Лабораторная работа 7
МОНИТОРИНГ СОБЫТИЙ И ПРОИЗВОДИТЕЛЬНОСТЬ СИСТЕМЫ

Цель лабораторной работы

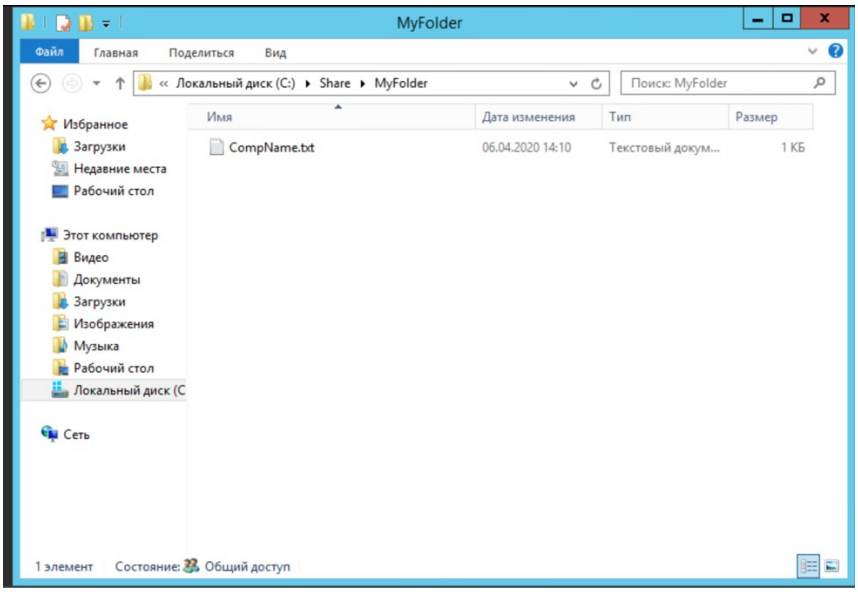
1. Изучить оснастку «Просмотр событий».
2. Ознакомиться с «Диспетчер задач».

Используемое программное обеспечение

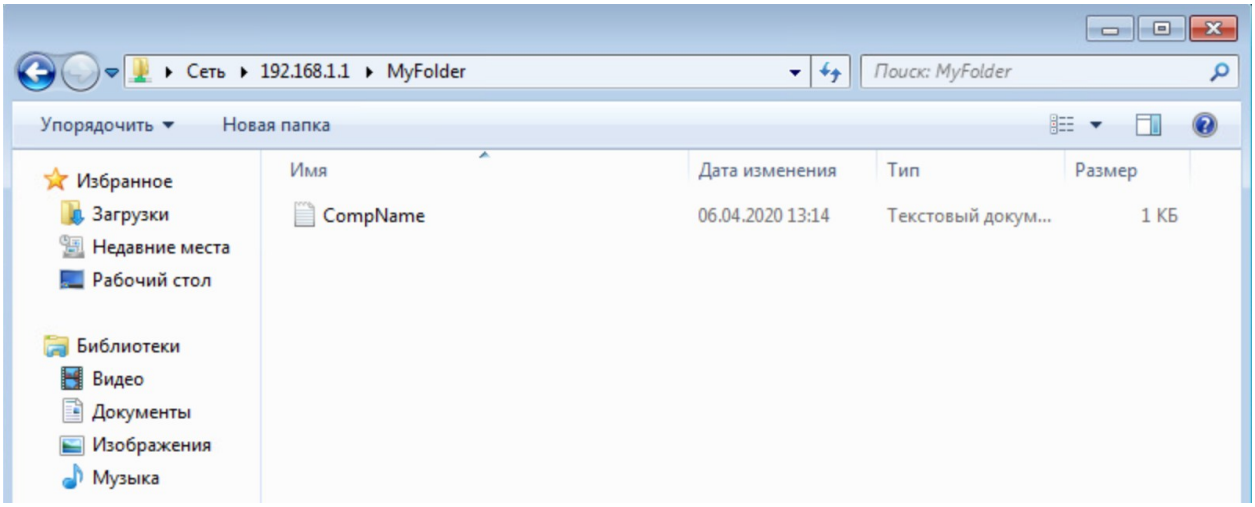
Для выполнения лабораторной работы используются ОС *Windows Server*.

