admin	Windows	0	
Планировщик заданий	ADMIN\$	C:\Windows	Windows	0	Удаленный Admin
Просмотр событий	CS	C:\	Windows	0	Стандартный общий р...
Общие папки	IPC\$		Windows	0	Удаленный IPC
Общие ресурсы	MyFolder	C:\Share\MyFolder	Windows	2	
Сеансы	NETLOGON	C:\Windows\SYSV...	Windows	0	Общий сервер входа
Открытые файлы	Share	C:\Users\Админис...	Windows	0	
Производительность	Share2	C:\Share	Windows	0	
Диспетчер устройств	student	C:\Share\student	Windows	0	
Запоминающие устройст	SYSVOL	C:\Windows\SYSV...	Windows	0	Общий сервер входа
Система архивации да	teacher	C:\Share\teacher	Windows	0	
Управление дисками	Users	C:\Users	Windows	0	
Службы и приложения					

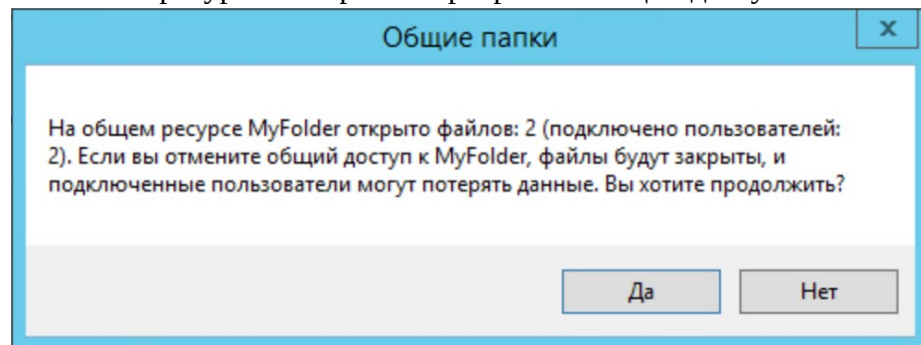
7. Откройте раздел «Сеансы». Здесь перечислены все открытые сеансы, т.е. какие пользователи и на каких компьютерах сейчас подключены к вашему компьютеру. Если вызвать контекстное меню раздела, то можно сразу отключить все сеансы.



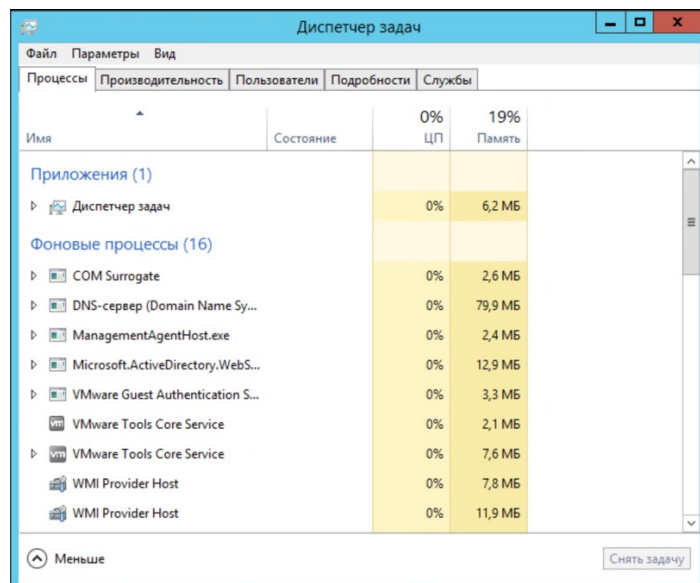
8. Закройте открытый файл. Для этого перейдите в раздел «Открытые файлы» и в контекстном меню файла выберите «Закрывать открытый файл».

