**Лабораторная работа 7**

**мониторинг событий и производительность системы**

**Цель лабораторной работы**

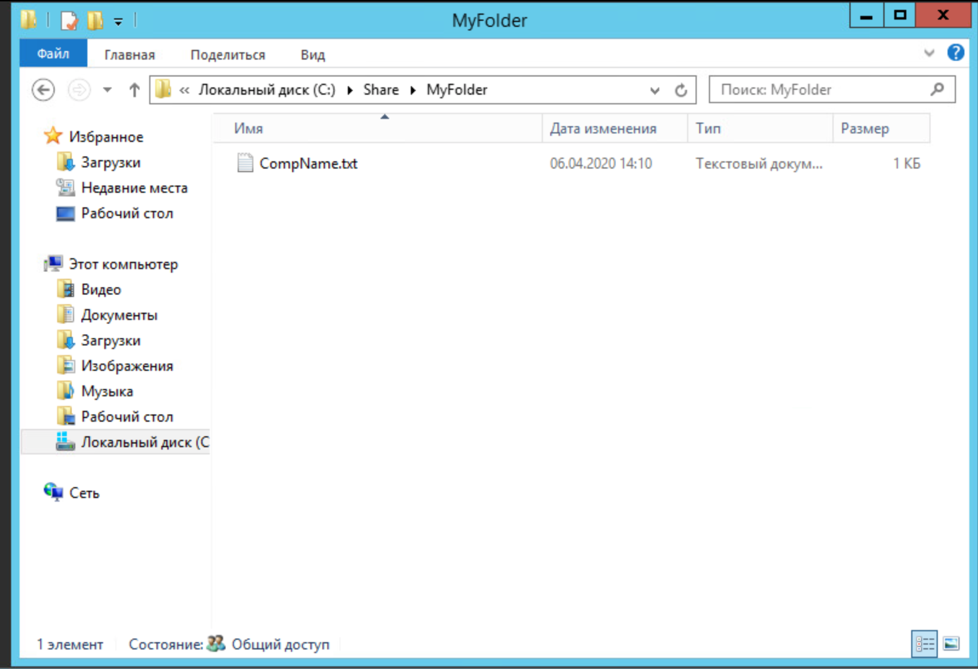
1. Изучить оснастку «Просмотр событий».
2. Ознакомиться с «Диспетчер задач».

**Используемое программное обеспечение**

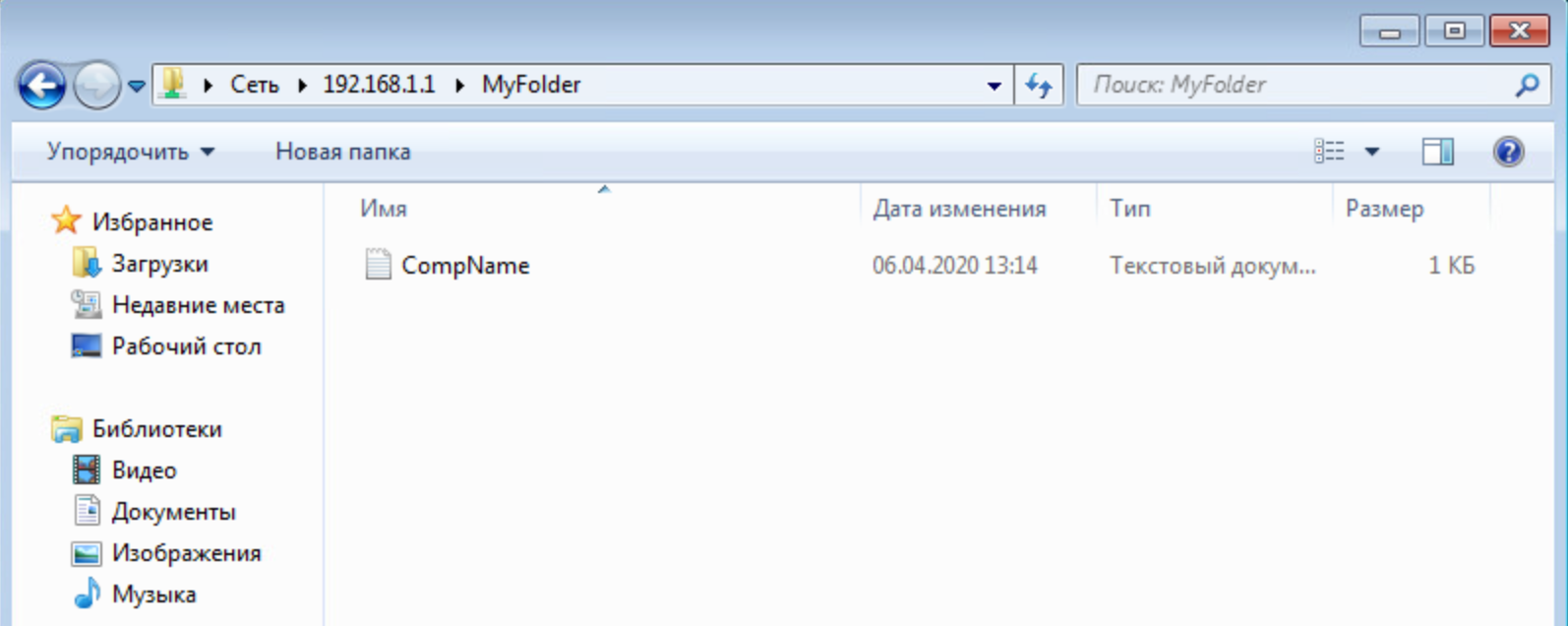
Для выполнения лабораторной работы используются ОС *Windows Server*.

