ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»

Сибирский колледж транспорта и строительства

# УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ ДЛЯ ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ ПМ.02 ОРГАНИЗАЦИЯ СЕТЕВОГО АДМИНИСТРИРОВАНИЯ

## МДК.02.02.ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ

(очной формы обучения)
для специальности
09.02.06 Сетевое и системное администрирование

*базовая подготовка*
*среднего профессионального образования*

Иркутск 2023

РАССМОТРЕНО:
ЦМК специальности 09.02.06 «Сетевое и системное администрирование»
Протокол №9 от «23 » мая 2023 г.
Председатель ЦМК: Саквенко Т.В.

Разработчик: Храмова В.К. преподаватель Сибирского колледжа транспорта и строительства ФГБОУ ВО «Иркутский государственный университет путей сообщения».

СОДЕРЖАНИЕ

Пояснительная записка

Учебно-методическое пособие разработано в соответствии с программой профессионального модуля ПМ.02.«Организация сетевого администрирования» для МДК.02.02.Программное обеспечение компьютерных сетей и предназначено для реализации требований Федерального государственного образовательного стандарта среднего профессионального образования по программам подготовки специалистов среднего звена для специальности 09.02.06 Сетевое и системное администрирование

## Практическое занятие №1 Оценка и определение параметров развертывания

***Цель работы:***

Изучить параметры развертывания. Оценка и определение

***Задание №1.*** Изучить материал, составить конспект и проверить работу указанных параметров.

Прежде чем создавать развертывание обновления программного обеспечения в Configuration Manager 2007, необходимо настроить некоторые параметры в зависимости от иерархии Configuration Manager 2007. Также необходимо создать шаблоны развертывания для общих сценариев развертывания, понять, как работают окна обслуживания на клиентских компьютерах и как ведут себя клиентские компьютеры при перезагрузке, определить, будут ли делегироваться задачи развертывания, а также спланировать развертывания на клиентах Systems Management Server (SMS) 2003.

### Параметры точки обновления программного обеспечения

При создании активной точки обновления программного обеспечения настраиваются классификации обновления, продукты и языки, с которыми синхронизируются метаданные обновления программного обеспечения. Синхронизированные обновления программного обеспечения отображаются на консоли Configuration Manager и могут быть развернуты на клиентских компьютерах. Эти параметры могут быть изменены в любое время, но прежде чем приступить к синхронизации и развертыванию обновлений программного обеспечения, необходимо уделить особое внимание языковым параметрам **Сводных данных**.

Очень важно выбрать все языки сводных данных, которые будут необходимы в конкретной иерархии Configuration Manager. При синхронизации активной точки обновления программного обеспечения на центральном сайте выбранные языки сводных данных определяют, какие метаданные обновления программного обеспечения следует извлечь. В случае изменения языков сводных данных после выполнения по крайней мере одной синхронизации извлечение метаданных для измененных языков сводных данных осуществляется только для новых или измененных обновлений программного обеспечения. В случае уже синхронизированных обновлений программного обеспечения метаданные для других языков извлекаться не будут, за исключением случаев изменения обновлений в Центре обновления Майкрософт.

### Параметры развертывания обновлений программного обеспечения

При создании развертывания обновлений программного обеспечения с помощью мастера развертывания обновлений программного обеспечения необходимо рассмотреть множество параметров развертывания. Предоставляются сведения о параметрах, содержащихся на каждой странице мастера развертывания обновлений программного обеспечения.

**Страница "Общие"**

На странице **Общие** можно указать имя развертывания и его описание. Данное имя должно быть уникальным в пределах сайта.

Рекомендации

Укажите имя и описание, благодаря которому можно будет отличить это развертывание от других. На консоли Configuration Manager развертывания упорядочиваются по именам. Развертывание легко найти, если их немного, но при большом количестве развертываний поиск необходимого может быть затруднителен. Прежде чем создавать развертывание, необходимо определиться с контекстом именования, который будет использоваться на сайте.

**Страница "Коллекция"**

На странице **Коллекция** указаны целевые коллекции развертывания обновления программного обеспечения. Элементы коллекций и вложенных коллекций, при соответствующей настройке, получают доступные развертывания во время следующего цикла получения и оценки политик компьютеров. На странице **Коллекция** доступны следующие параметры.

- **Коллекция**. Указывает целевую коллекцию для развертывания. Члены коллекции получают обновления программного обеспечения, определенные в развертывании.
- **Включить членов вложенных коллекций**. Указывает, получают ли члены вложенной коллекции из главной коллекции обновления программного обеспечения, определенные в развертывании. По умолчанию этот параметр включен, а члены коллекции и вложенной коллекции назначены на развертывание.

Рекомендации

При создании шаблонов развертывания не указывайте коллекцию как часть шаблона. Это позволит использовать шаблон для создания различных развертываний, предназначенных для разных коллекций.

**Страница "Параметры отображения и представления времени"**

На странице **Параметры отображения и представления времени** указывается, будет ли пользователь уведомлен о предстоящих обновлениях программного обеспечения, ходе установки обновлений программного обеспечения, рассчитывается ли клиентом расписание развертывания на основе местного времени или времени в формате UTC (Coordinated Universal Time), а также определяется интервал времени по умолчанию между появлением обновления программного обеспечения и крайним сроком развертывания. На странице **Параметры отображения и представления времени** доступны следующие параметры.

- **Параметры отображения**
- Выберите один из следующих параметров:
- **Разрешить отображение уведомлений о клиентах**. Указывает, что конечные пользователи будут получать информацию о доступных обновлениях программного обеспечения с помощью уведомлений на клиентах, а также смогут просматривать индикаторы хода выполнения во время установки обновления программного обеспечения. Данный параметр выбран по умолчанию, и на клиентах разрешено отображение уведомлений.
- **Подавить отображение уведомлений на клиентах**. Указывает, что уведомления не отображаются на клиентах и индикаторы хода выполнения не выводятся во время установки обновления. Значки уведомлений об обновлениях программного обеспечения будут по-прежнему отображаться на клиентах, и пользователи могут просмотреть информацию о доступных обновлениях, щелкнув значок уведомления.
- **Параметры времени**
- Выберите один из следующих параметров:
- **Местное время клиента**. Указывает, что клиенты используют местное время для определения доступности обновлений программного обеспечения, а также для выполнения принудительной установки обновлений программного обеспечения при наступлении крайних сроков (в случае выбора этого параметра).
- **Время в формате UTC**. Указывает, что клиенты используют формат UTC для определения доступности обновлений программного обеспечения, а также для выполнения принудительной установки обновлений программного обеспечения при наступлении крайних сроков (в случае выбора этого параметра). По умолчанию этот параметр выбран, и график развертывания составляется с помощью времени в формате UTC.

- **Параметры продолжительности**
- **Продолжительность**. Указывает продолжительность, используемую только в случае создания развертывания на основе шаблона. По умолчанию значение параметра крайнего срока равно времени, когда станет доступным обновление, а также настраиваемому значению продолжительности. По умолчанию задана продолжительность 2 недели.

**Страница "Параметры перезапуска"**

На странице **Параметры перезапуска** указывается поведение при перезапуске системы во время установки на клиентском компьютере обновления программного обеспечения, когда для завершения процесса установки требуется перезапуск. На странице **Параметры перезапуска** доступны следующие параметры.

**Подавить перезапуск системы на следующих объектах:**

- **Серверы**. Указывает, подавлять ли перезапуск операционной системы на серверах. Это действие запрашивается установкой обновления программного обеспечения, если перезапуск требуется для завершения установки. По умолчанию этот параметр отключен и серверы будут перезагружаться, если это потребуется при установке обновления программного обеспечения.
- **Рабочие станции**. Указывает, подавлять ли перезапуск операционной системы на рабочих станциях. Это действие запрашивается установкой обновления программного обеспечения, если перезапуск требуется для завершения установки. По умолчанию этот параметр отключен и рабочие станции будут перезагружаться, если это потребуется при установке обновления программного обеспечения.

**Укажите, разрешен ли перезапуск системы рабочих станций и серверов за пределами настроенных окон обслуживания.**

- **Разрешить перезапуск системы за пределами окон обслуживания**. Указывает, разрешен ли перезапуск системы рабочих станций и серверов за пределами настроенных окон обслуживания. По умолчанию этот параметр отключен, и если перезапуск необходим для завершения установки обновления программного обеспечения, он инициализируется только если в настроенном окне обслуживания остается не менее 10 минут.

Рекомендации

Подавление перезапусков системы может быть полезным в серверных или если нежелательно, чтобы компьютеры, на которых устанавливаются обновления программного обеспечения, перезапускались по умолчанию. Однако, принудительный перезапуск системы после установки обновления программного обеспечения гарантирует полное завершение обновления, в то время как подавление запроса на перезапуск после установки может оставить системы в небезопасном или нестабильном состоянии.

**Страница "Создание события"**

На странице **Создание события** указывается, отключаются ли предупреждения Microsoft Operations Manager при установке обновлений программного обеспечения, а также создается ли предупреждение Operation Manager в случае неудачного завершения обновления программного обеспечения. На странице **Создание события** доступны следующие параметры.

- **Отключить сообщения Operations Manager во время выполнения обновлений программного обеспечения**. Указывает, какие оповещения Operations Manager отключены во время установки обновления программного обеспечения. Этот параметр может оказаться полезным при развертывании обновлений программного обеспечения, которые повлияют на приложение, за которым следит Operations Manager. По умолчанию этот параметр отключен.

- **Выдать предупреждение Operation Manager, если не удалось установить обновление программного обеспечения**. Указывает, какие оповещения Operations Manager создаются для каждой ошибки при установке обновления программного обеспечения. По умолчанию этот параметр отключен.

Рекомендации

Эти параметры могут оказаться полезными при развертывании обновлений программного обеспечения, которые повлияют на приложение, за которым следит Operations Manager. Отключение оповещений во время установки обновления будет препятствовать созданию оповещений, например об остановке службы в результате установки обновления. По умолчанию эти параметры отключены.

**Страница "Параметры загрузки"**

На странице "Параметры загрузки" указывается, каким образом клиентские компьютеры Configuration Manager 2007 будут взаимодействовать с точками распространения при получении развертывания обновления программного

обеспечения. На странице **Параметры загрузки** доступны следующие параметры.

**Если клиент соединяется в пределах границ медленной или ненадежной сети.**

- **Не устанавливать обновления программного обеспечения**: указывает, что клиенты не устанавливают обновления программного обеспечения, если они находятся внутри границ сети, определенных как медленные или ненадежные. По умолчанию этот параметр выбран.

- **Загружать обновления программного обеспечения с точки распространения и устанавливать**: указывает, что клиенты загружают обновления программного обеспечения с точки распространения и устанавливают их, если они находятся внутри границ сети, определенных как медленные или ненадежные. Все работает так, как если бы клиент находился в пределах локальной сети.

**Необходимо указать, разрешено ли клиентам, находящимся в границах одной или более защищенных точек распространения, загружать и устанавливать обновления программного обеспечения с незащищенных точек распространения, если обновления недоступны на защищенных точках распространения.**

- **Не устанавливать обновления программного обеспечения**: указывает, что когда на защищенных точках распространения нет обновлений программного обеспечения, доступных для клиентов, находящихся в границах защищенной точки распространения, обновления программного обеспечения не устанавливаются.

- **Загружать обновления программного обеспечения с незащищенной точки распространения и устанавливать**: Указывает, что при отсутствии на защищенных точках распространения обновлений программного обеспечения, доступных для клиентов, находящихся в границах защищенной точки распространения, клиент загружает обновления программного обеспечения с незащищенной точки распространения и устанавливает их. По умолчанию этот параметр выбран.

**Страница "Параметры SMS 2003"**

На странице "Параметры SMS 2003" указывается, развертывать ли обновления программного обеспечения на клиентах SMS 2003, находящихся в целевой коллекции. Этот параметр доступен, только в случае синхронизации обновлений программного обеспечения в развертывании с помощью средства

инвентаризации обновлений Майкрософт, если для параметра **Готов к развертыванию на SMS 2003** установлено значение **Да**. На странице **Параметры SMS 2003** доступны следующие параметры.

**Развернуть обновления программного обеспечения для клиентов SMS 2003.**

Этот параметр указывает, развертывать ли обновления программного обеспечения при развертывании на клиентах SMS 2003, находящихся в целевой коллекции. Пакет, файлы инструкций для пакета и объявление создаются и отправляются на дочерние сайты SMS 2003 для поддержки установки обновления на клиентах SMS 2003. По умолчанию этот параметр отключен.

Важно**!**
Если этот параметр отключен в активном развертывании, включающем клиенты SMS 2003, включить его снова нельзя. Соответствующая программа и объявление, созданные для клиентов SMS 2003, отключаются. Прежде чем окончательно отменить выполнение этого развертывания на клиентах SMS 2003, убедитесь, что это действительно необходимо.

При выборе этого параметра доступны следующие параметры.

- **Выполнить инвентаризацию оборудования немедленно**. Позволяет указать, следует ли выполнять инвентаризацию оборудования на клиентах SMS 2003 непосредственно после установки обновления программного обеспечения. Этот параметр делает отчеты клиентов более точными, но при этом на клиентах SMS 2003 может увеличиться объем работы системы. По умолчанию этот параметр отключен, и инвентаризация оборудования выполняется во время запланированного цикла.

- **Когда точка распространения доступна локально**. Указывает, что клиенты SMS 2003 обрабатывают установку обновления программного обеспечения, если обновления доступны в локальной точке распространения, в соответствии со следующими параметрами.

    - **Выполнить установку обновления из точки распространения**. Позволяет указать, что обновления программного обеспечения устанавливаются из точки распространения. Этот параметр используется по умолчанию.

    - **Загрузить обновления из точки распространения и затем выполнить установку**. Позволяет указать, что обновления программного обеспечения загружаются из точки распространения, а затем устанавливаются на клиент.

- **Если клиент соединяется в пределах границ медленной или ненадежной сети**. Позволяет указать, что клиенты SMS 2003 обрабатывают установку обновления программного обеспечения, если обновления доступны только в удаленных точках распространения, в соответствии со следующими параметрами.
    - **Не выполнять установку обновления**. Позволяет указать, что установка обновления программного обеспечения выполняться не будет. Этот параметр используется по умолчанию.
    - **Загрузить обновления из удаленной точки распространения до установки обновления**. Позволяет указать, что обновления программного обеспечения загружаются из точки распространения, а затем устанавливаются на клиент.
    - **Выполнить установку обновления из удаленной точки распространения**. Позволяет указать, что обновления программного обеспечения устанавливаются с удаленной точки распространения.

Рекомендации

При загрузке и последующей установке обновлений программного обеспечения на клиенты SMS 2003 загружаются все обновления, содержащиеся в пакете, независимо от их применимости для клиента. При наличии в пакетах развертывания множества обновлений, которые могут быть неприменимы к клиенту SMS 2003, необходимо решить, запускать ли установку обновления непосредственно из точки распространения.

**Страница "Пакет развертывания"**

На странице **Пакет развертывания** указывается пакет, который будет использоваться для размещения обновлений программного обеспечения при выполнении развертывания. Обновления программного обеспечения во время развертывания загружаются и копируются в папку пакета развертывания на точках распространения, настроенных для пакета. Если все обновления программного обеспечения в развертывании были загружены и скопированы в общую папку пакета на точке распространения, страница **Пакет развертывания** мастера отображаться не будет, а развертывание будет автоматически настраиваться на использование пакета, загрузившего обновление. Если развертывание предназначено для клиентов SMS 2003, мастер всегда будет запрашивать пакет развертывания, независимо от того, загружались ли обновления ранее. На странице **Пакет развертывания** доступны следующие параметры.

- **Выбрать пакет развертывания**. Указывает, что существующий пакет используется для обновления программного обеспечения при развертывании. Можно выбрать пакеты развертывания, созданные на сайте. Пакеты, созданные на родительском сайте, не доступны.

- **Создать новый пакет развертывания**. Указывает, что создан новый пакет для обновления программного обеспечения при развертывании. Пакет развертывания включает в себя настройку следующих свойств.

  - **Имя пакета развертывания**: Указывает имя пакета развертывания. У пакета должно быть уникальное имя, описывающее содержимое пакета. Его длина ограничена 50 символами.

  - **Описание пакета развертывания**: Указывает описание пакета развертывания. Описание пакета должно подробно описывать содержимое пакета. Его длина ограничена 127 символами.

  - **Исходный пакет развертывания**: Указывает расположение исходных файлов обновления программного обеспечения. При создании развертывания исходные файлы сжимаются и копируются в точки распределения, связанные с пакетом развертывания. Исходное расположение необходимо ввести в формате сетевого пути (например, \\server\sharename\path). Также можно выполнить поиск данного расположения в сети, воспользовавшись для этого кнопкой "Обзор". Прежде чем перейти к следующей странице, необходимо вручную создать общую папку для исходных файлов пакета развертывания.

    Важно**!**
    Расположение источника пакета развертывания не должно использоваться другим развертыванием или пакетом распространения программного обеспечения.
    Важно**!**
    Учетной записи компьютера поставщика SMS и пользователю, который будет фактически загружать обновления программного обеспечения в расположение загрузки, требуется доступ на запись в расположении загрузки. Ограничьте доступ к месту загрузки, чтобы у злоумышленников было меньше шансов подделать исходные файлы обновлений программного обеспечения в месте загрузки.

  - **Приоритет передачи пакета развертывания**: Указывает приоритет передачи для пакета развертывания. Приоритет передачи используется для пакета развертывания во время его пересылки в точки распространения дочерних сайтов. Пакеты отправляются в порядке

приоритета: высокий, средний или низкий. Пакеты с идентичными приоритетами отправляются в том порядке, в котором они были созданы. При отсутствии задержек пакет будет обработан немедленно, независимо от его приоритета.

- **Включить двоичную дифференциальную репликацию**: Указывает, следует ли применять двоичное разностное сравнение к измененным исходным файлам пакета. Установка этого флажка включает этот режим и позволяет диспетчеру распространения передавать не весь файл, а только его измененные части. По сравнению с традиционным методом, при котором файл переносится полностью, такой метод позволяет сэкономить трафик при переносе изменений больших файлов. Дополнительные сведения см. в разделе "О двоичной дифференциальной репликации". Данное значение существующих пакетов можно изменить в свойствах пакета.

**Страница "Расположение загрузки"**

На странице **Расположение загрузки** указывается, откуда должны загружаться обновления программного обеспечения в пакет развертывания на компьютере с консолью Configuration Manager: из Интернета или из локальной сети. На странице **Расположение загрузки** доступны следующие параметры.

- **Загрузить обновления программного обеспечения по Интернету**. Задает, что обновления программного обеспечения загружаются из расположения в Интернете, указанного в определении обновления программного обеспечения. По умолчанию выбран этот вариант.

  **Примечание**
  Компьютер, на котором мастер запущен в консоли Configuration Manager, должен быть подключен к Интернету.

- **Загрузить обновления программного обеспечения из расположения в локальной сети**. Задает, что обновления программного обеспечения загружаются из локального каталога или общей папки. Используйте этот параметр, если компьютер, на котором запущен мастер, не имеет доступа к Интернету, или если обновления программного обеспечения доступны в локальной сети. Обновления программного обеспечения могут загружаться с любого компьютера, у которого есть доступ к Интернету, и храниться в локальной сети, в месте, доступном с компьютера, на котором запущен мастер..

**Рекомендации**

Если обновления программного обеспечения уже загружены на сервер служб Microsoft Windows Server Update Services (WSUS) на активной точке обновления программного обеспечения, можно выбрать вариант **Загрузить обновления программного обеспечения из расположения в локальной сети** и настроить \\<*Имя сервера WSUS*>\<*Путь_к_содержимому_WSUS*> для загрузки обновлений программного обеспечения с сервера WSUS, а не из Интернета.

Если компьютер, на котором запущена консоль Configuration Manager, не имеет доступа к Интернету, можно установить удаленную консоль на компьютере с доступом к Интернету, чтобы загрузить файлы обновления программного обеспечения в пакет.

**Страница "Выбор языка"**

На странице **Выбор языка** указываются языки, загружаемые для выбранных обновлений программного обеспечения. Обновления программного обеспечения загружаются, только если они доступны на выбранных языках. Обновления программного обеспечения, не зависящие от языка, загружаются всегда.

Если все обновления программного обеспечения для данного развертывания были предварительно загружены и скопированы в общую папку пакета на точке распространения, страница мастера **Пакет развертывания** не отображается. Развертывание автоматически настраивается на загрузку обновлений на тех языках, которые загружались ранее. На странице **Выбор языка** доступны следующие параметры.

- **Файл обновления**. Язык, для которого загружаются файлы с обновлениями программного обеспечения. По умолчанию выбраны языки, заданные в свойствах точки обновления программного обеспечения. При выборе дополнительных языков они не добавляются к настройкам языков выбранной точки обновления программного обеспечения. Для перехода на следующую страницу должен быть выбран хотя бы один язык. Если единственный выбранный на странице язык не поддерживается обновлением программного обеспечения, то обновление программного обеспечения загружено не будет.

**Расписание развертывания**

На странице **Расписание развертывания** указывается, когда развертывание обновления программного обеспечения станет активным и будет ли установка обновления программного обеспечения на клиентах выполняться принудительно. На странице **Расписание развертывания** доступны следующие параметры.

**Выберите дату и время, когда обновления программного обеспечения станут доступны клиентам:**

- **Как можно скорее**. Обновления программного обеспечения при развертывании становятся доступны клиентам сразу же, как только это возможно. После создания развертывания обновляется политика компьютера, клиенты оповещаются о развертывании в течение следующего цикла оценки политики компьютеров, после чего обновления становятся доступными для установки.

- **Дата и время**. Обновления программного обеспечения при развертывании становятся доступны клиентам только после определенной даты и времени. После создания развертывания политика компьютера обновляется, и клиенты оповещаются о развертывании в течение следующего цикла оценки политики компьютеров, но обновления программного обеспечения в развертывании не будут доступны для установки до установленной даты и времени.

**Укажите, должны ли обновления программного обеспечения автоматически устанавливаться на клиентах в заданный крайний срок развертывания:**

- **Не задавать крайний срок для установки обновления программного обеспечения**. Обновления программного обеспечения в развертывании являются необязательными, и их автоматическая установка до определенных даты и времени не требуется.

- **Задать крайний срок для установки обновления программного обеспечения**. Обновления программного обеспечения в развертывании являются обязательными, и их автоматическая установка должна быть выполнена до определенных даты и времени. Если наступает крайний срок, а обновления программного обеспечения в развертывании не были установлены на клиенте, установка запустится автоматически. При заданном крайнем сроке доступны следующие дополнительные параметры.

    - **Включить режим пробуждения по локальной сети**. При включенном режиме пробуждения по локальной сети при наступлении крайнего срока на компьютеры, требующие установки одного или нескольких обновлений в развертывании, отправляются пакеты пробуждения. Неработающие компьютеры запускаются при наступлении крайнего срока, что позволяет начать установку обновлений. Клиенты, не требующие обновлений во время развертывания, не запускаются. По умолчанию этот параметр

отключен, он становится доступен только при назначении крайнего срока развертывания.

- **Игнорировать окна обслуживания и выполнить установку сразу же при наступлении крайнего срока**. Обновления программного обеспечения в развертывании устанавливаются при наступлении крайнего срока независимо от настройки окна обслуживания. По умолчанию этот параметр отключен, он становится доступен только при назначении крайнего срока развертывания.

**Дополнительные сведения**

Если задан крайний срок, развертывание становится обязательным, а установка обновления программного обеспечения выполняется принудительно в заданную дату и время. Если при наступлении крайнего срока на клиентском компьютере не было произведено развертывание обновления программного обеспечения, установка запускается автоматически, вне зависимости от того, выполнял ли какой-либо пользователь вход в систему на этом компьютере. Если для завершения установки обновления программного обеспечения необходима перезагрузка системы, она может быть выполнена принудительно.

На клиентских компьютерах отображаются уведомления, сообщающие пользователю о готовых к установке обновлениях и о дате ближайшего из крайних сроков обновления. Например, при наличии двух развертываний, различие между крайними сроками которых составляет два дня, то в уведомлениях будет указан тот крайний срок развертывания, который наступит первым. После установки обновлений программного обеспечения, относящейся к развертыванию с ближайшим крайним сроком, на компьютере продолжат отображаться уведомления, но теперь в них будет указан крайний срок второго по очередности развертывания. Клиенты SMS 2003 в иерархии Configuration Manager для работы с назначенными им развертываниями также используют указанные даты и время крайнего срока.

**Страница "Оценка защиты доступа к сети"**

На странице **Оценка защиты доступа к сети** указывается, требуется ли обновление программного обеспечения в этом развертывании для соответствия при использовании защиты доступа к сети. Включите оценку защиты доступа к сети, чтобы включить обновления программного обеспечения в политику защиты доступа к сети, которая вступит в силу на клиентах с поддержкой NAP на основании настроенного расписания. После вступления политики в силу доступ клиентов с поддержкой защиты доступа к сети (NAP) может быть ограничен до тех пор, пока они не будут соответствовать выбранному обновлению программного обеспечения. Сетевое ограничение и исправление

зависят от того, каким образом настроены политики на сервере политики сети Windows. На странице **Расписание развертывания** доступны следующие параметры.

- **Включить оценку защиты доступа к сети**. Задает включение обновления программного обеспечения в политику защиты доступа к сети (NAP) и его оценку на клиентах с поддержкой защиты доступа к сети. При выборе этого параметра доступны следующие параметры.
- Укажите, когда эти параметры вступают в силу:
- **Как можно скорее**. Указывает, что обновление программного обеспечения включено в политику защиты доступа к сети (NAP), которая вступит в силу на клиентах с поддержкой защиты доступа к сети как можно быстрее.
- **Дата и время**. Указывает, что обновление программного обеспечения включено в политику защиты доступа к сети (NAP), которая вступит в силу на клиентах с поддержкой защиты доступа к сети в указанные дату и время. Значение даты и времени по умолчанию определяется путем добавления 14 дней к дате и времени крайнего срока развертывания, указанным на странице **Расписание развертывания**.

Страница **Оценка защиты доступа к сети** мастера развертывания обновлений программного обеспечения отображается только в том случае, если на сайте настроена защита доступа к сети.

**Использование шаблонов при создании развертываний**

В шаблонах развертывания хранятся многие свойства развертывания, которые могут не изменяться в ходе развертываний, благодаря чему администраторы экономят время при создании развертываний обновления программного обеспечения. Шаблоны можно создать для разных сценариев развертывания в среде. Например, можно создать шаблон для срочных развертываний обновления программного обеспечения и спланированных развертываний. При помощи шаблона для срочных развертываний можно подавить отображение уведомлений на клиентских компьютерах, установить крайний срок в 0 дней для расписания развертываний, а также позволить перезапуск системы вне окон обслуживания. При помощи шаблона для спланированного развертывания можно подавить отображение уведомлений на клиентских компьютерах и установить крайний срок в 14 дней для расписания развертываний.

Предварительно создав шаблоны развертывания для типичных сценариев развертывания в среде, можно создать развертывания при помощи шаблонов, заполняющих ряд свойств развертывания, которые обычно статичны для

определенного сценария развертывания. Используя шаблон развертывания, также можно сократить количество страниц мастера развертывания обновлений программного обеспечения до семи, что экономит время и позволяет избежать ошибок при настройке развертывания. В шаблоне развертывания можно настроить параметры развертывания, содержащихся на следующих страницах мастера.

- Коллекция
- Параметры отображения и представления времени
- Параметры перезапуска
- Создание события
- Параметры загрузки
- Параметры SMS 2003

Если при создании развертывания шаблон не используется, то эти свойства вводятся вручную. При необходимости их можно из мастера сохранить в виде шаблона для использования при дальнейших развертываниях..

**Окна обслуживания**

При настройке окон обслуживания в коллекциях, которые будут предназначены для развертывания обновлений программного обеспечения, необходимо рассмотреть следующие моменты.

- Каждому обновлению программного обеспечения по умолчанию дается 35 минут на установку и перезапуск, если он требуется (75 минут для пакетов обновлений). Если доступное время, оставшееся в окне обслуживания, меньше этого значения, установка обновления программного обеспечения не начнется до появления следующего окна обслуживания. При планировании развертывания в коллекции в окне обслуживания примите во внимание эти значение по умолчанию. Например, если для коллекции настроено окно обслуживания продолжительностью в 2 часа, а в развертывании содержатся четыре обновления программного обеспечения, то только три обновления программного обеспечения будут установлены в течение первого окна обслуживания; последнее обновление будет установлено во время второго окна обслуживания.
- Следующие параметры развертывания влияют на способ установки обновлений программного обеспечения на клиентских компьютерах, на которых используются окна обслуживания.

- **Разрешить перезапуск системы за пределами окон обслуживания.** Указывает, разрешен ли перезапуск системы рабочих станций и серверов за пределами настроенных окон обслуживания. По умолчанию этот параметр отключен. Этот параметр удобно использовать, когда требуется как можно скорее выполнить установку программного обеспечения на клиентских компьютерах. Если этот параметр не задан и оставшееся в окне обслуживания время составляет не более 10 минут, перезапуск системы не будет инициирован, поскольку он может помешать завершению установки и оставить клиентский компьютер в уязвимом состоянии до начала следующего окна обслуживания. Этот параметр доступен на странице **Параметры перезапуска** мастера шаблона развертывания или мастера развертывания обновлений программного обеспечения.

- **Игнорировать окна обслуживания и выполнить установку сразу же при наступлении крайнего срока.** Обновления программного обеспечения в развертывании устанавливаются при наступлении крайнего срока независимо от настройки окна обслуживания. По умолчанию этот параметр отключен и доступен только в том случае, если для развертывания назначен крайний срок. Этот параметр удобно использовать, когда требуется как можно скорее выполнить установку обновлений программного обеспечения на клиентских компьютерах, например обновлений в составе ускоренного развертывания. Этот параметр доступен на странице **Расписание** мастера развертывания обновлений программного обеспечения.

**Действия развертывания, приводящие к обновлению пакета**

Каждый раз, когда обновление программного обеспечения добавляется к развертыванию, предназначенному как для клиентов Configuration Manager, так и для клиентов SMS 2003, или когда изменяется параметр времени начала развертывания, обновляется исходный файл пакета, номер версии пакета развертывания увеличивается на единицу, а точки распространения, настроенные для пакета, обновляются. При добавлении обновлений программного обеспечения к развертыванию, которое не развертывает обновления программного обеспечения на клиентах SMS 2003, будут использоваться исходные файлы обновлений из пакета развертывания, содержащего обновления программного обеспечения, а пакет не будет обновлен.

**Поведение перезагрузки на клиентских компьютерах**

При наличии запущенных установок обновления программного обеспечения, для завершения которых необходим перезапуск, новые обновления, ставшие доступными, как и значок в области уведомлений, отображаться на клиентских компьютерах не будут. В случае наступления крайнего срока при обязательных обновлениях перезагрузка клиентских компьютеров инициируется автоматически. При установке для нескольких развертываний одного и того же крайнего срока все обновления программного обеспечения будут установлены при наступлении крайнего срока, после чего будет инициирована перезагрузка системы.

Примечание
Некоторые обновления программного обеспечения должны быть установлены эксклюзивно, вследствие чего перезагрузка системы может быть инициирована для этих обновлений программного обеспечения до установки прочих обновлений в том же развертывании или в развертываниях с одним и тем же крайним сроком.

**Сокрытие развертывания от конечных пользователей**

Чтобы скрыть развертывание и установку обновления программного обеспечения на клиентских компьютерах, воспользуйтесь параметром **Скрыть все развертывания от конечных пользователей** на вкладке **Установка обновления** в свойствах **Агента клиента обновления программного обеспечения**. Данный параметр указывает, что обновления программного обеспечения во всех развертываниях будут производиться на клиентских компьютерах без отображения каких-либо уведомлений или значков в области уведомлений. По умолчанию этот параметр не включен. Если этот параметр включен, для установки доступны только обновления программного обеспечения в обязательных развертываниях; при наступлении крайнего срока будет инициирована автоматическая установка. Если этот параметр выключен, скрытые развертывания станут видимыми на клиентских компьютерах.

**Обновления программного обеспечения с условиями лицензионного соглашения**

Если с обновлением программного обеспечения связаны условия лицензионного соглашения на использование программного обеспечения корпорации Майкрософт, и эти условия еще не были приняты, то перед открытием мастера развертывания обновлений программного обеспечения откроется диалоговое окно **Просмотреть и принять условия лицензионного соглашения**. После принятия условий лицензионного соглашения об обновлении программного обеспечения отобразится окно мастера, а развертывание обновлений программного обеспечения станет возможным. Для следующих развертываний этого обновления программного обеспечения принятие условий лицензионного соглашения не потребуется. При отклонении

условий лицензионного соглашения выполнение всего процесса будет отменено. Условия лицензионного соглашения можно также принять на консоли Configuration Manager, выделив одно или несколько обновлений программного обеспечения, а затем инициировав действие **Просмотреть и принять условия лицензионного соглашения**.

**Делегированное администрирование**

С помощью списка обновлений можно делегировать полномочия для развертывания обновлений программного обеспечения. Например, администратор на центральном сайте может выбрать обновления программного обеспечения, которые необходимо развернуть, и добавить их в список обновлений. Затем администраторы сайтов или дочерних сайтов, обладающие ограниченными правами доступа к объектам, могут воспользоваться списком обновлений и развернуть обновления, содержащиеся в списке, в соответствующих коллекциях.

**Планирование развертывания SMS 2003**

Если клиенты SMS 2003 находятся в иерархии Configuration Manager 2007, прежде чем выполнять на них развертывание обновлений программного обеспечения необходимо учесть определенные моменты и предпринять дополнительные действия.

**Обновления программного обеспечения, которые можно развернуть на клиентах SMS 2003**

На клиентах SMS 2003 могут быть развернуты все обновления программного обеспечения, синхронизированные с помощью средства инвентаризации Центра обновлений Майкрософт. После выполнения синхронизации каталога Центра обновлений Майкрософт для параметра **Готов к развертыванию на SMS 2003** будет установлено значение **Да**. Возможность развертывания на клиентах SMS 2003 доступна только при условии, что все обновления программного обеспечения готовы к развертыванию на SMS 2003.

**Метаданные обновлений программного обеспечения, перенесенные после выполнения обновления**

В процессе обновления к названию каждого обновления Configuration Manager 2007 присоединяется приставка (LEGACY). Это помогает идентифицировать перенесенные обновления программного обеспечения среди новых метаданных обновлений программного обеспечения, синхронизированных после обновления. Обновления программного обеспечения с приставкой (LEGACY) в названии не должны использоваться клиентами; они передаются только с целью распространения программного обеспечения и для отчетности. Можно

запустить сценарий для скрытия этих обновлений программного обеспечения в консоли Configuration Manager, так что будут отображаться только обновления, подлежащие развертыванию.

**Примечание**
Перенесенные обновления программного обеспечения, содержащиеся в развертывании обновления программного обеспечения, которое также было перенесено, не будут скрыты, пока перенесенное развертывание не будет удалено, или пока из развертывания не будут удалены обновления.

**Обновления программного обеспечения сохраняются после загрузки с помощью мастера развертывания обновлений программного обеспечения**

Если при создании развертывания обновлений программного обеспечения для клиентов SMS 2003 как минимум одно обновление не было загружено, будут загружены все обновления, не вошедшие в пакет обновления для развертывания, даже если первоначально они были загружены в составе другого пакета. Если все обновления программного обеспечения загружены до создания развертывания и входят в пакет обновлений развертывания или если в развертывании не выбран параметр **Развернуть обновления программного обеспечения для клиентов SMS 2003**, мастер загрузит только те обновления, которые ранее не загружались. Чтобы этого избежать, загрузите обновления программного обеспечения, которые не загружались до создания развертывания с помощью мастера загрузки обновлений или мастера списка обновлений.

**Использование шаблонов при создании развертываний SMS 2003**

Если все обновления программного обеспечения, выбранные для развертывания, готовы к развертыванию на SMS 2003, можно выбрать шаблон развертывания с выбранным параметром **Развернуть обновления программного обеспечения для клиентов SMS 2003** . Если хотя бы одно обновление программного обеспечения невозможно развернуть на клиентах SMS 2003, шаблоны, развертывающие обновления на клиентах SMS 2003, будут недоступны для использования при создании развертывания.

**Выборочная загрузка недоступна для клиентов SMS 2003**

Клиентские компьютеры Configuration Manager 2007 загружают только те обновления программного обеспечения, которые содержаться в необходимом пакете развертывания. Это позволяет администраторам создавать большие пакеты развертывания, поддерживающие несколько развертываний. По умолчанию при развертывании обновлений программного обеспечения на клиентах SMS 2003 установка обновления программного обеспечения запускается непосредственно из точки распространения. Если на странице

"Параметры SMS 2003" мастера развертывания обновлений программного обеспечения указано загружать обновления, а затем устанавливать их на клиентах SMS 2003, клиент SMS 2003 загрузит все обновления, содержащиеся в пакете развертывания, независимо от их применимости для клиента. При наличии в пакетах развертывания множества обновлений, которые могут быть неприменимы к клиенту SMS 2003, необходимо решить, запускать ли установку обновления непосредственно из точки распространения.

**Практическое занятие №2 Планирование стратегии управления образами**

***Цель работы:***

Изучить работу планирования стратегии управления образами

Образ операционной системы — это полный слепок состояний самой системы, записанный в файл. Слепок включает в себя не только саму ОС, но и все настройки, конфигураций и все программы, установленные на нее.

После того, как файл образа ОС создан, его можно загружать в различные облачные и виртуальные машины. После распаковки и выполнения образа получаем в своё распоряжение полностью рабочую машину с уже установленными программами и прописанными настройками.

Системным администраторам по долгу службы постоянно нужно ставить и настраивать много разных программ. Как правило, это сводится к набору однообразных и шаблонных операций. Например, поставить веб-сервер, запустить его, открыть порты доступа к серверу извне, настроить журналирование событий, открыть доступ к определенным файлам. Для этого нужно выполнить на рабочей машине ряд однотипных команд.

**Планирование управление образами ОС.**

Управление образами операционных систем, устанавливаемых при помощи сервера удаленной установки, составляет основу администрирования сервера удаленной установки. Сервер удаленной установки Windows Server 2003 может работать с перечисленными ниже типами образов ОС

| Тип образа | Особенности |
|---|---|
| Стандартный образ | Создается на консоли сервера удаленной установки на основе дистрибутива ОС;<br>создается на основе установочного компакт-диска Windows или интегрированного дистрибутива. |
| Образ эталонного | Создается при помощи утилиты riprep , запускаемой на эталонном компьютере; |

| | |
|---|---|
| компьютера | содержит полную копию всех файлов диска **C:** эталонного компьютера и предназначен для установки компьютеров с комплектом заранее предустановленного программного обеспечения;<br>для создания такого образа на сервере удаленной установки должен быть базовый образ ОС, на основе которого создается образ эталонного компьютера. |

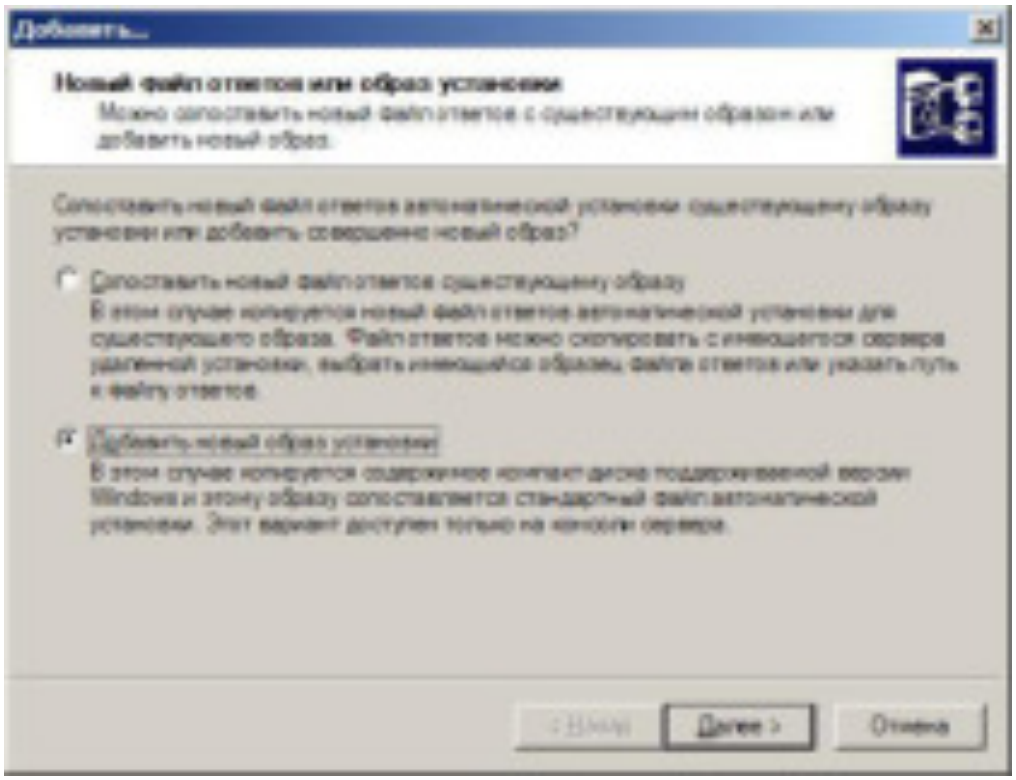

Рассмотрим общие вопросы управления образами ОС и создание стандартных образов ОС.

Для добавления, изменения или удаления образов ОС нажмите соответствующую кнопку (Добавить, Свойства, Удалить) на вкладке **Образы**.

**Установка дополнительных образов ОС.**

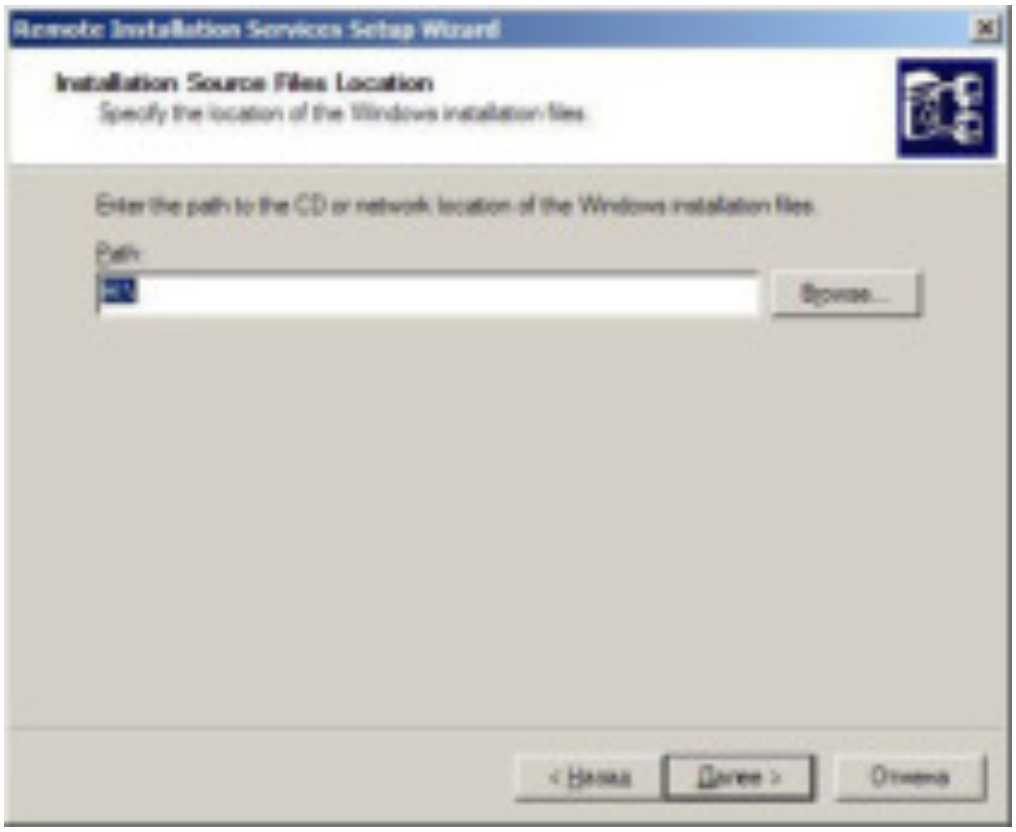
Для установки дополнительного образа ОС необходимо щелкнуть кнопку **Добавить** на вкладке Образы окна свойств сервера удаленной установки.

В появившемся окне мастера необходимо установить переключатель в положение Добавить новый образ установки и щелкнуть кнопку **Далее**. Будет запущен Мастер добавления образа установки.



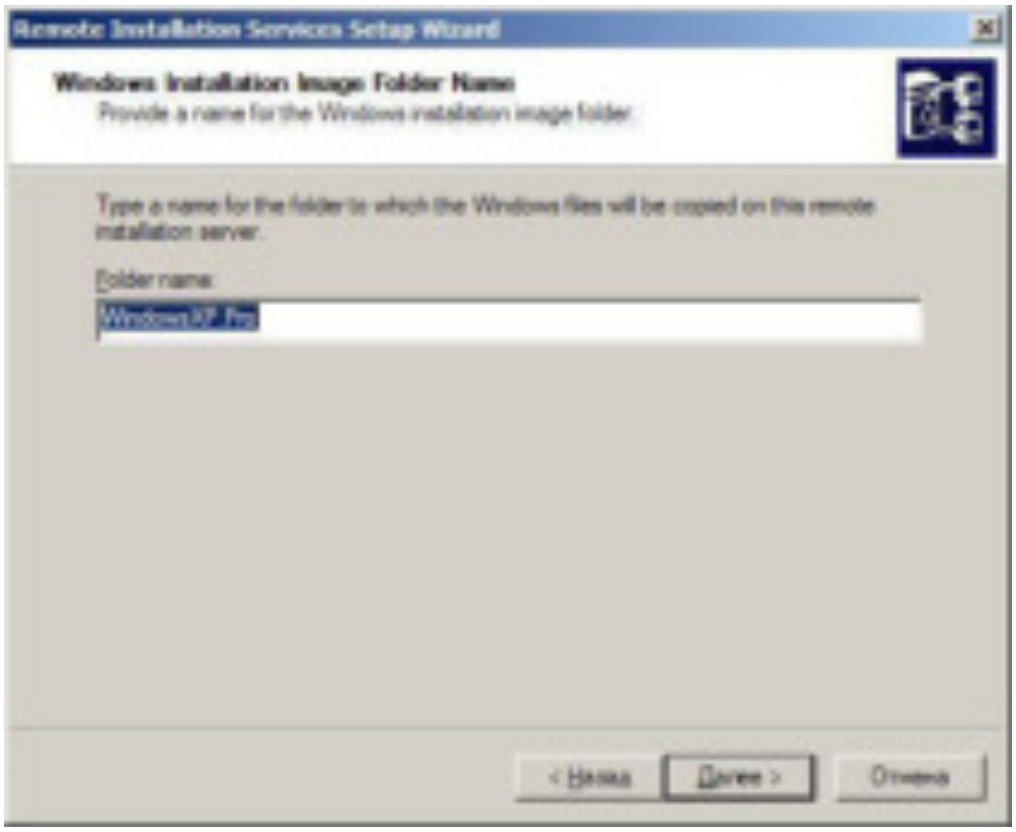

Возможность добавлять новые образы ОС доступна вам только с консоли сервера удаленной установки. При использовании средств удаленного администрирования вы можете только добавить файл ответов к уже существующему образу.

Возможность добавлять новые образы ОС доступна вам только с консоли сервера удаленной установки. При использовании средств удаленного администрирования вы можете только добавить файл ответов к уже существующему образу.

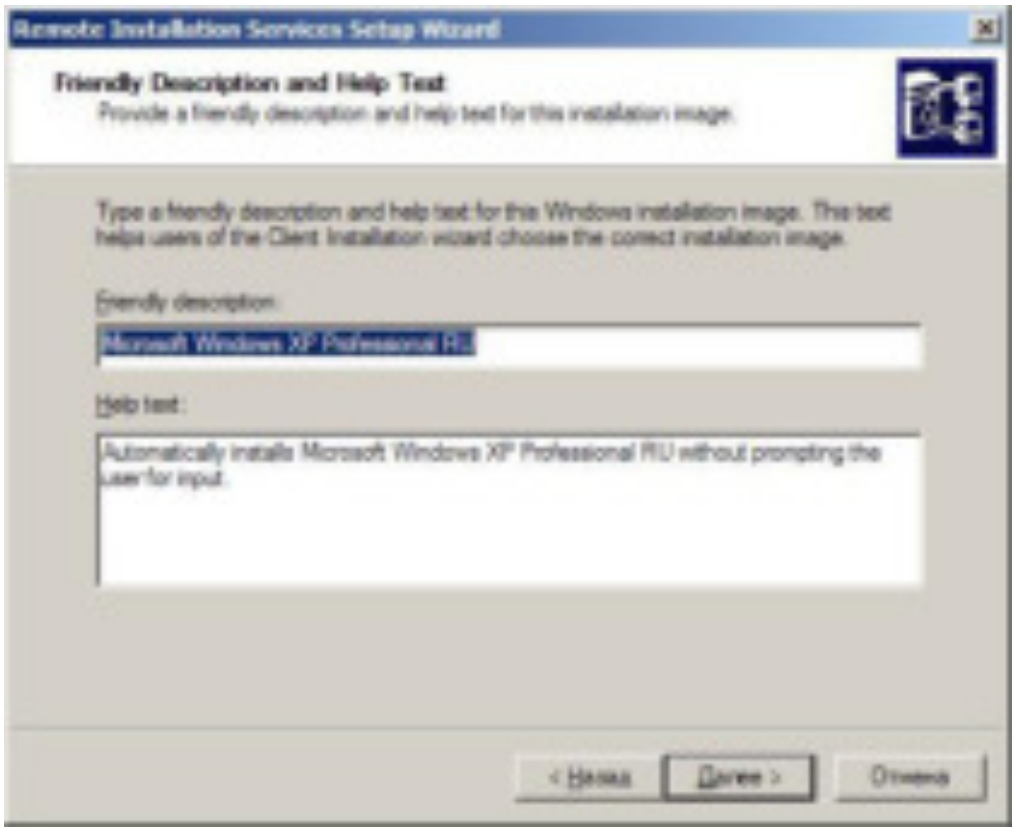


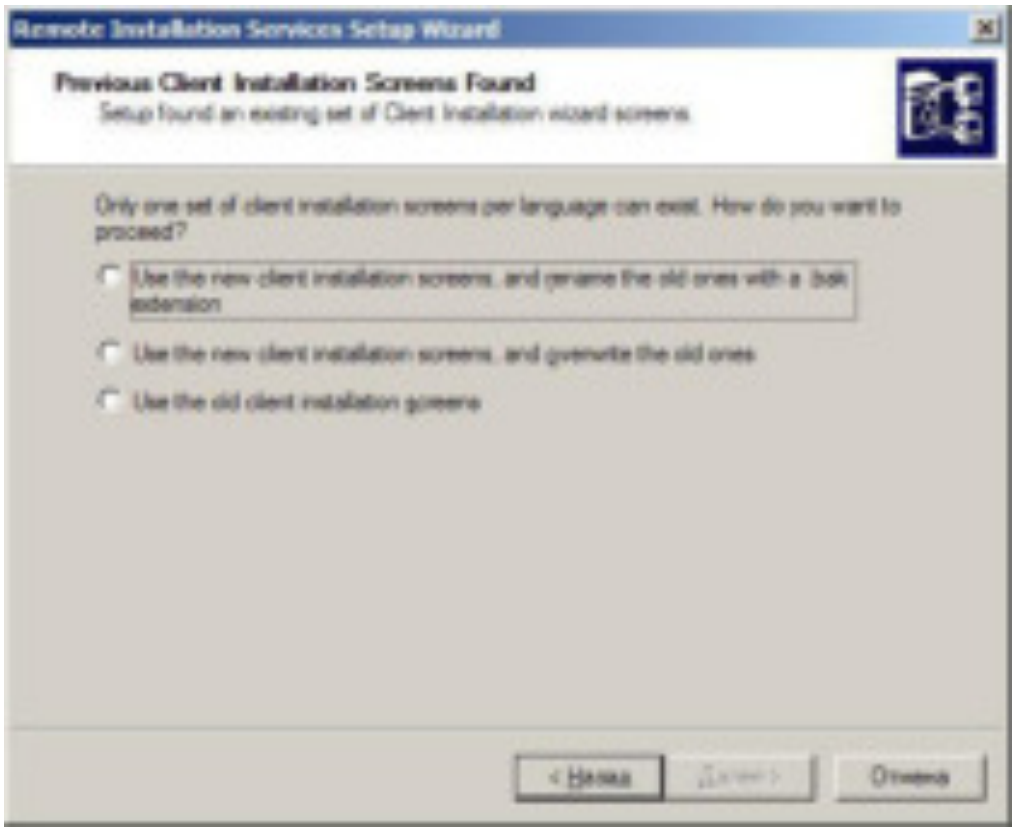

На первом шаге мастера необходимо указать путь к папке, содержащей установочные файлы нужной операционной системы. Для этих целей может использоваться как установочный компакт-диск, так и любая папка на локальном или сетевом диске, например, папка с интегрированным дистрибутивом ОС. Папка должна содержать в себе файлы, необходимые для идентификации дистрибутива (см. корневую папку установочного компакт-диска).

На следующем шаге мастера вы должны указать имя папки, в которую будут скопированы файлы, составляющие образ ОС.




Эта папка будет создана в папке **c:\RemoteInstall\Setup\язык\Images**. Рекомендуется имя папки строить по принципу название_ОС.редакция.пакет_обновления, например, для установочных файлов Windows 2000 Professional с интегрированным пакетом обновления 2 папку рекомендуется называть win2000.pro.sp2. Длина имени папки ограничена 39 символами (см. статью Q241427 Microsoft Knowledge Base).

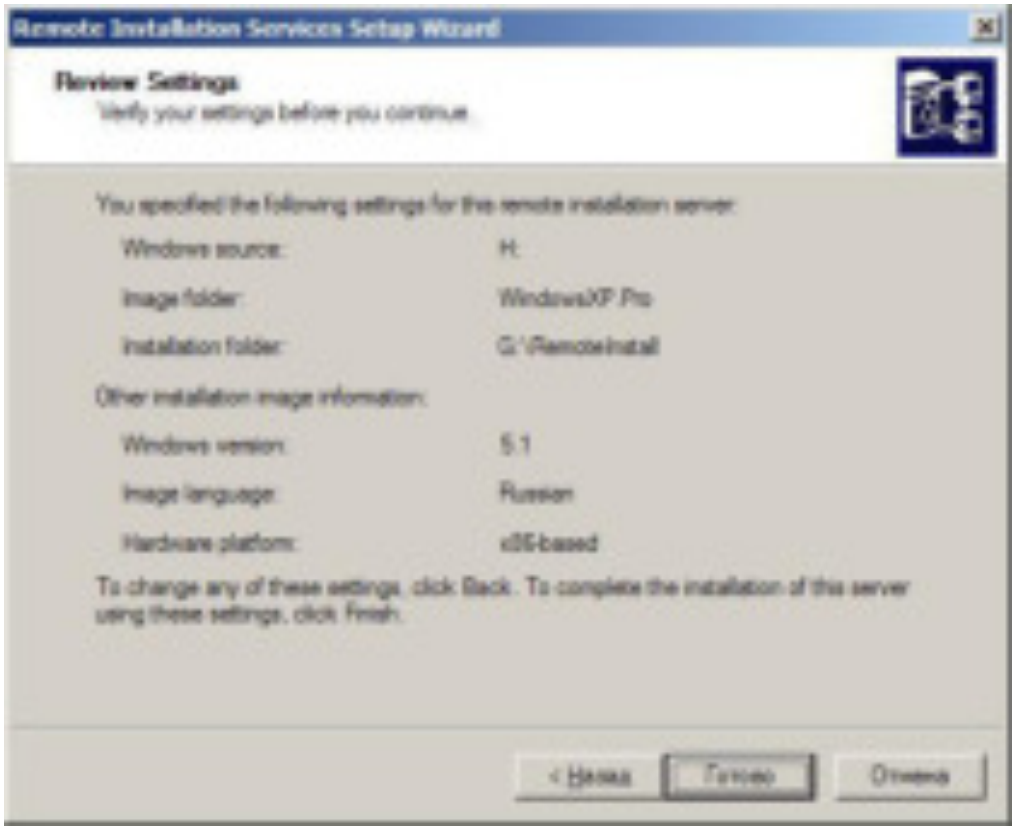



На следующем шаге мы должны определить, какие файлы экранов установки будут использоваться. Сервер удаленной установки Windows Server 2003 может использовать только один набор файлов для каждого языка хранимых образов.

Поэтому при добавлении нового образа ОС вам предлагается три варианта поведения:

- Использовать новый набор экранов и переименовать прежние экраны с расширением .bak - будет установлен новый набор файлов экранов; заменяемые файлы будут сохранены с расширением .bak;
- Использовать новый набор экранов и заменить прежние экраны - будет установлен новый набор файлов экранов; старые файлы сохранены не будут;
- Оставить для использования прежние экраны установки - мастер не выполняет никаких дополнительных операций с файлами экранов установки.




На следующем шаге выводится сводная информация о создаваемом образе. Если вы хотите изменить какие-то параметры образа, щелкните кнопку **Назад**. После щелчка по кнопке **Готово** будет запущен процесс создания нового образа.

В процессе добавления нового образа Windows выполняет следующие операции:

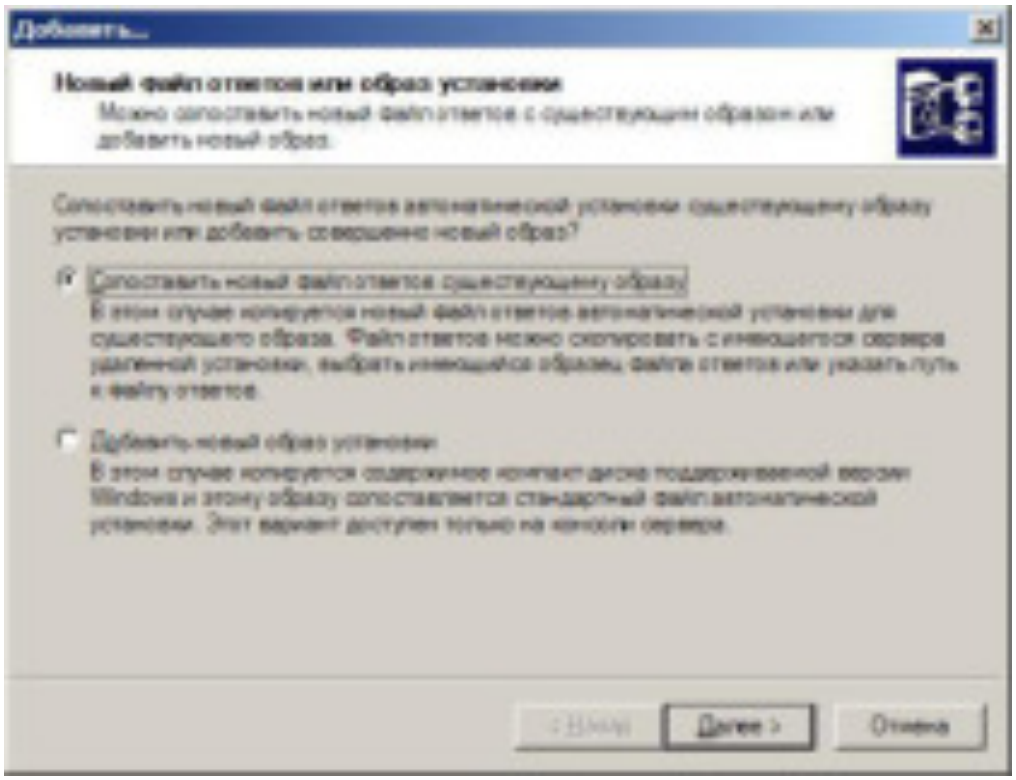
- Создает папку для хранения образа и копирует в нее необходимые файлы;
- Создает файл ответов для автоматической установки на основе файла txtsetup.sif, содержащегося в дистрибутиве Windows;

- При необходимости копирует файлы экранов удаленной установки;
- При необходимости запускаются необходимые службы удаленной установки.

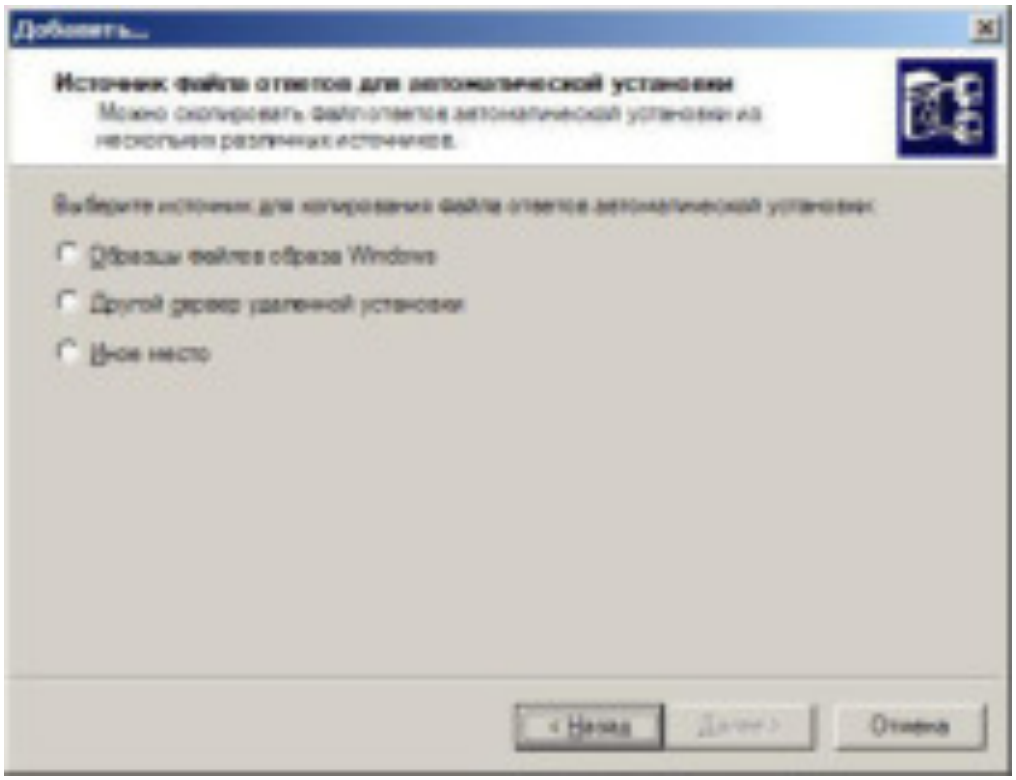
  После выполнения этих операций образ операционной системы будет создан.

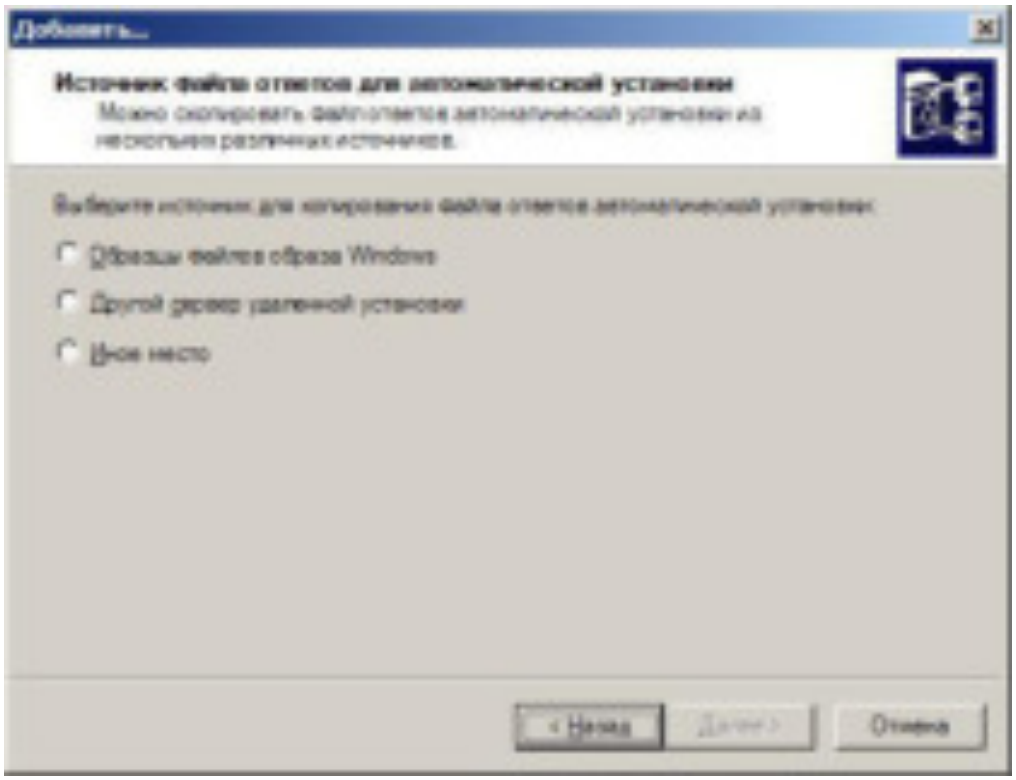

После установки образа ОС на сервер удаленной установки, этот образ появится в списке доступных образов на вкладке Образы окна свойств служб удаленной установки. Если этого не произошло, щелкните кнопку **Обновить** для обновления списка вручную.

**Установка дополнительных файлов ответов.** При необходимости иметь несколько различных вариантов установки ОС, базирующихся на одном и том же образе, совсем необязательно несколько раз устанавливать этот образ на сервер. Достаточно для уже существующего образа установить дополнительные файлы ответов. Эти файлы ответов будут отображаться в общем списке образов отдельными пунктами, однако при этом будет использоваться один комплект установочных файлов.
Для установки дополнительного файла ответов к уже установленному образу ОС необходимо щелкнуть кнопку **Добавить** на вкладке **Образы** окна свойств сервера удаленной установки.




В появившемся окне мастера необходимо установить переключатель в положение **Сопоставить новый файл ответов существующему образу** и щелкнуть кнопку **Далее.**






На следующем шаге мастера вы должны выбрать источник, из которого будет взят файл ответов. Вы можете выбрать один из следующих вариантов:

- **Образцы файлов образа Windows** - в качестве основы для нового файла ответов будет использован файл-шаблон txtsetup.sif одного из образов, установленных на сервере.
- **Другой сервер удаленной установки** - в качестве основы для нового файла ответов будет использован файл ответов одного из образов, установленных на другом сервере удаленной установки.
- **Иное место** - в качестве основы для нового файла ответов будет использован файл ответов, который вы укажете. Дальнейшие шаги мастера зависят от источника, выбранного вами.

## Практическое занятие №3 Настройка безопасности клиентских систем

***Цель работы:***
Изучить систему формирования политик безопасности домена. Научиться создавать подразделения домена с пользователями. Сформировать групповую политику для подразделения домена.

***Формирование политики безопасности домена***

1. Загрузить операционную систему Windows 2000 Server и виртуальную машину с ОС Windows XP.

2. В одноранговой сети параметры безопасности назначаются локально на каждом компьютере сети при помощи оснастки **Локальная политика безопасности**. На рабочих станциях домена политика безопасности формируется путем наложения на **Локальную политику безопасности** конкретного компьютера **Политики безопасности домена**, которая формируется централизованно на контроллере домена при помощи соответствующей оснастки **в меню Администрирование** (рис. 1 ,2).

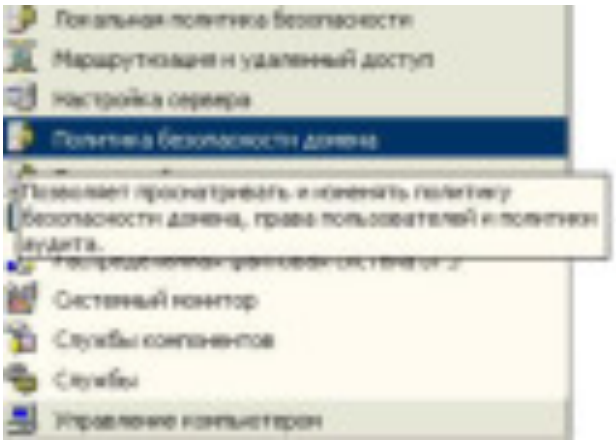



Рис.1. Меню **Администрирование** на контроллере домена

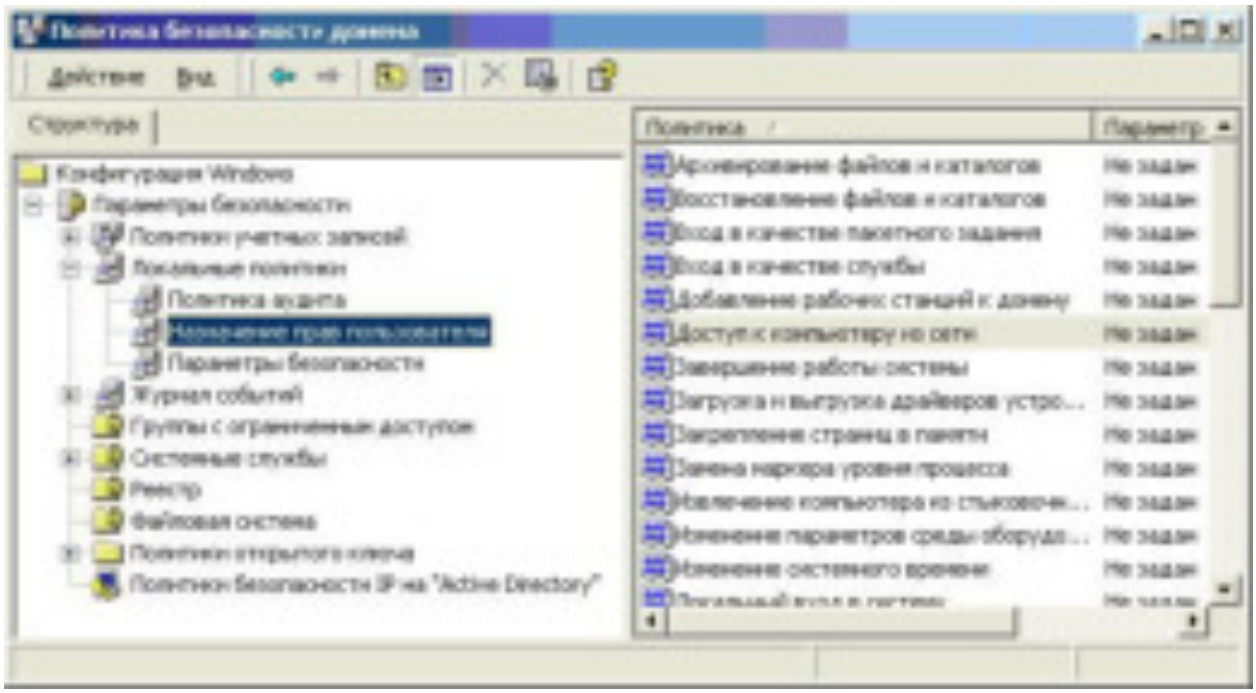



Рис. 2. Интерфейс оснастки **Политика безопасности домена**

При наличии в локальной политике безопасности и в политике безопасности домена одноименных параметров происходит их перекрытие, причем сначала в реестр загружаемой операционной системы компьютера записывается локальный параметр, а затем он замещается параметром домена.

Если в политике безопасности домена параметр локальной политики не задан, то действует локальный параметр.

Кроме этого, в домене для различных пользователей и компьютеров могут создаваться организационные единицы – **подразделения**, на которые могут назначаться **Групповые политики безопасности**, перекрывающие не только локальные политики безопасности, но и политики безопасности домена.

Групповая политика для пользователя определяет его возможности при работе на любой рабочей станции домена.

Групповая политика для компьютера определяет возможности любых пользователей домена при работе на этом компьютере.

Групповая политика может назначаться только подразделению. В меню оснастки **Active Directory – Пользователи и компьютеры** подразделение отображается как папка с пиктограммой в виде приоткрытой книги.

По умолчанию в домене создается только одно подразделение – **Domain Controllers** (рис. 3), членами которого являются компьютеры – контроллеры домена. Для них автоматически формируется специальная групповая политика, определяющая возможности допуска и работы на этих компьютерах различных пользователей домена. По умолчанию доступ к контроллерам домена обычным пользователям домена не разрешен.

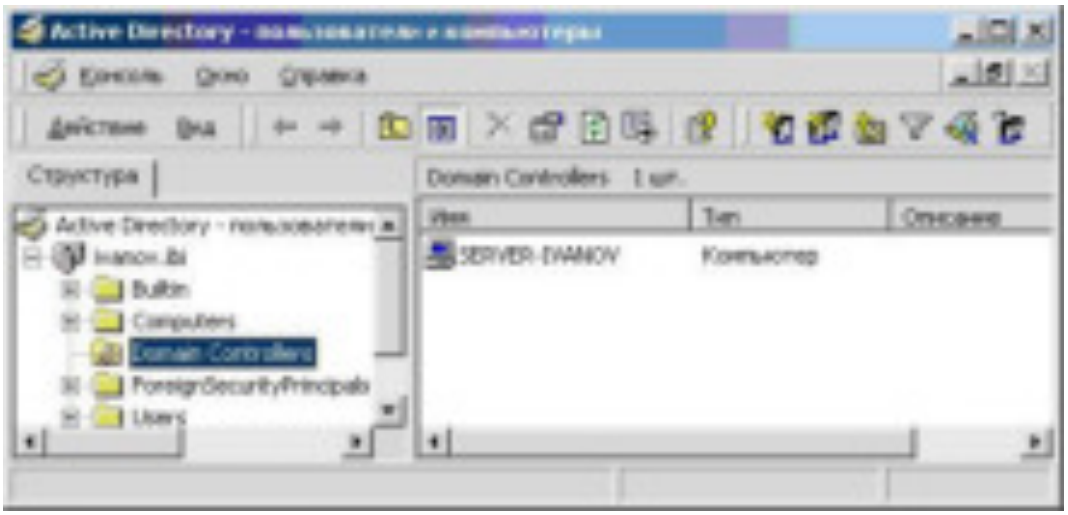



Рис. 3. Подразделение **Domain Controllers**

В свойствах подразделения (открываемых через контекстное меню) имеется закладка **Групповая политика** (рис.4), в которой можно создать необходимую групповую политику для членов этого подразделения или выбрать уже имеющуюся групповую политику (щелчком мыши) и открыть ее (двойным щелчком мыши или кнопкой **Изменить**).

Следует заметить, что одна из основных частей групповой политики подразделения **Domain Controllers** (рис.5), а именно **Параметры безопасности**, доступна также из меню **Администрирование** как **Политика безопасности контроллера домена** (рис.6).

Внутри любого подразделения могут создаваться другие подразделения со своими групповыми политиками, которые также участвуют в процессе перекрытия параметров безопасности. По умолчанию групповые политики вложенных (дочерних) подразделений перекрывают родительские.

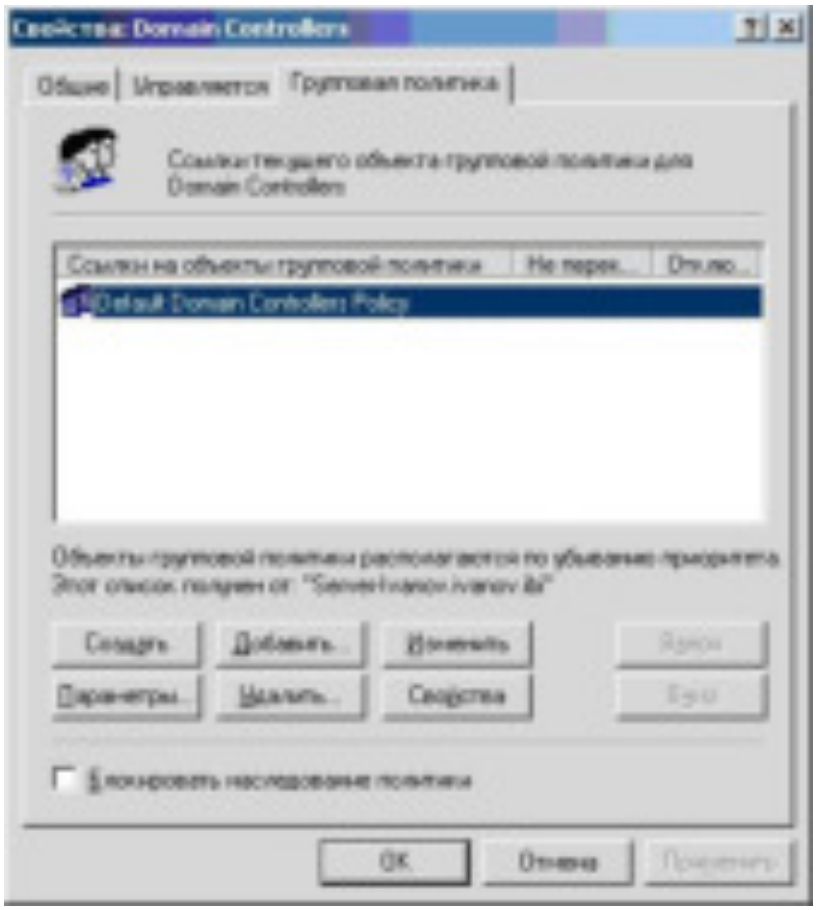



Рис.4. Вкладка **Групповая политика** в свойствах подразделения **Domain Controllers**

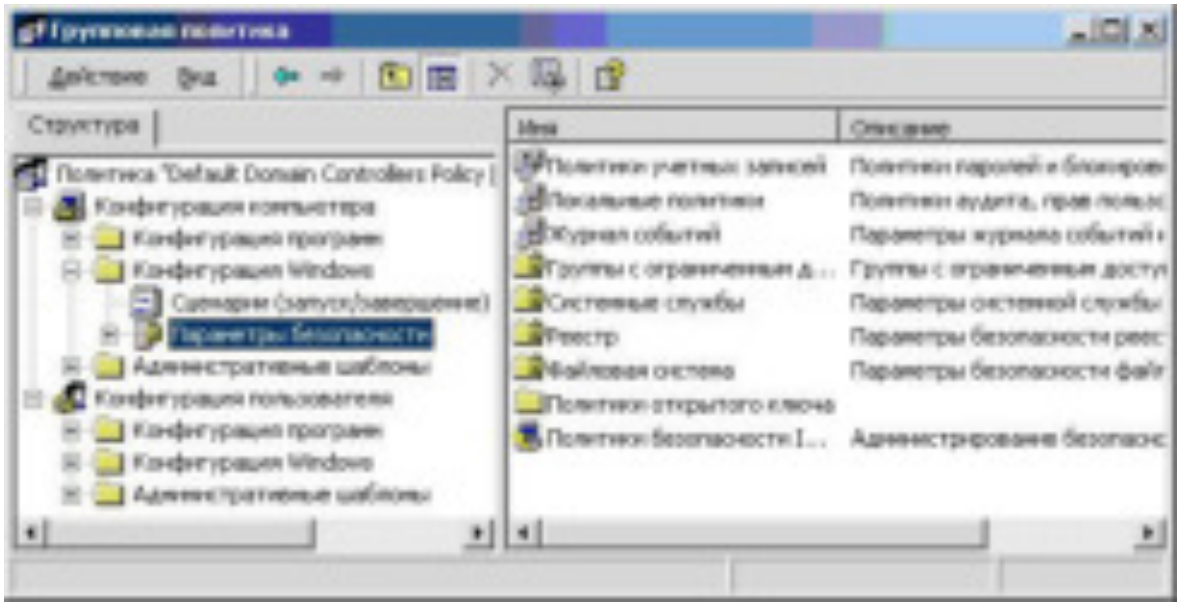


Рис.5. Состав групповой политики
подразделения **Domain Controllers**

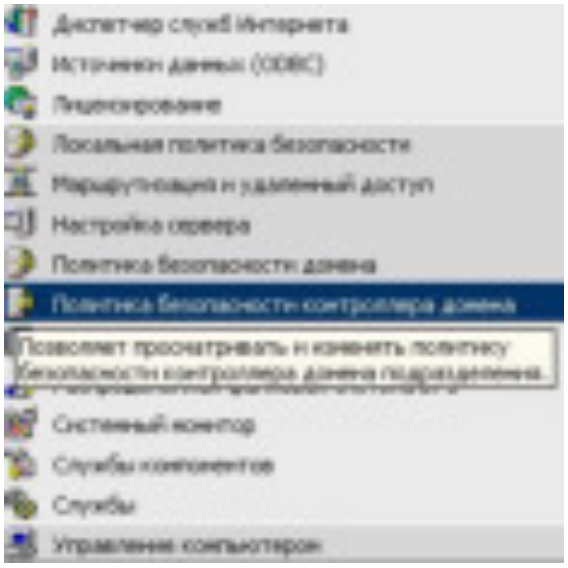



Рис.6. Пункт **Политика безопасности контроллера домена**
в меню **Администрирование**

Таким образом, политика безопасности домена в отношении конкретного пользователя формируется в результате перекрытия нескольких различных политик. Чтобы не возникло путаницы, рекомендуется пользоваться только групповыми политиками. Параметры локальной политики безопасности и политики безопасности домена следует изменять лишь в том случае, когда требуемые параметры безопасности нельзя реализовать при помощи групповых политик.

Для реализации этого правила все пользователи и компьютеры распределяются по подразделениям, на которые назначены необходимые групповые политики.

Если какие-то параметры безопасности нужно применить ряду подразделениям, то эти подразделения включаются в одно общее подразделение с общей групповой политикой.

Если многим пользователям требуется применить одинаковую политику безопасности, но эти пользователи находятся в разных подразделениях, то можно назначить одну групповую политику нескольким подразделениям.

***Создание подразделения домена***

1. На контроллере домена открыть оснастку **Active Directory – Пользователь и компьютеры**.

2. В контекстном меню домена с помощью пункта **Создать – Подразделение** (рис.7) сформировать подразделение домена с именем **студенты** (рис.8).

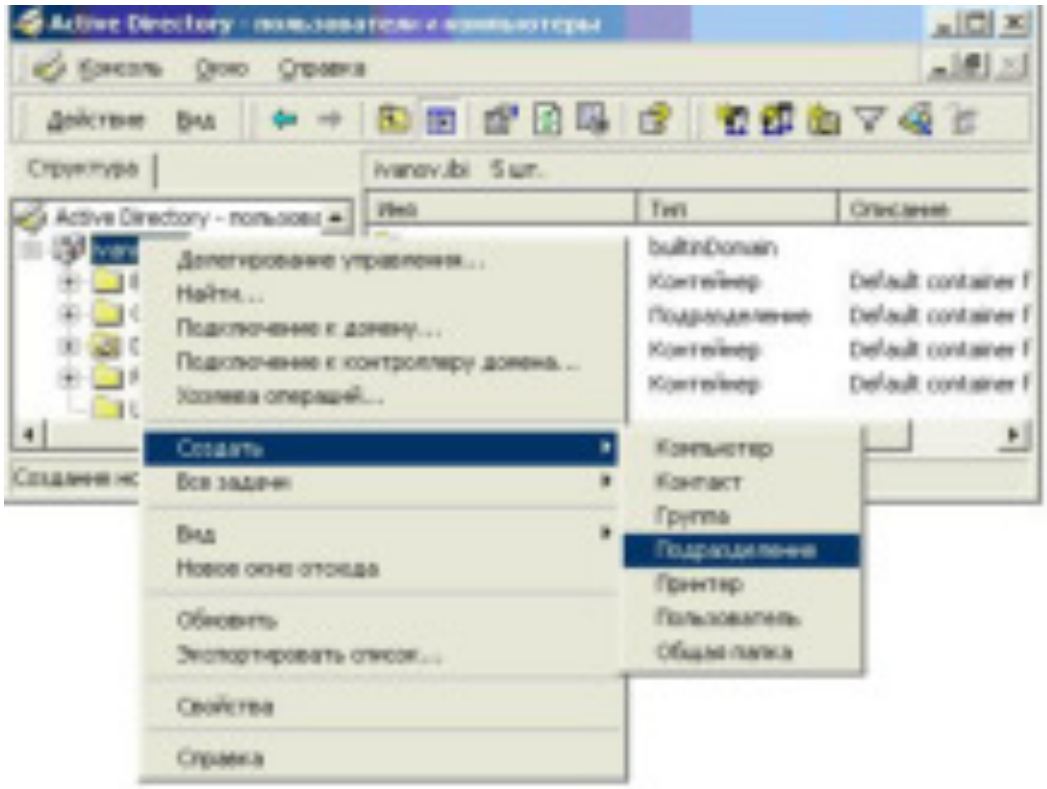



Рис.7. Создание подразделения

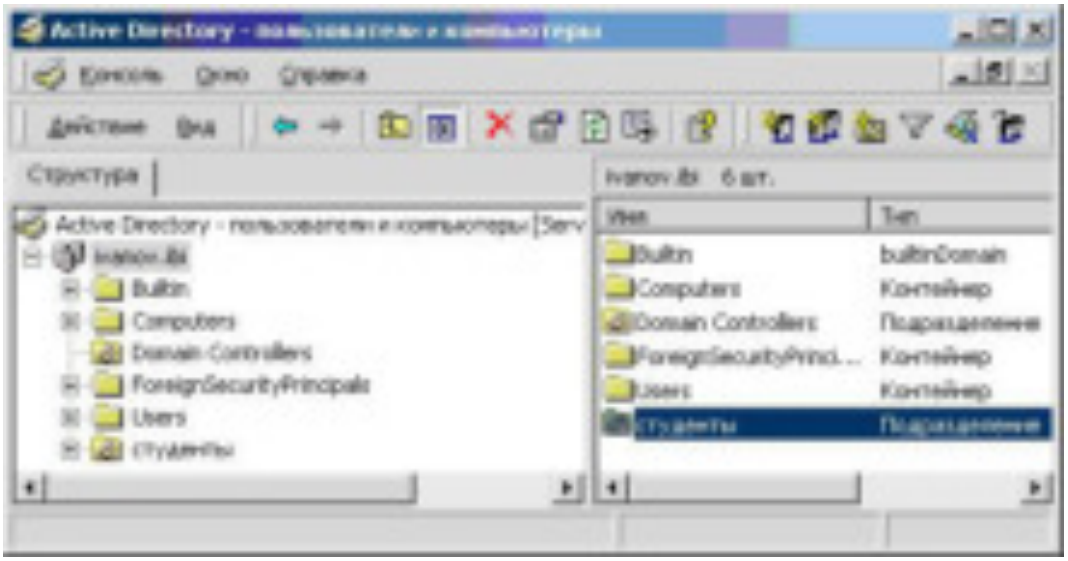



Рис.8. Пример подразделения с именем **студенты**

3. Путем копирования имеющейся учетной записи **студент** создать новые учетные записи пользователей **Петров**, **Сидоров** и **Пиров** с именами входа соответственно **petrov**, **sidorov**, **pirov** и паролем **123**.
4. Создать группу пользователей **студенты** как глобальную группу и включить в нее созданных пользователей (рис.9,10).

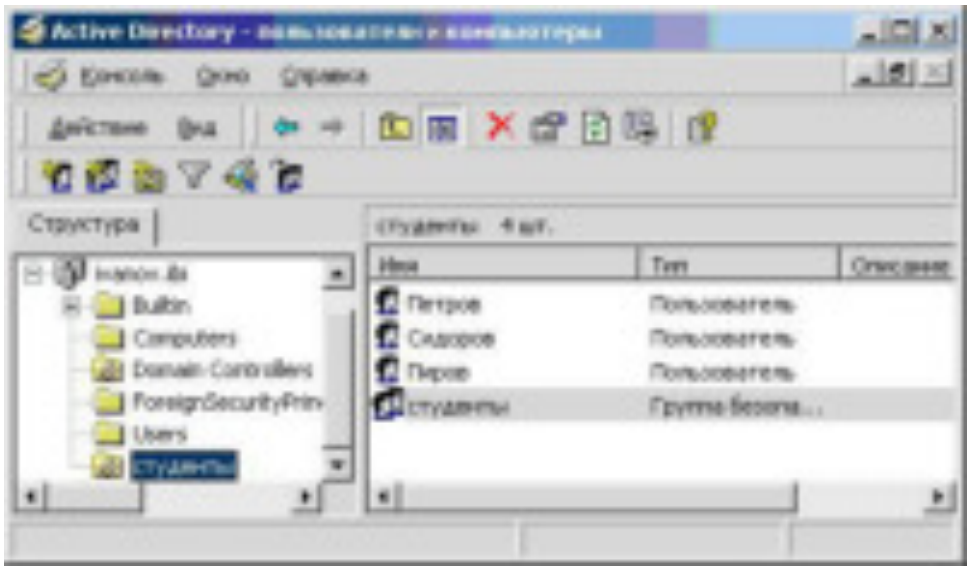



Рис.9. Состав подразделения **студенты**

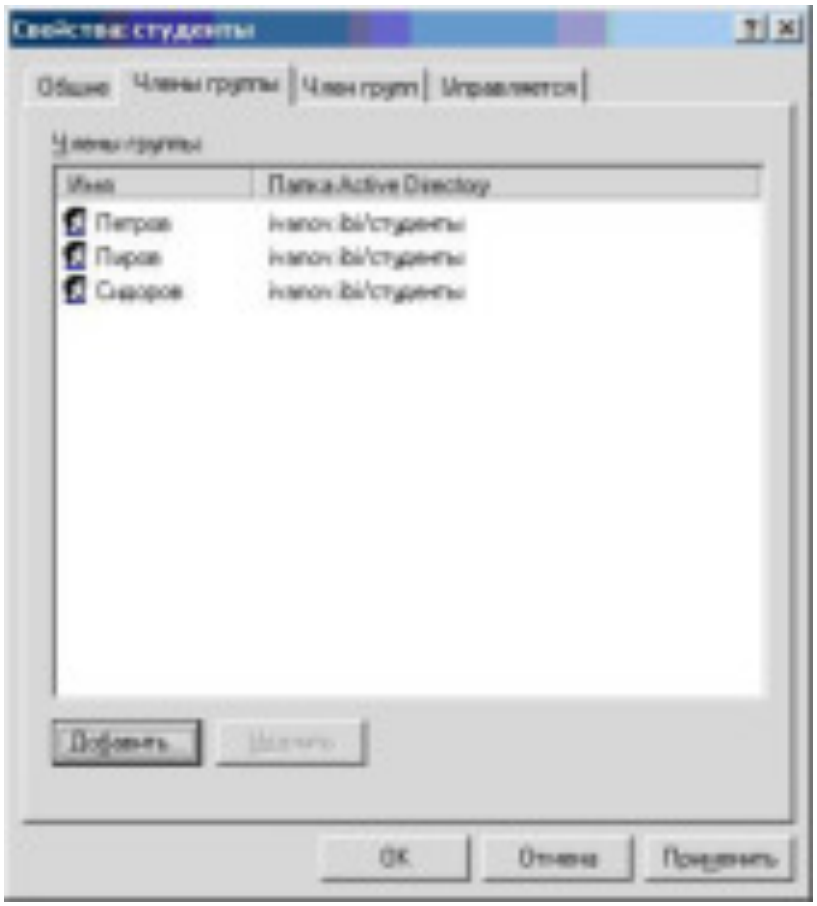



Рис.10. Состав группы пользователей **студенты**

***Создание групповой политики безопасности домена***

К членам подразделения могут применяться **групповые политики** безопасности. Членами подразделения могут быть как пользователи, так и компьютеры. Следует отметить, что включение в подразделение **группы**

**пользователей** домена не ведет к автоматическому включению в это подразделение членов указанной группы пользователей.

Для создания групповой политики подразделению **студенты** выполнить следующие действия:

1. При помощи контекстного меню подразделения **студенты** открыть свойства и выбрать закладку **Групповая политика** (рис.11).
2. При помощи кнопки **Создать** назначить новый объект групповой политики с именем **групповая политика студенты** (рис.12).

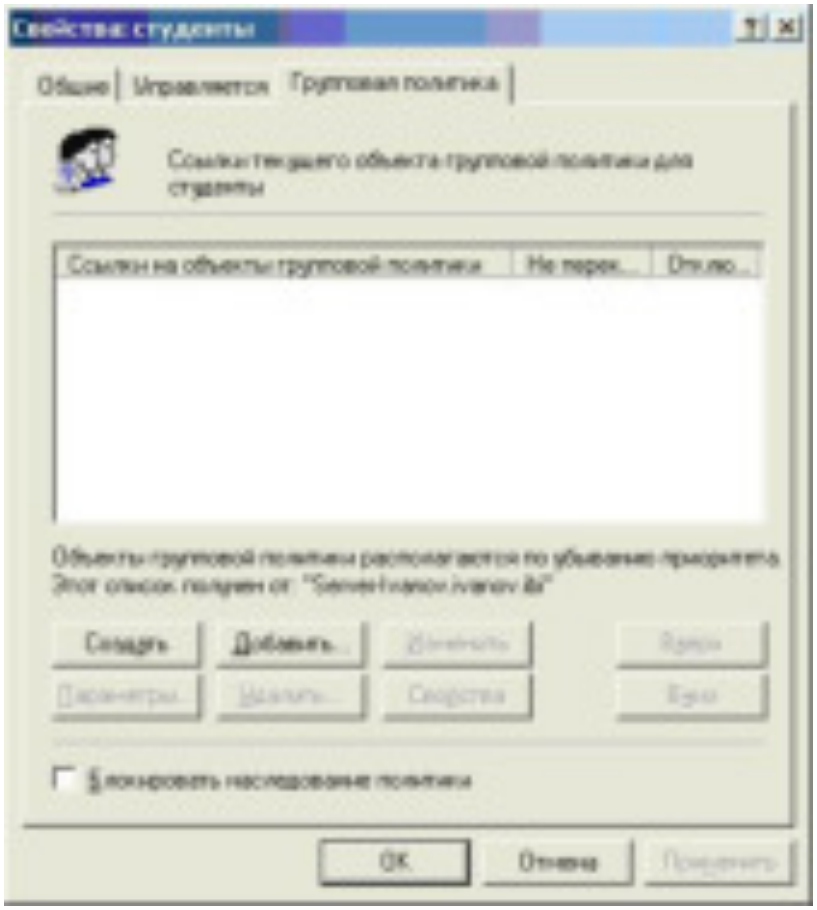



Рис.11. Вкладка **Групповая политика** в свойствах подразделения **студенты**

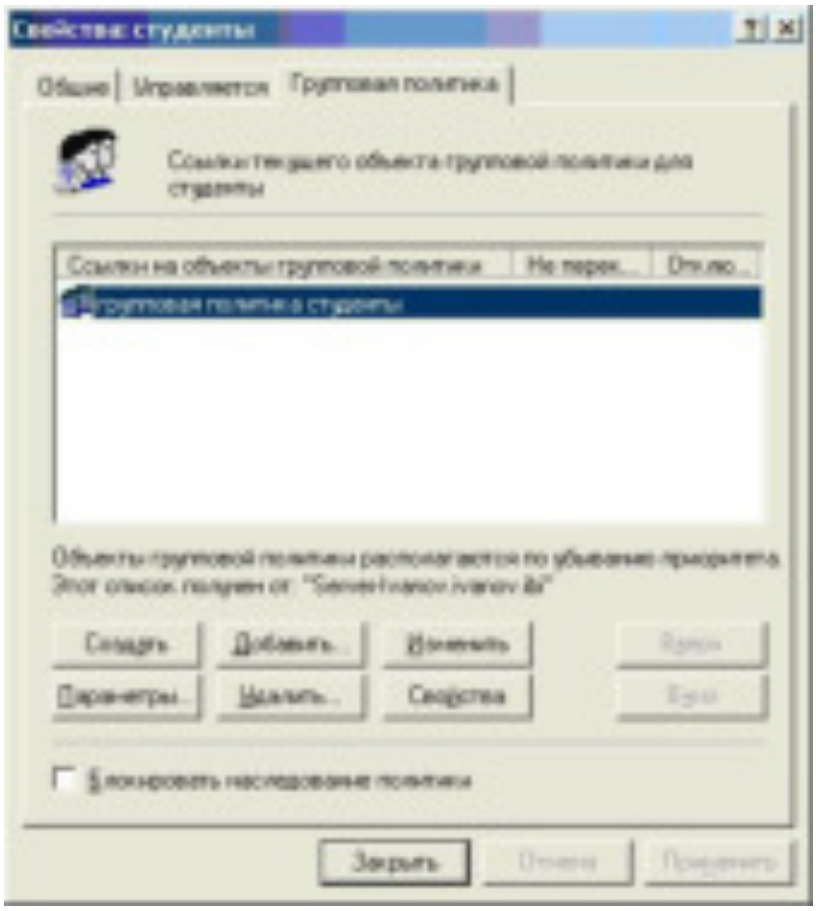



Рис.12. Назначение объекта групповой политики **групповая политика студенты**

3. Двойным щелчком мыши по выбранному объекту групповой политики или при помощи кнопки **Изменить** открыть окно управления параметрами созданной групповой политики (рис.13).

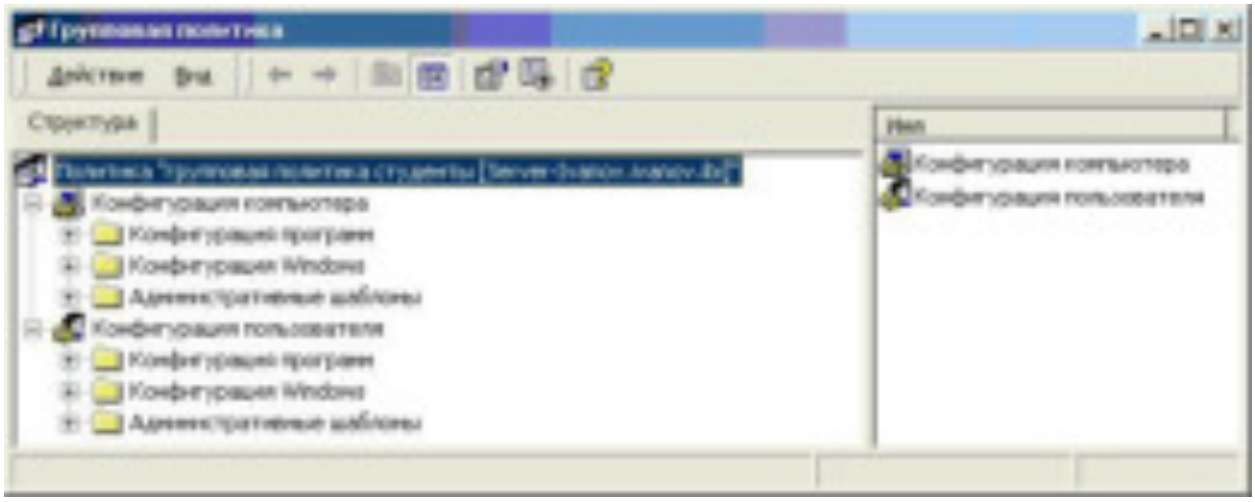



Рис.13. Состав объекта групповой политики

Каждая групповая политика (см. рис.13) имеет следующую структуру:

- **Конфигурация компьютера,** определяющая параметры компьютера при работе пользователя. Изменения этих политик применяются к рабочей станции при ее перезагрузке или через заданный интервал времени в

результате фонового обновления. На практике рекомендуется не включать фоновое обновление групповых политик.

- **Конфигурация пользователя**, определяющая настройки профиля пользователя на клиентской рабочей станции. Изменения этих политик применяются к рабочей станции при смене сеанса работы пользователя или через заданный интервал времени в результате фонового обновления.

В обеих частях имеются следующие узлы групповой политики (рис.14):

- **Конфигурация программ**, позволяющая задавать различные режимы установки новых программ на компьютере пользователя.
- **Конфигурация Windows**, служащая для настройки параметров системы безопасности компьютеров, на которые действует данная групповая политика.
- **Административные шаблоны**, задающие параметры реестра, рабочего стола, компонент операционной системы и приложений.

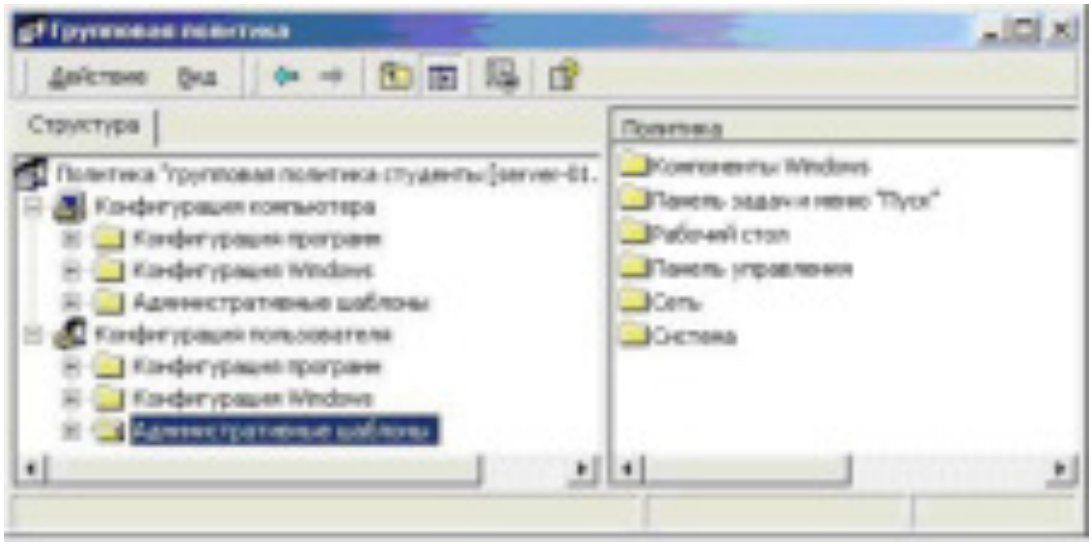



Рис.14. Состав компонента **Административные шаблоны** групповой политики

Наиболее часто в компьютерной сети фирмы (организации) необходимо конфигурировать параметры профиля пользователей, большая часть которых находится в компоненте **Административные шаблоны Конфигурации пользователя** (рис.14).

Настроить профиль пользователей, входящих в подразделение студенты, так, чтобы в программе **Проводник** в разделе меню **Сервис** отсутствовала команда **Свойства папки**, позволяющая открыть просмотр системных и скрытых файлов. Для этого необходимо выполнить следующие действия:

4. Открыть папку **Конфигурация пользователя – Административные шаблоны – Компоненты Windows** – **Проводник** и выбрать политику **Удалить команду «свойства папки» из меню «Сервис»** (рис.15).

5. Двойным щелчком мыши открыть свойства выбранной политики и включить выбранную политику (рис.16).

Открыть закладку **Объяснение** и изучить действие выбранной политики (рис.17). При помощи кнопок **Предыдущая политика** и **Следующая политика** можно изучать другие политики и управлять их назначением.

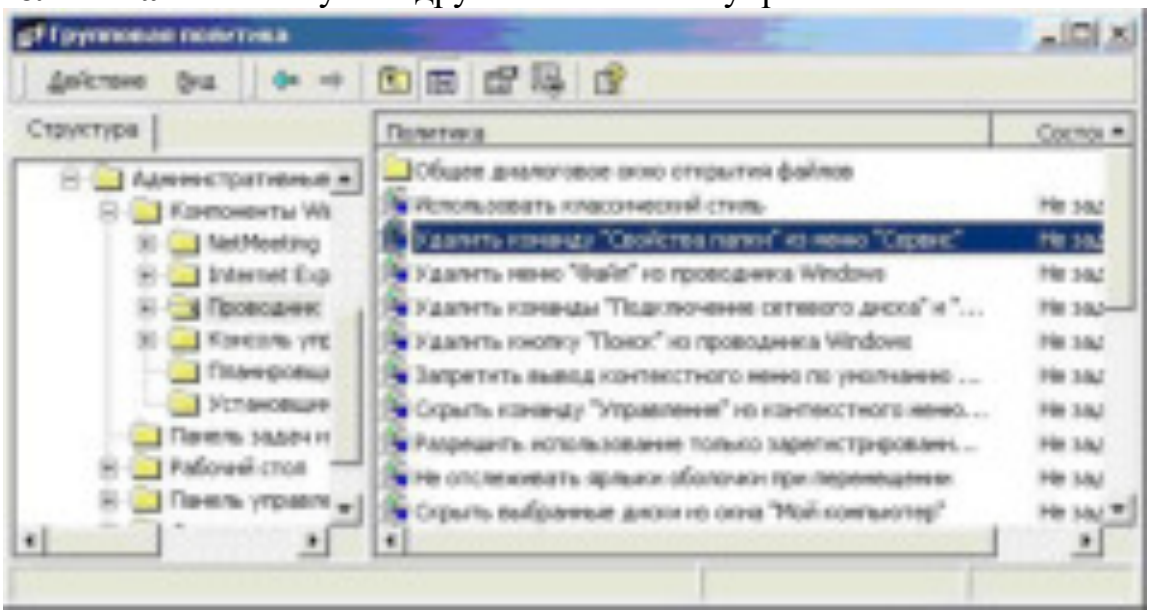



Рис.15. Состав возможных политик компонента **Проводник**

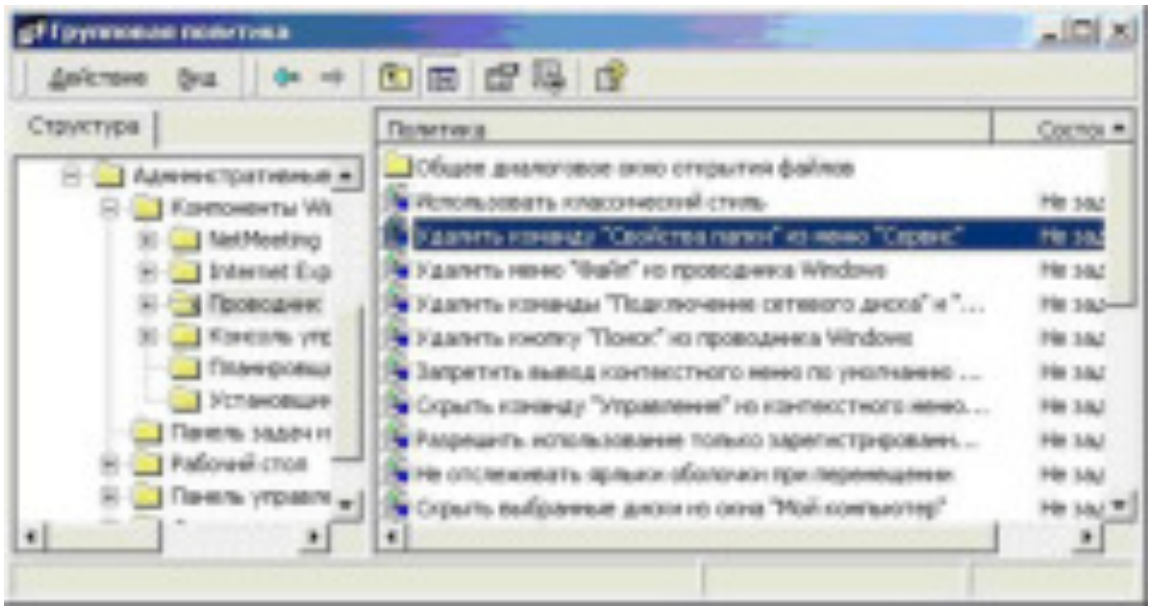



Рис.16. Пример свойств выбранной политики


Рис.17. Пример объяснения действия выбранной политики

6. Проверить действие выбранной политики на рабочей станции домена. Для этого войти в систему на виртуальной машине одним из пользователей подразделения **студенты**. Следует напомнить, что

политики узла **Конфигурация пользователя** применяются на любом компьютере при входе пользователя в домен.

7. В групповой политике подразделения **студенты** включить политику **Удалить команду «Выполнить» из меню «Пуск»** (рис.18), изучить объяснение выбранной политики и проверить ее действие. Рис.18. Политика **Удалить команду «Выполнить» из меню «Пуск»**
8. Изучить другие возможные политики узла **Конфигурации пользователя – Административные шаблоны**.

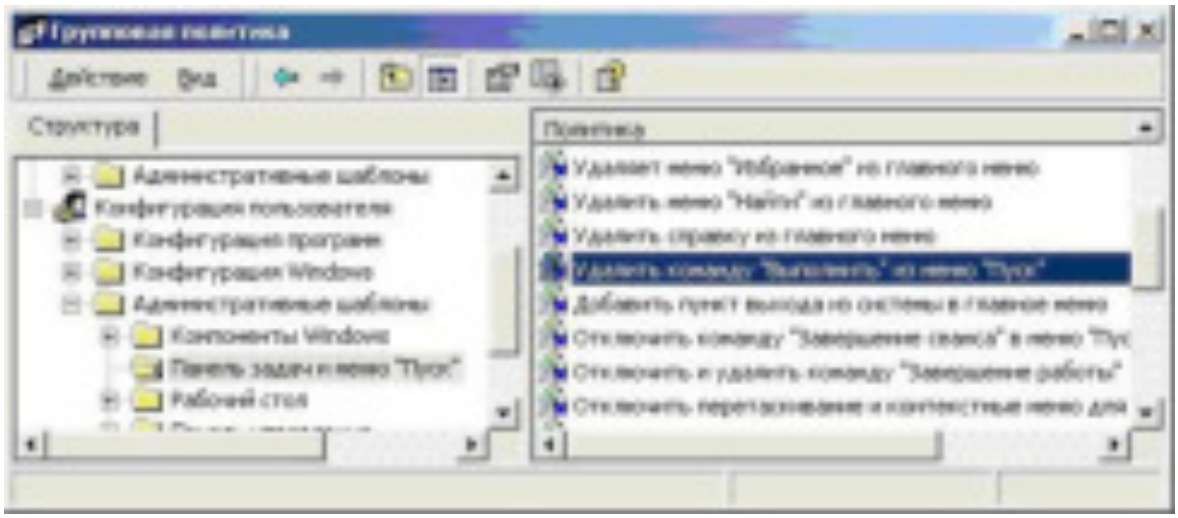



Рис. 8.18. Политика **Удалить команду «Выполнить» из меню «Пуск»**

### *Перенаправление папки Мои документы на домашнюю папку пользователя*

Среди политик узла **Конфигурация пользователя – Конфигурация Windows** полезно использовать политику **Перенаправление папки**, позволяющую в профиле пользователя перенаправить папку **Мои документы** на домашнюю папку пользователя.

Отметим преимущества перенаправления папки **Мои документы**.

Некоторые из следующих преимуществ относятся к перенаправлению любой папки, но перенаправление папки **Мои документы** может быть особенно выгодным, поскольку эта папка со временем увеличивается.

- Даже если пользователь входит в сеть с различных компьютеров, все документы всегда доступны.
- При использовании перемещаемого профиля пользователя только сетевой путь к папке **Мои документы** является его частью, а не сама папка. Поэтому ее содержимое не нужно копировать и перемещать между клиентом и сервером каждый раз при входе пользователя в систему или его выходе, что ускоряет процессы входа и выхода.

- Сетевой администратор может архивировать данные, хранящиеся на сервере. Это является более безопасным, поскольку не требуется вмешательство пользователя.
- Системный администратор может устанавливать дисковые квоты с помощью групповой политики, ограничивая дисковое пространство, выделенное пользователю для домашних папок.
- Данные пользователя могут быть перенаправлены на жесткий диск локального компьютера с другого жесткого диска, на котором хранятся системные файлы. Это обезопасит пользовательские файлы, если необходимо будет переустановить операционную систему.

10. В групповой политике подразделения **студенты** выбрать политику **Конфигурация пользователя – Конфигурация Windows – Перенаправление папки – Мои документы** (рис.19) и открыть ее свойства (рис.20).
11. В свойствах выбрать политику **Перенаправлять папки всех пользователей в одно место** и указать сетевой путь к конечной папке (рис.21). При этом можно воспользоваться кнопкой **Обзор**, позволяющей указать размещение в сети каталога **Homedir** (рис.22), в котором расположены домашние папки пользователей созданного домена. Чтобы пользователи получали доступ к своим домашним папкам, имя папки следует указать при помощи переменной **%Username%** (рис.21).

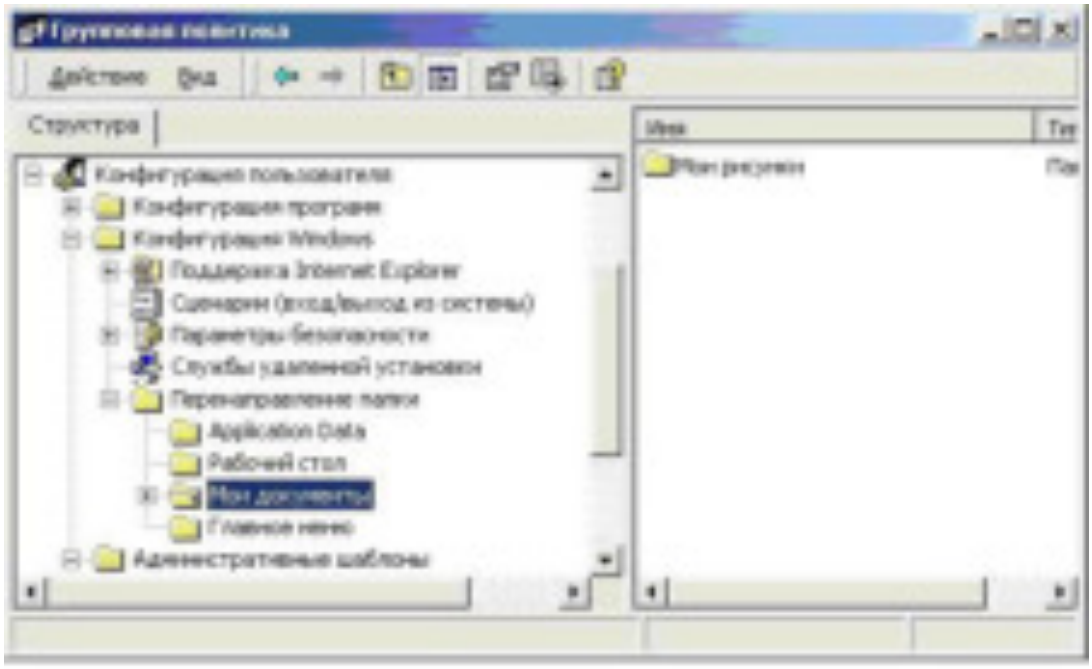



Рис.19. Политика **Перенаправление папки Мои документы**

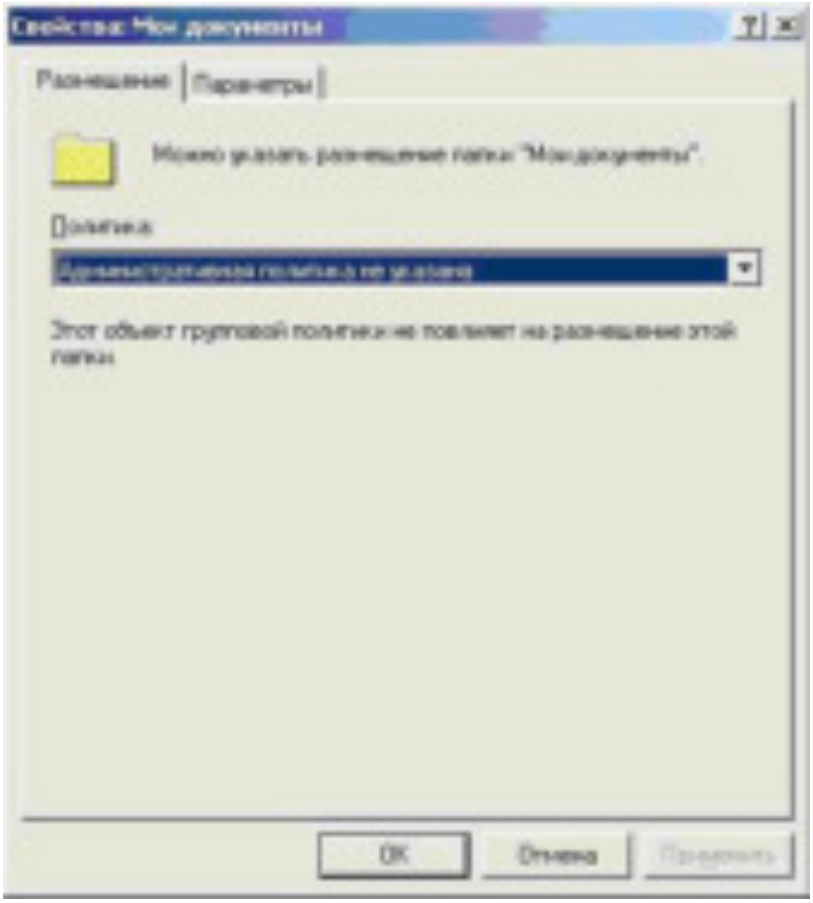



Рис.20. Окно свойств политики **Перенаправление папки Мои документы**

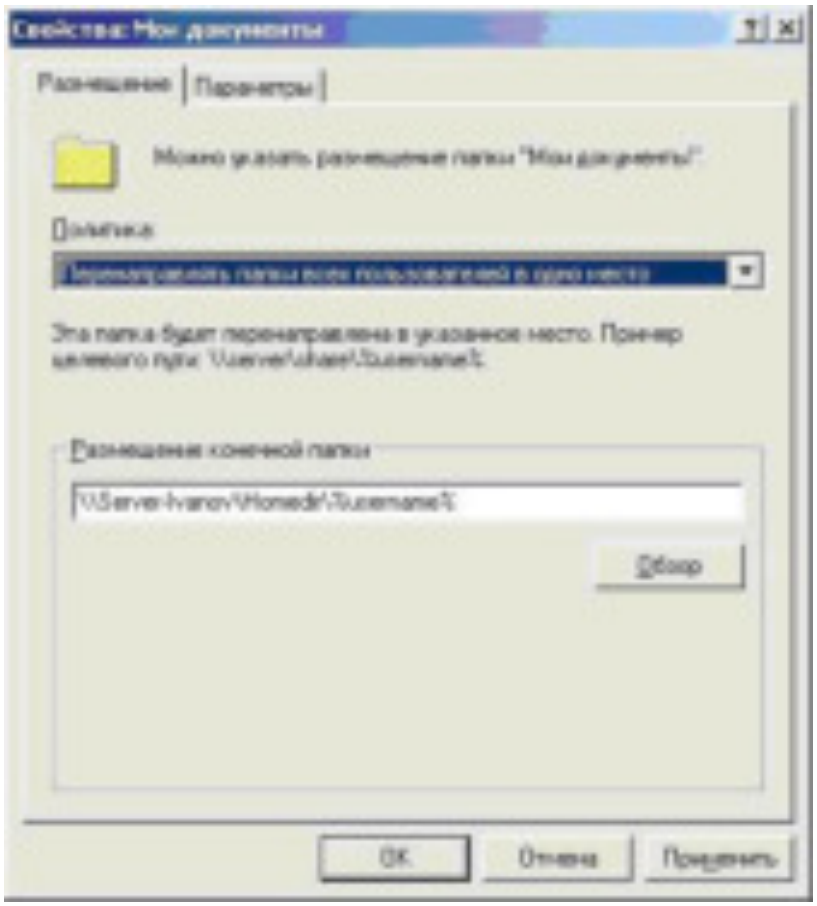



Рис.21. Формирование политики перенаправления папки **Мои документы** на домашнюю папку пользователя

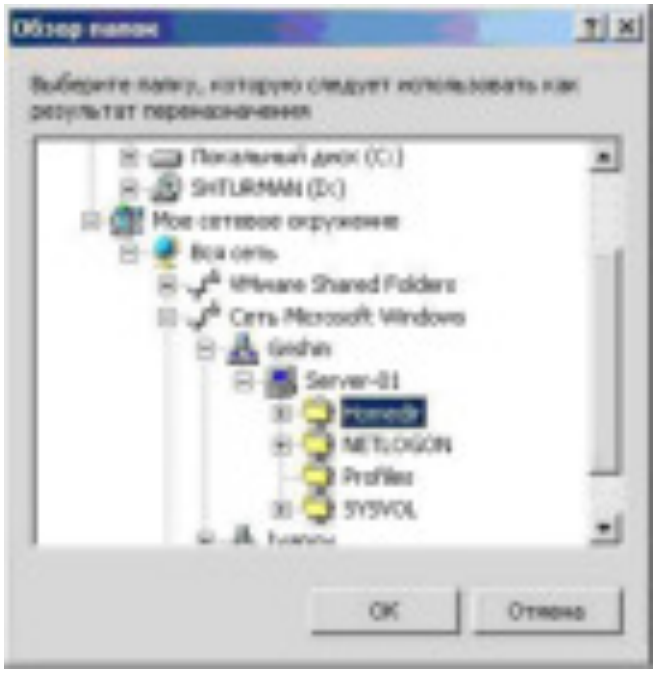



Рис.22. Указание сетевого пути к каталогу размещения домашних папок пользователей

12. Проверить действие политики перенаправления папки **Мои документы**. Для этого войти на рабочую станцию домена пользователем

подразделения **студенты**, сохранить произвольный документ в папке **Мои документы** и убедиться, что этот документ появился на сетевом диске **Z**.

## Практическое занятие №4 Настройка шифрования файлов с помощью EFS

***Цель работы:***

Изучить как работает шифрование EFS. Как зашифровать папки и файлы с помощью EFS. Как выполнить восстановление доступа к зашифрованным EFS данным или осуществить доступ к ним под другой учетной записью. Отличия шифрования Bitlocker и EFS в Windows

### Как работает шифрование EFS

EFS позволяет легко выполнить шифрование содержимого выбранных папок или отдельные файлы с помощью средств системы таким образом, что они будут доступны только для пользователя и на том компьютере, где выполнялось шифрование.

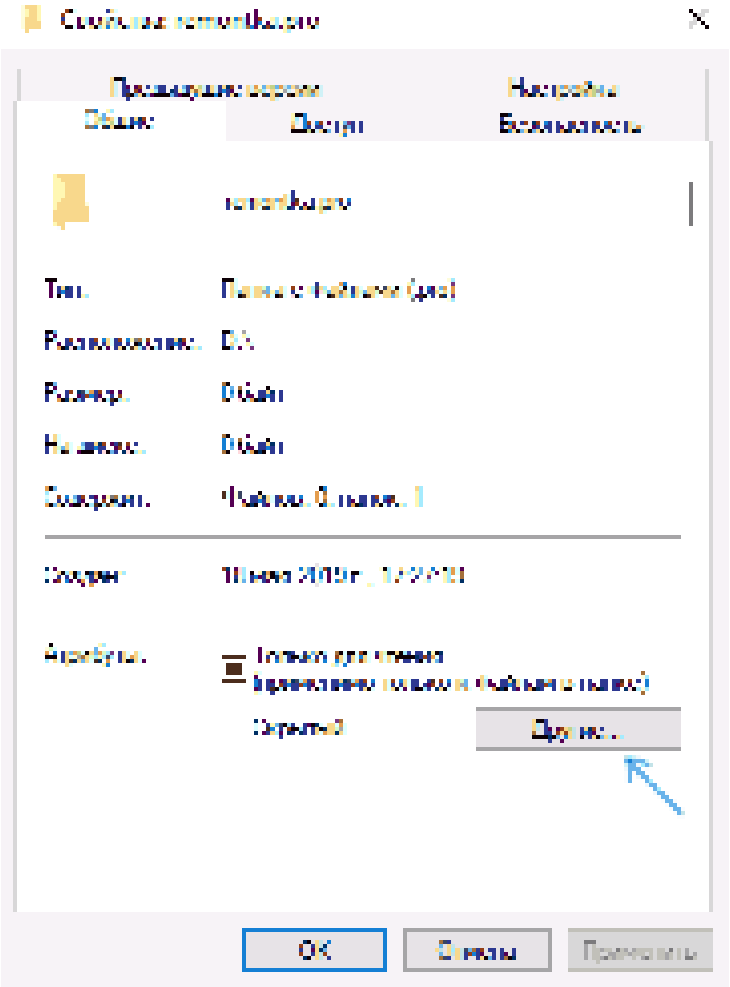
Другие пользователи на этом же или другом компьютере будут видеть файлы и их имена на накопителе, но не смогут получить доступ к ним (открыть их), даже если они имеют права администратора.

Этот способ менее безопасен чем шифрование Bitlocker, но если в вашем распоряжении лишь домашняя редакция Windows 10, 8.1 или Windows 7, а единственная задача — не дать пользователям других учетных записей просмотреть содержимое ваших файлов, вполне можно использовать и EFS: это будет удобно и быстро.

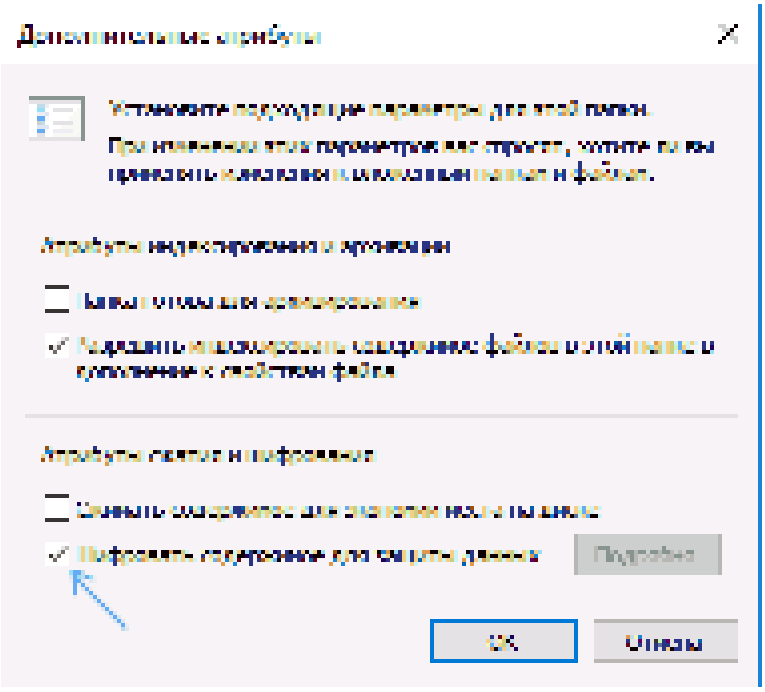
### Как зашифровать папки и содержащиеся в них файлы с помощью EFS

Шаги для шифрования папки и его содержимого с помощью шифрующей файловой системы EFS в самом простом варианте будут следующими (доступно только для папок на NTFS дисках и флешках):

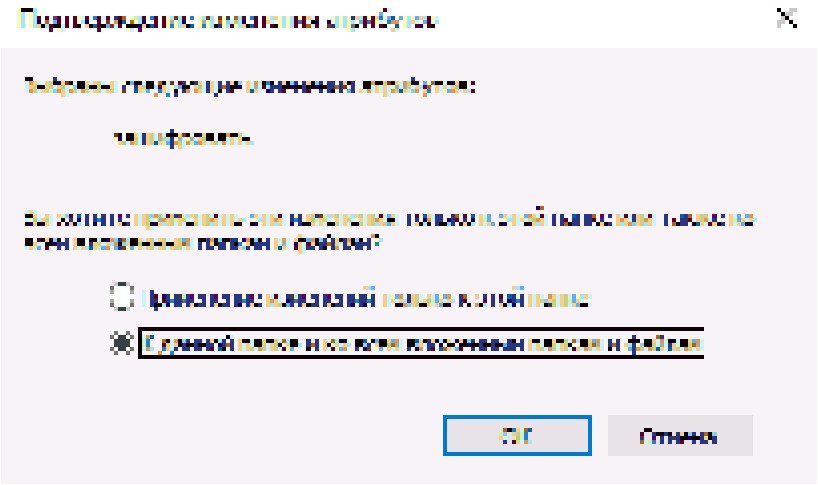
1. Откройте свойства нужной папки (правой кнопкой мыши — свойства).
2. В разделе «Атрибуты» нажмите кнопку «Другие».



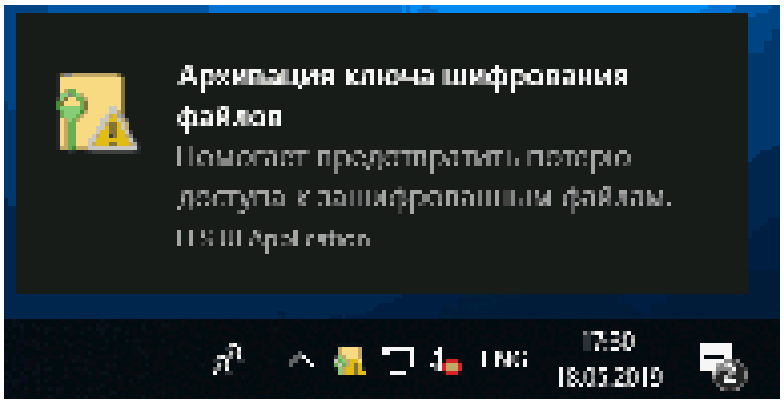
3. В разделе «Атрибуты сжатия и шифрования» в следующем окне отметьте «Шифровать содержимое для защиты данных» и нажмите «Ок».



4. Нажмите «Ок» в свойствах папки и примените изменения к вложенным файлам и папкам.

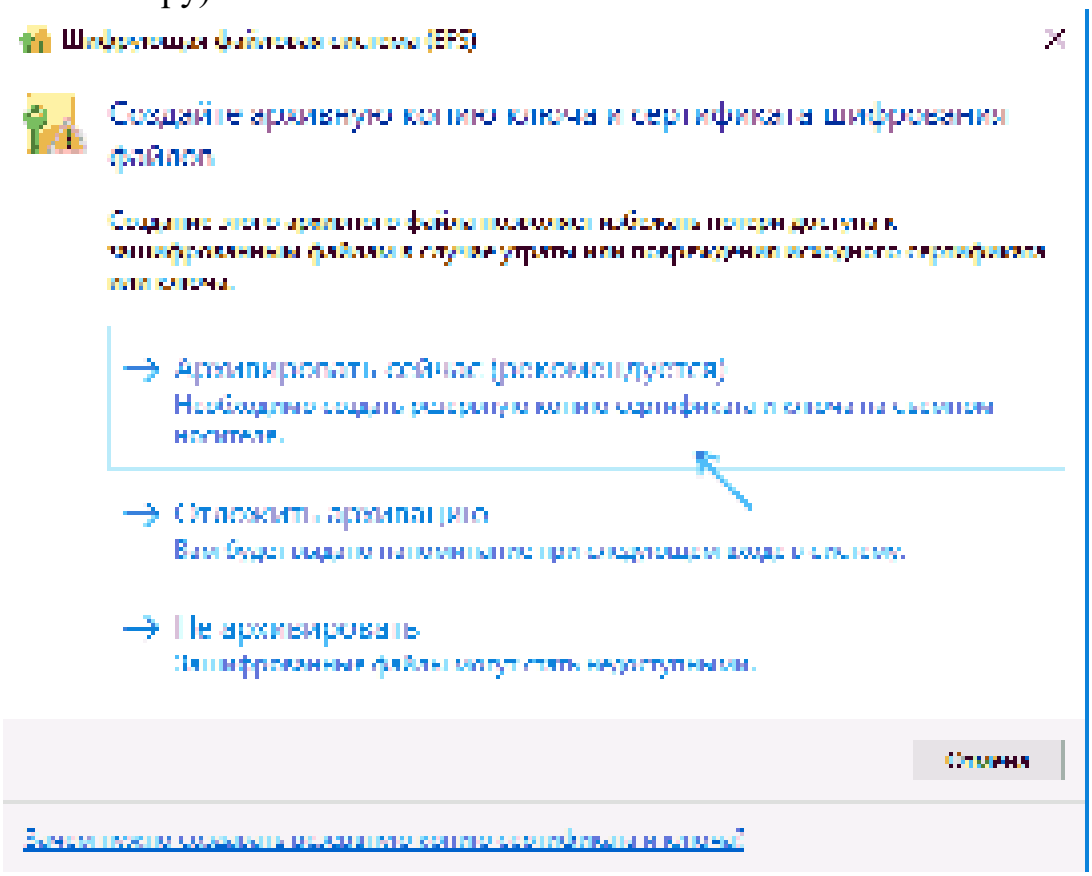


5. Сразу после этого появится системное уведомление, где вам предложат выполнить архивацию ключа шифрования. Нажмите по уведомлению.



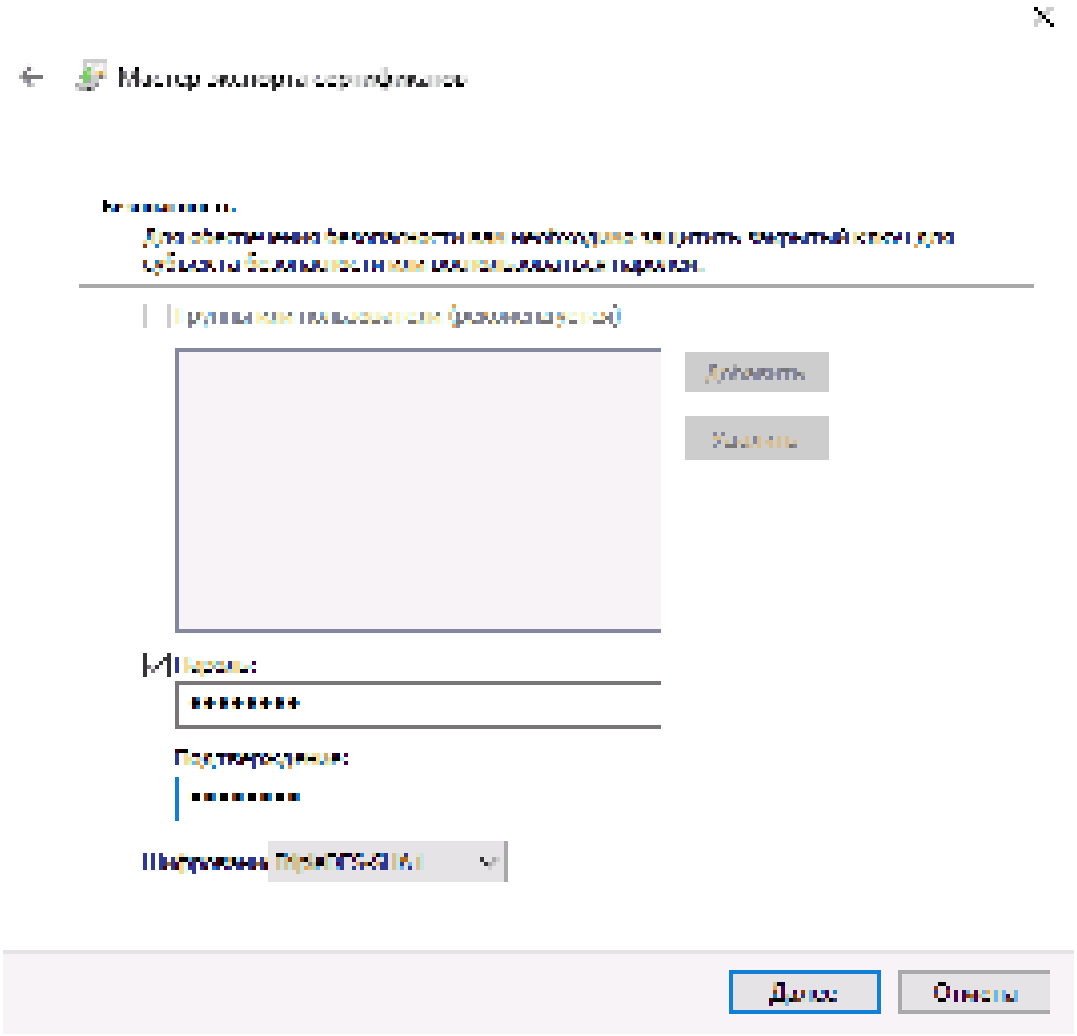

6. Нажмите «Архивировать сейчас» (ключ может потребоваться для восстановления доступа к данным, если вы потеряли свою учетную запись или доступ к этому

компьютеру).



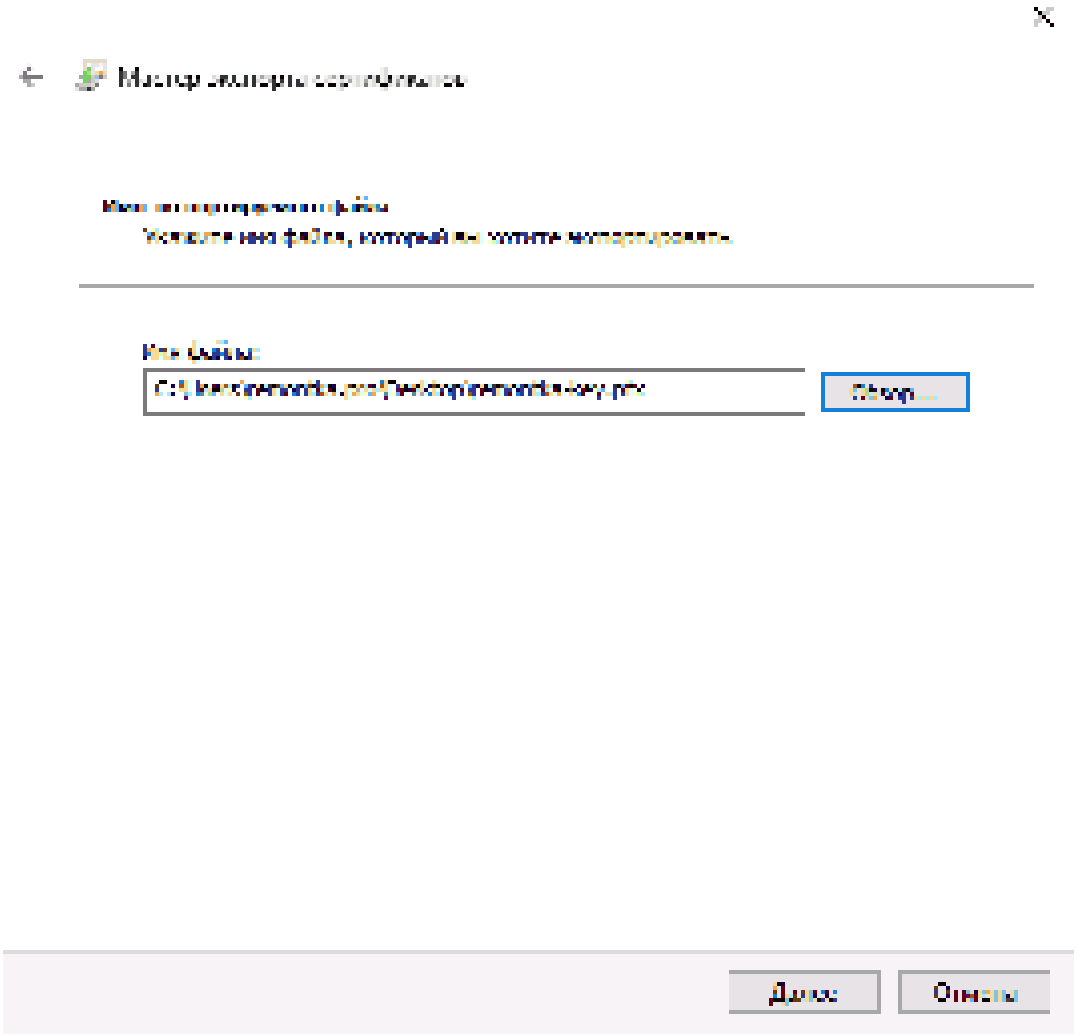

7. Запустится мастер экспорта сертификатов. Нажмите «Далее» и оставьте параметры по умолчанию. Снова нажмите «Далее».

8. Задайте пароль для вашего сертификата, содержащего ключи шифрования.

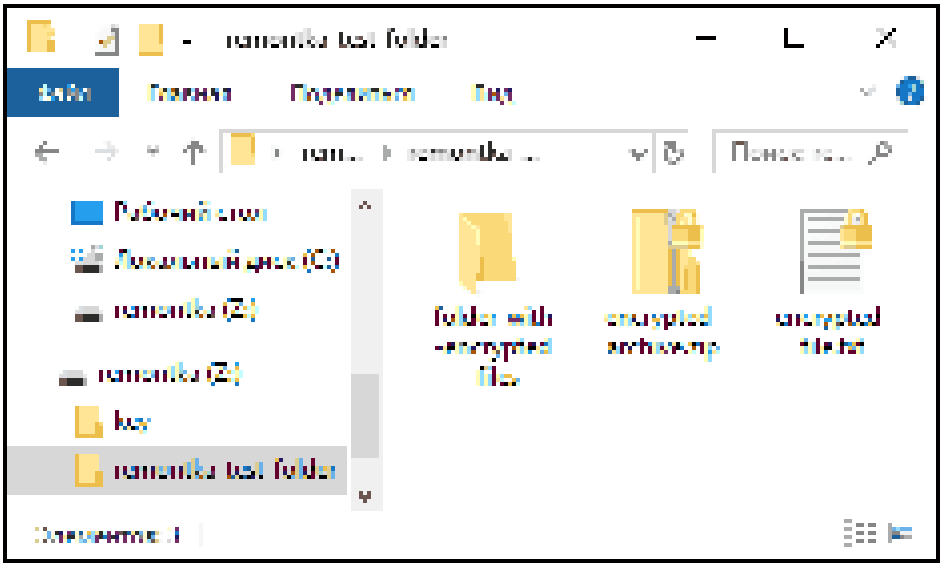


9. Укажите место хранения файла и нажмите «Готово». Этот файл пригодится для восстановления доступа к файлам после сбоев ОС или при необходимости иметь возможность открывать зашифрованные EFS файлы на другом компьютере или под другим пользователем (о том, как это сделать — в следующем разделе

инструкции).

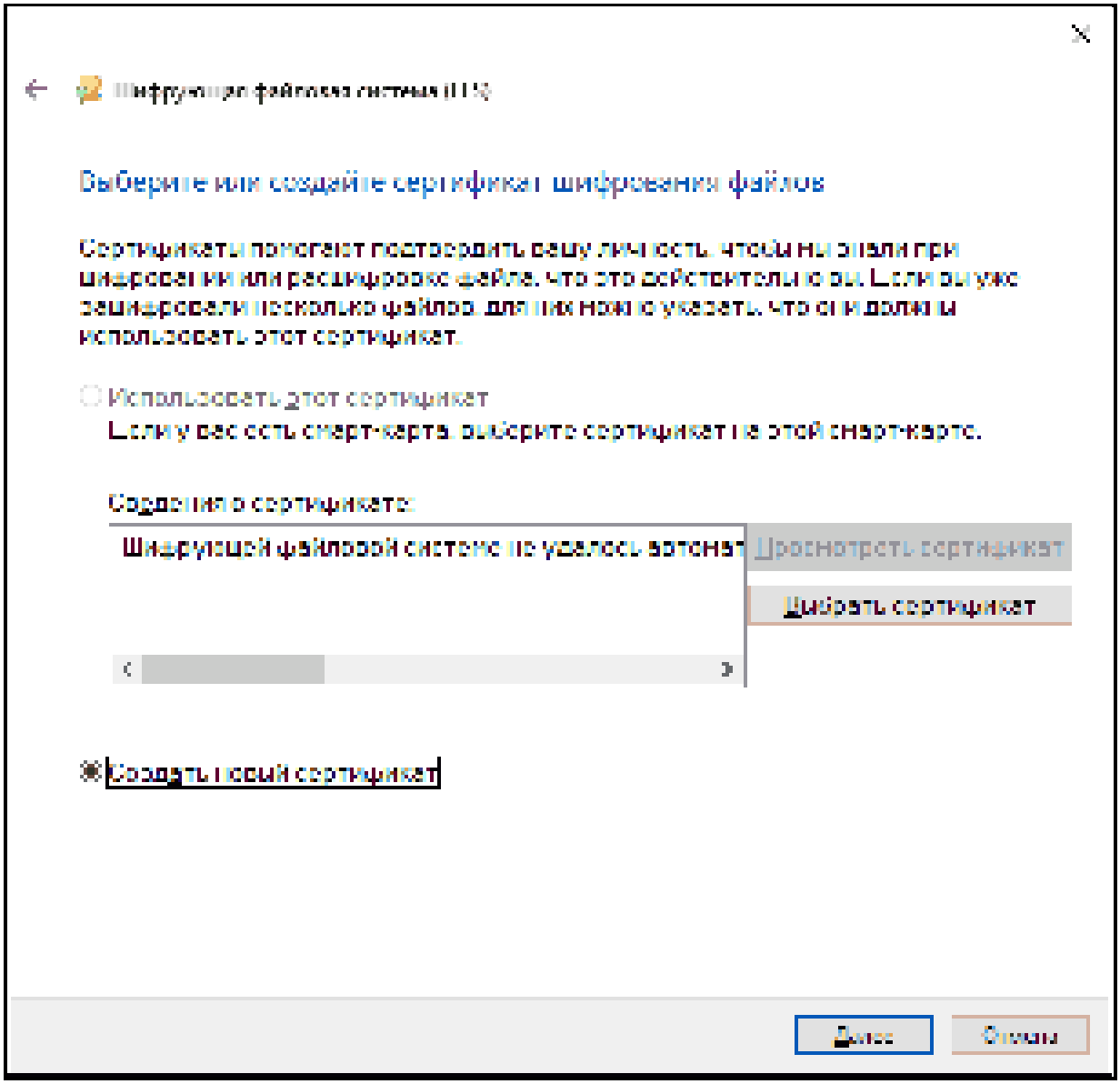


На этом процесс завершен — сразу после выполнения процедуры, все файлы в указанной вами папке, как уже имеющиеся там, так и создаваемые вновь приобретут на иконке «замок», сообщающий о том, что файлы зашифрованы.



Они будут без проблем открываться в рамках этой учетной записи, но под другими учетными записями и на других компьютерах открыть их не получится, система будет сообщать об отсутствии доступа к файлам. При этом структура папок и файлов и их имена будут видны.

При желании вы можете, наоборот, начать шифрование с создания и сохранения сертификатов (в том числе и на смарт-карте), а уже затем устанавливать отметку «Шифровать содержимое для защиты данных». Для этого, нажмите клавиши Win+R, введите *rekeywiz* и нажмите Enter.

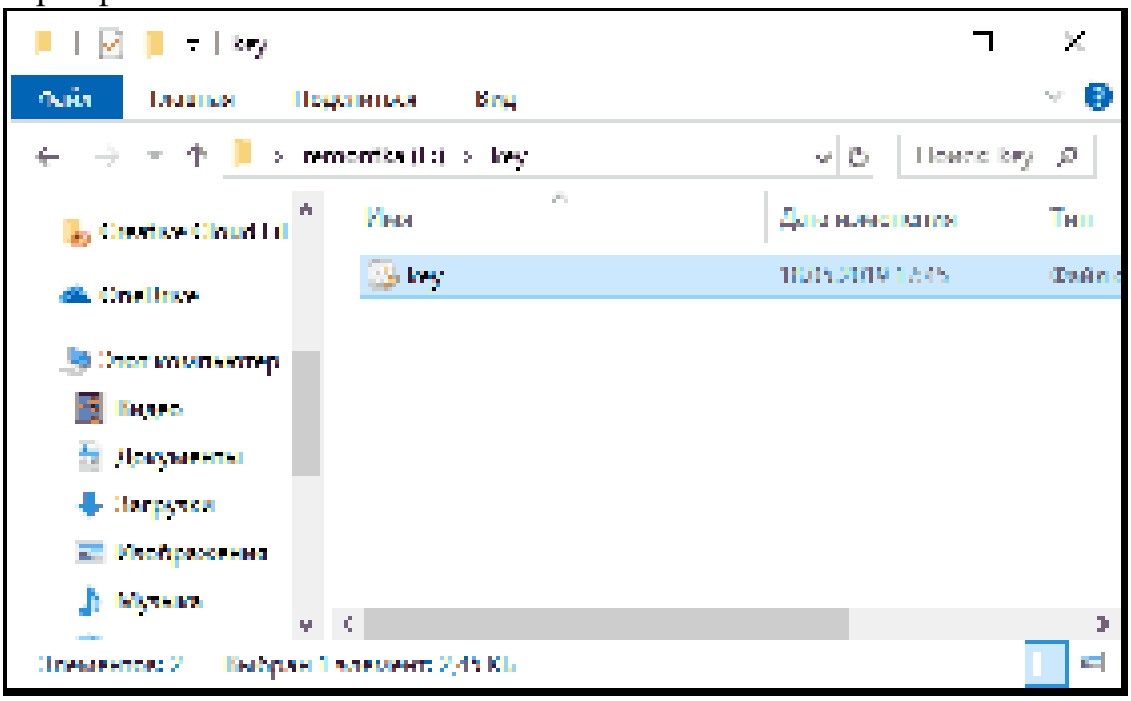



После этого выполните все шаги, которые предложит вам мастер настройки сертификатов шифрования файлов шифрующей файловой системы EFS. Также, при необходимости, с помощью rekeywiz вы можете задать использование другого сертификата для другой папки.

**Восстановление доступа к зашифрованным файлам, их открытие на другом компьютере или под другой учетной записью Windows**

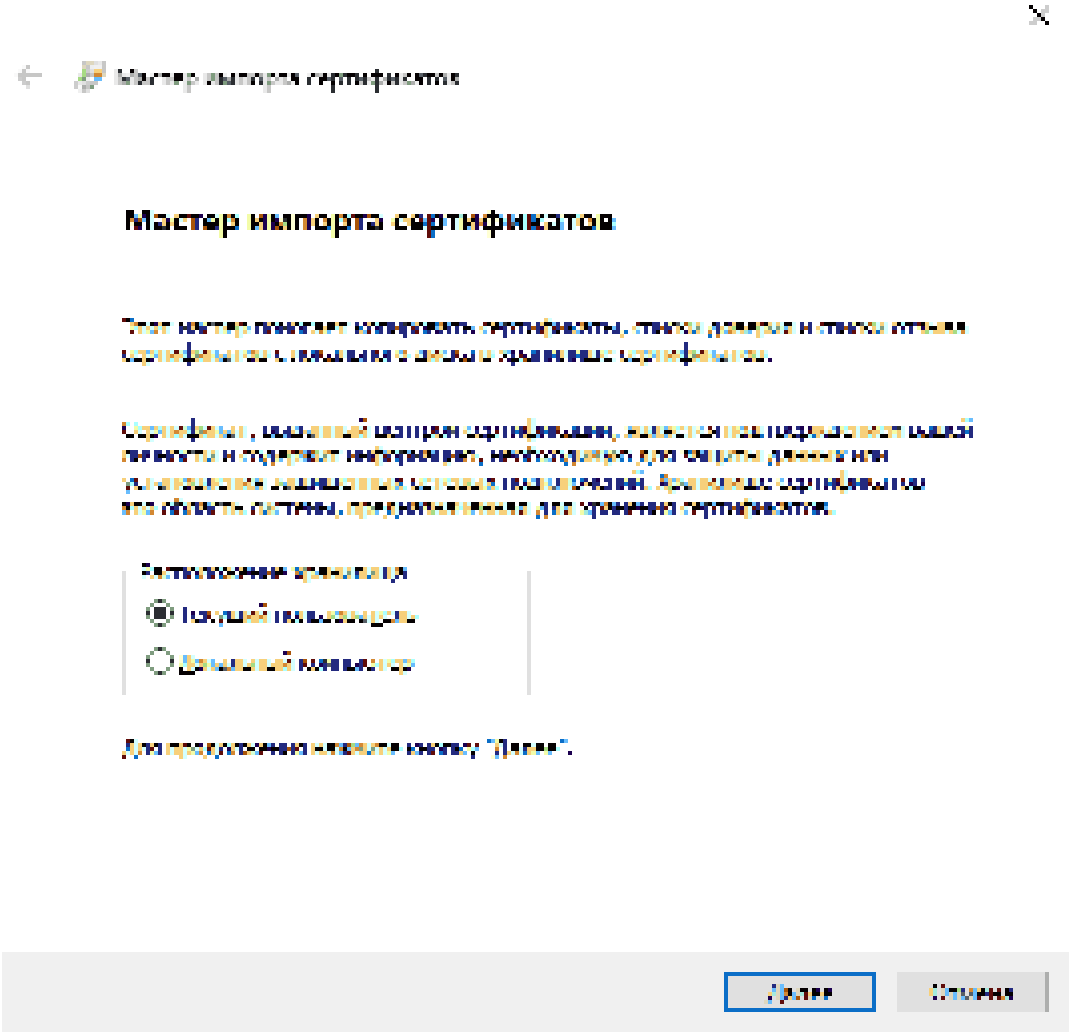
Если по той или иной причине (например, после переустановки Windows) вы потеряли возможность открыть файлы в зашифрованных EFS папках или вам потребовалась возможность открывать их на другом компьютере или под другим пользователем, сделать это легко:

1. На компьютере в той учетной записи, где нужно иметь доступ к зашифрованным файлам, откройте файл сертификата.

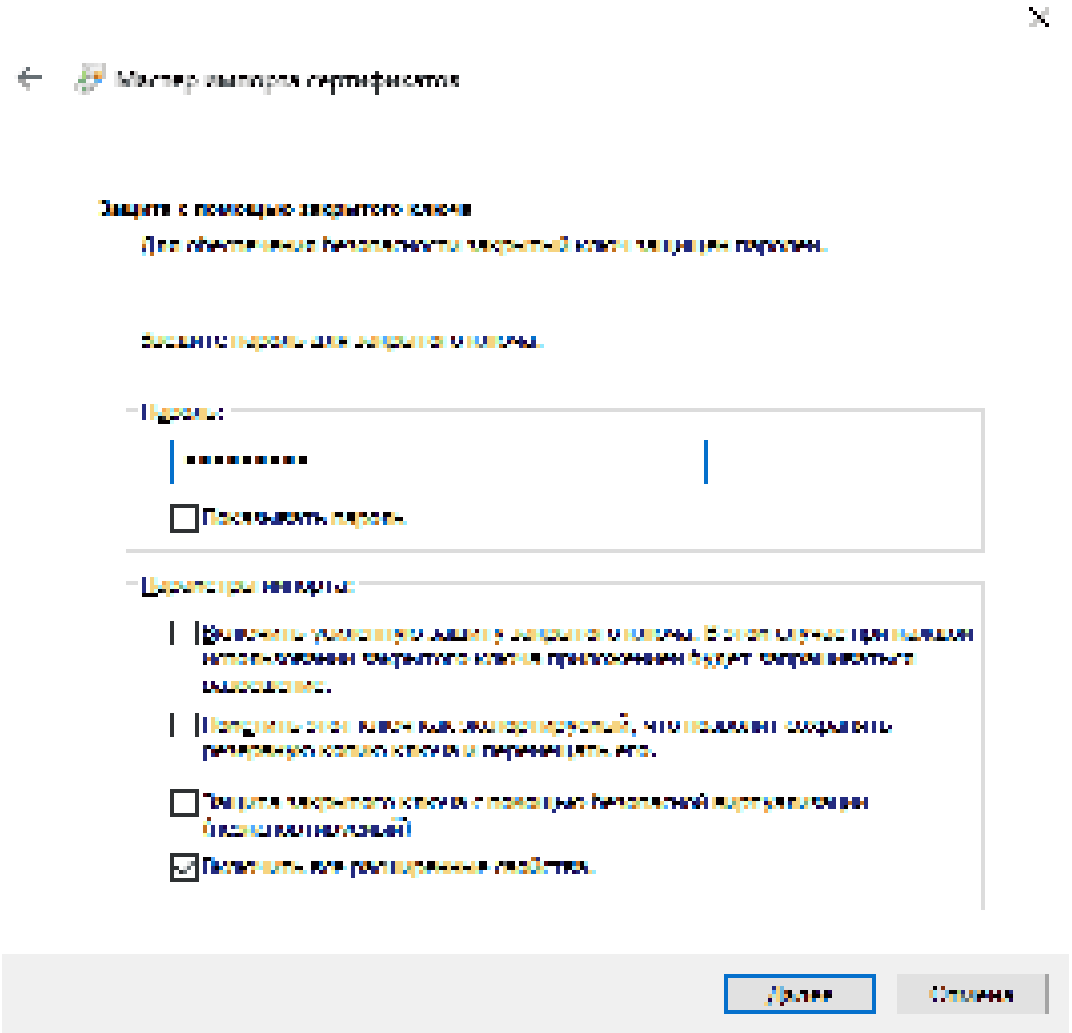


2. Автоматически откроется мастер импорта сертификатов. Для базового сценария в нем достаточно использовать параметры по

умолчанию.


Мастер импорта сертификатов
Мастер импорта сертификатов
Расположение хранилища
Текущий пользователь
Локальный компьютер
Для продолжения нажмите кнопку "Далее".
Далее
Отмена

3. Единственное, что потребуется — ввести пароль для сертификата.



4. После успешного импорта, о чем вы получите уведомление, ранее зашифрованные файлы будут открываться и на этом компьютере под текущим пользователем.

**Отличия шифрующей файловой системы EFS и Bitlocker**

Основные отличия, связанные с думая различными возможностями шифрования в Windows 10 — Windows 7

- Bitlocker шифрует целые диски (в том числе системные) или разделы дисков, в то время как EFS применяется к отдельным файлам и папкам. Впрочем, шифрование Bitlocker можно применить и к виртуальному диску (который на компьютере будет храниться как обычный файл).
- Сертификаты шифрования EFS привязываются к конкретной учетной записи Windows и хранятся в системе (также ключ можно экспортировать в виде файла на флешке или записать на смарт-карту).
- Ключи шифрования Bitlocker хранятся либо в аппаратном модуле TPM, либо могут быть сохранены на внешний накопитель. Открытый диск с

Bitlocker одинаково доступен всем пользователям системы, более того, если не использовался TPM, такой диск можно легко открыть и на любом другом компьютере или ноутбуке, достаточно будет ввести пароль.
- Шифрование для папок в случае использования EFS нужно включать вручную (файлы внутри будут в дальнейшем шифроваться автоматически). При использовании Bitlocker всё, что попадает на зашифрованный диск шифруется на лету.

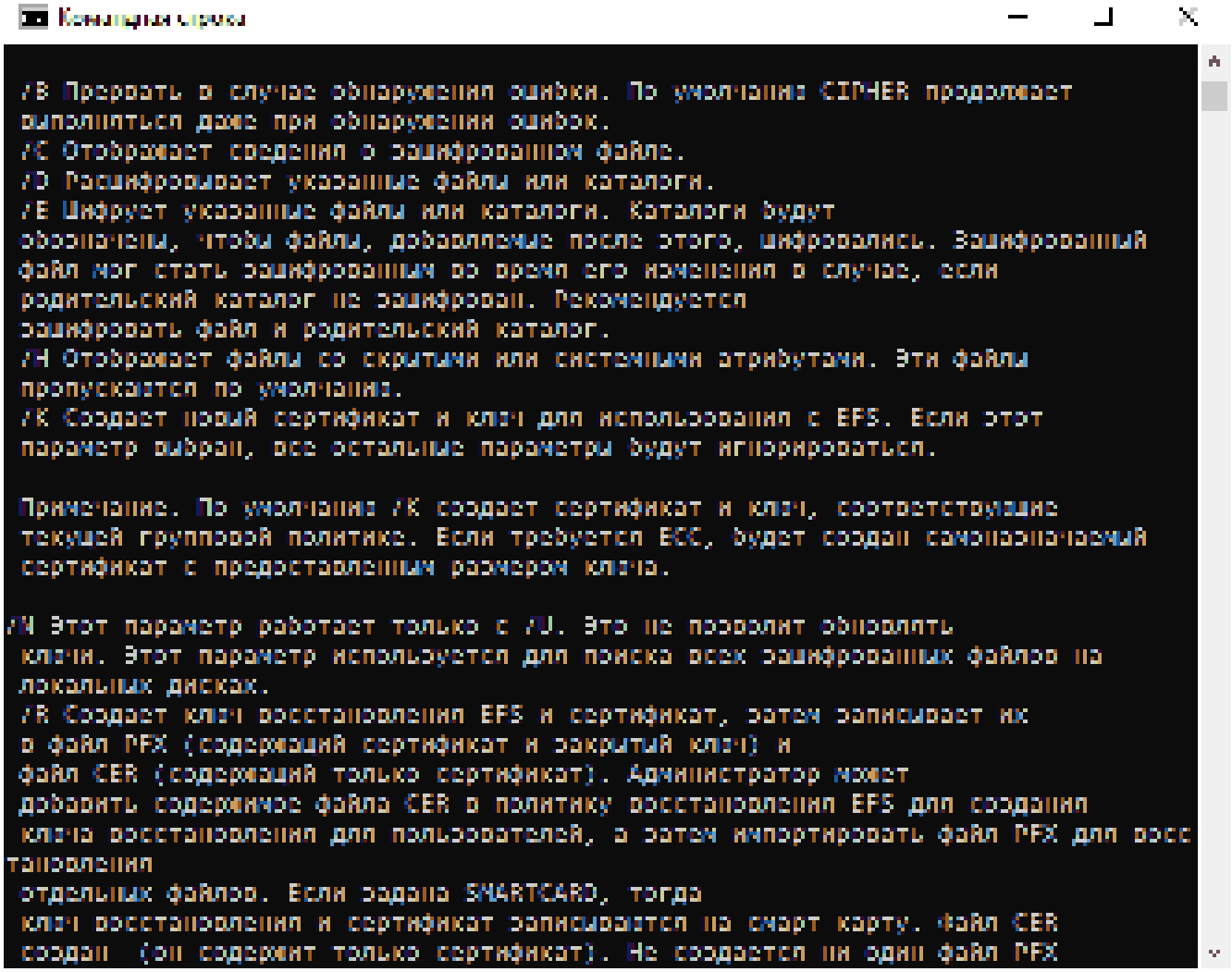
С точки зрения безопасности более эффективно использование Bitlocker. Однако, если требуется всего лишь не дать открыть ваши файлы другим пользователям Windows, а вы используете домашнюю редакцию ОС (где нет Bitlocker) — для этого подойдет и EFS.

**Дополнительная информация**

Некоторые дополнительные сведения об использовании шифрующей файловой системы EFS в Windows:

- Зашифрованные EFS файлы не защищены от удаления: удалить их сможет любой пользователь на любом компьютере.
- В системе присутствует утилита командной строки cipher.exe, которая может включать и отключить шифрование EFS для файлов/папок, работать с сертификатами, а также очищать содержимое зашифрованных папок на жестком диске, перезаписывая информацию случайными

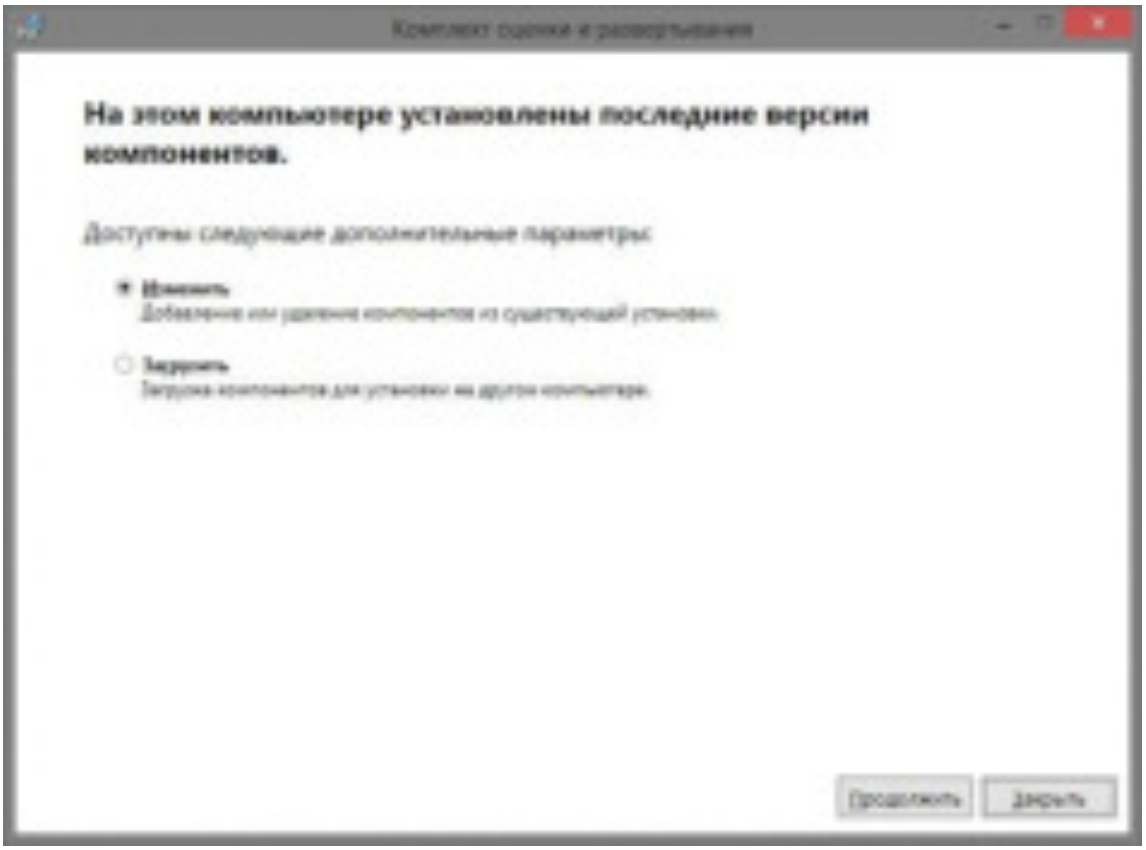
байтами.



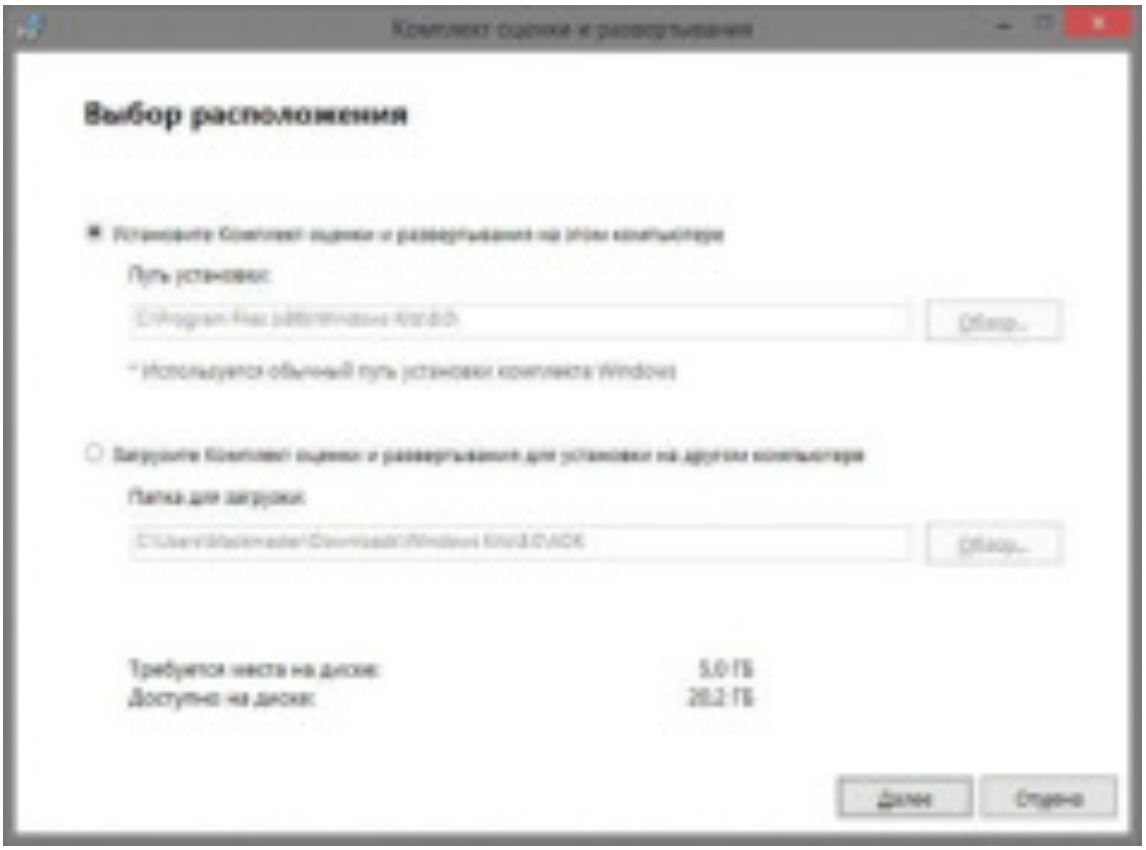

- Если вам требуется удалить сертификаты шифрования EFS с компьютера, сделать это можно следующим образом: зайдите в Панель управления — Свойства браузера. На вкладке «Содержание» нажмите кнопку «Сертификаты». Удалите ненужные сертификаты: в их описании внизу окна в поле «Назначение сертификата» будет указано «Шифрующая файловая система (EFS)».
- В том же разделе управления сертификатами в «Свойствах браузера» можно экспортировать файл сертификата для использования под другим пользователем или на другом компьютере.
- **Практическое занятие №5 Подготовка образа и среды предустановки Установка Windows ADK**
- ***Цель работы:***
- Изучить: комплект средств для оценки и развертывания Window. Изучить установку Windows ADK
- **Пакет Windows ADK**
- Пакет Windows ADK это комплект средств для оценки и развертывания Windows(R). (Windows ADK) – это набор средств и документов,

позволяющих настраивать, оценивать и развертывать операционные системы Windows на новых компьютерах. Это комплект утилит, позволяющий создать свою сборку Windows с предустановленными программами и обновлениями. В основном его используют системные администраторы при установке Windows на большой парк компьютеров, что позволяет в сжатые сроки получить рабочую систему.

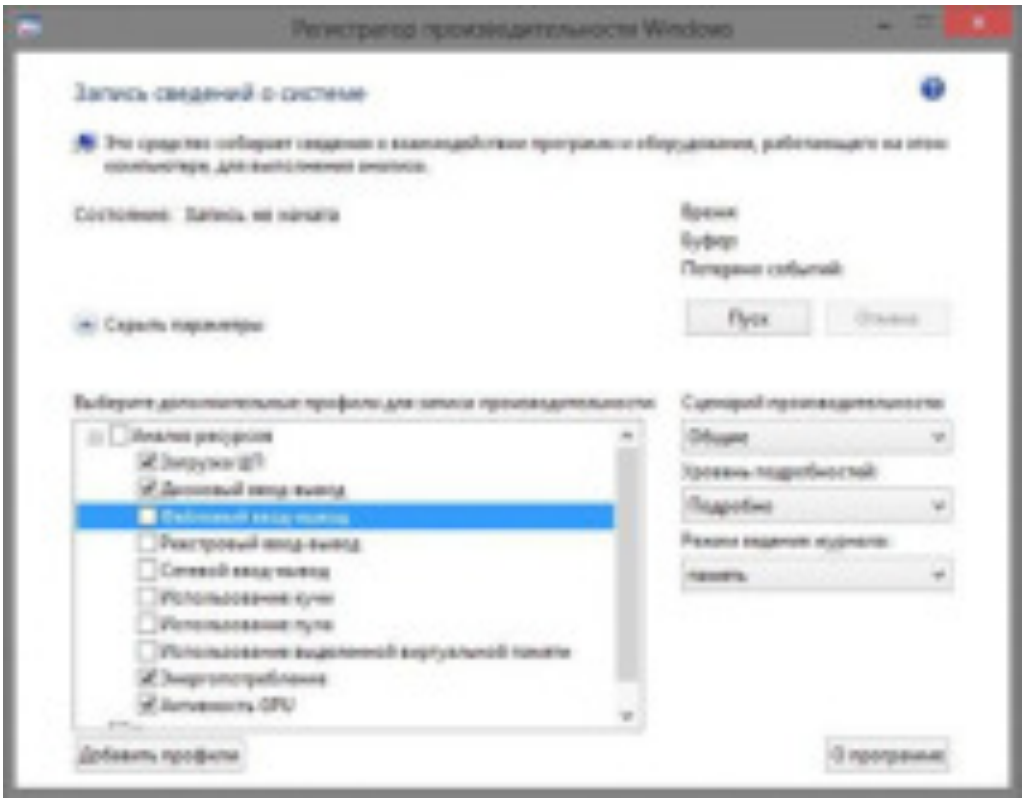
- Windows ADK объединил в себе несколько пакетов утилит для администраторов, перечисленных ниже:
- 1. Windows Performance Toolkit
  Используется для тестирования производительности операционной системы.
- 2. Windows Assessment Toolkit
  Новый пакет, используется для оценки и сравнения тех или иных параметров работы системы.
- 3. Windows Automated Installation Kit
  Пакет средств развертывания Windows. Содержит практически те же утилиты, что и предыдущая его версия. Естественно, что утилиты были обновлены для поддержки Windows 8
- **Установка пакета**
- Установщик Windows ADK теперь «весит» всего лишь 1,1 Мб. Такая компактность связана с тем, что скачиваемый установщик является веб-инсталлером, и сам скачивает все необходимые компоненты, в зависимости от выбора пользователя. За счет этого существенно экономится трафик, так как администратор теперь не должен скачивать весь дистрибутив пакета ради одного-двух необходимых ему компонентов. Также за счет этого можно не беспокоиться об обновлении пакета – в случае наличия обновлений установщик самостоятельно загружает и применяет их.

- 

- Итак, перейдем к процессу установки пакета.
- При запуске установщика администратор должен выбрать тип установки – либо установщик скачивает и сразу же устанавливает необходимые компоненты на конечный компьютер, либо же он просто загружает их на жесткий диск для последующего сетевого развертывания для экономии интернет-трафика.

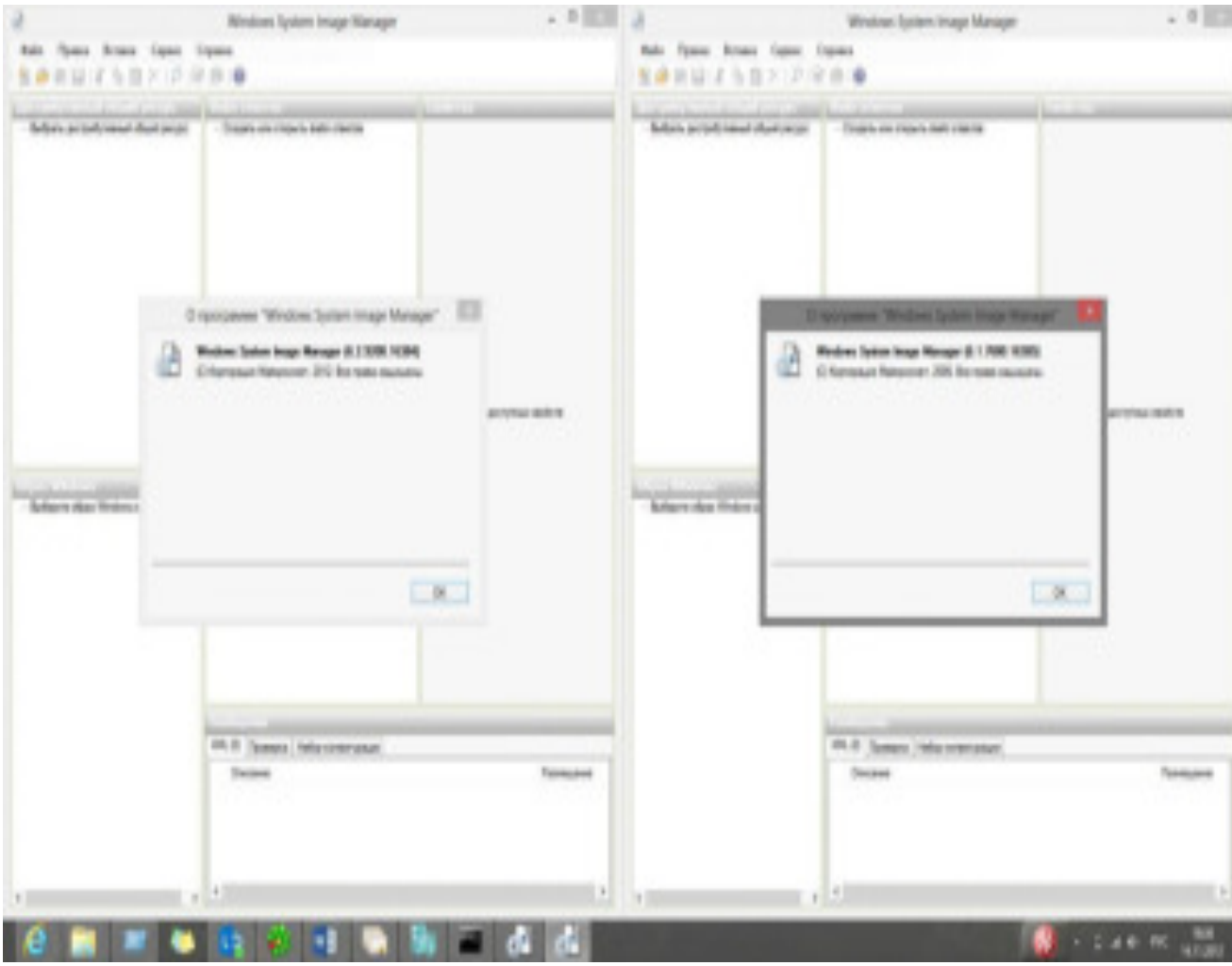
- 

- Далее необходимо выбрать компоненты для установки. Для подробного ознакомления с пакетом рекомендуется установить все компоненты, далее начнется загрузка и установка компонентов.
- **Windows Performance Analyzer**
- Данный компонент пакета предназначен для измерения производительности системы при выполнении рабочих задач. Вы запускаете мониторинг, а далее – ресурсоемкое приложение, игру либо выполняете любые действия, за производительностью при выполнении которых вам необходимо наблюдать.
- Мониторинг запускается путем запуска программы «Регистратор производительности Windows», щелчком по соответствующему файлу, либо командой wprui.exe




- В окне программы необходимо установить необходимые флажки, а далее нажать кнопку «Пуск». После этого можно начать выполнять необходимые действия. Как только потребуется остановить мониторинг, нужно будет нажать на кнопку «Сохранить», указать путь и имя файла для сохранения, ввести описание и еще раз нажать на «Сохранить» - начнется запись отчета в *.etl – файл.
- Как только отчет будет записан, его можно будет открыть в анализаторе, который можно запустит командой wpa.exe. Анализатор предоставляет средства для анализа отчета, с возможностями подробной детализации.
- **Windows Assessment Toolkit**
- Средства из этого пакета также предназначены для сбора данных о производительности системы, однако содержат в себе готовый набор тестов. Оценивается не производительность железа, а всей системы в целом. При этом ведется не просто запись данных в отчет, пакет сам выполняет необходимые действия, и участие администратора не требуется. Больше того, работа с системой во время выполнения теста может отрицательно сказаться на качестве тестирования.
- Запуск необходимого теста выполняется при помощи программы «Консоль оценки Windows».


- 
- 
- Во время работы теста крайне не рекомендуется работать с компьютером. Система сама будет делать необходимую нагрузку на него.
- **Windows Automated Installation Kit**
- Представляет собой пакет средств развертывания ОС. По сравнению со старой версией был обновлен для полной поддержки Windows 8 и Windows Server 2012
- Windows System Image Manager по прежнему остается основной утилитой, при помощи которой выполняется подготовка файлов ответов для автоматизации установки ОС. Он был обновлен, но его пользовательский интерфейс практически не изменился:



- Программа ImageX практически не изменилась. Как и в предыдущих версиях, она используется для захвата, применения и изменения образов системы Windows, хранящихся в файлах WIM
- Ее функции остались такими же:
- IMAGEX /APPEND – добавление образа в WIM-файл
- IMAGEX /APPLY – применение образа к конечному пути
- IMAGEX /CAPTURE – захват образа в новый WIM-файл
- IMAGEX /DELETE – удаление образа из WIM-файла
- IMAGEX /DIR – вывод содержимого образа
- IMAGEX /EXPORT – экспортирование образа из WIM-файла в новый WIM-файл
- IMAGEX /INFO – вывод информации об образе
- IMAGEX /SPLIT – разделение WIM-файла на несколько WIM-файлов заданного размера
- IMAGEX /MOUNT – монтирование образа к папке в правами на чтение
- IMAGEX /MOUNTRW – монтирование образа к папке с полными правами доступа

- IMAGEX /REMOUNT – восстановление связи смонтированного образа и папки, куда он был смонтирован
- IMAGEX /COMMIT – применение изменений к образу из папки, в которую он был смонтирован
- IMAGEX /UNMOUNT – размонтирование образа от папки
- IMAGEX /CLEANUP – очистка папок после некорректного размонтирования образа
- Таким образом, администратор может пользоваться ImageX так же, как и в предыдущей версии.
- Последним важным компонентом средств развертывания является среда Windows PE, в которой выполняется запуск программы установки setup.exe
- Как известно, Windows PE основана на ядре Windows, как следствие – с выходом пакета Windows ADK была полностью обновлена. Итак, в состав Windows ADK входит Windows PE 4.0. Как и в предыдущих версиях, она не содержит графического интерфейса, имеет ограничения по времени работы, и имеет ряд других ограничений. Однако, в четвертой версии был существенно расширен список доступных компонентов – теперь из Windows PE можно работать с чипом TPM, командлетами Power Shell, и самое главное – выполнять в ее среде приложения, написанные на основе .NET Framework.
- **Volume Activation Management Tool**
- Данное средство было в предыдущей версии пакета Windows AIK, однако в Windows ADK претерпело некоторые изменения.
- Во-первых, появились опции настройки активации клиентских и серверных систем через Active Directory. (доступно только для Windows 8 и Windows Server 2012)
- Во-вторых, был расширен функционал самой утилиты в сторону повышения управляемости корпоративными ключами
- В данной работе описана большая часть средств, входящих в новый пакет Windows ADK.

**Практическое занятие №6-7 Создание эталонного образа с помощью Windows SIM и Sysprep Создание файла ответов с помощью Windows SIM**

***Цель работы:***

Научиться создавать эталонный образ с помощью Windows SIM и Sysprep. Создавать файл ответов с помощью Windows SIM

**Создание эталонного образа с помощью Windows SIM и Sysprep**

## Общие понятия о Windows SIM

**Диспетчер установки Windows (Windows SIM) – приложение, входящее в состав WAIK и предназначенное для создания и управления файлами ответов автоматической установки Windows в графическом интерфейсе пользователя**. Позволяет не только создавать файлы ответов, но и выполнять другие административные задачи. Windows SIM входит в состав WAIK 2.0.

**Файл ответов – конфигурационный XML-файл, содержащий ответы на вопросы, генерируемые программой установки**.

Диспетчер установки Windows, к примеру, можно использовать для создания файла ответов, который разбивает диск на разделы и форматирует его перед установкой Windows. Диспетчер установки Windows также позволяет изменять параметры операционной системы и настраивает Windows для загрузки в режиме аудита после завершения установки. С помощью файла ответов, созданного утилитой Windows SIM, можно установить стороннее программное обеспечение, драйверы устройств, языковые пакеты и другие обновления. Диспетчер установки позволяет производить большое количество действий над устанавливаемым образом операционной системы.

Диспетчер установки Windows используется для создания файла ответов, в свою очередь, файл ответов используется при установке Windows для применения параметров к установке Windows. Сама утилита Windows SIM не изменяет параметры в файле образа Windows.

Окно диспетчера установки изображено на рис.1.

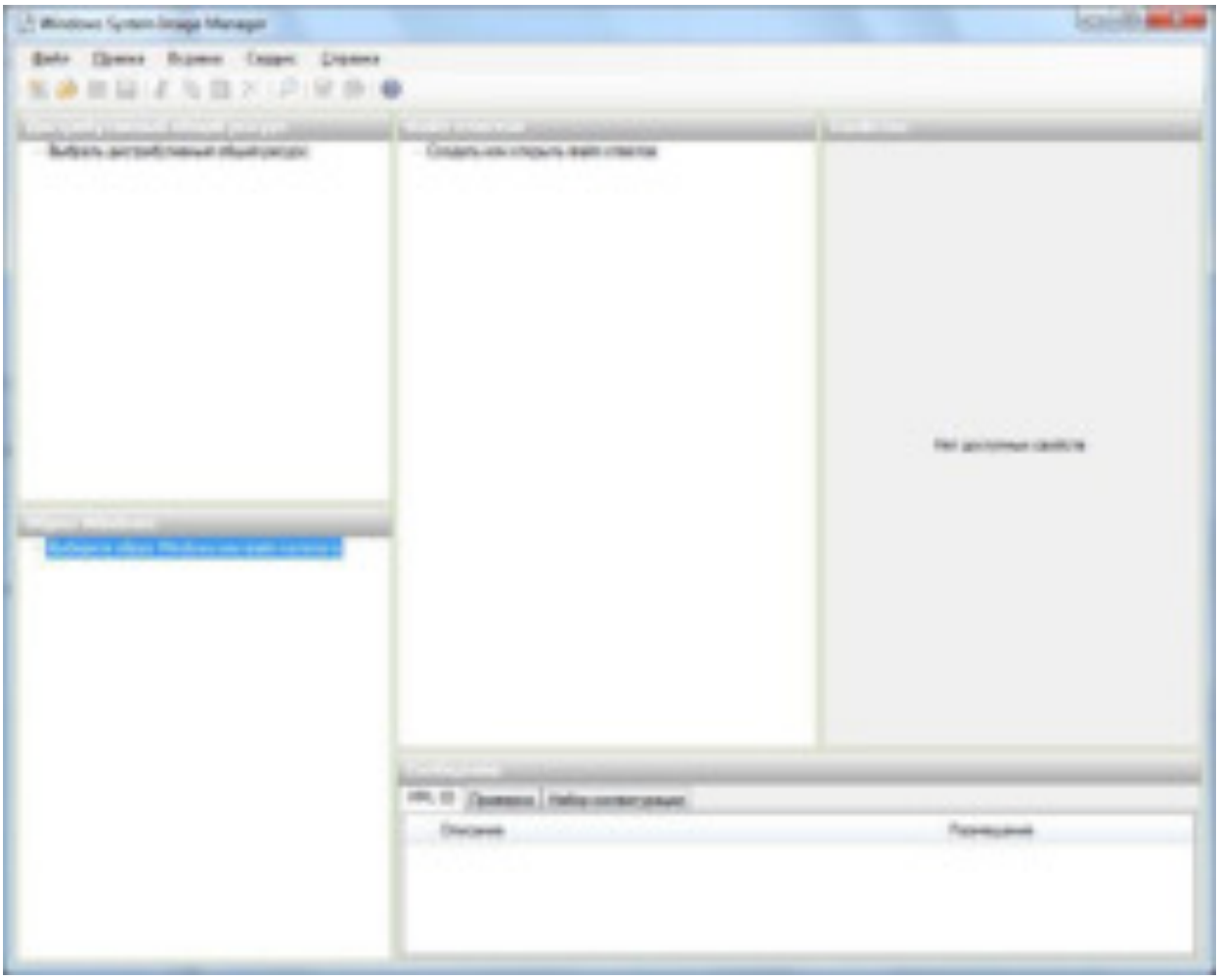


Рис.1.

Пять панелей Windows SIM используются в следующих целях:

- **Дистрибутивный общий ресурс**. Эта панель отображает открытый в данный момент ресурс. Она используется для работы с общими ресурсами: создание новых общих ресурсов, добавления элементов к этим ресурсам и закрытия открытых ресурсов.
- **Образ Windows**. Эта панель отображает открытый в данный момент Windows Image (.wim) файл. Для того, чтобы создать файл ответов необходимо предварительно открыть образ Windows. Именно на основании открытого образа строится список возможных компонентов и варианты их настроек. Таким образом, в зависимости от версии операционной системы, ее редакции и типа (клиентская – Windows 7 или серверная – Windows Server 2008 R2) строится индивидуальный список параметров. Можно попробовать задать несовместимые параметры, одинако, в процессе установки они не будут применены.
- **Файл ответов**. В этой панели можно создавать новый файл ответов и добавлять компоненты (группы параметров операционной системы) и пакеты (обновления ПО, языковые пакеты и т.д.) к существующему файлу ответов.

- **Свойства**. В этой панели вы можете задавать значения компонентам или пакетам, которые выбраны в панели файла ответа. В этой панели происходит непосредственное конфигурирование параметров файла ответов.
- **Сообщения**. Эта панель отображает ошибки, предупреждения и информационные сообщения касаемо синтаксиса и структуры вашего файла ответов, результаты проверки файла ответов и результаты работы по созданию набора конфигурации.

Используя различные файлы ответов можно при их помощи производить установку различных конфигураций операционной системы, драйверов и приложений основываясь только на одном образе операционной системы.

## Основные возможности утилиты Windows SIM

1. Создание и проверка файла ответов
2. Добавление драйверов
3. Интеграция обновлений
4. Создание набора конфигураций
5. Импорт пакетов

**Добавление дополнительных драйверов устройств в файл ответов**

При установке Windows с помощью диспетчера установки Windows можно добавлять драйверы устройств. При установке используется три вида драйверов.

- Драйверы, поставляемые с Windows. Драйверы, поставляемые с Windows, обрабатываются так же, как пакеты.
- Драйверы от производителя оборудования. Во время установки Windows с помощью диспетчера установки Windows можно добавлять дополнительные драйверы от производителя оборудования на основе INF-файлов. Обычно такие драйверы обрабатываются на этапе настройки **auditSystem**. Драйверы от производителя оборудования на основе INF-файла должны находиться во вложенной папке "Драйверы от производителя оборудования" дистрибутивного общего ресурса.
- Драйверы, поставляемые с Windows, устанавливаются вместе с файлом установщика Windows. Для драйверов, поставляемых с Windows, требуется файл установщика Windows, который добавляется таким же образом, как и приложения.

Драйверы для загрузки, которые требуется установить, необходимо добавлять в ходе этапа настройки **windowsPE** с помощью компонента Microsoft-Windows-PnpCustomizationsWinPE. Для добавления драйверов устройств в автономный образ Windows можно использовать систему обслуживания образов

развертывания и управления ими (DISM.exe). Данные драйверы являются необходимыми для корректной работы сетевой карты (если образ устанавливаемой системы находится на сервере или в общей сетевой папке) и обязательно в наличии должны быть драйверы для контроллеров дисков (чтобы корректно определить контроллер).

Диспетчер установки Windows позволяет добавить дополнительные приложения и драйверы, устанавливаемые в ходе работы программы установки Windows, с помощью дистрибутивного общего ресурса. В дистрибутивном общем ресурсе хранятся все приложения, драйверы устройств, сценарии и другие ресурсы, к которым можно получить доступ при установке Windows.

Дополнительные приложения, сценарии и другие двоичные файлы можно добавлять с помощью образа данных. Образ данных пакуется так же, как образ Windows. С помощью средства **ImageX** можно записать структуру папок с ресурсами, которые необходимо добавить в Windows (или другой раздел на компьютере) при установке Windows. С помощью параметра "DataImage" компонента Microsoft-Windows-Setup можно задать место применения образа данных.

Кроме того, для размещения двоичных файлов и других приложений в специальных расположениях во время установки Windows можно использовать структуру папок $OEM$. Приложения добавляются из дистрибутивных общих ресурсов во вложенные $OEM$-папки. Для запуска файла установщика Windows или EXE-файла, с помощью которых устанавливаются приложения, необходимо добавить параметр **RunSynchronous**.

**Обновление образа Windows в автономном режиме**

Диспетчер установки Windows позволяет автономно обновлять образ Windows, включая обновления программного обеспечения, драйверы устройств, языковые и другие пакеты, предоставляемые корпорацией Майкрософт.

Средство системы обслуживания образов развертывания и управления ими ( **DISM.exe** ) - это средство, которое можно использовать как с файлом ответов, так и без него для применения пакетов к образу Windows. Удаление и установка пакетов или изменения файла ответов применяются к образу Windows.

Пакеты, существующие на этапе настройки **offlineServicing**, применяются к автономному образу Windows.

**Создание набора конфигурации**

**Набор конфигурации - это вложенный набор файлов в дистрибутивном общем ресурсе, который явно вызывается в файле ответов**. При создании

набора конфигурации любой файл дистрибутивного общего ресурса, на который ссылается файл ответов, сохраняется в определенной папке. Пути к данным файлам обновляются в файле ответов, указывая на заданную папку.

Наборы конфигурации - это уменьшенные переносные версии дистрибутивного общего ресурса. Набор конфигурации идеален для установок без доступа к дистрибутивному общему ресурсу.

**Импорт пакетов в дистрибутивный общий ресурс**

Windows SIM импортирует пакеты, не являющиеся частью файла образа Windows (WIM), в дополнительный набор папок - дистрибутивный общий ресурс. Эти пакеты из дистрибутивного общего ресурса можно добавить в файл ответов. Импортировать пакеты в дистрибутивный общий ресурс нужно с помощью Windows SIM или API интерфейса CPI. Можно также импортировать пакеты прямо в файл ответов. Файл ответов содержит указатель пути пакета.

## Общее представление о дистрибутивных общих ресурсах и наборах конфигураций

**Дистрибутивный общий ресурс - это необязательный набор папок, содержащих файлы для настройки Windows с использованием автоматических файлов ответов**.При добавлении элементов дистрибутивного общего ресурса в файл ответов путь к элементу включается в файл ответов. Например, при подключении к дистрибутивному общему ресурсу в сети этот сетевой путь будет указан в файле ответов. Во время своей работы программа установки Windows использует этот путь для установки дополнительных приложений и драйверов устройств.

При создании дистрибутивного общего ресурса с помощью диспетчера системных образов Windows (Windows SIM) автоматически создаются три папки. Папки называются "Папки $OEM$", "Драйверы поставщика" и "Пакеты". При создании дистрибутивного общего ресурса он должен содержать хотя бы одну из следующих папок, чтобы Windows SIM распознал его как допустимый дистрибутивный общий ресурс.

**Папки "$OEM$"**

Папку "$OEM$" и ее подпапки можно использовать только при создании наборов конфигурации. Папки "$OEM$" использовались в предыдущих версиях Windows и в некоторых случаях не поддерживаются в ОС Windows 7.

Не перезаписывайте существующие файлы, обслуживаемые операционной системой. Использование папок $OEM$, чтобы обновить или переписать эти

файлы, может привести к непредсказуемому поведению системы и в результате - к серьезным проблемам.

Папка $OEM$ содержит все дополнительные папки и файлы для автоматической или настраиваемой установки Windows.

Поддерживаемые $OEM$ папки:

- **"\$OEM$ Folders\$$"** - содержит файлы, которые программа установки Windows копирует в папку %WINDIR% (например, C:\windows).
- **"\$OEM$ Folders\$$\System32"** – содержит файлы, которые программа установки Windows копирует в папку %WINDIR%\System32.
- **"\$OEM$ Folders\$1"** – представляет собой корневой каталог диска, на котором устанавливается Windows (также называемый загрузочным разделом), и содержит файлы, которые программа установки Windows копирует в загрузочный раздел во время установки.
- **"\$OEM$ Folders\$1\Pnpdrivers"** – содержит новые или обновленные драйверы самонастраивающихся устройств. Пользователь указывает имя папки в файле Unattend.xml для автоматической установки.
- **"\$OEM$ Folders\буква_диска\вложенная_папка"** – подпапка диска, содержащая файлы, которые программа установки Windows копирует в подпапку во время установки.

## Папки, используемые утилитой Windows SIM

### Папка сторонних драйверов

**Драйверы - это тип программного обеспечения, необходимый для правильной работы аппаратных средств или устройств**.

Папка "Драйверы поставщика" включает дополнительные драйверы устройств, которые пользователь устанавливает во время работы программы установки Windows. Можно добавить дополнительные драйверы устройств во время работы программы установки Windows с помощью Windows SIM. Существует три типа драйверов, используемых при установке. Типы драйверов мы разобрали чуть раньше.

Драйверы устройств, в обязательном порядке необходимые для загрузки, должны быть добавлены на этапе конфигурации **windowsPE**. Эти драйверы устройств добавляются с помощью компонента Microsoft-Windows-PnpCustomizationsWinPE. Драйверы устройств в автономный образ можно также добавлять с помощью системы обслуживания образов развертывания и управления ими (DISM.exe).

### Папка "Пакеты"

Пакеты следует импортировать в дистрибутивный общий ресурс с помощью Windows SIM. В папке "Пакеты" находятся программные обновления Microsoft Windows. Разными типами пакетов являются пакеты обновления, обновления безопасности, пакеты поддержки языков и другие пакеты, выпускаемые корпорацией Майкрософт. Для импорта пакетов используется Windows SIM. После того как пакет импортирован и доступен на панели дистрибутивного общего ресурса, его можно добавить в файл ответов.

**Наборы конфигурации**

После проверки и сохранения автоматического файла ответов можно создать набор конфигурации. Набор конфигурации - это подмножество дистрибутивного общего ресурса, которое можно создать с помощью Windows SIM. Наборы конфигурации полезны, когда общий сетевой ресурс недоступен. Наборы конфигурации можно хранить на съемном носителе и использовать на месте. При создании набора конфигурации двоичные файлы, указанные в автоматическом файле ответов, экспортируются и помещаются в автономный набор файлов, доступный из файла Unattend.xml.

Набор конфигурации содержит полный набор файлов, драйверов, приложений, пакетов исправлений и файлов ответов для настройки установки Windows. Набор конфигурации содержит все необходимые двоичные файлы, объединенные в пакет с соответствующим автоматическим файлом ответов.

Преимущества наборов конфигурации

- Набор конфигурации является уменьшенной и более мобильной версией дистрибутивного общего ресурса, размер которого может достигать нескольких гигабайт. Наборы конфигурации можно использовать для установки операционных систем Windows на месте.
- Наборы конфигурации являются полностью автономными и не содержат ссылок на ресурсы вне набора файлов.
- Можно продублировать набор конфигурации и затем модифицировать его для разных выпускаемых моделей компьютеров.

Если во время установки Windows используется набор конфигурации, все содержимое корневого каталога носителя, на котором находится файл ответов, копируется в новый экземпляр Windows. Программа установки Windows копирует в экземпляр Windows все файлы и папки, находящиеся на том же уровне, что и файл ответов. Следует иметь в виду, что это может замедлить процесс установки и в некоторых случаях привести к нехватке места на диске.

## Общее представление о файлах ответов

Файлы ответов, созданные в диспетчере образов системы Windows (Windows SIM), сопоставлены определенному образу Windows. Это позволяет согласовать параметры файла ответов с параметрами, доступными в образе Windows. Однако любой файл ответов можно использовать для установки любого образа Windows, и если в файле ответов содержатся параметры компонентов, отсутствующих в образе Windows, эти параметры пропускаются.

### Содержание файла ответов

В файле ответов содержится два раздела параметров: "Компоненты" и "Пакеты".

Раздел " **Компоненты"** - содержит все параметры компонентов, применяемые в ходе установки Windows. Компоненты сгруппированы в различные циклы (проходы) конфигурации: **windowsPE**, **offlineServicing**, **generalize**, **specialize**, **auditSystem**, **auditUser** и **oobeSystem**. Каждый этап настройки представляет собой отдельную фазу работы программы установки Windows. Параметры можно применить во время одного или нескольких циклов. Если параметр можно применить в нескольких циклах конфигурации, то необходимо выбрать цикл для применения параметра.

**Пакеты** – используются для распространения обновлений программного обеспечения, пакетов обновления и языковых пакетов. Пакеты могут также содержать отдельные компоненты Windows. Пакеты, добавляемые в образ Windows или удаляемые из него можно настраивать. Кроме того, можно изменять параметры компонентов, входящих в состав пакета. Компоненты Windows входят в состав базового пакета Windows, который содержится во всех образах Windows 7 и Windows Server 2008 R2. Например, универсальный проигрыватель, игры и программа резервного копирования - это компоненты Windows, включенные в базовый пакет Windows. Компоненты Windows могут быть включены или отключены. Если компонент включен, все ресурсы, исполняемые файлы и параметры этого компонента доступны для пользователей системы. Если компонент отключен, то ресурсы пакета недоступны, но они не удаляются из системы. Для включения установленной версии Windows некоторые компоненты Windows могут потребовать установки других компонентов. Следует проверить текущий файл ответов и установить необходимые пакеты. Например, можно отключить компонент "Универсальный проигрыватель", чтобы запретить пользователям запускать универсальный проигрыватель. Но, несмотря на то, что пакет отключен, ресурсы из образа Windows не удаляются. Пакеты в файле ответов применяются к образу Windows во время этапа настройки **offlineServicing**. Для добавления пакетов в автономный образ Windows можно использовать систему обслуживания образов развертывания и управления ими (DISM.exe).

Утилита Windows SIM это средство, помогающее в развертывании операционной системы и обладающая следующими функциями:

1. Создание файла ответа.
2. Интеграция драйверов.
3. Создание структуры каталогов.
4. Автоматическая установка приложений.

### Ключевые термины

**Диспетчер установки Windows (Windows SIM)** – приложение, входящее в состав WAIK и предназначенное для создания и управления файлами ответов автоматической установки Windows в графическом интерфейсе пользователя.

**Дистрибутивный общий ресурс** - это необязательный набор папок, содержащих файлы для настройки Windows с использованием автоматических файлов ответов.

**Драйверы** - это тип программного обеспечения, необходимый для правильной работы аппаратных средств или устройств.

**Набор конфигурации** - это вложенный набор файлов в дистрибутивном общем ресурсе, который явно вызывается в файле ответов.

**Пакеты** - это группы файлов, предоставляемые корпорацией Майкрософт, в состав которых входят пакеты обновлений, обновления безопасности, языковые пакеты и другие изменения компонентов Windows.

**Файл ответов** – конфигурационный XML-файл, содержащий ответы на вопросы, генерируемые программой установки.

## Настройка образа при помощи Windows SIM

### Создание дистрибутивного общего ресурса

**Дистрибутивный общий ресурс - это папка для хранения драйверов, приложений и пакетов, например, бюллетени по безопасности**.

Дистрибутивный общий ресурс можно создать при помощи диспетчера установки или вручную. Добавлять файлы в общий ресурс можно также двумя способами: диспетчером установки или с помощью проводника.

Чтобы создать дистрибутивный общий ресурс с помощью Windows SIM необходимо выполнить следующие действия:

1. Создаем папку, в которую хотим поместить дистрибутивный общий ресурс. Эта папка может находиться как на общем сетевом ресурсе, так и на локальном компьютере.
2. В области "Дистрибутивный общий ресурс" жмем правой кнопкой мыши и выбираем команду "Выбрать дистрибутивный общий ресурс", выбираем "Создать дистрибутивный общий ресурс". Появляется окно "Создание дистрибутивного общего ресурса".
3. Переходим в папку, созданную на этапе 1, и нажимаем "Открыть". На панели дистрибутивного общего ресурса отобразится папка дистрибутивного общего ресурса, при этом диспетчер установки Windows автоматически создает структуру папок для общего ресурса.

При создании дистрибутивного общего ресурса с помощью диспетчера установки Windows создается правильная структура папок внутри ресурса. Диспетчер установки Windows может открывать только дистрибутивные общие ресурсы, содержащие хотя бы одну из четырех особых папок: $OEM$ Folders, Out-of-Box Drivers, Packages и LangPacks.

**Создание дистрибутивного общего ресурса для многоязыкового образа**

Если планируется использовать программу установки Windows для развертывания многоязыкового выпуска Windows, можно скопировать один или несколько языковых пакетов в каталог **\Langpacks** дистрибутивного общего ресурса, обновить файл lang.ini, а затем воспользоваться программой установки для установки языковых пакетов, находящихся в дистрибутивном общем ресурсе. Это типичный сценарий для организаций, развертывающих Windows в многоязыковых средах, где пользователям нужна возможность переключения отображаемого языка между несколькими языками на одном компьютере. Согласно требованиям лицензии выпуски "Windows Максимальная" и "Windows Корпоративная" могут содержать несколько языков, остальные выпуски Windows 7 могут содержать только один язык. Выпуски, поддерживающие несколько языков называются многоязычными выпусками. Следующая процедура может применяться только к многоязыковым выпускам Windows. Добавление языковых пакетов в каталог **\Langpacks** может увеличить время установки Windows. Пакеты в каталоге **\Langpacks** добавляются в образ Windows во время этапа настройки **windowsPE**, перед фактической установкой Windows.