Открытый файл	Пользователь	Тип	Блокир.	Режим открытия
C:\Share\MyFolder\	Администратор	Windows	0	Чтение
C:\Share\MyFolder\	student	Windows	0	Чтение

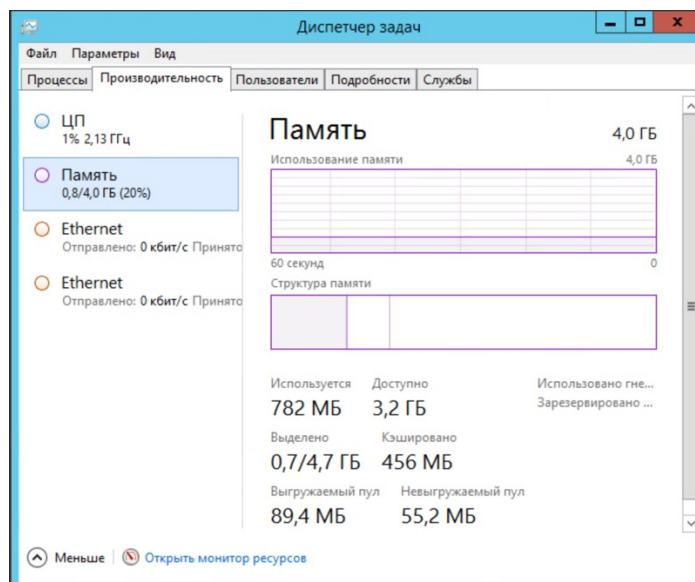
9. Отключите общий доступ к созданному ранее ресурсу «MyFolder». Для этого в контекстном меню ресурса выберите «Прекратить общий доступ».



10. На Windows Server просмотрите информацию о производительности системы: откройте окно диспетчера задач (CTRL+SHIFT+ESC). Нажмите «Подробнее».



11. Перейдите на вкладку «Процессы», просмотрите список и найдите процесс использующий наибольшее количество памяти.
12. Перейдите на вкладку «Производительность» и посмотрите количество выделенной памяти в соответствующем поле и ознакомьтесь с информацией о производительности сети.

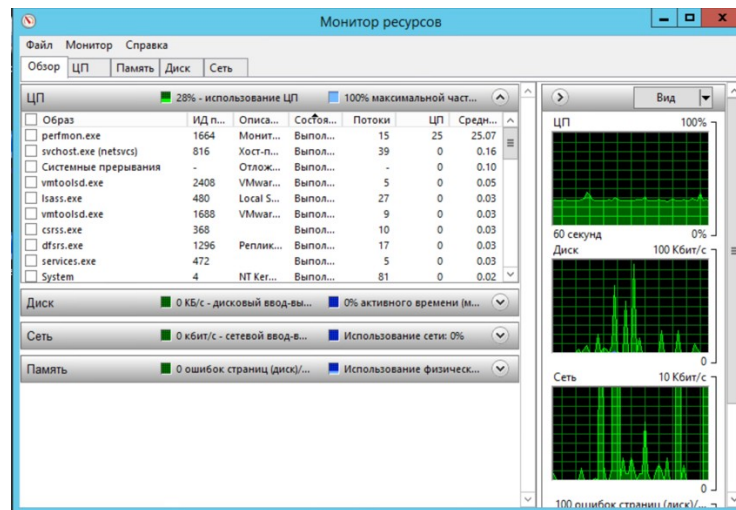


13. Перейдите на вкладку «Пользователи» просмотрите информацию о пользователях, зарегистрированных в системе.

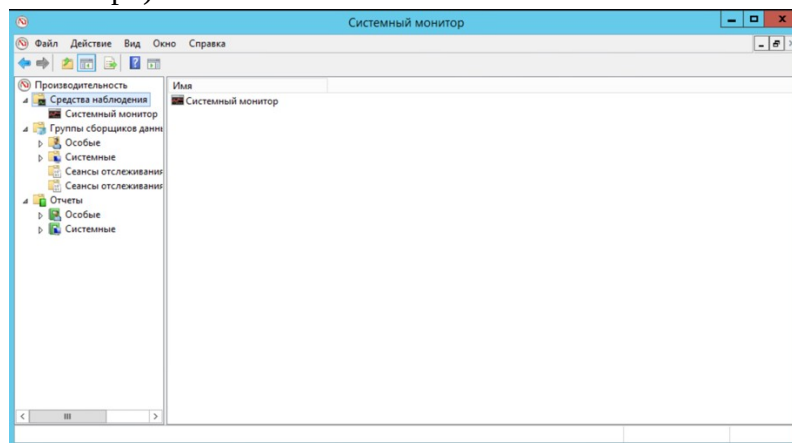
The screenshot shows the 'Пользователи' (Users) tab in Windows Task Manager. It displays a list of users and their resource usage. The table below summarizes the data shown:

Пользователь	Состояние	0% ЦП	19% Память
Администратор (7)		0%	47,3 МБ
VMware Tools Core Service		0%	2,2 МБ
Диспетчер задач		0%	7,1 МБ
Диспетчер окон рабочег...		0%	17,4 МБ
Проводник		0%	15,7 МБ
Программа входа в систе...		0%	0,9 МБ
Процесс исполнения кли...		0%	1,2 МБ
Хост-процесс для задач ...		0%	2,9 МБ

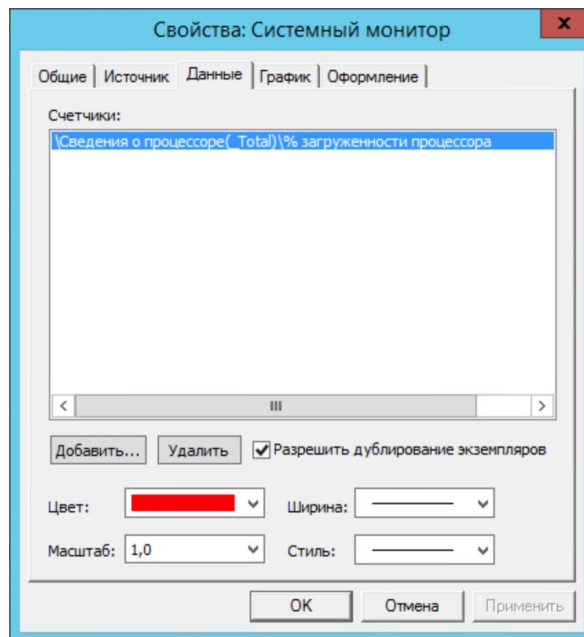
14. Соберите с помощью «Монитор ресурсов» информацию, указанную ниже:
 - а. Количество запущенных приложений.
 - б. Имя процесса, занимающего больше всех оперативной памяти. Количество выделенной памяти.
 - с. Имя процесса, большего всех обращается к диску.



15. Запустите оснастку «Системный монитор» («Диспетчер серверов» → «Средства» → «Системный монитор»).