Порядок выполнения работы

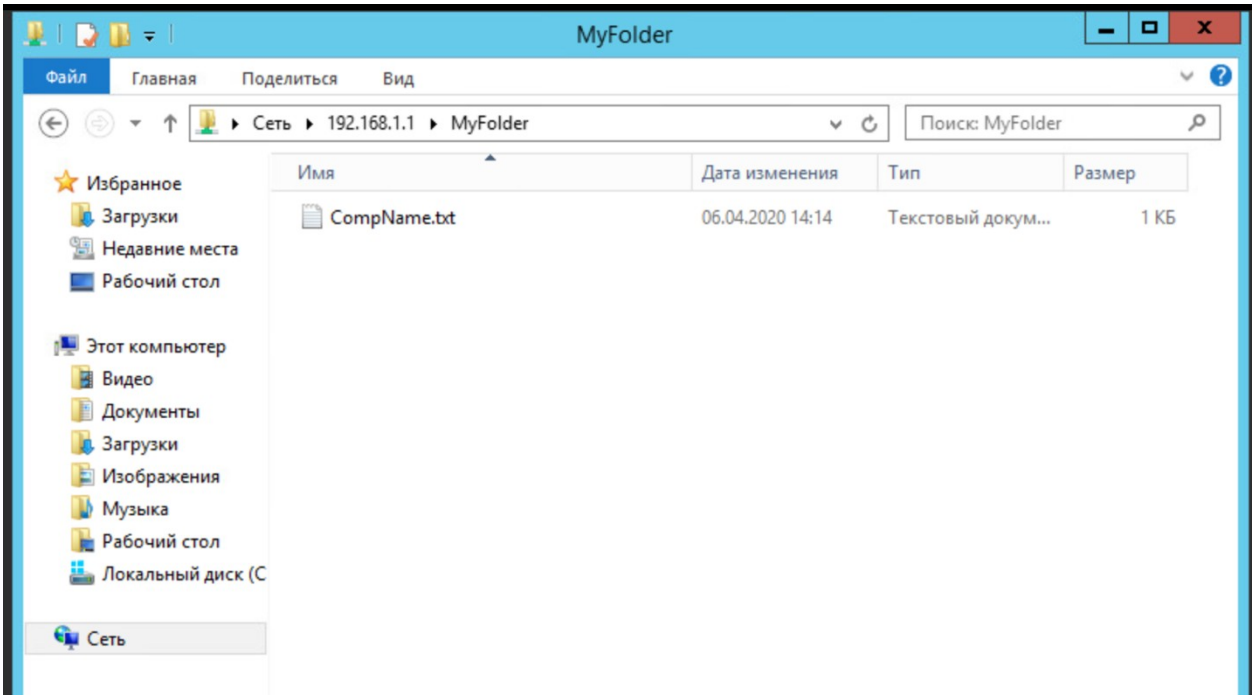
1. Войдите на *Windows Server*, в папке «Share» создайте папку «MyFolder» и разместите в ней документ с именем CompName.txt, содержащий сведения об IP-адресе и имени компьютера.



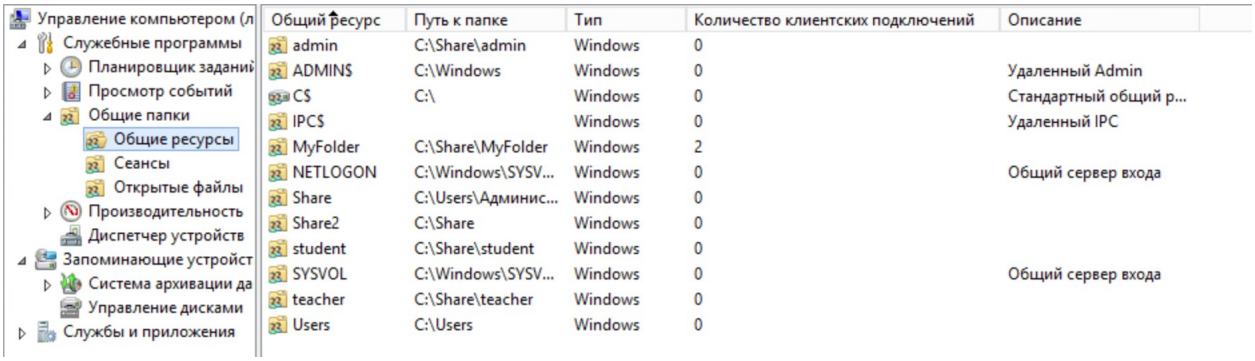
2. Откройте общий доступ к папке «MyFolder» для пользователей «Администратор» и «Student».
3. На *Windows Client* войдите пользователем «Student», перейдите в общую папку «MyFolder» и откройте файл «CompName.txt»



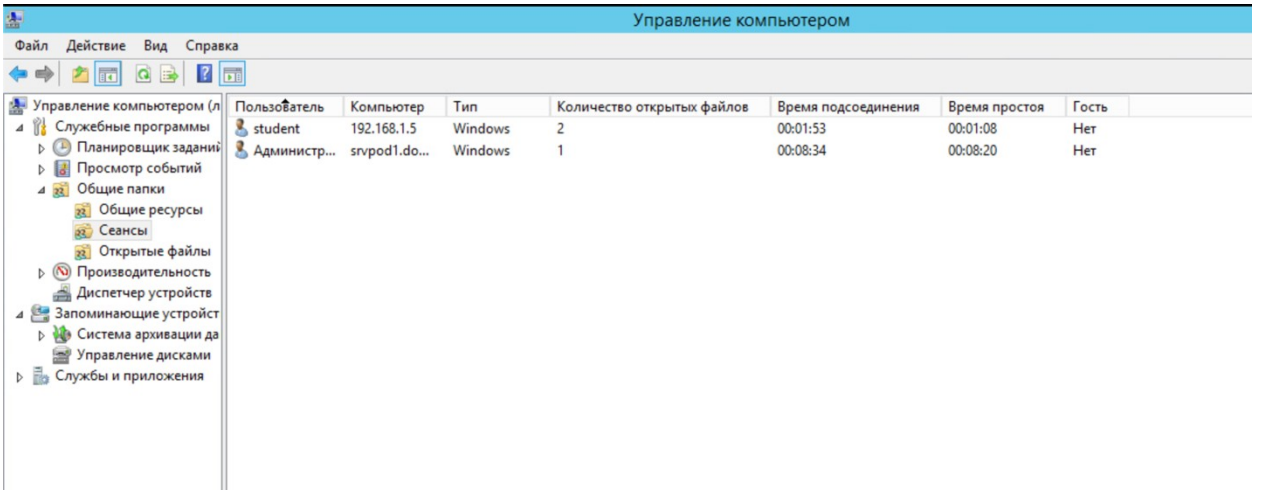
4. На *Windows Server* перейдите в общую папку «MyFolder» и откройте файл «CompName.txt».