Копирование языкового пакета в каталог **\Langpacks**

1. Копируем набор файлов Windows в локальный каталог. Например, скопируем содержимое DVD-диска Windows в каталог **C:\my_distribution**.
2. Создаем каталог **\Langpacks** в дистрибутивном общем ресурсе.

```
mkdir C:\my_distribution\langpacks
```

3. Копируем языковой пакет (Lp.cab) и родительскую папку (fr-FR, en-US и т. д.) в каталог **\Langpacks** дистрибутивного общего ресурса.

```
4.mkdir C:\my_distribution\langpacks\fr-fr
5.mkdir C:\my_distribution\langpacks\de-de
6.xcopy C:\LPs\fr-fr\lp.cab
  C:\my_distribution\langpacks\fr-fr\lp.cab
  xcopy C:\LPs\de-de\lp.cab
  C:\my_distribution\langpacks\de-de\lp.cab
```

7. Находим файл Lp.cab для языка, поддержку которого нужно добавить. Распаковываем содержимое файла Lp.cab в локальный каталог.

```
8.expand.exe -f:* C:\LPs\fr-fr\lp.cab C:\LPs\fr-
  fr\expanded
  expand.exe -f:* C:\LPs\de-de\lp.cab C:\LPs\de-
  de\expanded
```

9. Затем копируем каталоги с исходными файлами и файлами лицензии из распакованного языкового пакета в дистрибутивный общий ресурс.

```
10. xcopy C:\LPs\fr-fr\expanded\sources\license\*
  c:\my_distribution\sources\license\
11. xcopy C:\LPs\fr-fr\expanded\setup\sources\*
  c:\my_distribution\sources\
12. xcopy C:\LPs\de-de\expanded\sources\license\*
  c:\my_distribution\sources\license\
  xcopy C:\LPs\de-de\expanded\setup\sources\*
  c:\my_distribution\sources\
```

13. Подключаем образ Windows, находящийся в дистрибутивном общем ресурсе. Эта процедура требуется системе обслуживания образов развертывания и управления ими (DISM.exe) для отображения списка языков, установленных в WIM-файле, и повторного создания файла Lang.ini. С помощью системы DISM подключаем образ Windows

```
DISM.exe /Mount-Wim
/WimFile:C:\my_distribution\sources\install.wim
/index:1 /MountDir:C:\test\offline
```

14. Вводим список языков, доступных в дистрибутивном общем ресурсе или установленных в образе Windows, используя параметр /Get-Intl и указав дистрибутивный общий ресурс.

```
DISM.exe /image:c:\test\offline
/distribution:c:\my_distribution /Get-Intl
```

15. Проверяем наличие в списке необходимых доступных языков.
16. Повторно создаем файл Lang.ini файл и выбираем значения региональных настроек по умолчанию. Например, можно повторно создать файл Lang.ini и задать все региональные значения как французские, используя следующую команду.

    ```
    DISM.exe /image:c:\test\offline /Gen-LangINI
    /distribution:c:\my_distribution /Set-AllIntl:fr-fr
    ```

    При выполнении операции добавления или удаления языковых пакетов для дистрибутивного общего ресурса необходимо повторно создать файл Lang.ini. Файл Lang.ini используется программой установки Windows. Он содержит список всех доступных языковых пакетов, их расположение и язык по умолчанию, используемый программой установки. Если программа установки Windows запущена из полной операционной системы и язык по умолчанию не выбран, то будет предложено выбрать язык для программы установки Windows из доступных в дистрибутивном общем ресурсе. Если программа установки Windows запущена с загрузочного носителя или среды предустановки Windows (Windows PE), то для поддержки нескольких языков необходимо добавить дополнительные компоненты в файл Boot.wim.

17. Отключаем WIM-файл и фиксируем сделанные изменения.

    ```
    DISM.exe /unmount-Wim /MountDir:C:\test\offline
    /commit
    ```

Добавив языковые пакеты в дистрибутивный общий ресурс и повторно создав файл lang.ini, можно использовать программу установки Windows и файл ответов для создания многоязыкового образа, содержащего языки в дистрибутивном общем ресурсе. Кроме того, региональные языковые параметры по умолчанию можно в любой изменить одним из следующих способов.

- Для установки языков по умолчанию и региональных параметров используйте команды системы DISM для работы с региональными параметрами.
- Используйте файл ответов для указания языков и региональных параметров.

**Работа с ключами продуктов и активацией**

Ключи продуктов Windows используются для следующих действий:

- Определение выпуска Windows, установленного в системе.

- Идентификация каждой уникальной установки операционной системы Windows.

Для этих целей можно использовать различные ключи продуктов. Место ввода ключа продукта определяет, понадобится ли пользователю вводить ключ в экране приветствия Windows.

При установке Windows с одноразовым ключом продукта предусмотрено 30 дней, в течение которых следует активировать эту установку Windows. При установке Windows с многопользовательским ключом активации (MAK) корпоративной лицензии этот ключ должен быть задан с параметром "ProductKey" в компоненте Microsoft-Windows-Shell-Setup. Этапы ввода ключа продукта:

1. Microsoft-Windows-Setup\UserData\ProductKey\Key – применяется на этапе **windowsPE**. Он определяет образ Windows, используемый при выполнении установки Windows.
2. Microsoft-Windows-Shell-Setup\ProductKey - применяется на этапе **specialize** Он определяет ключ продукта для активации Windows. Если используется этот параметр, приветствие Windows не предлагает ввести ключ продукта. Задать его можно в параметре Microsoft-Windows-Setup\UserData\ProductKey\Key, при этом два ключа продукта могут быть различными.

При изменении образа Windows на выпуск более высокого уровня с помощью системы обслуживания образов и управления ими (DISM) ключ продукта не требуется. Установщик или конечный пользователь может добавить ключ продукта одним из следующих способов:

- Конечный пользователь может ввести ключ продукта в экране приветствия Windows.
- "ProductKey" можно задать в компоненте Microsoft-Windows-Shell-Setup на этапе настройки **specialize**.
- После перевода выпуска в автономный режим можно воспользоваться системой обслуживания образов развертывания и управления ими (DISM) с параметром командной строки для обслуживания выпуска Windows /Set-ProductKey.

**Настройка региональных параметров**

Во время установки Windows с помощью файла ответов можно указать язык, региональные параметры и клавиатуру по умолчанию. Существует два способа настроить региональные параметры в файле ответов.

- Создать файл ответов, использующий этап настройки **windowsPE** для настройки региональных параметров. Для многоязыковых развертываний в дистрибутивный общий ресурс и в образ можно добавлять языковые пакеты. Языковые пакеты в дистрибутивный общий ресурс можно добавить и настроить на этапе настройки **windowsPE** или добавить на этапе настройки **windowsPE**, а настроить на другом этапе настройки. Компонент Microsoft-Windows-International-Core-WinPE включает в себя параметры, которые можно использовать для изменения языка и региональных параметров на этапе настройки **windowsPE**. Также можно изменить пользовательский интерфейс программы установки Windows, указав значения в этом компоненте.
- Для развертывания одноязычного выпуска Windows создают файл ответов и определяют региональные параметры и клавиатуру на этапе настройки **specialize**. В этом сценарии языковой пакет добавляется в образ Windows до настройки региональных параметров. Компонент Microsoft-Windows-International-Core включает в себя параметры, которые можно использовать для изменения языка и региональных параметров во время этапов настройки **specialize** и **oobeSystem**. Можно выполнить предварительный выбор языка и пропустить выбор языка на странице пользовательского интерфейса экрана приветствия Windows, указав язык и региональные параметры на этапе настройки **oobeSystem** в компоненте Microsoft-Windows-International-Core. В общем случае пользователь может выбрать между языком программы установки по умолчанию и любым дополнительным языком, установленным в образе. Выбор языка обновит другие региональные параметры, задав для них значения по умолчанию, связанные с этим языком. Впоследствии пользователь сможет индивидуально изменить эти параметры по умолчанию.

Настройка региональных параметров на этапе настройки **windowsPE**:

1. Открываем диспетчер установки Windows и создаем файл ответов.
2. Добавляем в используемый файл ответов компонент Microsoft-Windows-PnpCustomizationsWinPE, чтобы применить параметры на этапе настройки **windowsPE**.
3. Настраиваем региональные параметры в компоненте Microsoft-Windows-International-Core-WinPE. Например, если в дистрибутивном общем ресурсе доступен русский языковой пакет, можно добавить значения "ru-RU" в параметры компонента на этапе настройки **windowsPE**. Для большинства языков системы требуется перезагрузка.
4. Сохраняем файл ответов и закрываем диспетчер установки Windows. При запуске программы установки Windows и задании этого файла ответов языковой пакет в дистрибутивном общем ресурсе будет добавлен автоматически с применением указанных региональных параметров.

Настройка региональных параметров на этапе настройки specialize:

1. Открываем диспетчер установки Windows и создаем новый файл ответов.
2. Добавляем компонент Microsoft-Windows-International-Core, чтобы применить параметры во время этапов настройки **specialize** и **oobeSystem**.

   Для большинства языков системы требуется перезагрузка. Если языковые параметры обрабатываются во время этапов настройки **specialize** или **oobeSystem**, компьютеру может понадобиться дополнительная перезагрузка.

3. Изменяем параметры компонента Microsoft-Windows-International-Core, чтобы настроить региональные параметры для конкретного региона. Например, добавляем значения "EN-US" к параметрам Microsoft-Windows-International-Core на этапе настройки **specialize**. Можно также заранее выбрать язык и задать язык и региональные параметры на этапе настройки **oobeSystem** в компоненте Microsoft-Windows-International-Core. В этом случае при загрузке для пользователя экрана приветствия Windows страница пользовательского интерфейса выбора языка будет пропущена. В общем случае пользователь может выбрать между языком программы установки по умолчанию и любым дополнительным языком, установленным в образе. Выбор языка обновит другие региональные параметры, задав для них значения по умолчанию, связанные с этим языком. Впоследствии пользователь сможет индивидуально изменить эти параметры по умолчанию.
4. Сохраняем файл ответов и закрываем диспетчер установки Windows. При запуске программы настройки Windows с этим файлом ответов будут применены региональные параметры, заданные в этом файле ответов.

В файле ответов можно настроить несколько различных языковых параметров с помощью определения разных значений, которые должны обрабатываться на разных этапах настройки. Для этого в файле ответов можно создать несколько разделов, которые будут обрабатывать различные языковые параметры на различных этапах установки Windows. Например, можно создать языковые и региональные параметры на этапе настройки **windowsPE** в компоненте Microsoft-Windows-International-Core-WinPE. Затем можно изменить параметры по умолчанию на этапе настройки **oobeSystem** или **specialize** путем добавления параметров в компонент Microsoft-Windows-International-Core.

Если языковые параметры обрабатываются на этапе настройки **oobeSystem**, может понадобиться перезагрузка компьютера. Следует также учесть, что время, затраченное компьютером на обработку языковых параметров, не даст быстро загрузиться экрану приветствия Windows.

## Создание разделов жесткого диска

### Создание разделов жесткого диска на базе BIOS с помощью диспетчера установки Windows

1. Открываем диспетчер установки Windows и файл ответов.
2. Добавляем параметр Microsoft-Windows-Setup\DiskConfiguration\Disk в этап настройки **windowsPE**.
3. Для каждого дополнительного жесткого диска щелкаем правой кнопкой мыши на параметр "DiskConfiguration" и выбираем "Вставить новый диск".
4. Для каждого диска задаем значение "DiskID". Первому жесткому диску соответствует значение 0 (ноль), второму - значение 1 и т.д.
5. Для каждого диска задаем значение "WillWipeDisk" равным "true".
6. Добавляем параметр Microsoft-Windows-Setup\DiskConfiguration\Disk\CreatePartitions в этап настройки **windowsPE**.
7. Жмем правой кнопкой мыши на параметр "CreatePartitions" и выбираем пункт "CreatePartition". Повторяем это действие для каждого раздела.
8. В параметре "CreatePartition" добавляем параметр "Order" для каждого раздела. Первому разделу диска соответствует значение 1, второму - значение 2 и т.д.
9. В параметре "CreatePartition" задаем тип каждого раздела. Задаем системный раздел как Type = Primary, другие разделы как Type = Primary, Extended или Logical.
10. В параметре "CreatePartition" настраиваем размер разделов. Для каждого раздела необходимо использовать либо Size = <размер>, либо Extend = true.
    - Чтобы указать размер раздела в мегабайтах (например, 15000), используйте Size.
    - Для последних основных или расширенных разделов используйте Extend = true, чтобы программа установки Windows задала размер раздела в соответствии с оставшимся пространством на жестком диске.
    - Если используются логические разделы, размер последнего из них можно установить в соответствии с оставшейся частью расширенного раздела. В Microsoft-Windows-Setup\DiskConfiguration\Disk\CreatePartitions\CreatePartition\Extend задайте Extend = false и задайте Size = 100. Изначально размер раздела составляет 100 МБ. Процесс его изменения описан в следующей части.

### Изменение разделов

1. Добавляем параметр Microsoft-Windows-Setup\DiskConfiguration\Disk\ModifyPartitions в этап настройки windowsPE.
2. Жмем правой кнопкой мыши параметр "ModifyPartitions" и выбираем пункт "ModifyPartition". Повторите это действие для каждого раздела, который требуется изменить.
    - Если используются только основные разделы, для каждого из них добавляем элемент "ModifyPartition". Эта структура позволяет использовать одни и те же значения для ModifyPartition\Order и "PartitionID" в следующих двух шагах для CreatePartition\Order.
    - Если используется расширенный раздел, добавляем один элемент "ModifyPartition" для каждого раздела. Обычно для расширенного раздела дальнейшие изменения не требуются. Эта структура позволяет использовать одни и те же значения для ModifyPartition\Order и "PartitionID" в следующих двух шагах.
3. В "ModifyPartition" необходимо использовать "Order", чтобы указать последовательность изменения разделов. Первому изменению раздела соответствует значение 1, второму - значение 2 и т.д.
4. В элементе "ModifyPartition" используется параметр "PartitionID", для идентификации каждого раздела.
    - Если используются только основные разделы, значение "PartitionID" совпадет со значением "Order".
    - Если используется расширенный раздел, первые основные разделы получают значение "PartitionID", совпадающее со значением "Order". Расширенный раздел сам по себе не получает "PartitionID". Однако каждый логический раздел в составе расширенного получает "PartitionID", начинающийся со значения "Order" расширенного раздела и продолжающий изменяться. Каждый основной раздел, за которым следует расширенный, продолжает данную последовательность.
5. В "ModifyPartition" указываем системный раздел как Active = true. Если отдельные системные разделы отсутствуют, необходимо указать раздел Windows.
6. В "ModifyPartition" можно использовать "Label", чтобы добавить подпись к каждому основному и логическому разделу.
7. В элементе "ModifyPartition" можно использовать параметр "Letter", чтобы задать буквы дисков для разделов Windows и данных. Для раздела Windows рекомендуется использовать параметр Letter = C. Если буква не задана, то по умолчанию используется первая доступная буква от C до Z.
8. При использовании логических разделов необходимо выбрать последний раздел и задать ModifyPartition\Extend = true, чтобы размер раздела соответствовал оставшемуся пространству в расширенном разделе.

**Определение раздела для установки Windows**

1. В параметре Microsoft-Windows-Setup\ImageInstall\OSImage необходимо либо очистить параметр "InstallToAvailablePartition", либо задать ему значение "false".
2. Добавляем параметр Microsoft-Windows-Setup\ImageInstall\OSImage\InstallTo.
3. В "InstallTo" в качестве значения "DiskID" указываем жесткий диск, где будет установлена ОС Windows.
4. В качестве значения "PartitionID" указываем раздел, где будет установлена ОС Windows.

**Создание разделов жесткого диска на базе UEFI с помощью диспетчера установки Windows**

1. Открываем диспетчер установки Windows и файл ответов.
2. Добавляем параметр: Microsoft-Windows-Setup\DiskConfiguration\Disk в этап настройки **windowsPE**.
3. Для каждого дополнительного жесткого диска жмем правой кнопкой мыши на параметр "DiskConfiguration" и выбираем "Вставить новый диск".
4. Для каждого диска задаем значение "DiskID". Первому жесткому диску соответствует значение 0 (ноль), второму - значение 1 и т.д.
5. Для каждого диска задаем значение "WillWipeDisk" равным true.
6. Добавляем параметр: Microsoft-Windows-Setup\DiskConfiguration\Disk\CreatePartitions в этап настройки windowsPE.
7. Жмем правой кнопкой мыши на параметр "CreatePartitions" и выбираем пункт "CreatePartition". Повторяем это действие для каждого раздела.
8. В параметре "CreatePartition" добавляем значение "Order" для каждого раздела. Первому разделу диска соответствует значение 1, второму - значение 2 и т.д.
9. В параметре "CreatePartition" задаем тип каждого раздела.
   - Определяем системный раздел EFI (ESP) как Type = EFI.
   - Определяем MSR-раздел как Type = MSR.
   - Определяем другие разделы как Type = Primary.
10. В параметре "CreatePartition" настраиваем размер разделов. Для каждого раздела используйте или параметр Size=<size>, или Extend=True, но не оба варианта сразу.
    - Чтобы задать размер раздела в мегабайтах, используйте параметр Size (например, 15000).
    - Для последнего основного раздела используйте параметр Extend = True, чтобы программа установки Windows расширила раздел на всю оставшуюся часть жесткого диска.

**Изменение разделов**

1. Добавляем параметр: Microsoft-Windows-Setup\DiskConfiguration\Disk\ModifyPartitions в этап настройки **windowsPE**.
2. Жмем правой кнопкой мыши параметр "ModifyPartitions" и выбираем пункт "ModifyPartition". Повторяем это действие для каждого раздела, который требуется изменить.
3. Добавляем элемент "ModifyPartition" для каждого раздела. Эта структура позволяет использовать одинаковые значения для элементов CreatePartition\Order, ModifyPartition\Order и параметра "PartitionID".
4. В элементе "ModifyPartition" необходимо использовать параметр "Order", чтобы задать последовательность, которая должна соблюдаться изменениями раздела. Первому изменению раздела соответствует значение 1, второму - значение 2 и т.д.
5. В элементе "ModifyPartition" используем параметр "PartitionID", чтобы идентифицировать каждый раздел. Значение "PartitionID" будет совпадать со значением элемента CreatePartition | Order.
6. В элементе "ModifyPartition" используем параметр "Label", чтобы пометить каждый основной раздел.
7. В элементе "ModifyPartition" используйте параметр "Letter", чтобы задать буквы дисков для разделов Windows и данных.

**Определение раздела для установки Windows**

1. В параметре Microsoft-Windows-Setup\ImageInstall\OSImage необходимо либо очистить параметр "InstallToAvailablePartition", либо задать ему значение "false".
2. Добавляем параметр Microsoft-Windows-Setup\ImageInstall\OSImage\InstallTo.
3. В "InstallTo" в качестве значения "DiskID" указываем жесткий диск, где будет установлена ОС Windows.
4. В качестве значения "PartitionID" указываем раздел, где будет установлена ОС Windows.

## Добавление пользовательских команд и сценариев

Чтобы добавить пользовательскую команду в файл ответов

1. Открываем диспетчер образов системы Windows.
2. Открываем файл ответов.
3. В меню "Вставка" выбираем пункт "Синхронная команда". В подменю выбираем цикл конфигурации (проходы). Откроется диалоговое окно "Создание синхронной команды".
4. В поле "Ввод" командной строки вводим команду с параметрами. В поле "Порядок" выбираем порядок выполнения команд и нажимаем кнопку

"OK". Команда будет добавлена в файл ответов в выбранный этап настройки.

- Команды, добавленные в этап настройки 1 **windowsPE**, отображаются в параметре Microsoft-Windows-Setup\RunSynchronous.
- Команды, добавленные в этап настройки 4 **specialize** или 6 **auditUser**, отображаются в параметре Microsoft-Windows-Deployment\RunSynchronous.
- Команды, добавленные в этап настройки 7 **oobeSystem**, отображаются в параметре Microsoft-Windows-Shell-Setup\FirstLogonCommands.

В файл ответов можно добавить пользовательский сценарий, который будет запускаться:

- сразу после завершения программы установки Windows

  После завершения программы установки Windows можно выполнить дальнейшую настройку системы путем добавления команд в файл %WINDIR%\Setup\Scripts\SetupComplete.cmd. Этот файл позволяет устанавливать дополнительные приложения, запускать специальные сценарии Windows (cscript или wscript) или вносить в систему другие изменения перед входом в нее пользователя. Команды в файле Setupcomplete.cmd выполняются с привилегией локальной системы. После установки Windows и перед появлением экрана входа в систему программа установки Windows выполняет поиск файла SetupComplete.cmd в каталоге **%WINDIR%\Setup\Scripts**. Если файл **SetupComplete.cmd** найден, он выполняется. В противном случае установка продолжается в обычном режиме. Программа установки Windows записывает действие в файл Setupact.log. Нельзя перезагрузить систему и возобновить выполнение файла SetupComplete.cmd. Программа установки не проверяет коды выхода или коды ошибок в сценарии после выполнения файла **SetupComplete.cmd**. Функции **Setupcomplete.cmd** отличаются от команд RunSynchronous и RunAsynchronous следующим образом: **Setupcomplete.cmd** выполняется после завершения программы установки Windows, а команды RunSynchronous и RunAsynchronous выполняются в процессе выполнения установки Windows. Если в процессе установки компьютер присоединяется к домену, то групповая политика, определенная в домене, не применяется к компьютеру до выполнения Setupcomplete.cmd. Это гарантирует, что действия групповой политики, связанные с настройкой, не повлияют на работу сценария.

- если в программе установки Windows возникает неустранимая ошибка.

Если в программе установки Windows возникает неустранимая ошибка, можно настроить программу установки на автоматический запуск сценария, содержащего специальные команды или действия. Неустранимая ошибка - это ошибка, не позволяющая программе установки Windows завершить работу. Данная функция полезна при автоматической установке нескольких систем сразу. Эта функция позволяет сразу обнаружить ошибку во время установки Windows и выполнить специальные действия. Если в программе установки Windows возникает неустранимая ошибка, не позволяющая программе установки завершить свою работу, то последняя выполняет поиск командного сценария в следующем каталоге: **%WINDIR%\Setup\Scripts\ErrorHandler.cmd**. Будет выполнено одно из двух действий в зависимости от того, найден ли сценарий. Если сценарий не найден, появится диалоговое окно с описанием ошибки. Пользователь должен закрыть диалоговое окно перед выходом из программы установки Windows. Если сценарий найден, то он выполняется синхронно. Диалоговое окно и описание ошибки не отображаются. После завершения сценария ErrorHandler.cmd выполняется выход из программы установки Windows. В зависимости от этапа установки Windows компьютер возвращается в ту среду, из которой выполнялась установка (например, в предыдущую версию операционной системы или в среду предустановки Windows). Существует несколько способов добавления файла ErrorHandler.cmd с помощью структуры каталогов $OEM$. Первый - создать папку **Sources\$OEM$\$$\Setup\Scripts** в дистрибутиве Windows и скопировать файл **ErrorHandler.cmd** в эту папку. Второй - создать временную папку, содержащую структуру папок **$$\Setup\Scripts** и скопировать в этот каталог файл ErrorHandler.cmd, а затем запустить программу установки Windows с параметром /m:временная_папка, где временная_папка - это временная папка, созданная в начале этого шага.

## Ключевые термины

**Дистрибутивный общий ресурс** - это папка для хранения драйверов, приложений

## Sysprep

**Программа подготовки системы (Sysprep) подготавливает установленную копию Windows к аудиту, дублированию и доставке конечному пользователю**.

Дублирование позволяет сохранять настроенный образ Windows, который затем можно повторно использовать в организации. Утилита **sysprep** может загрузить компьютер в режим аудита и позволяет добавлять к установке Windows дополнительные драйверы устройств и приложения. После установки

дополнительных драйверов и приложений можно проверить целостность установки Windows. Программа **Sysprep** также позволяет подготавливать образ для использования конечным пользователем. Когда пользователь запускает Windows, появляется экран приветствия.

Программа **Sysprep** должна использоваться только для настройки новых установок Windows. Ее можно запускать столько раз, сколько потребуется для построения и настройки установки Windows. Однако сбросить активацию Windows можно не больше трех раз. Нельзя использовать программу **Sysprep** для повторной конфигурации существующей уже развернутой установки Windows.

Если в дальнейшем планируется перенос образа Windows на другой компьютер, необходимо выполнить команду **sysprep** с ключом /generalize, даже если конфигурации оборудования целевого и исходного компьютеров совпадают. Команда sysprep /generalize удаляет из образа установки Windows уникальные сведения о системе, что позволяет повторно использовать этот образ на разных компьютерах. Если требуется установить образ Windows на компьютеры с той же конфигурацией оборудования, можно сохранить установку устройств и драйверов в образе Windows, используя параметр "PersistAllDeviceInstalls" в файле ответов.

При следующей загрузке образа Windows начнется этап настройки **specialize**. На этом этапе настройки при загрузке образа Windows на новый компьютер для многих компонентов должны быть выполнены определенные действия.

Любой способ переноса образа Windows на новый компьютер, как установка образа, так и копирование жесткого диска или другой способ, требует подготовки с помощью команды sysprep /generalize. Перенос или копирование образа Windows на другой компьютер без предварительного выполнения этой команды не поддерживается.

Программа **Sysprep** предоставляет следующие преимущества:

- Удаление из Windows системных данных. Программа **Sysprep** может удалить все сведения, относящиеся к операционной системе, из установленного образа Windows, включая идентификатор безопасности компьютера ( **SID** ). Затем установку Windows можно записать в образ и установить по всей организации.
- Настройка Windows для загрузки в режиме аудита. Режим аудита позволяет устанавливать приложения сторонних лиц и драйверы устройств, а также проверять работоспособность компьютера.
- Настройка загрузки экрана приветствия Windows. Программа **Sysprep** настраивает установку Windows на загрузку с экраном приветствия при следующем запуске компьютера. Как правило, систему следует

настраивать на загрузку с экраном приветствия перед поставкой компьютера заказчику.
- Сброс активации Windows. Программа **Sysprep** может сбрасывать активацию Windows до трех раз.

**Создание образа Windows для сборки по плану**

При использовании сценария сборки по плану создается один исходный образ Windows для установки на компьютеры, использующие такое же оборудование. Исходную установку Windows можно настраивать путем установки самой системы Windows и добавления дополнительных драйверов и приложений. Затем этот образ сохраняется и используется для установки на другие компьютеры. Дополнительных изменений в этом образе не производится.

Этот сценарий включает следующие этапы:

1. Устанавливаем Windows на компьютер-образец.
2. После завершения установки компьютер следует загрузить и установить на него дополнительные драйверы или приложения.
3. После обновления установки Windows выполняем команду sysprep /oobe /generalize. Параметр /generalize предписывает программе Sysprep удалить из установки Windows данные, относящиеся к операционной системе: журналы событий, уникальные идентификаторы безопасности (SID) и другие данные. После удаления уникальных сведений о системе работа компьютера завершается. Параметр /oobe предписывает установке Windows запустить экран приветствия при следующей загрузке компьютера.
4. Теперь можно записать установку Windows с помощью программы ImageX, создав исходный образ, который затем будет использоваться на компьютерах со сходным оборудованием.

**Загрузка в режиме аудита**

**Режим аудита позволяет изготовителям оборудования (OEM), сборщикам систем и корпорациям быстро настраивать установку Windows. В режиме аудита можно устанавливать приложения, добавлять драйверы устройств, выполнять сценарии, а также проверять правильность установки Windows**. В режиме аудита не требуется, чтобы применялись параметры экрана приветствия Windows.

Обычно Windows запускает экран приветствия сразу после установки. Однако при загрузке в режиме аудита можно пропустить экран приветствия Windows и сразу загрузить рабочий стол компьютера. Это позволит начать процесс настройки как можно скорее.

Также режим аудита позволяет проверить работоспособность компьютера перед его доставкой клиенту. Можно проверить правильность первого запуска системы, а также наличие всех заданных изготовителем оборудования (OEM) или сборщиком систем настроек и информации о поддержке.

Выполнить загрузку в режиме аудита можно несколькими способами:

- При ручной установке нажмите во время работы экрана приветствия клавиши CTRL+SHIFT+F3.
- При установке в автоматическом режиме добавьте компонент "Microsoft-Windows-Deployment" в этап настройки **oobeSystem**. В параметре "Reseal\ Mode" следует указать "Audit". Когда Windows закончит установку, компьютер выполнит перезагрузку в режиме аудита.
- Выполните команду sysprep /audit в окне командной строки.

**Ограничения программы Sysprep**

- Следует использовать только ту версию **Sysprep**, которая была установлена вместе с образом Windows. Программа **Sysprep** устанавливается с каждой версией Windows и всегда запускается из папки %WINDIR%\system32\sysprep.
- Программу **Sysprep** нельзя использовать при обновлениях установки. Запускайте **Sysprep** только при новых установках.
- Если планируется использовать команду imagex /apply для установки образа Windows на компьютер, разметка разделов на исходном и целевом компьютерах должна быть идентичной. Например, если образ Windows сохраняется на диске D, развертывать этот образ необходимо также на диск D конечного компьютера. В следующем списке описываются параметры разделов, которые должны быть идентичными на компьютере-образце и конечном компьютере при использовании команды imagex /apply.
    - Типы разделов (основной, дополнительный или логический) должны совпадать.
    - Если раздел сделан активным на компьютере-образце, на конечном компьютере он также должен быть активным.
- При копировании образов Windows между системами не требуется совместимость HAL (слоев абстрагирования оборудования) компьютера-образца и конечного компьютера. Параметр /detecthal данных конфигурации загрузки (BCD) позволяет системе, на которой уже запускалась программа Sysprep, устанавливать правильный уровень HAL.
- Устройства Plug and Play на компьютере-образце и конечном компьютере, такие как модемы, звуковые платы, сетевые адаптеры и видеоплаты, не обязательно должны быть одного и того же

производителя. Однако драйверы для этих устройств необходимо включить в установку.

- Автоматизировать выполнение **Sysprep** с помощью команды "RunSynchronous" на этапе настройки **auditUser** нельзя. Однако можно использовать параметр **generalize** в компоненте "Microsoft-Windows-Deployment" для автоматической подготовки компьютера к созданию образа после установки.
- Часы активации начинают отсчет при первом запуске Windows. Программу **Sysprep** можно использовать для сброса часов активации Windows не более трех раз. После третьего запуска программы **Sysprep** часы больше нельзя будет сбросить.
- Для установки с использованием образов требуется программа **ImageX**, сторонние приложения для создания образов дисков или аппаратные устройства копирования дисков. Эти средства создают двоичные образы жестких дисков компьютеров, а затем или дублируют образ на другом жестком диске, или сохраняют его в файле на отдельном диске.
- Программа **Sysprep** может быть запущена только в том случае, когда компьютер входит в рабочую группу, а не в домен. Если компьютер подсоединен к домену, он будет автоматически выведен из состава домена.
- При выполнении **Sysprep** программа приветствия Windows будет выдавать запрос на ввод ключа продукта. Для подавления выдачи такого запроса Sysprep можно использовать вместе с файлом ответов. Если в параметре "ProductKey" компонента "Microsoft-Windows-Shell-Setup" во время этапа **specialize** указан действующий ключ продукта, программа приветствия Windows не будет выдавать запрос на его ввод.
- Если компьютер входит в домен и групповая политика этого домена назначает ему политику надежного пароля, для всех учетных записей пользователей требуется надежный пароль. Выполнение средства **Sysprep** или приветствия Windows не удаляет политику надежных паролей. Если учетной записи пользователя не назначить надежный пароль перед выполнением **Sysprep** или приветствия Windows, вход на компьютер может быть запрещен. Рекомендуется всегда использовать надежные пароли для учетных записей пользователя.

### Принципы работы Sysprep

**Sysprep**. **exe** - главная программа, вызывающая другие исполняемые файлы, необходимые для подготовки установленной копии Windows. **Sysprep**. **exe** находится в каталоге %WINDIR%\system32\sysprep во всех установленных системах. Программа **Sysprep** должна запускаться из каталога %WINDIR%\system32\sysprep и выполняться в той версии Windows, в которой она была установлена.

При запуске Sysprep выполняется следующая процедура.

1. Проверка возможности выполнения **Sysprep**. Только администратор может запускать программу **Sysprep**, при этом одновременное выполнение нескольких экземпляров **Sysprep** не допускается. Кроме того, программа **Sysprep** должна выполняться в той версии Windows, в которой она была установлена.
2. Инициализация ведения журнала.
3. Анализ аргументов командной строки. Если аргументы командной строки не заданы, отображается окно **Sysprep** для пользовательского ввода действий **Sysprep**.
4. Обработка действий **Sysprep**, вызов соответствующих исполняемых и DLL-файлов и регистрация действий в файле журнала.
5. Подтверждение, что все DLL-файлы выполнили необходимые задачи с последующим выключением или перезагрузкой системы.

**Использование файлов ответов с программой Sysprep**

Не все этапы настройки выполняются во время установки Windows. Некоторые из этапов настройки можно выполнить только с помощью **Sysprep**. К ним относятся этапы **generalize**, **auditSystem** и **auditUser**. При добавлении параметров к файлу ответов для этих этапов настройки следует запустить **Sysprep** для применения этих параметров.

- Чтобы применить параметры на этапах настройки **auditSystem** и **auditUser**, следует загрузить систему в режиме аудита с помощью команды sysprep /audit.
- Чтобы применить настройки на этапе **generalize**, необходимо воспользоваться командой sysprep /generalize. Во время этапа настройки **generalize** удаляются параметры, специфические для конкретного компьютера, что позволяет развертывать один образ на нескольких компьютерах.

**Кэширование файлов ответов на компьютере**

Файл ответов, используемый при установке Windows, кэшируется в системе, благодаря чему при выполнении последующих этапов установки параметры из файла ответов применяются к системе.

Поскольку файл ответов кэшируется, то при выполнении команды **Sysprep** применяются параметры из кэшированного файла. При использовании параметров в другом файле ответов можно указать отдельный файл **Unattend.xml** с помощью параметра sysprep /unattend:filename.

**Сохранение драйверов устройств Plug and Play во время обобщения**

Можно сохранить драйверы устройств при выполнении команды **sysprep** с параметром /generalize, задав параметр "PersistentAllDeviceInstalls" в компоненте "Microsoft-Windows-PnPSysprep". Во время этапа **specialize** модуль "Plug and Play" проверяет наличие устройств в системе и устанавливает драйверы для обнаруженных устройств. По умолчанию эти драйверы устройств удаляются из системы на этапе **generalize**. Если в файле ответов задать для параметра "PersistAllDeviceInstalls" значение "true", **Sysprep** не удалит обнаруженные драйверы устройств.

**Требования к корпоративной лицензии и OEM-активации**

Для корпоративных лицензий поведение сброса часов активации различается в зависимости от типа лицензии.

- Активация может быть сброшена неограниченное число раз для клиентов активированной службы управления ключом (KMS). Для клиентов с неактивированной KMS часы активации могут быть сброшены до трех раз, как и при лицензии на один компьютер. Клиентам KMS рекомендуется использовать команду sysprep /generalize со значением параметра "SkipRearm", равным 1. После захвата данного образа следует использовать команду sysprep /generalize со значением параметра "SkipRearm", равным 0.
- Для клиентов с несколькими ключами активации (MAK) рекомендуется установить MAK непосредственно перед запуском команды **Sysprep** в последний раз, перед поставкой компьютера заказчику.

**Загрузка в режиме аудита или с экраном приветствия Windows**

При загрузке Windows 7 существует два режима:

- **Экран приветствия Windows - запуск при первом включении компьютера (режим OOBE), является первым доступным пользователю интерфейсом, позволяющим конечным пользователям настроить установку Windows**. Конечному пользователю предлагается создать учетные записи, ознакомиться и принять условия лицензионного соглашения корпорации Майкрософт, а также выбрать язык и часовой пояс. По умолчанию все установки Windows начинаются с экрана приветствия. Этап настройки **oobeSystem** выполняется непосредственно перед загрузкой экрана приветствия Windows.
- Режим аудита. **Режим аудита позволяет изготовителям оборудования (OEM) и корпорациям добавлять изменения к образам Windows**. В режиме аудита не требуется, чтобы применялись параметры экрана приветствия Windows. При обходе экрана приветствия Windows можно быстрее получить доступ к рабочему столу и внести изменения. Можно добавить дополнительные драйверы устройств, установить приложения и

проверить правильность установки. В режиме аудита обрабатываются параметры автоматического файла ответов этапов настройки **auditSystem** и **auditUser**. Во время работы в режиме аудита запустите команду sysprep /oobe, чтобы установка загружалась с экраном приветствия Windows. Изготовители оборудования (OEM) должны запустить команду sysprep /oobe перед отправкой компьютера конечному пользователю. При установке по умолчанию после выполнения установки Windows запускается экран приветствия Windows. Но можно пропустить экран приветствия Windows и загрузиться непосредственно в режиме аудита, нажав клавиши **CTRL+SHIFT+F3** на первом экране приветствия Windows. При автоматической установке можно настроить Windows загружаться в режиме аудита с помощью параметра "Microsoft-Windows-Deployment | Reseal" в файле ответов.

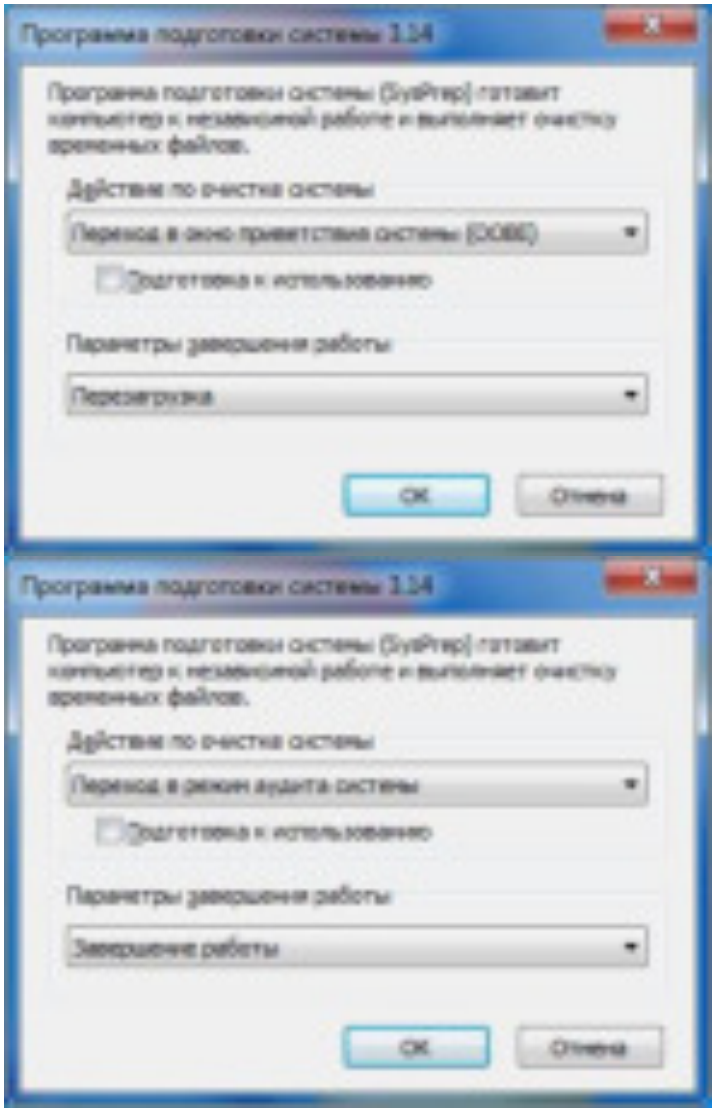
**Синтаксис команд Sysprep**

sysprep.exe [/oobe | /audit] [/generalize] [/reboot | /shutdown | /quit] [/quiet] [/unattend:файл_ответов]

- /audit **-** запускает компьютер в режиме аудита и позволяет добавлять дополнительные драйверы устройств и приложения. Можно также проверить установку Windows перед доставкой ее конечному пользователю. Если выбрана автоматическая установка Windows, режим аудита запускает этапы настройки auditSystem и auditUser.
- /generalize - подготавливает установку Windows перед созданием образа. Если этот параметр указан, все уникальные системные сведения удаляются из установки Windows. Идентификатор безопасности ( **SID** ) обнуляется, точки восстановления системы сбрасываются, журналы событий удаляются. При следующем запуске компьютера запускается этап настройки **specialize**. Создается новый идентификатор безопасности ( **SID** ) и сбрасываются часы активации Windows, если они еще не были сброшены трижды.
- /oobe - перезапускает компьютер в режиме экрана приветствия Windows. Экран приветствия Windows позволяет конечным пользователям настраивать операционную систему Windows, создавать новые учетные записи, переименовывать компьютер и выполнять прочие задачи. До запуска экрана приветствия Windows выполняется обработка всех параметров этапа настройки oobeSystem в файле ответов.
- /reboot - перезагружает компьютер. Используйте этот параметр для аудита компьютера и проверки работоспособности первого запуска системы.
- /shutdown - выключает компьютер после завершения команды sysprep.

- /quiet - отключает отображение запросов на подтверждение во время работы средства **Sysprep**. Используйте этот параметр при автоматизации работы средства **Sysprep**.
- /quit - закрывает средство **Sysprep** после выполнения указанных команд.
- /unattend:файл_ответов - применяет настройки файла ответов к Windows во время автоматической установки.

Графический интерфейс утилиты **sysprep.**




### Настройка oobe

Oobe.xml - это файл, который можно использовать вместе с Unattend.xml для хранения и развертывания корпоративных настроек и настроек изготовителей оборудования для экрана приветствия Windows, окна начального приложения изготовителя оборудования и мастера подключения к Интернету.

Oobe.xml обычно используется в следующих сценариях:

- Вместе с Unattend.xml - для задания значений по умолчанию для экрана приветствия Windows и мастера подключения к Интернету, устанавливаемых изготовителями оборудования (OEM) или организациями.
- Без Unattend.xml - для задания значений по умолчанию для экрана приветствия Windows и мастера подключения к Интернету, устанавливаемых изготовителями оборудования (OEM) или организациями.

**Oobe.xml с параметрами Unattend.xml**

Несмотря на то, что Oobe.xml может содержать все сведения для настройки экрана приветствия Windows, можно использовать параметры Unattend.xml, чтобы определить, каким образом конечный пользователь будет выбирать региональные настройки. Кроме того, параметры файла Unattend.xml можно использовать для отображения или скрытия отдельных страниц с целью проверки.

В следующем списке перечислены компоненты с параметрами Unattend.xml, которые могут использоваться для управления страницами экрана приветствия Windows.

- "Microsoft-Windows-Setup"
- "Microsoft-Windows-Shell-Setup"
- "Microsoft-Windows-International-Core"
- "Microsoft-Windows-International-Core-WinPE".

Этапы экрана приветствия Windows:

1. Региональные параметры:
    - "Microsoft-Windows-International-Core-WinPE | UILanguage"
    - "Microsoft-Windows-International-Core-WinPE | InputLocale"
    - "Microsoft-Windows-International-Core-WinPE | SystemLocale"
    - "Microsoft-Windows-International-Core-WinPE | UILanguageFallback"
    - "Microsoft-Windows-International-Core-WinPE | UserLocale"

    Если установлены все четыре параметра, то эта страница приветствия пропускается. Если некоторые параметры установлены, они не будут отображаться на странице приветствия.

2. Условия лицензии:
    - "Microsoft-Windows-Shell-Setup | OOBE | HideEULAPage"

    Если этот параметр установлен, данная страница будет пропущена. Предполагается, что администратор организации соглашается с

условиями лицензионного соглашения корпорации Майкрософт для пользователей.

3. Ключ продукта:
   - "Microsoft-Windows-Setup | UserData | ProductKey | Key"
   - "Microsoft-Windows-Setup | UserData | ProductKey | WillShowUI"

   Если обнаруживается, что пользователь уже ввел ключ, или допустимый ключ продукта указан в файле Unattend.xml, или используется установка с корпоративным лицензированием, эта страница не отобразится.

4. Имя пользователя:
   - "Microsoft-Windows-Shell-Setup | UserAccounts | LocalAccounts | LocalAccount | Description"
   - "Microsoft-Windows-Shell-Setup | UserAccounts | LocalAccounts | LocalAccount | DisplayName"
   - "Microsoft-Windows-Shell-Setup | UserAccounts | LocalAccounts | LocalAccount | Group"
   - "Microsoft-Windows-Shell-Setup | UserAccounts | LocalAccounts | LocalAccount | Name"
   - "Microsoft-Windows-Shell-Setup | UserAccounts | LocalAccounts | LocalAccount | Password | PlainText"
   - "Microsoft-Windows-Shell-Setup | UserAccounts | LocalAccounts | LocalAccount | Password | Value"

   Если учетная запись пользователя была создана с помощью этого параметра, эта страница не отобразится. Если эта страница не отображается, рисунок для пользователя выбирается автоматически. В файле Unattend.xml нет параметра для задания рисунка пользователя.

5. Имя компьютера:
   - "Microsoft-Windows-Shell-Setup | ComputerName"

   Если этот параметр установлен, страница Имя компьютера не будет отображаться на экране приветствия Windows. На этой странице также можно выбрать первоначальный фоновый рисунок. Если страница не отображается, первый фоновый рисунок Windows будет выбран по умолчанию

6. Защита компьютера
   - "Microsoft-Windows-Shell-Setup | OOBE | ProtectYourPC"

   Если этот параметр задан, страница отображаться не будет и параметру будет присвоено требуемое значение. Возможны следующие значения: 1

– Рекомендуемый, 2 - Только обновления установки, 3 - Защита отключена

**Oobe.xml без Unattend.xml**

При использовании только для фирменной символики и региональных настроек Oobe.xml отображает все страницы экрана приветствия Windows.

**Как работает Oobe.xml**

Возможности приветствия Windows и подписки поставщика услуг Интернета, получающие данные из Oobe.xml, выполнят поиск и загрузку файлов Oobe.xml в следующих папках в следующем порядке:

1. %WINDIR%\System32\Oobe\Info\Oobe.xml
2. %WINDIR%\System32\Oobe\Info\Default\Oobe.xml
3. %WINDIR%\System32\Oobe\Info\Default\<language>\Oobe.xml
4. %WINDIR%\System32\Oobe\Info\<country>\Oobe.xml
5. %WINDIR%\System32\Oobe\Info\<country>\<language>\Oobe.xml

При использовании настроек, охватывающих все страны и языки, файлы Oobe.xml можно разместить в папке, указанной в пункте 1.

При поставке одноязычной системы для одного региона настроенный файл Oobe.xml следует размещать в каталоге \Info или \Default, как показано в пунктах 1 и 2. Пункты 1 и 2 имеют одинаковое влияние.

Если при выполнении поставок в несколько стран параметры OOBE требуют настройки в зависимости от страны, причем для каждой используется один язык, то все файлы Oobe.xml следует размещать в папках, соответствующих пунктам 4 и 5 этого списка.

При поставке в несколько стран с несколькими языками нужно соблюдать следующие указания:

- Размещайте специфические для страны данные в папке пункта 4.
- Размещайте специфические для языка данные для каждой соответствующей страны в папке пункта 5.

**Параметры Oobe.xml**

В данном разделе описаны параметры, которые можно задать в файле Oobe.xml. Пример файла Oobe.xml поставляется с пакетом автоматической установки Windows (Windows AIK) в папке \Samples. В этом примере используется вымышленная компания Fabrikam, ее графика и предложения.

**Просмотр файлов примеров в экране приветствия Windows**

- Скопируйте папку \Info в папку **\Windows\System32\Oobe** и папку **\Fabrikam** в корневой каталог диска C:, где C - это буква диска, на котором установлена операционная система Windows.

**Просмотр экрана приветствия Windows с содержимым примера**

1. В меню "Пуск" укажите "Все программы", а затем выберите "Стандартные".
2. Щелкните правой кнопкой мыши пункт "Командная строка" и выберите команду "Запуск от имени администратора".
3. Примите параметры в диалоговом окне "Контроль учетных записей пользователей".
4. Перейдите к \Windows\System32\Sysprep.
5. Выполните sysprep /oobe.
6. Запустите компьютер.

## Краткие итоги

После ознакомления с данной лекцией необходимо помнить важные моменты:

1. Утилита **sysprep** позволяет подготовить установленную операционную систему так, что можно создать образ для его клонирования любое количество компьютеров.
2. Можно сбросить активацию не более 3 раз.
3. Sysprep можно использовать как в командной строке, так и в графическом интерфейсе.
4. Утилита **sysprep** позволяет загрузиться в режим аудита или провести настройку экрана приветствия.
5. Настройка экрана приветствия осуществляется с помощью конфигурационного файла oobe.xml, не совместимого с Windows SIM.
6. Если задать все необходимые параметры, применимые к **oobeSystem**, то экран приветствия Windows не будет отображаться.

Следующая лекция будет всецело посвящена утилите командной строки – **ImageX**, позволяющей создать образ операционной системы, скопировать его в общую папку или любой другой ресурс и в дополнении к этому осуществляет развертывание образа на диск.

**Oobe.xml** - это файл, который можно использовать вместе с Unattend.xml для хранения и развертывания корпоративных настроек и настроек изготовителей оборудования для экрана приветствия Windows, окна начального приложения изготовителя оборудования и мастера подключения к Интернету.

**Sysprep** – это штатный инструмент развёртывания Windows, утилита, предназначенная преимущественно для *OEM*-производителей и корпоративных *IT*-специалистов. Используется для подготовки брендовых и, соответственно, корпоративных сборок Windows. *OEM*-сборщики и *IT*-специалисты на компьютере или виртуальной машине подготавливают эталонный образ Виндовс: в установленную из официального дистрибутива систему внедряют обновления.

А также корпоративный, брендовый или партнёрский софт, удаляют или отключают встроенный в систему функционал, проводят нужные системные настройки. Затем уже настроенную систему отвязывают от комплектующих того компьютерного устройства, на котором проводилась работа, убирают идентифицирующие данные. И, наконец, запаковывают всё это в образ для развёртывания на конечных устройствах пользователей или сотрудников компании. Это может быть либо установочный *ISO*-файл, либо резервная копия. В этой цепочке действий *Sysprep* играет роль механизма отвязки от железа и идентифицирующих данных. В каких случаях эта утилита может пригодиться обычному пользователю, как она работает, какие у неё есть ограничения, и как с ними справиться – об этом всём ниже.

**Что такое Sysprep**

Утилита *Sysprep* удаляет драйверы комплектующих, обнуляет SID, чистит системный журнал событий и папки *«Temp»*, сбрасывает активацию *(до трёх раз)*, уничтожает точки восстановления. В общем, заботится о том, чтобы при новом запуске мы получили чистую операционную систему, только с определёнными предустановками.

**Области использования**

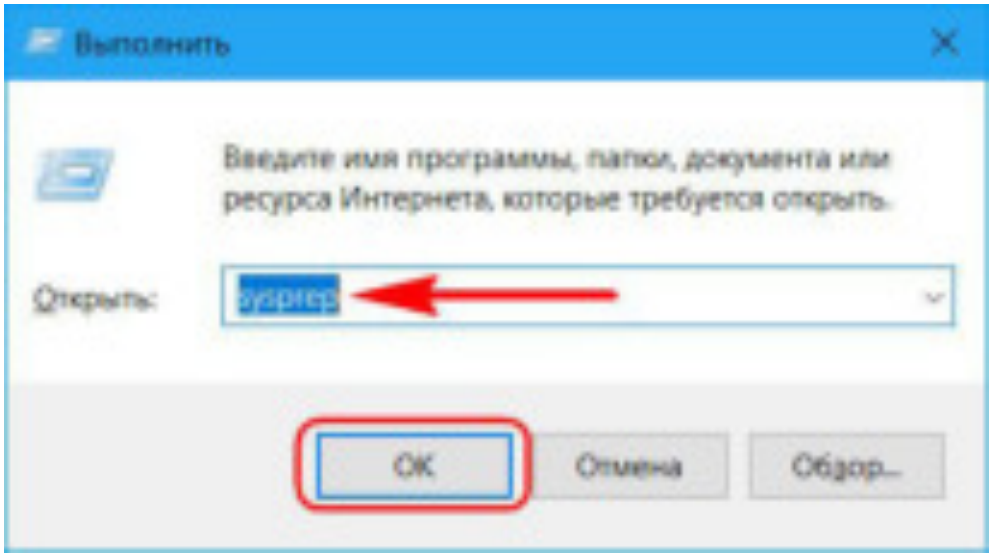
Создание эталонных образов модифицированных сборок Виндовс для развёртывания на множестве клиентских компьютеров – главная задача *Sysprep*. Но утилиту также могут использовать обычные пользователи на своих домашних устройствах. К её помощи можно прибегнуть в случае нестабильной работы Windows после замены комплектующих. А ещё лучше – применить её перед тем, как менять эти комплектующие.

*Sysprep* – это ещё и инструмент, с помощью которого можно перенести рабочую систему на другое компьютерное устройство с отличными комплектующими. *Бэкап*-софт профессионального уровня для таких случаев предусматривает функции типа **Universal Restore**, **Adaptive Restore** и *т.п.* Эти функции делают, по сути, то же, что и *Sysprep*, только на этапе восстановления. Благодаря чему в эталонный образ можно превратить любой старый бэкап Windows. Но такого рода функции редко когда встретишь на борту бесплатных

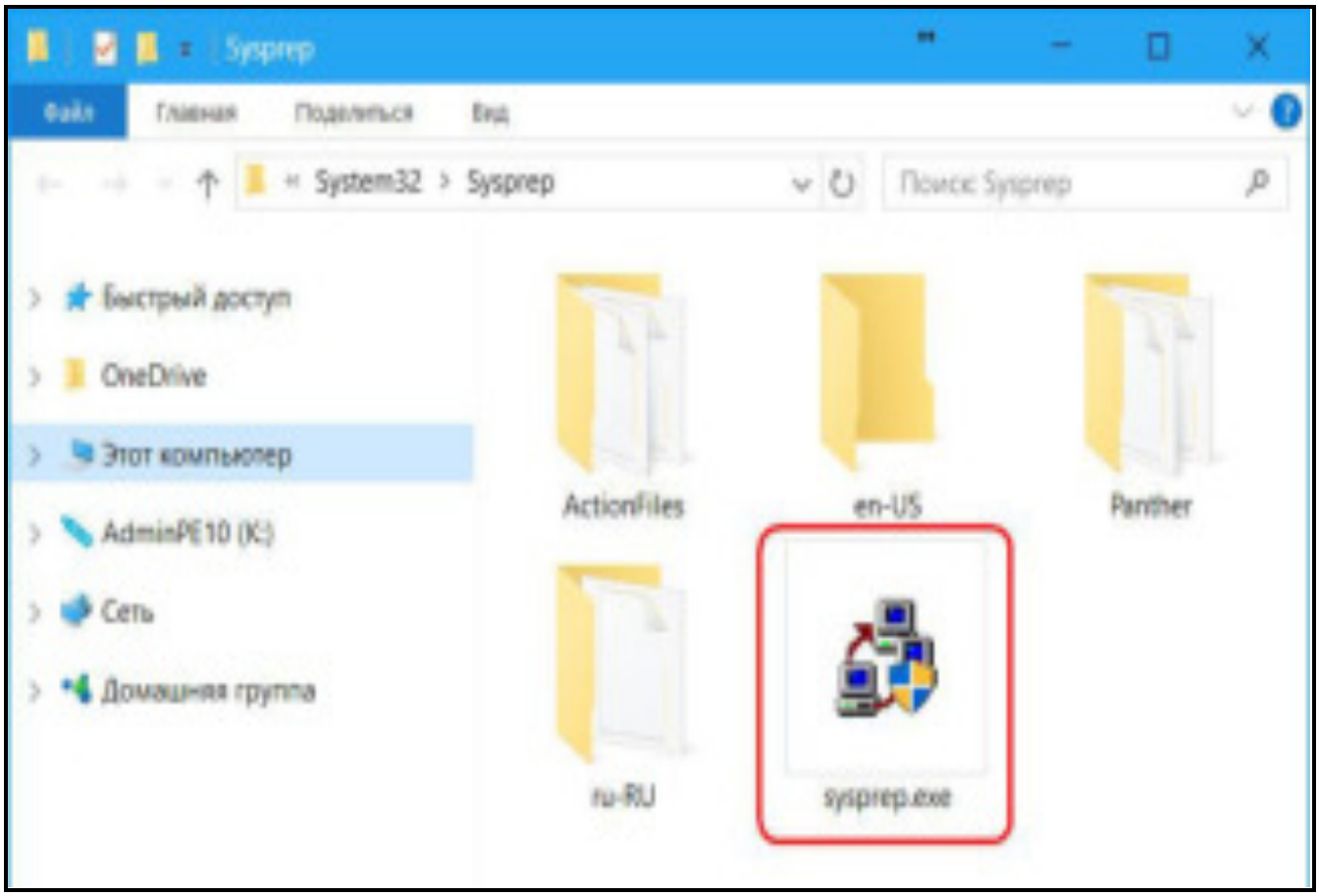
бэкаперов. К примеру, они есть на борту изначально платного ПО от **Acronis** и **Paragon**, а также поставляются только в платных редакциях ПО от **AOMEI** и **EaseUS**. Если Windows отвязать от комплектующих с помощью *Sysprep*, её можно перенести на другой компьютер с использованием загрузочных носителей бесплатных бэкаперов, например, от тех же разработчиков *AOMEI* и *EaseUS*.

**Запуск утилиты**

Запуск *Sysprep* проще всего осуществить с помощью команды Win+R.



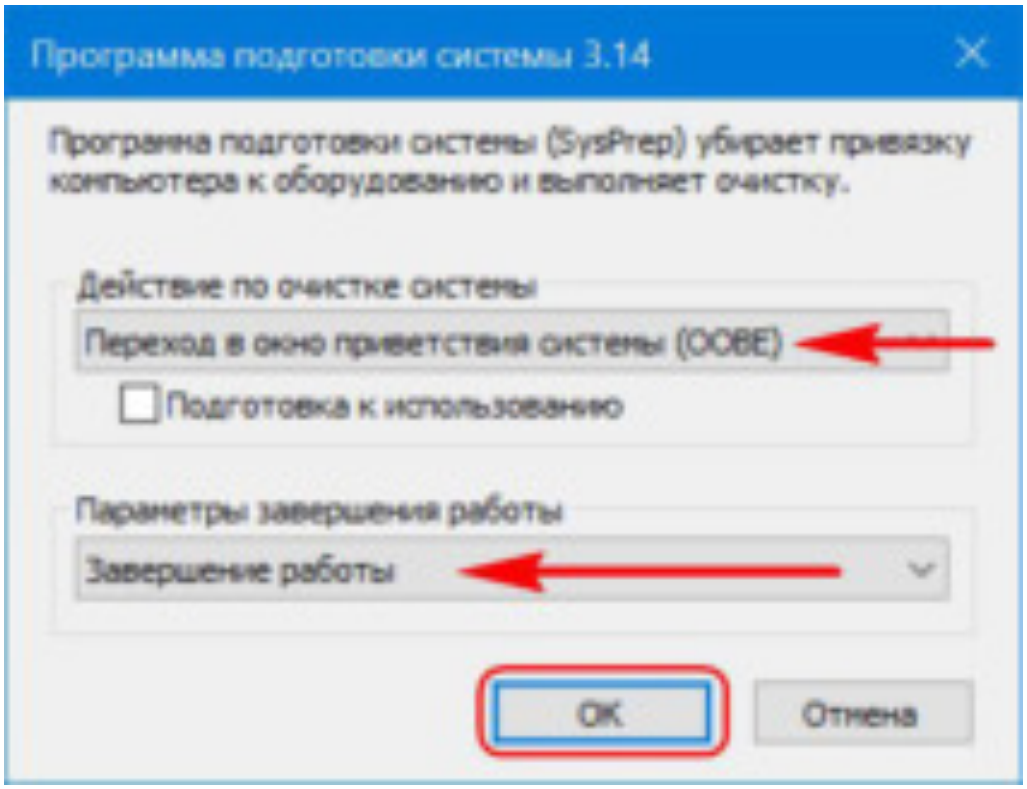

Таким образом в проводнике получим непосредственный доступ к файлу её запуска.




**Отвязка от комплектующих**

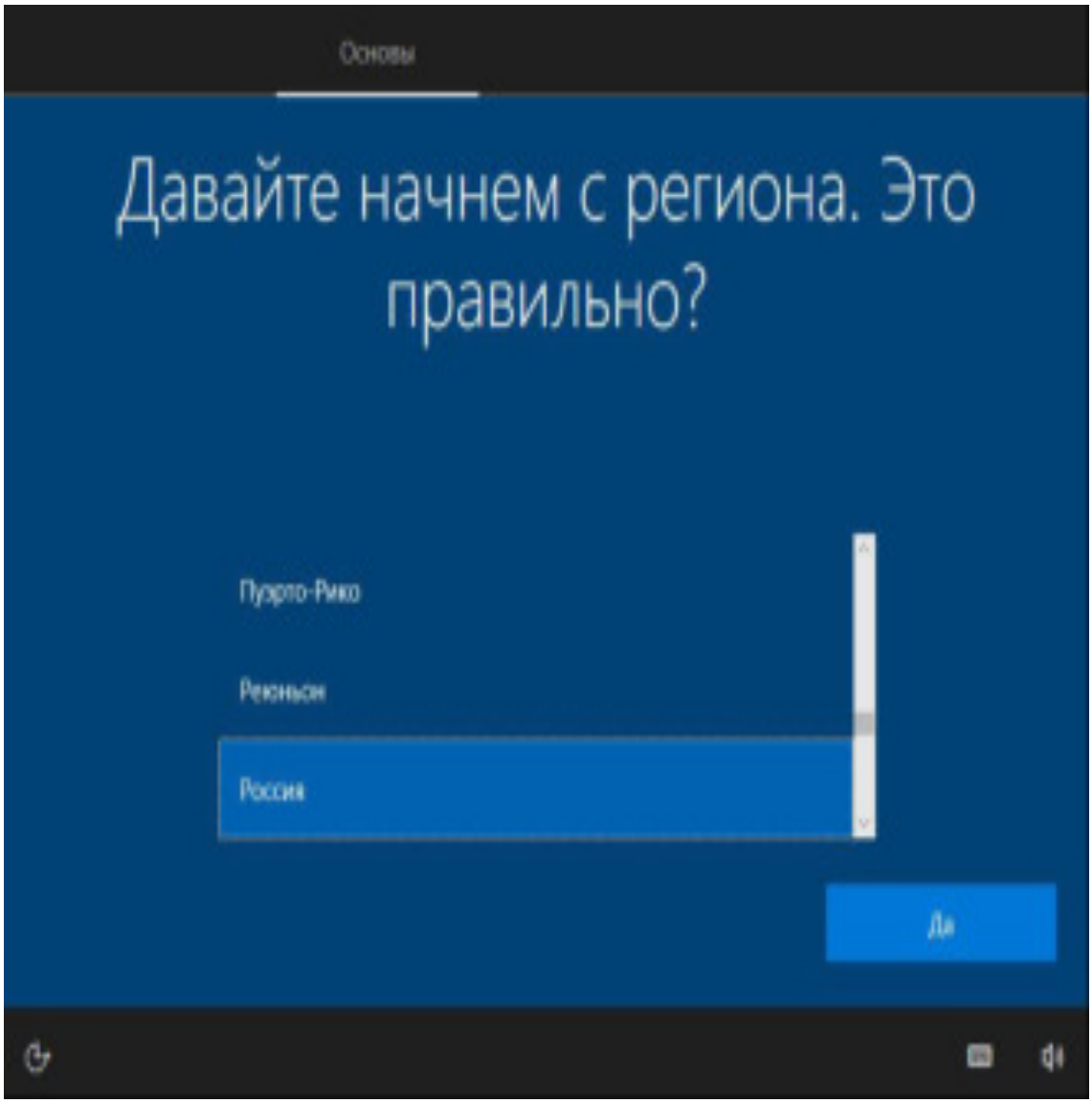
**Бэкап** (backup) - это резервное копирование данных, которое позволяет при необходимости восстановить файлы, диски или даже операционную систему целиком. При этом после восстановления состояние компьютера будет отличаться от того, которое было в момент начала резервного копирования. Это происходит из-за того, что резервное копирование занимает время, за это время некоторые файлы могут измениться.

Чтобы отвязать Windows от текущих комплектующих перед их заменой или созданием бэкапа системы для переноса на другое устройство, используем **«Переход в окно OOBE»** и выбираем **завершение работы**.




При таком раскладе утилита осуществит только сброс драйверов комплектующих. Если же выставить галочку опции **«Подготовка к использованию»**, будет проведён ряд мероприятий для передачи системы новому пользователю — чистка системного журнала и временных файлов, удаление точек восстановления, обнуление ***SID*****,** сброс активации и т.п.

Утилита выполнит свою работу, и компьютер выключится. Далее можно приступать к тем или иным действиям – менять комплектующие, бэкапить систему с загрузочного носителя. С новым включением – как на исходном устройстве, так и на том, куда система переносилась с помощью восстановления из бэкапа – сначала будем лицезреть, как устанавливаются драйверы на новые комплектующие, а затем попадём в окно ***OOBE***. Окно **OOBE** — это не что иное, как экран приветствия системы, который мы обычно видим на завершающем этапе установки Windows, где нужно указать региональные данные и создать свою учётную запись.

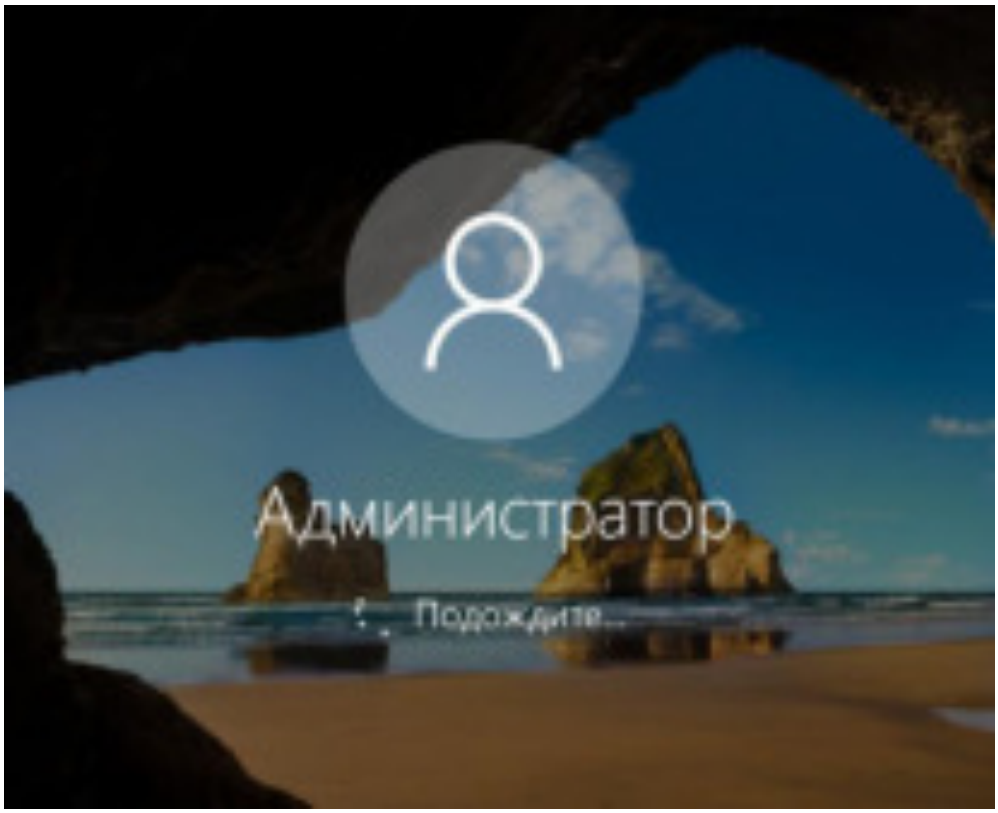



И поскольку при замене комплектующих или восстановлении Windows на других компьютерах в создании новой учётной записи нужды нет, спокойно можем сбросить этот процесс клавишами Ctrl+Shift+F3. Это клавиши входа в скрытую учётную запись администратора. Система попробует подгрузить её, но в доступе откажет. Жмём **«Ок»**.

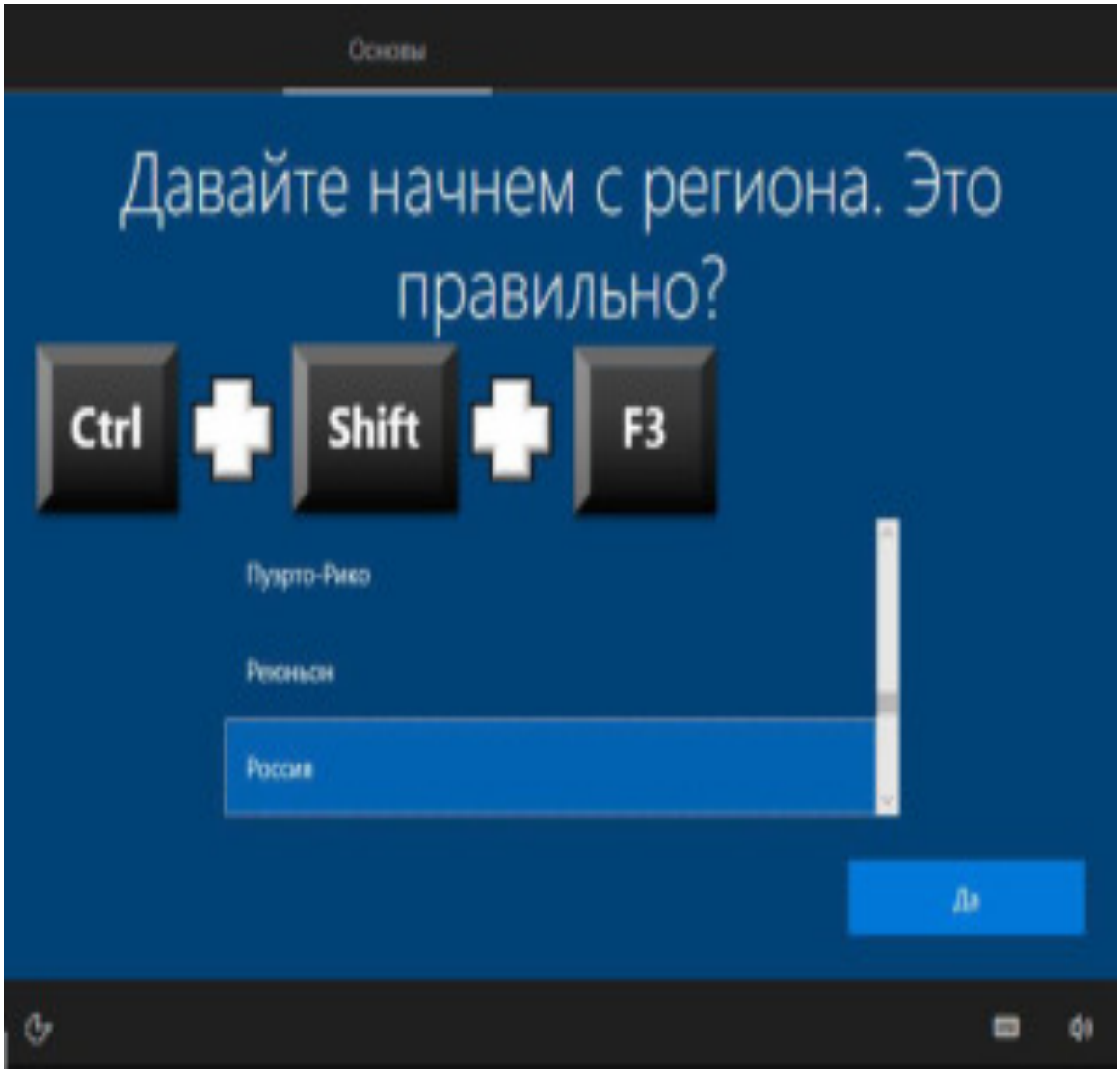

И после перезапуска увидим привычный экран блокировки со всеми существующими учётными записями.

**Режим аудита**

Режим аудита предоставляет возможность получить доступ к среде Виндовс без создания учётной записи конкретного пользователя, в режиме упомянутой учётной записи администратора.

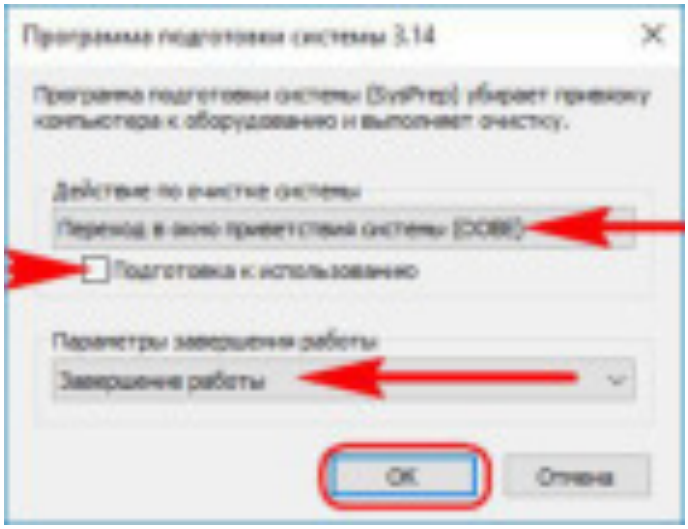


В этом режиме, собственно, и проводится *OEM*-производителями и *IT*-специалистами компаний настройка эталонного образа системы с нужными драйверами, параметрами и внедрённым софтом. Первичный вход в режим аудита выполняется на этапе установки Windows — той, что впоследствии должна стать эталонным образом, и на которой не должно существовать никаких пользовательских учётных записей и идентифицирующих данных. После этапа подготовки устройств попадём на завершающий этап установки системы, начинающийся с задания региональных настроек. И здесь жмём клавиши Ctrl+Shift+F3.

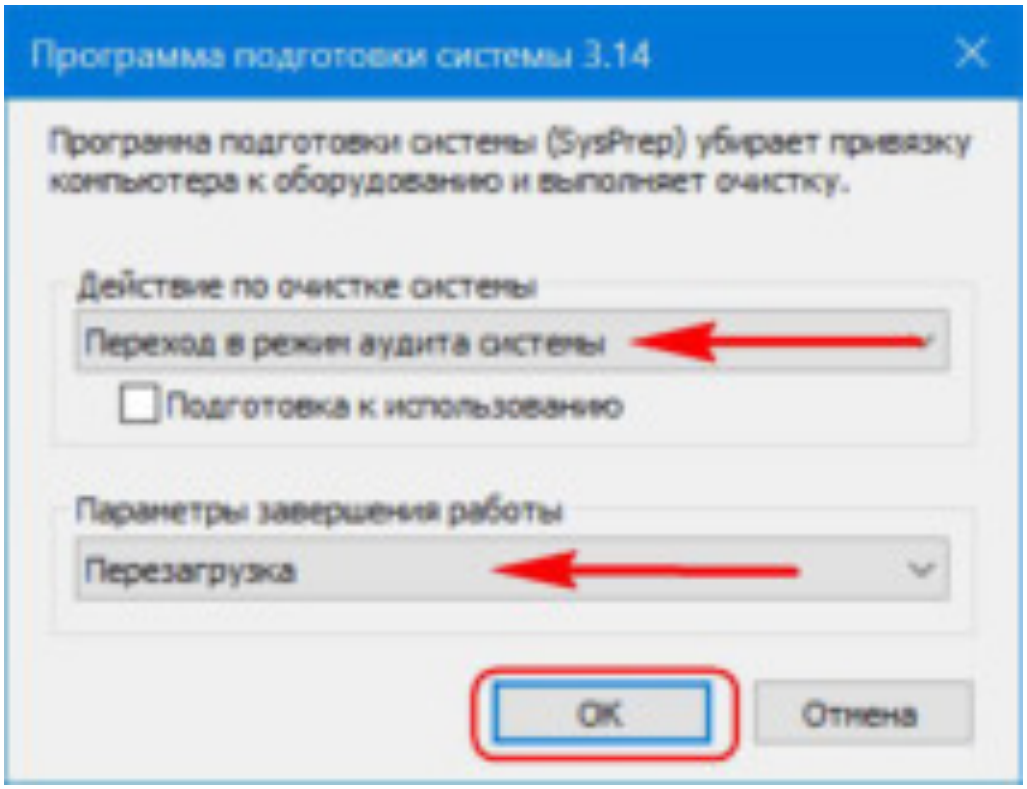



После перезагрузки попадём в режим аудита. Последний загружается с по умолчанию запущенным окном ***Sysprep*** для удобства. Вот, собственно, в таком режиме и можно приступать к модификации Windows. Если в процессе внесения правок в систему, например, при установке определённого софта потребуется перезагрузка, всё, что нужно сделать – это закрыть окно утилиты. И осуществить перезагрузку привычным образом. После перезагрузки система вновь запустится в режиме аудита. Завершается работа в этом режиме так, как

было рассмотрено в предыдущем пункте – выбором в окне ***Sysprep*** экрана ***OOBE***. И обычно с применением опции подготовки к использованию.




Эталонную модифицированную Windows обычно делают с чистой, только что установленной системы. Но возможен вариант создания эталона на базе наработанной системы. Для этого внутри рабочей Виндовс необходимо запустить ***Sysprep*** и выбрать в её окне **переход в режим аудита**. Завершающий работу параметр — **перезагрузка**.




Войдя в режим аудита, можем удалить учётные записи тех пользователей, которые доселе работали с системой, донастроить что нужно, а затем

выполнить отвязку от комплектующих *(и при необходимости от идентифицирующих данных)* с переходом в окно *OOBE*.

Вот только не с каждой рабочей системы удастся сделать эталонный образ. У этого механизма есть свои ограничения.

**Решение проблем с запуском Sysprep**

***Sysprep*** не сработает, если Windows была не установлена начисто, а обновлена с предыдущей версии, клонирована или восстановлена из бэкапа, созданного на другом железе. В таких случаях при запуске утилиты обычно получим такое вот уведомление.


В таком случае можно кое-что предпринять, правда, без гарантированного успеха во всех 100% случаев.

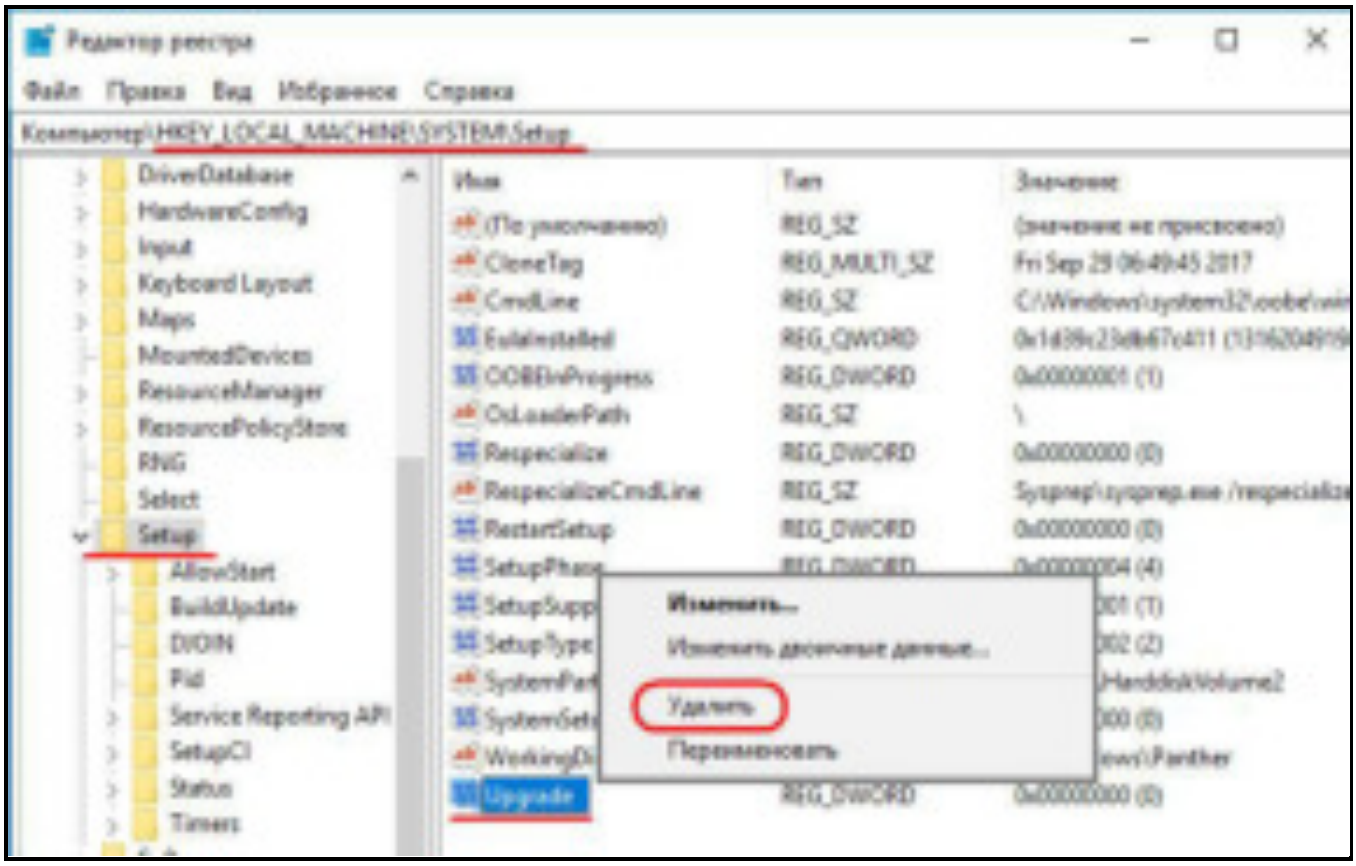
Создаём бэкап системы или хотя бы запасаемся точкой восстановления, поскольку далее будем работать с системным реестром.

Запускаем его.

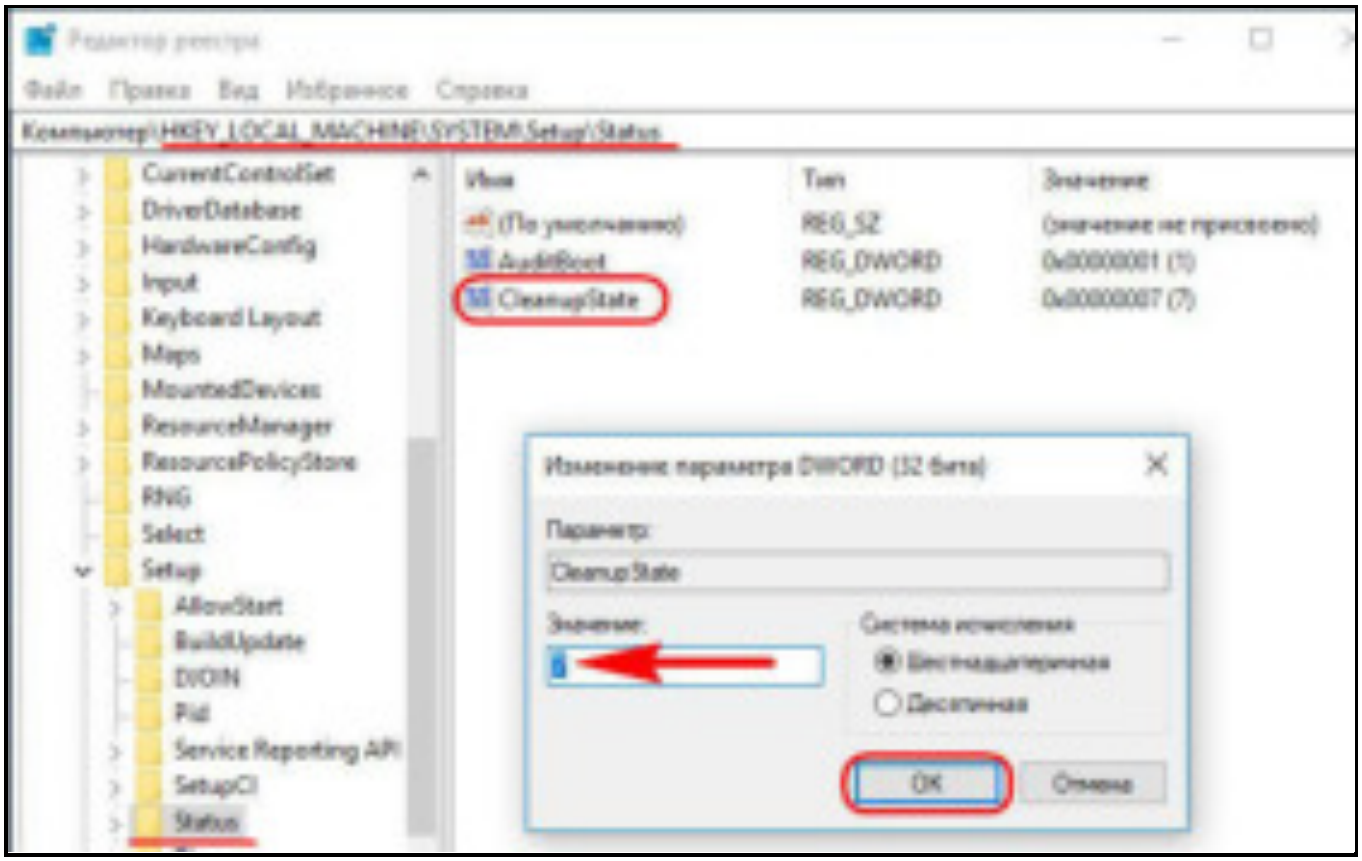
Раскрываем путь:

**HKEY_LOCAL_MACHINE\SYSTEM\Setup**

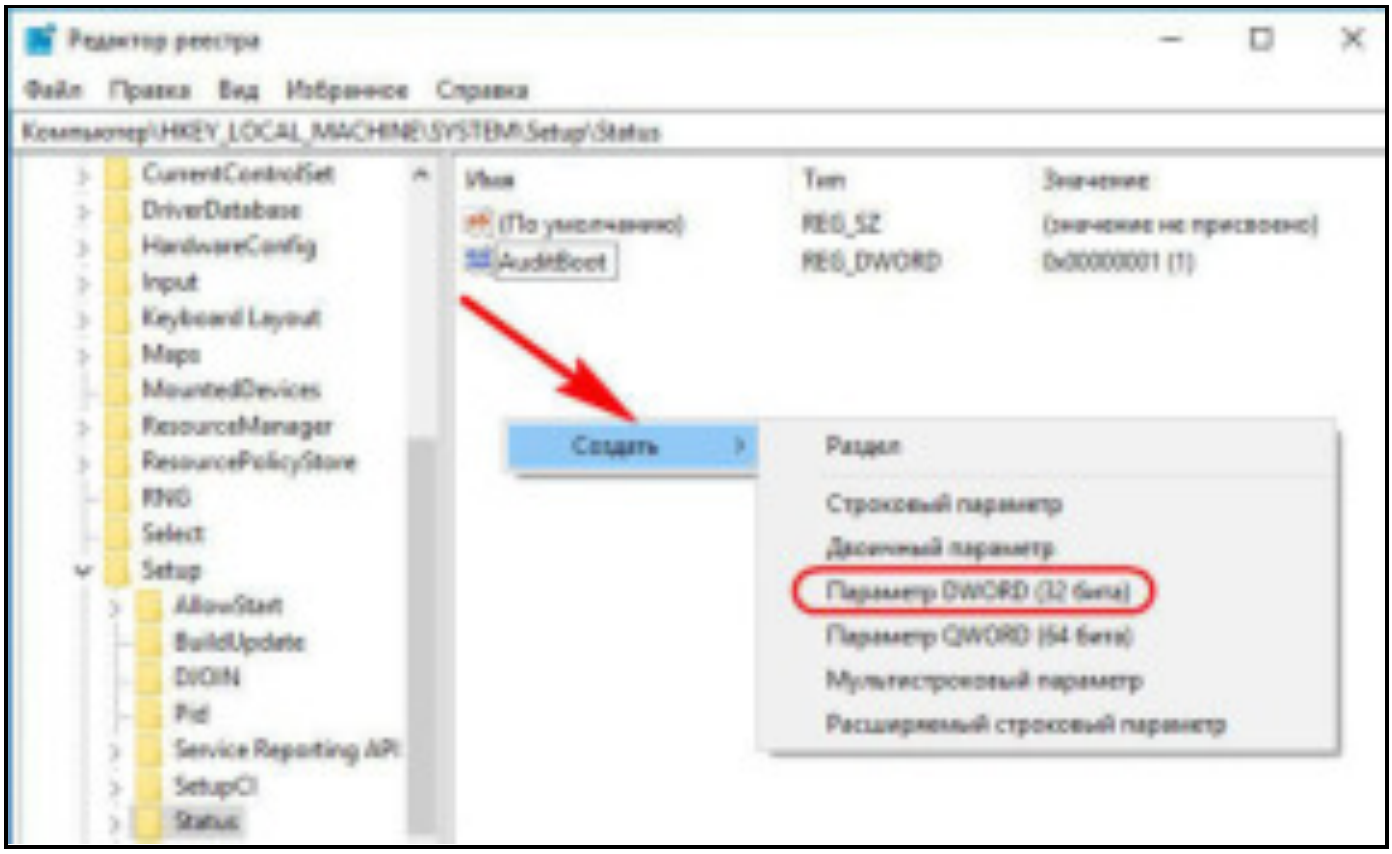
Если система обновлялась с предыдущей версии, в первую очередь в самом каталоге **«Setup»** удаляем параметр .



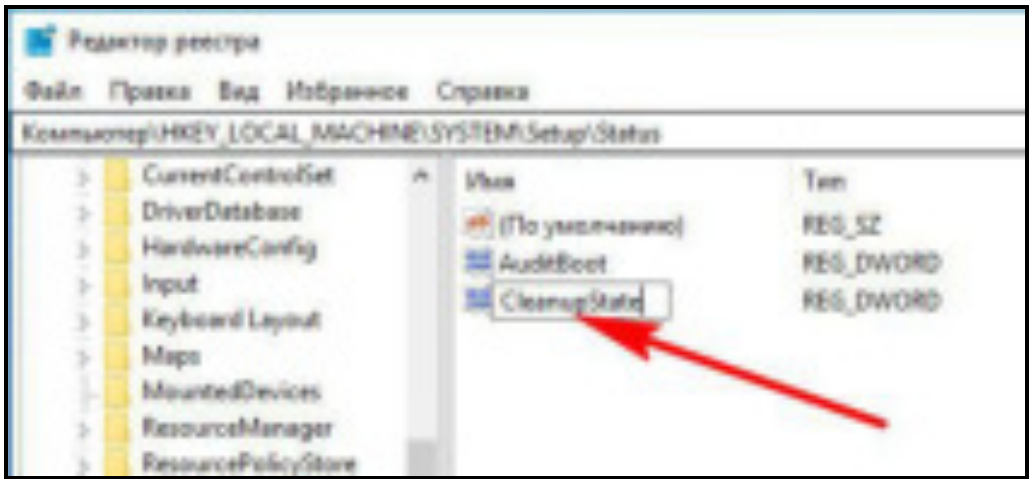

Затем раскрываем каталог **«Setup»**, кликаем подкаталог **«Status»**, здесь нам нужен параметр **«CleanupState»**. Устанавливаем его значение *7*.



Если такого параметра нет, создаём его. В контекстном меню окна реестра жмём **«Создать»**, затем – **«Параметр DWORD (32 бита)»**.




Даём имя параметру **«CleanupState»**.




Устанавливаем его значение *7*. После перезагрузки снова пробуем запустить ***Sysprep***.

**Создание файла автоматических ответов в Windows SIM**

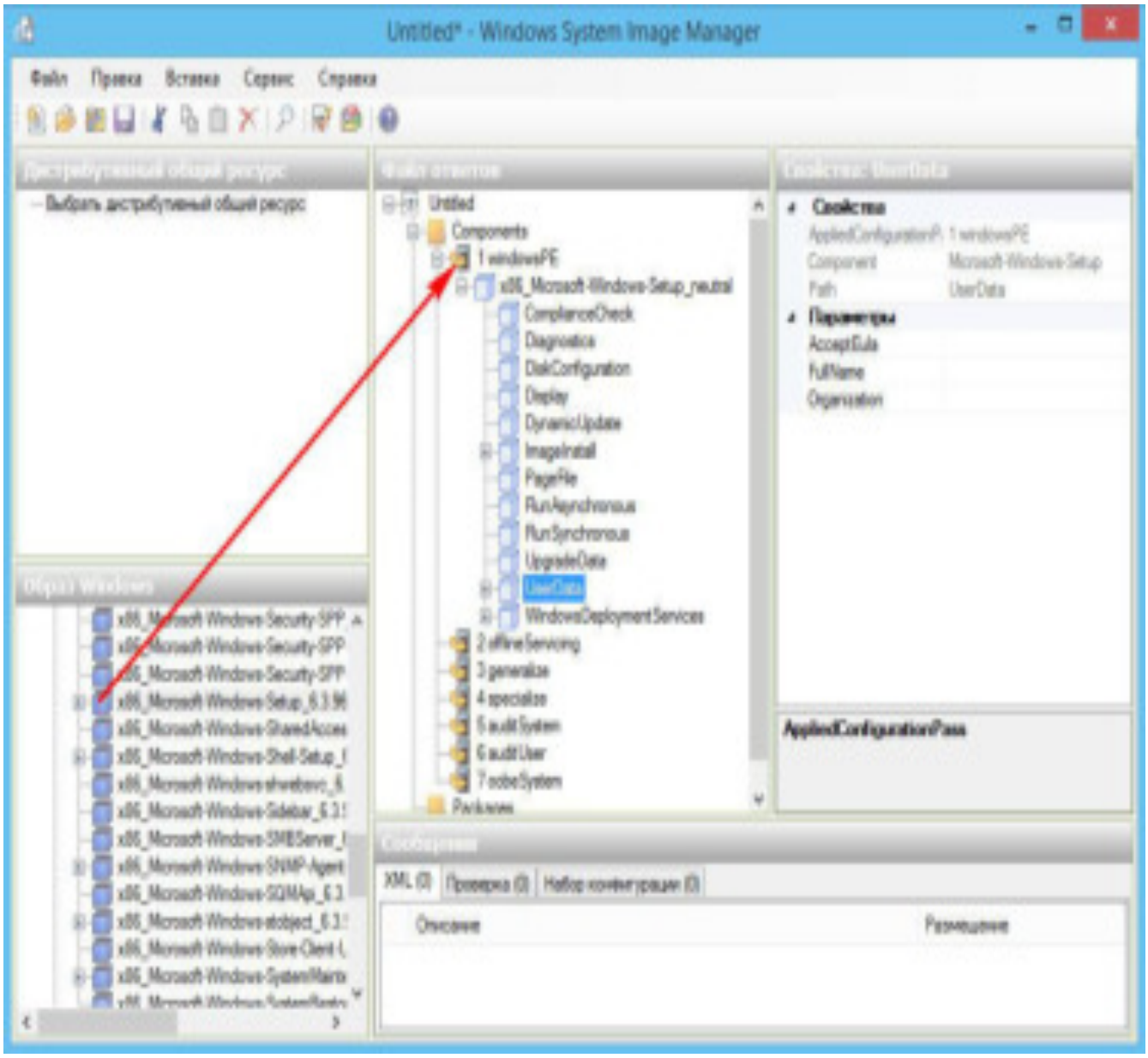
Использование файла автоматических ответов является одним из самых распространенных способов развертывания операционной системы Windows.

Избавляя от необходимости производить разбивку диска, настройку параметров и компонентов, этот метод развертывания позволяет экономить время во всех случаях, требующих оперативной установки Windows на несколько рабочих станций. Для создания файла используется утилита Windows SIM, входящая в состав комплекта средств развертывания и оценки ADK. Процедура создания файла ответов проходит в два этапа – экспорта образа install.wim и собственно самого генерирования команд в графическом интерфейсе Диспетчера Windows.

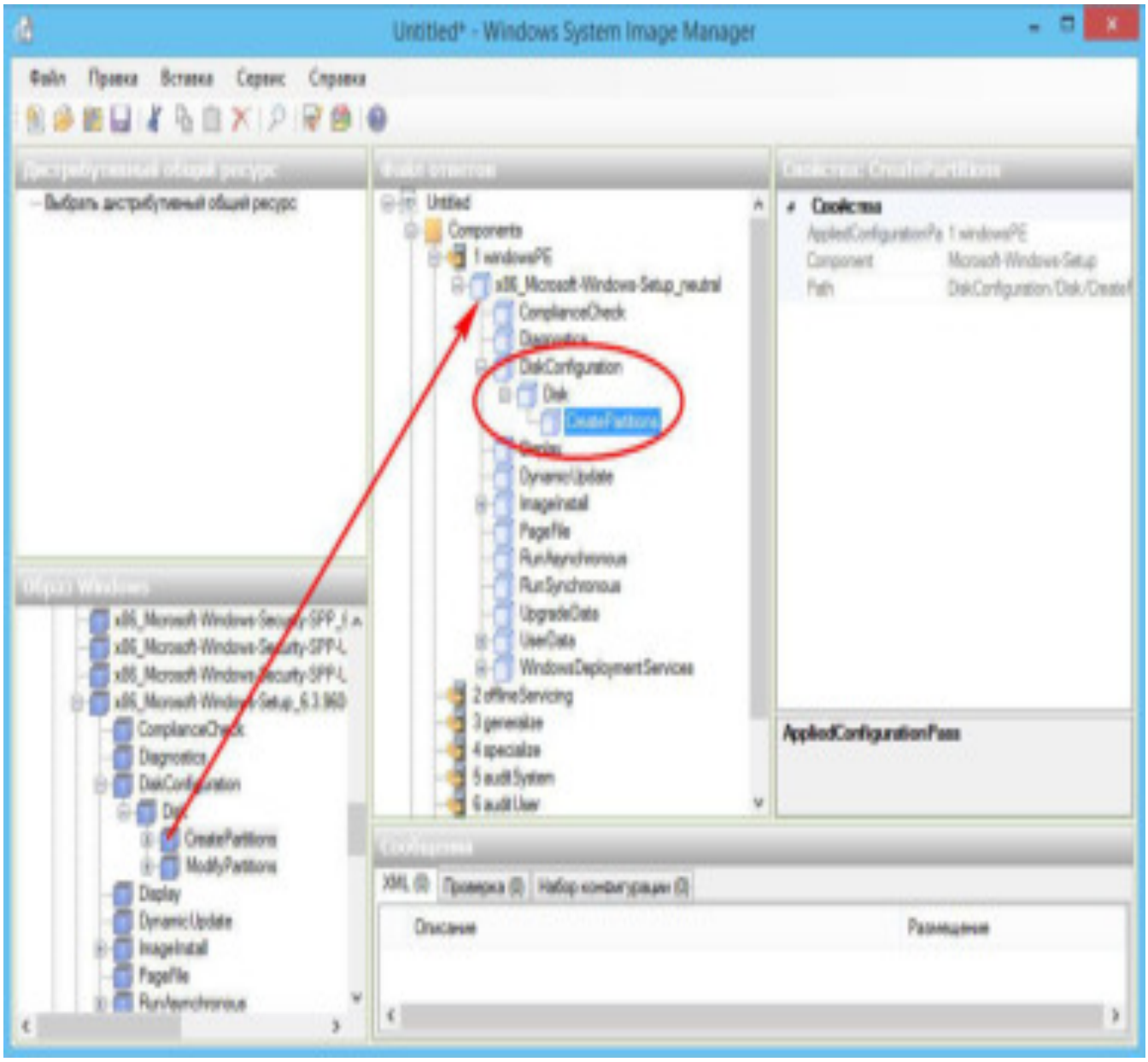
Этот второй этап мы как раз и рассмотрим. После подключения образа вам станут доступны каталоги Components и Packages. Они имеют древовидную структуру и содержат огромное количество компонентов и пакетов. Формирование файла ответов производится путём перетаскивания элементов в рабочую область Диспетчера. Как видите, файл ответов состоит из семи секций, также именуемыми фазами. Они не являются обязательными, вы можете задавать и настраивать только те этапы, которые вам нужны.

Первый компонент windowsPE позволяет автоматизировать базовые операции в начале установки Windows, например разбивку диска, выделение области под файл подкачки, ввод ключа продукта, настройку разрешения дисплея. OfflineServicing предназначается для обновления образа Windows, на этапе generalize из системы удаляется информация, относящаяся к оборудованию и безопасности. Этап specialize обеспечивает настройку специфических параметров системы, например настроек сети.

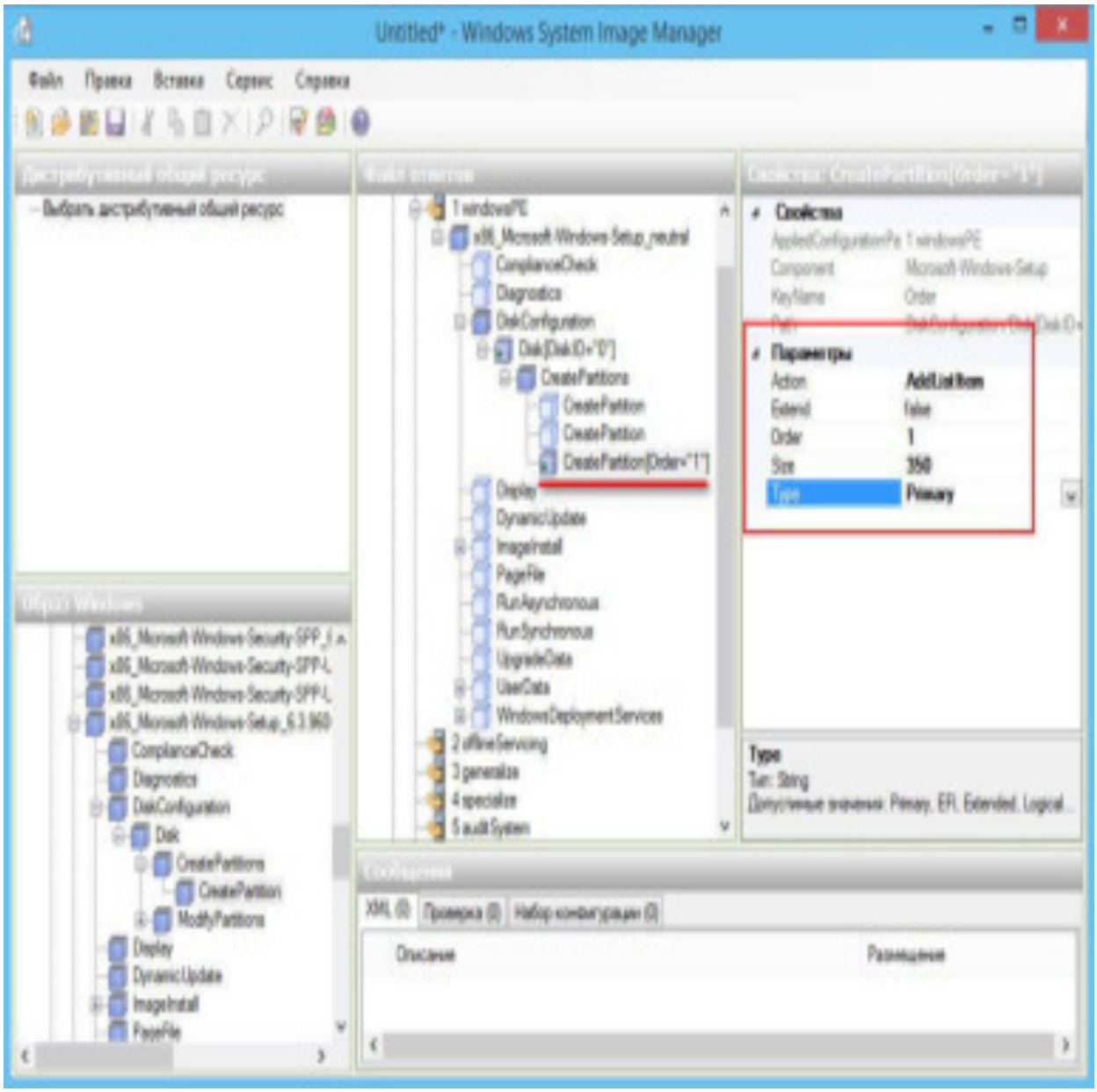
Фазы auditSystem и auditUser используется только в режиме аудита. Наконец, последний этап oobeSystem позволяет настраивать параметры первой загрузки клиента, то есть приветствия Windows. Однако на практике чаще всего используется фаза windowsPE. За параметры базовой настройки отвечает компонент Microsoft-Windows-Setup. Найдите его в списке «образ windows» и перетащите в файл ответов, а именно в подраздел windowsPE.



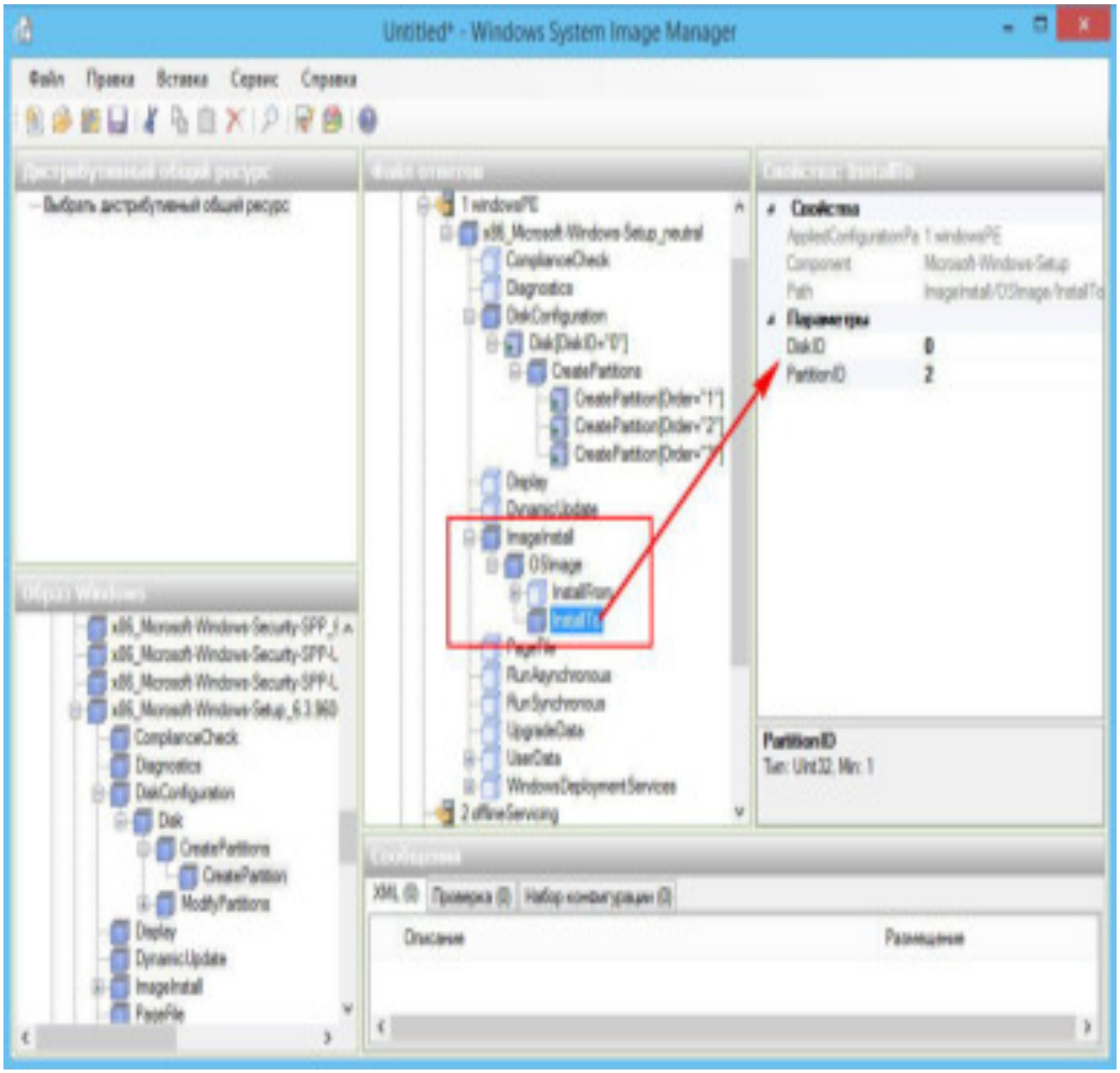

Допустим, нам нужно автоматизировать процесс подготовки разделов на жёстком диске. Опять же в списке «образ windows» находим компонент Microsoft-Windows-Setup, раскрываем его, отыскиваем в нем Create Partition и перетаскиваем его в корень Microsoft-Windows-Setup.



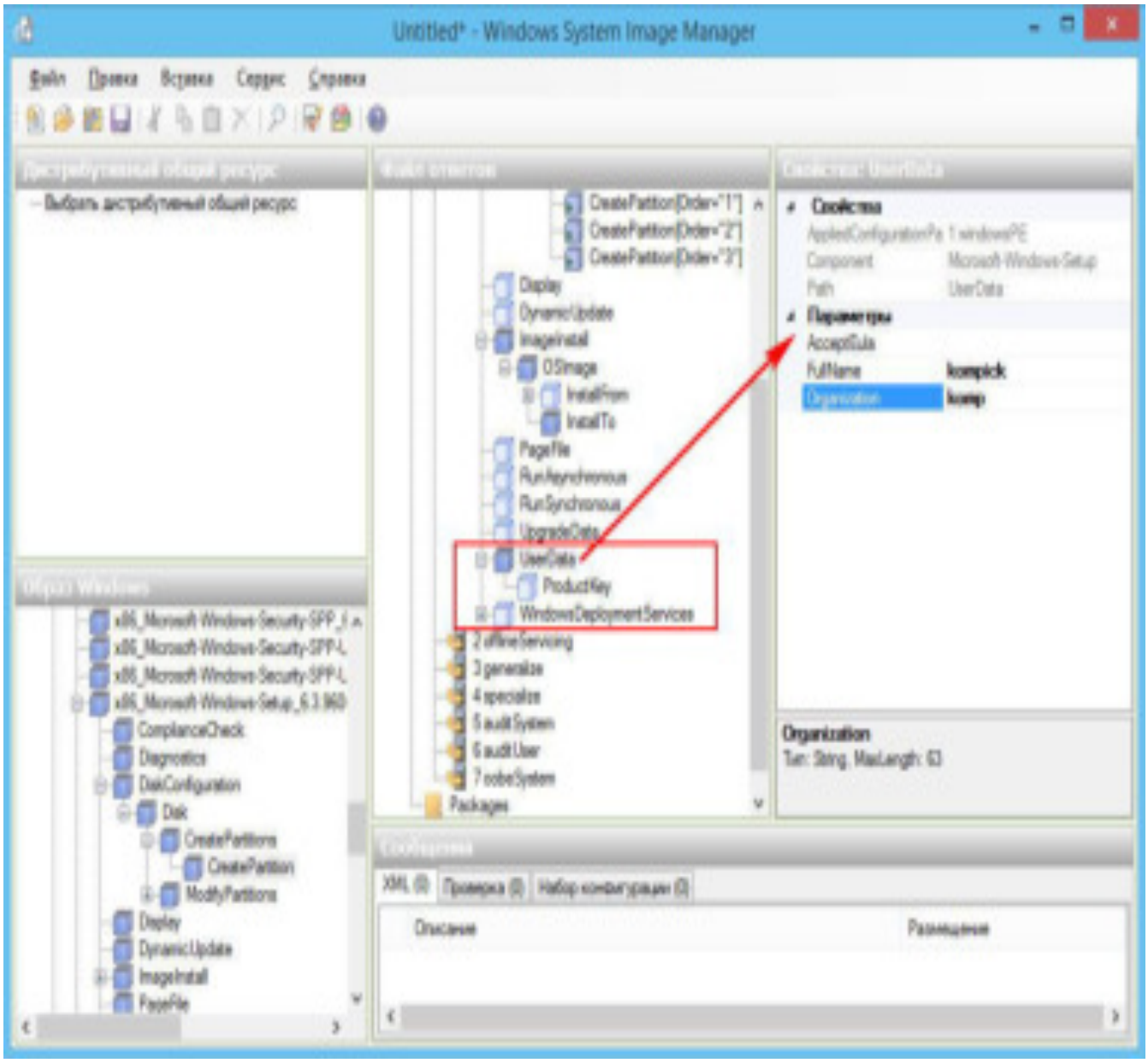

В свойствах диска идентификатор устанавливаем 0, в блок Create Partition забрасываем столько разделов, сколько нам нужно. В параметрах первого раздела номер устанавливаем равным 1, размер (в мегабайтах) не меньше 350, тип задаем Primary.



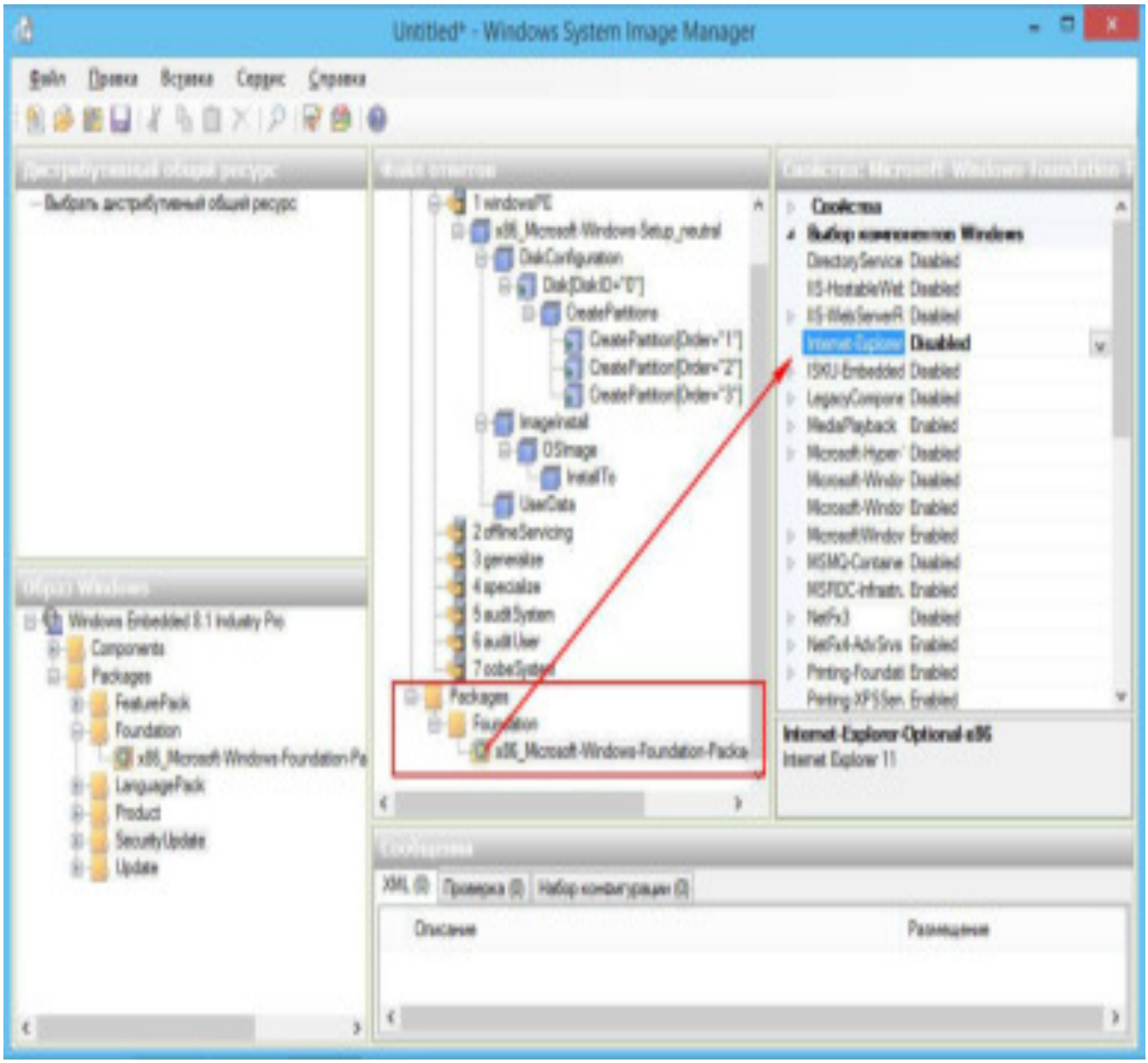

Соответственно второй раздел, на который будет устанавливаться операционная система будет иметь номер 2, размер не меньший чем того требует конкретная версия ОС, тип также устанавливаем Primary. При желании можете создать и логический раздел. Далее в разделе ImageInstsll (InstallTo) нужно указать идентификатор диска, как вы помните, он равен 0, и номер раздела, на который будет устанавливаться Windows. Это раздел номер 2.



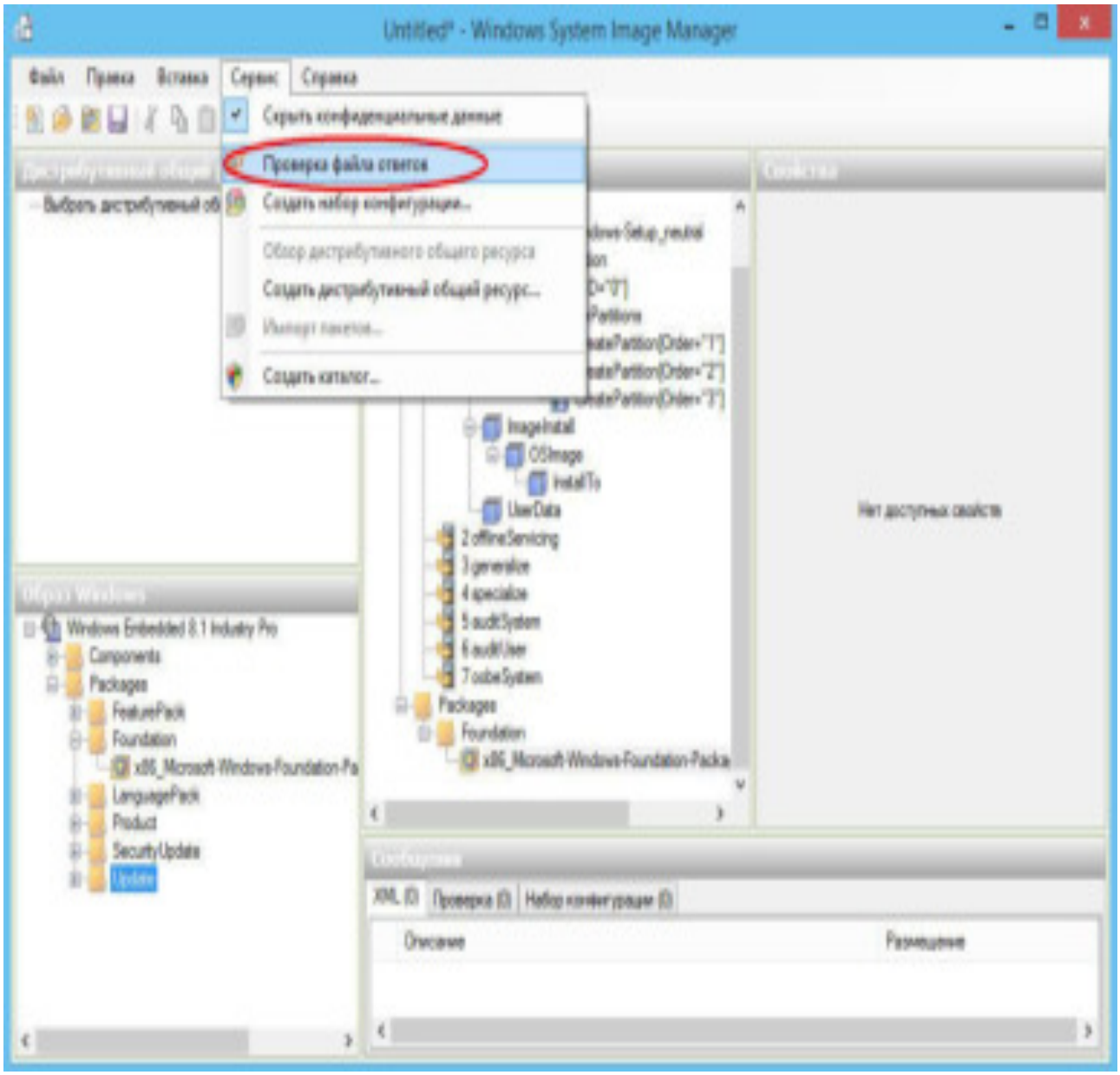

Другие параметры задаем по необходимости.



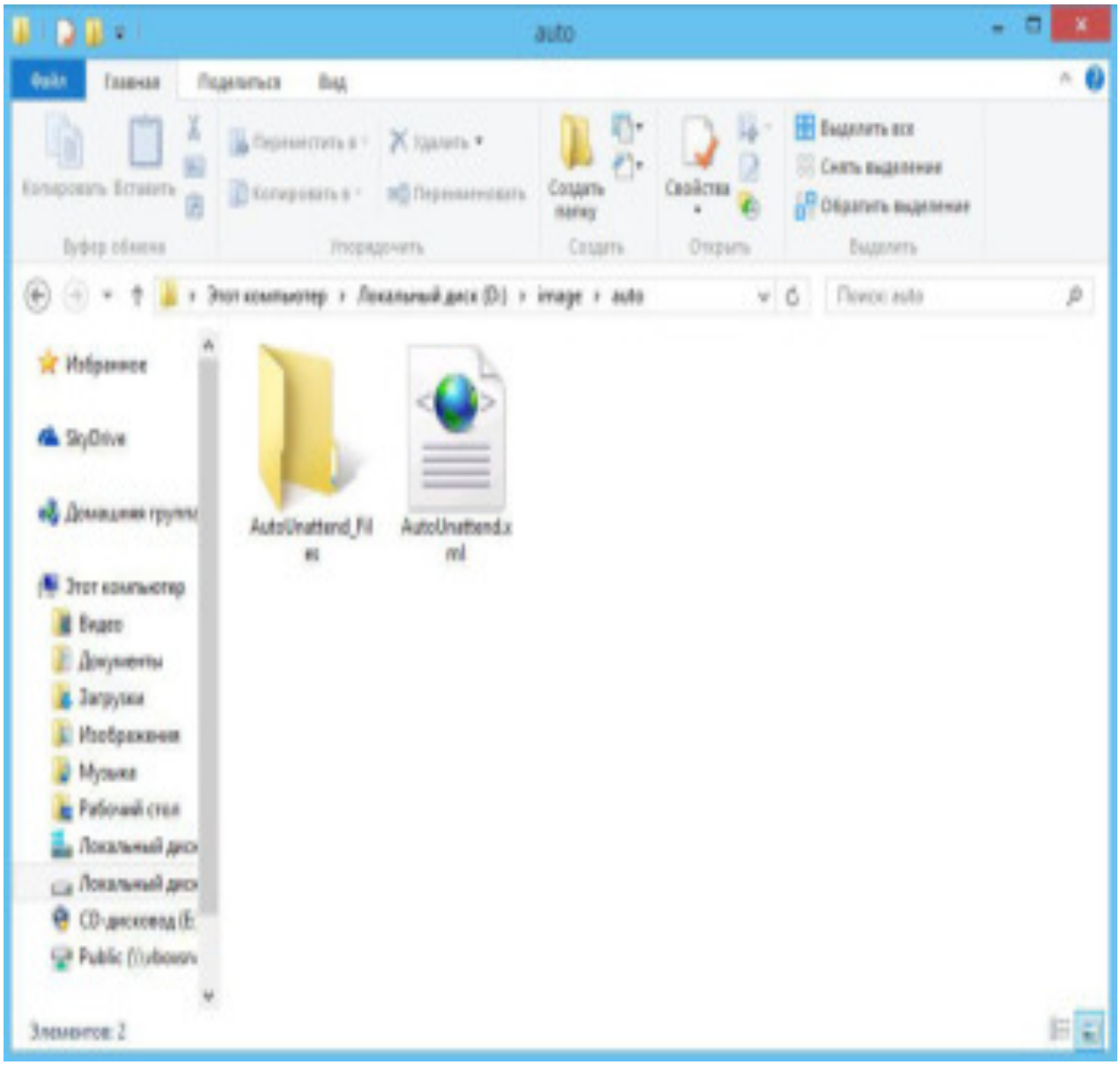

К примеру, в разделе UserData можно задать имя пользователя, название организации, к которой принадлежит компьютер, а также ключ продукта. Неиспользуемые разделы и подразделы следует удалить. Если вы их оставите, во время проверки Диспетчер выдаст вам сообщение об ошибке. Несколько иначе обстоит дело с пакетами. По сути, пакеты (packages) представляют особой отдельные программные компоненты Windows. Таковыми являются обновления, различные системные утилиты и т.п.




Последний шаг заключается в проверке файла ответов на ошибки.




Проверить работу можно через меню Сервис. В этом же меню есть опция «Создать набор конфигурации», она как раз и производит сохранение файла ответов в указанную папку. В результате вы получите каталог AutoUnattend_Files и XML-файл AutoUnattend, которые будет необходимо записать на чистую флешку.




Также как и диск с Windows накопитель с файлом автоматических ответов подключается к включенному компьютеру без операционной системы. Мастер будет считывать команды с файла AutoUnattend.xml и выполнять установку системы в автоматическом режиме, останавливаясь лишь на тех этапах, для которых в файле автоматических ответов не были заданы соответствующие параметры.

## Практическое занятие №8 Создание и обслуживание эталонного образа

***Цель работы:***

Научиться создавать эталонный образ Windows 10 с помощью набора средств развертывания Microsoft (MDT). Научиться создавать общий ресурс развертывания, настроить правила и параметры, импортировать все файлы

приложений и операционной системы, необходимые для создания эталонного изображения Windows10

**Область применения**

Для выполнения этой работы мы будем использовать 4 компьютера: DC01, MDT01, HV01 и PC0001. DC01 — контроллер домена, PC0001 — это Windows10 корпоративный клиент x64, а MDT01 — сервер Windows Server2012R2 Standard. HV01 — сервер узла Hyper-V, однако HV01 можно заменить на PC0001, если PC0001 располагает достаточной памятью и пригоден для Hyper-V. MDT01, HV01 и PC0001 — члены домена contoso.com вымышленной корпорации Contoso.


Рис.1. Используемые компьютеры.

**Эталонный образ**

Эталонный образ, предназначен для развертывания на физических компьютерах. Эталонный образ создается на виртуальной платформе, а затем автоматически запускается с помощью средства Sysprep и записывается в файл WIM. Причины для создания эталонного образа на виртуальной платформы следующие:

- Сокращение времени разработки и возможность использования моментальных снимков для быстрого тестирования разных конфигураций.
- Это позволяет исключить проблемы с оборудованием. Таким образом, создается лучший возможный образ, и если возникнет проблема, она вряд ли будет связана с оборудованием.
- Нежелательные приложения, которые могли бы быть установлены во время установки драйвера, не будут установлены, но и не будут удалены процессом Sysprep.
- Легко переключаться между промежуточной, тестовой и рабочей версиями.

**Настройка общей папки промежуточной версии развертывания MDT**

В Windows10 нет жесткой потребности в создании эталонных изображений; Тем не менее, чтобы уменьшить время, необходимое для развертывания, вам может потребоваться создать эталонный образ, содержащий несколько базовых приложений, а также все последние обновления. В этом разделе вы узнаете, как

создать и настроить общий доступ к развертыванию для лаборатории развертывания MDT, чтобы создать эталонный образ Windows10. Поскольку эталонные образы будут развернуты только на виртуальные машины во время создания с определенными параметрами (правилами), необходимо создать отдельную папку развертывания для этого процесса.

**Создайте общую папку промежуточной версии развертывания MDT.**

1. На компьютере MDT01 выполните вход с правами администратора в домен CONTOSO, используя пароль **P@ssw0rd**.
2. В Deployment Workbench щелкните правой кнопкой мыши **Deployment Shares** и выберите **New Deployment Share**.
3. Используйте следующие параметры для мастера создания общей папки развертывания:
4. Путь к общей папке развертывания: E:\MDTBuildLab
5. Имя общей папки: MDTBuildLab$
6. Описание общей папки развертывания: MDT Build Lab
7. <по умолчанию>
8. Проверьте доступ к общей папке \\MDT01\MDTBuildLab$.

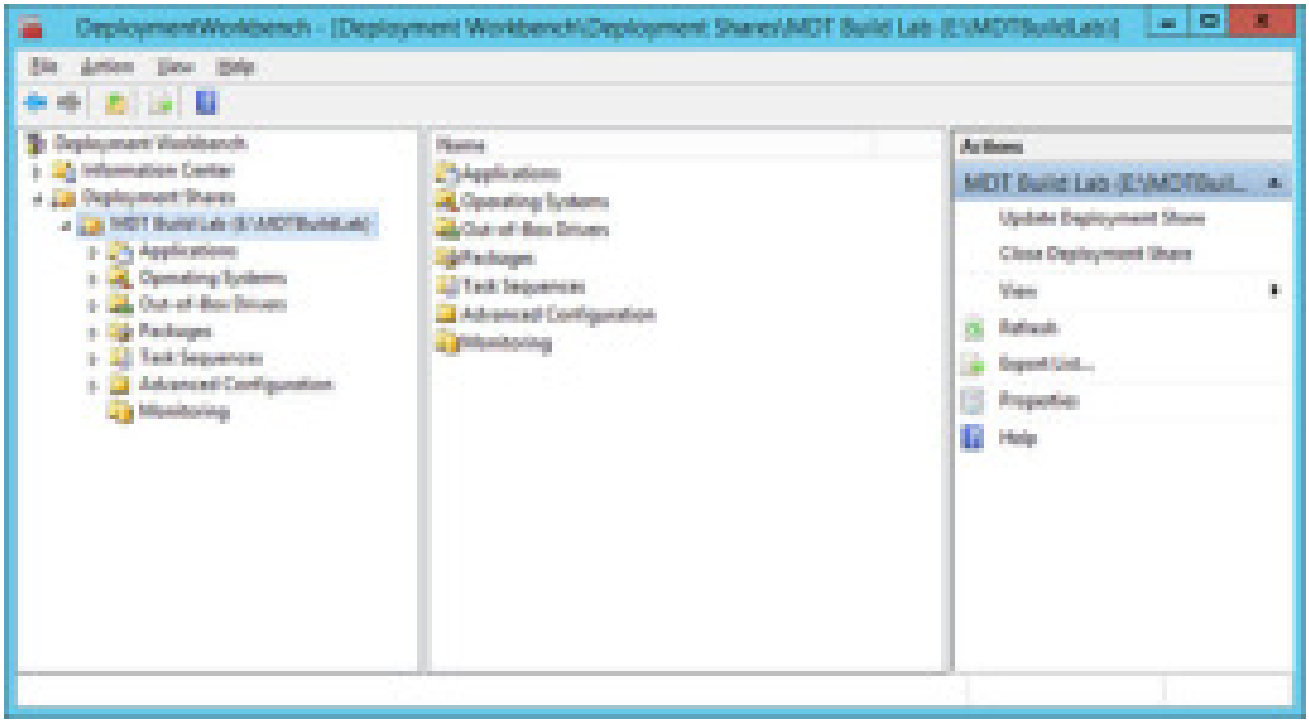


Рисунок 2. Deployment Workbench с созданной общей папкой промежуточной версии развертывания MDT.

**Настройка разрешений для общей папки развертывания**

Чтобы вновь записать эталонный образ в общую папку развертывания, необходимо задать разрешения на изменение учетной записи сборки MDT (MDT_BA) для вложенной папки **Captures** в папке **E:\MDTBuildLab**.

1. На MDT01 выполните вход в систему как **CONTOSO\Administrator**.
2. Измените разрешения NTFS для папки **E:\MDTBuildLab\Captures**, выполнив следующую команду в средстве Windows PowerShell с правами администратора:

```
icacls E:\MDTBuildLab\Captures /grant '"MDT_BA":(OI)(CI)(M)'
```

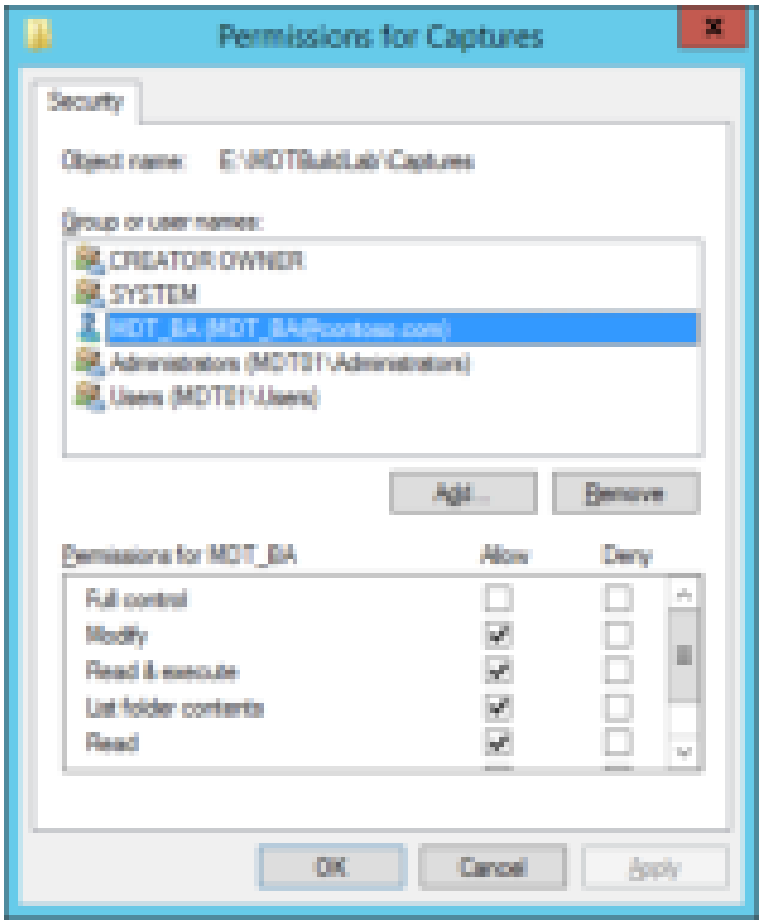



Рис.3. Разрешения, настроенные для пользователя MDT_BA.

**Добавление файлов установки**

В этом разделе показано, как заполнить общий доступ к развертыванию MDT с помощью исходных файлов операционной системы Windows10, которые обычно называют файлами настройки, которые будут использоваться для создания эталонного изображения. Файлы установки используются в процессе

создания эталонного образа и представляются собой основу для эталонного образа.

**Добавление установочных файлов Windows10**

MDT поддерживает добавление всех Windows10ных DVD-дисков (ИСОС) и пользовательских изображений, которые вы создали. В данном случае создается эталонный образ, поэтому можно добавить полные исходные файлы установки от Microsoft.

Используем имя папки W10EX64RTM вместо более описательного имени, например Windows10 Enterprise x64 RTM.

**Добавить Windows10 Enterprise x64 (полный источник)**

В этих инструкциях предполагается, что вы скопировали содержимое Windows10 Enterprise ISO x64 в папку **e:\довнлоадс\виндовс 10 Корпоративная 64** -разрядной версии.

1. На MDT01 выполните вход в систему как **CONTOSO\Administrator**.
2. В Deployment Workbench разверните узел **Deployment Shares** и затем **MDT Build Lab**.
3. Щелкните правой кнопкой мыши узел **Операционные системы** и создайте папку **Windows 10**.
4. Разверните узел **Operating Systems** , щелкните правой кнопкой мыши папку **Windows 10** и выберите **Import Operating System**. Используйте следующие параметры для Мастера импорта операционной системы:
5. Полный набор исходных файлов
6. Исходный каталог: E:\Downloads\Windows10 Enterprise x64
7. Имя целевого каталога: W10EX64RTM
8. После добавления операционной системы в папке **Операционные системы / Windows 10** дважды щелкните имя добавленной операционной системы в узле **Операционная система** и измените имя на следующее: **Windows 10 Корпоративная x64 RTM Default Image**

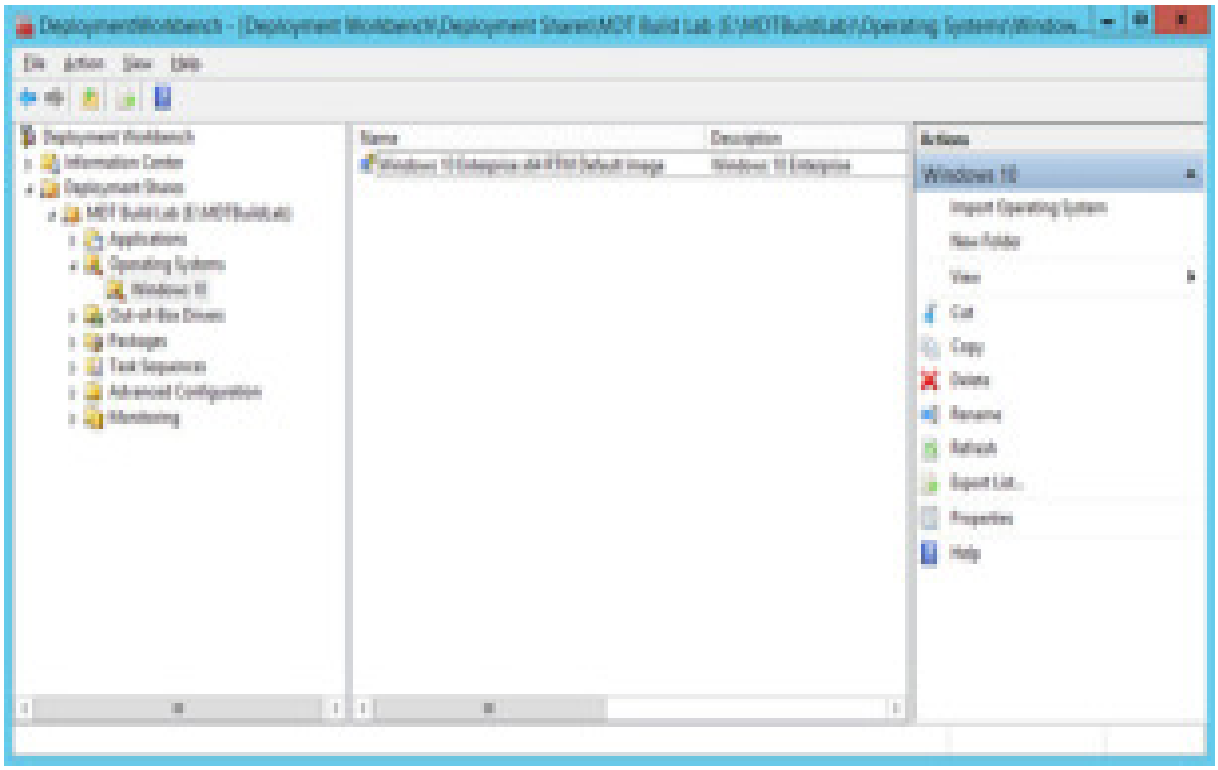


Рис.4. Импортированная Windows10 операционная система после переименования.

**Добавление приложений**

Прежде чем создавать последовательность задач MDT, необходимо добавить все приложения и другие образцы скриптов в общую папку MDT Build Lab.

В этом разделе используется строгий стандарт именования для приложений MDT. Необходимо использовать префикс «Install - » для обычной установки приложений, когда выполняется какой-либо установочный файл, либо префикс «Configure -», когда приложение настраивает параметры в операционной системе. Также необходимо добавить суффикс « - x86», « - x64» или «- x86-x64» для указания архитектуры приложения (у некоторых приложений есть программы установки для обеих архитектур). Рекомендуется стандарт именования скриптов при использовании MDT, поскольку это способствует упорядочиванию. Если сохранять элементы конфигурации в качестве приложений MDT, их будет легко перемещать между разными решениями или тестовой и рабочей средами. В пошаговых инструкциях этого раздела будут добавлены следующие приложения:

- Install - Microsoft Office 2013 Pro Plus - x86
- Install - Microsoft Silverlight 5.0 - x64
- Install - Microsoft Visual C++ 2005 SP1 - x86
- Install - Microsoft Visual C++ 2005 SP1 - x64
- Install - Microsoft Visual C++ 2008 SP1 - x86

- Install - Microsoft Visual C++ 2008 SP1 - x64
- Install - Microsoft Visual C++ 2010 SP1 - x86
- Install - Microsoft Visual C++ 2010 SP1 - x64
- Install - Microsoft Visual C++ 2012 Update 4 - x86
- Install - Microsoft Visual C++ 2012 Update 4 - x64

Предполагается, что перечисленное программное обеспечение загружено в папку E:\Downloads. Первое приложение добавляется с помощью графического интерфейса. Поскольку MDT поддерживает Windows PowerShell, остальные приложения добавляются с помощью Windows PowerShell.

**Создание программы установки: Microsoft Office профессиональный плюс 2013 x86**

Office 2013 можно настроить. В лицензионных версиях Office 2013 есть средство настройки Office для более тонкой настройки установки. Для этих шагов предполагается, что файлы установки Office 2013 скопированы в папку E:\Downloads\Office2013.

**Добавление файлов установки Microsoft Office профессиональный плюс 2013 x86**

После добавления приложения Microsoft Office профессиональный плюс 2013 x86 необходимо автоматизировать его установку путем запуска средства настройки Office. На самом деле MDT обнаруживает, что приложение Office Professional Plus 2013 x86 добавлено, и создает ссылку для действия. Вы также можете настроить установку Office с помощью файла Config.xml. Однако рекомендуется использовать средство настройки Office, как описано в следующих шагах, поскольку оно позволяет контролировать все параметры Office 2013.

1. В Deployment Workbench в общей папке развертывания MDT Build Lab разверните узел **Applications / Microsoft** и дважды щелкните **Install - Microsoft Office 2013 Pro Plus x86**.
2. На вкладке **Продукты Office** щелкните **Средство настройки Office** и затем **ОК** в диалоговом окне **Сведения**.

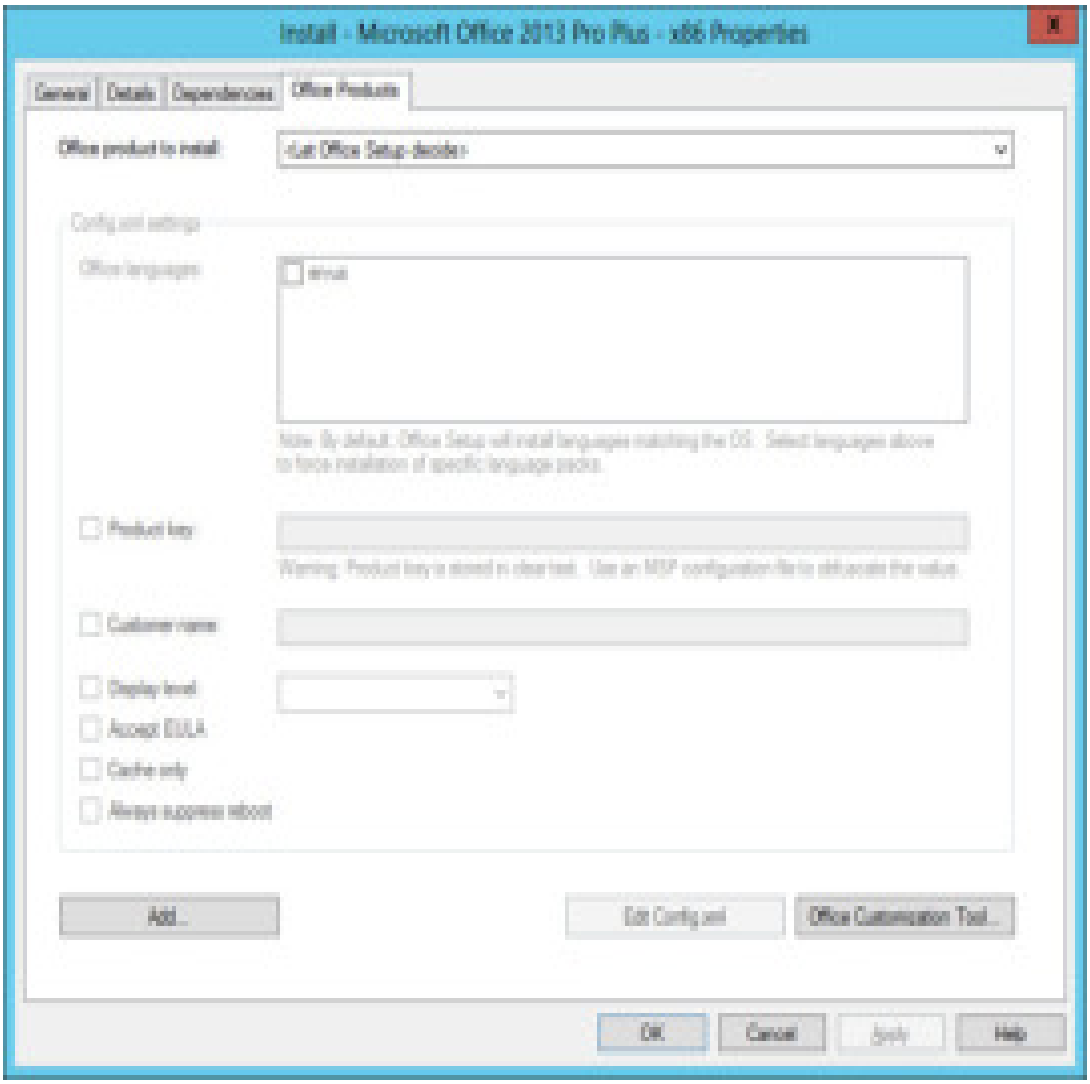



Рис.5. Параметры приложения для команды «Install - Microsoft Office 2013 Pro Plus - x86».

Примечание

Если не видно вкладку «Продукты Office», убедитесь, что используется лицензионная версия Office. Если развертывается Office 365, необходимо загрузить папку Admin с сайта Microsoft.

3. В диалоговом окне средства настройки Office выберите «Создать файл настройки программы установки для следующего варианта продукта», выберите продукт «Microsoft Office профессиональный плюс 2013 (32-разрядная версия)» и нажмите «ОК».
4. Чтобы сделать установку Office 2013 полностью автоматической, используйте следующие параметры:

    a. Расположение файлов установки и название организации
        - Название организации: Contoso
    b. Лицензирование и пользовательский интерфейс

1. Выберите «Использовать клиентский ключ KMS».
2. Выберите «Я принимаю условия» в лицензионном соглашении.
3. Выберите уровень отображения «Никакой».

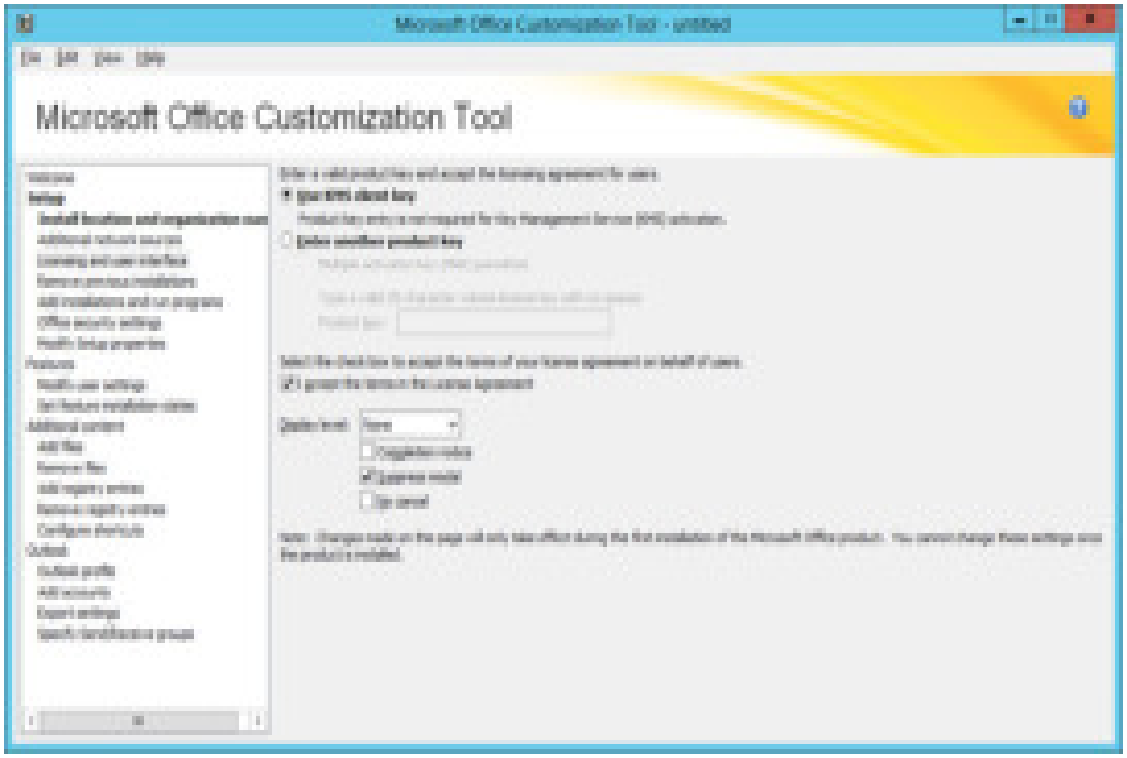



Рис.6. Страница лицензирования и пользовательского интерфейса в средстве настройки Microsoft Office

2. Изменение параметров установки
   - Добавьте свойство **SETUP_REBOOT** и задайте значение **Never**.
3. Изменение пользовательских параметров
   - В узле **Microsoft Office 2013** разверните **Конфиденциальность**, выберите **Центр сертификации** и включите параметр «Отключить мастер выбора параметров при первом запуске».

5. В меню **Файл** выберите **Сохранить** и сохраните конфигурацию в качестве 0_Office2013ProPlusx86.msp в папке **E:\MDTBuildLab\Applications\Install - Microsoft Office 2013 Pro Plus - x86\Updates**.

   Примечание

   Причина присвоения имени файлу 0 (нуль) — это то, что папка Updates также обрабатывает обновления Microsoft Office, и они устанавливаются в алфавитном порядке. Программа настройки Office 2013 работает правильно, если файл настройки устанавливаются до обновлений.

6. Закройте средство настройки Office, щелкните «Да» в диалоговом окне и затем в окне **Install - Microsoft Office 2013 Pro Plus - x86 Properties** также щелкните **ОК**.

**Подключение к общей папке развертывания с помощью Windows PowerShell**

Если требуется добавить много приложений, можно воспользоваться поддержкой PowerShell, которую обеспечивает MDT. Чтобы использовать PowerShell во время работы с общей папкой развертывания, сначала необходимо загрузить оснастку MDT PowerShell и сделать папку развертывания диском PowerShell (PSDrive).

1. На MDT01 выполните вход в систему как **CONTOSO\Administrator**.
2. Импортируйте оснастку и создайте диск PSDrive, выполнив следующие команды в командной строке PowerShell с правами администратора:

   syntax

```
2. Import-Module "C:\Program Files\Microsoft Deployment
   Toolkit\bin\MicrosoftDeploymentToolkit.psd1"
3. New-PSDrive -Name "DS001" -PSProvider MDTProvider -
   Root "E:\MDTBuildLab"
4.
```

**Создание программы установки: Microsoft Visual C++ 2005 x86 с пакетом обновления SP1**

Для этих шагов предполагается, что приложение Microsoft Visual C++ 2005 x86 с пакетом обновления SP1 уже загружено. Возможно, потребуется изменить путь к исходной папке для текущей среды. В данном примере исходный путь: E:\Downloads\VC++2005SP1x86.

1. На MDT01 выполните вход в систему как **CONTOSO\Administrator**.
2. Создайте приложение, выполнив следующие команды в командной строке PowerShell с правами администратора:

   syntax

```
2. $ApplicationName = "Install - Microsoft Visual C++
   2005 SP1 - x86"
3. $CommandLine = "vcredist_x86.exe /Q"
4. $ApplicationSourcePath =
   "E:\Downloads\VC++2005SP1x86"
```

```
5. Import-MDTApplication -Path
   "DS001:\Applications\Microsoft" -Enable "True" -Name
   $ApplicationName -ShortName $ApplicationName -
   Commandline $Commandline -WorkingDirectory
   ".\Applications\$ApplicationName" -
   ApplicationSourcePath $ApplicationSourcePath -
   DestinationFolder $ApplicationName
6. -Verbose
7.
```

**Создание программы установки: Microsoft Visual C++ 2005 x64 с пакетом обновления SP1**

Для этих шагов предполагается, что приложение Microsoft Visual C++ 2005 x64 с пакетом обновления SP1 уже загружено. Возможно, потребуется изменить путь к исходной папке для текущей среды. В данном примере исходный путь: E:\Downloads\VC++2005SP1x64.

1. На MDT01 выполните вход в систему как **CONTOSO\Administrator**.
2. Создайте приложение, выполнив следующие команды в командной строке PowerShell с правами администратора:

   syntax

```
2. $ApplicationName = "Install - Microsoft Visual C++
   2005 SP1 - x64"
3. $CommandLine = "vcredist_x64.exe /Q"
4. $ApplicationSourcePath =
   "E:\Downloads\VC++2005SP1x64"
5. Import-MDTApplication -Path
   "DS001:\Applications\Microsoft" -Enable "True" -Name
   $ApplicationName -ShortName $ApplicationName -
   Commandline $Commandline -WorkingDirectory
   ".\Applications\$ApplicationName" -
   ApplicationSourcePath $ApplicationSourcePath -
   DestinationFolder $ApplicationName
6. -Verbose
7.
```

**Создание программы установки: Microsoft Visual C++ 2008 x86 с пакетом обновления SP1**

Для этих шагов предполагается, что приложение Microsoft Visual C++ 2008 x86 с пакетом обновления SP1 уже загружено. Возможно, потребуется изменить

путь к исходной папке для текущей среды. В данном примере исходный путь: E:\Downloads\VC++2008SP1x86.

1. На MDT01 выполните вход в систему как **CONTOSO\Administrator**.
2. Создайте приложение, выполнив следующие команды в командной строке PowerShell с правами администратора:

   syntax

```
2.$ApplicationName = "Install - Microsoft Visual C++
  2008 SP1 - x86"
3.$CommandLine = "vcredist_x86.exe /Q"
4.$ApplicationSourcePath =
  "E:\Downloads\VC++2008SP1x86"
5.Import-MDTApplication -Path
  "DS001:\Applications\Microsoft" -Enable "True" -Name
  $ApplicationName -ShortName $ApplicationName -
  Commandline $Commandline -WorkingDirectory
  ".\Applications\$ApplicationName" -
  ApplicationSourcePath $ApplicationSourcePath -
  DestinationFolder $ApplicationName
6.-Verbose
7.
```

**Создание программы установки: Microsoft Visual C++ 2008 x64 с пакетом обновления SP1**

Для этих шагов предполагается, что приложение Microsoft Visual C++ 2008 x64 с пакетом обновления SP1 уже загружено. Возможно, потребуется изменить путь к исходной папке для текущей среды. В данном примере исходный путь: E:\Downloads\VC++2008SP1x64.

1. На MDT01 выполните вход в систему как **CONTOSO\Administrator**.
2. Создайте приложение, выполнив следующие команды в командной строке PowerShell с правами администратора:

   syntax

```
2.$ApplicationName = "Install - Microsoft Visual C++
  2008 SP1 - x64"
3.$CommandLine = "vcredist_x64.exe /Q"
4.$ApplicationSourcePath =
  "E:\Downloads\VC++2008SP1x64"
5.Import-MDTApplication -Path
  "DS001:\Applications\Microsoft" -Enable "True" -Name
```

```
$ApplicationName -ShortName $ApplicationName -
Commandline $Commandline -WorkingDirectory
".\Applications\$ApplicationName" -
ApplicationSourcePath $ApplicationSourcePath -
DestinationFolder $ApplicationName
6. -Verbose
7.
```

**Создание программы установки: Microsoft Visual C++ 2010 x86 с пакетом обновления SP1**

Для этих шагов предполагается, что приложение Microsoft Visual C++ 2010 x86 с пакетом обновления SP1 уже загружено. Возможно, потребуется изменить путь к исходной папке для текущей среды. В данном примере исходный путь: E:\Downloads\VC++2010SP1x86.

1. На MDT01 выполните вход в систему как **CONTOSO\Administrator**.
2. Создайте приложение, выполнив следующие команды в командной строке PowerShell с правами администратора:

   syntax

```
2. $ApplicationName = "Install - Microsoft Visual C++
   2010 SP1 - x86"
3. $CommandLine = "vcredist_x86.exe /Q"
4. $ApplicationSourcePath =
   "E:\Downloads\VC++2010SP1x86"
5. Import-MDTApplication -Path
   "DS001:\Applications\Microsoft" -Enable "True" -Name
   $ApplicationName -ShortName $ApplicationName -
   CommandLine $CommandLine -WorkingDirectory
   ".\Applications\$ApplicationName" -
   ApplicationSourcePath $ApplicationSourcePath -
   DestinationFolder $ApplicationName
6. -Verbose
7.
```

**Создание программы установки: Microsoft Visual C++ 2010 x64 с пакетом обновления SP1**

Для этих шагов предполагается, что приложение Microsoft Visual C++ 2010 x64 с пакетом обновления SP1 уже загружено. Возможно, потребуется изменить путь к исходной папке для текущей среды. В данном примере исходный путь: E:\Downloads\VC++2010SP1x64.

1. На MDT01 выполните вход в систему как **CONTOSO\Administrator**.
2. Создайте приложение, выполнив следующие команды в командной строке PowerShell с правами администратора:

   syntax

```
2.$ApplicationName = "Install - Microsoft Visual C++
  2010 SP1 - x64"
3.$CommandLine = "vcredist_x64.exe /Q"
4.$ApplicationSourcePath =
  "E:\Downloads\VC++2010SP1x64"
5.Import-MDTApplication -Path
  "DS001:\Applications\Microsoft" -Enable "True" -Name
  $ApplicationName -ShortName $ApplicationName -
  CommandLine $CommandLine -WorkingDirectory
  ".\Applications\$ApplicationName" -
  ApplicationSourcePath $ApplicationSourcePath -
  DestinationFolder $ApplicationName
6.-Verbose
7.
```

**Создание программы установки: Microsoft Visual C++ 2012 x86 с пакетом обновления Update 4**

Для этих шагов предполагается, что приложение Microsoft Visual C++ 2012 x86 с пакетом обновления Update 4 уже загружено. Возможно, потребуется изменить путь к исходной папке для текущей среды. В данном примере исходный путь: E:\Downloads\VC++2012Ux86.

1. На MDT01 выполните вход в систему как **CONTOSO\Administrator**.
2. Создайте приложение, выполнив следующие команды в командной строке PowerShell с правами администратора:

   syntax

```
2.$ApplicationName = "Install - Microsoft Visual C++
  2012 Update 4 - x86"
3.$CommandLine = "vcredist_x86.exe /Q"
4.$ApplicationSourcePath = "E:\Downloads\VC++2012Ux86"
5.Import-MDTApplication -Path
  "DS001:\Applications\Microsoft" -Enable "True" -Name
  $ApplicationName -ShortName $ApplicationName -
  CommandLine $CommandLine -WorkingDirectory
  ".\Applications\$ApplicationName" -
```

```
ApplicationSourcePath $ApplicationSourcePath -
DestinationFolder $ApplicationName
6.-Verbose
7.
```

**Создание программы установки: Microsoft Visual C++ 2012 x64 с пакетом обновления Update 4**

Для этих шагов предполагается, что приложение Microsoft Visual C++ 2012 x64 с пакетом обновления Update 4 уже загружено. Возможно, потребуется изменить путь к исходной папке для текущей среды. В данном примере исходный путь: E:\Downloads\VC++2012Ux64.

1. На MDT01 выполните вход в систему как **CONTOSO\Administrator**.
2. Создайте приложение, выполнив следующие команды в командной строке PowerShell с правами администратора:

   syntax

```
2.$ApplicationName = "Install - Microsoft Visual C++
  2012 Update 4 - x64"
3.$CommandLine = "vcredist_x64.exe /Q"
4.$ApplicationSourcePath = "E:\Downloads\VC++2012Ux64"
5.Import-MDTApplication -Path
  "DS001:\Applications\Microsoft" -Enable "True" -Name
  $ApplicationName -ShortName $ApplicationName -
  CommandLine $CommandLine -WorkingDirectory
  ".\Applications\$ApplicationName" -
  ApplicationSourcePath $ApplicationSourcePath -
  DestinationFolder $ApplicationName
6.-Verbose
7.
```

**Последовательность задач для создания эталонного образа**

Чтобы создать и захватить эталонный образ Windows10 для развертывания с помощью MDT, вы создадите последовательность задач. Последовательность задач будет ссылаться на операционную систему и приложения, которые ранее были импортированы в общий ресурс развертывания для сборки MDT для создания эталонного образа Windows10. После создания последовательности задач необходимо настроить ее и разрешить обновления через сервер Windows Server Update Services (WSUS). Последовательность задач Windows поддерживает обновления из Центра обновления Майкрософт, однако более стабильные обновления можно получать с помощью локального сервера WSUS. Сервер WSUS также упрощает подтверждение развертываемых обновлений.

**Драйверы и эталонный образ**

Так как мы используем современные виртуальные платформы для создания эталонных изображений, вам не нужно беспокоиться о драйверах при создании эталонных изображений для Windows10. В среде используется Hyper-V, а среда предустановки Windows (Windows PE) уже имеет все необходимые драйверы для Hyper-V.

**Создание последовательности задач для Windows 10 Корпоративная**

Для создания последовательности задач для образа ссылки Windows10 процесс выглядит следующим образом:

1. В Deployment Workbench в общей папке развертывания MDT Build Lab щелкните правой кнопкой мыши **Task Sequences** и создайте новую папку **Windows 10**.
2. Разверните узел **Task Sequences**, щелкните правой кнопкой мыши новую папку **Windows 10** и выберите **New Task Sequence**. Используйте следующие параметры в мастере создания последовательности задач:
    1. Идентификатор последовательности задач: REFW10X64-001
    2. Имя последовательности задач: Windows 10 Корпоративная x64 RTM Default Image
    3. Комментарии последовательности задач: эталонная сборка
    4. Шаблон: стандартная последовательность задач клиента
    5. Выбор операционной системы: Windows 10 Корпоративная x64 RTM Default Image
    6. Укажите ключ продукта: не указывайте ключ продукта на этом этапе
    7. Полное имя: Contoso
    8. Организация: Contoso
    9. Домашняя страница Internet Explorer:http://www.contoso.com
    10. Пароль администратора: не указывайте пароль администратора на этом этапе

**Изменение последовательности задач Windows10**

Приведенные ниже инструкции описывают процесс изменения последовательности задач для образа ссылки Windows10, чтобы включить действия, необходимые для обновления эталонного изображения с помощью последних обновлений из служб WSUS, установка ролей и компонентов, а также установка Microsoft Office 2013.

1. В папке последовательности задач или Windows10 щелкните правой кнопкой мыши последовательность задач для изображений по умолчанию для Windows10 Enterprise RTM и выберите пункт Свойства.

2. На вкладке " **последовательность задач** " Настройте последовательность задач для изображений по умолчанию для Windows10 в корпоративной версии x64 со следующими параметрами:
    1. Восстановление состояния. Включите действие «Обновление Windows (установка до приложений)». **Примечание** . чтобы включить действие, перейдите на вкладку Параметры и снимите флажок отключить этот шаг.
    2. Восстановление состояния. Включите действие «Обновление Windows (установка после приложений)».
    3. Восстановление состояния. Включите действие «Обновление Windows (установка после приложений)». Восстановление состояния. После действия **Татуировка** добавьте новое действие **Группа** со следующим параметром:
        - Имя: настраиваемые задачи (обновление перед установкой Windows)
    4. Восстановление состояния. После выполнения действия «Обновление Windows (установка после приложений)» переименуйте настраиваемые задачи в «Настраиваемые задачи (обновление после установки Windows)». **Обратите внимание** на то, что при добавлении приложений после восстановленного действия, но до запуска центра обновления Windows — просто сэкономить время в ходе развертывания. Таким образом, добавляются все приложения, которые обновят некоторые встроенные компоненты, при этом удастся избежать ненужного обновления.
    5. Восстановление состояния / настраиваемые задачи (обновление до установки Windows). Добавьте новое действие «Установить роли и компоненты» со следующими параметрами:

1. Имя: Install - Microsoft NET Framework 3.5.1
    2. Выбор операционной системы, для которого необходимо установить роли: Windows 10
    3. Выбор ролей и компонентов, которые необходимо установить: .NET Framework 3.5 (включает .NET 2.0 и 3.0)

Важно!

Возможно, это самый важный этап в создании эталонного образа. Платформа .NET Framework требуется многим приложениям, поэтому настоятельно рекомендуется добавить ее в образ. Отличие от других компонентов заключается в том, что .NET Framework 3.5.1 не включена в файл WIM. Платформа устанавливается из папки **Sources\SxS** на носителе, поэтому ее сложнее добавить после развертывания образа.

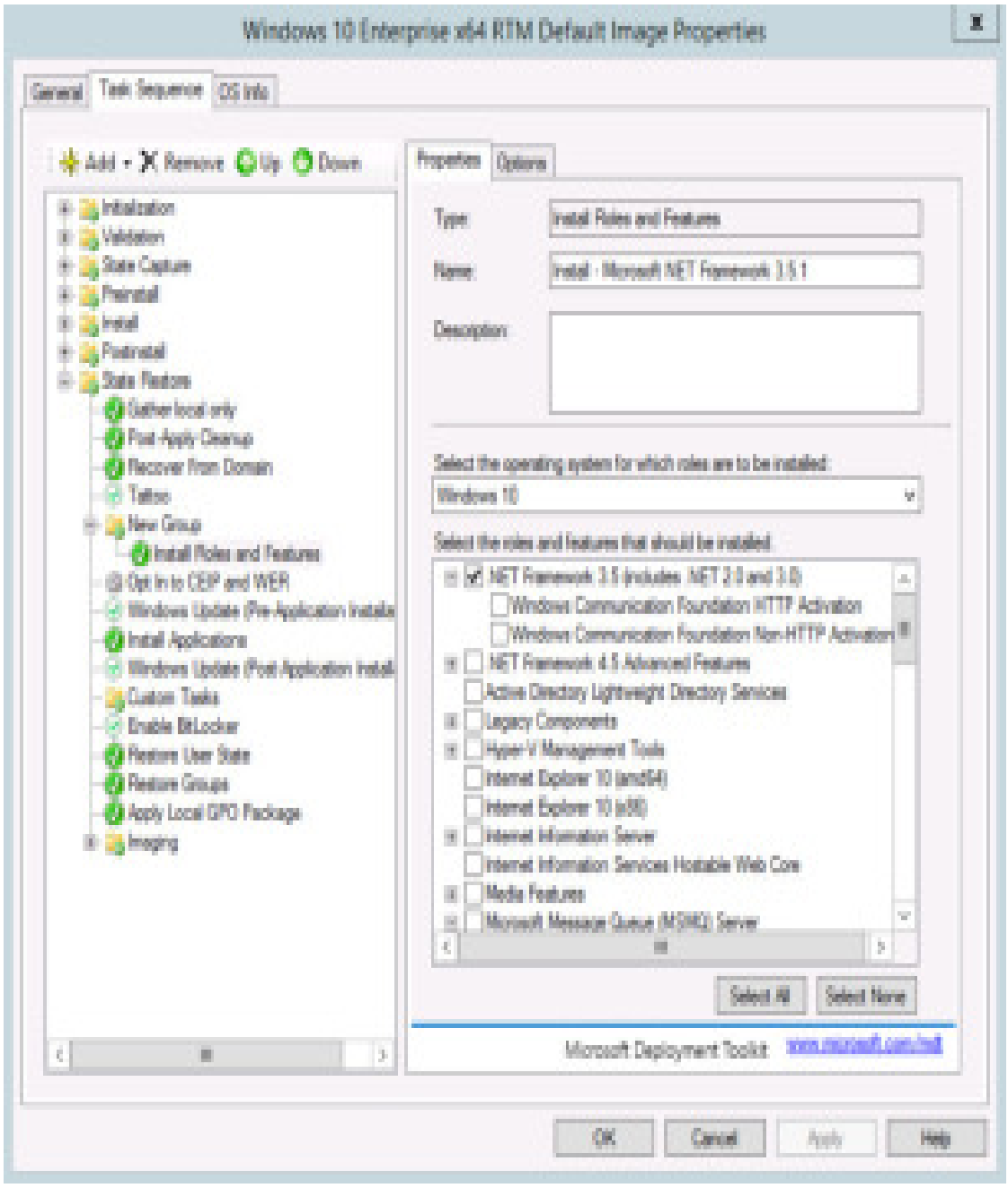



Рисунок 7. Последовательность задач после создания группы «Настраиваемые задачи (обновление до установки Windows)» и добавления действия «Install - Microsoft NET Framework 3.5.1».

6. Восстановление состояния — настраиваемые задачи (обновление до установки Windows). После действия **Install - Microsoft NET Framework 3.5.1** добавьте новое действие **Install Application** со следующими параметрами:

0. Имя: Install - Microsoft Visual C++ 2005 SP1 - x86
    1. Установка одного приложения: Install - Microsoft Visual C++ 2005 SP1 - x86-x64
7. Повторите предыдущий шаг (добавление действия **Install Application**), чтобы добавить следующие приложения:

0. Install - Microsoft Visual C++ 2005 SP1 - x64
1. Install - Microsoft Visual C++ 2008 SP1 - x86
2. Install - Microsoft Visual C++ 2008 SP1 - x64
3. Install - Microsoft Visual C++ 2010 SP1 - x86
4. Install - Microsoft Visual C++ 2010 SP1 - x64
5. Install - Microsoft Visual C++ 2012 Update 4 - x86
6. Install - Microsoft Visual C++ 2012 Update 4 - x64
7. Install - Microsoft Office 2013 Pro Plus - x86

8. После действия «Install - Microsoft Office 2013 Pro Plus - x86» добавьте действие «Перезапустить компьютер».

3. Нажмите кнопку **ОК**.

**Необязательная конфигурация: добавление приостановки**

Цель при создании эталонного образа заключается в том, чтобы автоматизировать все операции. Однако иногда бывают особые параметры, или требуется установка приложения, которые занимают слишком много времени при автоматизации. Если требуется ручная настройка, можно добавить малоизвестный компонент Lite Touch Installation (LTI) Suspend. При добавлении скрипта LTISuspend.wsf в качестве настраиваемого действия в последовательности задач скрипт приостановит последовательность задач, пока вы не нажмете значок «Возобновить последовательность задач» на рабочем столе. Помимо использования компонента LTI Suspend для ручной настройки или установки можно также использовать скрипт для проверки эталонного образа, прежде чем разрешить продолжить последовательность задач, а с помощью Sysprep сделать снимок виртуальной машины.

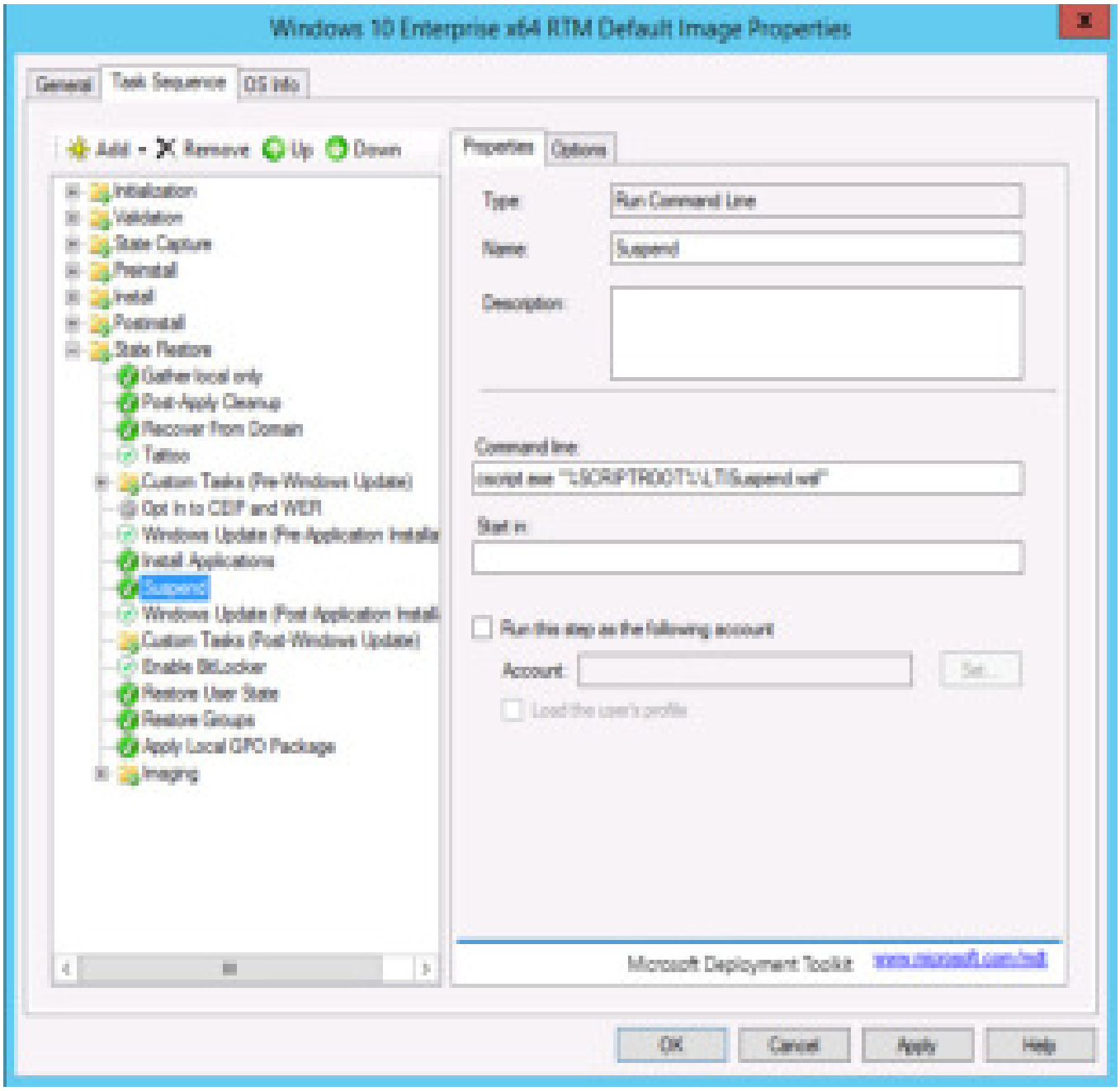



Рисунок 8. Последовательность задач с необязательным действием приостановки LTISuspend.wsf.

Рисунок 9. Рабочий стол Windows 10 с ярлыком для возобновления последовательности задач.

**Изменение файла Unattend. XML для Windows10 Enterprise**

При использовании MDT не нужно изменять файл Unattend.xml очень часто, потому что большинство параметров находятся под контролем MDT. Тем не менее, если, например, вы хотите настроить поведение Интернет-Explorer11, вы можете изменить файл Unattend. XML. Изменять базовые параметры Internet Explorer с помощью Unattend.xml легко, однако для более расширенных параметров потребуется средство Internet Explorer Administration Kit (IEAK).

Предупреждение

Не используйте **SkipMachineOOBE** или **SkipUserOOBE** в файле Unattend.xml. Эти параметры считаются устаревшими и могут оказывать непредусмотренное влияние при использовании.

Примечание

Кроме того, с помощью файла Unattend. XML можно включить компоненты в Windows10, например клиент Telnet или клиент Hyper-V. Лучше всего это сделать через действие **Установка ролей и компонентов** или с помощью средства командной строки DISM, поскольку в этом случае можно выполнить добавление в качестве приложения, динамическим образом, с особыми параметрами и т.д. Также при добавлении пакетов через Unattend.xml нужно учитывать версии, поэтому Unattend.xml должен содержать версию обслуживаемой операционной системы.

Следуйте этим инструкциям, чтобы настроить параметры Internet Explorer в файле Unattend. XML для стандартной последовательности задач для изображений по умолчанию для Windows10 в корпоративной версии x64.

1. В Deployment Workbench щелкните правой кнопкой мыши последовательность задач **Windows 10 Корпоративная x64 RTM Default Image** и выберите **Свойства**.
2. На вкладке **OS Info** щелкните **Edit Unattend.xml**. MDT создает файл каталога. Это занимает несколько минут, после этого запускается диспетчер установки Windows (Windows SIM).
3. В Windows SIM разверните узел **4 specialize** в области **Файл ответов** и выберите запись amd64_Microsoft-Windows-IE-InternetExplorer_neutral.
4. В окне **amd64_Microsoft-Windows-IE-InternetExplorer_neutral properties** (окно справа) установите следующие значения:
   - DisableDevTools: true
5. Сохраните файл Unattend.xml и закройте Windows SIM.
6. На странице Параметры изображения по умолчанию для Windows10 Enterprise x64 RTM нажмите кнопку **ОК**.

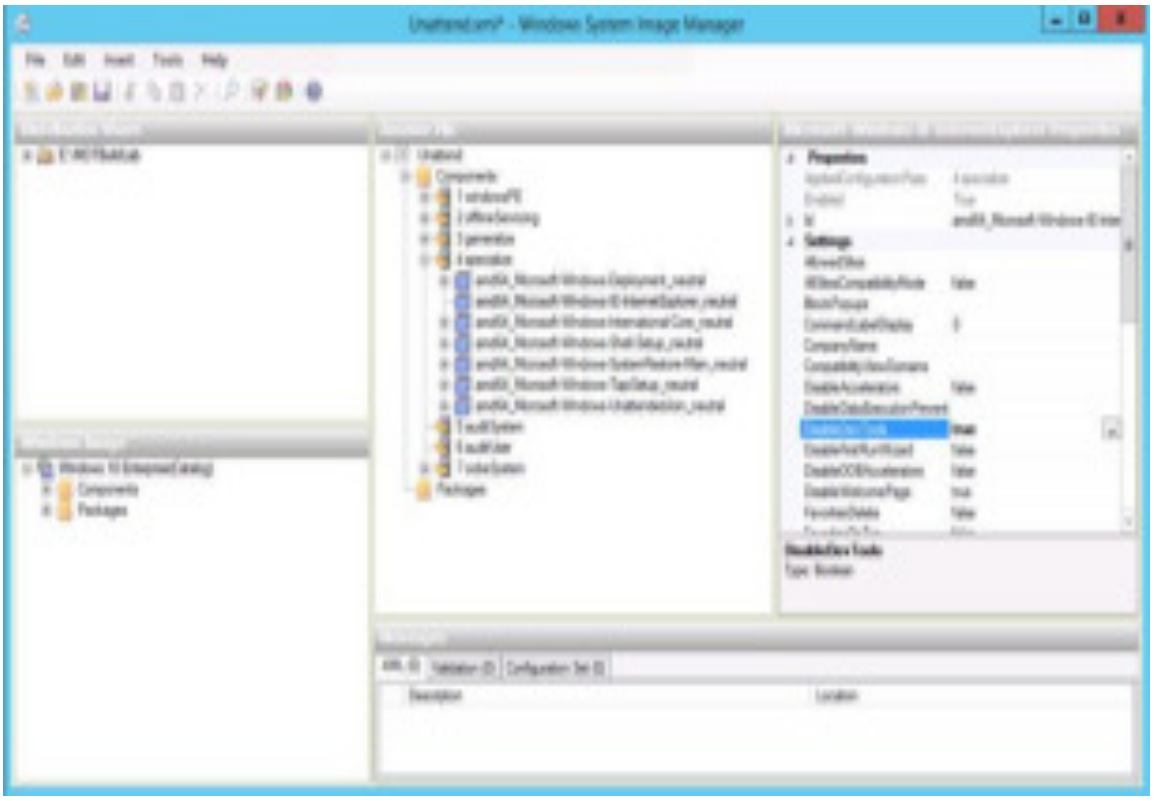


Рисунок 10. Диспетчер установки Windows с файлом Unattend.xml для Windows 10.

**Настройка правил общей папки развертывания MDT**

Понимание правил очень важно для успешного использования MDT. Правила настраиваются с помощью вкладки «Правила» свойств общей папки развертывания. Вкладка «Правила», в сущности, представляет собой ссылку на файл CustomSettings.ini, который находится в папке E:\MDTBuildLab\Control. В этом разделе рассматривается настройка правил общей папки развертывания MDT как части развертывания Windows 10 Корпоративная.

**Обзор правил общей папки развертывания MDT**

В MDT всегда 2 файла правил: CustomSettings.ini и Bootstrap.ini. Можно добавлять практически любые правила в оба файла. Файл Bootstrap.ini копируется из папки Control в образ загрузки, поэтому его необходимо обновлять каждый раз после изменения файла. По этой причине добавляйте только минимальный набор правил в Bootstrap.ini, например, к какому серверу развертывания и общей папке необходимо подключаться: значение DEPLOYROOT. Поместите другие правила в файл CustomSettings.ini, потому что этот файл обновляется сразу после нажатия кнопки «ОК». Выполните следующие шаги, чтобы настроить правила для общей папки развертывания MDT Build Lab:

1. В Deployment Workbench щелкните правой кнопкой мыши **общую папку развертывания MDT Build Lab** и выберите **Свойства**.
2. Перейдите на вкладку **Правила** и внесите следующие изменения:

   syntax

- [Settings]

```
Priority=Default
[Default]
_SMSTSORGNAME=Contoso
UserDataLocation=NONE
DoCapture=YES
OSInstall=Y
AdminPassword=P@ssw0rd
TimeZoneName=Pacific Standard Time
JoinWorkgroup=WORKGROUP
HideShell=YES
FinishAction=SHUTDOWN
DoNotCreateExtraPartition=YES
WSUSServer=http://mdt01.contoso.com:8530
ApplyGPOPack=NO
SLSHARE=\\MDT01\Logs$
SkipAdminPassword=YES
SkipProductKey=YES
SkipComputerName=YES
SkipDomainMembership=YES
SkipUserData=YES
SkipLocaleSelection=YES
SkipTaskSequence=NO
SkipTimeZone=YES
SkipApplications=YES
SkipBitLocker=YES
SkipSummary=YES
SkipRoles=YES
SkipCapture=NO
SkipFinalSummary=YES
```

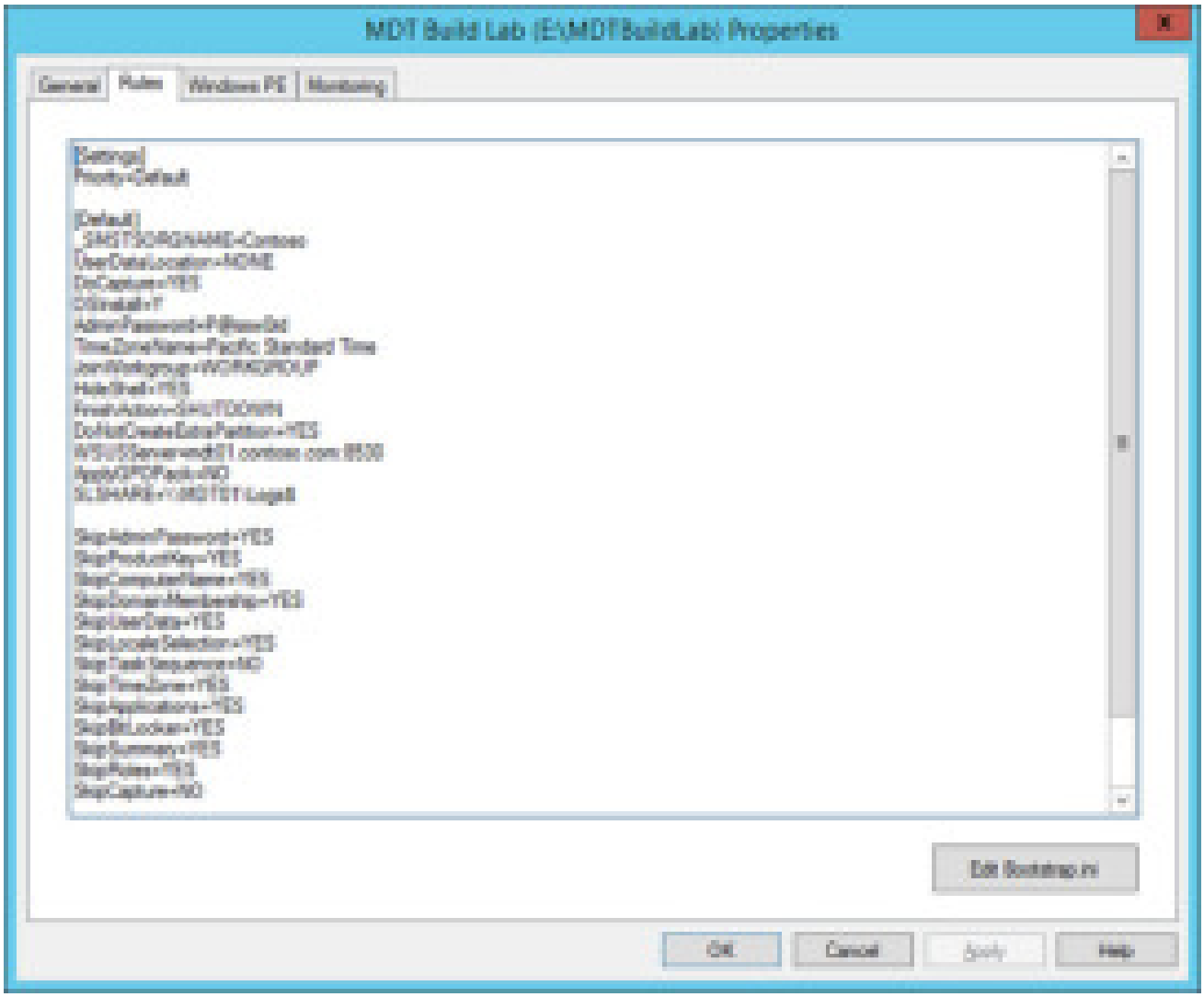



Рисунок 11. Серверные правила для общей папки развертывания MDT Build Lab.

- Щелкните **Изменить Bootstrap.ini** и внесите следующие изменения:

syntax

```
3.[Settings]
4.Priority=Default
5.[Default]
6.DeployRoot=\\MDT01\MDTBuildLab$
7.UserDomain=CONTOSO
8.UserID=MDT_BA
9.UserPassword=P@ssw0rd
10.SkipBDDWelcome=YES
```

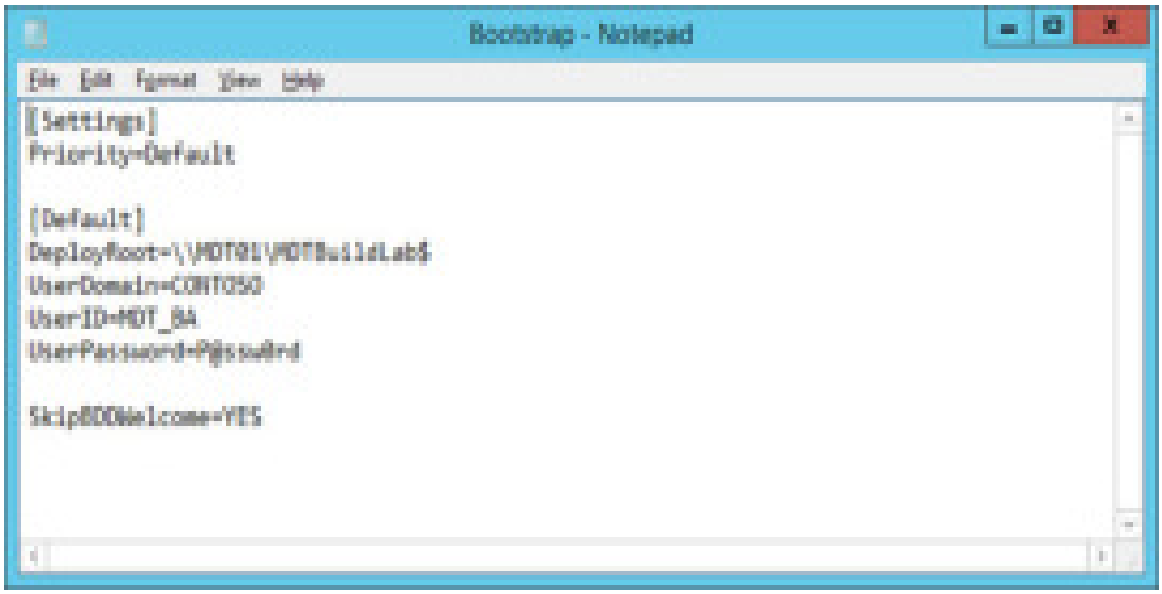



Рисунок 12. Правила образа загрузки для общей папки развертывания MDT Build Lab.

Примечание

Обычно по соображениям безопасности пароль не добавляют в файл Bootstrap.ini. Однако поскольку эта общая папка развертывания предназначена для создания только сборок эталонного образа и не будет публиковаться в рабочей сети, можно добавить пароль.

11. На вкладке **Windows PE** в раскрывающемся списке **Платформа** выберите **x86**.
12. В области **Lite Touch Boot Image Settings** настройте следующие параметры:
    1. Описание образа: MDT Build Lab x86
    2. Имя файла ISO: MDT Build Lab x86.iso
13. На вкладке **Windows PE** в раскрывающемся списке **Платформа** выберите **x64**.
14. В области **Lite Touch Boot Image Settings** настройте следующие параметры:
    1. Описание образа: MDT Build Lab x64
    2. Имя файла ISO: MDT Build Lab x64.iso
15. Нажмите кнопку **ОК**.

Примечание

В MDT образ загрузки x86 может развертывать как операционную систему x86, так и x64 (за исключением компьютеров на основе интерфейса Unified Extensible Firmware Interface).

**Обновление общей папки развертывания**

После настройки общей папки развертывания ее необходимо обновить. В ходе этого процесса выполняется создание образов загрузки Windows PE.

1. В Deployment Workbench щелкните правой кнопкой мыши **MDT Build Lab deployment share** и выберите **Update Deployment Share**.
2. Используйте параметры по умолчанию для мастера обновления общей папки развертывания.

Примечание

Процесс обновления займет от 5 до 10 минут.

**Пояснения к правилам**

После настройки общей папки развертывания MDT Build Lab (то есть папки, которая используется для создания эталонных образов) можно рассмотреть разнообразные параметры, которые используются в файлах Bootstrap.ini и CustomSettings.ini.

Файлы Bootstrap.ini и CustomSettings.ini работают вместе. Файл Bootstrap.ini всегда присутствует в образе загрузки и его чтение происходит в первую очередь. Основная цель файла Bootstrap.ini заключается в предоставлении базовых сведений для MDT по нахождению файла CustomSettings.ini.

Файл CustomSettings.ini обычно хранится на сервере в папке «Общая папка развертывания\Control», но он также может находиться на носителе (при использовании автономного носителя).

Примечание

Параметры или свойства, которые используются в правилах (CustomSettings.ini и Bootstrap.ini), перечислены в документации MDT в разделе «Справка по Microsoft Deployment Toolkit / Свойства / Определение свойств».

**Файл Bootstrap.ini**

Файл Bootstrap.ini можно открыть через диалоговое окно «Свойства» в общей папке развертывания или через папку E:\MDTBuildLab\Control на MDT01.

syntax
```
[Settings]
Priority=Default
[Default]
DeployRoot=\\MDT01\MDTBuildLab$
```

```
UserDomain=CONTOSO
UserID=MDT_BA
UserPassword=P@ssw0rd
SkipBDDWelcome=YES
```

Ниже рассматриваются параметры.

- **Приоритет.** Он определяет порядок чтения разделов. Данный файл Bootstrap.ini содержит только один раздел [Default].
- **DeployRoot.** Это расположение общей папки развертывания. Обычно это значение задается MDT, однако после перемещения на другой сервер или в другую общую папку его необходимо обновить вручную. Если значение не указано, мастер развертывания Windows запросит расположение.
- **UserDomain, UserID и UserPassword.** Эти значения используются для автоматического входа в общую папку развертывания. Если значения не указаны, мастер запросит их.

  Предупреждение

  Соблюдайте осторожность. Эти значения сохраняются в открытом виде в образе загрузки. Используйте их только для общей папки развертывания MDT Build Lab, а не MDT Production, создание которой будет рассмотрено в следующем разделе.

- **SkipBDDWelcome.** Несмотря на то, что приятно видеть приветствие при каждом запуске развертывания, рекомендуется пропустить страницу приветствия в мастере развертывания Windows.

Примечание

Свойства, которые начинаются с параметра «Skip», управляют только отображением области в мастере развертывания Windows. Для большинства областей также требуется установка одного или нескольких значений.

**Файл CustomSettings.ini**

Файл CustomSettings.ini, содержимое которого отображается на вкладке «Правила» диалогового окна «Свойства» общей папки развертывания, содержит большую часть свойств, используемых в конфигурации.

syntax

```
[Settings]
Priority=Default
[Default]
_SMSTSORGNAME=Contoso
```

```
UserDataLocation=NONE
DoCapture=YES
OSInstall=Y
AdminPassword=P@ssw0rd
TimeZoneName=Pacific Standard Time
JoinWorkgroup=WORKGROUP
HideShell=YES
FinishAction=SHUTDOWN
DoNotCreateExtraPartition=YES
WSUSServer=http://mdt01.contoso.com:8530
ApplyGPOPack=NO
SLSHARE=\\MDT01\Logs$
SkipAdminPassword=YES
SkipProductKey=YES
SkipComputerName=YES
SkipDomainMembership=YES
SkipUserData=YES
SkipLocaleSelection=YES
SkipTaskSequence=NO
SkipTimeZone=YES
SkipApplications=YES
SkipBitLocker=YES
SkipSummary=YES
SkipRoles=YES
SkipCapture=NO
SkipFinalSummary=YES
```

- **Приоритет.** Выполняет такую же функцию, что и для файла Bootstrap.ini. Приоритет определяет порядок чтения разделов. Данный файл CustomSettings.ini содержит только один раздел [Default]. Как правило, если несколько разделов задают одно и то же значение, значение из первого раздела имеет более высокий приоритет. Редкие исключения перечислены в файле ZTIGather.xml.
- **_SMSTSORGNAME.** Название организации, отображаемое в индикаторе хода выполнения последовательности задач во время развертывания.
- **UserDataLocation.** Управляет параметрами для пользовательской резервной копии состояния. Нет необходимости использовать этот параметр во время построения и создания снимка эталонного образа.
- **DoCapture.** Настраивает последовательность задач для запуска средства подготовки системы Sysprep и сохранения снимка образа в файл при установке операционной системы.
- **OSInstall.** Должно быть значение Y или YES (код находит только букву Y) для того, чтобы установка продолжилась.

- **AdminPassword.** Задает пароль учетной записи локального администратора.
- **TimeZoneName.** Задает часовой пояс для использования. Не следует путать это значение со значением TimeZone, которое используется только в старых операционных системах (Windows 7 и Windows Server 2003).

  **Обратите внимание** , что самый простой способ найти текущее имя часового пояса на компьютере с Windows 10 — выполнить команду tzutil/g в командной строке. Можно также выполнить команду tzutil /l, чтобы перечислить все доступные имена часовых поясов.

- **JoinWorkgroup.** Настраивает Windows для присоединения к группе.
- **HideShell.** Скрывает оболочку Windows во время развертывания. Это особенно полезно для развертывания Windows 10, когда мастер развертывания в противном случае будет работать за плиткой.
- **FinishAction.** Предписывает MDT, что делать, когда последовательность задач выполнена.
- **DoNotCreateExtraPartition.** Настраивает последовательность задач так, чтобы не создавать дополнительный раздел для BitLocker. Это не нужно делать для эталонного образа.
- **WSUSServer.** Определяет, какой сервер служб WSUS (и порт, если необходимо) следует использовать во время развертывания. Без этого параметра MDT будет использовать Центр обновления Майкрософт напрямую. Это увеличит время развертывания и ограничит возможности по выбору применяемых обновлений.
- **SLSHARE.** Предписывает MDT копировать файлы журнала в общую папку сервера при возникновении проблем во время развертывания, или если развертывание успешно завершено.
- **ApplyGPOPack.** Позволяет развернуть политику локальных групп, созданную диспетчером SCM.
- **SkipAdminPassword.** Пропускает область, которая запрашивает пароль администратора.
- **SkipProductKey.** Пропускает область, которая запрашивает ключ продукта.
- **SkipComputerName.** Пропускает область с именем компьютера.
- **SkipDomainMemberShip.** Пропускает область членства в домене. Если задано значение «Да», необходимо настроить свойство JoinWorkgroup либо свойства JoinDomain, DomainAdmin, DomainAdminDomain и DomainAdminPassword.
- **SkipUserData.** Пропускает область для миграции состояния пользователя.
- **SkipLocaleSelection.** Пропускает область для выбора языка и параметров клавиатуры.
- **SkipTimeZone.** Пропускает область установки часового пояса.

- **SkipApplications.** Пропускает область приложений.
- **SkipBitLocker.** Пропускает область BitLocker.
- **SkipSummary.** Пропускает исходную область сводки мастера развертывания Windows.
- **SkipRoles.** Пропускает область «Установка ролей и компонентов».
- **SkipCapture.** Пропускает область захвата.
- **SkipFinalSummary.** Пропускает конечную область сводки мастера развертывания Windows. Поскольку используется FinishAction=Shutdown, необходимо, чтобы мастер не остановился в конце и пользователю не пришлось нажимать кнопку «ОК» для выключения компьютера.

**Построение эталонного образа Windows 10**

После создания последовательности задач можно переходить к созданию эталонного образа Windows 10. Это можно сделать путем запуска последовательности задач с виртуальной машины, которая автоматически выполнит создание эталонного образа и снимка. Приведенные ниже шаги охватывают процесс, используемый для загрузки виртуальной машины с помощью образа загрузки ISO, созданного MDT, и выполнения последовательности задач для создания эталонного образа и снимка Windows 10.

1. Скопируйте файл E:\MDTBuildLab\Boot\MDT Build Lab x86.iso на MDT01 в папку C:\ISO на узле Hyper-V.

   **Примечание** . в MDT вы можете использовать загрузочный образ x86 для развертывания образов операционной системы x86 и x64. Поэтому можно использовать образ загрузки x86 вместо образа загрузки x64.

2. Создайте виртуальную машину со следующими параметрами:
   1. Имя: REFW10X64-001
   2. Местоположение: C:\VMs
   3. ОЗУ: 1024 МБ
   4. Сеть: внешняя (сеть должна быть подключена к той же инфраструктуре, что и MDT01)
   5. Жесткий диск: 60 ГБ (динамический диск)
   6. Файл образа: C:\ISO\MDT Build Lab x86.iso
3. Создайте снимок виртуальной машины REFW10X64-001 и назовите его **Clean with MDT Build Lab x86 ISO**.

   **Примечание** . Создание снимка полезно, если вам необходимо перезапустить процесс и убедиться, что вы можете начать очистку.

4. Запустите виртуальную машину REFW10X64-001. После загрузки в Windows PE завершите мастер развертывания Windows со следующими параметрами:
    1. Выбор последовательности задач для выполнения на этом компьютере: Windows 10 Корпоративная x64 RTM Default Image
    2. Укажите, следует ли создавать снимок образа: создать снимок для этого эталонного компьютера
        - Местоположение: \\MDT01\MDTBuildLab$\Captures
    3. Имя файла: REFW10X64-001.wim

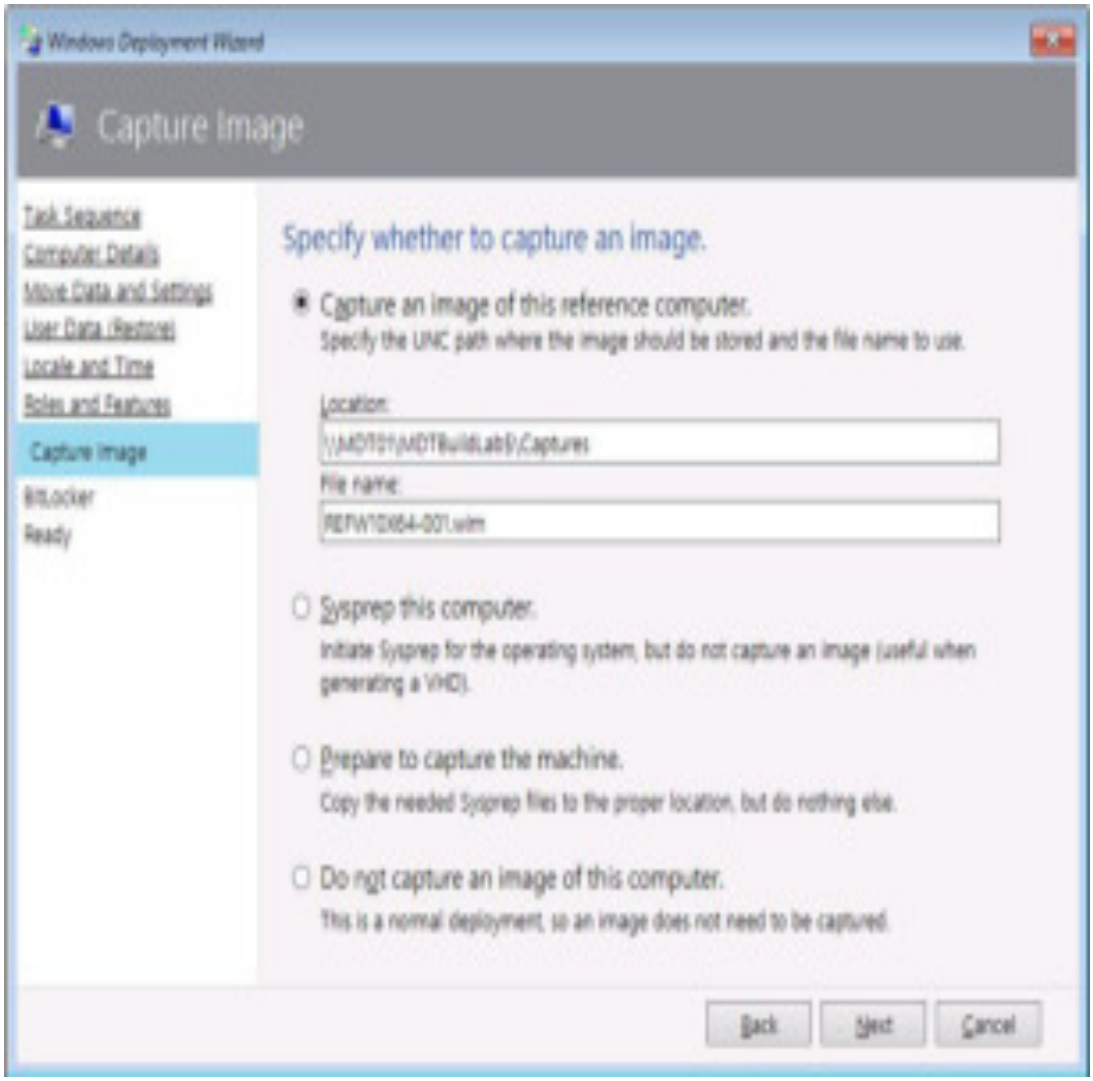



Рисунок 13. Мастер развертывания Windows для эталонного образа Windows 10.

5. Программа установки будет запущена и выполнит следующие действия.
    1. Установит операционную систему Windows 10 Корпоративная.
    2. Установит добавленные приложения, роли и компоненты.
    3. Обновит операционную систему через локальный сервер служб Windows Server Update Services (WSUS).

4. Сохранит Windows PE на локальном диске.
5. Выполнит средство подготовки системы Sysprep и перезагрузится в Windows PE.
6. Создаст снимок установки и сохранит его в файл WIM.
7. Отключит виртуальную машину.

Через некоторое время вы будете иметь полностью исправленный и работающий с помощью Sysprep образ для Windows10 Enterprise x64, который находится в папке E:\мдтбуилдлаб\каптурес на сервере развертывания. Имя файла — REFW10X64-001.wim.

## Практическое занятие №9 Настройка и управление Windows Deployment Services Планирование среды Windows Deployment Services

***Цель работы:***
Научиться выполнять настройки и управлять Windows Deployment Services Выполнять планирование среды Windows Deployment Services.

Одной из основных задач ИТ-отдела, независимо от масштабов организации, типа бизнеса и парка ПК, является развертывание рабочих мест. «Глубина» этого процесса может варьироваться, но в любом случае важность его эффективной организации подчеркивает традиционное мнение руководства о том, что новый ПК должен быть готов буквально по первому же требованию.

Для решения задачи развертывания ПК «в лоб» действительно необходимо немало времени и, как правило, участие специалиста. А если таких ПК – 10, 50, 100? А если больше? А если они еще и физически размещены далеко друг от друга – пусть даже в другой комнате, в двадцати шагах прямо по коридору или этажом выше? А ведь, кроме ОС, нужно установить еще и некоторый набор программного обеспечения, выполнить определенную настройку...

Службы развертывания Windows (WDS) — отличное дополнение к набору продуктов Windows. В стандартной конфигурации WDS обеспечивает развертывание виртуальных машин (ВМ) Windows, а если внести небольшие изменения, его можно использовать также для создания серверов Linux и VMware. Причем все это можно сделать из меню загрузки с возможностью выбора Preboot eXecution Environment (PXE).

Чтобы настроить WDS для развертывания систем Windows и Linux, необходимо внести несколько изменений в командной строке. По сути, нужно заменить загрузчик PXE, используемый Windows, на загрузчик для Linux. После этого создается пункт меню, позволяющий меню загрузки PXE для Linux переключаться на меню Windows для загрузки Windows, а для создания веб-интерфейса для загрузки файлов конфигурации Linux используется IIS.

Настройки WDS, позволяют развертывать Windows, CentOS и ESXi.  можно использовать и другие.

На пустом сервере Windows нужно выделить диск C: объемом 60 ГБ для операционной системы и диск WDS объемом 300 ГБ для различных файлов WIM, необходимых для развертывания Windows, и для файлов установки Linux.