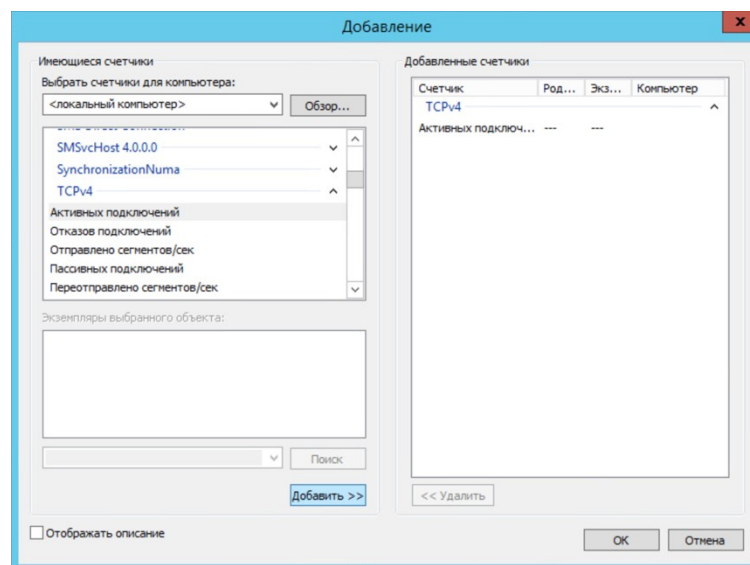


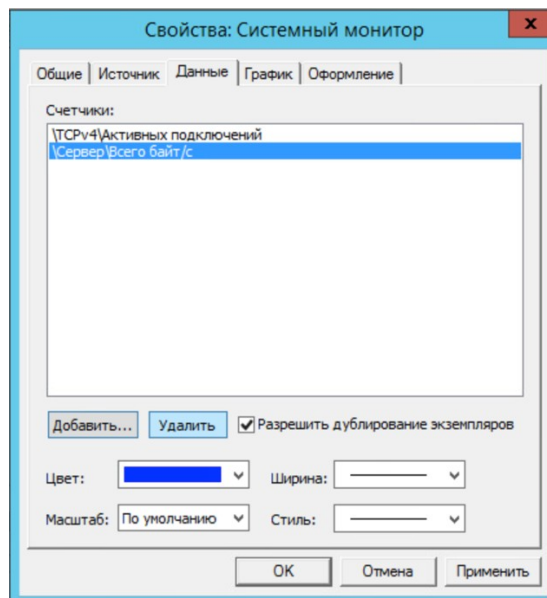
16. Удалите все счетчики из системного монитора:
- активируйте «Системный монитор»;
 - откройте диалоговое окно свойств «Системного монитора» кнопкой «Свойства»;
 - перейдите на вкладку Данные;
 - выделите один из счетчиков и удалите его кнопкой Удалить;
 - аналогично удалите все остальные счетчики.



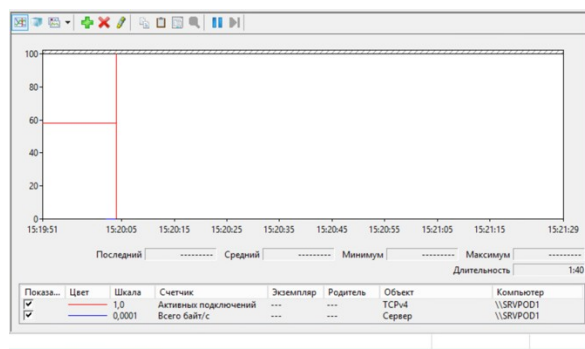
17. Добавьте счетчик активных подключений TCP:

- активируйте добавление счетчика кнопкой **Добавить**;
- выберите в раскрывающемся списке **Объект** – **TCPv4**;
- выберите в списке **Выбрать счетчик из списка** – **Активных подключений**;
- добавьте счетчик кнопкой **Добавить**.
- самостоятельно добавьте счетчик **Всего байт/сек** для объекта **Сервер**;
- закройте окно добавления счетчиков кнопкой **Заккрыть**.





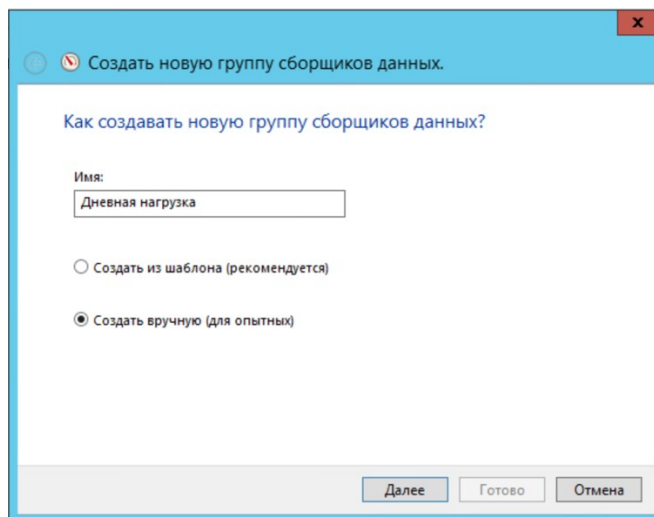
18. Закройте диалоговое окно свойств «Системного монитора» кнопкой «ОК».
19. В правой области начнет отображаться информация добавленных счетчиков в графическом виде.