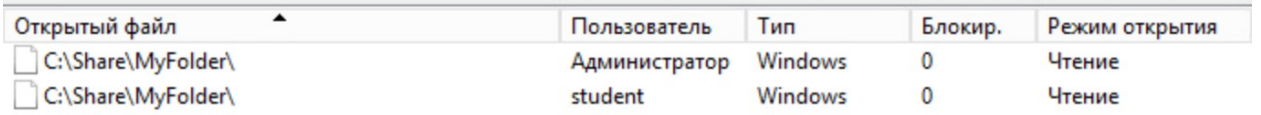
5. Перейдите на *Windows Server* и откройте оснастку «Управление компьютером» («Диспетчер серверов» → «Средства» → «Управление компьютером»).
6. Разверните раздел «Общие ресурсы». Здесь перечислены все опубликованные (общие) ресурсы вашего компьютера.



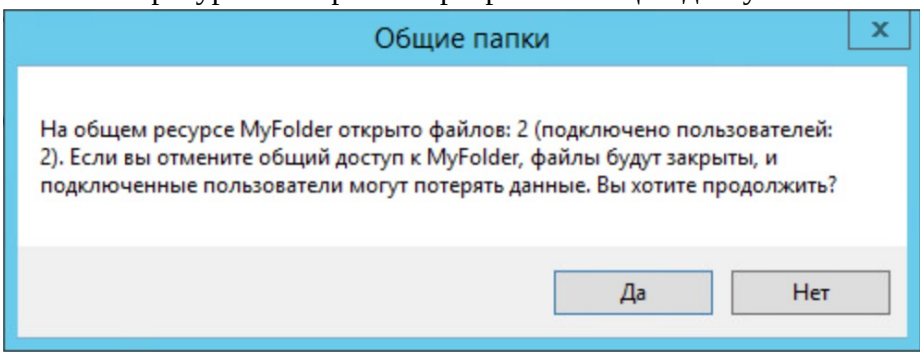
7. Откройте раздел «Сеансы». Здесь перечислены все открытые сеансы, т.е. какие пользователи и на каких компьютерах сейчас подключены к вашему компьютеру. Если вызвать контекстное меню раздела, то можно сразу отключить все сеансы.



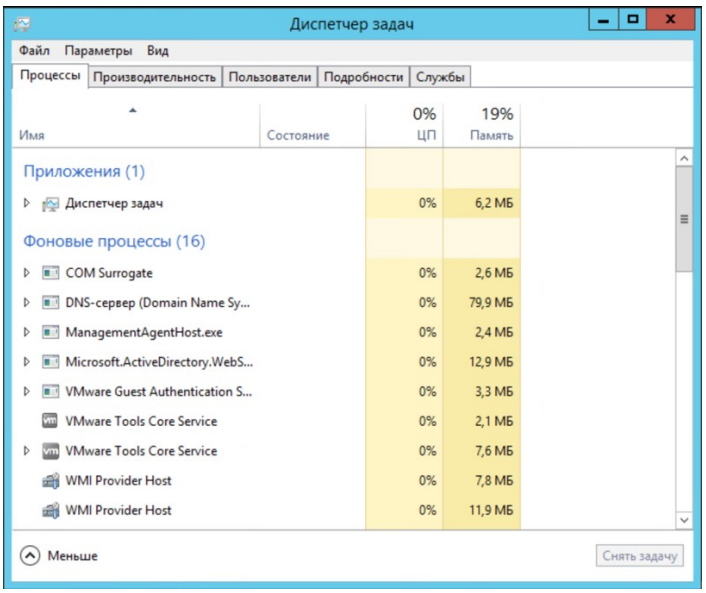
8. Закройте открытый файл. Для этого перейдите в раздел «Открытые файлы» и в контекстном меню файла выберите «Закрыть открытый файл».