**Порядок выполнения работы**

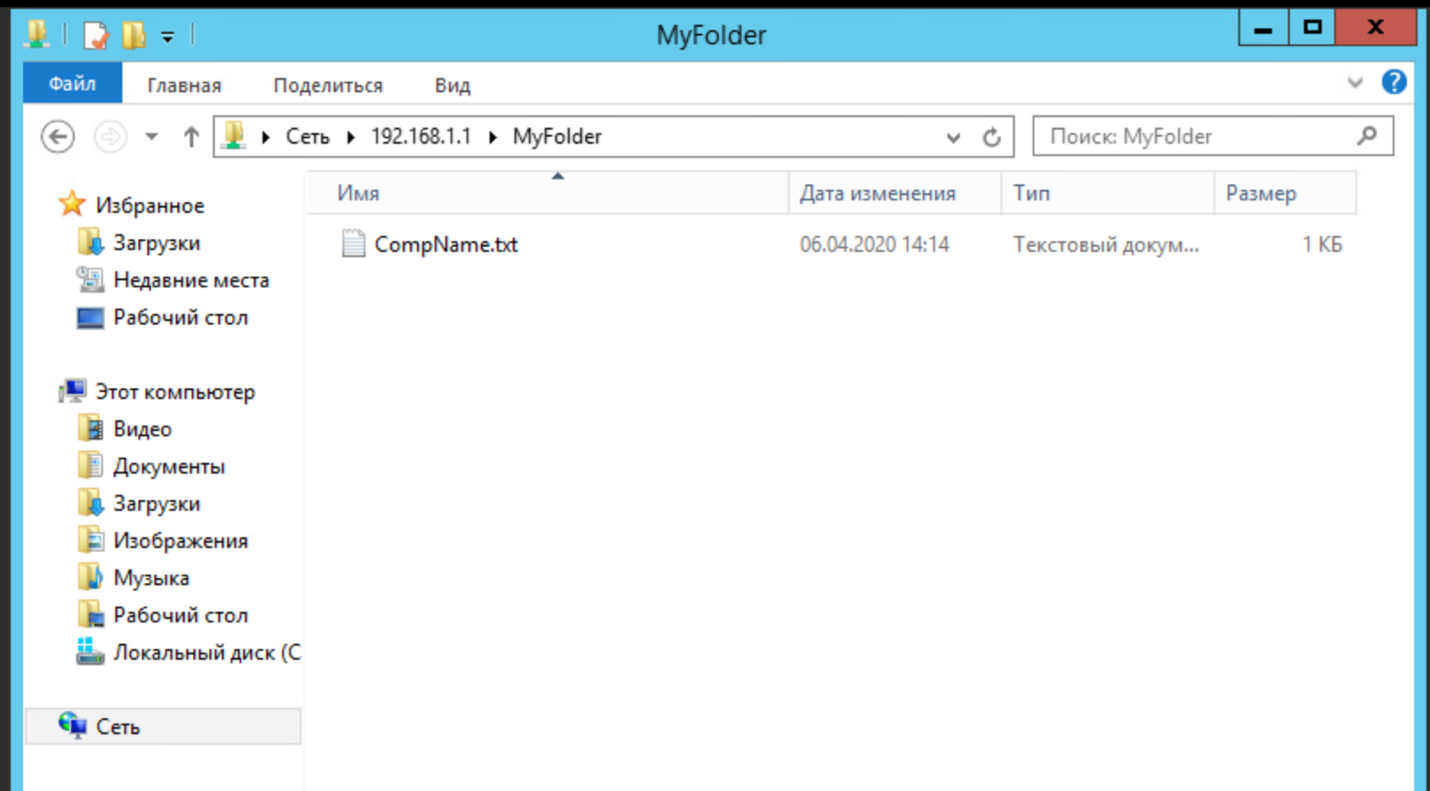
1. Войдите на *Windows Server*, в папке «Share» создайте папку «MyFolder» и разместите в ней документ с именем CompName.txt, содержащий сведения об IP-адресе и имени компьютера.



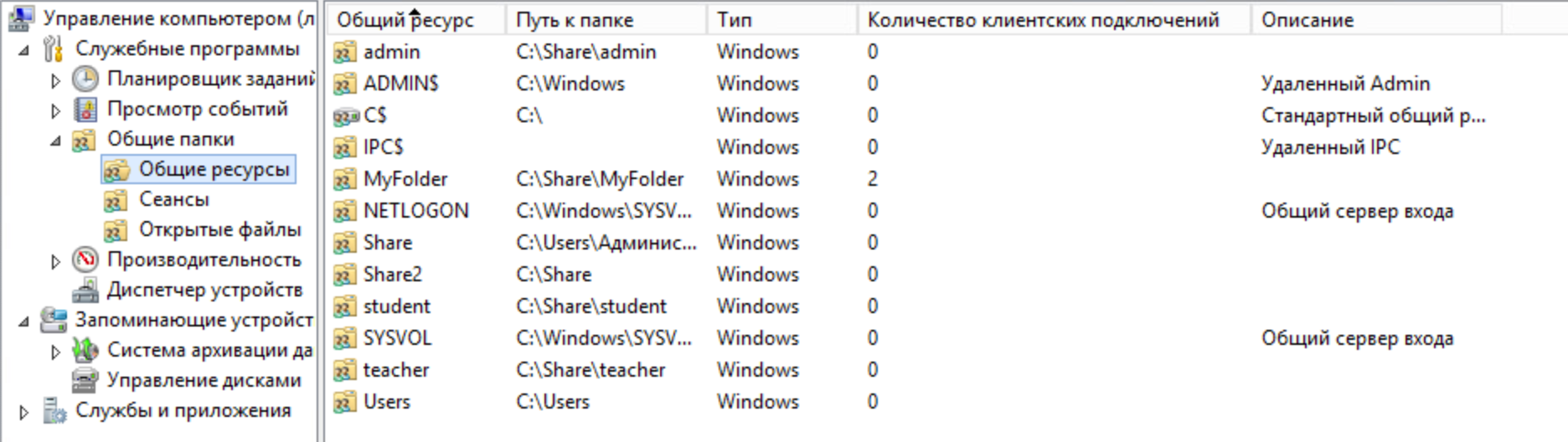
1. Откройте общий доступ к папке «MyFolder» для пользователей «Администратор» и «Student».
2. На *Windows Client* войдите пользователем «Student», перейдите в общую папку «MyFolder» и откройте файл «CompName.txt»



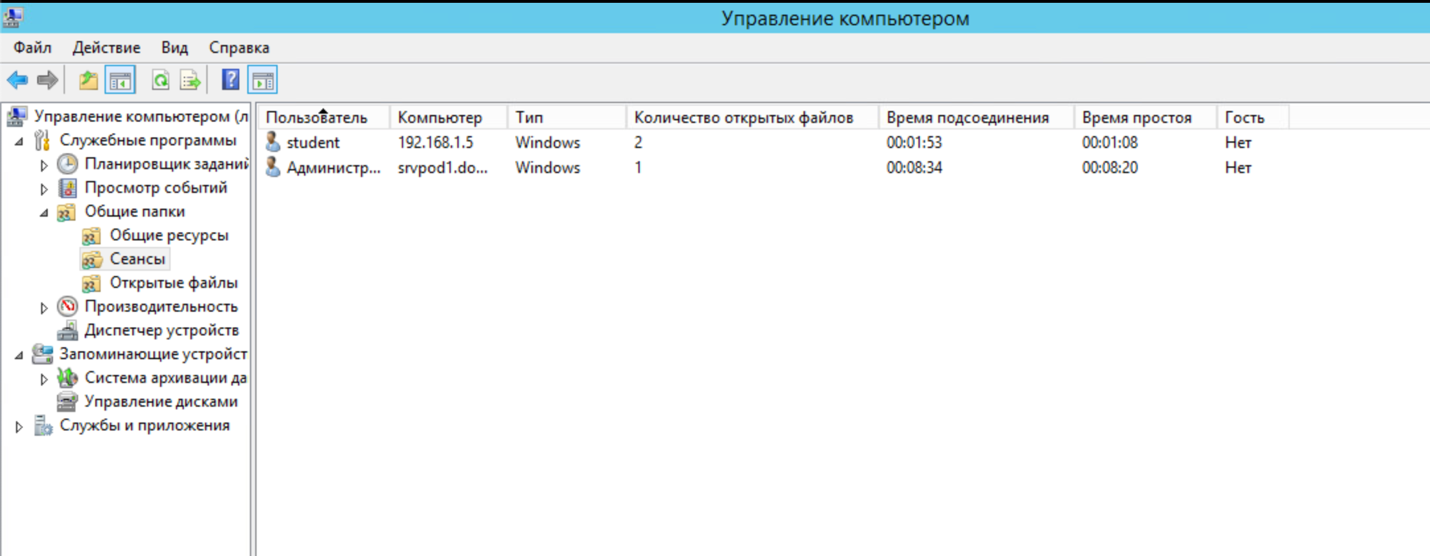
1. На *Windows Server* перейдите в общую папку «MyFolder» и откройте файл «CompName.txt».