Установка и настройка выполняются в несколько этапов:

**Настройка сервера WDS**

На сервере должны быть установлены WDS и IIS. Это можно сделать с помощью программы Windows Server Manager или с помощью PowerShell.

```
Install-WindowsFeature–nameWeb-server                    -
includemanagementtools
Install-Windowsfeature –name WDS -includemanagementtools
```

Теперь, когда у нас установлен базовый сервер служб развертывания Windows, нужно внести некоторые изменения в пул DHCP. При желании можно добавить вторую сетевую плату на этот сервер и создать выделенную сеть, но мы будем создавать серверы в основной сети, поэтому обновимь центральный сервер DHCP с помощью дополнительных атрибутов DHCP WDS:

Будем использовать следующие настройки DHCP:

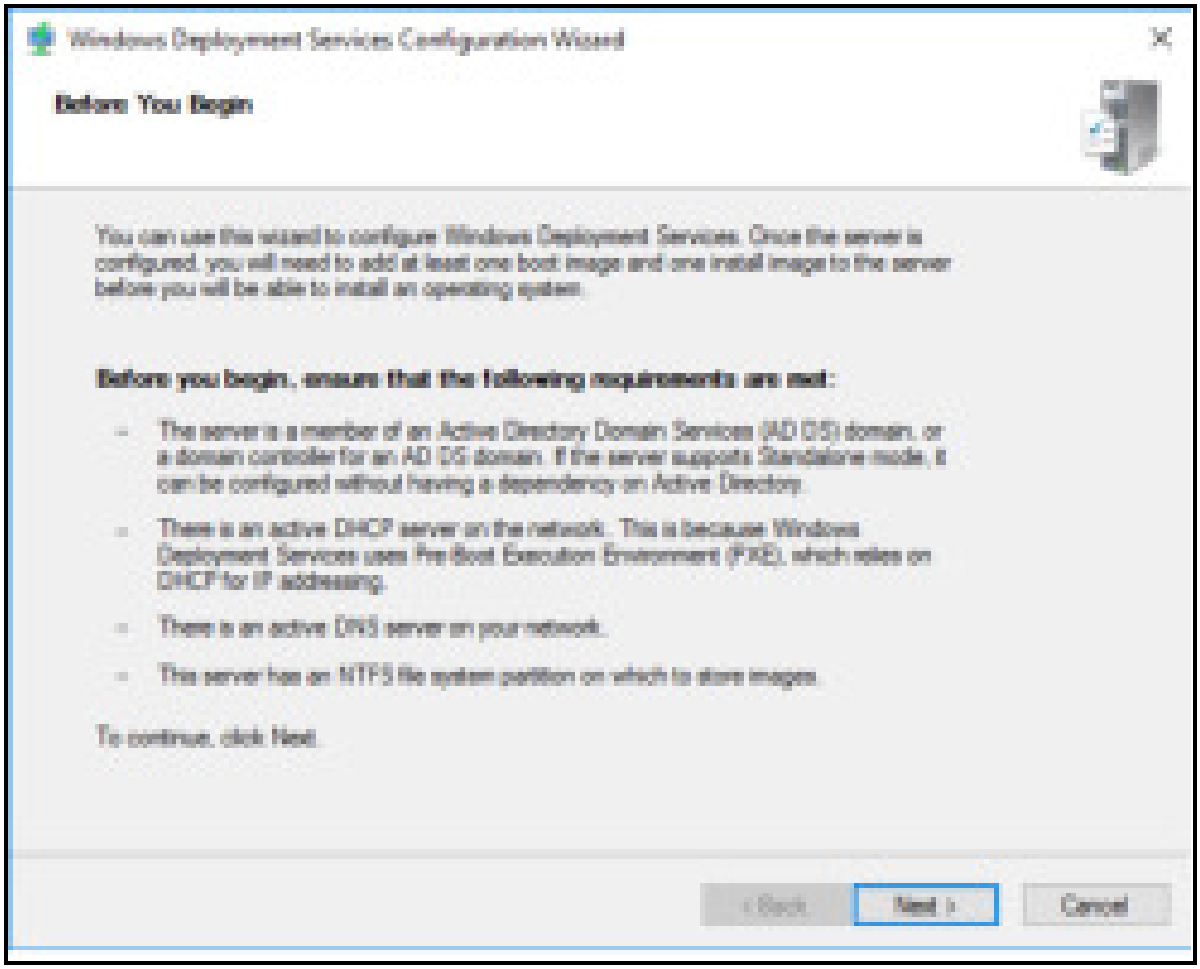
| Option Name | Vendor | Value | Class |
|---|---|---|---|
| 003 Router | Standard | 10.253.1.254 | None |
| 066 Boot Server Host Name | Standard | 10.253.1.26 | None |
| 067 Bootfile Name | Standard | boot\pxe\wdsnbp.com | None |
| 006 DNS Servers | Standard | 10.253.1.44, 10.253.1.42 | None |
| 015 DNS Domain Name | Standard | gdvnet.com | None |

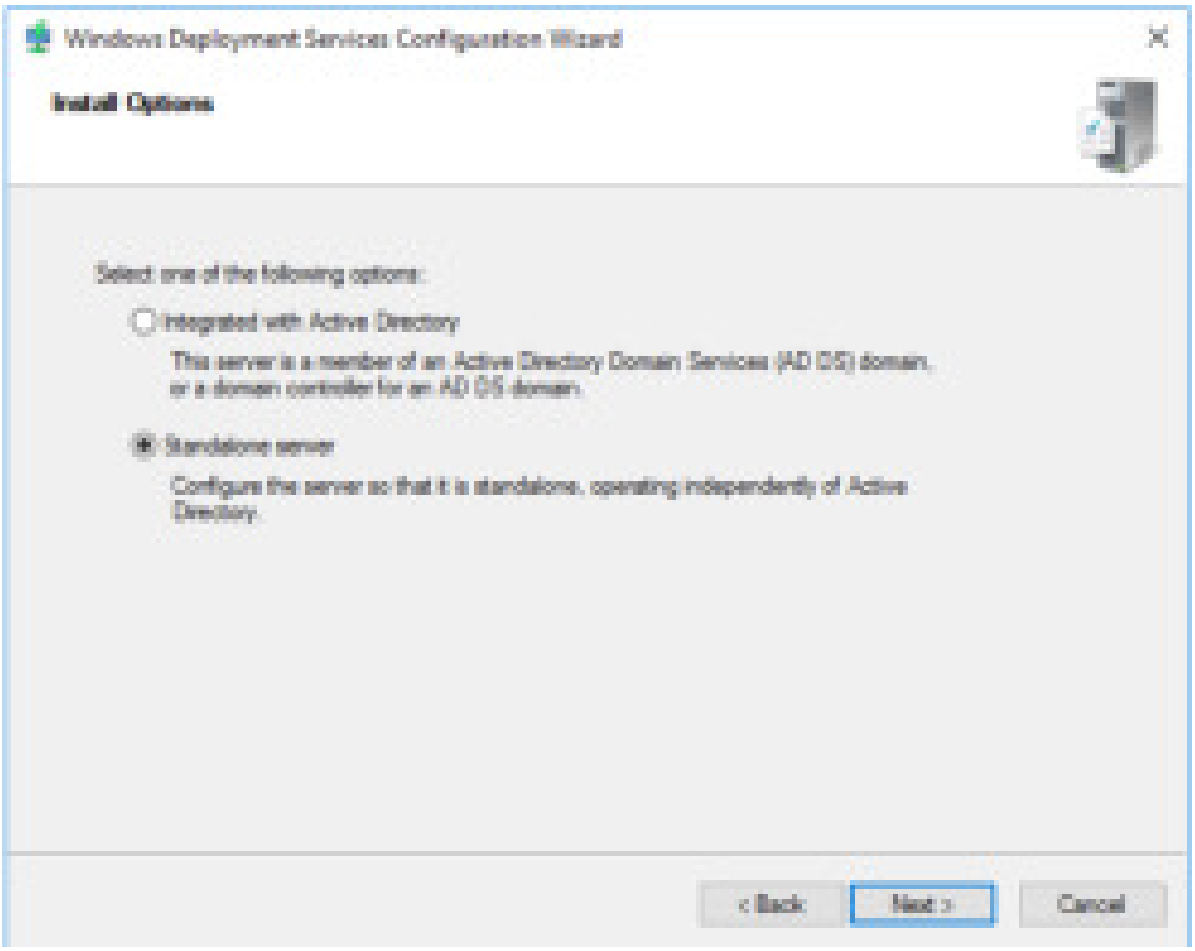
**«Имя узла сервера загрузки»** — IP-адрес сервера WDS.

**«Имя файла загрузки»** — исполняемый файл WDS, который должен быть запущен клиентом.

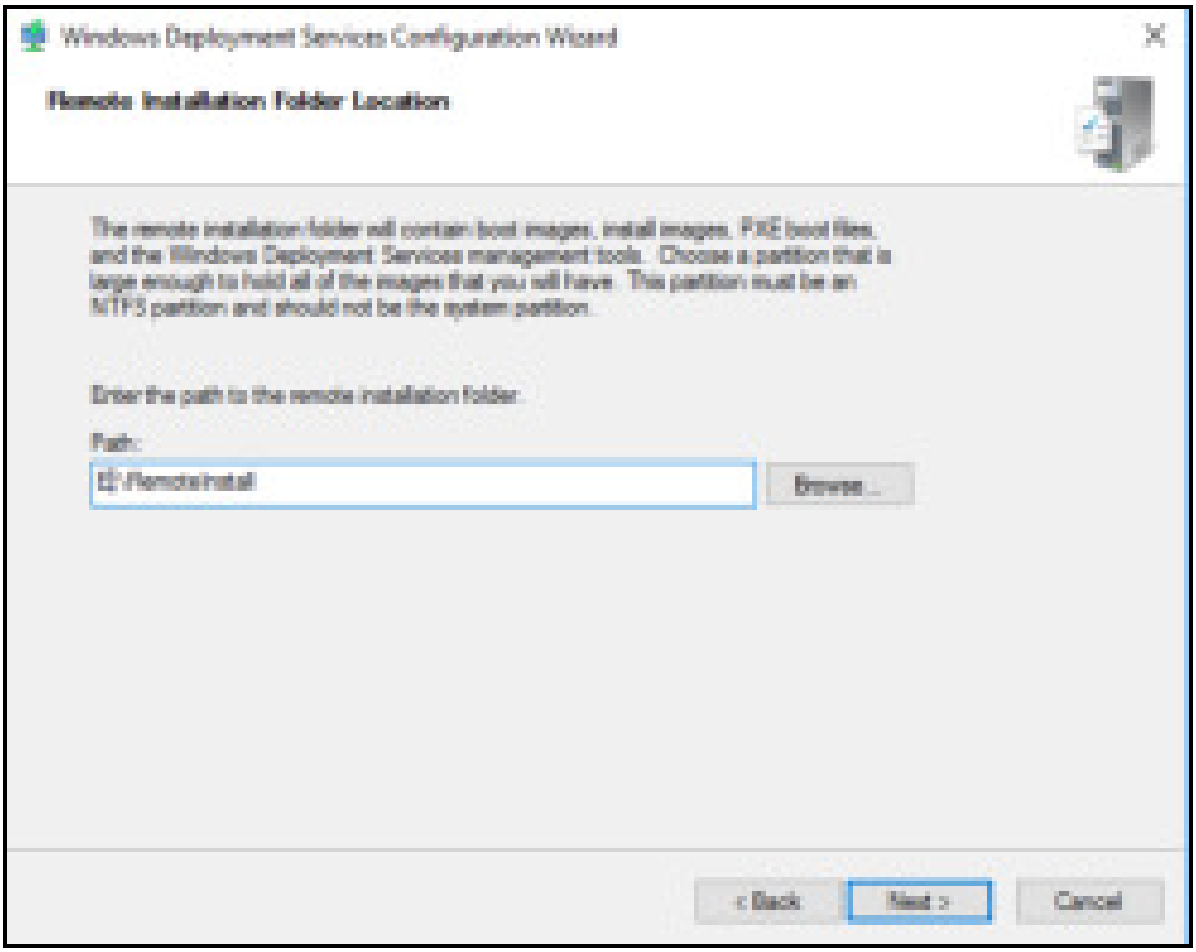
Три других параметра — стандартные для большинства настроек DHCP.

Запустите мастер настройки на сервере WDS и завершите настройку WDS. Сделаем несколько небольших изменений в настройках.

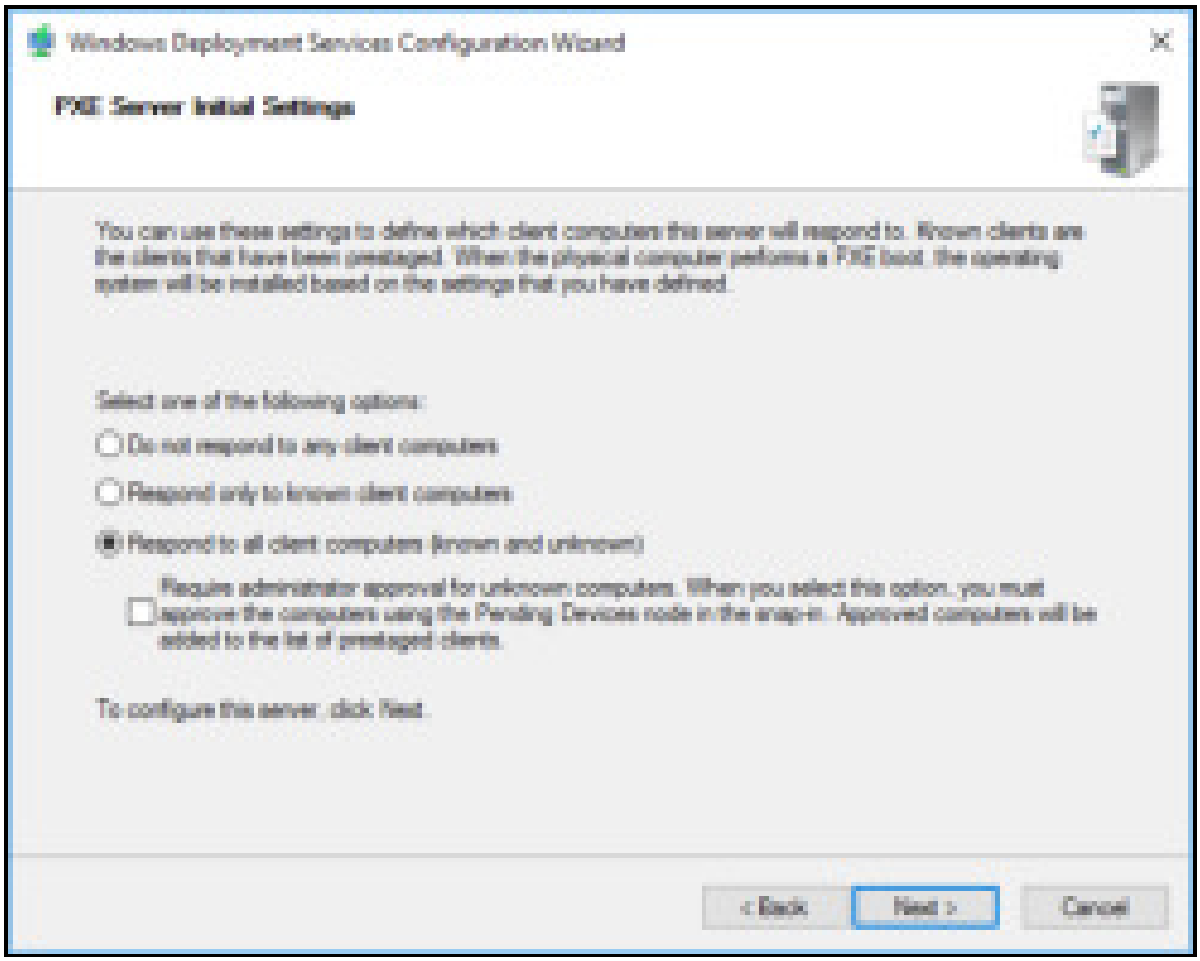

Windows Deployment Services Configuration Wizard
Before You Begin
You can use this wizard to configure Windows Deployment Services. Once the server is configured, you will need to add at least one boot image and one install image to the server before you will be able to install an operating system.
Before you begin, ensure that the following requirements are met:
The server is a member of an Active Directory Domain Services (AD DS) domain, or a domain controller for an AD DS domain. If the server supports Standalone mode, it can be configured without having a dependency on Active Directory.
There is an active DHCP server on the network. This is because Windows Deployment Services uses Pre-Boot Execution Environment (PXE), which relies on DHCP for IP addressing.
There is an active DNS server on your network.
This server has an NTFS file system partition on which to store images.
To continue, click Next.
< Back
Next >
Cancel




Сервер можно интегрировать с AD, поскольку в этот момент мы настраиваем параметры Windows, но будем использовать автономный сервер, который отвечает на все запросы без предварительного размещения в AD.

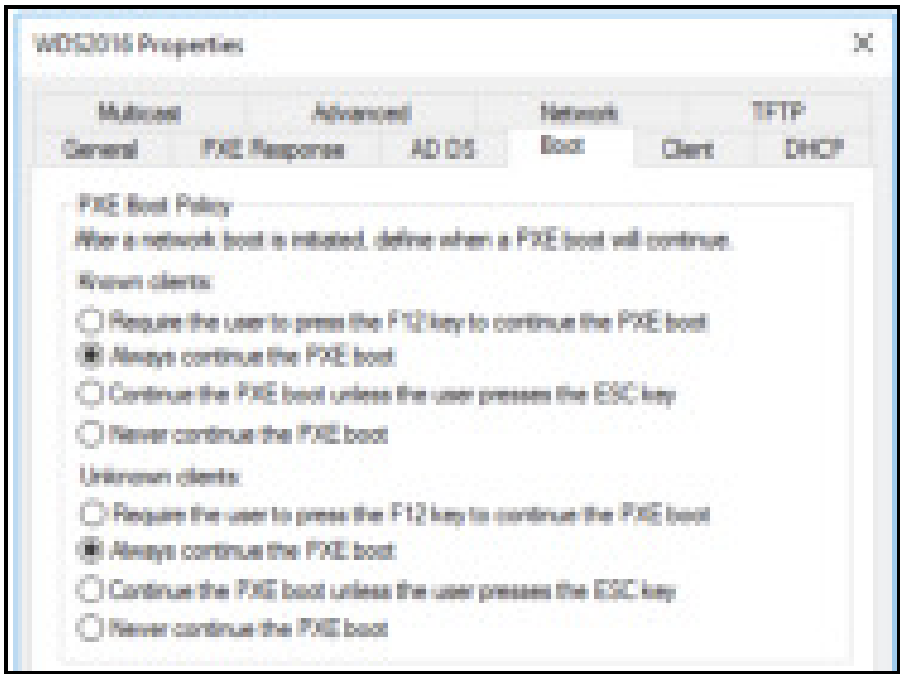



Меняем C:\RemoteInstall на E:\RemoteInstall. **E:** — это второй диск, который мы добавляем на сервер WDS специально для файлов WIM, файлов Linux и т. п.




Мы хотим чтобы сервер PXE сам отвечал на все запросы, не тратя времени на получение подтверждения от AD.

Последний параметр, который надо изменить, находится в меню PXE. Для этого нужно запустить консоль развертывания WDS, щелкнуть правой кнопкой мыши на имени сервера и изменить значение параметра на вкладке загрузки с «**Require the user to press F12 key to continue the PXE boot**» («Пользователь должен нажать клавишу F12 для продолжения загрузки PXE») на «**Always continue the PXE boot**» («Всегда продолжать загрузку PXE»).




Теперь в WDS можно добавить файлы .WIM. Достаточно скопировать файлы «**boot.wim**» и «**install.wim**» из образа **2016 ISO**, и тогда можно развернуть образы Windows с помощью WDS.

Можно запустить ВМ с помощью загрузки PXE и открыть стандартный экран загрузки WDS, на котором будет только ОС Windows. На этом этапе стоит протестировать развертывание и убедиться, что все работает, потому что теперь мы начинаем вносить фундаментальные изменения в WDS, которые позволят использовать службы для установки Linux и ESXi.

**Изменение загрузчика служб развертывания Windows**

Сервер WDS уже может выполнить развертывание образов Windows, но мы хотим, чтобы он делал не только это. Он должен также справляться с образами Linux, поэтому первое мы меняем загрузчик WDS на загрузчик Linux PXE.

Для этого нужно скачать sysLinux. НЕ СКАЧИВАЙТЕ версии позже 3.86 — они не будут работать с ESXi, поскольку их установщик по-прежнему использует версию 3.86.

Скачав **sysLinux 3.86**, распакуйте архив во временную папку. Теперь нужно переместить несколько файлов. Это такая часть процесса установки, которая требует аккуратности!

Извлеките из архива sysLinux 3.86:

- **core\pxeLinux.0**
  **com32\menu\vesamenu.c32**
  **com32\modules\chain.c32**
- **Переименуйте pxeLinux.0 to pxeLinux.com**
- **Скопируйте файлы в папки remoteinstall\boot\x64 и remoteinstall\boot\x86**
- **В обеих папках x86 и x64 переименуйте pxeboot.n12 в pxeboot.0**

Из командной строки выполните следующие команды, чтобы заменить загрузчик по умолчанию на загрузчик Linux PXE:

```
wdsutil /set-server /bootprogram:boot\x86\pxeLinux.com /architecture:x86
wdsutil /set-server /N12bootprogram:boot\x86\pxeLinux.com /architecture:x86
wdsutil /set-server /bootprogram:boot\x64\pxeLinux.com /architecture:x64
wdsutil /set-server /N12bootprogram:boot\x64\pxeLinux.com /architecture:x64
```

В обеих папках x86 и x64 создайте подпапки с именем **pxeLinux.cfg,** а в них создайте файл с именем «**default**» и скопируйте в него следующий текст, чтобы настроить меню загрузки:

**DEFAULT vesamenu.c32**

**PROMPT 0**

**NOESCAPE 0**

**ALLOWOPTIONS 0**

**# Timeout in units of 1/10 s**

**TIMEOUT 0**

**MENU MARGIN 10**

**MENU ROWS 16**

**MENU TABMSGROW 21**

**MENU TIMEOUTROW 26**

**MENU COLOR BORDER 30;44 #20ffffff #00000000 none**

**MENU COLOR SCROLLBAR 30;44 #20ffffff #00000000 none**

**MENU COLOR TITLE 0 #ffffffff #00000000 none**

**MENU COLOR SEL 30;47 #40000000 #20ffffff**

**MENU BACKGROUND flow.jpg**

**MENU TITLE PXE Boot Menu**

**#---**

**LABEL wds**

**MENU LABEL Windows Deployment Services**

**MENU DEFAULT**

**KERNEL pxeboot.0**

**#---**

**LABEL CentOS68**

**MENU LABEL CentOS 6.8**

**KERNEL /web/CentOS/6.8/images/pxeboot/vmlinuz**

**append initrd=/web/CentOS/6.8/images/pxeboot/initrd.img root=/dev/ram0 init=/Linuxrc ramdisk_size=100000 ks=https://[IP-адрес сервера WDS]/CentOS/6.8/centos-base-ks.cfg**

**#---**

**LABEL CentOS72**

**MENU LABEL CentOS 7.2**

**KERNEL /web/CentOS/7.2/images/pxeboot/vmlinuz**

**append initrd=/web/CentOS/7.2/images/pxeboot/initrd.img**

**#---**

**LABEL VMWare500U3**

**MENU LABEL VMWare 5.0.0 U3**

**KERNEL /web/VMWare/5.0.0/U3/mboot.c32**

**APPEND -c /web/VMWare/5.0.0/U3/boot.cfg**

**#---**

**LABEL VMWare553b**

**MENU LABEL VMWare 5.5 U3b**

**KERNEL /web/VMWare/5.5.0/U3b/mboot.c32**

**APPEND -c /web/VMWare/5.5.0/U3b/boot.cfg**

**#---**

**LABEL VMWare60**

**MENU LABEL VMWare 6.0**

**KERNEL /web/VMWare/6.0/mboot.c32**

**APPEND -c /web/VMWare/6.0/boot.cfg**

**#---**

**LABEL VMWare65**

**MENU LABEL VMWare 6.5**

**KERNEL /web/VMWare/6.5/mboot.c32**

**APPEND -c /web/VMWare/6.5/boot.cfg**

**#---**

**LABEL Abort**

**MENU LABEL AbortPXE**

**Kernel abortpxe.0**

**#---**

**LABEL local**

**MENU LABEL Boot from Harddisk**

**LOCALBOOT 0**

**Type 0x80**

**Изменение настроек IIS**

IIS необходимы для размещения установочных файлов CentOS и ESXi. Создадим структуру веб-файлов на VMDK. Она выглядит так:

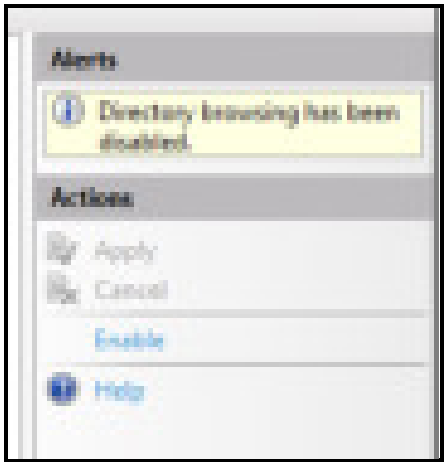
E:\web — корневой каталог, на который указывает IIS

E:\web\centos\7.x\7.1 — файлы установки CentOS 7.1

E:\web\vmware\6.5 — файлы установки VMware 6.5

В IIS необходимо включить просмотр файлов, чтобы установщик Linux и установщик VMware могли их извлечь.

Запустите программу администрирования IIS, выберите свой сервер -> Сайт по умолчанию -> Просмотр каталога и включите его.




Полезно также настроить защищенное соединение с сервером по протоколу HTTPS.

**Добавление Linux**

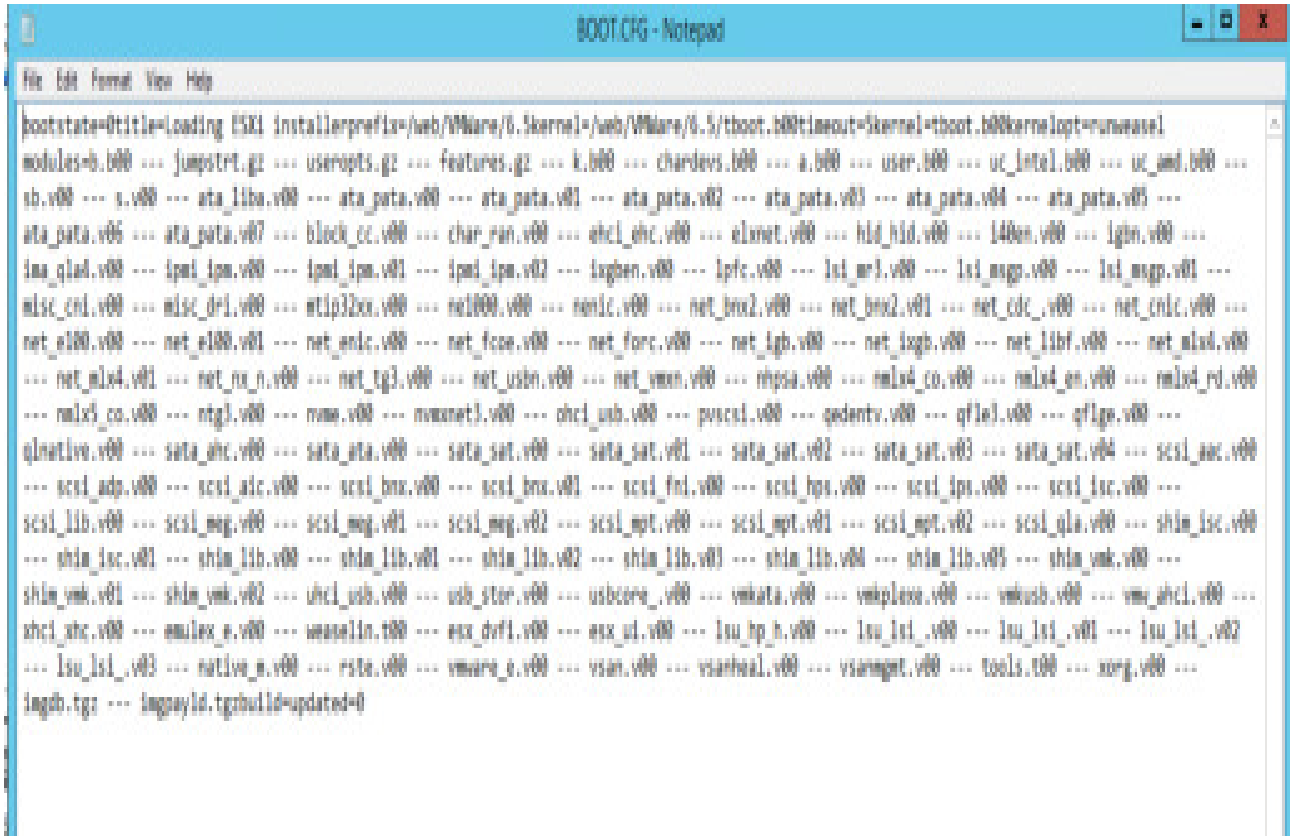
Теперь можно добавить Linux. Сделаем это так:

Скачаем самую маленькую ISO-версию CentOS (как правило, это образ minimal), монтируем образ ISO и копируем его содержимое в директорию «E:\web\centos\7.x\7.\[версия]» или другую, которую легко запомнить. После этого можно добавить, например, kickstart-файл, чтобы автоматизировать установку. Вот пример строк, которые добавим к файлу pxeLinux.cfg, используемому по умолчанию:

```
LABEL CentOS72

MENU LABEL CentOS 7.2

KERNEL /web/CentOS/7.2/images/pxeboot/vmlinuz

append initrd=/web/CentOS/7.2/images/pxeboot/initrd.img inst.repo=[IP-адрес сервера WDS]/CentOS/7.2 ks=[IP-адрес сервера WDS]/CentOS/7.2/centos-base-ks.cfg
```

**Добавление VMware**

Добавим ESXi 6.5. Для этого тоже надо просто скопировать все файлы из ISO-образа VMware в соответствующую папку на сервере WDS, но после этого надо изменить файл boot.cfg в папке VMware, удалив пробелы. Это выглядит так:



Изменение настроек сервера WDS, IIS и различных файлов конфигурации может потребовать некоторых усилий, но, сделав это, можно использовать меню PXE для переключения на WDS и выбрать любую ОС Windows, которая поддерживает WIM-файлы. С ее помощью можно также запускать установку Linux или VMware в полностью автоматическом режиме. Кроме того, для удобства можно добавить и другие приложения, такие как GParted и Memtest.

**Практическое занятие №10. Планирование и реализация миграции пользовательской среды**

***Цель работы:***

Изучить сценарии переноса данных. Научиться выполнять перенос данных с использованием WET

Одним из важных моментов процесса развертывания, является необходимость миграции пользовательских данных и настроек. Если пользователь настраивал какие-либо приложения под себя, то бывает достаточно трудно повторить все эти манипуляции. Ну, и самое важное для пользователей это пользовательские данные. Ни один пользователь не обрадуется установке новой операционной системы, если при этом он потеряет все свои важные документы.

В данной практической работе мы разберем различные варианты переноса данных и настроек при помощи утилиты WET.

## Перенос данных с помощью WET

С помощью утилиты **Средство переноса данных Windows (Windows Easy Transfer – WET)** можно осуществлять перенос файлов и настроек с одного компьютера, работающего под управлением ОС Windows более ранних версий, чем Windows 7, на другой компьютер, работающий под управлением Windows 7. Данные со старого компьютера не удаляются.

Утилита WET является встроенным средством и в основном направлена на использование в домашних условиях или для работы нетребовательным системным администраторам. К основным положительным сторонам относятся: простота работы (работа осуществляется при помощи пошагового мастера), является встроенным средством и не требует установки, перенос данных при помощи различных носителей (кабель переноса, локальная сеть, съемное устройство), обеспечение защиты переносимых данных.

Для запуска данной утилиты существует несколько способов:

1. "Пуск" -> "Поиск" -> "Перенос" -> "Средство переноса данных Windows".

2. "Пуск" -> "Все программы" -> "Стандартные" -> "Служебные" -> "Средство переноса данных Windows".

Начальное окно программы изображено на рис.1.

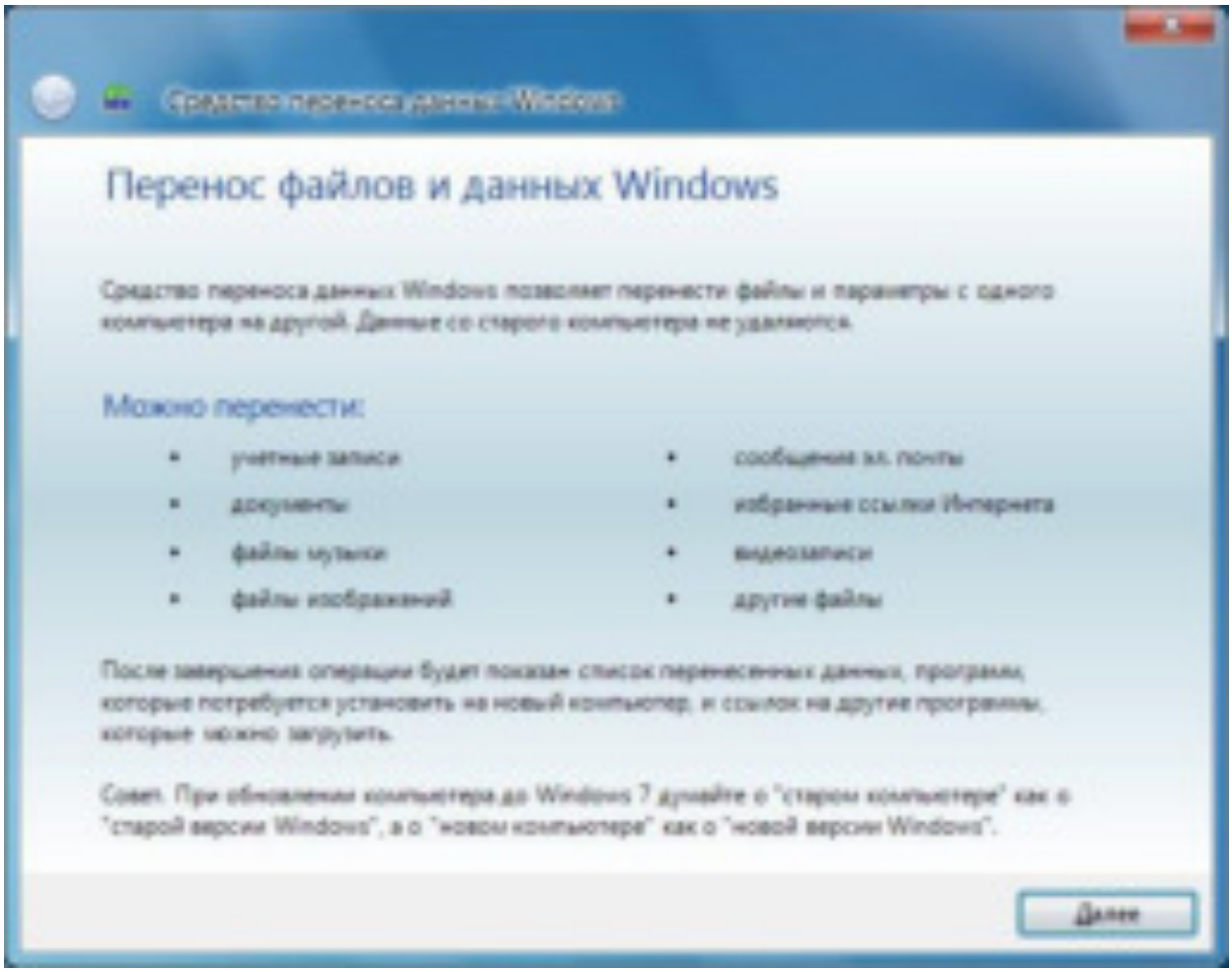



Рис.1.

Возможности приложения **WET**:

1. Способ переноса данных:
   - Кабель для переноса данных
   - Сетевое подключение
   - Съемное устройство (flash-носитель, CD/DVD, внешний жесткий диск)
2. Данные для переноса:
   - Файлы и папки
   - Учетные записи
   - Сообщения электронной почты, контакты
   - Мои документы (фотографии, видео, музыка)
   - Настройки подключения к Интернет
   - Настройки программ
   - Настройки Windows

Утилита **WET** представляет собой пошаговый мастер, значительно облегчающий процесс переноса данных и настроек. Весь процесс сводится к простым операциям выбора способа переноса данных, выбора необходимых данных для переноса и непосредственно применение перенесенных данных на новый компьютер.

**Сценарии переноса данных между компьютерами**

Сценарий переноса данных с помощью кабеля переноса:

1. Запускаем утилиту **WET** на двух компьютерах. Если на старом компьютере установлена операционная система Windows XP или Windows Vista, следует вначале установить средство переноса данных Windows. Чтобы установить средство переноса данных существует несколько вариантов:
   - Скачать данную утилиту из Интернет (Средство переноса данных Windows для переноса данных из 32-разрядной версии Windows XP в систему Windows 7 - http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=734917d8-0663-4c26-89d0-2d00b632ebdb, Средство переноса данных Windows для переноса данных из 64-разрядной версии Windows XP в систему Windows 7 - http://www.microsoft.com/downloads/details.aspx?FamilyID=75649781-1e3d-4000-a6ce-638fe694de02&displaylang=en, Средство переноса данных Windows для переноса данных из 32-разрядной версии Windows Vista в систему Windows 7 - http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=09d80814-2a73-4245-a63b-8e780d0430cb, Средство переноса данных Windows для переноса данных из 64-разрядной версии Windows Vista в систему Windows 7 - http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=30c4da6d-0522-4d28-aac3-ce9d70ac6a6a)
   - Скопировать файл установки с нового компьютера (запущенного под операционной системой Windows 7) с помощью мастера.
   - Выбираем тип компьютера (новый или исходный).
2. Соединяем 2 компьютера кабелем переноса данных.
3. Запускаем синхронизацию.
4. Переносим необходимые данные.

Сценарий переноса данных с помощью сети:

- Подключаем оба компьютера в локальную сеть.
- Запускаем утилиту **WET** на двух компьютерах. Если данная утилита не установлена, производим установку одним из указанных ранее способом.
- Выбираем тип компьютера.

- Получаем ключ для подключения к исходному компьютеру. Вводим его на новом компьютере.
- Запускаем синхронизацию.
- Переносим необходимые данные.

Сценарий переноса данных с помощью съемного носителя (внешний диск или USB устройство флэш-памяти):

- Запускаем утилиту **WET** на старом компьютере. Если данная утилита не установлена, произвести установку указанным ранее способом.
- Выбираем тип компьютера – исходный.
- Производим проверку возможности переноса.
- Выбираем необходимые данные для переноса.
- Сохраняем данные на съемный носитель.
- Запустить утилиту **WET** на новом компьютере.
- Выбрать тип компьютера – новый.
- Указать съемный носитель.
- Произвести перенос данных.

**Перенос данных с помощью кабеля переноса**

Для переноса файлов и настроек с одного компьютера на другой Microsoft рекомендует использовать кабель переноса данных ( **Easy Transfer Cable** ). Если ваш компьютер был поставлен без кабеля переноса данных, его можно заказать через Интернет или приобрести в электронном магазине. Если кабель переноса данных не был включен в комплект поставки, можно применить другие методы.

Для осуществления данного сценария необходимо запустить программу **WET** на двух компьютерах. В окне "Средства переноса данных" выбрать "Кабель переноса данных" (рис.2).

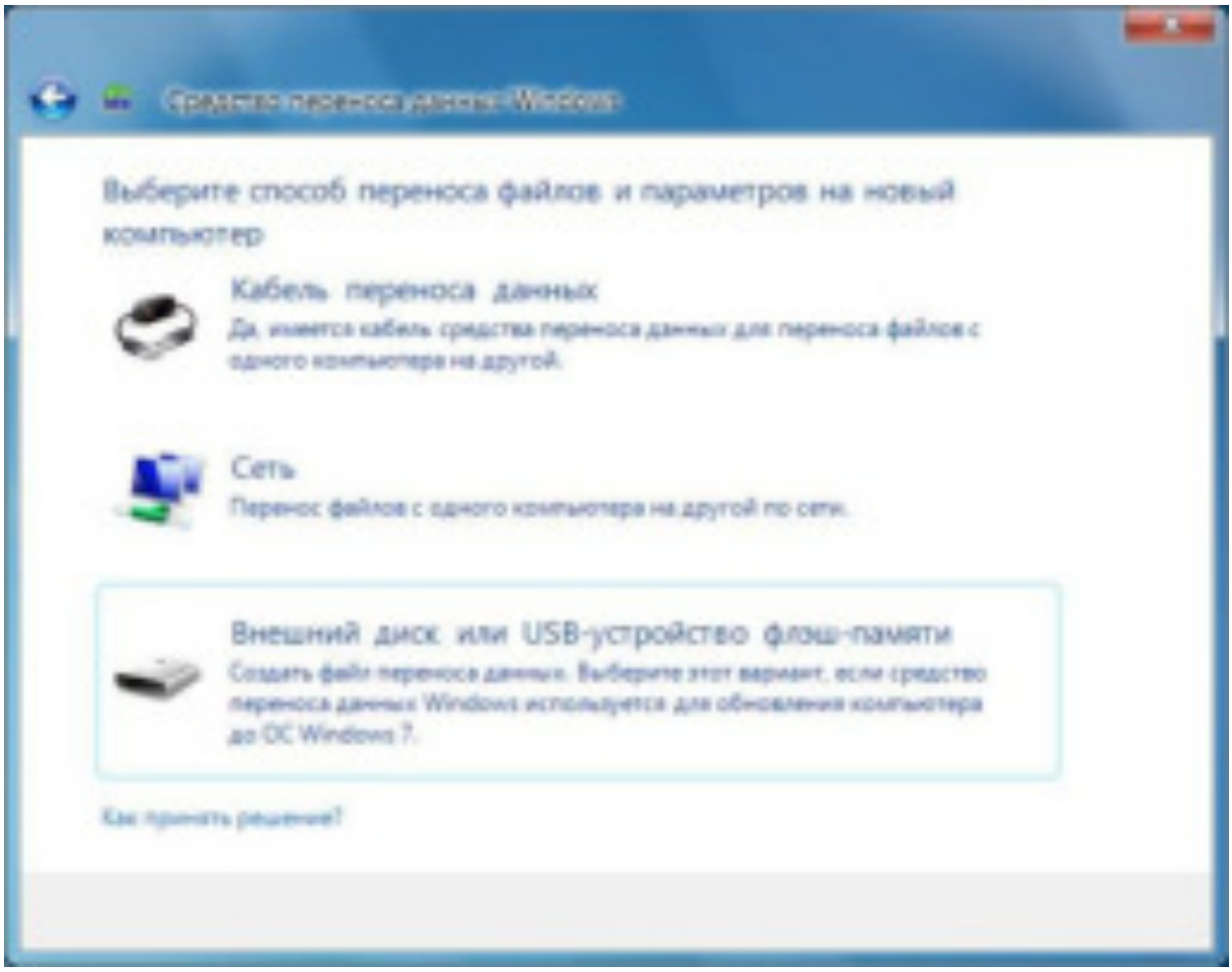



Рис.2.

После выбора способа переноса необходимо указать, какой компьютер используется (рис.3): исходный – компьютер на котором расположены необходимые данные, новый – "чистый" компьютер, на который необходимо перенести данные.

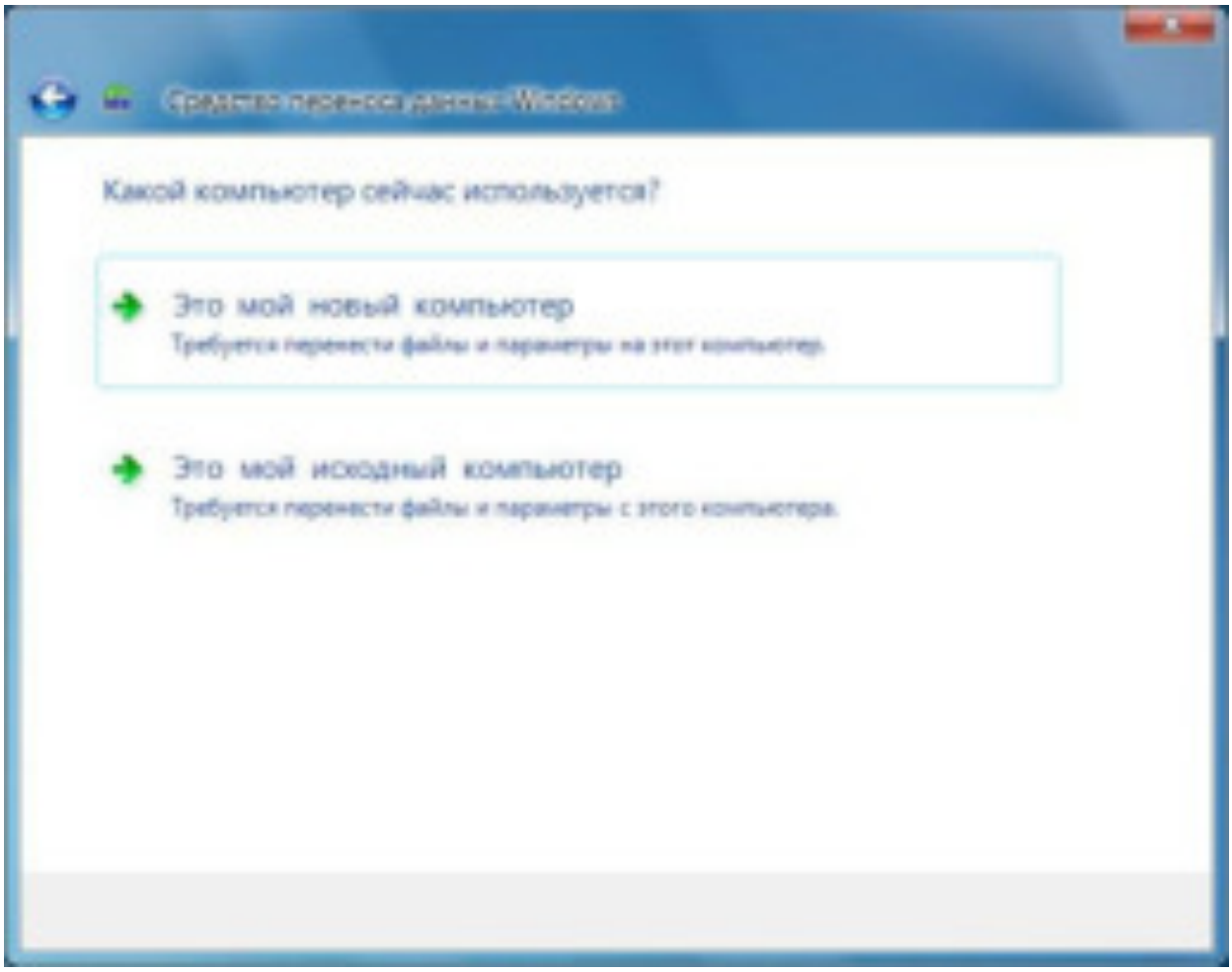



Рис.3.

После выбора типа компьютера нужно указать, необходимо ли установить средство переноса данных Windows (рис.4).

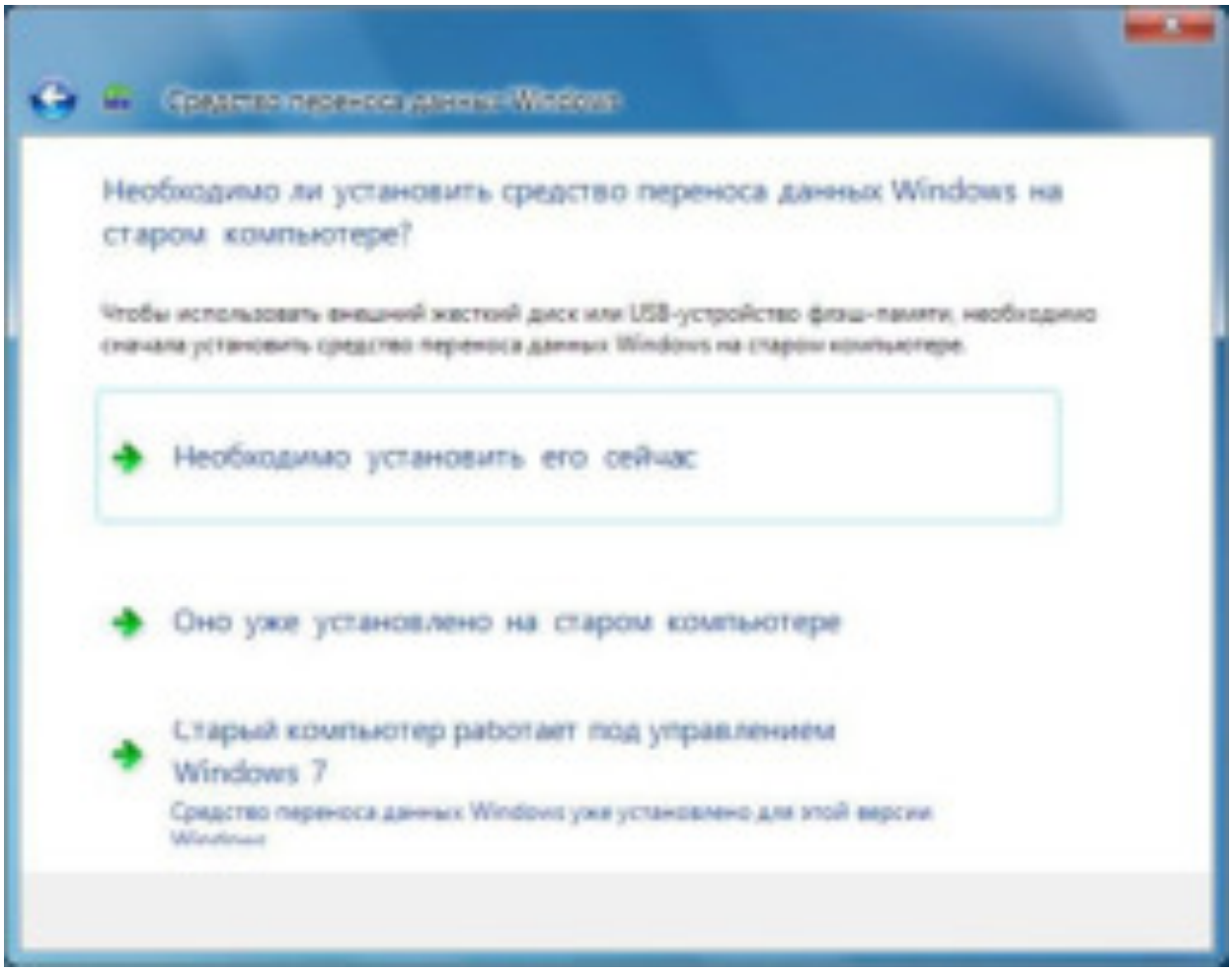



Рис.4.

Если необходимо установить приложение, то нужно выбрать способ установки (рис.5):

1. Внешний жесткий диск или общая сетевая папка.
2. Флэш-накопитель USB.

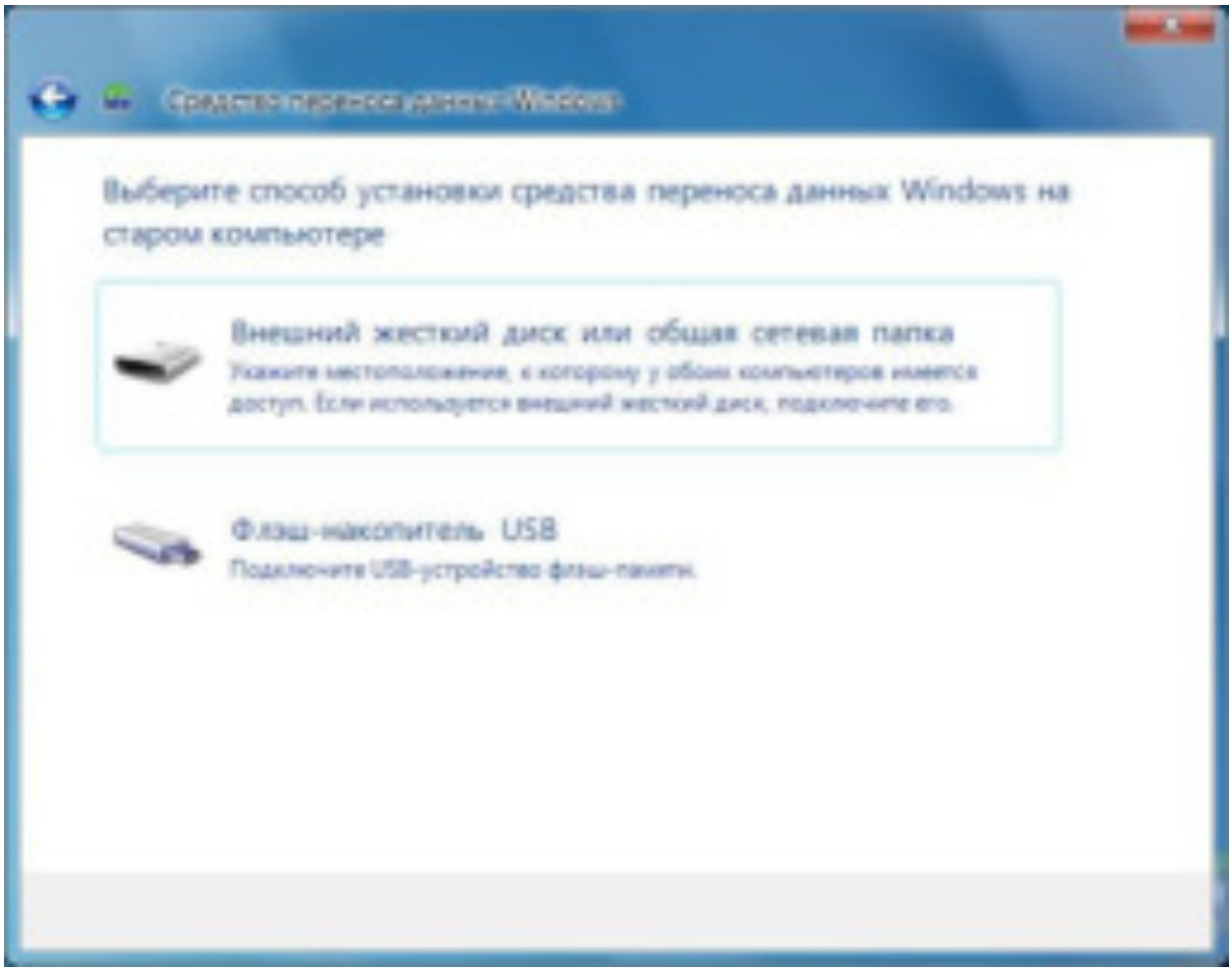



Рис.5.

Если нет необходимости устанавливать средство переноса данных, будет показана инструкция по переносу (рис.6).

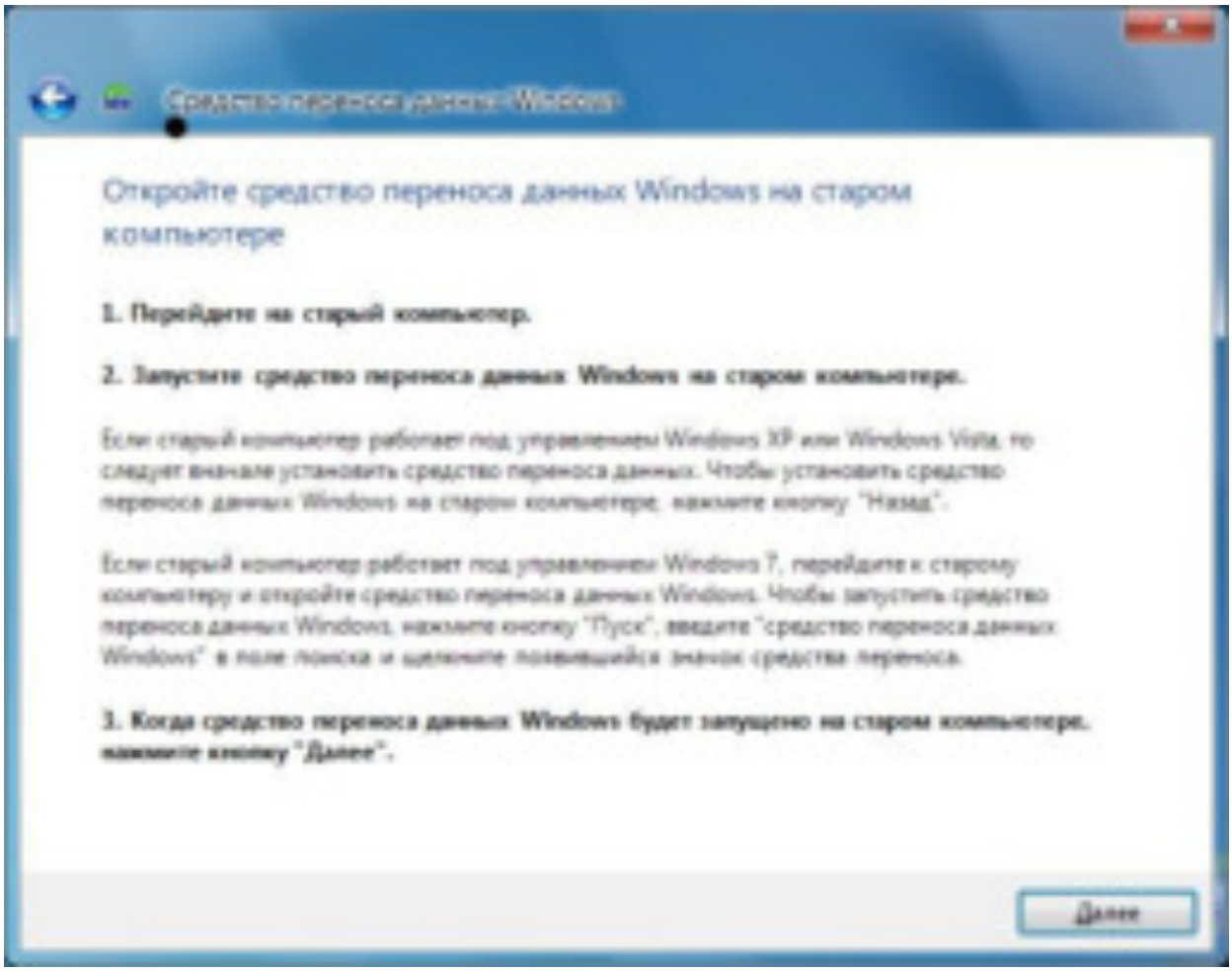



Рис.6.

**Перенос данных с помощью съемного носителя**

Для этого метода достаточно только USB-устройство флэш-памяти (на каждом компьютере должен быть USB-порт) или внешний жесткий диск, совместимый с обоими компьютерами.

Во время процесса переноса средство переноса Windows оценивает необходимое место на диске для передачи выбранных объектов. При использовании USB-устройства флэш-памяти самым простым способом является применение одного накопителя с достаточной емкостью для всего переноса. Если вместимость USB-устройства флэш-памяти недостаточна для переноса всех объектов за один раз, можно скопировать на него максимально возможное количество файлов, перенести их на новый компьютер, затем подключить накопитель к старому компьютеру и повторить процесс.

Помимо флэш-памяти можно использовать и другие съемные устройства, такие как внешний жесткий диск или оптические носители, запись на которые поддерживается непосредственно самой операционной системой (CD или DVD диски).

Для использования данного сценария необходимо запустить утилиту **WET**. В окне "Средства переноса данных" выбрать "Внешний диск или USB-устройство флэш-памяти".

После выбора способа переноса необходимо указать, какой компьютер используется: исходный или новый.

После выбора типа компьютера "Это мой новый компьютер" необходимо указать, было ли выполнено сохранение файлов со старого компьютера (рис.7).

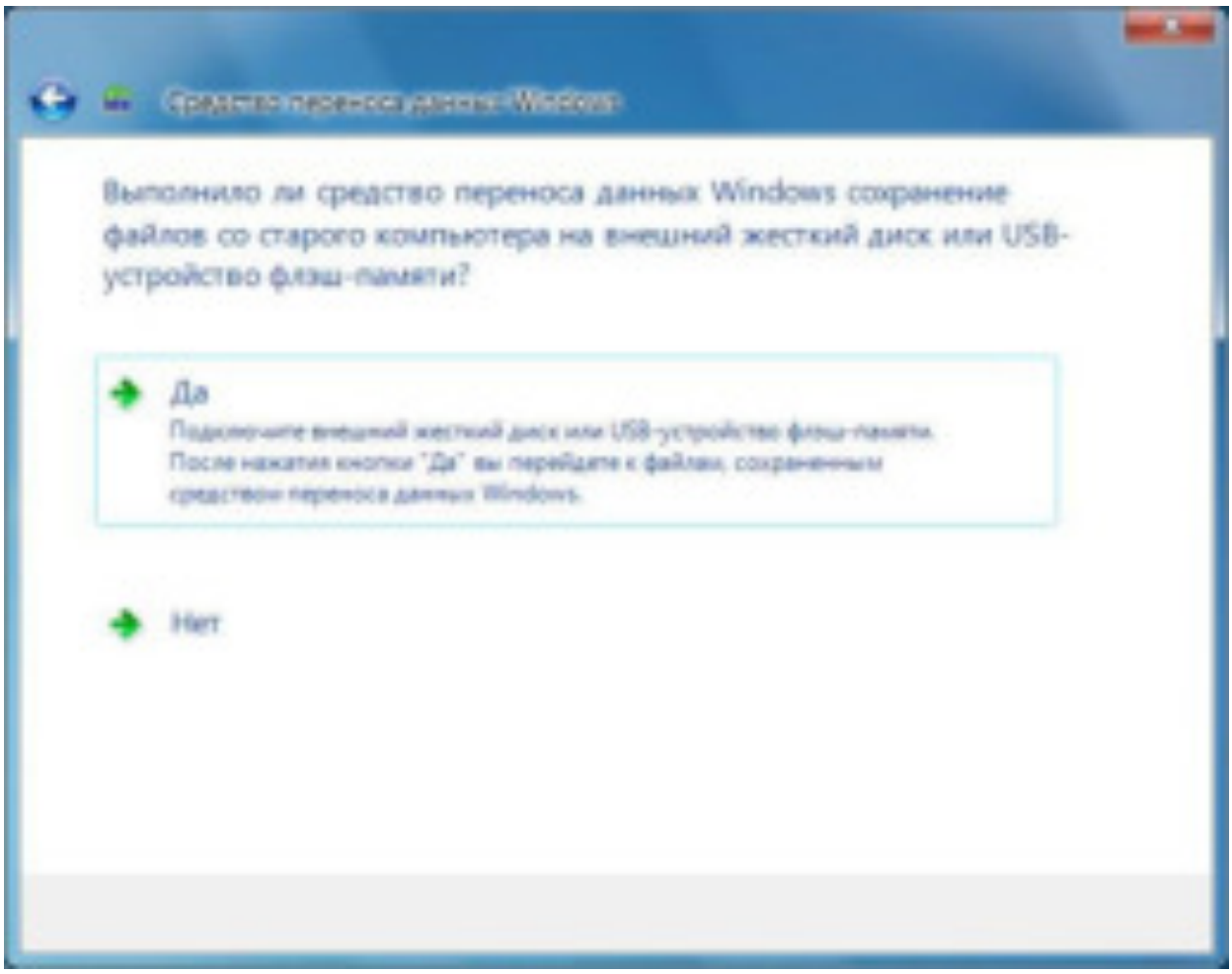



Рис.7.

Если ответить утвердительно, то мастер предложит открыть файл переноса данных (файл с расширением .mig). Если ответить отрицательно, мастер предложит выбрать, установлено ли данное приложение на старом компьютере (рис.8).

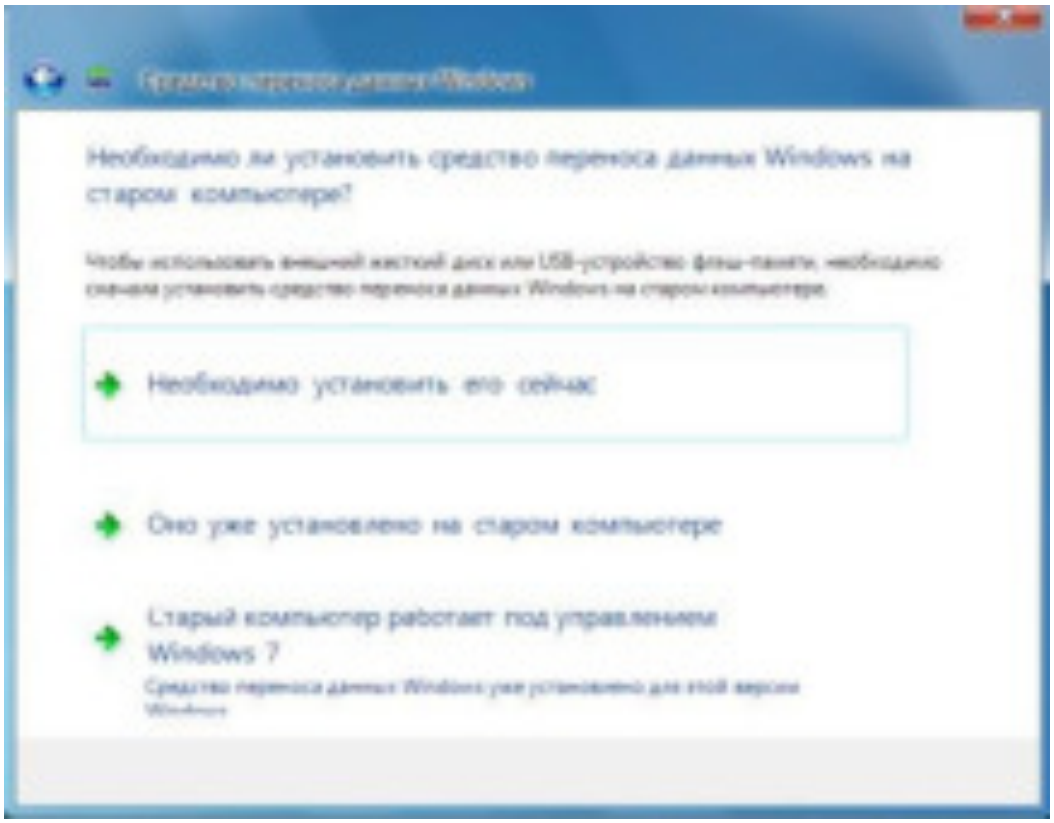



Рис.8.

Если приложение не установлено, то мастер поможет создать дистрибутивную папку на съемном носителе. Если приложение установлено, мастер отразит инструкцию по запуску средства переноса данных на старом компьютере (рис.9).

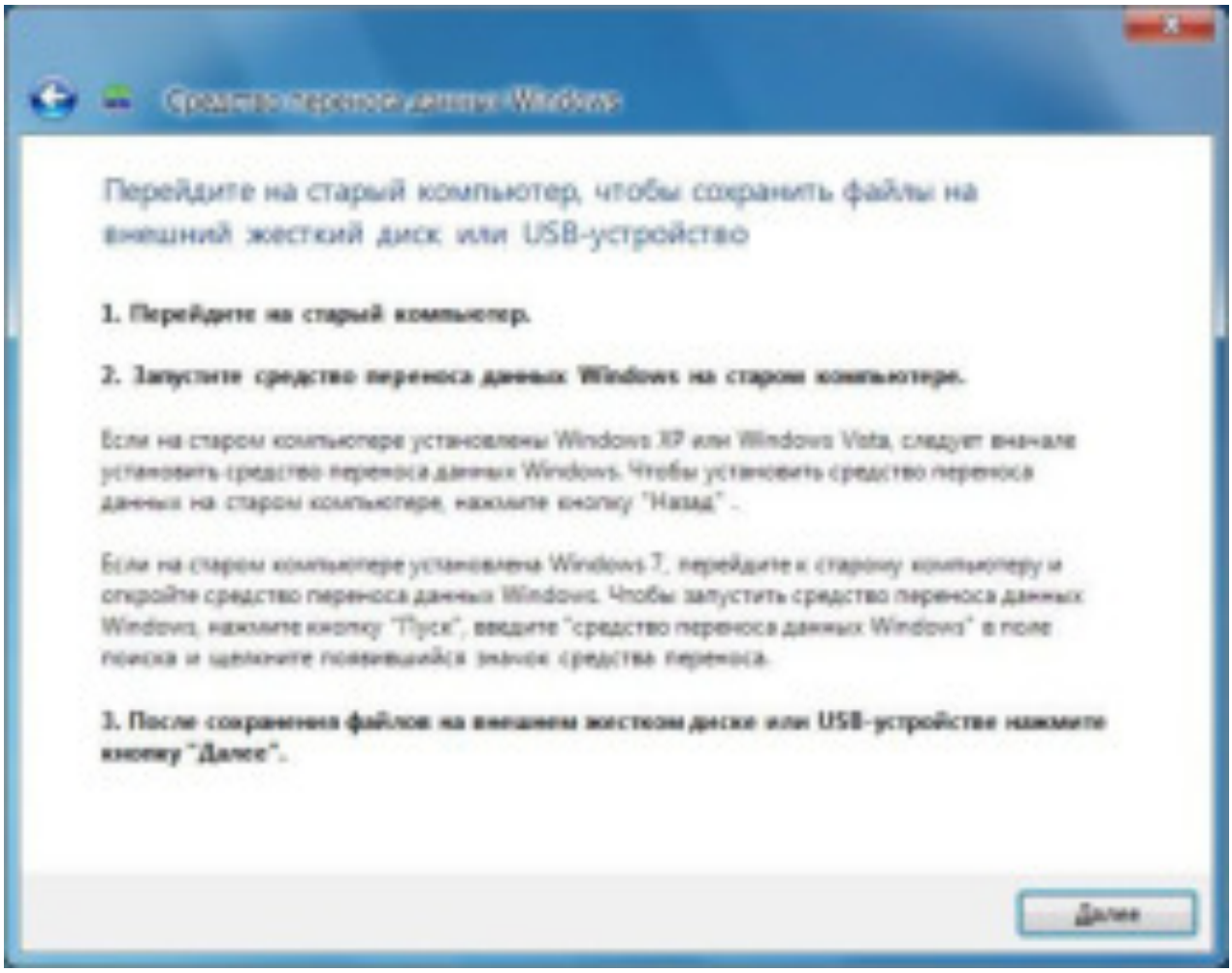



Рис.9.

При выборе исходного компьютера будет произведено сканирование компьютера. По окончании сканирования можно выбрать необходимый профиль. Для дополнительного изменения параметров переносимых данных можно воспользоваться функцией "Настройка". При необходимости можно задать пароль для защиты этого файла переноса. Затем нужно указать место для сохранения файла в формате .mig

**Перенос данных с помощью сети**

При выполнении этого метода оба компьютера должны быть подключены к одной и той же домашней или корпоративной сети.

При выборе способа переноса выбрать параметр "Сеть". При необходимости произвести установку утилиты WET на старом компьютере. На исходном компьютере необходимо получить ключ вида 111-111. Для переноса данных необходимо воспользоваться инструкцией изображенной на рис.10.

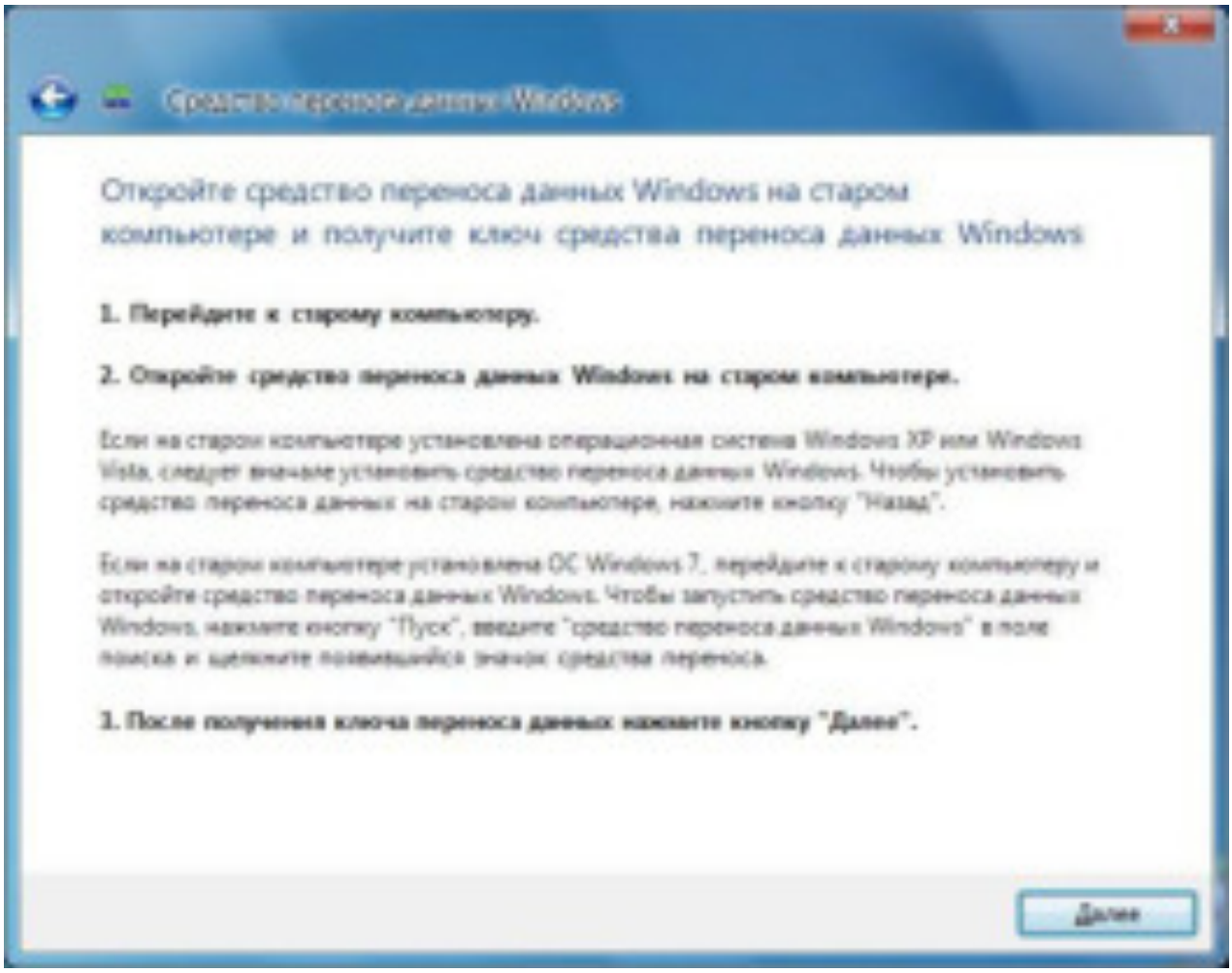



Рис.10.

**ЗАДАНИЕ: Выполнить Перенос пользовательских данных с помощью WET**

**Задачи**:

1. Установить WET на компьютер с операционной системой Windows 7.
2. Создать файл переноса на старом компьютере.
3. Применить файл переноса на новом компьютере.

**Требования**:

1. Операционная система на новом компьютере – Windows 7.
2. Операционная система на старом компьютере – Windows XP.
3. Программа переноса данных для 32-разрядной операционной системы - http://www.microsoft.com/downloads/details.aspx?displaylang=ru&FamilyID=734917d8-0663-4c26-89d0-2d00b632ebdb, для 64-разрядныой операционной системы - http://www.microsoft.com/downloads/details.aspx?FamilyID=75649781-1e3d-4000-a6ce-638fe694de02&displaylang=en.

**Задача№1**:

1. На компьютере с Windows XP запускаем файл wet7xp_x86.exe или wet7xp_x64.exe в зависимости от разрядности операционной системы.
2. Установка WET для Windows XP подобна установке обновлений. В окне приветствия жмем Далее.
3. Принимаем лицензионное соглашение и жмем Далее.
4. Установка WET для Windows XP подобна установке обновлений.
5. По окончании установки жмем Готово.

**Задача №2**:

1. Запускаем утилиту переноса данных. Она расположена в Пуск -> Все программы -> Средство переноса данных для Windows 7.
2. В первом окне жмем Далее.
3. Выбираем тип переноса – Внешний диск или USB-устройство флэш-памяти.
4. На следующем шаге выбираем – Это исходный компьютер.
5. Далее происходит сканирование компьютера. Выбираем необходимые данные напротив учетной записи. Также можно произвести дополнительные настройки нажатием ссылки Настройка. Жмем Далее.
6. На следующем шаге указываем пароль (123) и подтверждаем его. Жмем сохранить.
7. Указываем место для сохранения файла переноса (съемный носитель). Жмем Сохранить.
8. В окне с подтверждением об успешном сохранении файлов жмем Далее.
9. В окне с инструкцией по использованию средства переноса жмем Далее.
10. В завершение жмем Закрыть.

**Задача №3**:

1. Вставляем съемный носитель с файлом переноса данных.
2. Запускаем файл переноса.
3. В окне ввода пароля вводим 123. Жмем Далее.
4. Выбираем файлы для переноса и жмем Перенести.
5. В окне, подтверждающем успешный перенос файлов жмем Закрыть.

## Практическое занятие №11. Миграция состояния пользователя с созданием жестких ссылок

***Цель работы:***

Выполнить перенос пользовательских данных и настроек при помощи **жестких связей**

***Перенос пользовательских данных и настроек***

## USMT 4.0 и методы миграции

USMT – User State Migration Tools — многофункциональный набор приложений, позволяющих автоматизировать процесс переноса данных пользователя в корпоративной среде. Обладает большим количеством настроек, имеется возможность собственноручно создавать конфигурацию переносимых данных. Возможность переноса при помощи жестких связей (hardlink), повышающая скорость миграции в несколько раз.

Операционную систему Windows Vista с пакетом обновлений 1 (SP1) можно обновить до Windows 7, т.е. можно установить Windows 7 и сохранить прежние приложения, файлы и настройки, использовавшиеся в предыдущей версии Windows. Если вместо обновления решено установить Windows 7 независимо от Windows Vista, существующие приложения и настройки не будут сохранены. Личные файлы пользователя, а также все файлы и папки Windows будут перемещены в папку Windows.old. Данные в папке Windows.old становятся доступными после завершения установки Windows.

Если нужно выполнить обновление от Windows XP до Windows 7, необходимо выполнить выборочную установку Windows 7, а затем перенести нужные файлы и настройки из Windows XP. Средство переноса данных Windows (WET) позволит сохранить все файлы и настройки. Для переноса их можно скопировать на другой жесткий диск, сетевой ресурс или иное устройство хранения перед установкой Windows 7. После завершения установки средство переноса данных Windows загрузит файлы и настройки на обновленный компьютер. Затем понадобится заново установить приложения.

### Основные возможности и функции

Для автоматизации миграции при развертываниях операционной системы Windows 7 на большое количество компьютеров можно использовать мастер переноса файлов и параметров (User State Migration Tools).

**USMT (User State Migration Tools) – набор утилит, предназначенных для переноса пользовательских данным (личных файлов, настроек приложений), как с операционных систем Windows Vista и Windows 7, так и с более ранних, например Windows XP**.

USMT 4.0 использует XML-файлы настраиваемых правил миграции, обеспечивающих точное управление тем, какие учетные записи пользователей,

пользовательские файлы, настройки операционной системы и настройки приложений будут перенесены. В зависимости от того, какой способ миграции подходит вам больше всего, USMT можно использовать как для параллельных миграций, в которых выполняется замена оборудования, так и для поэтапных миграций (или миграций обновления), когда обновляется только операционная система.

При выполнении обновлений многоязыкового образа Windows USMT не поддерживает обновления между языками. При обновлении или переносе для операционной системы с несколькими установленными многоязыковыми пакетами выполнить обновление или перенос можно только на используемый по умолчанию язык пользовательского интерфейса системы.

При использовании одноязычного образа Windows, соответствующего используемому по умолчанию языку пользовательского интерфейса многоязыковой операционной системы, перенос будет выполнен. Однако все языковые пакеты будут удалены, и после завершения обновления понадобится их повторная установка.

Поддерживаемые операционные системы:

1. Сканирование файлов для переноса:
    - Windows XP Professional 32- или 64-разрядная версия
    - Windows Vista 32- или 64-разрядная версия
    - Windows 7 32- или 64-разрядная версия
2. Применение файлов для переноса:
    - Windows Vista 32- или 64-разрядная версия
    - Windows 7 32- или 64-разрядная версия

Поддерживается перенос данных с 32-разрядной на 64-разрядную и наоборот.

Для успешного переноса данных утилита должна запускаться пользователем, обладающим административными правами в Windows XP и в режиме администратора (Запуск от имени администратора) в Windows Vista и Windows 7. Применение перенесенных данных на новый (конечный) компьютер необходимо осуществлять после установки всех приложений, так как возможно будут перезаписаны настройки установленных приложений.

Состав USMT 4.0:

1. **ScanState.exe** – предназначена для резервного копирования пользовательских данных.
2. **LoadState.exe** – предназначена для восстановления (применения) пользовательских данных.

3. **XML файлы** – определение файлов для резервного копирования и восстановления.
4. **USMTUtils.exe** – используется для удаления локального хранилища миграции.

Важными отличиями от предыдущей версии данной утилиты являются:

- Возможность собирать настройки в "Offline" (не из действующей операционной системы).

  Например после того как на диск со старой операционной системой была установлена Windows Vista или Windows 7.

- Перенос данных и настроек путем создания жестких ссылок ( **hardlink** ) на файлы.

**Жесткая ссылка – ссылка на файл, которая в отличие от символьной ссылки (ярлык) указывает не на имя файла, а на его дескриптор,** (Дескриптор файла - это целое число без знака, с помощью которого процесс обращается к открытому файлу.Количество дескрипторов файлов, доступных процессу, ограничено параметром **/OPEN_MAX**, заданным в файле **sys/limits.h**.) **таким образом, над файлом можно производить различные действия, такие как переименование или удаление, пока не будет удалена последняя жесткая ссылка на файл, сам файл не будет удален из файловой системы**. Данная функция возможна только при установке операционной системы (Windows Vista или Windows 7) поверх старой (Windows XP) без форматирования диска. В этом случае папки старой операционной системы (Windows, Program Files, Document and Settings) переносятся в папку Windows.old. Оттуда утилита USMT, при миграции данных и настроек создает жесткие ссылки, а не производит процесс копирования, что занимает гораздо меньше времени и уменьшает нагрузку на диск.

- Перенос доменных пользователей без участия контроллера домена (Domain Controller).

  Теперь имеется возможность переносить учетные записи доменных пользователей между двумя компьютерами без участия контроллера домена. Основное условие – новый компьютер, перед переносом, должен быть включен в состав домена, т.е. являться его участником.

- Интеграция с SCCM и MDT.

  Благодаря интеграции USMT 4.0 с сервером SCCM и MDT процесс переноса данных значительно облегчился. После предварительных

настроек он осуществляется полностью автоматическим способом, не требуя участия администратора в своей работе.

- Поддержка теневого копирования (Volume Shadow Copy).

  Необходимо запустить scanstate.exe с параметров /vsc. Это означает, что можно осуществлять копирование файлов, открытых на редактирования другими приложениями, т.е. для успешно копирования файлов пропадает необходимость производить перезагрузку компьютера.

- Перенос пользователей в другую локальную группу безопасности.

  Новая возможность позволяет во время миграции пользовательских данных и настроек произвести перенос учетной записи пользователя и изменить его членство в локальной группе. Например, перенести пользователя из группы администраторы в группу пользователи.

- Возможность вывести список файлов, подверженных миграции.

  Перед началом переноса данных можно посмотреть список переносимых файлов. Для этого используется ключ /listfiles.

- Новая функция поддержки AES шифрования.

Сейчас мы разберем несколько сценариев переноса данных.

**Сценарий обновления операционной системы**

- **Обновление операционной системы и перенос данных с использованием жестких ссылок**:
  1. Утилита сканирования запускается с ключом /hardlink, тем самым создается хранилище данных.
  2. Удаляется старая операционная система и все приложения.
  3. Устанавливается новая операционная система (без форматирования дисков), приложения и драйверы.
  4. Запускается процедура применения данных.
- **Обновление операционной системы и перенос данных с использованием папки Windows.old и жестких ссылок**:
  1. На старый компьютер устанавливается новая операционная система. Форматирование дисков не производится. Необходимо убедиться, что во время установки старые данные будут перенесены в папку Windows.old. Далее устанавливаются необходимые приложения и драйверы.
  2. На компьютере поочередно запускаются утилиты сканирования и применения перенесенных данных с параметром /hardlink.

**Сценарий замены операционной системы**

- **Замена операционной системы и перенос данных с использованием сервера для хранения данных**:
    1. Сканирование запускается на каждом компьютере. Данные сохраняются на сервере в общей сетевой папке.
    2. На компьютере устанавливается новая операционная система (Windows Vista или Windows 7) набор необходимых приложений и драйверов.
    3. Запускается процедура применения сохраненных на первом шаге данных и настроек.
- **Автоматическая сетевая миграция данных и настроек**:
    1. На компьютере запускается утилита сканирования. Запуск осуществляется автоматически при помощи скриптов, bat-файлов, SCCM. Данные сохраняются на сервере.
    2. На компьютере устанавливается новая операционная система и набор приложений, в том числе и драйверы устройств.
    3. На новой операционной системе в автоматическом режиме запускается утилита применения файлов и настроек при помощи скриптов, bat-файлов, SCCM.
- **Оффлайн миграция с использованием Windows PE**:
    1. Компьютер запускается с загрузочного диска с средой предустановки Windows PE. Запускается утилита сканирования, данные сохраняются на внешний носитель или сервер.
    2. На компьютер устанавливается новая операционная система, приложений и драйверы.
    3. На новой операционной системе запускается процесс применения файлов и настроек.

**Этапы миграции**

Разобравшись с основными возможностями и сценариями миграции, выясним этапы, пройдя через которые, осуществляется непосредственно процесс переноса данных:

1. **Сбор информации** – сканирование системы на наличие файлов и настроек, доступных для переноса. Сканирование осуществляется на старом компьютере (компьютере доноре), при использовании сценария обновления – на том же компьютере. Утилита для сканирования системы – scanstate.exe. Для просмотра потенциальных файлов переноса необходимо запустить scanstate.exe с параметром /listfiles.
2. **Создание хранилища** – это непосредственный перенос файлов для временного хранения. Для примера, хранилищем может служить общая сетевая папка на сервере, на которую имеется права на запись. Если

миграция происходит при сценарии обновления, то хранилищем является, к примеру, папка Windows.old.

3. **Применение настроек из хранилища** – перенос файлов и настроек на новый компьютер. Для применения файлов и настроек используется утилита loadstate.exe. При использовании сценария миграции к файлам, расположенным, к примеру, в папке Windows.old создаются жесткие ссылки, значительно уменьшающие время переноса. Для этого используется ключ /hardlink. Если хранилище расположено на сервере, то происходит физический перенос данных. В зависимости от объема переносимых данных, этот процесс может занимать достаточно длительное время.

Итак, каким же образом происходит миграция пользовательских данных и настроек? Чтобы ответить на этот вопрос, необходимо разобрать ключи, которые можно передать утилитам scanstate и loadstate. Если установка Windows WAIK произведена в папку по умолчанию, то эти утилиты будут расположены по адресу **C:\Program Files\Windows AIK\Tools\USMT**. В папке USMT расположены еще 2 папки x86 и amd64. Утилиты, расположенные в них, предназначены для запуска на 32-разрядной и 64-разрядной операционной системе соответственно.

**Конфигурирование утилит USMT**

Перед тем как производить миграцию, необходимо познакомиться с некоторыми моментами и знать:

1. Где хранится конфигурация переносимых данных? Как утилиты USMT узнают, какие пользовательские данные переносить?
2. Ключи, с которыми запускаются утилиты USMT.

Для начала разберемся, где хранится информация, о файлах и параметрах, которые необходимо перенести. Данная информация хранится в XML файлах настроек:

1. **MigApp.xml** – содержит параметры для переноса приложений.
2. **MigDocs.xml** – инициализирует **MigXmlHelper.GenerateDocPatterns** для автоматического поиска пользовательских документов без необходимости непосредственного участия конечного пользователя.
3. **MigUser.xml** – описывает правила для миграции пользовательских профилей и данных.

**MigUser.xml** не переносит данные если:

1. Файлы расположены вне пользовательского профиля и их расширения не соответствуют расширениям перечисленным в **MigUser.xml**.

2. Список контроля доступа (ACL) на папки, расположенные вне пользовательских профилях.

Особенности переноса данных при использовании **MigUser.xml**:

1. Расширения файлов: .accdb, .ch3, .csv, .dif, .doc*, .dot*, .dqy, .iqy, .mcw, .mdb*, .mpp, .one*, .oqy, .or6, .pot*, .ppa, .pps*, .ppt*, .pre, .pst, .pub, .qdf, .qel, .qph, .qsd, .rqy, .rtf, .scd, .sh3, .slk, .txt, .vl*, .vsd, .wk*, .wpd, .wps, .wq1, .wri, .xl*, .xla, .xlb, .xls*.
2. Папки из пользовательских профилей: Мои документы, Мое видео, Моя музыка, Мои картинки, файлы с рабочего стола, Меню Пуск, ярлыки быстрого запуска приложений и избранное.
3. Папки профилей All Users и Public: данные переносятся из профиля All Users в Windows XP и профиля Public в Windows Vista и Windows 7.

При использовании **MigApp.xml** переносятся настройки следующих приложений:

- Adobe Acrobat Reader 9
- AOL Instant Messenger 6.8
- Apple iTunes 7, 8
- Apple QuickTime Player 7
- Apple Safari 3.1.2
- Google Chrome beta
- Google Picasa 3
- Google Talk beta
- IBM Lotus 1-2-3 9.8
- IBM Lotus Notes 8
- IBM Lotus Organizer 9.8
- IBM Lotus WordPro 9.8
- Mozilla Firefox 3
- Microsoft Office Access 2003, 2007
- Microsoft Office Excel 2003, 2007
- Microsoft Office FrontPage 2003, 2007
- Microsoft Office OneNote 2003, 2007
- Microsoft Office Outlook 2003, 2007
- Microsoft Office PowerPoint 2003, 2007
- Microsoft Office Publisher 2003, 2007
- Microsoft Office Word 2003, 2007
- Opera Software Opera 9.5
- Microsoft Outlook Express (только файл mail.box)
- Microsoft Project 2003, 2007
- Microsoft Office Visio® 2003, 2007
- RealPlayer Basic 11

- Skype 3.8

Более полный список можно посмотреть в файле USMT.chm входящий в состав утилиты WAIK 2.0.

Разобравшись с конфигурационными файлами переноса, выясним ключи используемые утилитами USMT. Для этого необходимо воспользоваться справкой прилагаемой к каждой утилите.

**Ключи утилит USMT**

Основные ключи ScanState.exe:

- StorePath – путь до папки хранилища данных. Нельзя использовать путь **C:**.
- /o – указывает утилите scanstate перезаписывать данные в хранилище и конфигурации config.xml. Если не указать этот параметр, то при выполнении записи в существующее хранилище приложение завершится с ошибкой.
- /vsc – означает использовать теневое копирование.
- /nocompress – отключает сжатие данных.
- /hardlink – указывает использовать жесткие связи. Для своей работы требует ключ /nocompress.
- /offlinedir:path – указывает путь до windows папки. Это может быть папка windows.old или папка windows, если произведена загрузка с Windows PE.
- /i:file – указывать файлы настроек для миграции (MigApp.xml, MigUser.xml или любые другой/другие пользовательские .xml файлы).
- /genconfig:FileName – генерирует конфигурационный .xml файл. Используется с ключом /config. Пример, scanstate /i:migapp.xml /i:miguser.xml /genconfig:config.xml
- /config:FileName – указывает файл конфигурации (config.xml) для создания хранилища данных. Пример, scanstate \\fileserver\migration\mystore /config:config.xml /i:miguser.xml /i:migapp.xml
- /auto:path to script files – эквивалент командам /i:MigDocs.xml /i:MigApp.xml /v:13.
- /localonly – указывает переносить данные, расположенные на локальном компьютере.
- /listfiles:FileName – создает текстовый файл, в котором перечислены файлы для переноса.
- /c – указывает утилите продолжать работать без остановки, если не появилась фатальная ошибка. Прочие ошибки записываются в лог.
- /all – мигрирует всех пользователей данного компьютера.
- /ui:DomainName\UserName (localusername) – мигрирует только указанных пользователей.

- /ue:DomainName\UserName – мигрирует пользователей, за исключением перечисленных в этом параметре. Нельзя использовать совместно с ключом /all. В имени пользователя можно использовать (*), заменяющего любой символ/символы.
- /encrypt – шифрует информацию, переносимую в хранилище данных. Ключ передается при помощи параметров: /key:KeyString или /key:"Key String" или /keyfile:[Path\]FileName

Ключи программы loadstate аналогичны ключам scanstate. Дополнительные ключи LoadState.exe:

- /md:OldDomain:NewDomain – миграция компьютера из старого домена (рабочей группы) в новый домен.
- /mu:OldDomain\OldUserName:[NewDomain\]NewUserName – миграция пользователя из старого домена (локального компьютера) в новый домен.
- /lac:[Password] – позволяет создать пользователя в процессе миграции.
- /lae – включает учетную запись пользователя, созданную при помощи ключа /lac.
- /decrypt – расшифровывает информацию в хранилище данных при помощи указанного ключа.

Основные ключи USMTUtils.exe:

- /ec – отображает поддерживаемые алгоритмы шифрования.
- /rd <storeDir> - удаляет хранилище данных.

За дополнительной информацией обращайтесь к Руководству пользователя USMT 4.0 (usmt.chm), устанавливаемой совместно с WAIK.

**Задание.** Выполнить миграцию пользовательских данных и настроек при помощи утилиты User State Migration Tools.

Обновление операционной системы и перенос данных с использованием папки Windows.old и жестких ссылок.

**Требования**:

1. 2 доступных клиентских компьютера (или виртуальные машины) и 1 сервер.
2. Дистрибутив Windows 7.
3. Дистрибутив Windows XP.
4. Дистрибутив продукта WAIK 2.0 или набор утилит USMT 4.0.

**Выполнение работы**:

1. При необходимости устанавливаем операционную систему Windows XP на компьютер.
2. Устанавливаем необходимые приложения (Office 2007 или любая другая версия).
3. Добавляем пользователя usr1 (Пуск -> Выполнить -> cmd -> net user usr1 1234567 /add). Таким же образом добавляем пользователя usr2 с паролем 1234567. Теперь у нас 3 пользователя Администратор, usr1 и usr2.
4. Под пользователем Администратор на рабочем столе создаем текстовый документ doc1.doc. В котором пишем: "Этот документ расположен на рабочем столе пользователя Администратор".
5. Заходим в папку Мои документы (пользователя администратор). Создаем документ doc2.doc, в котором пишем: "Этот документ расположен в Моих документах пользователя Администратор".
6. Заходим на диск C:\ и создаем документ doc3.doc, в котором пишем: "Этот документ расположен в корне диска C:\".
7. Заходим под пользователем usr1 (пароль 1234567) и создаем на рабочем столе документ doc4.doc с текстом: "Этот документ расположен на рабочем столе пользователя usr1".
8. Заходим в папку Мои документы и создаем файл doc5.doc. В нем пишем: "Этот документ расположен в папке Мои документы пользователя usr1".
9. Вставляем диск с операционной системой Windows 7.
10. Перезагружаем компьютер.
11. Производим запуск с установочного диска Windows 7.
12. Выбираем язык установщика (опционально).
13. Выбираем язык установки – Russian (Опционально).
14. Начинаем установку (Install Now).
15. Принимаем лицензионное соглашение. Далее.
16. Тип установки – пользовательский (custom).
17. Выбираем диск, на котором установлена операционная система Windows XP. Далее.
18. В окне предупреждения жмем Ок.
19. Дожидаемся установки операционной системы.
20. По окончании установки вводим имя пользователя usr2, имя компьютера usr2-PC. Далее.
21. Окно ввода пароля пропускаем.
22. Автоматическое обновление выключаем.
23. При необходимости указываем дату и время. Далее.
24. Указываем тип сети (опционально).
25. Устанавливаем все необходимые приложения.
26. Заходим на диск C:\ и замечаем, что документ doc3.doc не был удален.
27. Устанавливаем WAIK 2.0 или копируем папку USMT с любого компьютера с установленным WAIK 2.0. К примеру, копируем папку USMT на диск C:\.

28. Жмем Пуск -> В строке поиска пишем -> cmd -> На ярлыке cmd нажимаем правой кнопкой мыши и выбираем Запуск от имени администратора.
29. Переходим в каталог C:\USMT и подкаталог x86 (32-разрядная) или amd64 (64-разрядная) в зависимости от архитектуры текущей операционной системы. Например, cd C:\USMT\x86.
30. Вводи команду scanstate C:\hardlinkstore /offlinewinold:c:\windows.old\windows /nocompress /hardlink /auto жмем "Enter".
31. По окончании работы scanstate вводим команду loadstate C:\windows.old /auto /nocompress /hardlink
32. Делаем выход текущего пользователя (usr2) и заходим под учетной записью usr1. При первом входе, так как мы не задали пароль во время миграции, необходимо использовать пустой пароль, далее операционная система предлагает задать новый пароль. Вводим пароль 1234567
33. Повторяем его. Подтверждаем смену пароля. Совершаем вход.
34. Проверяем, что документы doc4.doc и doc5.doc успешно мигрировали.
35. Заходим под учетной записью администратор.
36. Проверяем документы doc1.doc и doc2.doc.
37. После успешной проверки необходимо удалить хранилище. Для этого открываем командную строку с помощью учетной записи администратор и вводим: C:\usmt\x86\usmtutils.exe /rd c:\store
38. После успешного удаления хранилища мы можем удалить папку windows.old

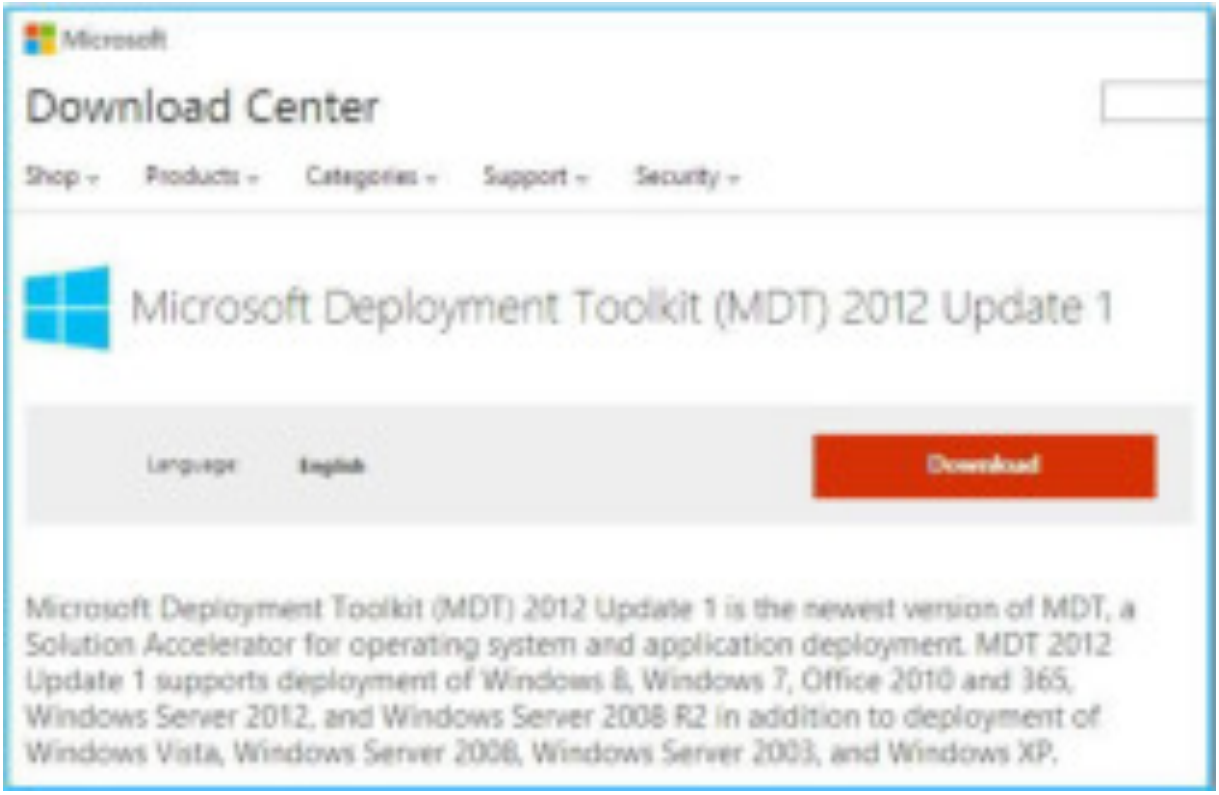
## Практическое занятие №12-13 Планирование и развертывание клиентских ОС с помощью MDT

***Цель работы:***
Установка Microsoft Deployment Toolkit (MDT) 2012 Update 1, создание папки развертывания, добавление ОС, приложений, языкового пакета

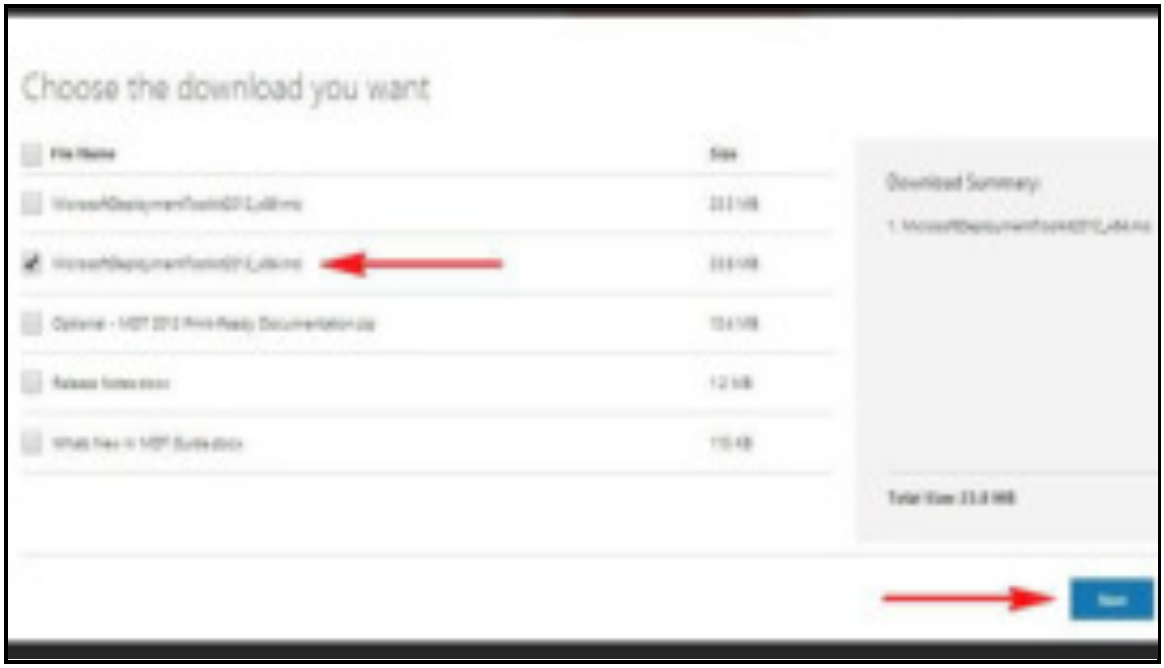
**Microsoft Deployment Toolkit (MDT) - это** новейшая версия набора инструментальных средств и предложений по автоматическому развертыванию операционных систем Microsoft. Данный пакет системные администраторы применяют для развертывания **операционных систем** начиная с Windows XP, Windows 7 и заканчивая Windows 8, Windows Server 2012 на компьютеры своей организации.

В этой работе мы установим пакет Microsoft Deployment Toolkit (MDT) 2012 Update 1, создадим папки развертывания, добавим ОС и приложения, языкового пакета.
произведём - Развертывание захваченного образа Windows 7 при помощи MDT 2012 Update 1.

1. Скачиваем пакет (MDT) 2012 Update 1 по ссылке
**http://www.microsoft.com/en-us/download/details.aspx?id=25175**

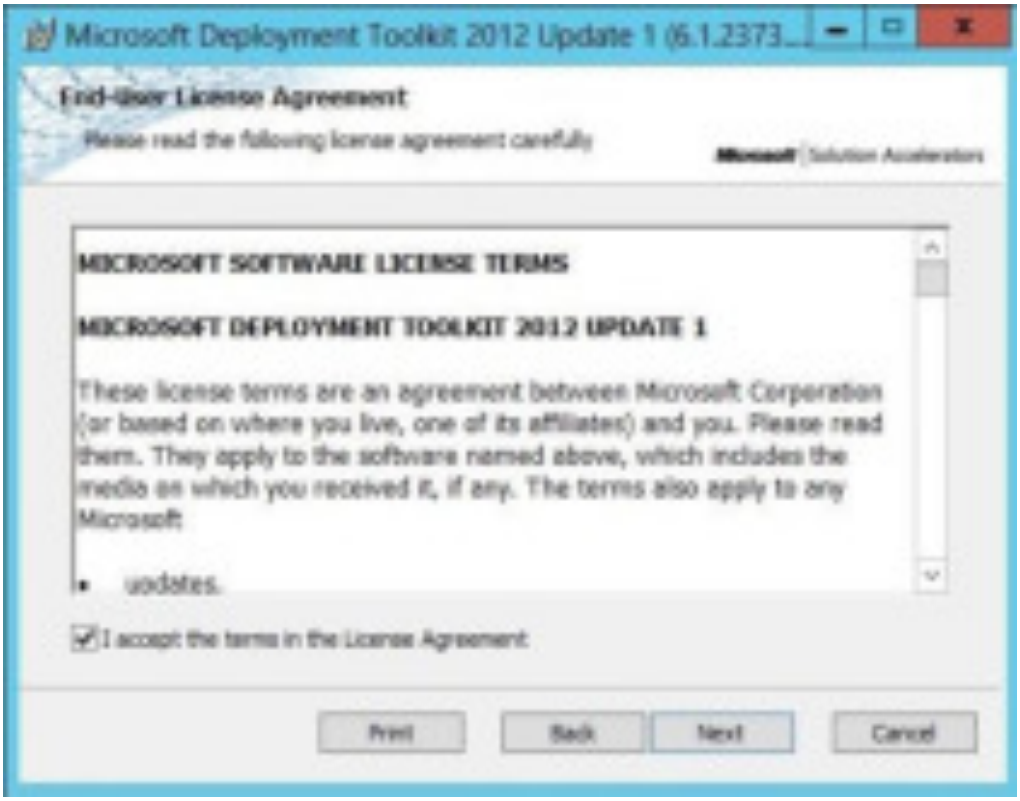



Так как в нашем случае пакет (MDT) 2012 Update 1 будет устанавливаться на Windows Server 2012, то выбираем 64 битную версию пакета.
MicrosoftDeploymentToolkit2012_x64.msi - 23.8 MB

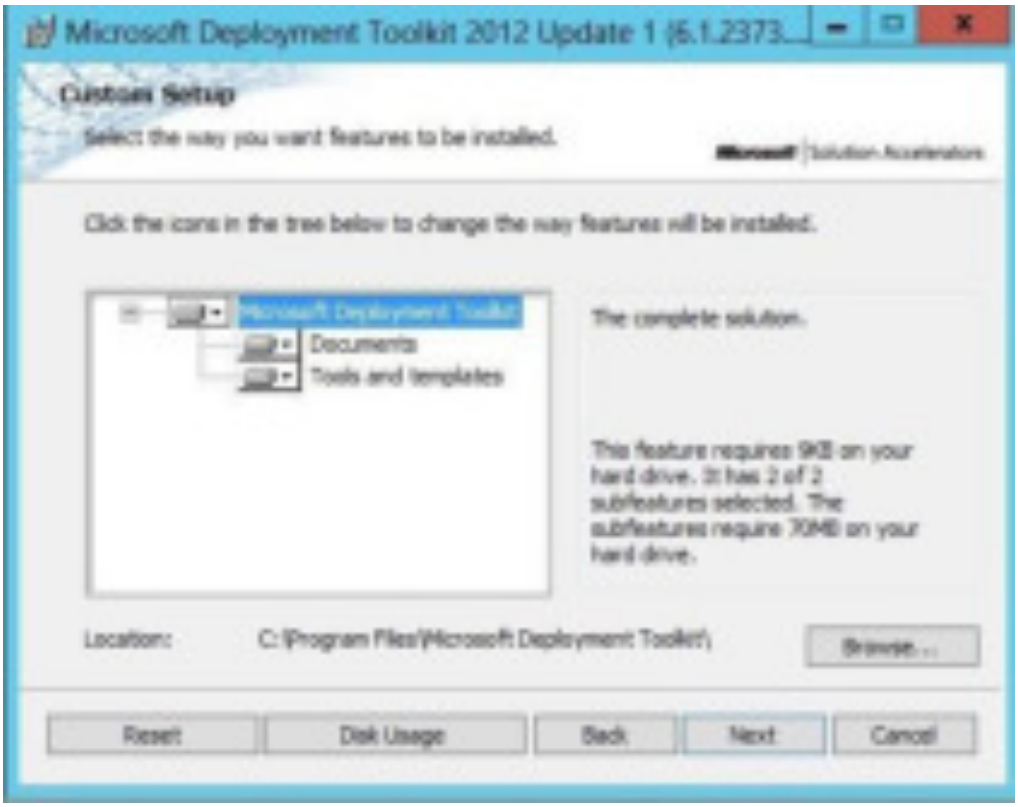



После скачивания производим его установку

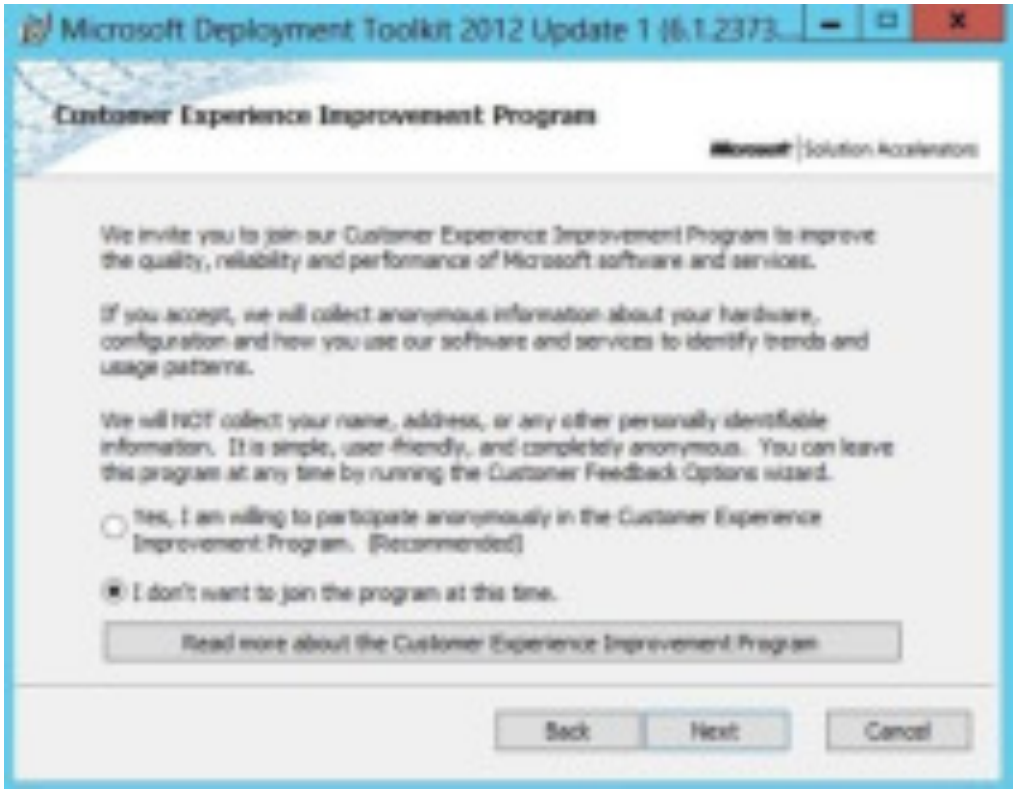

Соглашаемся с лицензионным соглашением



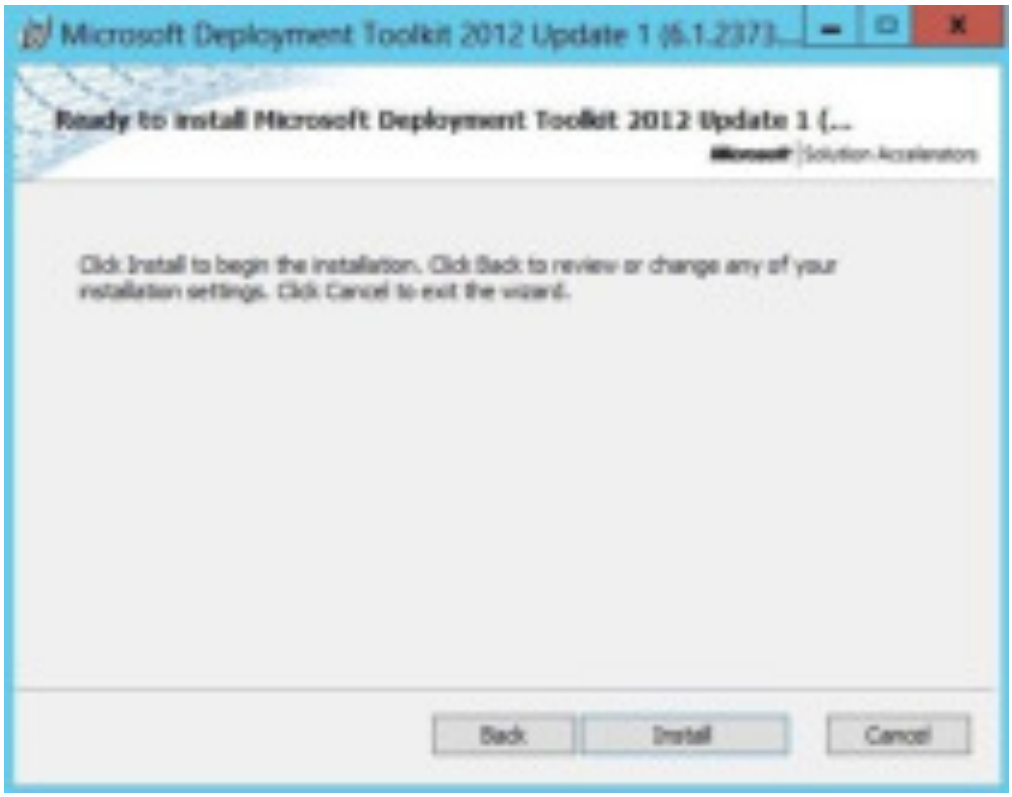

Далее



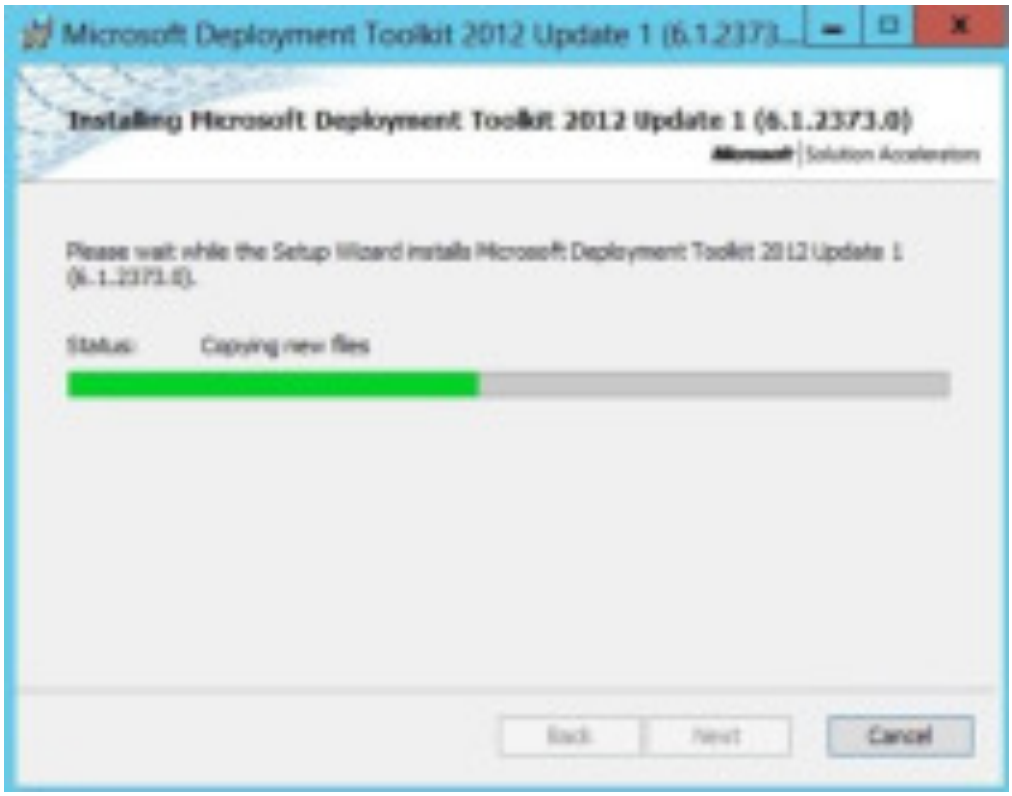

Далее



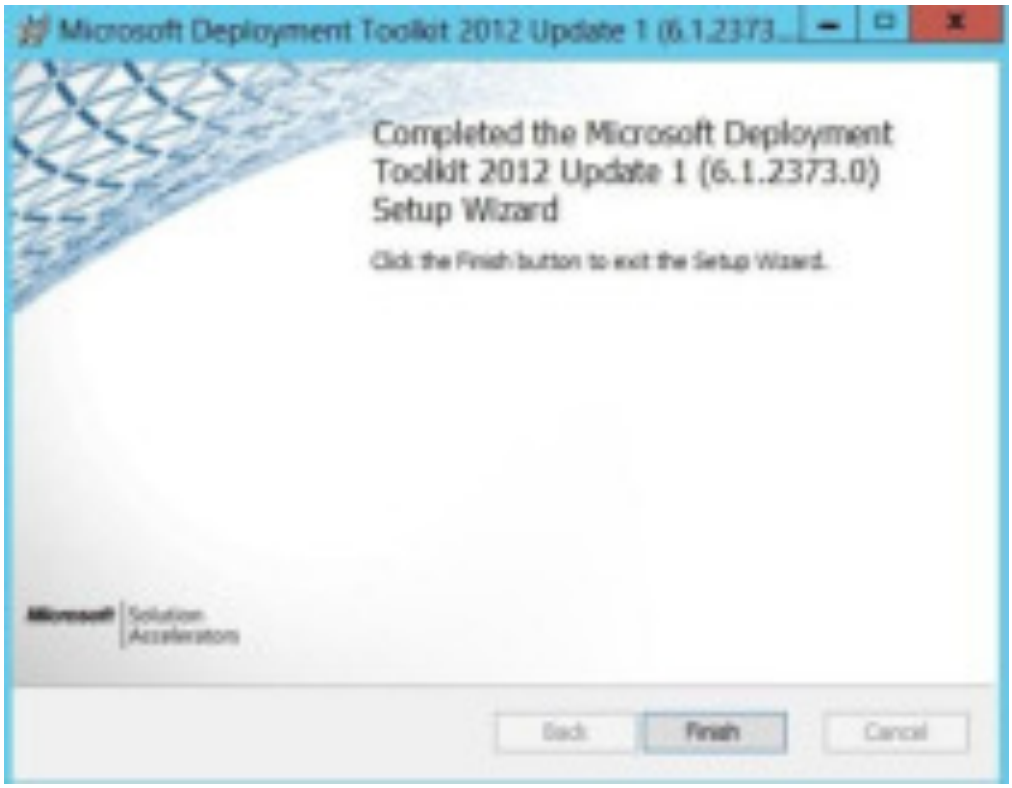

Начинаем установку



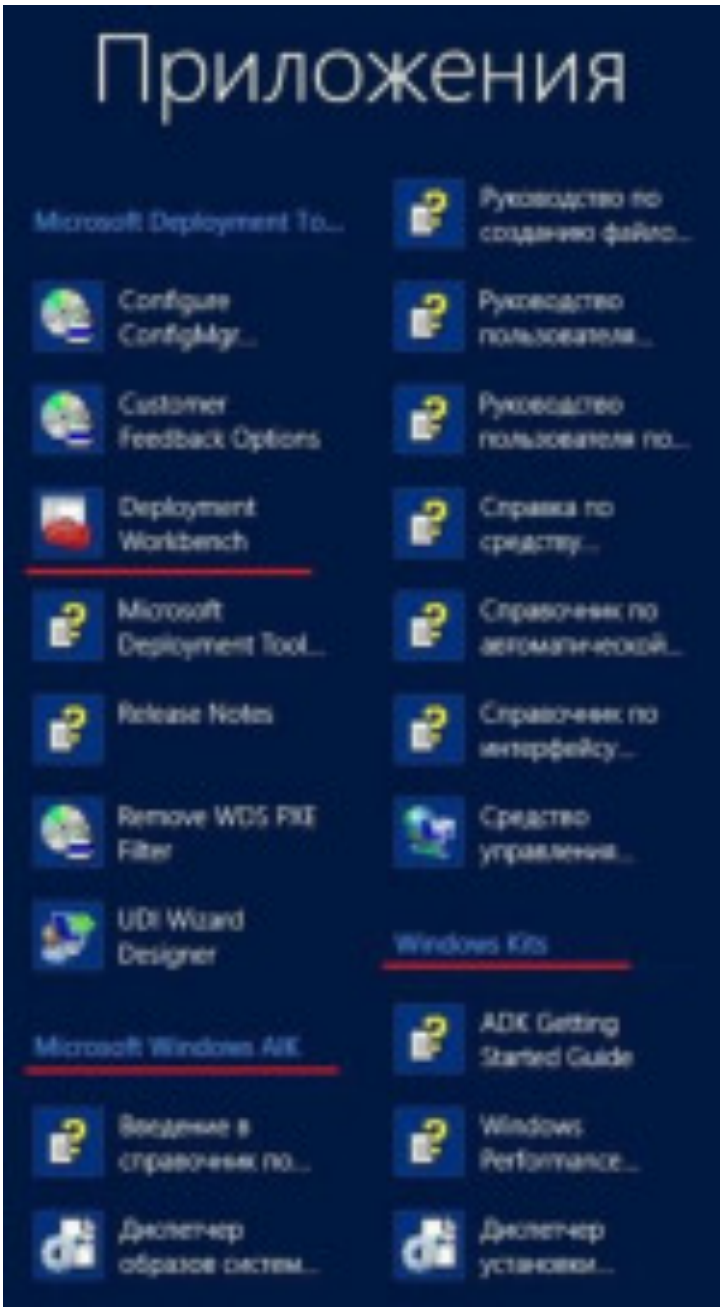

Идет установка



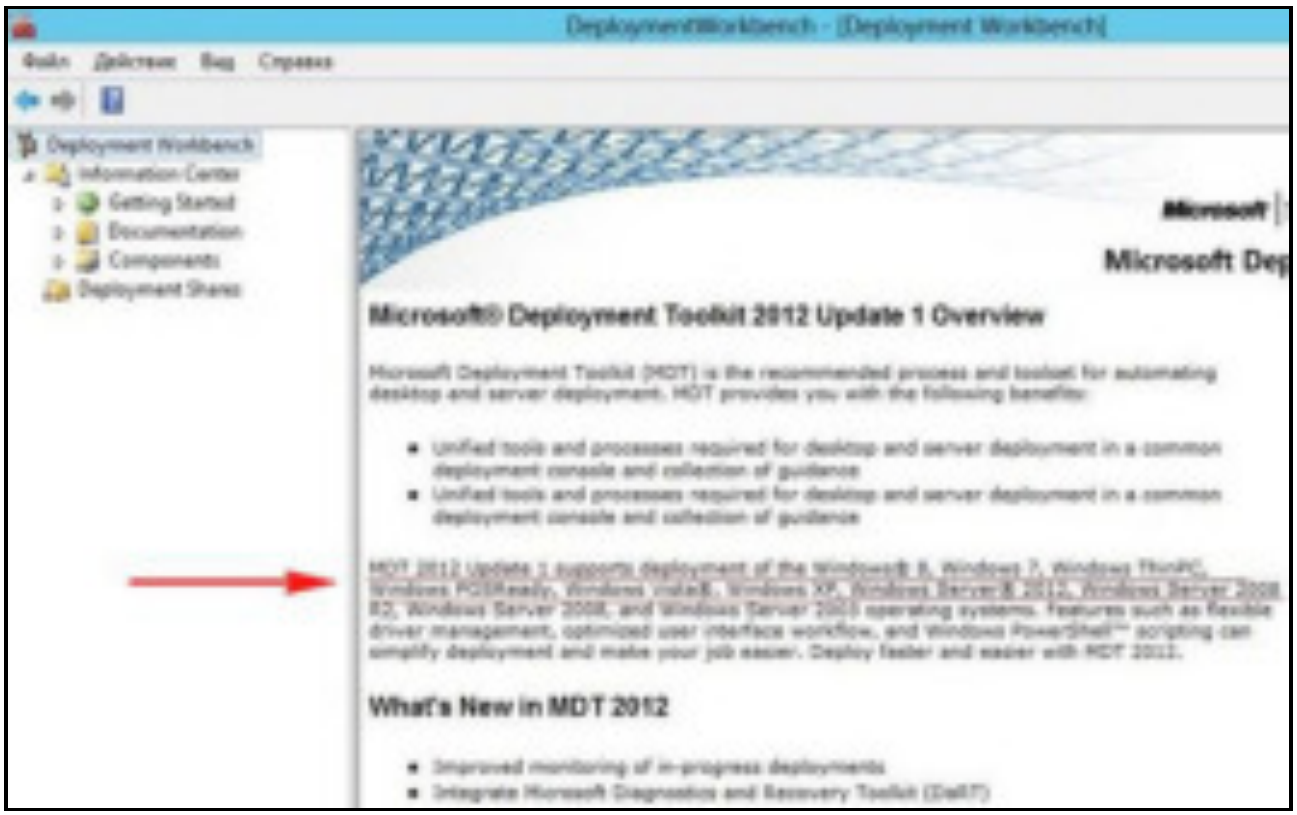

Установка завершена



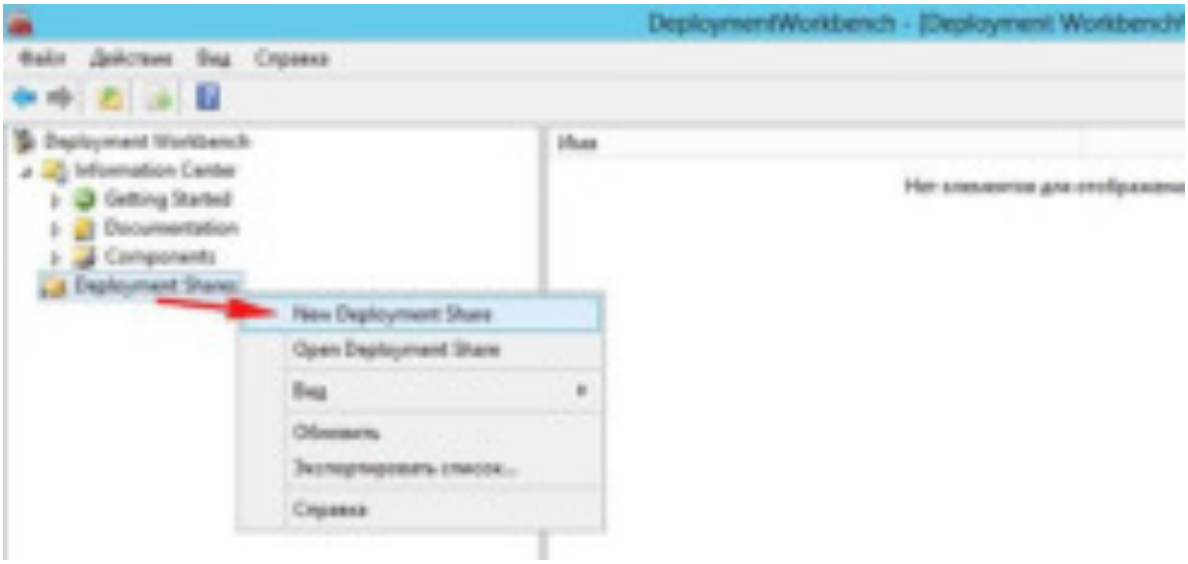

Нас интересует инструмент Deployment Workbench, для работы которого необходимо, чтобы на компьютере были установлены Windows AIK для Windows 7 и Windows ADK 8.0. Как видим, они у нас установлены. Запускаем  Deployment Workbench



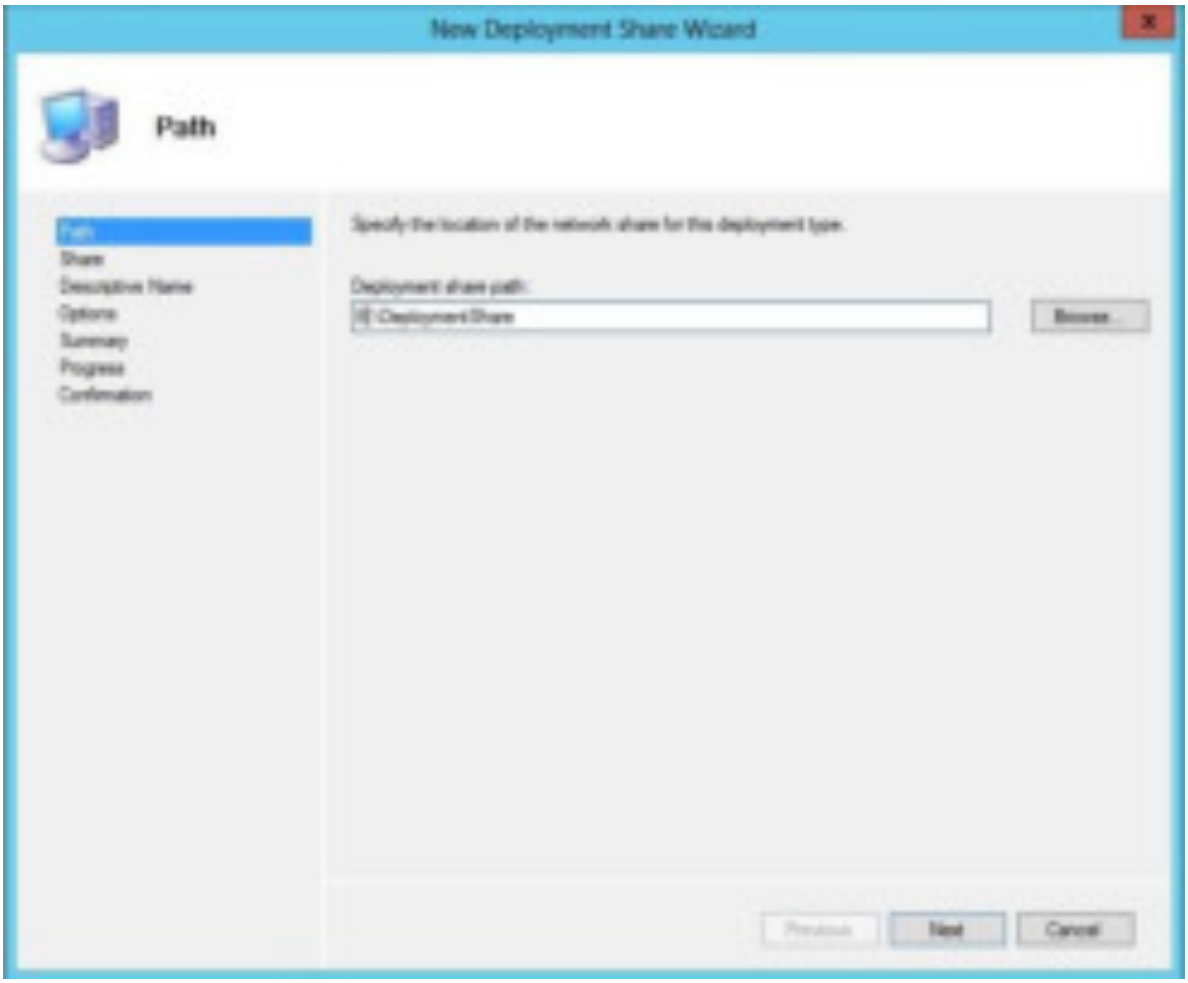

(MDT) 2012 Update 1 поддерживает развертывание операционных систем начиная с Windows XP и заканчивая Windows 8, Windows Server 2012



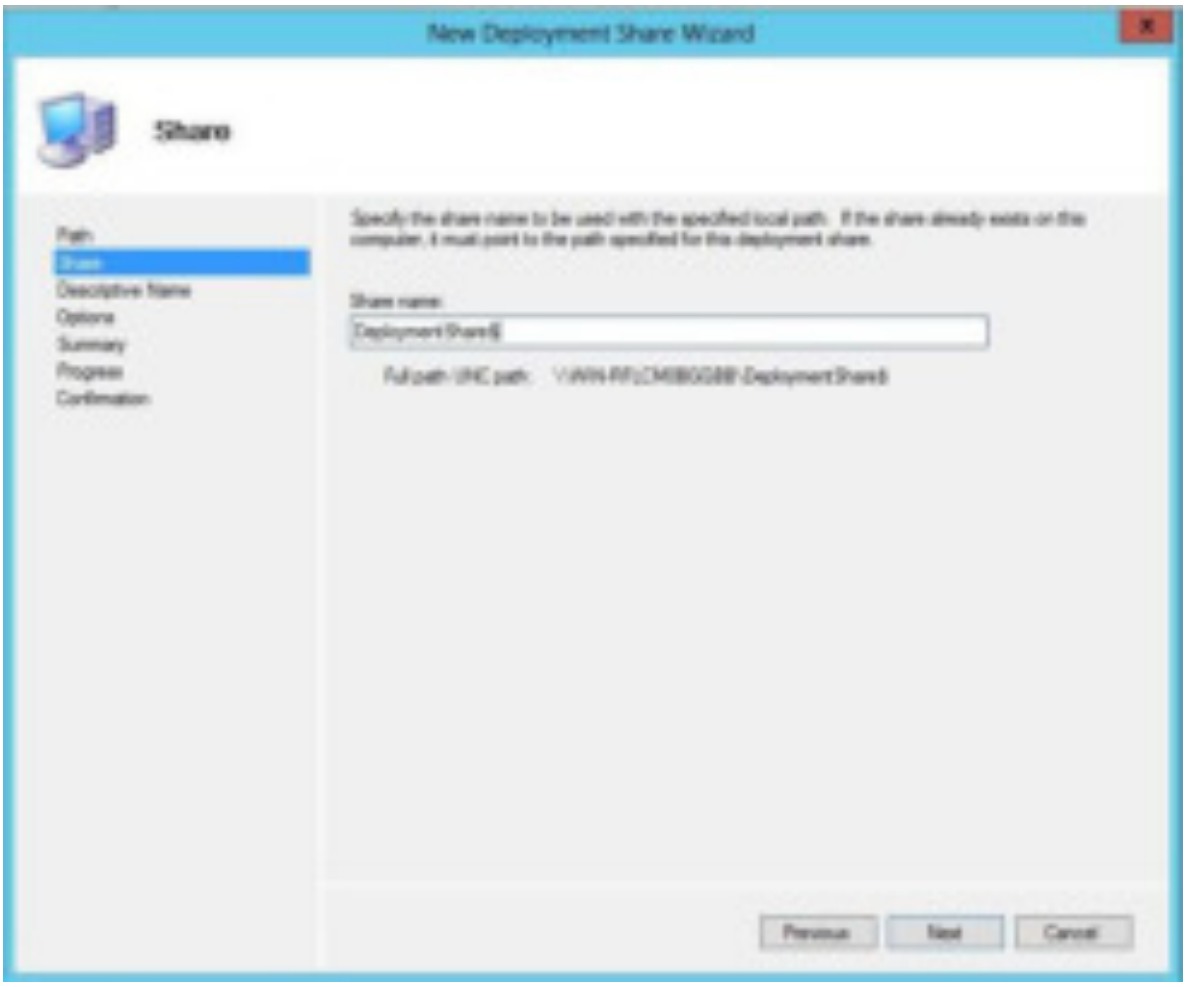

Щелкаем по DeploymentShares и выбираем New Deployment Share



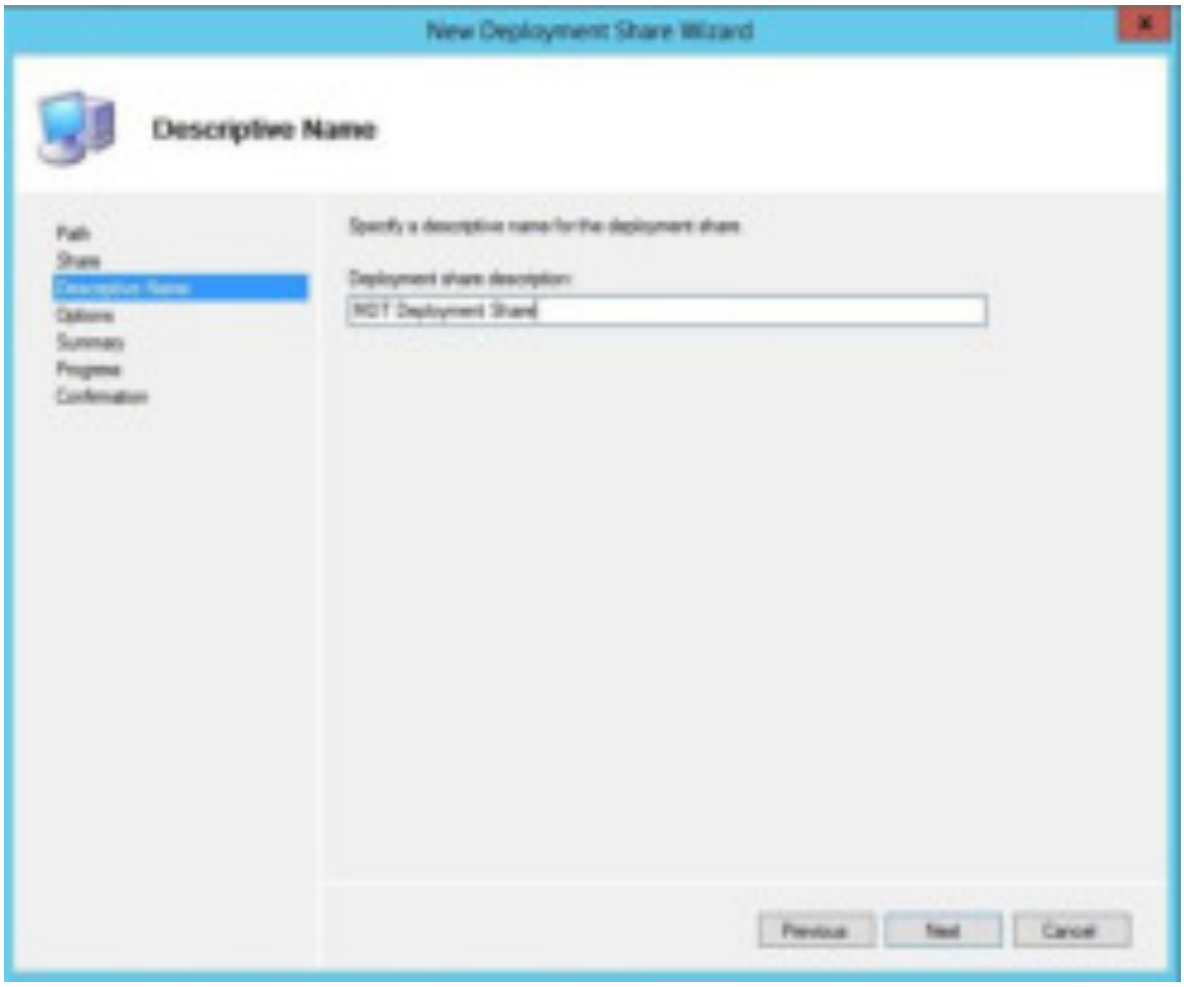

По умолчанию мастер предлагает создать папку развертывания на системном диске (что делать не рекомендуется) поэтому мы создадим ее на другом разделе жесткого диска, в нашем случае на разделе E:


New Deployment Share Wizard
Path
Path
Share
Descriptive Name
Options
Summary
Progress
Confirmation
Specify the location of the network share for this deployment type.
Deployment share path:
Deployment Share
Browse...
Previous
Next
Cancel

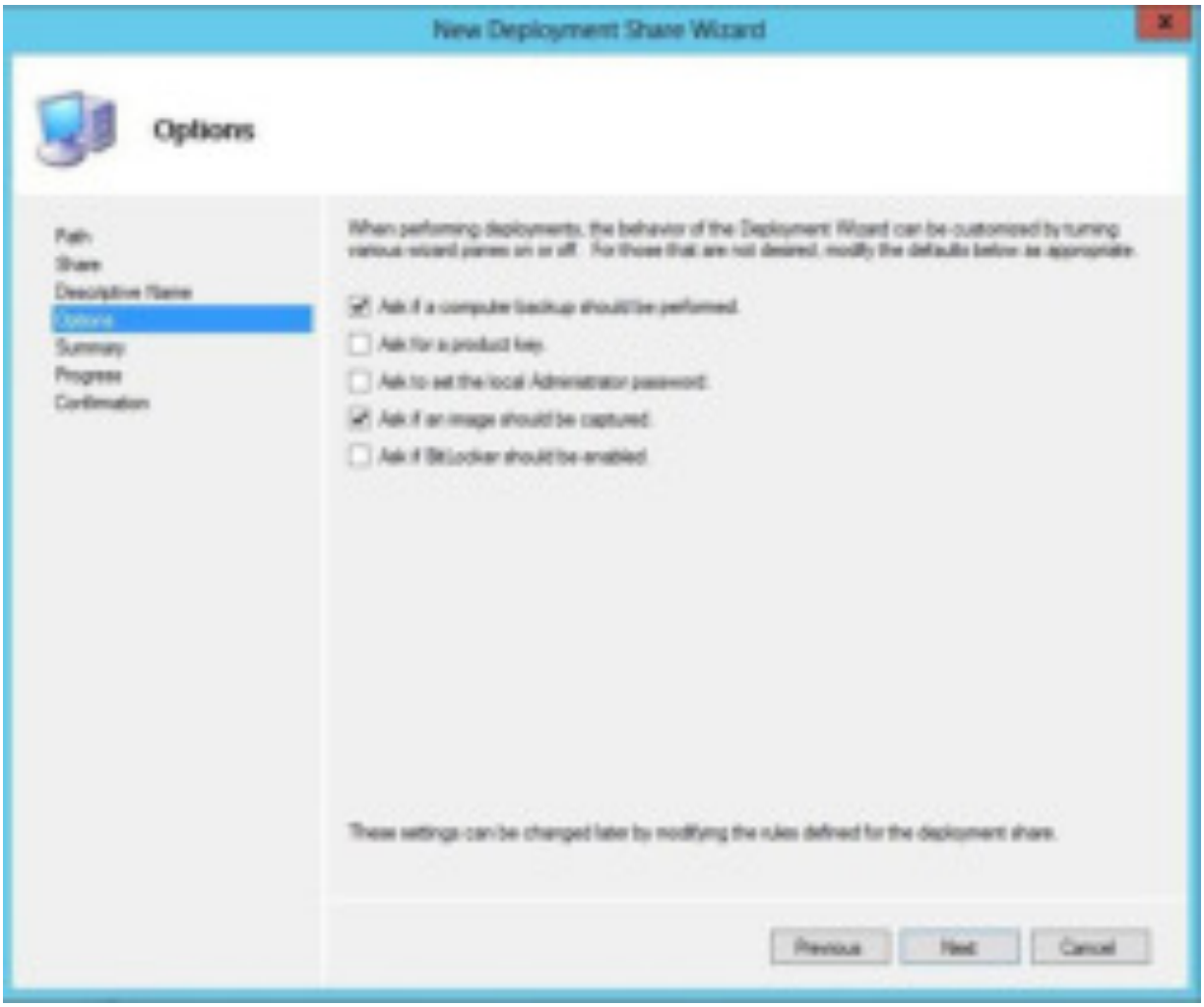
Далее


New Deployment Share Wizard
Share
Path
Share
Descriptive Name
Options
Summary
Progress
Confirmation
Share name:
Deployment Share$
Previous
Next
Cancel

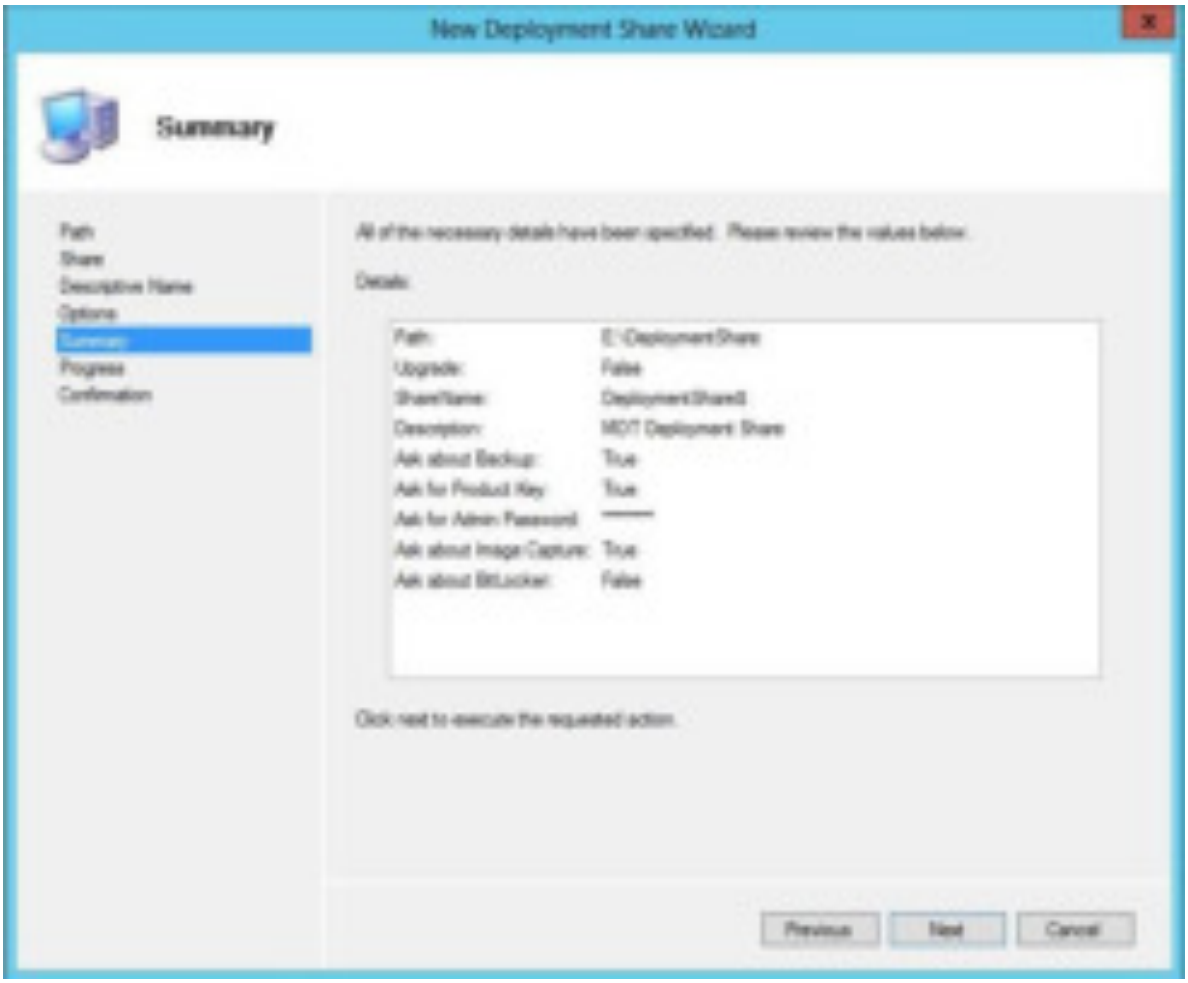
Далее



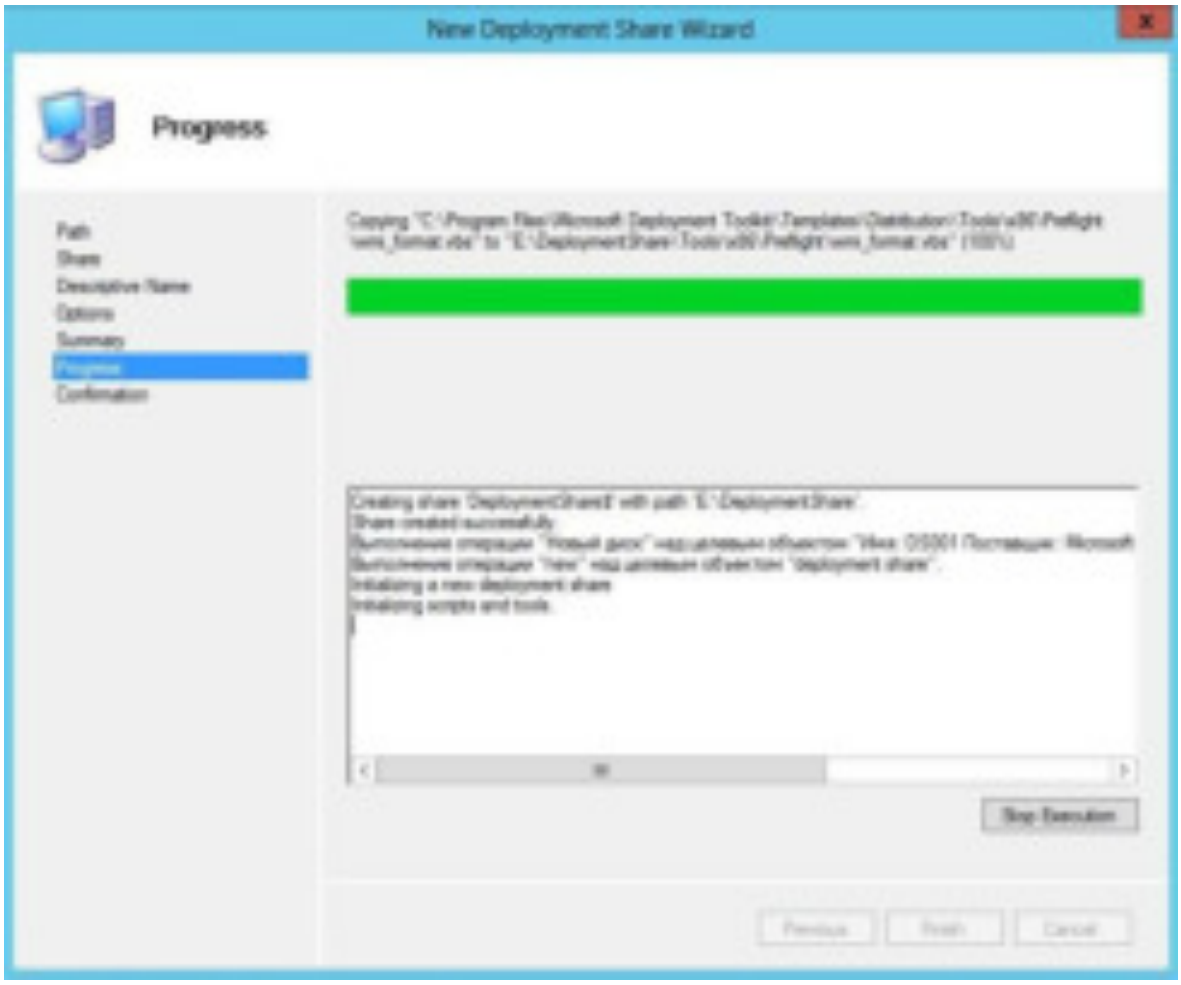

Выбираем параметры как на скриншоте. Далее


New Deployment Share Wizard
Options
Path
Share
Descriptive Name
Options
Summary
Progress
Confirmation
Ask if a computer backup should be performed.
Ask for a product key.
Ask to set the local Administrator password.
Ask if an image should be captured.
Ask if BitLocker should be enabled.
These settings can be changed later by modifying the rules defined for the deployment share.
Previous
Next
Cancel

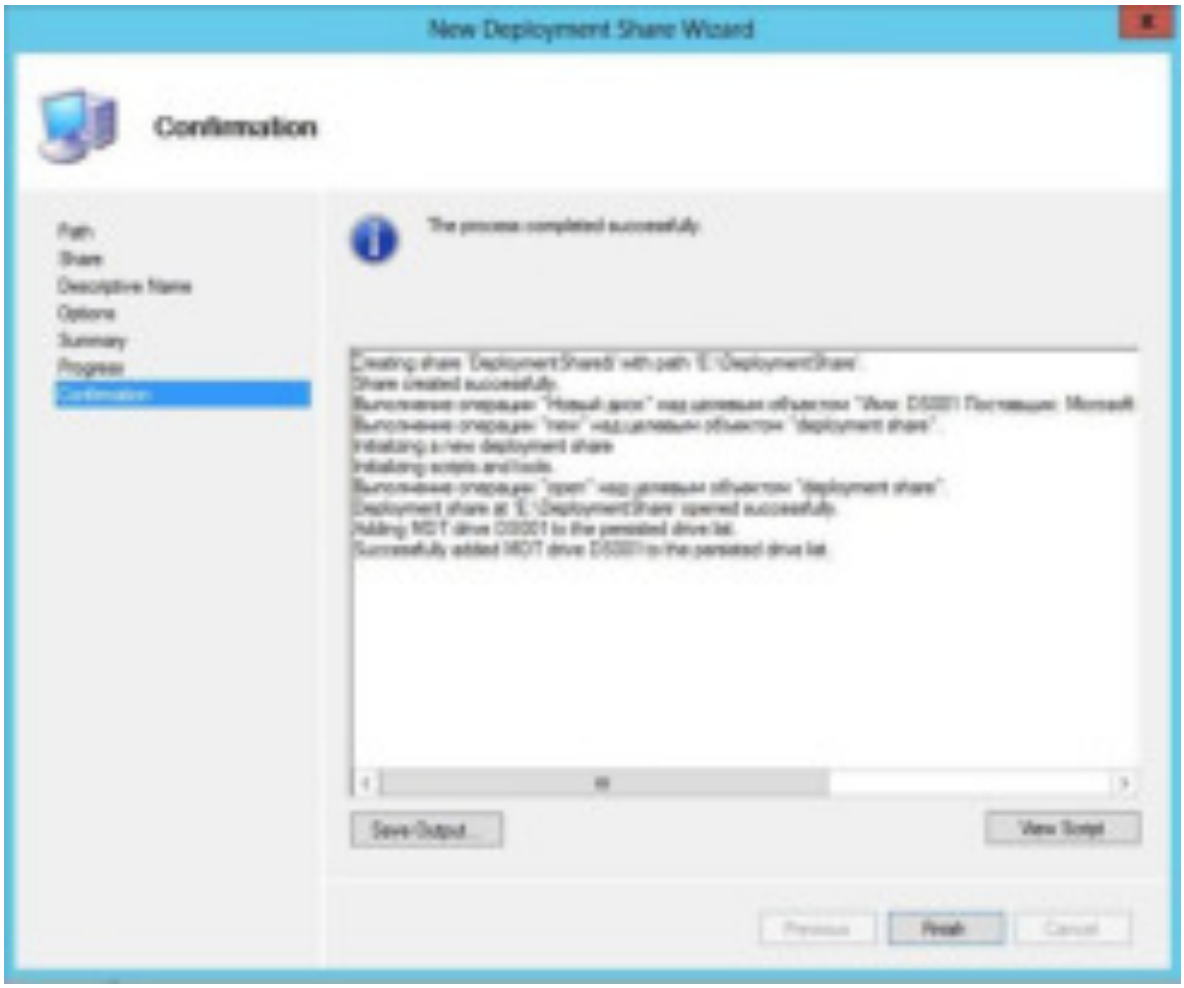
Далее



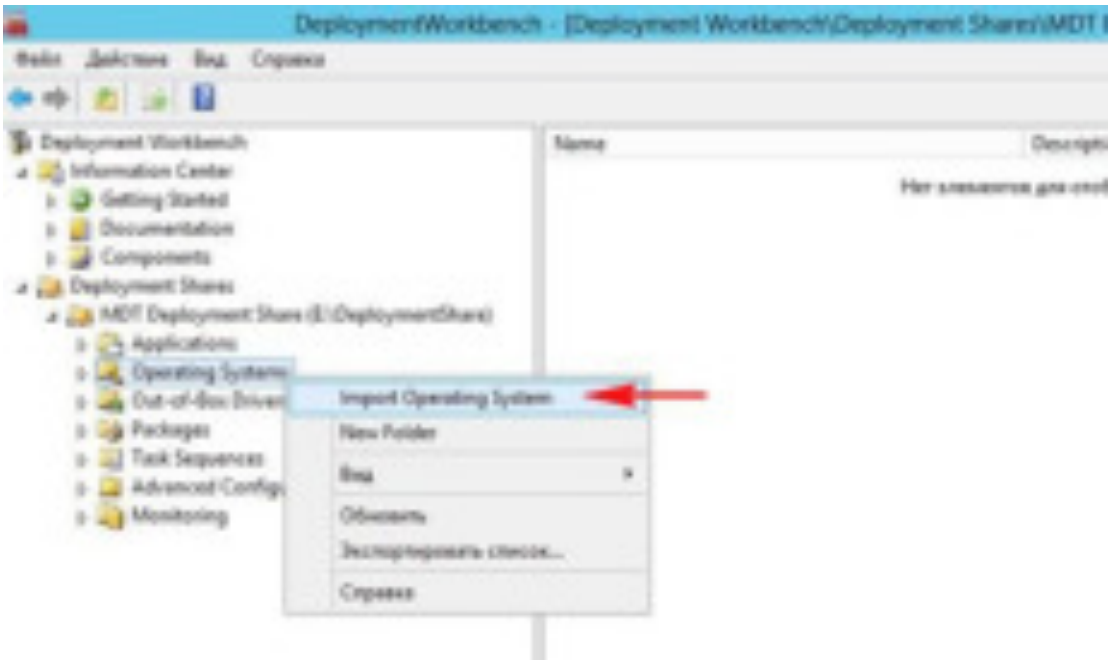

Идет процесс создания папки развертывания




Создание папки развертывания завершено

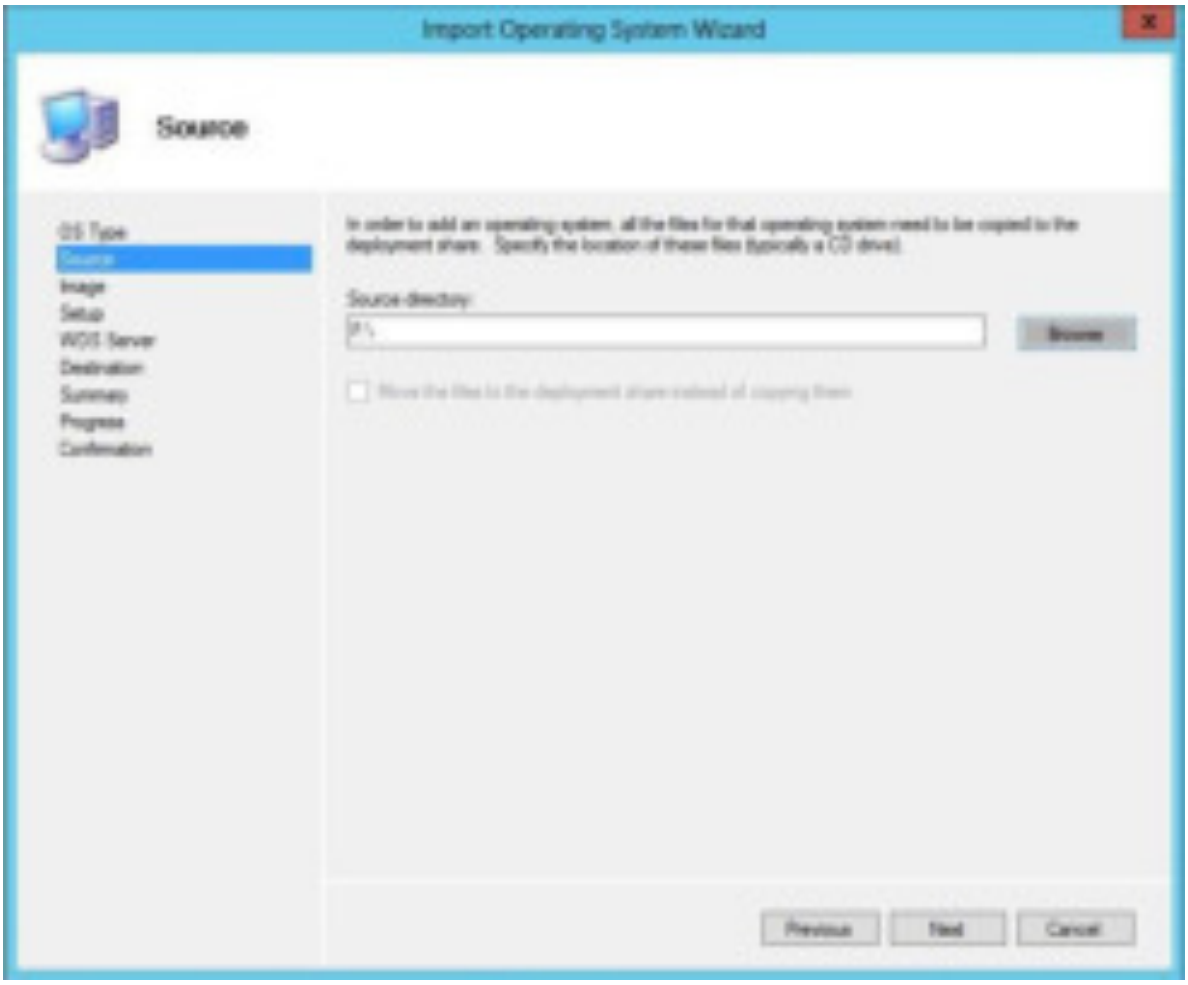


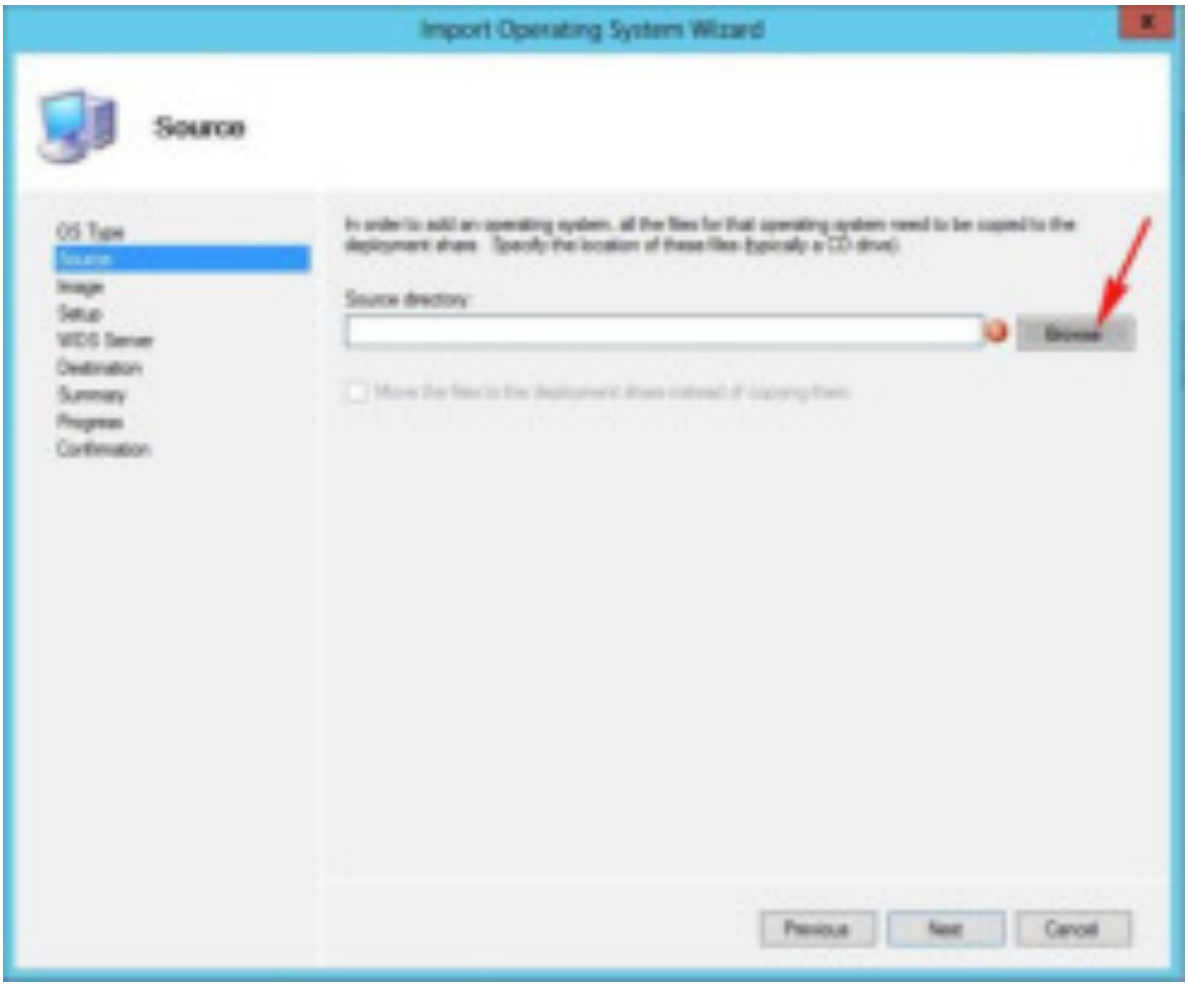

Появилась наша папка развертывания MDT Deployment Share. Разворачиваем ее и выбираем в списке папку Operating System, далее Import Operating System

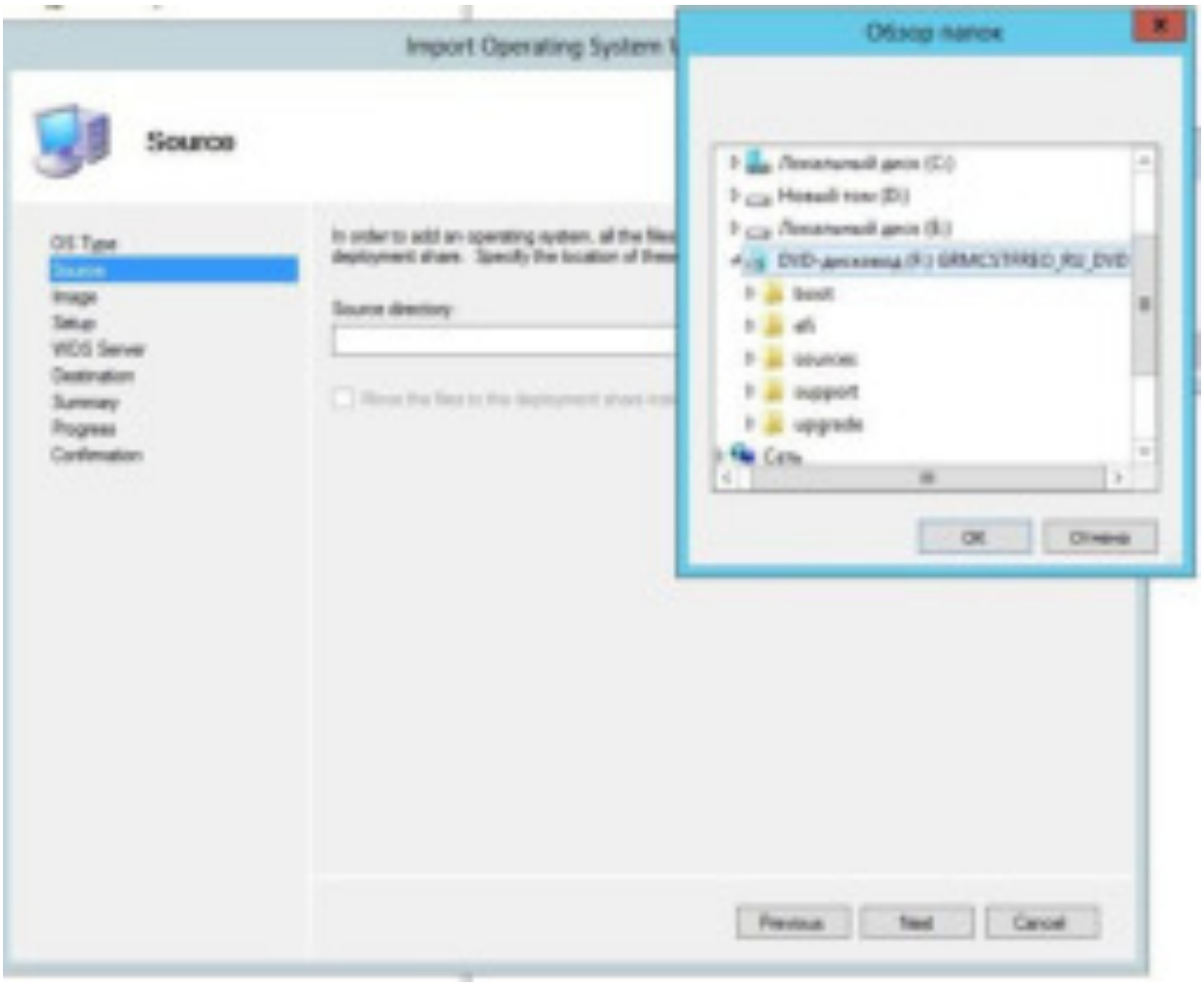


Доступны несколько вариантов добавления операционной системы в папку развертывания: это как добавить файлы напрямую с установочного диска, существует вариант с добавлением захваченного образа системы в формате wim, копирование установочного образа с сервера WDS. Выбираем первый вариант. Далее

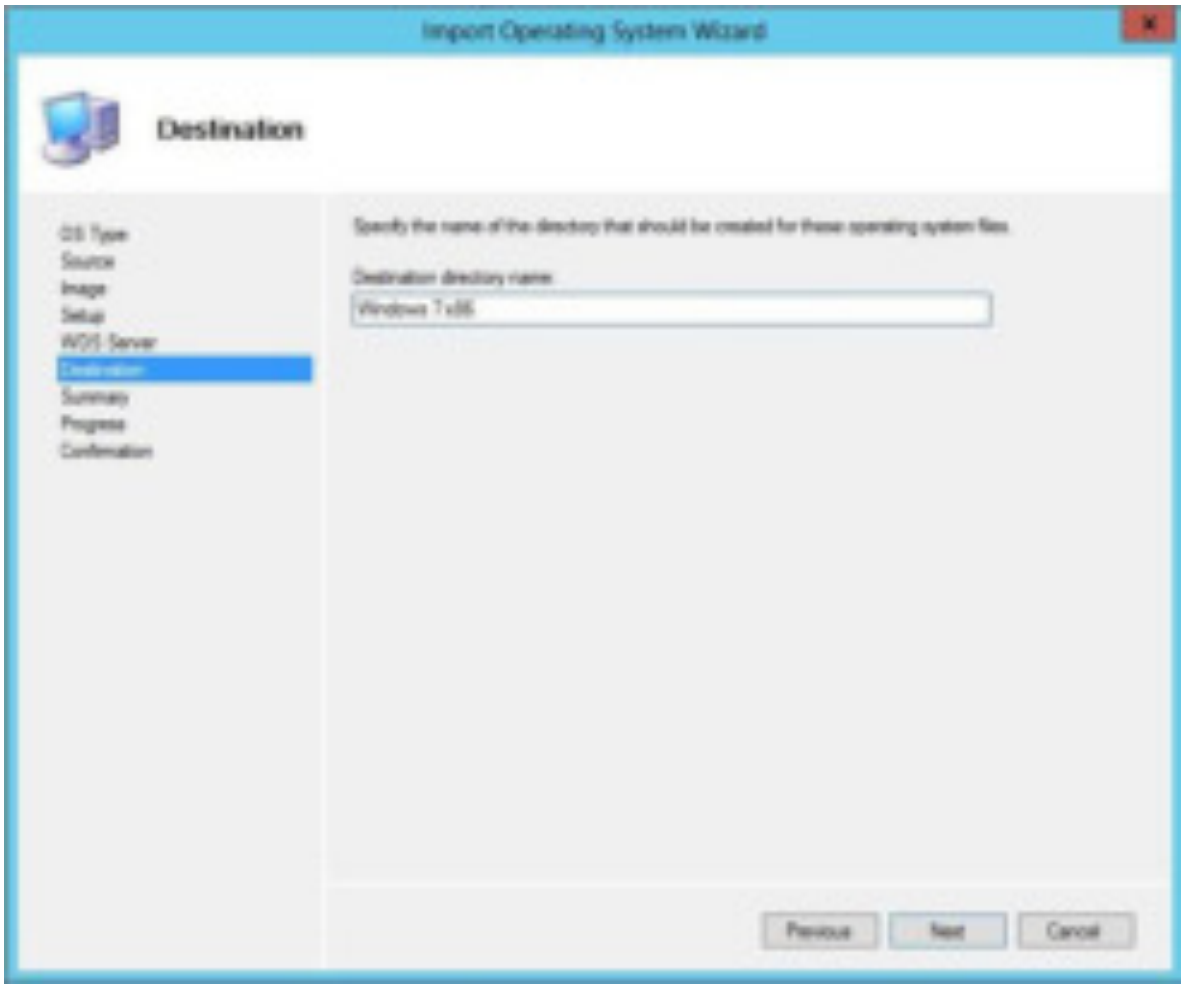

Выбираем расположение установочных файлов (в нашем случае они находятся на установочном диске)


Import Operating System Wizard
Source
OS Type
Source
Image
Setup
WDS Server
Destination
Summary
Progress
Confirmation
In order to add an operating system, all the files for that operating system need to be copied to the deployment share. Specify the location of these files (typically a CD drive).
Source directory:
Browse
Previous
Next
Cancel

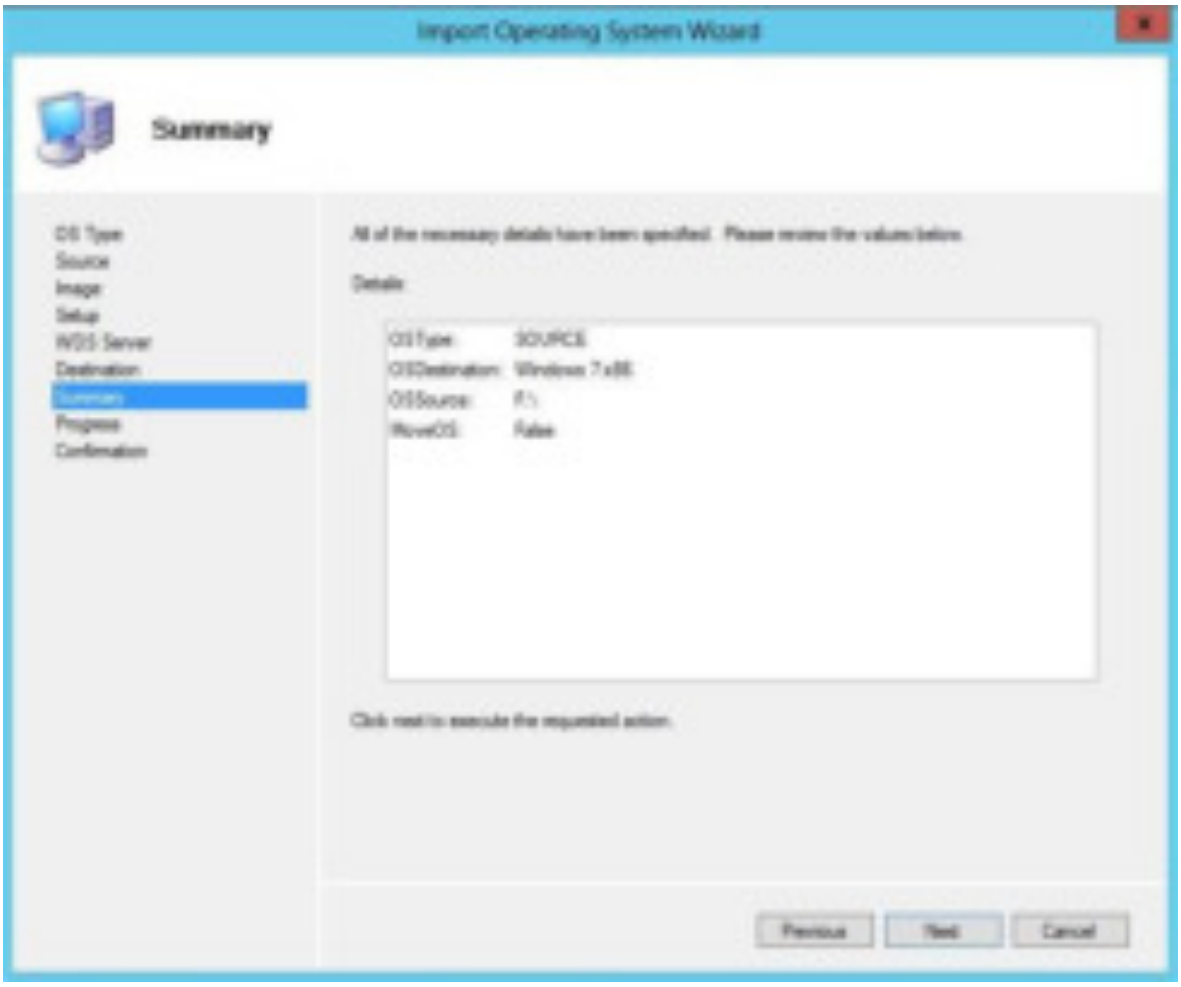

Import Operating System Wizard
Source
OS Type
Source
Image
Setup
WDS Server
Destination
Summary
Progress
Confirmation
Source directory:
Browse
Previous
Next
Cancel


Import Operating System
Sources
OS Type
Source
Image
Setup
WDS Server
Destination
Summary
Progress
Confirmation
Source directory
Previous
Next
Cancel
Обзор папок
Локальный диск (C:)
Новый том (D:)
Локальный диск (E:)
DVD-дисковод (F:) GRMCSVRRD_RU_DVD
boot
efi
sources
support
upgrade
Сеть
OK
Отмена

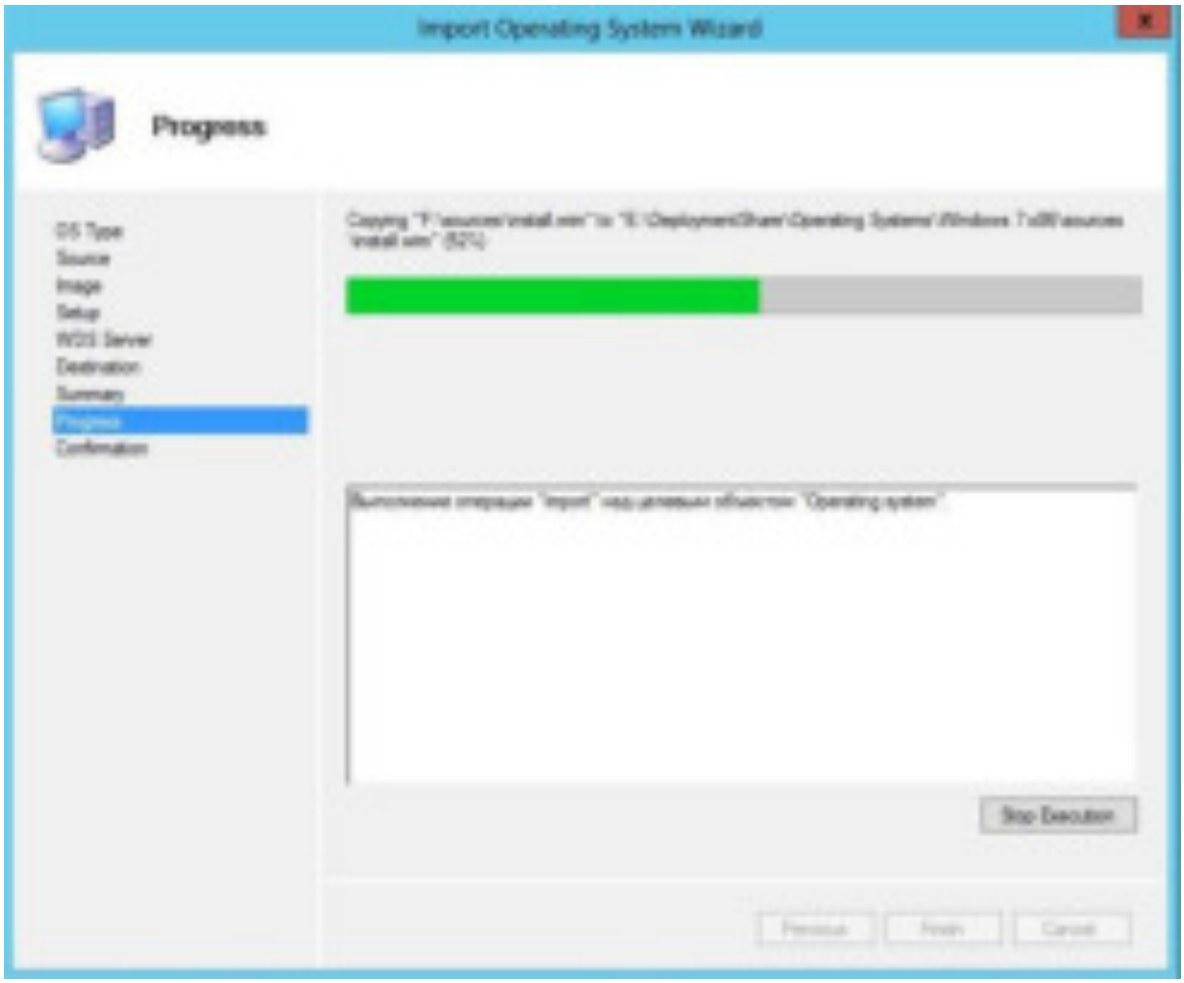
Далее


Import Operating System Wizard
Destination
OS Type
Source
Image
Setup
WDS Server
Destination
Summary
Progress
Confirmation
Specify the name of the directory that should be created for these operating system files.
Destination directory name:
Windows 7 x86
Previous
Next
Cancel

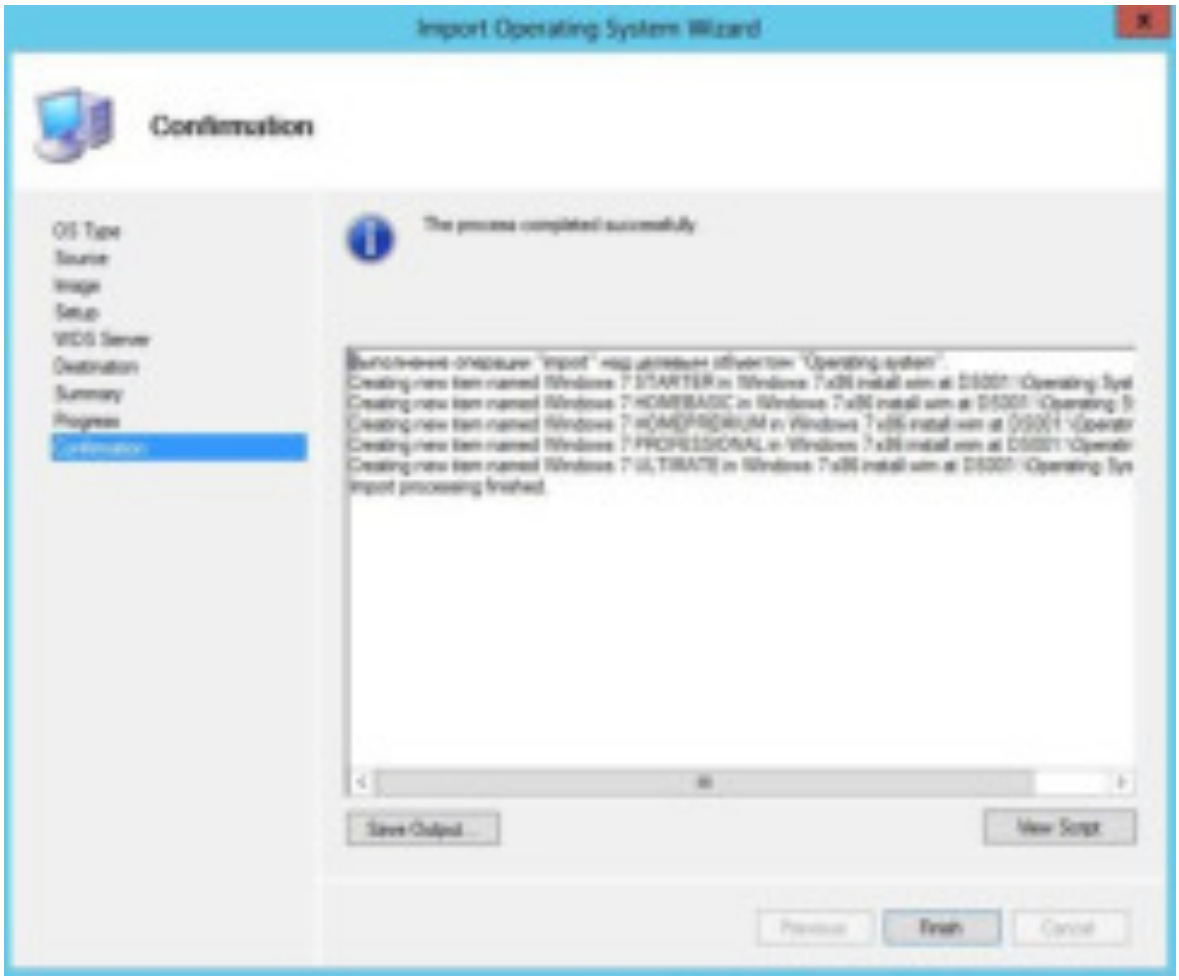
Далее



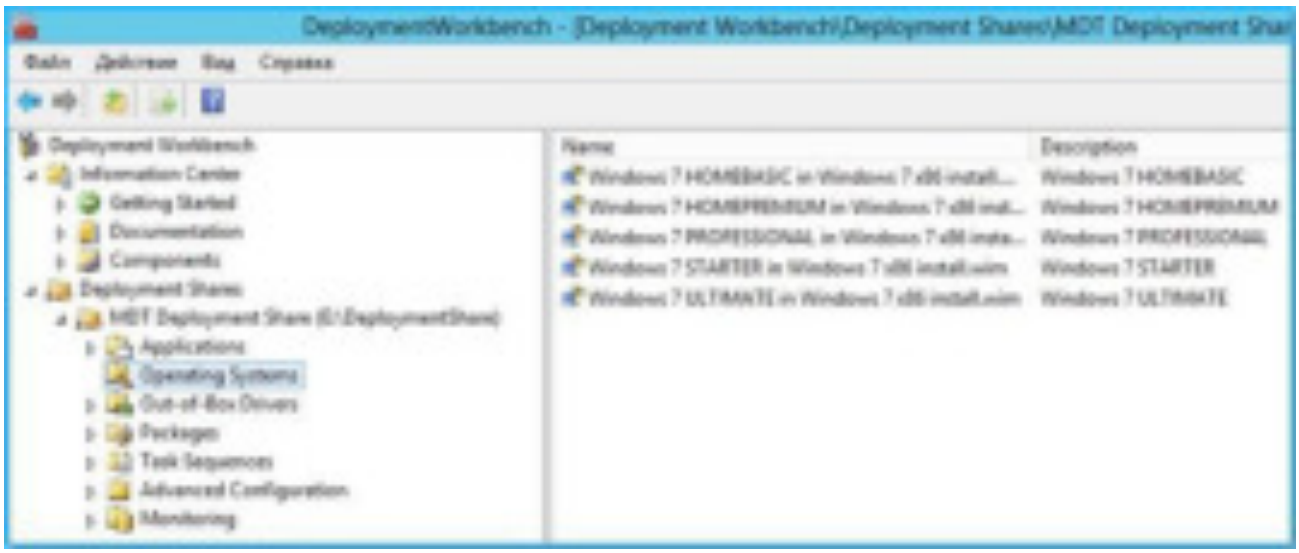

Идет добавление файлов операционной системы в папку развертывания.