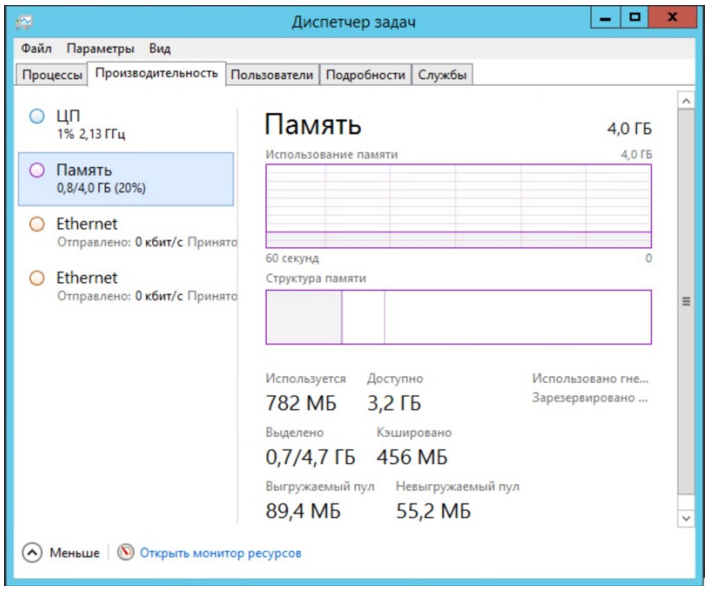
9. Отключите общий доступ к созданному ранее ресурсу «MyFolder». Для этого в контекстном меню ресурса выберите «Прекратить общий доступ».



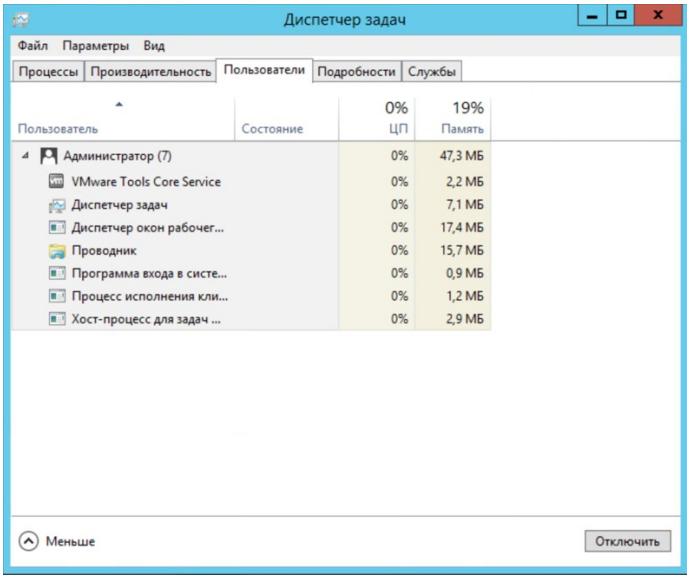
10. На *Windows Server* просмотрите информацию о производительности системы: о откройте окно диспетчера задач (CTRL+SHIFT+ESC). Нажмите «Подробнее».



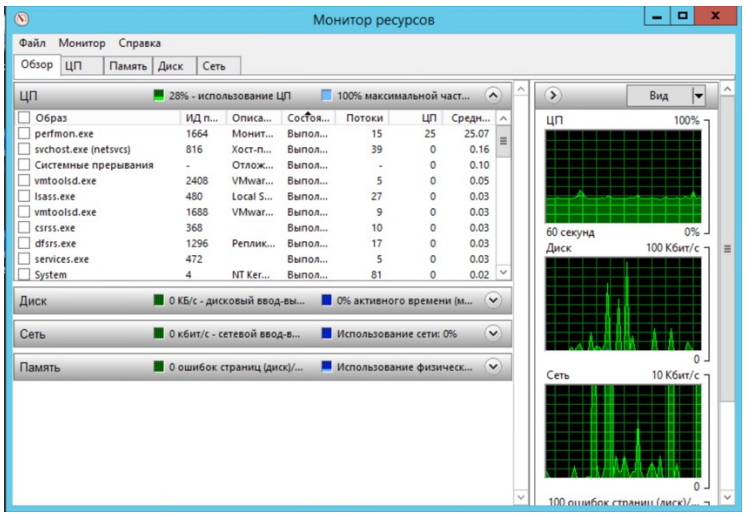
11. Перейдите на вкладку «Процессы», просмотрите список и найдите процесс использующий наибольшее количество памяти.
12. Перейдите на вкладку «Производительность» и посмотрите количество выделенной памяти в соответствующем поле и ознакомьтесь с информацией о производительности сети.



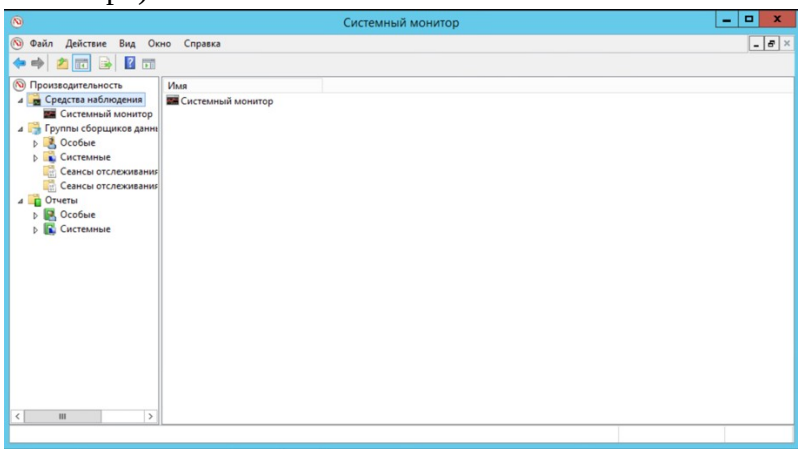
13. Перейдите на вкладку «Пользователи» просмотрите информацию о пользователях, зарегистрированных в системе.