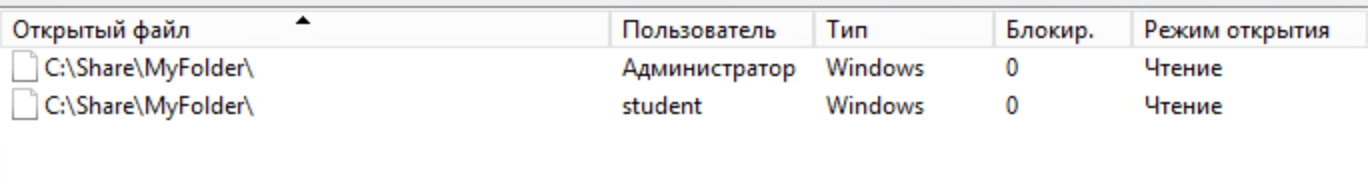
1. Перейдите на *Windows Server* и откройте оснастку «Управление компьютером» («Диспетчер серверов» → «Средства» → «Управление компьютером»).
2. Разверните раздел «Общие ресурсы». Здесь перечислены все опубликованные (общие) ресурсы вашего компьютера.



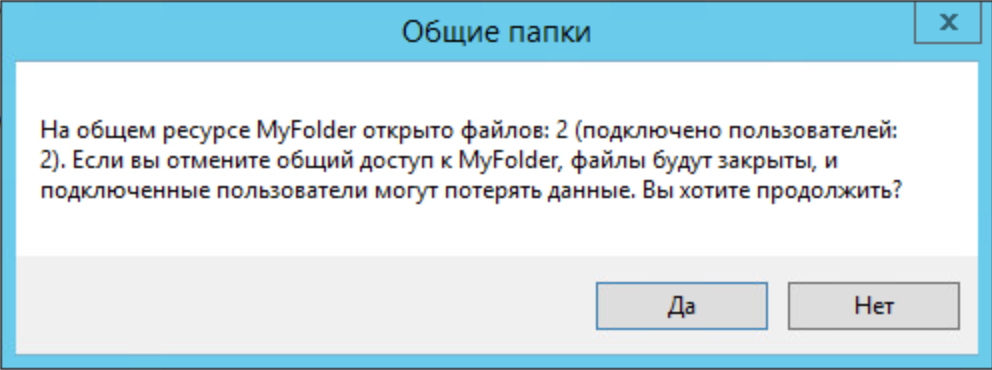
1. Откройте раздел «Сеансы». Здесь перечислены все открытые сеансы, т.е. какие пользователи и на каких компьютерах сейчас подключены к вашему компьютеру. Если вызвать контекстное меню раздела, то можно сразу отключить все сеансы.



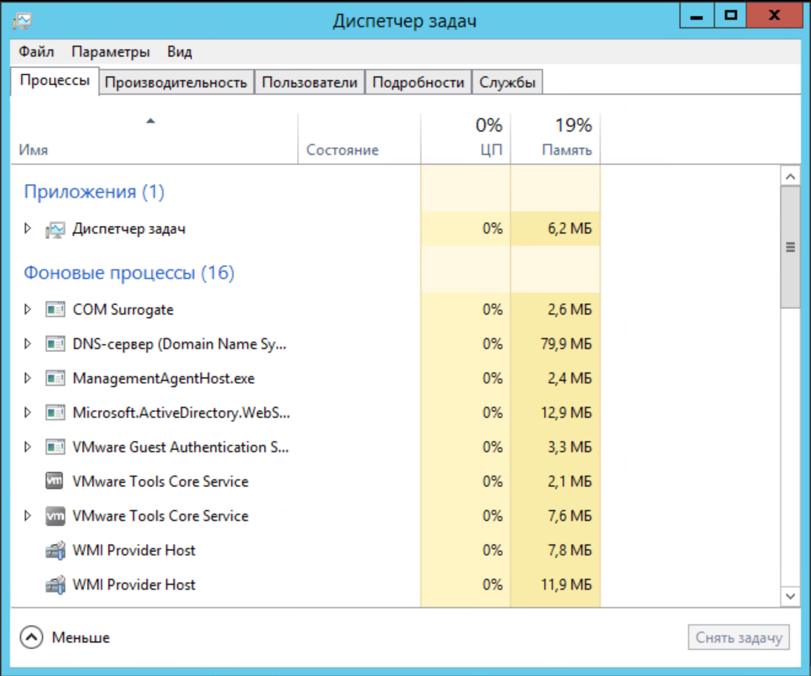
1. Закройте открытый файл. Для этого перейдите в раздел «Открытые файлы» и в контекстном меню файла выберите «Закрыть открытый файл».



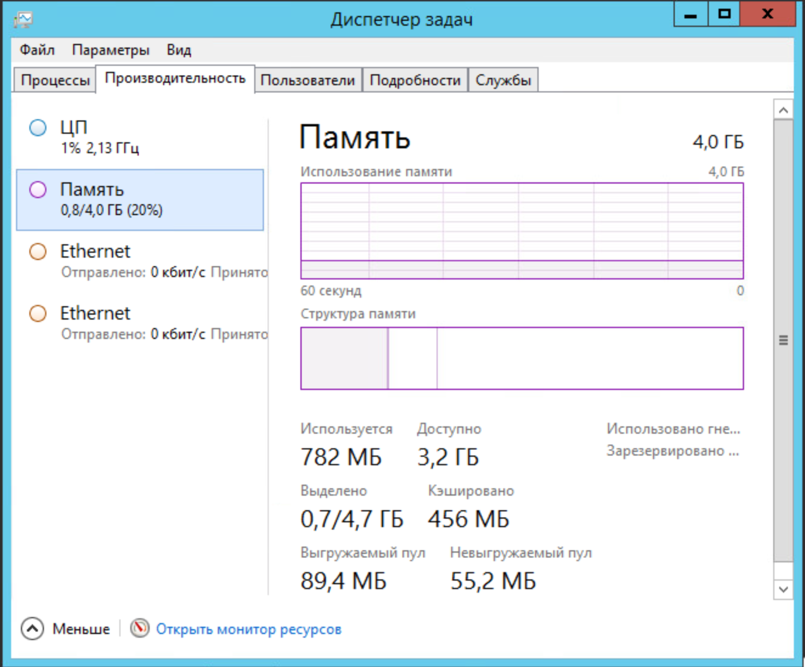
1. Отключите общий доступ к созданному ранее ресурсу «MyFolder». Для этого в контекстном меню ресурса выберите «Прекратить общий доступ».