Добавление файлов операционной системы завершено

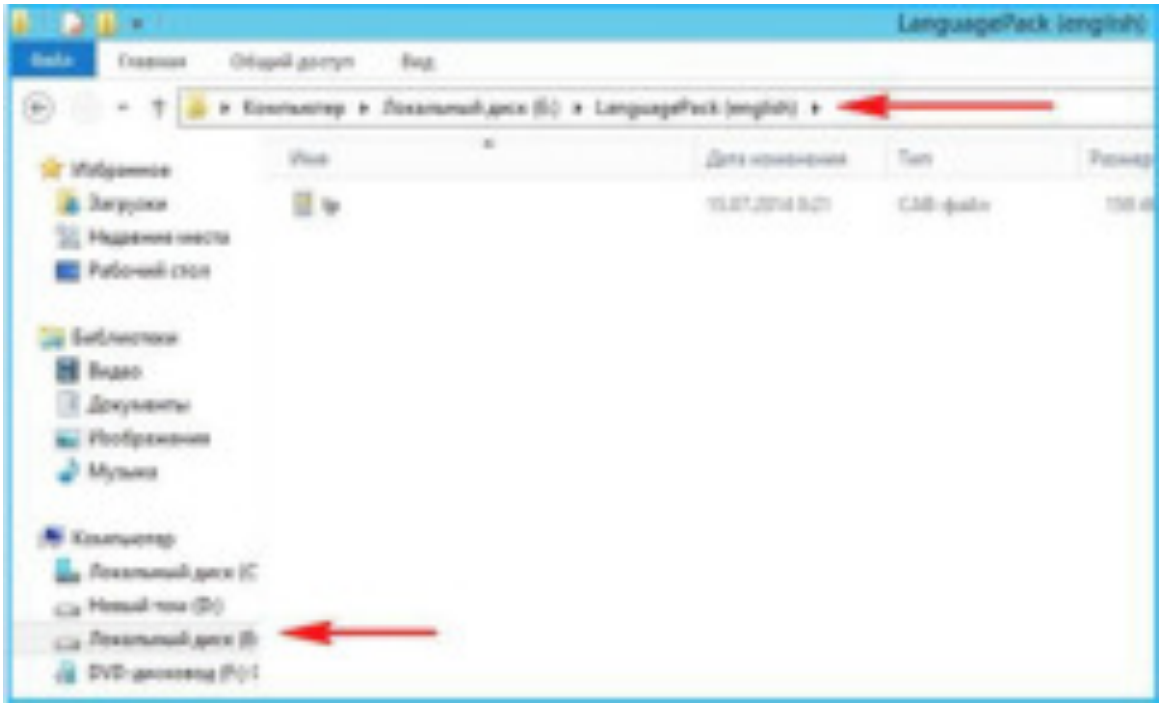


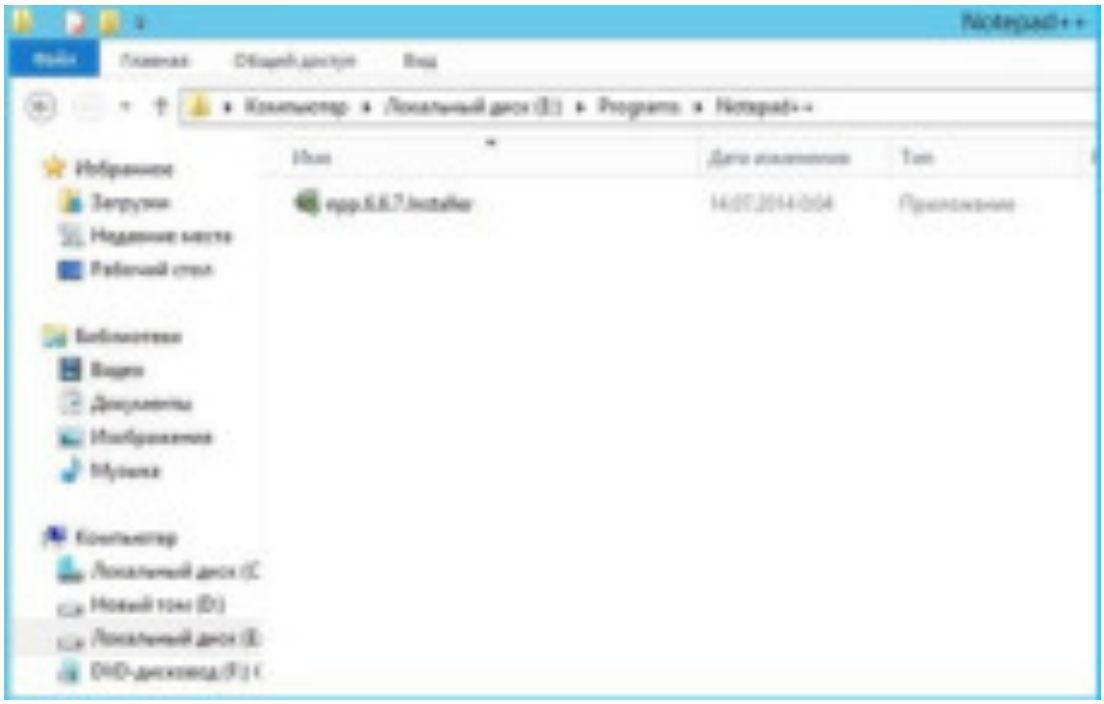

Как видим, дистрибутив содержит несколько редакций операционной системы Windows 7 x86

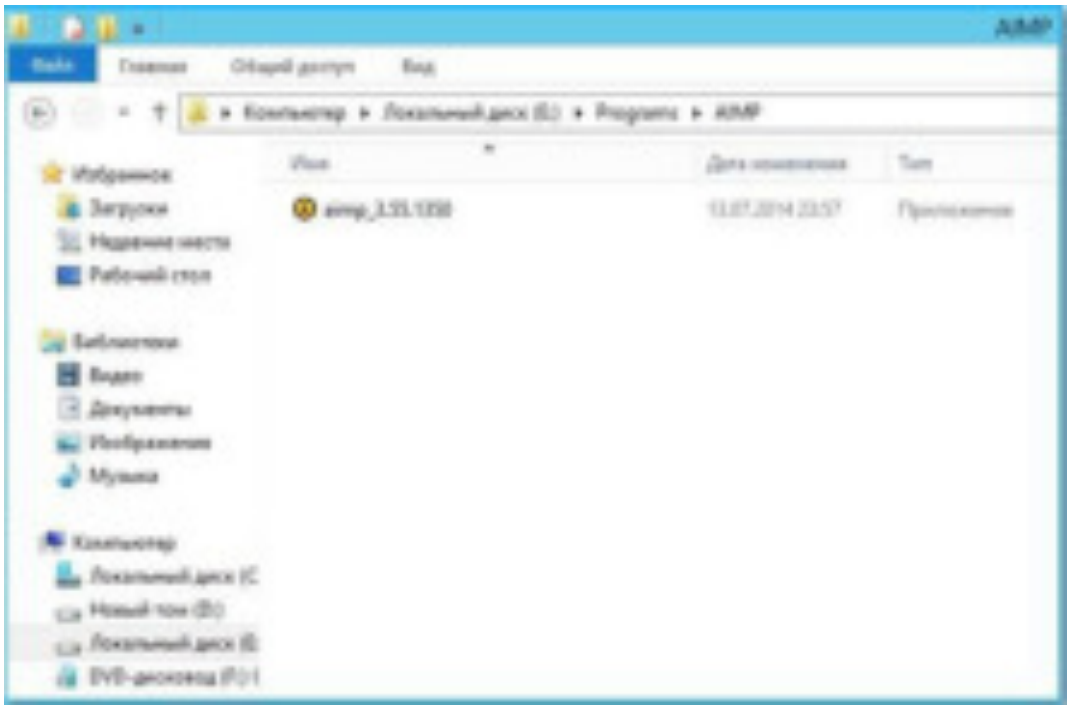



Предварительно на сервере на разделе E: были созданы папки: LanguagePack (english) - в папку был скопирован языковой пакет для Windows 7 с английской локализацией

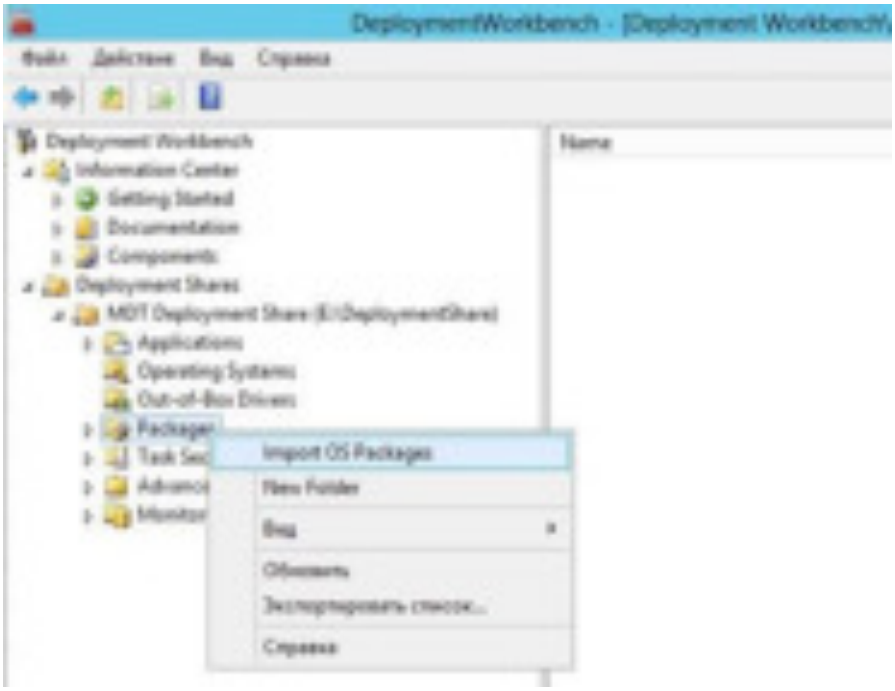
Папки AIMP и Notepad++, в которые были скопированы установочные файлы данных программ



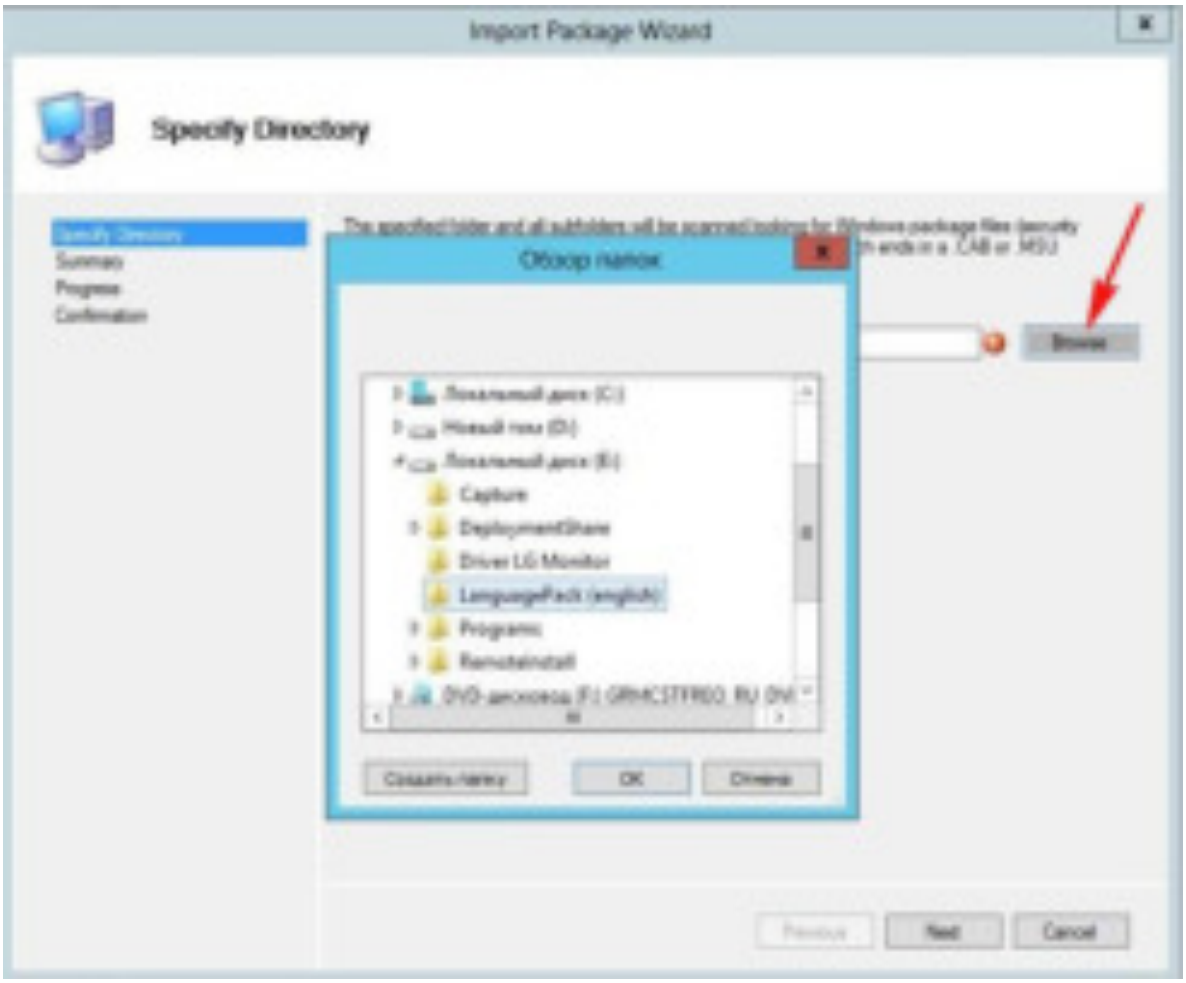




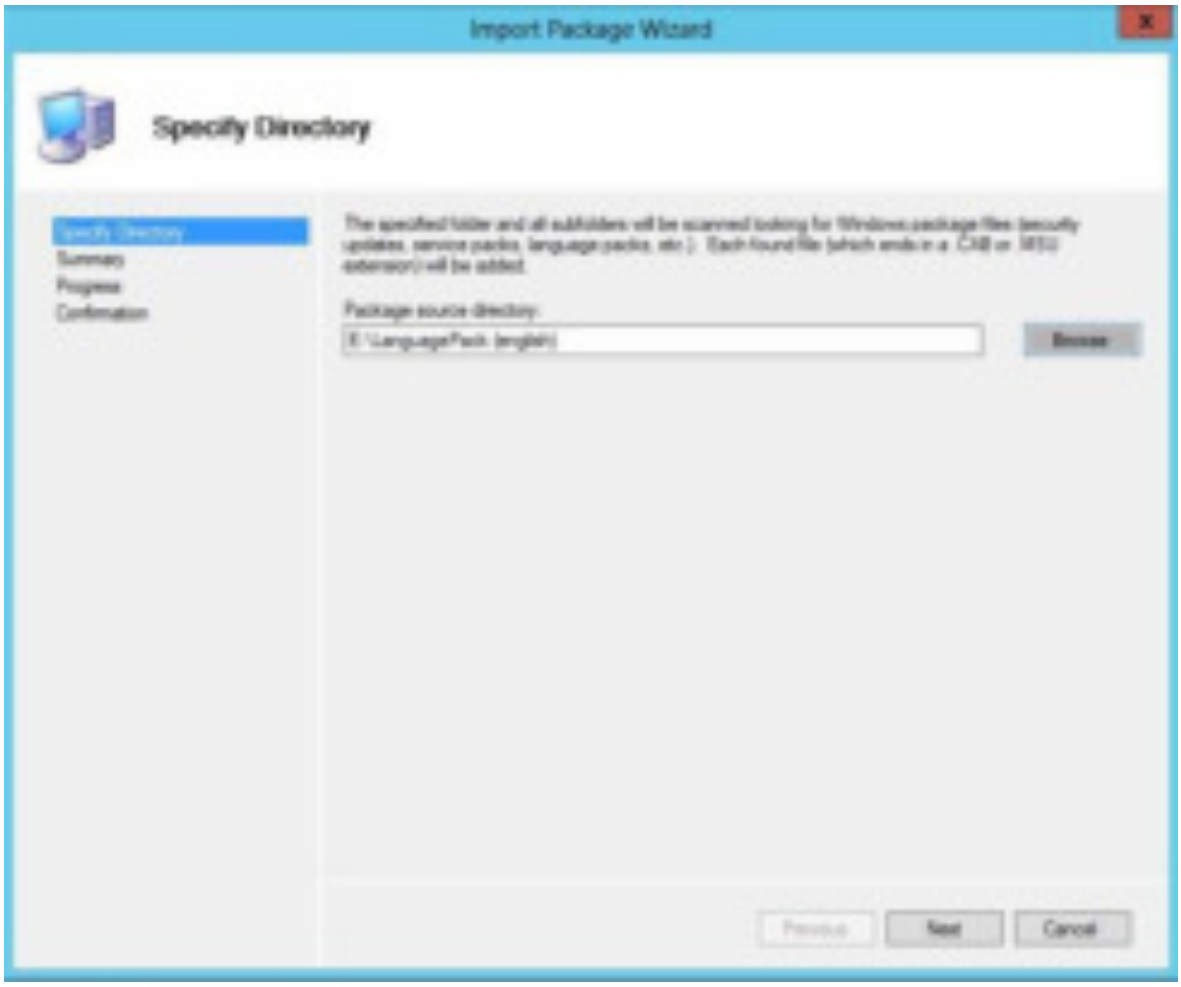
Добавляем наш языковой пакет в папку развертывания. Выбираем Packages, далее Import OS Packages



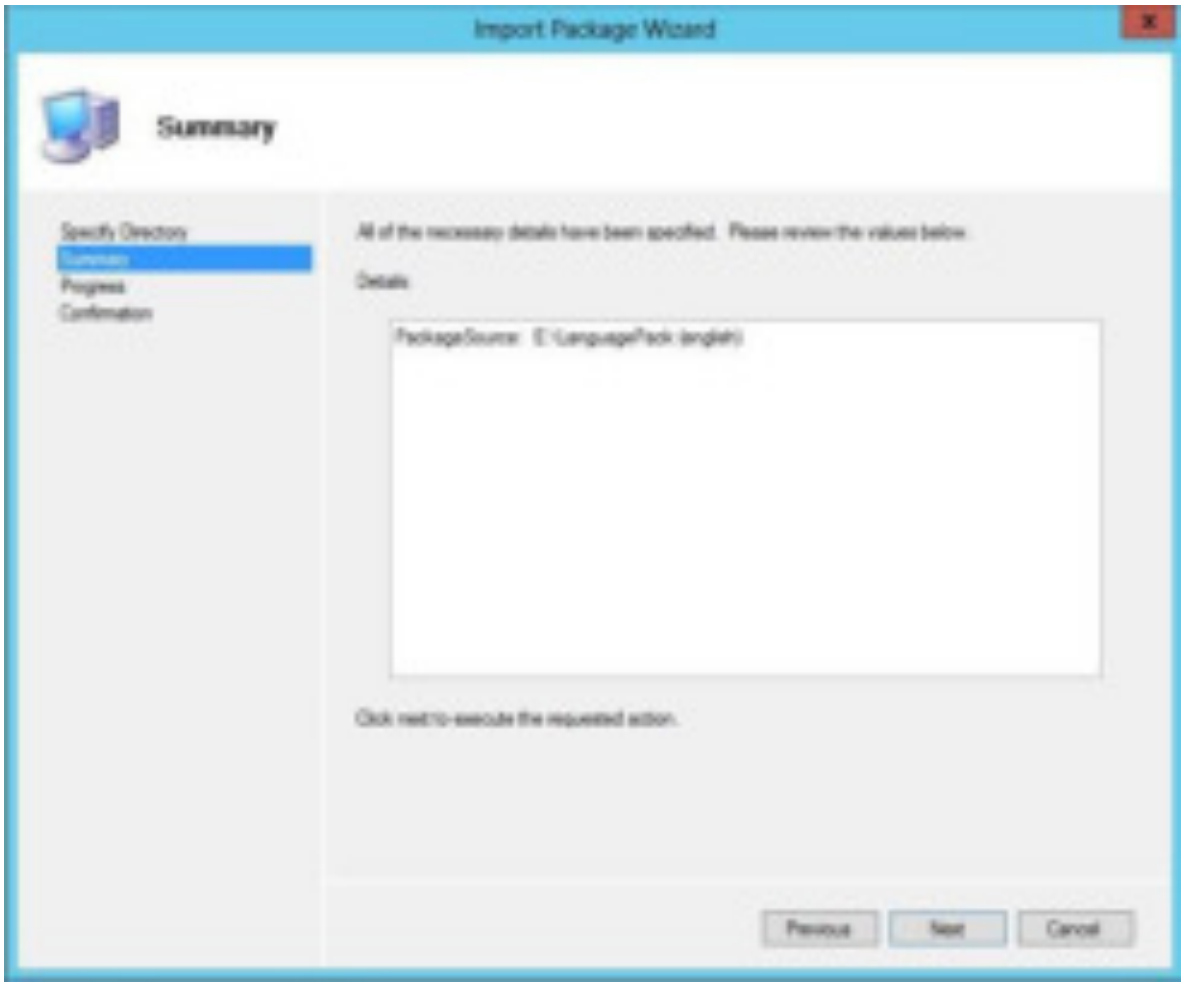

Выбираем местоположение языкового пакета, он у нас сохранен на разделе E: в папке LanguagePack (english)


Import Package Wizard
Specify Directory
Summary
Progress
Confirmation
Обзор папок
Capture
DeploymentShare
Driver LG Monitor
LanguagePack (english)
Programs
RemoteInstall
OK
Browse
Next
Cancel

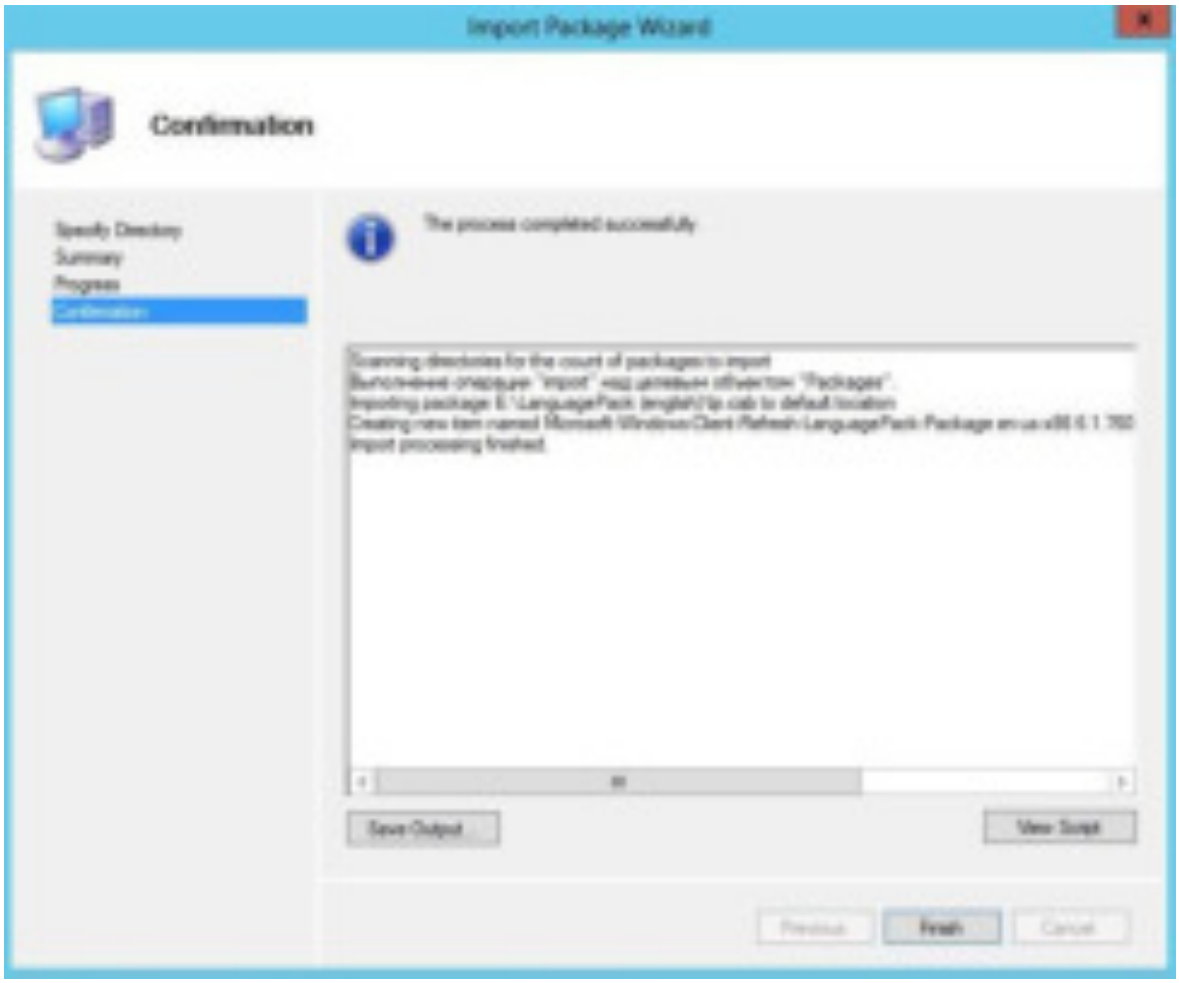
Далее


Import Package Wizard
Specify Directory
Summary
Progress
Confirmation
Package source directory:
Next
Cancel

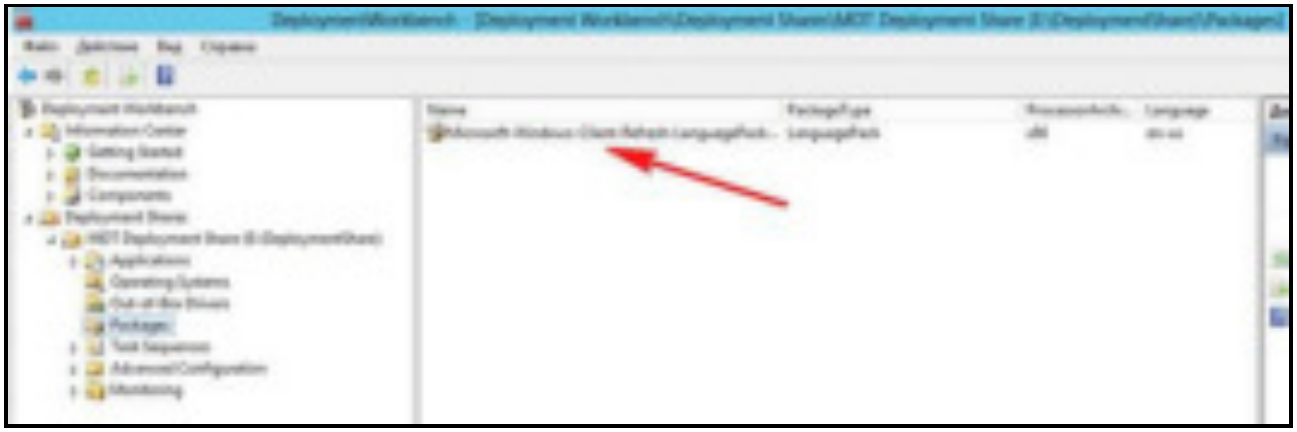
Далее



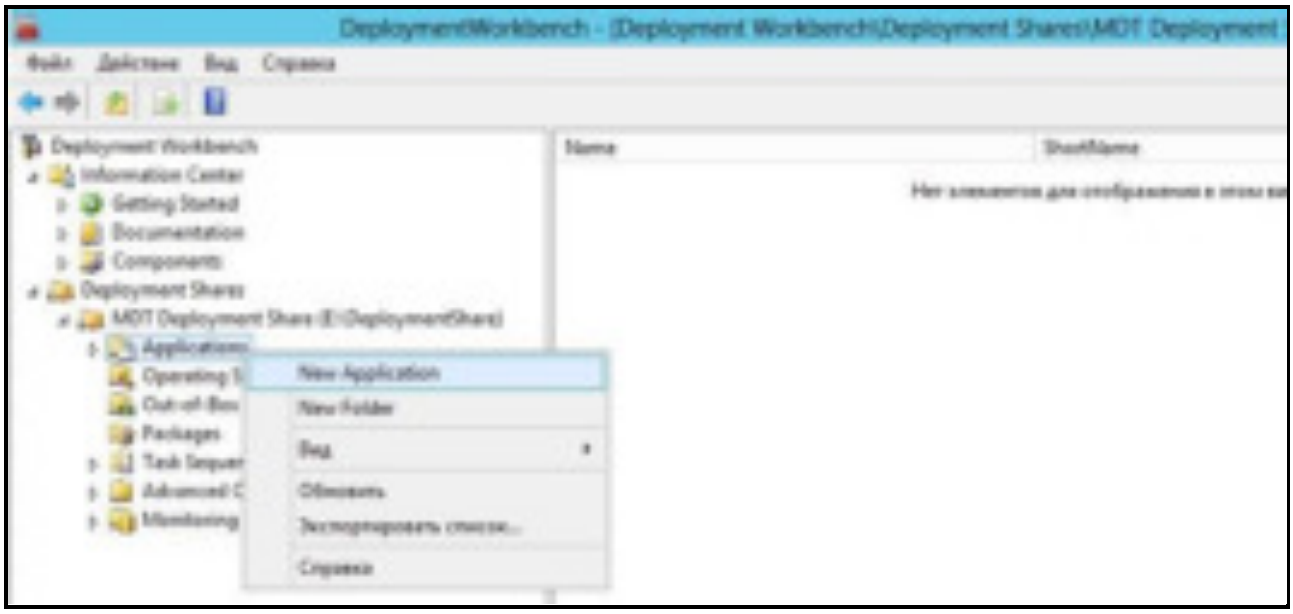

Добавление языкового пакета успешно завершено



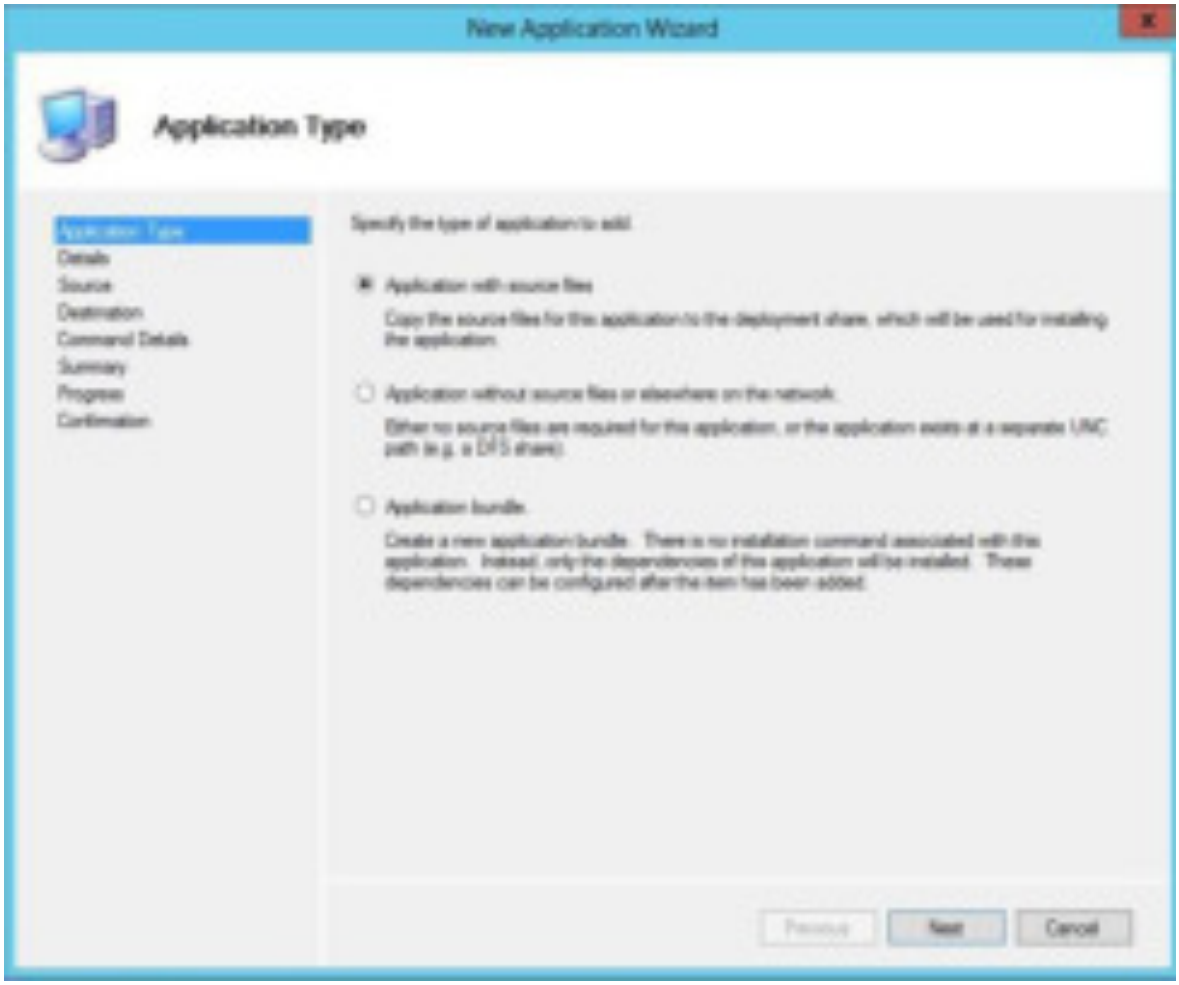

Появился наш языковой пакет



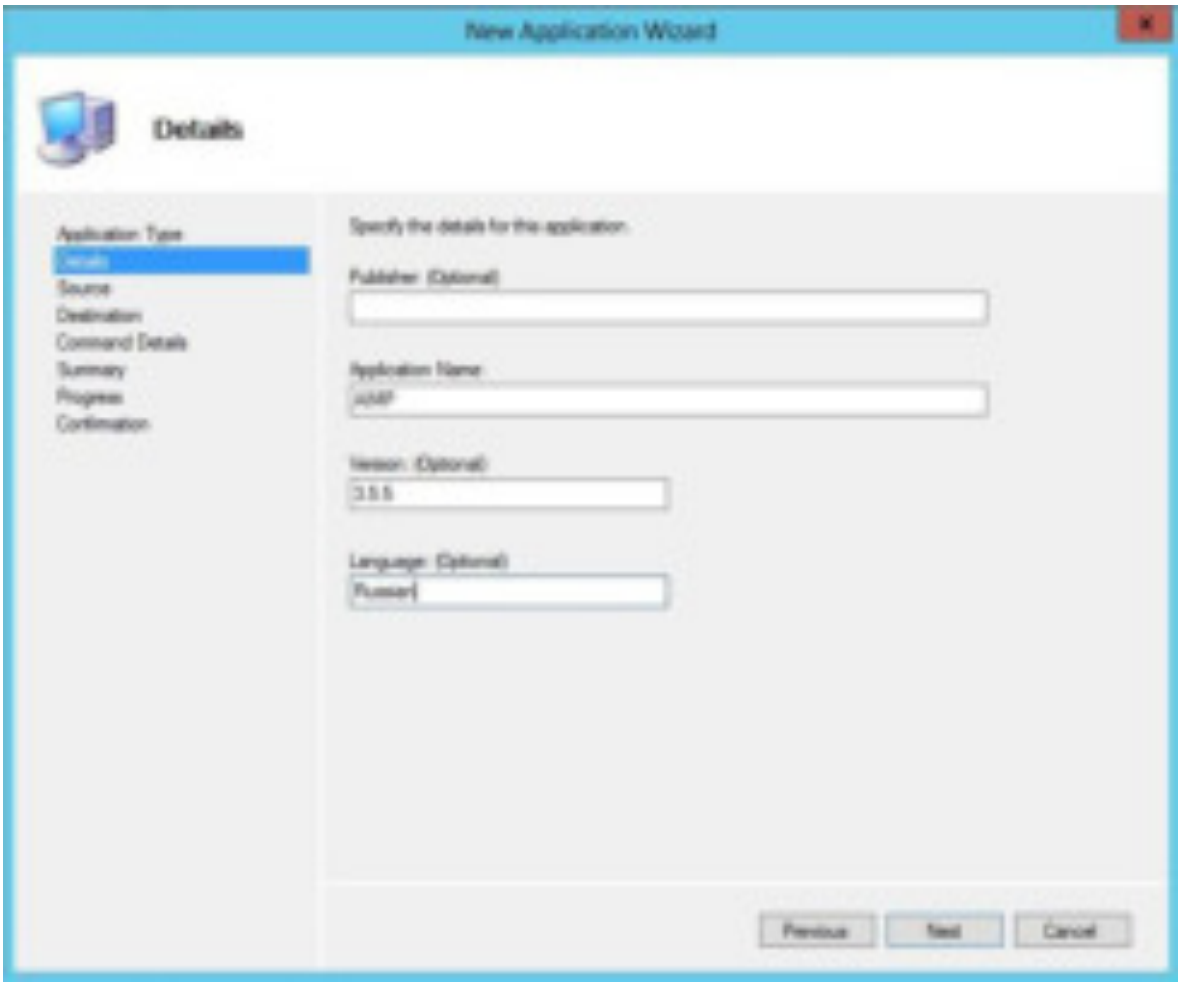
Добавляем в нашу папку развертывания приложения: аудио проигрыватель AIMP и программу Notepad++.  Выбираем папку Applications, далее выбираем New Application.



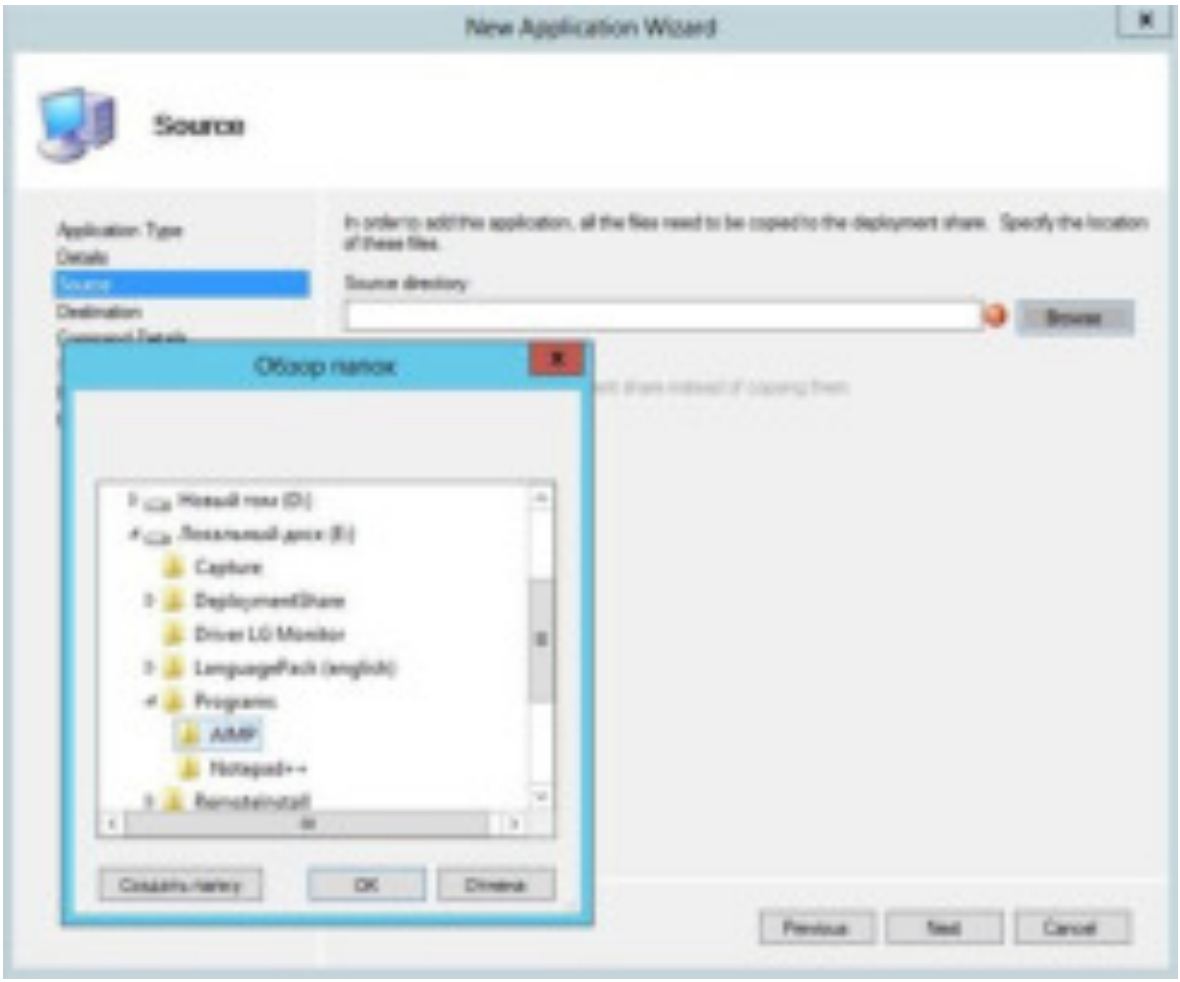

Нас интересует первый вариант добавления установочного файла программы в папку развертывания. Далее



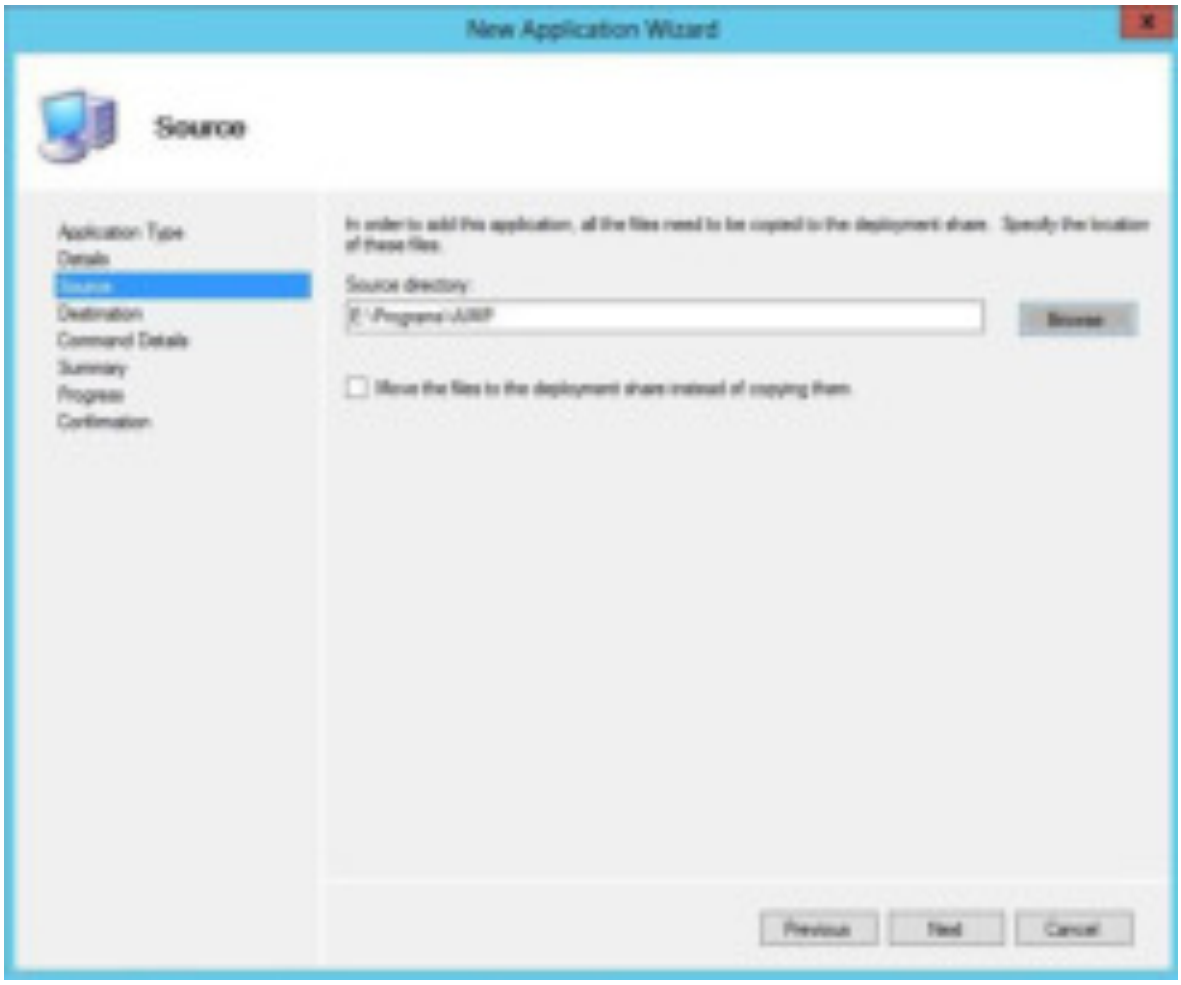

Вводим название программы, ее версию и язык. Далее



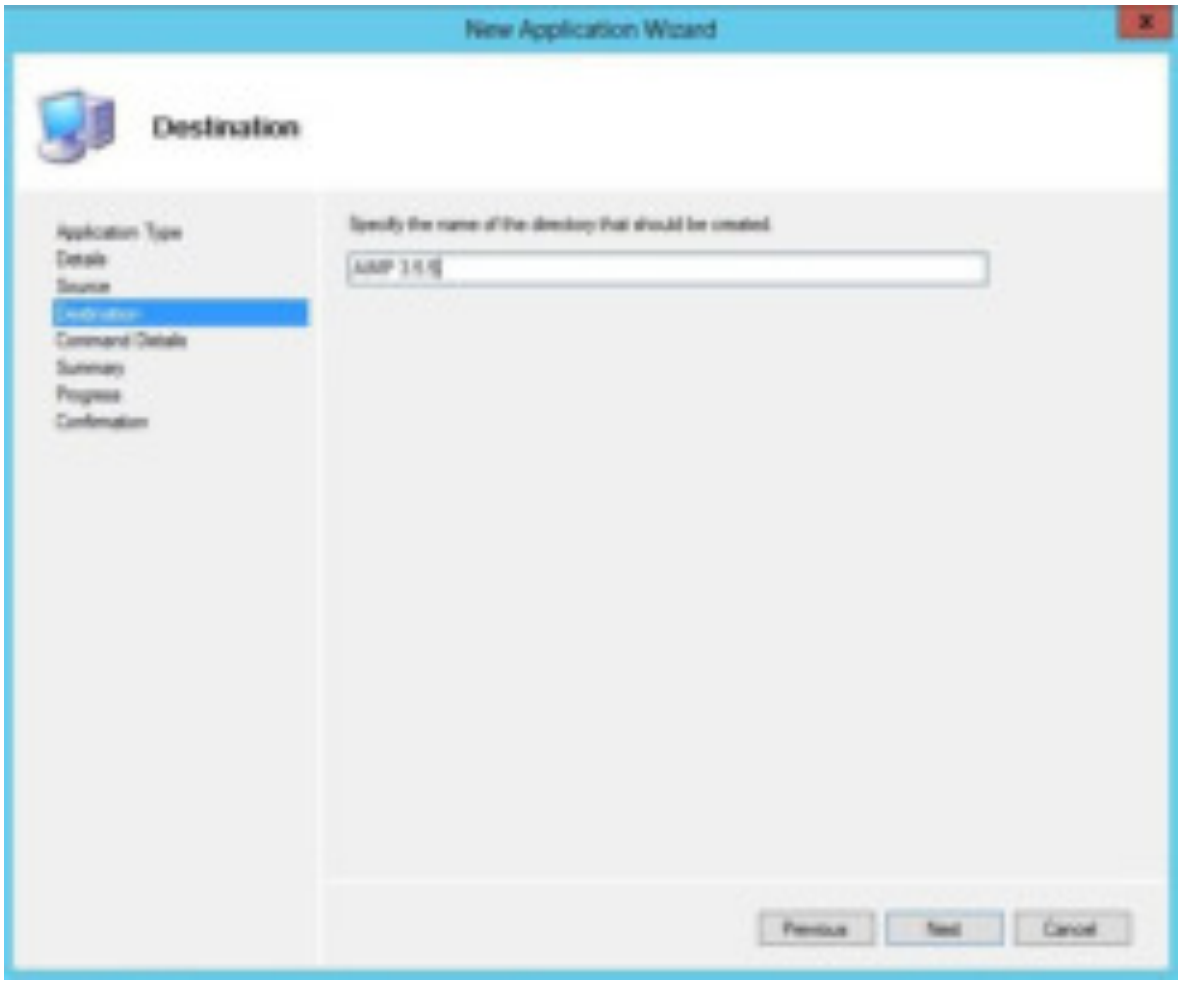

Выбираем местоположение установочного файла


New Application Wizard
Source
Application Type
Details
Source
Destination
Source directory
Browse
Обзор папок
Capture
Deployment$hare
Driver LG Monitor
Programs
AIMP
Notepad++
Remoteinstall
OK
Previous
Next
Cancel

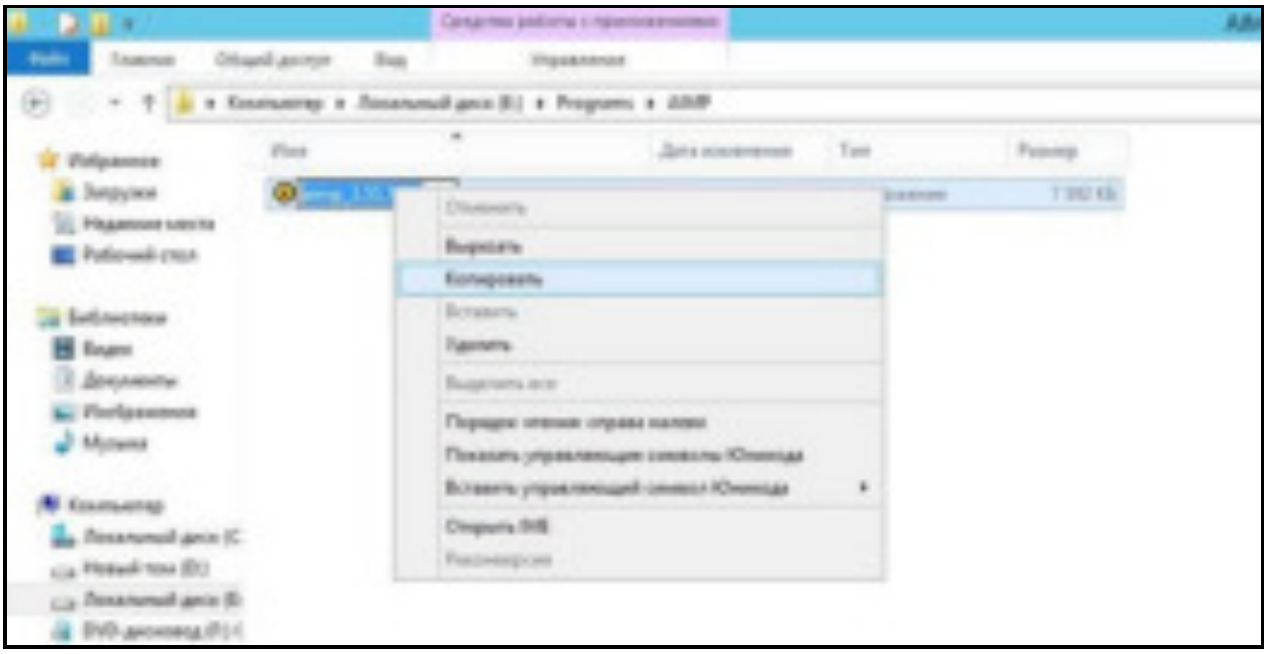
Далее


New Application Wizard
Source
Application Type
Details
Source
Destination
Command Details
Summary
Progress
Confirmation
Source directory:
Browse
Move the files to the deployment share instead of copying them
Previous
Next
Cancel

Далее

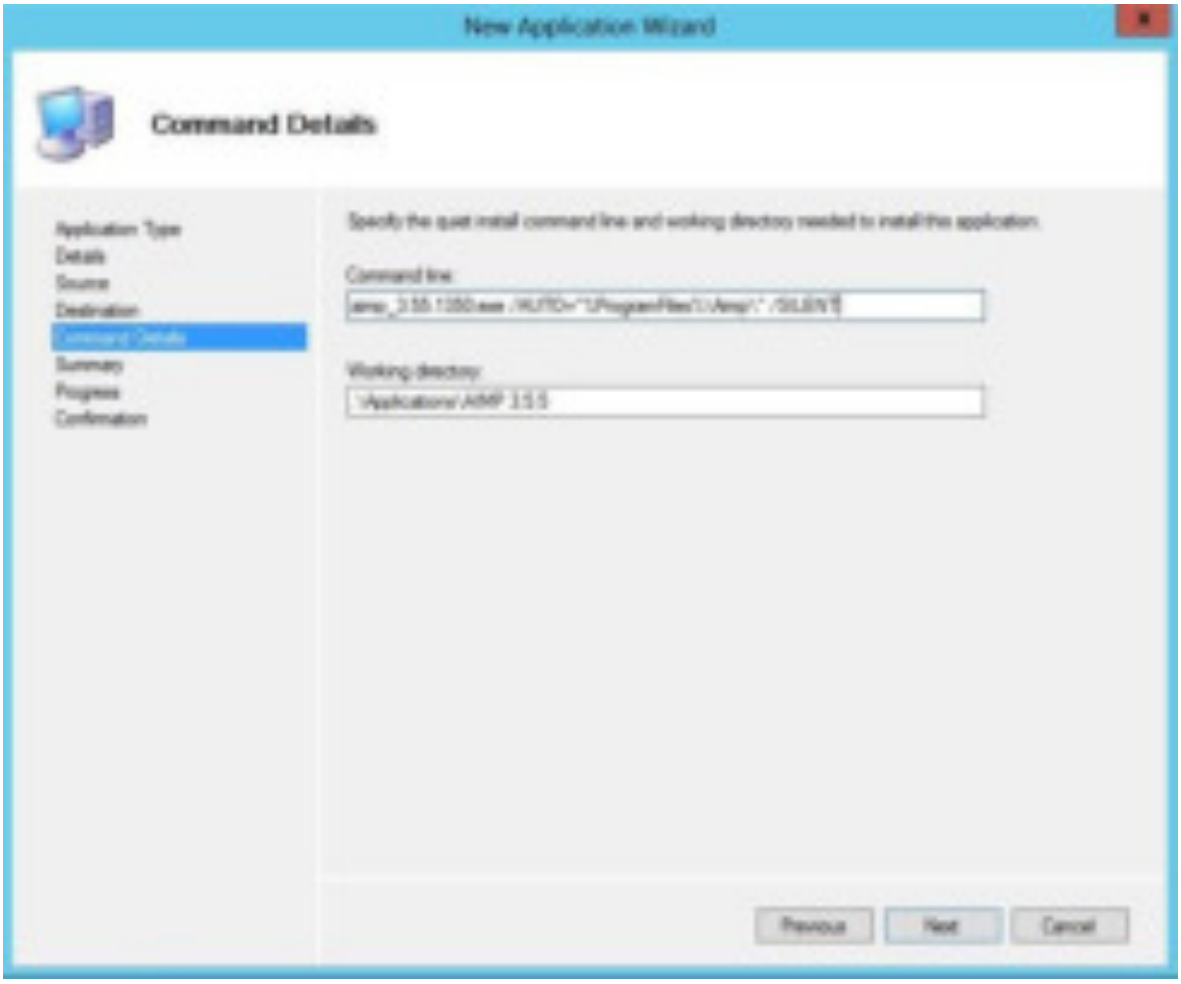



Идем на раздел E: в папку с установочным файлом программы AIMP и копируем его название

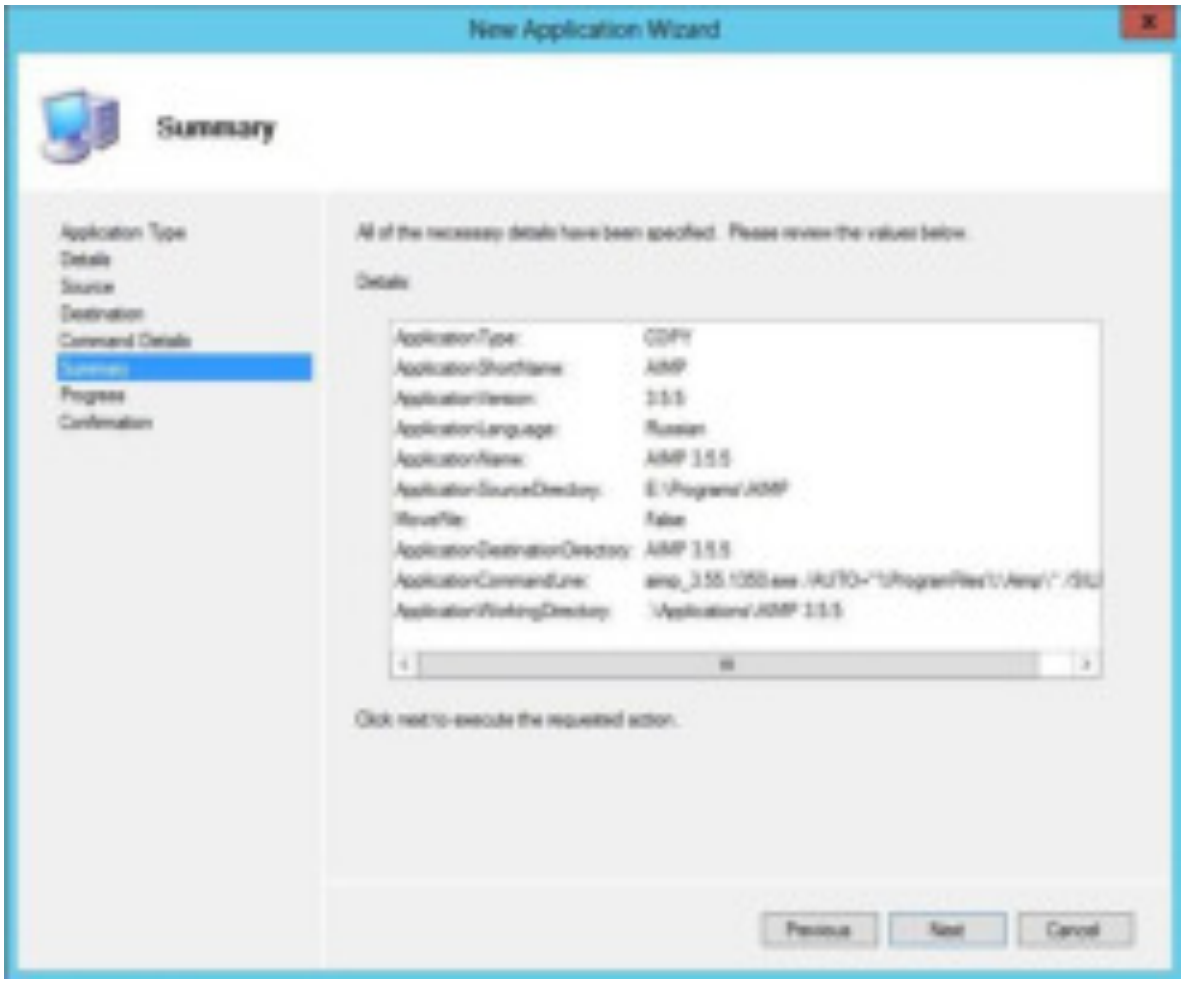



В строке Command line вводим имя установочного файла и прописываем ключ для тихой установки данного приложения, которое представляет собой

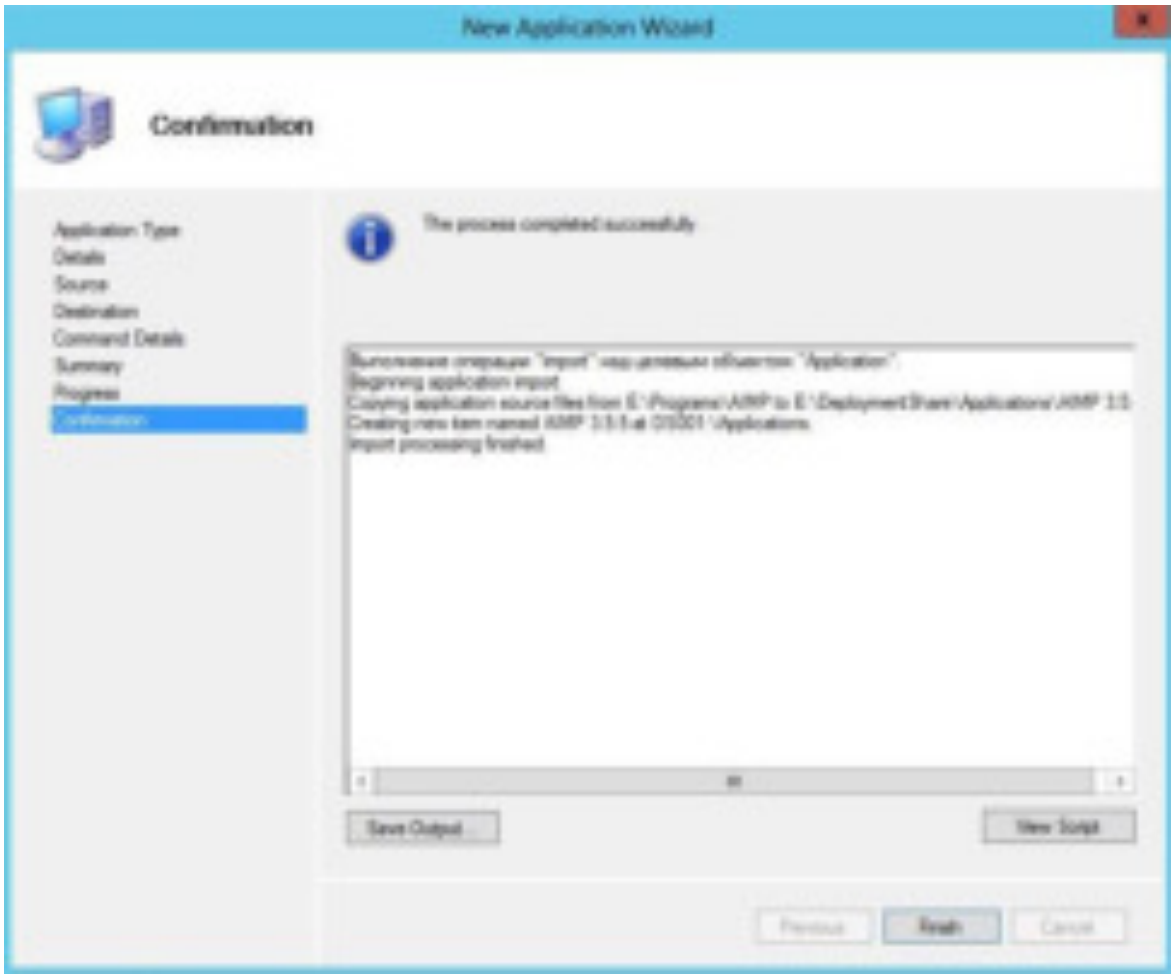
следующее выражение: /AUTO="%ProgramFiles%\Aimp\" /SILENT. В итоге в строке Command line вводим aimp_3.55.1350.exe /AUTO="%ProgramFiles%\Aimp\" /SILENT. Далее



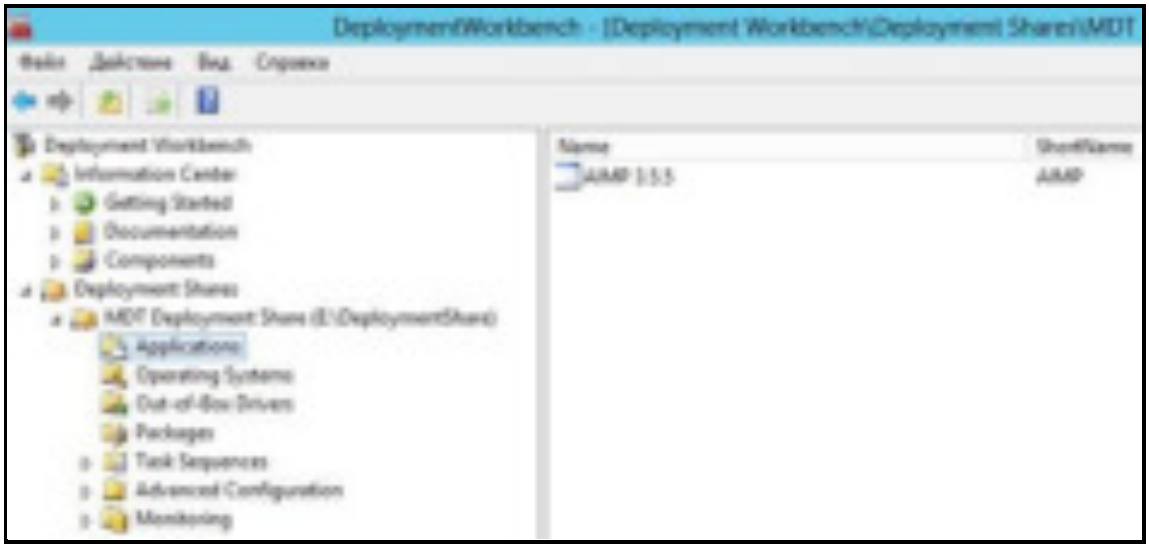

Далее



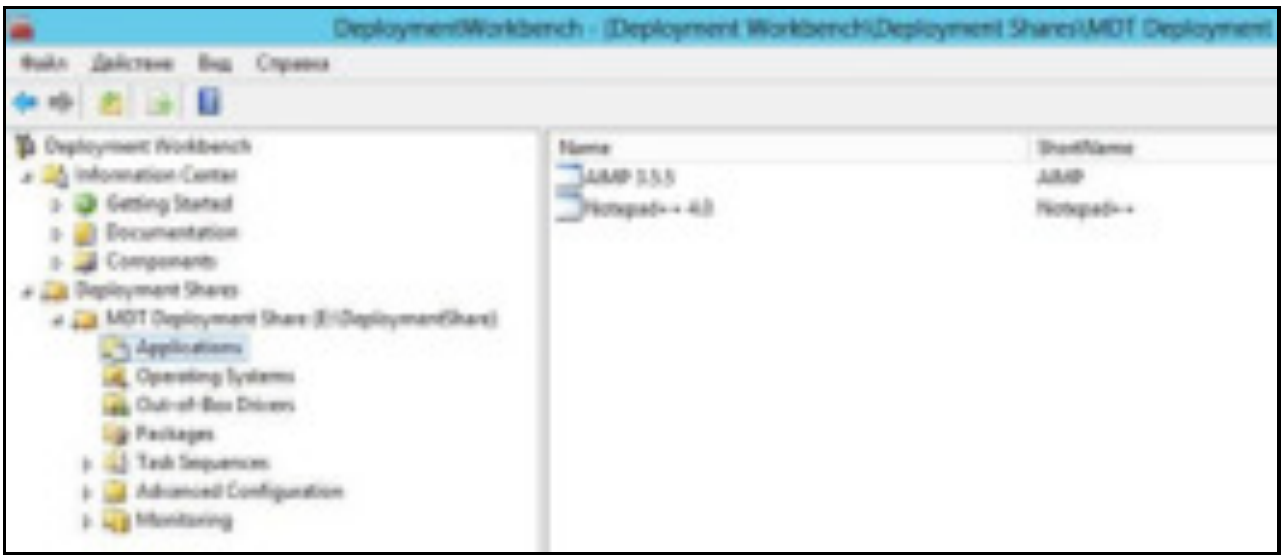

Приложение успешно добавлено в папку развертывания



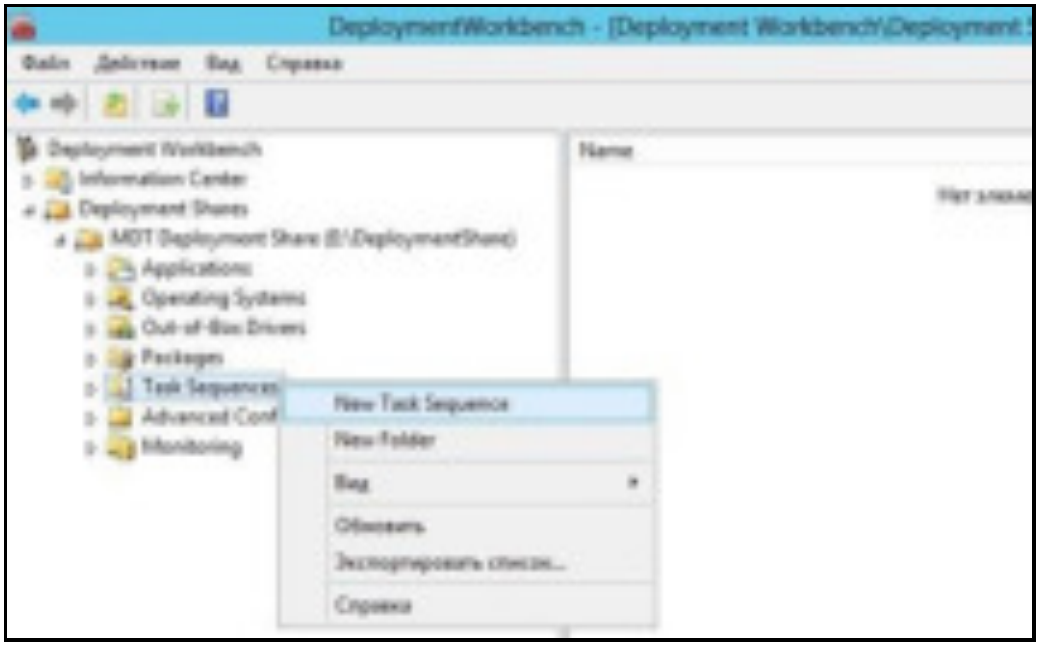

Вот и само приложение AIMP



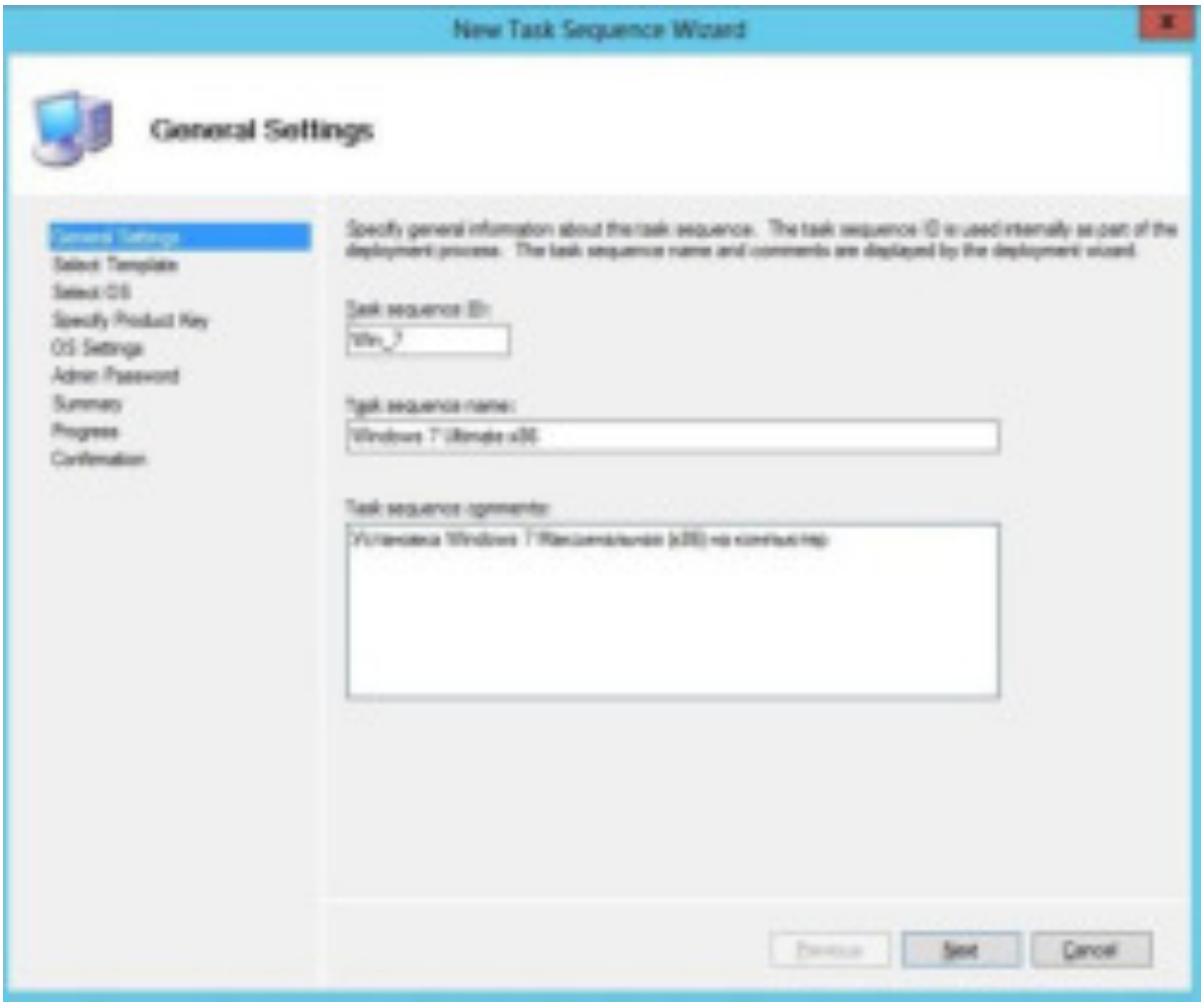

Аналогичным образом добавляем приложение Notepad++.
В строке Command Line для данного приложения нужно ввести следующее
npp.6.6.7.Installer.exe /S
После добавления приложений должно получится следующее



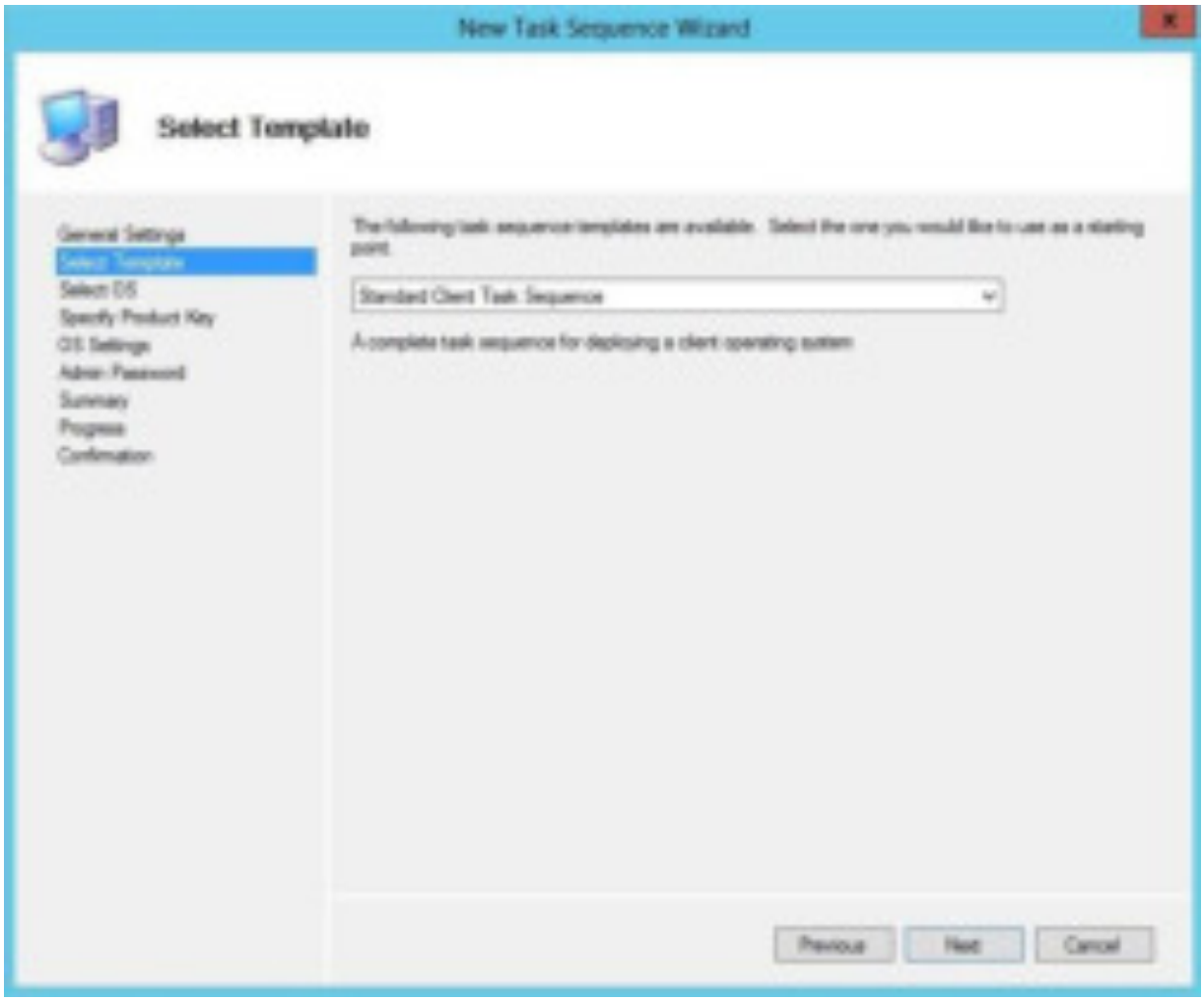

Выбираем папку Task Sequences, далее выбираем New Task Sequences



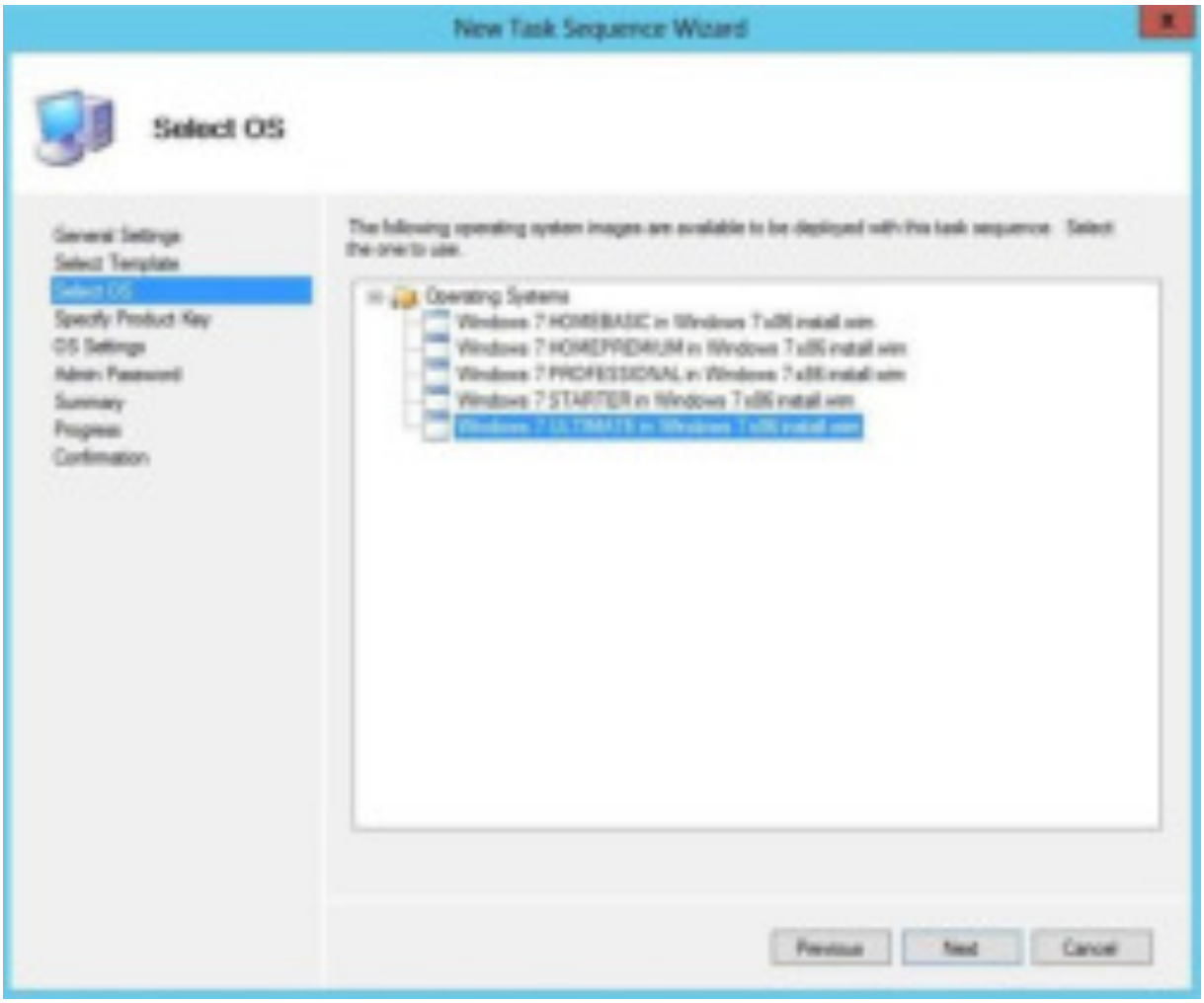

Вводим идентификатор ID, например Win_7, так же вводим имя последовательности задач и небольшой комментарий



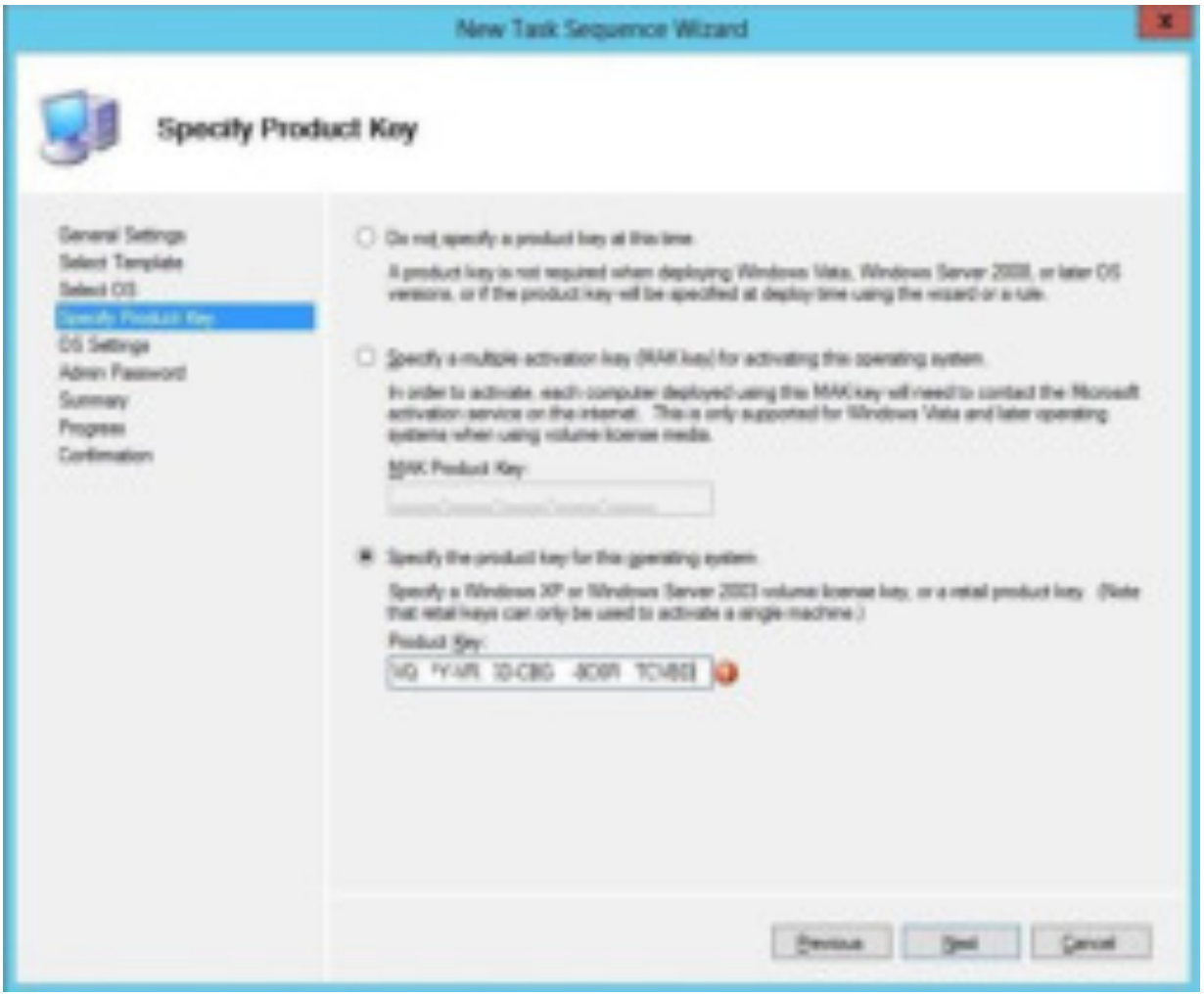

Выбираем из списка самый первый шаблон т.е Standard Client Task Sequence. Далее



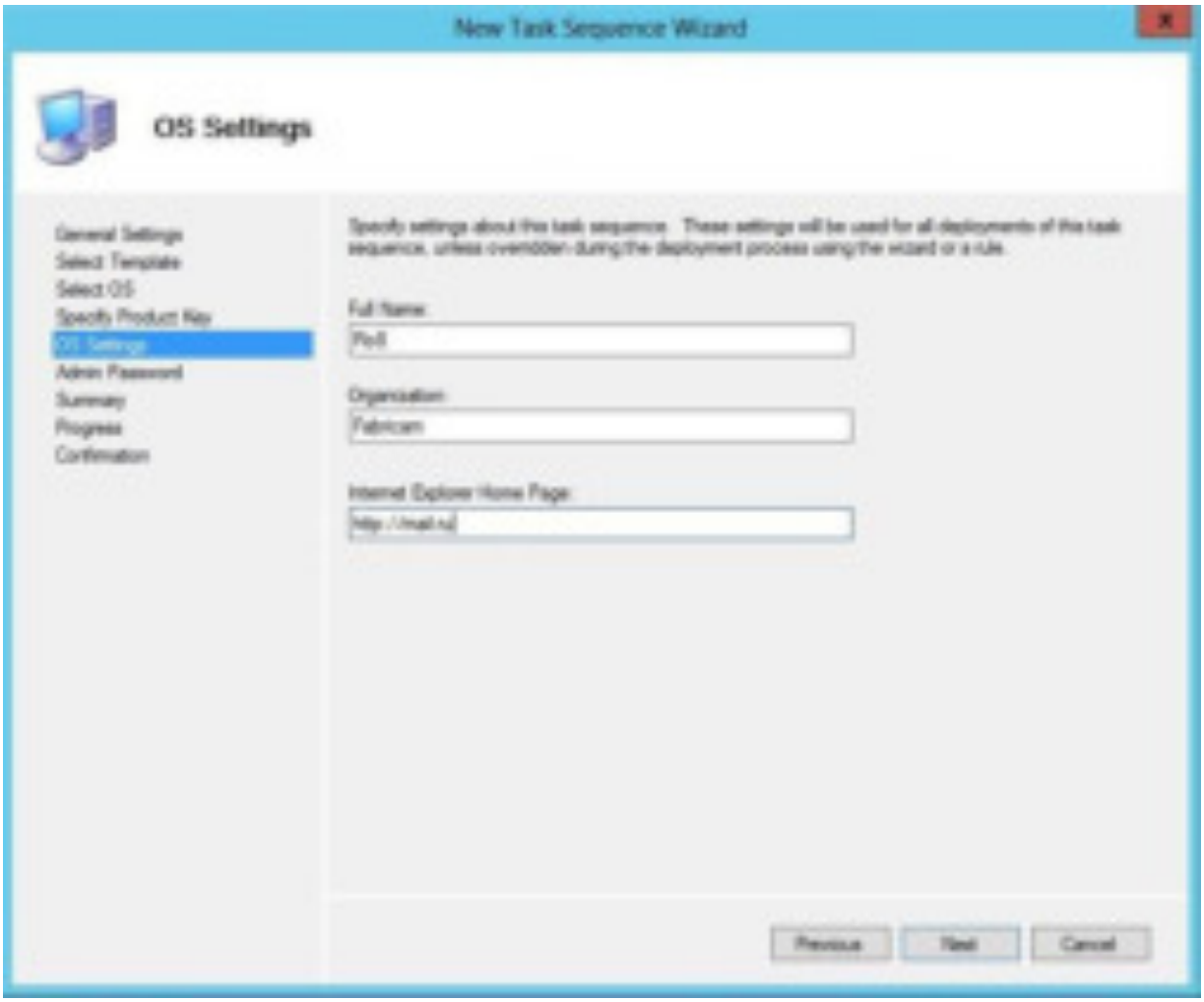

Выбираем из списка нужную операционную систему, в нашем случае это Windows 7 Ultimate x86



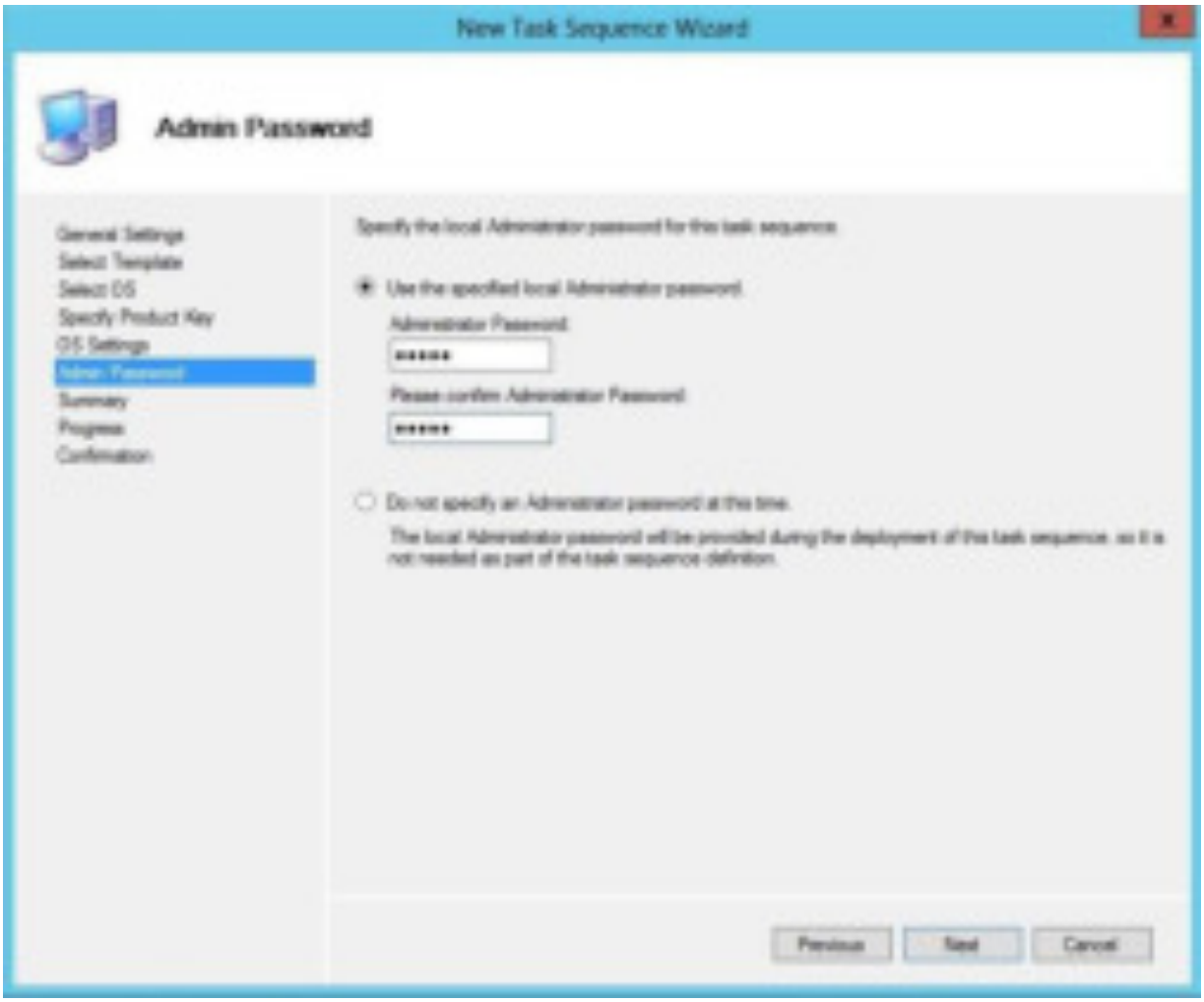

Вводим ключ устанавливаемой редакции, далее



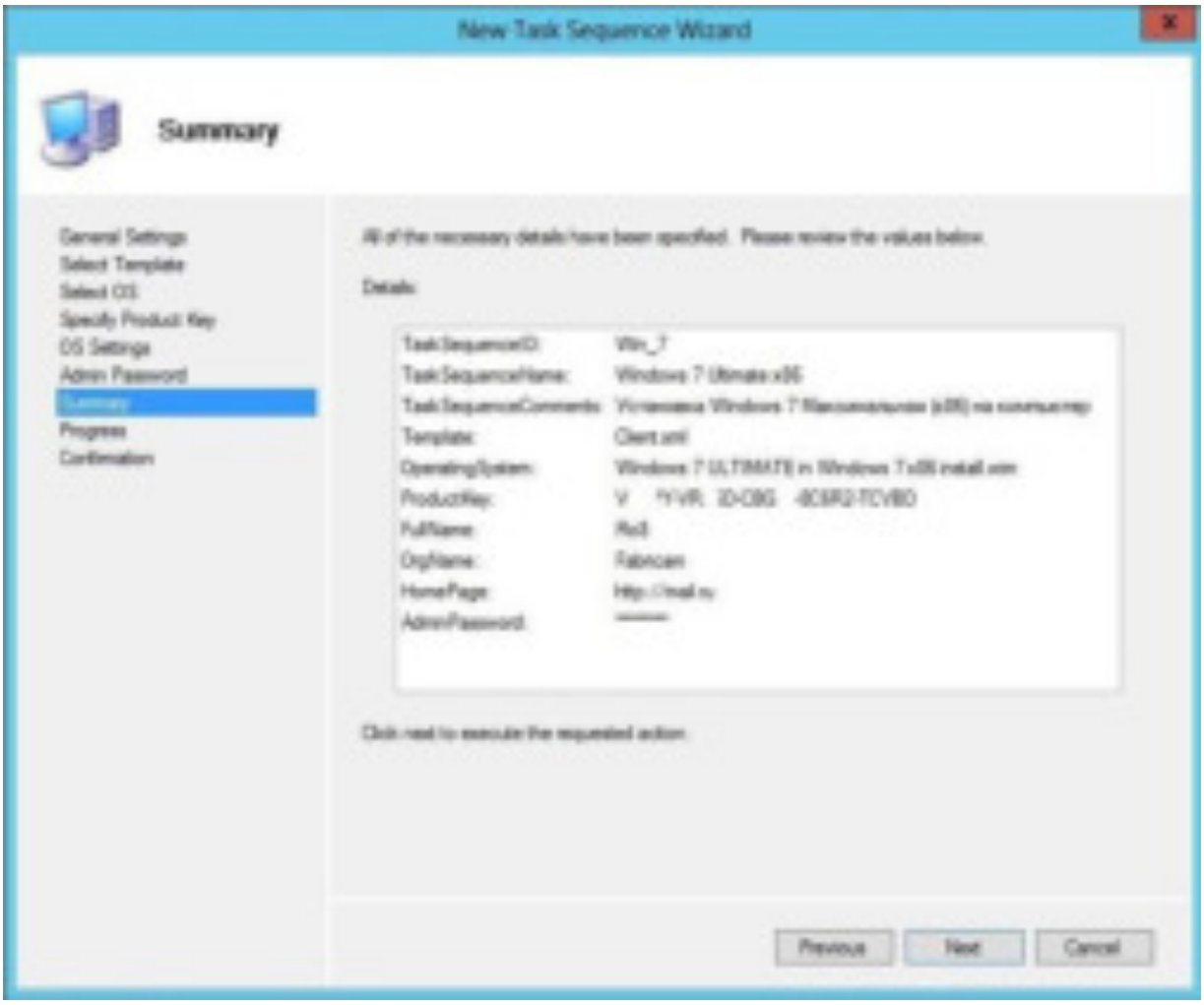

Вводим имя владельца системы, название организации, при желании можно указать начальную страницу браузера Internet Explorer



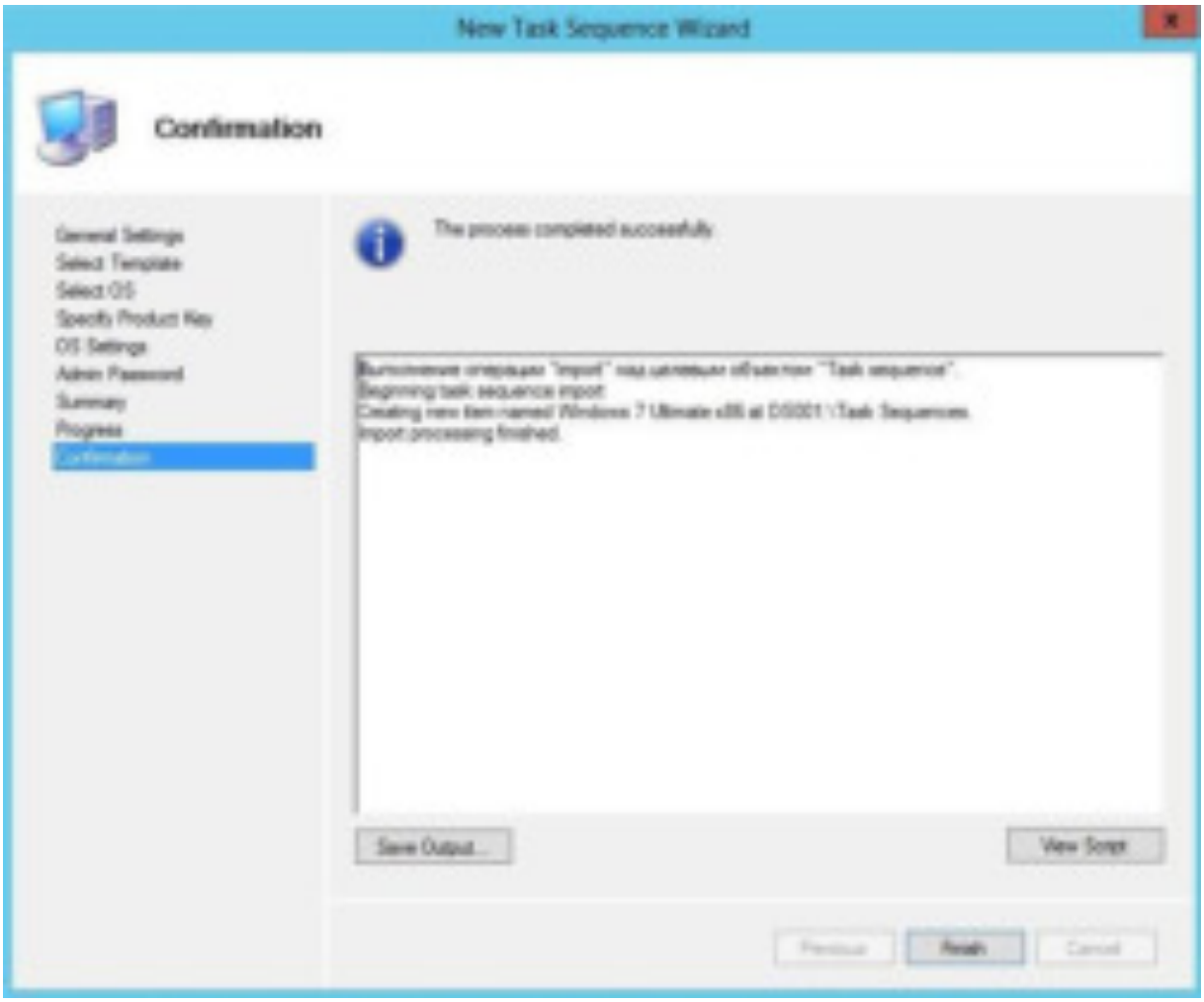

Вводим пароль администратора



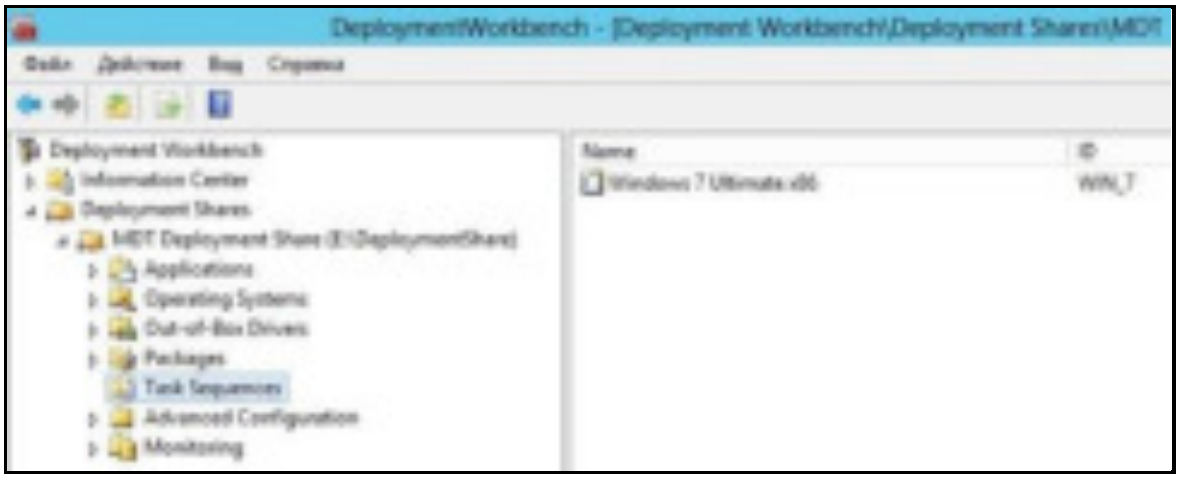

Если все сведения введены верно, жмем Далее



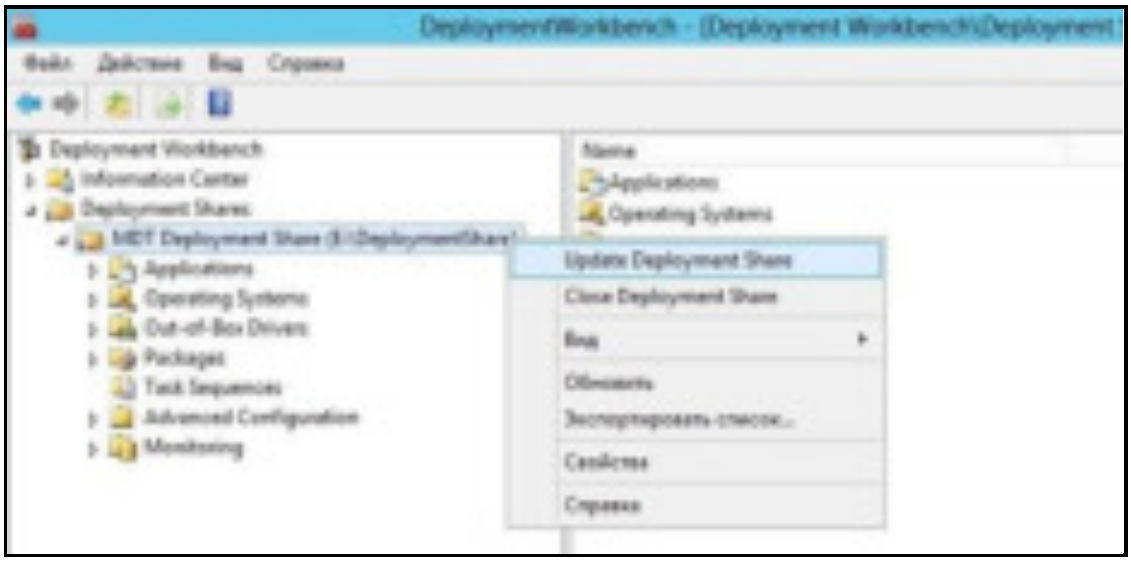

Последовательность задач успешно создана



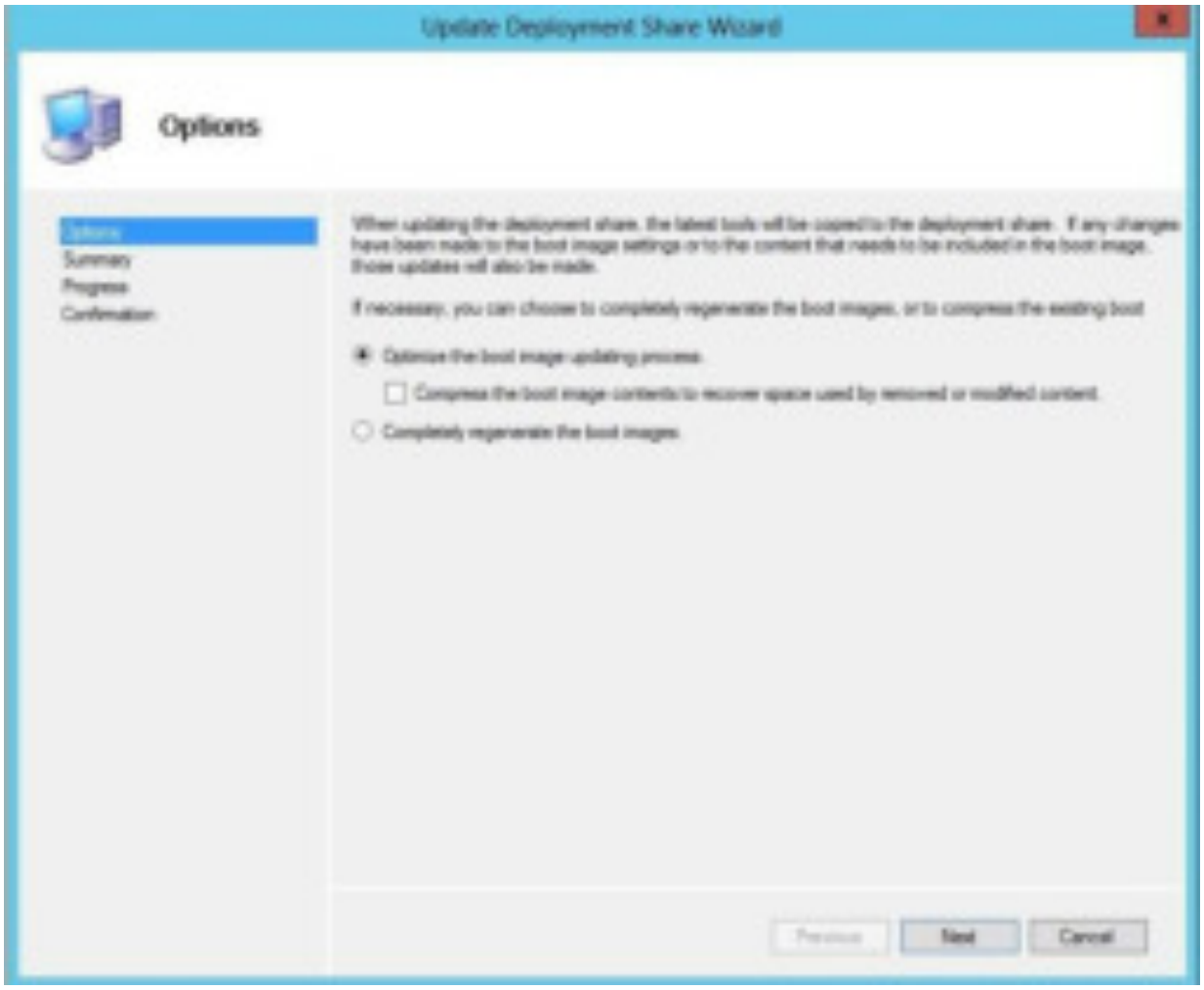

Вот появилась наша последовательность задач



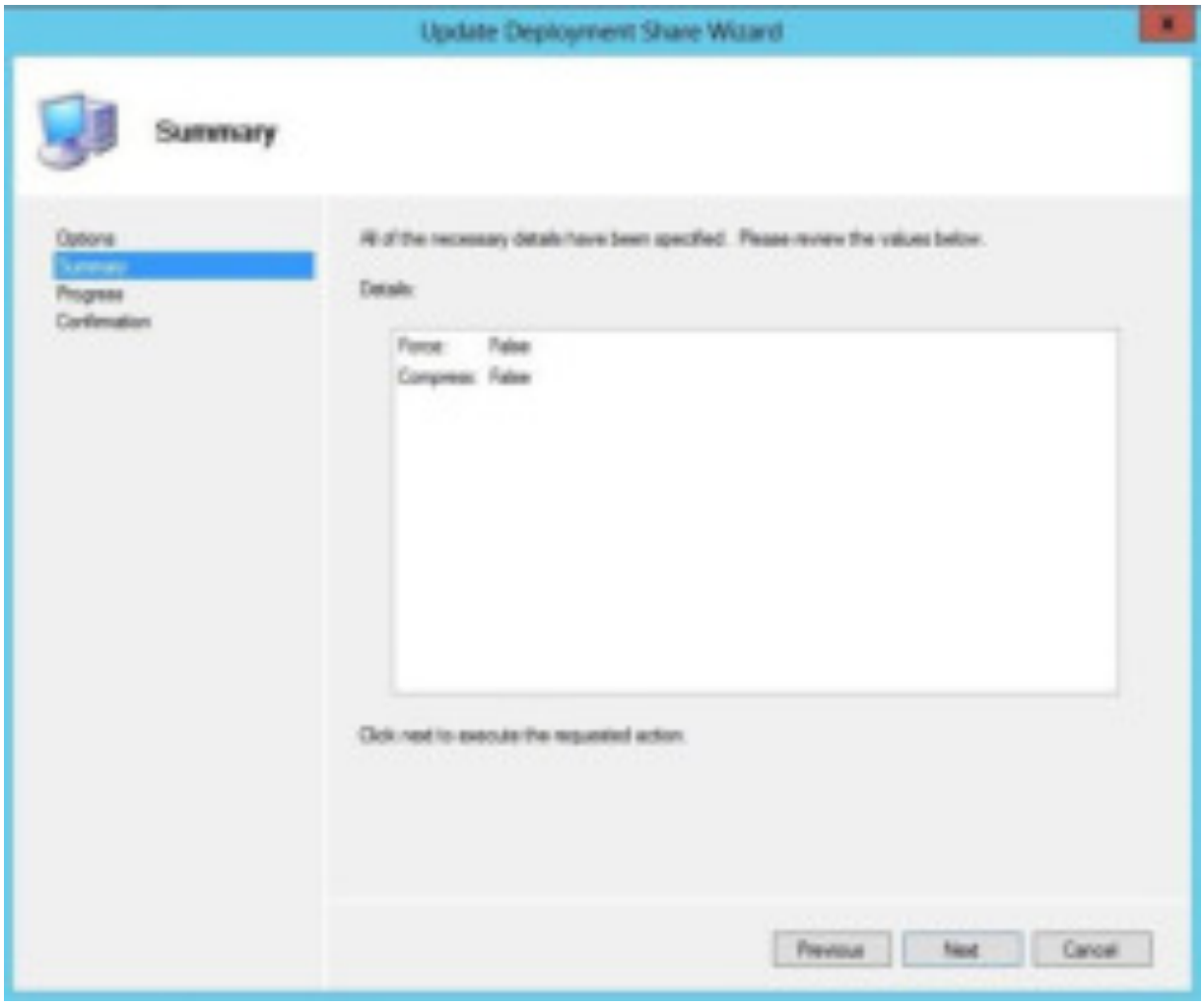

Выделяем нашу папку развертывания MDT Deployment Share и выбираем Update Deployment Share



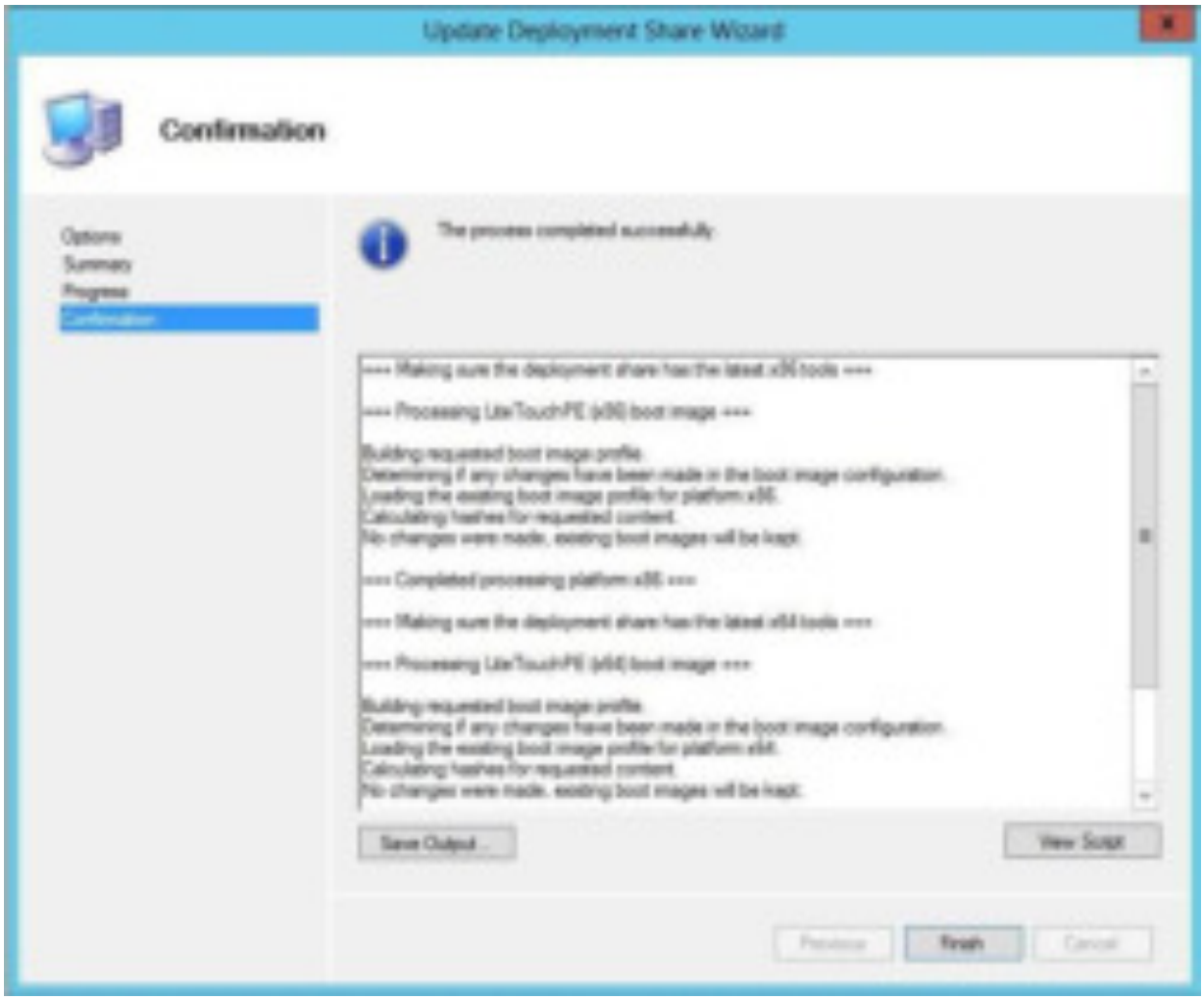

Так как мы обновляем нашу папку развертывания впервые, то выбираем Optimize the boot image updating process. Далее



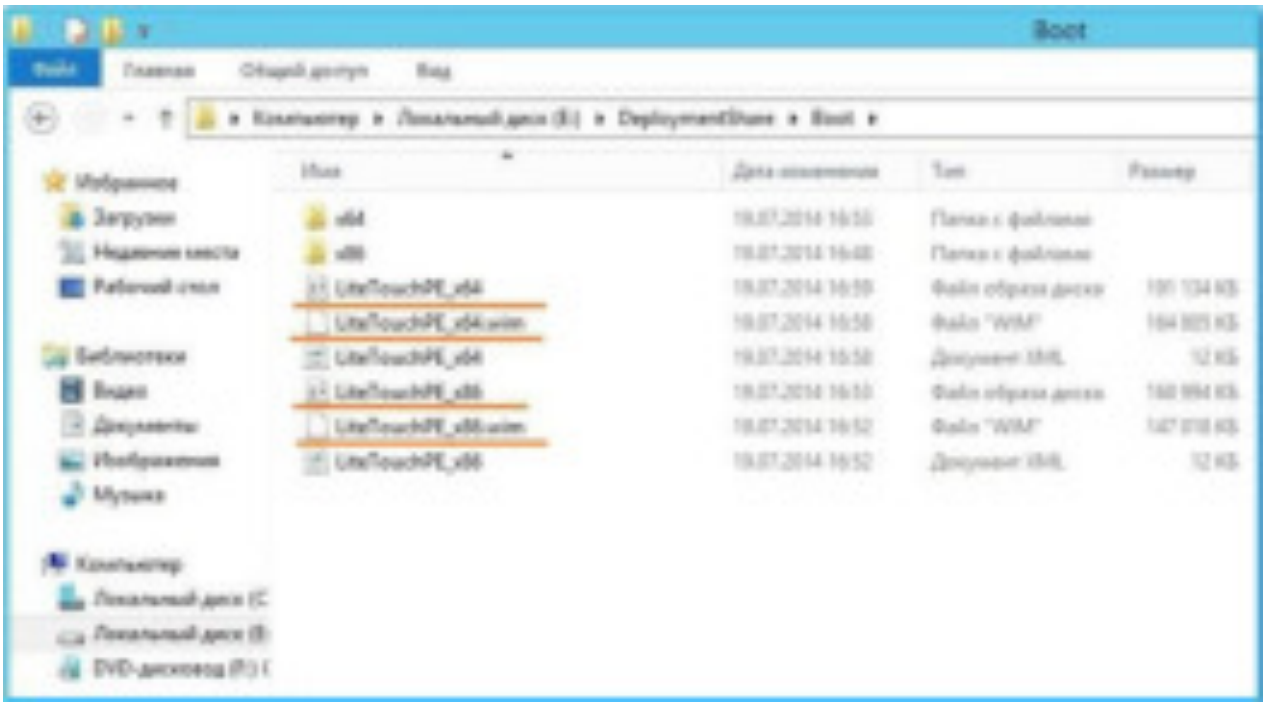

Далее



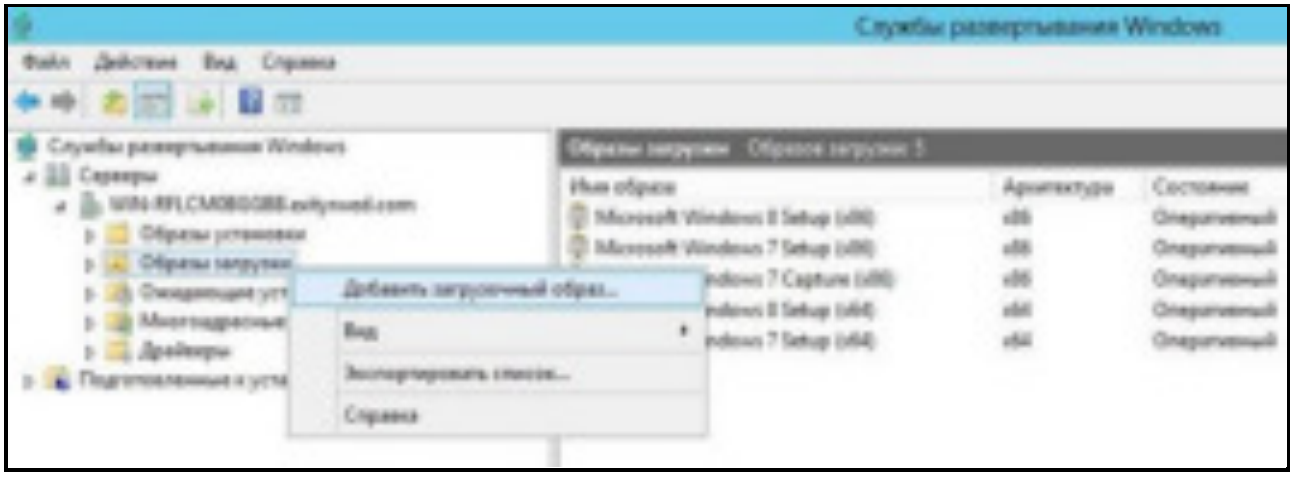

Процесс обновления папки развертывания успешно завершен




Перейдем на раздел E: в папку DeploymentShare, далее откроем папку Boot и смотрим ее содержимое. В ней находятся два файла образа диска и два файла .wim. Образы диска предназначены для записи на диск. В нашем случае мы воспользуемся файлами .wim. Так как у нас установлена служба развертывания WDS, добавим файлы LiteTouchPE_x64.wim и LiteTouchPE_x86.wim в список загрузочных образов

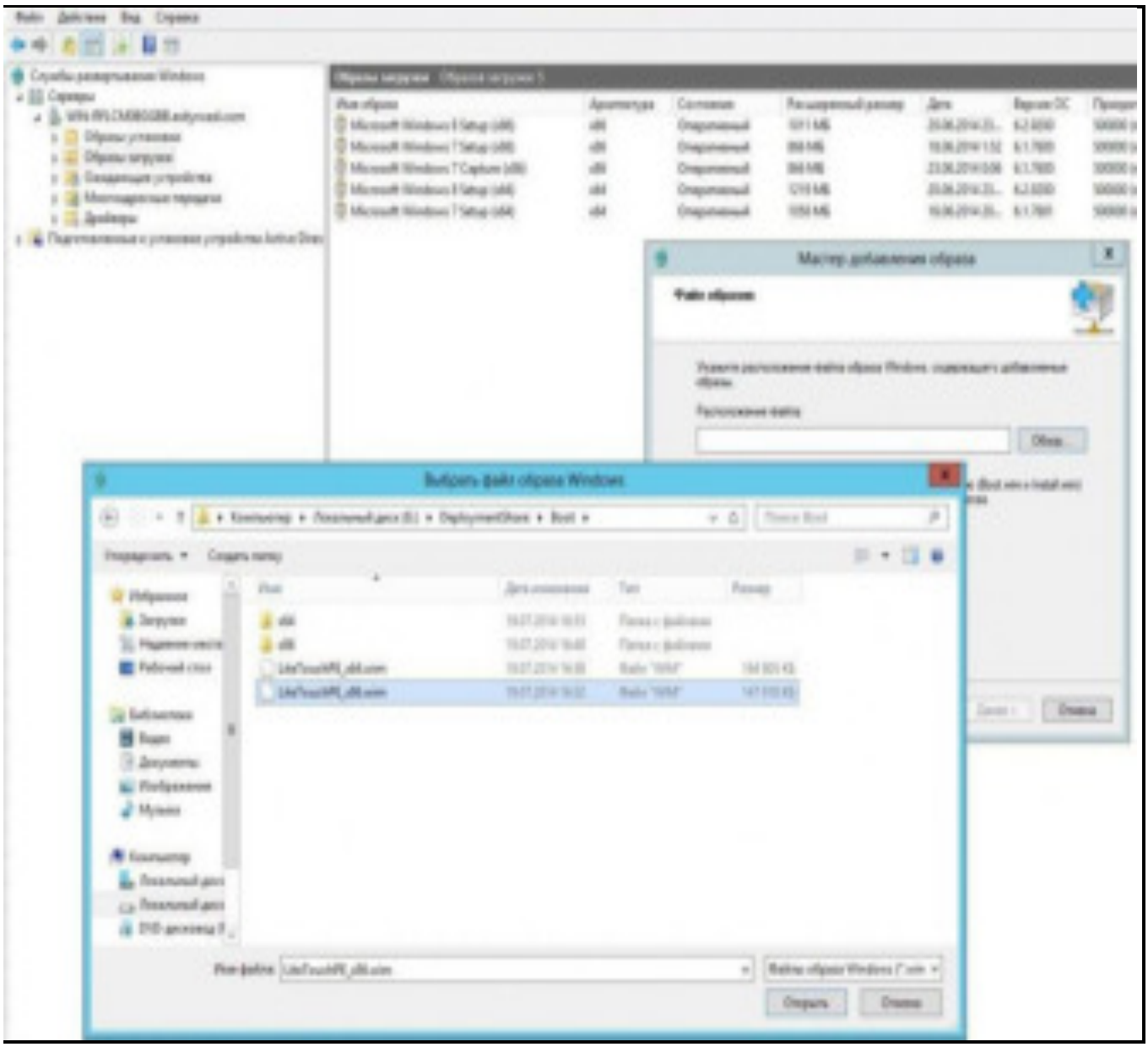



Переходим в консоль управления службами развертывания Windows, выбираем наш сервер WIN-RFLCCM0BGGBB, далее щелкаем по папке образы загрузки и выбираем Добавить загрузочный образ

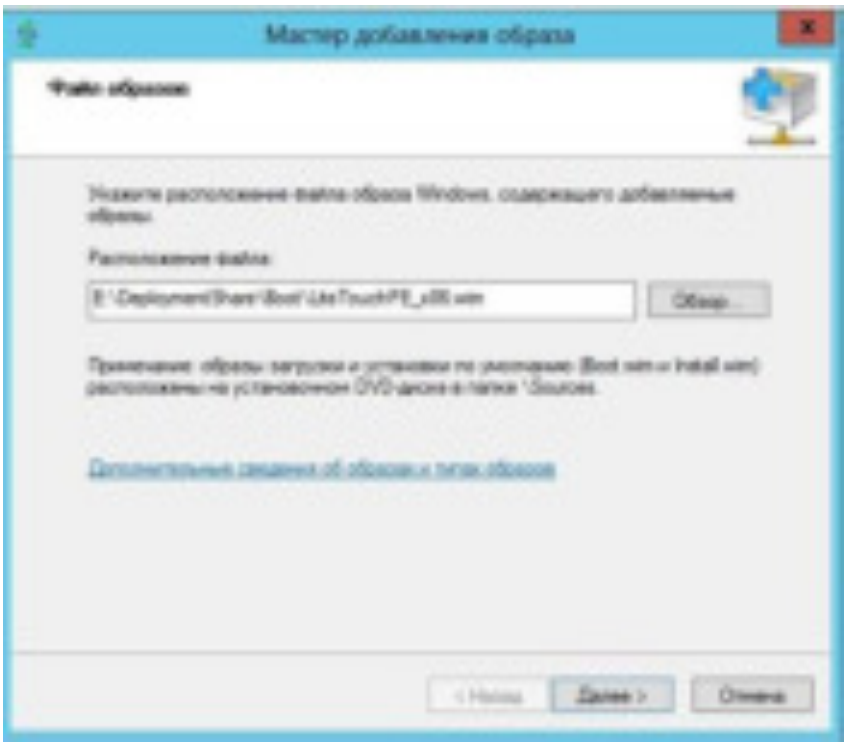



Указываем местоположение загрузочного образа LiteTouchPE_x86.wim, нажимаем Открыть

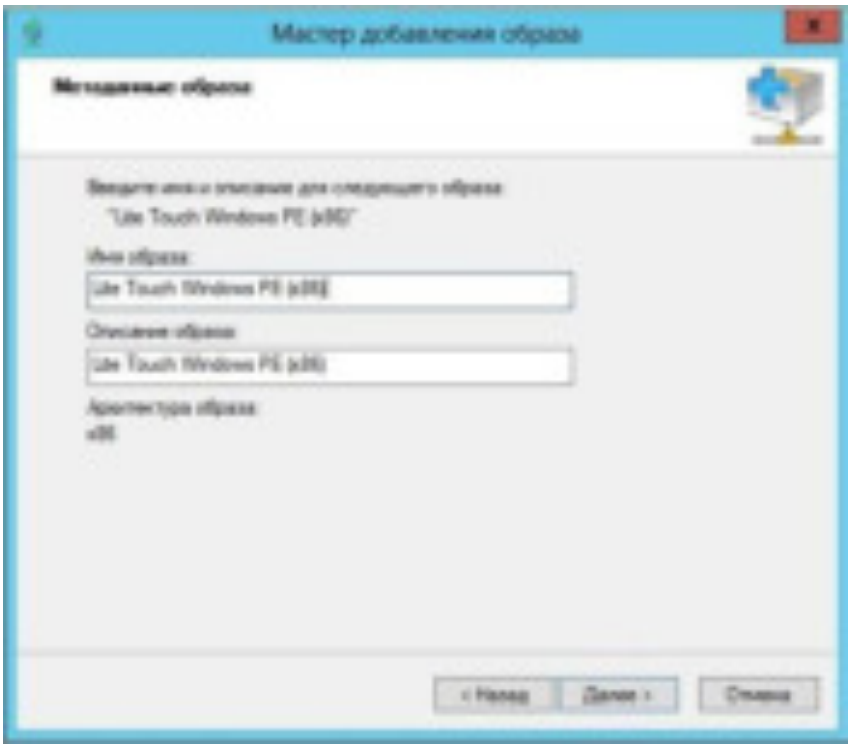
Щёлкните левой мышью и прибавьте скриншот



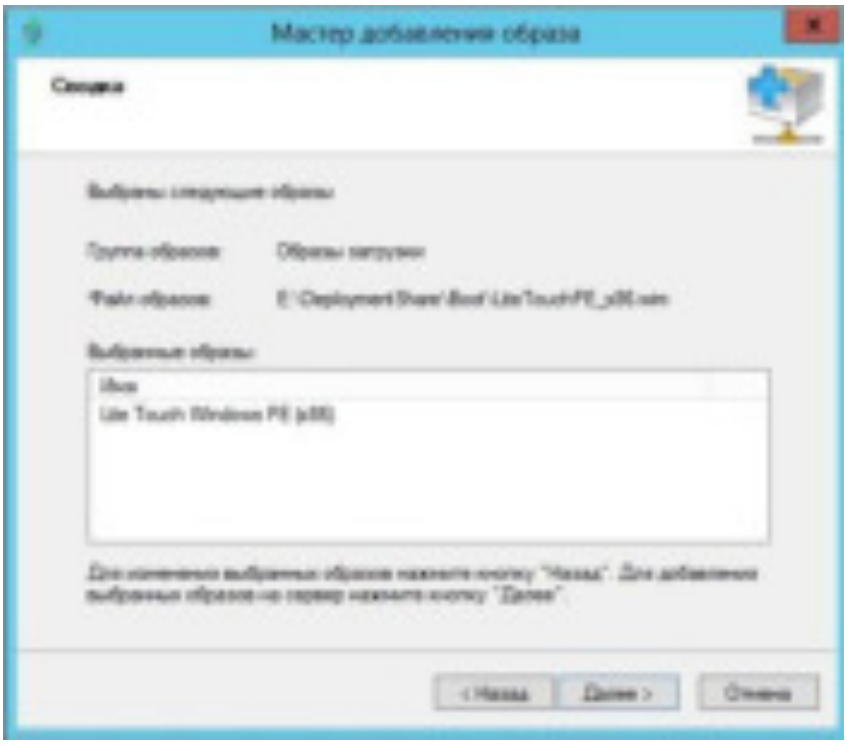

Далее



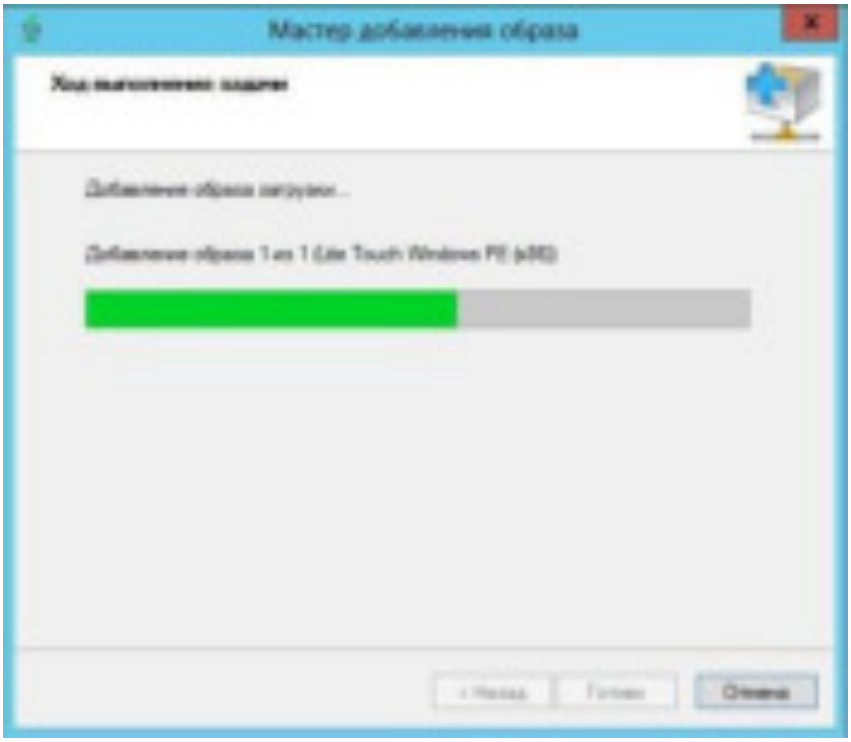

Вводим имя и описание образа (лучше оставить по умолчанию)



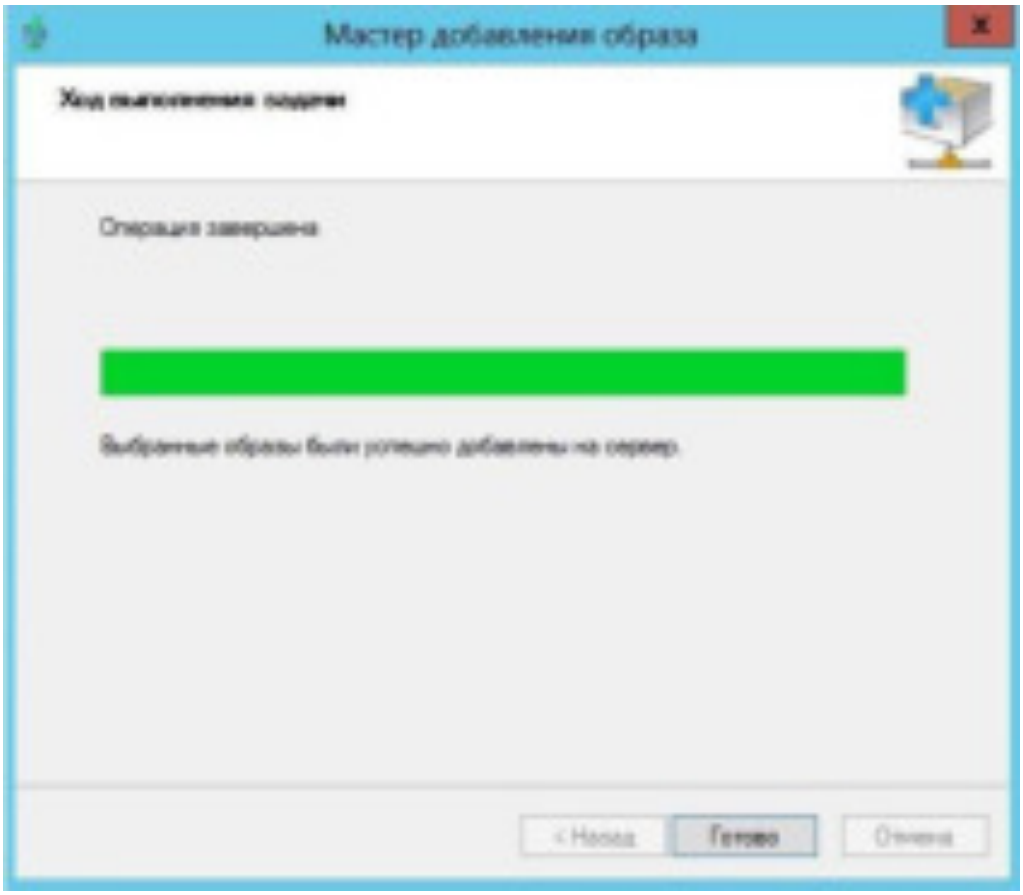

Далее



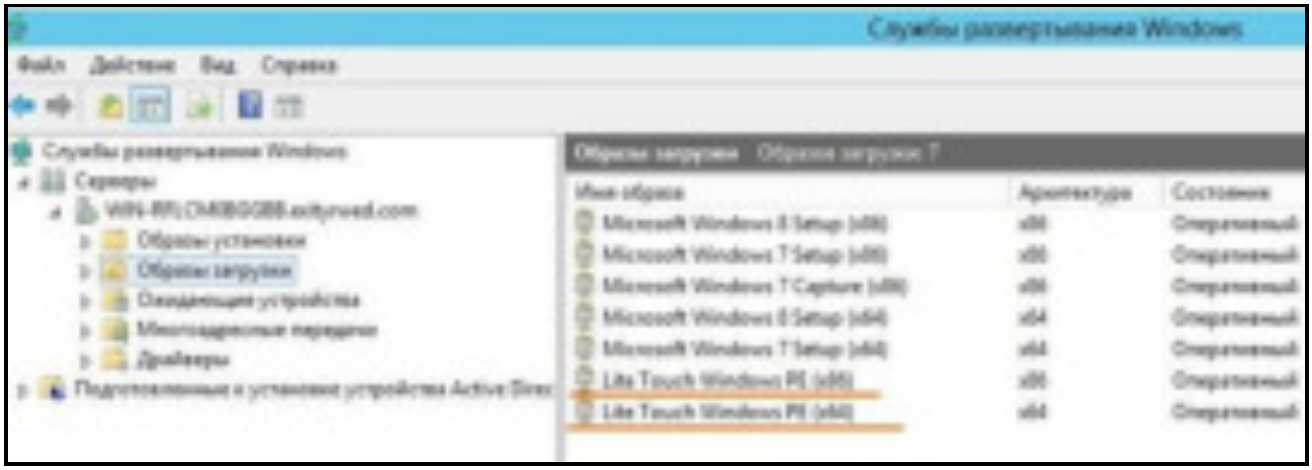

Идет добавление загрузочного образа




Образ успешно добавлен на сервер

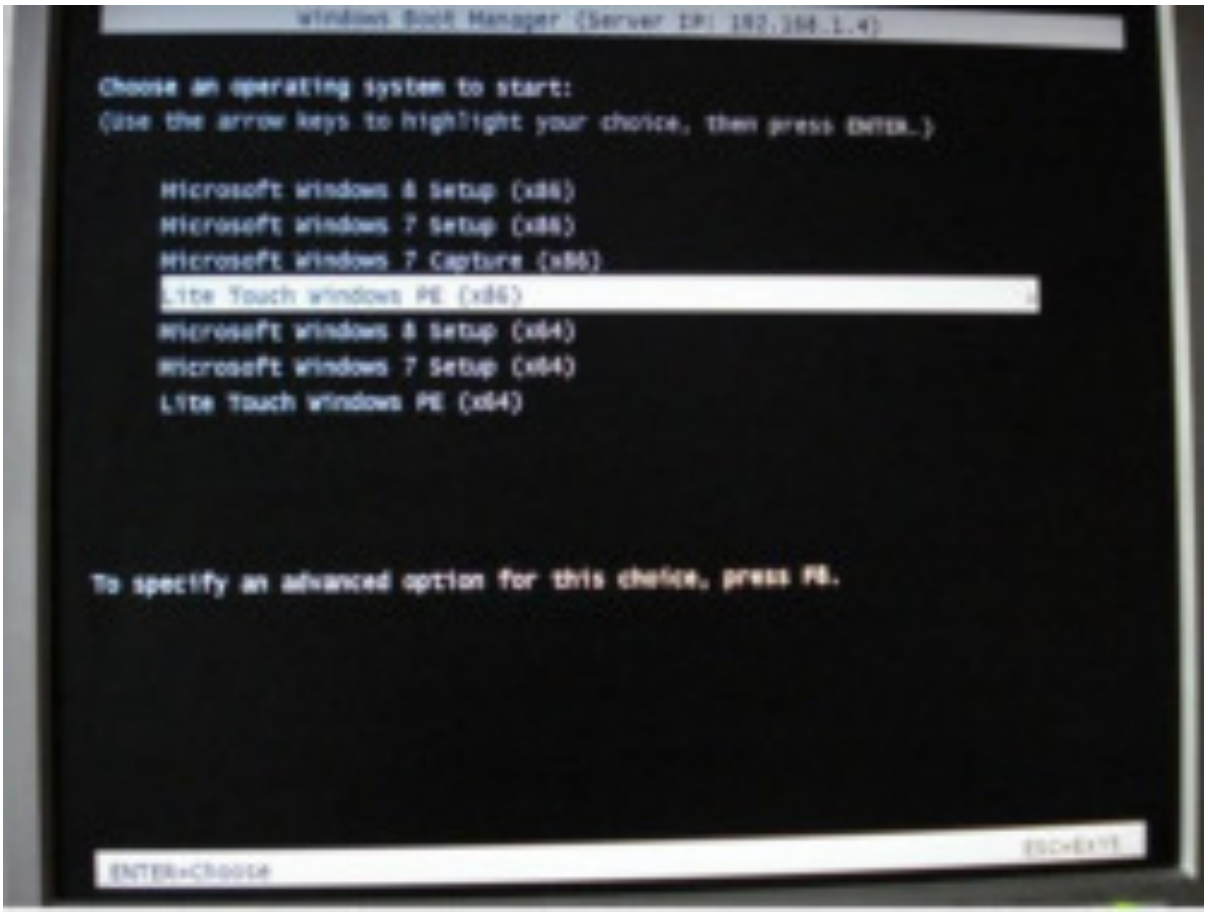



Также добавляем и образ LiteTouchPE_x64.wim. После добавления образов должно получится следующее

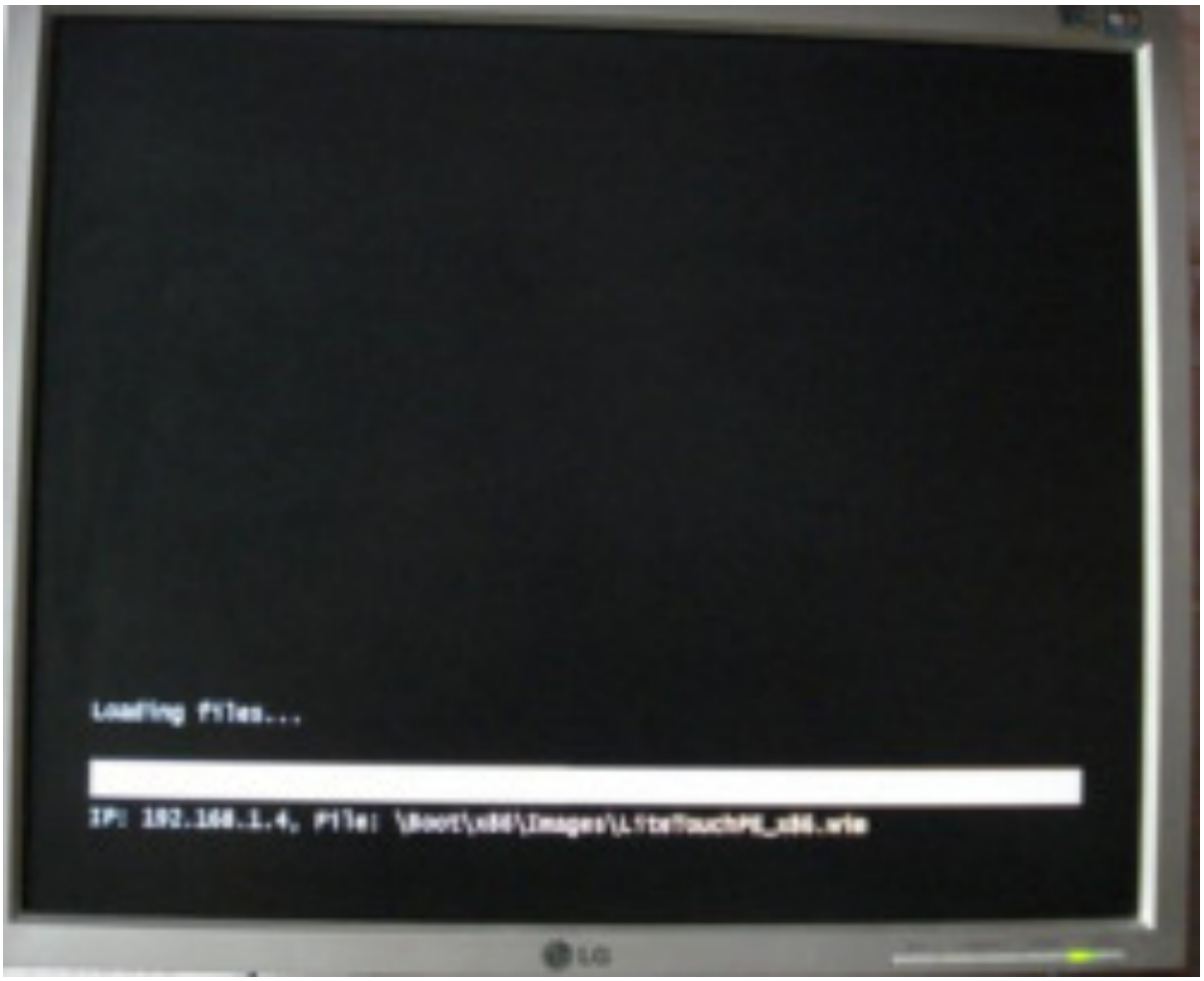



Образы LiteTouch WindowsPE (X86) и (x64) присутствуют в списке загрузочных образов.
Загружаем компьютер на который требуется установить Wndows по сети

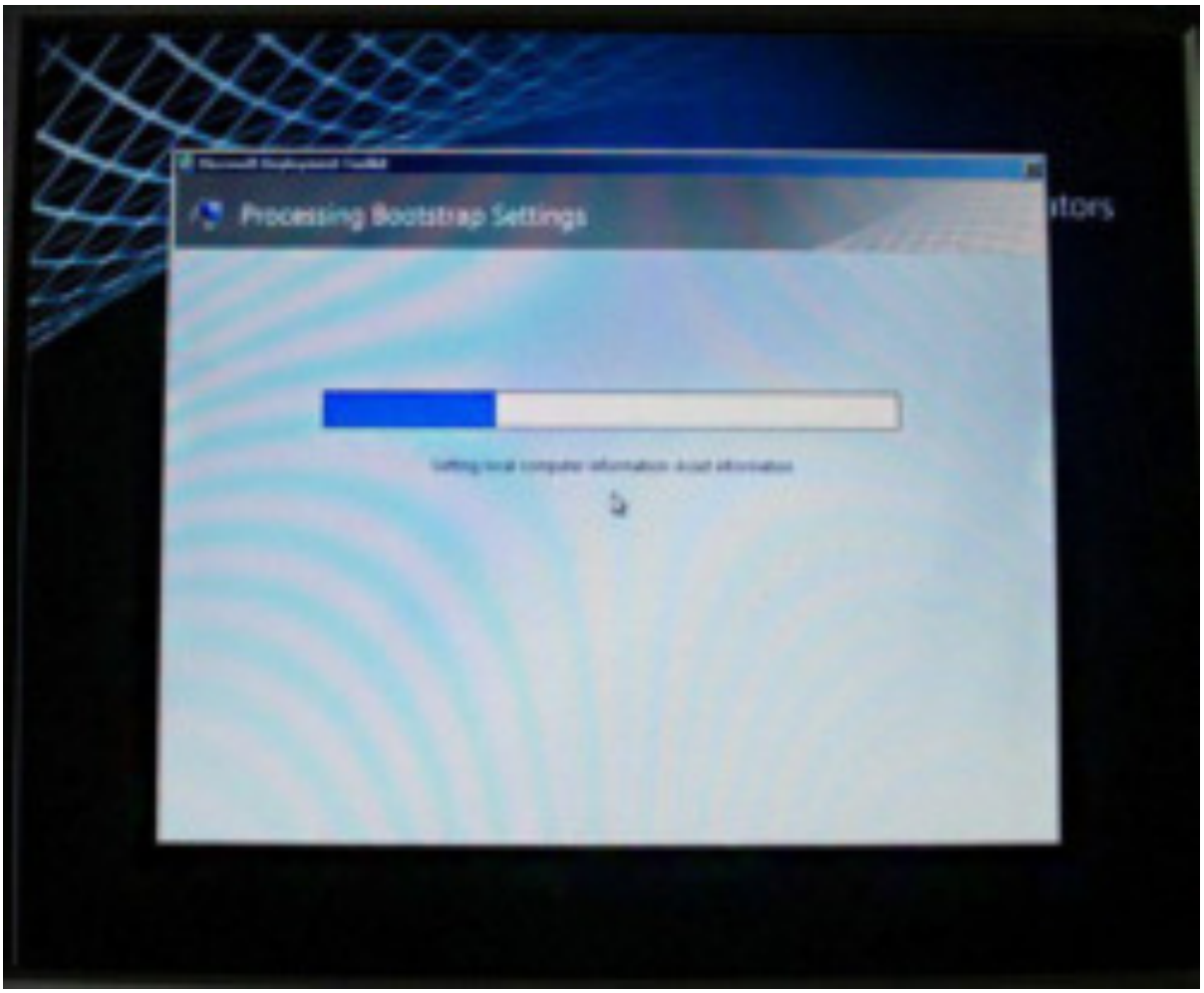

Так как мы будем устанавливать Windows 7 32 разрядную, то выбираем из списка Lite Touch Windows PE (x86)




Идет загрузка


Loading Files...
IP: 192.168.1.4, File: \Boot\x86\Images\LiteTouchPE_x86.wim

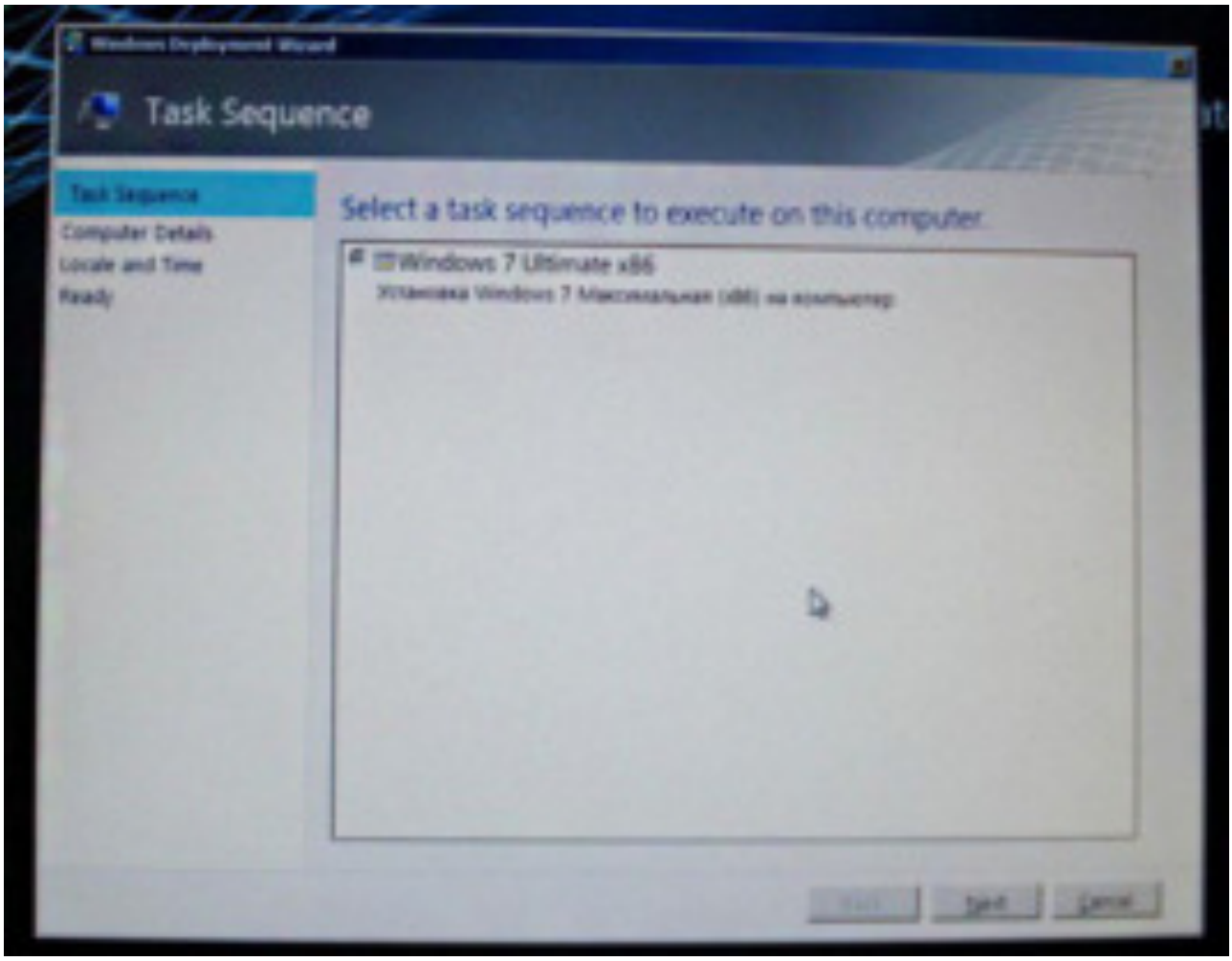

Спустя некоторое время открывается вот такое окно



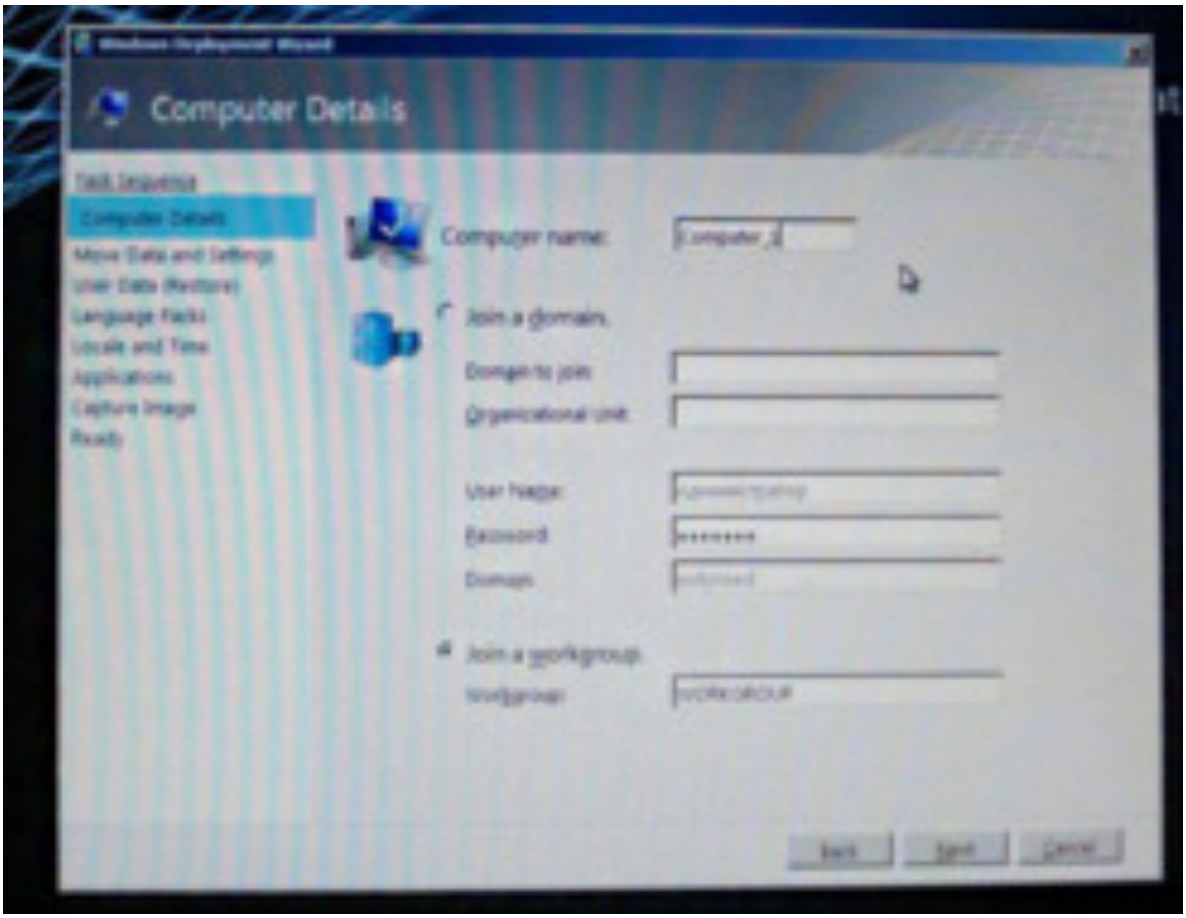

Дальше откроется вот такое окно, в котором щелкаем по пункту Run the Deployment Wizard to install a new Operating System


Дальше откроется вот такое окно, в котором нужно ввести имя пользователя, пароль, домен для подключения к сетевой папке развёртывания


После ввода данных откроется вот такое окно, в котором видим созданную нами последовательность задач  под названием Windows 7 Ultimate x86. Ее и выбираем

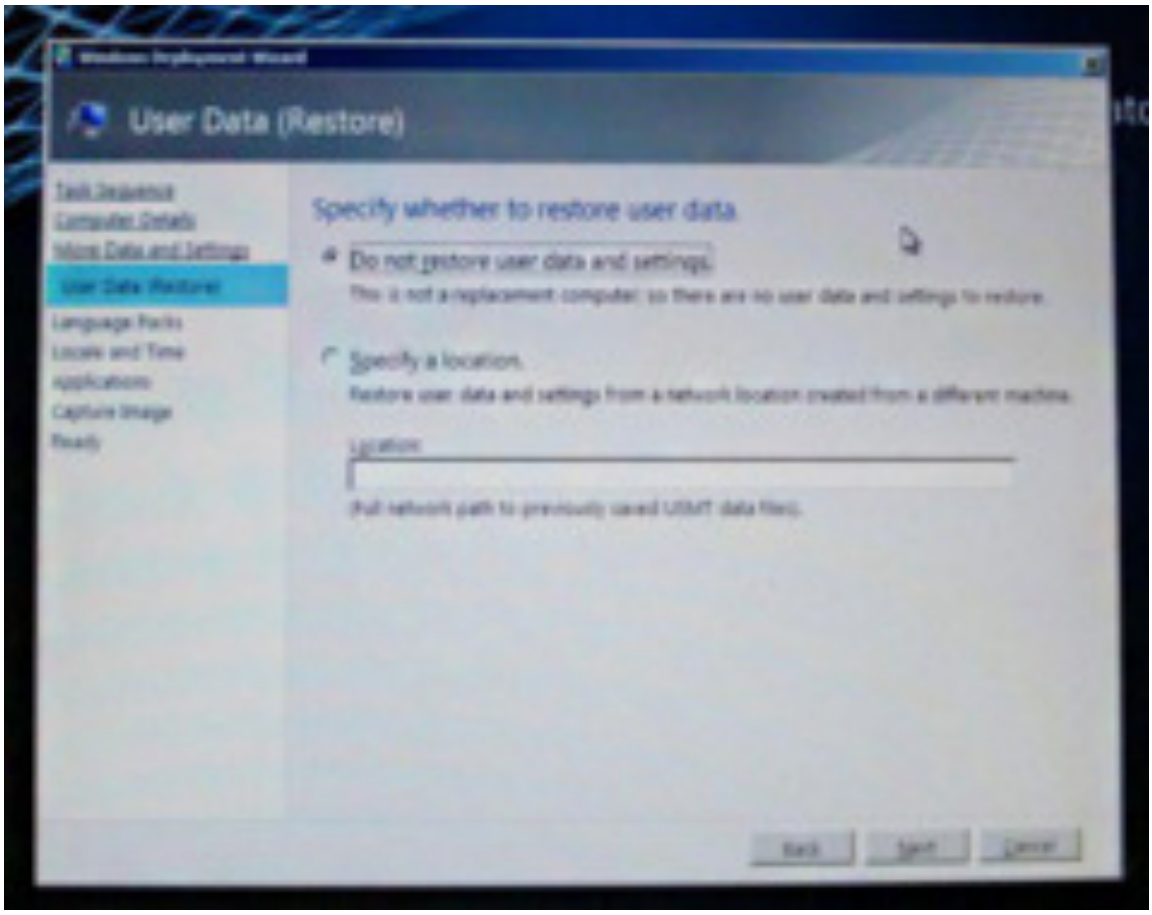



Вводим имя компьютера, в нашем случае это будет Computer_1, Далее.

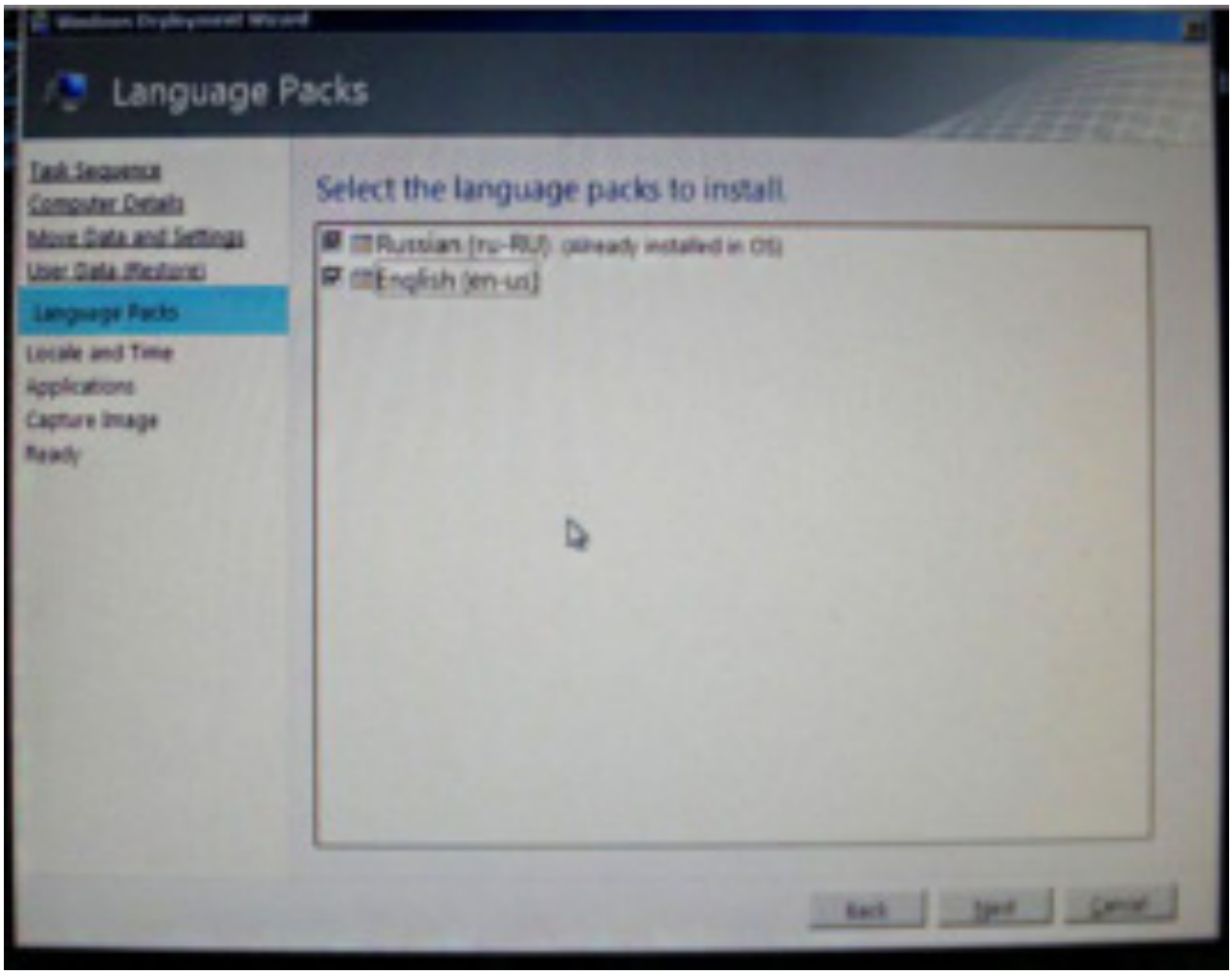



Выбираем Do not move user data and settings, так как мы устанавливаем систему с нуля

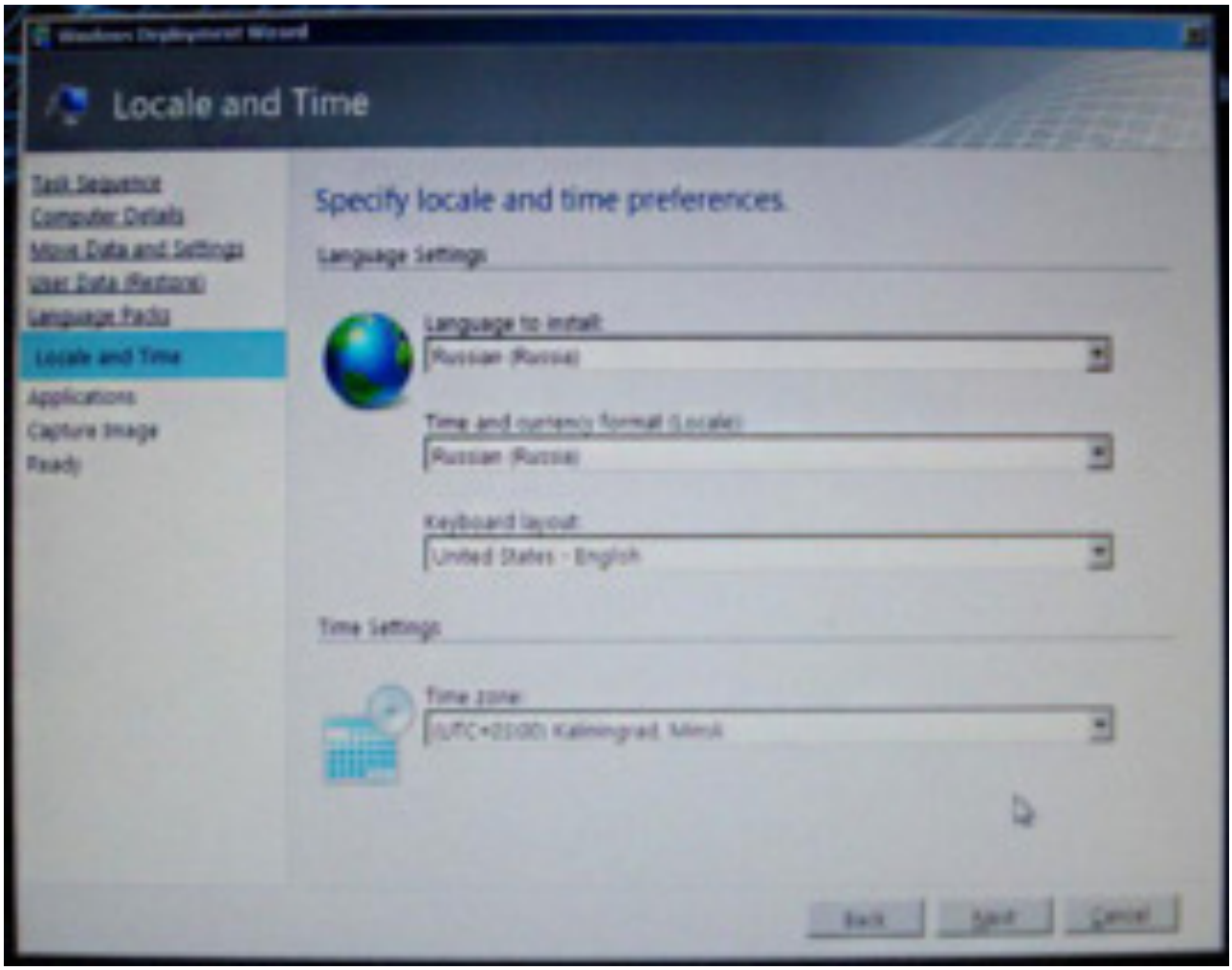

Выбираем Do not restore user data and settings. Далее



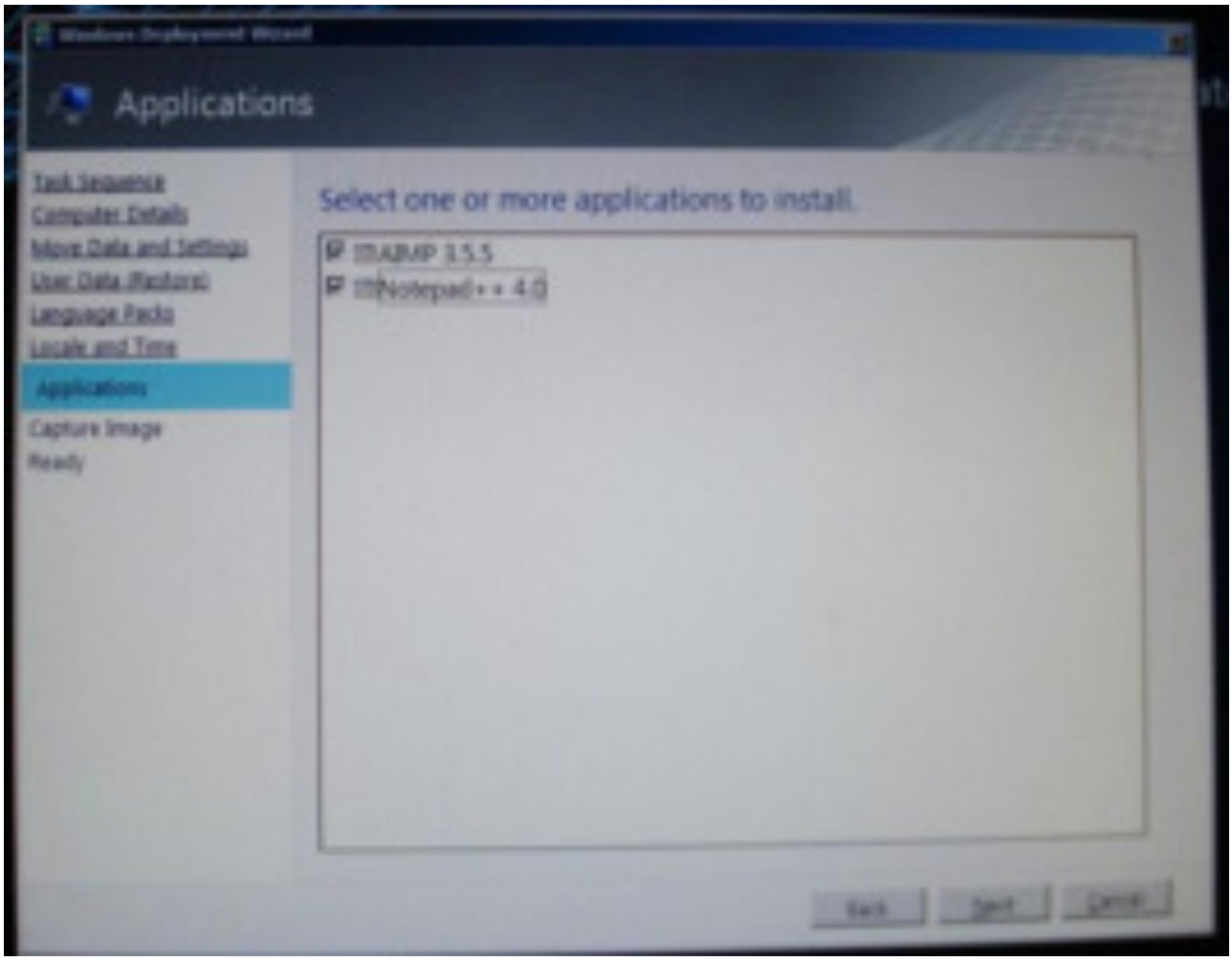

Выбираем наш языковой пакет (английский) который мы хотим установить дополнительно к русскому.



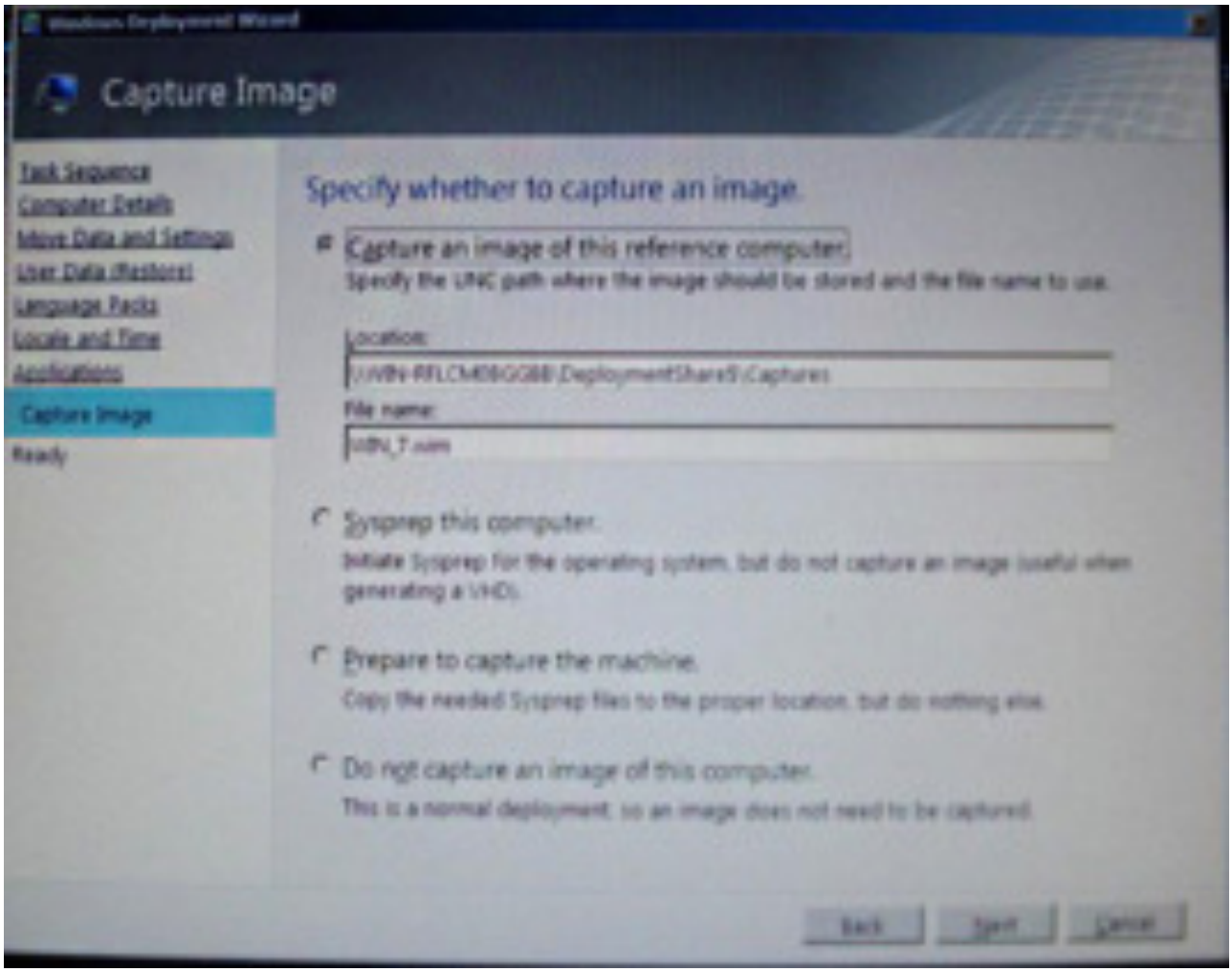

Выбираем языковые параметры, часовой пояс



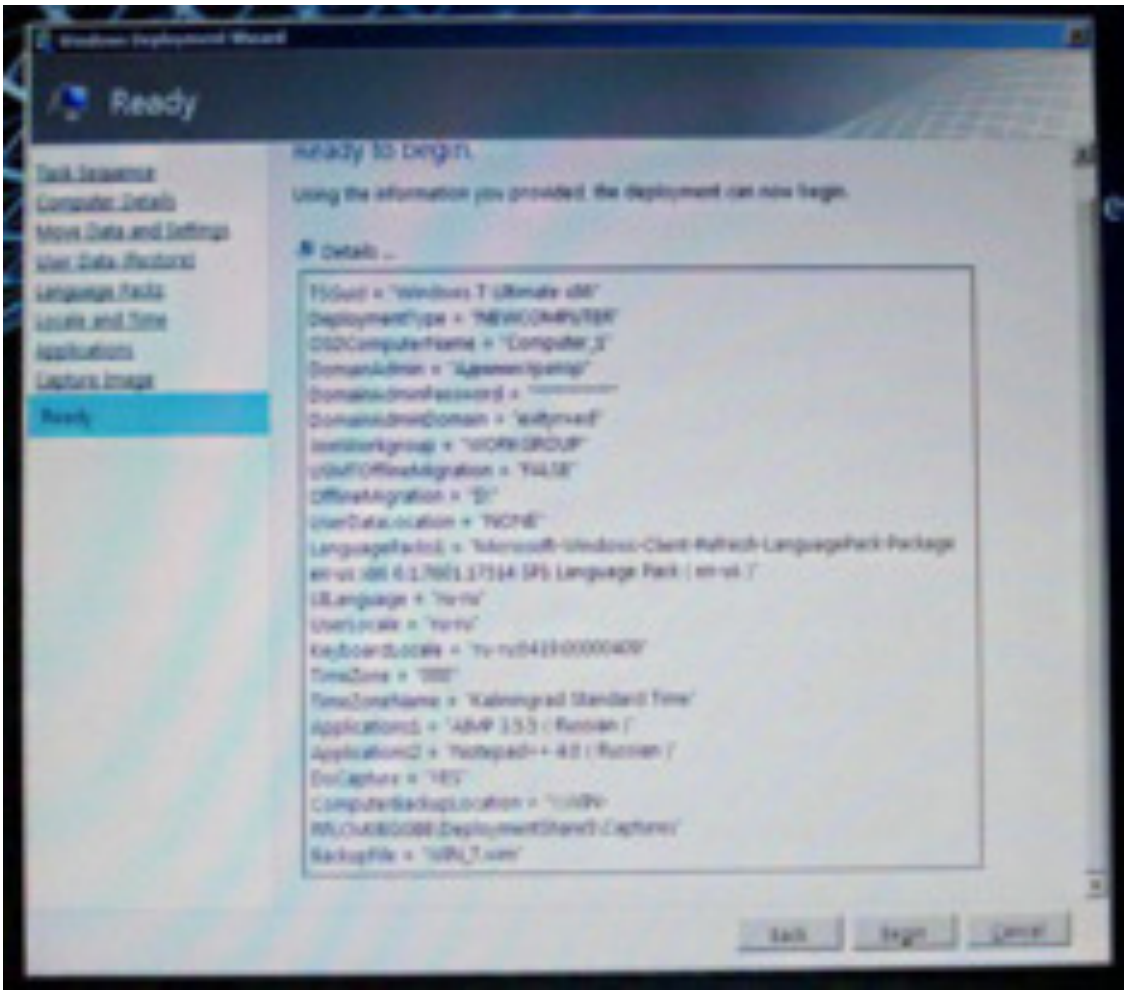

Выбираем приложения, которые хотим установить



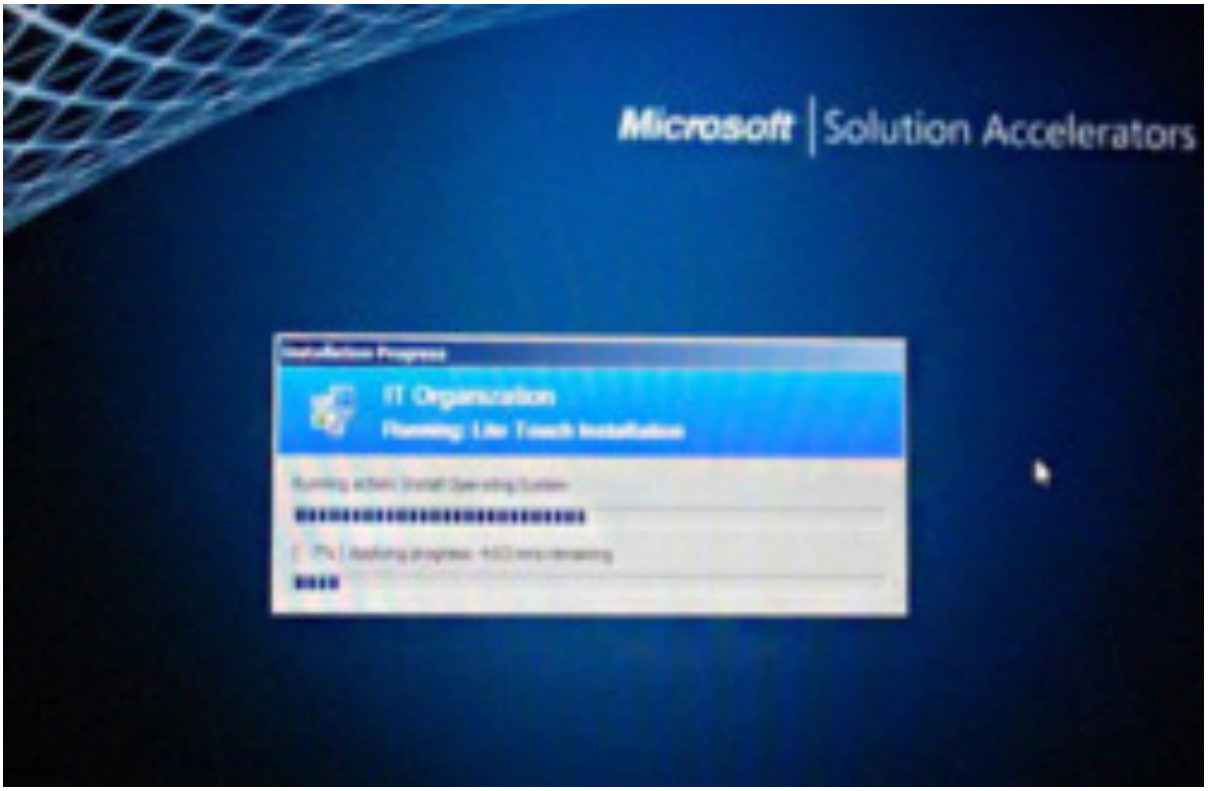

На этом шаге особое внимание нужно уделить пункту Capture an image of this reference computer. Если поставить на него переключатель, то после установки операционной системы она будет обработана улилитой Sysprep и в дальнейшем будет произведен захват подготовленной системы в .wim файл, который будет сохранен в нашей папке развертывания. Далее

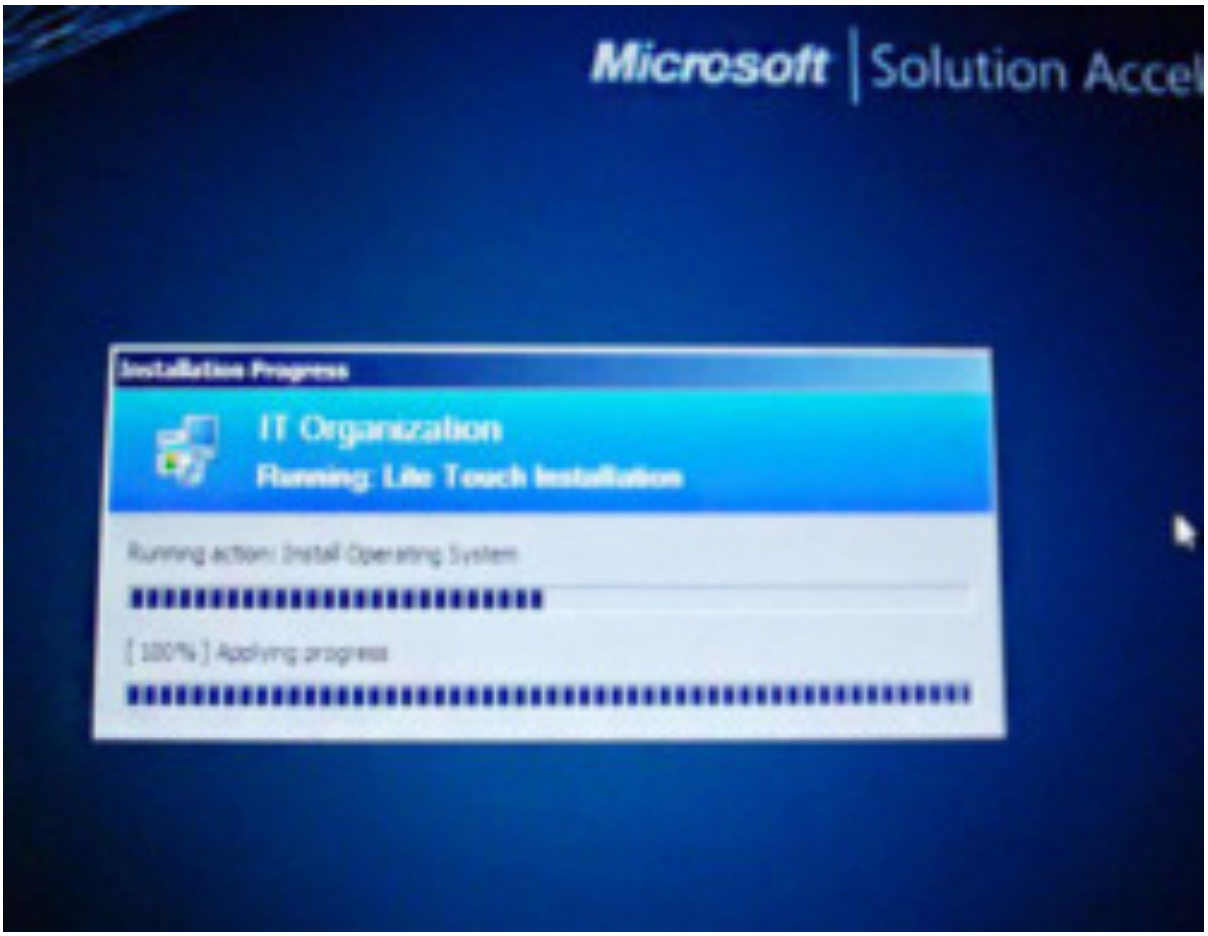



Нажимаем Begin



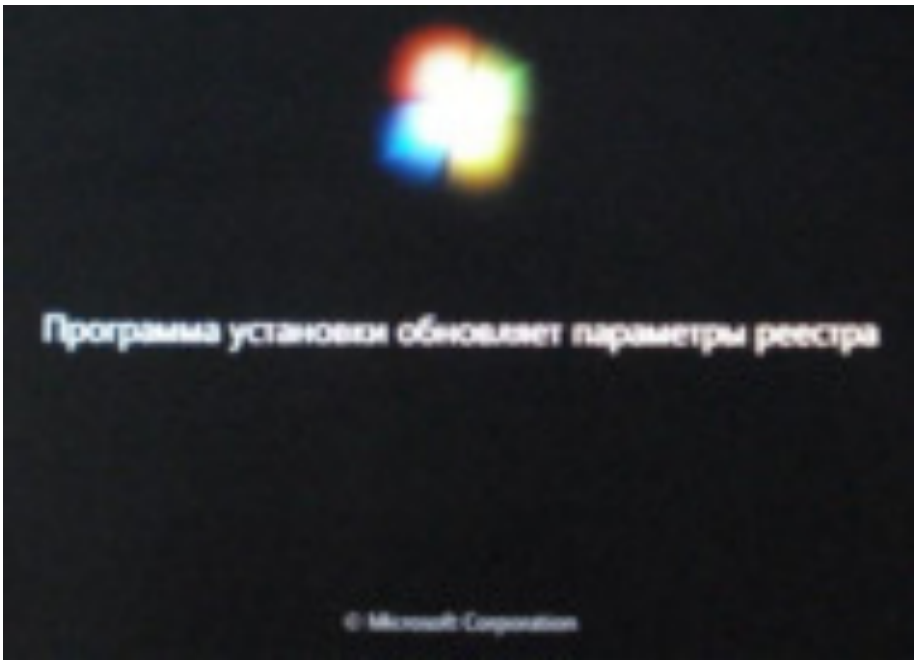

Идет процесс установки операционной системы



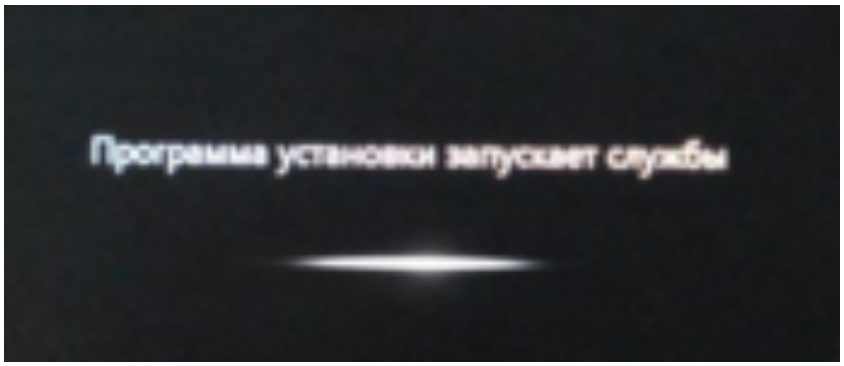



Запуск Windows

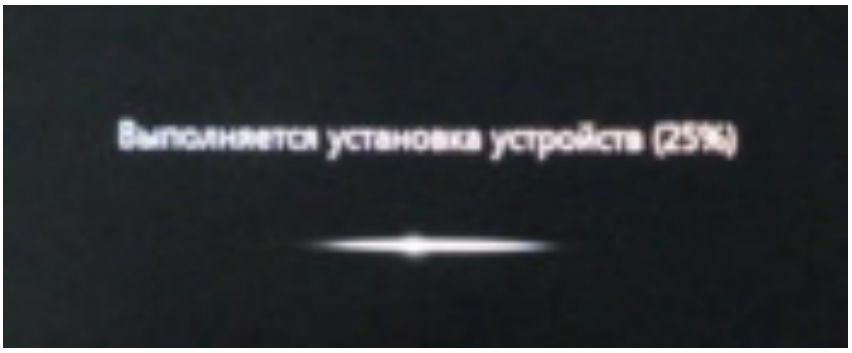

Обновление параметров реестра



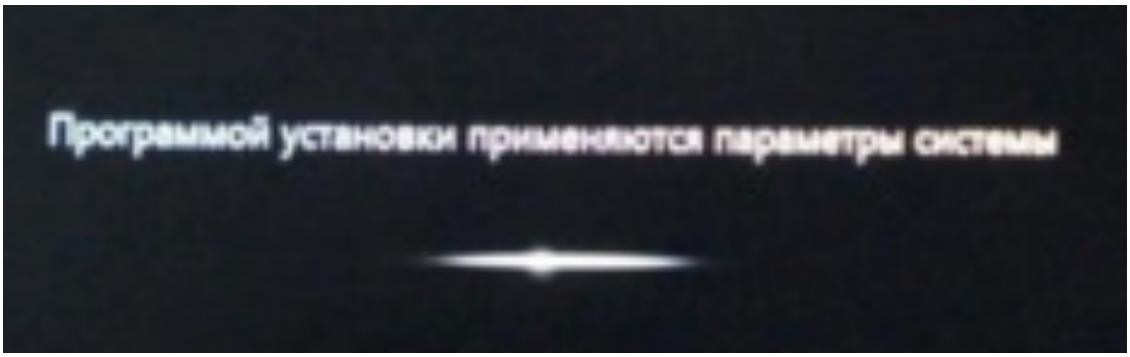

Запуск служб



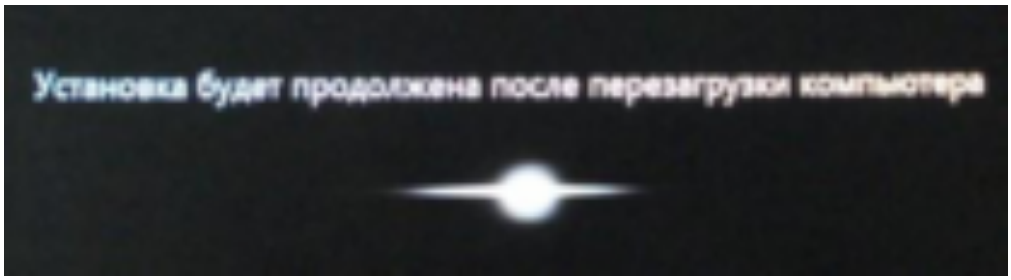

Установка устройств




Применение параметров системы



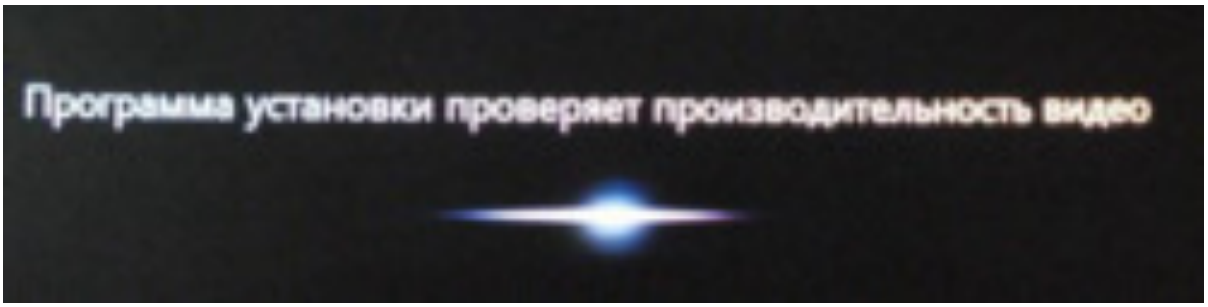

Перезагрузка



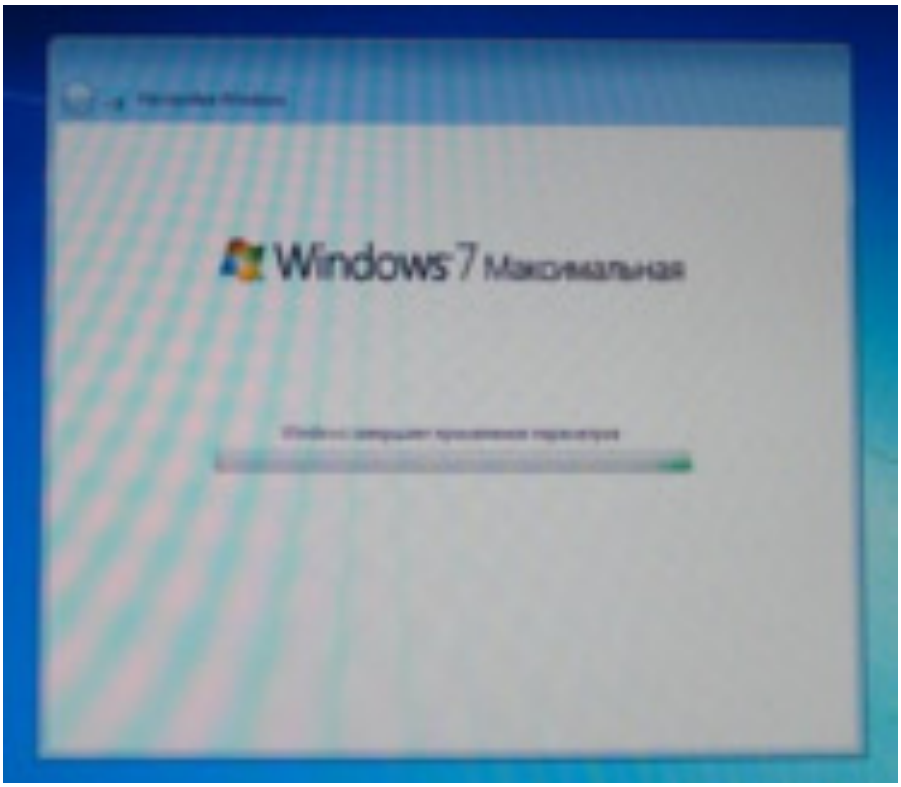

Запуск Windows

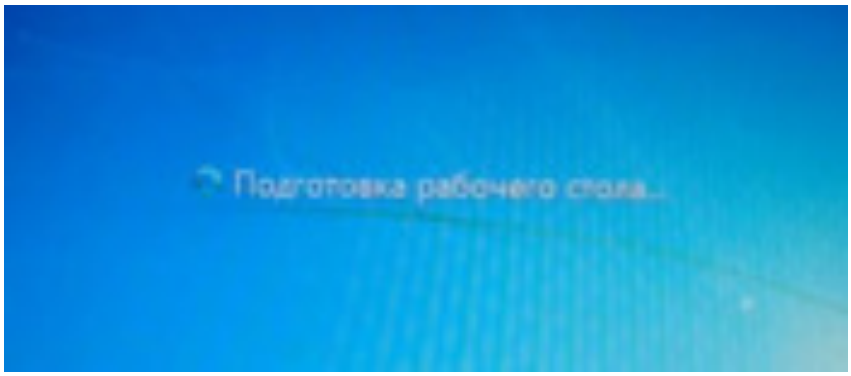

Подготовка к первому использованию


Проверка производительности видео

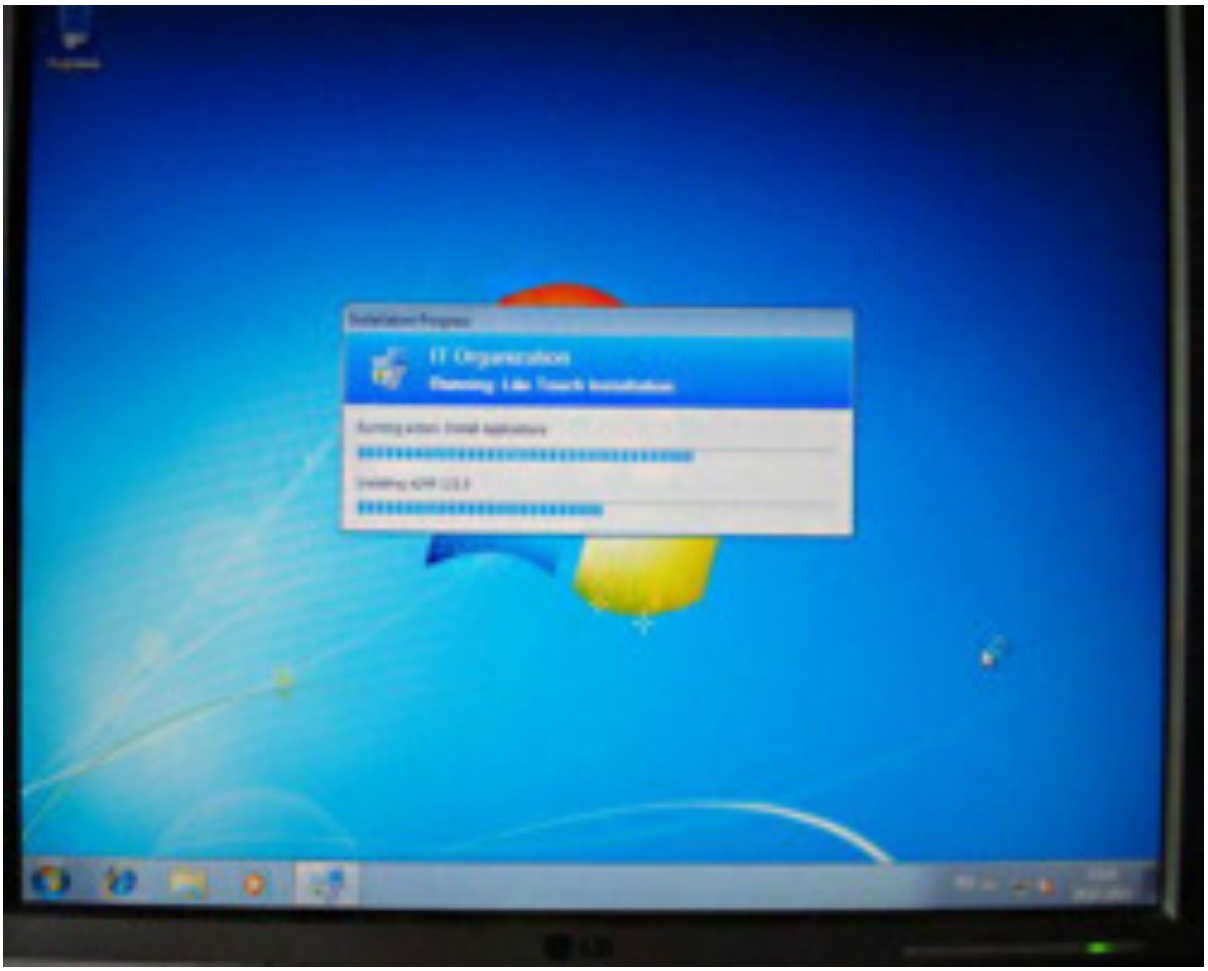



Завершение применения параметров

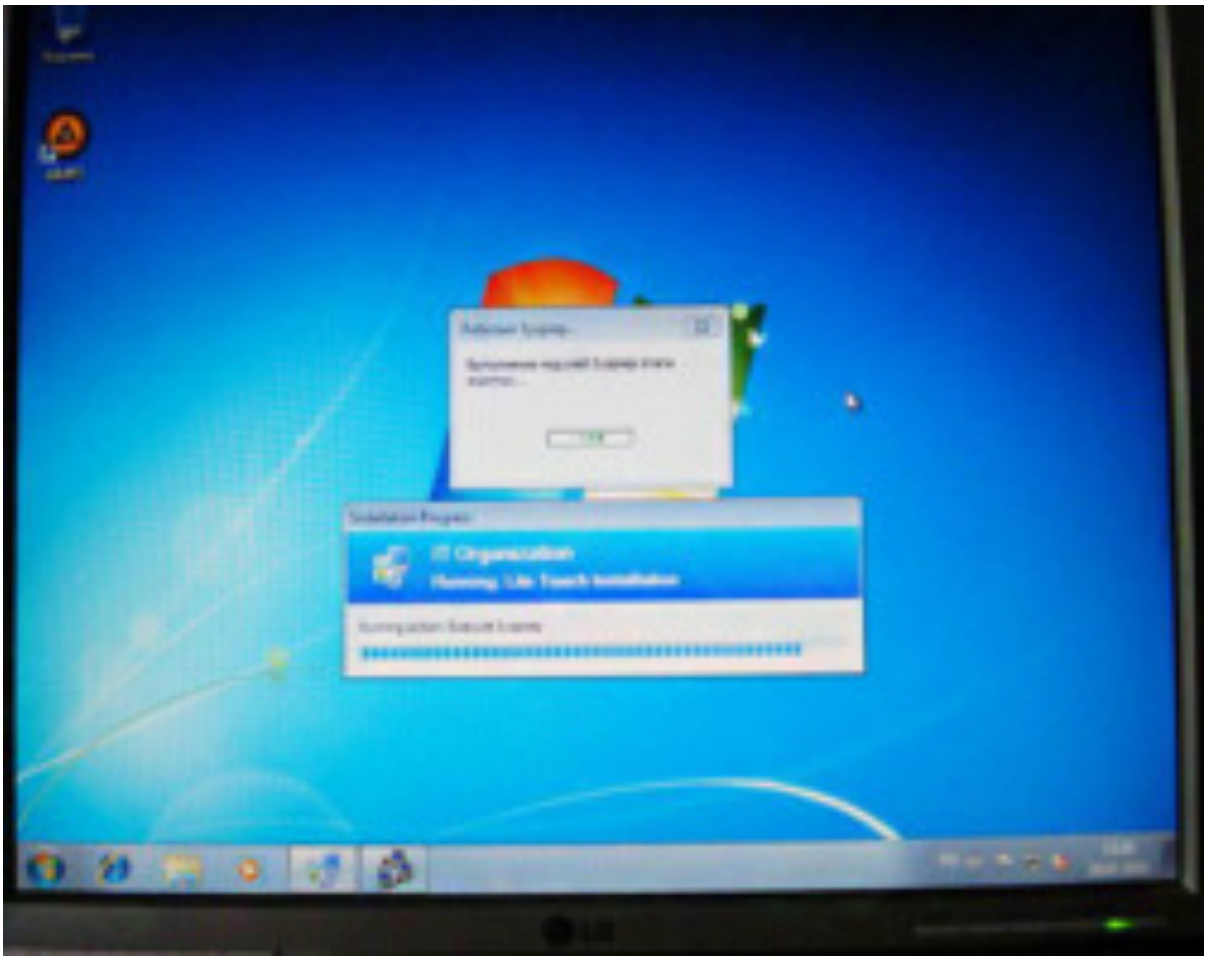




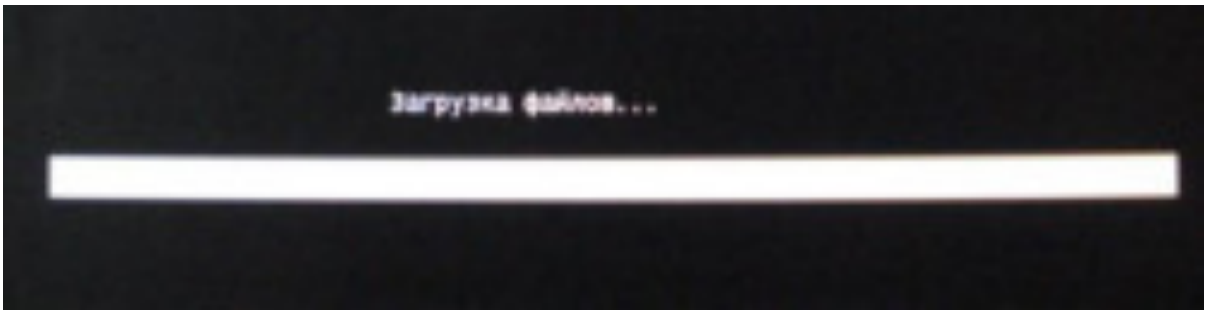

После входа в систему начинается автоматическая установка приложений

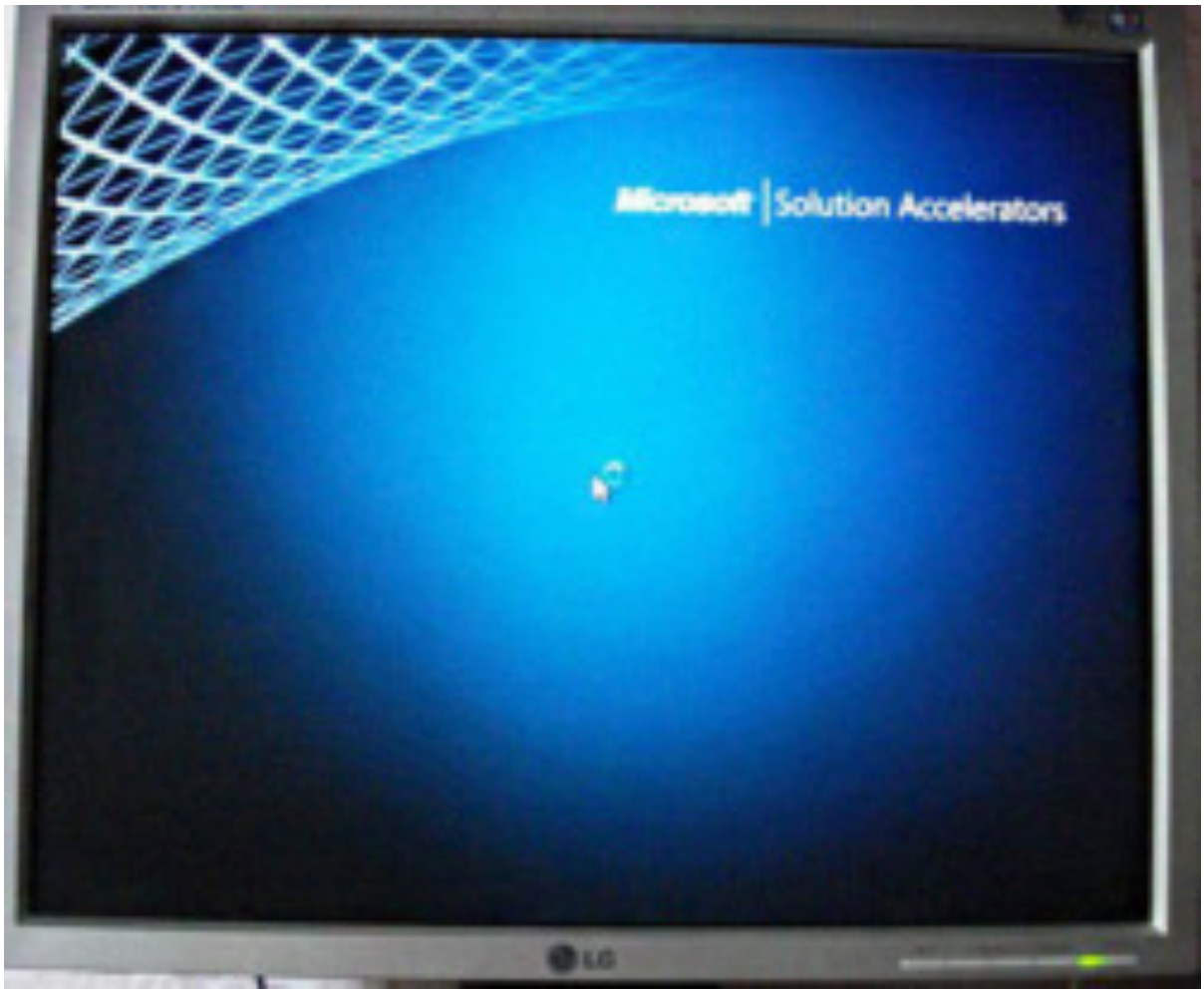



После установки приложений автоматически запускается утилита Sysprep

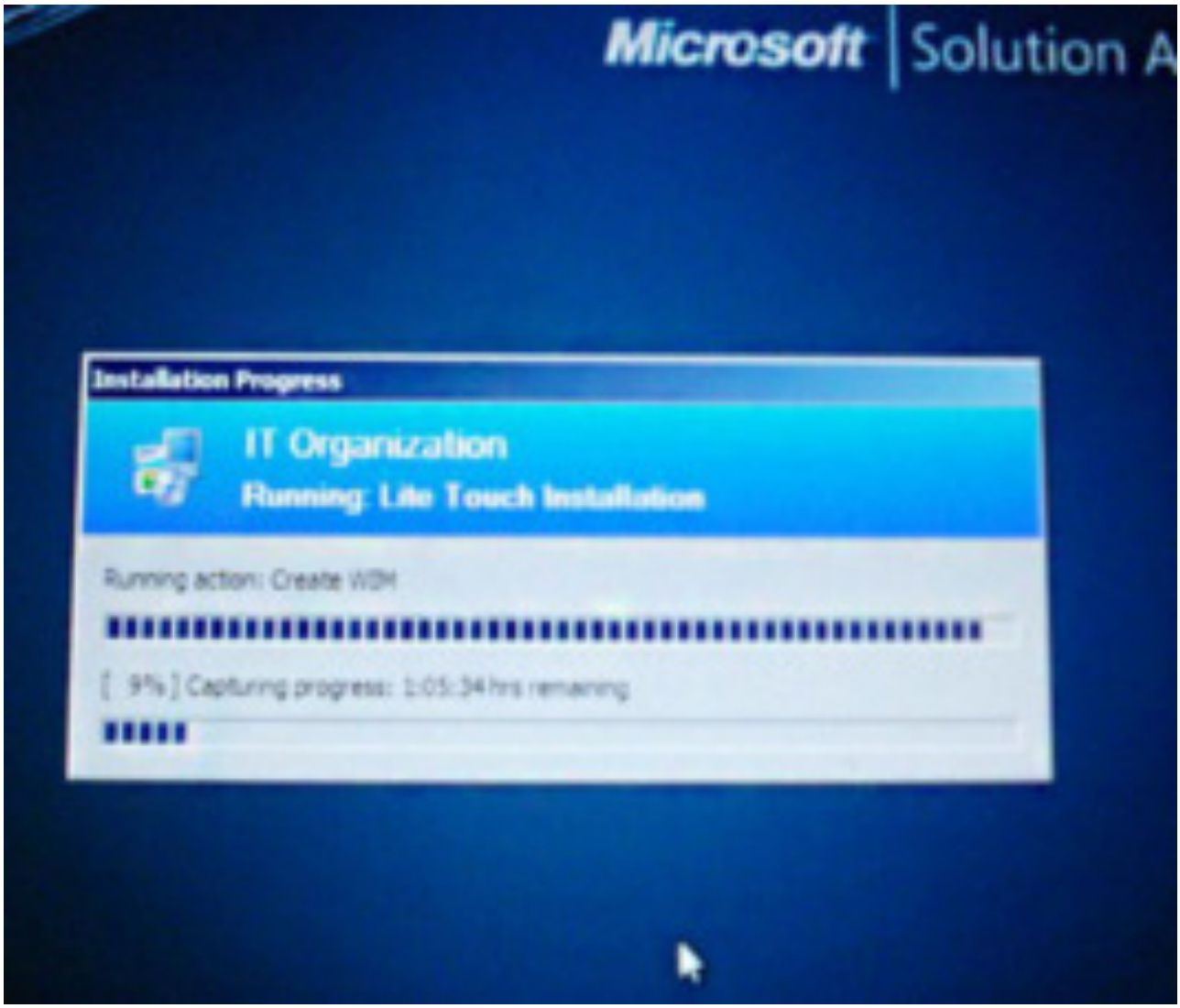


После того как утилита Sysprep отработала компьютер уходит на перезагрузку. Загрузка файлов

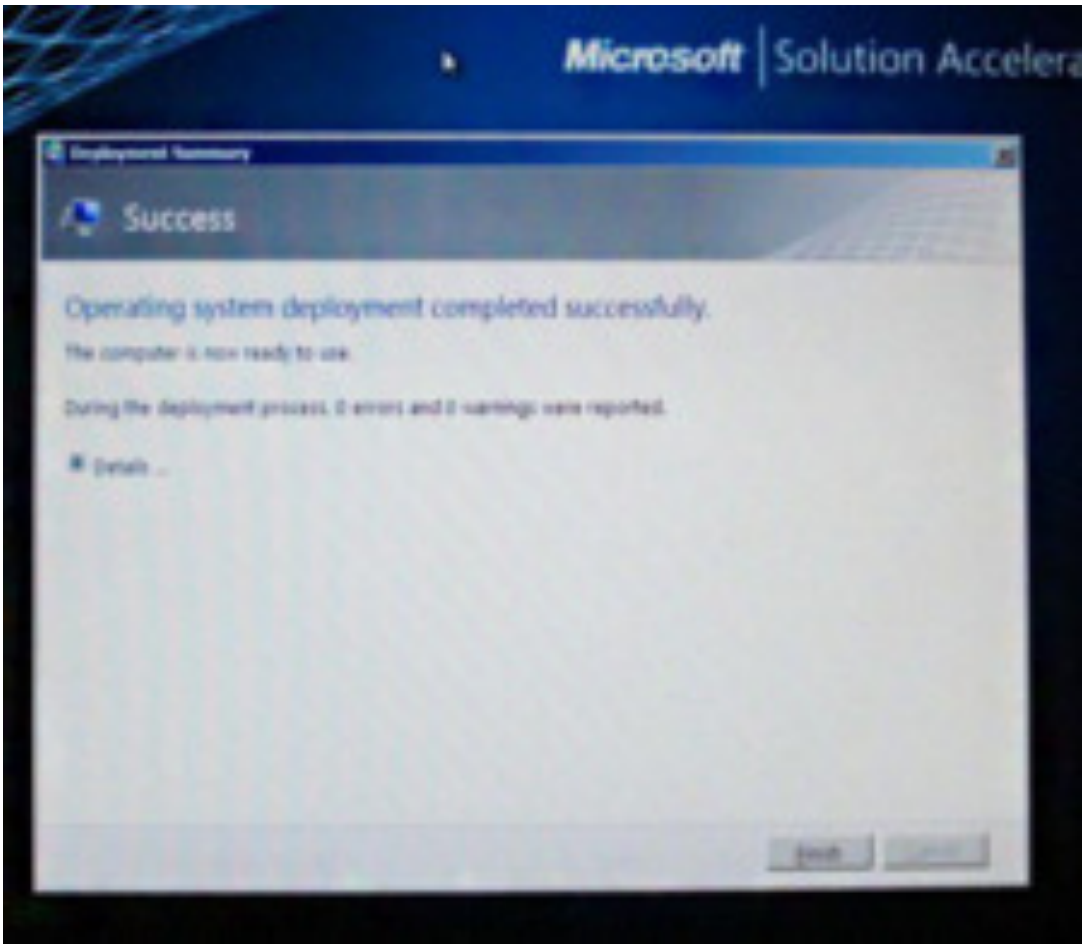




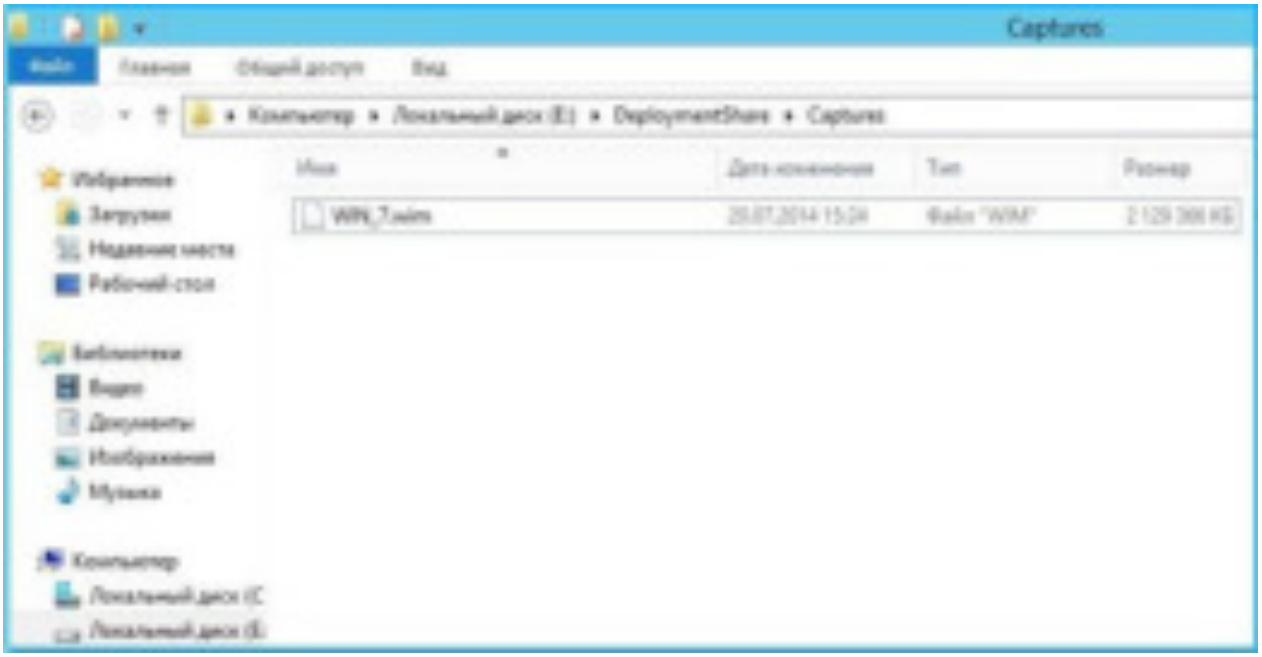

Начался процесс захвата подготовленной при помощи утилиты Sysprep системы в .wim файл




Успешно завершено, 0 ошибок, 0 предупреждений.




Заходим на наш сервер на раздел E: в папку DeploymentShare, далее в папку Captures и видим в ней файл WIN_7.wim, это и есть наш образ захваченной системы.



## Практическое занятие №14 Подготовка среды для развертывания операционной системы

***Цель работы:***
Изучить систему подготовка среды для развертывания операционной системы

Существует несколько способов развертывания операционной системы.

Независимо от используемого метода развертывания необходимо выполнить несколько обязательных действий:

- определение драйверов устройств Windows, необходимых для запуска развертываемого образа загрузки или образа операционной системы;
- определение загрузочного образа, который требуется использовать для запуска конечного компьютера
- использование последовательности задач для записи образа операционной системы, который требуется развернуть; кроме того, можно использовать образ операционной системы по умолчанию;
- передача загрузочного образа, образа операционной системы и другого связанного содержимого на точку распространения;
- создание последовательности задач с шагами для развертывания образа загрузки и образа операционной системы;
- развертывание последовательности задач в коллекции компьютеров;
- мониторинг развертывания.

Используем службу развертывания Windows (WDS) — которая является дополнением к набору продуктов Windows. В стандартной конфигурации WDS обеспечивает развертывание виртуальных машин (ВМ) Windows, а если внести небольшие изменения, его можно использовать также для создания серверов Linux и VMware. Причем все это можно сделать из меню загрузки с возможностью выбора Preboot eXecution Environment (PXE).