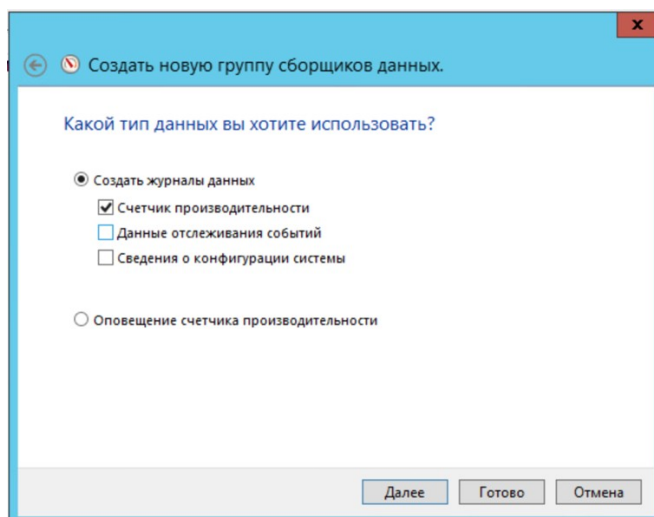
20. Переключите вид отображения информации счетчиков в текстовый вид кнопкой «Изменить тип диаграммы» на панели инструментов.

Имя	Значение
\\SRVPOD1 TCPv4 Активных подключений	58,000
Сервер Всего байт/с	0,000

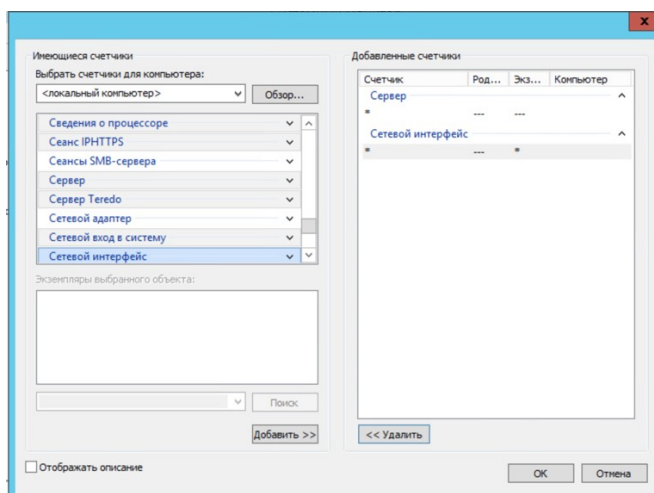
21. Настройте автоматический сбор информации о загрузке сервера в период с 8.00:
 - a. активируйте раздел «Группы сборщиков данных» → «Особые» в левой части окна «Производительность»;
 - b. активируйте создание новых параметров журнала («Действие» → «Создать» → «Группа сборщиков данных»);
 - c. введите название журнала в поле Имя – «Дневная нагрузка» и подтвердите кнопкой «Далее»;



- d. выберете «Создать журнал данных» → «Счетчик производительности». Нажмите «Далее»;

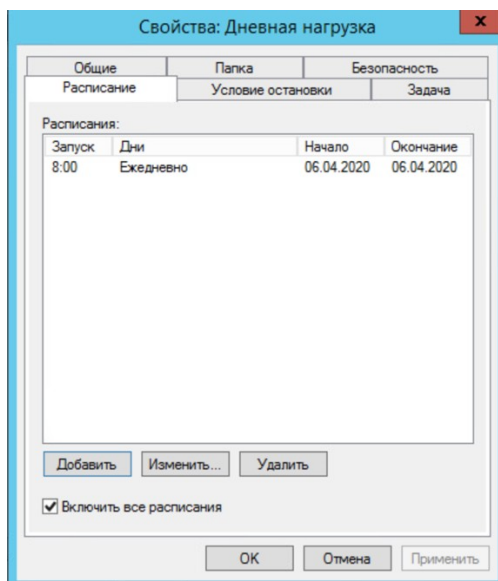


- e. откройте окно добавления объектов кнопкой Добавить объект;
f. выделите в списке Объект – Сервер;
g. добавьте объект кнопкой Добавить;
h. аналогично добавьте объект Сетевой интерфейс;
i. закройте окно добавления объектов кнопкой «ОК»;

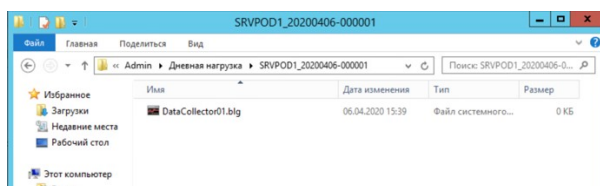


- j. нажмите «Готово». Откройте «Свойства» объекта «Дневная нагрузка».