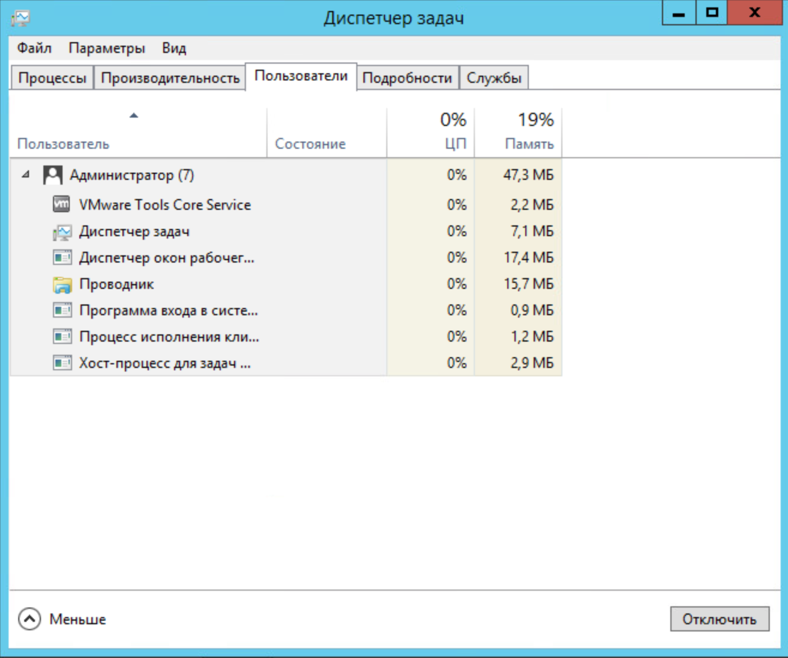
1. На *Windows Server* просмотрите информацию о производительности системы: o откройте окно диспетчера задач (CTRL+SHIFT+ESC). Нажмите «Подробнее».



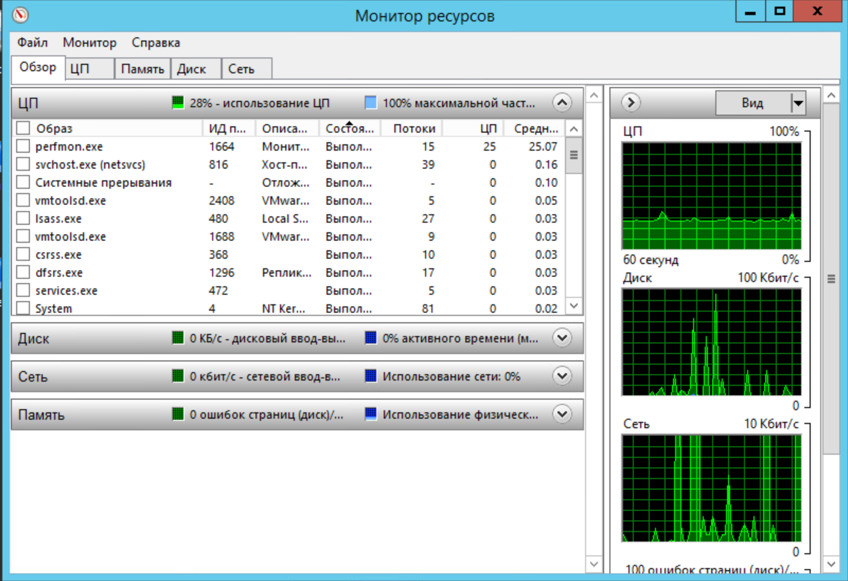
1. Перейдите на вкладку «Процессы», просмотрите список и найдите процесс использующий наибольшее количество памяти.
2. Перейдите на вкладку «Производительность» и посмотрите количество выделенной памяти в соответствующем поле и ознакомьтесь с информацией о производительности сети.



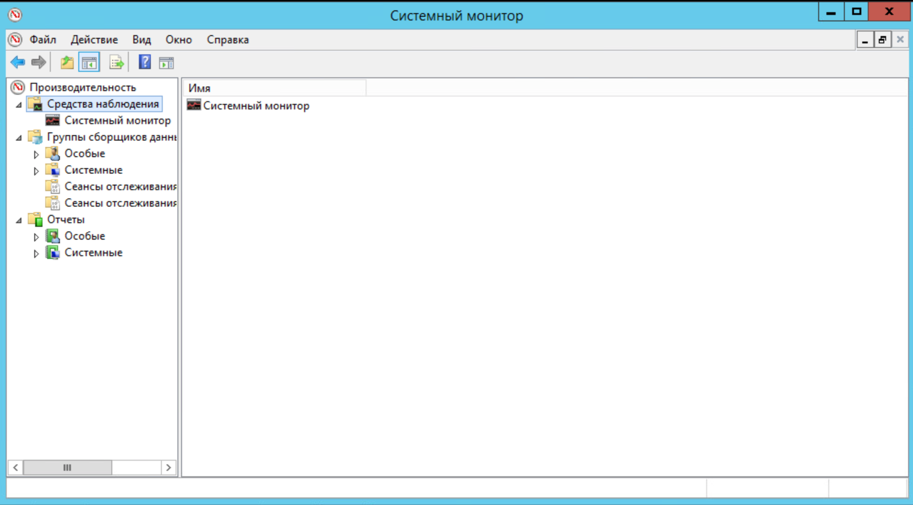
1. Перейдите на вкладку «Пользователи» просмотрите информацию о пользователях, зарегистрированных в системе.