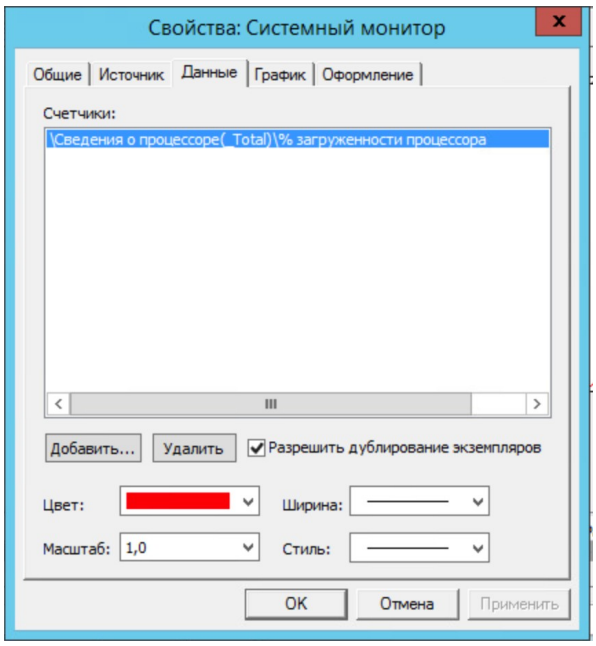
14. Соберите с помощью «Монитор ресурсов» информацию, указанную ниже:
    a. Количество запущенных приложений.
    b. Имя процесса, занимающего больше всех оперативной памяти. Количество выделенной памяти.
    c. Имя процесса, большего всех обращается к диску.



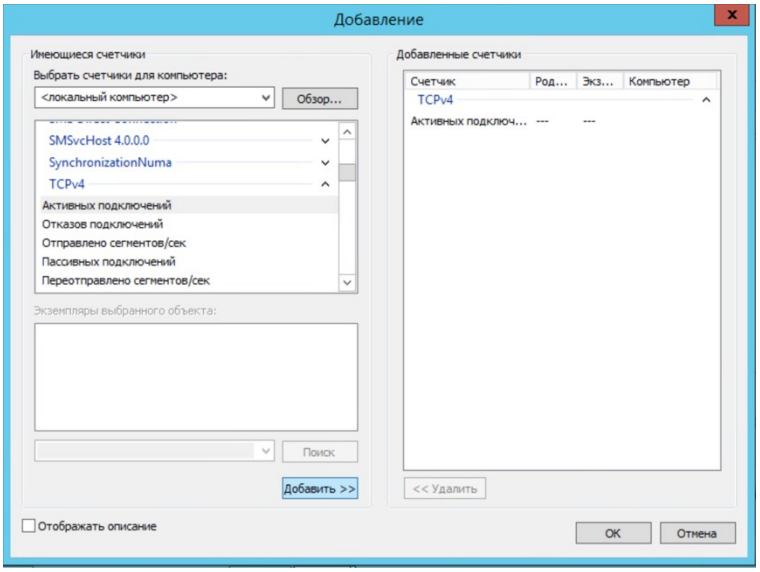
15. Запустите оснастку «Системный монитор» («Диспетчер серверов» → «Средства» → «Системный монитор»).

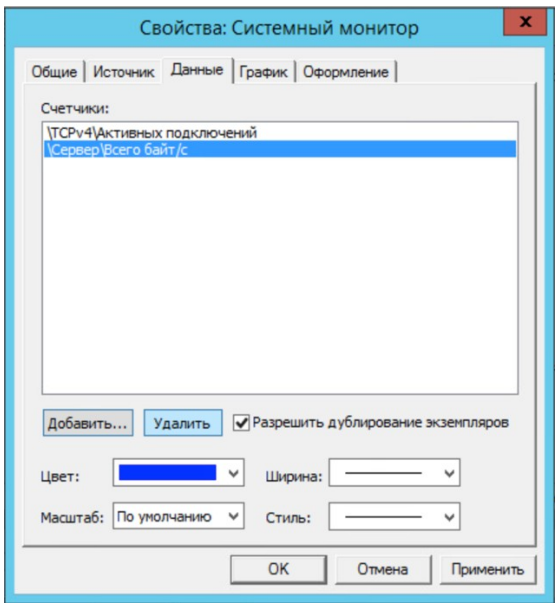


16. Удалите все счетчики из системного монитора:
    a. активируйте «Системный монитор»;
    b. откройте диалоговое окно свойств «Системного монитора» кнопкой «Свойства»;
    c. перейдите на вкладку Данные;
    d. выделите один из счетчиков и удалите его кнопкой Удалить;
    e. аналогично удалите все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

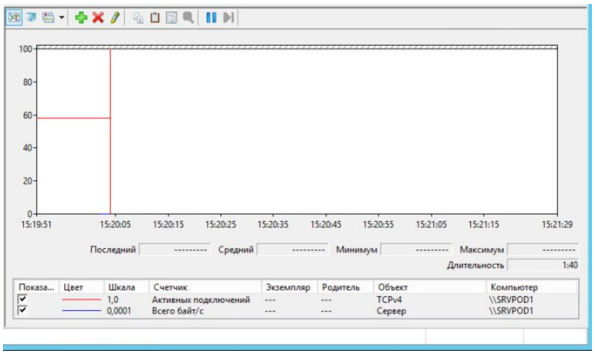


17. Добавьте счетчик активных подключений TCP:
    a. активируйте добавление счетчика кнопкой Добавить;
    b. выберите в раскрывающемся списке Объект – TCPv4;
    c. выберите в списке Выбрать счетчик из списка – Активных подключений;
    d. добавьте счетчик кнопкой Добавить.
    e. самостоятельно добавьте счетчик Всего байт/сек для объекта Сервер;
    f. закройте окно добавления счетчиков кнопкой Закрыть.