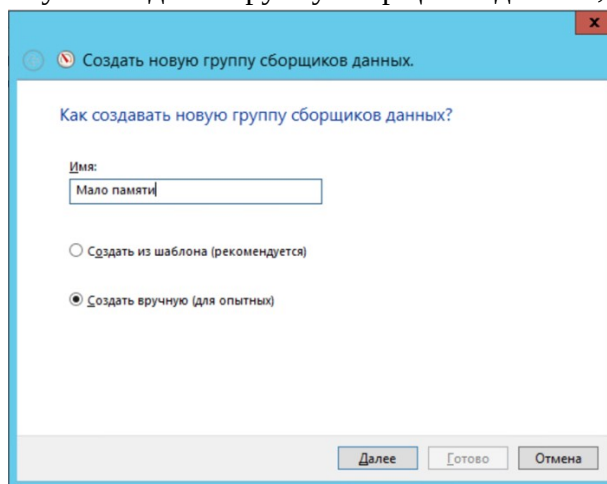
- к. перейдите на вкладку «Расписание». Установите в поле Время – 8.00;



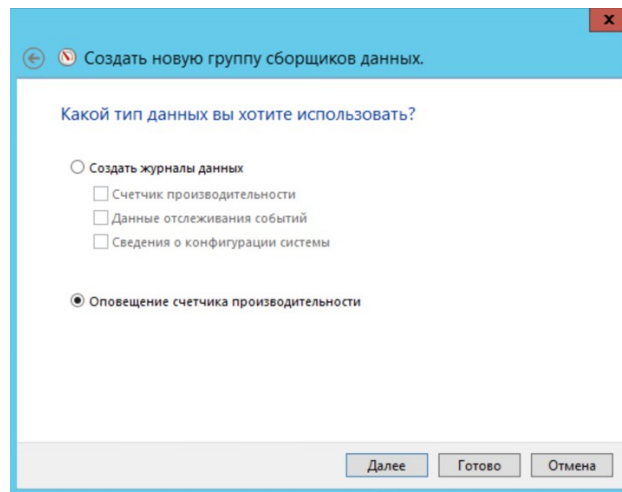
- л. закройте диалоговое окно параметров нового журнала кнопкой «ОК».
м. в правой части окна нажмите «Пуск» на журнале «Дневная нагрузка». Просмотреть результат работы журнала можно в папке «C:\perflogs».



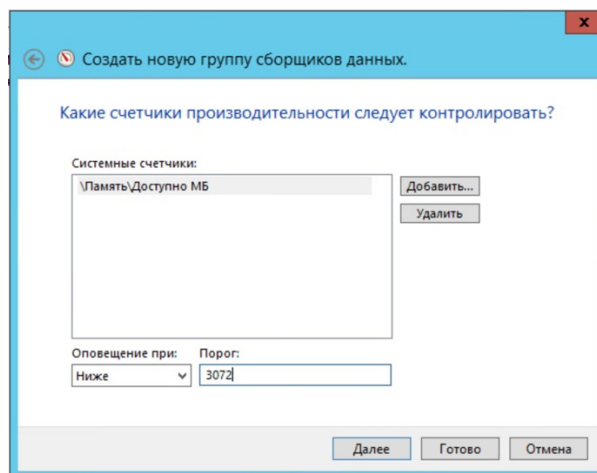
22. Настройте оповещение, если количество доступной памяти станет менее 3072 Мб.
а. Аналогично пункту 21 создайте группу сборщиков данных;