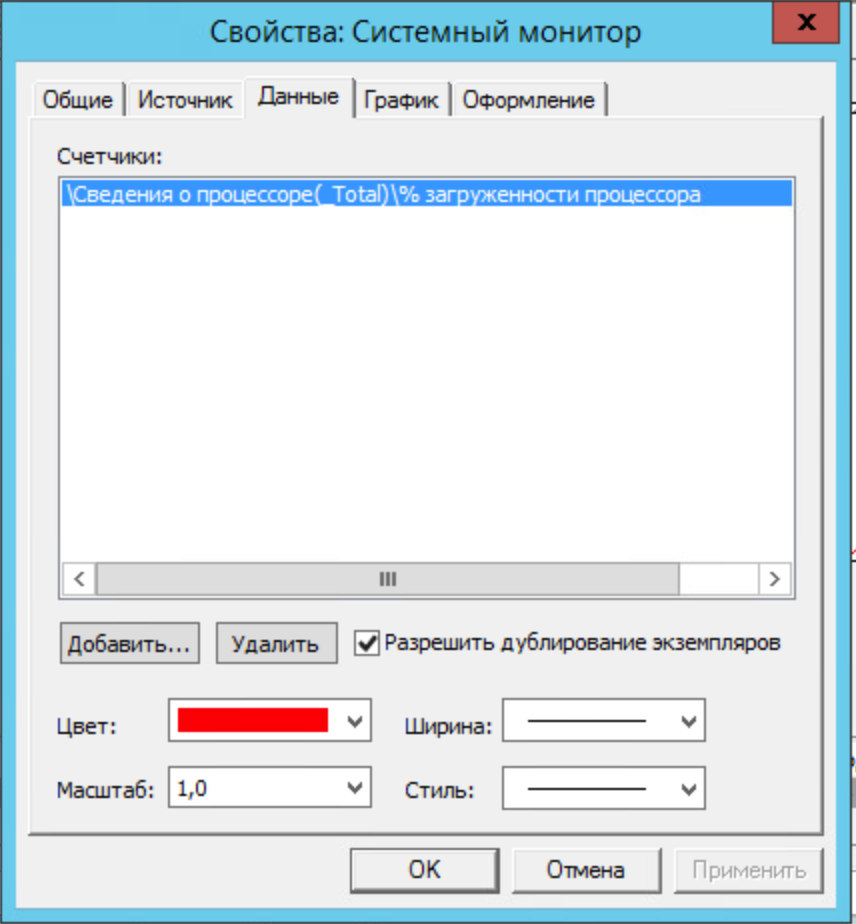
1. Соберите с помощью «Монитор ресурсов» информацию, указанную ниже:
   1. Количество запущенных приложений.
   2. Имя процесса, занимающего больше всех оперативной памяти. Количество выделенной памяти.
   3. Имя процесса, большего всех обращается к диску.



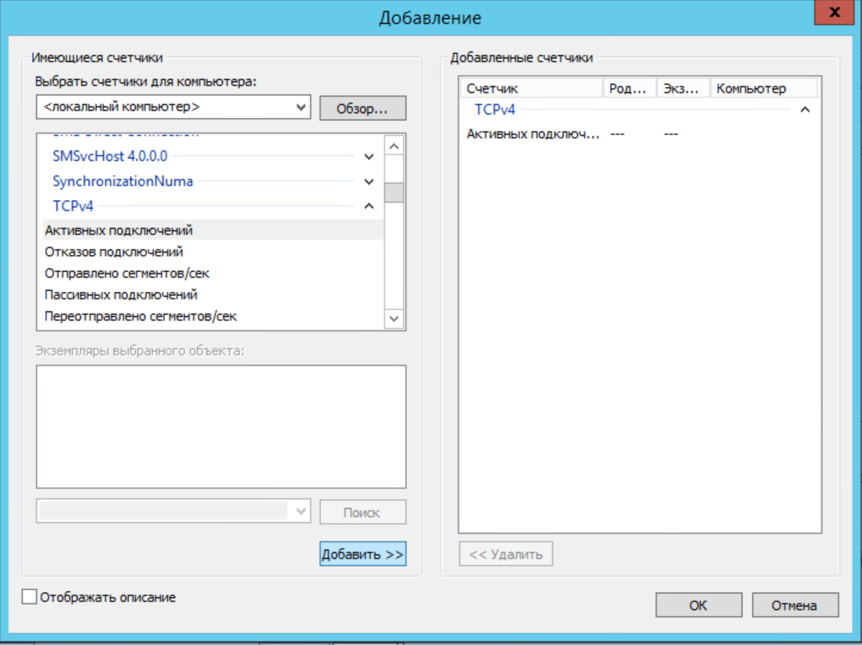
1. Запустите оснастку «Системный монитор» («Диспетчер серверов» → «Средства» → «Системный монитор»).

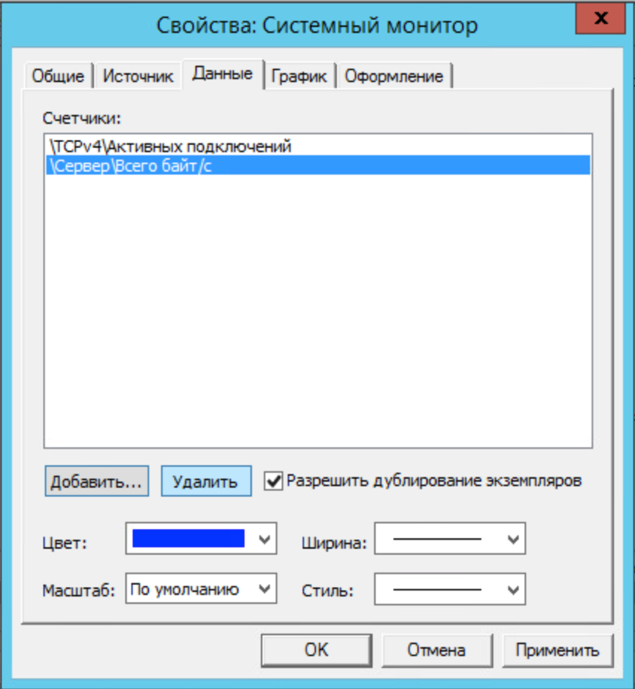


1. Удалите все счетчики из системного монитора:
   1. активируйте «Системный монитор»;
   2. откройте диалоговое окно свойств «Системного монитора» кнопкой «Свойства»;
   3. перейдите на вкладку Данные;
   4. выделите один из счетчиков и удалите его кнопкой Удалить;
   5. аналогично удалите все остальные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

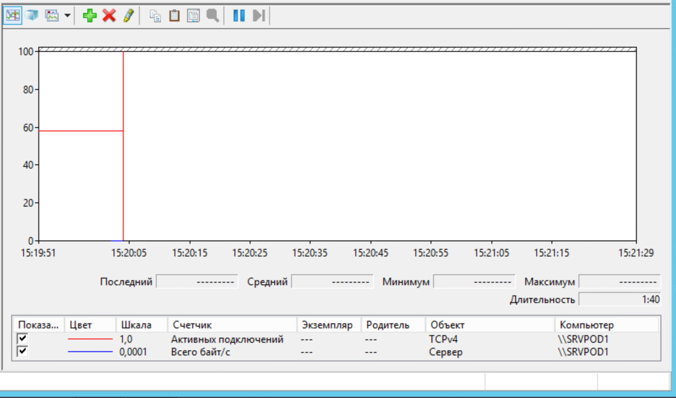


1. Добавьте счетчик активных подключений TCP:
   1. активируйте добавление счетчика кнопкой Добавить;
   2. выберите в раскрывающемся списке Объект – TCPv4;
   3. выберите в списке Выбрать счетчик из списка – Активных подключений;
   4. добавьте счетчик кнопкой Добавить.
   5. самостоятельно добавьте счетчик Всего байт/сек для объекта Сервер;
   6. закройте окно добавления счетчиков кнопкой Закрыть.