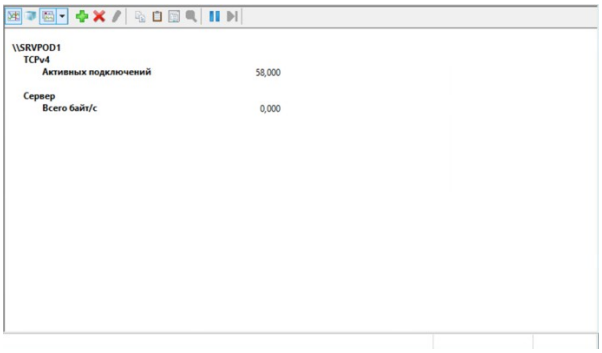




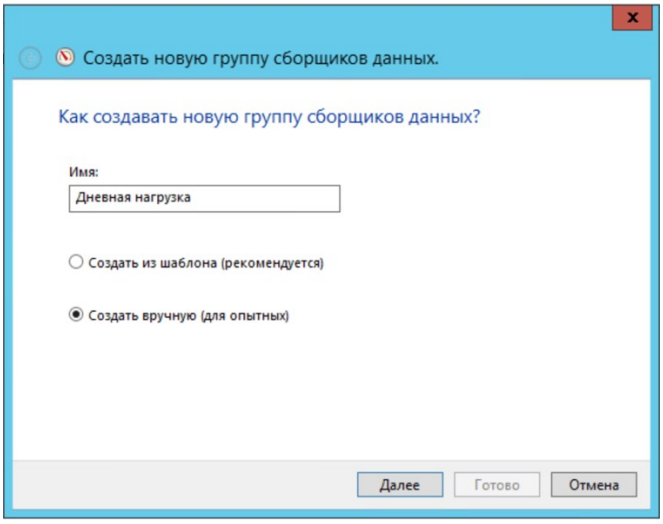
18. Закройте диалоговое окно свойств «Системного монитора» кнопкой «ОК».
19. В правой области начнет отображаться информация добавленных счетчиков в графическом виде.



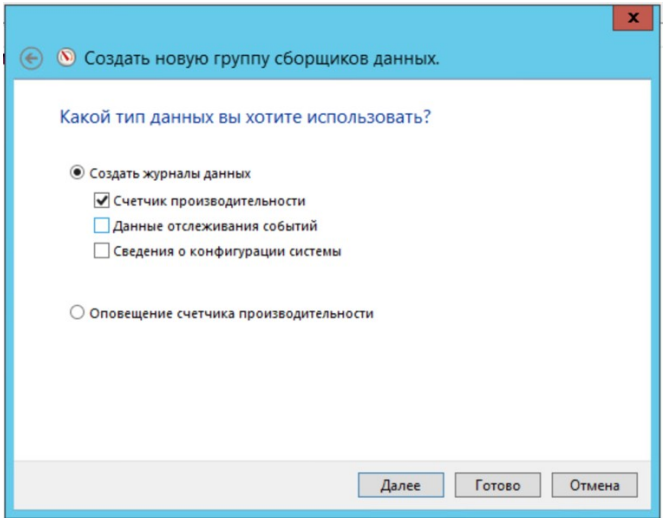
20. Переключите вид отображения информации счетчиков в текстовый вид кнопкой «Изменить тип диаграммы» на панели инструментов.



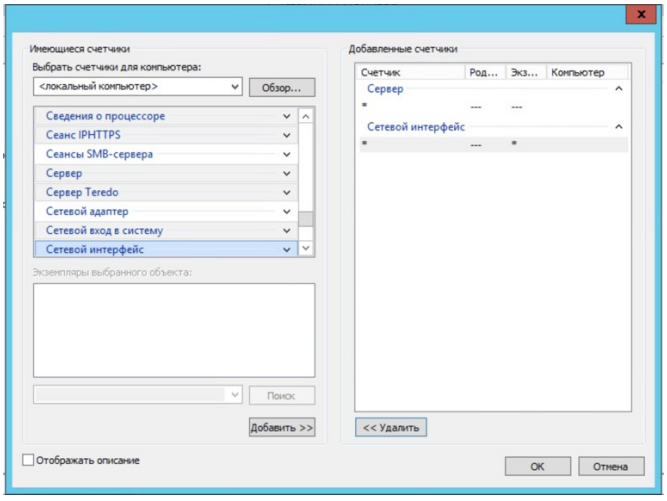
21. Настройте автоматический сбор информации о загруженности сервера в период с 8.00:
    a. активируйте раздел «Группы сборщиков данных» → «Особые» в левой части окна «Производительность»;
    b. активируйте создание новых параметров журнала («Действие» → «Создать» → «Группа сборщиков данных»);
   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