Чтобы настроить WDS для развертывания систем Windows и Linux, необходимо внести несколько изменений в командной строке. Нужно заменить загрузчик PXE, используемый Windows, на загрузчик для Linux. После этого создается пункт меню, позволяющий меню загрузки PXE для Linux переключаться на меню Windows для загрузки Windows, а для создания веб-интерфейса для загрузки файлов конфигурации Linux используется IIS.

Настройки WDS, позволяют развертывать Windows, CentOS и ESXi.

На пустом сервере Windows нужно выделить диск C: объемом 60 ГБ для операционной системы и диск WDS объемом 300 ГБ для различных файлов

WIM, необходимых для развертывания Windows, и для файлов установки Linux.

Установка и настройка выполняются в несколько этапов:

**Настройка сервера WDS**

На сервере должны быть установлены WDS и IIS. Это можно сделать с помощью программы Windows Server Manager или с помощью PowerShell.

```
Install-WindowsFeature –name Web-server -
includemanagementtools
Install-Windowsfeature –name WDS -includemanagementtools
```

Теперь, когда у нас установлен базовый сервер служб развертывания Windows, нужно внести некоторые изменения в пул DHCP. При желании можно добавить вторую сетевую плату на этот сервер и создать выделенную сеть, но мы будем создавать серверы в основной сети, поэтому обновим центральный сервер DHCP с помощью дополнительных атрибутов DHCP WDS:

Будем использовать следующие настройки DHCP:

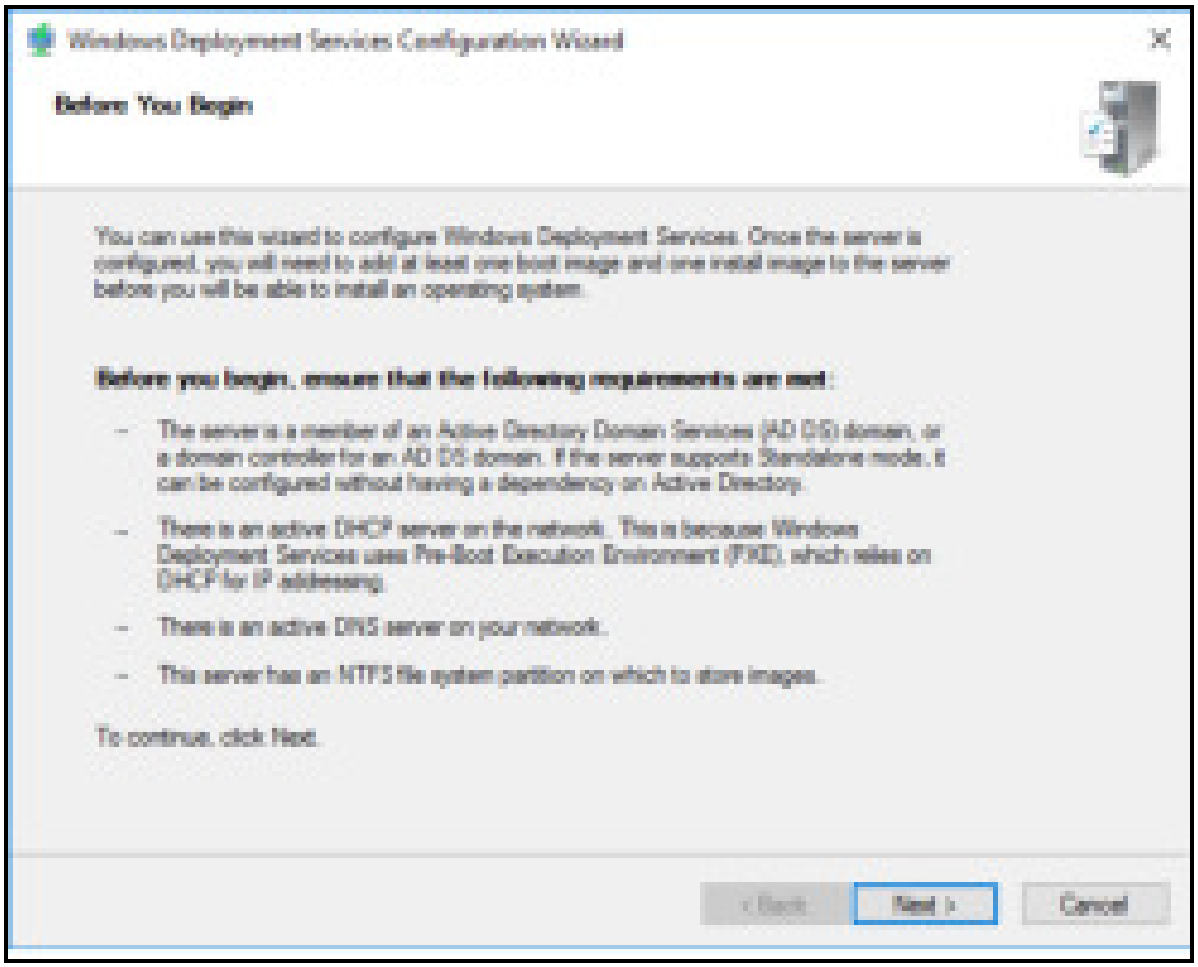
| Option Name | Vendor | Value | Class |
|---|---|---|---|
| 003 Router | Standard | 10.253.1.254 | None |
| 066 Boot Server Host Name | Standard | 10.253.1.26 | None |
| 067 BootFile Name | Standard | boot\pb4\pxelinbp.com | None |
| 006 DNS Servers | Standard | 10.253.1.44, 10.253.1.42 | None |
| 015 DNS Domain Name | Standard | gdvnet.com | None |

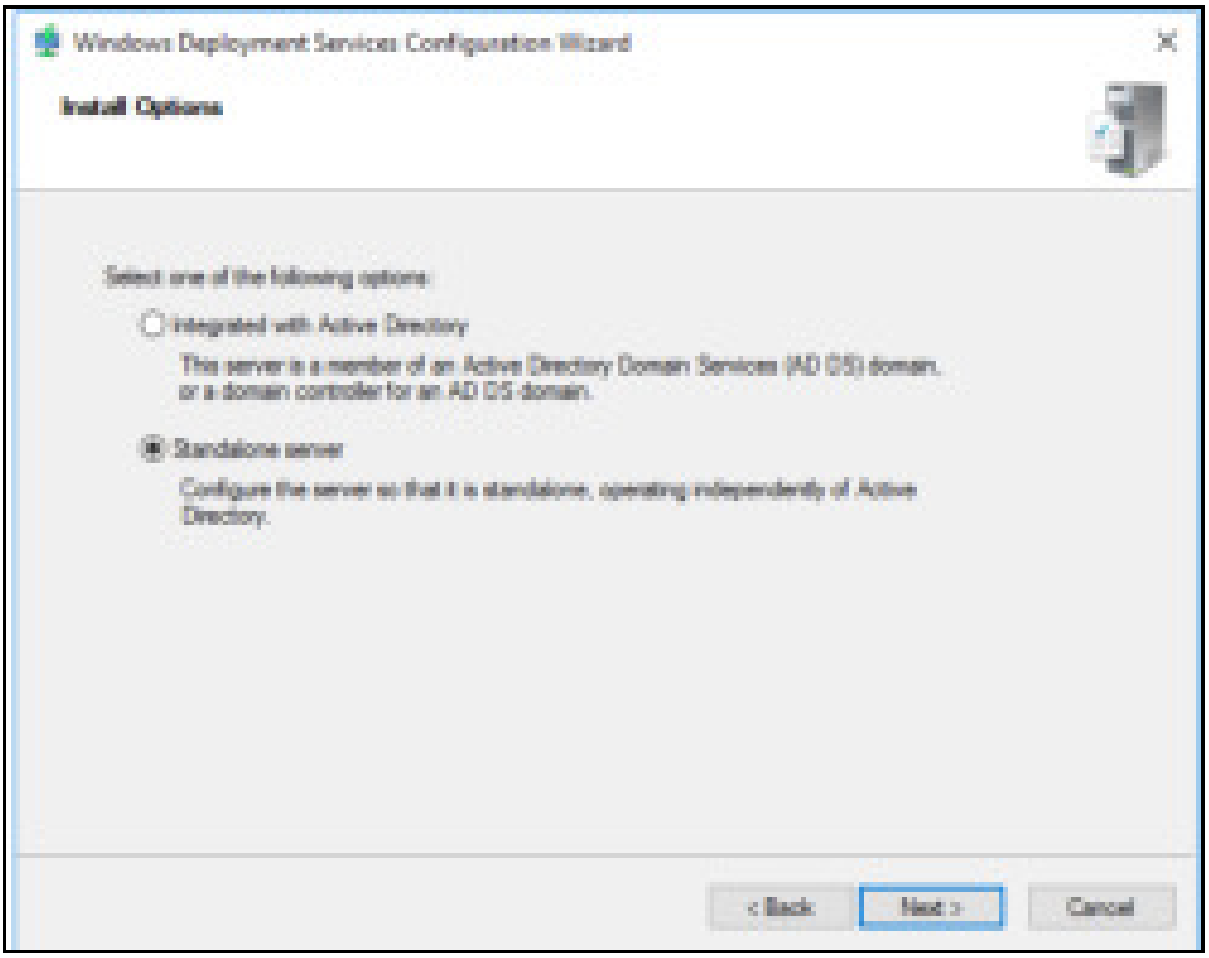
**«Имя узла сервера загрузки»** — IP-адрес сервера WDS.

**«Имя файла загрузки»** — исполняемый файл WDS, который должен быть запущен клиентом.

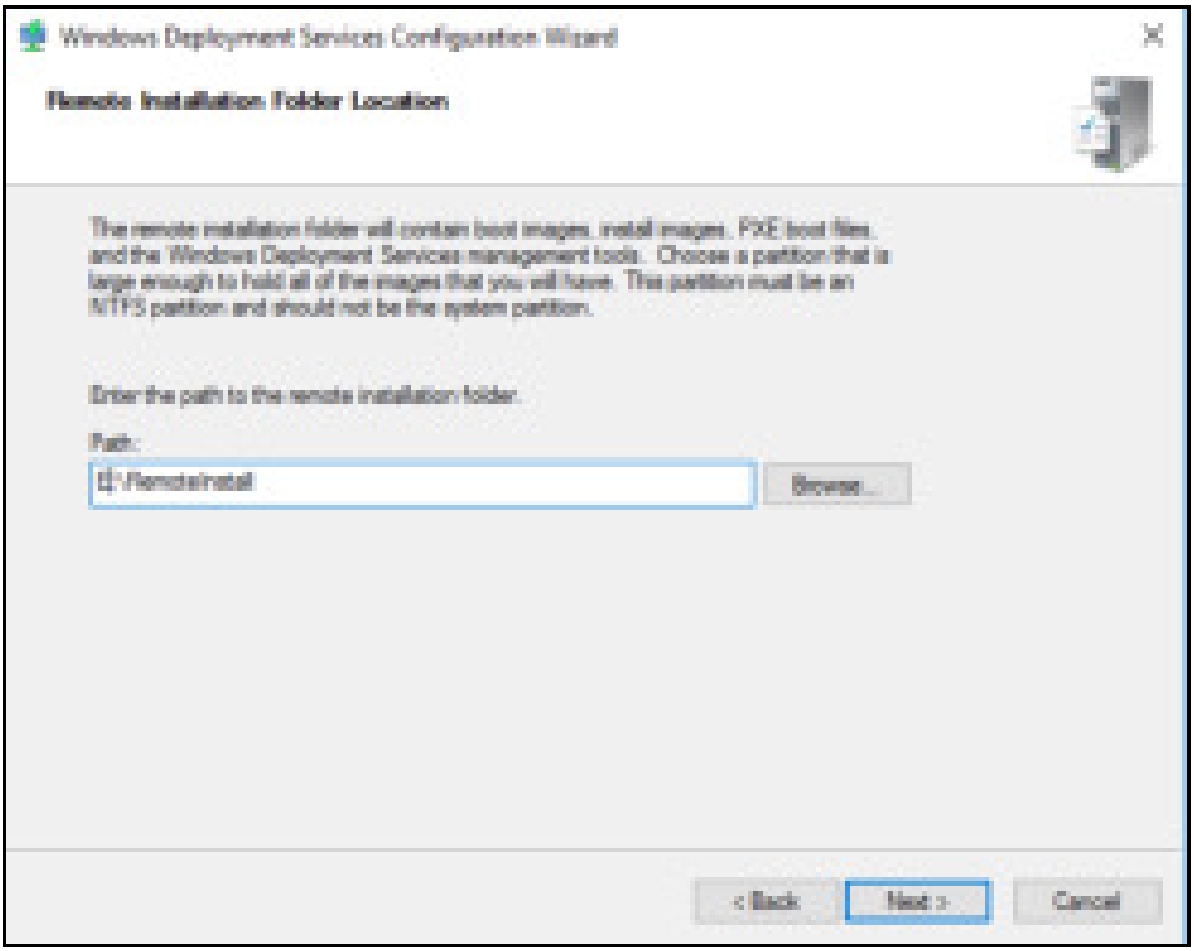
Три других параметра — стандартные для большинства настроек DHCP.

Запустите мастер настройки на сервере WDS и завершите настройку WDS. Сделаем несколько небольших изменений в настройках.

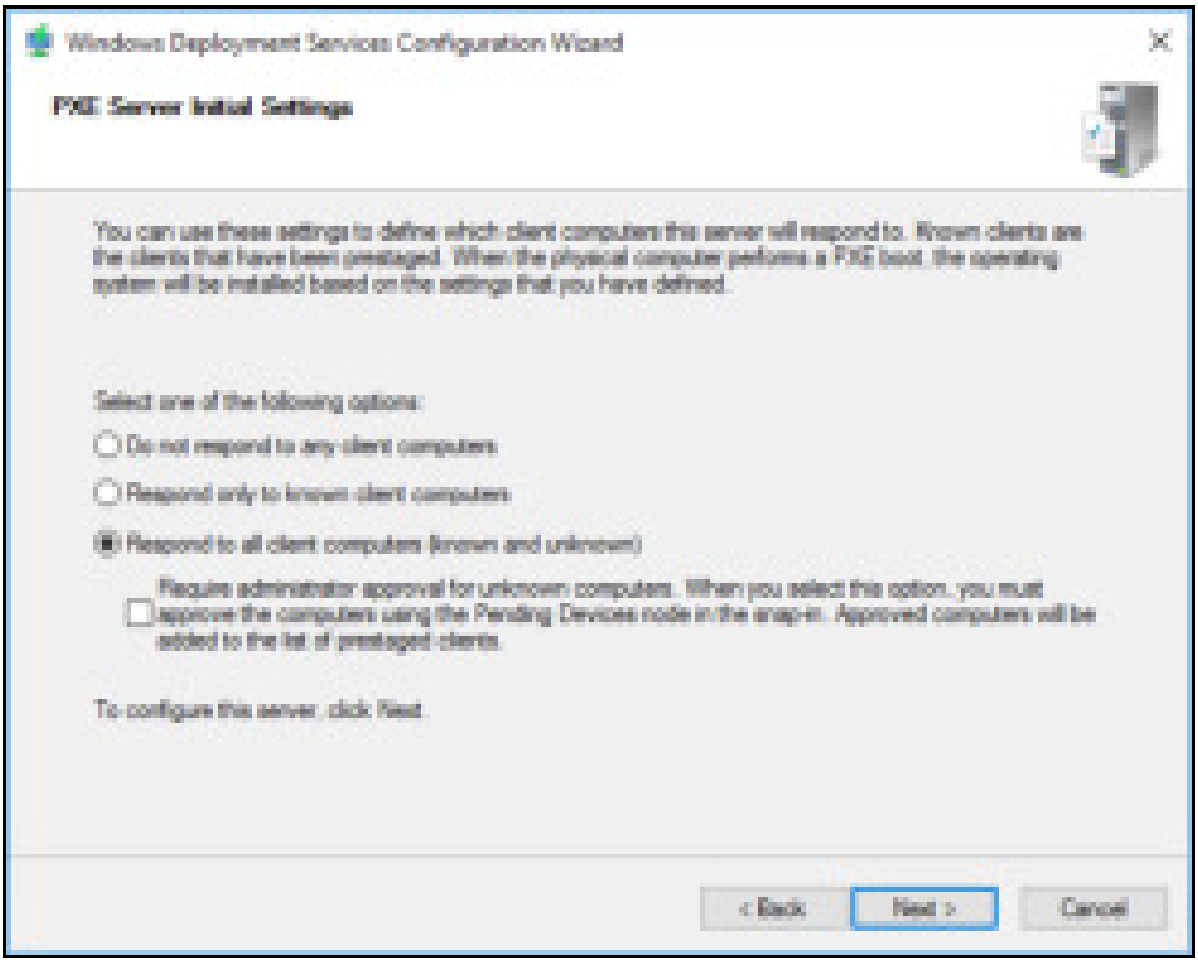

Windows Deployment Services Configuration Wizard
Before You Begin
You can use this wizard to configure Windows Deployment Services. Once the server is configured, you will need to add at least one boot image and one install image to the server before you will be able to install an operating system.
Before you begin, ensure that the following requirements are met:
– The server is a member of an Active Directory Domain Services (AD DS) domain, or a domain controller for an AD DS domain. If the server supports Standalone mode, it can be configured without having a dependency on Active Directory.
– There is an active DHCP server on the network. This is because Windows Deployment Services uses Pre-Boot Execution Environment (PXE), which relies on DHCP for IP addressing.
– There is an active DNS server on your network.
– This server has an NTFS file system partition on which to store images.
To continue, click Next.
< Back
Next >
Cancel




Сервер можно интегрировать с AD, поскольку в этот момент мы настраиваем параметры Windows, но мы предпочтем автономный сервер, который отвечает на все запросы без предварительного размещения в AD.

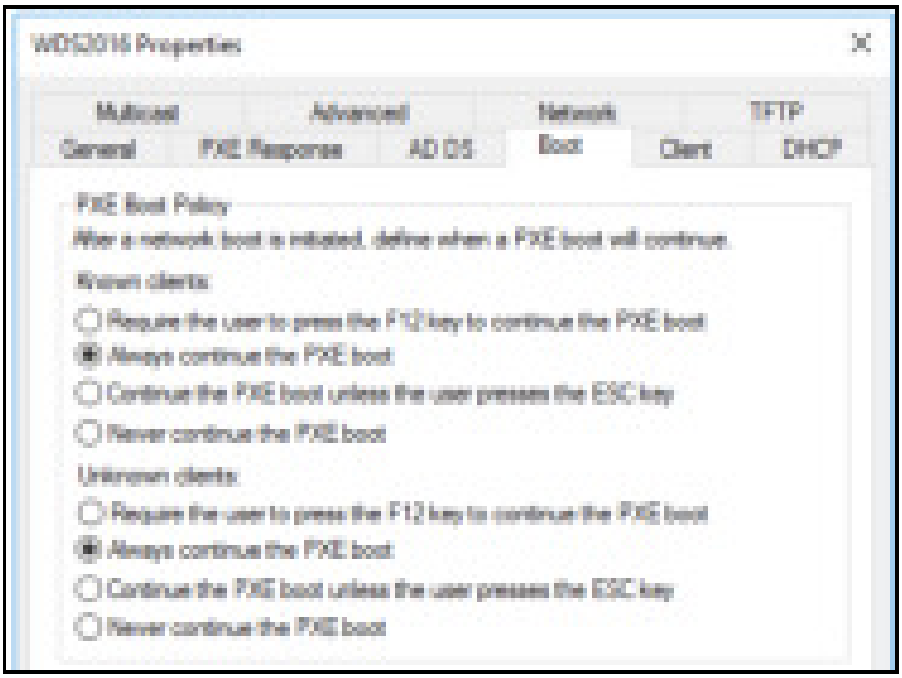



Меняем C:\RemoteInstall на E:\RemoteInstall. **E:** — это второй диск, который добавим на сервер WDS специально для файлов WIM, файлов Linux и т. п.




Сделаем это для того, чтобы сервер PXE сам отвечал на все запросы, не тратя времени на получение подтверждения от AD.

Последний параметр, который надо изменить, находится в меню PXE. Для этого нужно запустить консоль развертывания WDS, щелкнуть правой кнопкой мыши на имени сервера и изменить значение параметра на вкладке загрузки с «Require the user to press F12 key to continue the PXE boot» («Пользователь должен нажать клавишу F12 для продолжения загрузки PXE») на «Always continue the PXE boot» («Всегда продолжать загрузку PXE»).




Теперь в WDS можно добавить файлы .WIM. Достаточно скопировать файлы «boot.wim» и «install.wim» из образа 2016 ISO, и тогда можно развернуть образы Windows с помощью WDS.

Запустите ВМ с помощью загрузки PXE и откройте стандартный экран загрузки WDS, на котором будет только ОС Windows. На этом этапе стоит протестировать развертывание и убедиться, что все работает, потому что теперь мы начинаем вносить фундаментальные изменения в WDS, которые позволят использовать службы для установки Linux и ESXi.

**Изменение загрузчика служб развертывания Windows**

Сервер WDS уже может выполнить развертывание образов Windows, но мы хотим, чтобы он делал не только это. Он должен также справляться с образами Linux, поэтому первым делом мы меняем загрузчик WDS на загрузчик Linux PXE.

Для этого нужно скачать sysLinux. НЕ СКАЧИВАЙТЕ версии позже 3.86 — они не будут работать с ESXi, поскольку их установщик по-прежнему использует версию 3.86.

Скачав sysLinux 3.86, распакуйте архив во временную папку. Теперь нужно переместить несколько файлов. Это самая занудная часть процесса установки, которая требует аккуратности!

Извлеките из архива sysLinux 3.86:

core\pxeLinux.0
com32\menu\vesamenu.c32
com32\modules\chain.c32
Переименуйте pxeLinux.0 to pxeLinux.com
Скопируйте файлы в папки remoteinstall\boot\x64 и remoteinstall\boot\x86
В обеих папках x86 и x64 переименуйте pxeboot.n12 в pxeboot.0

Из командной строки выполните следующие команды, чтобы заменить загрузчик по умолчанию на загрузчик Linux PXE:

```
wdsutil /set-server /bootprogram:boot\x86\pxeLinux.com
/architecture:x86
wdsutil /set-server /N12bootprogram:boot\x86\pxeLinux.com
/architecture:x86
wdsutil /set-server /bootprogram:boot\x64\pxeLinux.com
/architecture:x64
wdsutil /set-server /N12bootprogram:boot\x64\pxeLinux.com
/architecture:x64
```

В обеих папках x86 и x64 создайте подпапки с именем pxeLinux.cfg, а в них создайте файл с именем «default» и скопируйте в него следующий текст, чтобы настроить меню загрузки:

```
DEFAULT      vesamenu.c32
PROMPT       0
NOESCAPE     0
ALLOWOPTIONS 0
# Timeout in units of 1/10 s
TIMEOUT 0
MENU MARGIN 10
MENU ROWS 16
MENU TABMSGROW 21
MENU TIMEOUTROW 26
MENU COLOR BORDER 30;44                    #20ffffff #00000000 none
MENU COLOR SCROLLBAR 30;44                 #20ffffff #00000000 none
MENU COLOR TITLE 0                         #ffffffff #00000000 none
MENU COLOR SEL   30;47                     #40000000 #20ffffff
```

MENU BACKGROUND flow.jpg

MENU TITLE PXE Boot Menu

#---

LABEL wds

MENU LABEL Windows Deployment Services

MENU DEFAULT

KERNEL pxeboot.0

#---

LABEL CentOS68

MENU LABEL CentOS 6.8

KERNEL /web/CentOS/6.8/images/pxeboot/vmlinuz

append initrd=/web/CentOS/6.8/images/pxeboot/initrd.img root=/dev/ram0 init=/Linuxrc ramdisk_size=100000 ks=https://**[IP-адрес сервера WDS]**/CentOS/6.8/centos-base-ks.cfg

#---

LABEL CentOS72

MENU LABEL CentOS 7.2

KERNEL /web/CentOS/7.2/images/pxeboot/vmlinuz

append initrd=/web/CentOS/7.2/images/pxeboot/initrd.img

#---

LABEL VMWare500U3

MENU LABEL VMWare 5.0.0 U3

KERNEL /web/VMWare/5.0.0/U3/mboot.c32

APPEND -c /web/VMWare/5.0.0/U3/boot.cfg

#---

LABEL VMWare553b

MENU LABEL VMWare 5.5 U3b

KERNEL /web/VMWare/5.5.0/U3b/mboot.c32

APPEND -c /web/VMWare/5.5.0/U3b/boot.cfg

#---

LABEL VMWare60

MENU LABEL VMWare 6.0

KERNEL /web/VMWare/6.0/mboot.c32

APPEND -c /web/VMWare/6.0/boot.cfg

#---

LABEL VMWare65

MENU LABEL VMWare 6.5

KERNEL /web/VMWare/6.5/mboot.c32

APPEND -c /web/VMWare/6.5/boot.cfg

#---

LABEL Abort

MENU LABEL AbortPXE

Kernel abortpxe.0

#---

LABEL local

MENU LABEL Boot from Harddisk

LOCALBOOT 0

Type 0x80

**Изменение настроек IIS**

IIS необходимы для размещения установочных файлов CentOS и ESXi. Создадим структуру веб-файлов на VMDK. Она выглядит так:

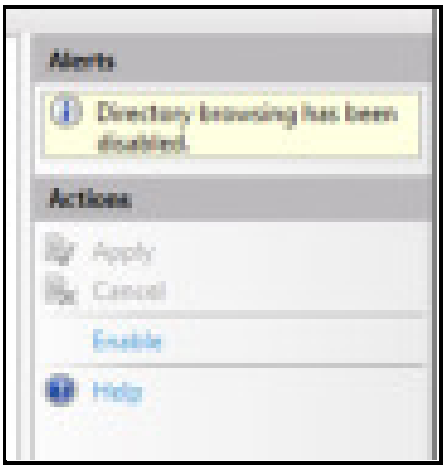
E:\web — корневой каталог, на который указывает IIS

E:\web\centos\7.x\7.1 — файлы установки CentOS 7.1

E:\web\vmware\6.5 — файлы установки VMware 6.5

В IIS необходимо включить просмотр файлов, чтобы установщик Linux и установщик VMware могли их извлечь.

Запустите программу администрирования IIS, выберите свой сервер -> Сайт по умолчанию -> Просмотр каталога и включите его.




Полезно также настроить защищенное соединение с сервером по протоколу HTTPS.

**Добавление Linux**

Теперь можно добавить Linux.

Скачаем самую маленькую ISO-версию CentOS (как правило, это образ minimal), монтируем образ ISO и копируем его содержимое в директорию «E:\web\centos\7.x\7.\[версия]» или другую, которую легко запомнить. После этого можно добавить, например, kickstart-файл, чтобы автоматизировать установку. Вот пример строк, которые добавим к файлу pxeLinux.cfg, используемому по умолчанию:

LABEL CentOS72

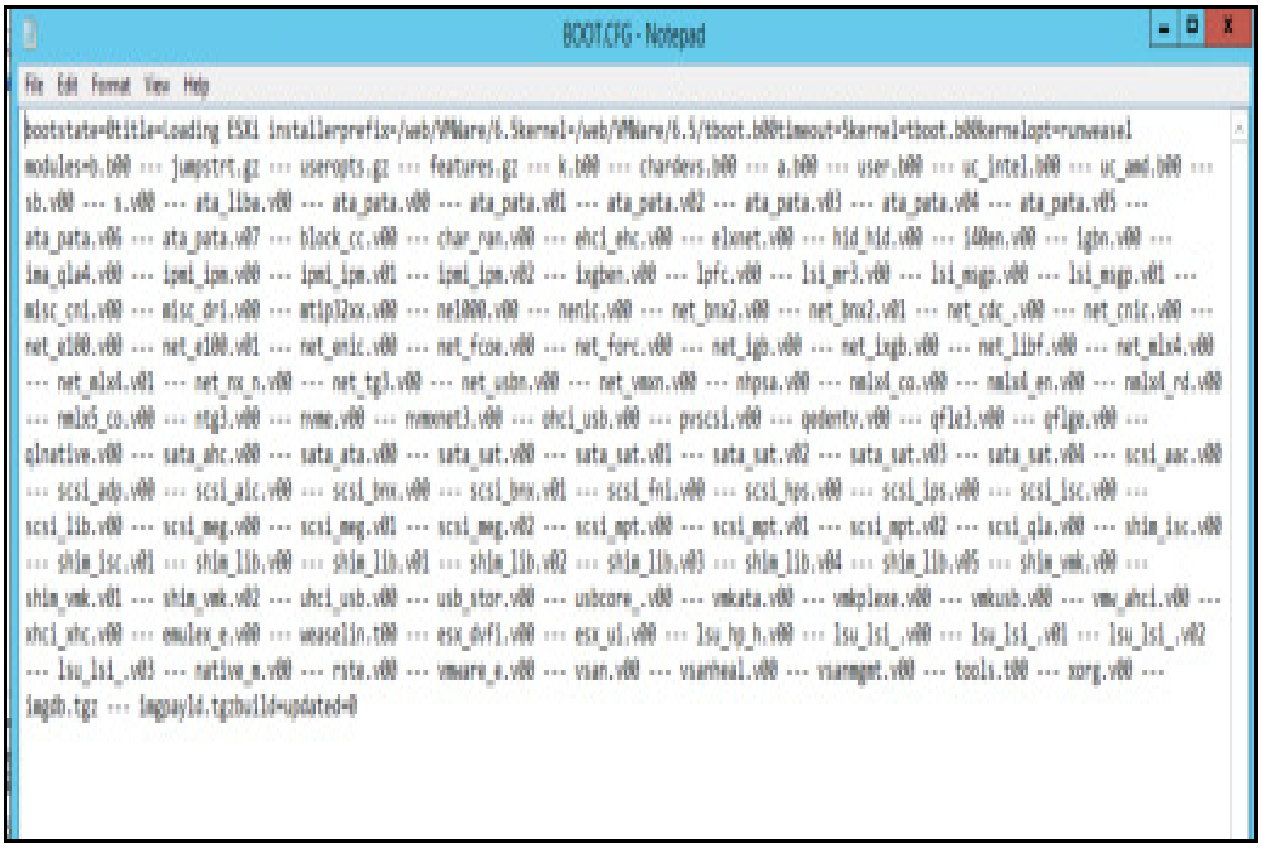
MENU LABEL CentOS 7.2

KERNEL /web/CentOS/7.2/images/pxeboot/vmlinuz

append initrd=/web/CentOS/7.2/images/pxeboot/initrd.img inst.repo=**[IP-адрес сервера WDS]**/CentOS/7.2 ks=**[IP-адрес сервера WDS]**/CentOS/7.2/centos-base-ks.cfg

**Добавление VMware**

Добавим ESXi 6.5. Для этого тоже надо просто скопировать все файлы из ISO-образа VMware в соответствующую папку на сервере WDS, но после этого надо изменить файл boot.cfg в папке VMware, удалив пробелы. Это выглядит так:




Изменение настроек сервера WDS, IIS и различных файлов конфигурации может потребовать некоторых усилий, но, сделав это, можно использовать меню PXE для переключения на WDS и выбрать любую ОС Windows, которая поддерживает WIM-файлы. С ее помощью можно также запускать установку Linux или VMware в полностью автоматическом режиме. Кроме того, для удобства можно добавить и другие приложения, такие как GParted и Memtest.

## Практическое занятие №15 Планирование и реализация инфраструктуры Remote Desktop Services

***Цель работы:***

Изучить систему планирования и реализации инфраструктуры Remote Desktop Services

Установим службы удаленного рабочего стола , терминального сервера RDS TS на Windows Server

Пример тестового стенда windows server 2016 2019 RDS TS для standard и datacenter , не для essentials

1)Вводим Windows сервер в домен join server to domain Active Directory

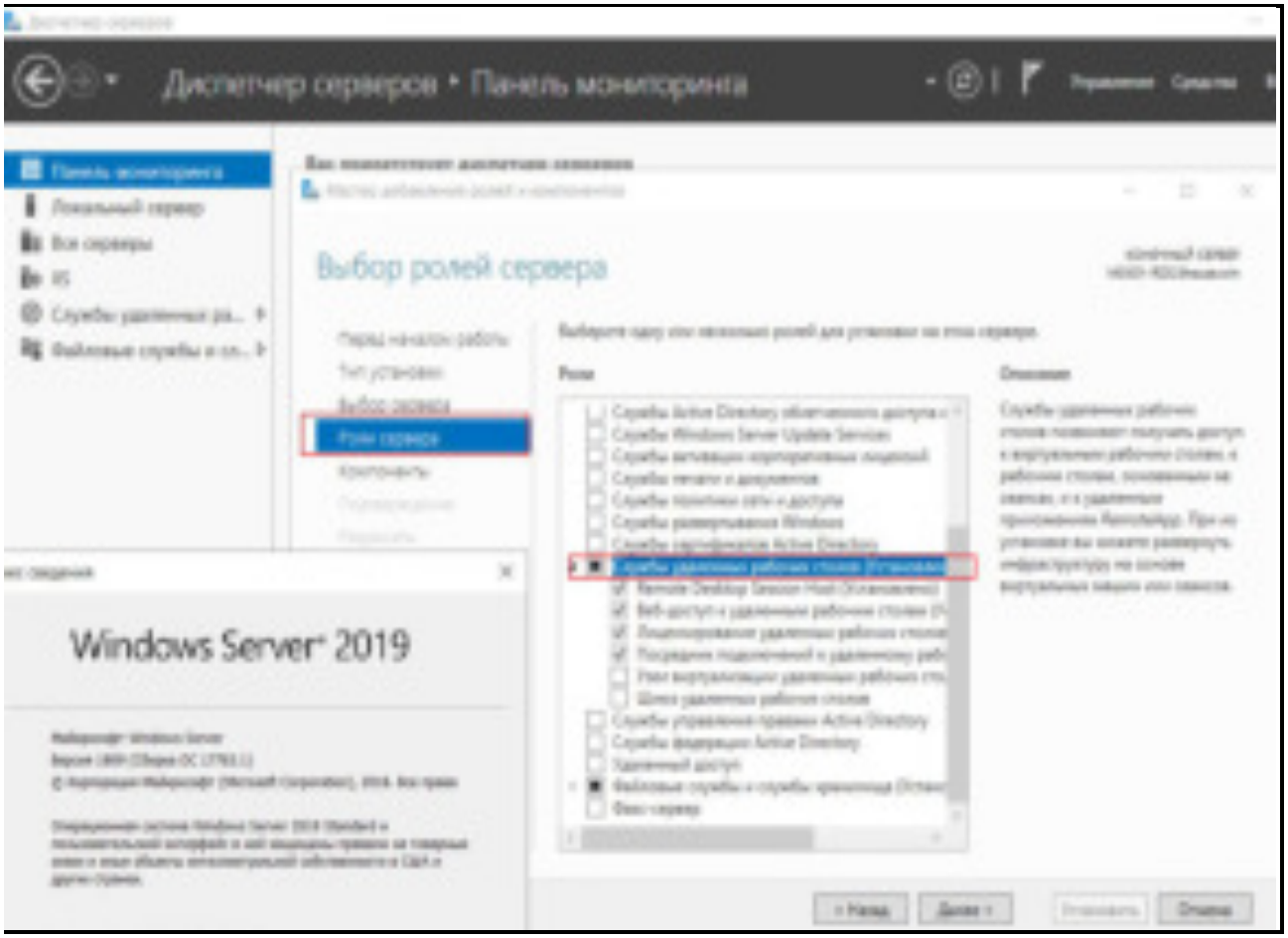
**add-computer -domainname 5house.win -cred 5house.win\Администратор restart-computer**

## 2) Залогинится с правами администратора на windows север

Добавляем роль и компоненты служб удаленного рабочего стола на основе сеансов добавим функцию RDS , Add the role and components of Remote Desktop Services based on sessions add RDS function PS

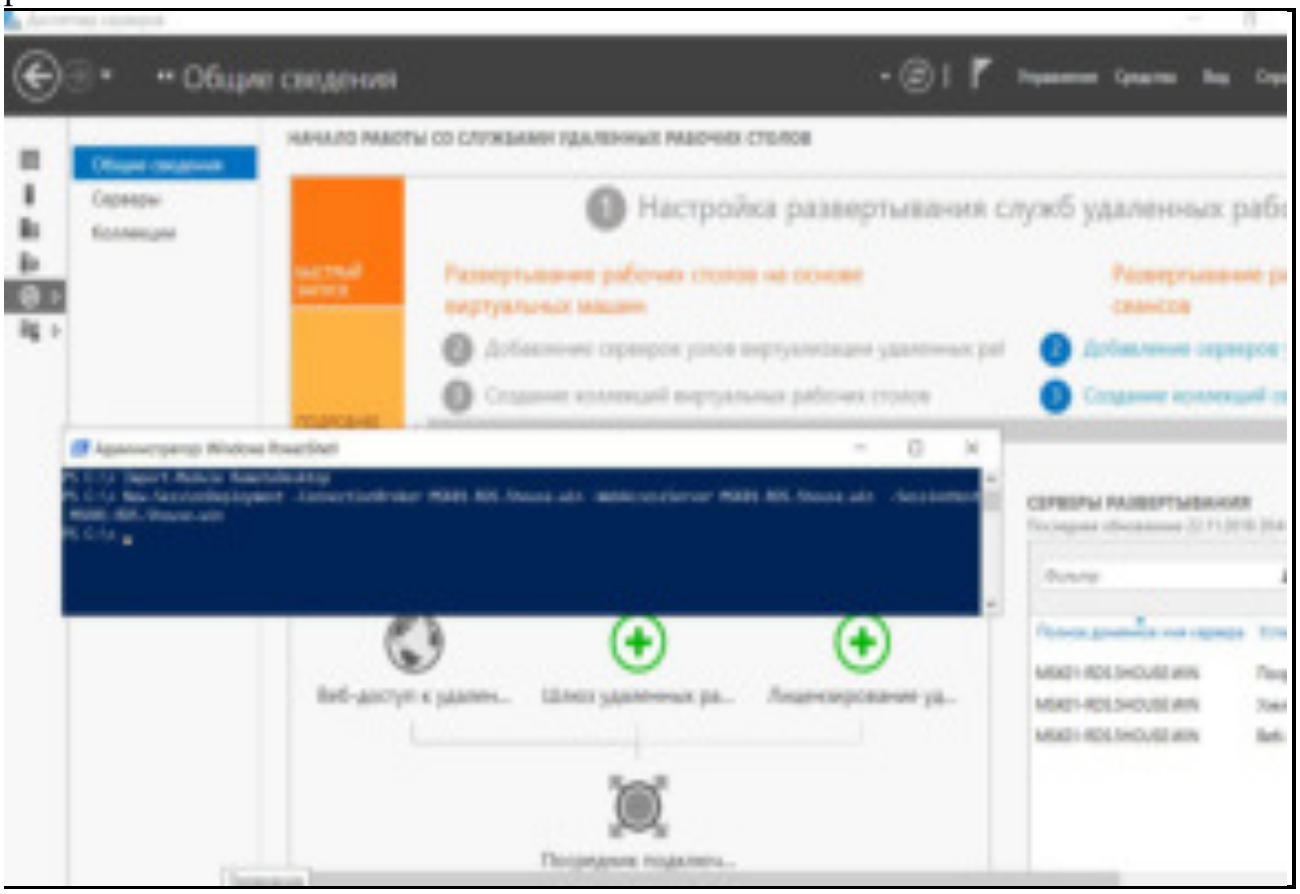
Add-WindowsFeature –Name RDS-RD-Server –IncludeAllSubFeature -Restart

Remote Desktop Services-RDS-install-gui




3)Чтобы установить три обязательных компонента RDS в стандартном развертывании, используйте командлет **New-SessionDeployment**, как показано ниже, заменив значения параметров **-ConnectionBroker**, **-WebAccessServer** и **-SessionHost** с именами серверов, на которых вы хотите для установки этих

ролей.




Import-Module RemoteDesktop

New-SessionDeployment –ConnectionBroker MSK01-RDS.5house.win –WebAccessServer MSK01-RDS.5house.win –SessionHost MSK01-RDS.5house.win

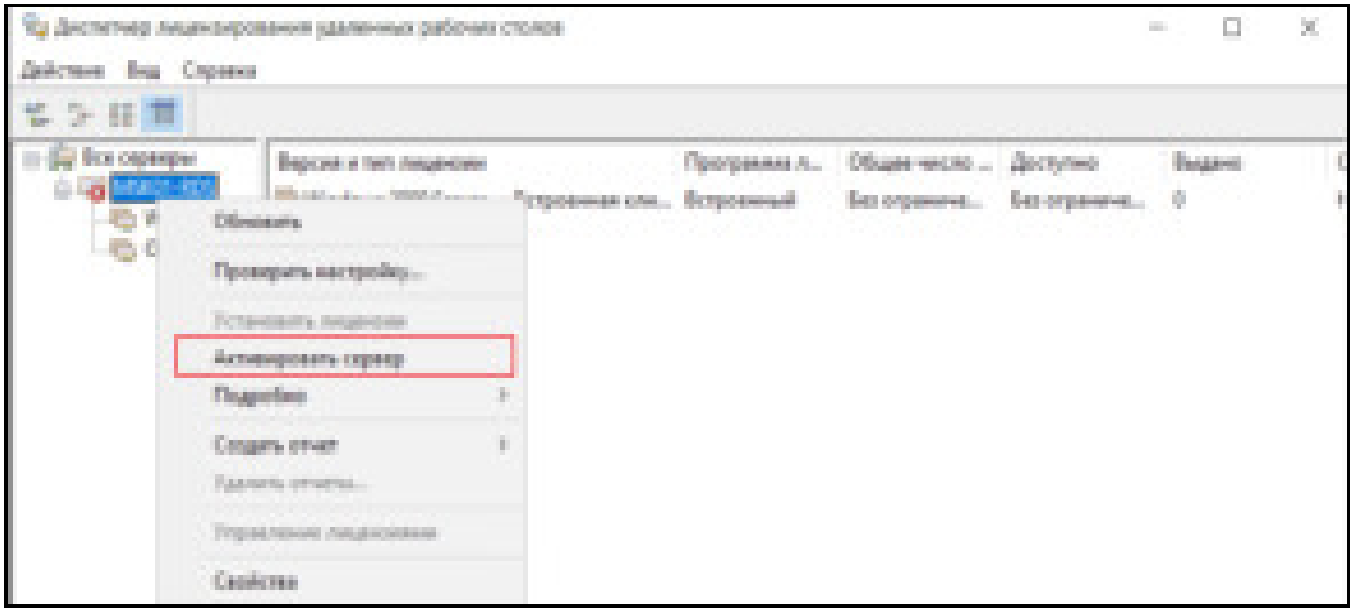
**4)**Теперь нам нужно активировать наш сервер лицензий и установить клиентские лицензии через графический интерфейс диспетчера лицензирования на сервере лицензий.

Активируем сервер лицензий и установим клиентские лицензии PerUser.
Типы клиентских терминальных лицензий (**RDS CAL**)
Каждый пользователь или устройство, которое подключается к серверам Remote Desktop Session должно иметь клиентскую лицензию (**CAL** — client access license). Есть два типа терминальных CAL.
**На устройство (Per Device CAL)** – это постоянный тип лицензии, назначающаяся компьютеру или устройству, которое подключается к RDS серверу более одного раза (при первом подключении устройства ему выдается временная лицензия). Данные лицензии не являются конкурентными, т.е. если у вас 10 лицензий Per Device, то к вашему RDS серверу смогут подключится всего 10 хостов.
**На пользователя (Per User CAL)** – такой тип лицензии позволяет одному пользователю подключаться к серверу RDS с любого количества

компьютеров/устройств. Данный тип лицензий привязывается к пользователю Active Directory, но выдается не навсегда, а на определенный период времени (90 дней по-умолчанию).
Давайте настроим наше развертывание для лицензирования. Для этого используется командлет ниже:

```
PS C:\> Set-RDLicenseConfiguration -LicenseServer MSK01-RDS.5house.win -Mode PerUser -ConnectionBroker MSK01-RDS.5house.
win

Подтверждение
Параметры лицензии для развертывания удаленных рабочих столов будут изменены. Вы хотите продолжить?
[Y] Да - Y  [N] Нет - N  [S] Приостановить - S  [?] Справка (значением по умолчанию является "Y"): y

Вы хотите продолжить?
Серверы "MSK01-RDS.5house.win" не являются допустимыми серверами лицензирования.
[Y] Да - Y  [N] Нет - N  [S] Приостановить - S  [?] Справка (значением по умолчанию является "Y"): y
PS C:\>
```

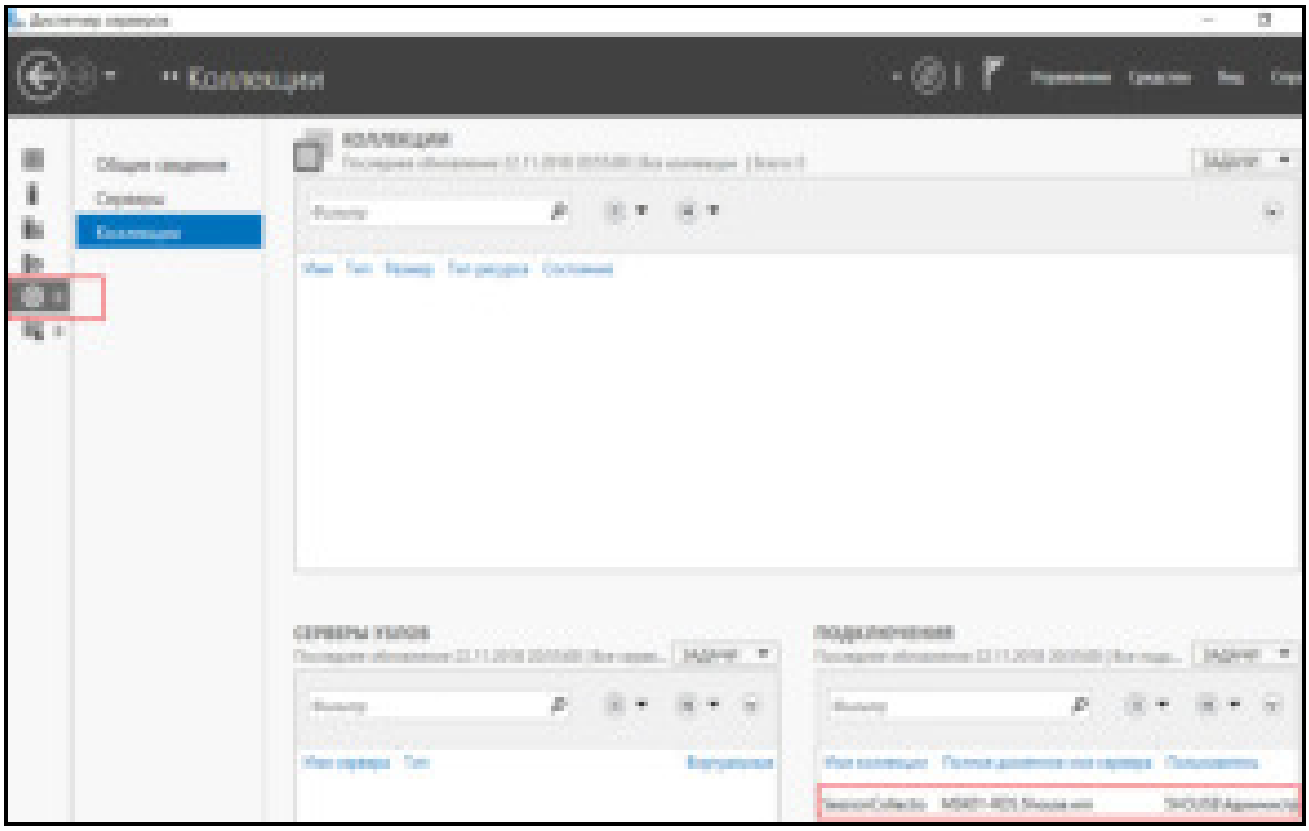
Set-RDLicenseConfiguration -LicenseServer MSK01-RDS.5house.win -Mode PerUser -ConnectionBroker MSK01-RDS.5house.win




5)Создадим коллекцию со списком подключения

```
PS C:\> New-RDSessionCollection -CollectionName SessionCollection -SessionHost MSK01-RDS.5house.win -CollectionDescripti
on "This Collection is for Desktop Sessions" -ConnectionBroker MSK01-RDS.5house.win

CollectionName      Size  ResourceType      CollectionType    CollectionDescription
--------------      ----  ------------      --------------    ---------------------
SessionCollection   1     Удаленный рабоч...PooledUnmanaged   This Collection is for Desktop Sessions
```

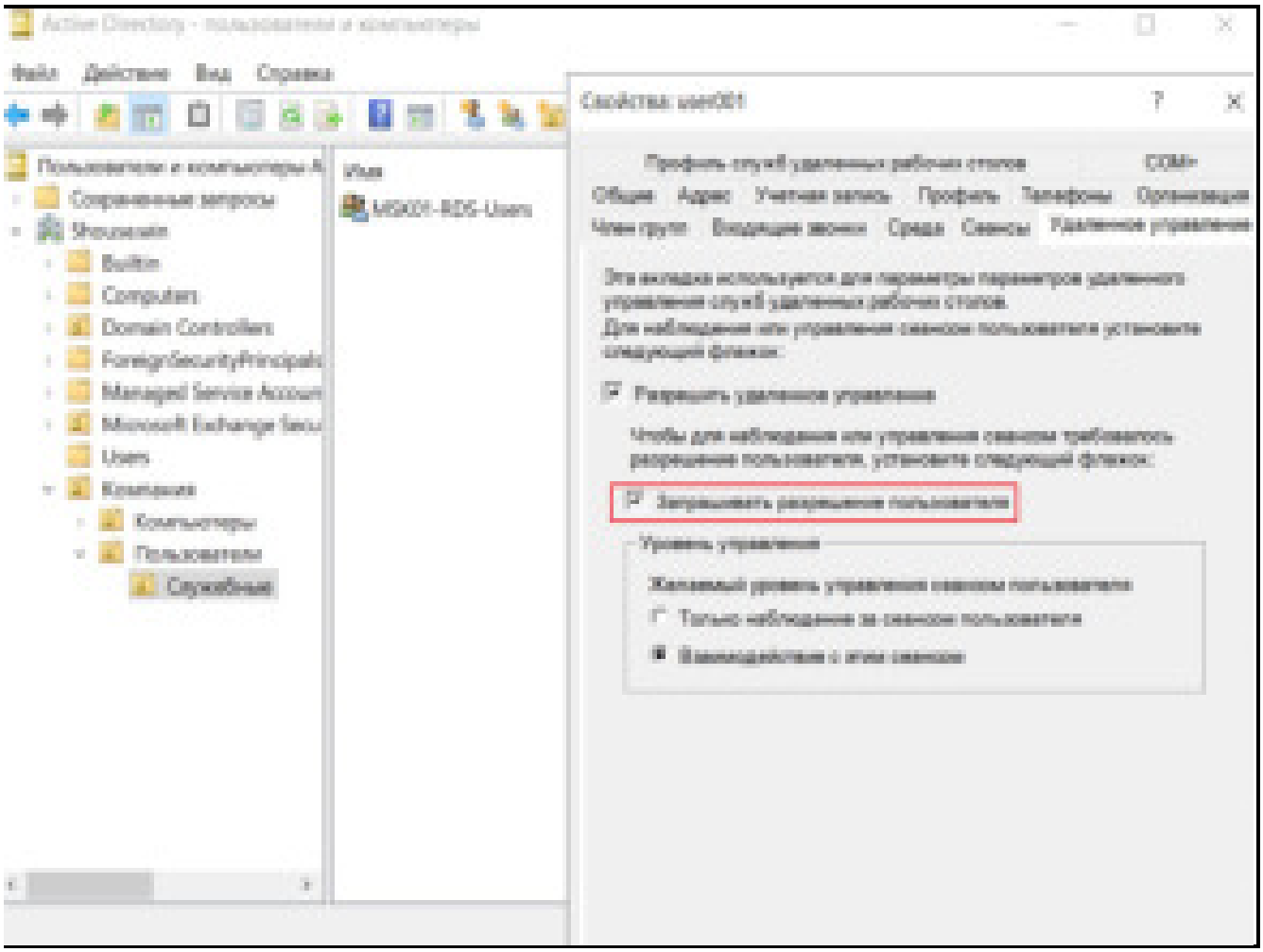
New-RDSessionCollection –CollectionName SessionCollection –SessionHost MSK01-RDS.5house.win –CollectionDescription “This Collection is for Desktop Sessions” –ConnectionBroker MSK01-RDS.5house.win

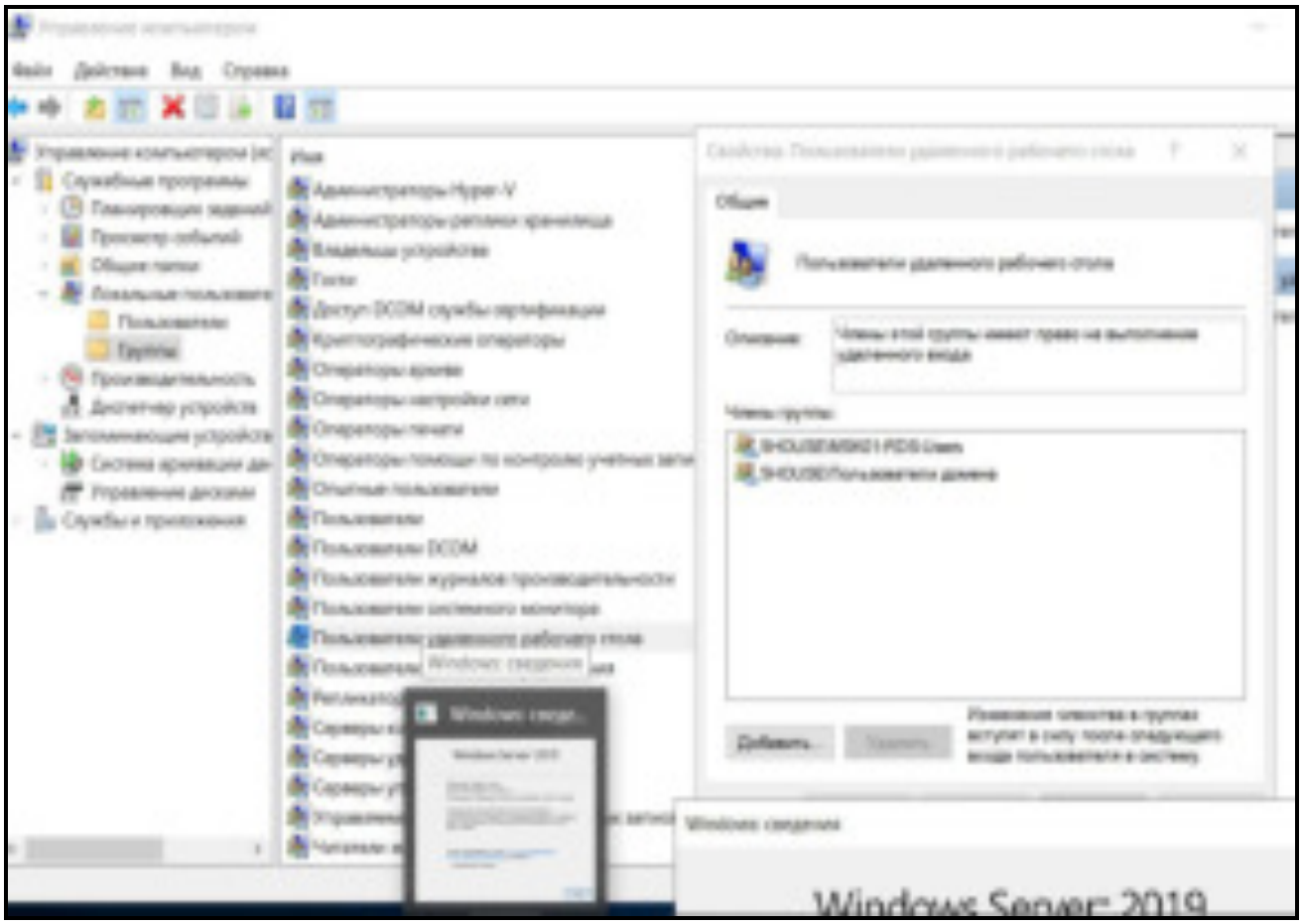


6)Контроль доступа на основе группы для подключения (dsa.msc) к RDP сервера msk01-rds

Удалив на сервере msk01-rdp в **локальной группе** Пользователи удаленного рабочего стола группу

5HOUSE\Пользователи домена и добавить доменную группу 5HOUSE\MSK01-RDS-Users , выключить запрос разрешения пользователя на удаленное управление для конкретного пользователя в ad

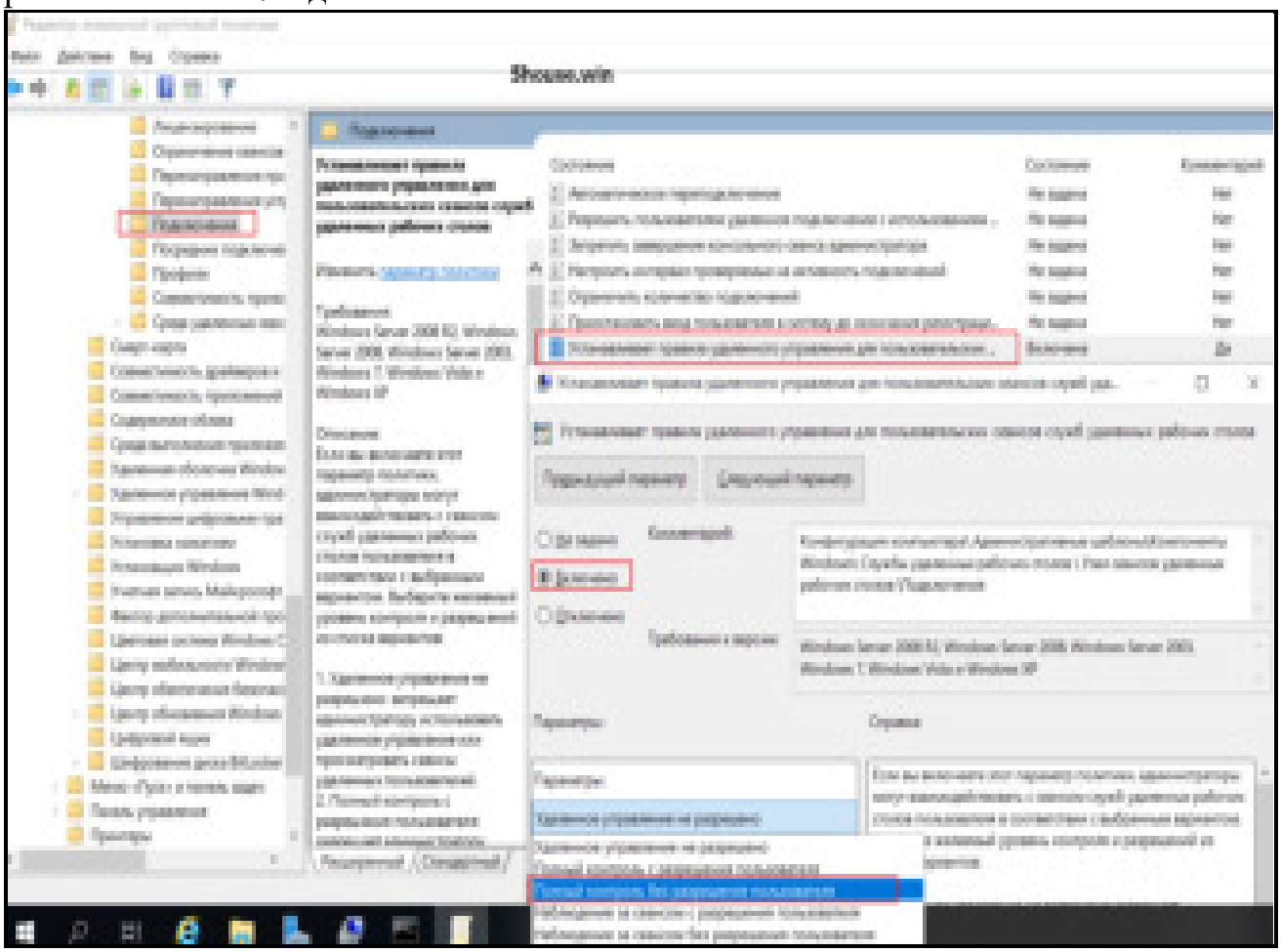

Файл
Действие
Вид
Справка
Свойства: user001
Имя
Builtin
Computers
Domain Controllers
Users
Компьютеры
Пользователи
Служебные
Общие
Адрес
Учетная запись
Профиль
Телефоны
Организация
Разрешить удаленное управление
Уровень управления




7)Групповая политика GPO или gpedit.msc согласие пользователя на теневое подключение shadow connection

Конфигурация Компьютера \ Административные шаблоны\Компоненты Windows\ Службы удаленных рабочих столов \ Узел сеансов удаленных

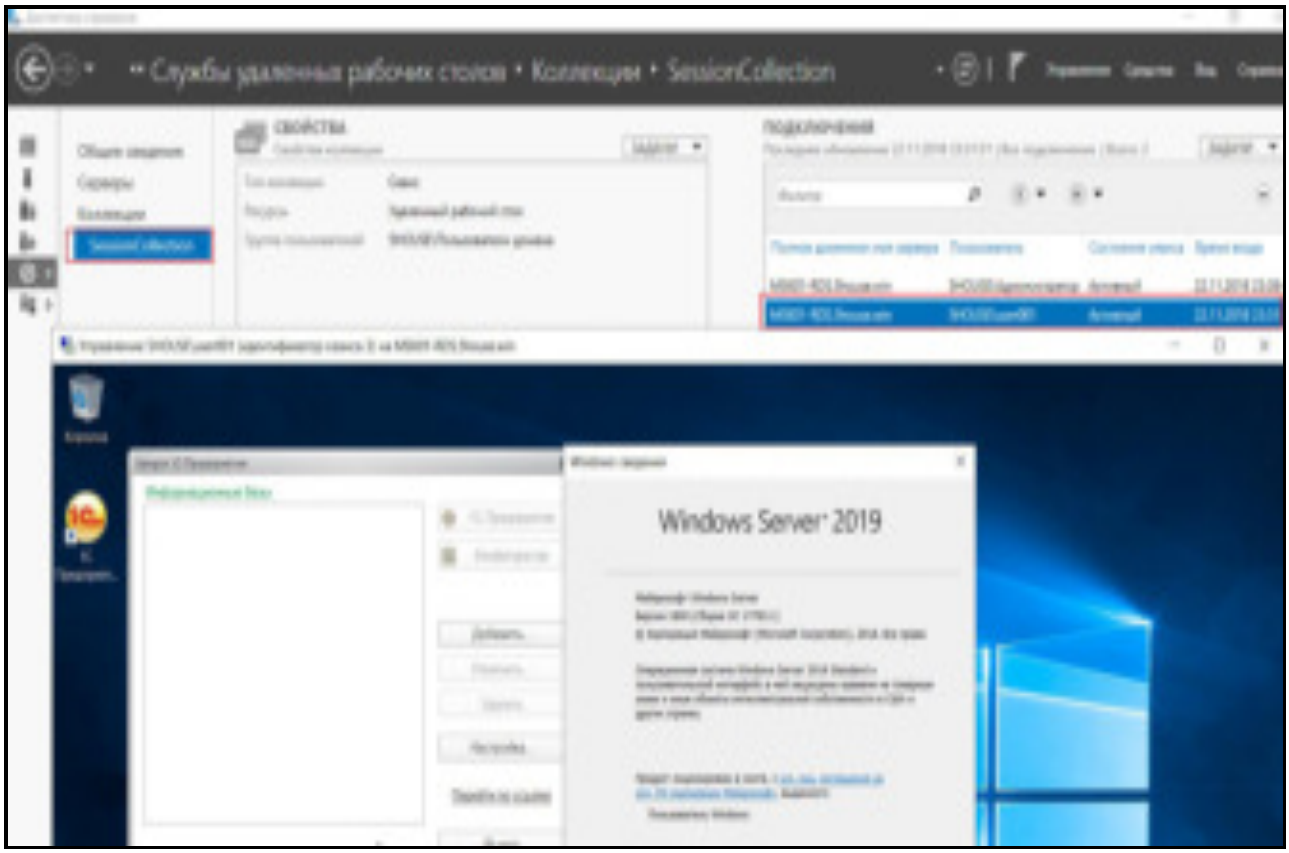
рабочих столов \Подключения



cmd
gpupdate /force

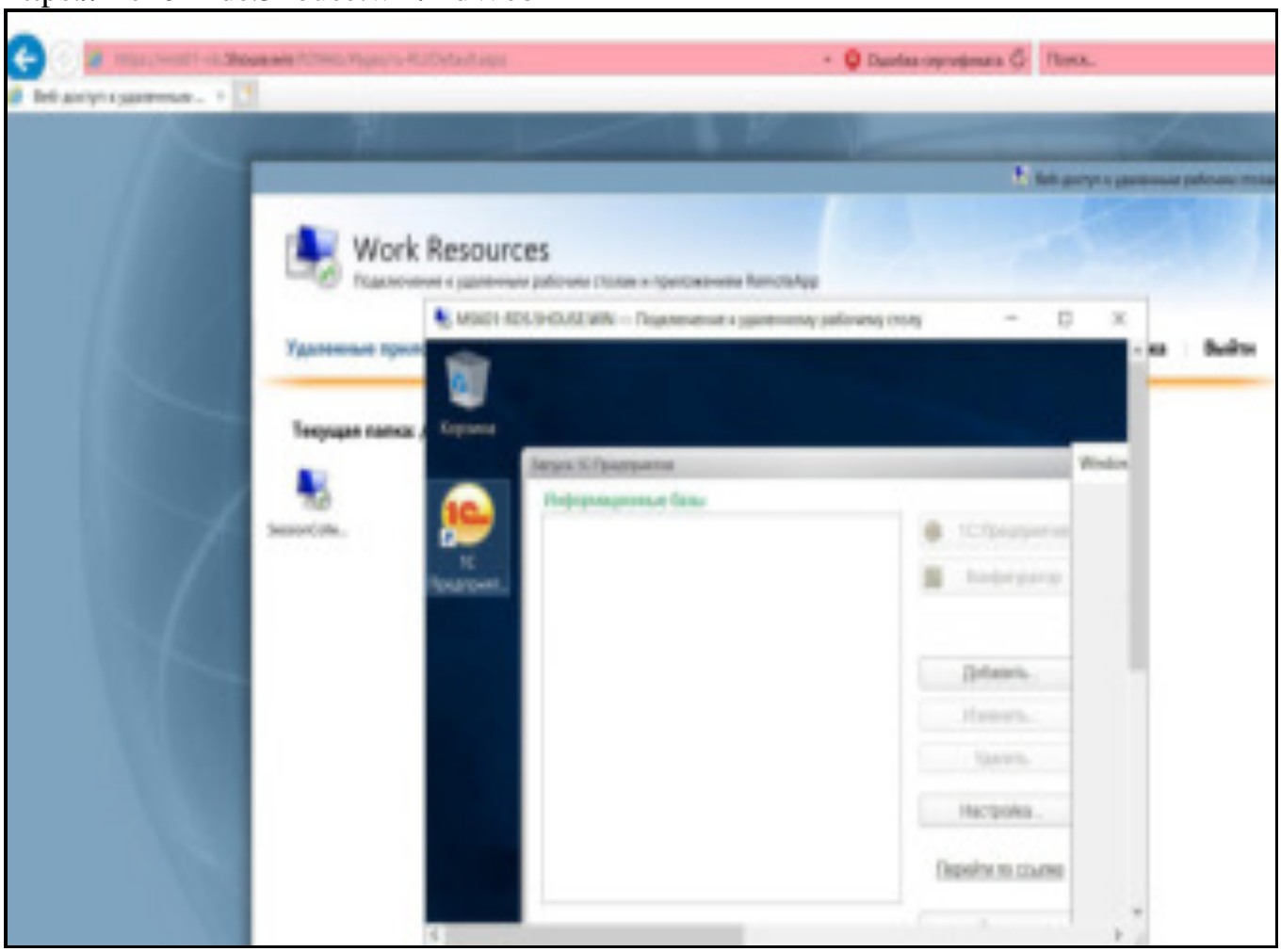
при малом белом квадрате mstsc — перезагрузите сервер MSK01-RDS

8)Диспетчер серверов\Службы удаленных рабочих столов\Коллекции\SessionCollection Remote Desktop Services-RDS-shadow-connect




9)Веб доступ к удаленным рабочим столам URL

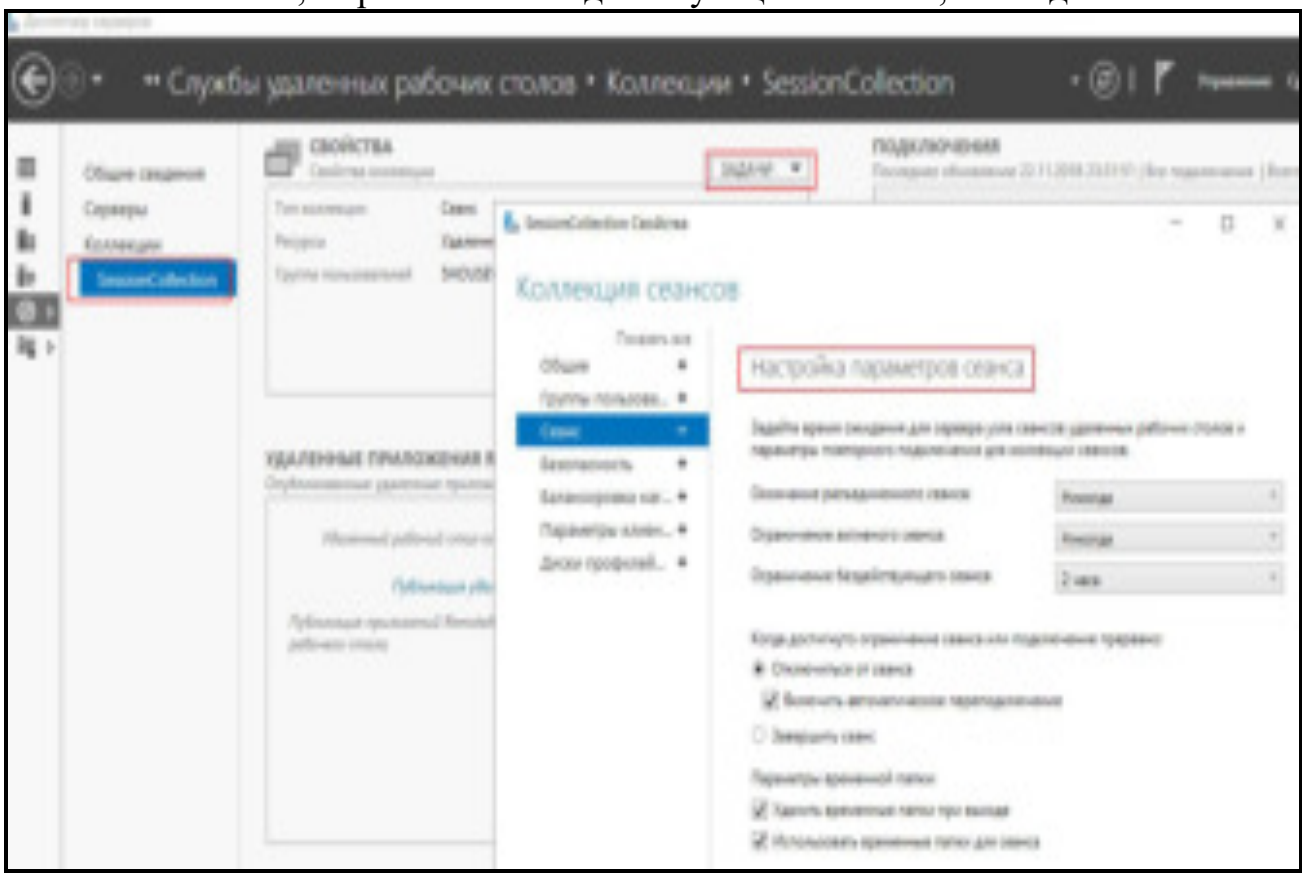
https://msk01-rds.5house.win/RdWeb




10)Настройки параметров сеанса Session Settings RDS

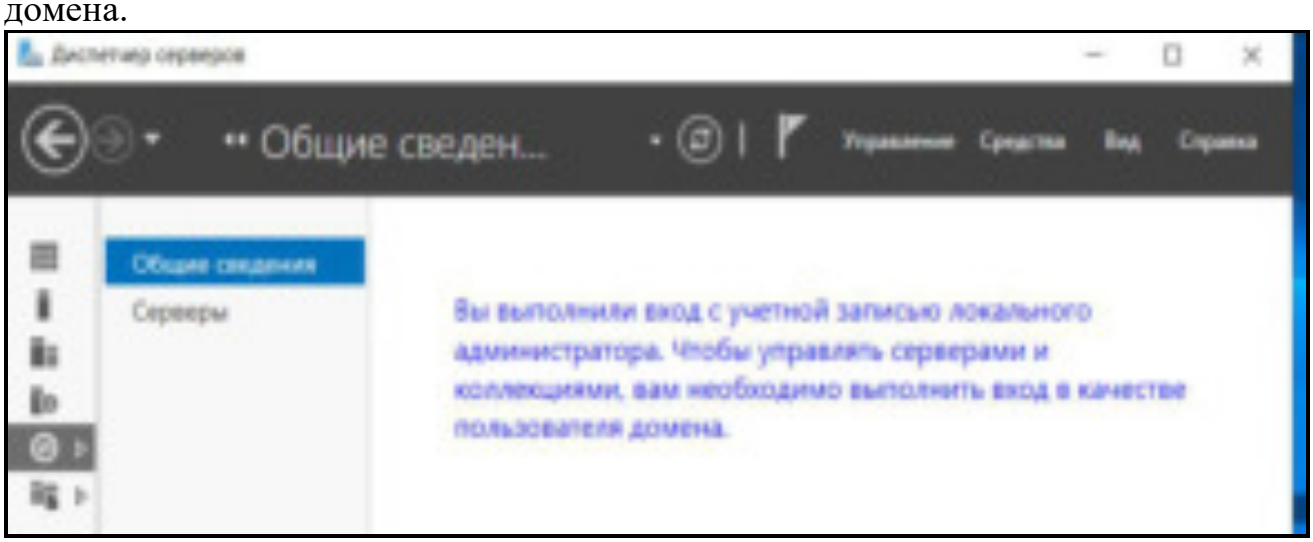
Диспетчер серверов\ Службы удаленных рабочих столов\ коллекции \свойства \задачи \ Коллекция сеансов

настройка параметров сеанса : Окончание разъединенного сеанса , Ограничение активности сеанса, Ограничение бездействующего сеанса ; никогда 2 часа




https://blogs.technet.microsoft.com/askperf/2015/03/04/step-by-step-instructions-for-installing-rds-session-deployment-using-powershell-in-windows-server-2012-r2/

Выполнили вход с учетной записью администратора. Чтобы управлять серверами и коллекциями, необходимо выполнить вход в качестве пользователя домена.



## Практическое занятие №16-17 Расширение доступа к Интернет для инфраструктуры RDS

***Цель работы:***

Изучить структуру RDS- Службы удалённого рабочего стола

**Службы удалённого рабочего стола (RDS)**, известные как службы терминалов в Windows Server 2008 и более ранних версиях — один из компонентов Microsoft Windows Server, который позволяет пользователю управлять удалённым компьютером или виртуальной машиной по сетевому соединению. RDS — это реализация Microsoft тонкого клиента, где программное обеспечение Windows и весь рабочий стол компьютера, работающего под управлением RDS, становятся доступными для удалённой клиентской машины, поддерживающей протокол удалённого рабочего стола (RDP). С RDS в клиентскую систему передаются только пользовательские интерфейсы программного обеспечения. Все входные данные клиентской системы передаются на сервер, где выполняется выполнение программного обеспечения. Это отличает от систем потоковой передачи приложений, такими как Microsoft App-V, в которых компьютерные программы передаются клиенту по требованию и выполняются на клиентской машине.

**Среда исполнения**

В рассматриваемом примере мы будем строить ферму RDCB из 5 виртуальных серверов одинаковой конфигурации на базе **Hyper-V** из **Windows Server 2012 Datacenter EN**. На всех виртуальных серверах устанавливается **Windows Server 2012 Standard EN**.

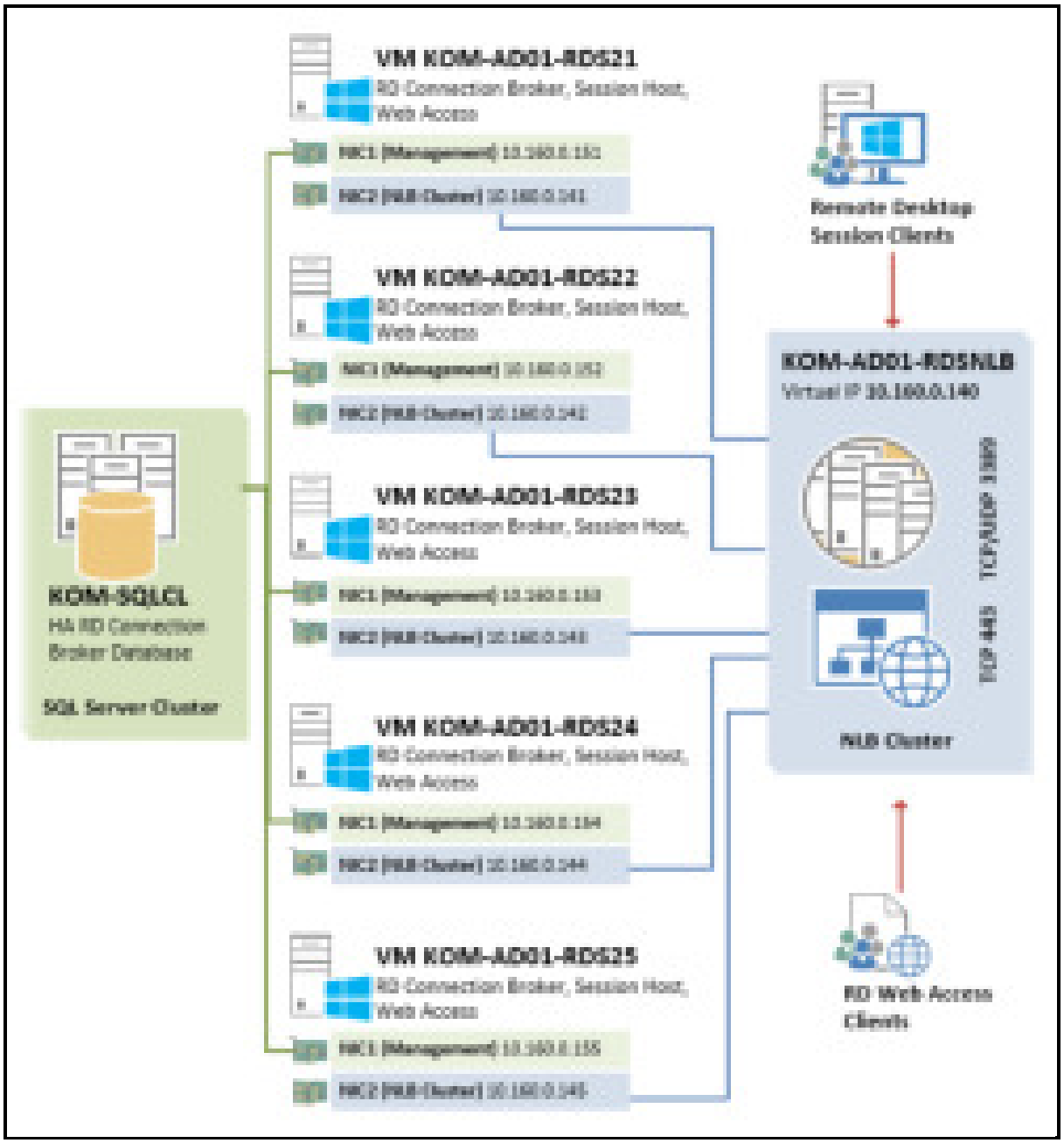
Каждый из виртуальных серверов будет иметь по два сетевых интерфейса, настройка которых будет рассмотрена далее.

Серверам присвоены имена – **KOM-AD01-RDS21** , **KOM-AD01-RDS22** , **KOM-AD01-RDS23** , **KOM-AD01-RDS24** , **KOM-AD01-RDS25**

Создаваемый в процессе описания высоко-доступный экземпляр **RD Connection Broker** а также **NLB**-кластер **RD Web Access** будут использовать общее виртуальное имя **KOM-AD01-RDSNLB**.

База данных высоко-доступного экземпляра RDCB будет расположена на отдельном кластере **SQL Server** с именем **KOM-SQLCL**

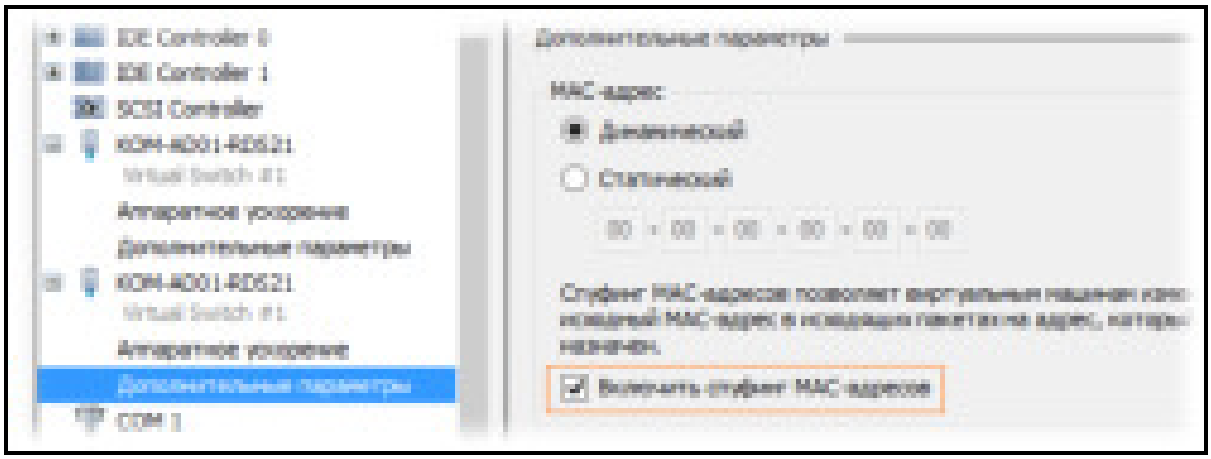
С точки зрения сетевого взаимодействия, упрощённая схема отказоустойчивой фермы RDS в нашем случае будет выглядеть следующим образом:




**Подготавливаем виртуальные сервера**

У каждого виртуального сервера создадим по 2 сетевых адаптера. Назовём их условно на каждом сервере таким образом, чтобы было понятно за что отвечает этот интерфейс - **NIC1 (Management)** и **NIC2 (NLB Cluster)**.

При создании второго сетевого адаптера **NIC2**, который будет использоваться для построения NLB в свойствах виртуальной машины Hyper-V необходимо разрешить спуфинг MAC адресов (**Enable spoofing of MAC addresses**)



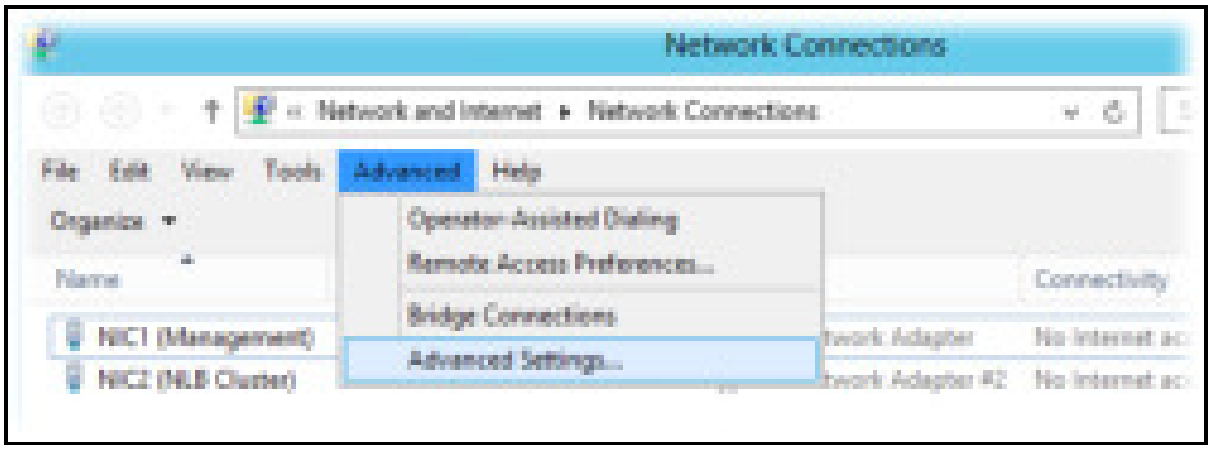

Согласно нашей схемы, выделим и распределим статические IP адреса на серверах следующим образом:

| Имя сервера | Настройки IP NIC1 | Настройки IP NIC2 (NLB Cluster) |
|---|---|---|
| KOM-AD01-RDS21 | IP 10.160.0.151/24 | IP 10.160.0.141/24 |
| KOM-AD01-RDS22 | IP 10.160.0.152/24 | IP 10.160.0.142/24 |
| KOM-AD01-RDS23 | IP 10.160.0.153/24 | IP 10.160.0.143/24 |
| KOM-AD01-RDS24 | IP 10.160.0.154/24 | IP 10.160.0.144/24 |
| KOM-AD01-RDS25 | IP 10.160.0.155/24 | IP 10.160.0.145/24 |

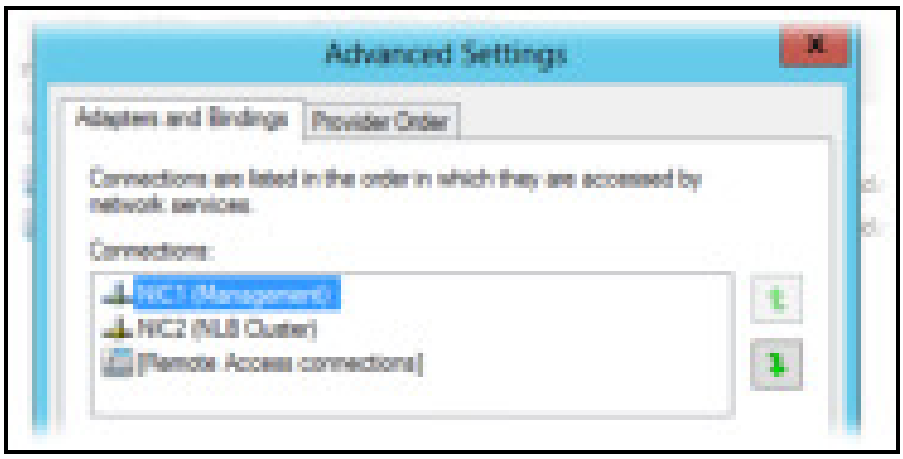
На всех интерфейсах используются одинаковые настройки адреса шлюза по умолчанию -10.160.0.254 и адресов DNS - 10.160.0.253, 10.160.1.253.

Интерфейс **NIC1** будет отвечать за управление самим сервером (будет зарегистрирован в **DNS** на FQDN имя сервера), а **NIC2** (для которого включён спуфинг MAC адресов) будет участником **NLB** кластера. Выполним настройку сетевых интерфейсов на каждом из серверов согласно вышеприведённой таблицы на примере сервера **KOM-AD01-RDS21**

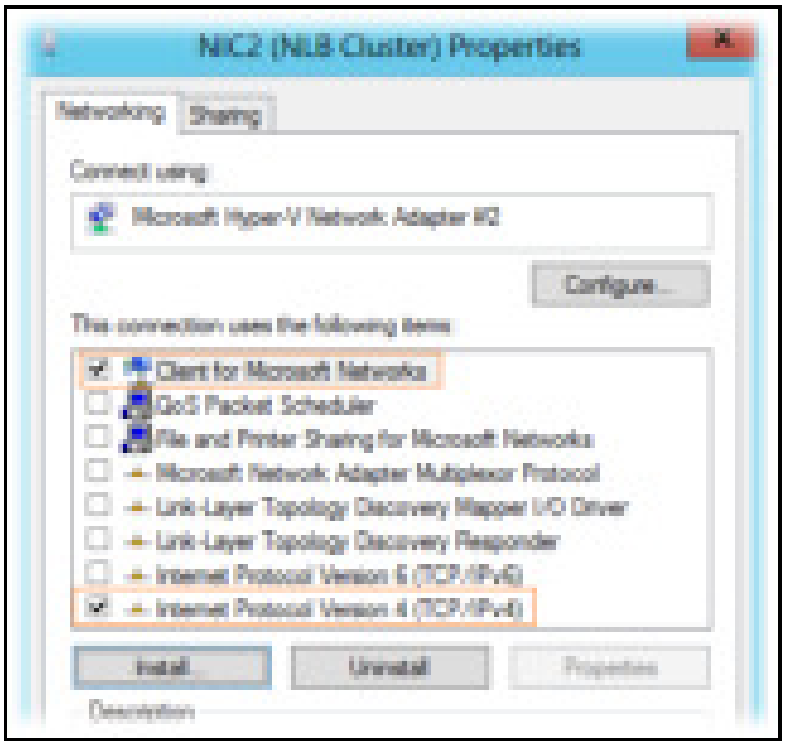
Откроем окно настройки сетевых подключений и в меню **Advanced** > **Advanced Settings** и проверим порядок использования подключений (**Connections**).



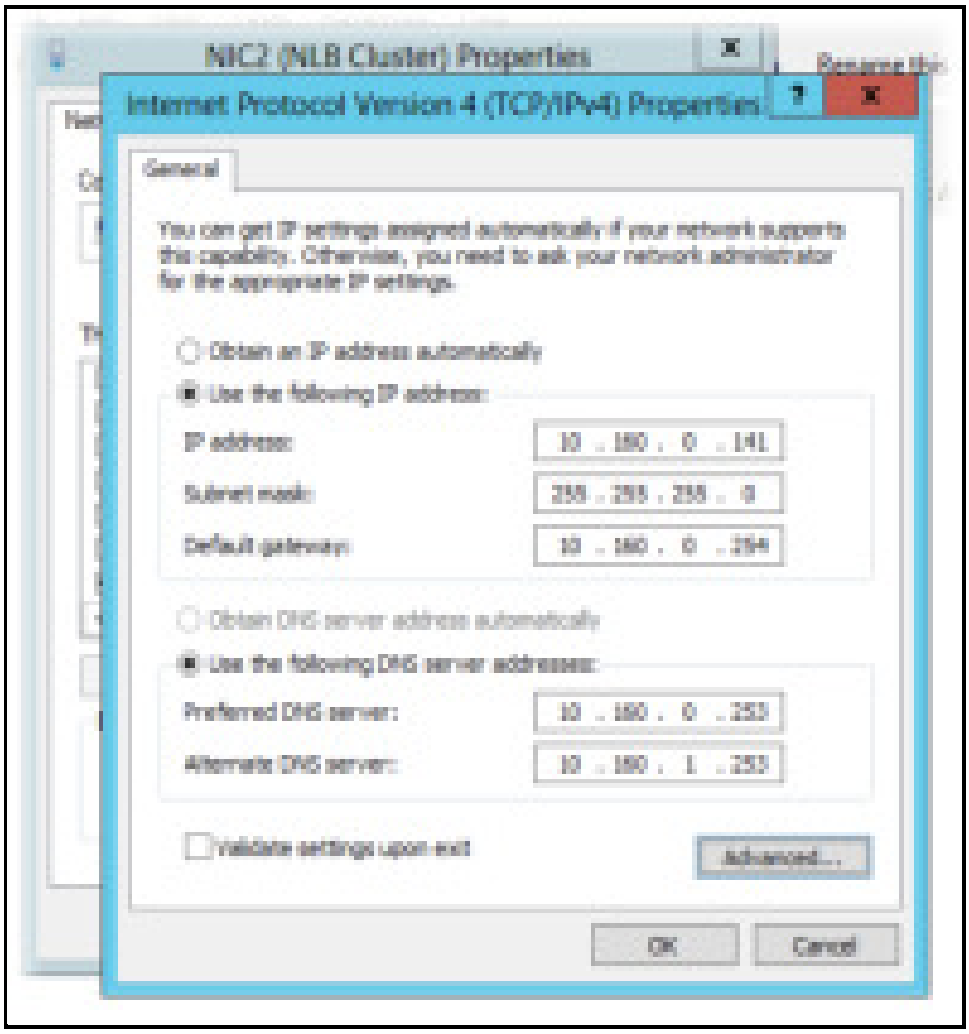

NIC1 должен иметь приоритет над NIC2.



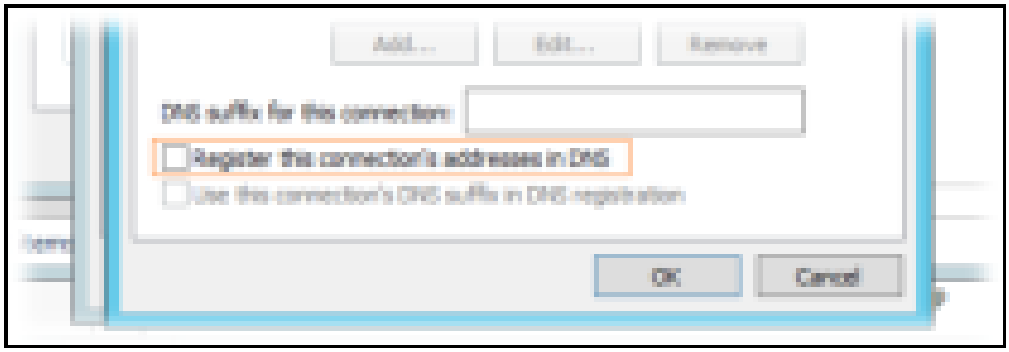

В свойствах сетевого подключения, которое будет использоваться для подключения к NLB кластеру (**NIC2**) можно отключить все компоненты, за исключением **TCP/IPv4** и **Client for Microsoft Networks**:



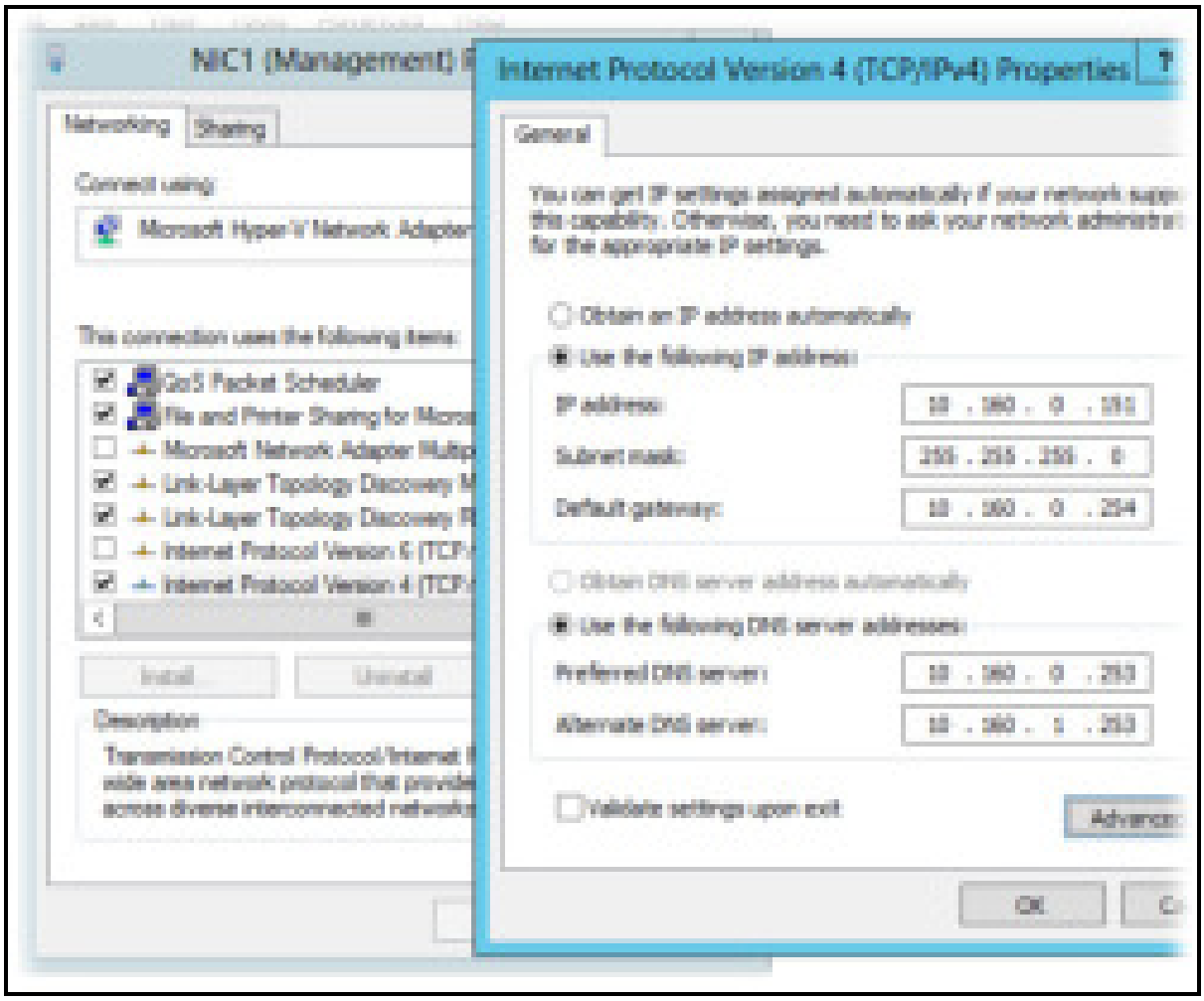

В свойствах компонента **TCP/IPv4** зададим настройки согласно приведённой ранее таблицы и по кнопке **Advanced** откроем окно дополнительных настроек



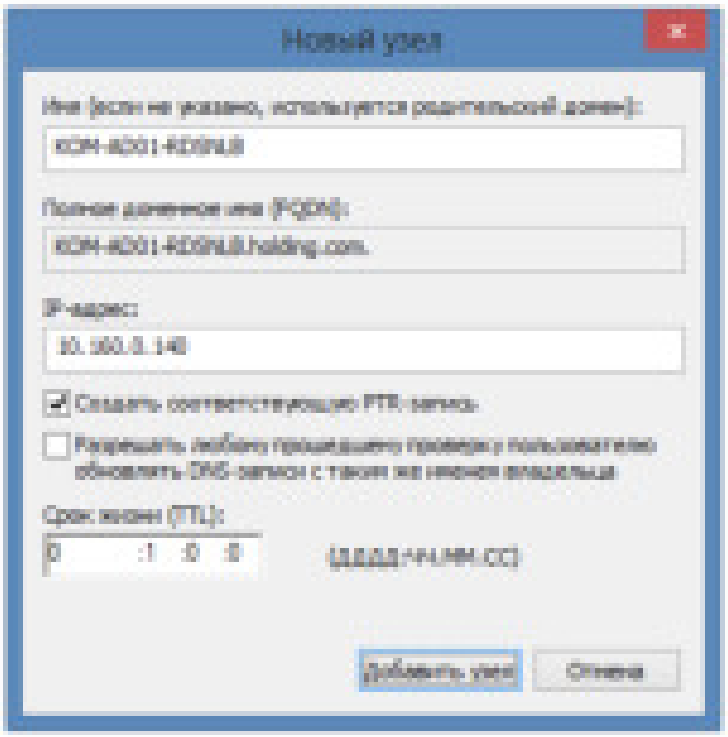

В окне дополнительных настроек TCP/IP на закладке **DNS** отключим механизм регистрации в DNS:



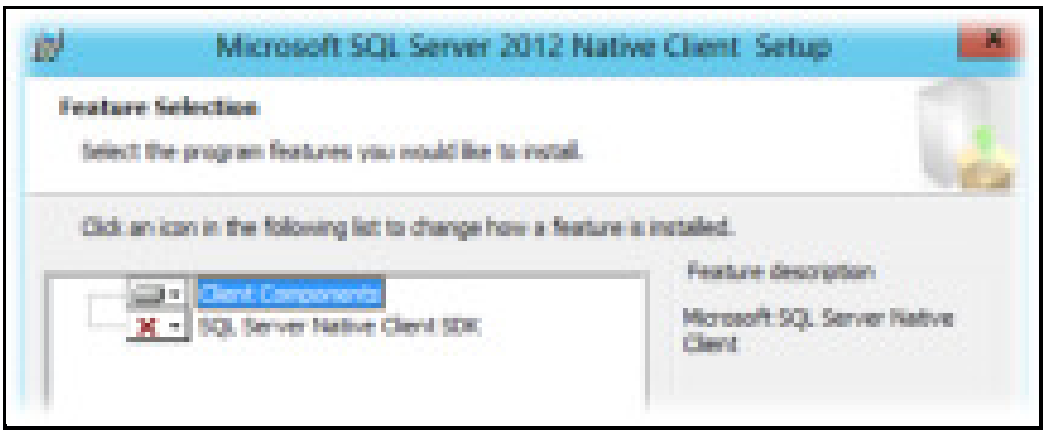

Интерфейс **NIC1** настроим согласно вышеприведённой таблицы аналогичным образом, за исключением того, что на нём может быть включена опция регистрации в **DNS** и обязательно должны быть включены компоненты **TCP/IPv4** , **Client for Microsoft Networks** и **File and Printer Sharing for Microsoft Networks**




После того как описанным способом настроены сетевые интерфейсы на всех серверах, зарегистрируем их имена в доменной зоне прямого просмотра **DNS** (если запрещена динамическая регистрация в DNS и/или отключена опция регистрации в свойствах интерфейсов NIC1). Для пакетной регистрации Дополнительно сразу же создаём статическую **А-запись** для будущего **NLB** кластера.

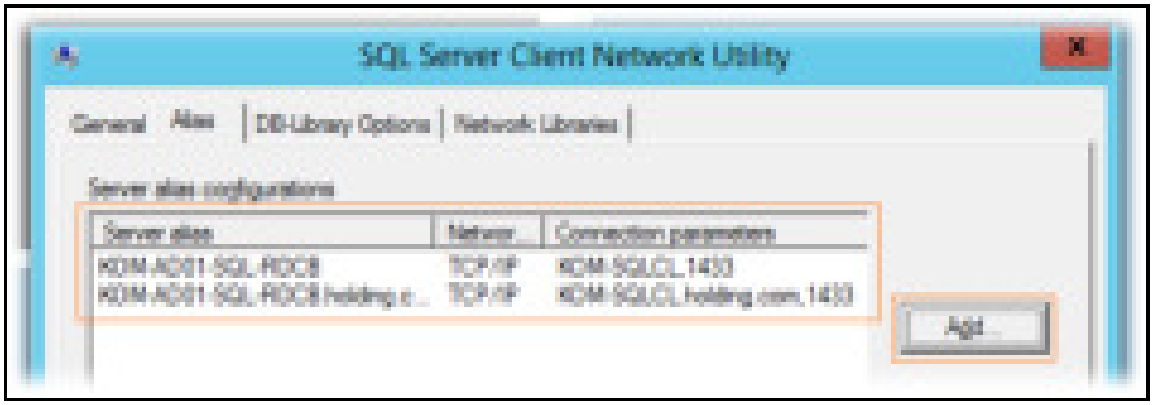



**RD Connection Broker** использует для хранения БД сессий общий экземпляр **SQL Server**, поэтому все сервера RDCB должны иметь "на борту" клиентские компоненты SQL Server, а также привилегии доступа к SQL Server. Настройку доступа к SQL Server выполним позже, а пока установим на каждый сервер, где планируется развертывание **RD Connection Broker**, свежую версию пакета **Microsoft SQL Server 2012 Native Client** (в нашем случае установка нужна на всех пяти виртуальных серверах).



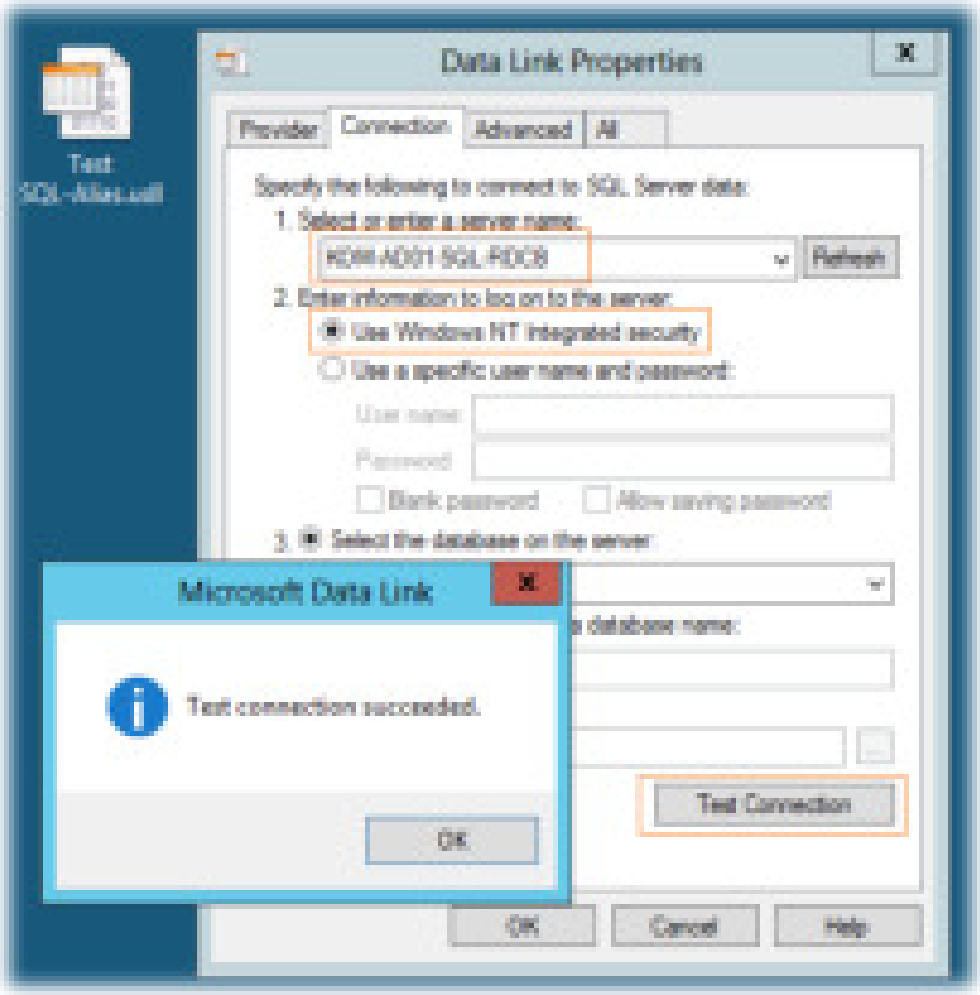

После установки клиента SQL Server создадим на каждом сервере SQL-Alias, который будем в дальнейшем использовать для подключения серверов RDCB к серверу SQL Server. Этого конечно можно и не делать, но это может оказаться полезным (даст нам дополнительную гибкость) в случае необходимости переноса БД на другой SQL-сервер или даже экземпляр. Запустим встроенную в ОС утилиту **SQL Server Client Network Utility**

(**C:\windows\system32\cliconfg.exe**) и добавим два новых алиаса – с коротким именем сервера и FQDN




Фактически созданные SQL-алиасы в интерфейсе утилиты были записаны в ключ реестра **HKLM\SOFTWARE\Microsoft\MSSQLServer\Client\ConnectTo**

Теперь нужно проверить созданные нами SQL-алиасы. Для этого создадим пустой файл **Universal Data Link** с расширением ***.udl** и запустим его. На закладке **Connection** укажем SQL-алиас, выберем режим аутентификации **Use Windows NT Integrated security** и нажмём кнопку **Test Connection**



Если мы всё сделали правильно, то получим положительный результат подключения. При этом перечень всех активных БД на новом SQL сервере будет доступен в выпадающем списке **Select the database on the server**. Таким образом проверим алиас созданный как по NetBIOS имени так и по FQDN.

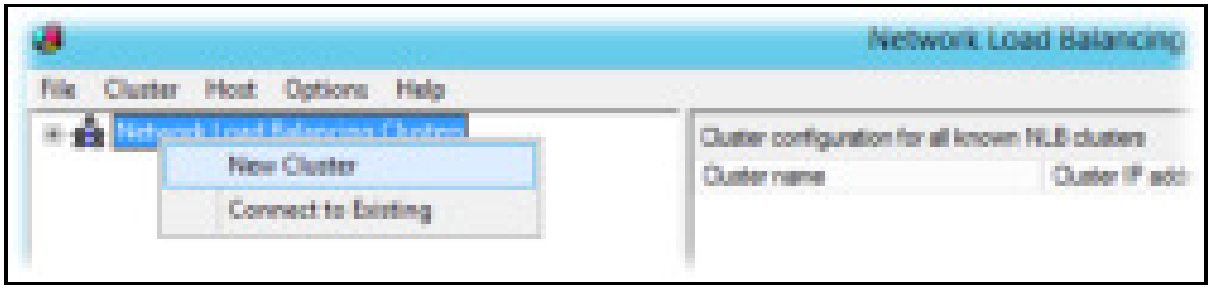
***

Далее, с помощью **PowerShell** установим на каждый сервер исполняемые компоненты **NLB**

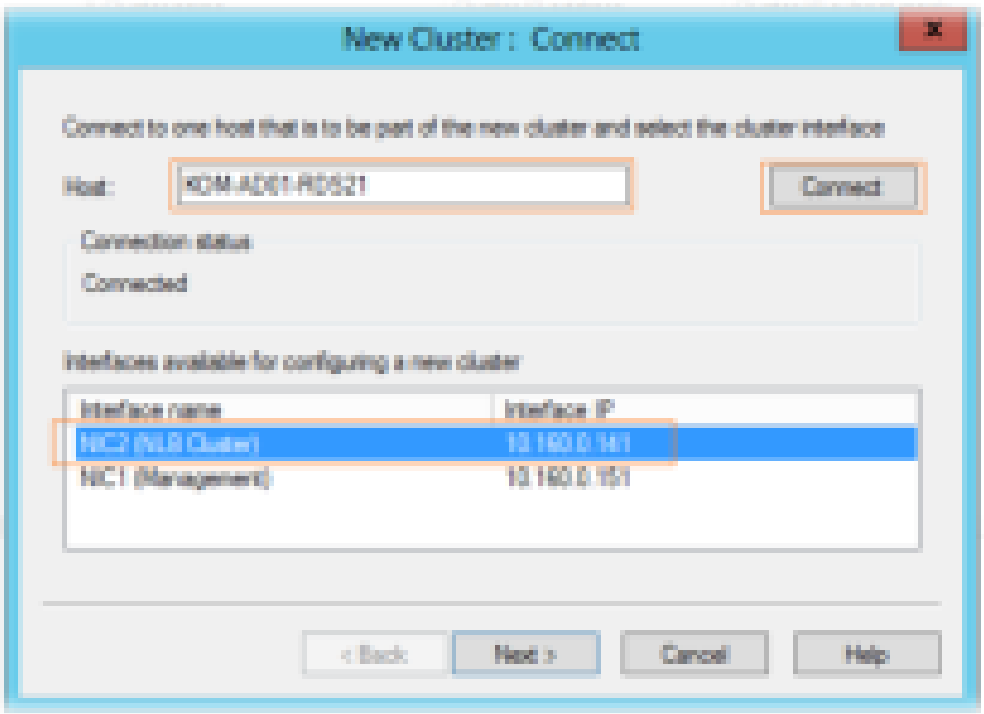
**Import-Module** "ServerManager"
**Add-WindowsFeature** "NLB" *-IncludeManagementTools*

**Создаём кластер NLB**

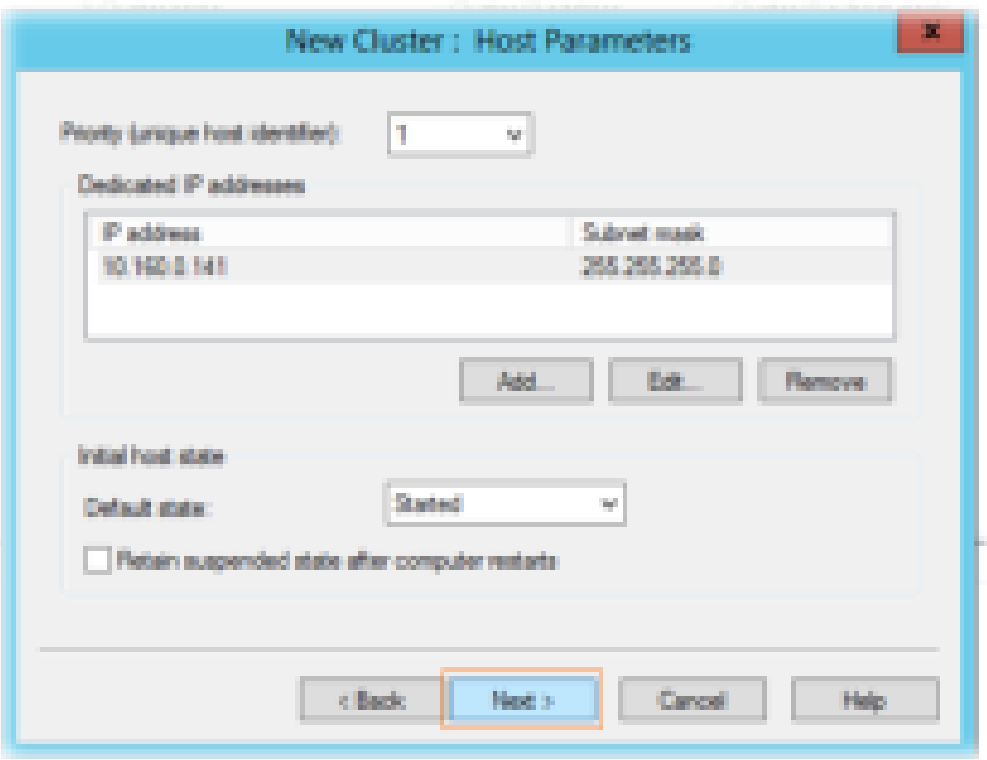
На первом виртуальном сервере (**KOM-AD01-RDS21**) открываем консоль **Network Load Balancing Manager** (nlbmgr.exe). Выбираем пункт меню **Cluster > New Cluster**



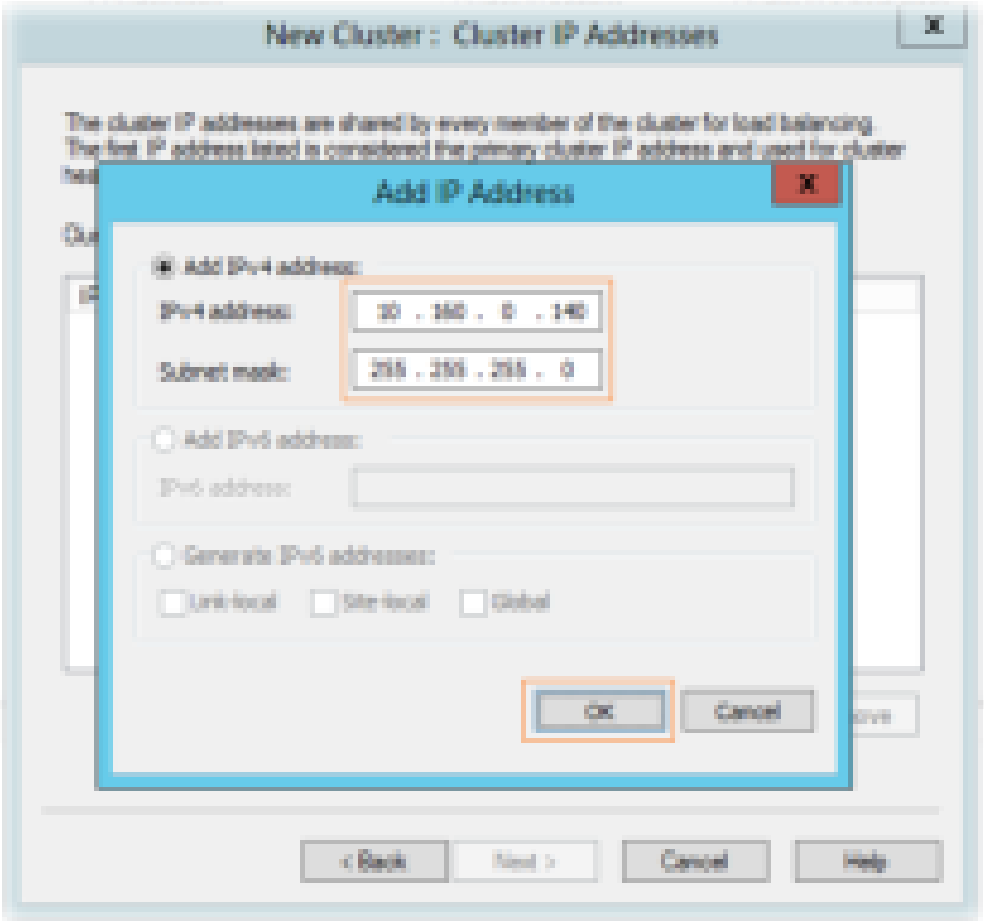

Вводим имя первого узла, который хотим добавить в NLB, кнопкой **Connect** подключаемся к нему, и получив с него набор доступных интерфейсов, выбираем тот который хотим сделать участником кластера:



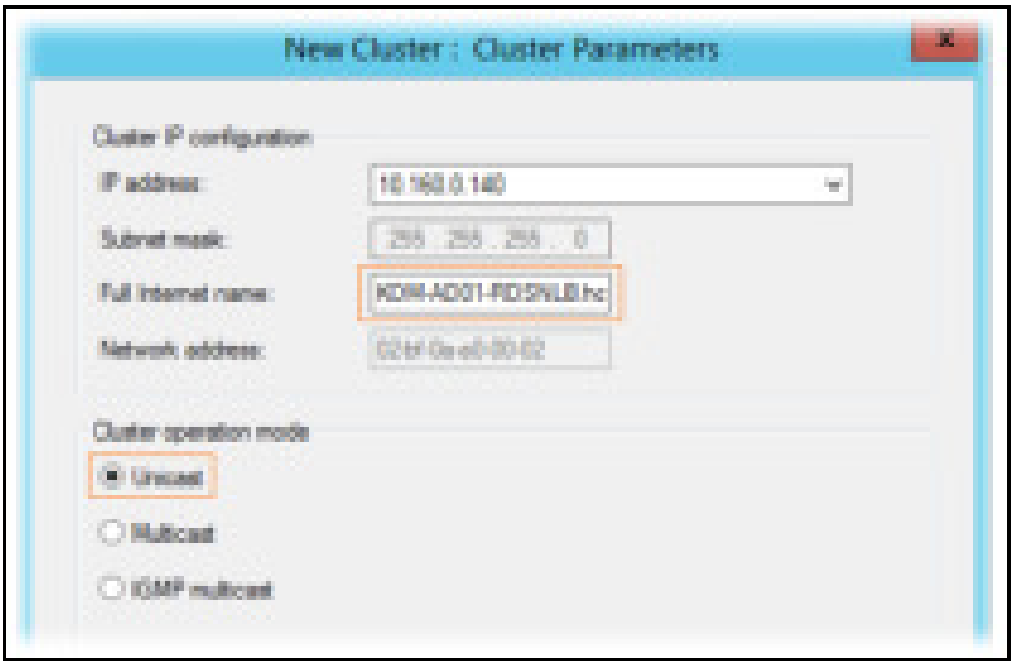

На странице параметров хоста (**Host Parameters**) оставляем настройки по умолчанию:




В следующем окне мастера создания кластера добавляем **IP** адрес **NLB** кластера, на который мы ранее в DNS зарегистрировали А-запись.

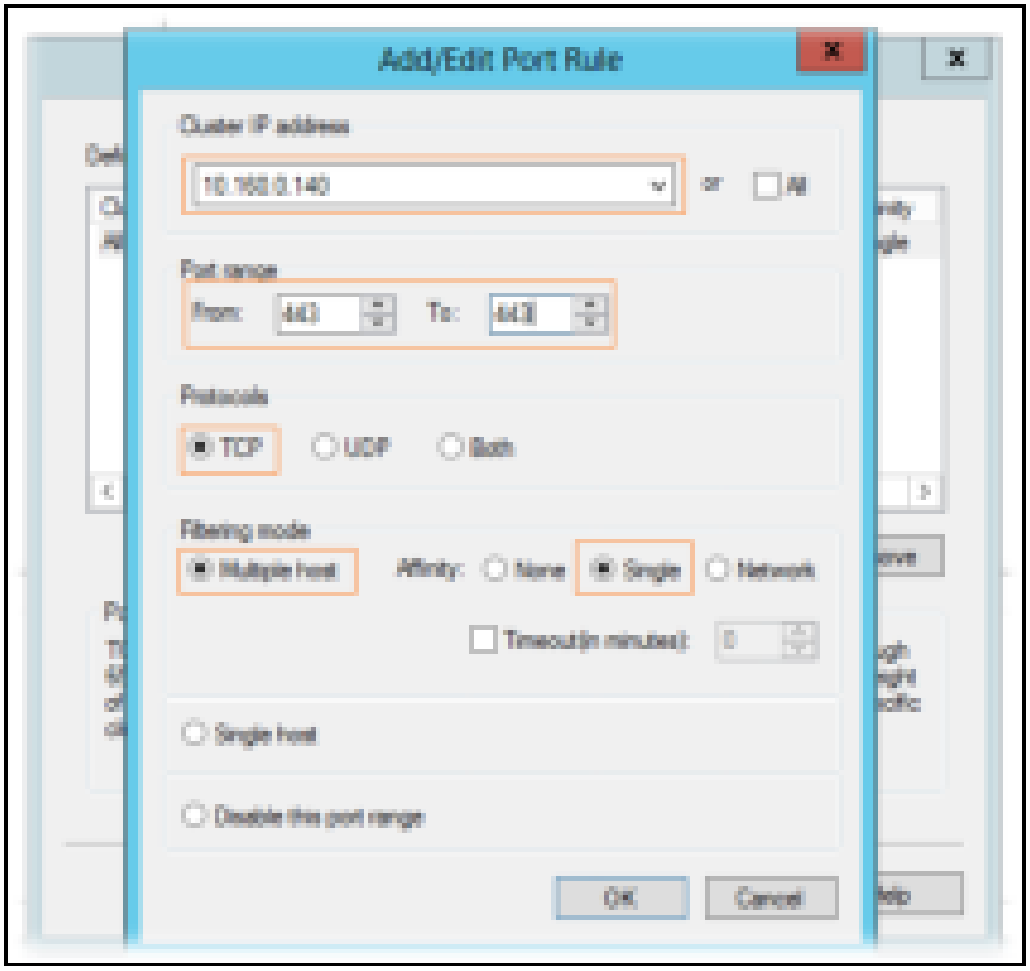



Далее указываем **FQDN** кластера **NLB** (по той самой А-записи), а также режим его работы. Режим работы кластера – режим одноадресной рассылки – **Unicast**.



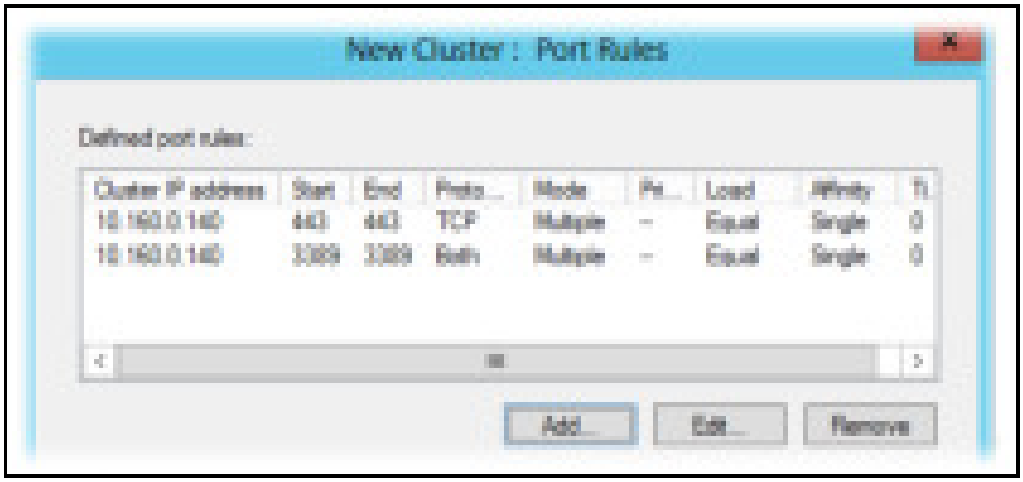

На странице правил портов (**Port rules**) удаляем имеющееся по умолчанию правило и добавляем необходимые нам правила. При добавлении правила

портов убираем флажок **All** и указываем конкретный интерфейс NLB и диапазон портов, который хотим добавить в кластер NLB.

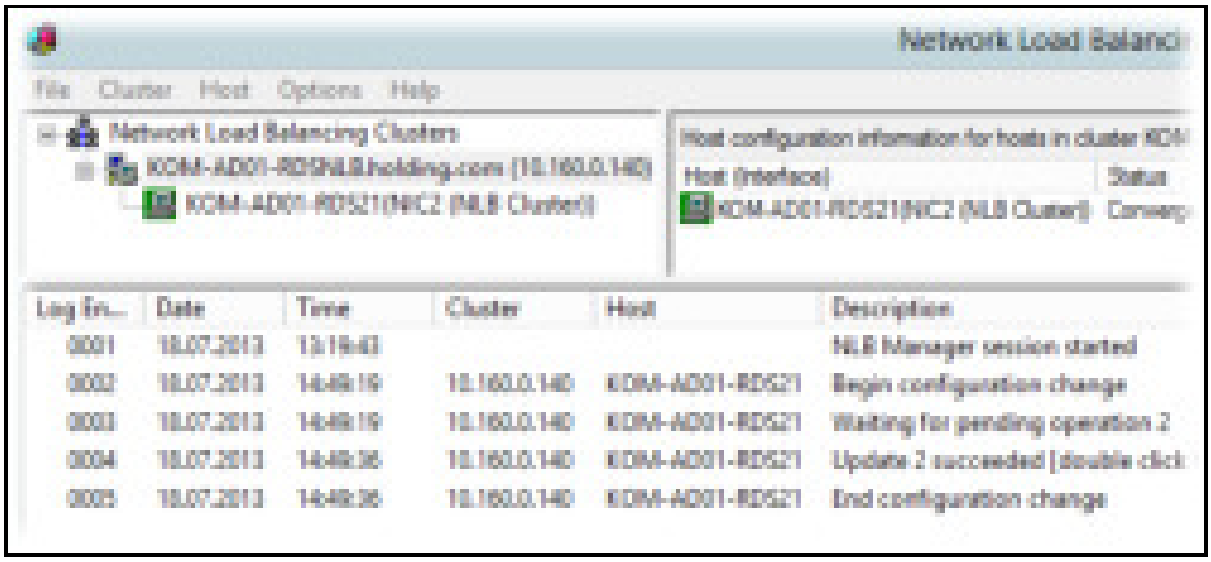



В общей сложности, в нашем примере балансировке в NLB кластере мы будем подвергать следующие порты:

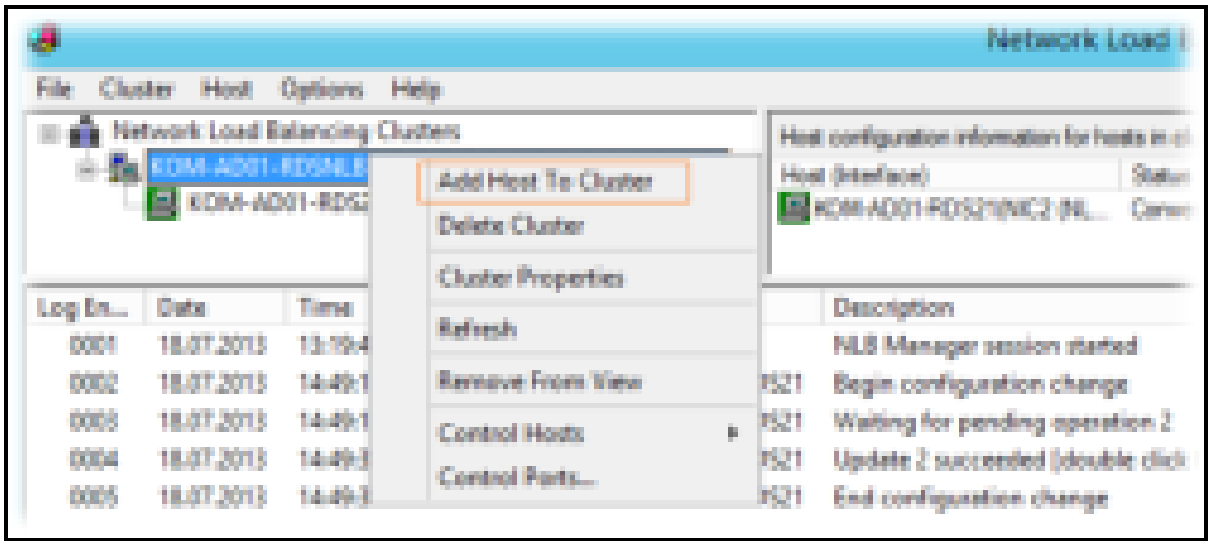
**TCP 443** – для подключения клиентов к **RD Web Access**;
**TCP/UDP 3389** – для подключения клиентов к **RD Connection Broker/Session Host**;



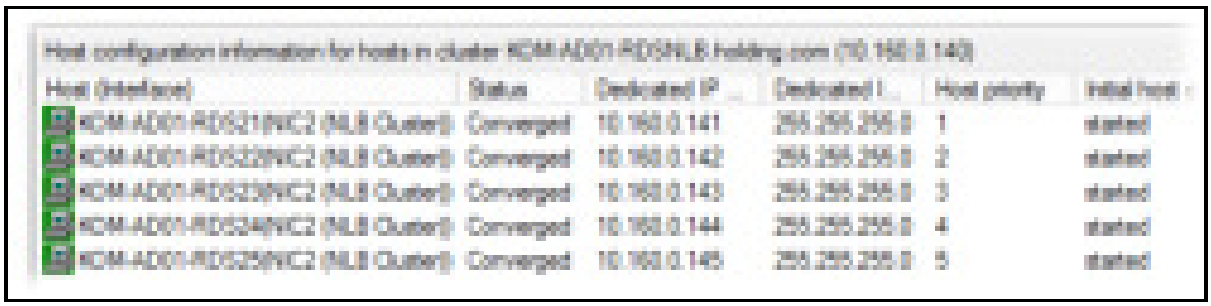
Все необходимые параметры кластера заданы, создаем его по нажатию кнопки **Finish** и после первоначальной инициализации, если в конфигурации не допущены ошибки, NLB кластер запуститься в конфигурации с одним узлом




Далее, переходим на имя NLB кластера и пунктом меню **Add Host to Cluster** вызываем мастер добавления второго и последующих серверов в кластер.



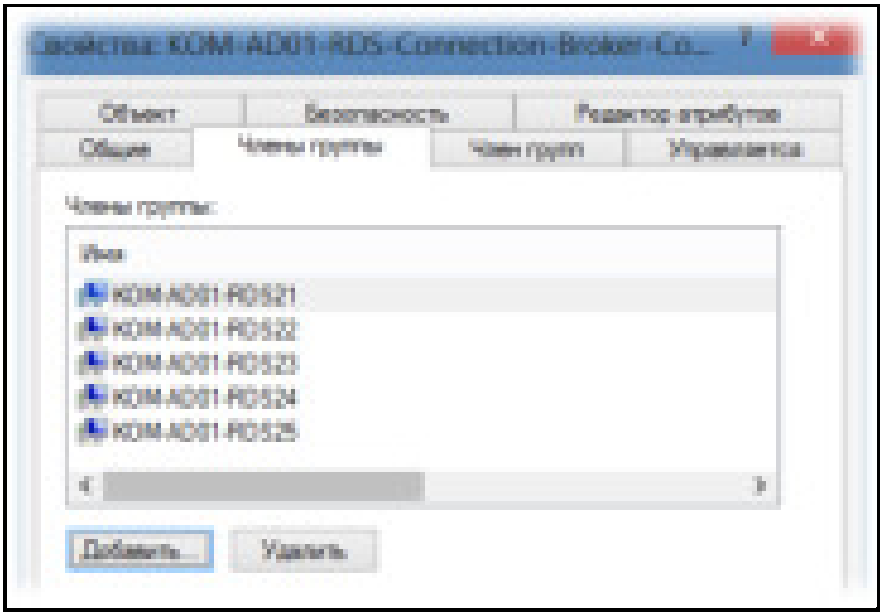

В конечном итоге после добавления (по аналогии с первым узлом) всех серверов мы получим работоспособный Windows NLB кластер



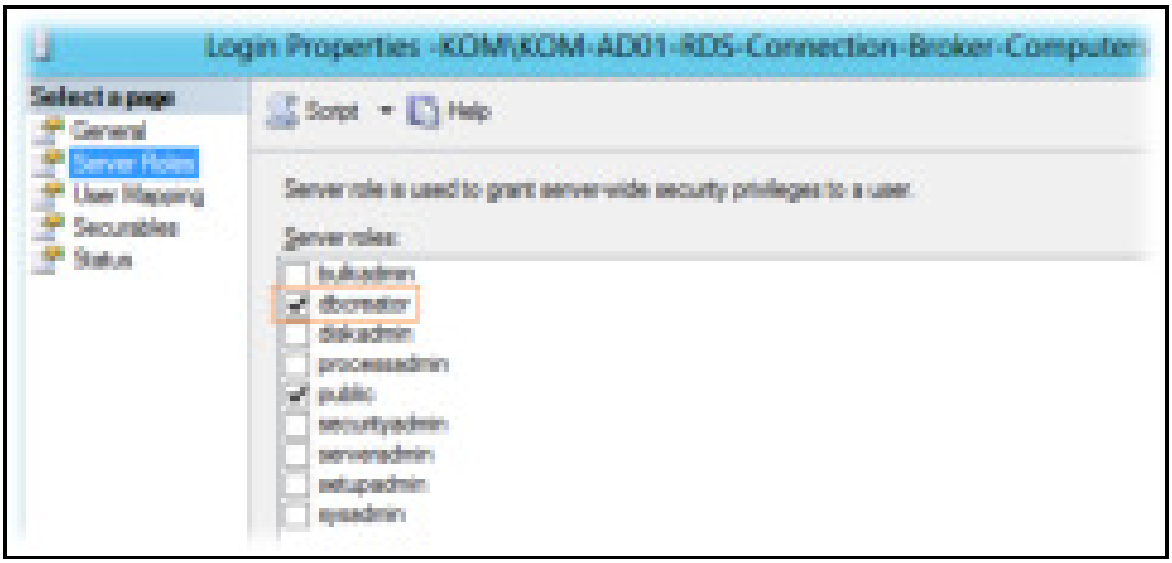
С помощью **Ping -t** проверяем из клиентской подсети доступность кластерного интерфейса по очереди перезагружая узлы кластера, а затем друг за другом выключая их до тех пор пока в кластере не останется один живой узел.

**Подготавливаем SQL Server**

Создадим в AD группу безопасности, например **KOM-AD01-RDS-Connection-Broker-Computers**, и включим в нее учетные записи наших виртуальных серверов.



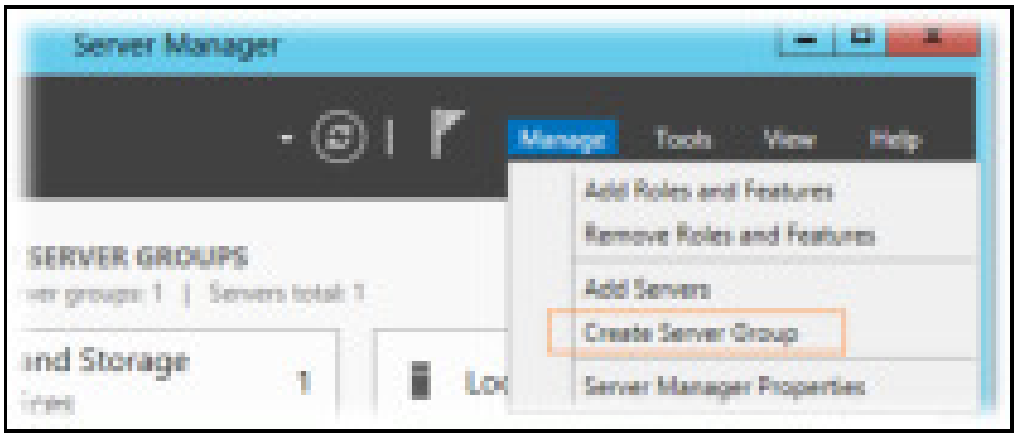

После этого подключимся к экземпляру **SQL Server** на котором будет размещаться БД RDCB (в нашем случае это отдельный кластер SQL Server из двух серверов), создадим новый **SQL Login** с привязкой к указанной доменной группе. При создании SQL-логина ему будет присвоена серверная роль SQL Server – **public**, которая даст право подключаться к экземпляру SQL Server. Включим ещё одну серверную роль – **dbcreator**. Эта роль понадобится нам лишь на время первоначальной инициализации БД RDCB для того, чтобы учетная запись сервера, на котором мы будем запускать процесс создания отказоустойчивого RDCB, смогла выполнить операцию создания новой БД.



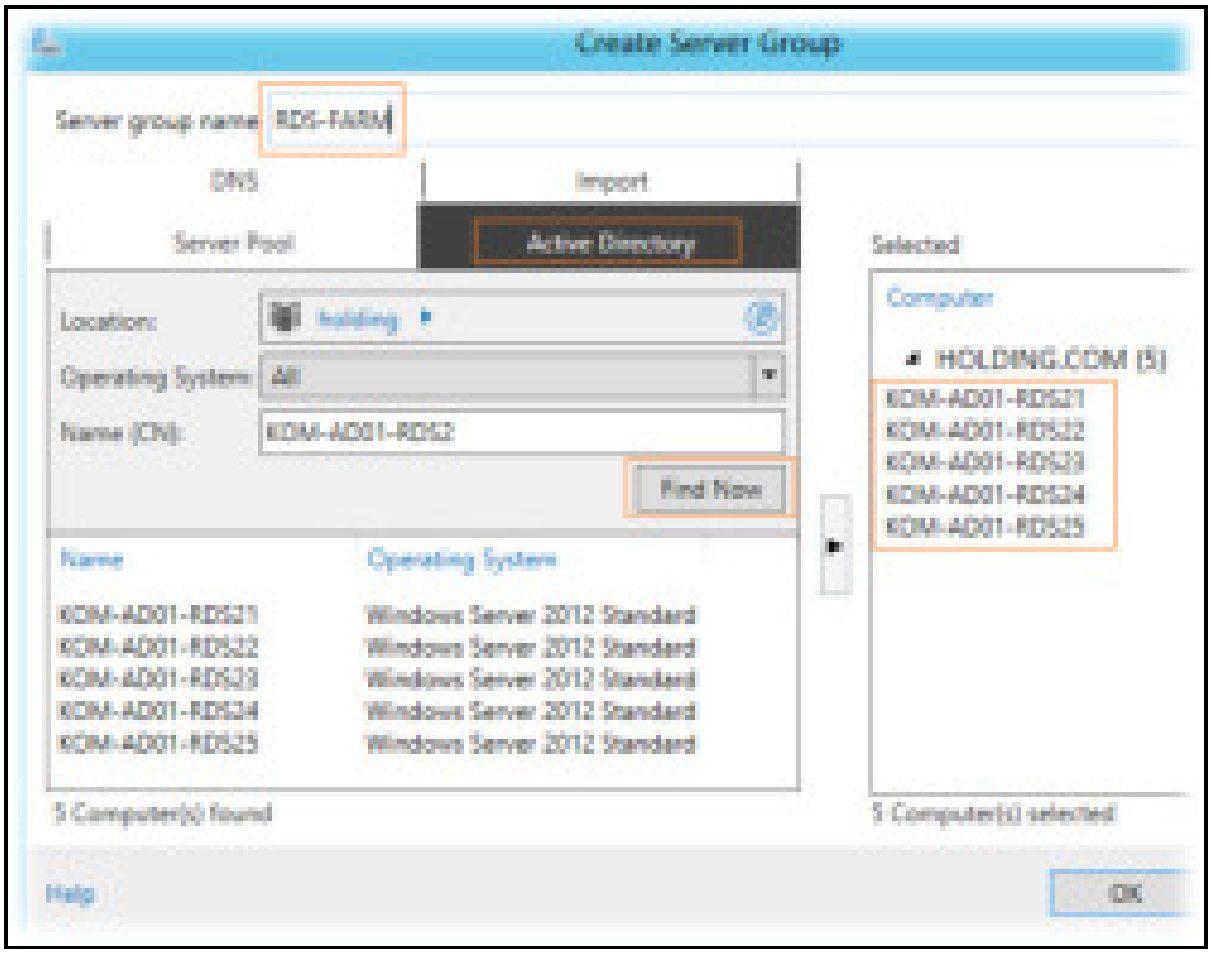

Дополнительно на SQL сервере создадим каталог для файлов базы данных RDCB. В нашем случае это будет каталог **U:\SQLData_SQL01_RDCB** на кластерном диске SQL сервера.

**Устанавливаем роли Remote Desktop Services**

Так как консоль **Server Manager** в **Windows Server 2012** поддерживает групповую настройку сразу нескольких серверов, перед тем как разворачивать на наши виртуальные сервера роли RDS, объединим их в логическую группу. На любом из виртуальных серверов, например на **KOM-AD01-RDS21**, откроем консоль **Server Manager** и выберем пункт меню **Manage** > **Create Server Group**

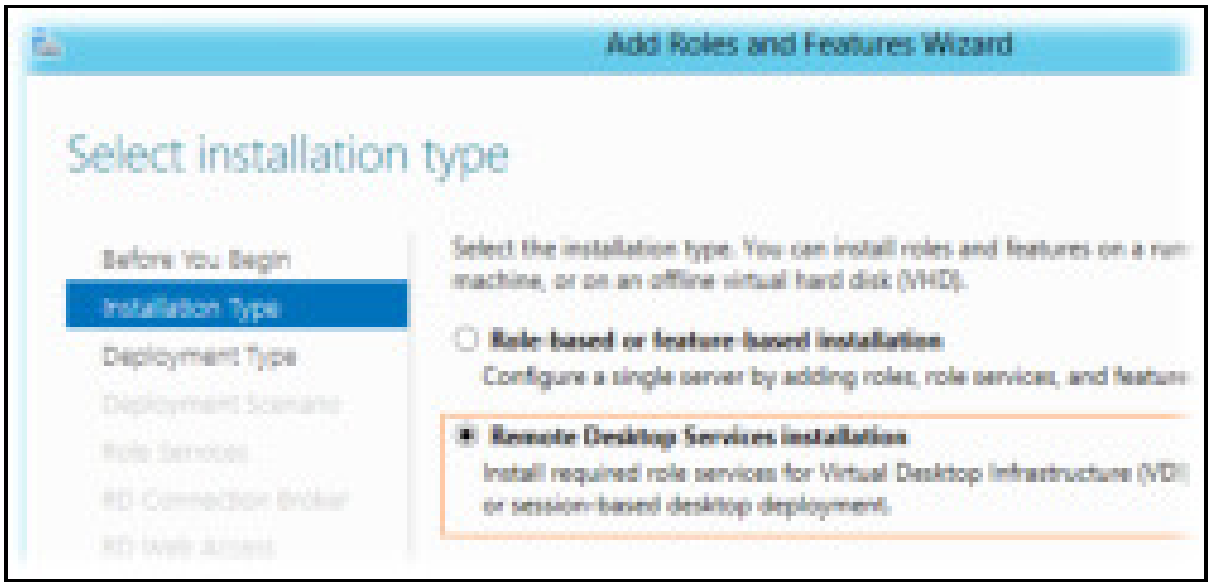



добавим пять наших виртуальных серверов в группу и дадим ей название, например **RDS-FARM**.

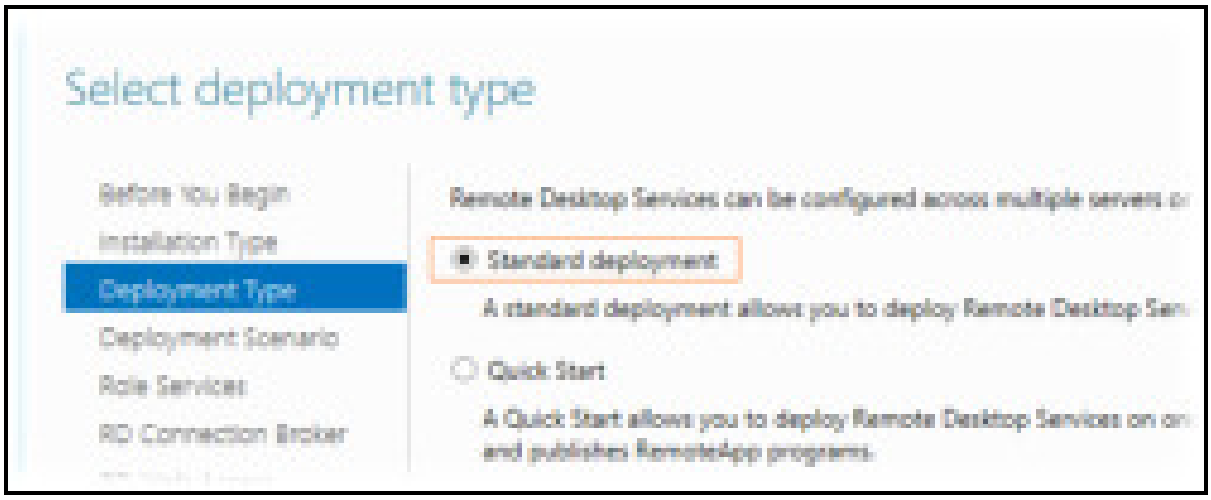



После этого выберем пункт меню **Manage > Add Roles and Features Wizard**

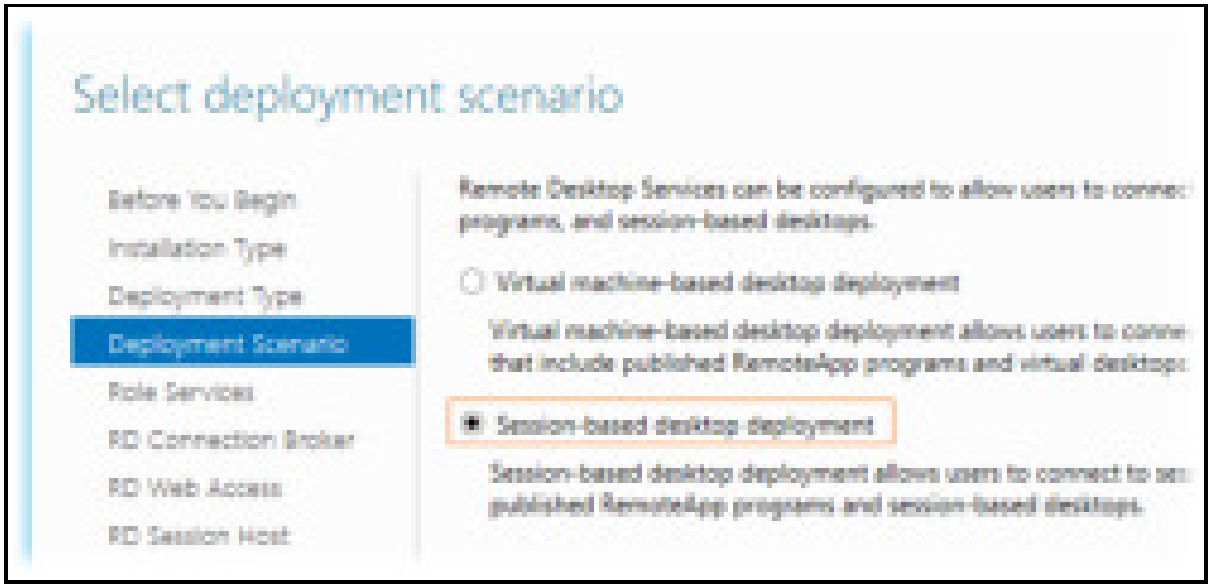
В открывшемся мастере добавления ролей выберем режим установки служб RDS - **Remote Desktop Services installation**



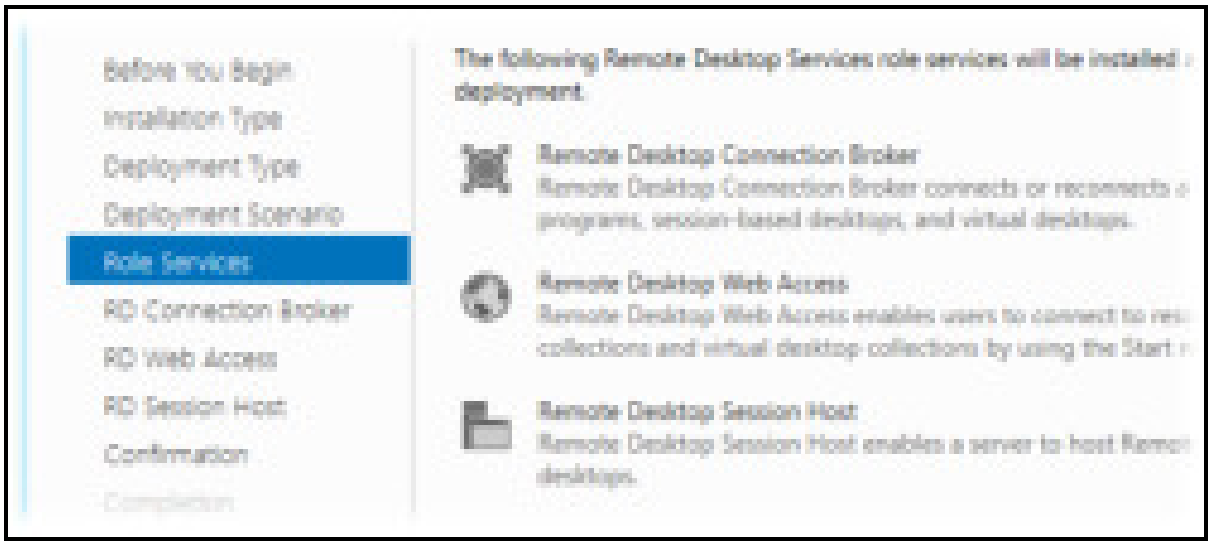

Тип развёртывания - **Standard deployment**



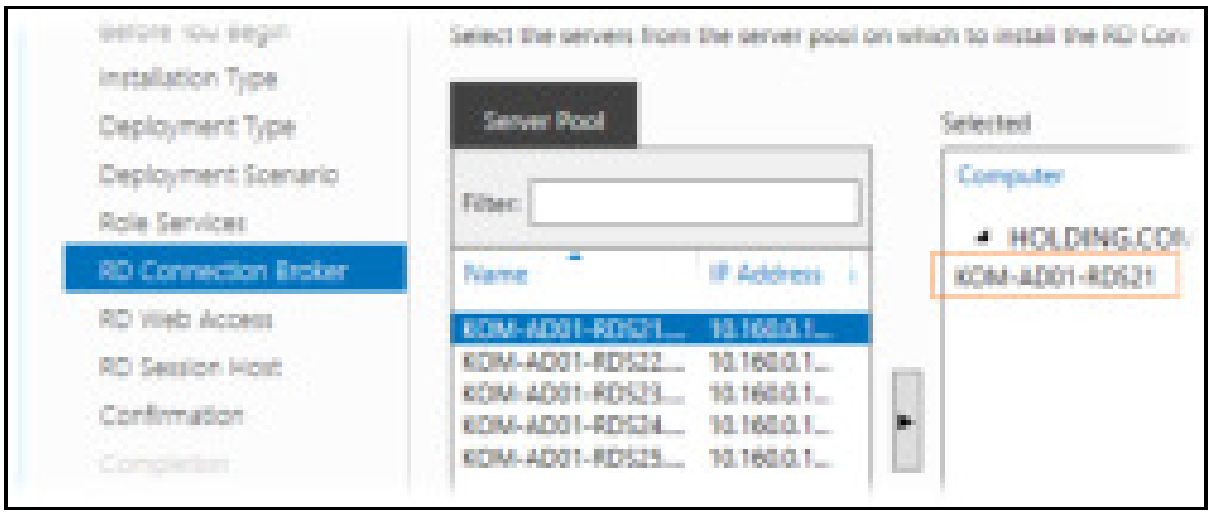

Сценарий развертывания выбираем **Session-based desktop deployment**, так как планируется развертывание серверов сеансов, а не серверов инфраструктуры VDI



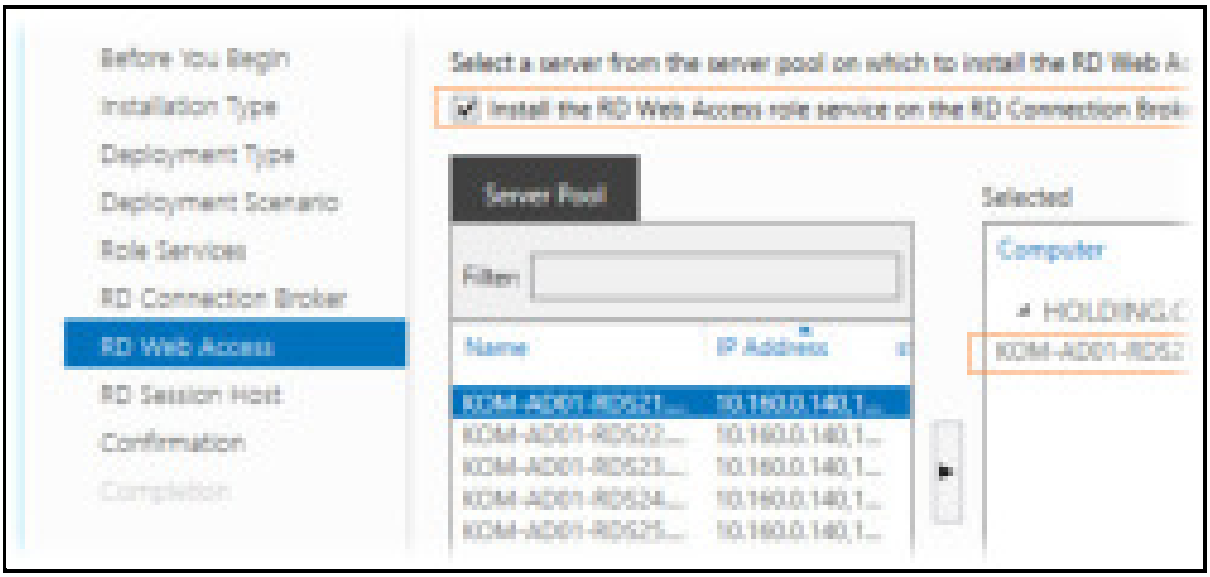

На этапе выбора ролей RDS нас предупредят о том, что будет выполняться развертывание сразу трёх ролей - **RD Connection Broker**, **RD Session Host**, **RD Web Access**, не оставляя при этом нам никакого выбора…



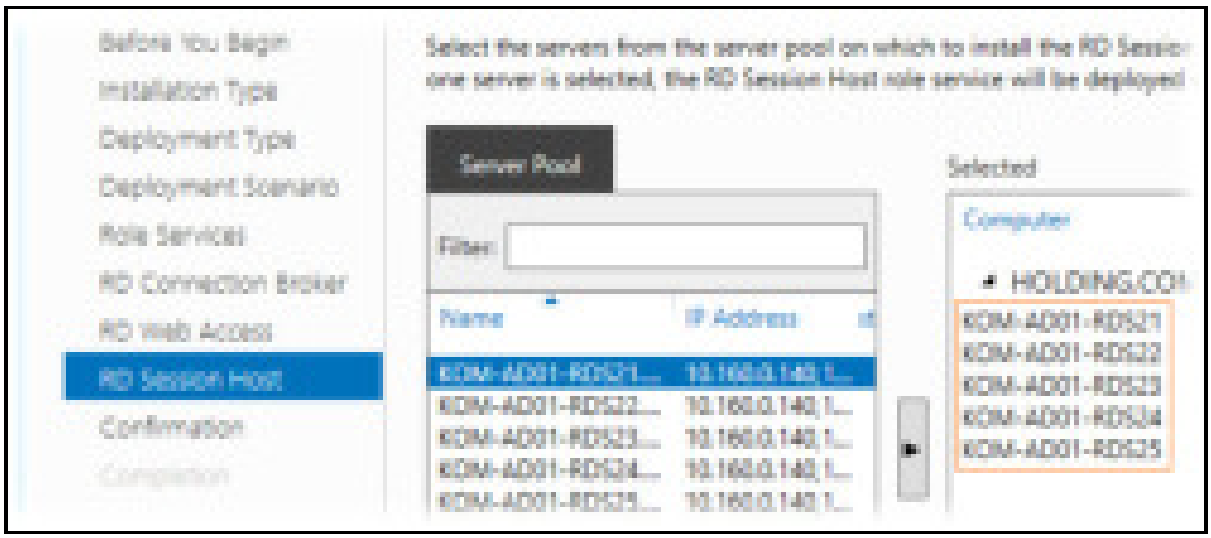

На этапе выбора серверов для роли **RD Connection Broker** выбираем один сервер, ибо мастер не даст нам выбрать более одного сервера. Так как всю первоначальную настройку мы выполняем на сервере **KOM-AD01-RDS21**, то соответственно и выберем его для этой роли…



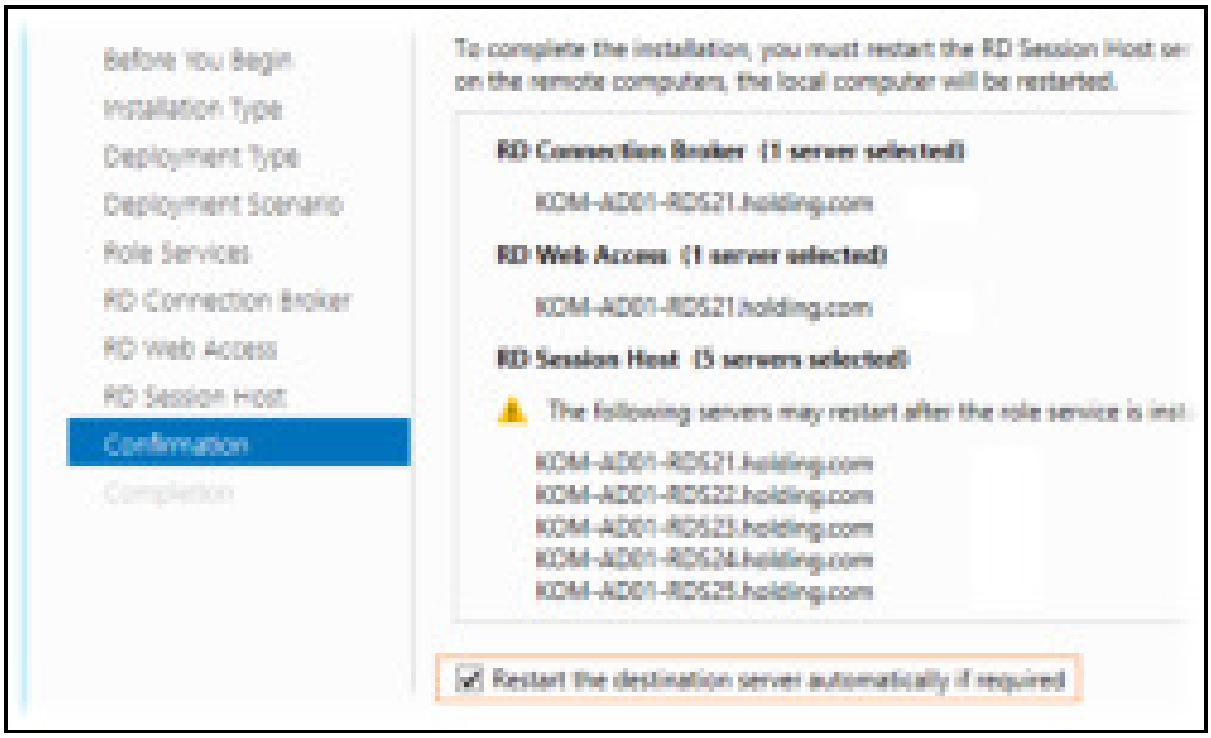

На этапе выбора серверов для роли **RD Web Access** включим опцию **Install the RD Web Access role on the RD Connection Broker server** для того чтобы эта роль была установлена на тот же сервер, который был выбран для роли RDCB. Выбирать какой-то другой сервер в нашей ситуации особого смысла нет, да и потом мастер опять таки не даст нам выбрать для установки этой роли более чем один сервер…



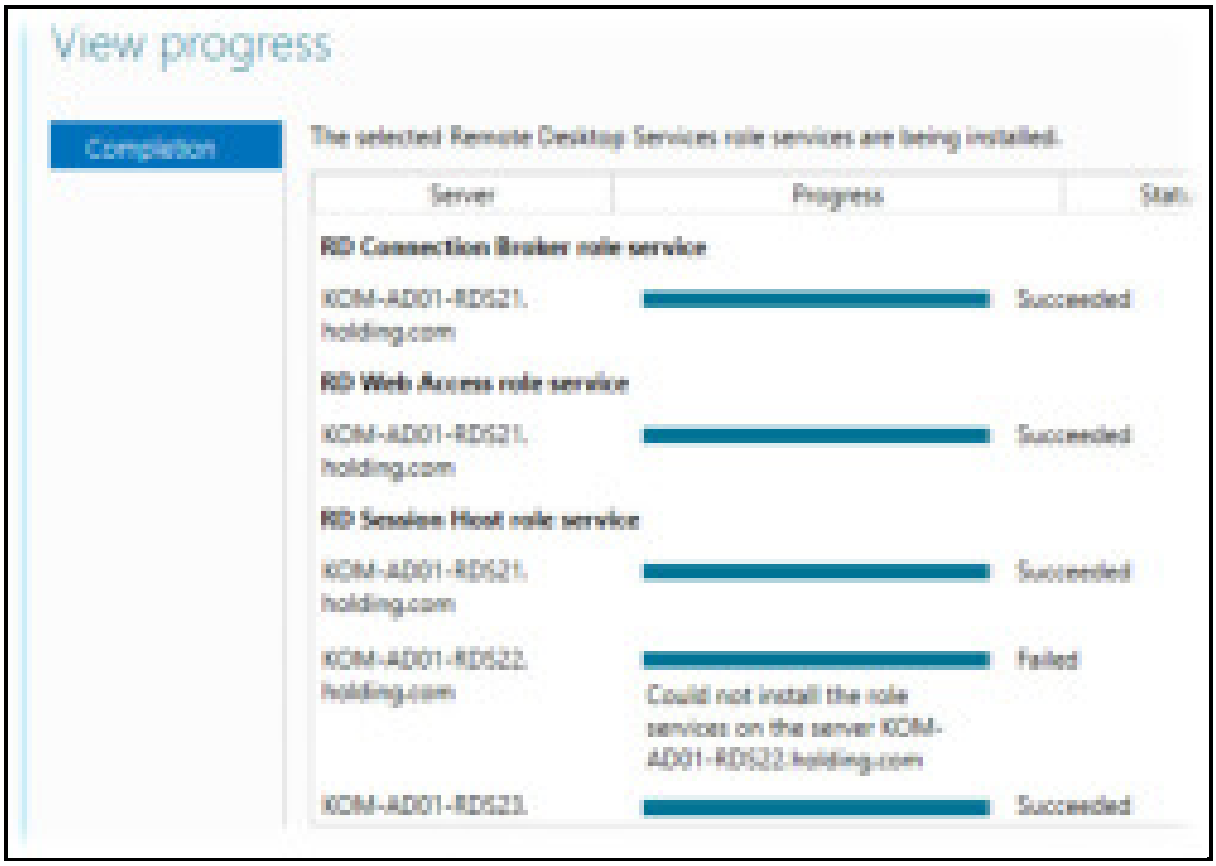

На этапе выбора серверов для роли **RD Session Host** мы сможем выбрать все сервера…



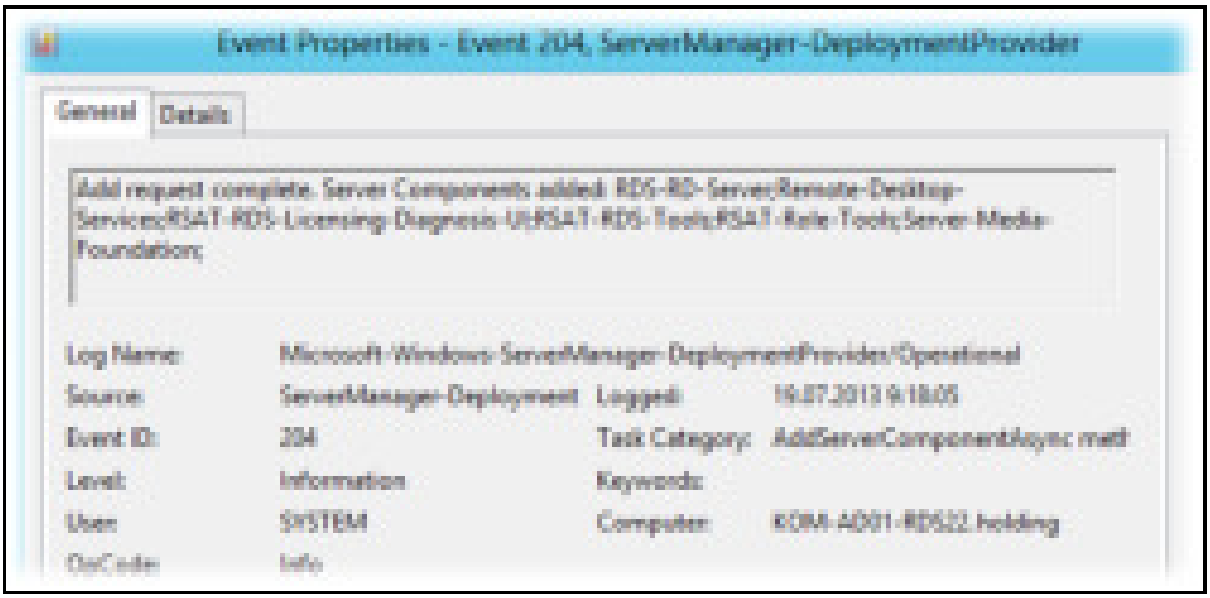

На странице подтверждения мы видим предупреждение, что серверы могут быть перезагружены после установки роли **RD Session Host**. Включим опцию автоматической перезагрузки серверов - **Restart the destination server automatically if required** и запустим процесс развёртывания..



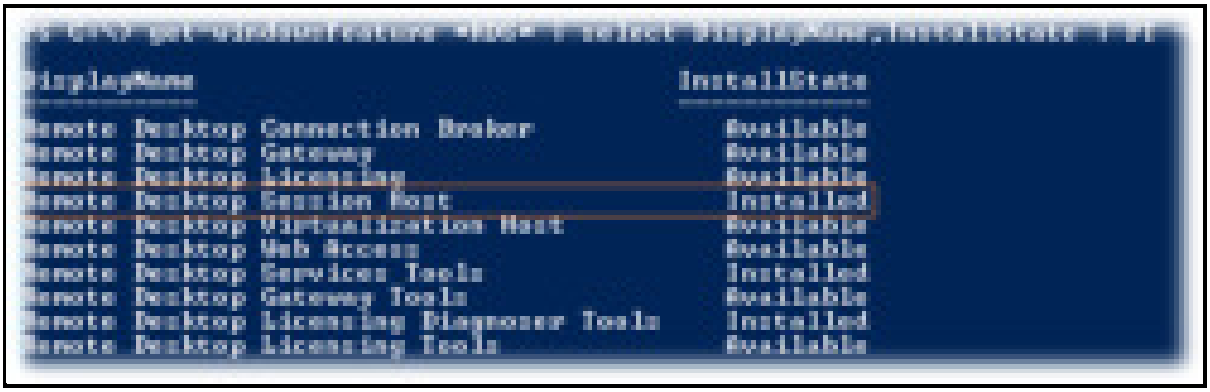

В процессе установки ролей первым будет автоматически перезагружен сервер, с которого мы запустили весь этот процесс, поэтому мы отвалимся от его консоли. Пугаться не надо… После того, как система поднимется из перезагрузки, снова залогинимся и запустим консоль **Server Manager**, где через несколько секунд автоматически запустится мастер развертывания ролей RDS и мы сможем убедиться в том, что процесс развертывания успешно прошёл до конца на всех серверах.



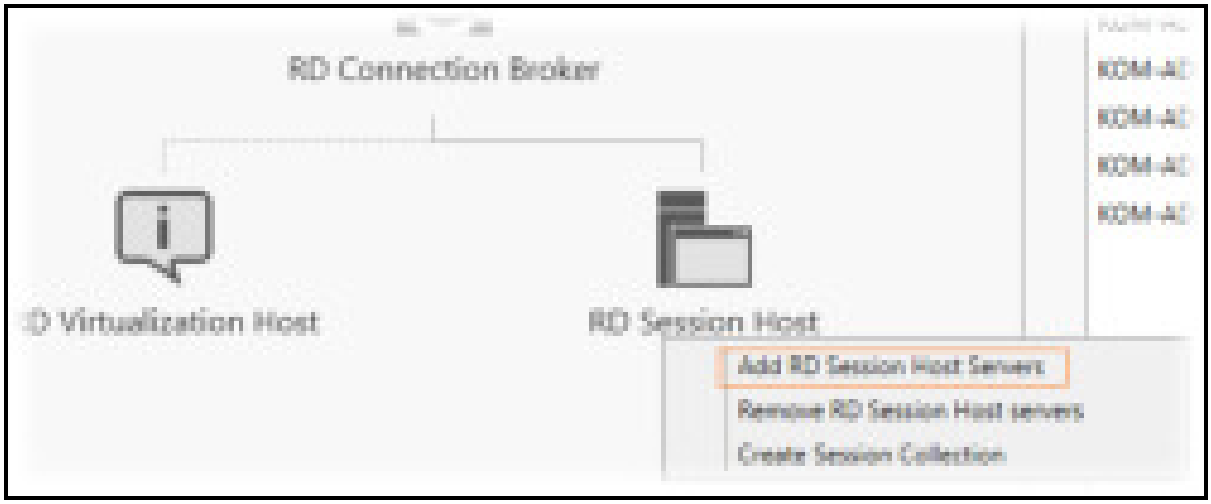

В нашем примере мастер сообщил о том, что на двух серверах из пяти не удалось установить службу RDSH, хотя последующая проверка этих серверов свидетельствовала об обратном. В системном журнале **Applications and Services Logs > Microsoft > Windows > ServerManager-DeploymentProvider > Operational** было зарегистрировано событие говорящее об успешной установке компонент…



Ну и соответственно PS-запрос состояния компонент RDS показывал что роль RDSH установлена..

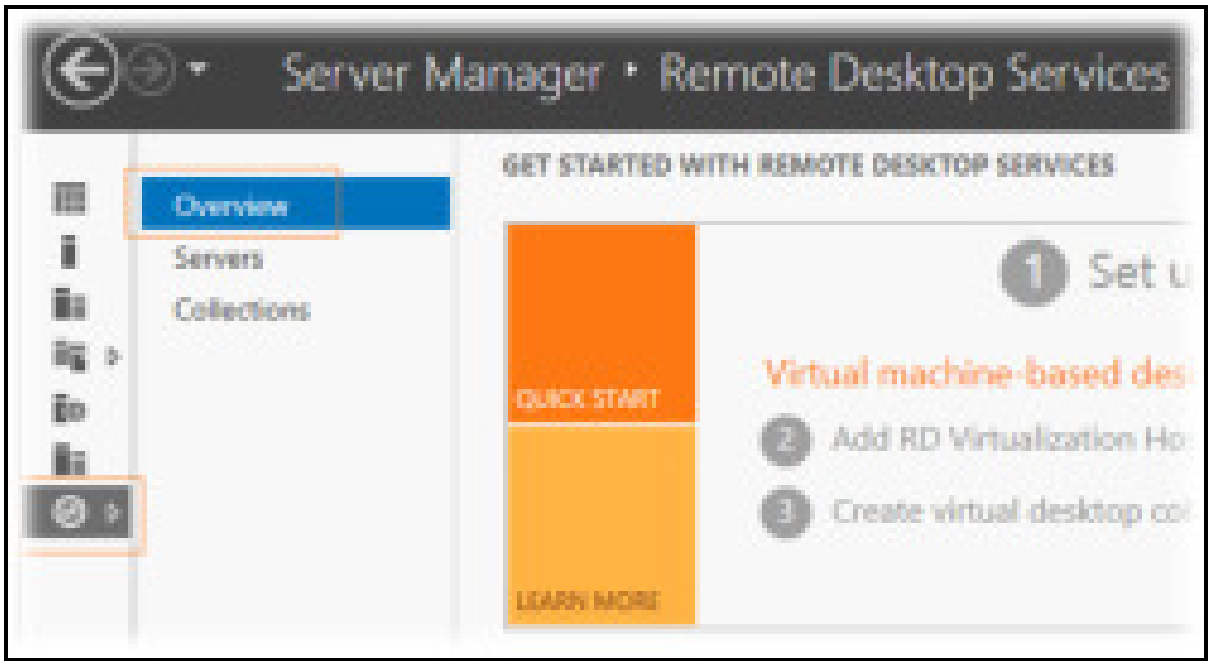



В любом случае если **Server Manager** упорно будет говорить вам о том, что роль **RD Session Host** не установлена на каких-то серверах, то для того чтобы заставить её "прокашляться", можно повторить процедуру установки через мастер добавления ролей RDS на вкладке управления службами **Remote Desktop Services > Overview**



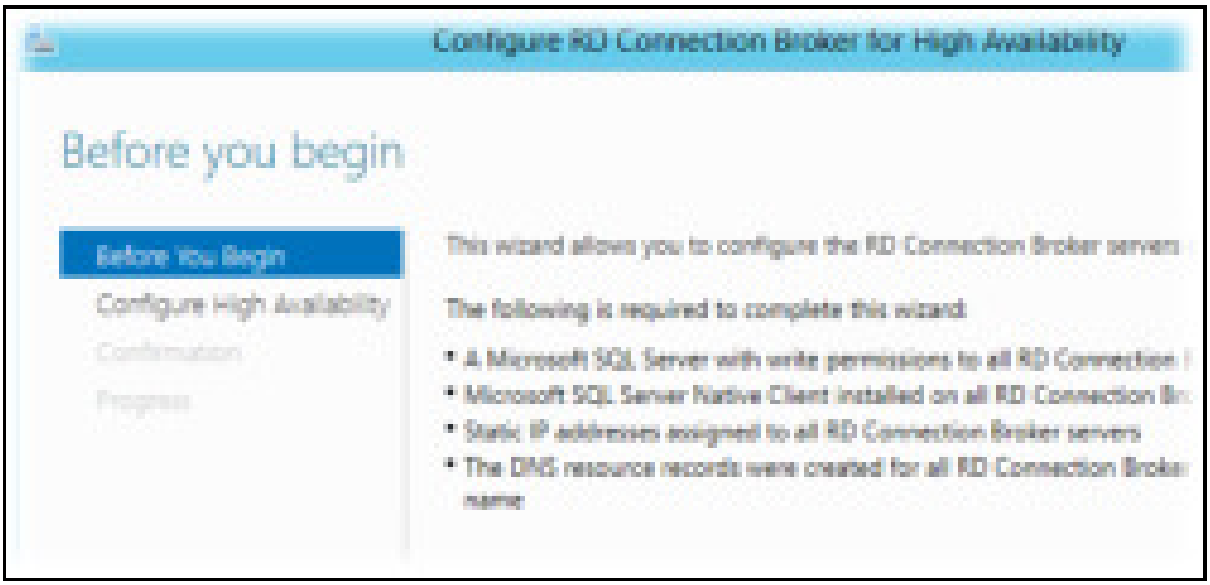

**Создаём высоко-доступный RD Connection Broker**

После окончания процесса установки ролей в консоли **Server Manager** и перейдём на вкладку управления службами **Remote Desktop Services > Overview**, чтобы приступить к созданию отказоустойчивой конфигурации **RD Connection Broker**.




На схеме инфраструктуры RDS выберем изображение роли **RD Connection Broker** и правой кнопкой мыши вызовем меню, в котором выберем пункт **Configure High Availability**.


Запустится мастер создания высоко-доступного экземпляра RDCB, где нас предупредят о необходимых условиях, которые мы уже предварительно выполнили, за исключением последнего пункта, который предполагает создание в DNS A-записей с одинаковым FQDN именем RDCB и IP адресами всех серверов (для работы механизма Round Robin). Откажемся от концепции использования DNS Round Robin для получения клиентами имени точки подключения к ферме RDCB. Вместо этого мы будем использовать имя созданного ранее NLB кластера.




На следующем шаге мастера **Configure High Availability** заполняем значения трёх полей:

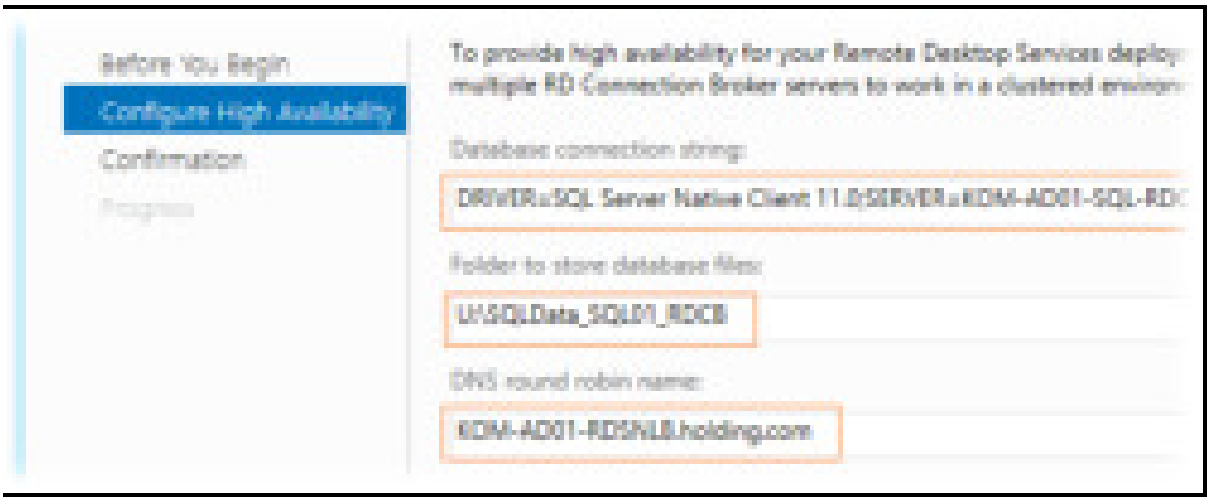
**Database connection string** – строка подключения к БД SQL Server. Значение должно иметь вид: DRIVER=SQL Server Native Client 11.0 (10.50 для SQL Server 2008 R2);SERVER=<FQDN-Имя или SQL-Alias сервера SQL Server>;Trusted_Connection=Yes;APP=Remote Desktop Services Connection Broker;DATABASE=<Имя БД>

В нашем случае это значение будет иметь следующий вид:

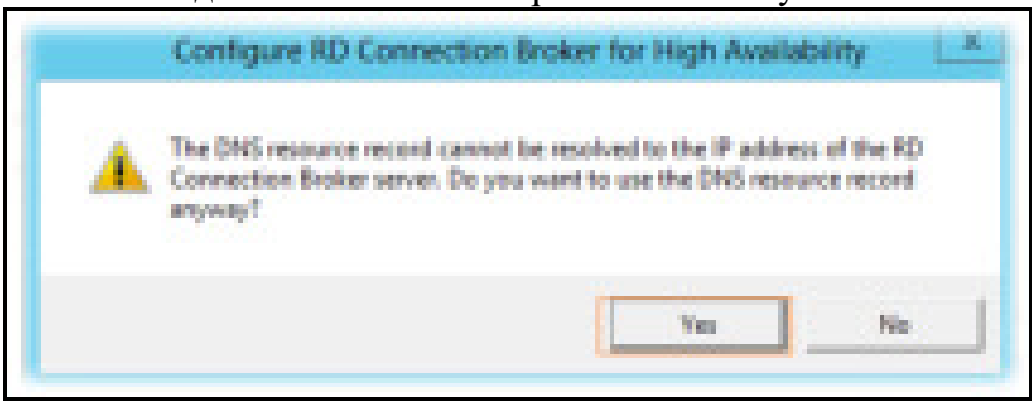
**DRIVER**=SQL Server Native Client 11.0;**SERVER**=KOM-AD01-SQL-RDCB.holding.com;**Trusted_Connection**=Yes;**APP**=Remote Desktop Services Connection Broker;**DATABASE**=RDS_ConnectionBroker

**Folder to store database files** - путь ранее подготовленного каталога **U:\SQLData_SQL01_RDCB** на кластерном диске SQL сервера. В этом каталоге будут размещены файл данных и лога транзакций SQL Server при создании БД RDCB.

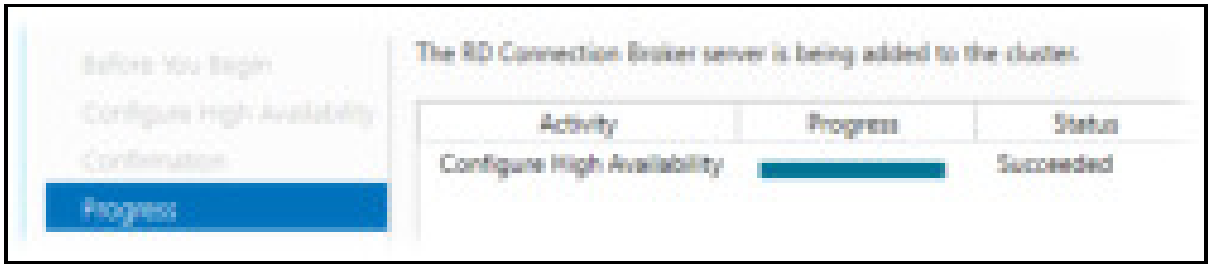
**DNS round robin name** – имя точки подключения клиентов. Как я уже сказал, здесь предполагается ввод значения FQDN-имени созданного в DNS с несколькими А-записями. В нашем примере, в качестве такого имени, мы будем использовать имя созданного ранее NLB кластера – **KOM-AD01-RDSNLB.holding.com**




Далее мы получим предупреждение о том, что указанное нами имя DNS RR имеет отличный IP адрес от того, для которого выполняется установка HA RDCB. Мы идём на этот шаг намеренно и поэтому соглашаемся…




Дожидаемся успешного окончания процесса конфигурирования высокой доступности.

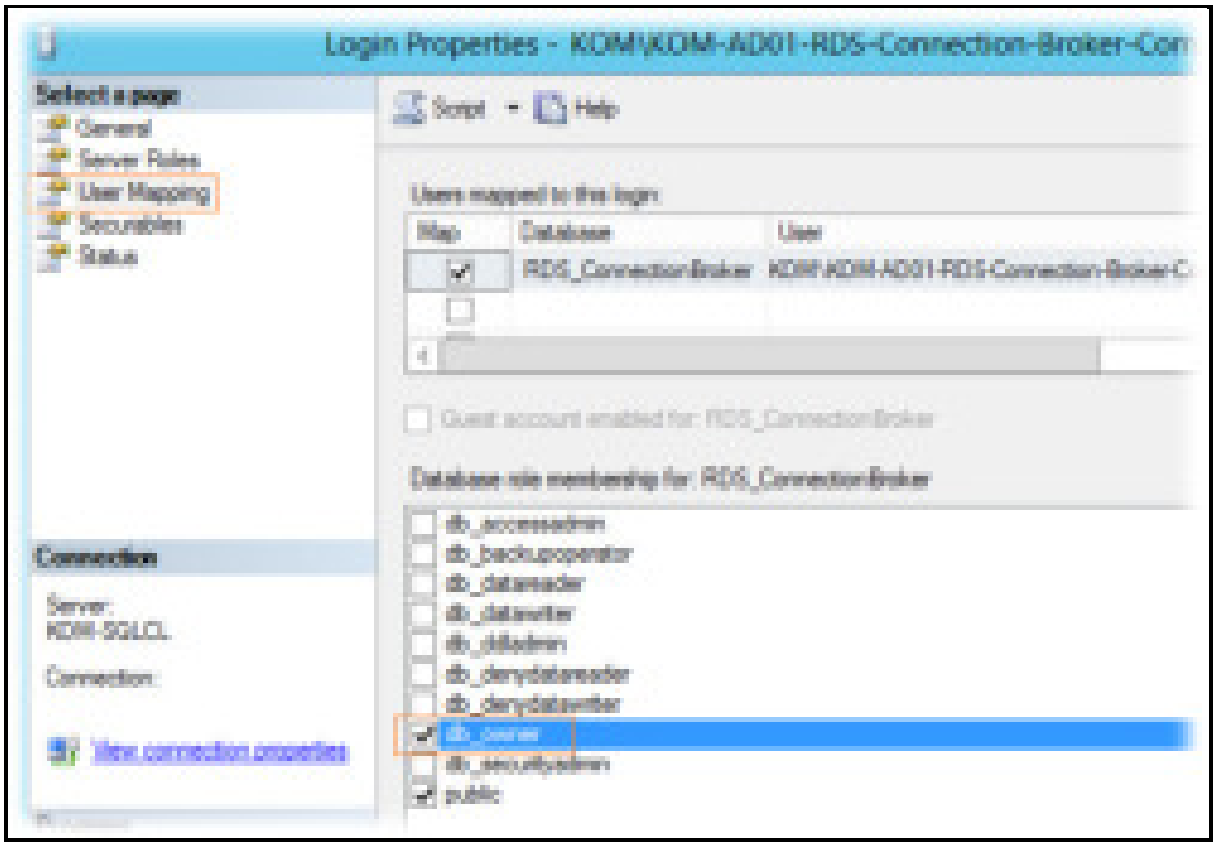



В ходе этого процесса на SQL-сервере будет создана БД высоко-доступного экземпляра RDCB.

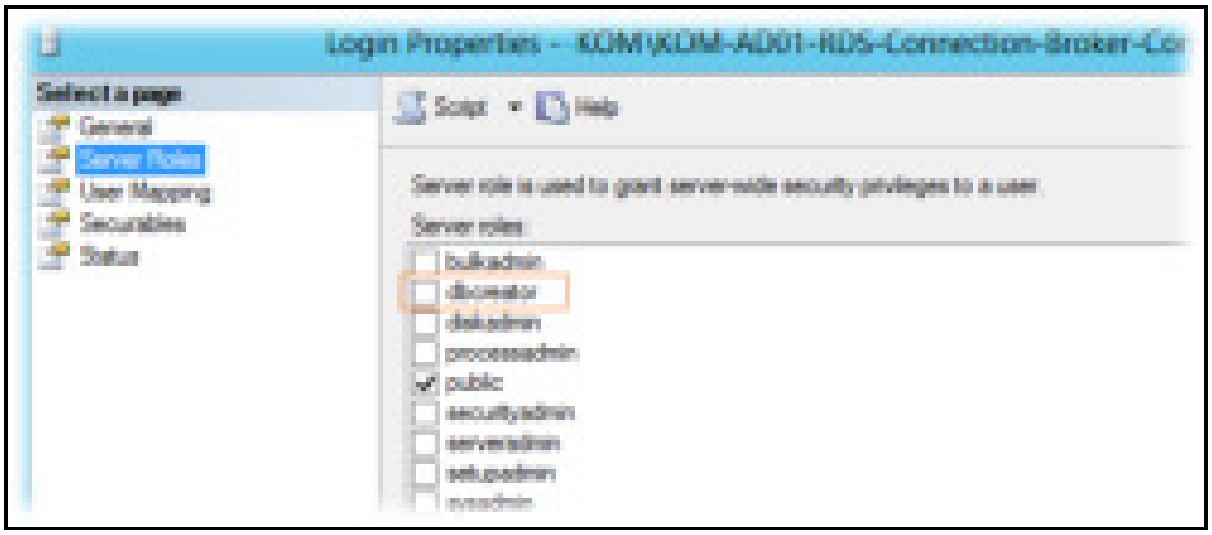
***

Переключимся на наш **SQL Server** с только что созданной БД и выполним пару настроек…

В обязательном порядке для SQL-логина, который мы создавали на подготовительном этапе (**KOM-AD01-RDS-Connection-Broker-Computers**), нужно дать роль **db_owner** для созданной базы **RDS_ConnectionBroker**




Помимо этого, для данного SQL-логина можно отключить добавленную ранее серверную роль **dbcreator**, так как БД уже создана и больше данная привилегия этому SQL-логину не потребуется.



Если резервное копирование баз данных SQL Server выполняется такими инструментами как например **SC 2012 DPM**, то при желании мы можем поменять модель восстановления созданной БД (**Recovery Model**) с **Full** на **Simple**.

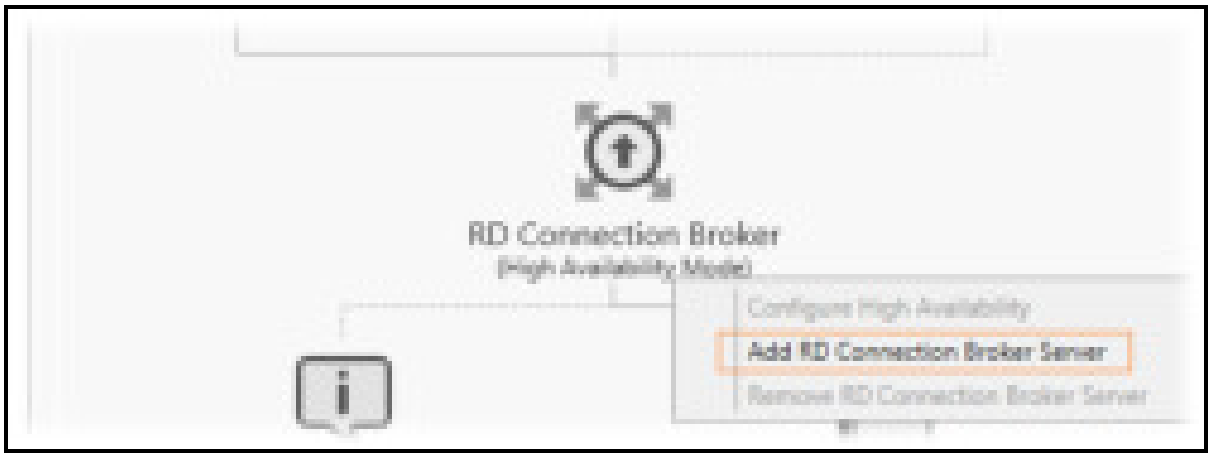
***

Вернёмся на наш сервер **KOM-AD01-RDS21** и обратим внимание на то, что в консоли **Server Manager** в схеме инфраструктуры RDS статус роли RDCB поменялся на **High Availability Mode**

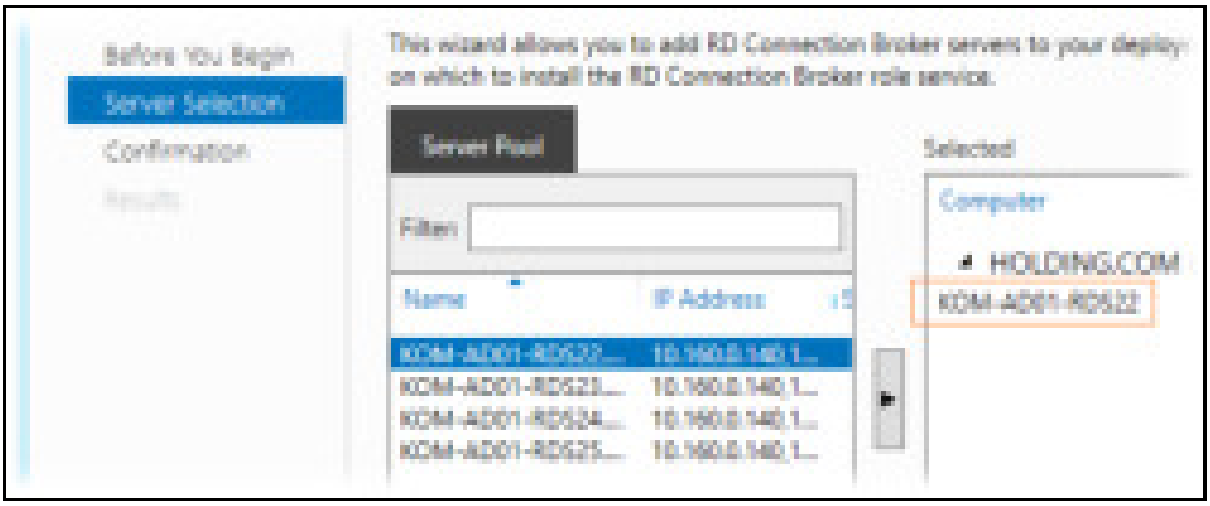

Теперь для того чтобы задуманная нами связка NLB + RDCB работала так как нужно, нам необходимо до-установить роль **RD Connection Broker** на оставшиеся четыре сервера.

**Добавляем сервера в высоко-доступный RD Connection Broker**

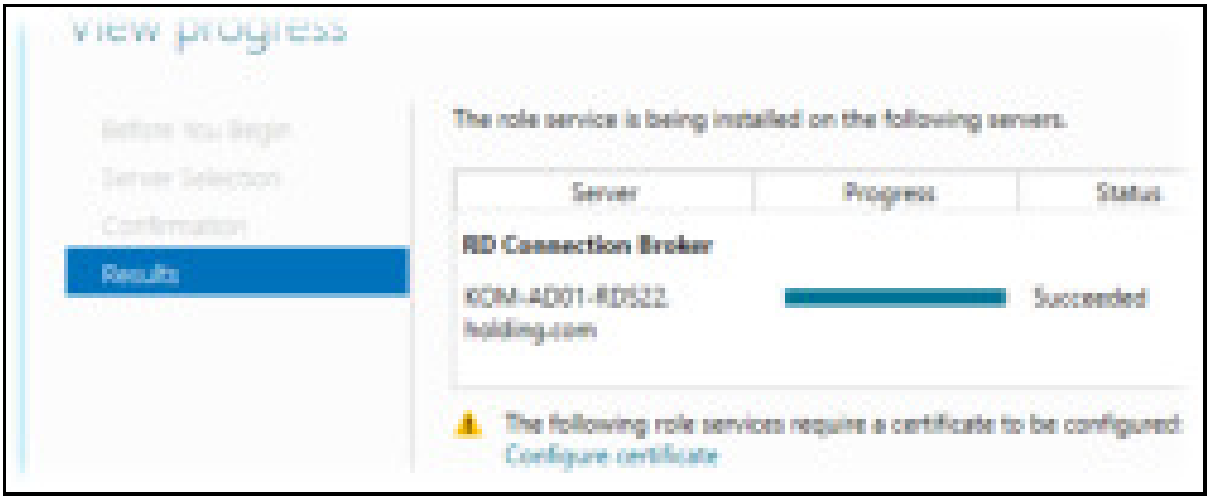
Добавление серверов к высоко-доступной конфигурации RDCB делается через то же самое контекстное меню в схеме развертывания RDS на странице **Overview**.




В открывшемся мастере добавляем следующий сервер (мастер также не даст добавить более одного сервера)




После успешного добавления роли на выбранный сервер и подключение этого сервера к БД HA RDCB мы получим предупреждение о необходимости настройки сертификатов, которое пока можем проигнорировать, так как займёмся сертификатами позже.

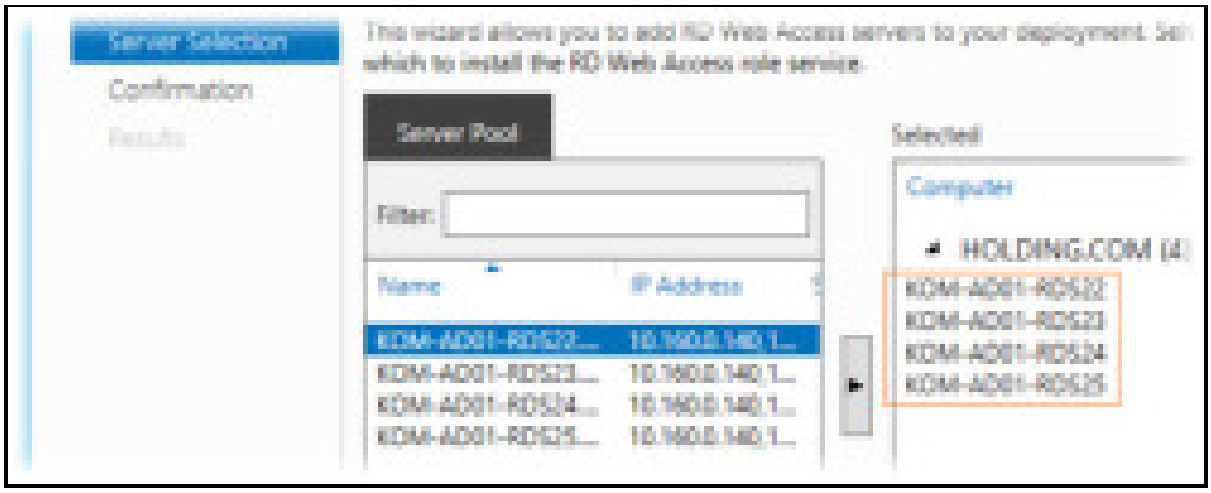


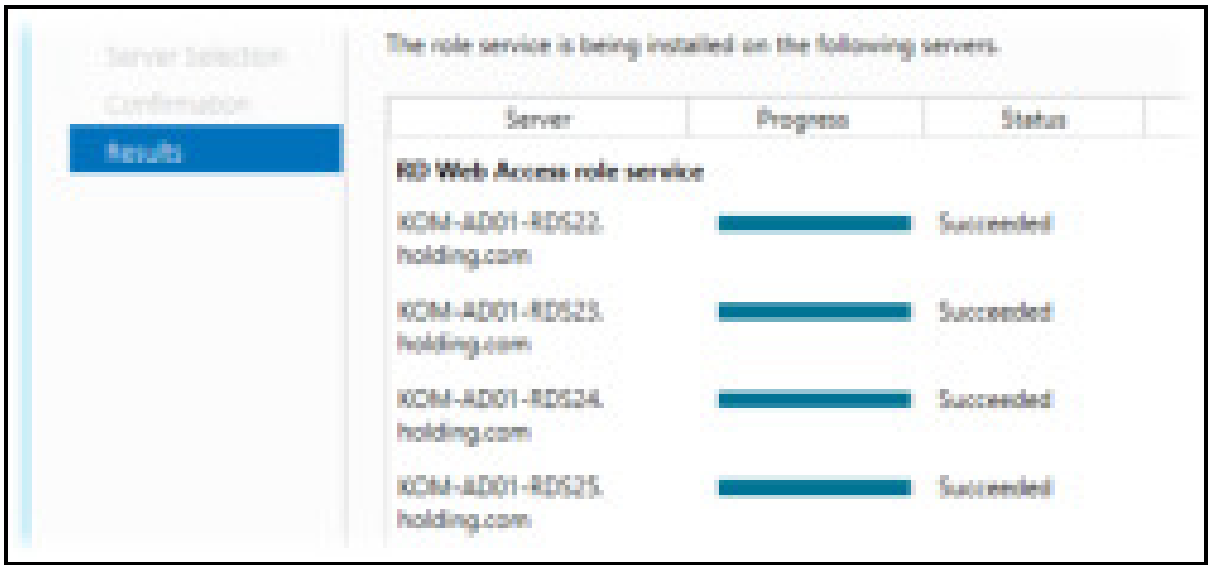
Аналогичным образом мы по одному серверу должны добавить роль HA RDCB на все оставшиеся сервера, те. KOM-AD01-RDS23, KOM-AD01-RDS24 и KOM-AD01-RDS25.

**Добавляем на сервера роль RD Web Access**

Так как мы хотим иметь отказоустойчивую конфигурацию роли **RD Web Access**, нам нужно до-установить эту роль на оставшиеся четыре сервера (на KOM-AD01-RDS21 эта роль уже установлена). Делаем это в уже знакомом нам месте через мастер добавления ролей

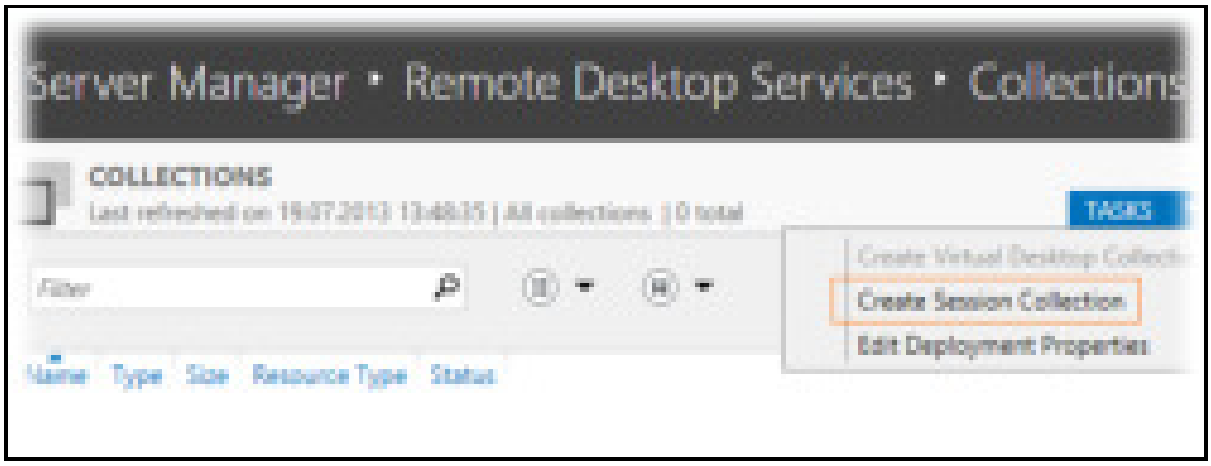

Здесь уже мы сможем выбрать сразу все серверы и выполнить установку роли RDWA оптом…



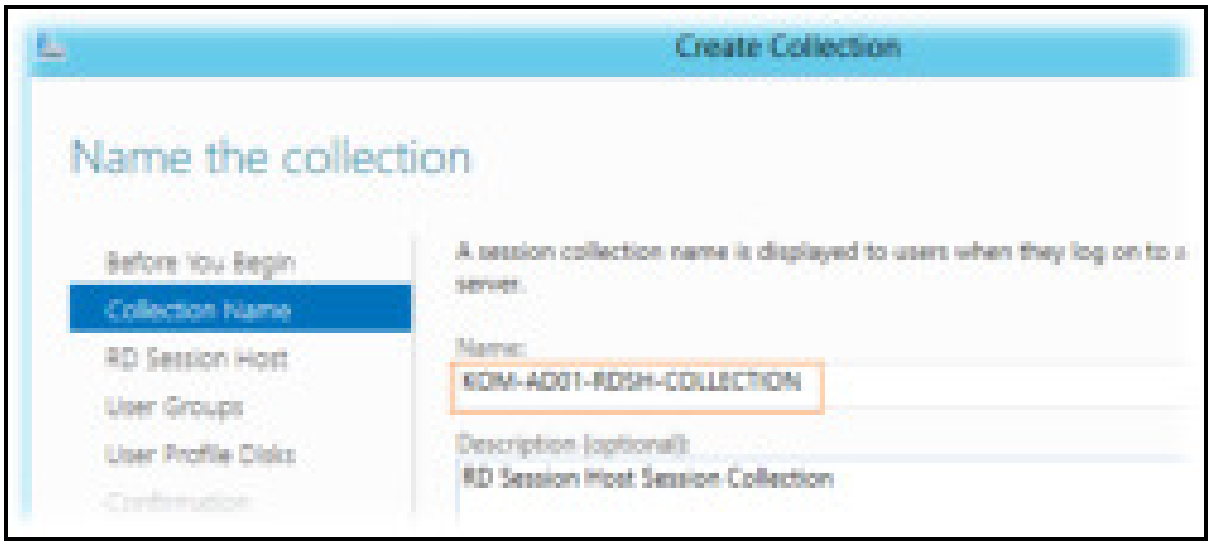



**Создаём коллекцию сеансов – Session Collection**

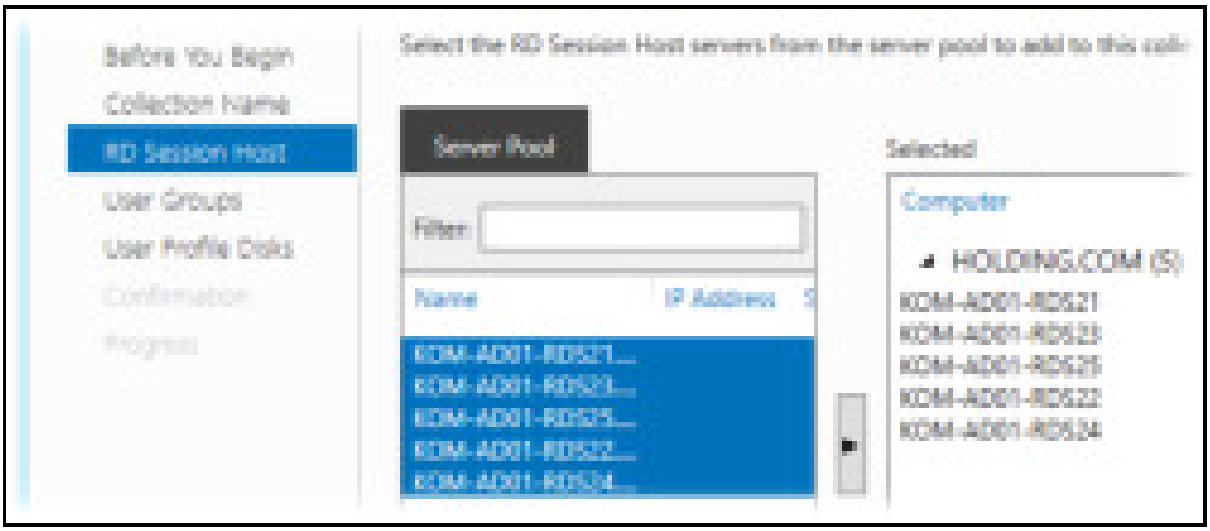
Все наши сервера с ролью RD Session Host мы должны объединить в логическую единицу – коллекцию сеансов (**Session Collection**). Делаем это в оснастке **Server Manager** на вкладке **Remote Desktop Services > Collections** выбрав задачу **Create Session Collection** в таблице перечисления коллекций.