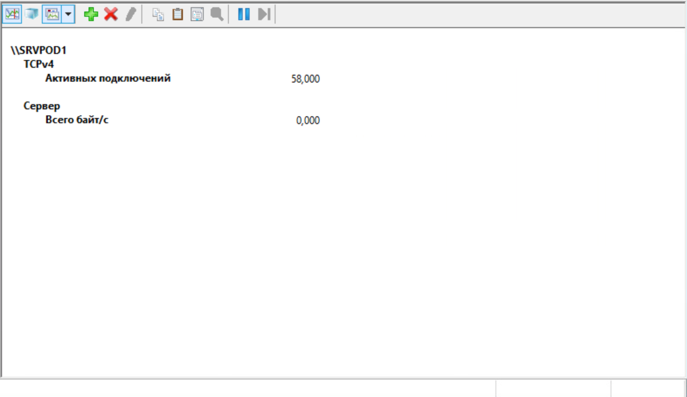




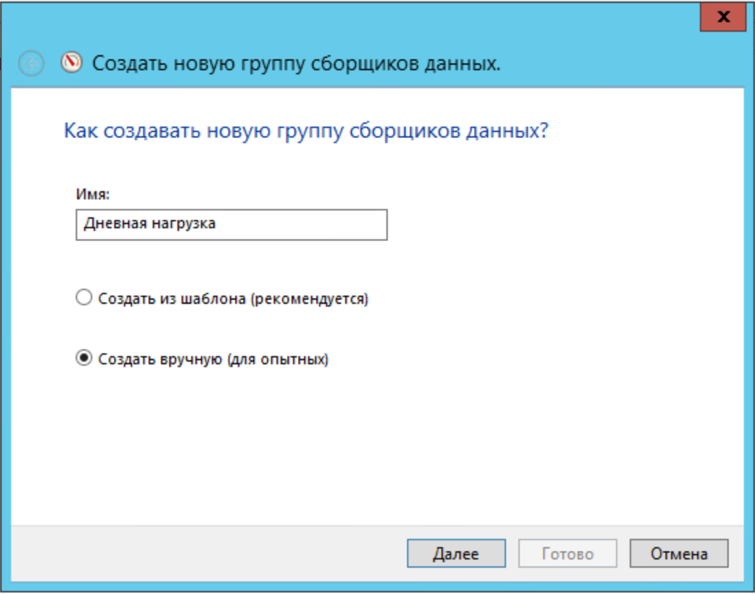
1. Закройте диалоговое окно свойств «Системного монитора» кнопкой «ОК».
2. В правой области начнет отображаться информация добавленных счетчиков в графическом виде.



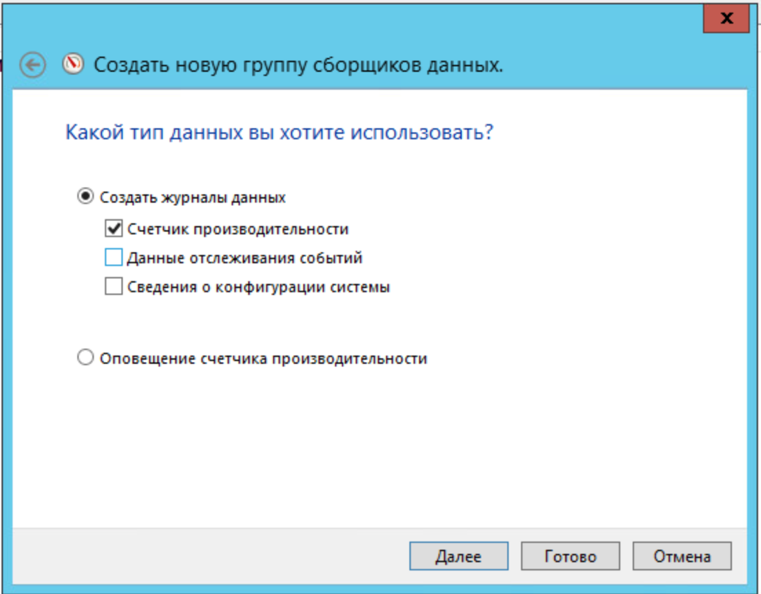
1. Переключите вид отображения информации счетчиков в текстовый вид кнопкой «Изменить тип диаграммы» на панели инструментов.



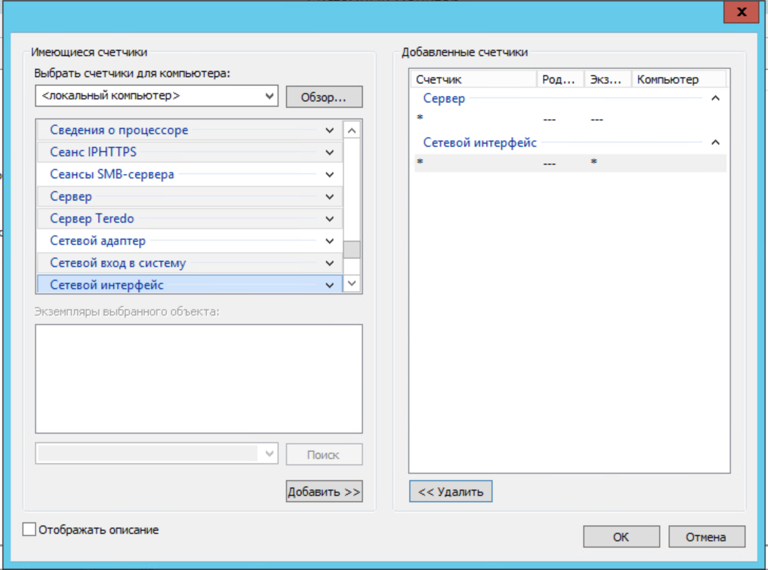
1. Настройте автоматический сбор информации о загруженности сервера в период с 8.00:
   1. активируйте раздел «Группы сборщиков данных» → «Особые» в левой части окна «Производительность»;
   2. активируйте создание новых параметров журнала («Действие» → «Создать» → «Группа сборщиков данных»);
   3. введите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