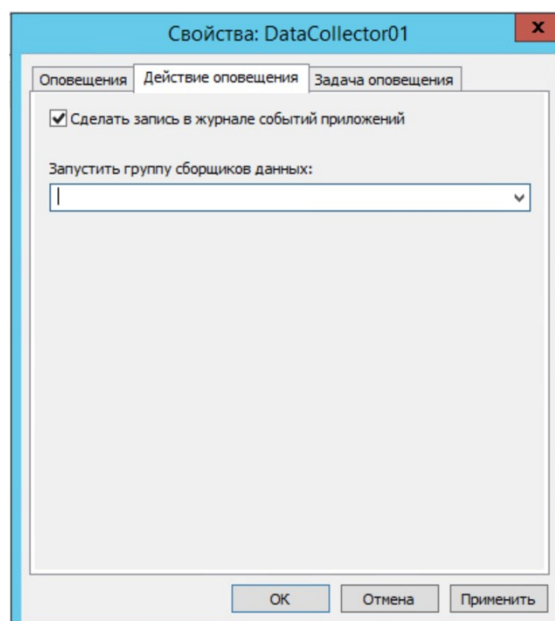
- б. выберете «Оповещение счетчика производительности»;



- с. добавьте счетчик Доступно МБ для объекта Память;
- д. введите в поле Порог значение, при котором должно срабатывать оповещение – 3072;

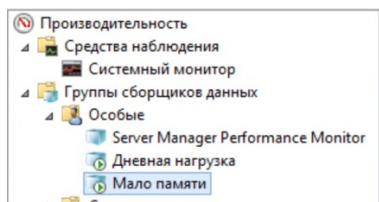


- е. Нажмите «Готово». Откройте свойства «DataCollector01» объекта «Мало памяти» и установите флаг «Сделать запись в журнале событий приложений».

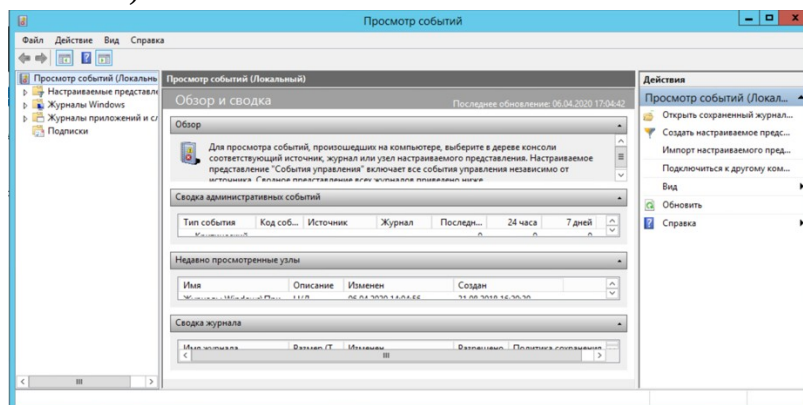


- ф. закройте диалоговое окно параметров нового журнала кнопкой «ОК».

g. в правой части окна нажмите «Пуск» на журнале «Мало памяти».

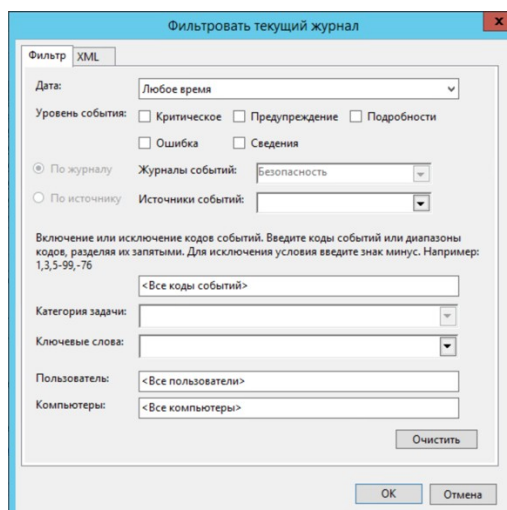


23. Откройте оснастку «Просмотр событий» («Диспетчер серверов» → «Средства» → «Просмотр событий»).