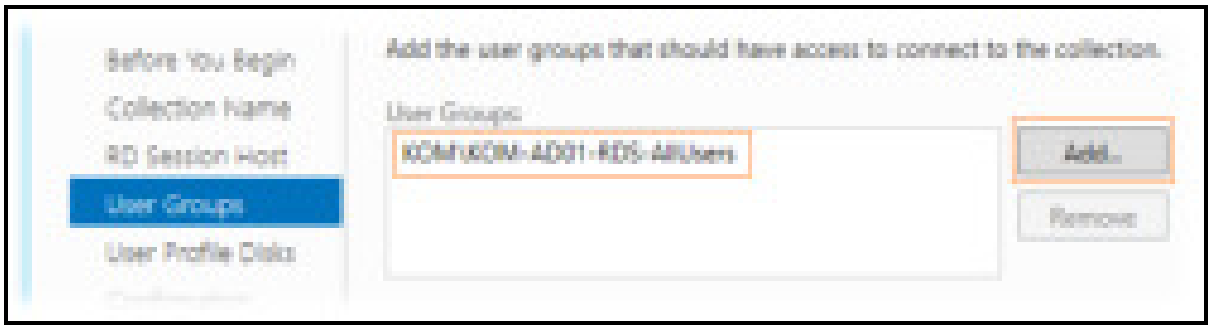

В открывшемся мастере создания коллекции зададим имя коллекции и при желании описание




Затем выбираем все сервера, которые хотим сделать членами коллекции…



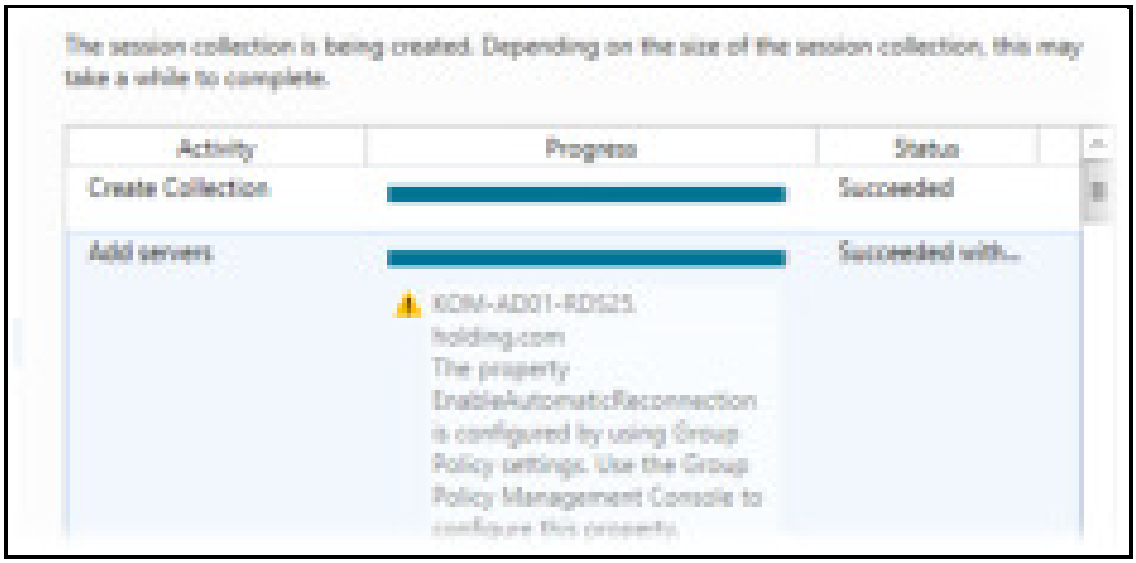

Далее мы должны определить доменную группу безопасности которой будет разрешено подключаться к коллекции сеансов. Убираем выбранную по умолчанию группу доступа **Domain Users** и добавляем специально созданную группу доступа, в нашем случае **KOM-AD01-RDS-AllUsers**, ограничив тем самым круг пользователей которые смогут подключаться к серверам коллекции.



На следующем шаге определяемся с тем, хотим ли мы использовать новую технологию **Windows Server 2012 – User profile disks (UPD)**, которая, как я понял, предлагается в качестве альтернативы механизму перемещаемых профилей - **Roaming User Profiles.** Новая технология подразумевает централизованное хранение файлов пользователя в отдельных **VHD** дисках, которые располагаются где-то на выделенном файловом ресурсе. В силу того, что на данный момент нет уверенности в стабильности работы данного механизма из-за полученной информации в обсуждении Windows Server 2012 RDS - [User Profile Disk] VS [Roaming Profiles + Folder Redirection] я решил пока не использовать данный функционал и поэтому он не будет рассмотрен в данной заметке.


А пока не будут разрешены имеющиеся на данный момент проблемы с **UPD** будем использовать связку технологий **Roaming User Profiles** и **Folder Redirection**, настройка которых рассматривалась ранее в заметке Remote Desktop Services – Используем перенаправление профилей пользователей и перемещаемые папки

В результате работы мастера все наши сервера успешно добавляются в коллекцию с предупреждениями о том, что желательна настройка групповых политик для задания параметров RDP на этих серверах…



**Настраиваем цифровые сертификаты**

При попытке подключения к ферме **RD Connection Broker** по **FQDN**-имени кластера **NLB** клиенты могут получать предупреждение безопасности, говорящее о том, что нет доверия сертификату того сервера сеансов, на который он был перенаправлен. Если открыть свойства этого сертификата, мы увидим, что сертификат создаваемый на сервере RDSH по умолчанию является самоподписанным. Чтобы избежать таких предупреждений нам нужно создать для развёртывания RDS сертификат подписанный доверенным Центром сертификации (ЦС), например локальным изолированным или доменным ЦС. Этот сертификат после создания мы развернём на всех серверах фермы.

При создании запроса на сертификат нужно использовать как минимум 2 политики применения:

**Client Authentication (1.3.6.1.5.5.7.3.2)**
**Server Authentication (1.3.6.1.5.5.7.3.1)**

Хотя в нашей ситуации альтернативные имена в сертификате **Subject Alternative Name (SAN)** иметь вовсе необязательно, я всё-таки рассмотрю вариант создания именно такого сертификата, то есть чтобы помимо имени NLB кластера в сертификате содержались имена отдельных серверов.

Для того чтобы наш локальный ЦС мог корректно обрабатывать запросы сертификатов с SAN он должен быть настроен для этого. О том как это сделать можно прочитать в заметке Remote Desktop Services – Строим отказоустойчивую ферму RD Connection Broker

Подготовим файл параметров для создания запроса на получение нужного нам сертификата. Это обычный текстовый файл, назовём его например **RequestPolicy.inf**

Содержимое этого файла в нашем примере выглядит так:

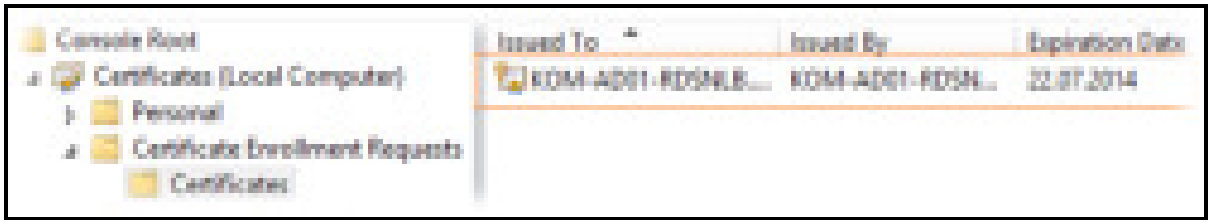
```
[Version]
Signature="$Windows NT$"

[NewRequest]
Subject = "CN=KOM-AD01-RDSNLB.holding.com" ;
Exportable = TRUE; Private key is exportable
KeyLength = 2048
KeySpec = 1; Key Exchange – Required for encryption
KeyUsage = 0xA0; Digital Signature, Key Encipherment
MachineKeySet = TRUE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
```

```
RequestType = PKCS10

[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1 ; Server Authentication
OID=1.3.6.1.5.5.7.3.2 ; Client Authentication

[RequestAttributes]
SAN  = "dns=KOM-AD01-RDSNLB.holding.com&"
_continue_ = "dns=KOM-AD01-RDS21.holding.com&"
_continue_ = "dns=KOM-AD01-RDS22.holding.com&"
_continue_ = "dns=KOM-AD01-RDS23.holding.com&"
_continue_ = "dns=KOM-AD01-RDS24.holding.com&"
_continue_ = "dns=KOM-AD01-RDS25.holding.com&"
_continue_ = "dns=KOM-AD01-RDSNLB&"
_continue_ = "dns=KOM-AD01-RDS21&"
_continue_ = "dns=KOM-AD01-RDS22&"
_continue_ = "dns=KOM-AD01-RDS23&"
_continue_ = "dns=KOM-AD01-RDS24&"
_continue_ = "dns=KOM-AD01-RDS25&"
```

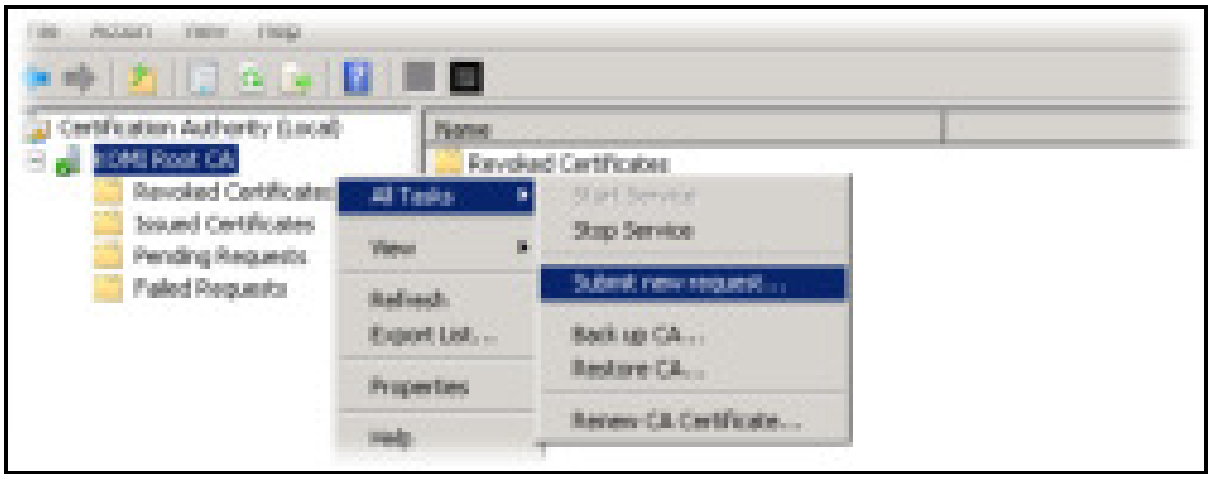
С помощью встроенной в ОС утилиты **CertReq.exe** создадим файл запроса на основе файла параметров:

**cd /d C:\Temp**
**CertReq –New RequestPolicy.inf RequestFile.req**

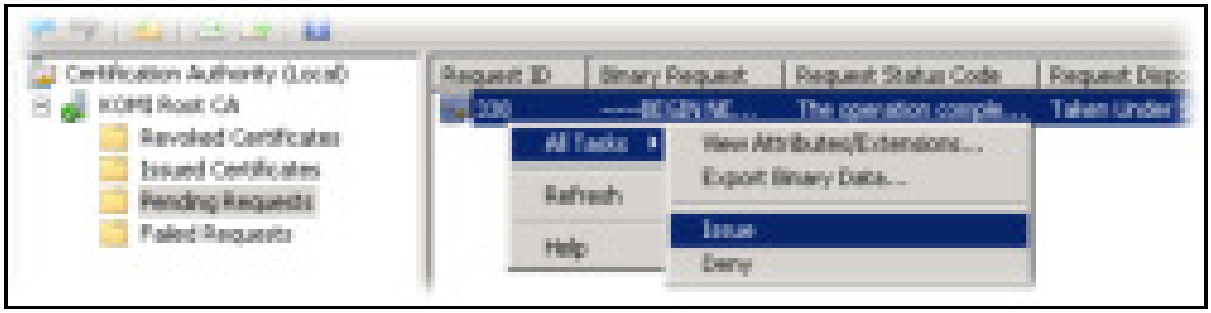
Выполнять эту команду надо локально на сервере RDS. В нашем случае команда выполняется на сервере **KOM-AD01-RDS21**. После выполнения команды откроем консоль управления локальными сертификатами (**mmc.exe** > **Add/Remove snap-in** > **Certificates** > **Add** > **Computer account**) для хранилища **Local Computer** и убедимся в появлении ожидающего запроса в разделе **Certificate Enrollment Request**



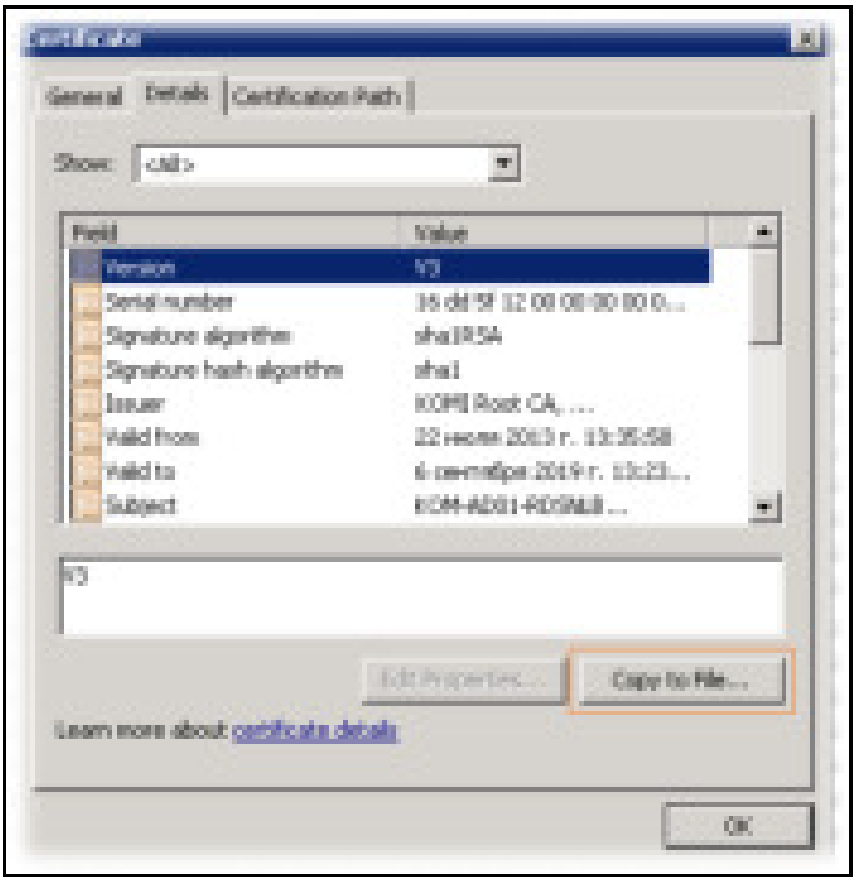

Полученный файл запроса **RequestFile.req** добавляем в локальный центр сертификации через консоль управления **Certification Authority** (**certsrv.msc**) (**All Tasks** > **Submit new request**)



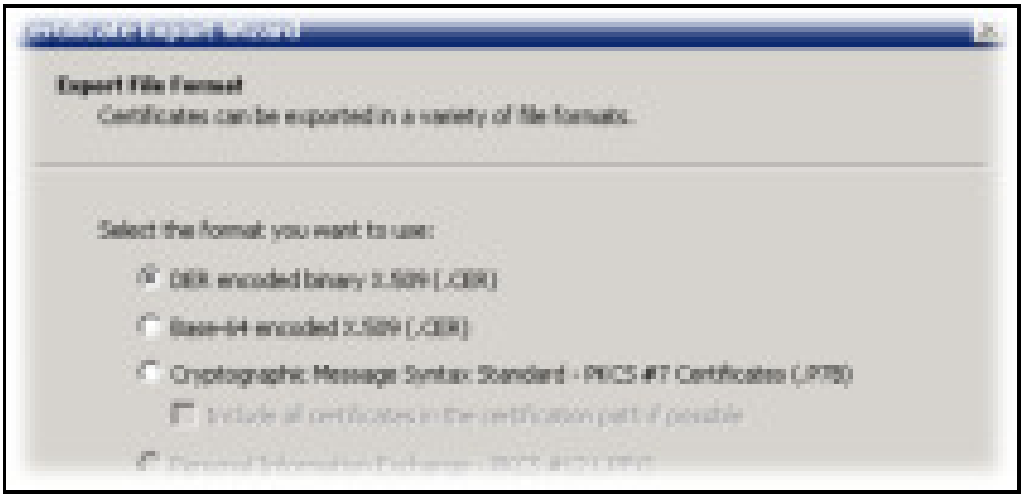

Затем в этой же консоли в разделе **Pending Requests** проверяем наш добавленный запрос и разрешаем выдачу сертификата по нему (Выбираем запрос > **All Tasks** > **Issue** )

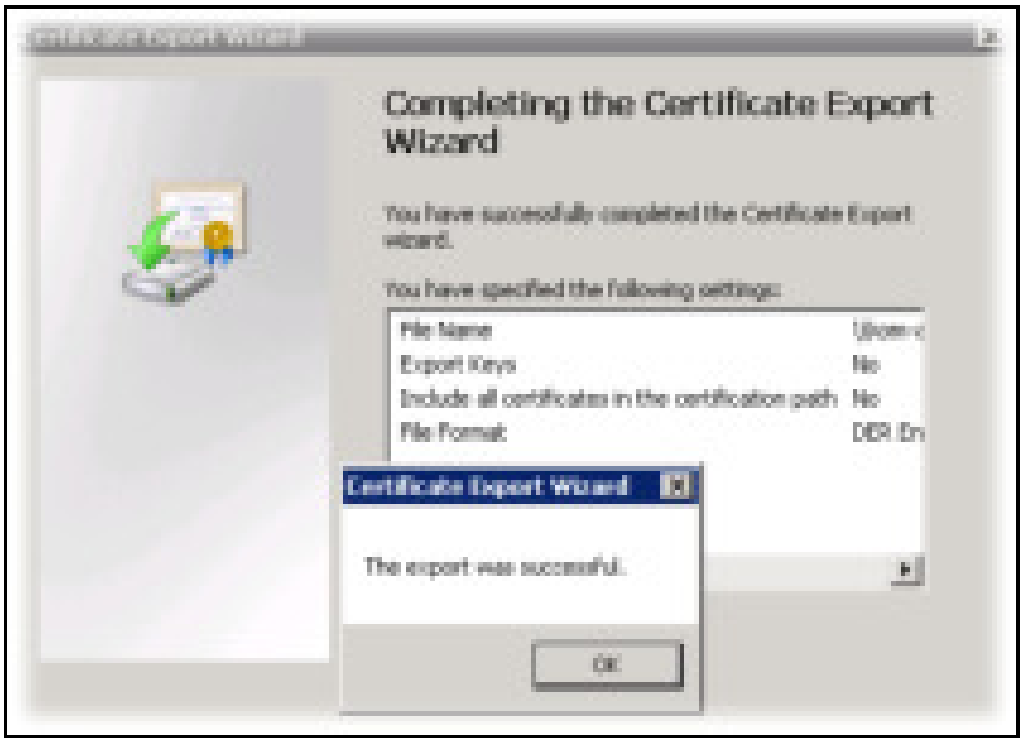



Переходим в раздел выданных сертификатов - **Issued Certificates**, находим сертификат, открываем его свойства и на закладке **Details** вызываем мастер экспорта сертификата (**Copy to File**)

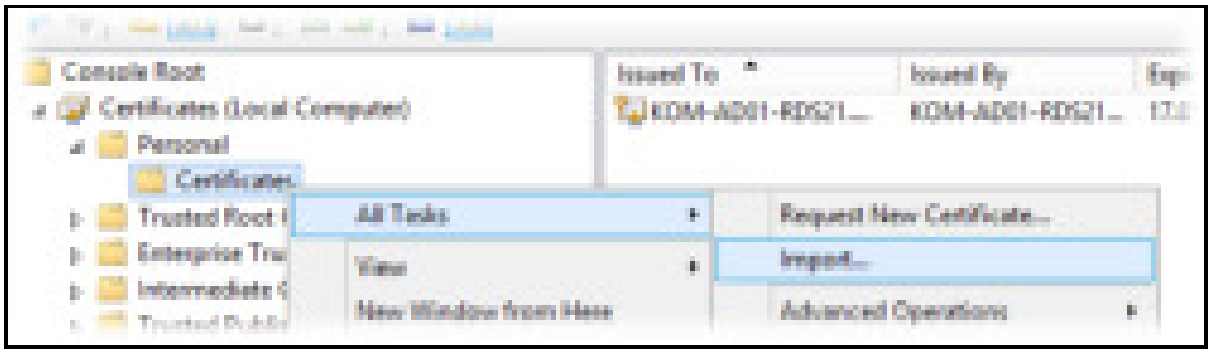



В открывшемся мастере выбираем формат экспорта **DER X.509** и сохраняем файл например с именем **NLBCert.cer**

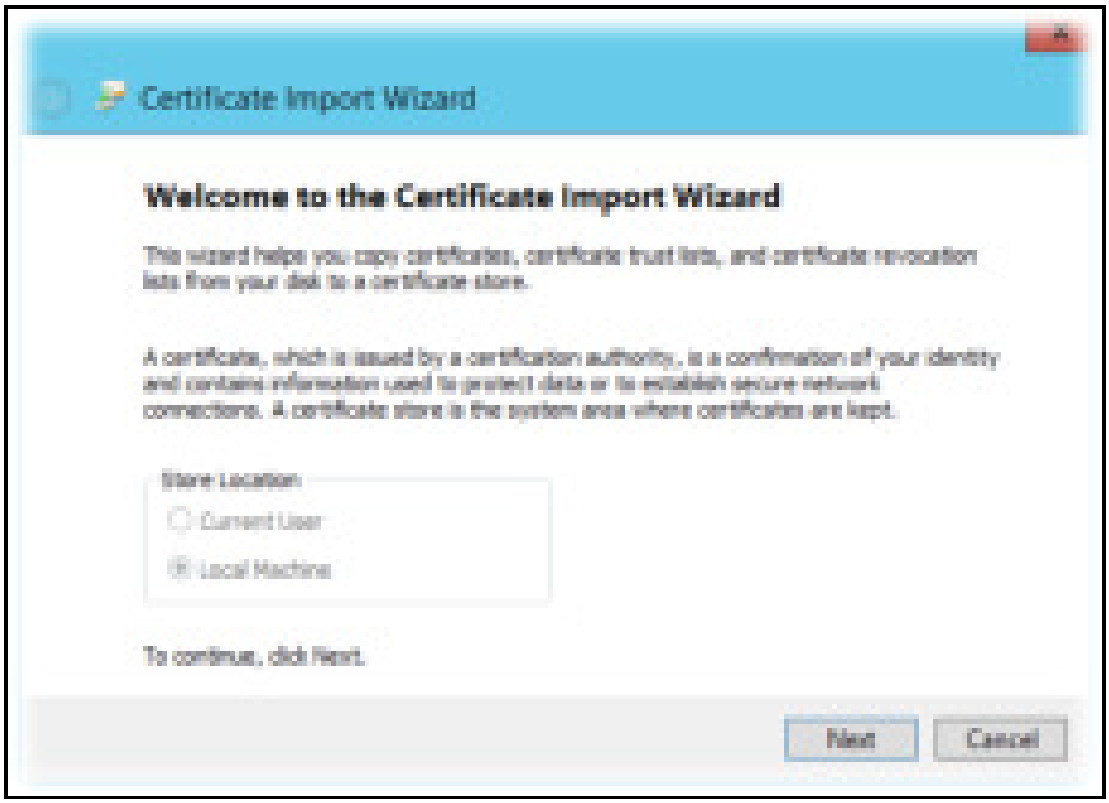




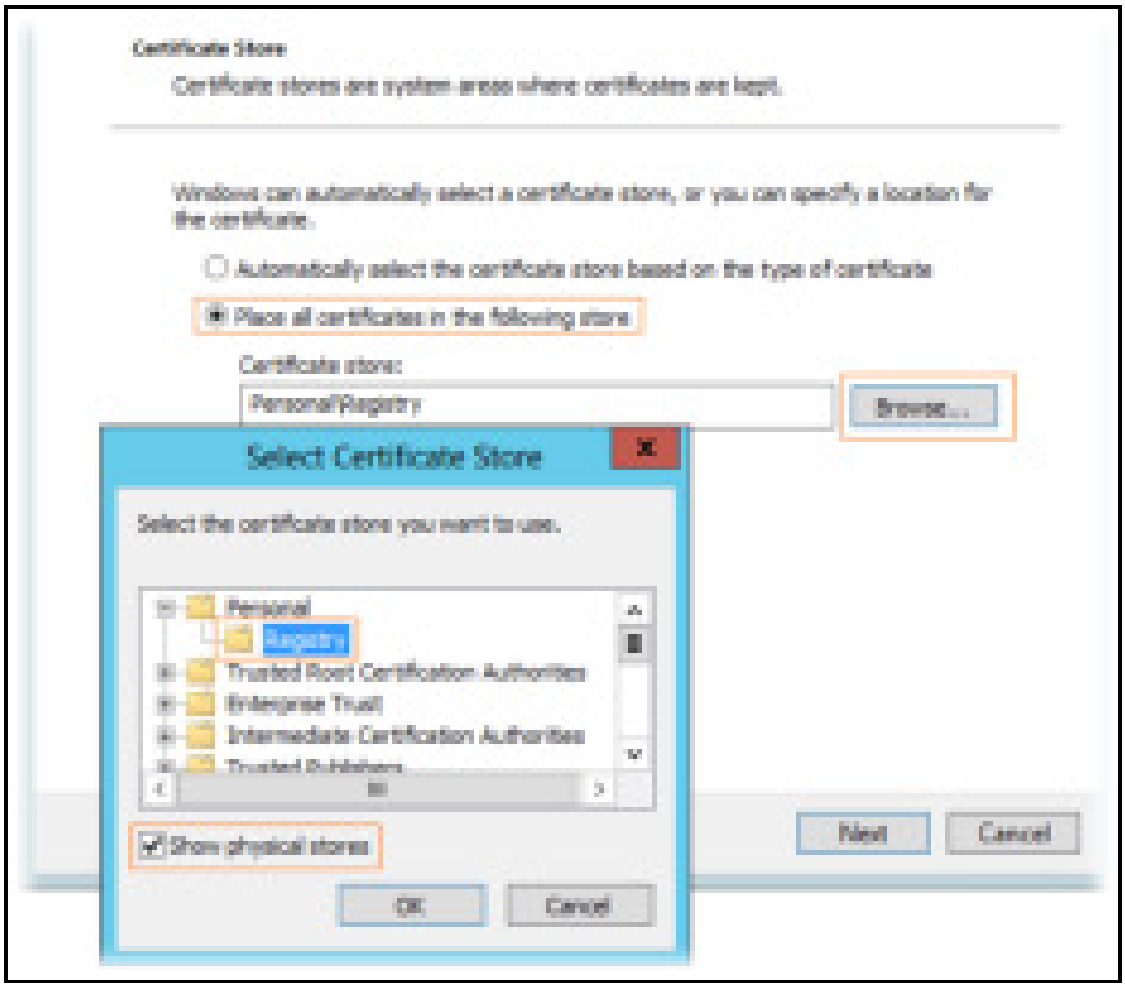

Скопируем полученный файл **NLBCert.cer** на сервер RDS, где мы создавали запрос на сертификат (**KOM-AD01-RDS21**) и вернёмся в консоль управления локальными сертификатами этого сервера. Выберем хранилище **Personal** > **Certificates** и вызовем мастер импорта сертификатов (**All Tasks** > **Import**)



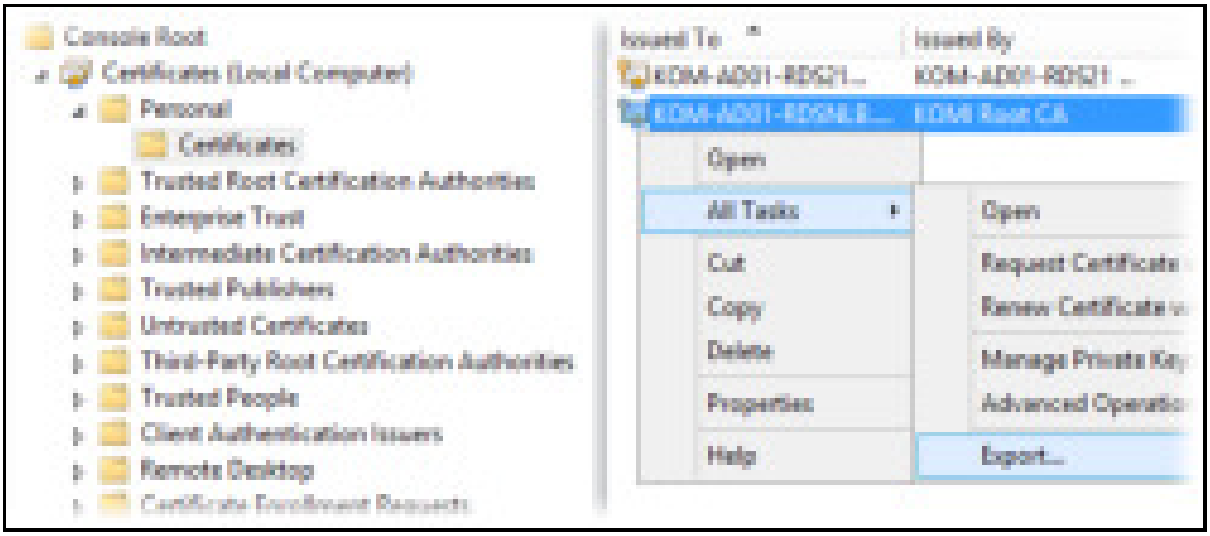

В мастере импорта автоматически будет выбрано хранилище **Local Machine**



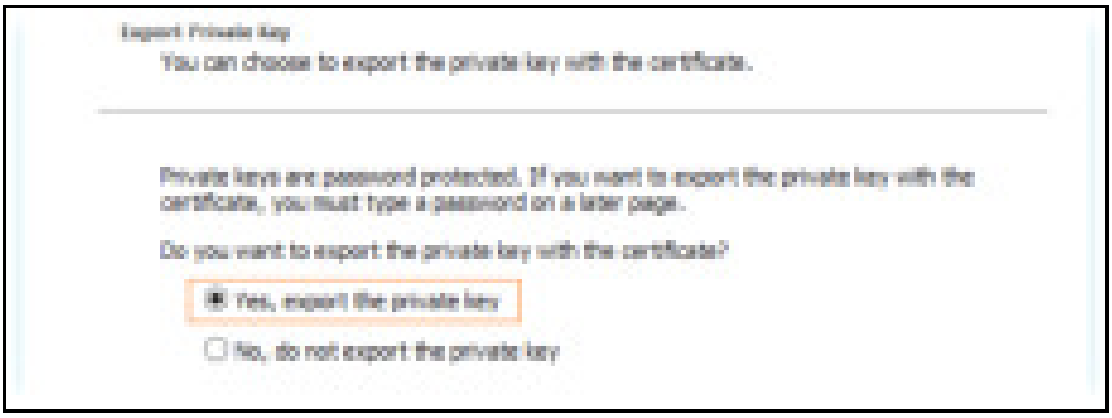

Далее выберем импортируемый файл сертификата **NLBCert.cer** и укажем раздел хранилища **Personal\Registry**. Чтобы этот раздел был доступен для выбора, нужно включить опцию **Show physical stores**.



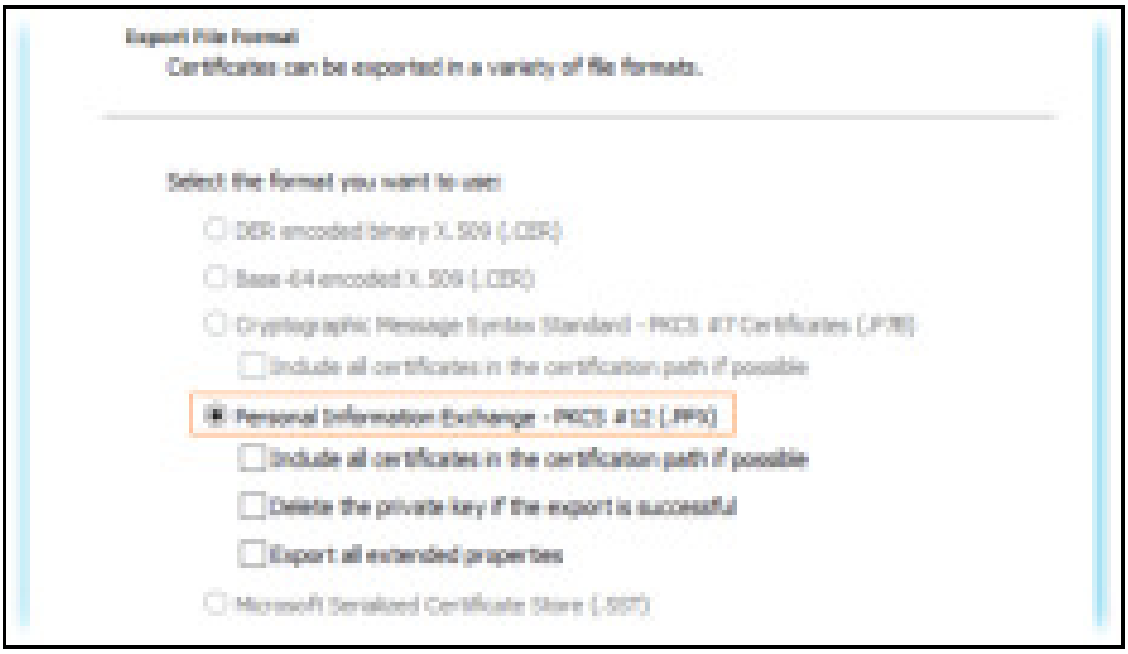

После того как импорт сертификата выполнен, убеждаемся что он появился в соответствующем хранилище и с ним связан его закрытый ключ (присутствует значок ключика на иконке). При этом в разделе **Certificate Enrollment Request** информация о запросе должна исчезнуть.



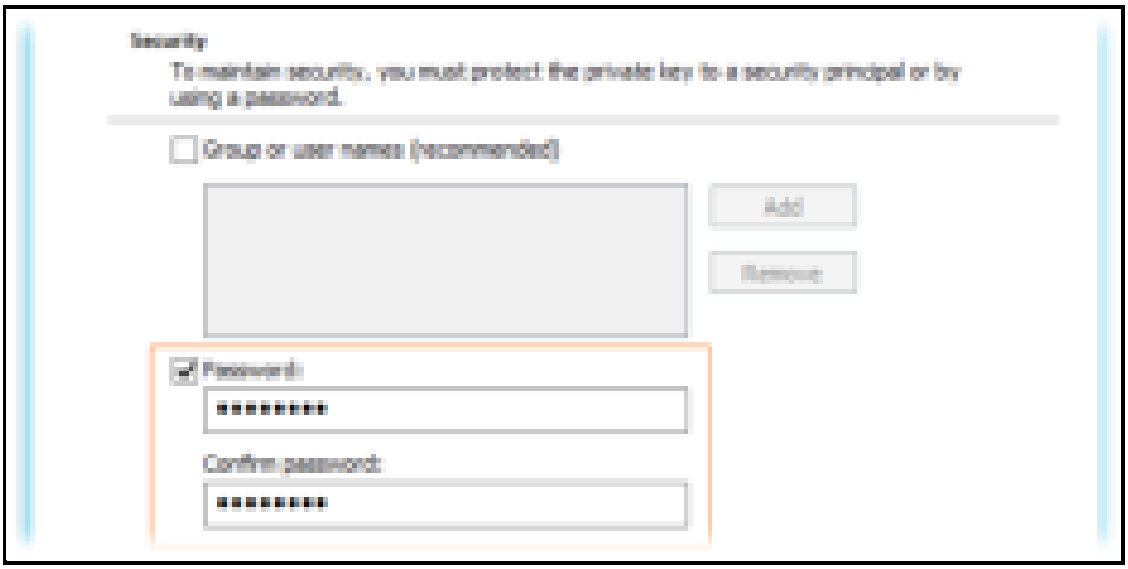
Далее выбираем установленный сертификат и вызываем мастер экспорта (**All Task > Export**). В мастере экспорта выбираем опцию экспорта закрытого ключа при экспорте сертификата – **Yes, export the private key**




В качестве формата экспорта используем единственно возможный и нужный нам формат **.PFX**

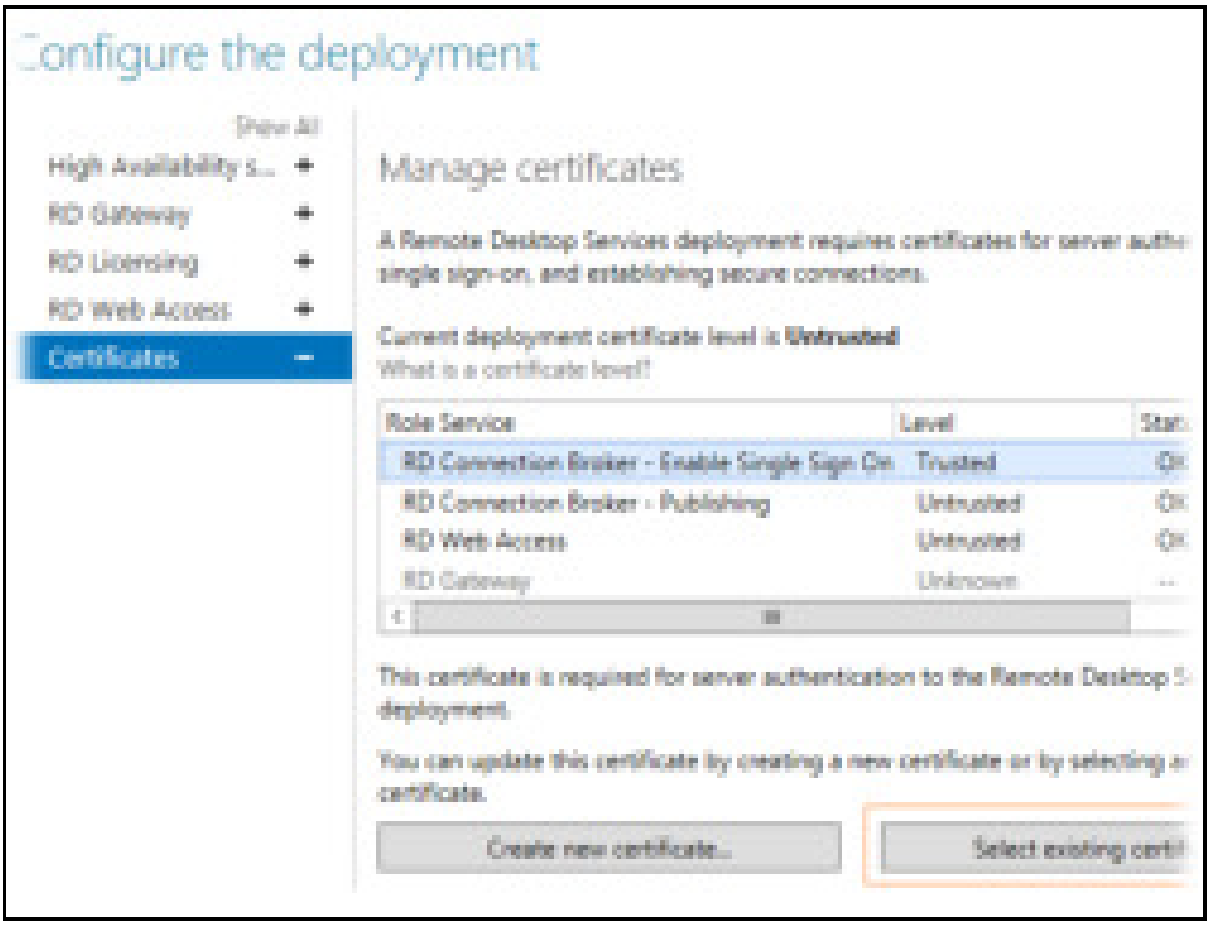



Далее задаем пароль (он потребуется нам в дальнейшем для назначения этого сертификата в развёртывании RDS)

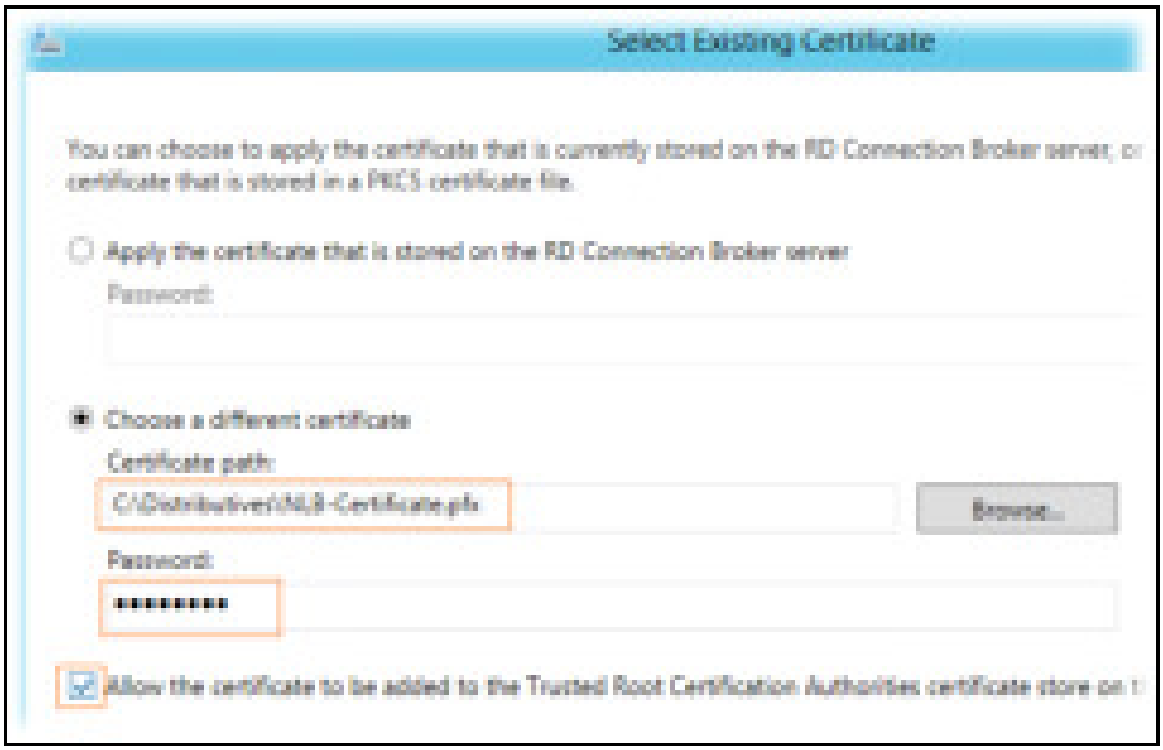



После того как сертификат экспортирован, переходим в консоль **Server Manager\Remote Desktop Services\Overview** и на схеме развёртывания в списке задач выбираем пункт редактирования развёртывания (**TASKS** > **Edit Deployment Properties**)

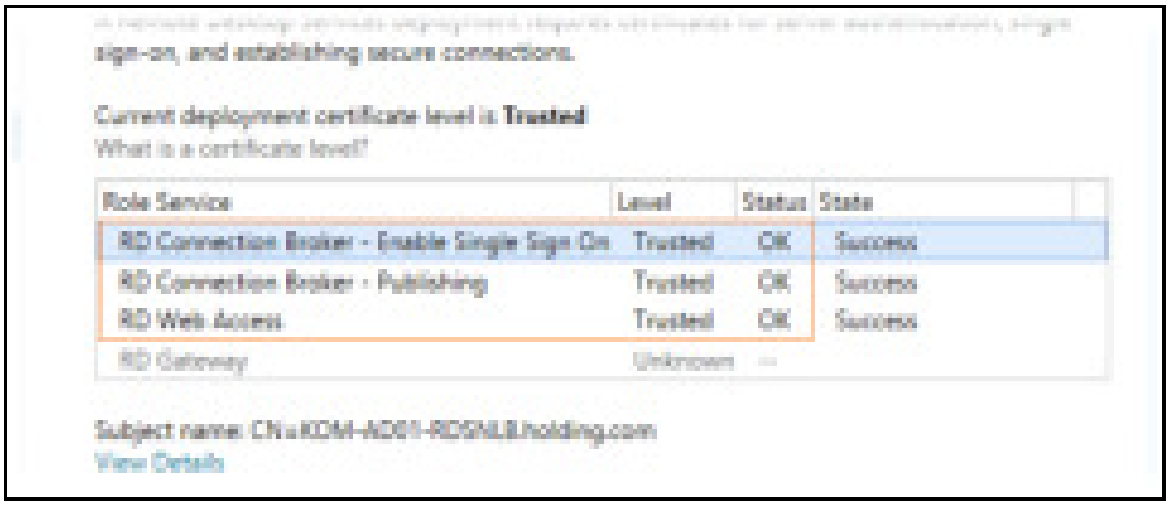

На вкладке **Certificates** используем кнопку **Select existing cerificates** для того чтобы назначить сделанный нами сертификат для той или иной роли RDS…




В окне выбора сертификата определяем, что мы хотим использовать файл **PFX** полученный нами ранее и задаём пароль с которым этот сертификат был экспортирован. Хотя опция **Allow the certificate to be added to the Trusted Root CA** нам по сути не нужна, так как созданный нами сертификат сделан в ЦС, которому предположительно все наши сервера уже доверяют, её всё таки придётся отметить, так как если она не отмечена, кнопка **OK** недоступна…



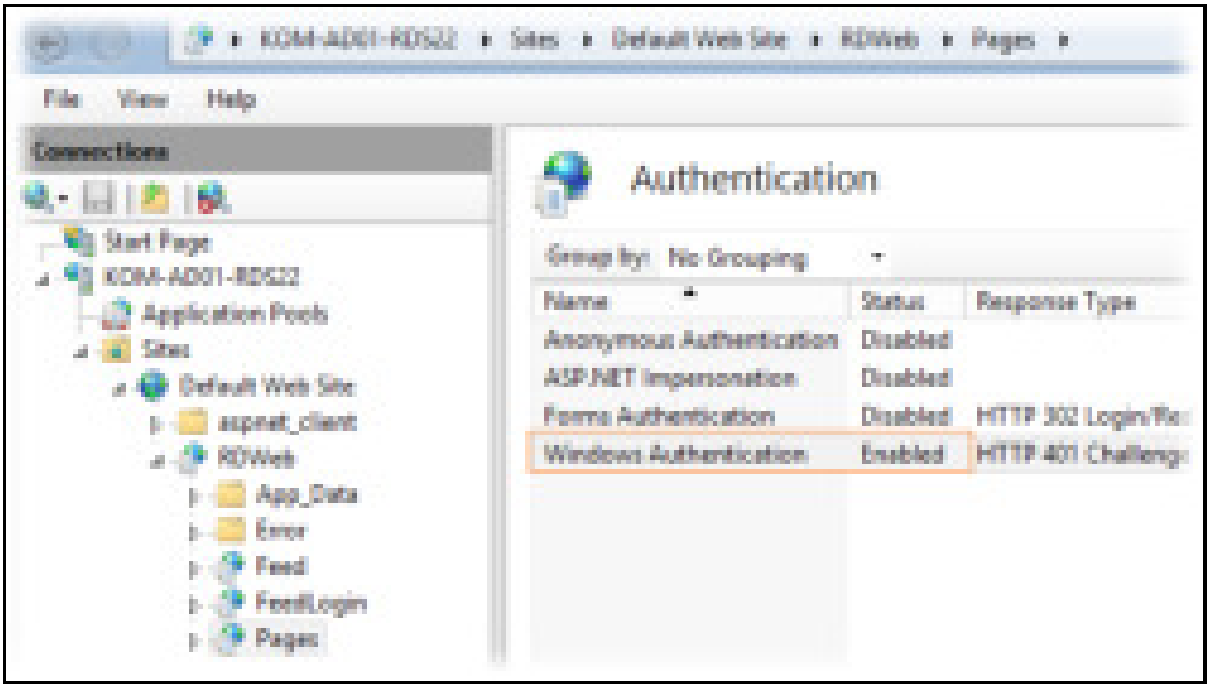

После закрытия этого окна по **ОК**, мы увидим что в таблице статус сертификата изменился на **Ready to apply**..Нажмём кнопку **Apply** и через несколько секунд наш сертификат будет назначен роли соответствующей RDS. Описанным методом мы выполним привязку сертификатов ко всем развёрнутым у нас ролям и в конечном итоге получим примерно следующий вид:




Назначенные нами сертификаты будут автоматически установлены на все сервера, которые участвуют в нашем RDS развёртывании.

**Настраиваем веб-узлы RD Web Access**

По умолчанию при обращении в стартовой веб-странице RDWA от пользователя в явном виде требуется ввод учетной записи и пароля. Если мы используем RDWA для доменных пользователей внутри локальной сети, то для удобства нам нужно будет задействовать механизм прозрачного входа **Single sign-on** (**SSO**) при обращении к веб-узлу RDWA. Для этого на каждом сервере с установленной ролью RDWA в оснастке **IIS Manager** откроем свойства веб-приложения **RDWeb** > **Pages** выберем в разделе настроек пункт **Authentication**…**выключим** анонимную аутентификацию (**Anonymous Authentication**), аутентификацию на основе формы (**Forms Authentication**) и **включим Windows Authentication**:




***

После входа на веб-страницу RDWA можно обнаружить уже знакомый нам по предыдущей версии опцию **I am using a private computer that complies with my organization's security policy** (в русском варианте - **Я использую личный компьютер, соответствующий политике безопасности моей организации**).


Ранее, в заметке RDS Web Access – Опция "Я использую личный компьютер…", я писал о том, как выставить эту опцию во включенное состояние по умолчанию, чтобы избежать повторного запроса аутентификации

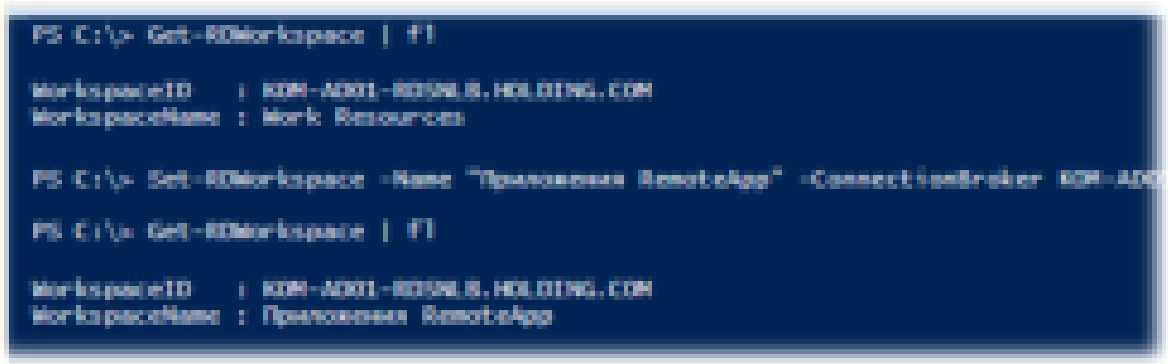
при подключении к опубликованным приложениям **RemoteApp** в **Windows Server 2008 R2**. Это рецепт работает и для **Windows Server 2012**.

***

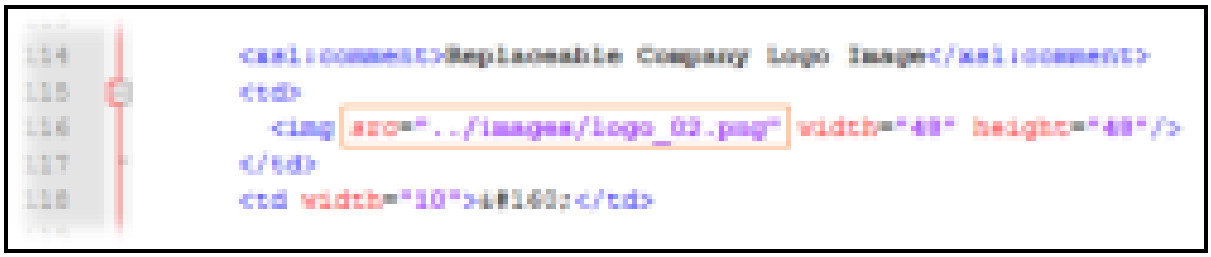
Верхняя часть страниц RDWA по умолчанию оформлена в виде заголовочной надписи **Work Resources** и изображения размером 48*48 пикселей.


Для того чтобы заменить заголовочную надпись можно использовать командлет **PowerShell** (один раз для всей коллекции серверов):

Set-RDWorkspace -Name "Приложения RemoteApp" -ConnectionBroker KOM-AD01-RDS21.holding.com




Для того чтобы заменить имеющееся изображение на другое, например с корпоративной символикой, можно внести корректировки в файл %windir%\Web\RDWeb\Pages**Site.xsl** – найти секцию с комментарием "Replaceable Company Logo Image"…



… и заменить ссылку на файл изображения, указав собственный файл размещённый в соответствующем подкаталоге %windir%\Web\RDWeb\Pages\images

В результате мы получим примерно следующий вид верхней части страниц RDWA:

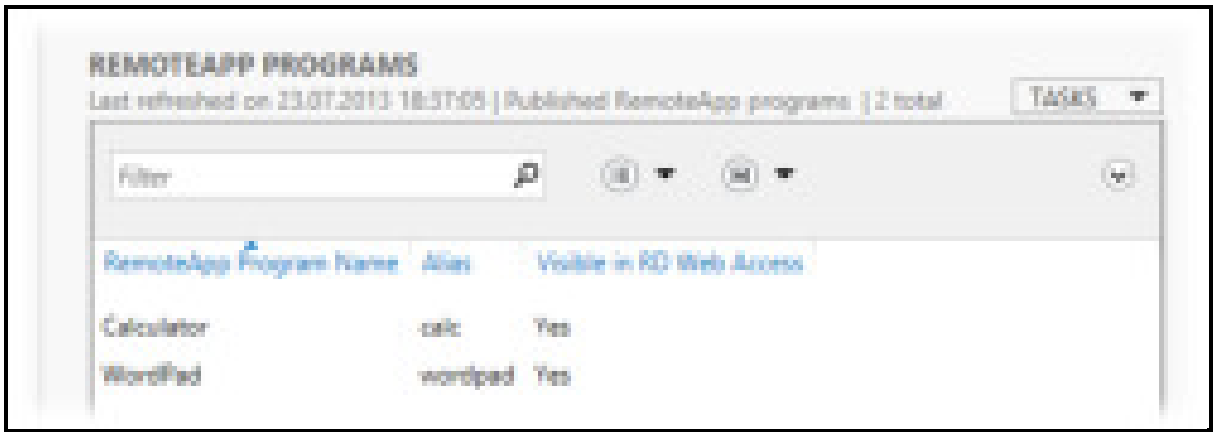

**Настраиваем Roaming User Profiles и Folder Redirection**

Так как пользователи нашей фермы RDS от сеанса к сеансу могут попадать на разные сервера, нам необходимо обеспечить идентичность пользовательской среды на всех этих серверах. Для этого мы будем использовать механизмы перемещаемых профилей (**Roaming User Profiles** ) и перенаправления папок (**Folder Redirection**). Для настройки этих механизмов настраиваем групповую политику применяемую к серверам нашей фермы RDS. Здесь мы не будем рассматривать эту процедуру, так как она уже была ранее описана мной в заметке Remote Desktop Services – Используем перенаправление профилей пользователей и перемещаемые папки

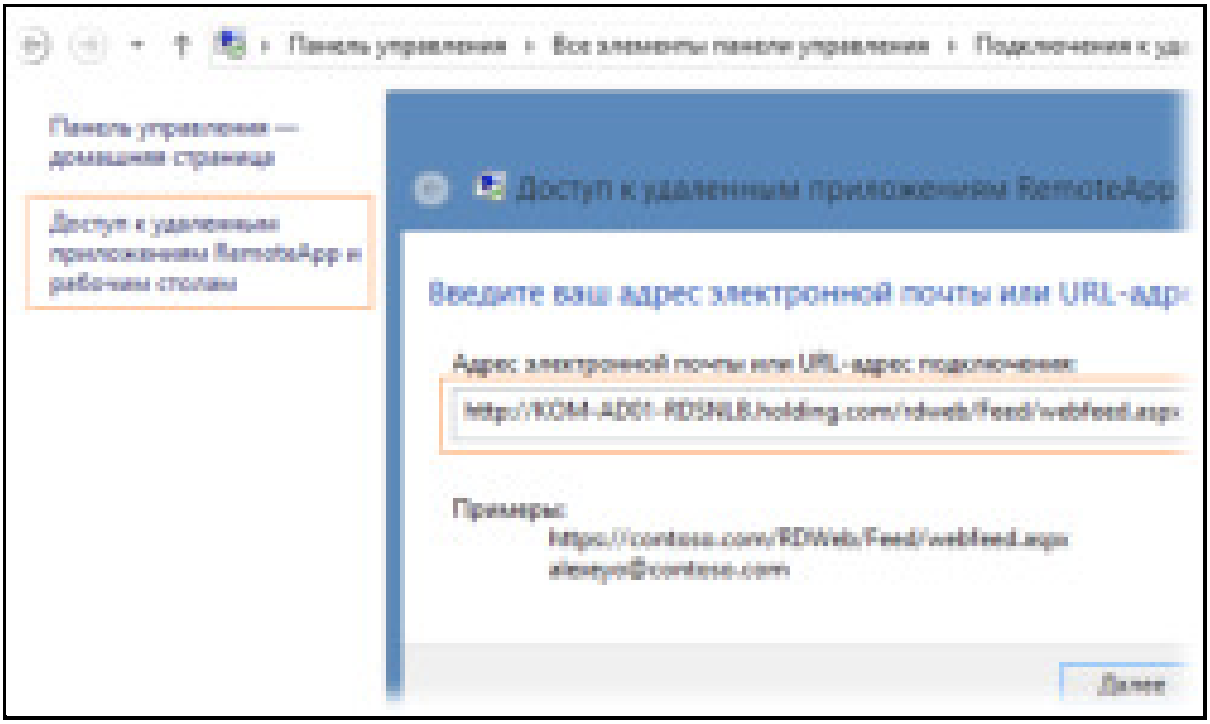
**Публикуем приложения RemoteApp**

Чтобы опубликовать в ферме RDS приложения **RemoteApp** переходим в консоль **Server Manager** в раздел **Remote Desktop Services** > **Collections** > выбираем нашу коллекцию **KOM-AD01-RDSH-COLL** и публикуем необходимые приложения в окне **REMOTEAPP PROGRAMS**. В меню задач выбираем пункт публикации **TASKS** > **Publish RemoteApp Programs**


Для примера опубликуем два простых приложения **Calculator** и **WordPad**



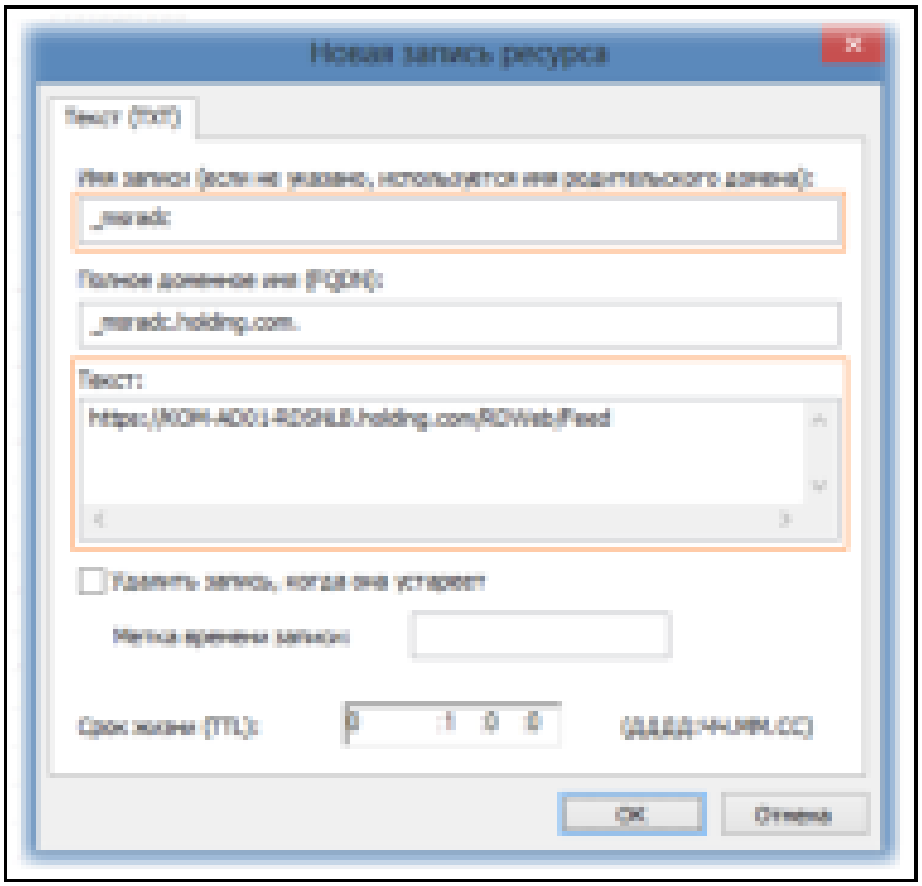

Опубликованные приложения доступны клиентам нашей фермы RDS двумя основными способами – через веб-интерфейс RD Web Access и через непосредственную доставку ярлыков запуска на клиентские компьютеры. С первым способом, полагаю, всё итак понятно, рассмотрим второй. Для того чтобы ярлыки опубликованных приложений RemoteApp стали доступны на клиенте с **Windows 7/8**, нужно выполнить подписку на узел RDWA в **Панели управления** (апплет **Подключения к удаленным рабочим столам и приложениям RemoteApp**). Щелкнув по ссылке **Доступ к удалённым приложениям RemoteApp и рабочим столам** мы вызовем мастер подключения, где в адресной строке укажем **URL RDWA** в формате http://KOM-AD01-RDSNLB.holding.com/RDWeb/Feed/WebFeed.aspx



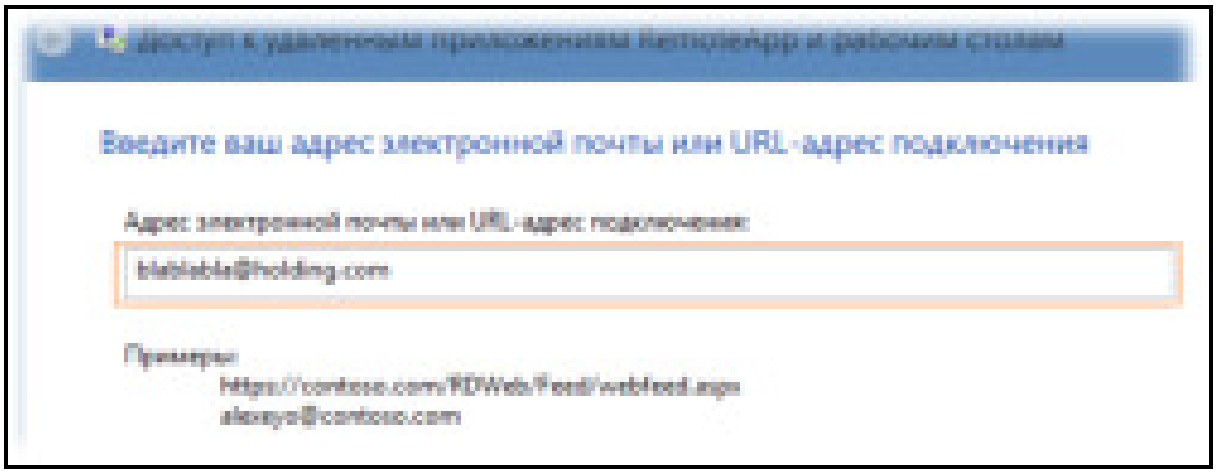

В примерах описанных в окне подключения можно заметить вариант с указанием адреса, похожего на адрес электронной почты - alexeyo@contoso.com. На самом деле такой метод указания адреса не столько имеет отношение к электронной почте, сколько относится к методу

автоматического обнаружения сервера публикации RemoteApp с помощью специальных записей в зоне прямого просмотра **DNS**. То есть мастеру подключения важно лишь то, что указано после символа @ – имя зоны DNS. До символа @ можно написать любую ерунду. Например, в нашем примере в DNS используется зона holding.com и в качестве адреса мы можем указать например blablabla@holding.com

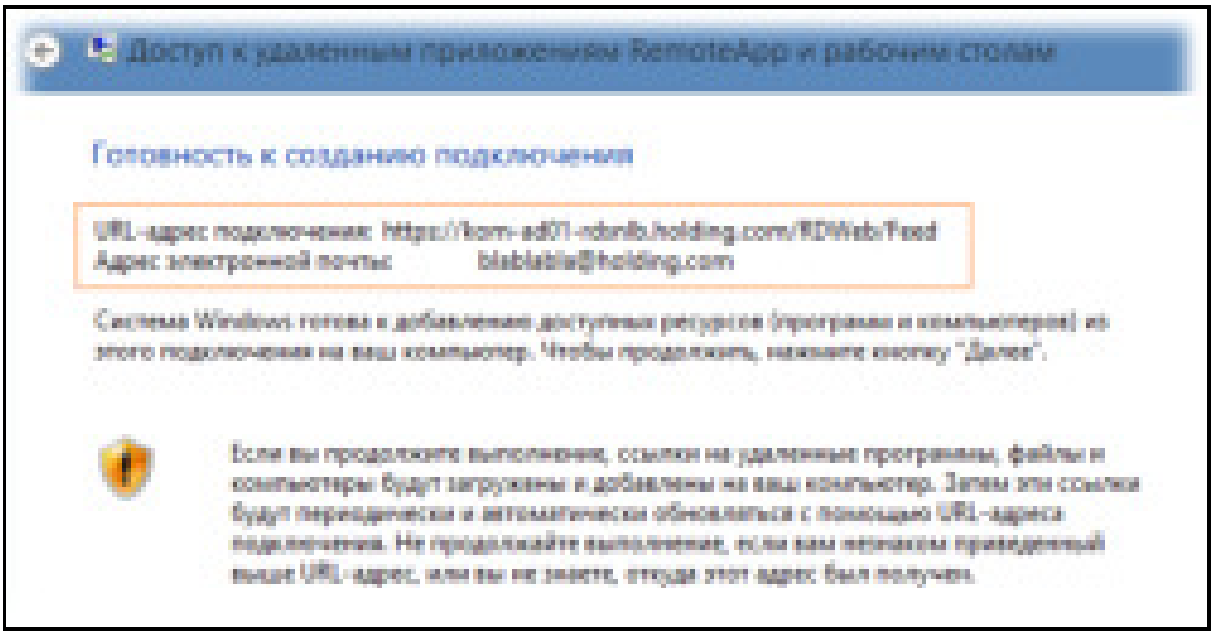
В зоне **DNS** соответственно при использовании такого метода должна быть создана специальная запись формата **TXT** с именем **_msradc** и текстовым значением в формате https://rds.domain.com/rdweb/feed Соответственно в нашем примере запись будет иметь следующий вид:



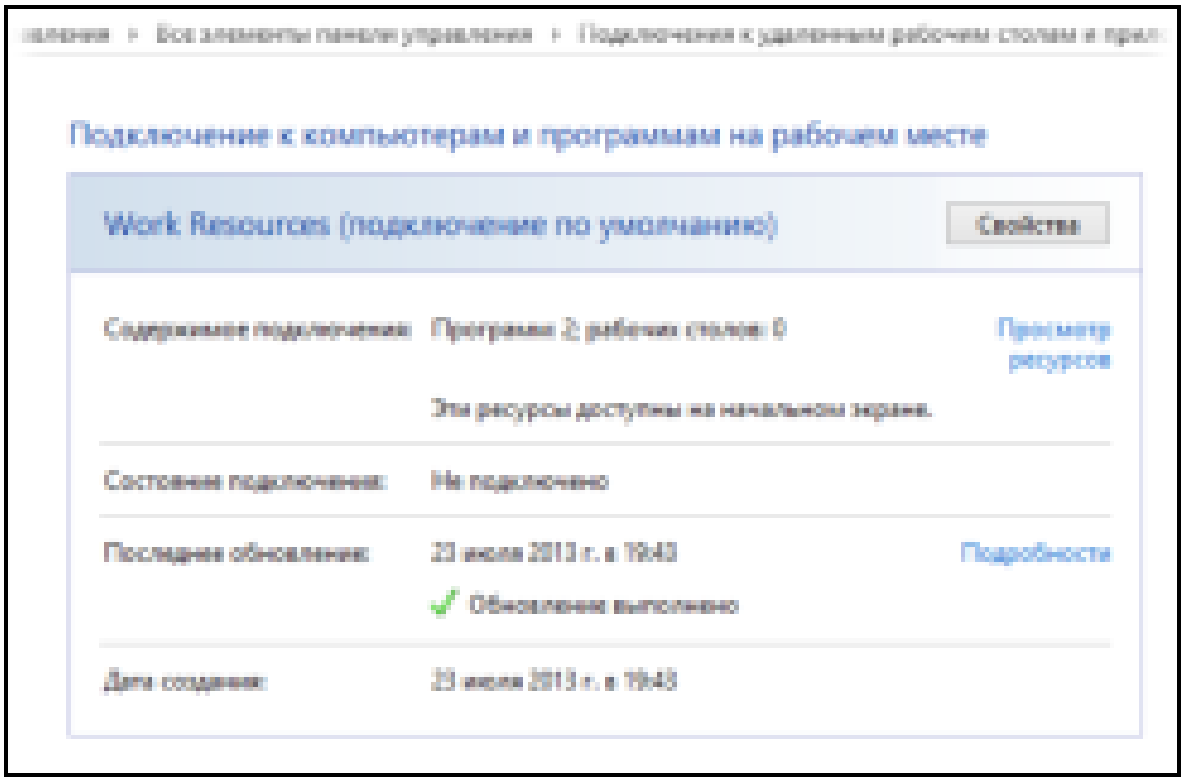

После того как запись создана, проверим то, что DNS сервер возвращает нам значение этой записи с помощью утилиты **nslookup** в режиме **set querytype=TXT** и если всё в порядке, то теперь в качестве адреса подключения можем указать соответствующее значение



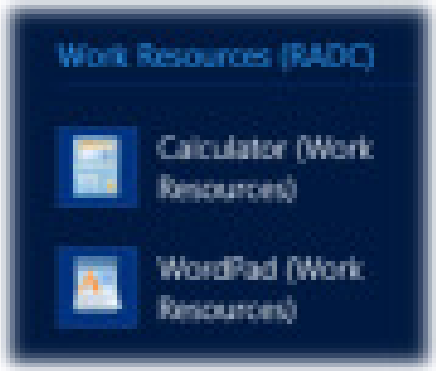

При этом из DNS будет возвращён URL-адрес подключения…



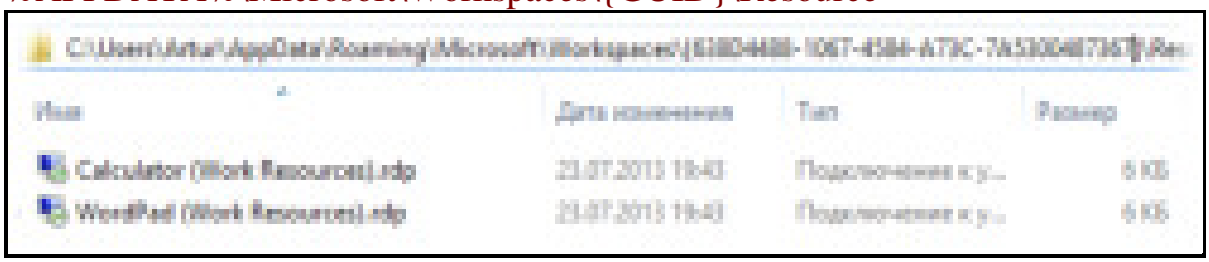

После этого может последовать запрос на ввод учетных данных пользователя, чтобы узел RDWA выполнил идентификацию пользователя и определил какие ярлыки на приложения RemoteApp можно показать пользователю согласно доменных групп безопасности, включенных в правилах публикации. В нашем примере будет отображена информация об успешном подключении и количестве доступных пользователю программ



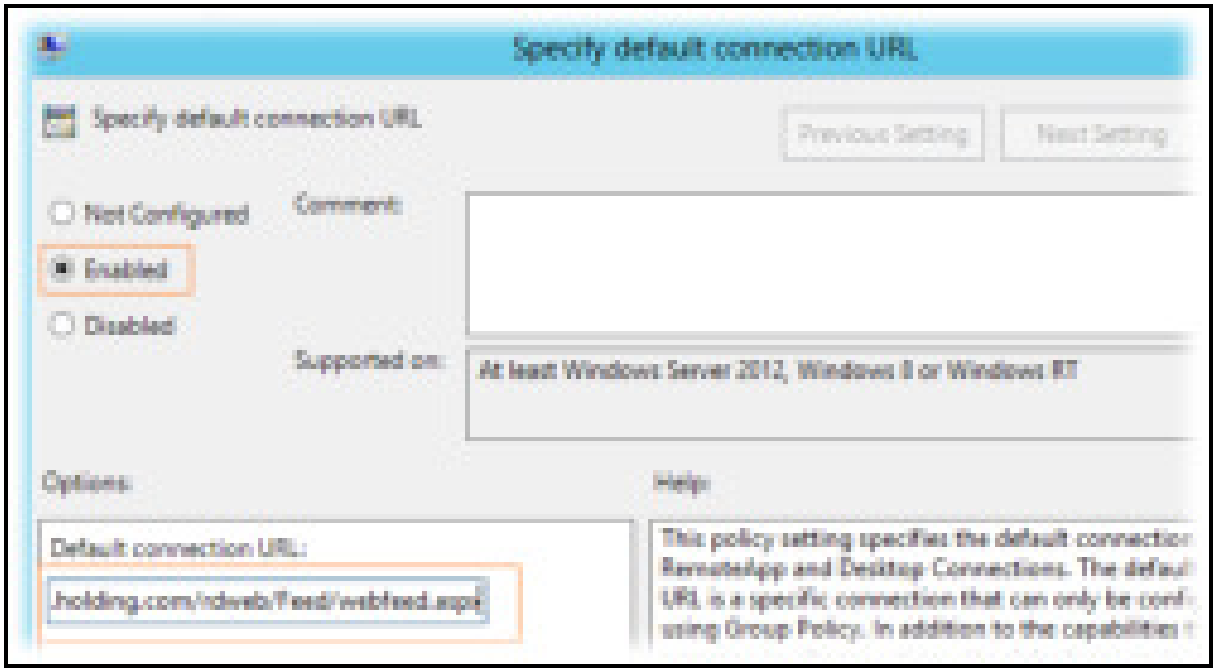

При этом в меню “Пуск” для Windows 7 и в стартовом экране для Windows 8 в отдельной группе появятся ярлыки на запуск приложений RemoteApp




Если вам потребуется каким-то альтернативным способом распространять ярлыки на приложения RemoteApp, то их можно будет найти на клиентской машине подключённой вышеописанным способом к точке публикации RDWA в каталоге %APPDATA%\Microsoft\Workspaces\{GUID}\Resource



Нововведением **Windows 8** стал ещё один способ подключения клиентов к точке публикации – с помощью групповых политик (**GPO**). За это отвечает параметр
**Specify default connection URL** в разделе **User Configuration/Policies/Administrative Templates/Windows Components/Remote Desktop Services/RemoteApp and Desktop Connections**. Для настройки клиентов нужно включить этот параметр и указать значение URL-адреса подключения в формате: https://KOM-AD01-RDSNLB.holding.com/rdweb/Feed/webfeed.aspx



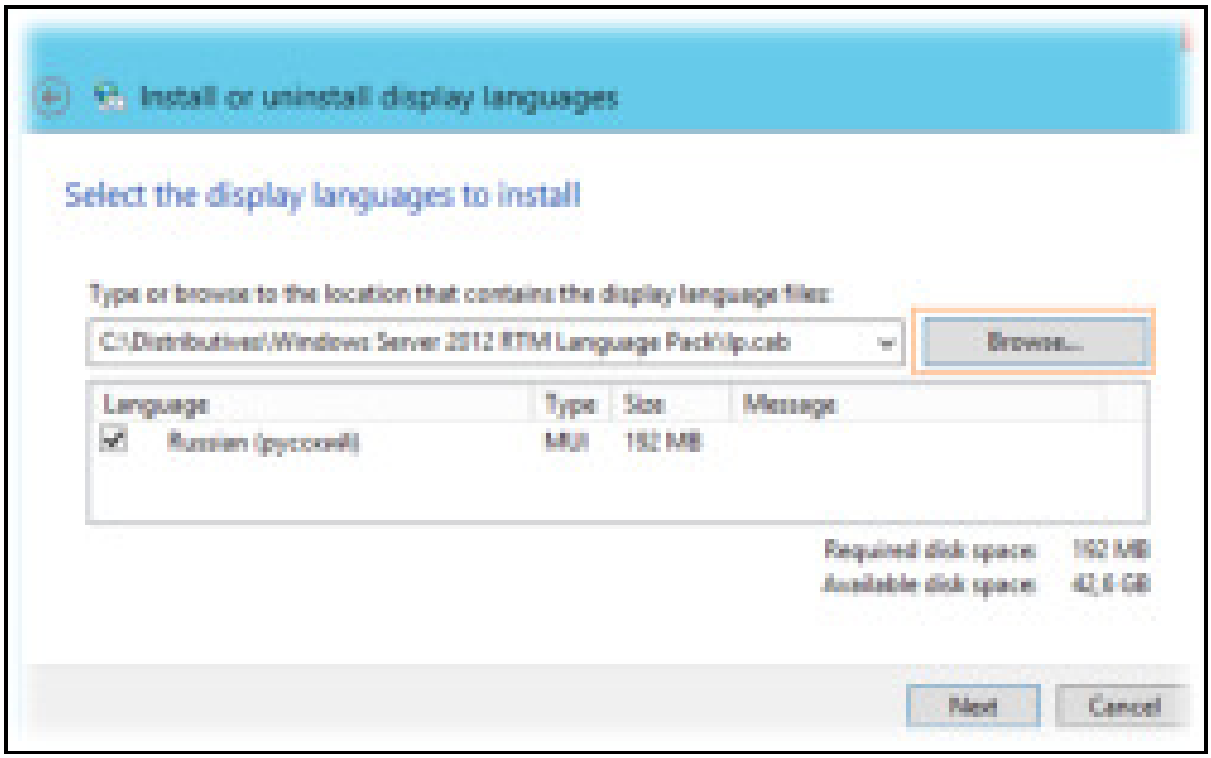

Как я уже сказал, этот параметр поможет нам настроить только клиентов **Windows 8**, но если у вас есть сильное желание раздать через GPO настройку и для клиентов **Windows 7** – читайте статью Concurrency Blog - How to deliver RemoteApps from Windows Server 2012 RDS. Метод заключается в применении на клиентских машинах **PowerShell** скрипта Configure RemoteApp and Desktop Connection on Windows 7 Clients с передачей ему в виде параметра файла настроек в следующем формате:

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<workspace name="Enterprise Remote Access"
xmlns="http://schemas.microsoft.com/ts/2008/09/tswcx"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
<defaultFeed url="https://KOM-AD01-RDSNLB.holding.com/rdweb/Feed/webfeed.aspx" />
</workspace>
```

**Устанавливаем языковой пакет**

Так как в нашем примере на серверах фермы RDS используется англоязычная система, нам потребуется установка языкового пакета для локализации интерфейса пользователя. Чтобы получить файлы русского языкового пакета распаковываем образ содержащий все языковые пакеты для **Windows Server 2012 RTM SW_DVD5_NTRL_Win_Svr_Language_Pack_2012_64Bit_MultiLang_FPP_VL_OEM_X18-27741.ISO**

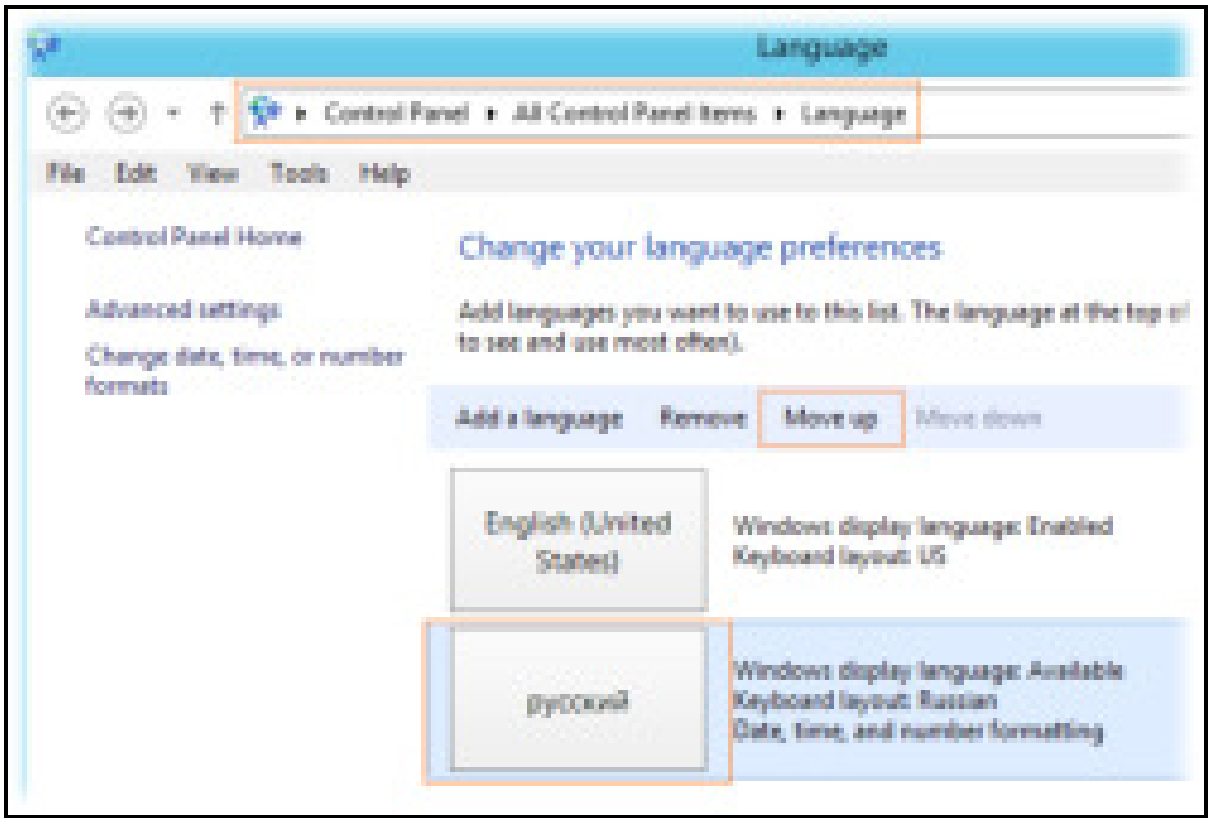
Извлекаем файл langpacks\ru-ru**lp.cab** из состава образа и вызываем на сервере RDS мастер установки языковых пакетов командой **lpksetup**



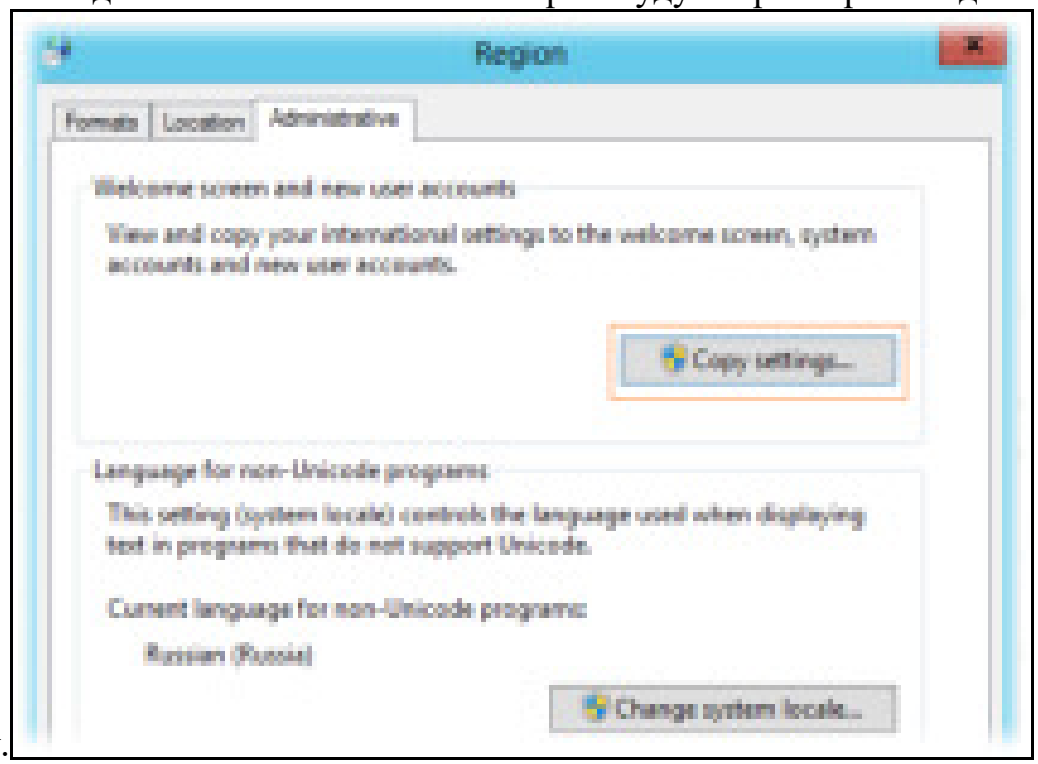

Помимо этого установку языкового пакета можно выполнить командой:

Dism /online /Add-Package /PackagePath:"C:\Distributives\WS2012RTMLanguagePack\lp.cab"

Практика показывает, что после выполнения этой команды, для того чтобы в панели управления появилась информация о том, что языковой пакет действительно установлен, – необходима перезагрузка системы. После перезагрузки сервера RDS переходим в панель управления в раздел **Language** и выделив **русский** язык кнопкой **Move Up** поднимаем его на первую позицию, сделав его таким образом приоритетным языком интерфейса.

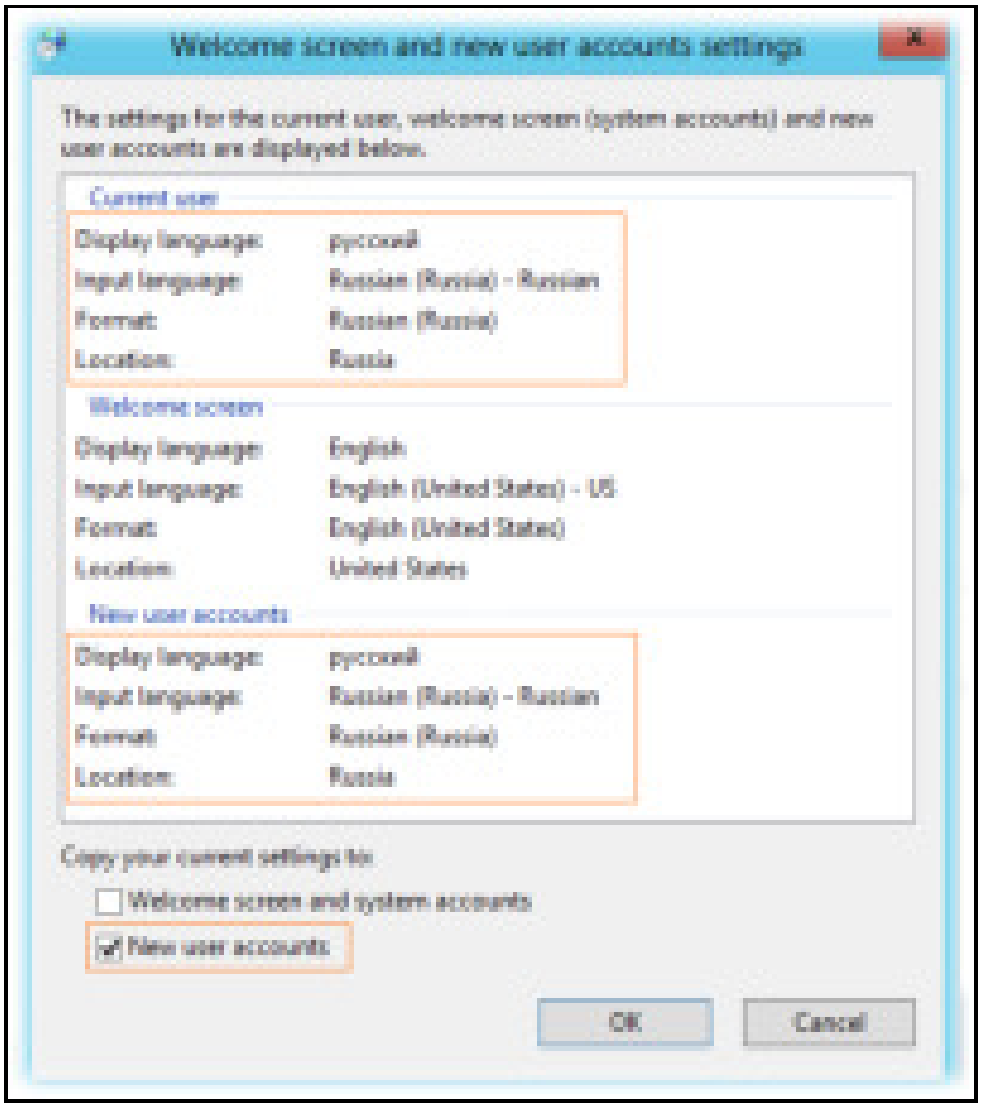



Далее открываем апплет панели управления **Control Panel** > **Region** (**intl.cpl**) , проверяем и при необходимости настраиваем параметры на родной язык на закладках **Formats** и **Locations** , а затем на закладке **Administrative** нажимаем **Copy settings**, чтобы скопировать языковые предпочтения текущего пользователя для всех пользователей которые будут первый раз входить в эту




систему.

Убедимся что у текущего пользователя установлены такие настройки, которые мы хотим иметь у всех пользователей сервера RDS и включим галочку **New user accounts**




Не рекомендую использовать опцию копирования русских настроек в системный профиль (галка **Welcome screen and system accounts**), так как это в перспективе может привести к невменяемой работе некоторых “буржуйских” программ, проблемы в которых возникают чаще всего из-за знака разделителя целой и дробной части.

### Настраиваем перенаправление печати

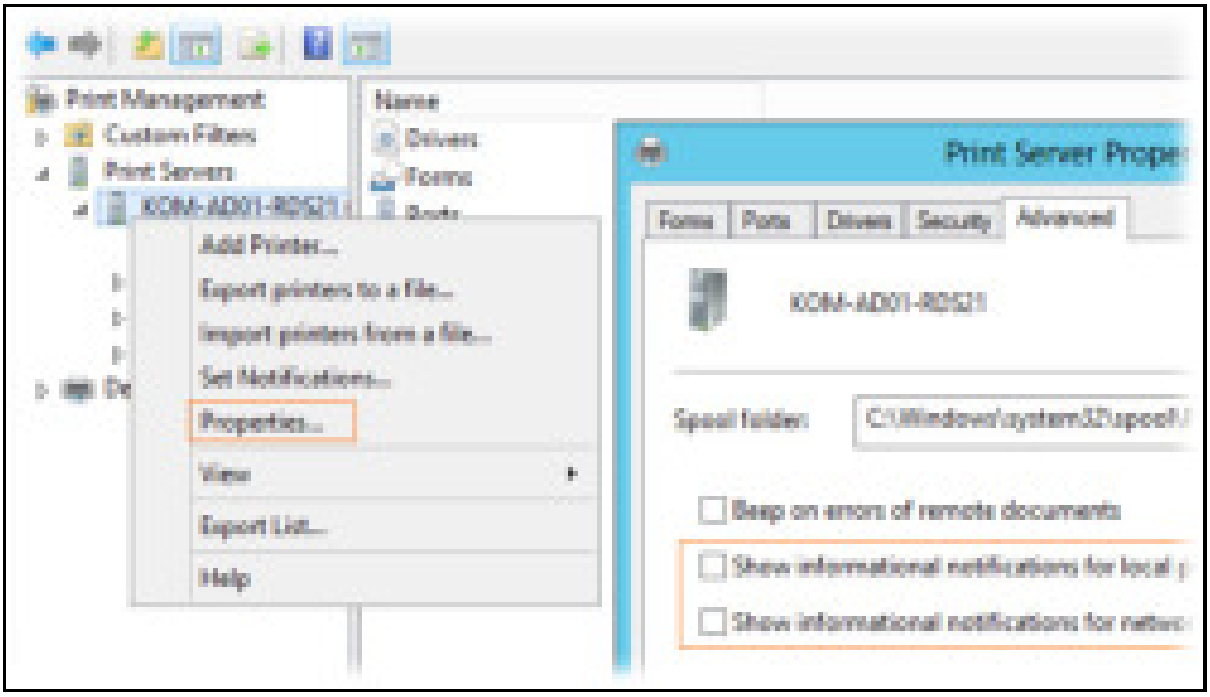
Для того чтобы пользователи служб удалённых рабочих столов смогли выполнять печать на перенаправленные с их клиентских мест устройств печати, выполним ряд нехитрых манипуляций.

Установим на сервера RDS консоль управления службой печати – **Print Management**, например с помощью **PowerShell**:

**Add-WindowsFeature** RSAT-Print-Services

Если есть сильное желание управлять службой печати на всех серверах например с рабочей станции Администратора, то для того, чтобы можно было удалённо подключаться к службе печати, на серверах необходимо включить параметр групповой политики **Allow Print Spooler to accept client connections** в разделе **Computer Configuration\Policies\Administrative Templates\Printers**. После применения политики на серверах нужно перезапустить службу очереди печати - **Print Spooler**.
На мой взгляд использовать локально установленную на серверах консоль – более предпочтительно.

После установки открываем консоль, добавляем в неё наши сервера, и в свойствах сервера печати для каждого сервера выполняем необходимые изменения настроек, например на закладке **Advanced** отключаем включённые по умолчанию оповещения сетевых и локальных принтеров…



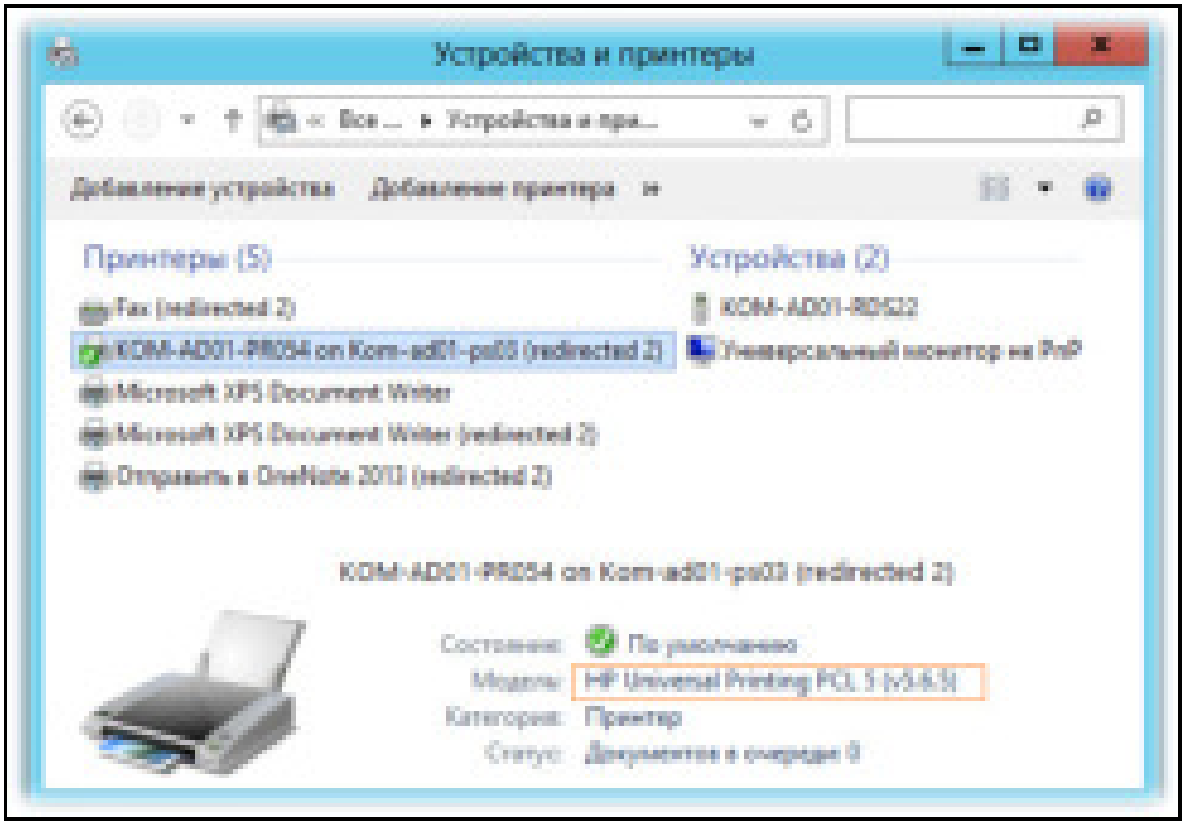

К слову об использовании именно локальной консоли…эти две опции недоступны для изменения (попросту не видны) если вы подключаетесь консолью удалённо.

На закладке **Drivers** добавляем драйвера принтеров, которые используются для печати на клиентских компьютерах. Драйвера принтеров нужно добавлять исходя из принципа разумного минимума. Например вместо того чтобы для принтеров **Hewlett-Packard** добавлять несколько драйверов для конкретных

моделей лучше добавить один универсальный драйвер **HP Universal Print Driver** (**UPD**), в случае если принтеры поддерживают работу на данном драйвере. В нашем примере используется текущая версия (на момент написания этой заметки) **UPD** совместимая с **Windows Server 2012 - 5.6.5.15717**. Разумеется добавлять драйвера производителей оборудования вообще имеет резон только в том случае если тесты показывают, что принтер не выполняет поставленные задачи печати на драйвере **Remote Desktop Easy Print**.

В конфигурации по умолчанию для принтеров перенаправляемых с пользовательских компьютеров система будет использовать драйвер **Remote Desktop Easy Print**. Если мы загружаем на сервера RDS драйвера производителей принтеров, как например тот же HP UPD, то возможно нам стоит переопределить такое поведение, то есть, чтобы приоритетным для использования считался драйвер вендора железки, а уж если его не удалось найти – использовать RD Easy Print. Задаётся это параметром групповой политики **Use Remote Desktop Easy Print printer driver first = Disabled** в разделе **Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Printer Redirection**

После применения GPO в пользовательской терминальной сессии проверяем какой драйвер был назначен для перенаправленного принтера…



На этом, в целом, можно считать, что мы выполнили основные этапы создания и настройки отказоустойчивой фермы **RD Connection Broker** на базе **Windows Server 2012**. В отдельной следующей заметке мы рассмотрим пример настройки пользовательского интерфейса на сервера **RD Session Host**.

## Практическое занятие №18 Развертывание и поддержка виртуализации профиля пользователя

***Цель работы:***
Изучить систему развертывания и поддержка виртуализации профиля пользователя.

Для того, чтобы пользователи всегда имели доступ в документам, с которыми они работают при использовании удаленных приложений, нужно обеспечить высокую доступность этих данных. Обеспечить это можно разными способами:

- **Перемещаемые профили (Roaming Profiles)**. В этом случае профиль пользователя, как правило, размещается на сервере. Заходя под своим профилем на любой машине в доменной сети, пользователь загружает локально свой профиль с сервера. Профиль хранится в виде набора файлов.
- **Перенаправление папок (Folder Redirection)**. В этом случае, отдельные папки профиля пользователя перенаправляются, как правило, на сервер. Пользователь по сути работает со своим профилем непосредственно на сервере, локально хранятся автономные файлы профиля, на случай отключения от сети. Перенаправленные папки хранятся в виде набора файлов.
- **Диски профилей пользователей (User Profile Disks, UPD)**. В этом случае используется не общий профиль пользователя, а только профиль на сервере удаленных приложений. Выбранные папки профиля могут быть сохранены на сервере. Сами папки хранятся в виде vhdx файлов.

В то время как первые 2 способа влияют непосредственно на профиль пользователя в домене, последний влияет только на локальный профиль пользователя на терминальном сервере, что делает его внедрение более простым. В любом случае, какой бы вариант хранения профилей не использовался, необходимо обеспечить высокую доступность данных, что хранятся в профиле пользователя.

**User Profile Disks** (**UPD**, диски профилей пользователей) – новый функционал Remote Desktop Services в Windows Server 2012. User Profile Disks представляют собой **альтернативу** использованию технологий **перемещаемых профилей** (roaming profile) и **перенаправления папок** (folder redirection) в терминальных сценариях RDS. Идея UPD – данные пользователя и его приложений (т.е. его профиль) хранятся в виде отдельного виртуального **vhdx** диска на некоем выделенном общем файловом ресурсе. Этот виртуальный диск монтируется в

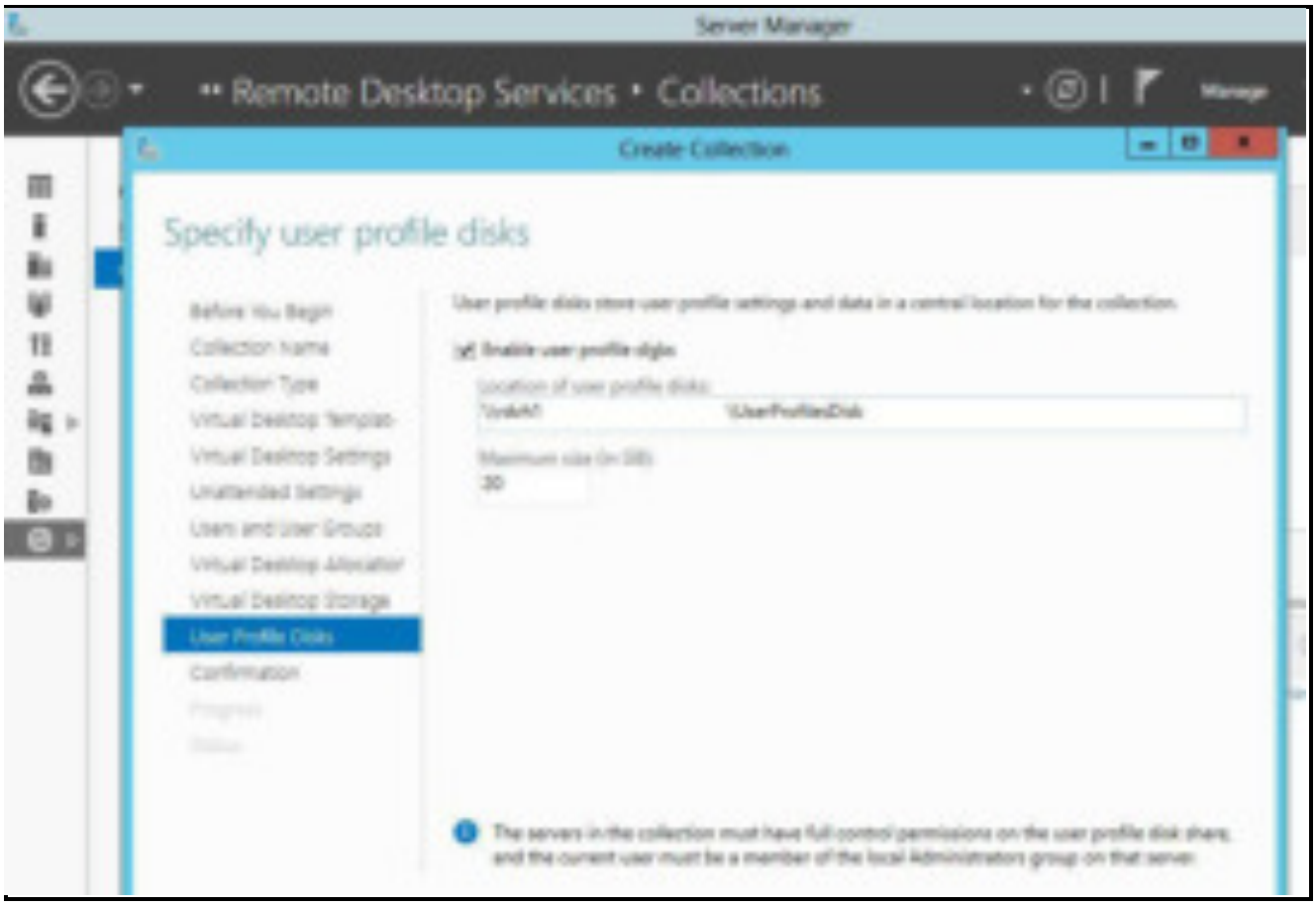
сессию пользователя при его входе на RDS-сервер, и отключается при выходе (конечно, с сохранением всех изменений в профиле).

**Настройка User Profile Disks в Windows Server RDS**

В первую очередь необходимо на любом файловом сервере организации создать общую сетевую папку, в которой будут храниться файлы с профилями пользователей в формате VHDX дисков (если вы хотите обеспечить высокую доступность UPD дисков, можно разместить файлы UPD на кластерном файловом ресурсе). В нашем примере, путь к такому каталогу будет выглядеть так: *\\srv01\DemoLabOficeApps*. Необходимо предоставить серверам, входящим в коллекцию RDS полные права доступа на данный каталог и файловую систему.

В рамках одной коллекции RDS для каждого пользователя может существовать только один vhdx файл с UPD профилем. Если пользователь подключается к ресурсам из двух разных RDS коллекций, для каждой из них будет создан отдельный vhdx файл с профилем пользователя.

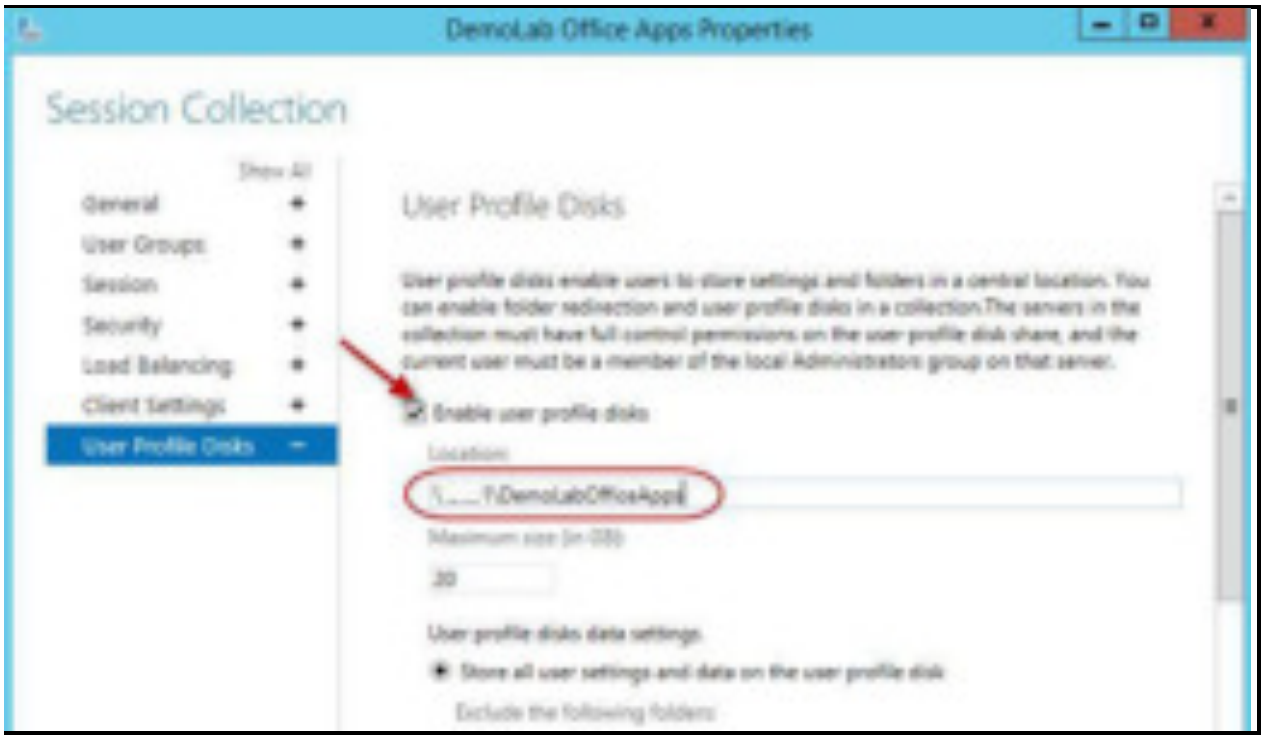
Режим User Profile Disks включается и настраивается в параметрах коллекций Remote Desktop. Этот режим можно включить непосредственно при создании коллекции, или уже после того, как коллекция создана.



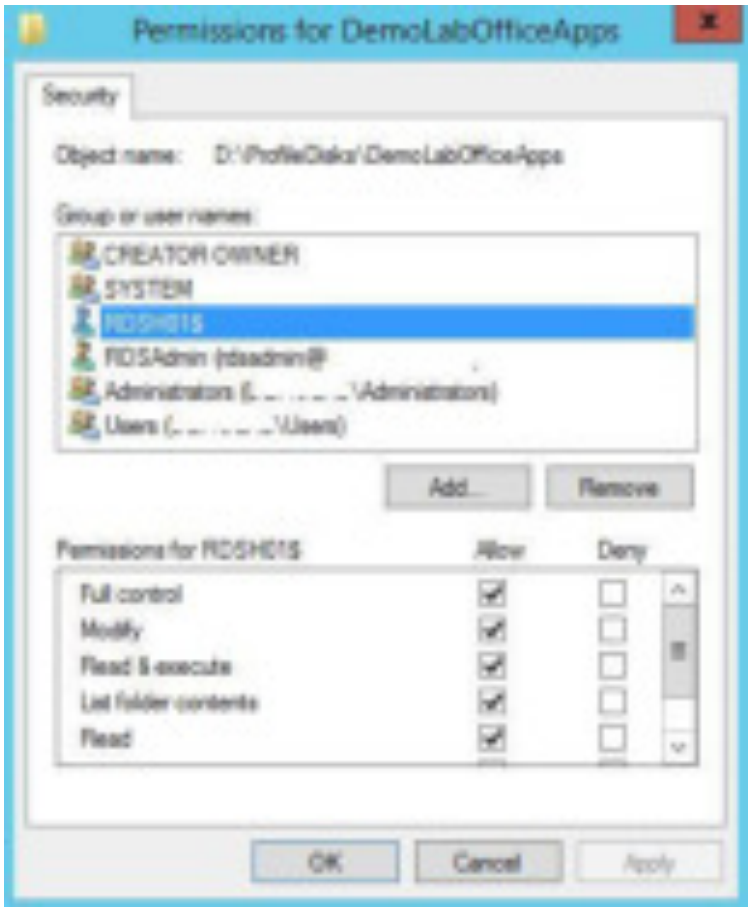

В нашем примере коллекция уже существует, поэтому в консоли Server

Manager выбираем имеющуюся коллекцию, и в верхнем левом углу выбираем **Tasks-> Edit Properties**.

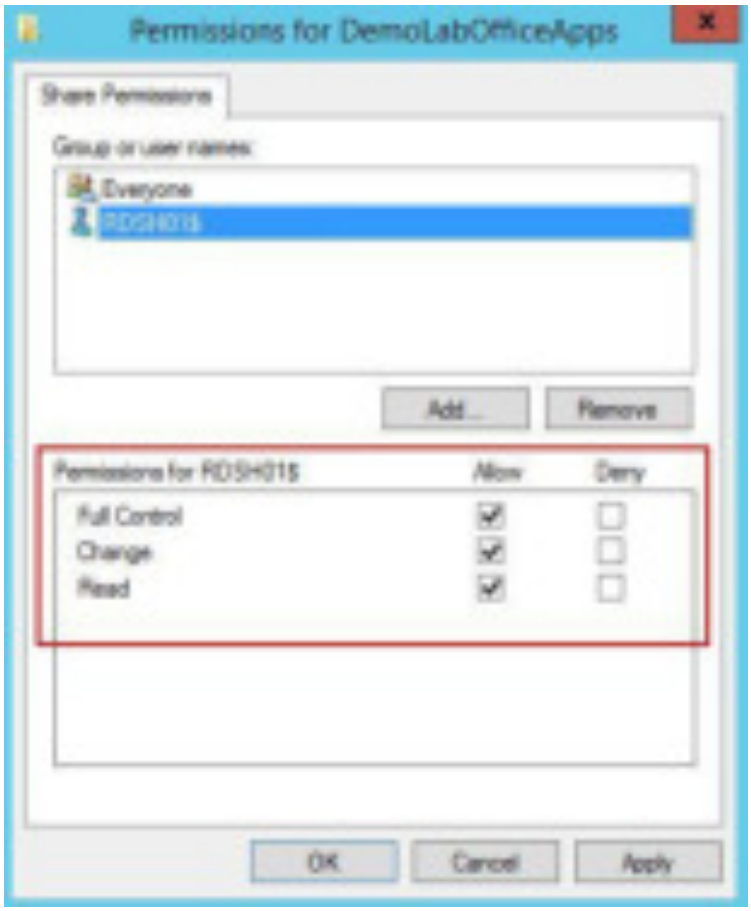

Затем в разделе User Profile Disks ставим чекбокс на **Enable user profile disks**, указываем путь к созданной ранее сетевой папке (\\srv01\DemoLabOficeApps) и максимальный размер диска с профилем (пусть это будет 20 Гб). Сохраняем изменения.




После сохранения изменений, проверьте что NTFS разрешения на каталог с дисками профилей были изменены. В нашем случае коллекция состоит из одного сервера RDSH01, которому предоставлены полные права на папку.



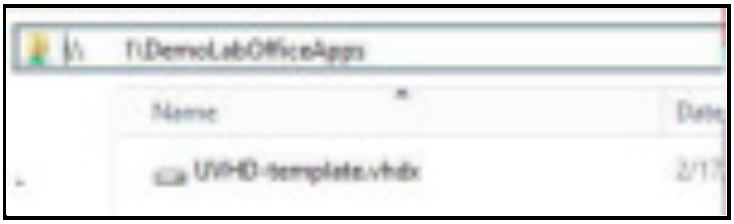

На уровне сетевой папки (шары) серверу RDSH01$ предоставлены права Full Control.



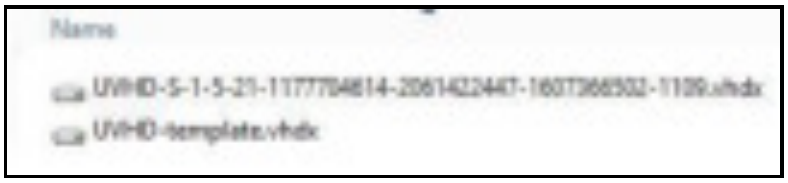

При добавлении новых серверов RD Session Host в коллекцию RDS серверов, мастер автоматически изменит разрешения на каталог, предоставив доступ новым серверам. Это очень удобно, т.к. при масштабировании терминальной фермы не нужно каждый раз вспоминать о настройке разрешений на сетевую папку с профилями.

**VHDX файл с UPD профилем пользователя**

Перейдем в наш общий сетевой каталог с профилями пользователей. Теперь в нем хранится файл вида **UVHD-template.vhdx**.

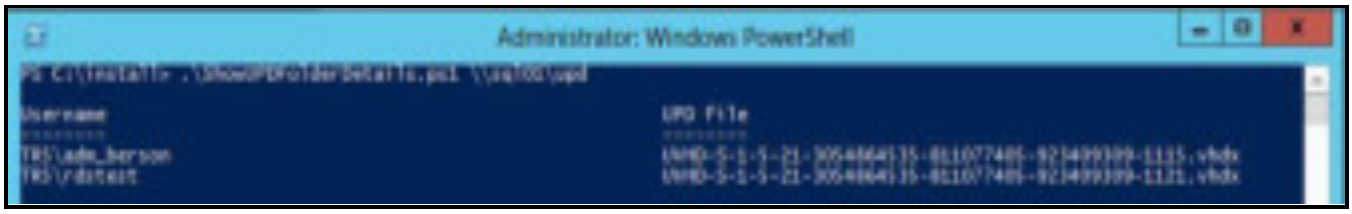



Этот файл представляет собой шаблон диска с профилем пользователя. При первом RDP входе пользователя на сервер RDS, этот шаблон копируется и переименовывается в vhdx файл, содержащий в имени SID пользователя.

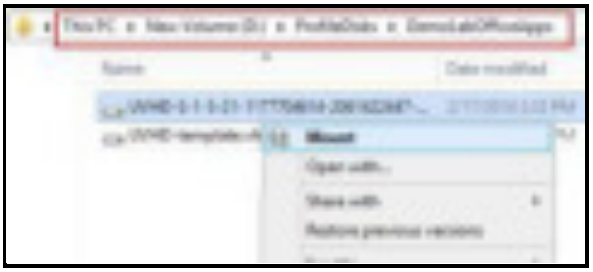



**Т**еперь, чтобы сопоставить имя файла UPD с именем пользователя, приходится пользоваться отдельным скриптом. Например, ShowUPDFolderDetails.ps1 или можно преобразовать SID в имя учетной записи с помощью командлета Get-ADUser:

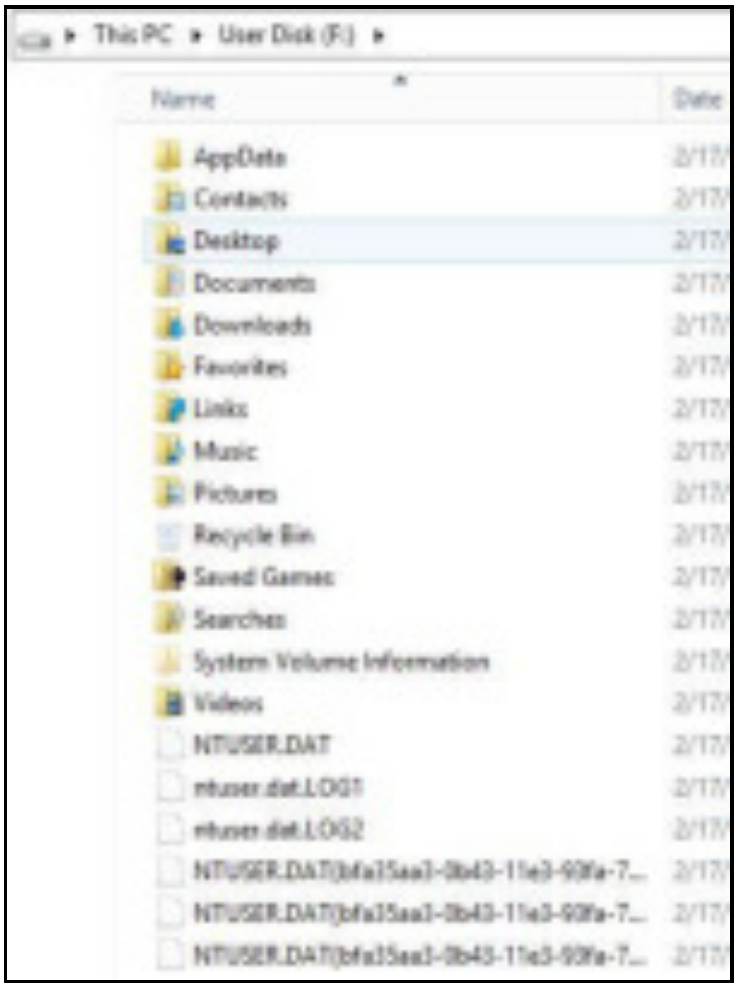
```
Get-ADUser -Identity S-1-5-21-305647651-3952524288-
2944781117-23711116
```



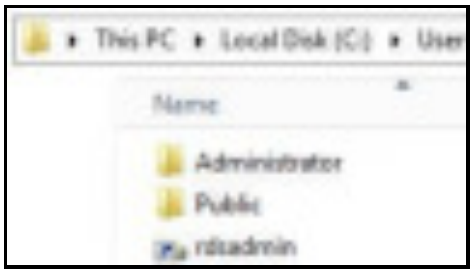

Посмотрим, что представляет собой диск с профилем пользователя. Для этого смонтируем его, щелкнув по vhdx файлу ПКМ и выбрав пункт **Mount**. Диск UPD можно использовать только в одной сессии на одном RDS хосте (монопольный доступ). Вы не сможете смонтировать UPD VHDX диск, если в настоящий момент его использует пользователь на RDS сервере).



Как вы видите, содержимое vhdx диска представляет набор каталогов и файлов обычного профиля пользователя. При входе в систему пользователь получает абсолютно прозрачный доступ к данным, хранящимся в его профиле.




На стороне сервера RD Session Host .vhdx файл пользователя монтируется в каталог **C:\users\<username>** и выглядит таким образом:



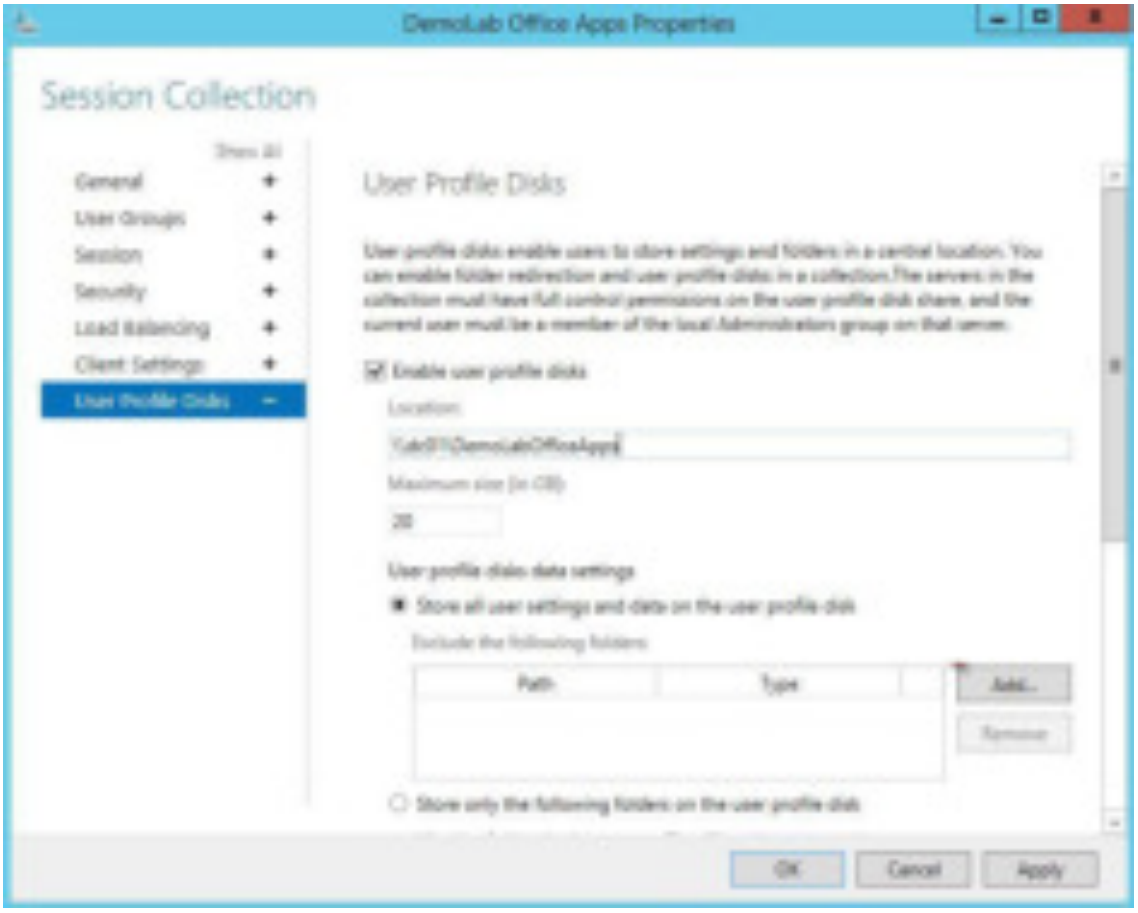

Обратите внимание, что UPD диск привязан к версии Windows RDS сервера. Вы не сможете перенести UPD профиль пользователя с RDS сервера с одной версии Windows Server на другую.

Запись данных в файл vhdx ведется в реальном времени. Т.е. при копировании данных в профиль пользователя на сервере RDS, размер vhdx файла на общем хранилище увеличивается сразу.

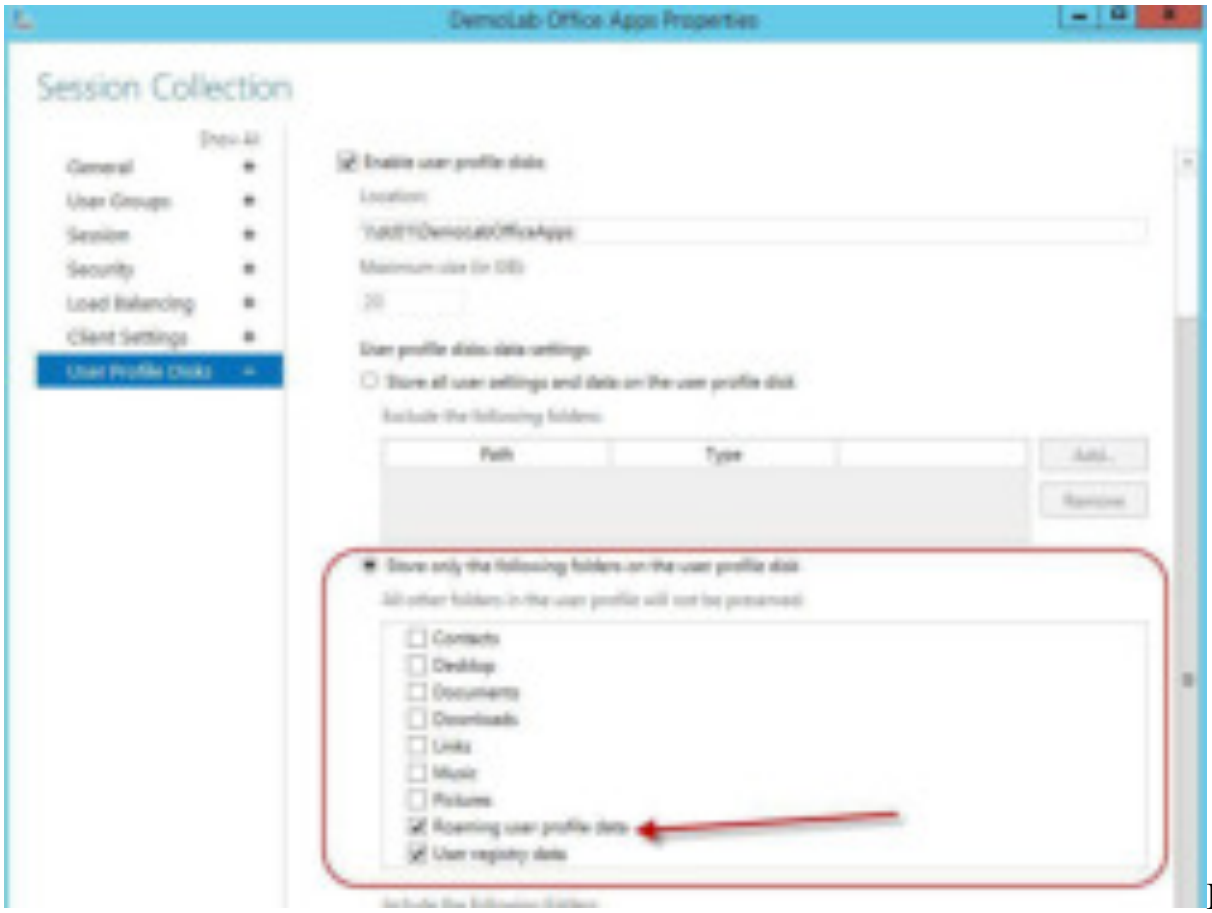
В том случае, если в системе уже присутствует каталог с профилем пользователя, каталог со старым профилем переименовывается в формат **<username>-BACKUP-<number>**.


VHDX диск монтируется при старте сессии пользователя на VDI или RDS сервере. Список подключенных UPD дисков с профилями можно вывести с помощью утилиты **mountvol**.

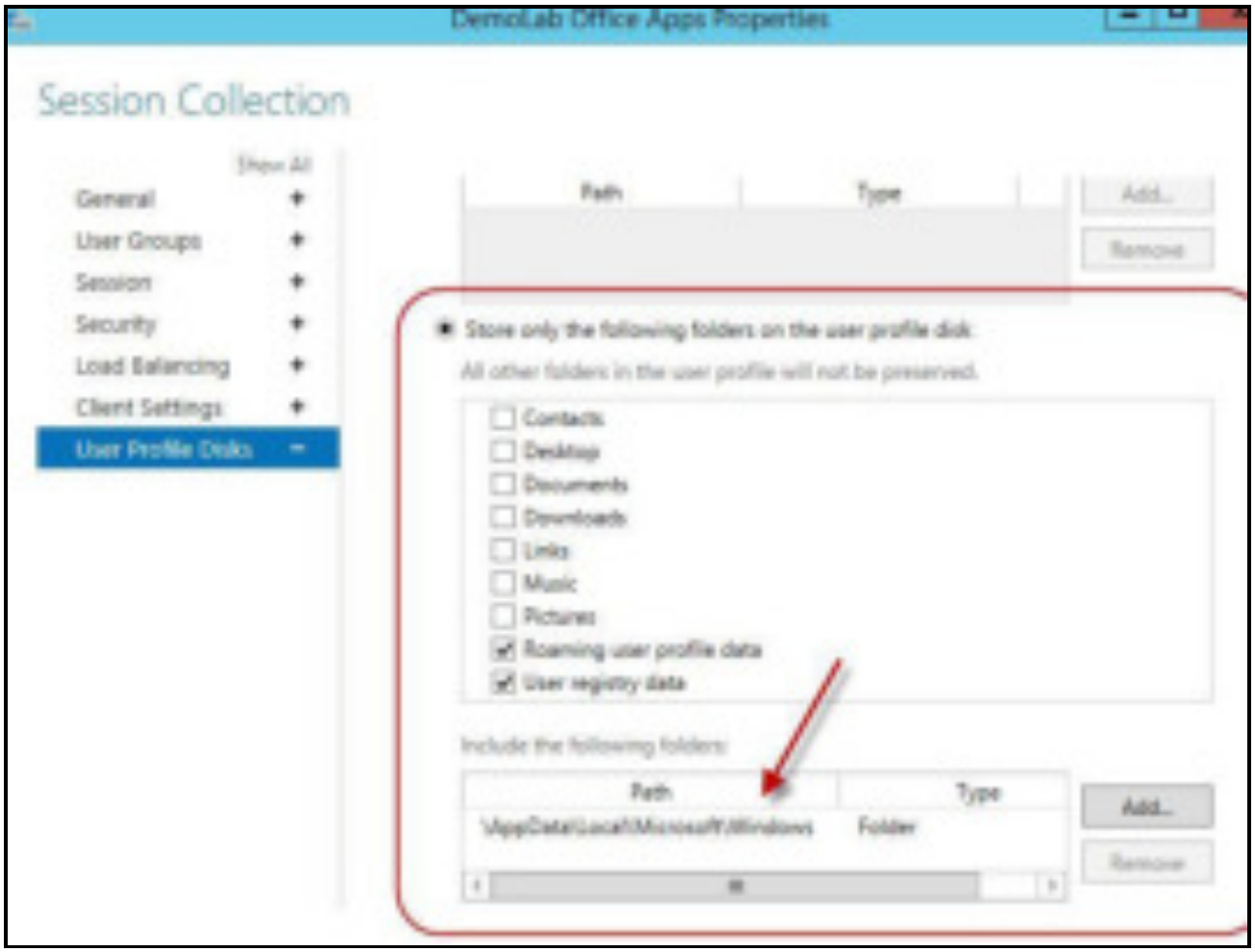
По-умолчанию диск с пользовательским профилем содержит в себе все содержимое профиля пользователя. Однако, в настройках RDS коллекции можно исключить определенные папки из списка синхронизируемых каталогов, либо указать, что должны сохранятся только определённые папки. Таким образом все изменения, которые вносятся в терминальной сессии пользователя в список исключенных папок профиля, не сохраняются на vhdx диске в сетевом каталоге.




Второй вариант позволяет настроить сохранение в UPD профиле только указанных каталогов.




В случае необходимости, второй вариант позволяет реализовать сценарии сохранения настроек стартового экрана, хранящихся в файле appsfolder.itemdata-ms. В данном примере мы просто добавили путь к каталогу \AppData\Local\Microsoft\Windows в качестве дополнительного пути, который нужно сохранять в UPD.



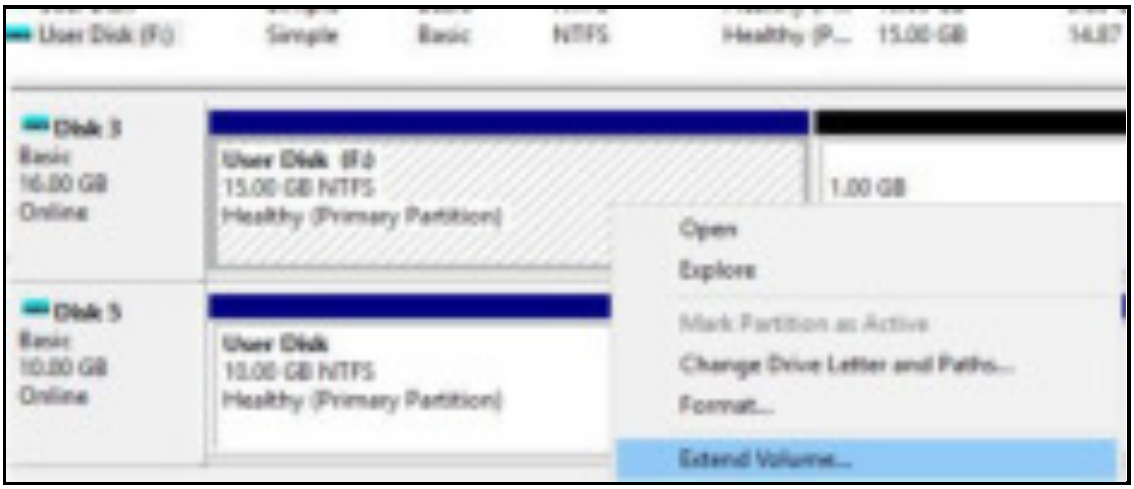

**Как расширить диск User Profile Disk с помощью PowerShell**

Вы можете расширить виртуальный vhdx диск с UPD профилем конкретного пользователя с помощью PowerShell командлета Resize-VirtualDisk из модуля Hyper-V.

```
Net use U: \\srv01\DemoLabOficeApps
Resize-VHD -Path u:\UVHD-<SID>.vhdx -SizeBytes 30GB
Net use U: /delete
```

Если вы используете командлет Resize-VHD с рабочей станцией под Windows 10, то в системе необходимо установить роль Hyper-V -> ПлатформаHyper-V -> Службы Hyper-V.

Теперь нужно расширить диск из графического интерфейса консоли Управления дисками (Disk Manager). Действие –> Подключить виртуальный жесткий диск -> Расширить том.




Либо воспользуемся таким PoSh скриптом:

```
<#
.Synopsis
This script extend size of VHDX file and resize the disk
partition to Max
#>
Param(
[Parameter(Mandatory=$true,ValueFromPipeline=$true)]
[alias("Path")]
[string]$vhdxFile,
[Parameter(Mandatory=$true,ValueFromPipeline=$true)]
[alias("Size")]
[int64]$vhdxNewSize
)
begin{
try {
Mount-VHD -Path $vhdxFile -ErrorAction Stop
}
catch {
Write-Error "File $vhdxFile is busy"
Break
}
$vhdx = Get-VHD -Path $vhdxFile
if ($vhdx.Size -ge $vhdxNewSize){
Write-Warning "File $vhdxFile already have this size!"
$vhdx | Dismount-VHD
Break
}
}
process{
Dismount-VHD -Path $vhdxFile
Resize-VHD -Path $vhdxFile -SizeBytes $vhdxNewSize
```

```
$vhdxxpart = Mount-VHD -Path $vhdxFile -NoDriveLetter -
Passthru | Get-Disk | Get-Partition
$partsize = $vhdxxpart | Get-PartitionSupportedSize
$vhdxxpart | Resize-Partition -Size $partsize.SizeMax
}
end{
Dismount-VHD -Path $vhdxFile
}
```

Нельзя расширить UPD диск пользователя с активной RDS сессией.

Чтобы уменьшить размер файла UPD (при условии, что вы удалили данные пользователя внутри vhdx файла и размер файлов на диске меньше выделенного ему размера) можно воспользоваться командами:

```
resize-VHD \\srv01\DemoLabOficeApps\UVHD-<SID>.vhdx -
ToMinimumSize
```

А затем:

```
Optimize-vhd -path \\srv01\DemoLabOficeApps\UVHD-
<SID>.vhdx -mode full
```

Мы рассмотрели основные особенности работы технологии User Profile Disks в RDS/VDI решениях на базе Windows Serer 2016 и 2012 R2. Настройка UPD намного проще чем процесс настройки перемещаемых профилей и перенаправляемых папок. Диски привязаны к коллекции RDS и не могут повредиться при попытке совместного использования профиля несколькими терминальными серверами (в отличии от обычных профилей). Диски профилей пользователей могут храниться на SMB шарах, CSV, SOFS, в SAN или на локальных дисках. Также Microsoft отмечает, что скорость загрузки рабочей среды пользователя в случае использования UPD уменьшается.

Если вы планируете использовать для хранения UPD профилей DFS сервера, то имейте в виду, что на них должна использоваться Windows Server 2012 R2. При использовании предыдущих версий Windows Server вы получите ошибку:

```
Unable to enable user disks on rVHDShare. Could not
create template VHD.  Error Message: The network location
"\\winitpro.ru\namespace\UPD1" is not available.
```

Также на стороне файлового сервера желательно использовать (Windows Server 2012 R2) или выше.

В любом случае, т.к. технология User Profile Disks относительно свежая, рекомендуется перед крупными внедрениями UPD откатать их работу и возможные проблемы в тестовой среде.

## Практическое занятие №19. Проектирование и реализация файловых служб

***Цель работы:***

Выполнить проектирование изучить приемы работы с файловым сервером на базе Windows Server

Реализация файловой системы связана с такими вопросами, как поддержка понятия логического блока диска, связывания имени файла и блоков его данных, проблемами разделения файлов и управления дисковым пространством.

Файловая система должна организовать эффективную работу с данными, хранящимися во внешней памяти, и предоставить пользователю возможности для запоминания и выборки этих данных.

Для организации хранения информации на диске пользователь вначале обычно выполняет его форматирование, выделяя на нем место для структур данных, которые описывают состояние файловой системы в целом. Затем пользователь создает нужную ему структуру каталогов (или директорий), которые, по существу, являются списками вложенных каталогов и собственно файлов. И наконец, он заполняет дисковое пространство файлами, приписывая их тому или иному каталогу. Таким образом, ОС должна предоставить в распоряжение пользователя совокупность системных вызовов, которые обеспечивают его необходимыми сервисами.

Кроме того, файловые службы могут решать проблемы проверки и сохранения целостности файловой системы, проблемы повышения производительности и ряд других.

**<u>Какие проблемы будут решены после оптимизации файлового сервера:</u>**

1) Зайдя на файловый сервер человек будет видеть только “свои” папки.

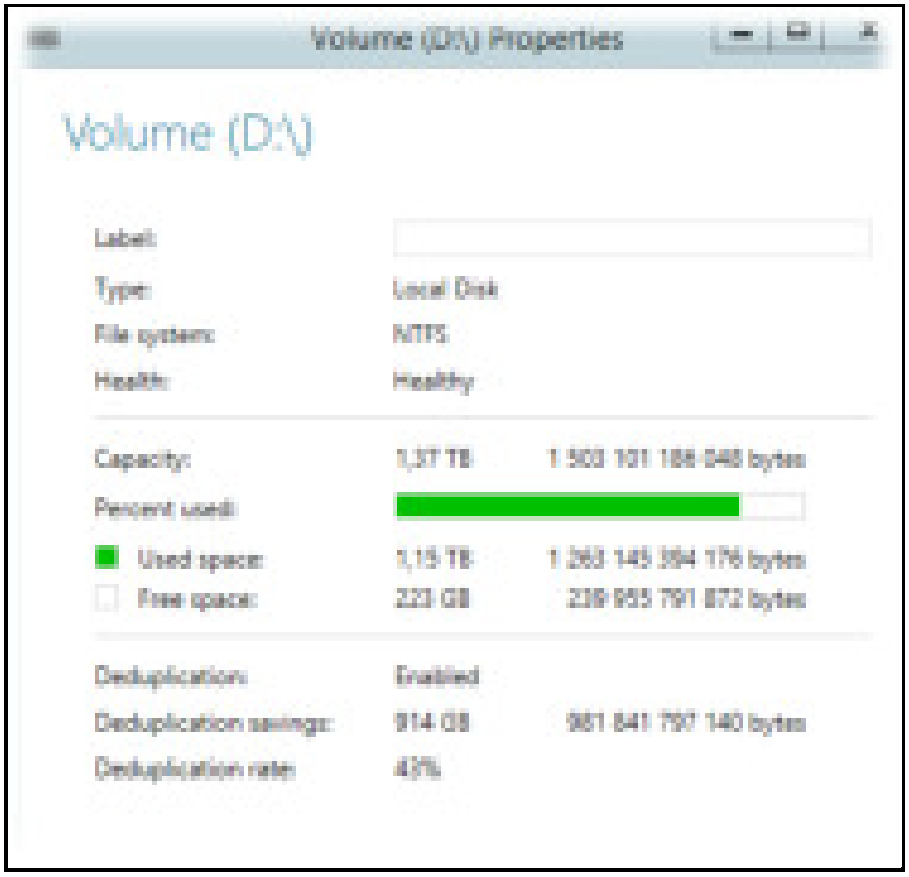
2) Доступ к папкам будет предоставляться через ролевые группы на базе групп Active Directory.

При таком подходе предоставление доступа к ресурсу осуществляется лишь добавлением определенного пользователя в требуемую группу через оснастку **Active Directory Administrative Center**.

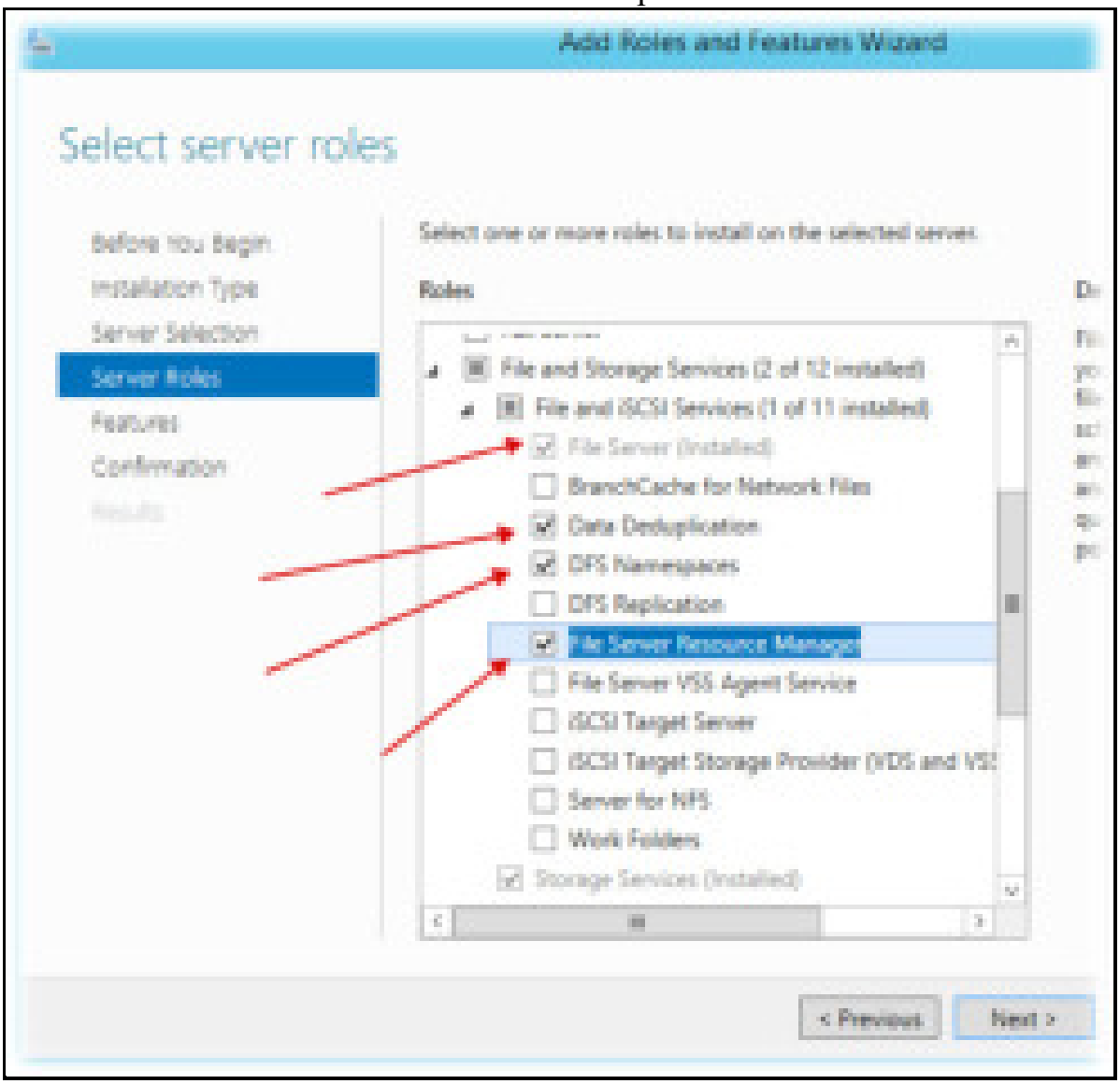
3) Файловый сервер будет работать на базе технологии **Distributed File System**.

4) Будет активирована технология **Data Deduplication**.

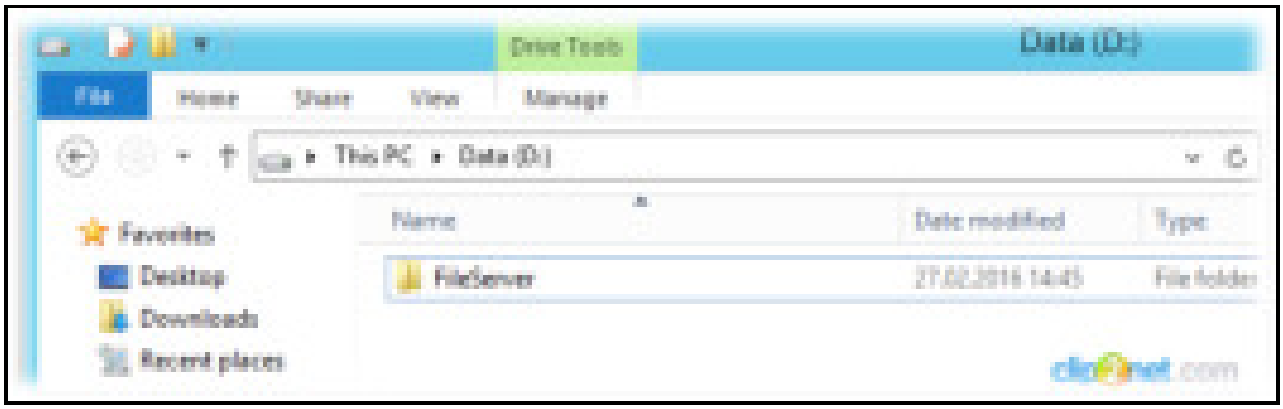
К примеру Deduplication rate (при дефолтовых настройках) составляет 43%:



Устанавливаем роли:

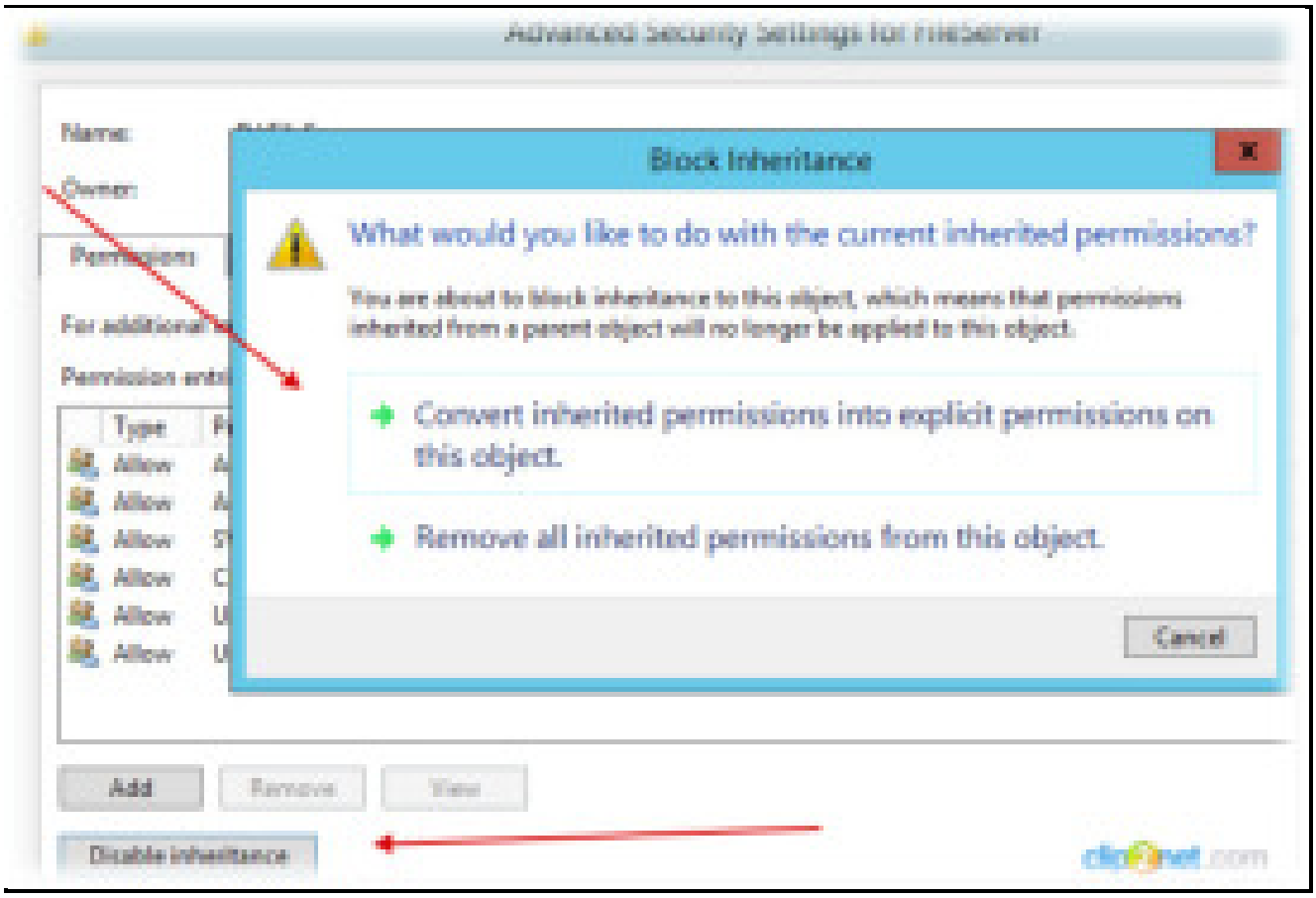



Создаем папку самого верхнего уровня:

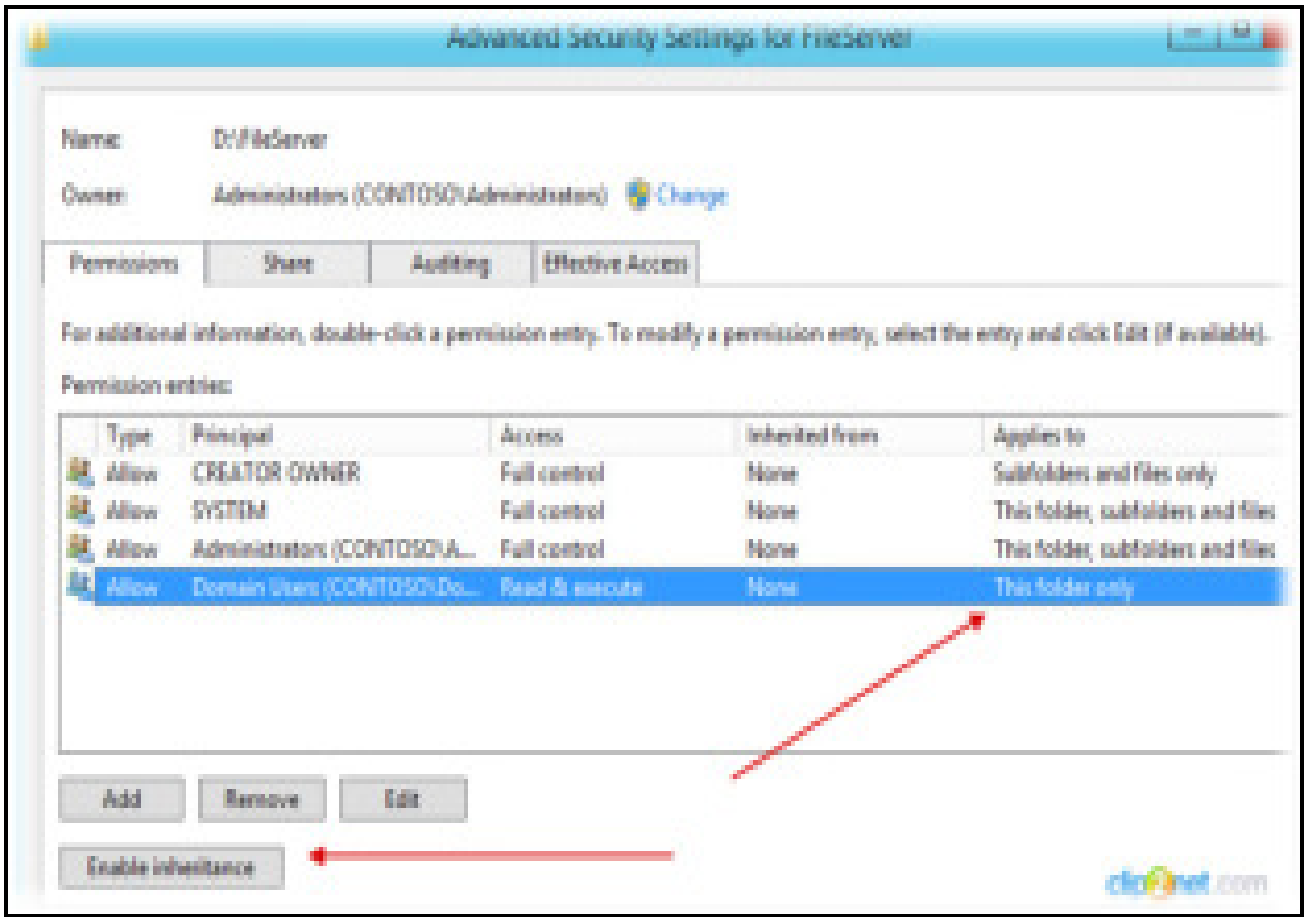



Когда создаем папку или папки верхнего уровня лучше использовать английские буквы и не использовать в названии пробелы. Если этим пренебречь, то к примеру некоторые Linux клиенты могут при монтировании этой папки испытывать дополнительные проблемы.

Далее заходим в свойства этой папки на вкладку **Security –> Advanced** и выключаем наследование прав:

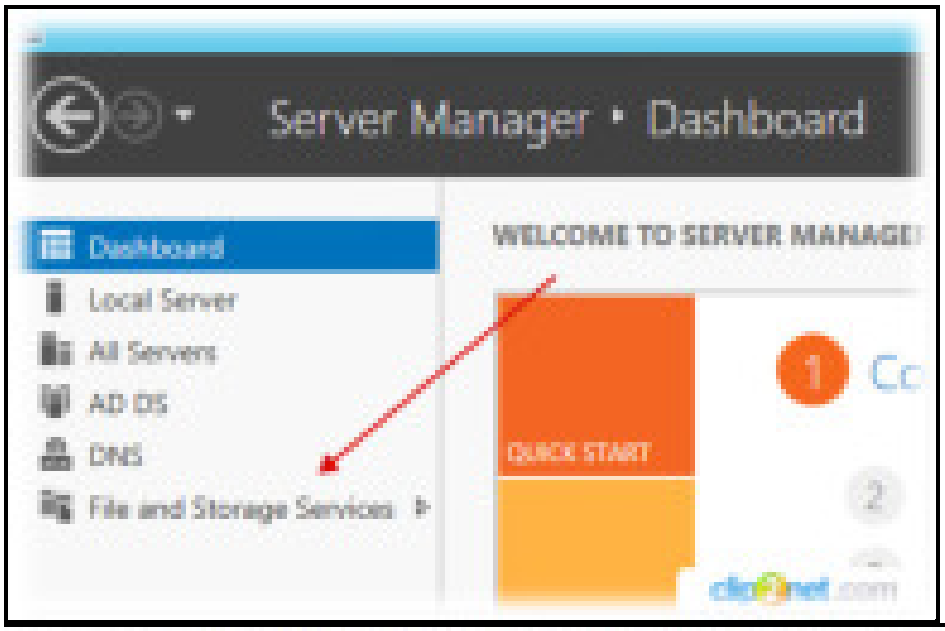


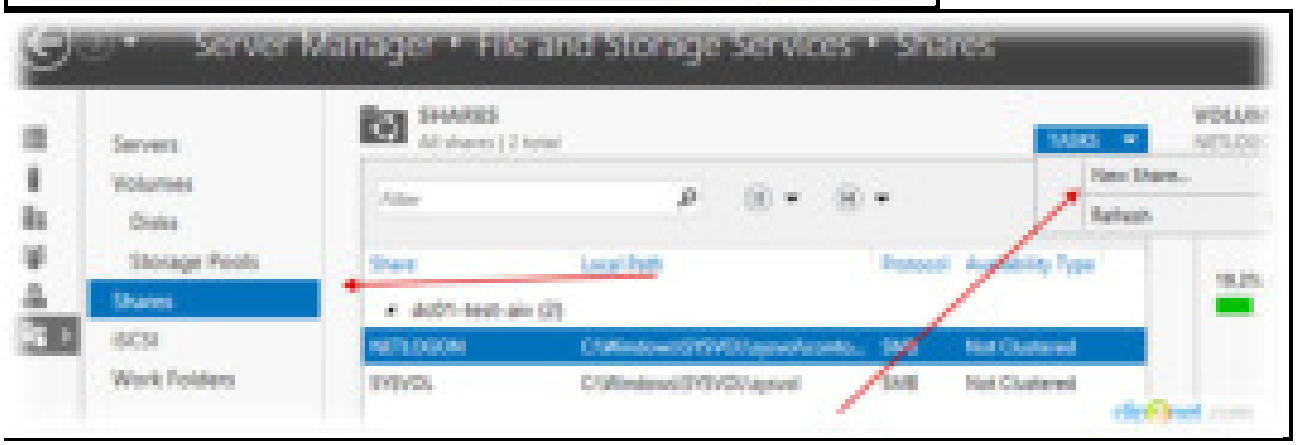

Далее приводим группы в такое соответствие:

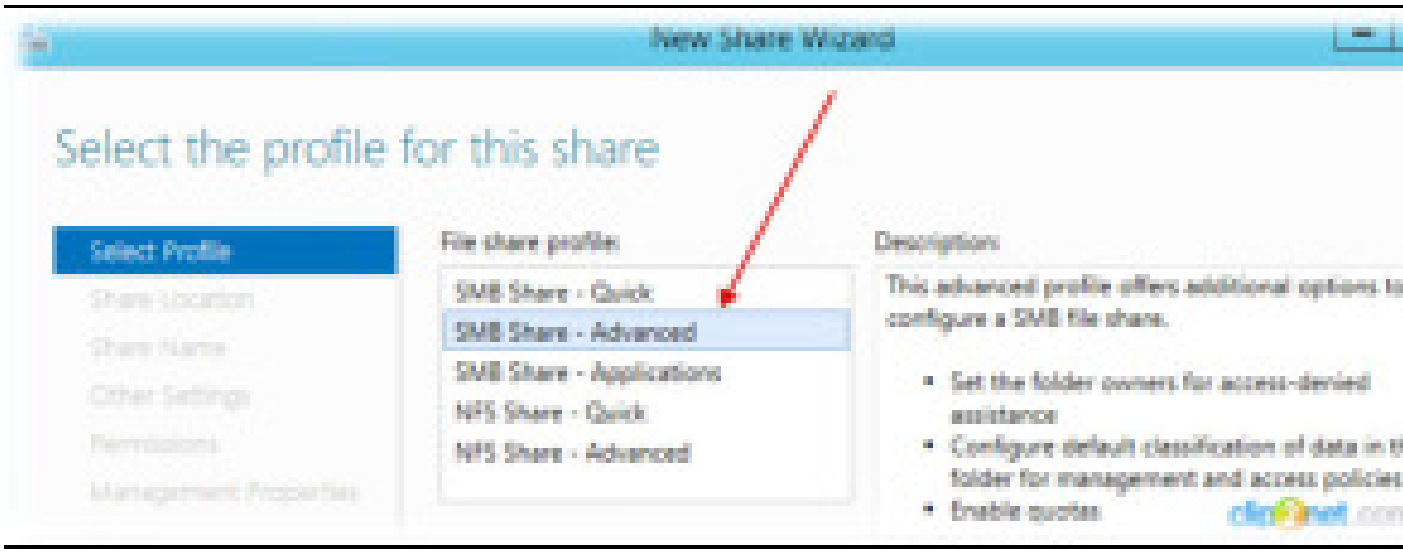



Если группе **Domain Users** не сделать **This folder Only**, то технология ABE не отработает. Плюс мы выключили наследование прав.

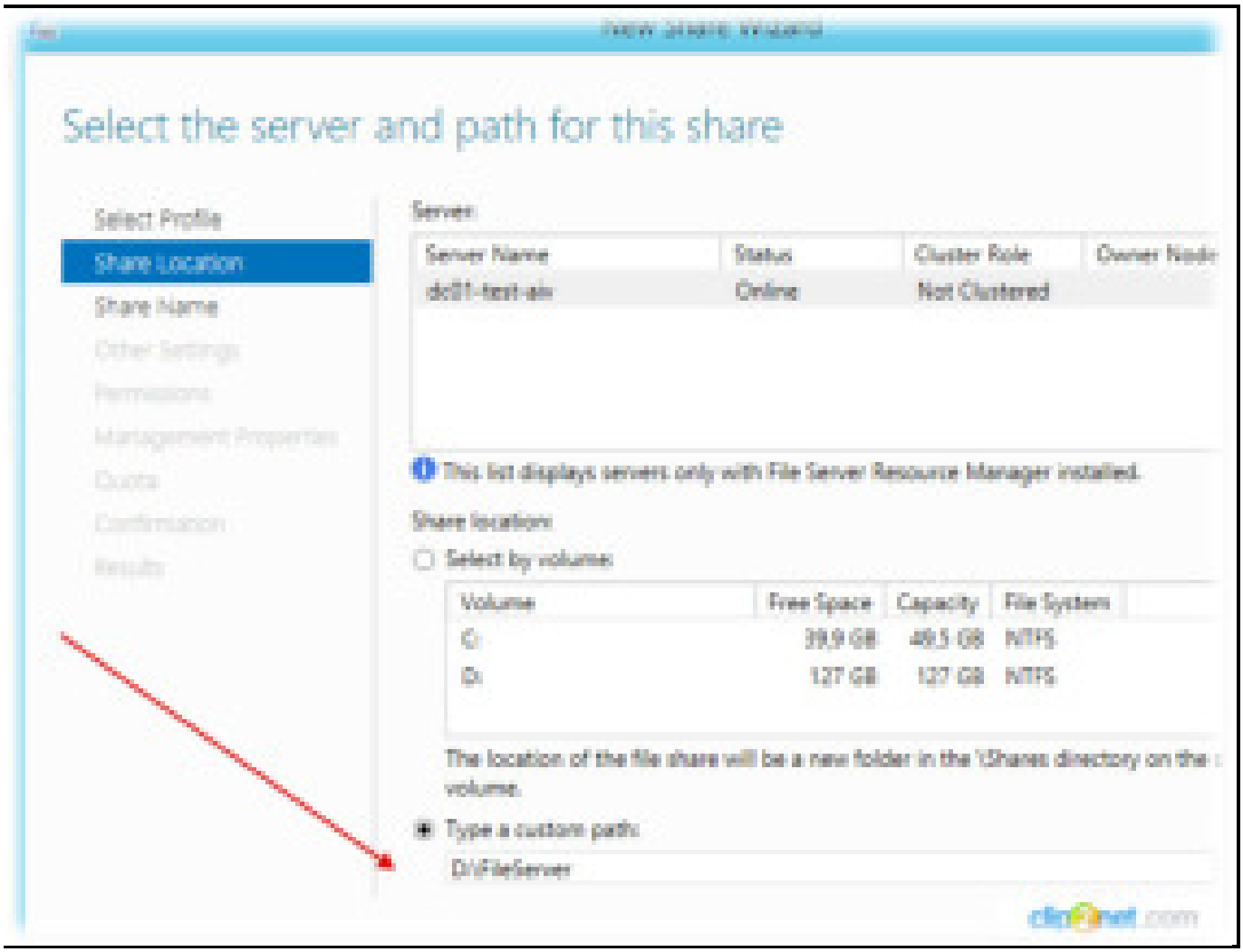
Далее открываем **Server Manager** переходим:



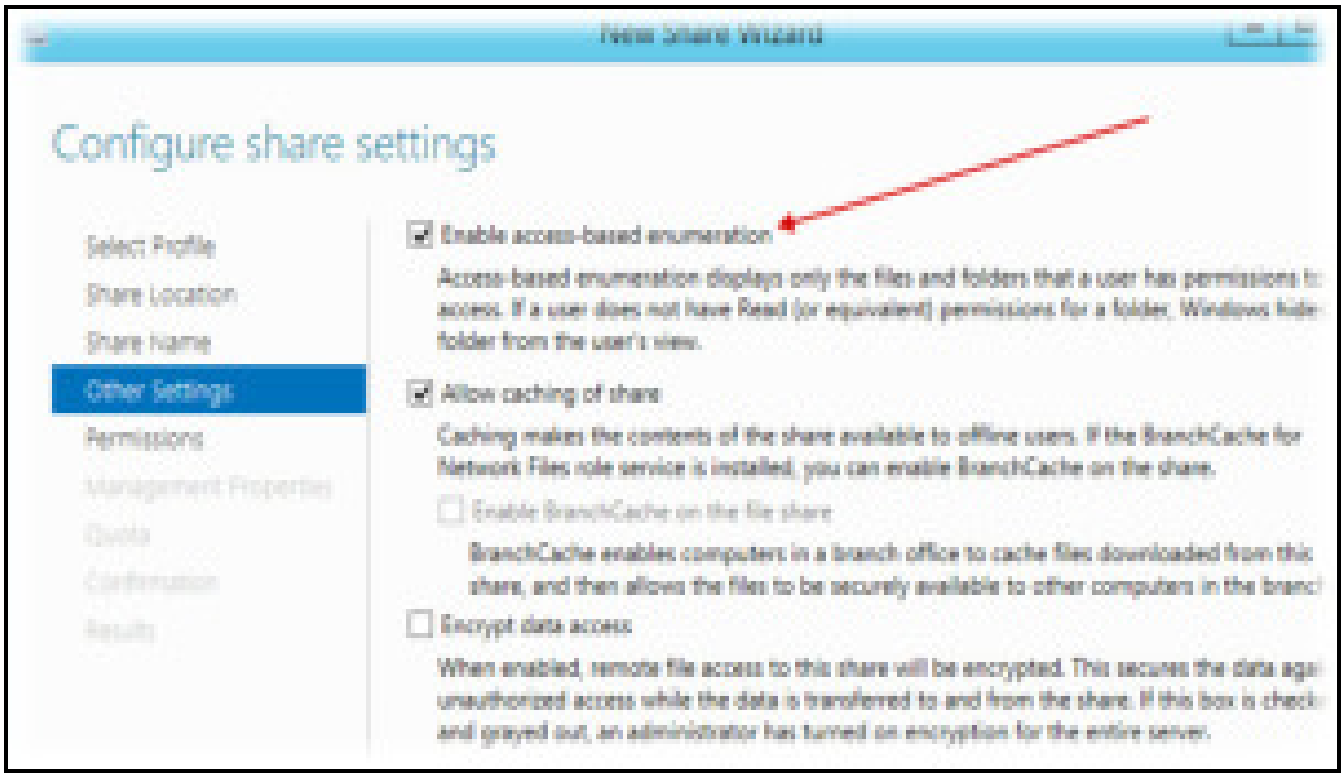




Выбираем нашу папку верхнего уровня:

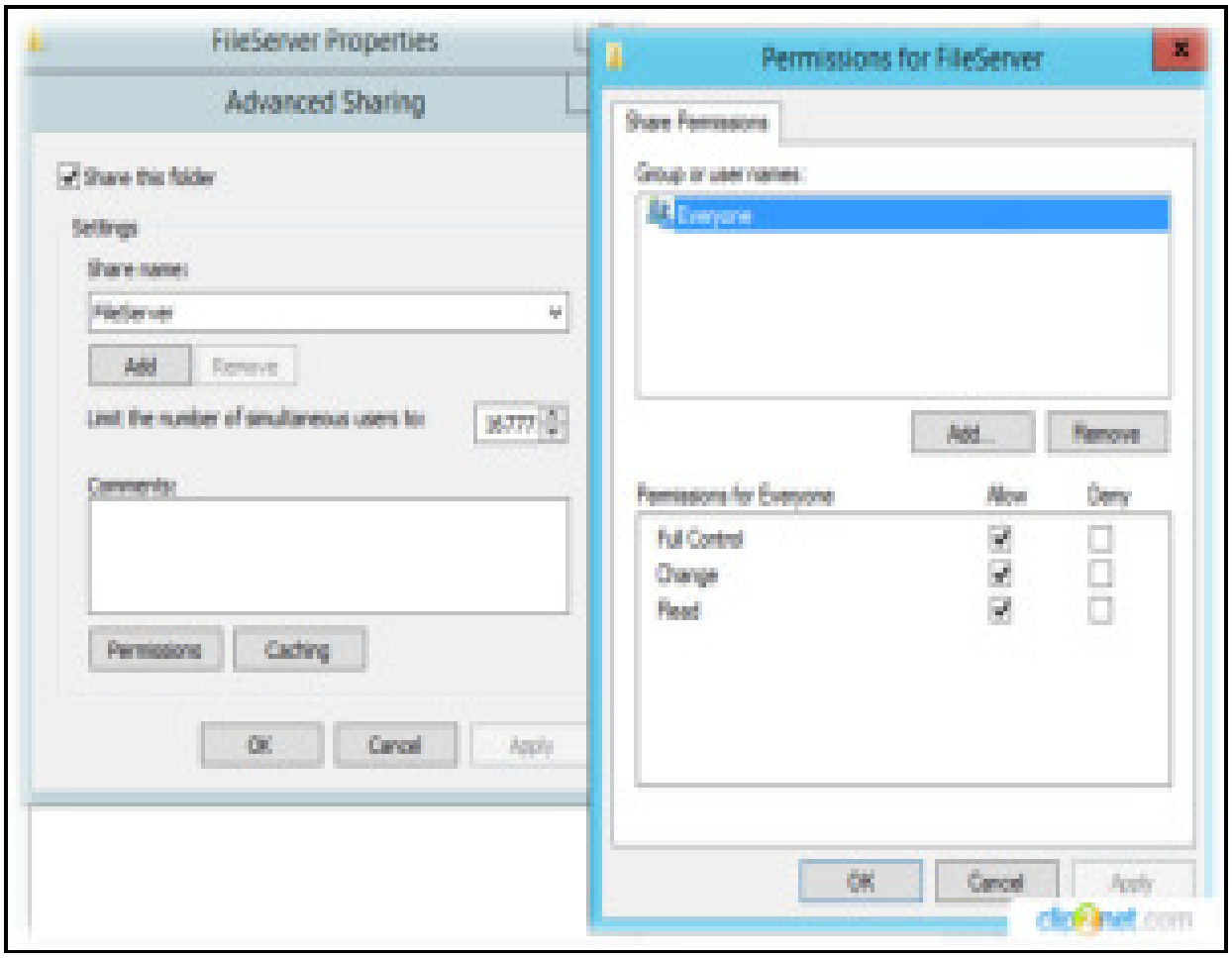



На следующем шаге включаем технологию ABE:




**Permissions** мы уже указали. **Management Properties** и **Quota** мы конфигурировать так же не будем.

В конечном итоге доходим до конца мастера и нажимаем **Create** и получаем такие результаты:



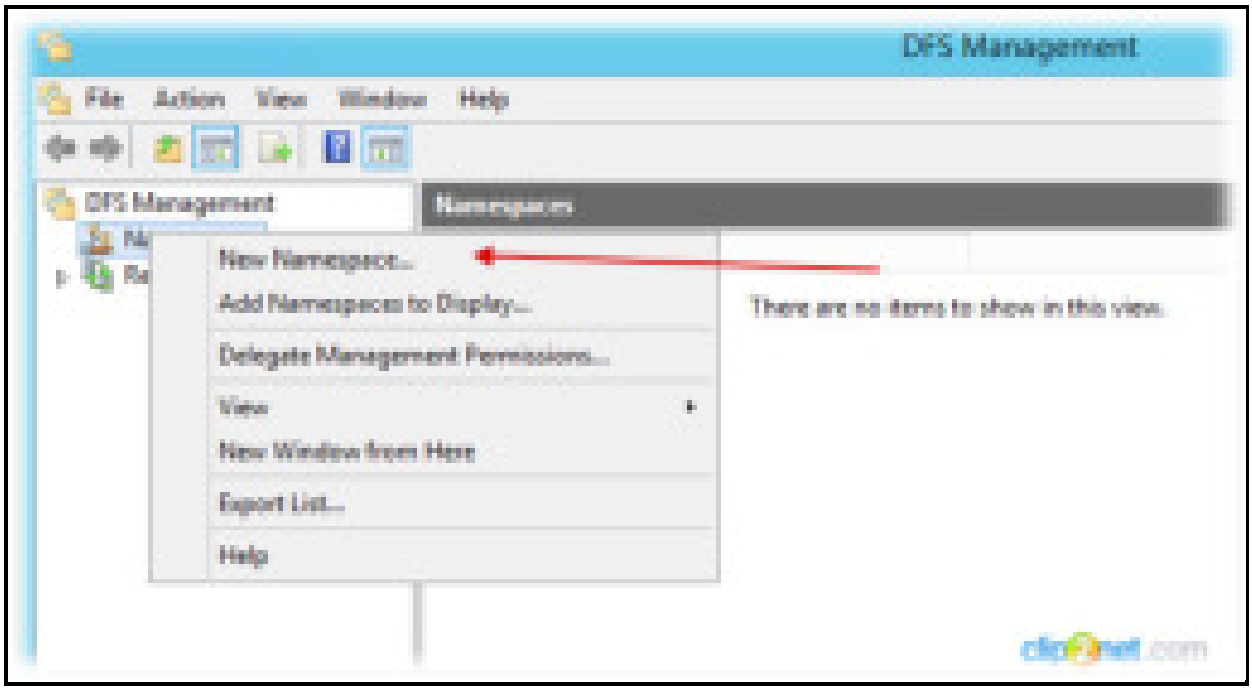

На этом этапе стоит пояснить одну фундаментальную вещь.

Как известно, при доступе к общим ресурсам (сетевым папкам) мы различаем 2 типа прав:

Share Permissions NTFS Rights

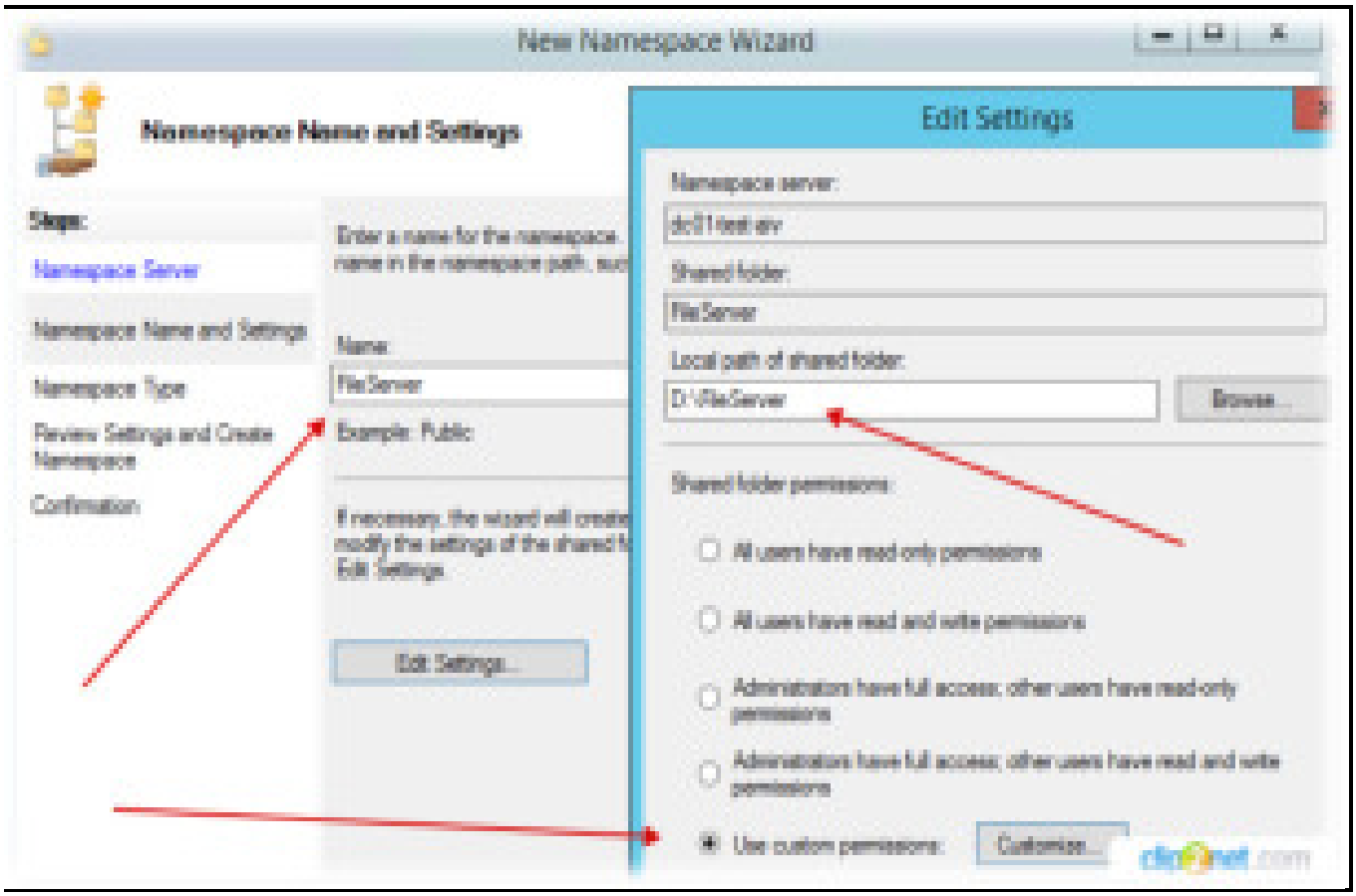
Оба типа прав влияют на результирующие (эффективные) права пользователя при доступе к сетевому ресурсу. В общем смысле эффективные права будут являть собой наиболее ограничивающее разрешение из обоих типов прав. Например, на ресурс установлено право Share Permissions = Read, а NTFS = Full Control, то исходя из наиболее ограничивающего разрешения эффективным будет Read. Если Share Permissions = FullControl, а NTFS = Modify, то эффективным правом для пользователя будет Modify. Вот такая несложная схема. Т.е. там, где прав меньше, те и будут ваши :-) Как известно, эта проблема редко кого касается, т.к. обычно на уровне Share Permissions выдают FullControl на ресурс и дальше уже права регулируют за счёт NTFS

Теперь запускаем **DFS Management** и создадим **New NameSpace…**:

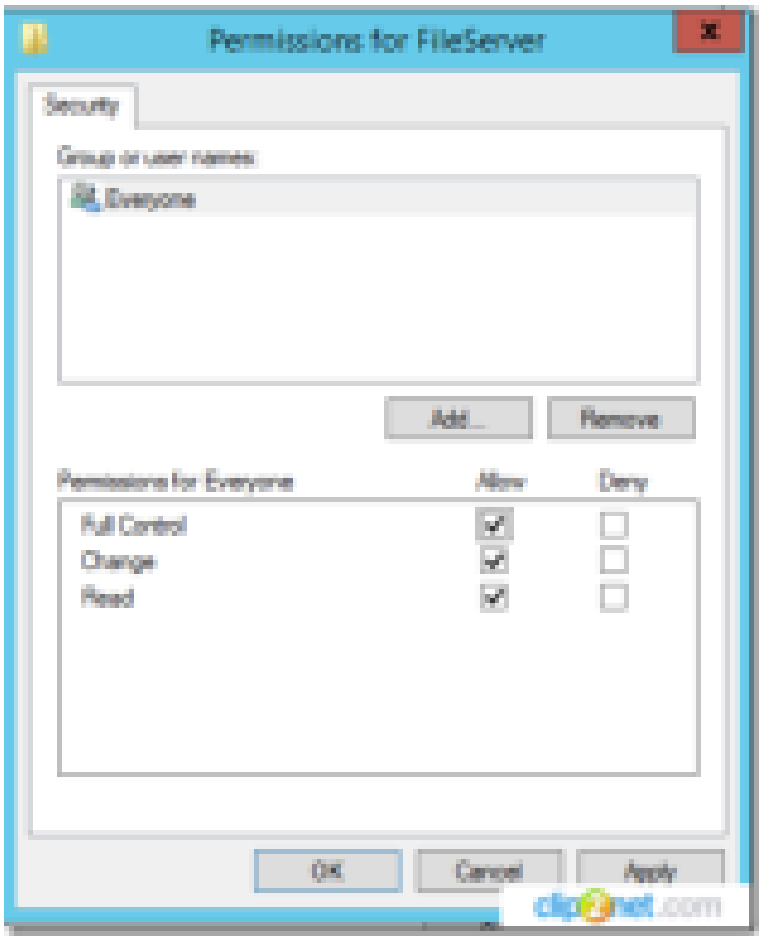



Практически всегда ваш файловый сервер должен “жить” в пространстве DFS. При таком подходе доступ к файловому серверу или серверам осуществляется через единый NameSpace в нашем случае \\Contoso.com\FileServer

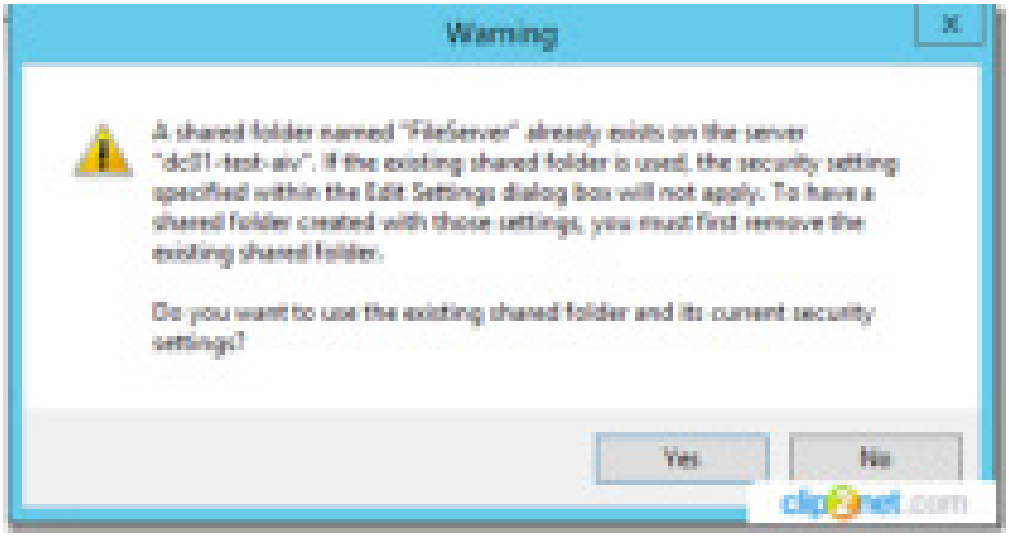
Запускаем мастер вводим **Name**, далее **Edit Settings** и выбираем нашу первую папку в иерархии:




Далее кнопка **Customize** и поправим права иначе мастер нам их сбросит:

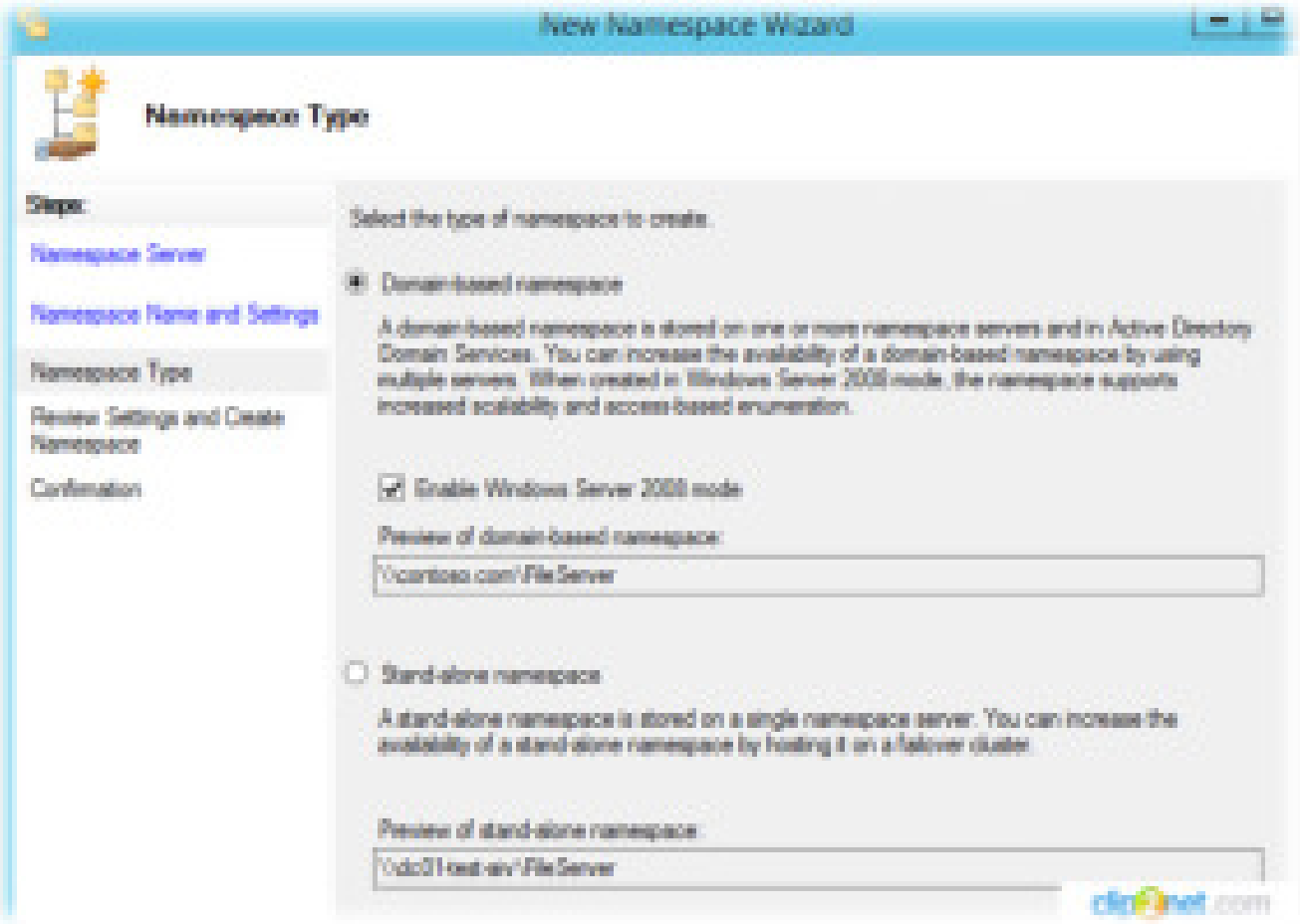



Нажимаем **Next** и получаем предупреждение:

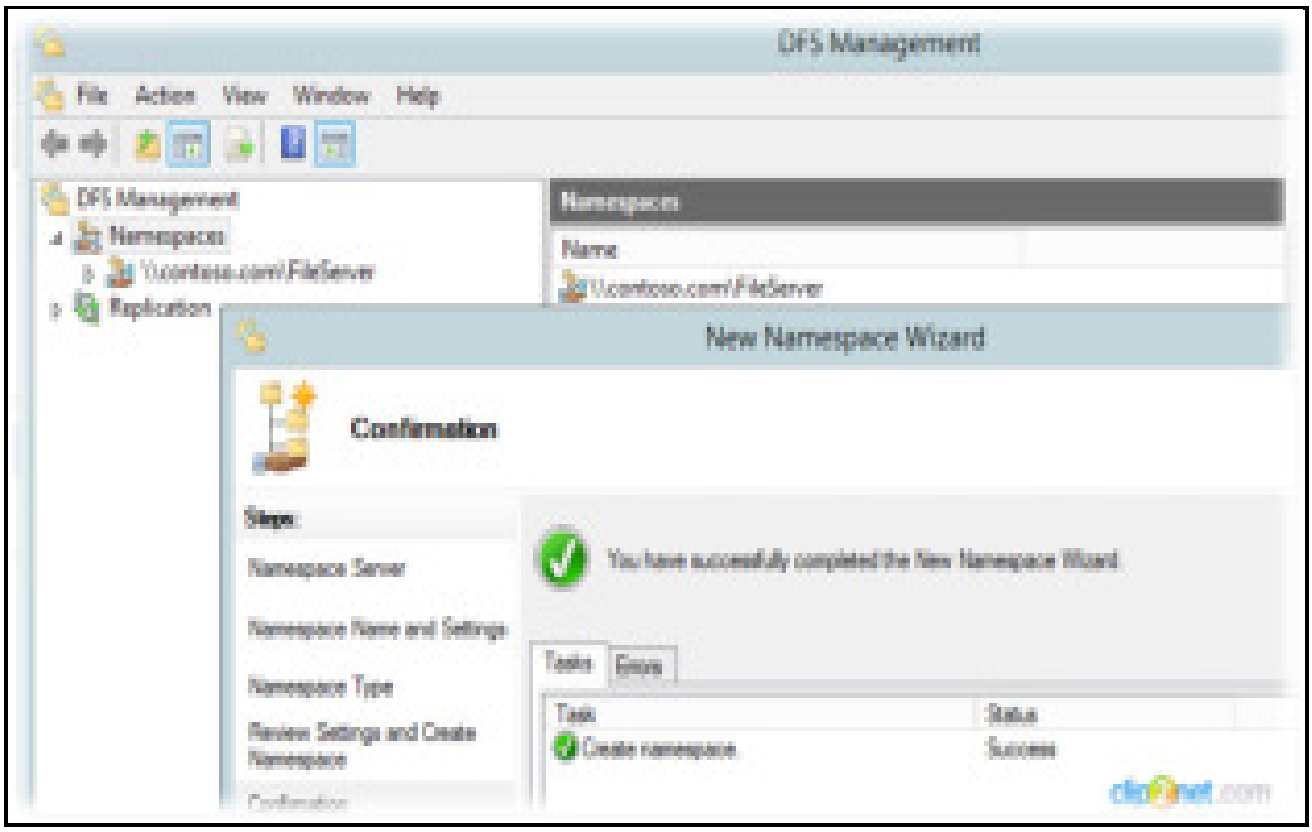



Так как для папки мы уже заранее все настроили отвечаем на вопрос - **Yes**.

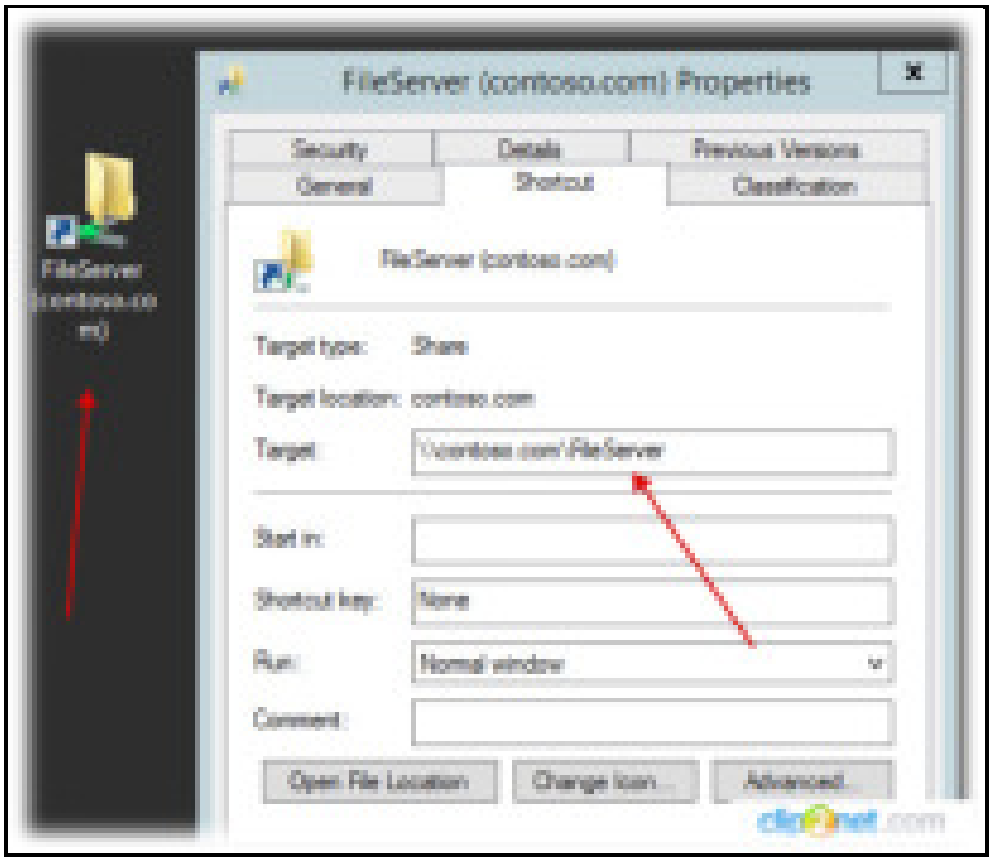
На следующем шаге оставляем все как есть:



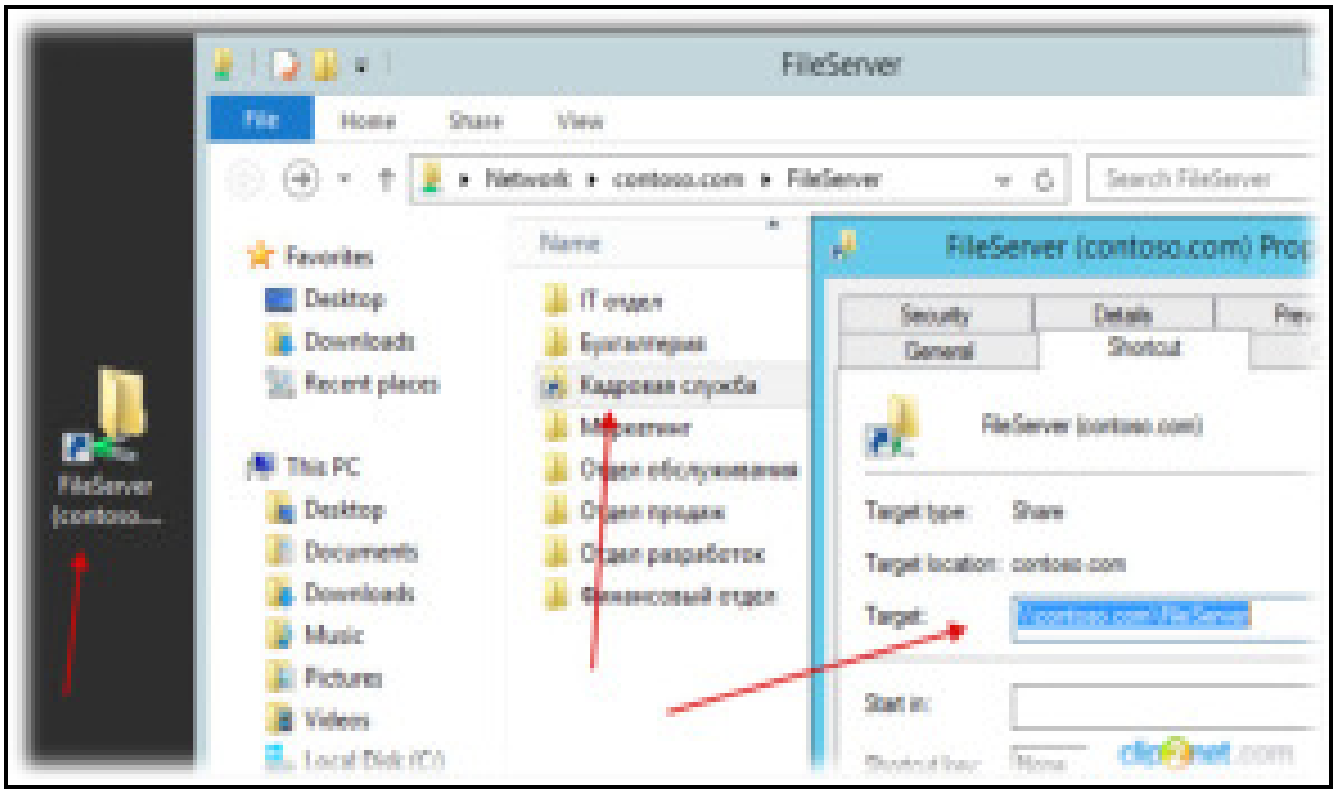

Конечный результат:



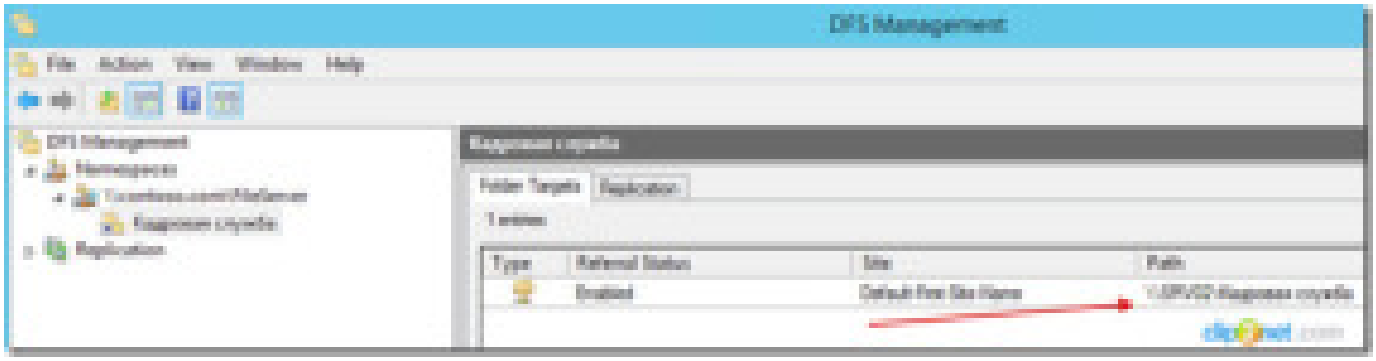
Теперь на клиенте можно создавать такие ярлыки (удобно это делать через групповую политику):




Теперь если мы захотим добавить к нашему файловому серверу еще один сервер и начнем уже там размещать новые данные, то конечный пользователь даже не поймет, что был добавлен второй файловый сервер:

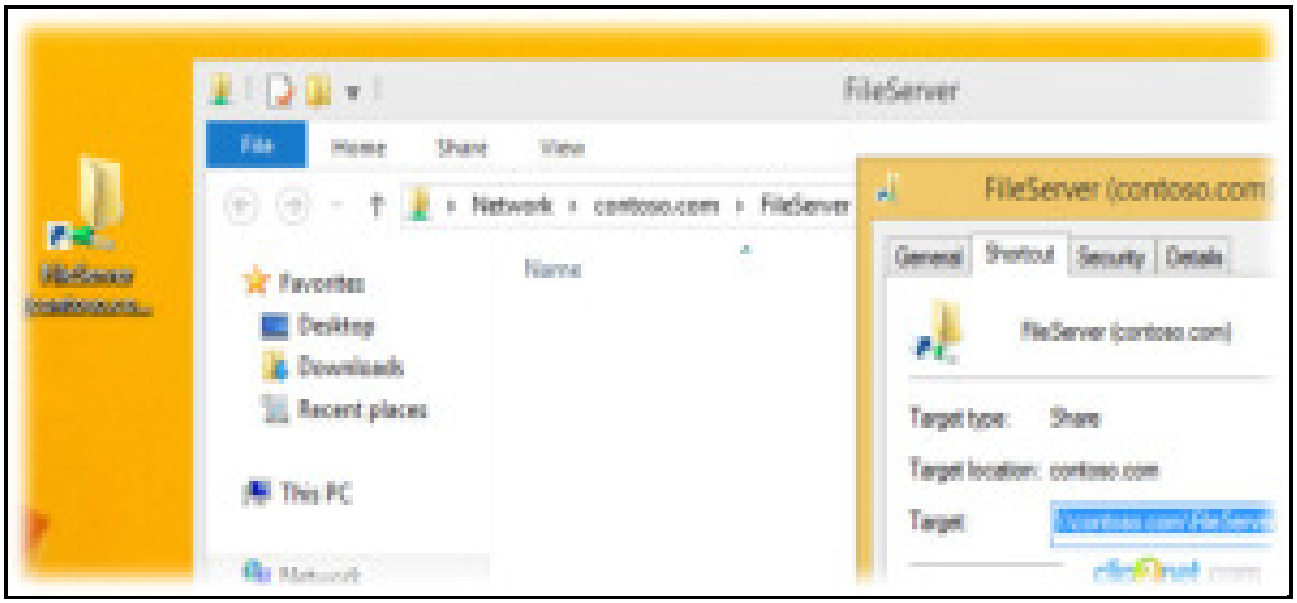



Папка “Кадровая служба” физически располагается на втором файловом сервере, но путь ко всем папкам один **\\Contoso.com\FileServer**:



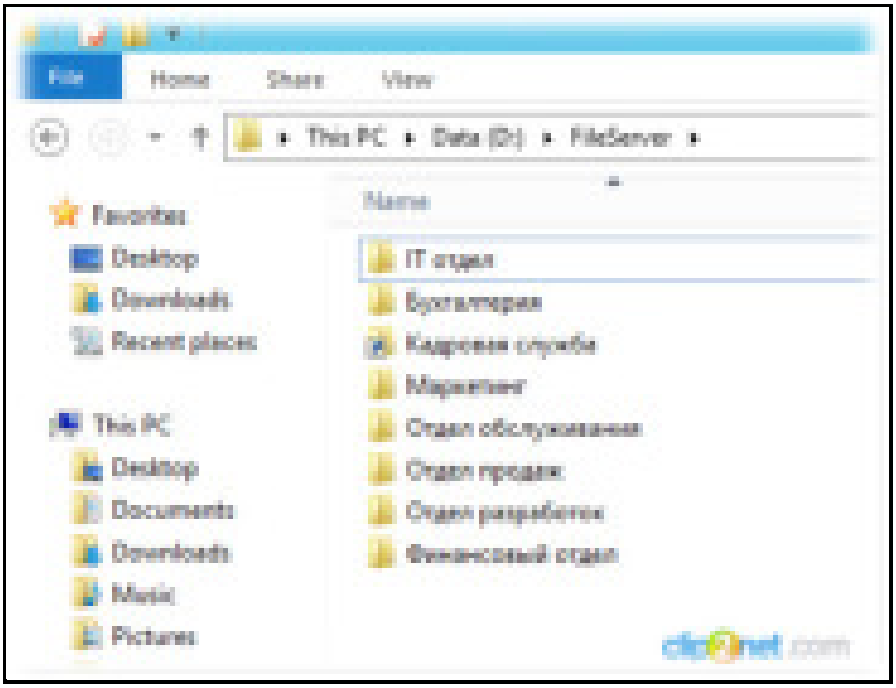

Как это реализовать в этой заметке рассказано не будет.

Если на данном этапе реализации файлового сервера взять обычного пользователя и попытаться открыть наш файл сервер, то никаких файлов и папок мы не увидим, хотя они там есть:




Отрабатывает технология **Access-based enumeration**:

Скрин со стороны сервера:




Нашему тестовому вновь созданному пользователю не предоставлено по умолчанию никаких прав, а мы помним если задействована технология ABE и пользователь не имеет хотя бы права **Read** на файл или папку то ему этот файл или папка не видны.

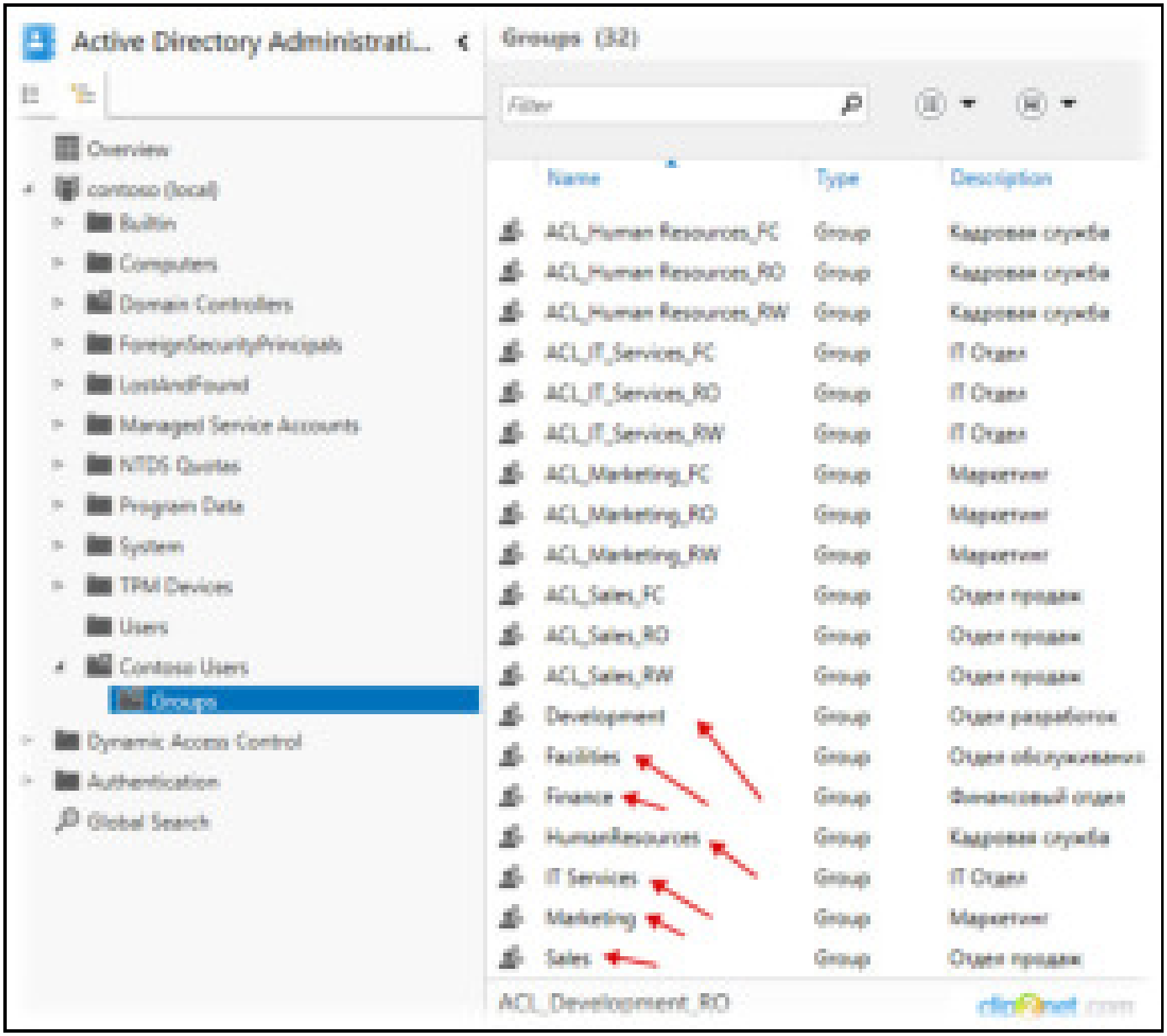
Пришло время создать ролевые группы, вначале этой заметке я уже приводил цитату из книги, но хочу добавить еще одну:

Цитата из книги “Эффективное Администрирование. Windows Server 2008.” Автор: Холме Дэн:

Ролевые группы определяют набор компьютеров или пользователей на основе сходства, которым обладают объекты в бизнесе, их территориального размещения, подразделений, функций, трудового стажа или статуса, команд, проектов или любых других связанных с бизнесом характеристик

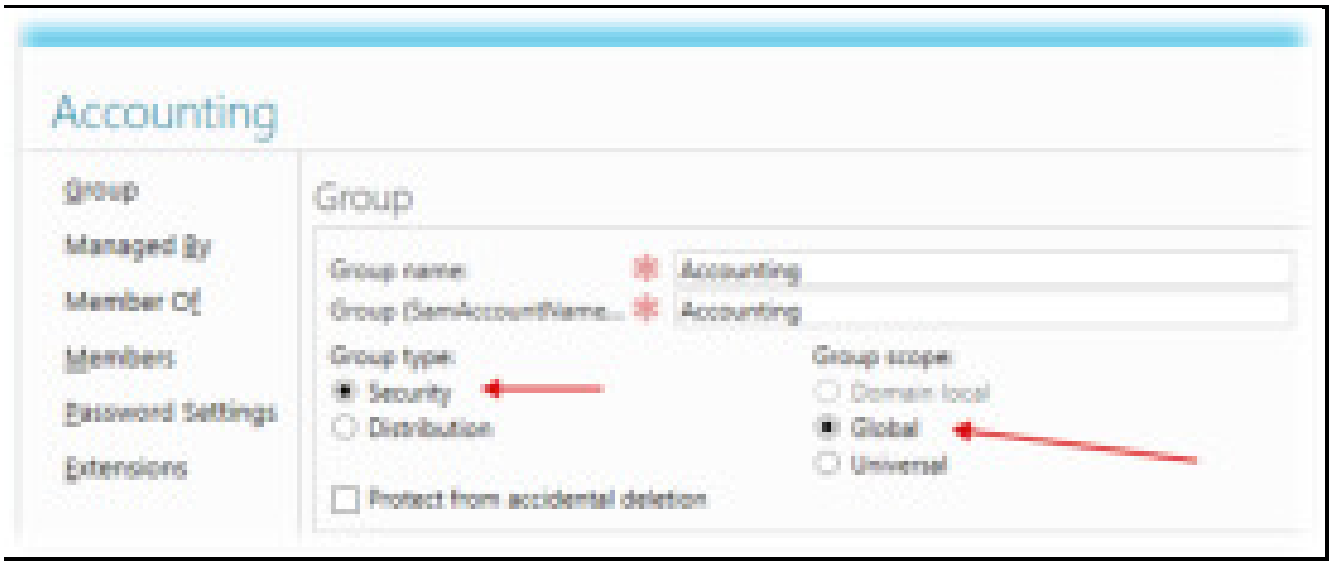
Создали типичную структуру отделов-подразделений компании (предыдущий скриншот).

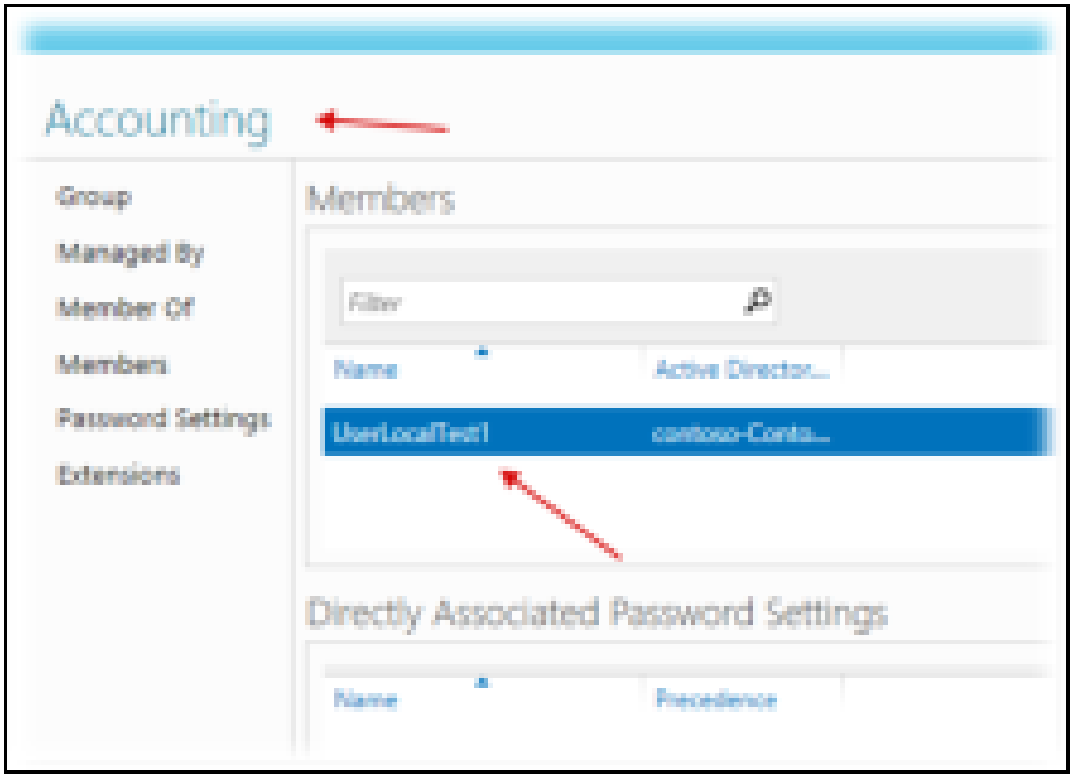
На основании этой структуры создадим первые ролевые группы (отмечены стрелочками):



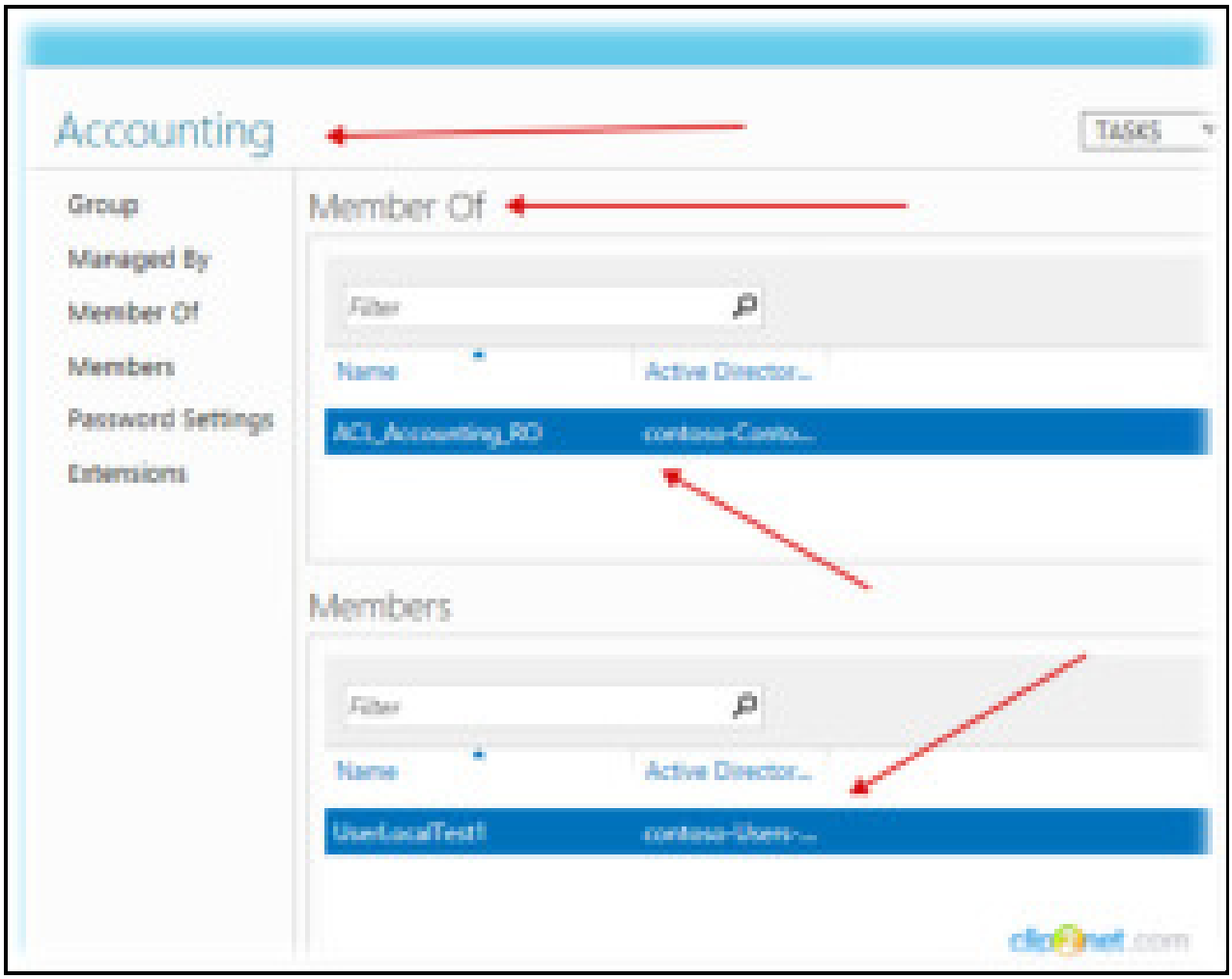
Так как  в AD DS не рекомендовано использовать русский язык кроме поля Description в названиях групп мы используем английские аналоги, но для удобства в поле Description можно вписать русское название.

**Имя_Группы** к примеру **Accounting** (ролевая группа) – глобальная группа в этот тип групп у нас входят пользователи.




Группа **Accounting** входит в состав (Member Of) группы **ACL_Accounting_FC или RW или RO**




**<u>Еще раз:</u>**

**User –> Accounting –> ACL_Accounting_RO (Read Only) –> Папка Бухгалтерии**

**User –> Accounting –> ACL_Accounting_RW (Read and Write) –> Папка Бухгалтерии**

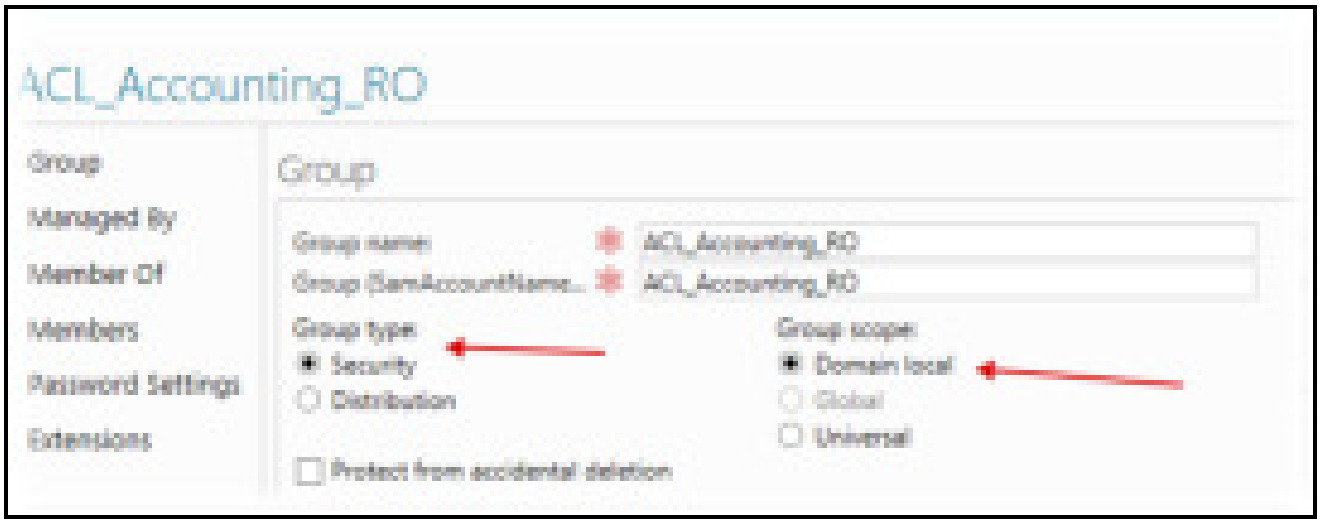
**User –> Accounting –> ACL_Accounting_FC (Full Control) –> Папка Бухгалтерии**

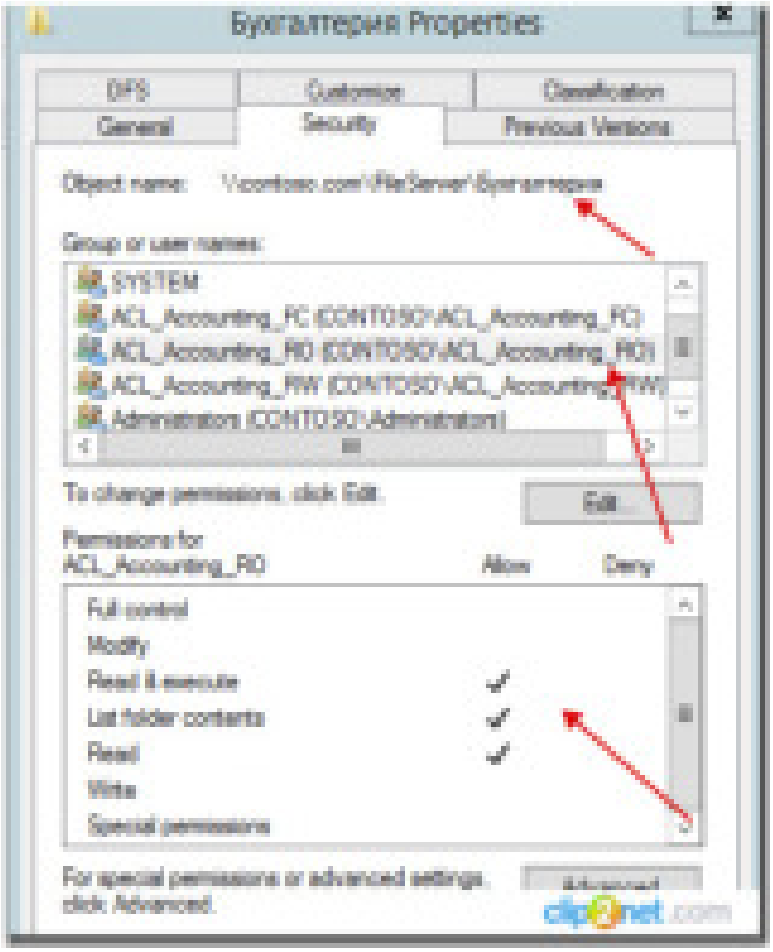
**ACL_Имя_Группы_FC или RW или RO -** это доменно локальная группа которая регулируют уровень доступа к файлам и папкам.

**<u>Теперь раздаем разрешения:</u>**

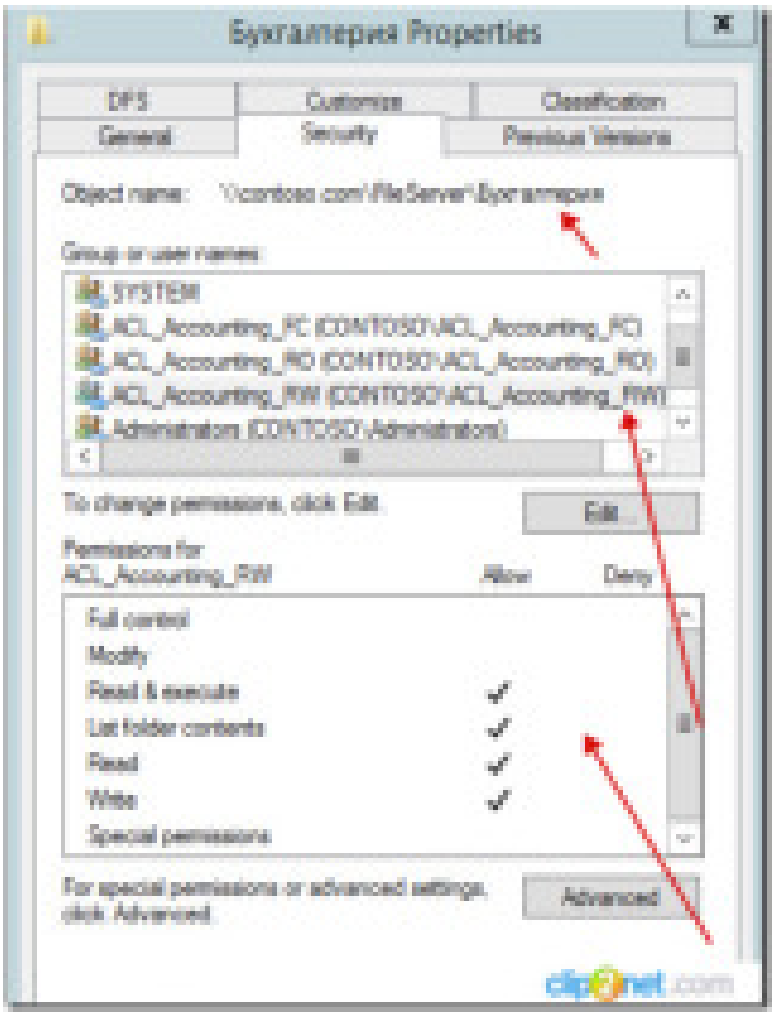
**ACL_Accounting_RO** – доменно локальная группа. NTFS разрешения на папку или файл **Read Only**

**<u>Доменно локальная группа это:</u>**

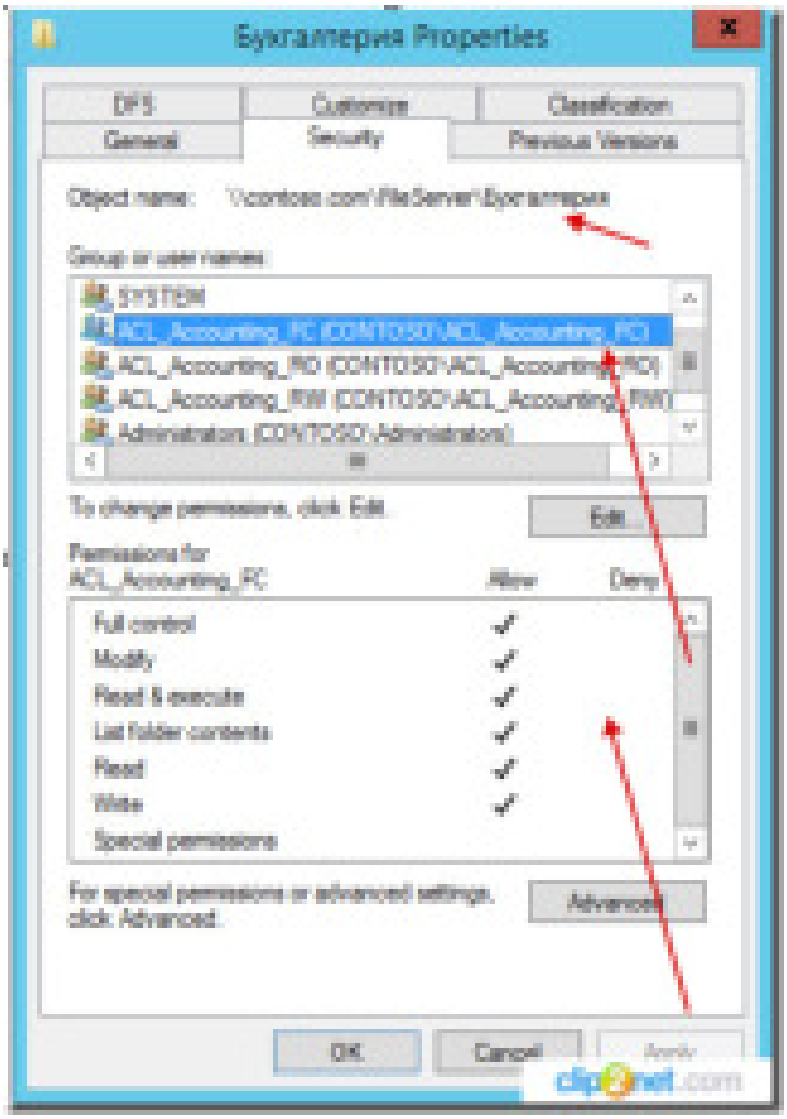



**ACL_Accounting_RW** - доменно локальная группа. NTFS разрешения на папку или файл **Read and Write**




**ACL_Accounting_FC** - доменно локальная группа. NTFS разрешения на папку или файл **Full Control**




**<u>Сценарий 1:</u>**

Предоставить право на чтение и запись в папку Бухгалтерия пользователю User2.

”Вложить” пользователя User2 в группу **ACL_Accounting_RW** - это решит поставленную задачу, но противоречит нашей логике ролевого доступа.

“Вложить” пользователя User2 в ролевую группу **Accounting,** в свою очередь группа **Accounting** должна входить в группу доступа **ACL_Accounting_RW –** это решит поставленную задачу, но при таком подходе встает вопрос, а если части сотрудников отдела Бухгалтерия нужно дать доступ типа **Read Only** или **Full Control** на папку Бухгалтерия? В какую ролевую группу мы должны включить этого сотрудника?

Создаем ролевую группу **Accounting_RO** в которую будет входить наш пользователь, а сама группа будет входит в группу доступа **ACL_Accounting_RO**

Можно сразу пойти по такому пути и создавать группы по такой логике:

**Accounting_FC --> ACL_Accounting_FC**

**Accounting_RW --> ACL_Accounting_RW**

**Accounting_RO --> ACL_Accounting_RO**

Такой подход требует больших первоначальных трудозатрат, но когда дело касается практики он себя оправдает.

**Вернемся к нашему вопросу:**

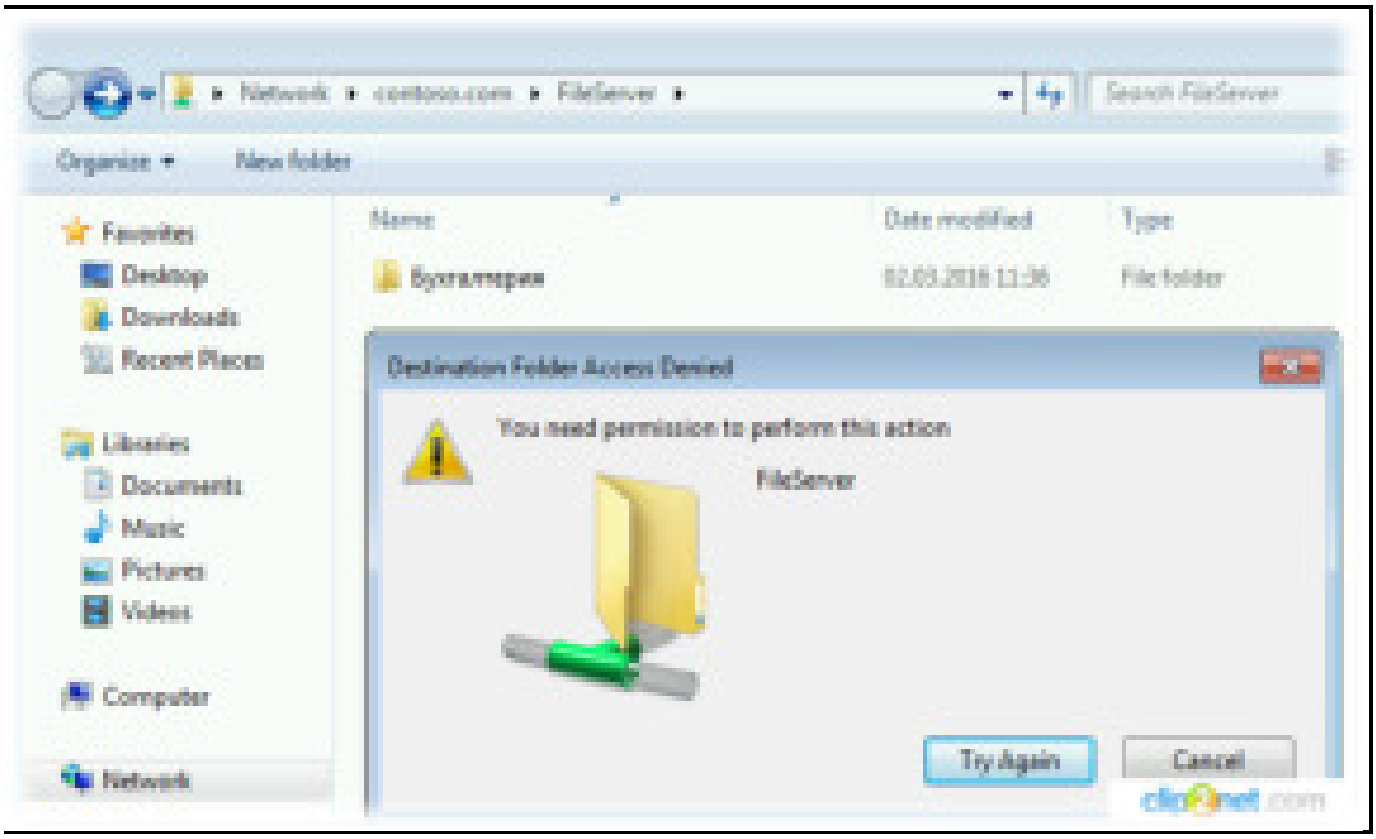
Предоставить права на чтение и запись в папку Бухгалтерия пользователю User2.

**Решение:**

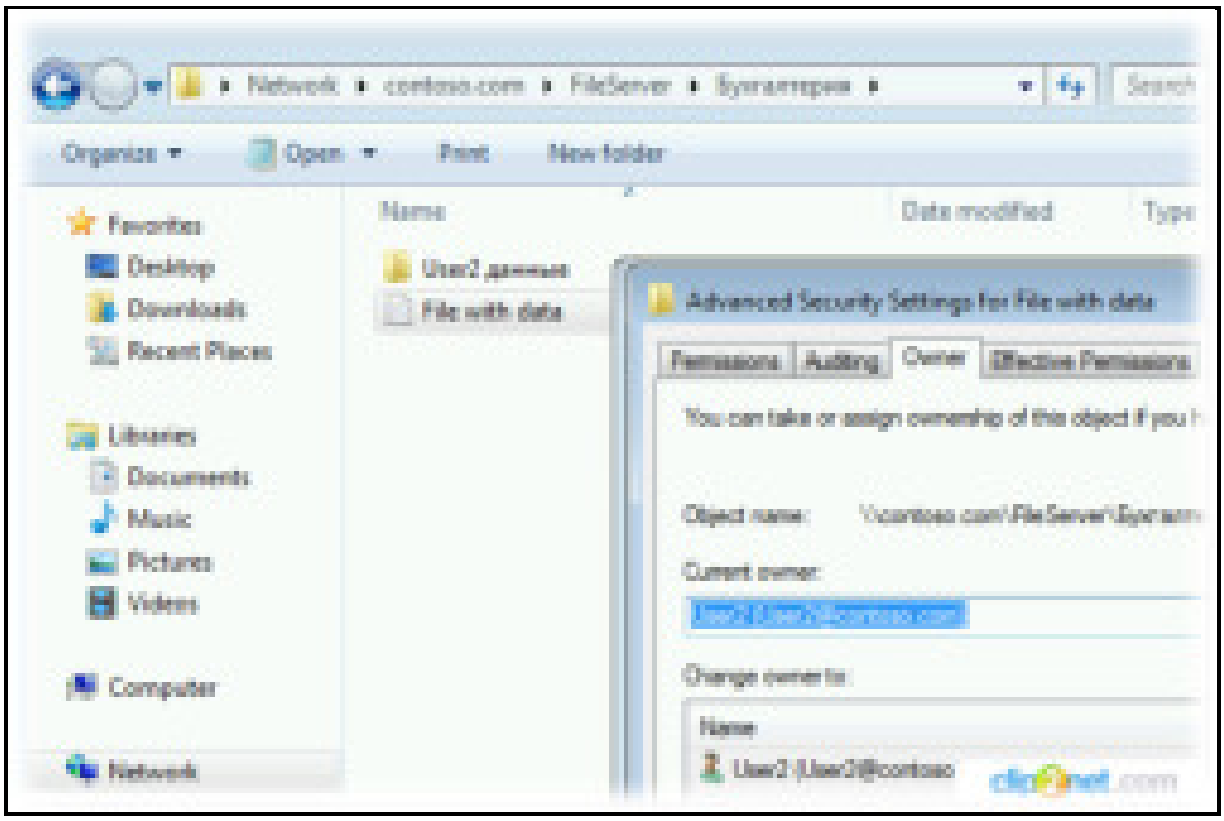
Ответственный инженер добавит пользователя User2 в ролевую группу **Accounting_RW.**

**Результат:**

В итоге пользователь видит только свою папку. Так же в корневой папке он не имеет никаких прав:




Идем в папку бухгалтерия и видим, что уже в папке бухгалтерия пользователь User2 имеет права **Read and Write**:



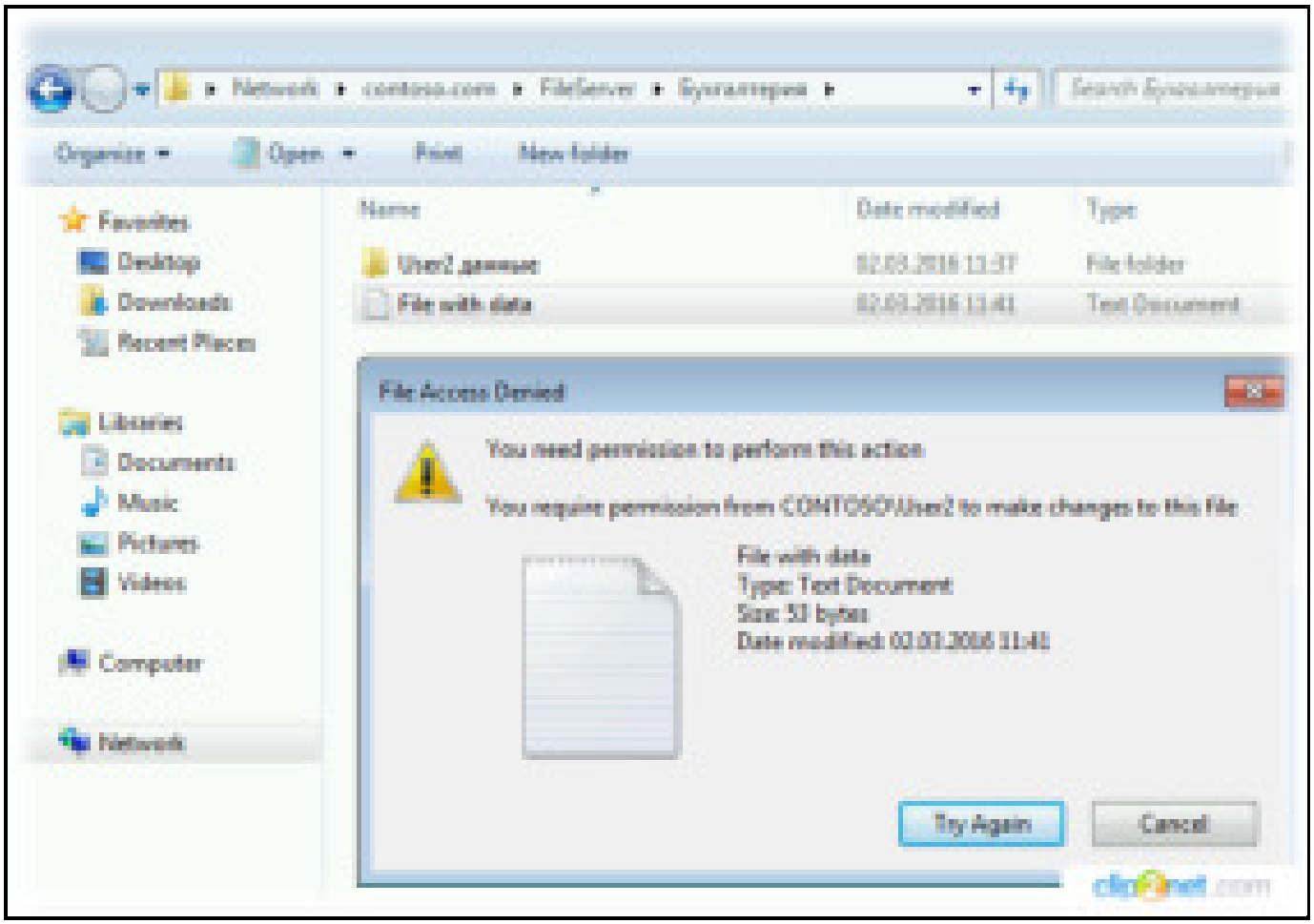
**<u>Сценарий 2:</u>**

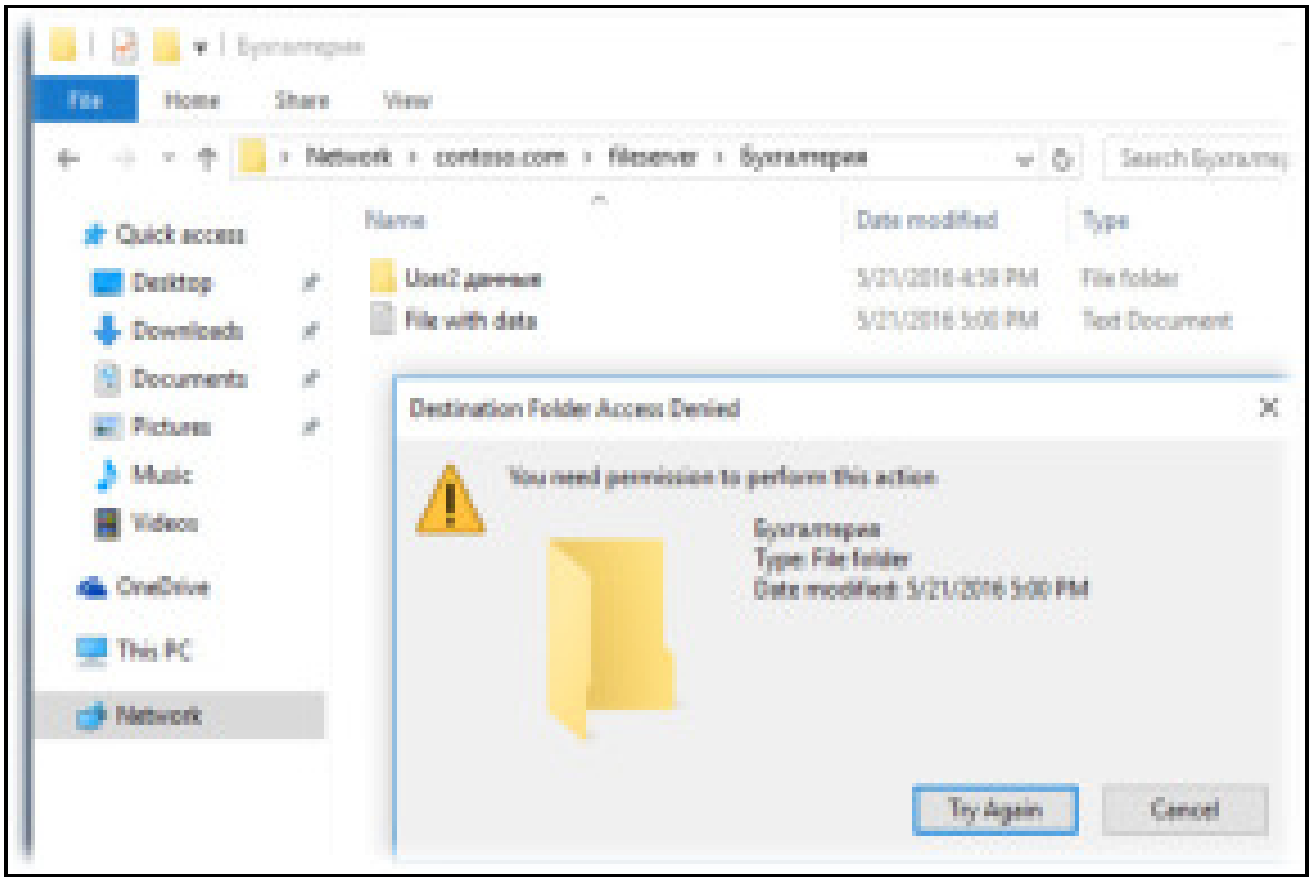
Предоставить права **Read Only** в папку Бухгалтерия пользователю User3.

**<u>Решение:</u>**

Ответственный инженер добавит пользователя User3 в ролевую группу **Accounting_RO**

Так же как и User2, User3 увидит на файловом сервере только папку Бухгалтерия, но уже записать и удалить какие либо файлы не сможет:


Network
contoso.com
FileServer
Бухгалтерия
Organize
Open
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
User2 данные
File folder
File with data
Text Document
File Access Denied
You need permission to perform this action
You require permission from CONTOSO\User2 to make changes to this file.
File with data
Type: Text Document
Size: 53 bytes
Date modified: 02.03.2016 11:41
Try Again
Cancel


Бухгалтерия
File
Home
Share
View
Network
contoso.com
fileserver
Бухгалтерия
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
User2 данные
File folder
File with data
Text Document
Destination Folder Access Denied
You need permission to perform this action
Бухгалтерия
Type: File folder
Date modified: 5/21/2016 5:00 PM
Try Again
Cancel

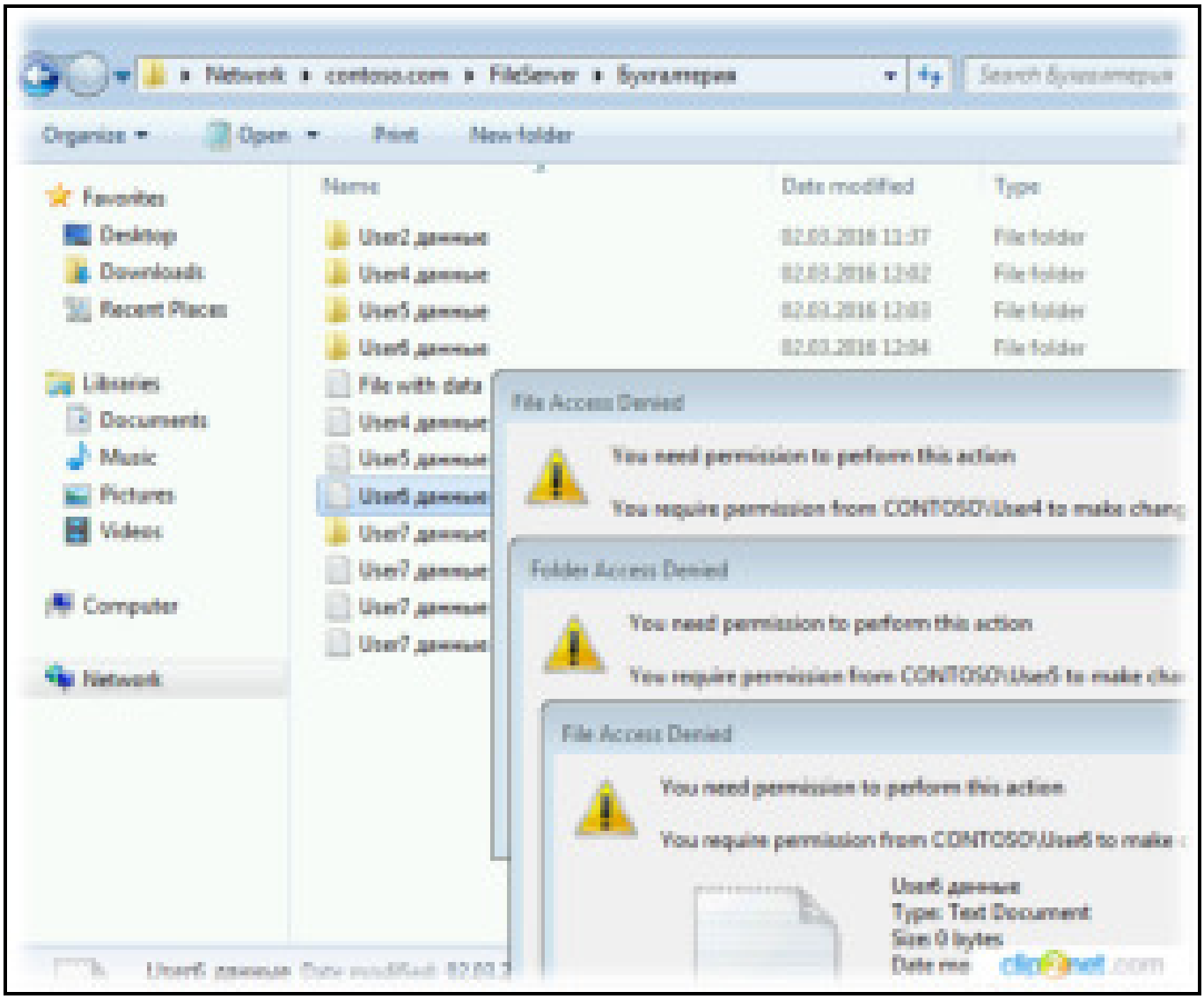
**Сценарий 3:**

Предоставить права **Read and Write** в папку Бухгалтерия для User7 , но при увольнении User7 захочет удалить все файлы из папки Бухгалтерия.

**Решение:**

Ответственный инженер добавит пользователя User7 в ролевую группу **Accounting_RW.**

По легенде в папку бухгалтерия складывают свою данные еще четыре бухгалтера – это User2,4,5,6, но User7 при увольнении решил удалить все бухгалтерские документы, к счастью удаление файлов у которых пользователь не является владельцем удалить нельзя.



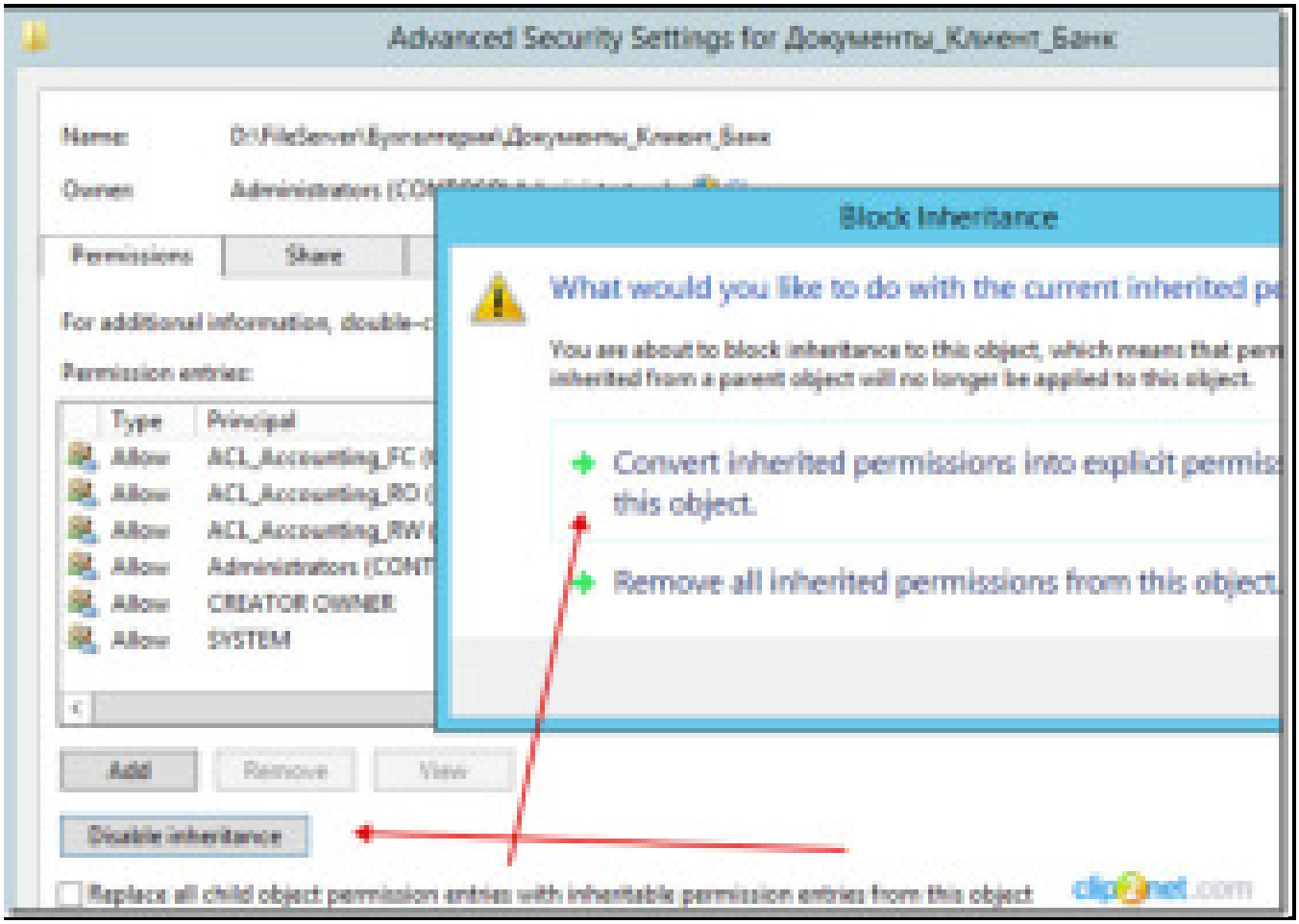

Но если у пользователя права **Full Control**, то в конечной папке он может делать все что ему вздумается.

**Сценарий 4:**

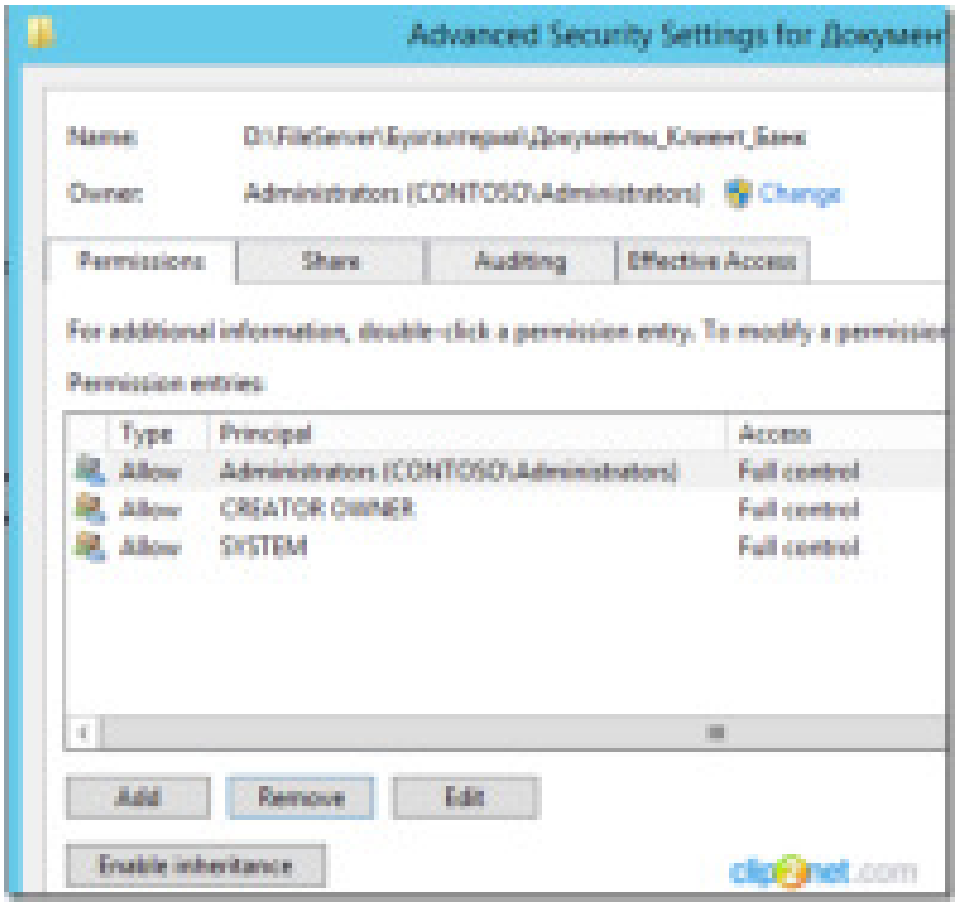
В папке Бухгалтерия должна быть создана подпапка **Документы_Клиент_Банк**. Эта папка будет использовать ответственными сотрудниками для хранения документов экспортируемые из клиент банков. Эту папку должны видеть только ответственные сотрудники.

**Решение:**

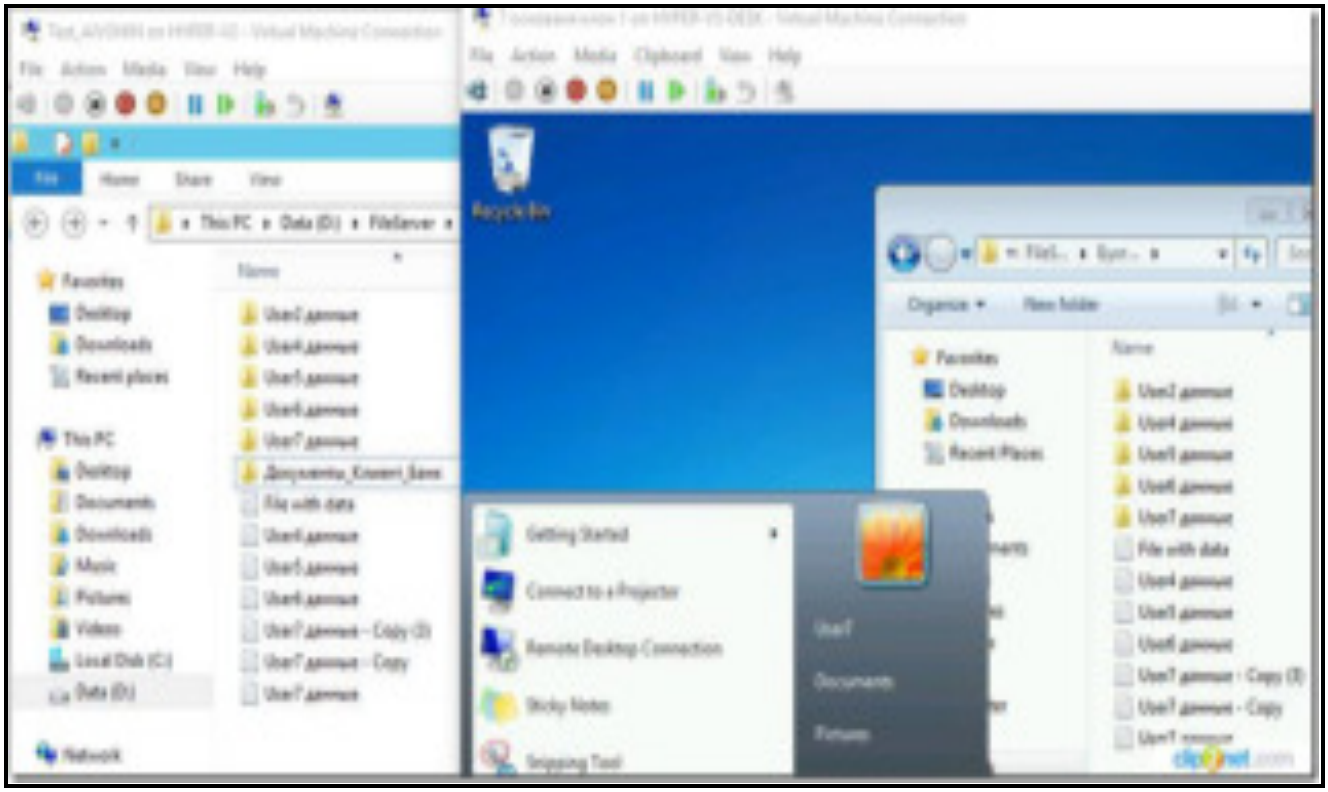
Первым делом выключаем наследовании этой подпапки Документы_Клиент_Банк:



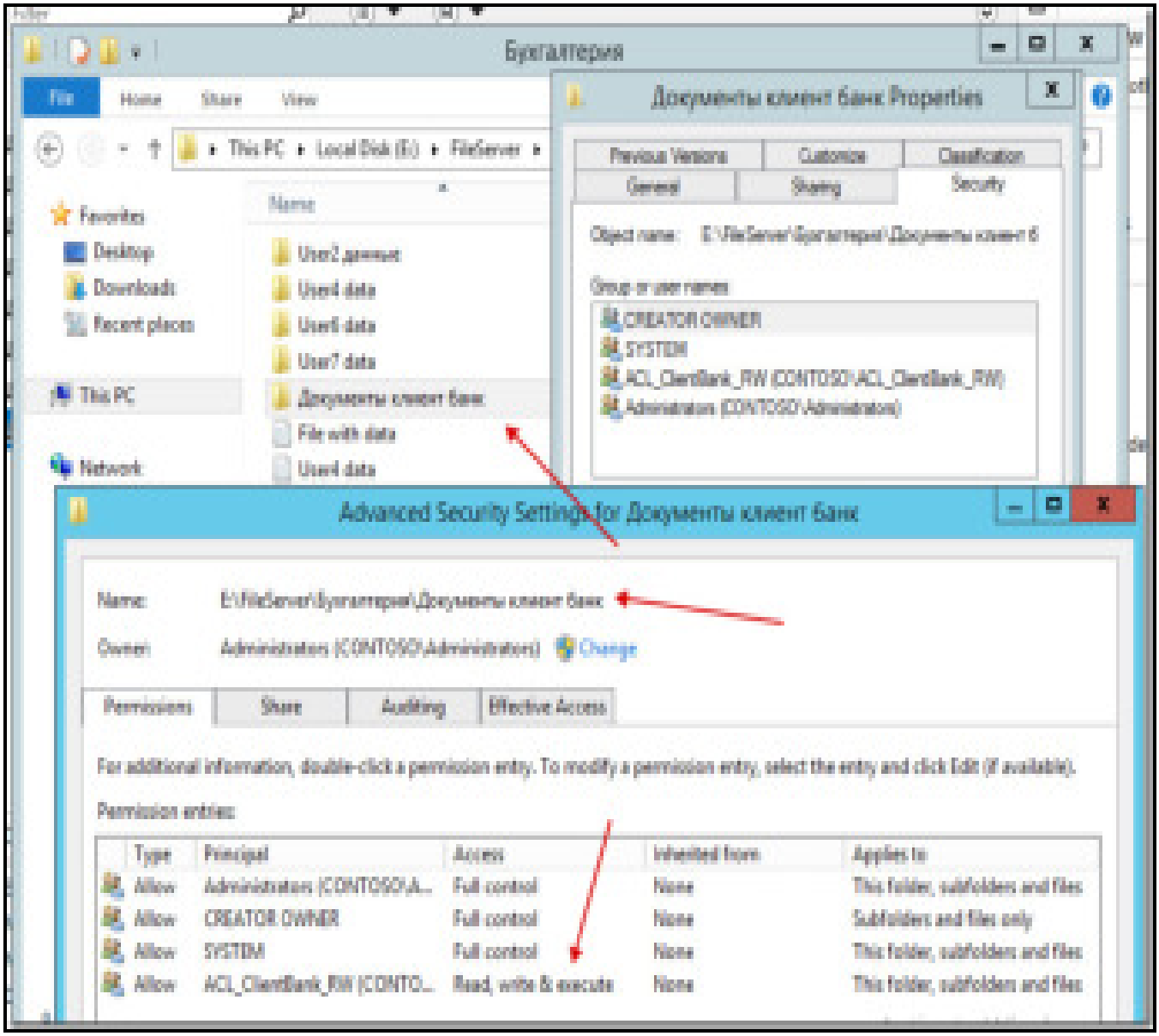

Удаляем все унаследованные группы кроме:



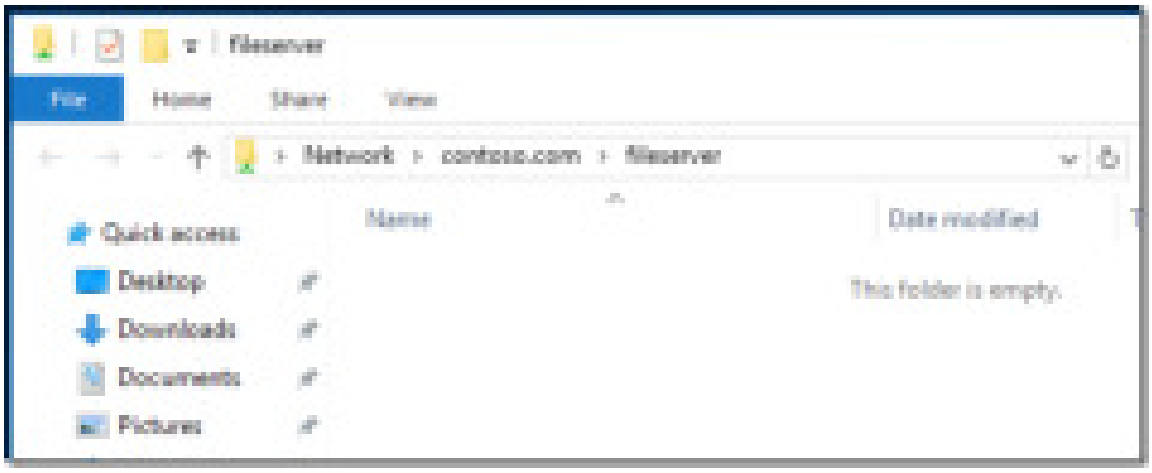

Итог, на файловом сервере папка есть, но пользователь с правами которая предоставляет ролевая группа **Accounting_RW** или **Accounting_FC** или **Accounting_RO** ее не видит:



Дальше создаем ролевую группу к примеру **ClientBank_RW** (глобальаня) –> **ALC_ClientBank_RW** (доменно локальная) и назначаем разрешения:



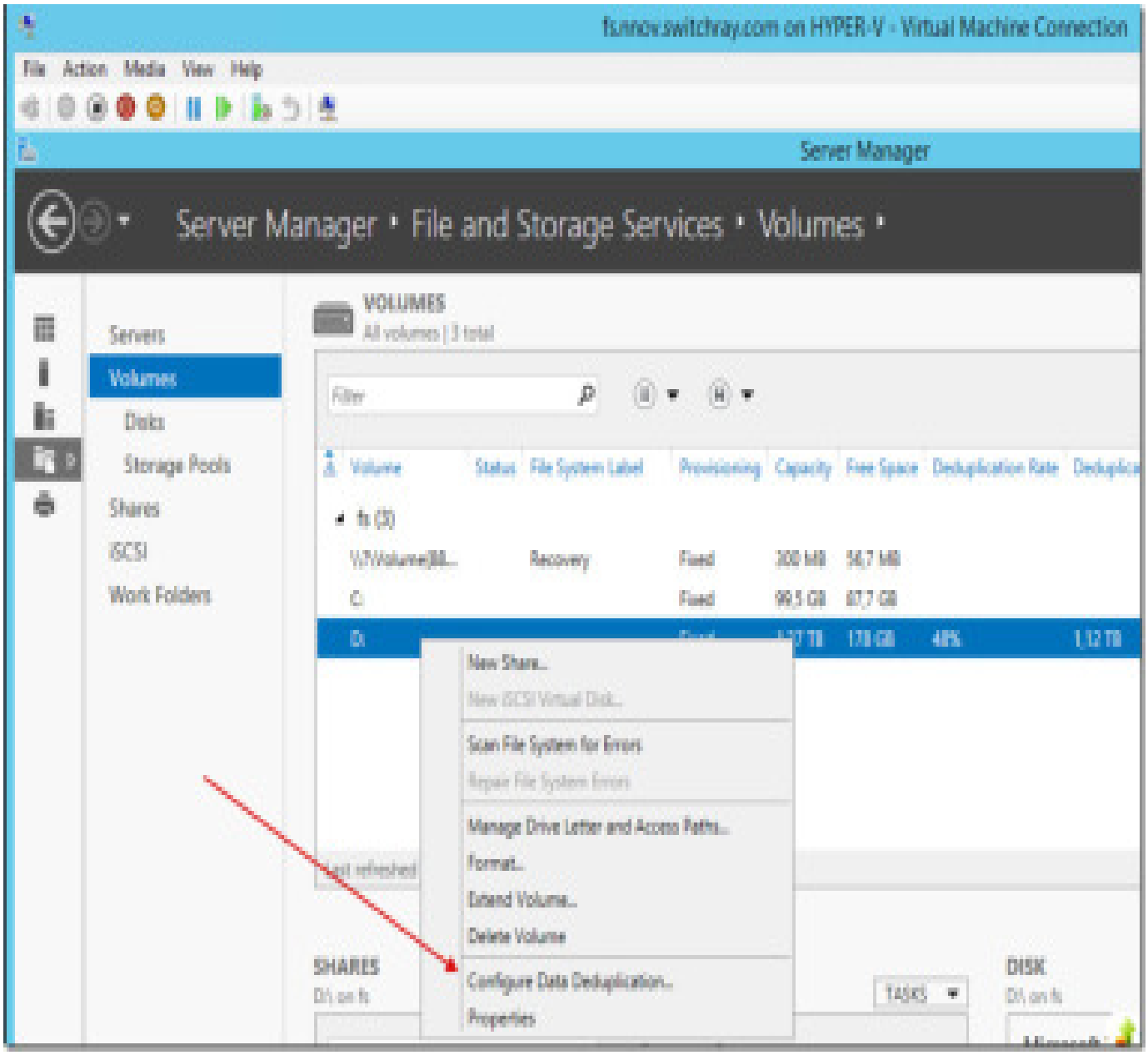

Но так как папка Документы клиент банк вложена в папку Бухгалтерия и если просто добавить пользователя в группу **ClientBank_RW**, то пользователь увидит такую картину:

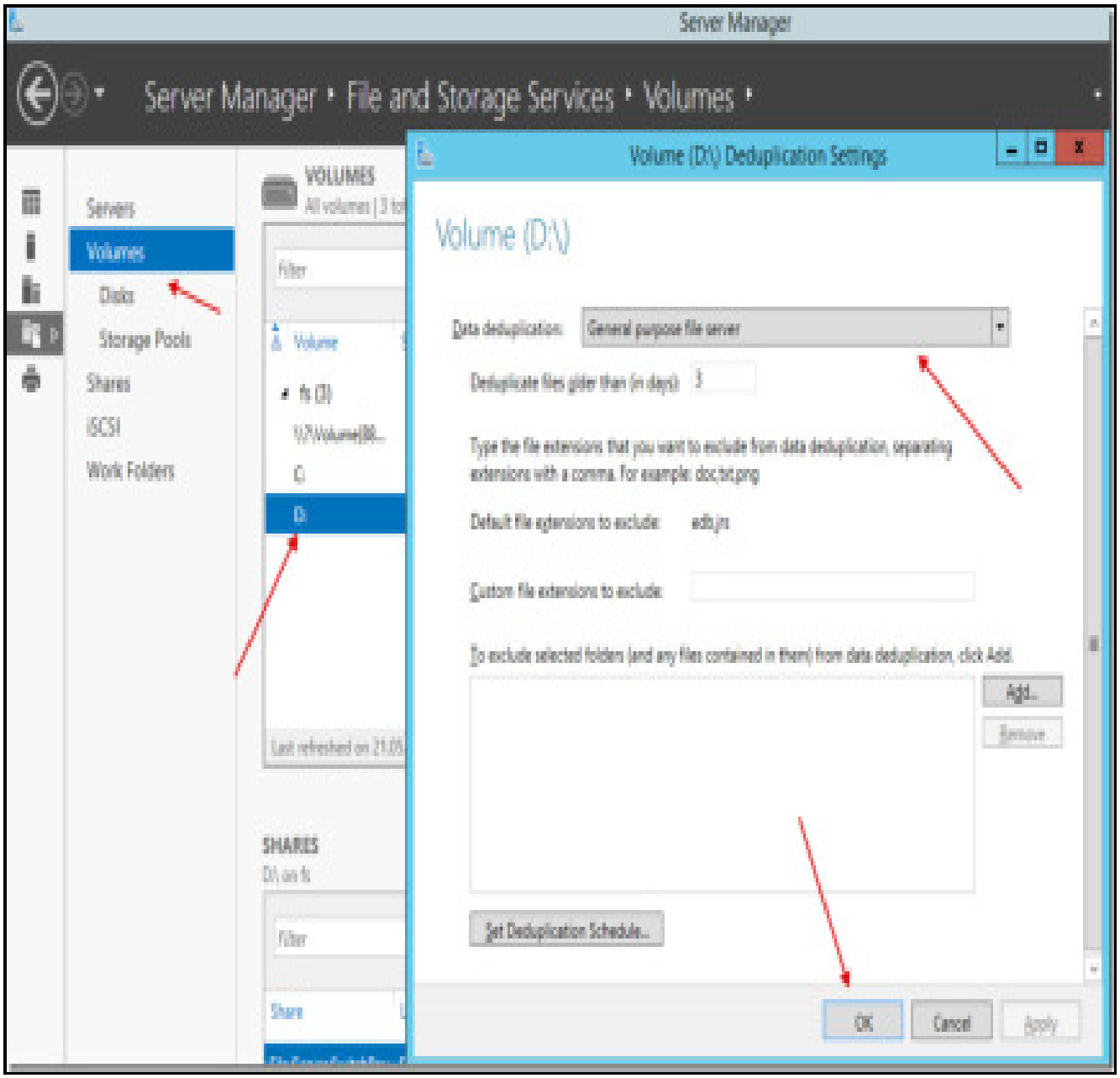



Почему? У пользователя нет никаких прав на папку верхнего уровня Бухгалтерия.

К примеру если он взаимодействует только с папкой Документы клиент банк то ему достаточно будет дать права **Accounting_RO** и **ClientBank_RW** после этого он сможет без проблем добраться до папки Документы клиент банк.

**<u>И в заключении включаем Data Dedeuplication:</u>**


fs.nnov.switchay.com on HYPER-V - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager • File and Storage Services • Volumes •
Servers
Volumes
Disks
Storage Pools
Shares
iSCSI
Work Folders
VOLUMES
All volumes | 3 total
Filter
Volume
Status
File System Label
Provisioning
Capacity
Free Space
Deduplication Rate
fs (3)
Recovery
Fixed
300 MB
56,7 MB
C:
Fixed
99,5 GB
87,7 GB
D:
48%
1,12 TB
New Share...
New iSCSI Virtual Disk...
Scan File System for Errors
Repair File System Errors
Manage Drive Letter and Access Paths...
Format...
Extend Volume...
Delete Volume
Configure Data Deduplication...
Properties
SHARES
TASKS
DISK




Мы создали файл сервер с ролевым типом доступа. Каждый пользователь файлового сервера видит только свои папки. Наш файловый сервер “живет” в пространстве DFS, что позволяет в будущем при необходимости масштабировать. Задействовали технологию Data Deduplication. Соблюли вложенность групп в AD DS.

**Практическое занятие №20.** Реализация Client Endpoint Protection Настройка точки Endpoint Protection

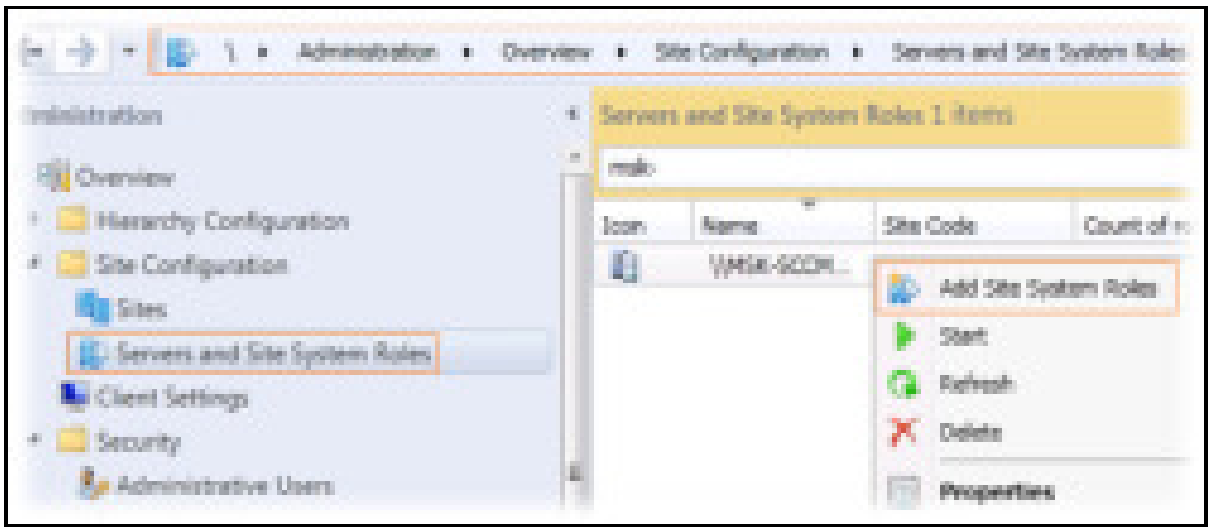
***Цель работы:***

Научиться выполнять настройки точки Endpoint Protection и реализацию Client Endpoint Protection.

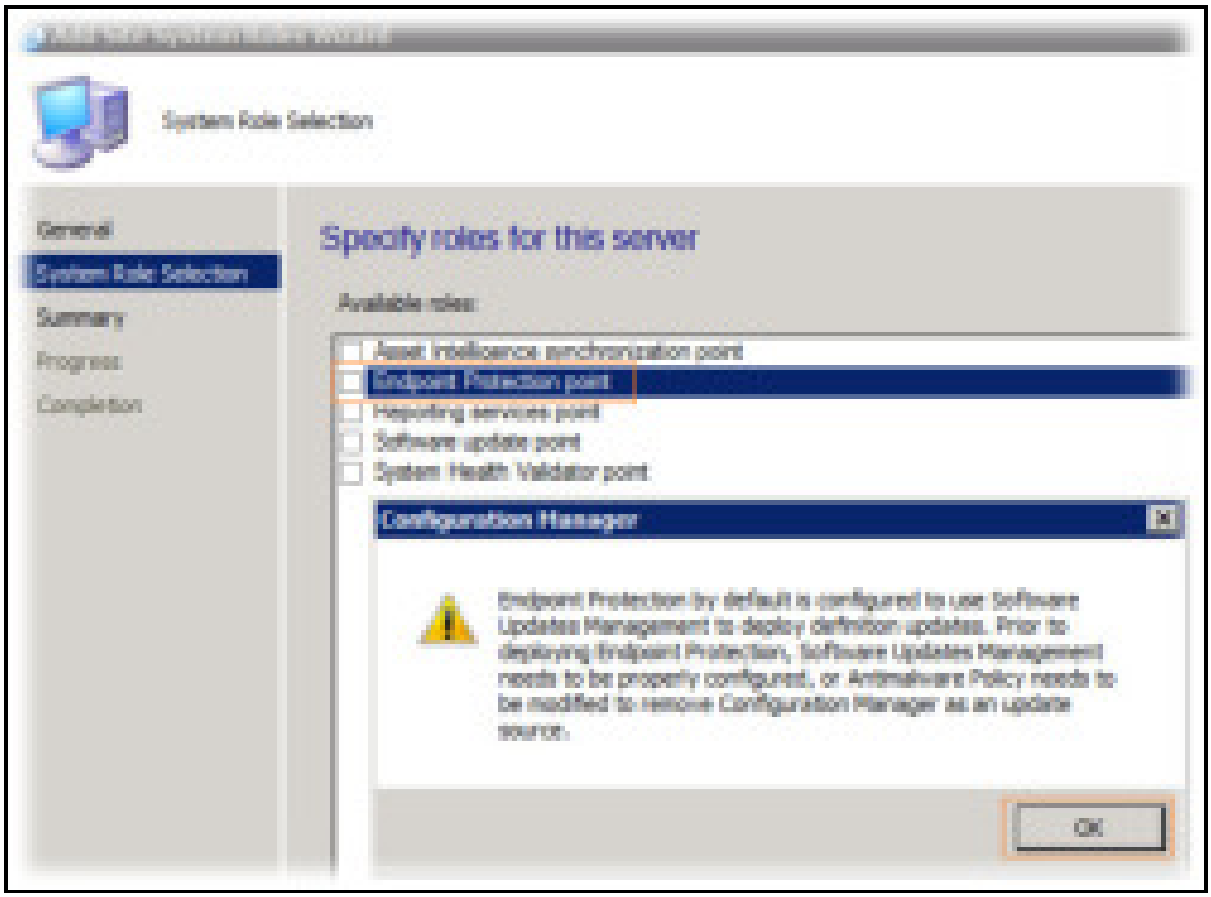
SCCM 2012 - Настраиваем System Center 2012 Endpoint Protection. Настройку Endpoint Protection (SCEP) в System Center 2012 Configuration **Manager** (**SCCM**) начинаем с поднятия роли **Endpoint Protection Point** (**EPP**) на сервере сайта верхнего уровня иерархии SCCM. В нашем случае таким сервером является сервер **Central Administration site** (**CAS**). После включения роли EPP на сайте верхнего уровня функциональность SCEP станет доступна на всех сайтах нижнего уровня иерархии.

**Включение роли Endpoint Protection Point**

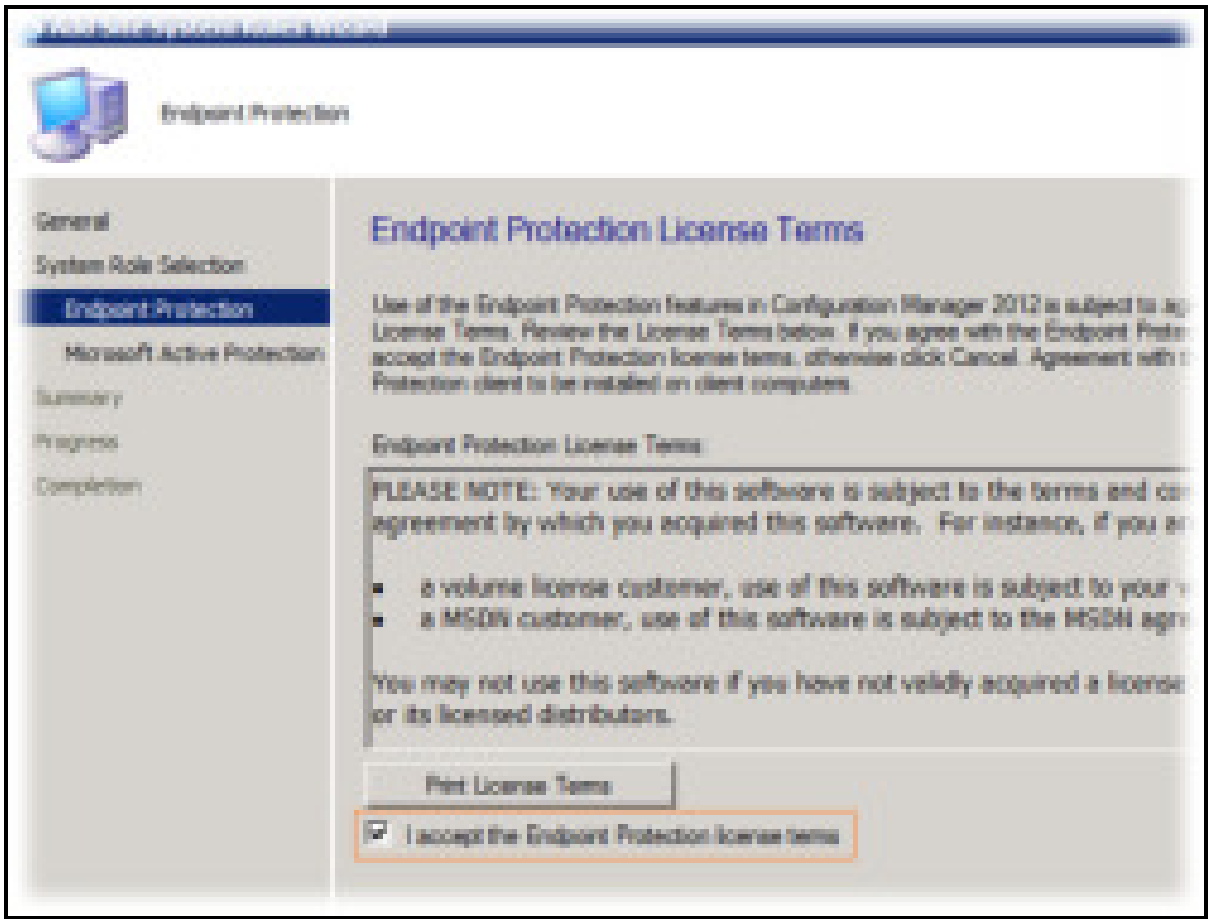
В консоли SCCM переходим в раздел **Administration\Overview\Site Configuration\Servers and Site System Roles** и выбрав сервер CAS вызываем мастер добавления ролей **Add Site System Roles**




Выбираем соответствующую роль - **Endpoint Protection Point** и принимаем предупреждение о том что необходима дополнительная настройка источников обновления антивирусных описаний.



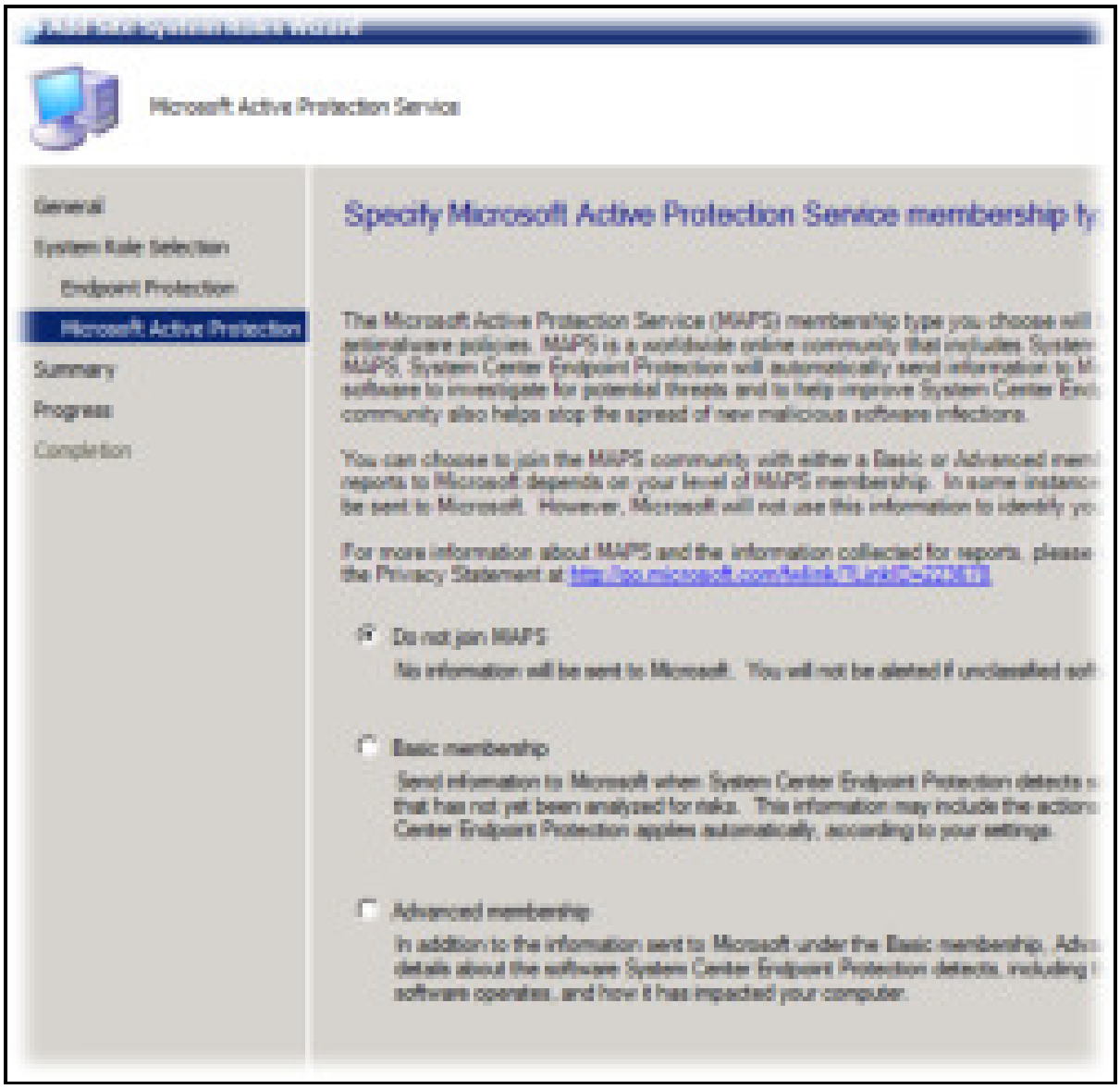

Следующим шагом принимаем условия лицензии и подтверждаем то, что у нас действительно есть право использовать SCEP в инфраструктуре SCCM




Затем нам будет предложено выбрать вариант членства в программе **Microsoft Active Protection Service** (**MAPS**) - уровень информации, которую требуется отправлять в Microsoft для помощи в разработке новых определений. Выдержка из документации по этому поводу:

Присоединитесь к службе Microsoft Active Protection Service, чтобы повысить уровень защиты своих компьютеров, предоставляя корпорации Майкрософт образцы вредоносных программ, и быстрее получать новые определения для антивредоносных приложений. Кроме того, присоединение к Microsoft Active Protection Service позволяет клиенту Endpoint Protection использовать службу динамических подписей для загрузки новых определений до того, как они будут опубликованы в Центре обновления Windows.

Если обновление антивирусных описаний более одного раза в сутки не требуется, то вполне можно отказаться от участия в данной программе.

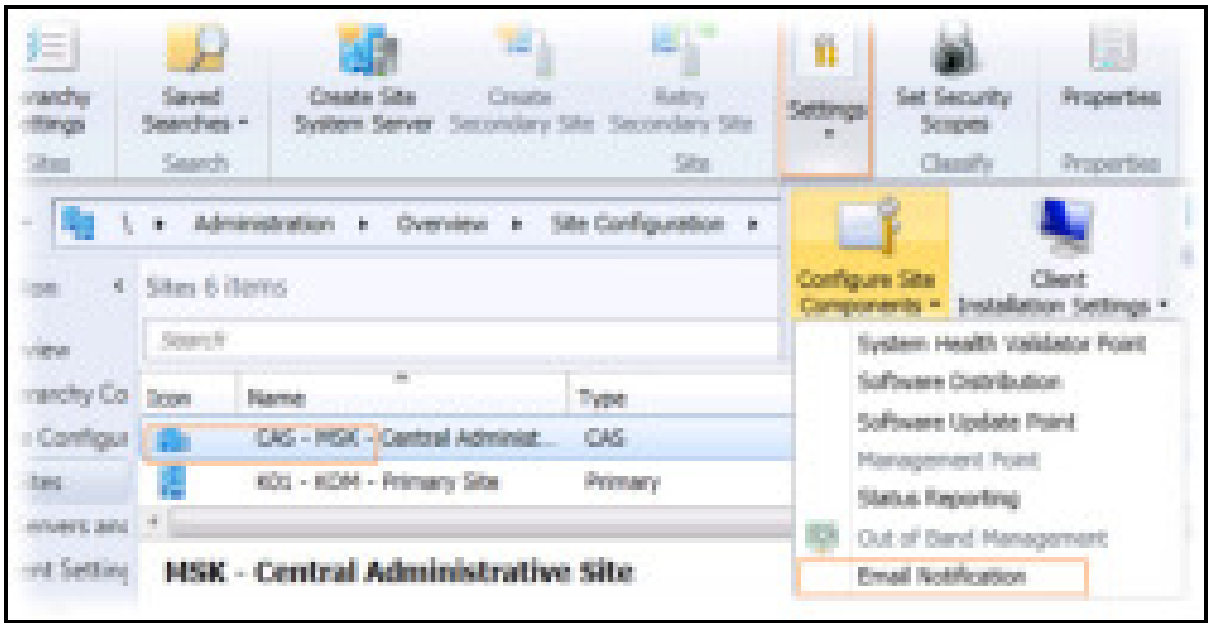



По окончании работы мастера добавления роли можно выполнить настройку общих параметров оповещений для роли FEP. Эта настройка является глобальной для всей иерархии и должна выполняться на CAS.

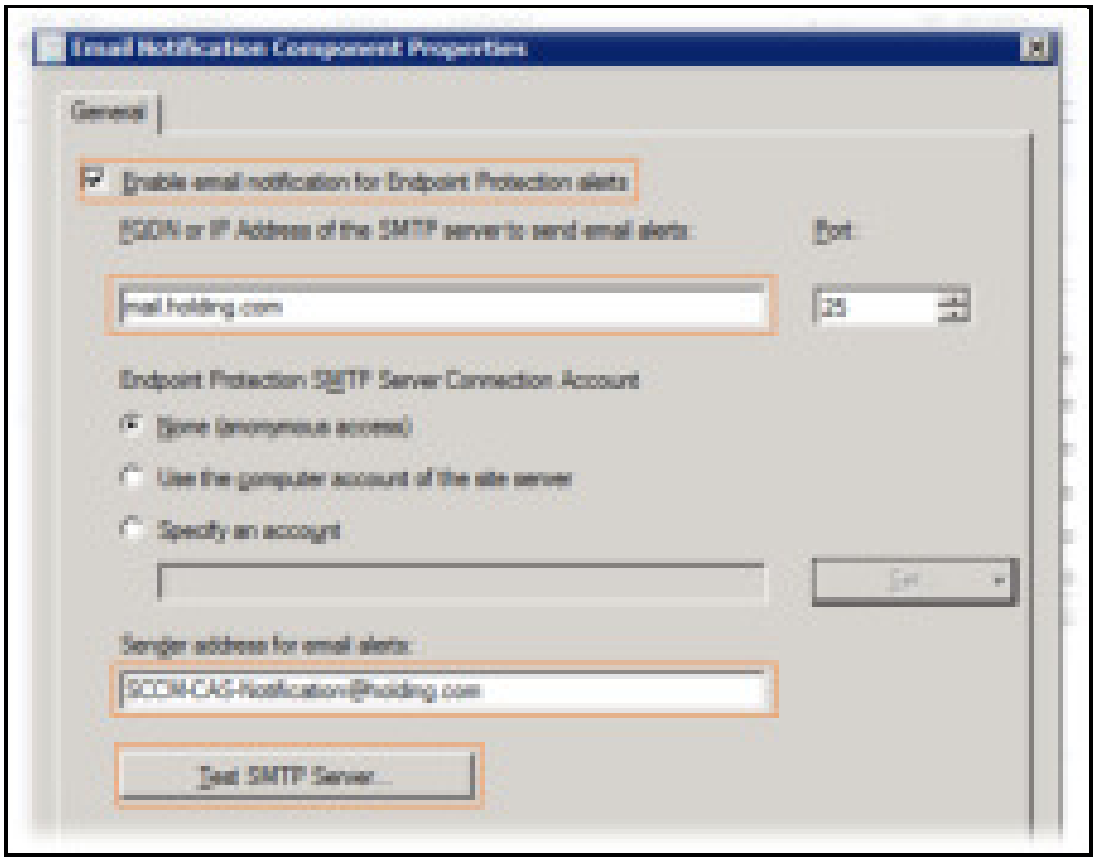
Для оповещения о проблемах SCEP (отсутствие активности клиентов, вирусные “вспышки” и т.п.) можно использовать электронную почту, создавая на сайтах иерархии соответствующие подписки на уведомления.

Прежде чем можно будет приступать к настройке подписок электронной почты на сайтах нижних уровней для получения уведомлений, необходимо настроить SMTP-сервер в иерархии. SMTP-сервер можно указать только в сайте верхнего уровня иерархии Configuration Manager.

В консоли SCCM переходим в раздел **Administration\Overview\Site Configuration\Sites** и выбрав CAS вызываем настройку его компоненты **Settings > Email Notification**




Включаем опцию оповещений, указываем имя SMTP-сервера и почтовый адрес, с которого будут отправляться оповещения. Здесь же можно протестировать функцию отправки почты.



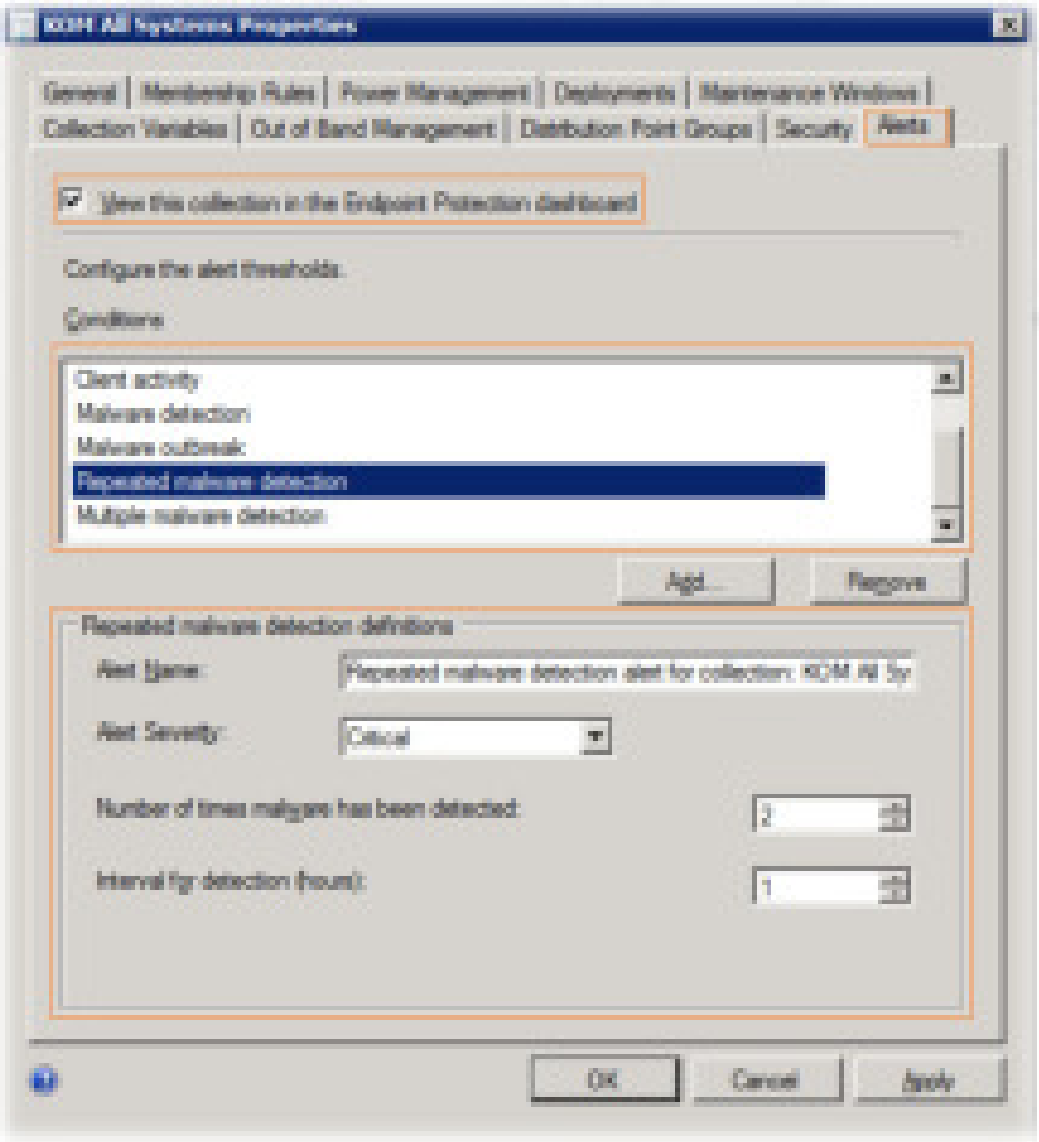

На этом глобальные настройки верхнего уровня закончены.

Теперь можно перейти к подчинённому первичному сайту и начать настройку уже под конкретное клиентское окружение.

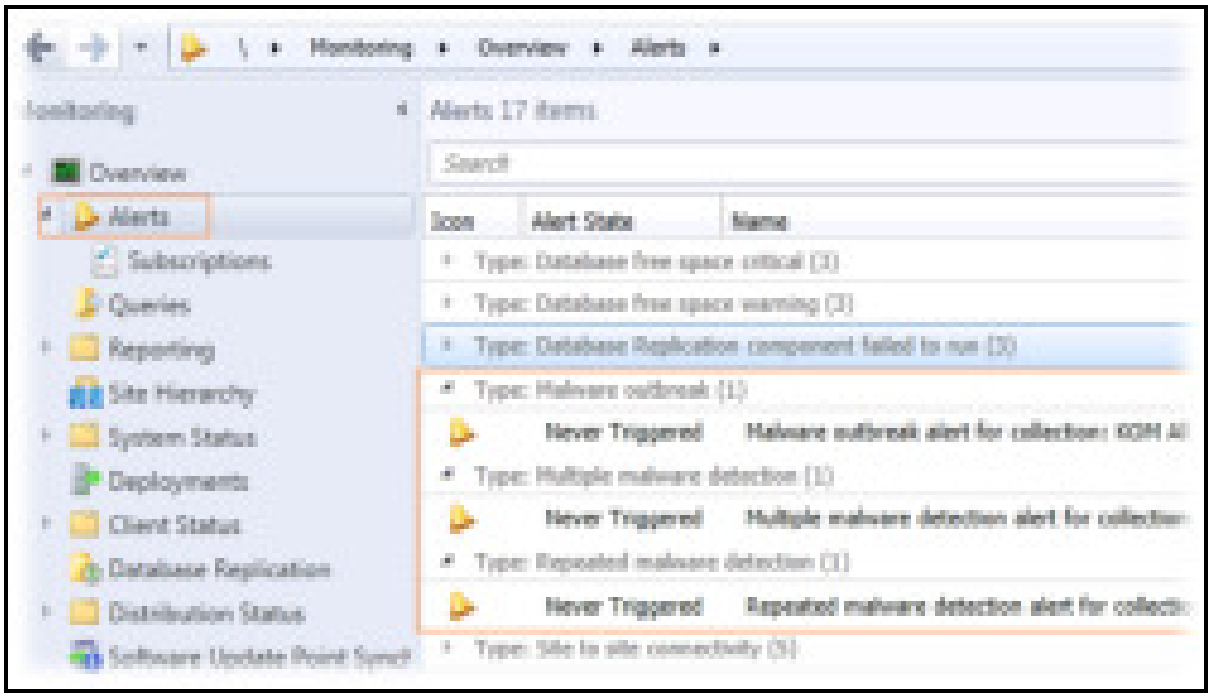
**Настройка оповещений по коллекциям**

Определившись с тем, для каких коллекций компьютеров мы будем включать установку и использование SCEP, мы сразу можем настроить оповещения для этих самых коллекций. Сразу два замечания:- Нельзя настраивать оповещения для коллекций пользователей - Настройка недоступна для коллекции Все системы (All Systems).

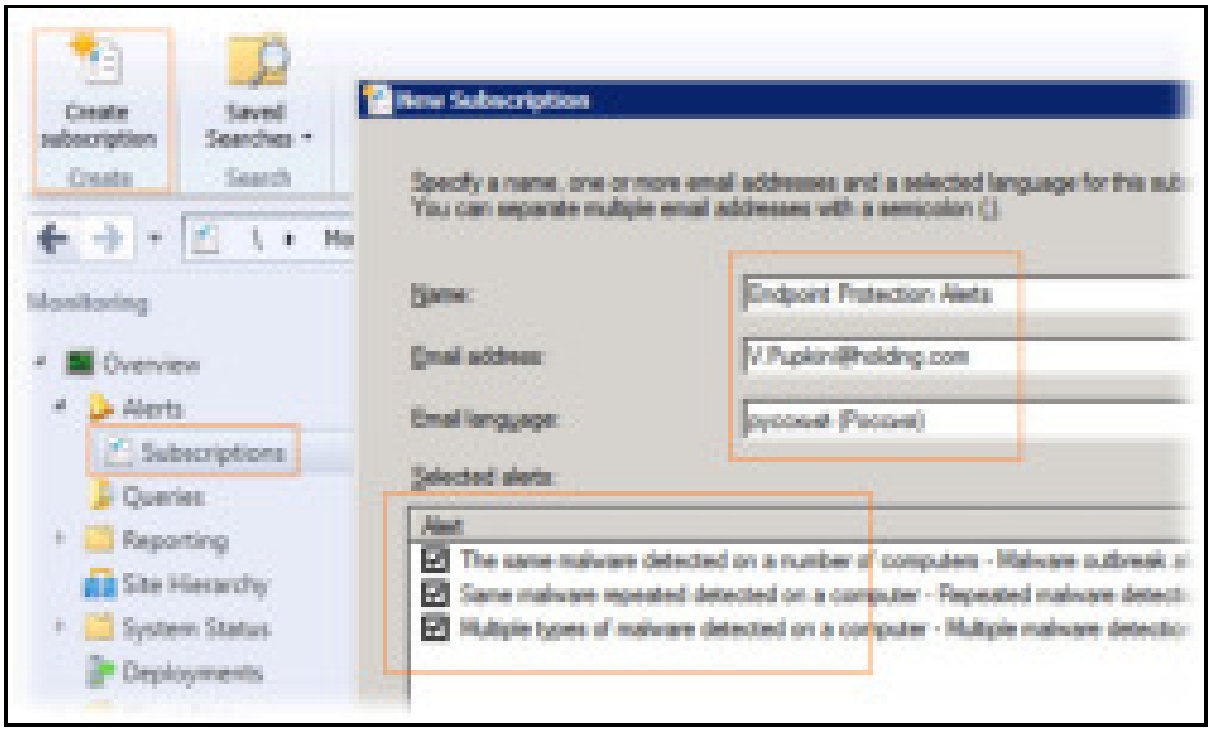
В разделе консоли SCCM **Assets and Compliance\Overview\Device Collections** переходим к списку коллекций и открыв свойства интересующей нас коллекции переходим на закладку **Alerts** Вот настройки, которые нам доступны на данный момент:




После того как включено оповещение для нужных коллекций, можно увидеть сводную информацию по всем оповещениям в разделе консоли **Monitoring\Overview\Alerts**




На включенные оповещения создаём подписки в разделе консоли **Monitoring\Overview\Alerts\Subscriptions** где указываем кому именно и по каким событиям будут отправляться письма.

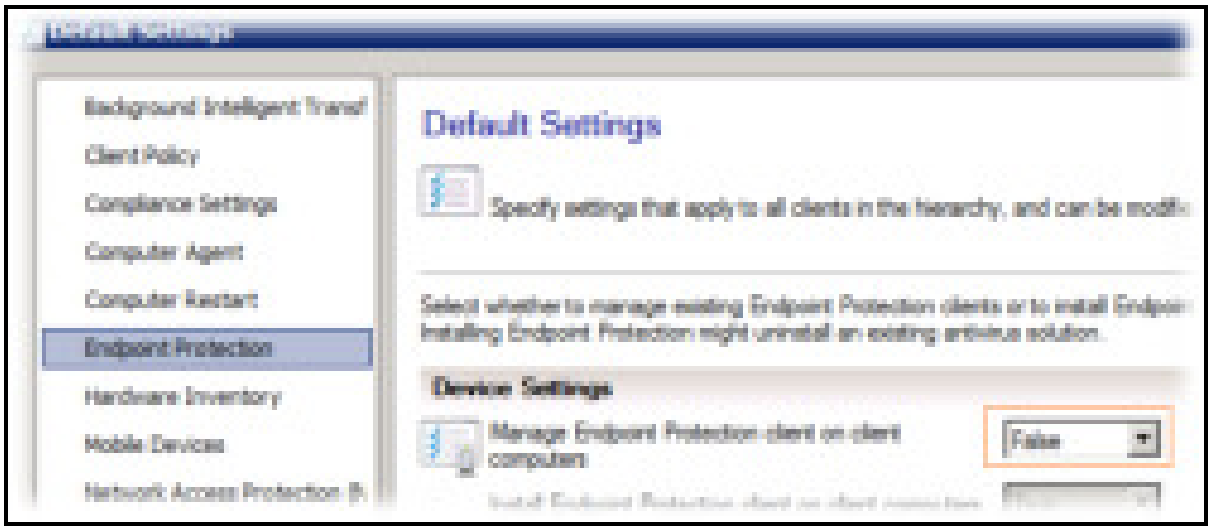



## Настройка политик клиентов

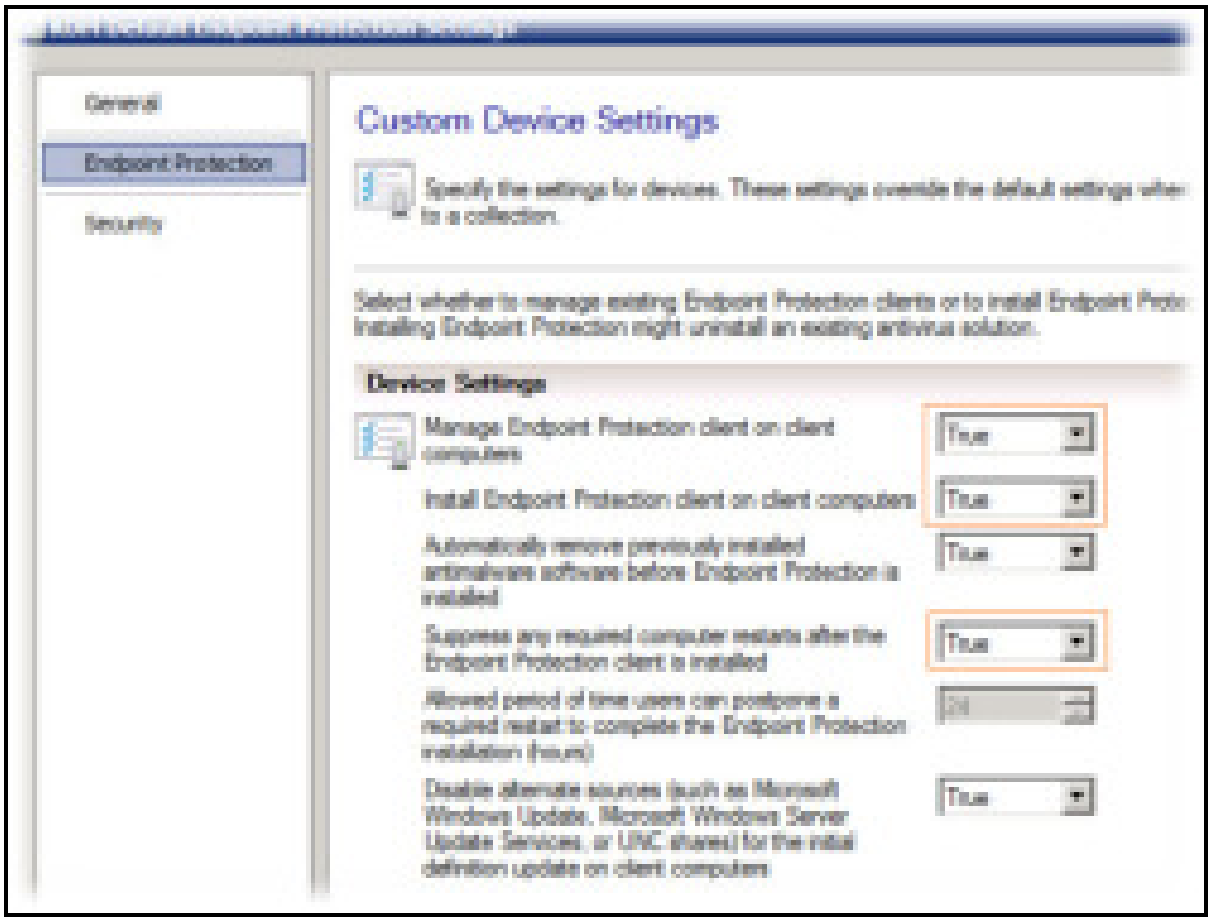
В силу того, что дистрибутив клиента SCEP фактически распространяется на компьютеры уже при установке клиента SCCM (файл

**%windir%\ccmsetup\SCEPInstall.exe**), то всё что нам нужно сделать для того, чтобы установить клиента SCEP на какую-либо коллекцию компьютеров, – это включить параметры политики клиента в разделе консоли **Administration\Overview\Client Settings**

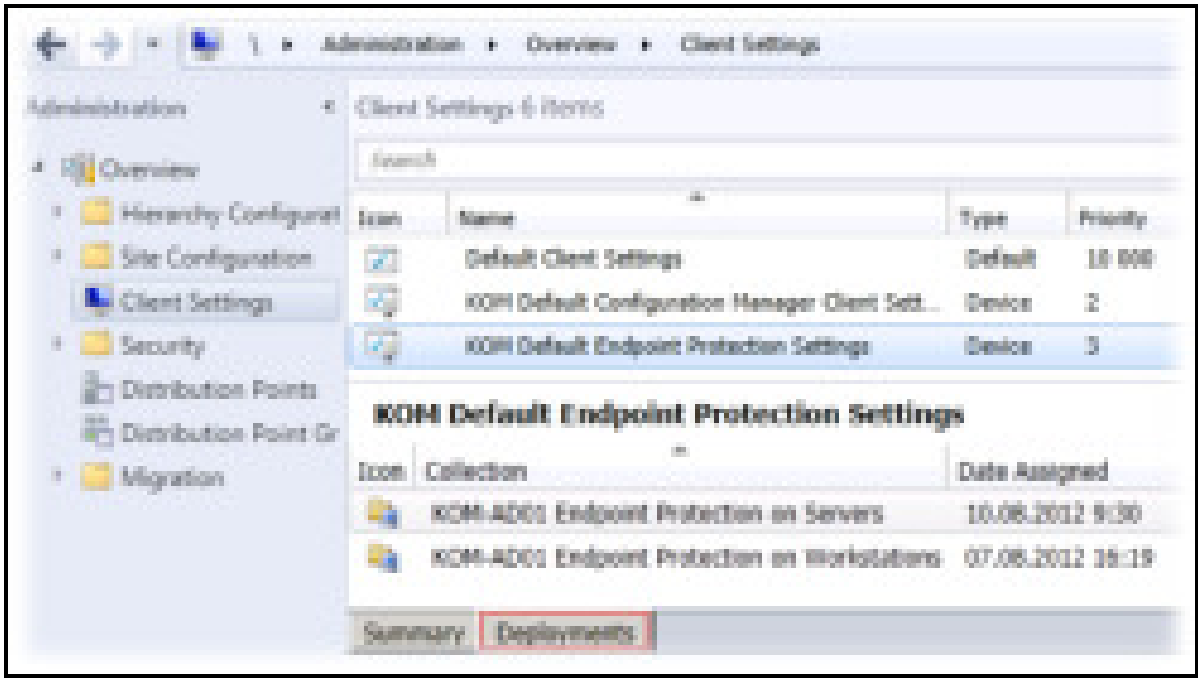
Если вы не хотите запускать установку SCEP сразу на всех компьютерах являющихся клиентами SCCM, то в клиентской политике по-умолчанию **Default Client Settings** можно выключить настройки в разделе **Endpoint Protection**…




…и создать отдельную клиентскую политику с включенными параметрами SCEP…




… а затем нацелить эту клиентскую политику на определённые коллекции компьютеров, на которые вы хотите выполнить установку.




## Настройка политик защиты от вредоносных программ

Разворачиваемые клиенты SCEP управляются с помощью параметров, передаваемых через механизм политик защиты от вредоносных программ - **Antimalware Policies**.

Подробно о настройке этих политик можно прочитать в статье Создание и развертывание политик защиты от вредоносных программ для Endpoint Protection в Configuration Manager. Несколько цитат:

Политики включают сведения о расписании проверок, типах проверяемых файлов и папок, а также действиях, выполняемых при обнаружении вредоносных программ. При включении Endpoint Protection стандартная политика защиты от вредоносных программ применяется к клиентским компьютерам; однако вы можете использовать дополнительные стандартные шаблоны политик или создать собственные политики для настройки параметров работы функции в конкретной среде.

При создании и развертывании новой политики защиты от вредоносных программ для коллекции такая политика переопределяет политику по умолчанию.

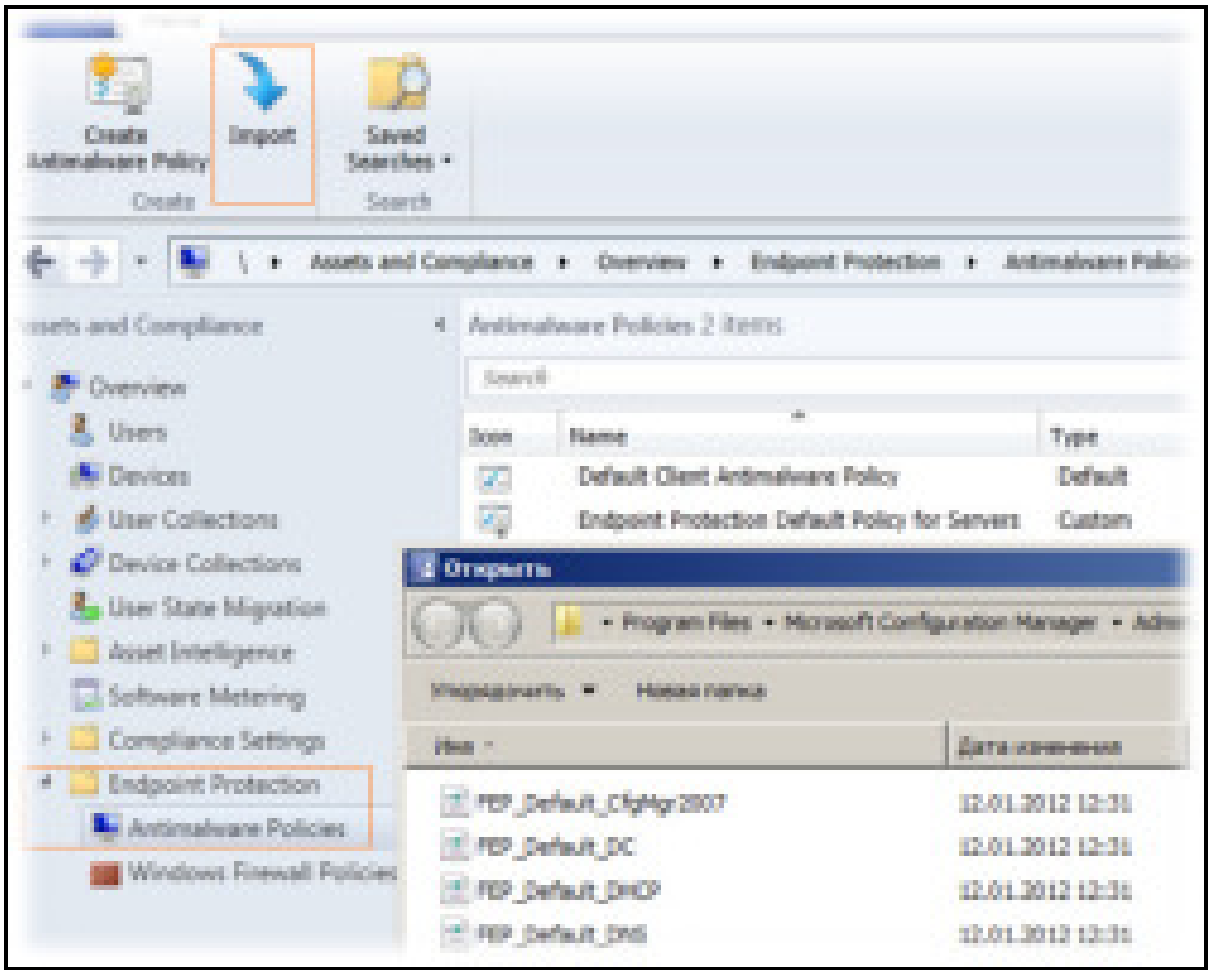
Configuration Manager включает несколько стандартных шаблонов, оптимизированных для использования в различных сценариях, которые можно импортировать в Configuration Manager. Эти шаблоны можно найти в папке ***<папка установки Configuration Manager>*\AdminConsole\XMLStorage\EPTemplates.**

В этой папке находится 25 шаблонов, оптимизированных в основном под разные серверные роли. Можно собрать в основном различающиеся настройки реестра для веток.

**SOFTWARE\Policies\Microsoft\Microsoft Antimalware\Exclusions\Paths**
**SOFTWARE\Policies\Microsoft\Microsoft Antimalware\Exclusions\Processes**

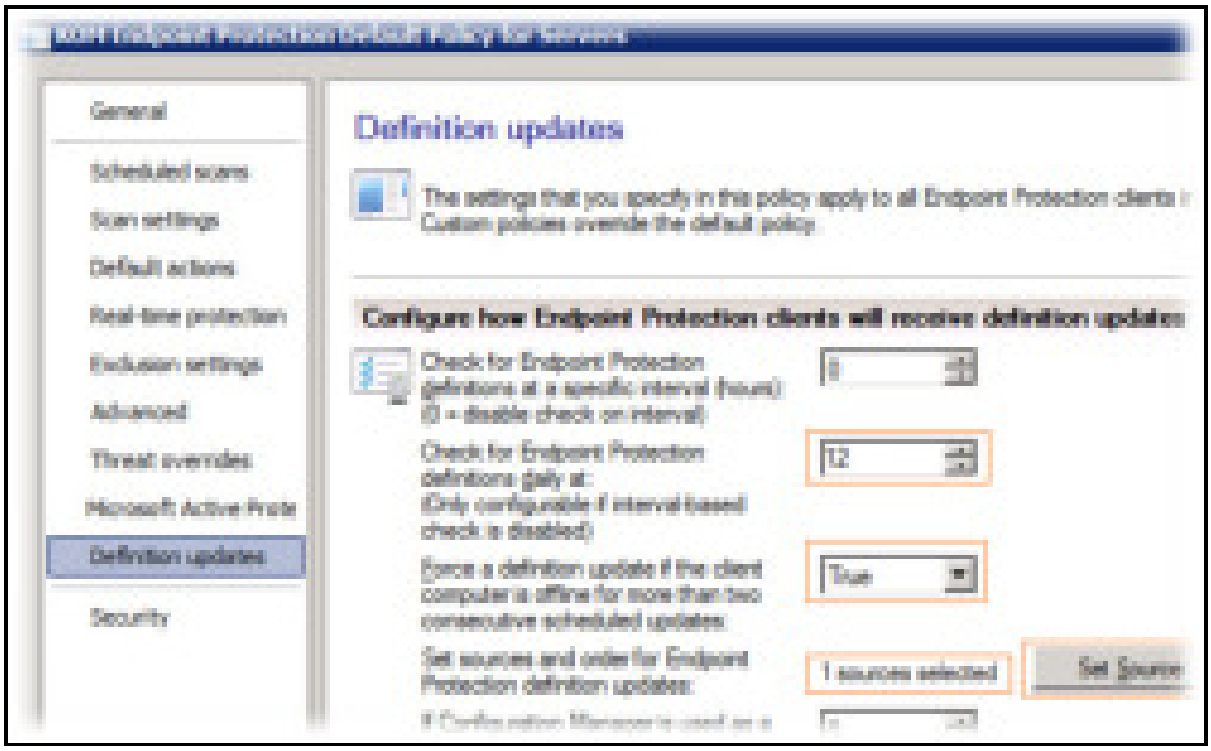
в один XML шаблон для серверных систем. За основу можно взять содержимое шаблона **FEP_Default_DC.xml**

Изучить политику по-умолчанию (**Default Client Antimalware Policy**) или импортировать из шаблона новую политику можно в разделе консоли SCCM: **Assets and Compliance\Overview\Endpoint Protection\Antimalware Policies**

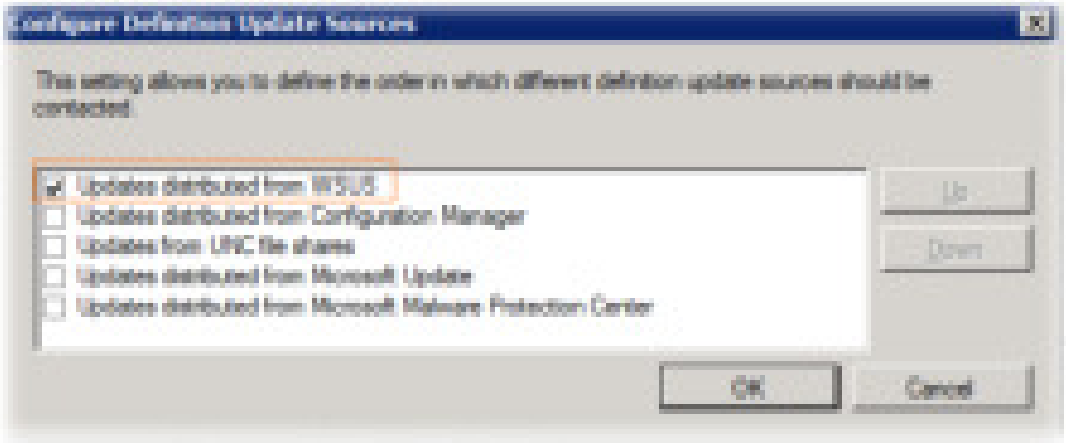



Настройки политики особой сложности не представляют, и если у вас возникнут вопросы по настройке каких либо отдельных параметров можно воспользоваться разделом **Список параметров политики защиты от вредоносных программ** в ранее указанном документе. Вопрос по механизму применения исключений, снят в ветке обсуждения **SCEP 2012 и список исключений.**

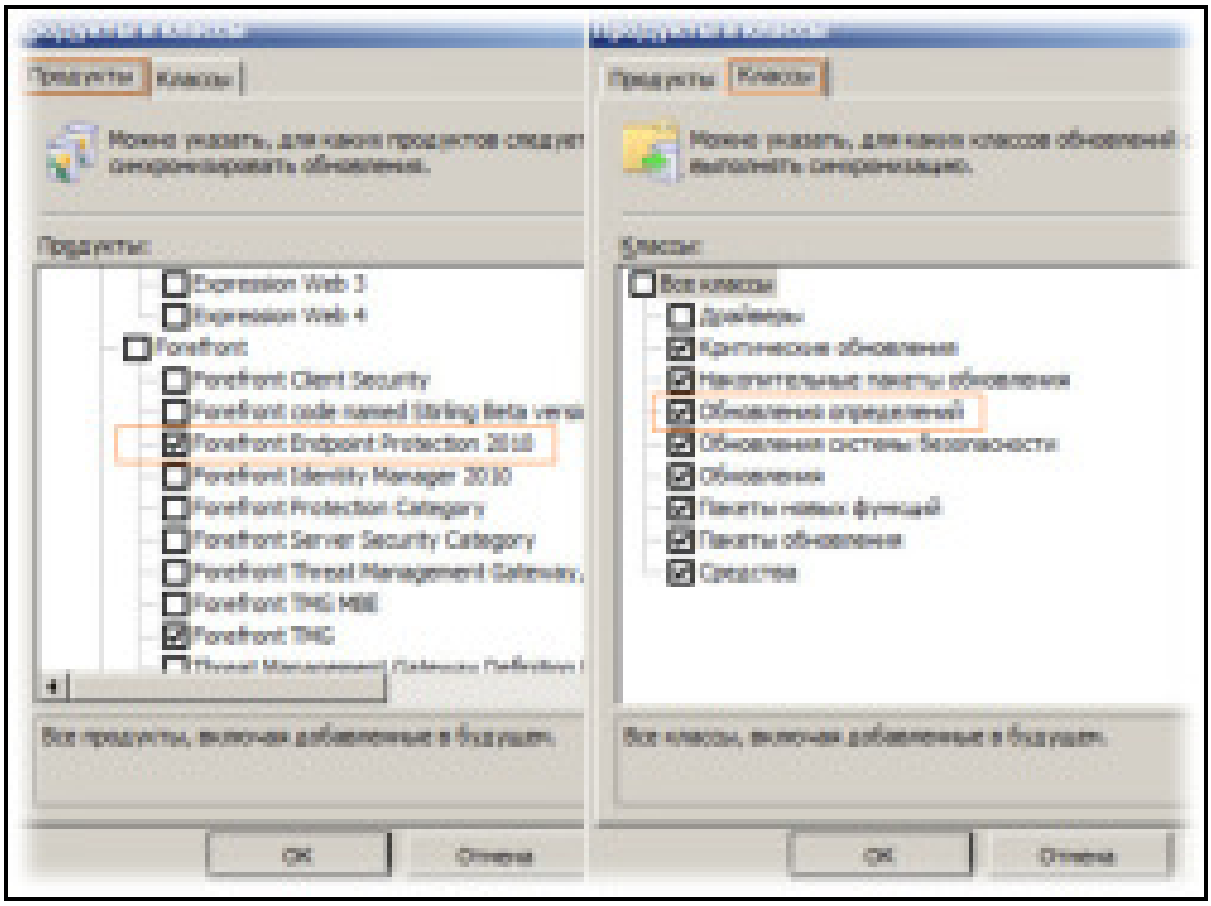
Особое внимание строит обратить на параметры настройки источников обновления антивирусных описаний. Если в SCCM не используется роль **Software Update Point** (**SUP**), и для установки обновлений Windows используется локальный сервер **WSUS** – то его можно определить в качестве основного источника обновлений.



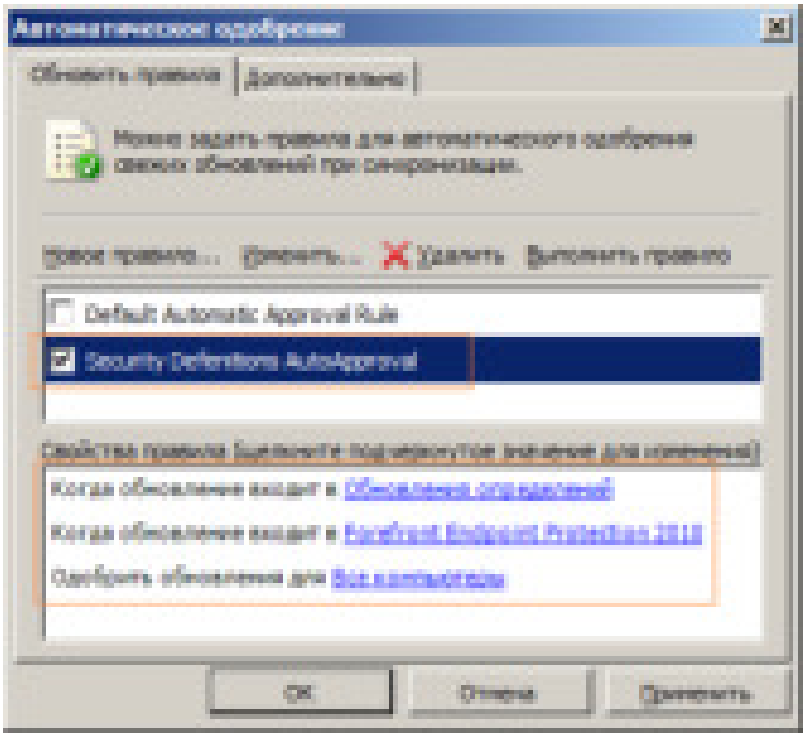

Источник обновлений можно указывать как единственный так и использовать их комбинацию, самостоятельно определяя приоритет их использования.




Для того чтобы локальный сервер WSUS мог выступать в качестве источника обновлений антивирусных описаний SCEP на нём должна быть включена категория **Forefront Endpoint Protection 2010** и класс **Обновления определений** в настройках параметров синхронизации с серверами **Microsoft Windows Update**.




Помимо этого на WSUS должно быть создано и включено правило автоматического одобрения с соответствующими условиями

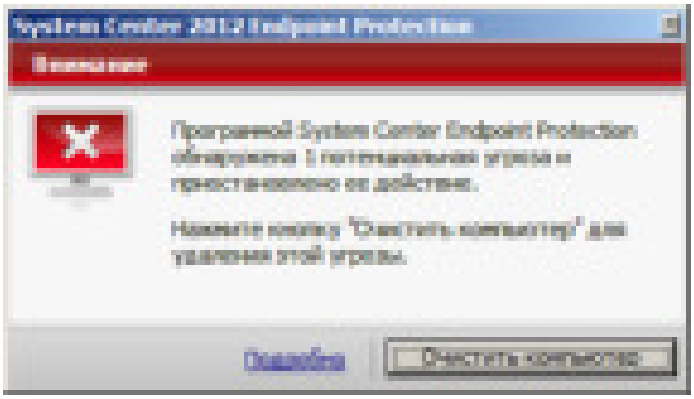


**Быстрая проверка работоспособности**

Когда антивирус уже развёрнут и настроен можно быстро проверить работоспособность реал-тайм сканирования, создав на любом защищаемом компьютере текстовый файл со следующим содержимым:

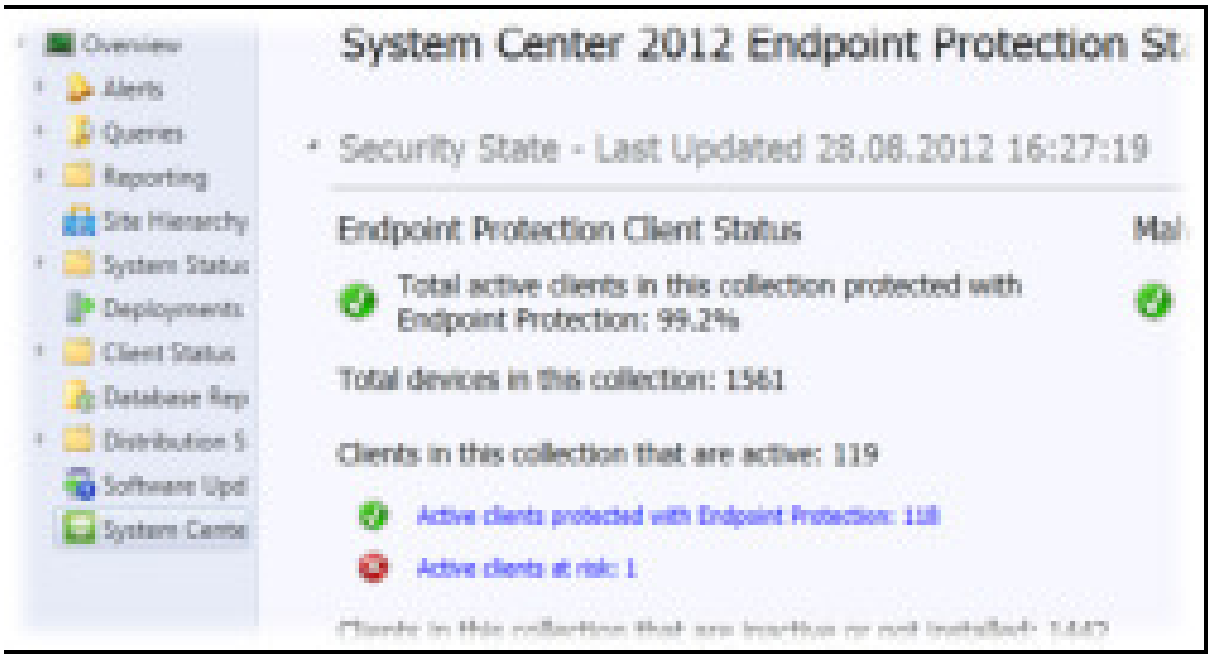
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Сохраняем файл и смотрим на реакцию антивируса, который тут же должен будет заблокировать доступ к файлу и сообщить о найденной угрозе

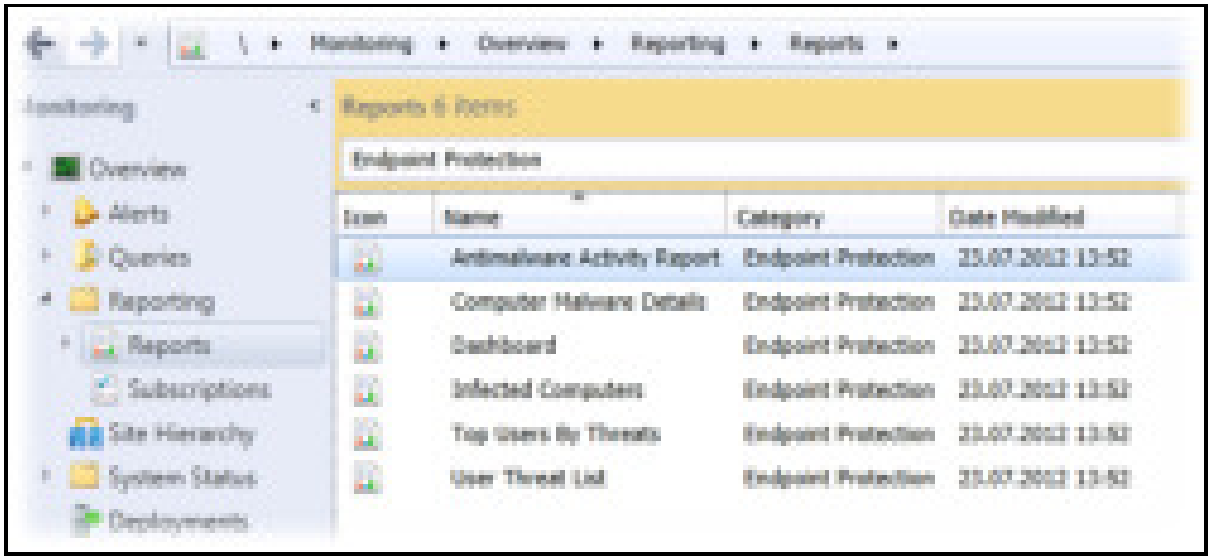


**Мониторинг**

Статус текущего состояния инфраструктуры Endpoint Protection в SCCM можно видеть в разделе консоли
**Monitoring\Overview\System Center 2012 Endpoint Protection Status**




Также доступна группа отчетов в разделе консоли **Monitoring\Overview\Reporting\Reports**




Для расширения анализа ситуации можно самостоятельно разработать собственные отчёты.

Дополнительно есть возможность мониторить состояние клиентов SCEP с помощью пакетов мониторинга (Management/Monitoring Pack) SCCM/FEP для **System Center 2012 Operations Manager**.

В следующих заметках мы рассмотрим процедуру настройки роли SUP в SCCM и создание правила автоматического развёртывания (**Automatic Deployment Rule**) для антивирусных описаний SCEP.

**Практическое занятие №21. Настройка Data Protection для данных клиентского компьютера**

***Цель работы:***

Изучить: настройку пакета Data Protection для данных клиентского компьютера

**Настройка Microsoft DPM**

Установим и настроим Microsoft Data Protection Manager. Для этого необходимо

скачать System Center 2012 Data Protection Manager. Для его работы нам понадобится Microsoft SQL сервер, у нас будет Microsoft SQL Server 2012 SP 1, скачаем его тоже. Совместимость с версиями MS SQL по данным technet.microsoft.com следующая:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

Внимательно отнеситесь к языку системы – если скачиваемый пакет MS SQL имеет отличный от системы язык, то на выходе Вы получите ошибку вроде вот этой: “The SQL Server license agreement cannot be located for the selected edition”

Системные требования DPM 2012 R2
Требования для установки:

Windows Server 2012 R2, выпуски Datacenter и Standard

Windows Server 2012, выпуски Datacenter и Standard

Windows Server 2008 R2 с пакетом обновления 1 (SP1), выпуски Standard и Enterprise

Платформа Microsoft .NET Framework 4.0 в том числе на защищаемых серверах.

Установщик Windows версии 4.5 или более поздней

Распространяемый пакет Microsoft Visual C++ 2008

Windows PowerShell 3.0

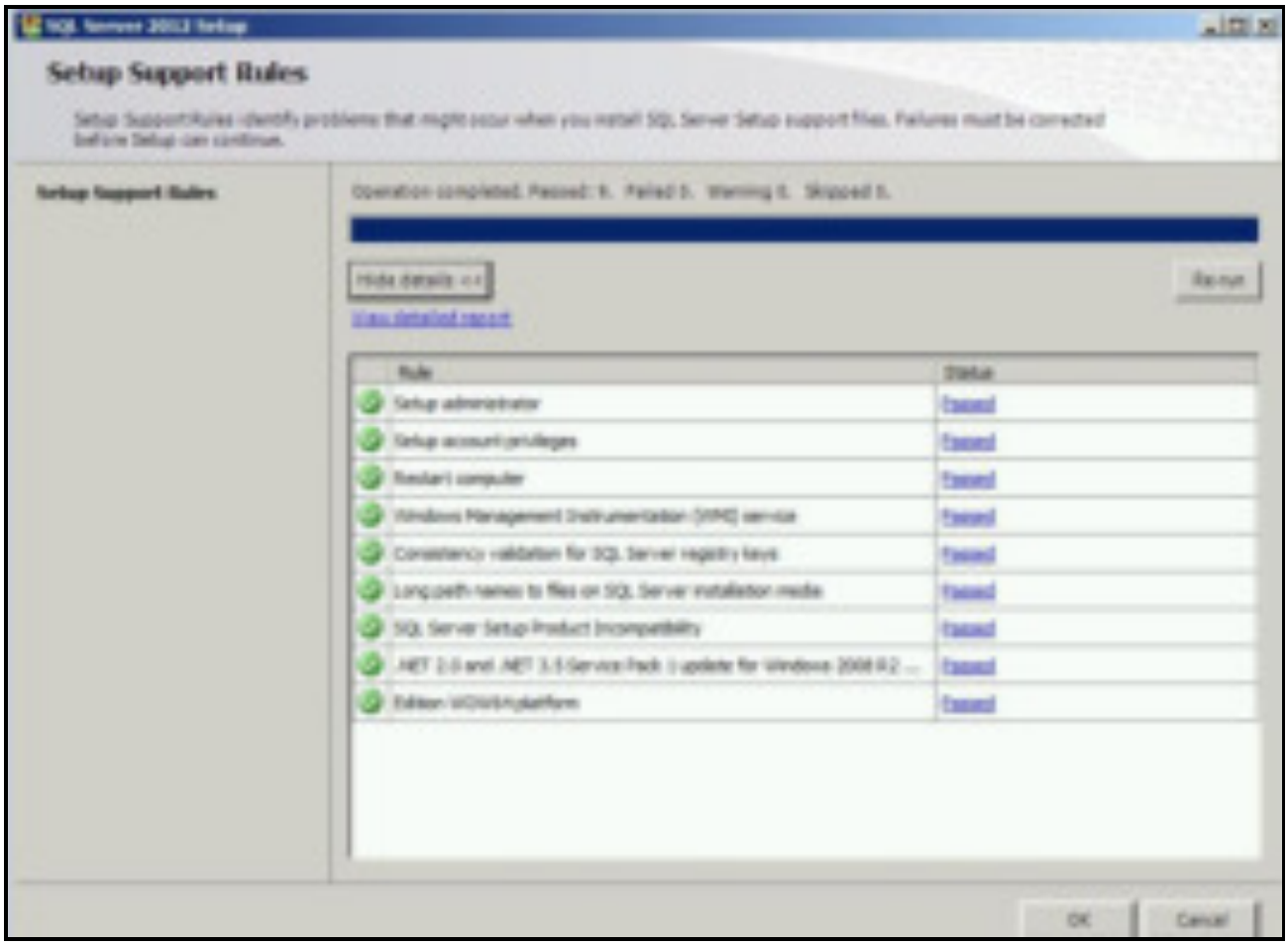
Хранилище единственных копий Windows (SIS)

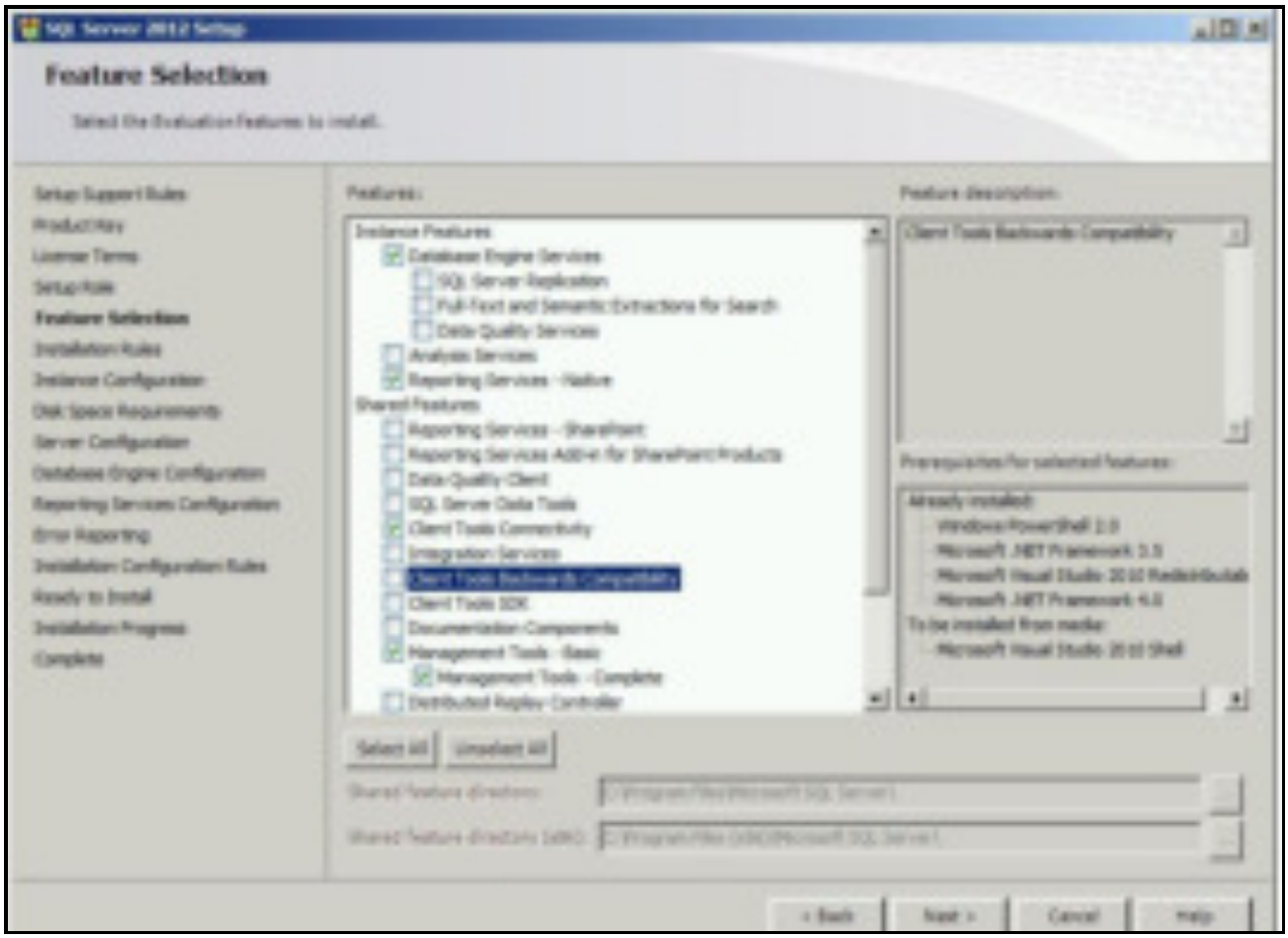
Сообщения об ошибках в приложениях Майкрософт

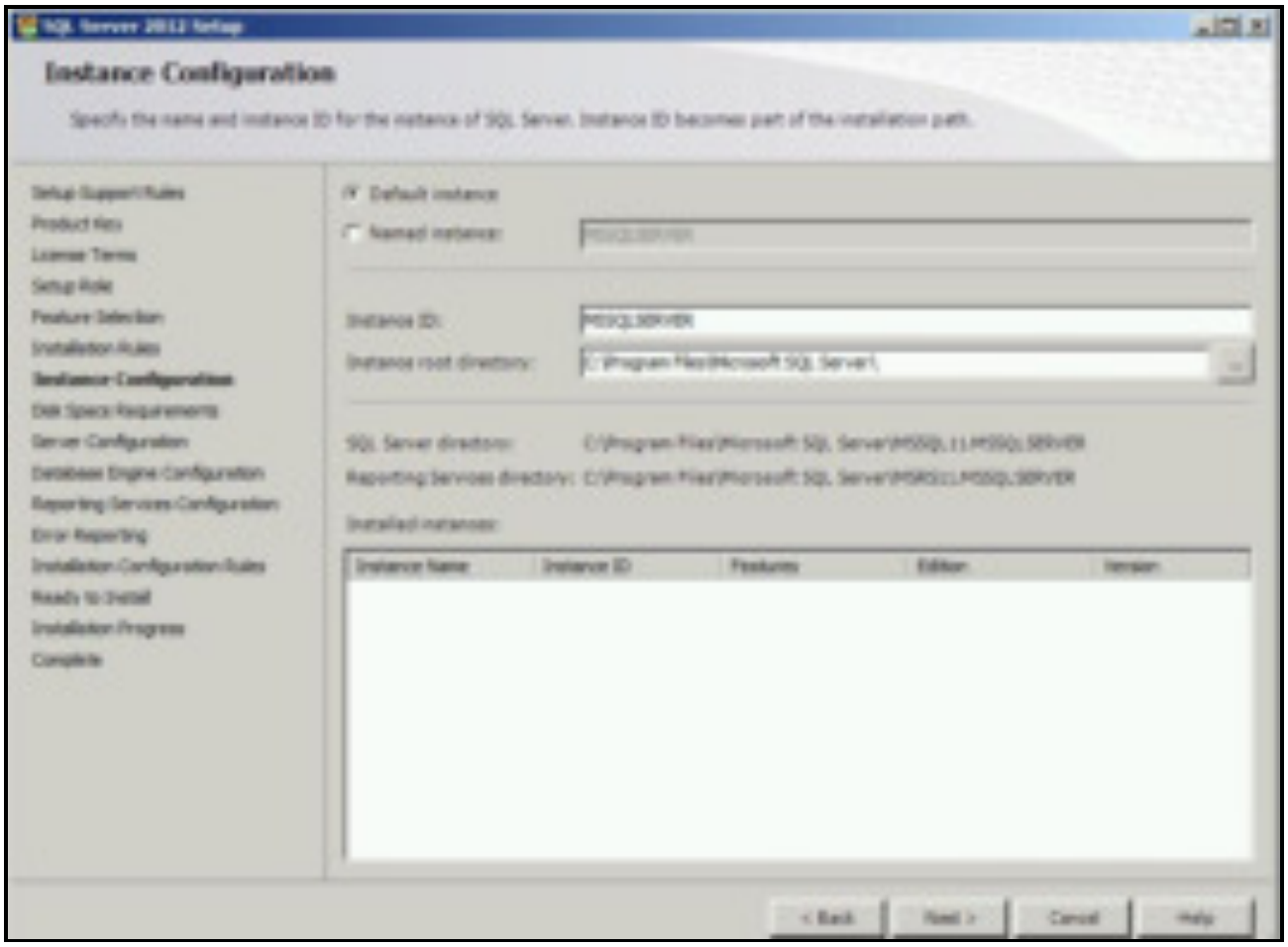
Программа установки автоматически устанавливает эти пакеты, если они не установлены.

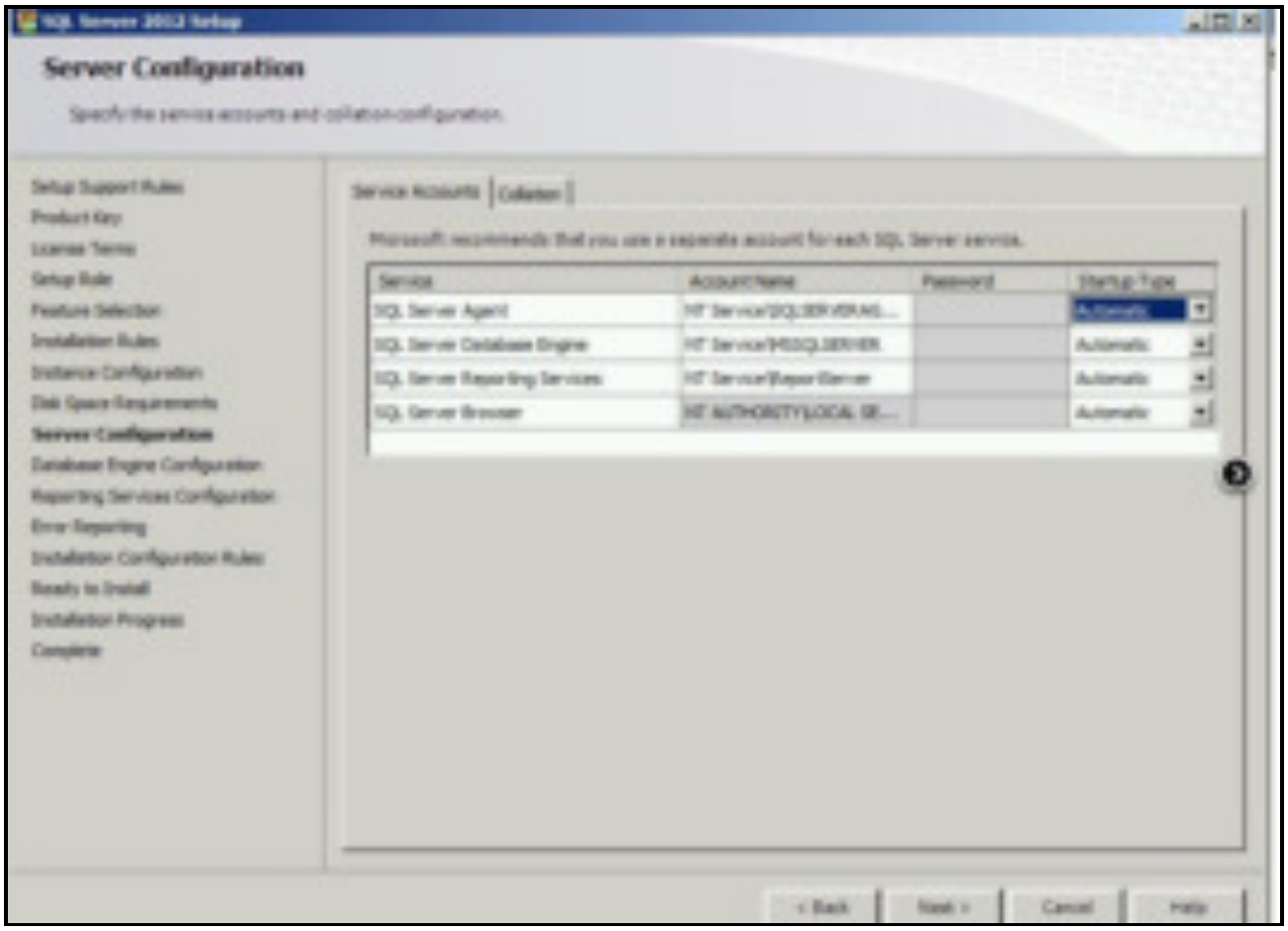
Установите Windows Management Framework 3.0.

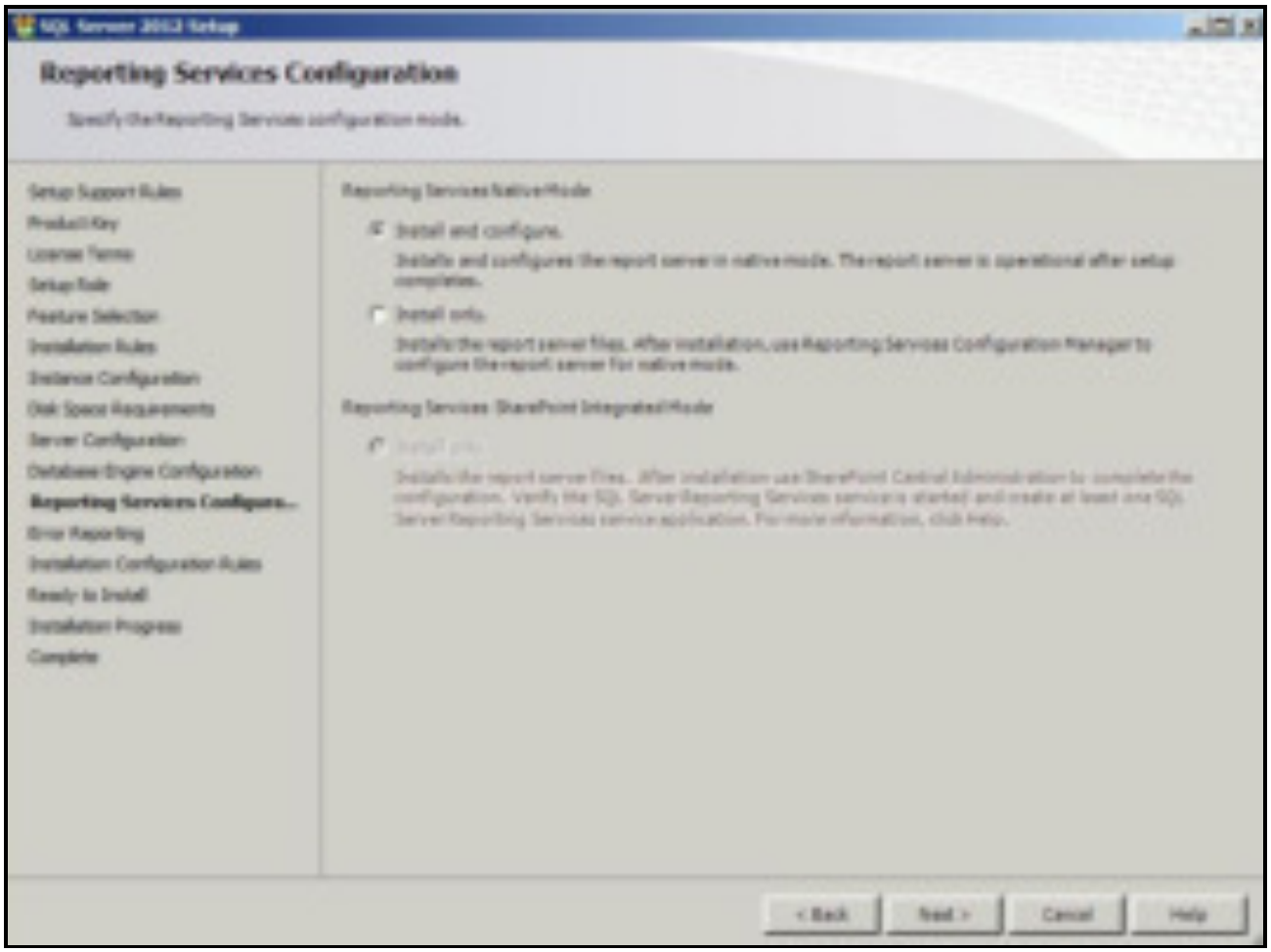
Первое установим SQL сервер.

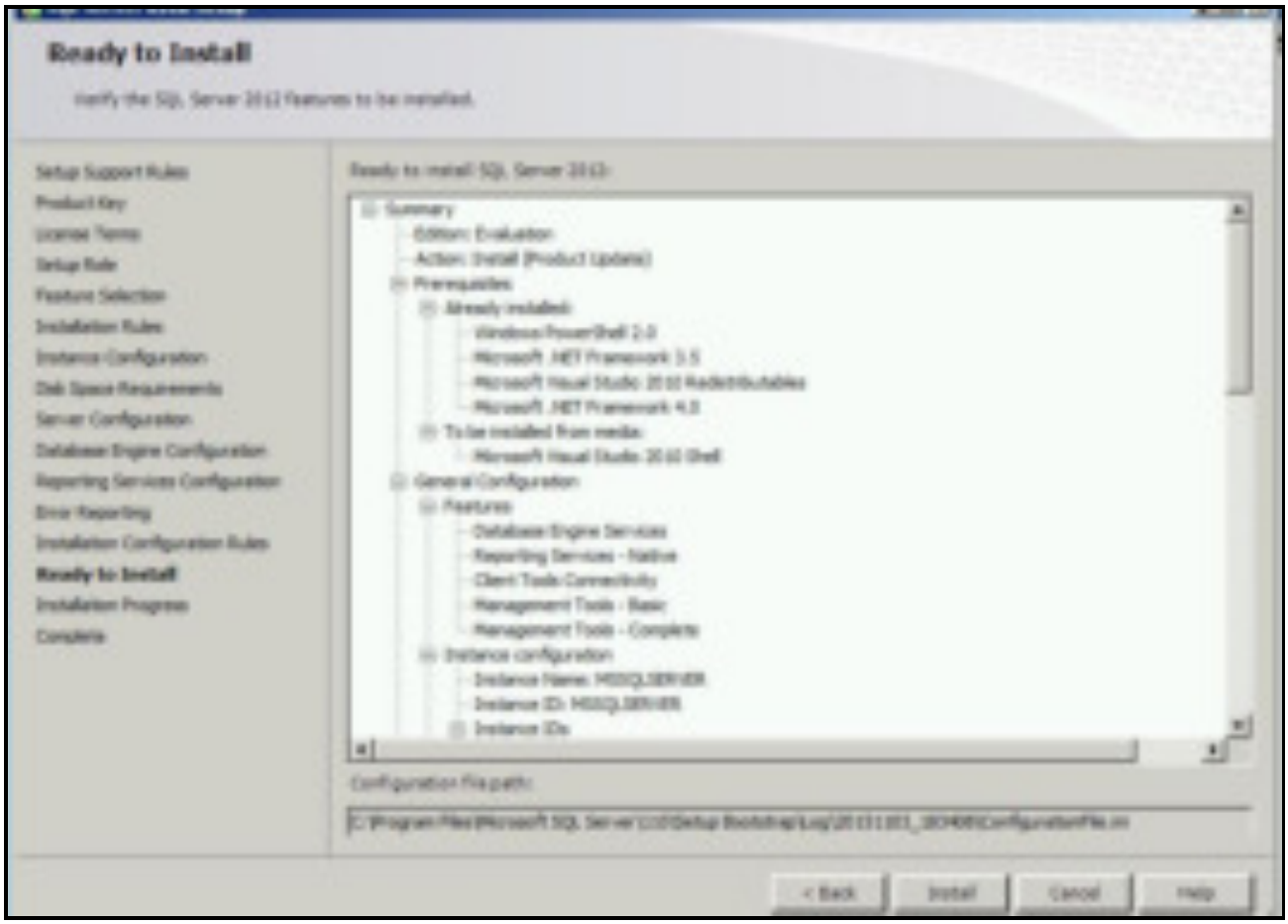

Setup Support Rules
Setup Support Rules
Rule
Status
Setup administrator
Setup account privileges
Restart computer
Consistency validation for SQL Server registry keys
Long path names to files on SQL Server installation media
SQL Server Setup Product Incompatibility
Passed
OK
Cancel

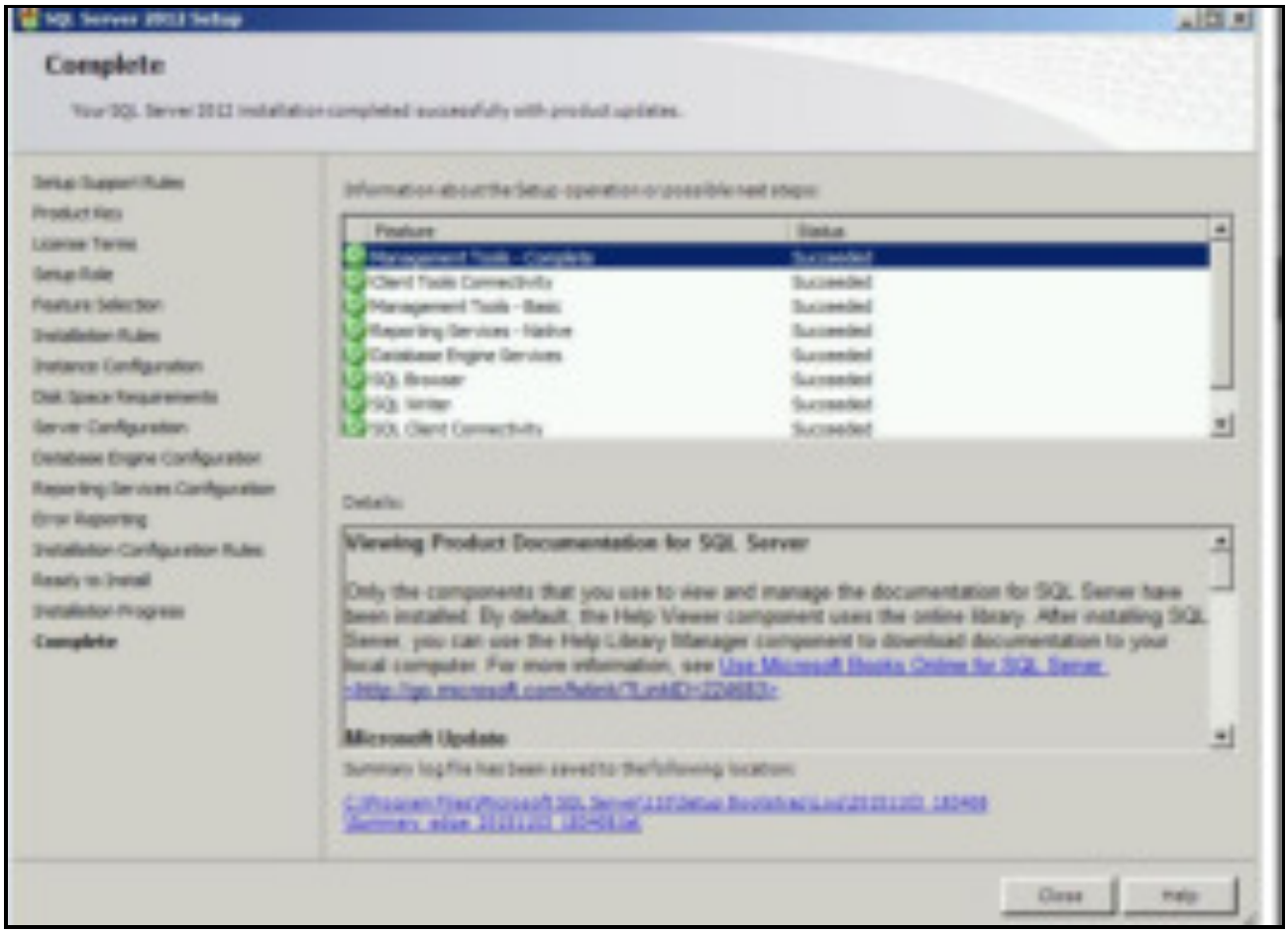

Feature Selection
Setup Support Rules
Product Key
License Terms
Setup Role
Feature Selection
Installation Rules
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Error Reporting
Installation Configuration Rules
Ready to Install
Installation Progress
Complete
Features:
Instance Features
Database Engine Services
SQL Server Replication
Full-Text and Semantic Extractions for Search
Data Quality Services
Analysis Services
Reporting Services - Native
Shared Features
Reporting Services - SharePoint
Reporting Services Add-in for SharePoint Products
Data Quality Client
SQL Server Data Tools
Client Tools Connectivity
Integration Services
Client Tools Backwards Compatibility
Client Tools SDK
Documentation Components
Management Tools - Basic
Management Tools - Complete
Distributed Replay Controller
Feature description:
Client Tools Backwards Compatibility
Prerequisites for selected features:
Already installed:
Windows PowerShell 2.0
Microsoft .NET Framework 3.5
Microsoft Visual Studio 2010 Redistributable
Microsoft .NET Framework 4.0
To be installed from media:
Microsoft Visual Studio 2010 Shell
Select All
Unselect All
< Back
Next >
Cancel
Help


Instance Configuration
Default instance
Named instance:
Instance ID:
Instance root directory:
SQL Server directory:
Reporting Services directory:
Installed instances:
Instance Name
Instance ID
Features
Edition
Version
< Back
Next >
Cancel
Help

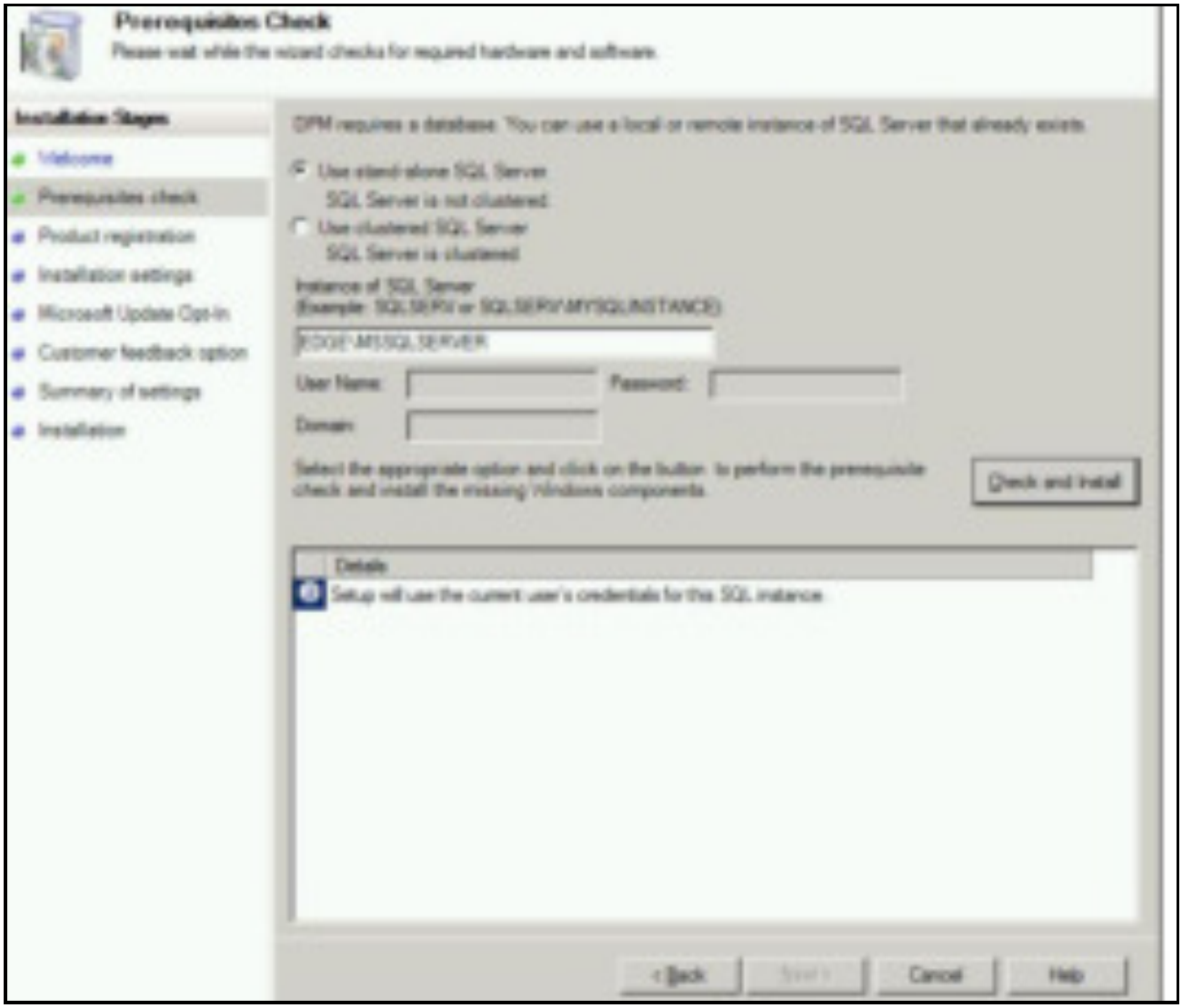

Server Configuration
Service Accounts
Collation
Service
Account Name
Password
Startup Type
SQL Server Agent
SQL Server Database Engine
SQL Server Reporting Services
SQL Server Browser
Automatic
< Back
Next >
Cancel
Help


Reporting Services Configuration
Setup Support Rules
Product Key
License Terms
Setup Role
Feature Selection
Installation Rules
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Reporting Services Configura...
Error Reporting
Installation Configuration Rules
Ready to Install
Installation Progress
Complete
Reporting Services Native Mode
Install and configure.
Reporting Services SharePoint Integrated Mode
< Back
Next >
Cancel
Help

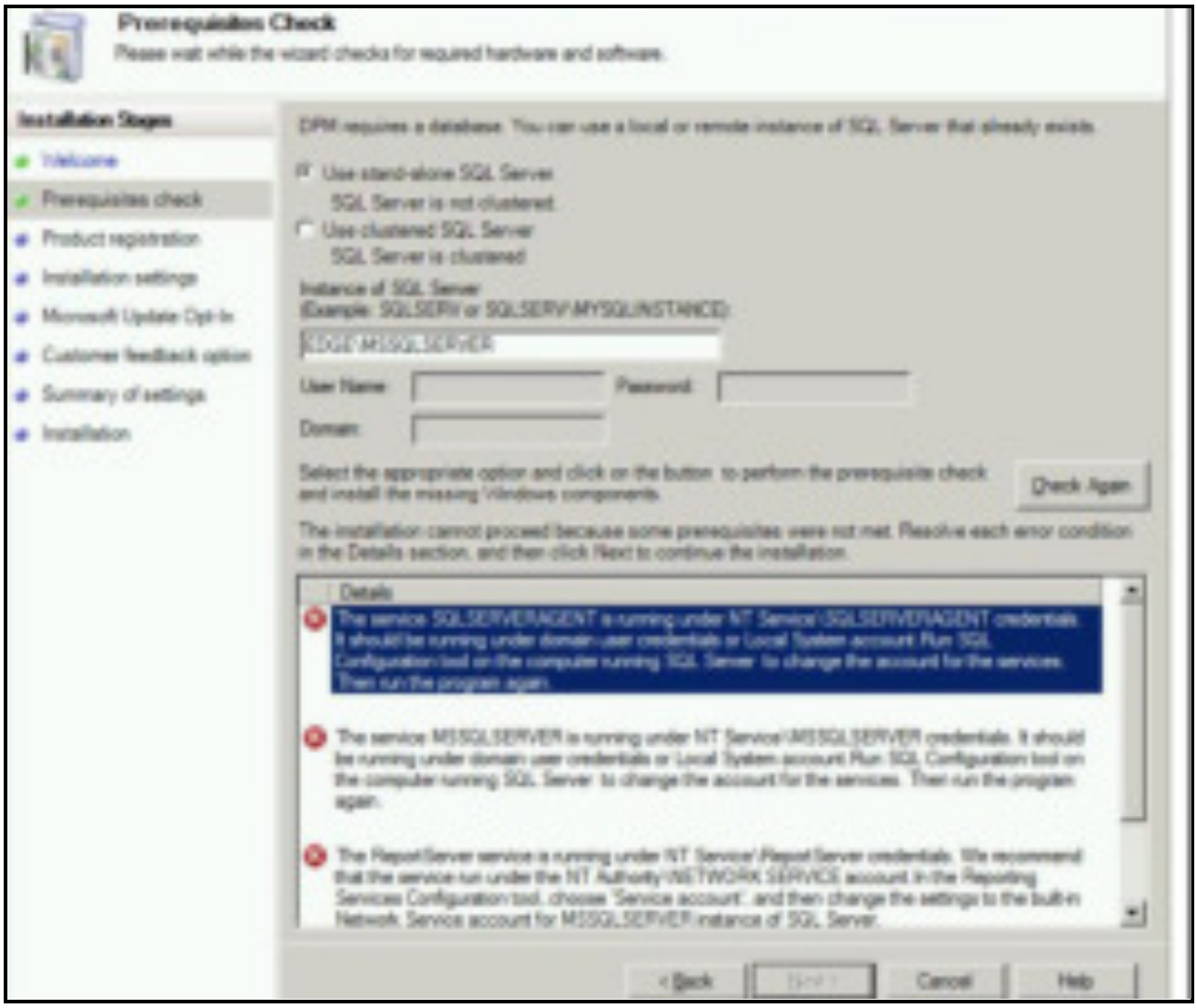

Ready to Install
Setup Support Rules
Product Key
License Terms
Setup Role
Feature Selection
Installation Rules
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Error Reporting
Installation Configuration Rules
Ready to Install
Installation Progress
Complete
Summary
Prerequisites
General Configuration
Features
Instance configuration
Configuration file path:
< Back
Install
Cancel
Help


Complete
Setup Support Rules
Product Key
License Terms
Setup Role
Feature Selection
Installation Rules
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Error Reporting
Installation Configuration Rules
Ready to Install
Installation Progress
Complete
Feature
Status
Management Tools - Complete
Succeeded
Client Tools Connectivity
Succeeded
Management Tools - Basic
Succeeded
Reporting Services - Native
Succeeded
Database Engine Services
Succeeded
SQL Browser
Succeeded
SQL Writer
Succeeded
SQL Client Connectivity
Succeeded
Details:
Viewing Product Documentation for SQL Server
Microsoft Update
Close
Help

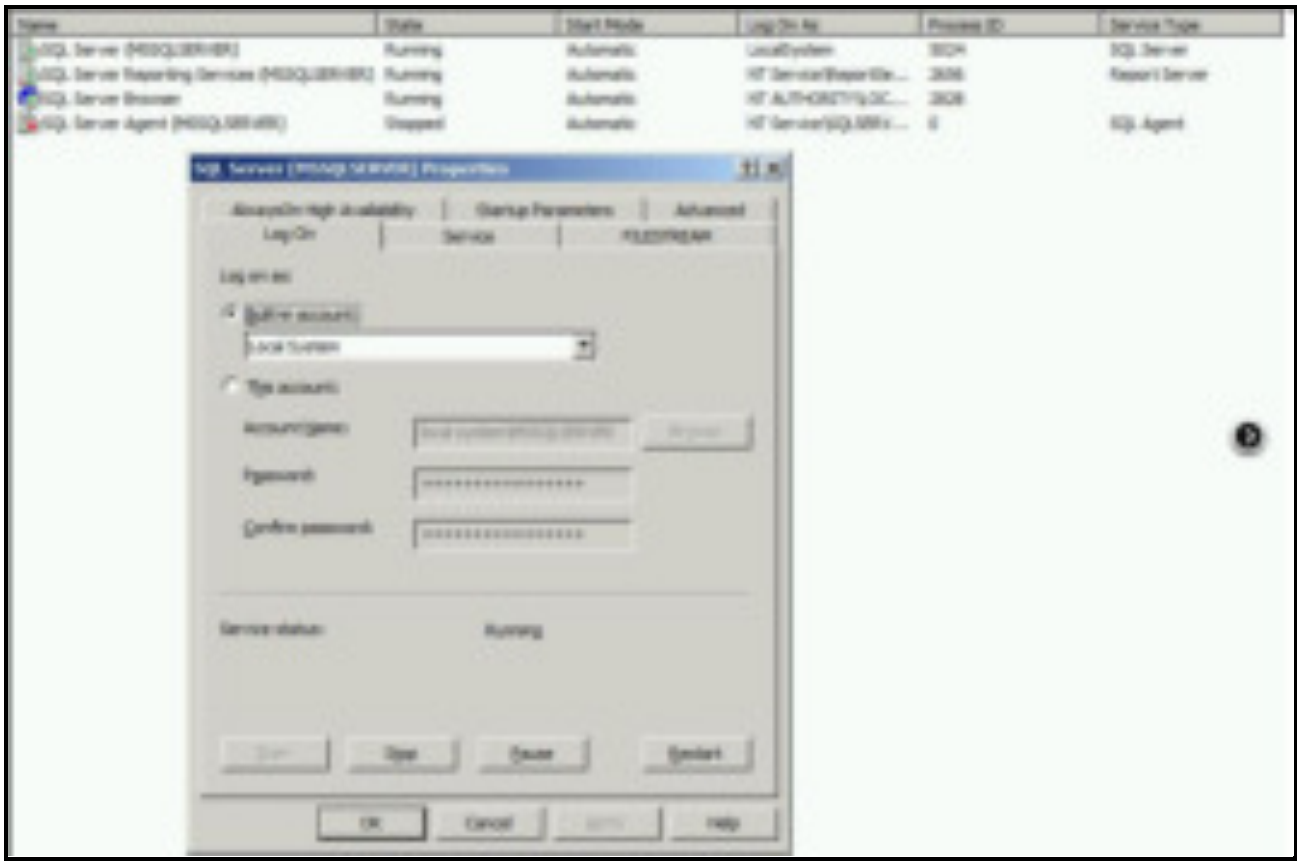
Теперь запускаем установку DPM, указываем наш сервер и instance MS SQL.

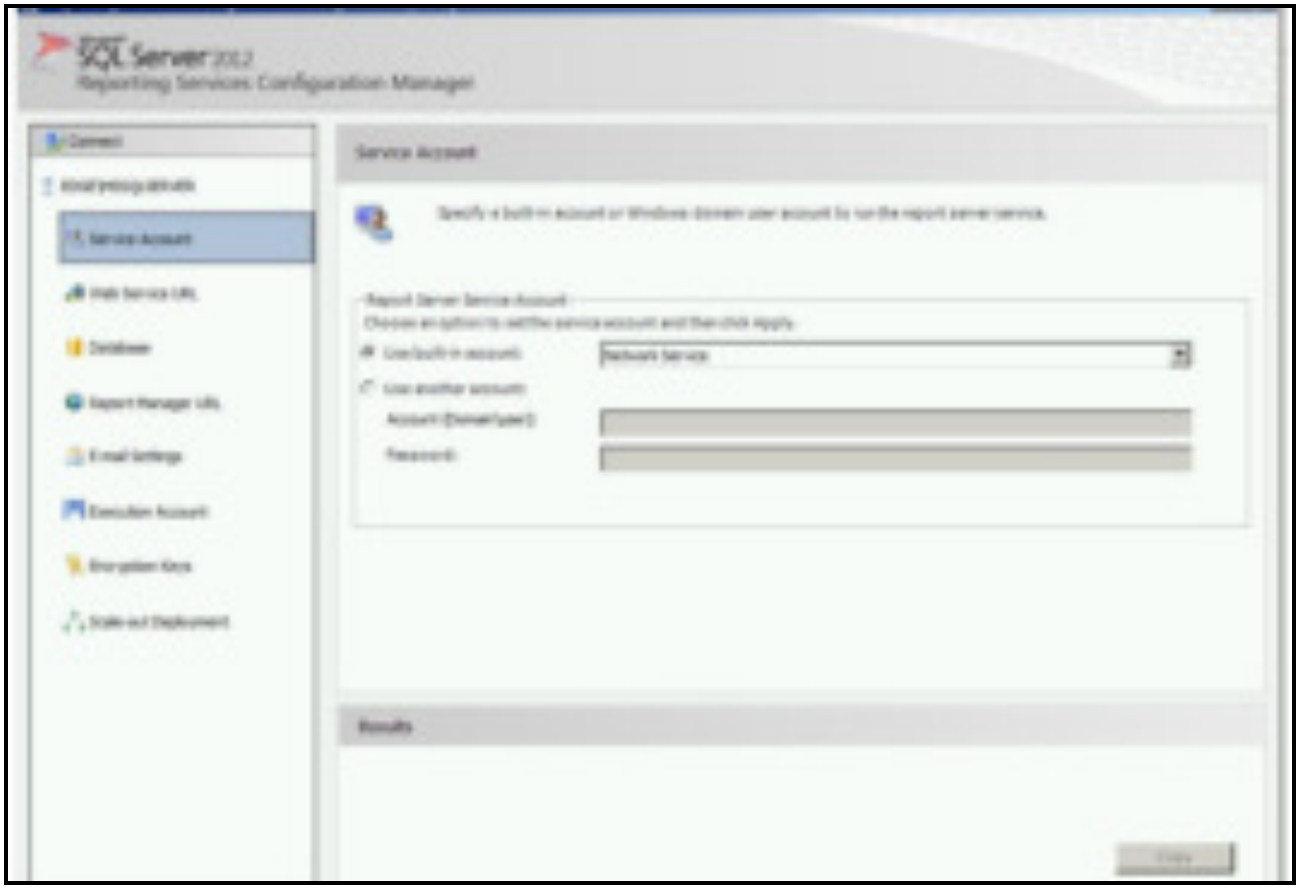



Нажимаем check and install и получаем следующие ошибки:

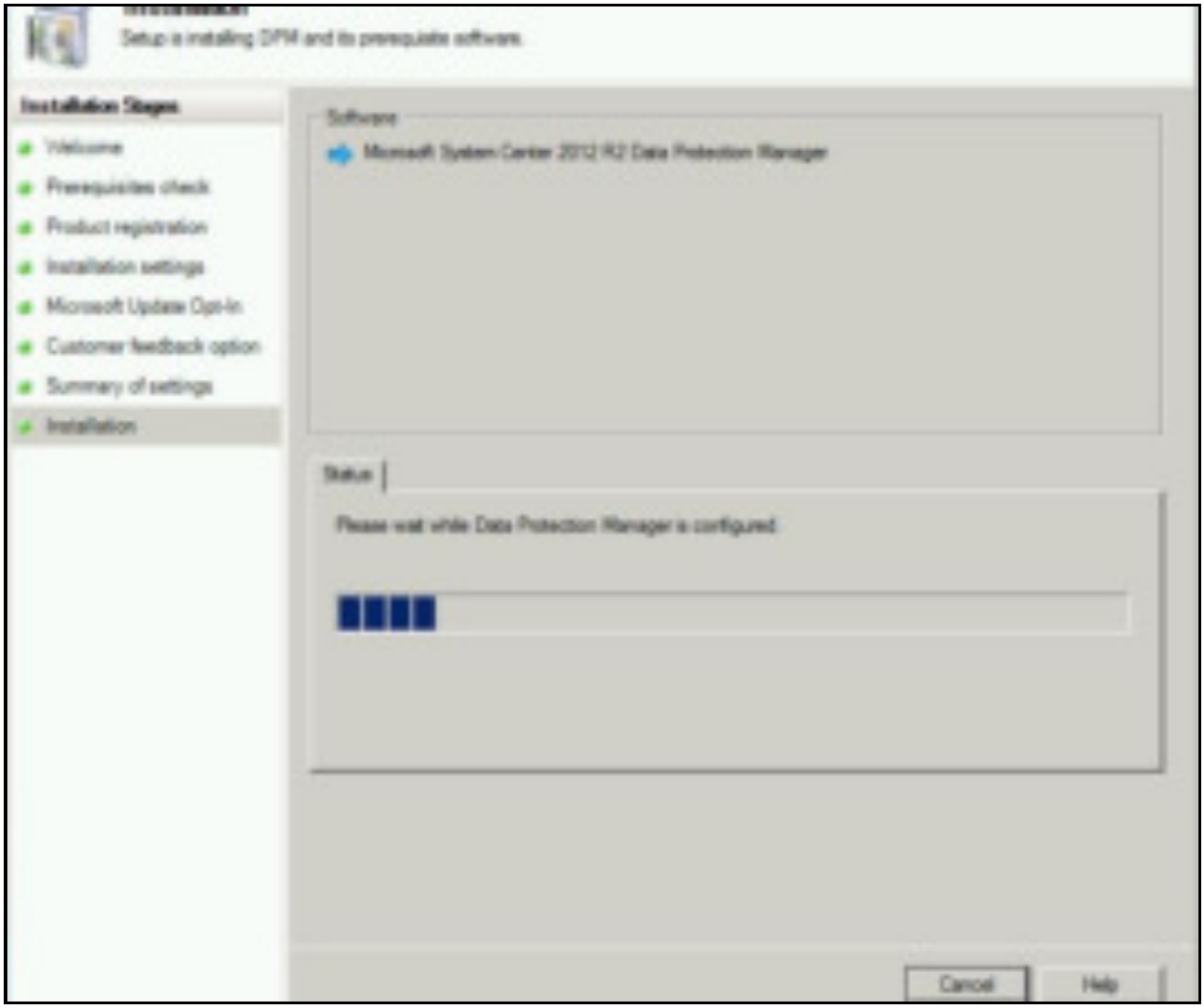


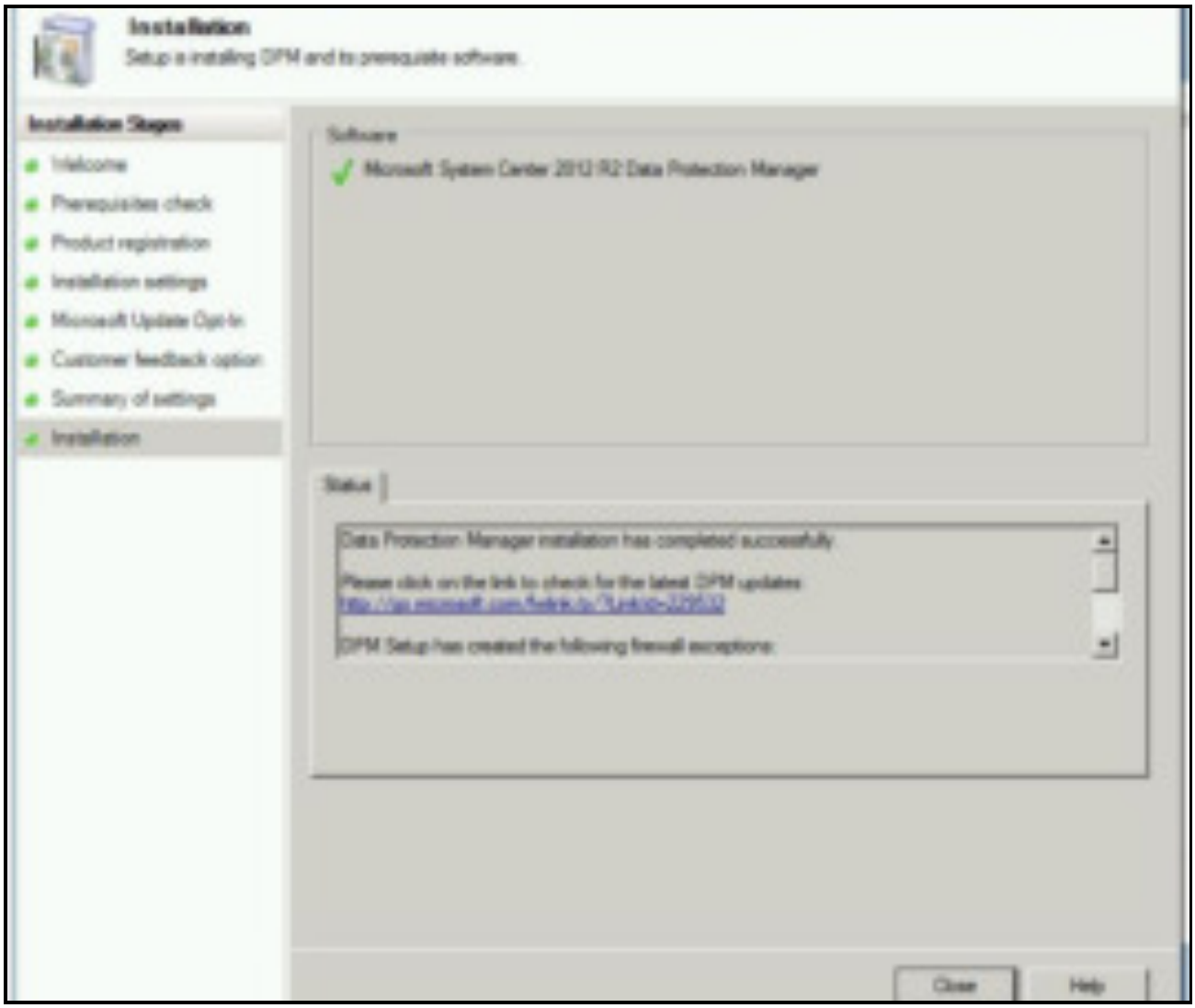

Поэтому сконфигурируем запуск служб так, как этого просит установщик. Запуск Reporting services настраиваем через его панель управления.




SQL Server 2012
Reporting Services Configuration Manager
Service Account
Results

Теперь установка успешно запускается и успешно продолжается.



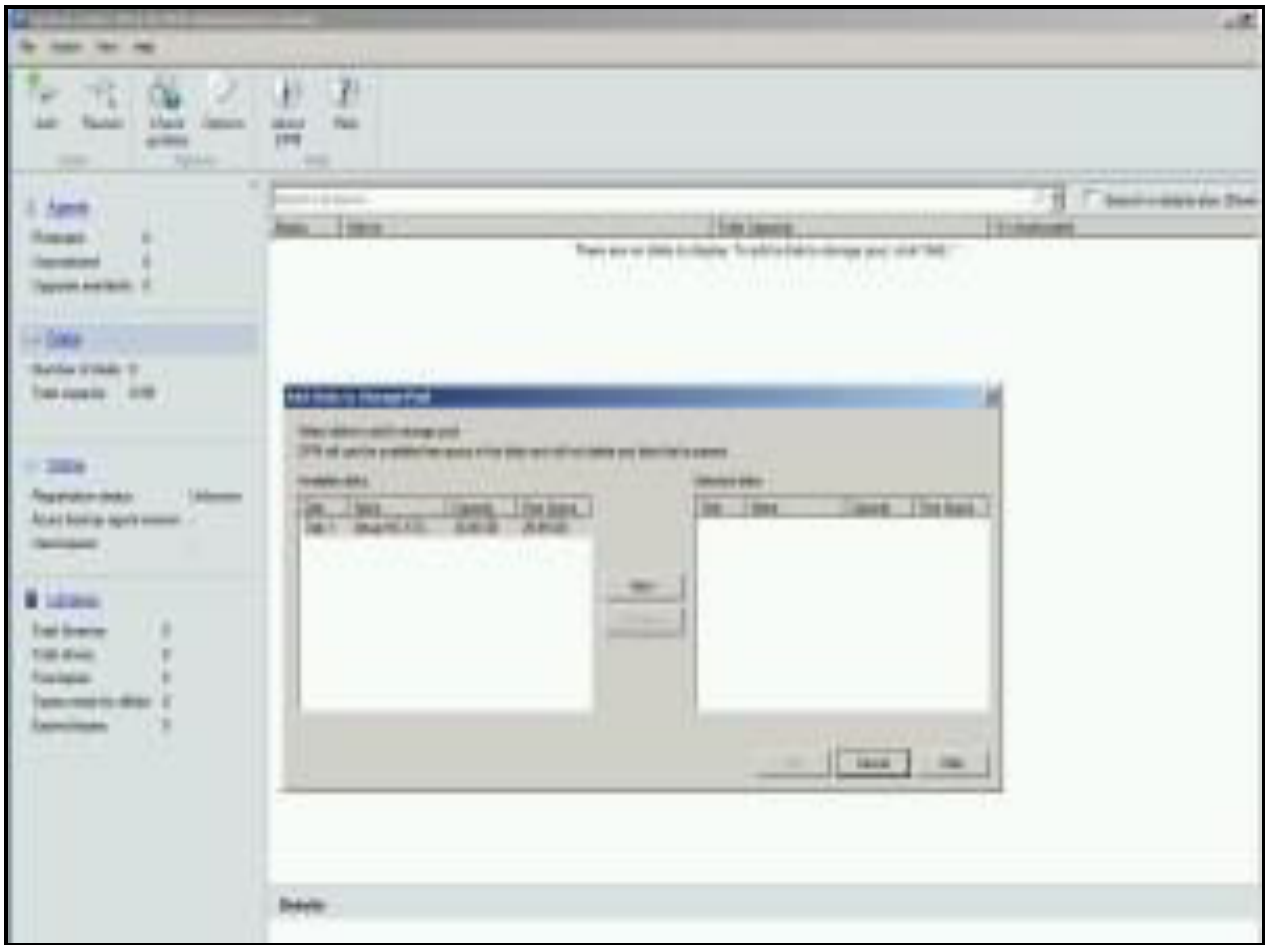


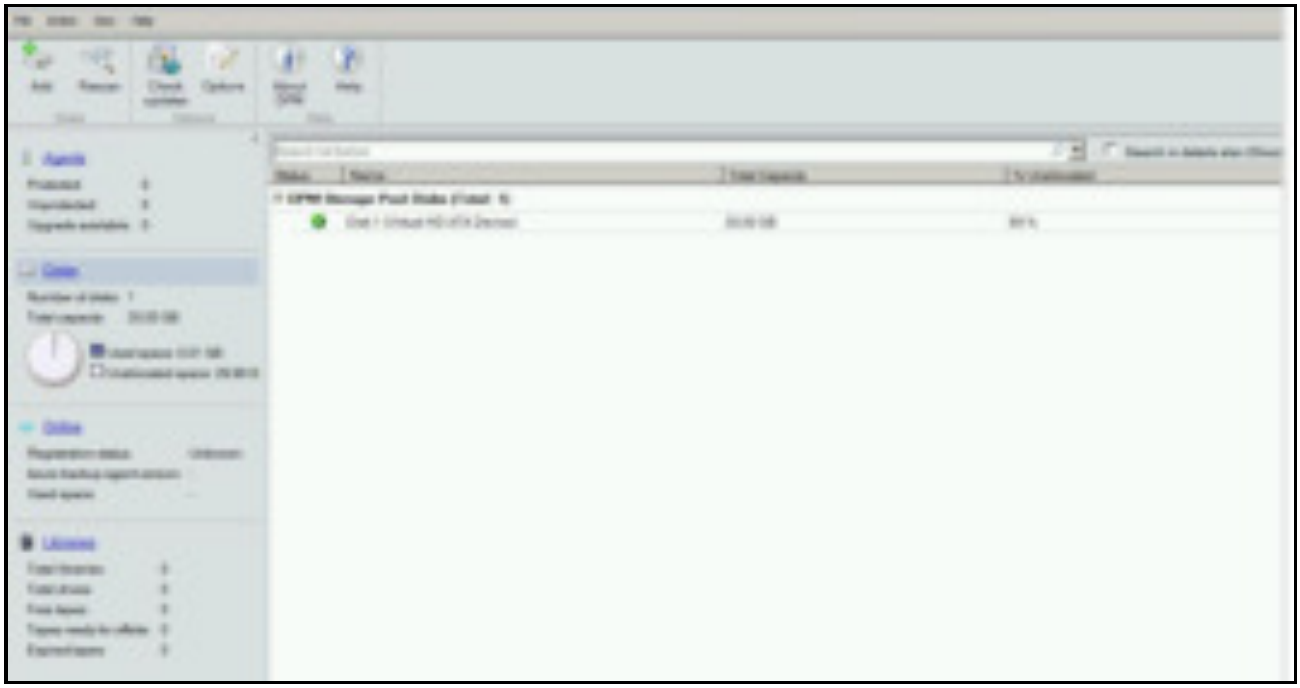

Далее нам нужно настроить DPM. Добавим систему хранения для бэкапов.

Добавить можно ленточную библиотеку, хранить данные в облаке microsoft azure, вот примерные расценки:

| DATA STORED PER PROTECTED INSTANCE PER MONTH | PRICE |
|---|---|
| Instances up to 50GB of data | PhP250 per protected instance + Storage consumed |
| Instances between 50GB to 500GB of data | PhP500 per protected instance + Storage consumed |
| Instances greater than 500GB of data | Increments of PhP500 for each 500GB + Storage consumed |

Перейдем в раздел managment-disks-add. На диске не должно быть разделов.



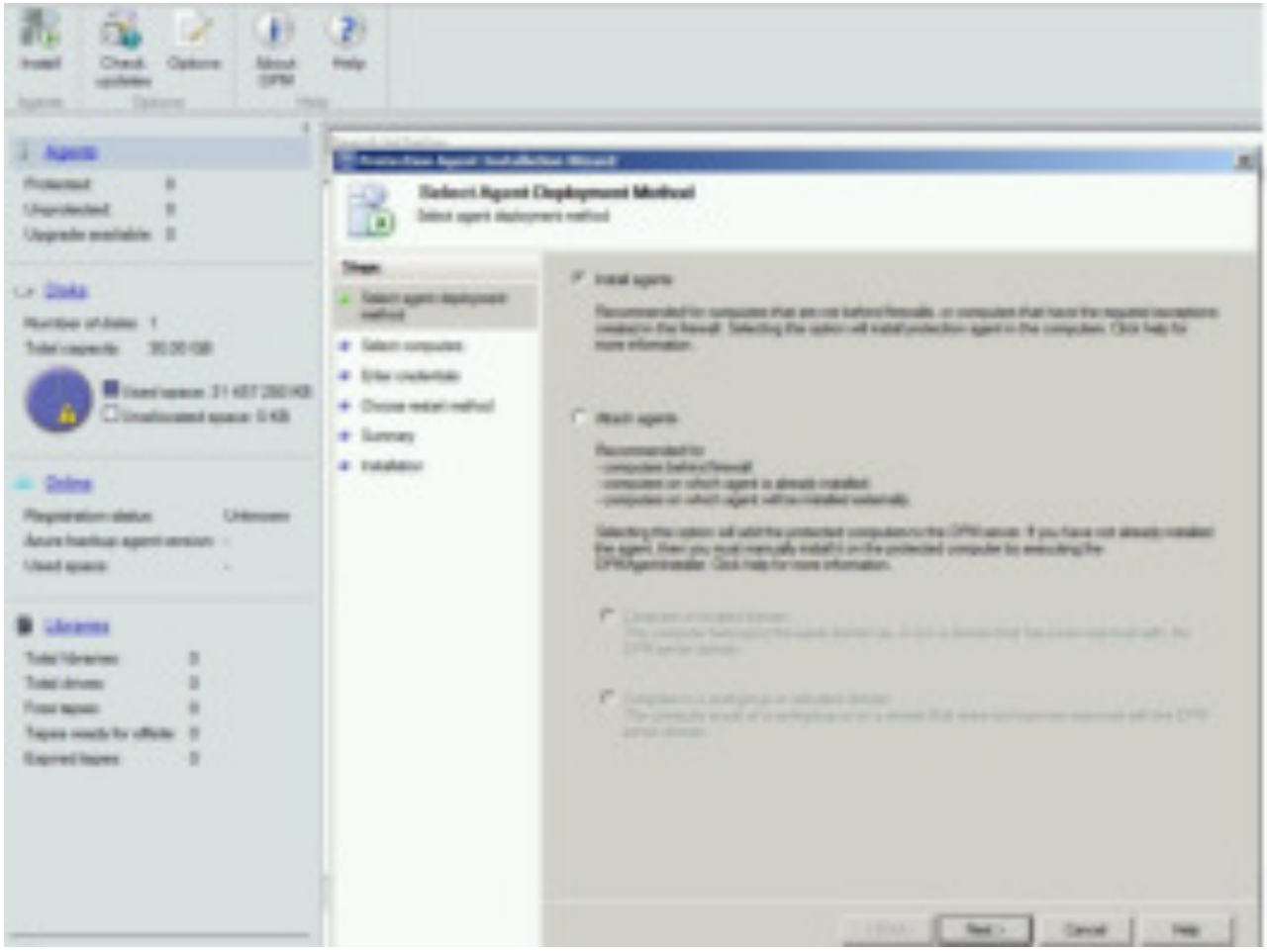


Теперь можно установить агенты защиты на нужные нам компьютеры. Если это компьютеры в домене – выбираем install agents, если же доступ ограниченный выбираем attach agents.

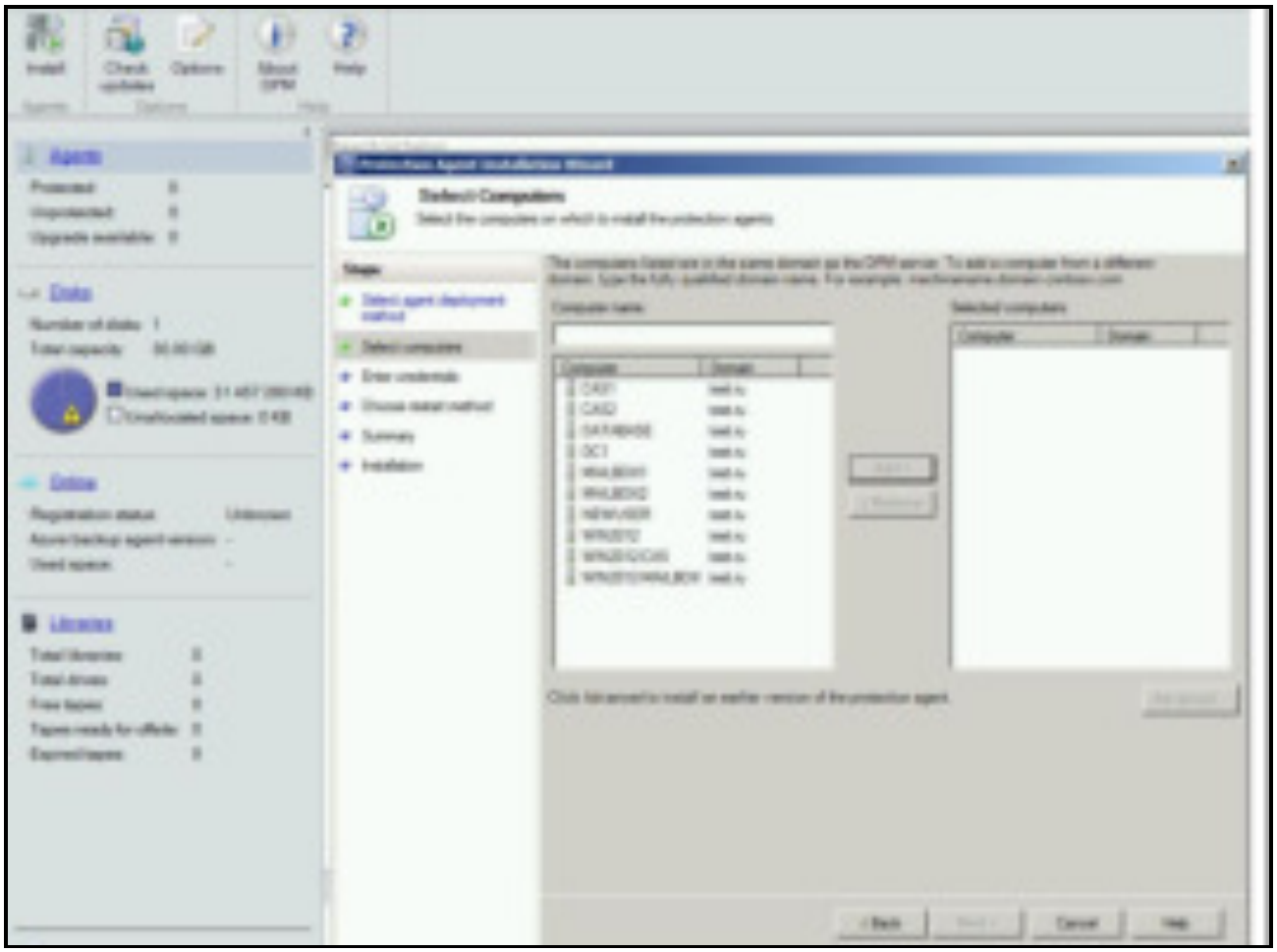
В этом случае предварительно нужно будет вручную установить агента DPM на компьютер. Установщики находятся по следующему пути: “C:\Program Files\Microsoft DPM\DPM\ProtectionAgents\RA\”

Подробный мануал для такого случая расписан на technet.microsoft.com.

Установим агентов напрямую и выберем пункт “install”. Список портов которые нужны для функционирования DPM можно посмотреть здесь.

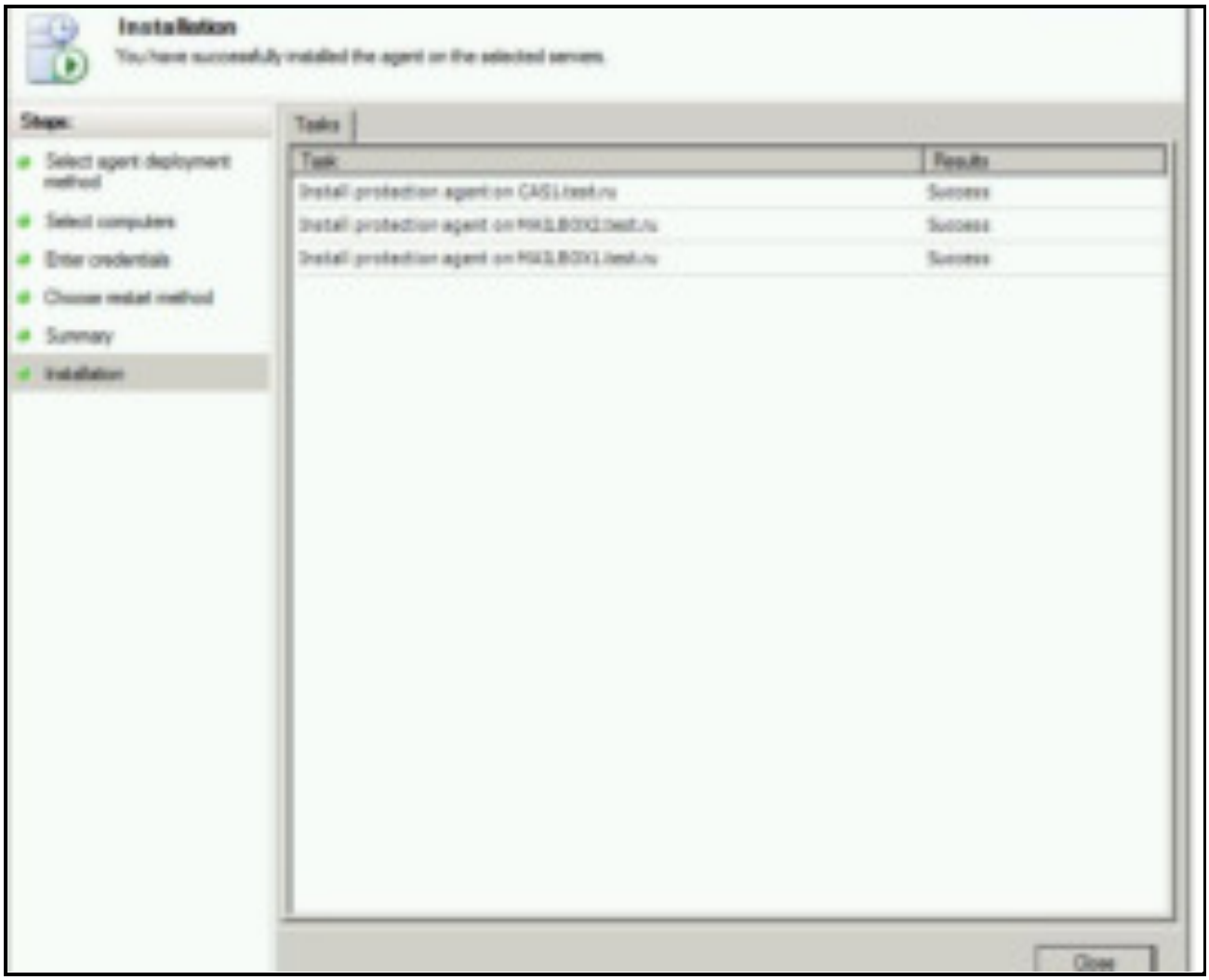


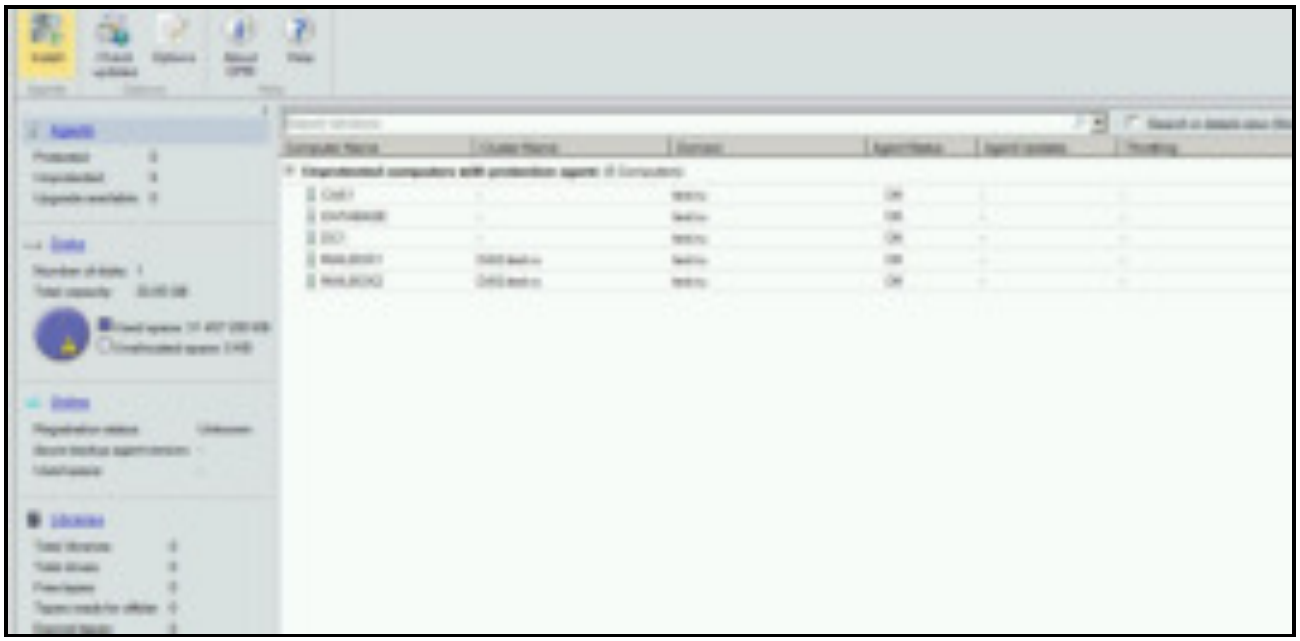
Далее сможем выбрать те сервера, которые желаем защитить:



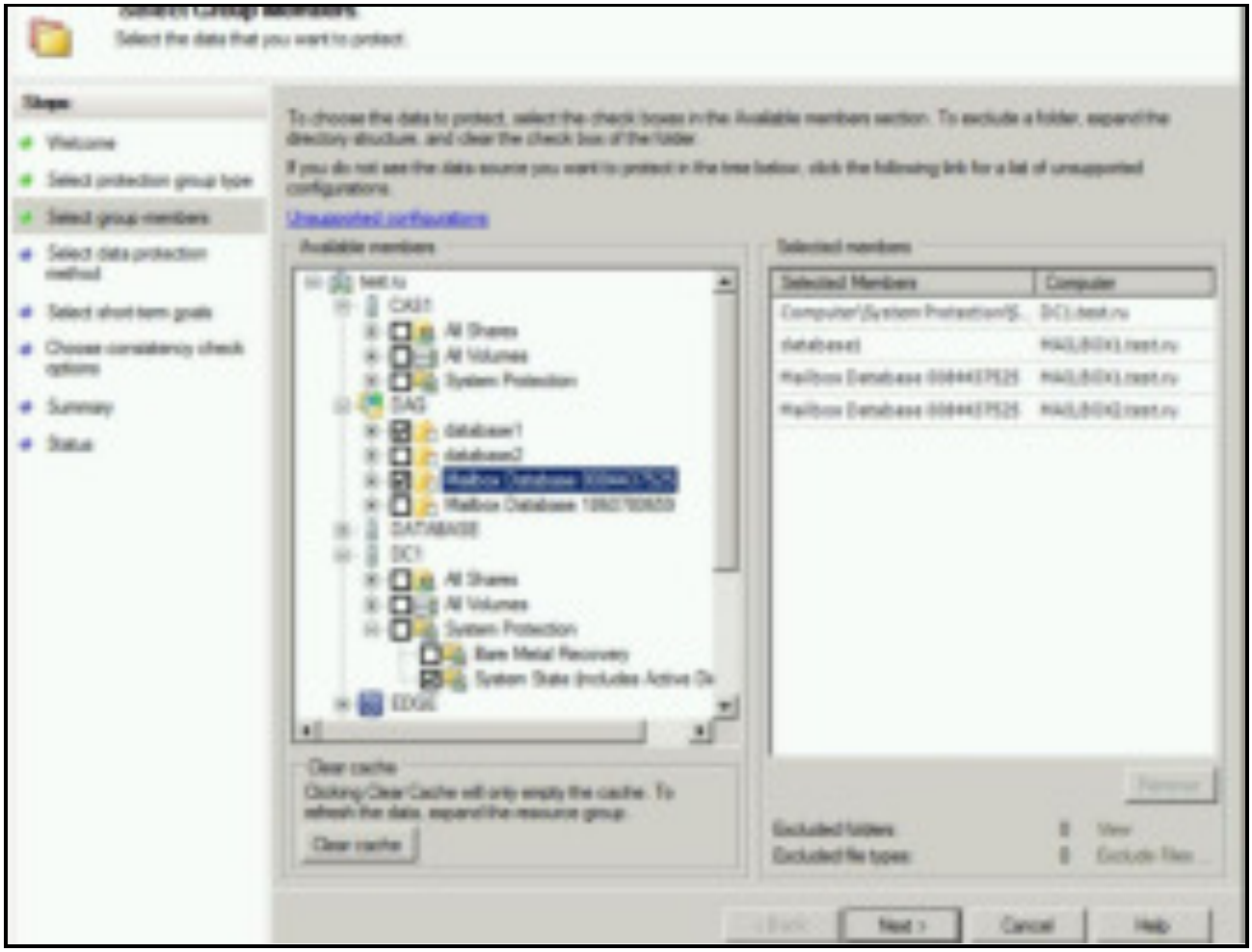
Не забудьте, что на защищаемых серверах должен быть установлен Microsoft .NET Framework 4.0.

При удачной установке мы увидим примерно следующую картину:

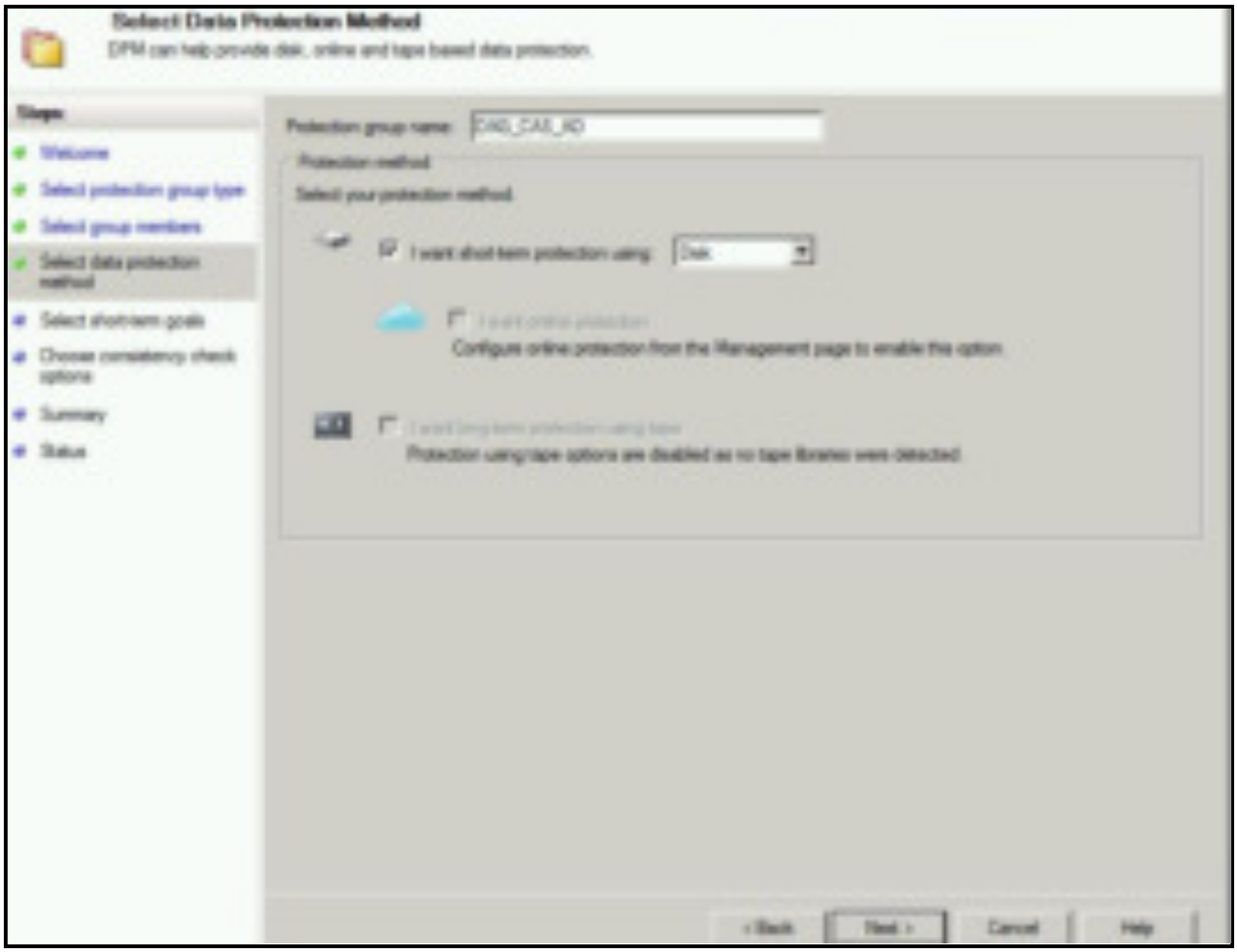

Installation
Steps:
Select agent deployment method
Select computers
Enter credentials
Choose restart method
Summary
Installation
Tasks
Task
Results
Success
Success
Success
Close



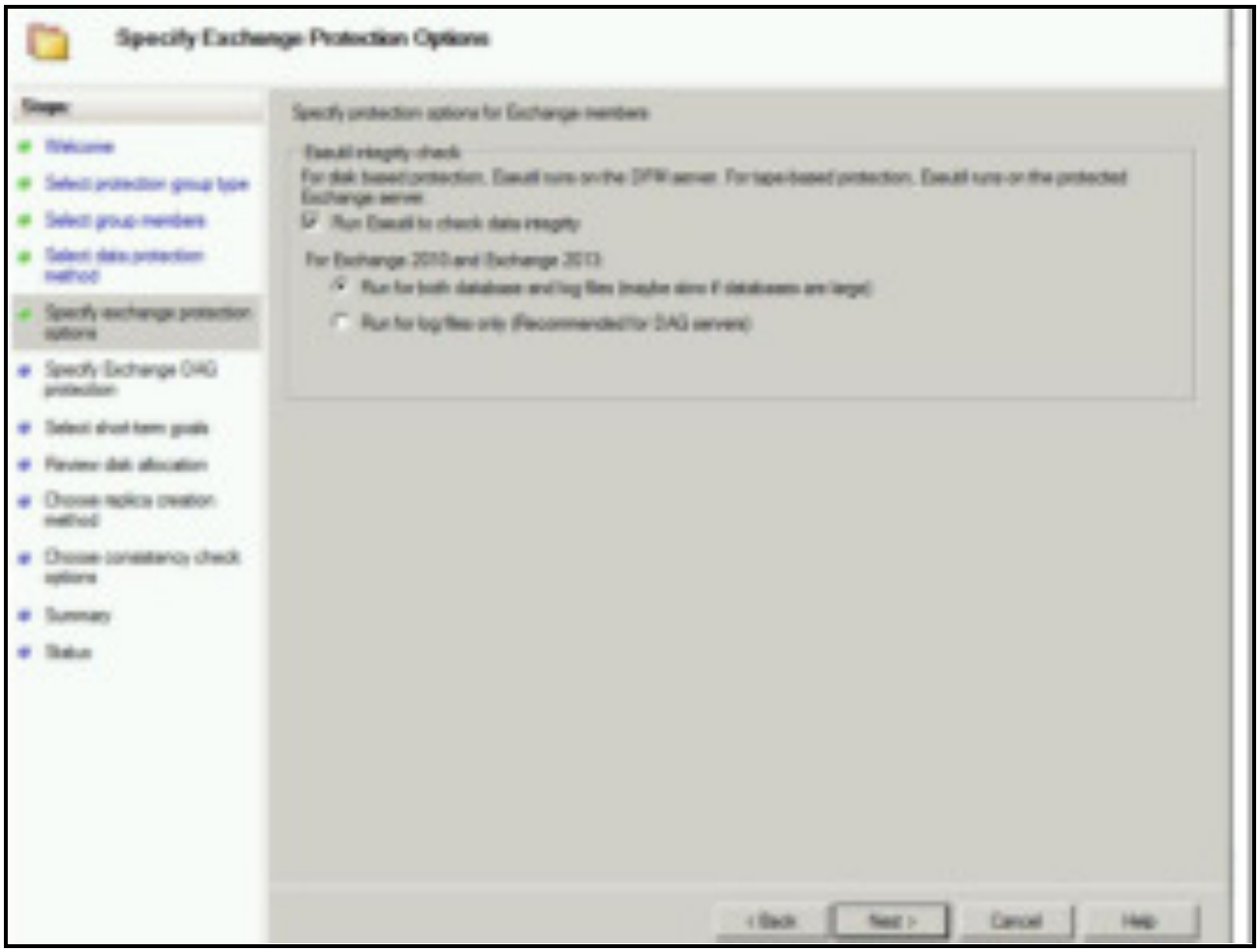
Теперь нам нужно создать группу защиты. Заходим в меню protection-new. Выбираем что будем защищать – клиентские машины или сервера, в нашем случае у нас сервера. И выбираем что конкретно хотим хранить в резервной копии.



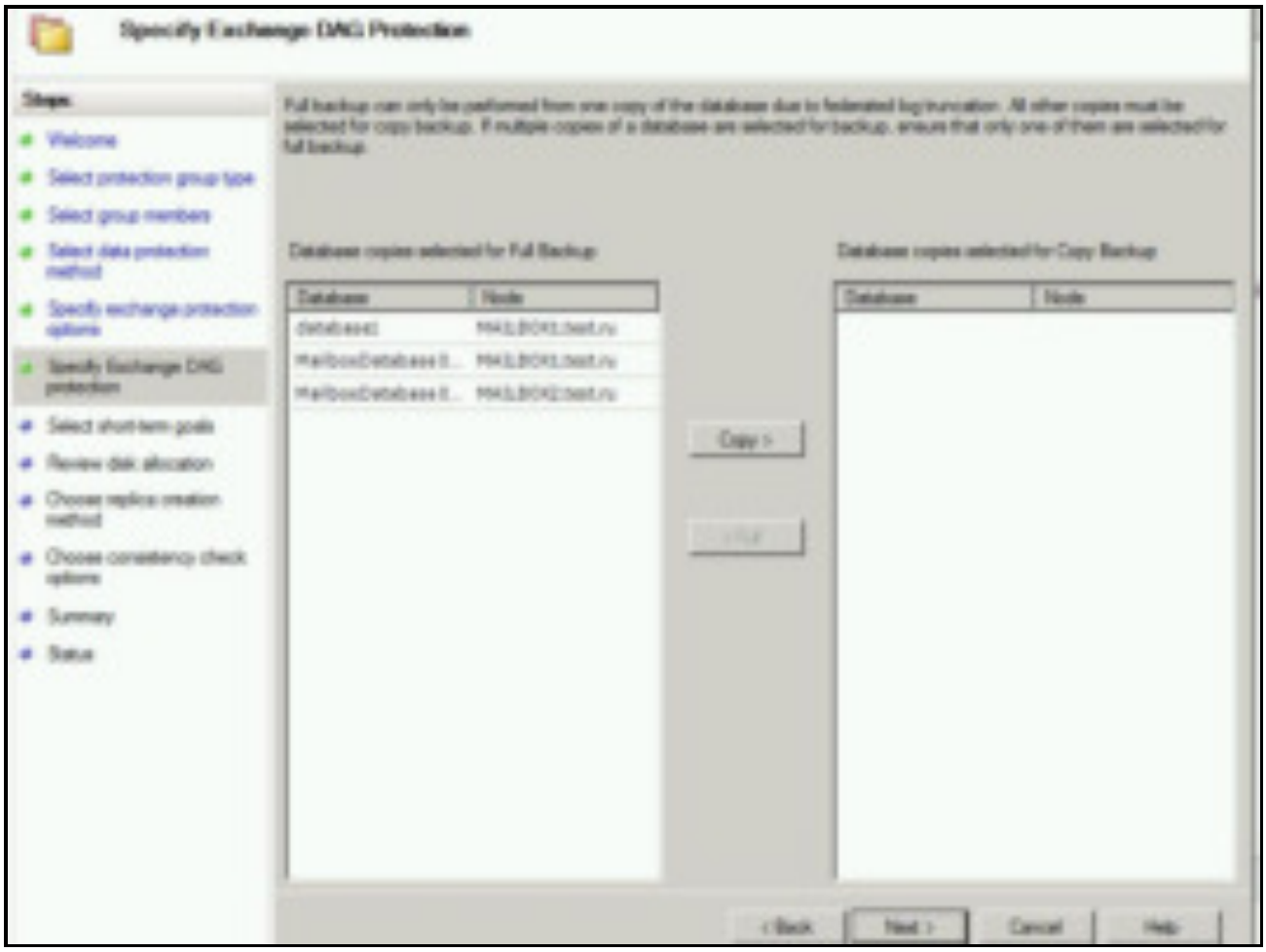

Придумываем осмысленное название для группы хранения, ставим галочку “short-term protection”, то есть краткосрочное хранение (долгосрочное возможно при использовании ленточных библиотек)



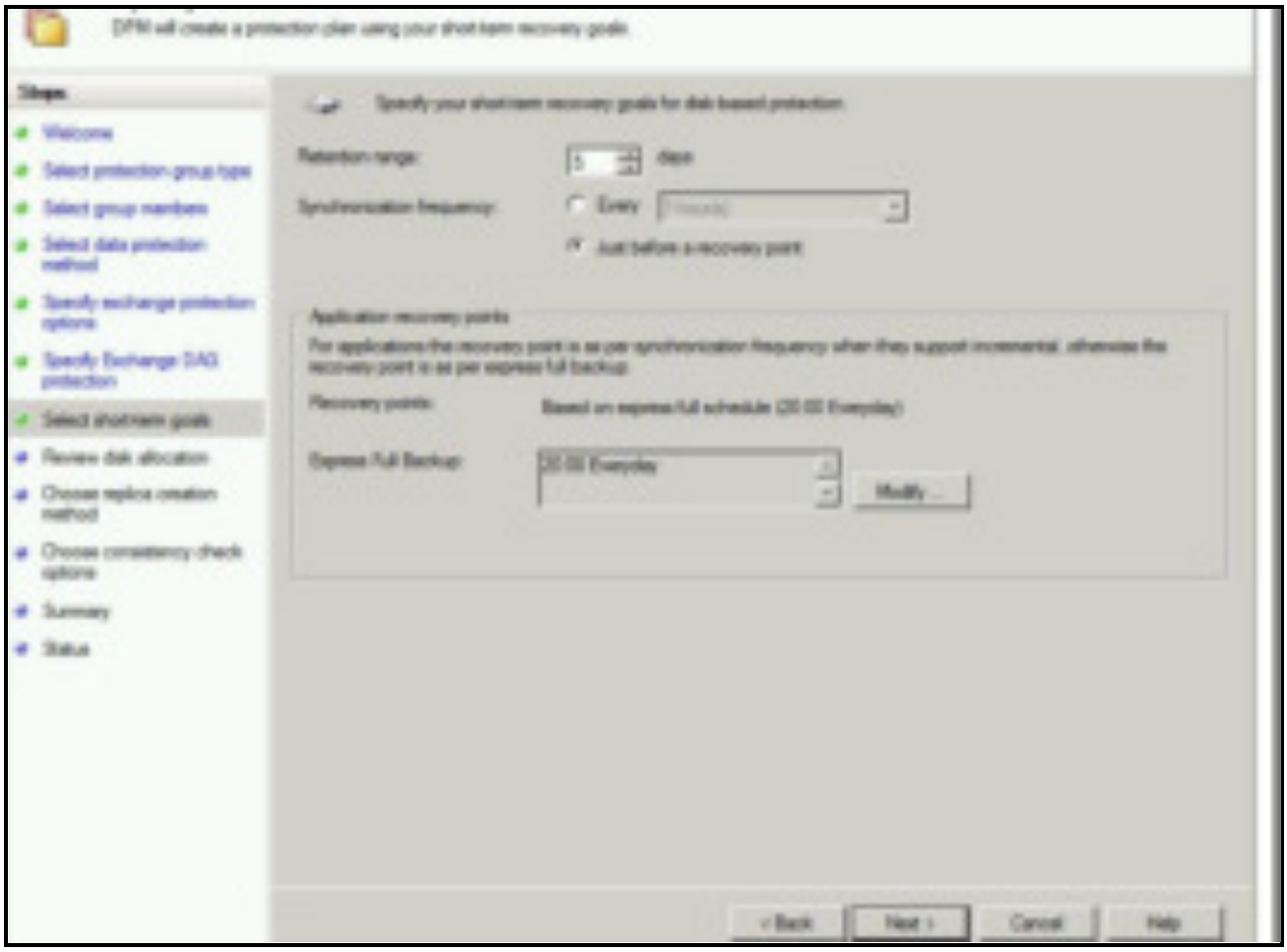

Далее можно выбрать проверку базы exchange утилитой esutil.



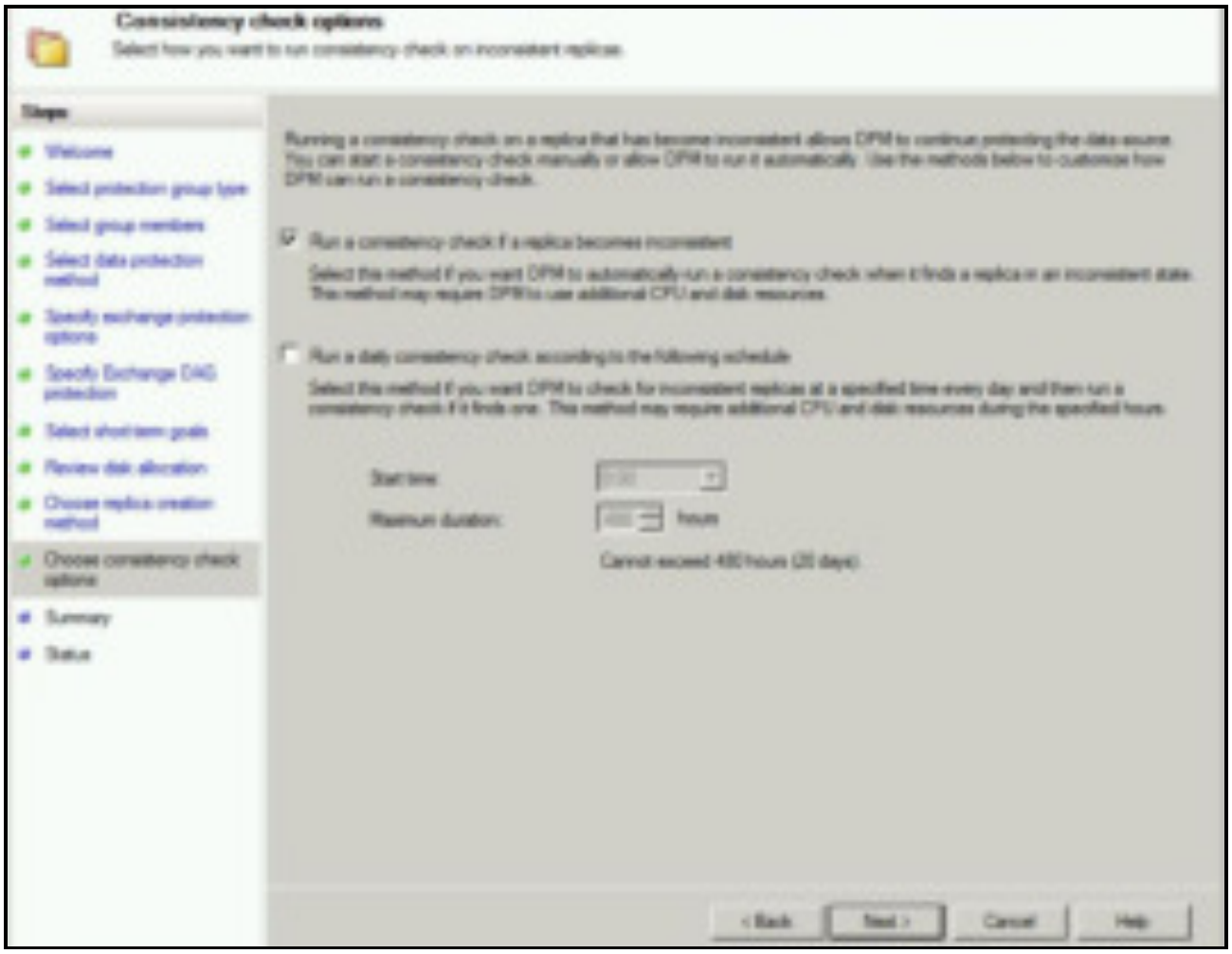

На следующем этапе выбираем full backup для баз exchange с усечением логов.




Выбираем сколько мы хотим хранить сохранённые данные, и когда делать очередной бэкап.




Выбираем проверку целостности реплики:




Настраиваем время запуска, переходим на вкладку monitoring и наблюдаем за процессом копирования данных.

**Практическое занятие №22 Мониторинг производительности и работоспособности инфраструктуры клиентских ОС Настройка**

***Цель работы:***

Изучить: Мониторинг производительности и работоспособности инфраструктуры клиентских ОС. Настройка

**Мониторинг производительности**

Рассмотрим два основных инструмента мониторинга производительности систем Windows Server — программу " ***Диспетчер задач*** ", которая предназначена для мониторинга работы приложений и служб сервера в реальном времени, и консоль " ***Производительность*** ", которая может осуществлять мониторинг производительности как в реальном времени, так и путем накопления статистики о работе системы за определенный период