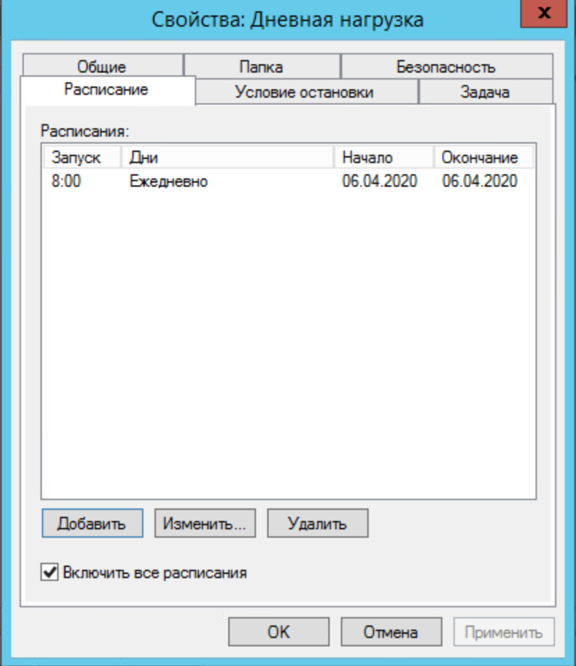
* 1. выберете «Создать журнал данных» → «Счетчик производительности». Нажмите «Далее»;



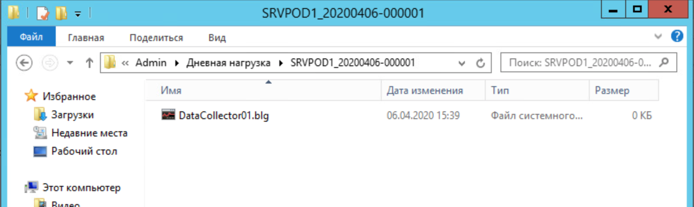
* 1. откройте окно добавления объектов кнопкой Добавить объект;
  2. выделите в списке Объект – Сервер;
  3. добавьте объект кнопкой Добавить;
  4. аналогично добавьте объект Сетевой интерфейс;
  5. закройте окно добавления объектов кнопкой «ОК»;



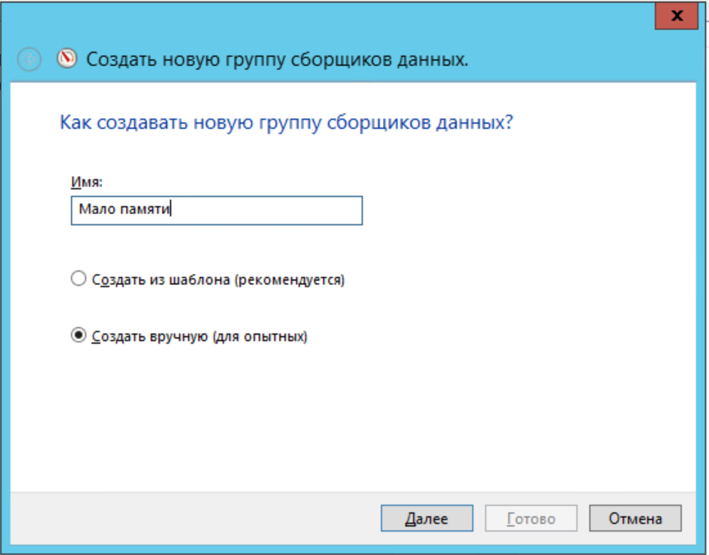
* 1. нажмите «Готово». Откройте «Свойства» объекта «Дневная нагрузка».
  2. перейдите на вкладку «Расписание». Установите в поле Время – 8.00;



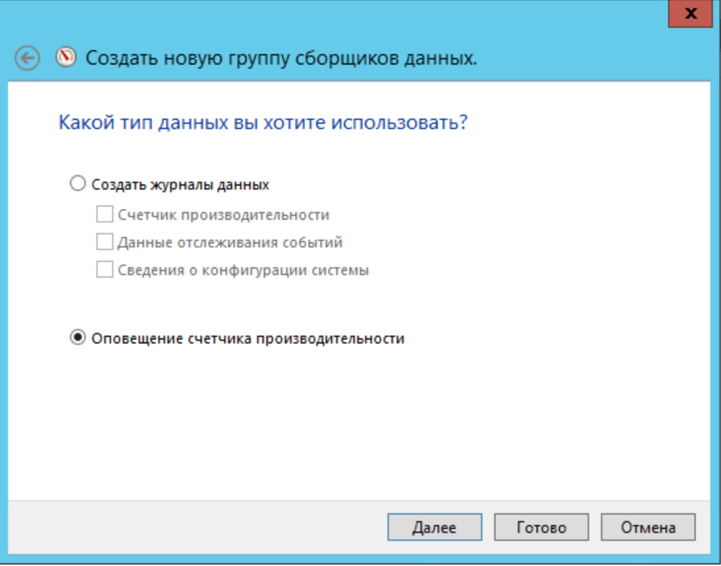
* 1. закройте диалоговое окно параметров нового журнала кнопкой «ОК».
  2. в правой части окна нажмите «Пуск» на журнале «Дневная нагрузка». Просмотреть результат работы журнала можно в папке «C:\perflogs».



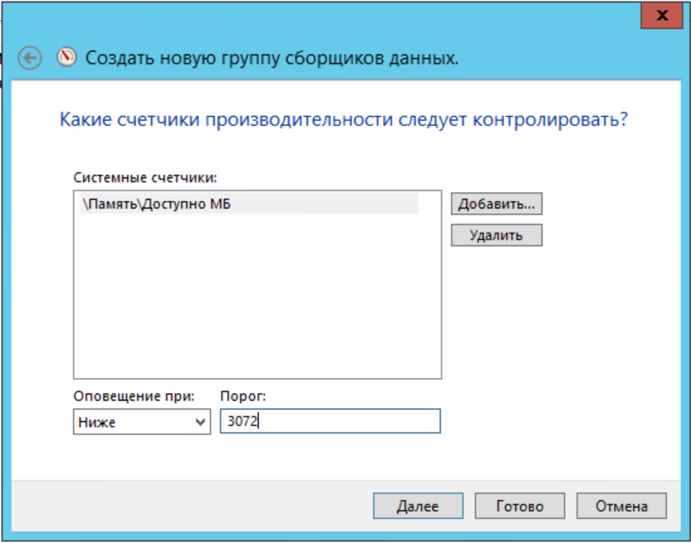
1. Настройте оповещение, если количество доступной памяти станет менее 3072 Мб.
   1. Аналогично пункту 21 создайте группу сборщиков данных;