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

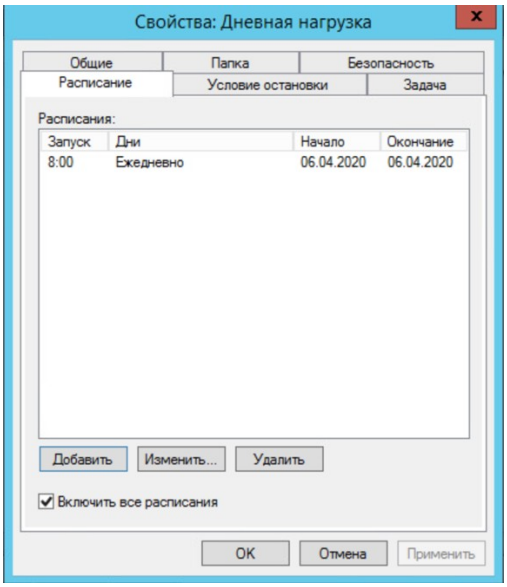


e. откройте окно добавления объектов кнопкой Добавить объект;
f. выделите в списке Объект – Сервер;
g. добавьте объект кнопкой Добавить;
h. аналогично добавьте объект Сетевой интерфейс;
i. закройте окно добавления объектов кнопкой «ОК»;



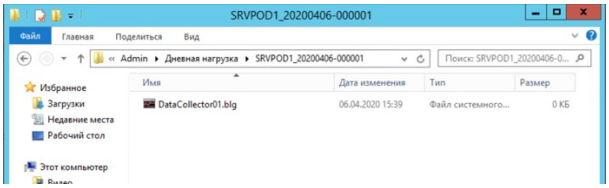
j. нажмите «Готово». Откройте «Свойства» объекта «Дневная нагрузка».

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



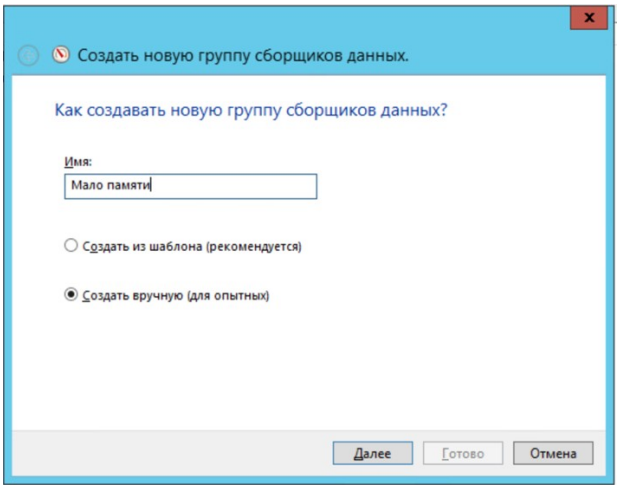
l. закройте диалоговое окно параметров нового журнала кнопкой «OK».

m. в правой части окна нажмите «Пуск» на журнале «Дневная нагрузка». Просмотреть результат работы журнала можно в папке «C:\perflogs».

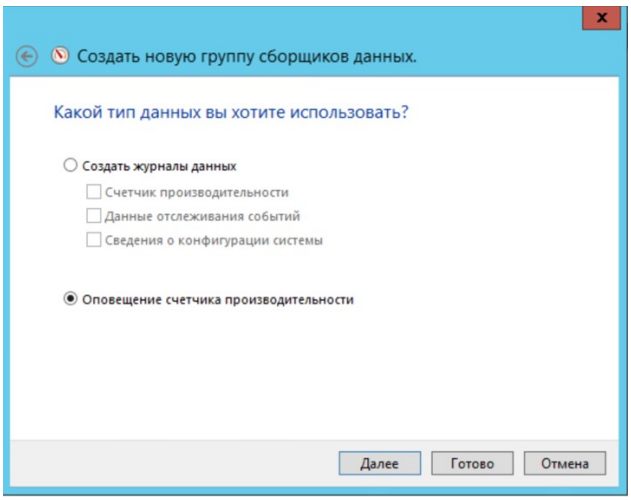


22. Настройте оповещение, если количество доступной памяти станет менее 3072 Мб.