24. Просмотрите события Службы безопасности:

- перейдите в раздел «Журналы Windows» → «Безопасность» в левой части оснастки. Справа отобразятся все события данной службы;
- выполните фильтрацию событий только для компьютера «srvpod1.domain.local»:
 - откройте диалоговое окно «Фильтр текущего журнала» раздела Безопасность;

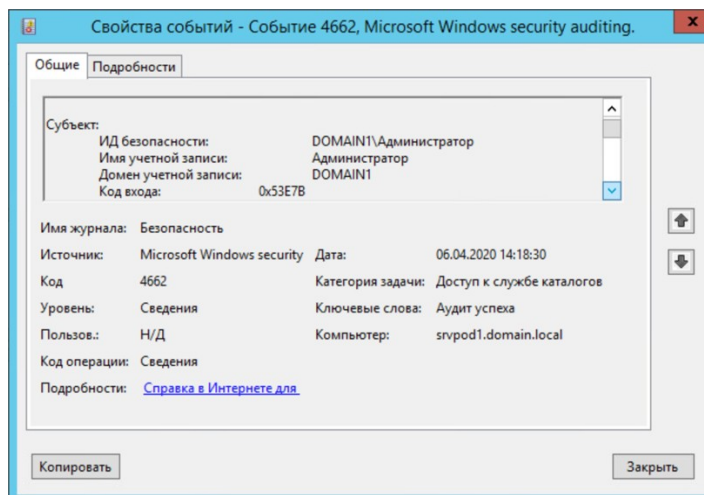


- введите в поле Компьютер имя компьютера, для которого необходимо отобразить события, например «srvpod1.domain.local»;
 - подтвердите применение фильтра кнопкой ОК.
- просмотрите событие «Доступ к службе каталогов»:
 - найдите указанное событие в правой части окна оснастки (код события – 4662);

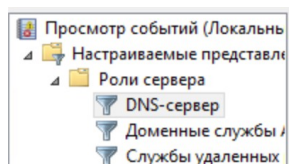
Отфильтровано: Журнал Security; Компьютер: srvpod1.domain.local; Источник: ; Код события: 4662; Событий: 86

Ключевые слова	Дата и время	Источник	Код события	Категория задачи
Аудит успеха	06.04.2020 17:19:36	Microsoft Wind...	4662	Доступ к службе каталогов
Аудит успеха	06.04.2020 16:19:36	Microsoft Wind...	4662	Доступ к службе каталогов
Аудит успеха	06.04.2020 15:19:36	Microsoft Wind...	4662	Доступ к службе каталогов
Аудит успеха	06.04.2020 14:18:38	Microsoft Wind...	4662	Доступ к службе каталогов
Аудит успеха	06.04.2020 14:18:38	Microsoft Wind...	4662	Доступ к службе каталогов
Аудит успеха	06.04.2020 14:18:37	Microsoft Wind...	4662	Доступ к службе каталогов
Аудит успеха	06.04.2020 14:18:37	Microsoft Wind...	4662	Доступ к службе каталогов
Аудит успеха	06.04.2020 14:18:30	Microsoft Wind...	4662	Доступ к службе каталогов

- ii. откройте диалоговое окно свойств выбранного события;
- iii. ознакомьтесь с информацией события, найдите имя компьютера к которому осуществлялся доступ;



- iv. закройте диалоговое окно события кнопкой «Закрыть»;
- v. снимите установленный ранее фильтр;
- d. Экспортируйте список событий для раздела DNS-сервер в текстовый файл:
 - i. активизируйте раздел DNS-сервер;



- ii. откройте диалоговое окно экспорта (Действие/Экспортировать ...);
- iii. введите имя файла в поле Имя;
- iv. сохраните файл кнопкой Сохранить;
- v. просмотрите сохраненный файл стандартной программой Блокнот

Отчет должен содержать

1. Титульный лист.
2. Текст задания.
3. Скриншоты выполненных действий по пунктам 6, 7, 8, 9, 14, 19, 21, 22, 24.
4. Выводы.