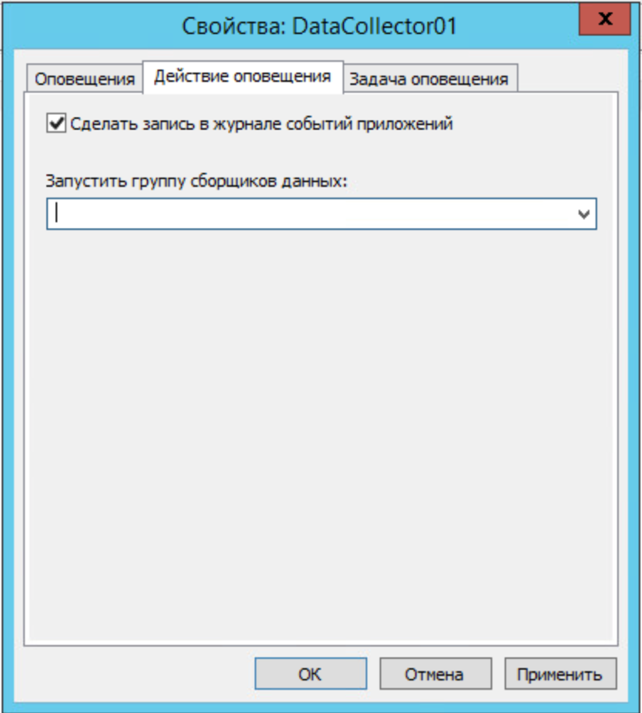
* 1. выберете «Оповещение счетчика производительности»;



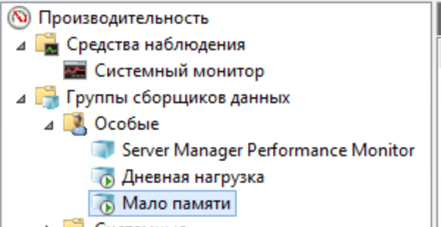
* 1. добавьте счетчик Доступно МБ для объекта Память;
  2. введите в поле Порог значение, при котором должно срабатывать оповещение – 3072;



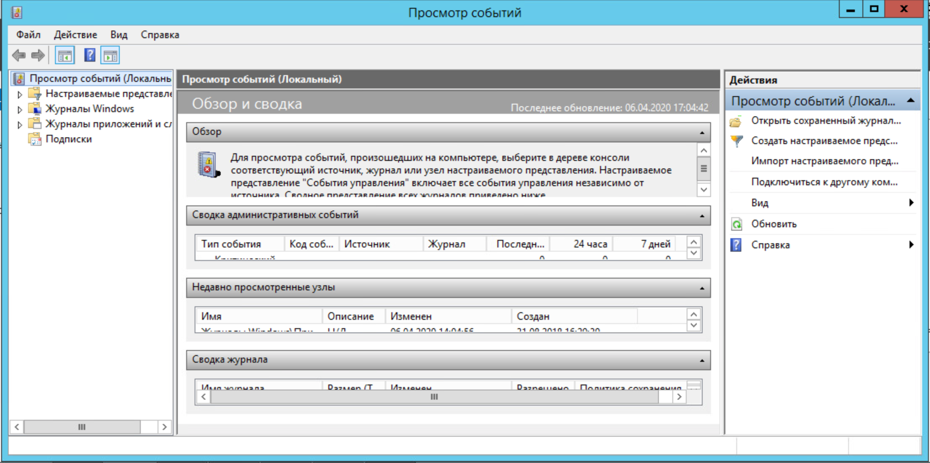
* 1. Нажмите «Готово». Откройте свойства «DataCollector01» объекта «Мало памяти» и установите флаг «Сделать запись в журнале событий приложений».



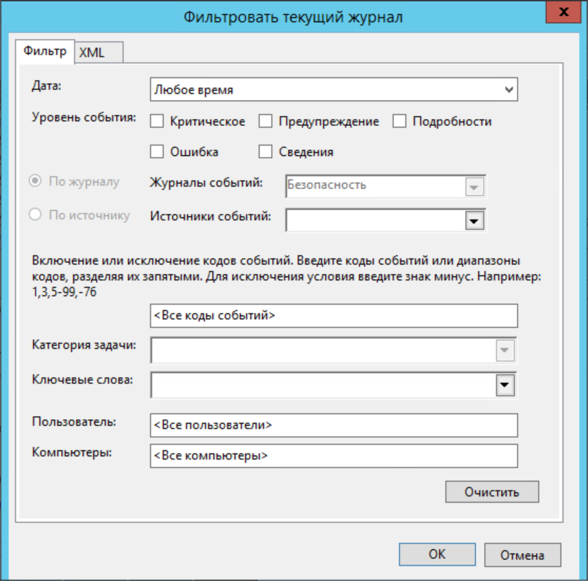
* 1. закройте диалоговое окно параметров нового журнала кнопкой «ОК».
  2. в правой части окна нажмите «Пуск» на журнале «Мало памяти».



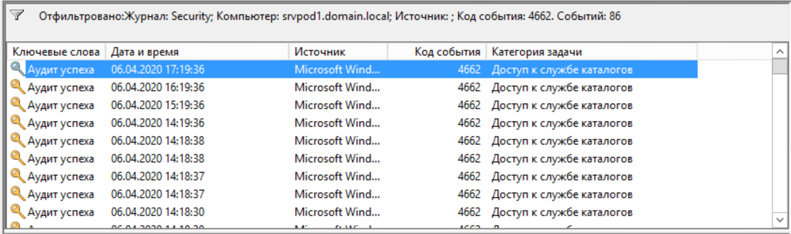
1. Откройте оснастку «Просмотр событий» («Диспетчер серверов» → «Средства» → «Просмотр событий»).



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



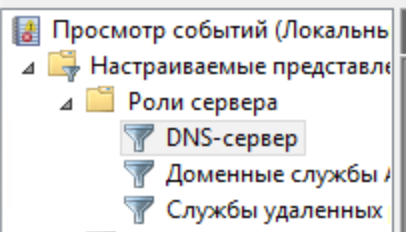
* + 1. введите в поле Компьютер имя компьютера, для которого необходимо отобразить события, например «srvpod1.domain.local»;
    2. подтвердите применение фильтра кнопкой ОК.
  1. просмотрите событие «Доступ к службе каталогов»:
     1. найдите указанное событие в правой части окна оснастки (код события – 4662);



* + 1. откройте диалоговое окно свойств выбранного события;
    2. ознакомьтесь с информацией события, найдите имя компьютера к которому осуществлялся доступ;



* + 1. закройте диалоговое окно события кнопкой «Закрыть»;
    2. снимите установленный ранее фильтр;
  1. Экспортируйте список событий для раздела DNS-сервер в текстовый файл:
     1. активизируйте раздел DNS-сервер;



* + 1. откройте диалоговое окно экспорта (Действие/Экспортировать …);
    2. введите имя файла в поле Имя;
    3. сохраните файл кнопкой Сохранить;
    4. 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.