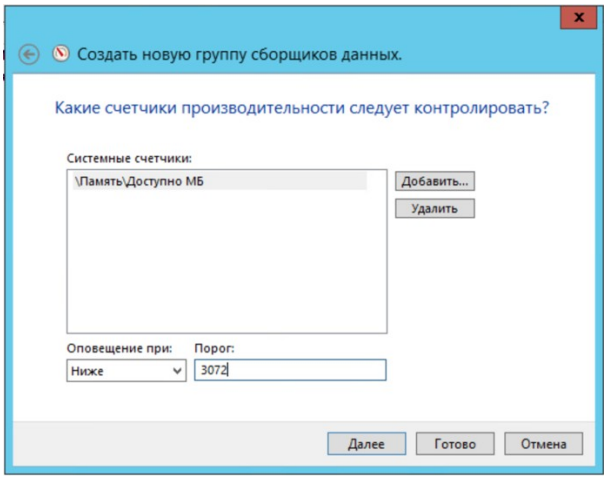
a. Аналогично пункту 21 создайте группу сборщиков данных;



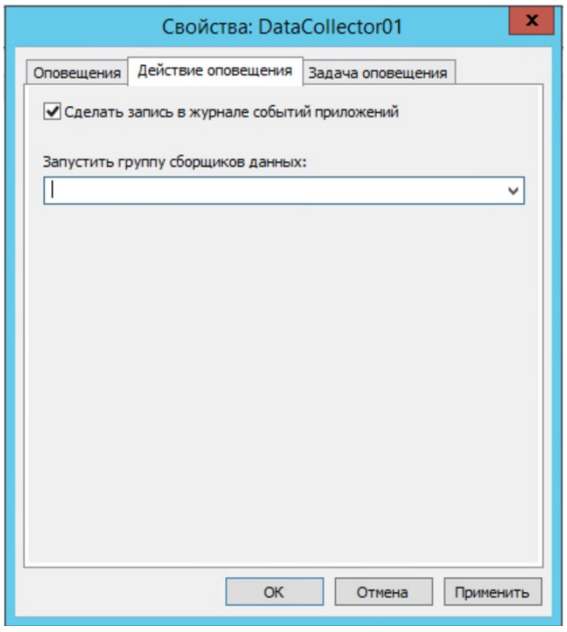
b. выберете «Оповещение счетчика производительности»;



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

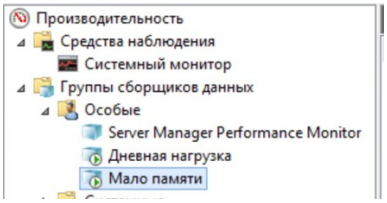


e. Нажмите «Готово». Откройте свойства «DataCollector01» объекта «Мало памяти» и установите флаг «Сделать запись в журнале событий приложений».

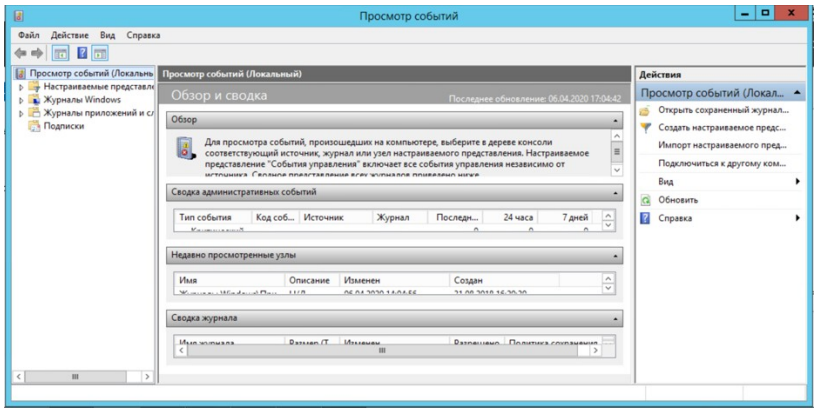


f. закройте диалоговое окно параметров нового журнала кнопкой «OK».

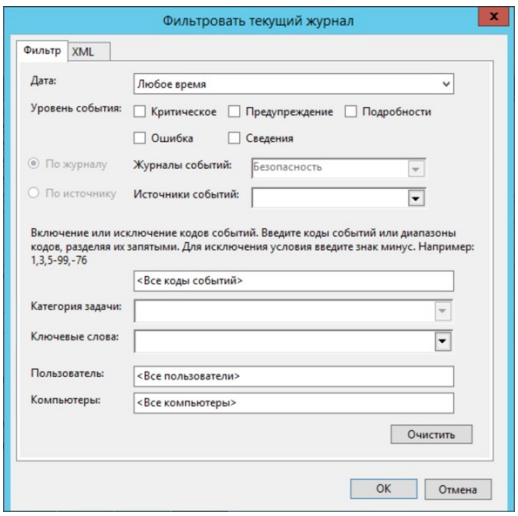
g. в правой части окна нажмите «Пуск» на журнале «Мало памяти».



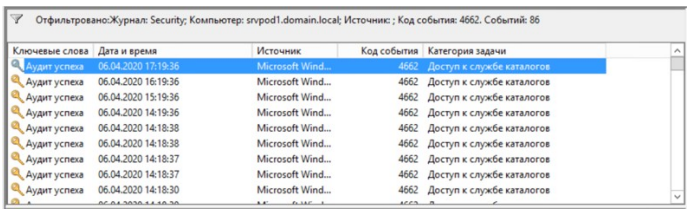
23. Откройте оснастку «Просмотр событий» («Диспетчер серверов» → «Средства» → «Просмотр событий»).



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



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



ii. откройте диалоговое окно свойств выбранного события;

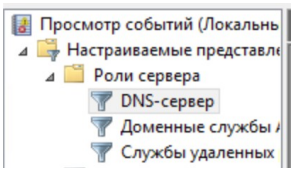
iii. ознакомьтесь с информацией события, найдите имя компьютера к которому осуществлялся доступ;

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.