времени, причем консоль " ***Производительность*** " может показывать и собирать данные одновременно с нескольких систем.

**Диспетчер задач**

Чтобы открыть " ***Диспетчер задач*** ", основной инструмент мониторинга и управления системными процессами и приложениями, нужно выполнить одно из перечисленных действий:

- нажать комбинацию клавиш CTRL+SHIFT+ESC;
- нажать комбинацию клавиш CTRL+ALT+DELETE и нажать кнопку " *Диспетчер задач* ";
- нажать кнопку " *Пуск* ", выбрать пункт меню " *Выполнить* ", ввести taskmgr и нажать кнопку " *ОК* ";
- щелкнуть правой кнопкой мыши на панели задач и выбрать в контекстном меню команду " *Диспетчер задач* ".

Настройка общих параметров " *Диспетчера задач* "

Прежде чем изучать работу данной программы по управлению приложениями и процессами, сделаем некоторые настройки, позволяющие повысить удобство использования программы:

- в меню " *Параметры* " уберем галочку у параметра "Поверх остальных окон" ("Диспетчер задач" не будет перекрывать окна других программ);
- в меню " *Вид* " у параметра " *Скорость обновления* " установим значение " *Низкая* " (это снизит нагрузку на процессор системы со стороны самого " *Диспетчера задач* ").

**Управление приложениями**

На закладке " *Приложения* " показан статус программ, работающих в данный момент в системе (рис.1)

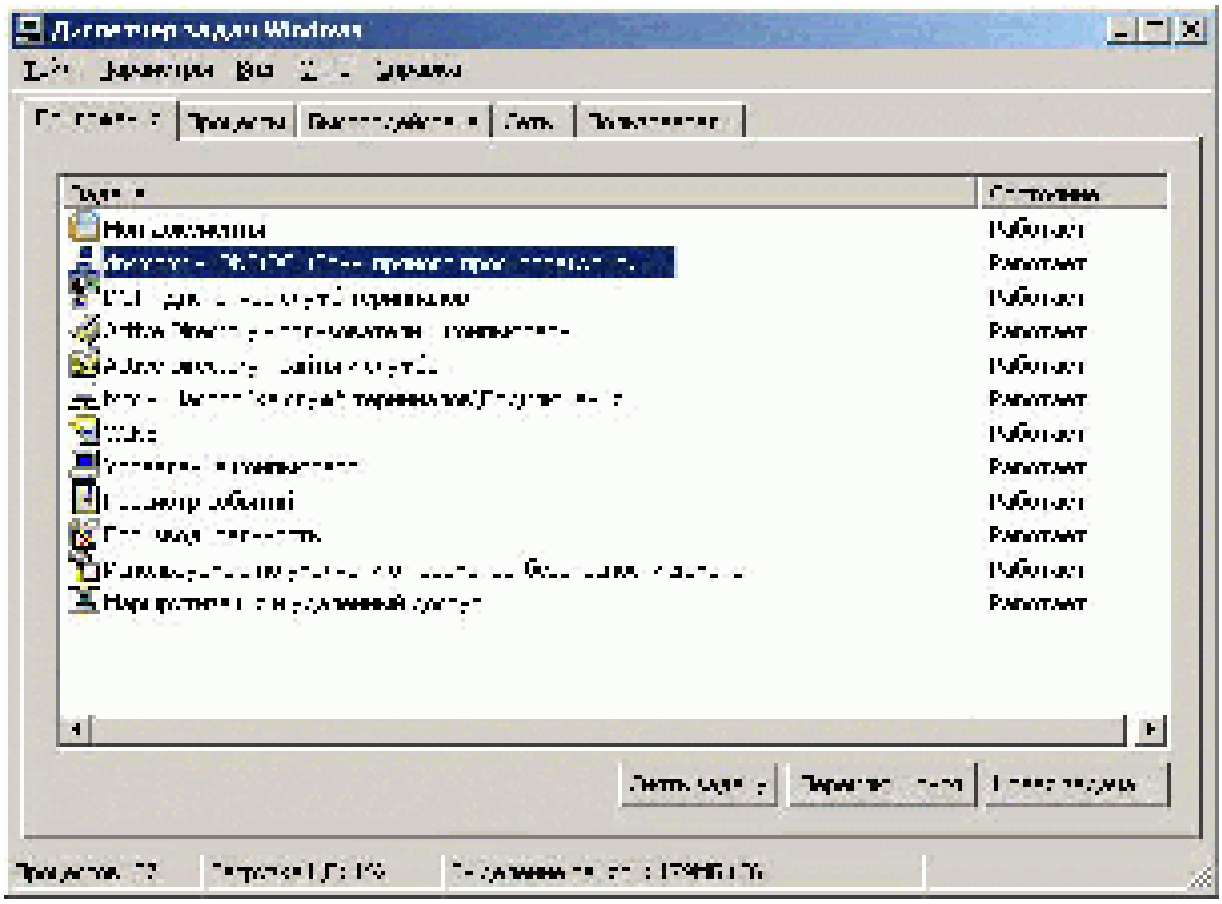


**Рис.1**

Кнопки в нижней части вкладки предназначены для выполнения следующих действий:

- остановка работы приложения — выберите приложение и щелкните кнопку " *Снять задачу* ";
- переход к окну нужного приложения — выберите приложение и щелкните кнопку " *Переключиться* ";
- запуск новой программы — щелкните кнопку " *Новая задача* " и введите команду для запуска приложения (кнопка " *Новая задача* " функционально аналогична команде " *Выполнить* " из меню " *Пуск* ").

**Замечание**. В столбце " *Состояние* " для каждого приложения указано, нормально ли выполняется данное приложение. Статус " *Не отвечает* " свидетельствует о том, что приложение, возможно, "зависло" и надо завершить связанные с ним процессы. Однако некоторые приложения не отвечают на запросы системы в ходе выполнения интенсивных расчетов. Поэтому, прежде чем закрыть приложение, убедитесь, что оно действительно "зависло".

Контекстное меню списка приложений

При щелчке правой кнопкой мыши на строке приложения или группы приложений в списке отображается контекстное меню, позволяющее:

- переходить к приложению и делать его активным;
- переводить приложение на передний план;
- сворачивать и восстанавливать приложение;
- изменять расположение окон приложений;
- закрывать приложение;
- выделять на вкладке " *Процессы* " процесс, связанный с этим приложением.

**Замечание**. Команда " *Перейти к процессу* " полезна, когда необходимо найти основной процесс для приложения, запустившего несколько процессов.

**Управление процессами**

Подробная информация о выполняемых процессах отображается на закладке " *Процессы* " (рис.2):

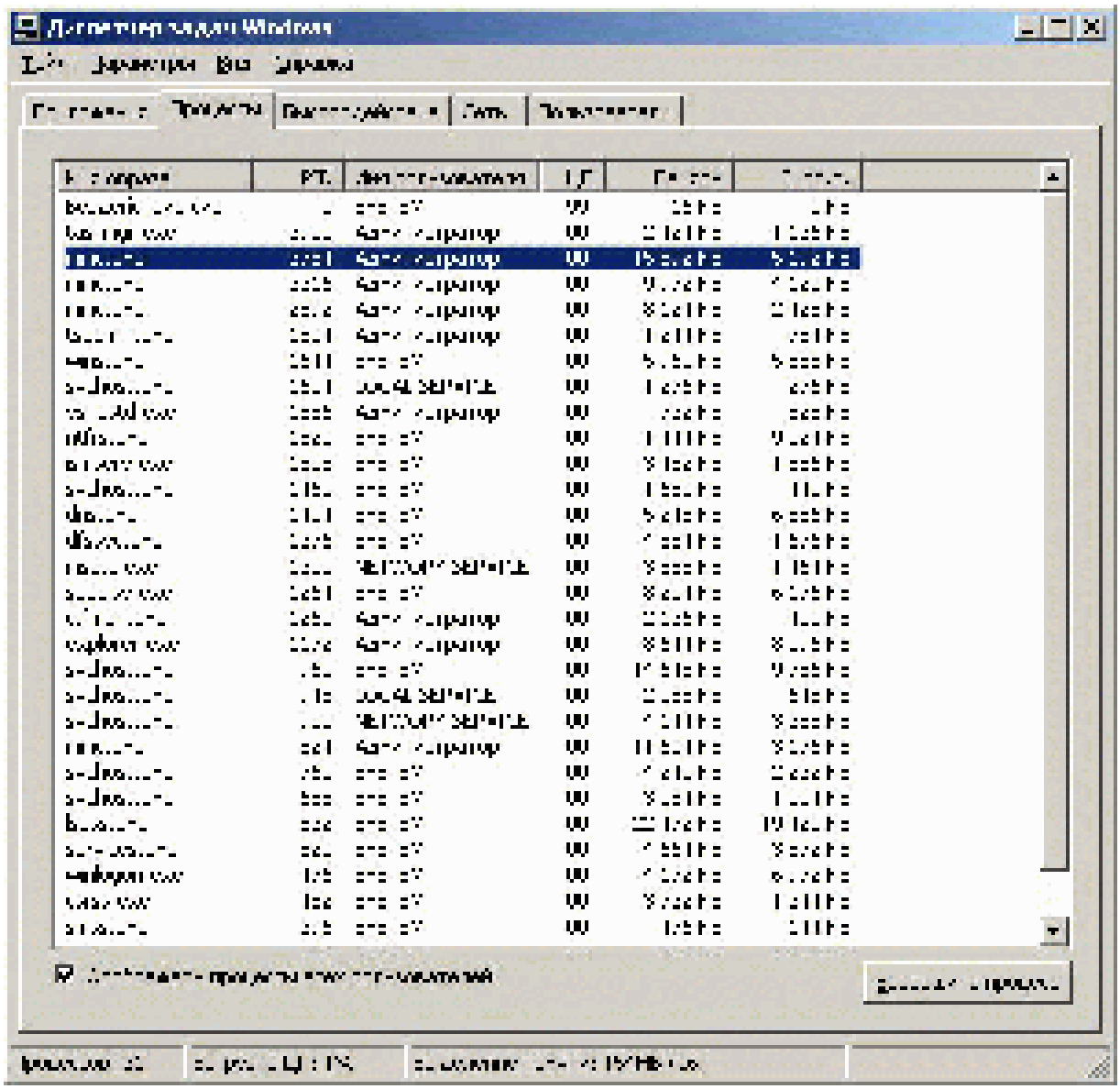


**Рис.2**

По умолчанию в этом окне перечислены только процессы, запущенные ОС, локальными службами, сетевыми службами и интерактивным пользователем, т. е. пользователем, локально зарегистрировавшимся на компьютере. Чтобы увидеть процессы, запущенные удаленными пользователями, например подключившимися с помощью удаленного рабочего стола, надо установить галочку у поля " *Отображать процессы всех пользователей* ".

В столбцах на закладке " *Процессы* " содержится информация о выполняемых процессах. Она позволяет выявить те из них, которые поглощают системные ресурсы, например, процессорное время или память. По умолчанию отображаются следующие столбцы:

- *Имя образа* — имя процесса или исполняемого файла, запустившего процесс;

- *Имя пользователя* — имя пользователя или системной службы, запустившей процесс;
- *ЦП* — доля ресурсов ЦП (в процентах), занимаемая данным процессом;
- *Память* — объем оперативной памяти, занятой процессом в данный момент.

При выборе в меню " *Вид* " команды " *Выбрать столбцы* ", откроется диалоговое окно, из которого на закладку " *Процессы* " можно добавить другие столбцы (Рис.3):

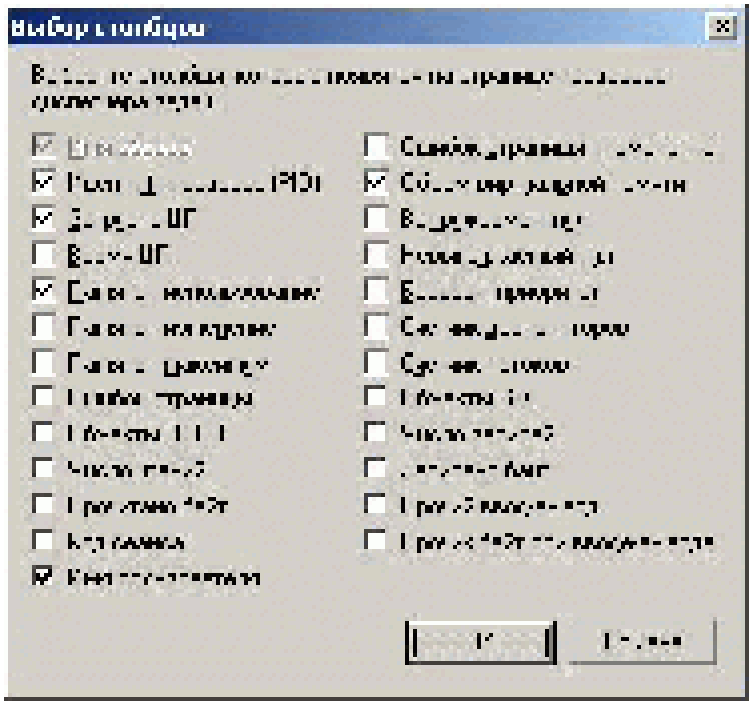


**Рис.3**

Некоторые из них могут оказаться очень полезными при поисках причин системной проблемы.

- *Идентиф. процесса (PID)* — цифровой идентификатор процесса в системе (позволяет найти процесс по его номеру, отображаемому не только в " *Диспетчере задач* ", но и в других утилитах управления);
- *Объем виртуальной памяти* — объем памяти данного процесса в килобайтах, выгруженной в данный момент в файл подкачки;
- *Базовый приоритет* — мера объема системных ресурсов, выделенных процессу; чтобы задать приоритет процесса, щелкните его правой кнопкой мыши, раскройте подменю " *Приоритет* " и выберите нужный вариант — " *Низкий* ", " *Ниже среднего* ", " *Средний* ", " *Выше среднего* " и " *Реального времени* "; большинству процессов по умолчанию назначен средний приоритет; наивысший приоритет назначается процессам реального времени;
- *Время ЦП* — процессорное время, затраченное на выполнение процесса с момента его запуска; чтобы найти процессы, на выполнение которых

расходуется больше всего времени, отобразите этот столбец и щелкните его заголовок, чтобы отсортировать процессы по содержимому столбца;

- *Выгружаемый пул, Невыгружаемый пул* — выгружаемым пулом называется область системной памяти, предназначенная для объектов, которые при ненадобности можно хранить на диске; невыгружаемый пул — это область системной памяти для объектов, которые на диск записывать нельзя (стоит обращать внимание на процессы, которым требуется значительный объем невыгружаемой памяти — если на сервере недостаточно свободной памяти, эти процессы могут стать причиной большого количества ошибок);
- *Ошибок страницы* — ошибка страницы возникает, если процесс запрашивает страницу памяти, а система не находит ее по указанному адресу; если запрашиваемая страница хранится в другой области памяти, ошибка называется программной; если запрашиваемую страницу приходится считывать с диска, ошибка называется ошибкой физической памяти; процессоры, как правило, справляются с большинством программных ошибок; ошибки физической памяти могут существенно замедлить работу системы
- *Память - максимум* — максимальный объем памяти, использованной процессом (на разницу между этим параметром и текущим объемом памяти, занятой процессом, тоже следует обращать внимание — если приложению, например, Microsoft SQL Server, в моменты пиковых нагрузок требуется гораздо больше памяти, чем при обычной работе, возможно, стоит сразу при запуске выделять ему больше памяти);
- *Счетчик дескрипторов* — полное число дескрипторов файлов, поддерживаемых процессом; эта характеристика позволяет оценить, насколько процесс зависит от файловой системы (С некоторыми процессами связаны тысячи дескрипторов открытых файлов, и каждый из них занимает некоторый объем системной памяти);
- *Счетчик потоков* — текущее число потоков, используемых процессом; большинство серверных приложений являются многопотоковыми, что позволяет одновременно выполнять несколько запросов процесса; некоторые приложения способны динамически управлять числом одновременно исполняемых потоков, что позволяет повысить их производительность; чрезмерное увеличение количества потоков ухудшает производительность, так как ОС приходится слишком часто переключать контексты потоков;
- *Число чтений, Число записей* — полное число операций чтения с диска и записи на диск с момента запуска процесса; этот параметр показывает, насколько активно процессом используется диск (если рост числа операций ввода-вывода не согласуется с реальной активностью сервера, процесс, вероятно, не способен кэшировать файлы или кэширование файлов неверно настроено).

**Замечание**. В списке процессов присутствует процесс " *Бездействие системы* ". Он отслеживает объем неиспользуемых ресурсов. Так, число 99 в столбце ЦП (CPU) означает, что 99% системных ресурсов в настоящий момент не используется. Приоритет этого процесса задать нельзя.

Просматривая информацию о процессах, надо помнить, что одно приложение может породить несколько процессов. Обычно все они зависят от родительского процесса и формируют расходящееся от него дерево процессов. Чтобы найти главный (родительский) процесс для данного приложения, на закладке "Приложения" щелкните приложение правой кнопкой мыши и выберите команду " *Перейти к процессу* ". Чтобы корректно завершить работу приложения с помощью " *Диспетчера задач* ", останавливайте либо само приложение, либо его главный процесс. Не останавливайте по отдельности зависимые процессы.

Остановить главный процесс приложения и порожденные им вторичные процессы можно несколькими способами:

- выделить приложение на закладке " *Приложения* " и щелкнуть кнопку " *Снять задачу* ";
- на закладке "Процессы" щелкнуть правой кнопкой мыши главный процесс приложения и выбрать команду " *Завершить процесс* ";
- на закладке "Процессы" щелкнуть правой кнопкой мыши главный или вторичный процесс приложения и выбрать команду " *Завершить дерево процессов* ".

## Мониторинг загруженности системы

На закладке " *Быстродействие* " в виде графиков и статистических данных отображается степень использования процессора и памяти (**Рис.4**).

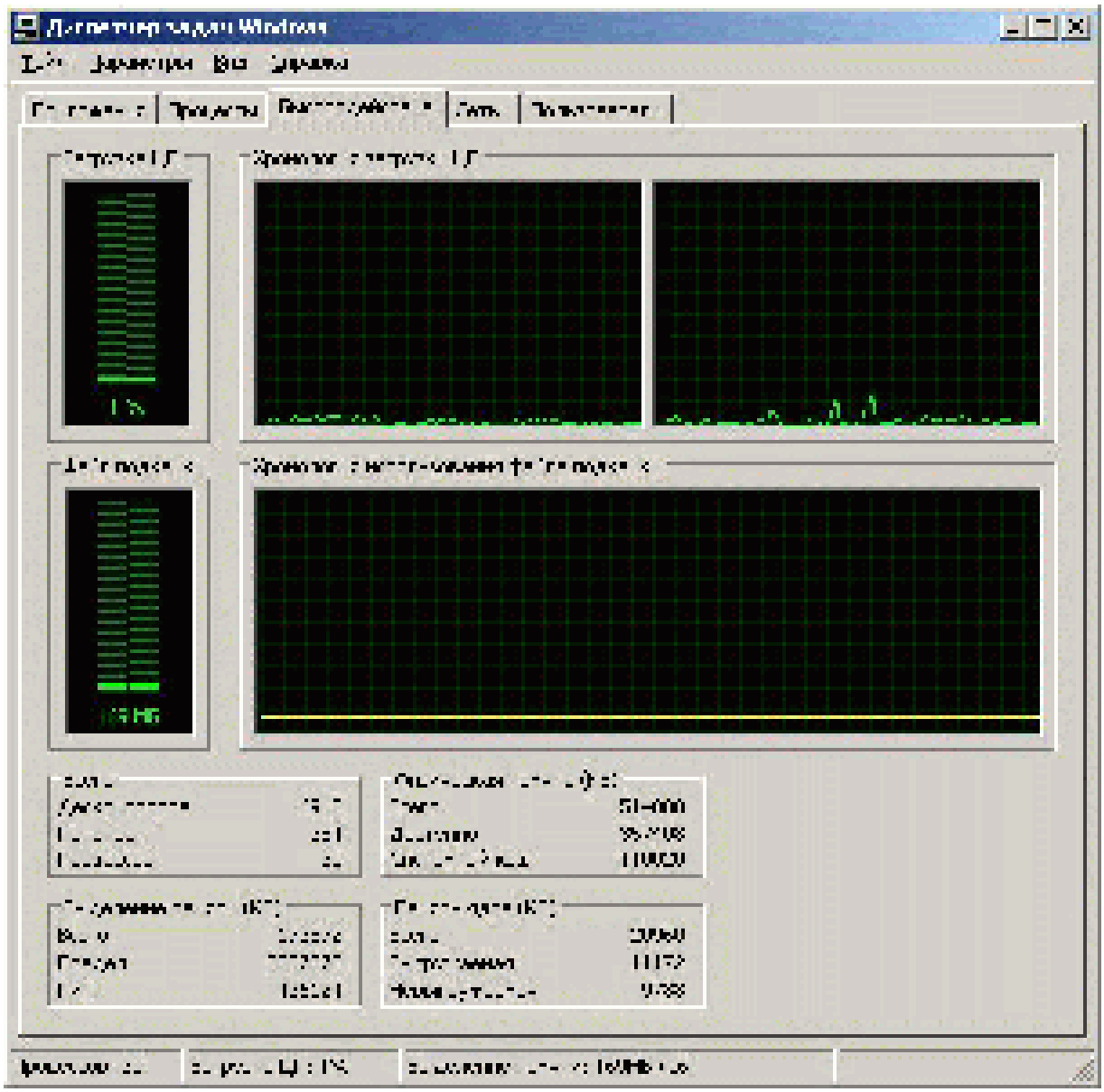


**Рис.4**

Эта информация позволяет быстро оценить нагрузку на системные ресурсы. Чтобы получить более подробные сведения, необходимо использовать консоль " *Производительность* ".

На графиках закладки " *Быстродействие* " отображена следующая информация:

- *Загрузка ЦП* — процент используемых в данный момент ресурсов процессора;
- *Хронология загрузки ЦП* — график изменения нагрузки на процессор (если в компьютере несколько процессоров, то по умолчанию для каждого процессора будет отображаться свой график загруженности); чтобы увеличить диаграмму, щелкните ее дважды, повторный двойной щелчок вернет обычный режим просмотра;

- *Файл подкачки* — объем файла подкачки (т. е. виртуальной памяти), занятый системой в настоящий момент;
- *Хронология использования файла подкачки* — график использования файла подкачки.

**Замечание**. Если нагрузка на процессор остается неизменно высокой даже в обычных условиях, для выяснения причин этого стоит заняться более детальным исследованием работы системы. Зачастую причина снижения производительности скрыта в памяти. Проверьте эту возможность, прежде чем принимать решение об обновлении процессора или о добавлении дополнительных процессоров.

Отображение графиков можно настроить или обновить с помощью команды меню Вид.

- команда " *Скорость обновления* " позволяет изменить скорость обновления графиков, а также приостановить обновление; вариант " *Низкая* " соответствует обновлению каждые 4 секунды, вариант " *Обычная* " — обновлению каждые 2 секунды, вариант " *Высокая* " — обновлению дважды в секунду;
- команда " *Загрузка ЦП* " в многопроцессорных системах позволяет задать отображение графиков для отдельных процессоров (отдельная диаграмма для каждого процессора) или все графики на одной диаграмме;
- команда " *Вывод времени ядра* " позволяет отобразить процессорное время, использованное ядром операционной системы (ресурсы, используемые ядром, на графиках отображаются красными линиями).

Под графиками приведены статистические данные:

- *Всего* — общая информация о загрузке процессора; в поле " *Дескрипторов* " указано количество используемых дескрипторов ввода-вывода, в поле " *Потоков* " — число потоков, в поле " *Процессов* " — число процессов;
- *Выделение памяти* — информация об общем объеме памяти, используемой ОС; в поле " *Всего* " отображается объем физической и виртуальной памяти, используемой в *данный момент*, в поле " *Предел* " — вся доступная физическая и виртуальная память, в поле " *Пик* " — максимальный объем памяти, использованный системой с момента загрузки;
- *Физическая память* — информация об общем объеме оперативной памяти в системе; в поле " *Всего* " указан объем физической оперативной памяти, в поле " *Доступно* " — оперативная память, не используемая в данный момент, в поле " *Системный кэш* " — память, используемая ОС для кэширования (если доступный объем памяти невелик, скажем, менее

5% всей физической памяти, стоит подумать об установке дополнительной памяти);

- *Память ядра* — информация о памяти, используемой ядром ОС; значительная часть ядра должна работать в оперативной памяти и не может выгружаться в виртуальную память, объем этой памяти указан в поле " *Невыгружаемая* ", объем памяти ядра, которую допустимо выгружать в виртуальную память, отображен в поле " *Выгружаемая* ", общий объем памяти, используемой ядром, указан в поле " *Всего* ".

## Мониторинг производительности сети

На закладке " *Сеть* " приводятся сведения о сетевых адаптерах, используемых системой, — процент загрузки, скорость соединения и статус. Если в системе установлен единственный сетевой адаптер, на сводной диаграмме (Рис.5) показана информация об изменении со временем трафика через этот адаптер:

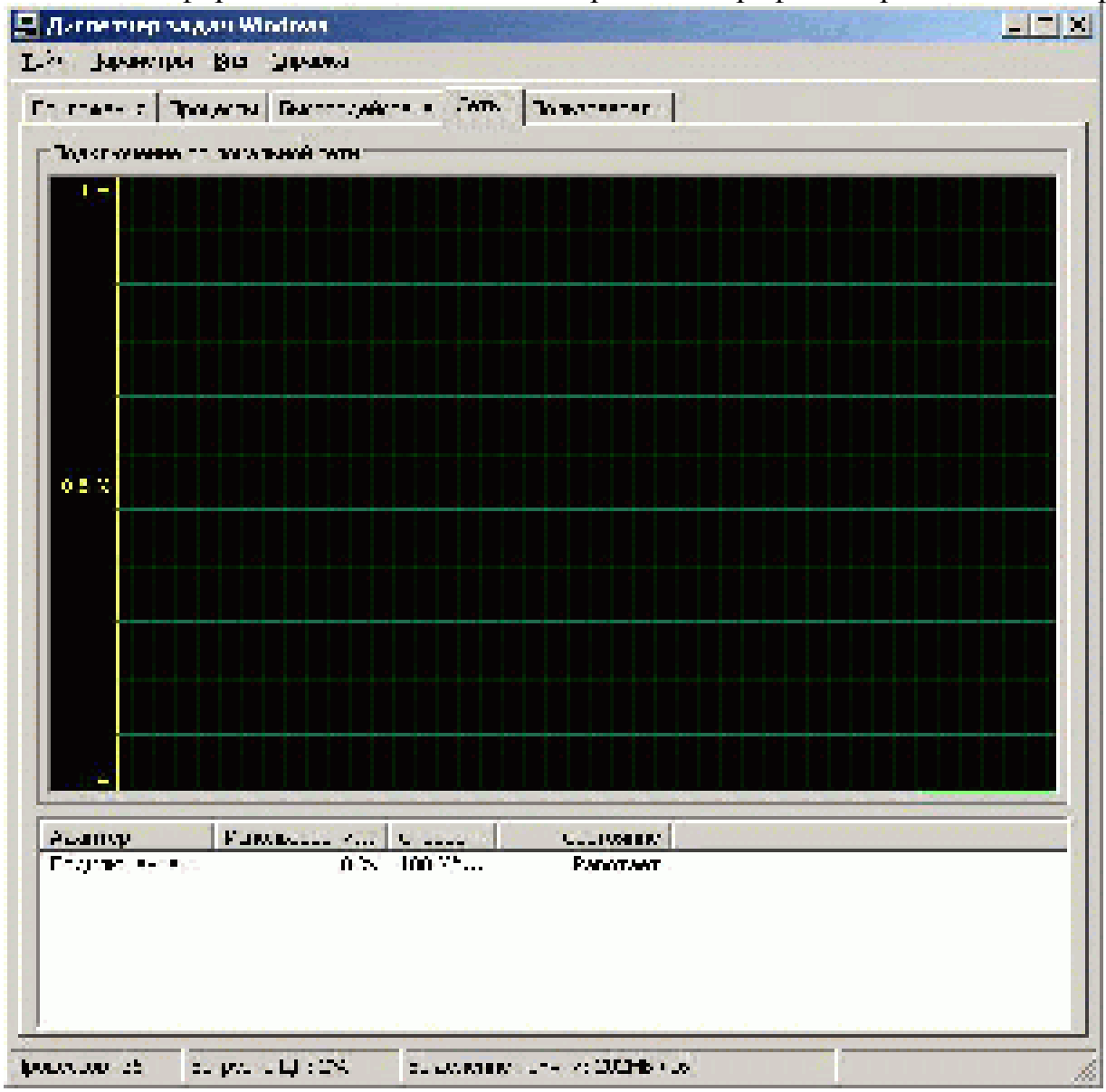


**Рис.5**

Если сетевых адаптеров в системе несколько, на диаграмме отображается сводный показатель использования всех сетевых подключений. По умолчанию это суммарное количество байт, переданных по сети.

В полях закладки " *Сеть* " содержится множество сведений о входящем и исходящем сетевом трафике сервера. С их помощью можно, например, установить объем поступающих на сервер данных. По умолчанию отображаются следующие поля:

- *Адаптер* — имя, под которым адаптер значится в папке Сетевые подключения;
- *Использование сети* — загрузка сети в процентах от исходной скорости подключения для данного интерфейса (например, адаптер с исходной скоростью подключения 100 Мбит/с и текущим трафиком 10 Мбит/с загружен на 10%);
- *Скорость линии* — скорость подключения через данный интерфейс;
- *Состояние* — состояние сетевого адаптера.

**Замечание**. Если загрузка адаптера часто достигает 50% или больше, внимательнее следите за сетевой активностью сервера и подумайте о приобретении дополнительных сетевых адаптеров.

Для исследования работы сети могут понадобиться дополнительные столбцы на закладке " *Сеть* ". Можно выбрать в меню " *Вид* " пункт " *Выбрать столбцы* " и установить отображение следующих столбцов:

- *Пропускная способность отправки* — процент использования текущей полосы пропускания исходящим трафиком;
- *Пропускная способность получения* — процент использования текущей полосы пропускания входящим трафиком;
- *Пропускная способность всего* — процент использования текущей полосы пропускания всем трафиком через данный адаптер;
- *Отправлено байт* — полное число байт, отправленных по данному подключению;
- *Получено байт* — полное число байт, полученных по данному подключению;
- *Байт* — полное число байт, переданных по данному подключению в обоих направлениях.

## Мониторинг удаленных подключений

Удаленные пользователи подключаются к системе через службы терминалов, или удаленные рабочие столы. Подключения с помощью удаленного рабочего стола активизируются автоматически при установке Windows Server 2003. " *Диспетчер задач* " предоставляет один из способов управления такими подключениями. Перейдите на закладку " *Пользователи* ", где перечислены

пользовательские сеансы как для локальных, так и для удаленных пользователей (Рис.6):

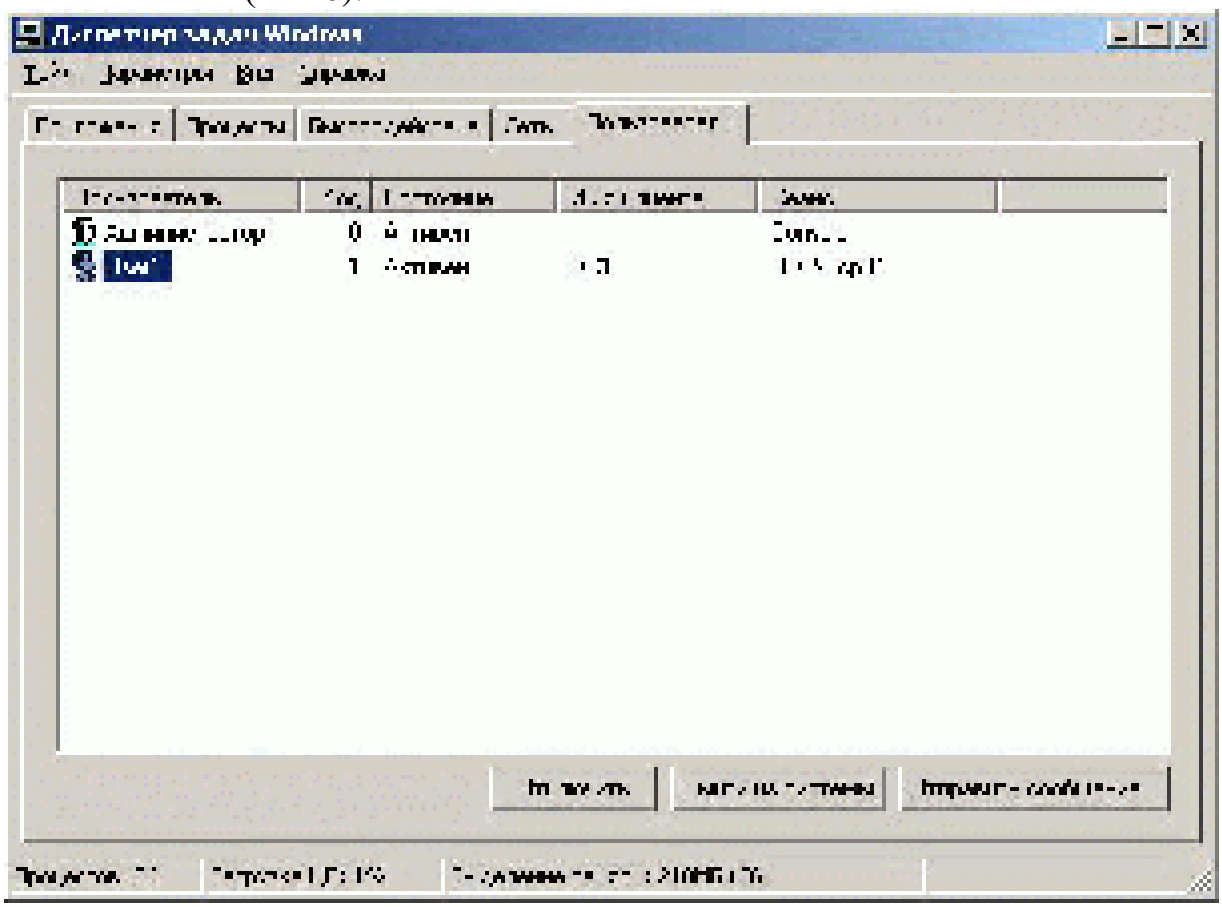


**Рис.6**

Для каждого подключения указаны: имя пользователя, код сеанса, состояние, клиентский компьютер и тип сеанса. Пользователю, зарегистрировавшемуся локально, соответствует тип сеанса " *Консоль* " ( *Console* ). Для других пользователей в этом столбце указан протокол подключения, например, RDP-Tcp для подключения с помощью протокола *RDP* ( *Remote Desktop Protocol* ) и транспортного протокола TCP. Щелкнув сеанс правой кнопкой мыши, получаем доступ к следующим командам:

- *Подключить* — подключение неактивного сеанса;
- *Отключить* — отключение пользовательского сеанса, с сохранением в сеансе всех запущенных пользователем приложений;
- *Выход из системы* — принудительное завершение пользовательского сеанса;
- *Удаленное управление* — переход к удаленному управлению пользовательским сеансом из сеанса администратора (совместная работа в сеансе);
- *Отправить сообщение* — отправка сообщения пользователям, зарегистрировавшимся на сервере терминалов.

## Консоль "Производительность"

Консоль " *Производительность* " (находящая в разделе " *Администрирование* " Главного меню системы Windows) позволяет более детально исследовать функционирование системы по сравнению с " *Диспетчером задач* ". И, кроме того, данная консоль позволяет накапливать статистику о работе системы в фоновом режиме, без непосредственного наблюдения администратором системы, а также собирать данные о производительности с нескольких компьютеров одновременно. Данная консоль содержит два раздела — "*Системный монитор*" и "*Журналы и оповещения производительности*". "*Системный монитор*" предназначен для наблюдения за системой (или системами в режиме реального времени), "*Журналы и оповещения производительности*" используются для накопления статистики в фоновом режиме и последующего изучения накопленных данных.

Работа консоли "*Производительность*" основана на понятиях "*Объект*" и "*Счетчик*". Понятие " *Объект*" относится к той или иной компоненте системы или к определенному приложению и состоит из набора "*Счетчиков*", числовых показателей, измеряющих степень загруженности данной компоненты. Набор доступных объектов и счетчиков обновляется при установке служб и дополнительных компонент. Например, после установки на сервере службы DNS консоль "*Производительность*" пополняется рядом объектов и счетчиков для отслеживания работы этой службы.

" *Системный монитор* "

Если открыть консоль "*Производительность*", то мы сразу попадем в раздел "*Системного монитора*". При этом на экране отображаются 3 самых важных с точки зрения операционной системы счетчика: "*Обмен страниц в сек* " (объекта " *Память*"), " *Средняя длина очереди диска* " (объекта " *Физический диск* ") и " *% загруженности процессора* " (объекта " *Процессор* "); обновление данных на экране производится раз в секунду (Рис.7).

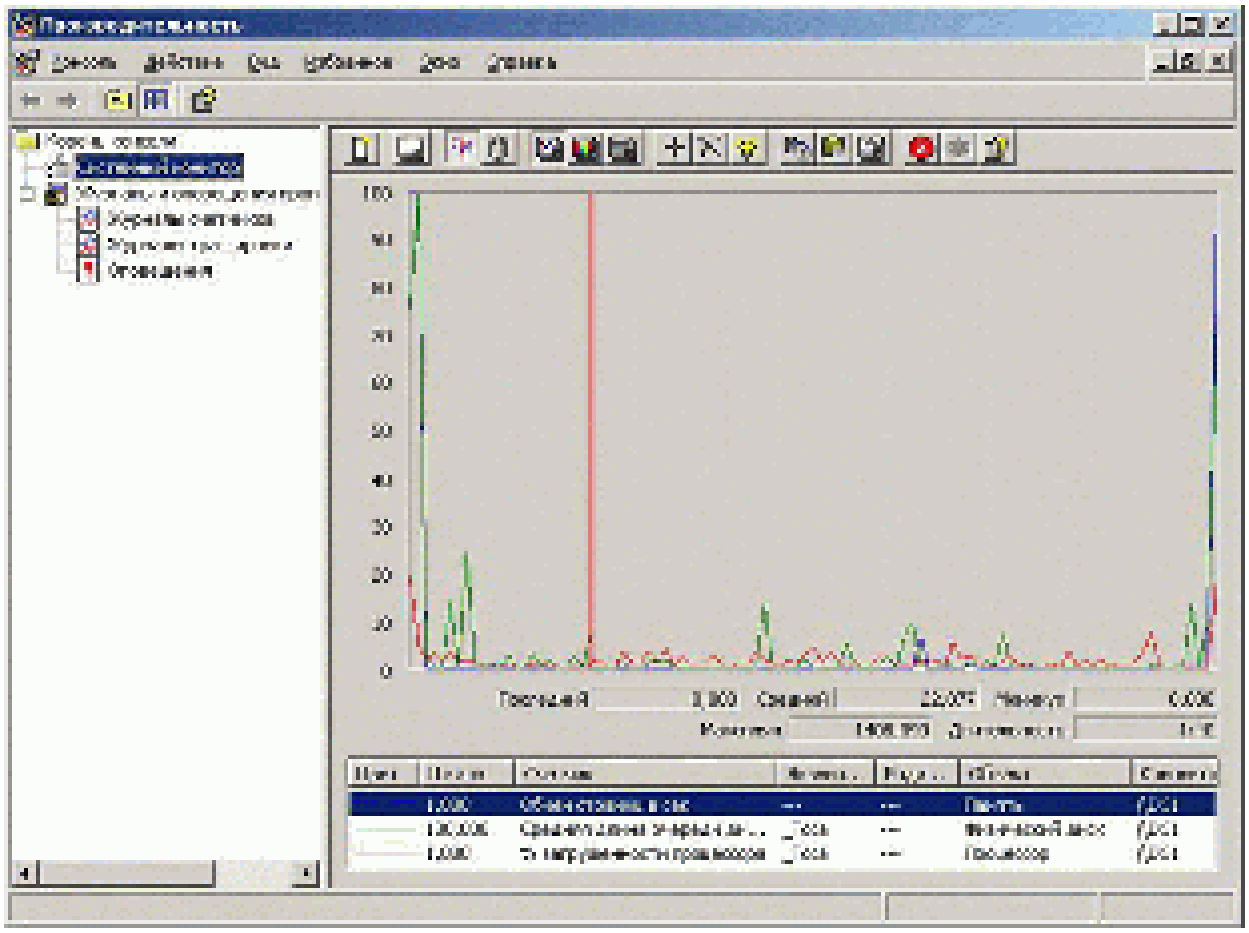


Рис.7

Для выбранного мышью активного процесса регистрируются показатели:

- *Последний* — последнее полученное значение счетчика;
- *Средний* — среднее из всех полученный значений счетчика;
- *Минимум* — минимальное значение счетчика за период наблюдений;
- *Максимум* — максимальное значение счетчика за период наблюдений.

Если открыть *Свойства* счетчика, то можно изменить способ отображения данного счетчика на экране: цвет, толщину и стиль линии и масштаб (от 1:10000000 до 10000000:1), также изменить частоту сбора показаний.

Нажатием комбинации клавиш CTRL+H можно выделить активный счетчик белым цветом (так лучше видно активный счетчик среди большого количества счетчиков).

Нажатием кнопки со знаком "+" на панели инструментов можно добавить другие счетчики, в том числе полученные с других компьютеров сети (Рис.8):

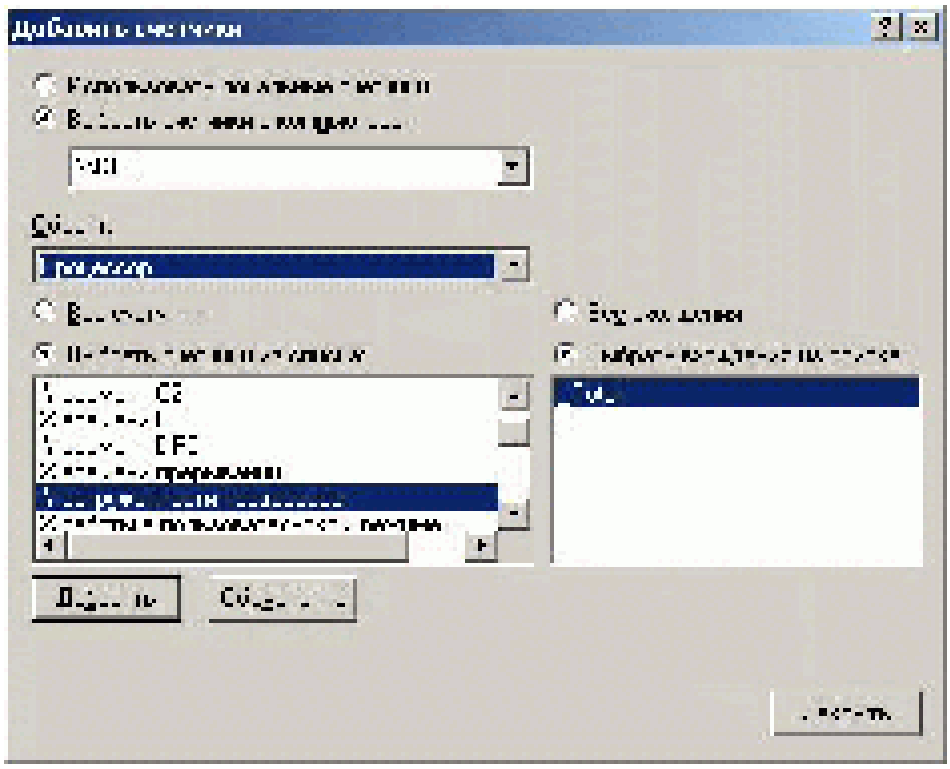


**Рис.8**

" *Журналы и оповещения производительности* "

Раздел " *Журналы и оповещения производительности* " в свою очередь состоит из трех частей:

- " *Журналы счетчиков* " — выполняют ту же задачу, что и " *Системный монитор* ", но делают это в фоновом режиме и накапливают данные в файле журнале на жестком диске или в базе данных (это наиболее часто используемый раздел журналов производительности);
- " *Журналы трассировки* " — отслеживание запуска и работы приложений (универсальный системный отладчик, позволяет определить некоторые ошибки в функционировании тех или иных приложений и системных задач);
- " *Оповещения* " — отслеживание значений счетчиков, но не для накопления в журнале, а для отправки оповещения назначенным для этой задачи пользователям (по электронной почте, с помощью системной компоненты " *Оповещатель* " ( *Messenger* ), и др.).

Рассмотрим подробнее использование " *Журналов счетчиков* ".

Основное назначение этих журналов — накопление статистики загруженности системы, поиск "узких мест" в работе сервера и выработка рекомендаций по модернизации или замене системы (если возникает такая потребность).

Для создания нового журнала в меню " *Действие* " необходимо выбрать пункт " *Новые параметры журнала* ". Далее надо задать имя журнала (к введенному администратором имени система добавит последовательность цифр, отображающую номер журнала, при каждом новом запуске журнала его номер будет увеличиваться, (Рис.9).

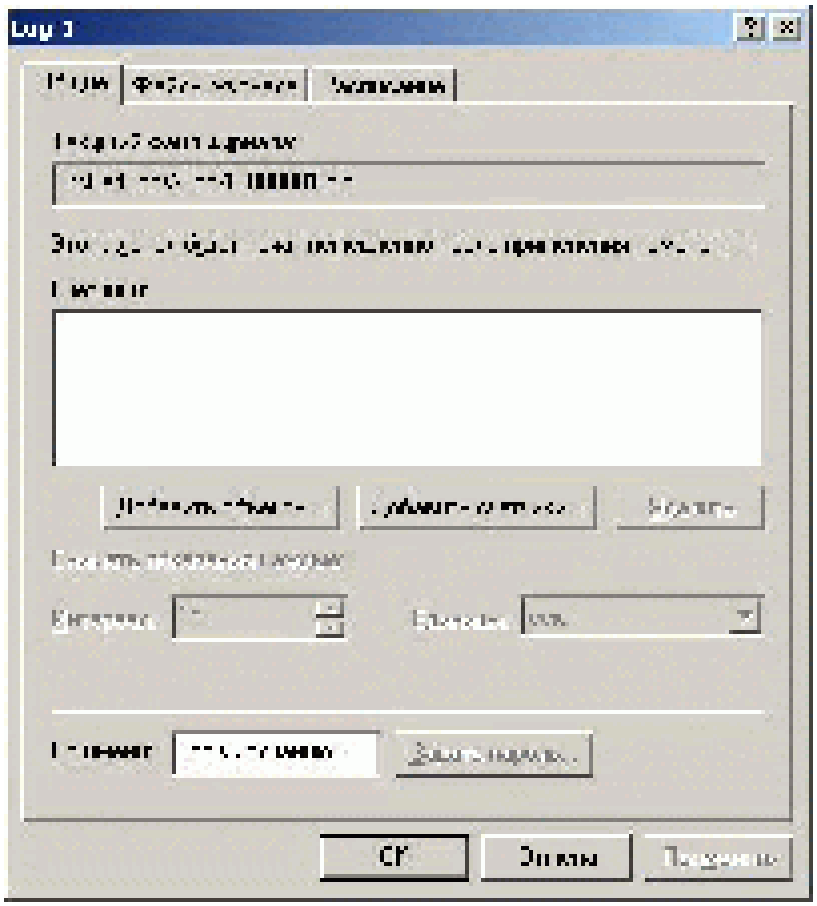


**Рис.9**

При создании самого первого журнала на томе с системой Windows создастся папка Perflogs, в которой и будут сохраняться все файлы с журналами. Далее нажатием кнопок " *Добавить объекты* " или " *Добавить счетчики* " можно добавить соответственно необходимые для мониторинга объекты (целиком со всем набором счетчиков) или отдельные счетчики. Для примера создадим журнал с именем Log-1, выберем счетчики " *Память\Обмен страниц в сек* ", " *Процессор\% загруженности процессора* " и " *Физический диск\Средняя длина очереди диска* " для сервера *DC1*, установим интервал опроса для сбора данных — 1 секунду (Рис.10). Нажмем кнопку " *Применить* ".

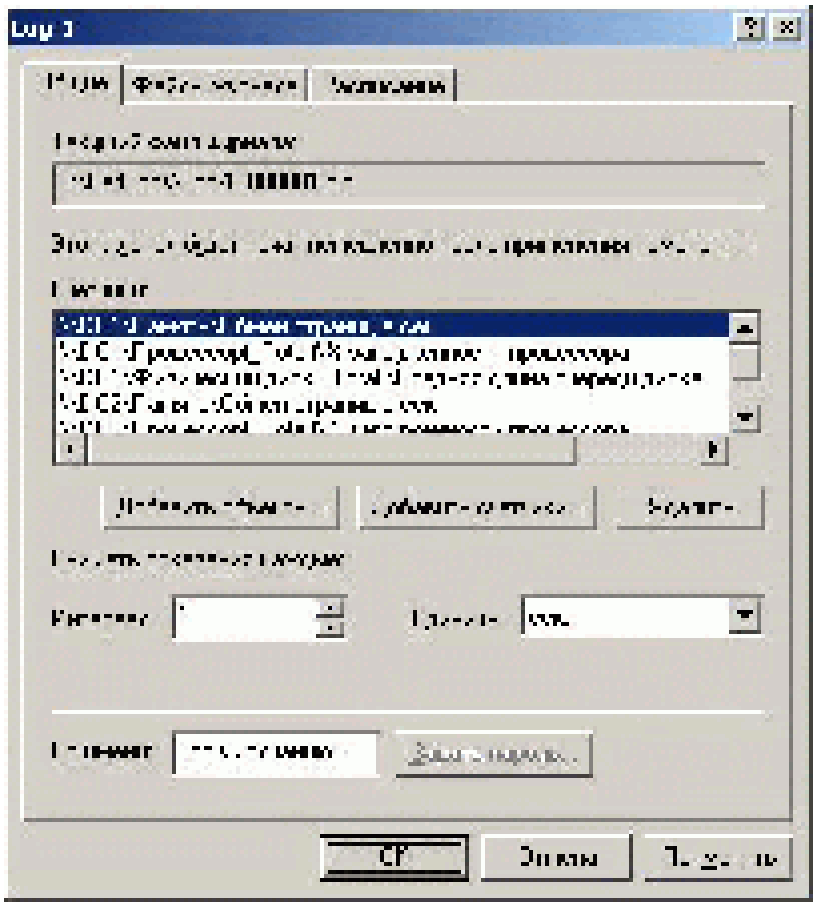


**Рис.10**

Теперь можно менять другие параметры журнала. На закладке " *Файлы журнала* " можно указать, где накапливать данные — в двоичном файле с расширением " .blg " (по умолчанию), в текстовом с разделителями в виде табуляции или запятой, в базе данных. На закладке " *Расписание* " задается время и дата запуска журнала. Назначим режим запуска журнала " *Вручную* " и нажмем кнопку " *ОК* ". Теперь запустим журнал для накопления данных (Рис.11). Саму консоль " *Производительность* " можно закрыть (и даже завершить сеанс работы в системе).

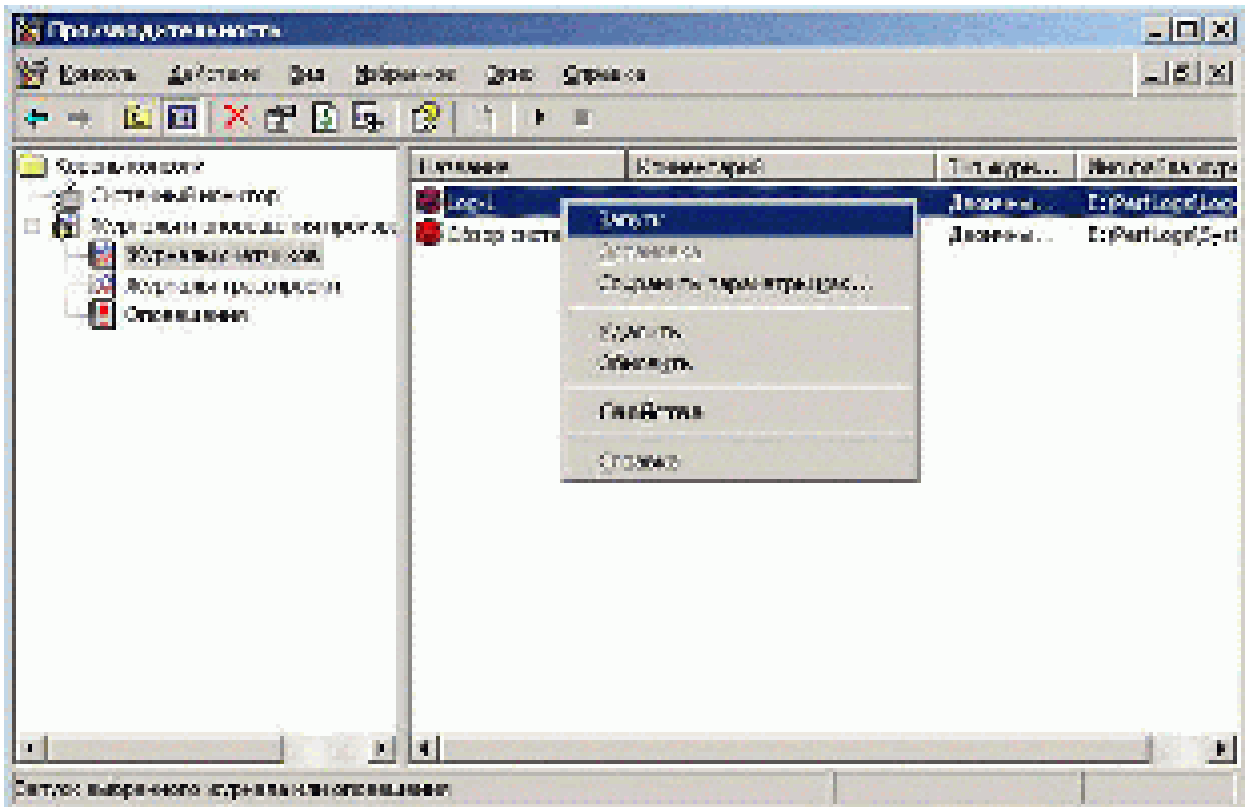


**Рис.11**

Для тестового примера запустим подряд несколько управляющих консолей и приложений, а также процесс копирования большого объема данных из одной папки в другую (все это в совокупности достаточно сильно нагрузит и процессор, и дисковую подсистему), причем сделаем это несколько раз в течение определенного интервала времени.

По окончании процесса накопления данных снова запустим консоль " *Производительность* " и удалим автоматически открытые счетчики. Для того чтобы открыть файл журнала для анализа накопленных данных, выполним следующие действия: нажмем кнопку " *Просмотр данных журнала* " (Рис.12) или комбинацию клавиш CTRL+L, выберем для источника данных вариант " *Файлы журнала* ", нажмем кнопку " *Добавить* ", укажем путь к файлу с накопленными данными, откроем этот файл, нажмем кнопку " *Применить* " (Рис.13).

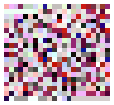


**Рис.12**

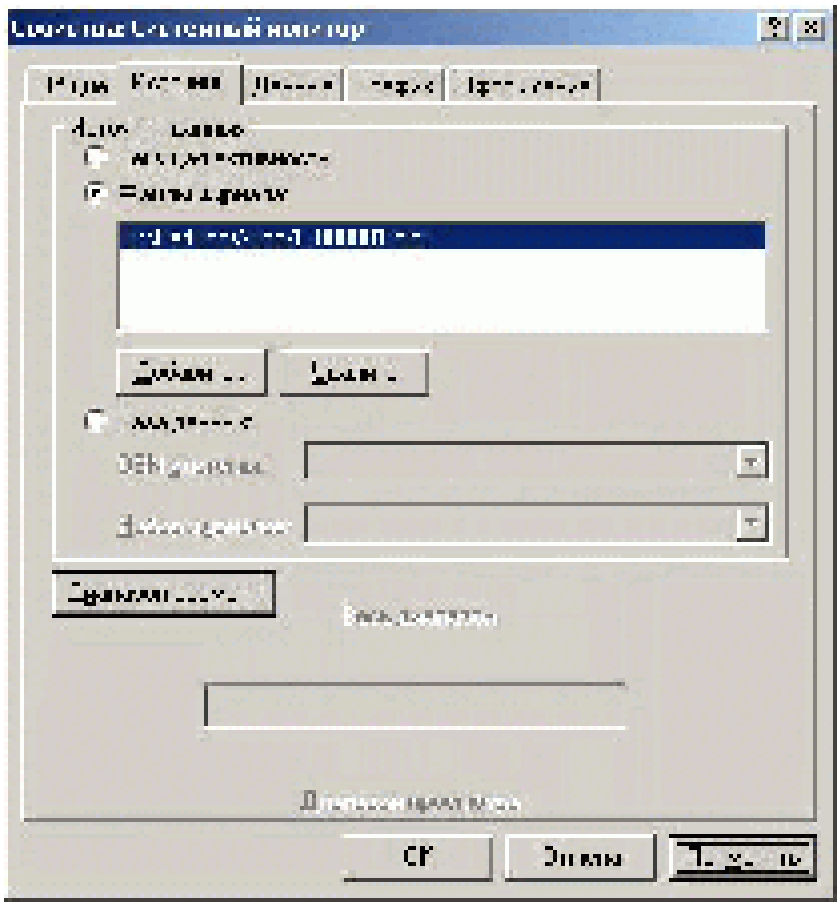


**Рис.13**

Перейдем на закладку " *Данные* " и добавим нужные счетчики. Нажмем " *ОК* ". Если период накопления был достаточно долгий, то данных будет накоплено много и картинка получится не очень разборчивая (Рис.14).

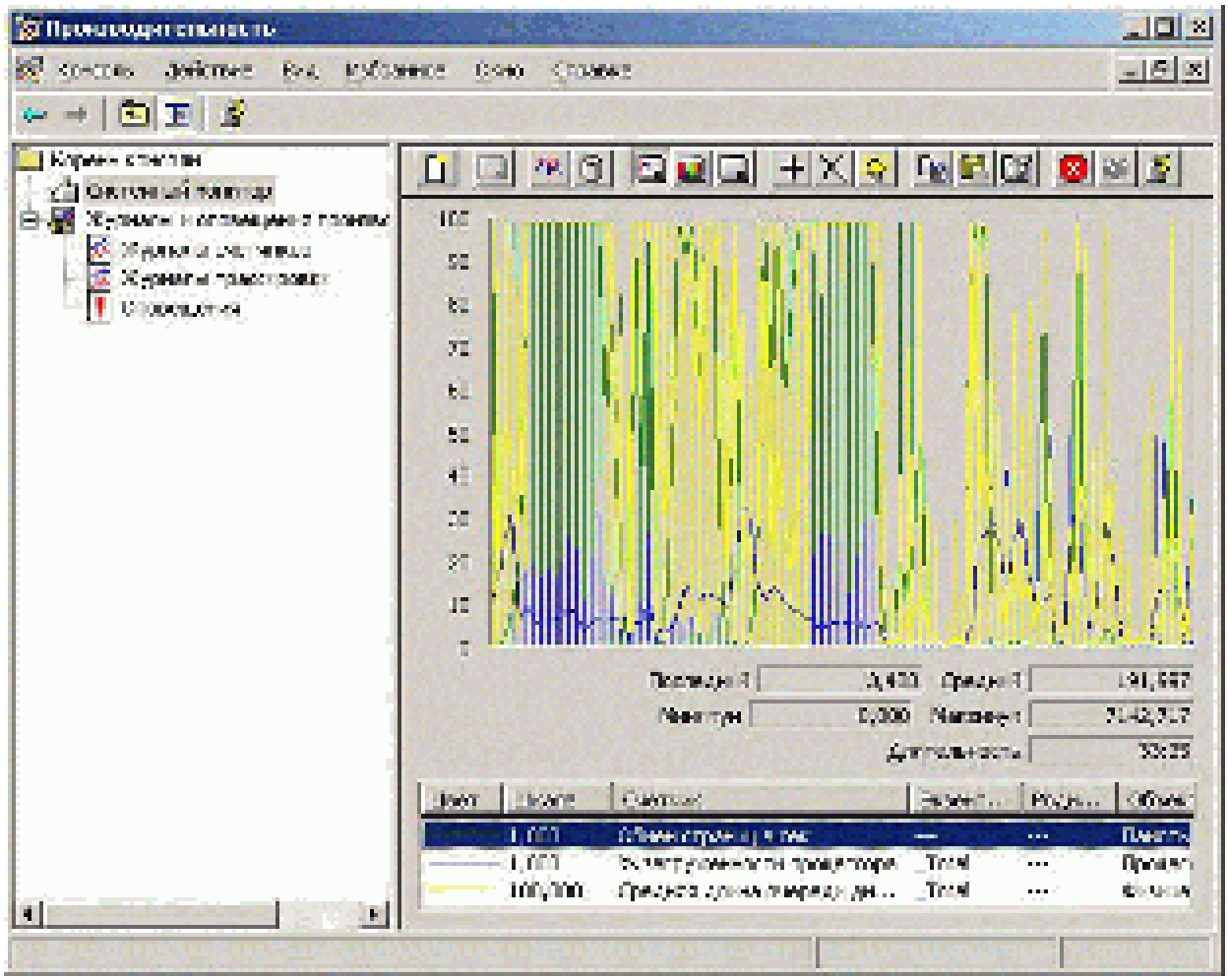


**Рис.14**

Для сужения интервала времени, который подвергается анализу, откроем *Свойства* любого из счетчиков и перейдем на закладку " *Источник* ". В нижней части панели подвинем границы анализируемого интервала и установим нужный нам " *Диапазон просмотра* " (Рис.15).

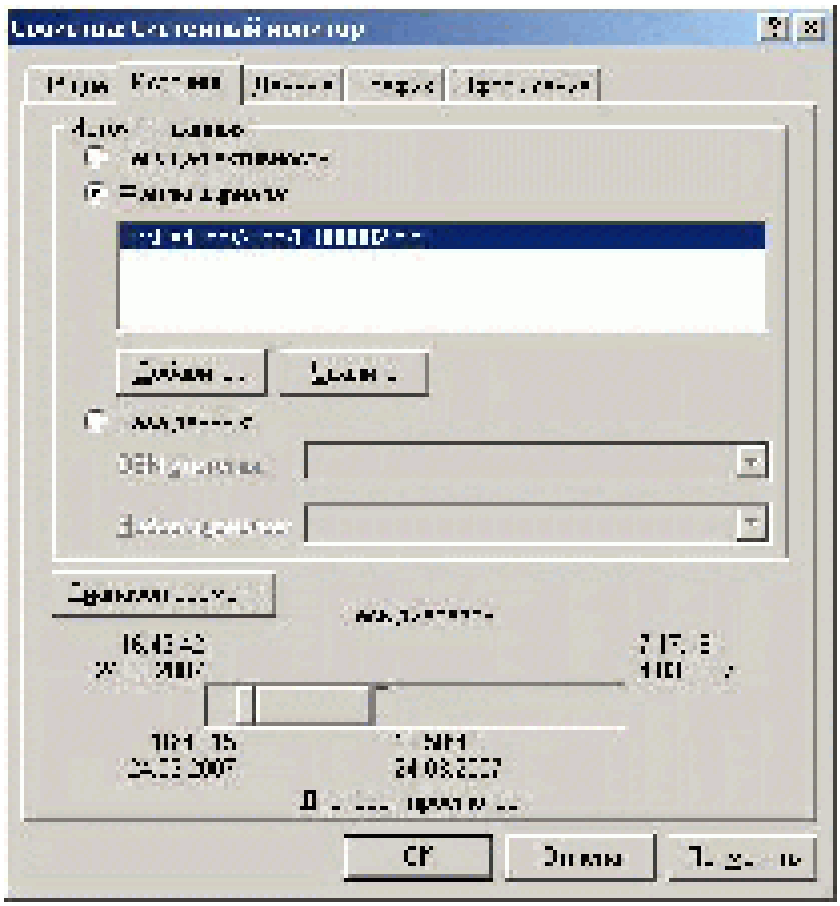


**Рис.15**

После этого график приобретет вид (Рис.16):

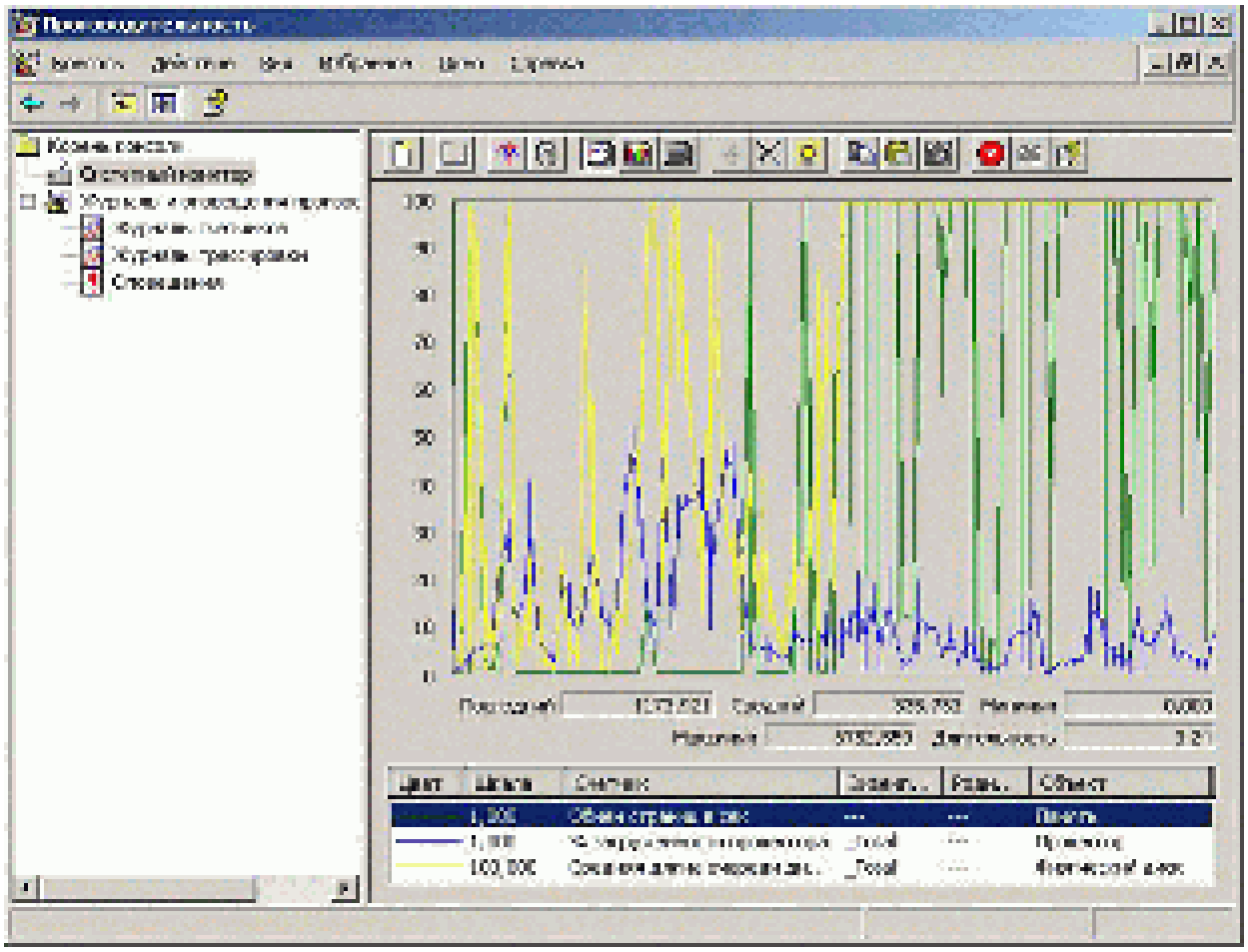


**Рис.16**

Чтобы значения некоторых графиков не выходили за границы экрана просмотра, произведем масштабирование этих графиков. В итоге получится картинка, вполне пригодная для изучения и анализа (Рис.17):

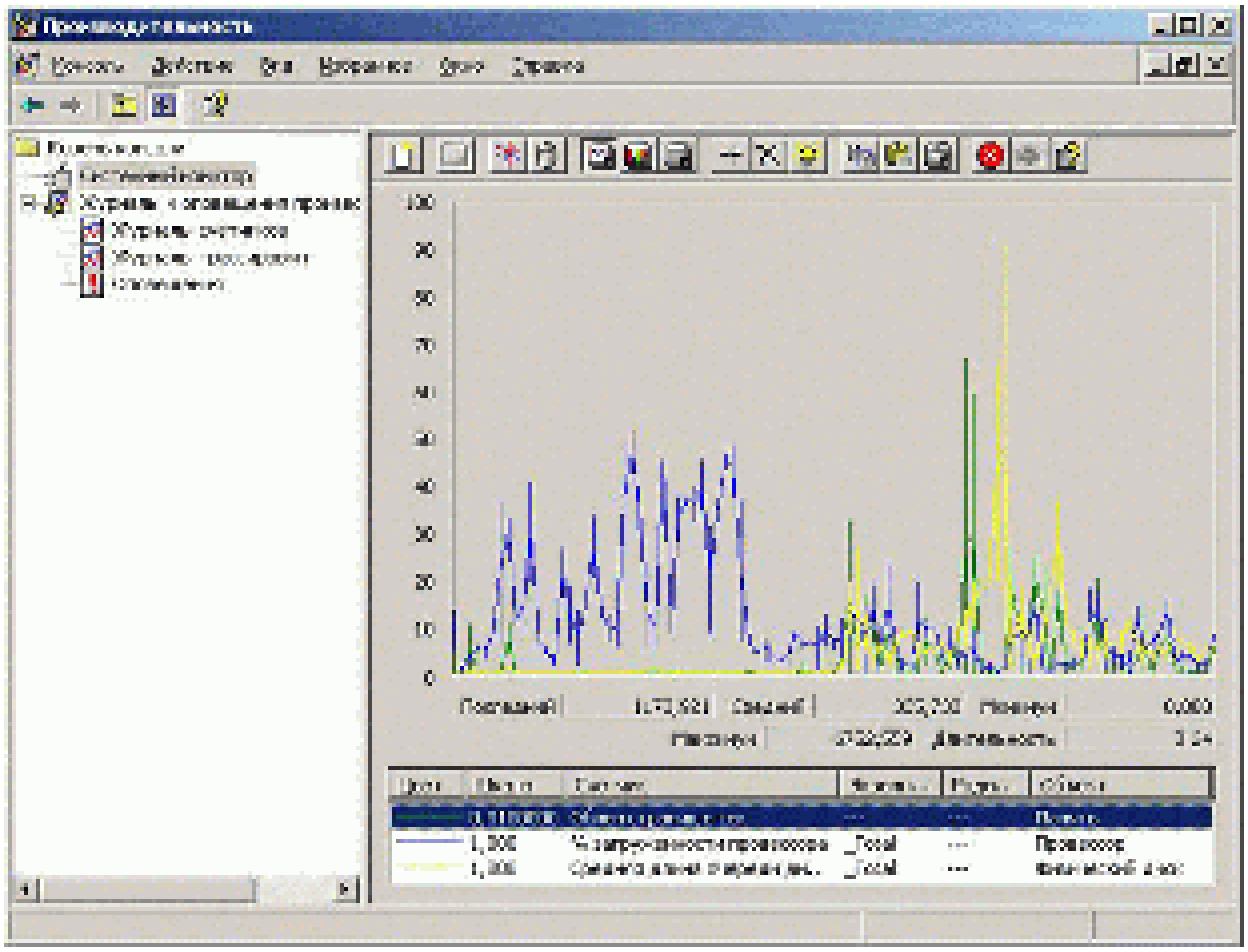


**Рис.17.**

Диапазон просмотра можно менять и переключаться на другие промежутки времени. Соответственно может потребоваться настроить масштаб отображения графиков.

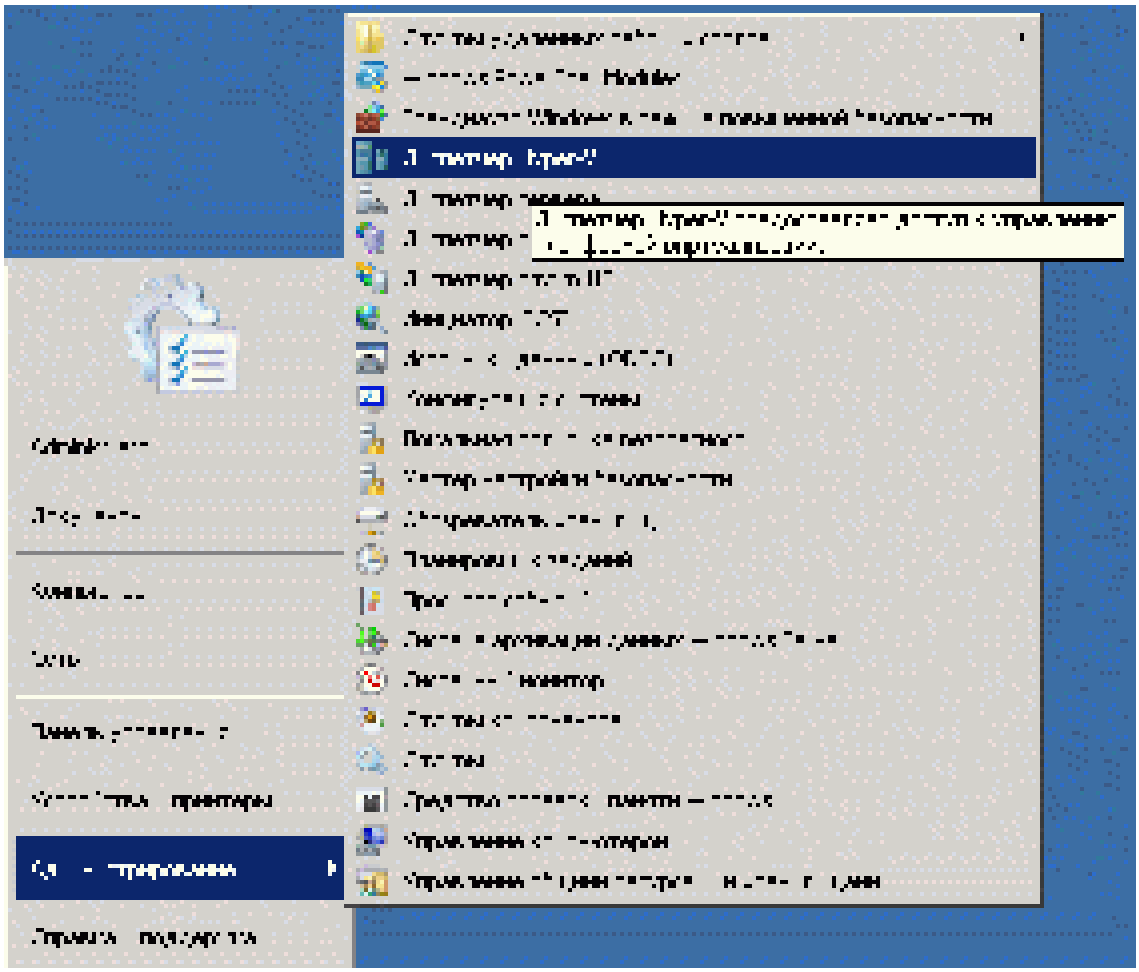
**Практическое занятие №23. Создание виртуальной машины Hyper2 - V**

***Цель работы:***

Целью данной практической работы является подробное рассмотрение процесса создания виртуальной машины Hyper-V

**Создание виртуальной машины Hyper2 - V**

После установки роли Hyper - V в разделе Администрирование станет доступен Диспетчер Hyper-V, при помощи которого и осуществляется управление виртуальными машинами.

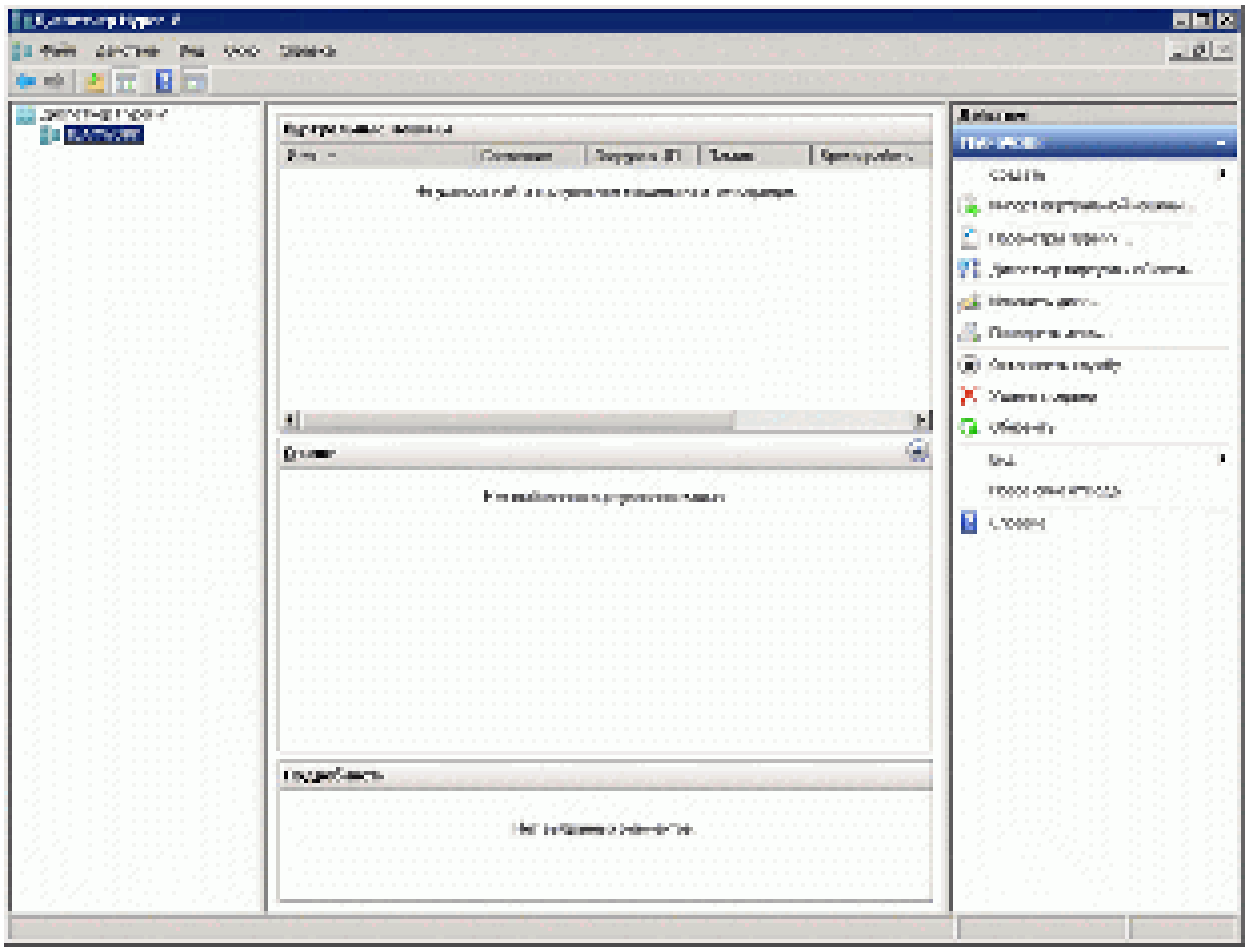


Для создания виртуальной машины запустите Диспетчер Hyper - V.

В зависимости от конфигурации дискового хранилища, можно создавать виртуальные машины двух типов:

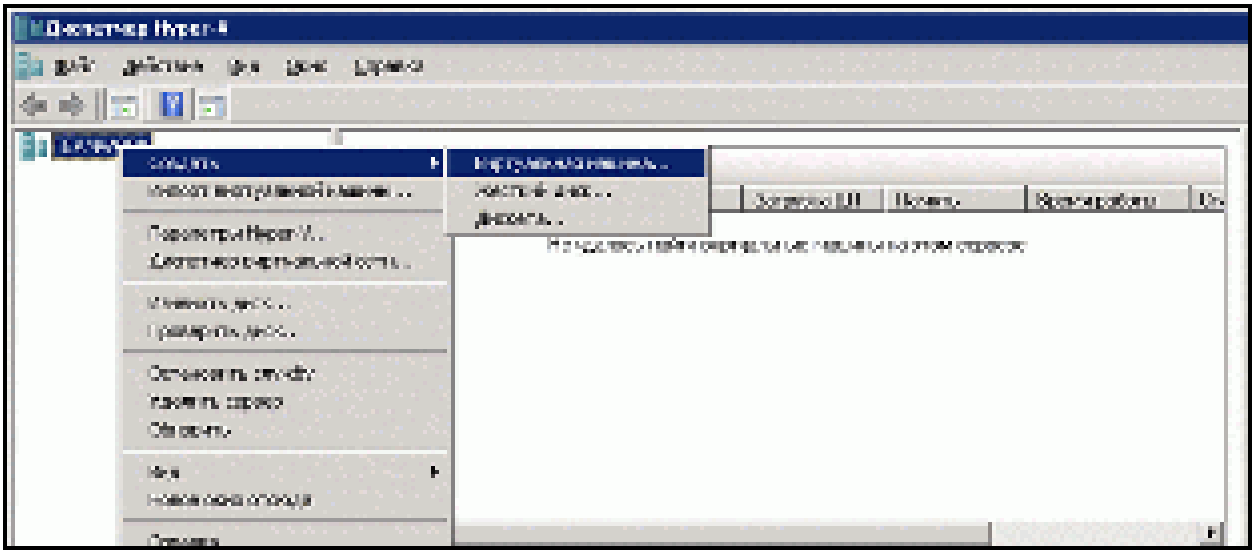
1. виртуальная машина, гостевая операционная система которой установлена на виртуальном диске, представленном в виде файла, хранящегося на винчестере хоста;
2. виртуальная машина, операционная система которой установлена на отдельном жестком диске хоста (транзитный диск- passthrough disk).

В рамках данной практической работы мы рассмотрим создание виртуальной машины каждого типа.

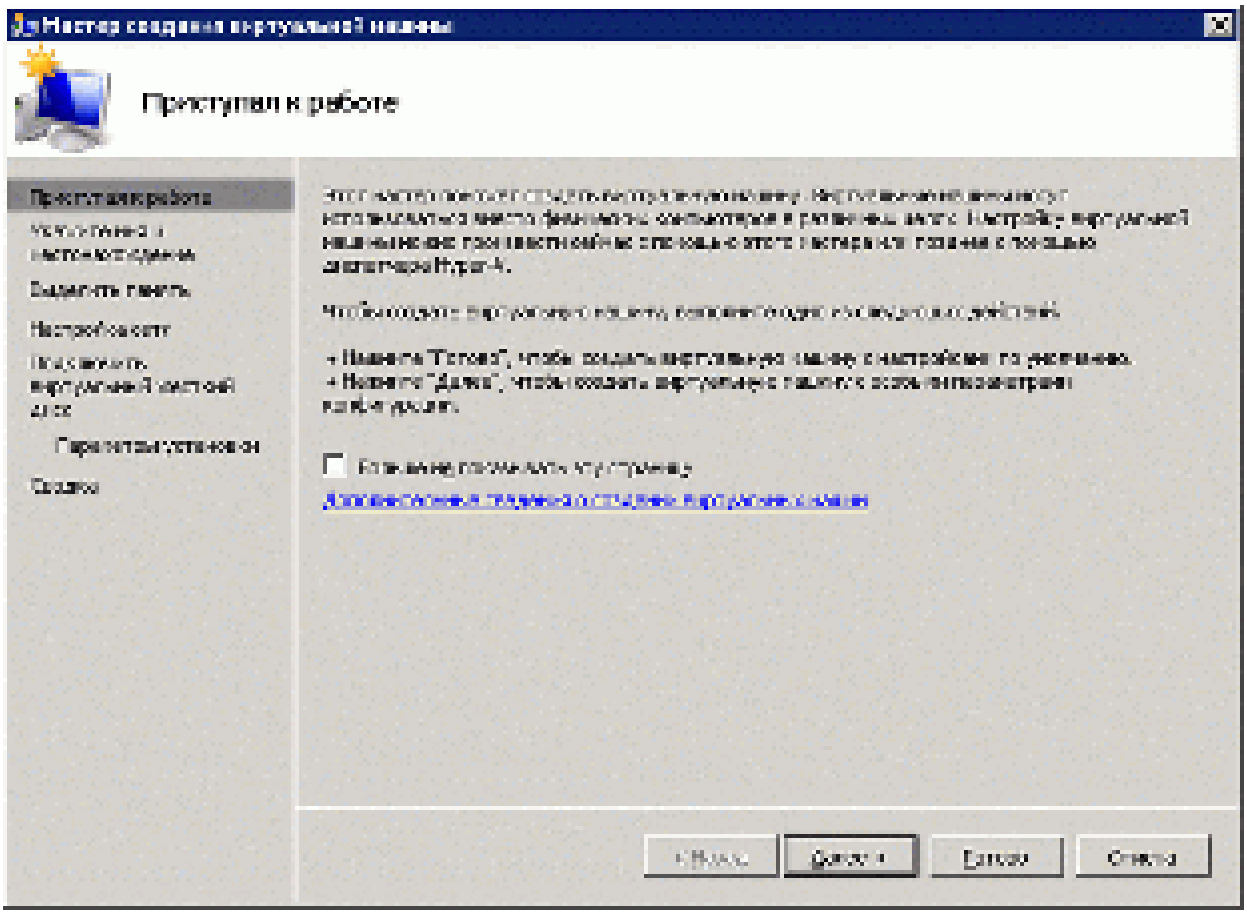


**Создание виртуальной машины с использованием виртуального жесткого диска**

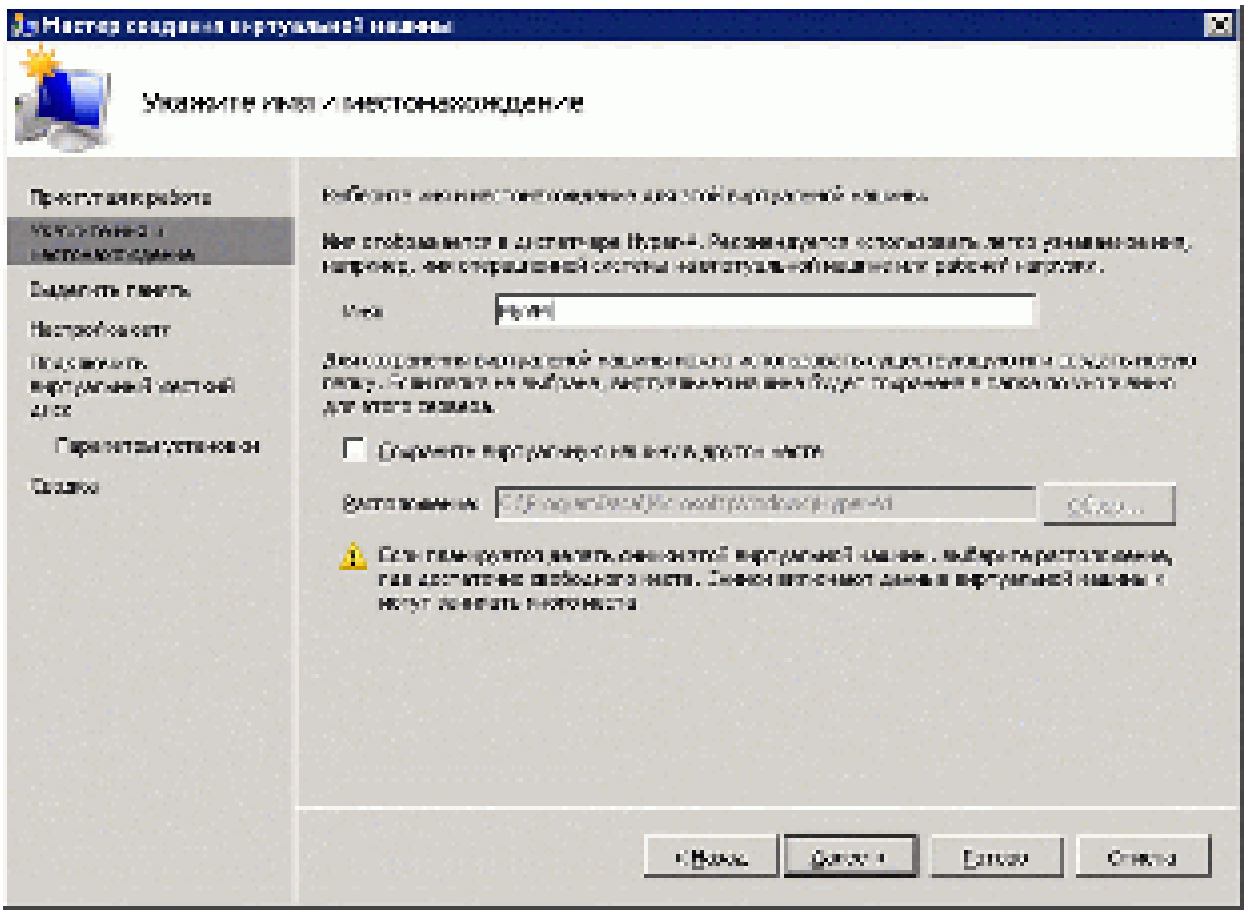
1. Щелкните правой кнопкой мыши на имени Hyper-V сервера и выберите "Создать - Виртуальная машина".



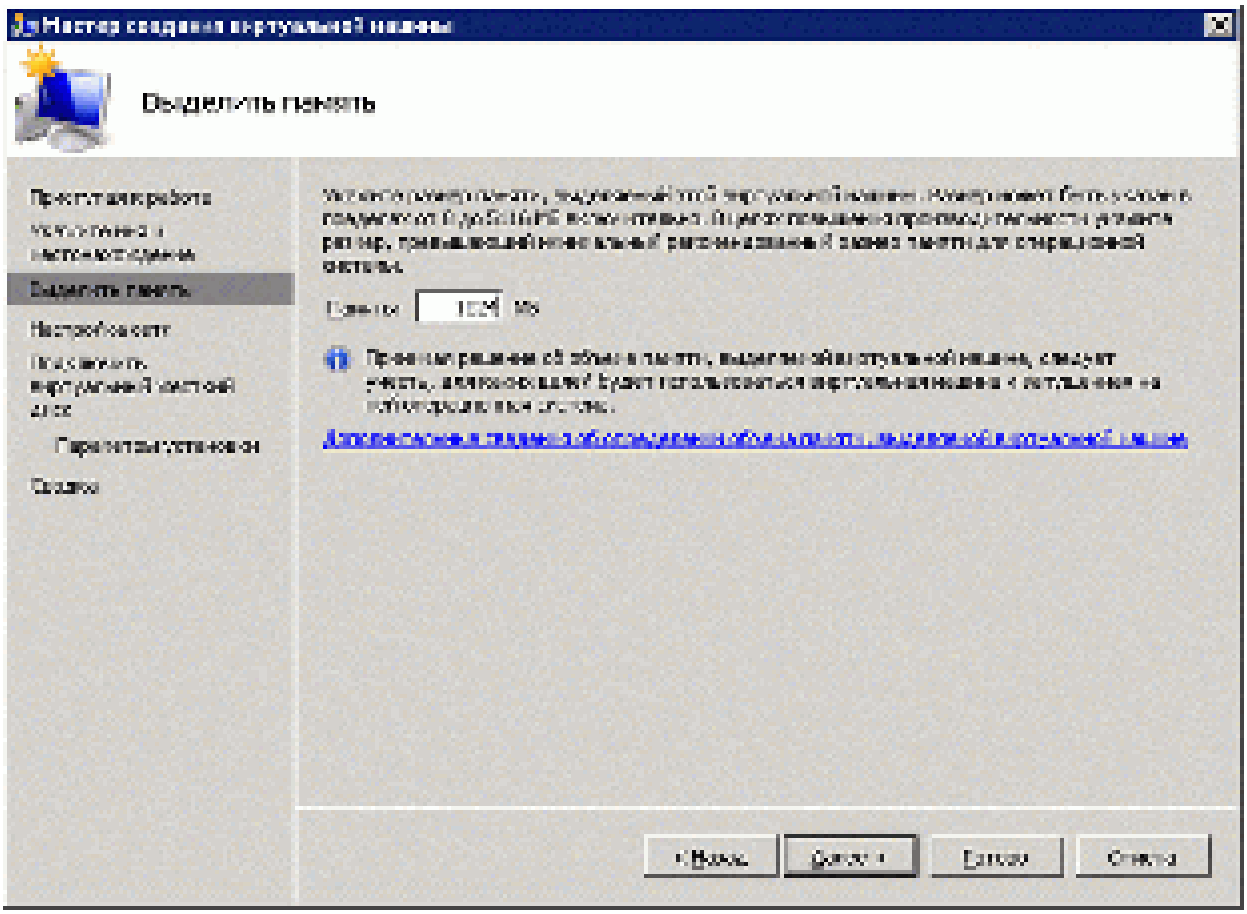
2. Для настройки параметров создаваемой ВМ нажмите кнопку "Далее".



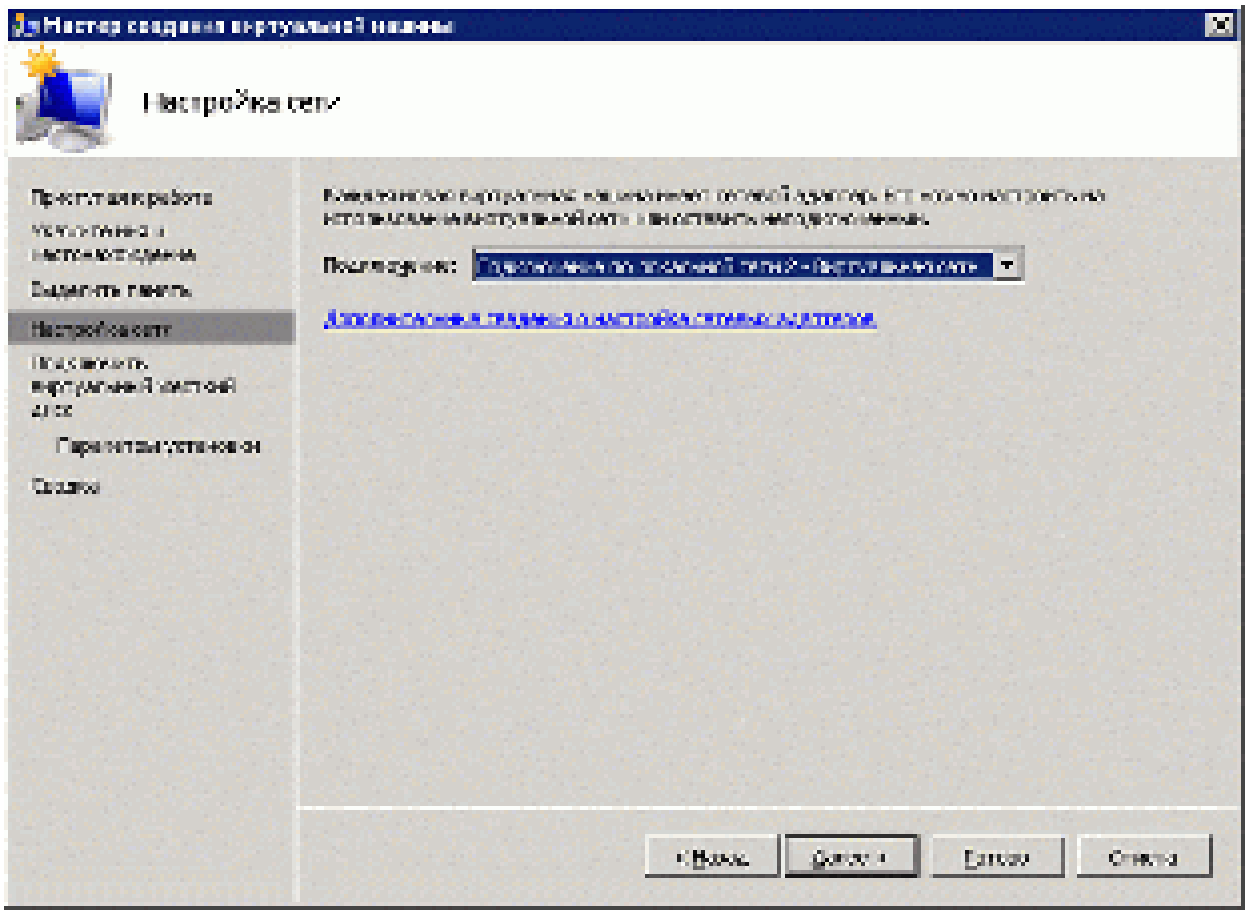

3. На следующем шаге необходимо задать имя виртуальной машины и указать путь хранения файлов виртуальной машины. После определения указанных параметров нажмите "Далее".



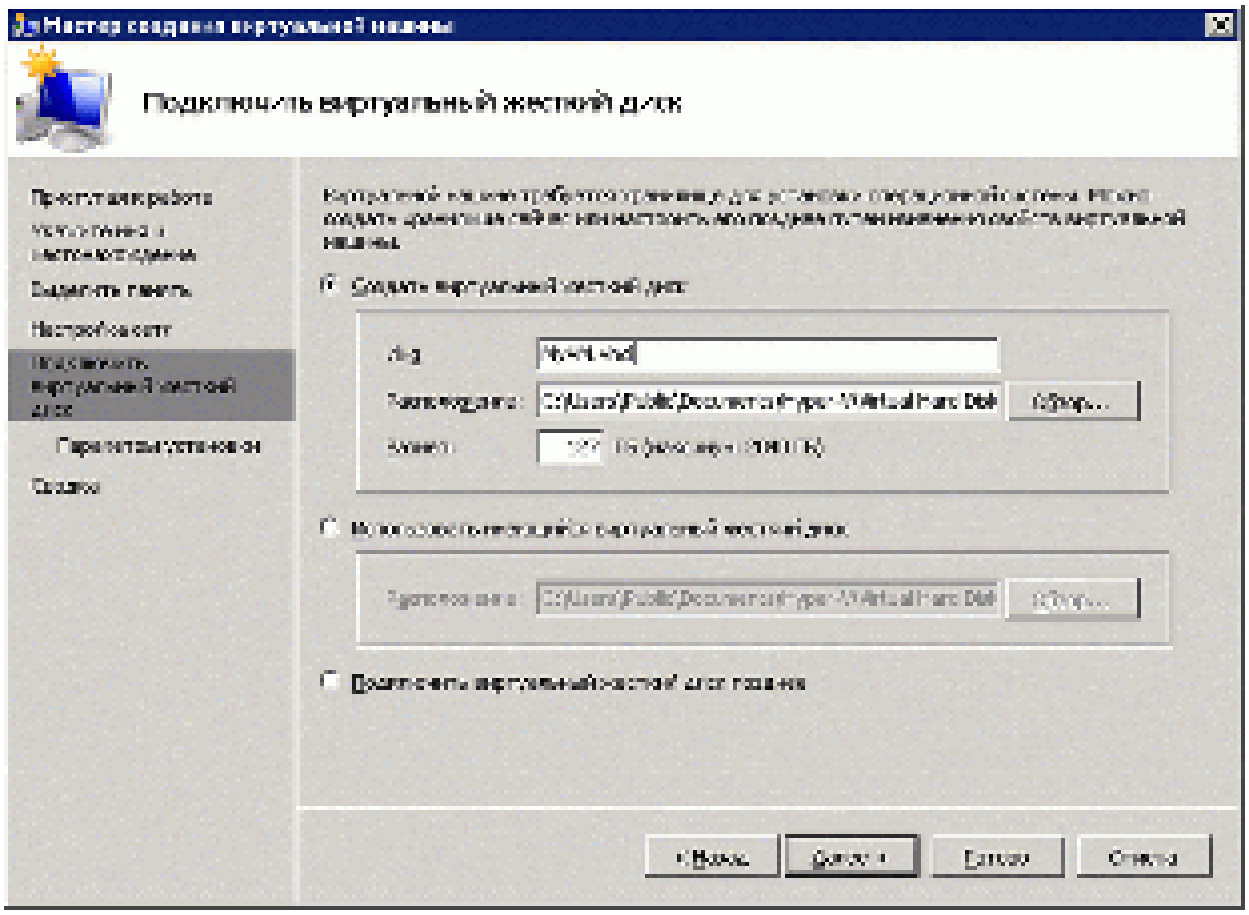

4. Укажите объем выделяемой оперативной памяти для виртуальной машины и нажмите "Далее".



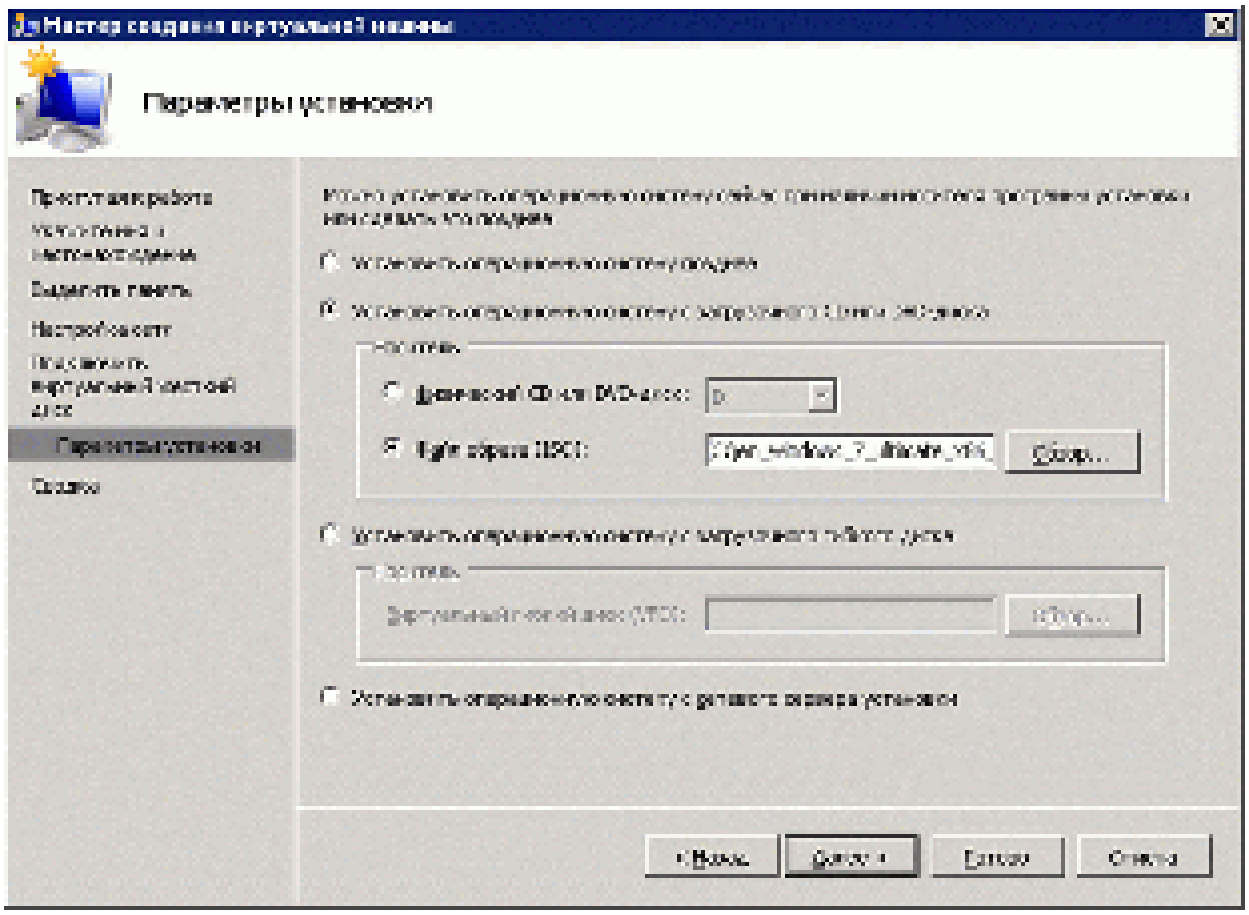

5. Укажите сетевое подключение, которое будет использоваться для доступа к сети. В случае, если виртуальные сети не были созданы при установке роли Hyper-V будет доступен только параметр "Нет подключения". Нажмите кнопку "Далее".



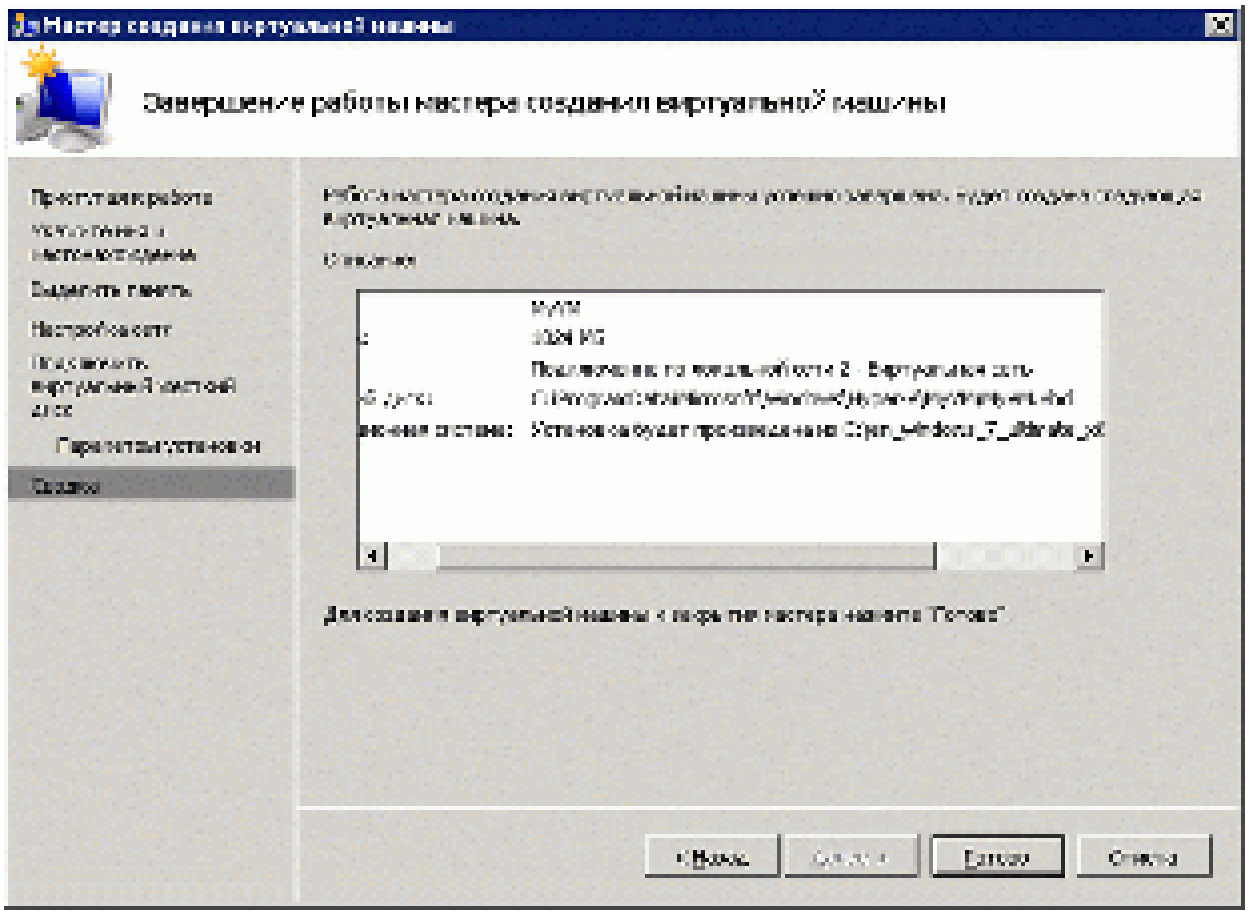

6. Укажите параметры виртуального жесткого диска создаваемой виртуальной машины. Можно как создать новый виртуальный HDD, так и использовать уже имеющийся. Кроме того, виртуальный HDD можно будет подключить к ВМ позднее. Нажмите кнопку "Далее".



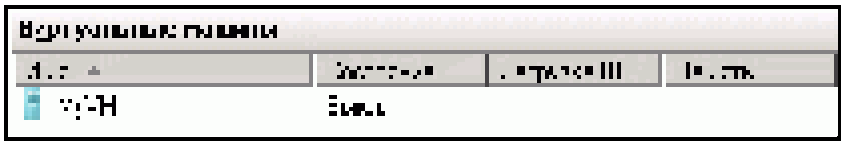

7. На следующем шаге необходимо определить параметры установки гостевой ОС. По - умолчанию виртуальная машина создается без ОС. В данном примере мы будем использовать .iso - образ загрузочного диска с Windows 7. Нажмите кнопку "Далее".




8. На последнем шаге создания виртуальной машины необходимо убедиться, что все параметры заданы верно и нажать кнопку "Готово".

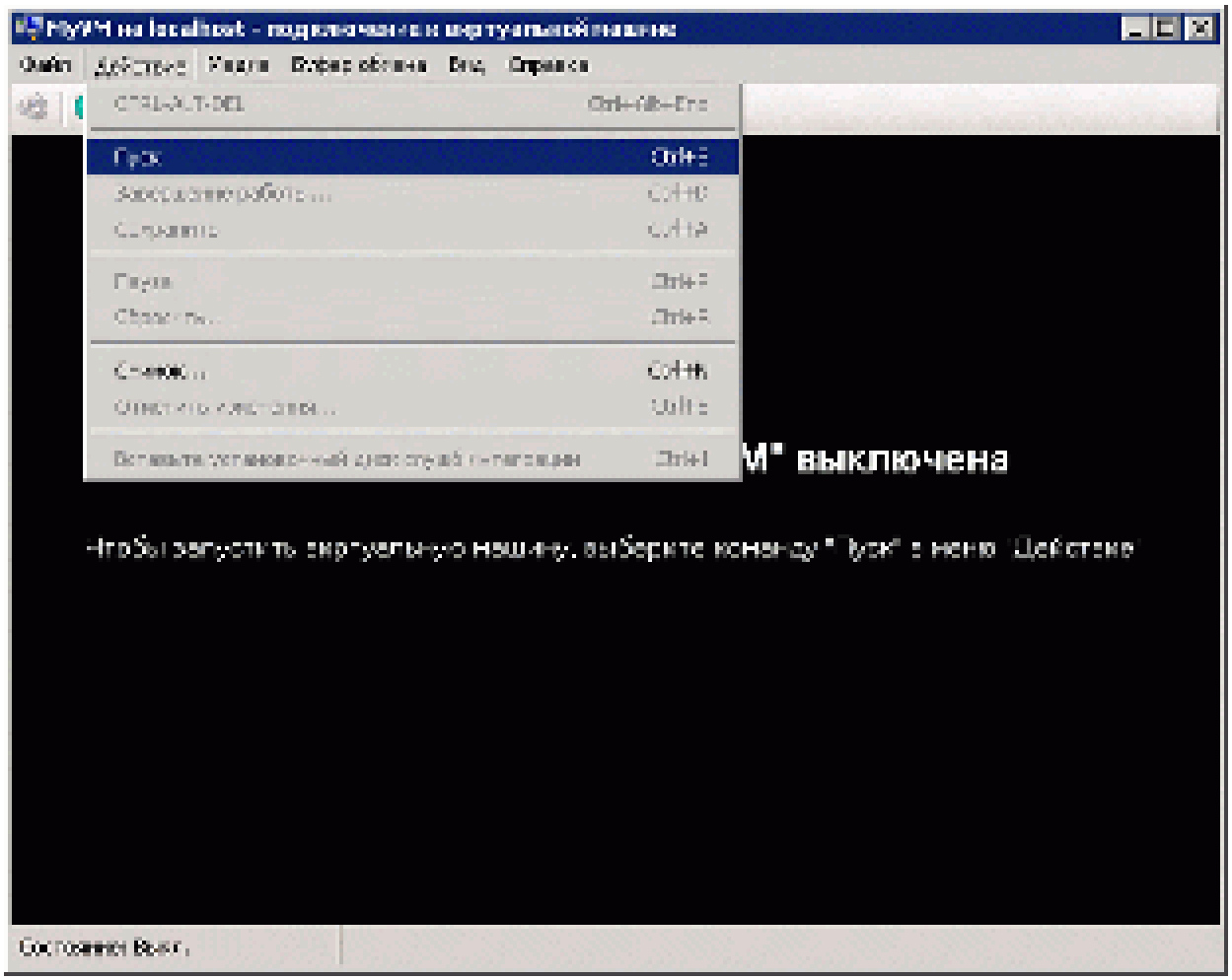


9. Дождитесь окончания процесса создания виртуальной машины. В списке виртуальных машин Диспетчера Hyper - V появится только что созданная ВМ.



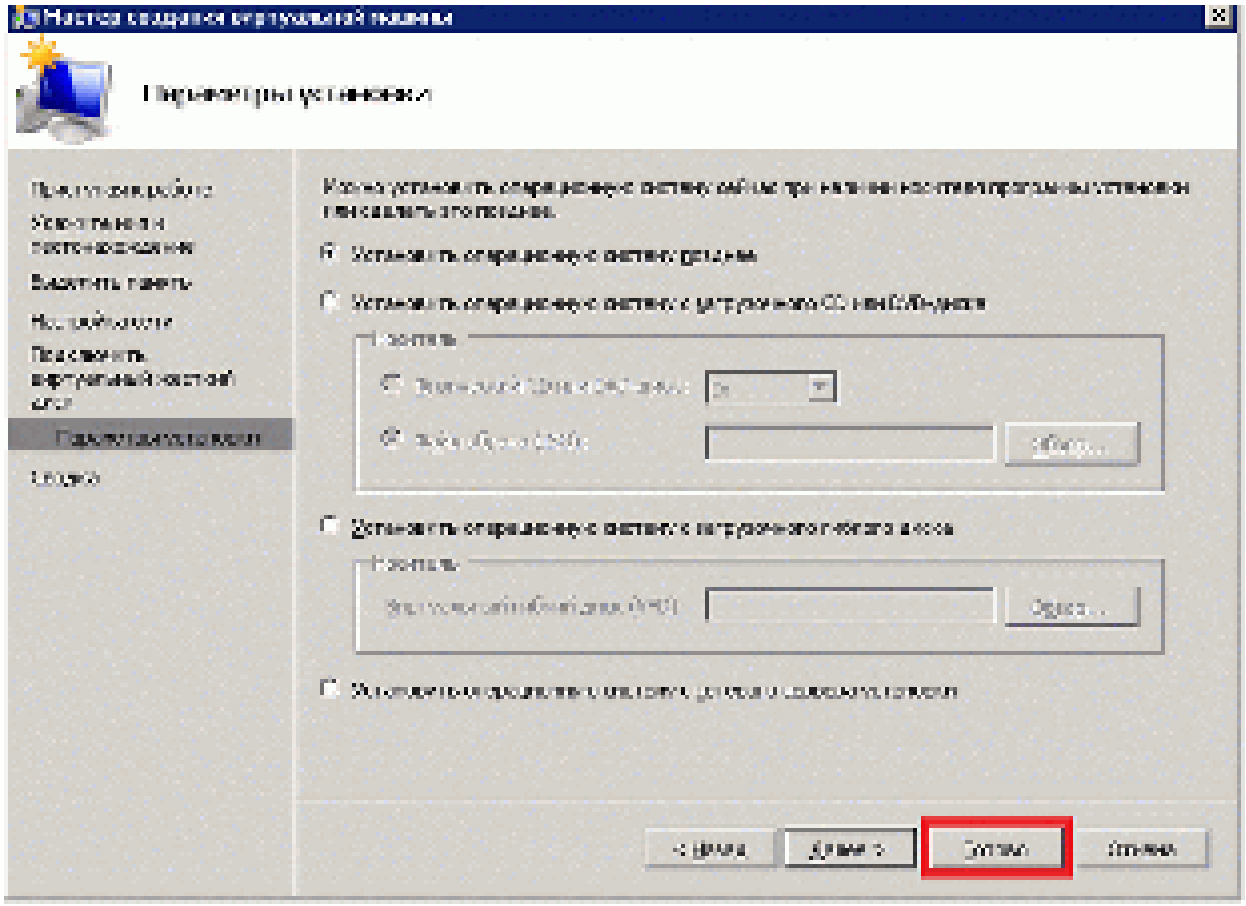
10. Для запуска виртуальной машины щелкните на ней правой кнопкой мыши и выберите "Подключить".

Откроется окно виртуальной машины. Для начала работы с ней необходимо выбрать в меню "Действие" пункт "Пуск".



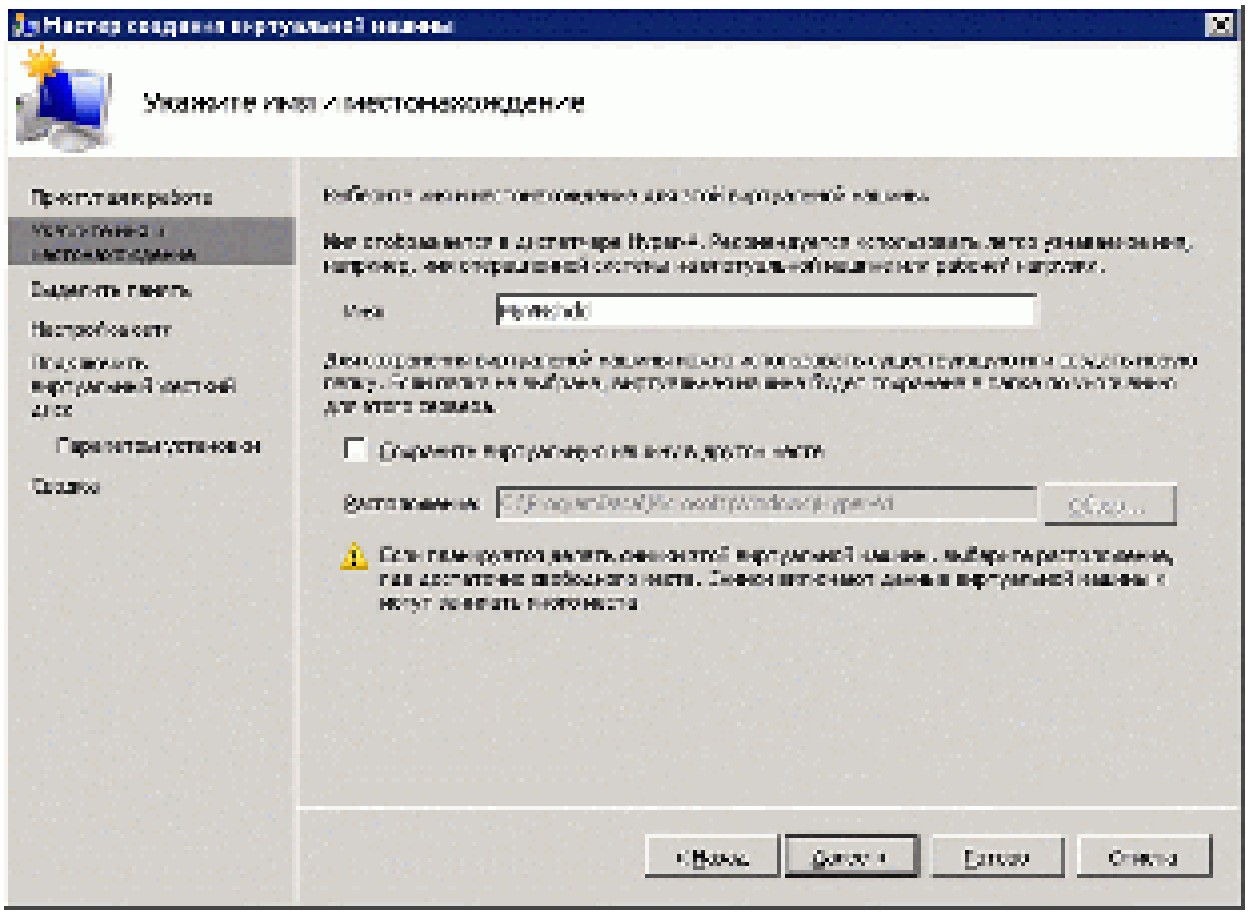

Можно создать виртуальную машину, не настраивая вышеуказанных параметров, достаточно только нажав кнопку "Готово" на первом шаге мастера создания виртуальной машины. В этом случае будет создана виртуальная машина с следующей конфигурацией по - умолчанию:

| | |
|---|---|
| Имя ВМ: | Новая виртуальная машина |
| Расположение: | Расположение по - умолчанию (в данном примере: C:\ProgramData\Microsoft\Windows\Hyper-V\) |
| Объем ОП: | 512 Мб |
| Сетевое подключение: | без сетевого подключения |
| Виртуальный HDD: | динамически расширяемый жесткий диск (127Гб) |
| Гостевая ОС: | без ОС |

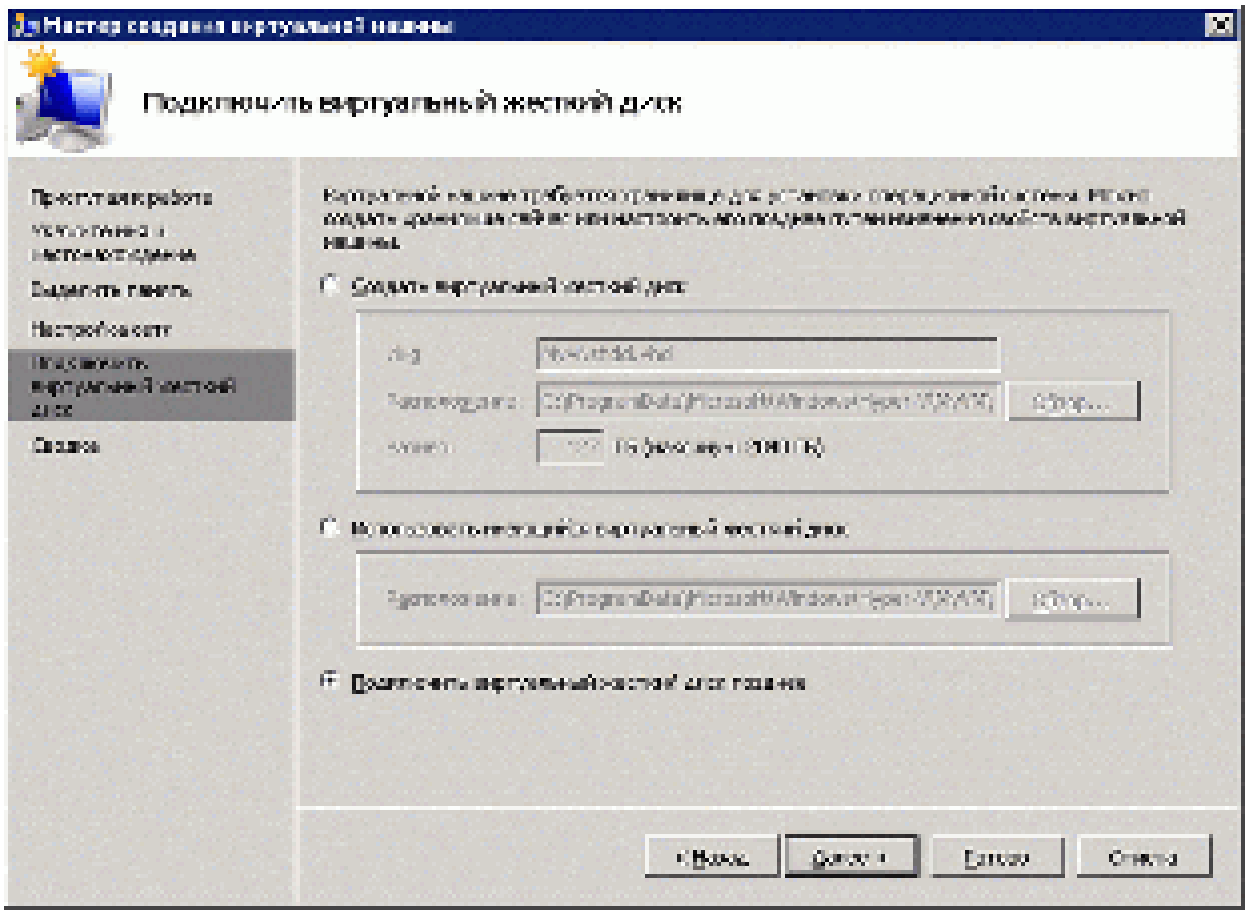


**Создание виртуальной машины с добавлением транзитного жесткого диска.**

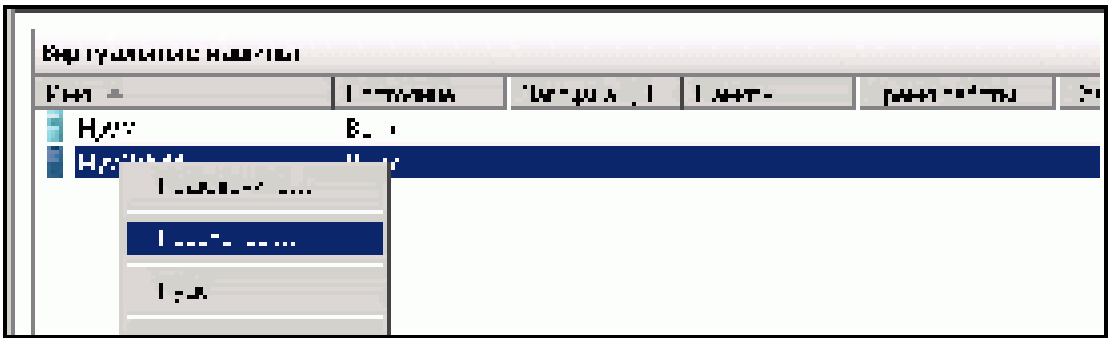
1. Запустите мастер создания новой виртуальной машины, укажите ее имя и нажмите "Далее".



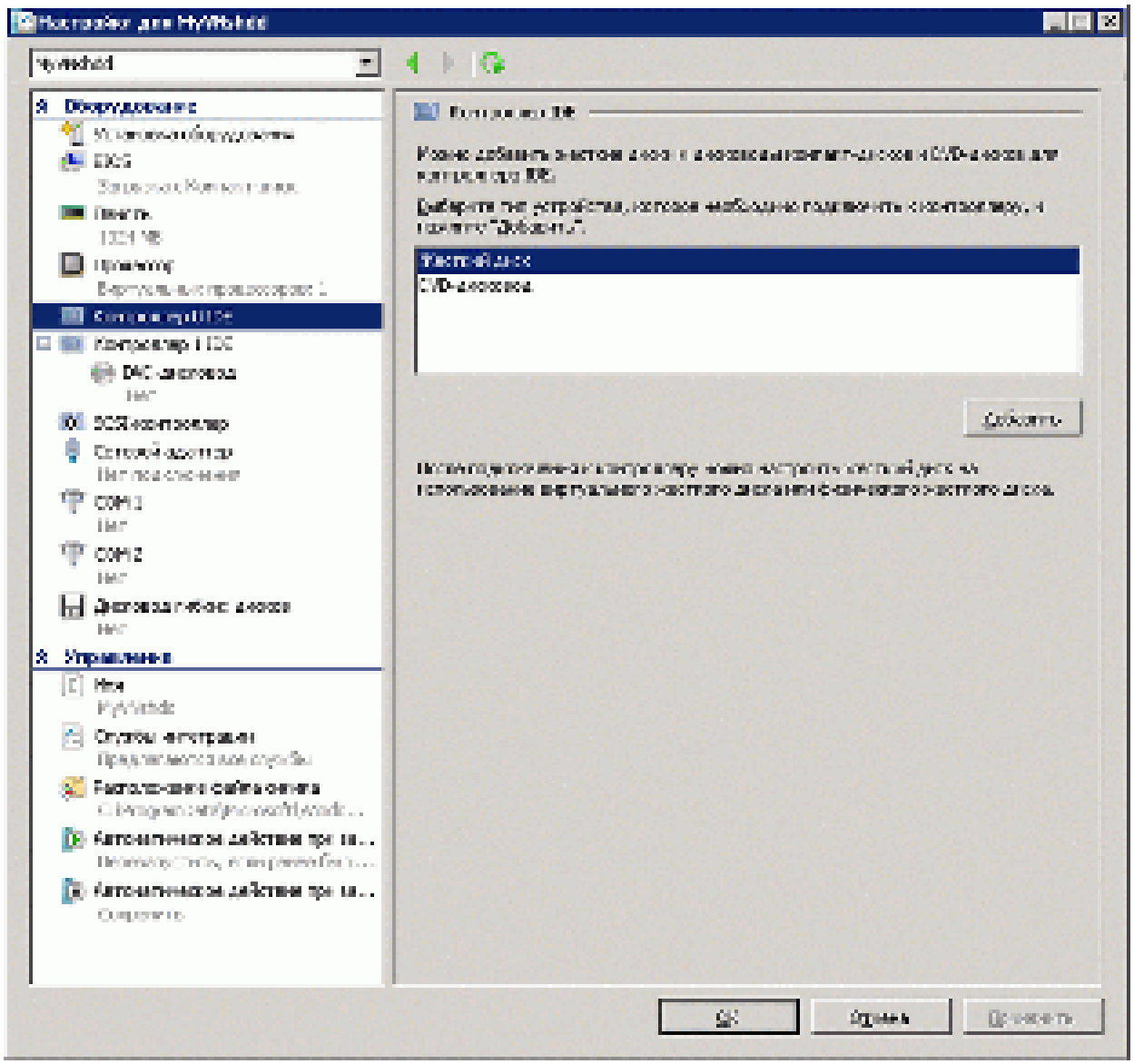
2. Дальнейшее создание виртуальной машины аналогично созданию таковой с виртуальным жестким дискам вплоть до этапа настройки виртуального жесткого диска, на котором необходимо выбрать пункт "Подключить виртуальный жесткий диск позднее".



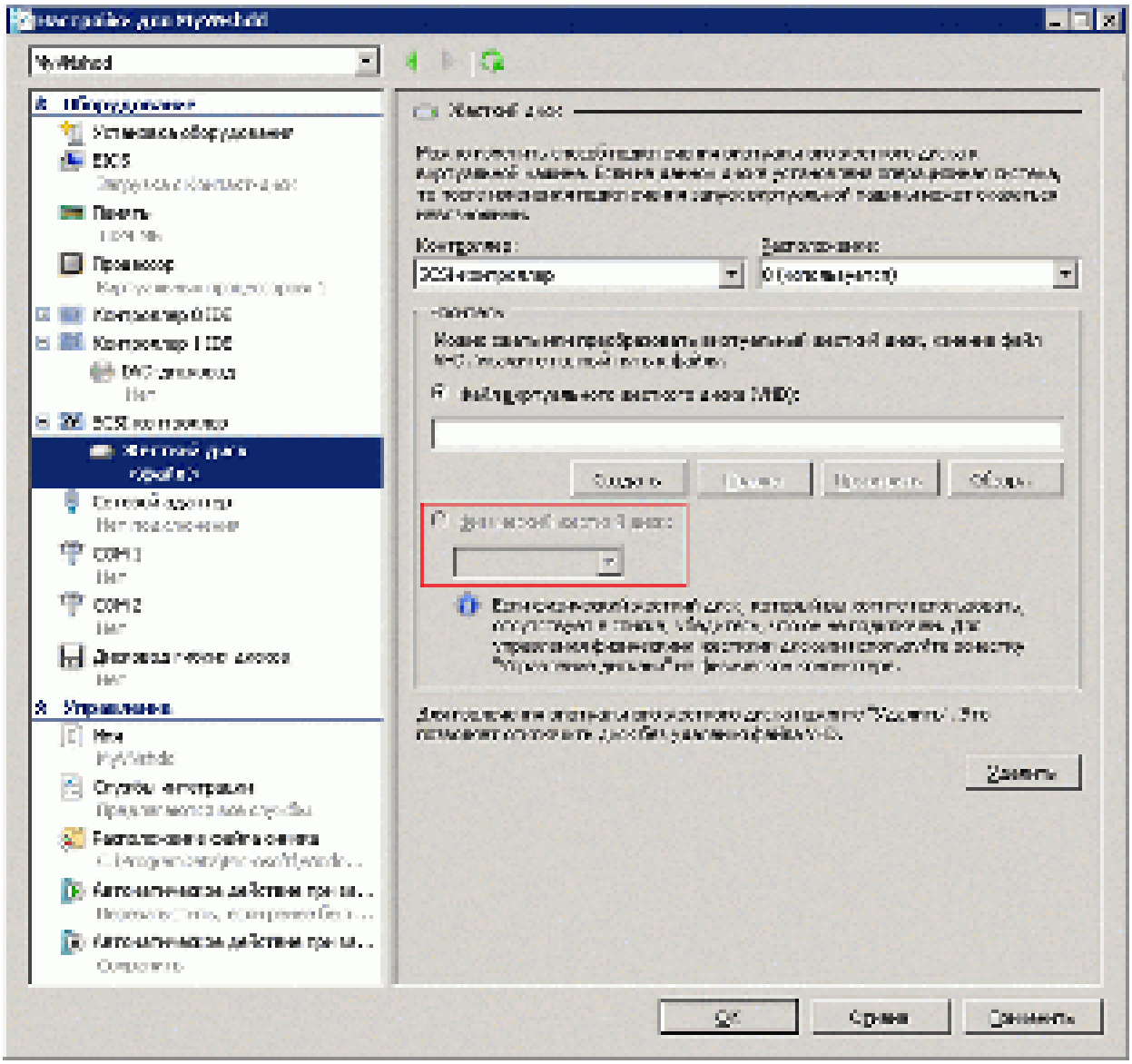

3. Выберите пункт выпадающего меню "Параметры".



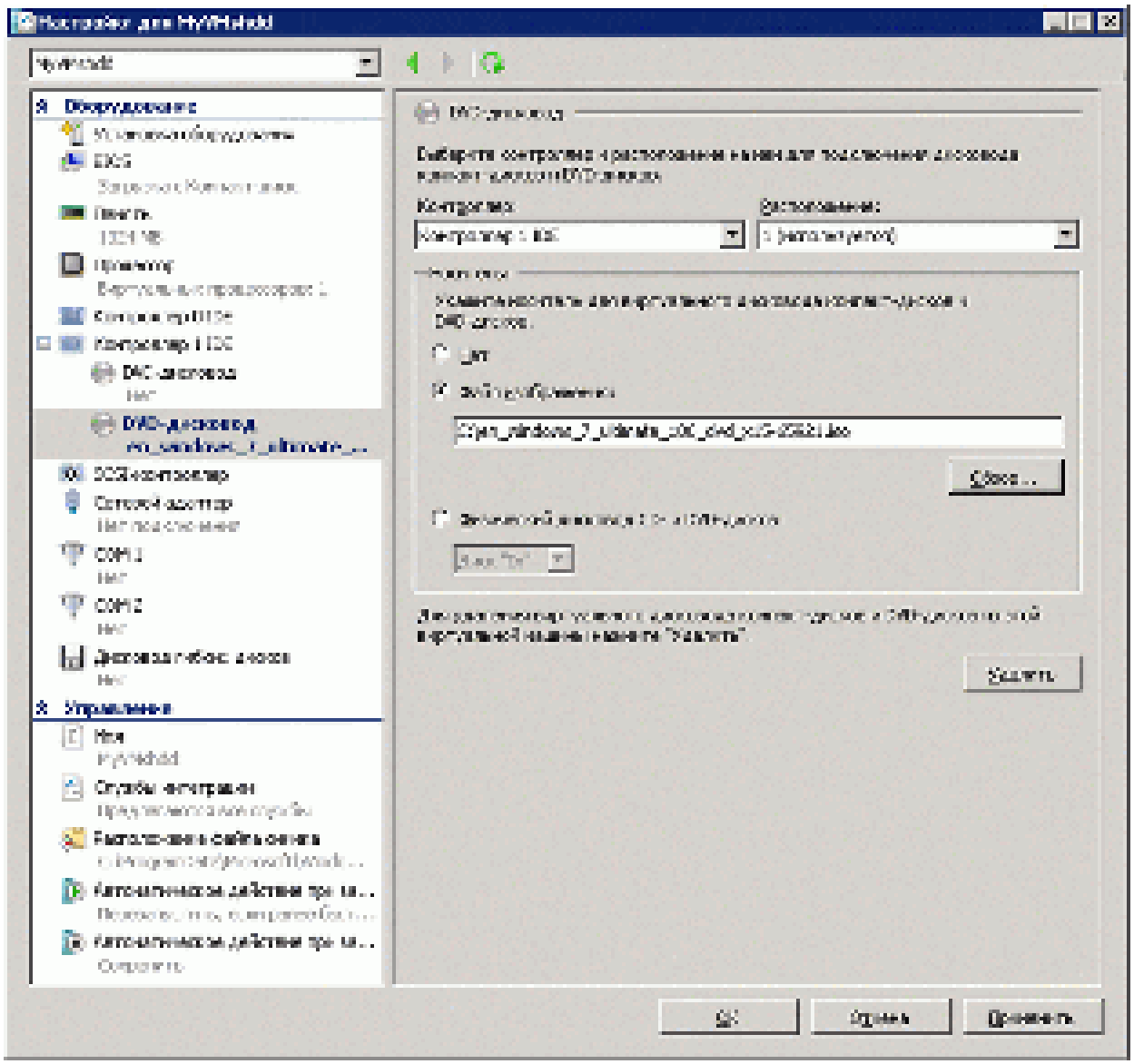
4. Выберите из списка оборудования контроллер жесткого диска и нажмите "Добавить".



5. Выберите физический жесткий диск, который будет использоваться виртуальной машиной.



6. Далее необходимо задать параметры установки гостевой ОС. Выберите в списке оборудования контролер CD/DVD привода и укажите тип носителя для установки ОС.



7. Нажмите кнопку Применить для сохранения изменений. Остается только запустить виртуальную машину и установить гостевую ОС.

## Практическое занятие №24 Установка и настройка Hyper-V_1

***Цель работы:***

Целью данной практической работы является подробное рассмотрение процесса установки Hyper-V роли на примере Windows Server 2008 R2.

Hyper-V позволяет запускать несколько операционных систем в виде виртуальных машин в Windows. В частности, Hyper-V предоставляет возможность выполнять виртуализацию оборудования. Это означает, что каждая виртуальная машина работает на виртуальном оборудовании. Hyper-V позволяет создавать виртуальные жесткие диски, виртуальные коммутаторы и

ряд других виртуальных устройств, каждое из которых можно добавить в виртуальную машину.

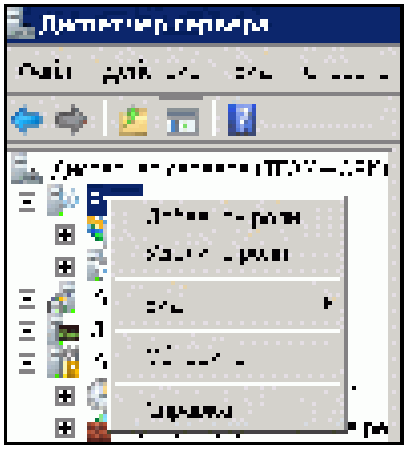
**Установка и настройка Hyper-V**

Требования к аппаратному обеспечению:

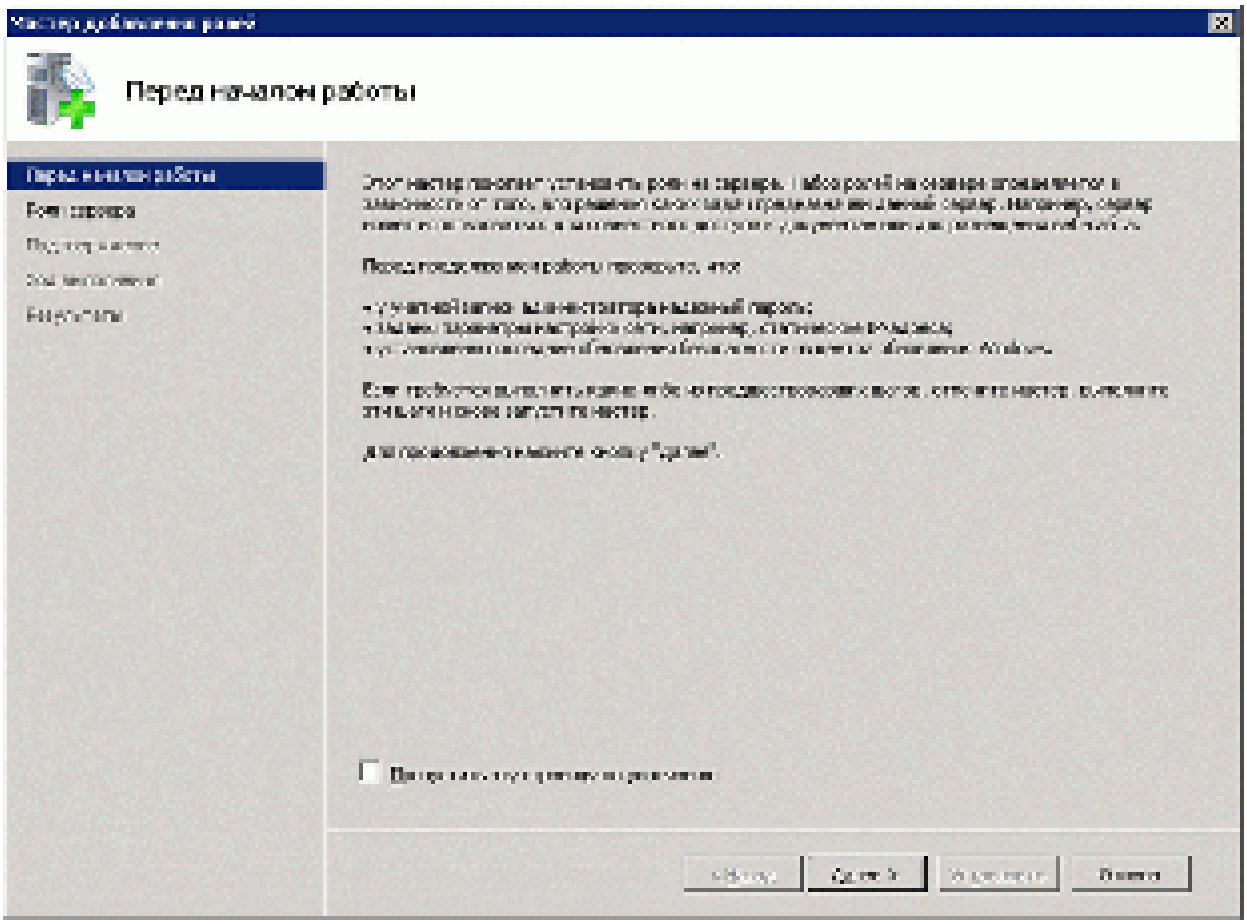
- x64 процессор;
- процессор, поддерживающий виртуализацию (hardware-assisted virtualization), к примеру, линейки процесоров Intel VT и AMD-V;
- должно быть доступно использование аппаратного предотвращения выполнения данных (DEP).

**Пошаговая установка Hyper - V роли Windows 2008 Server R2**

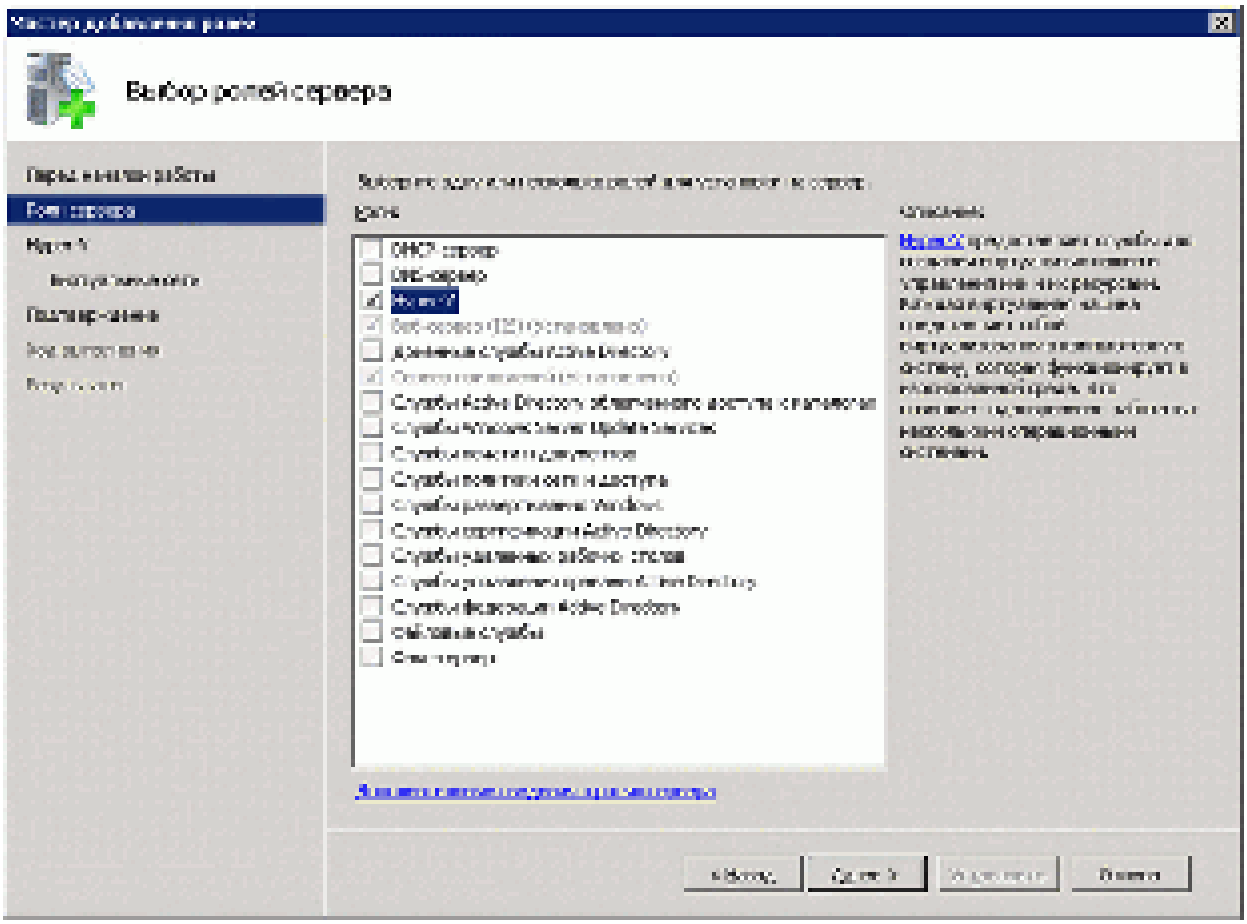
1. Запустите диспетчер сервера (Пуск-Администрирование-Диспетчер сервера (Server Manager)). На левой панели щелкните правой кнопкой мыши на выпадающем пункте меню "Роли" и выберите "Добавить роли".



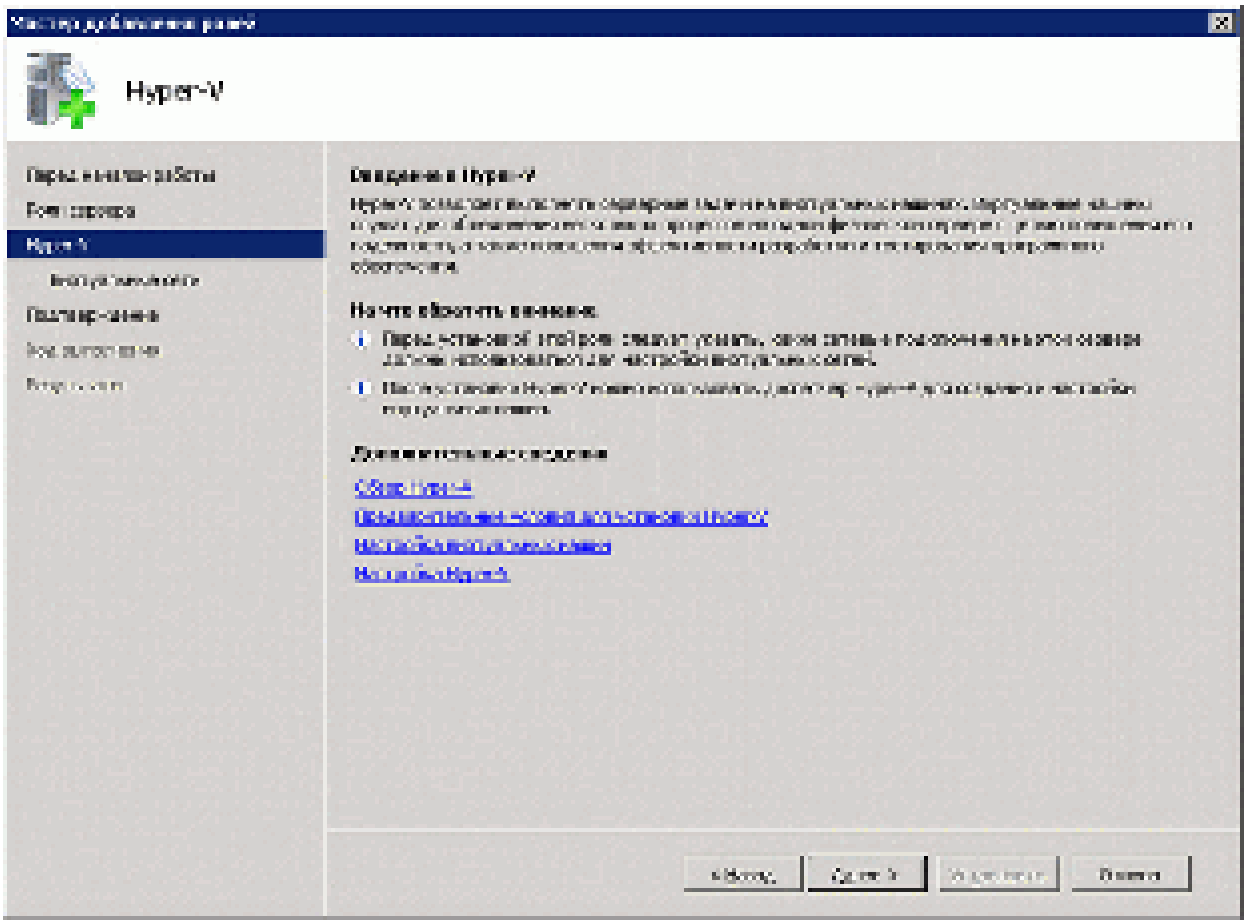
2. В открывшемся окне "Мастер добавления роли" нажмите на кнопку "Далее".



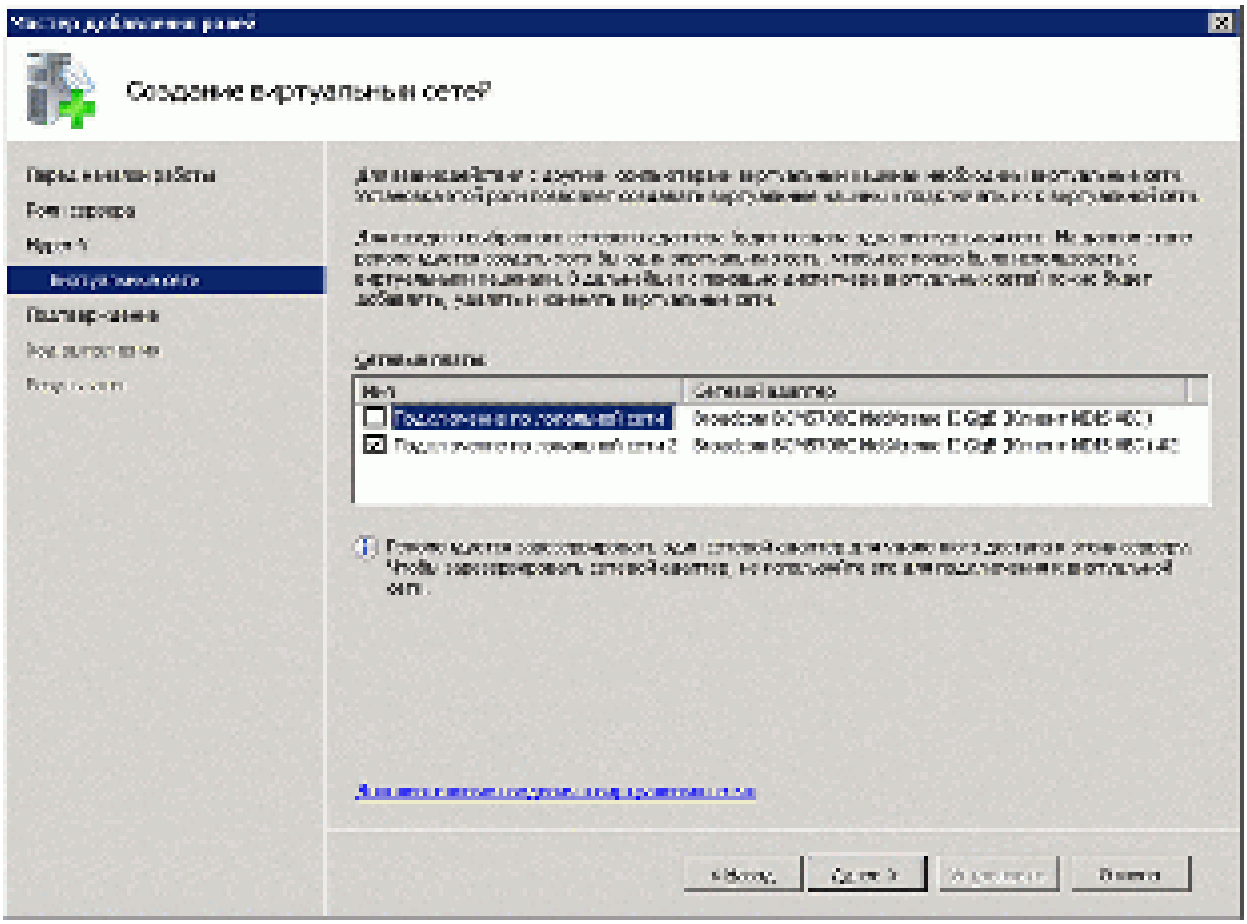

3. В следующем окне будут доступными для выбора роли Windows Server 2008. Выберите роль "Hyper-V" и нажмите кнопку "Далее".



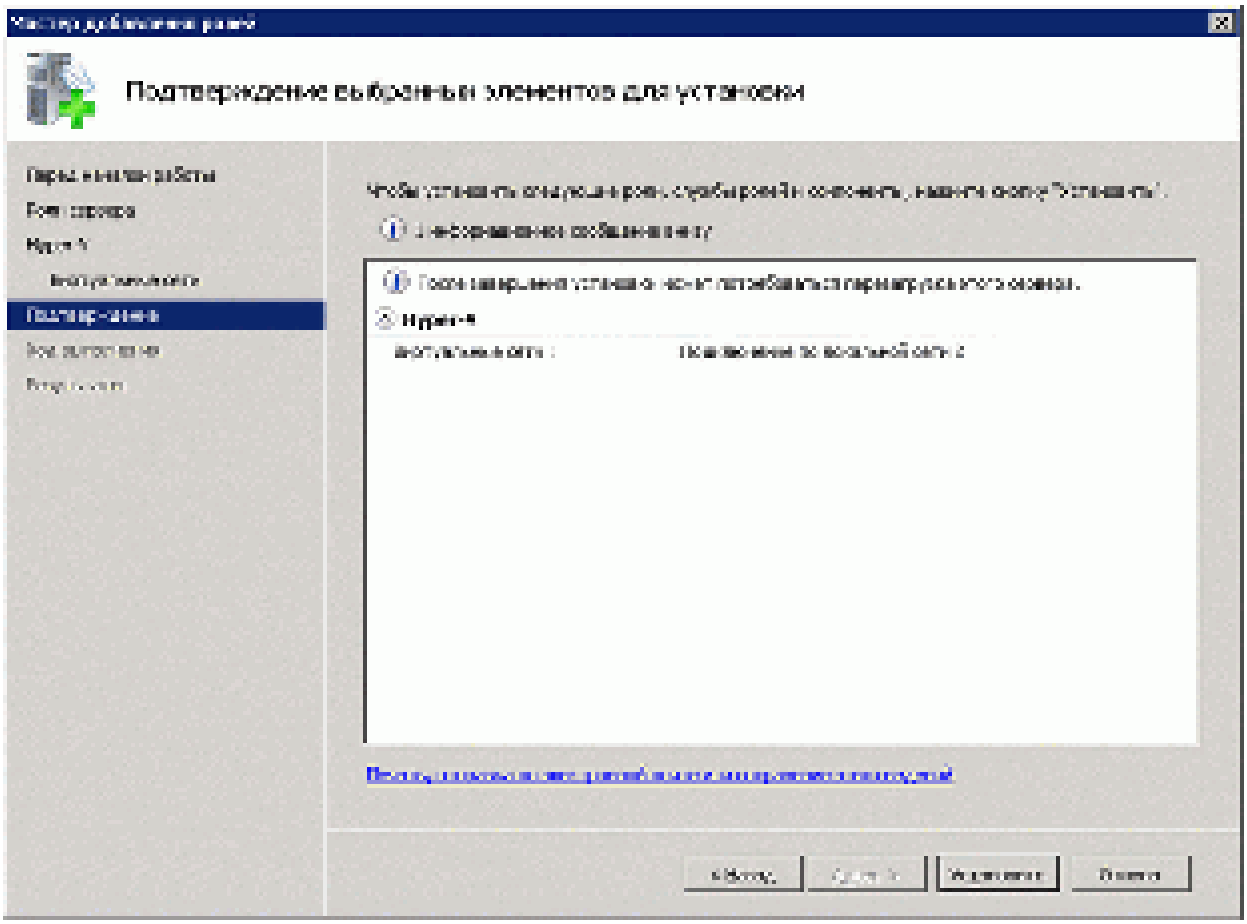

4. Следующее окно содержит информацию о роли Hyper-V и некоторых ее особенностях, на которые нужно обратить внимание. После ознакомления с информацией нажмите кнопку "Далее".



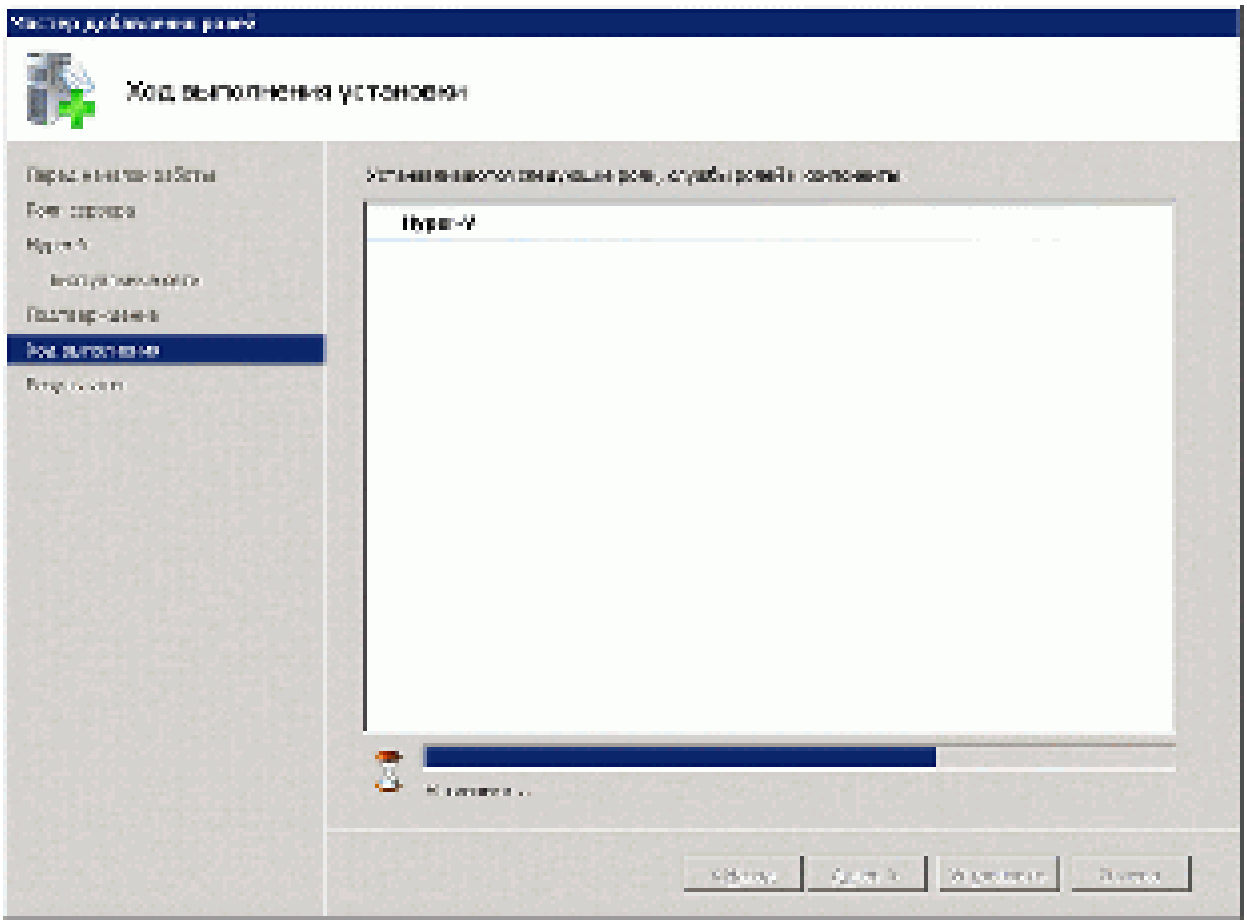

5. В окне мастера добавления установки "Создание виртуальных сетей" необходимо выбрать сетевой интерфейс, к которому будут привязаны виртуальные сети. После завершения процесса установки, при помощи диспетчера настройки виртуальных сетей можно будет создавать и настраивать виртуальные сети. Выберите, по крайней мере, одну сетевую плату и нажмите кнопку "Далее".



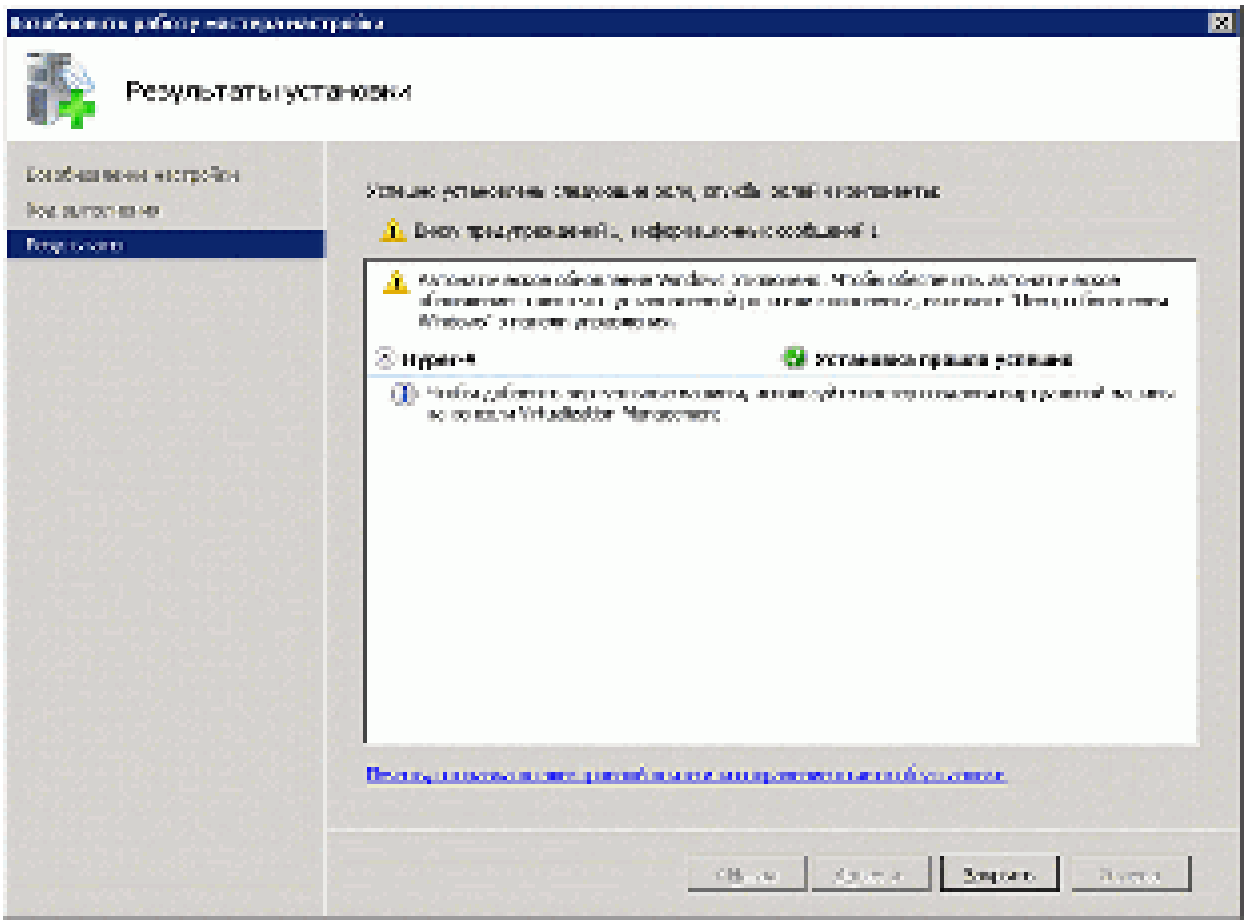

6. В окне "Подтверждение выбранных элементов для установки" можно ознакомиться с ролями и компонентами, которые будут установлены. Нажмите кнопку "Далее".




7. В процессе установки появится сообщение о необходимости перезагрузки компьютера. После перезагрузки установка Hyper-V будет продолжена. Дождитесь окончания процесса установки.




8. После установки, в случае, если процесс прошел штатно, появится сообщение об успешном завершении создания роли Hyper. Для завершения процесса установки нажмите кнопку "Закрыть".




Был рассмотрен процесс добавления роли Hyper - V операционной системы Windows Server 2008 R2.

**Практическое занятие №25. Экспорт и импорт виртуальных машин Hyper3-V**

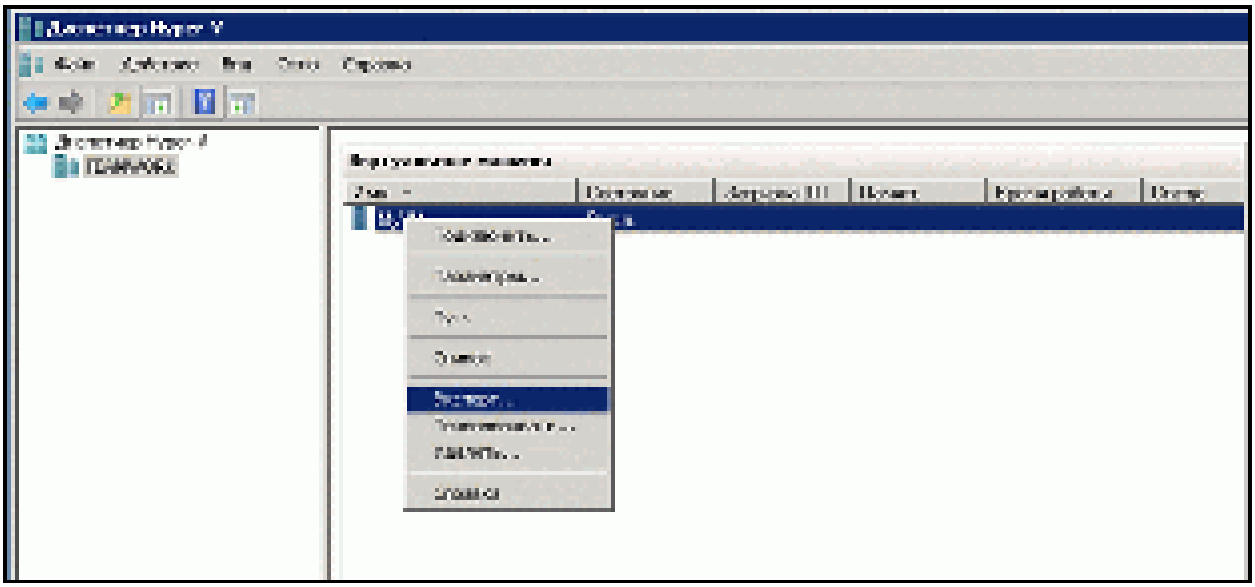
***Цель работы:***

Целью данной практической работы является подробное рассмотрение процессов экспорта и импорта виртуальных машин стандартными средствами Hyper-V и понятие снимок виртуальной машиной

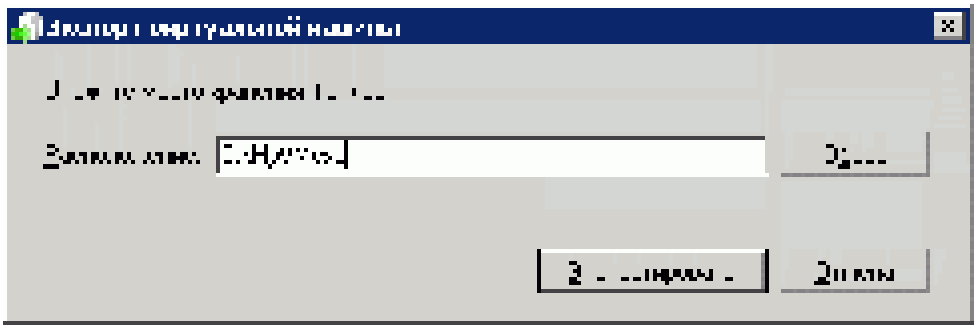
**Экспорт виртуальной машины**

Процесс экспорта виртуальной машины средствами Hyper-V не составляет труда. Единственный параметр, который необходимо определить - путь сохранения файлов виртуальной машины. Для экспорта ВМ необходимо:

1. Щелкнув правой кнопкой мыши на виртуальной машине выбрать пункт меню Экспорт.



2. Указать место хранения файлов экспортированной виртуальной машины и нажать кнопку Экспортировать.



В качестве места хранения файла может быть указан не только логический том локального жесткого диска, но также каталог на внешнем жестком диске или удаленном сервере.

На следующем рисунке представлено содержимое папки экспортированной виртуальной машины:

**Config.xml** -файл, содержащий информацию об исходном местоположении файлов виртуальных жестких дисков экспортируемой машины.

В папке **Virtual Machines** находится .exp файл, содержащий сведения об экспортированной виртуальной машине. В ходе импорта данный файл преобразуется в конфигурационный xml - файл.

В папке **Virtual Hard Disks** находятся файлы виртуальных жестких дисков экспортированной машины.

В папке **Snapshots** содержит сведения о моментальных снимках виртуальной машины (.avhd, .vsv, .bin).

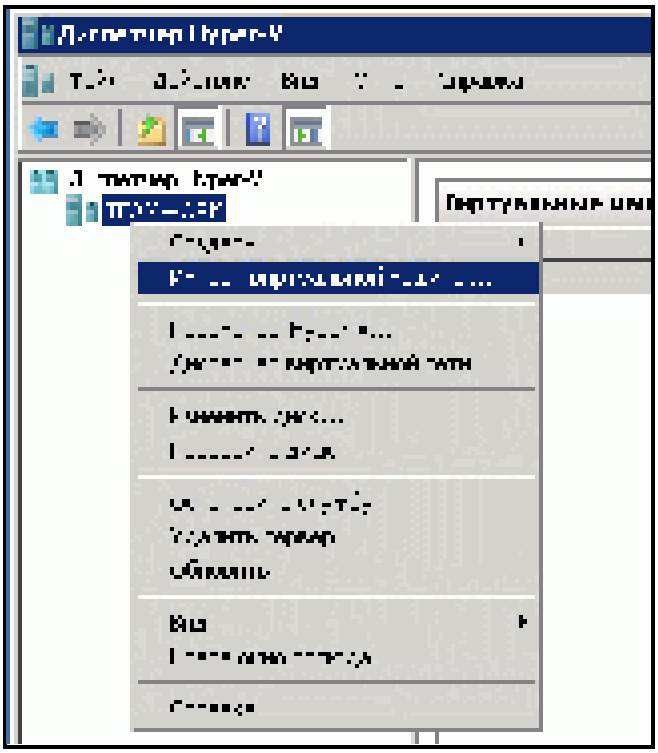
**Импорт виртуальной машины**

Отметим особенности импорта виртуальных машин Hyper - V:

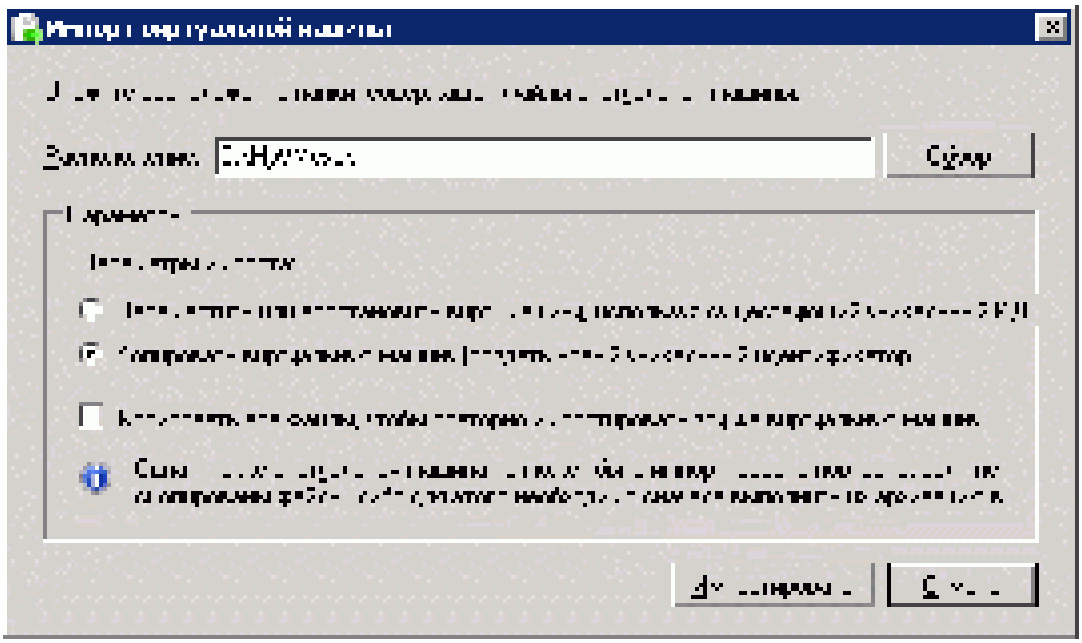
1. Импортировать в Hyper-V можно только виртуальные машины другого Hyper-V сервера. Импорт виртуальных машин Virtual PC или Virtual Server невозможен, поскольку конфигурация виртуальных машин, создаваемых этими решениями отличается от Hyper-V, несмотря на то, что все решения используют .vhd - файлы виртуальных жестких дисков.
2. Виртуальную машину можно экспортировать только один раз. Как уже отмечалось, создаваемый при экспорте .exp - файл сведений о виртуальной машине, в процессе импорта преобразуется в xml - файл конфигурации. В связи с этим, при возникновении ошибок импорта единственным способом продолжения работы с импортируемой виртуальной машиной является создание новой с аналогичной конфигурацией на основе уже имеющихся файлов виртуальных жестких дисков.

Для импорта виртуальной машины необходимо:

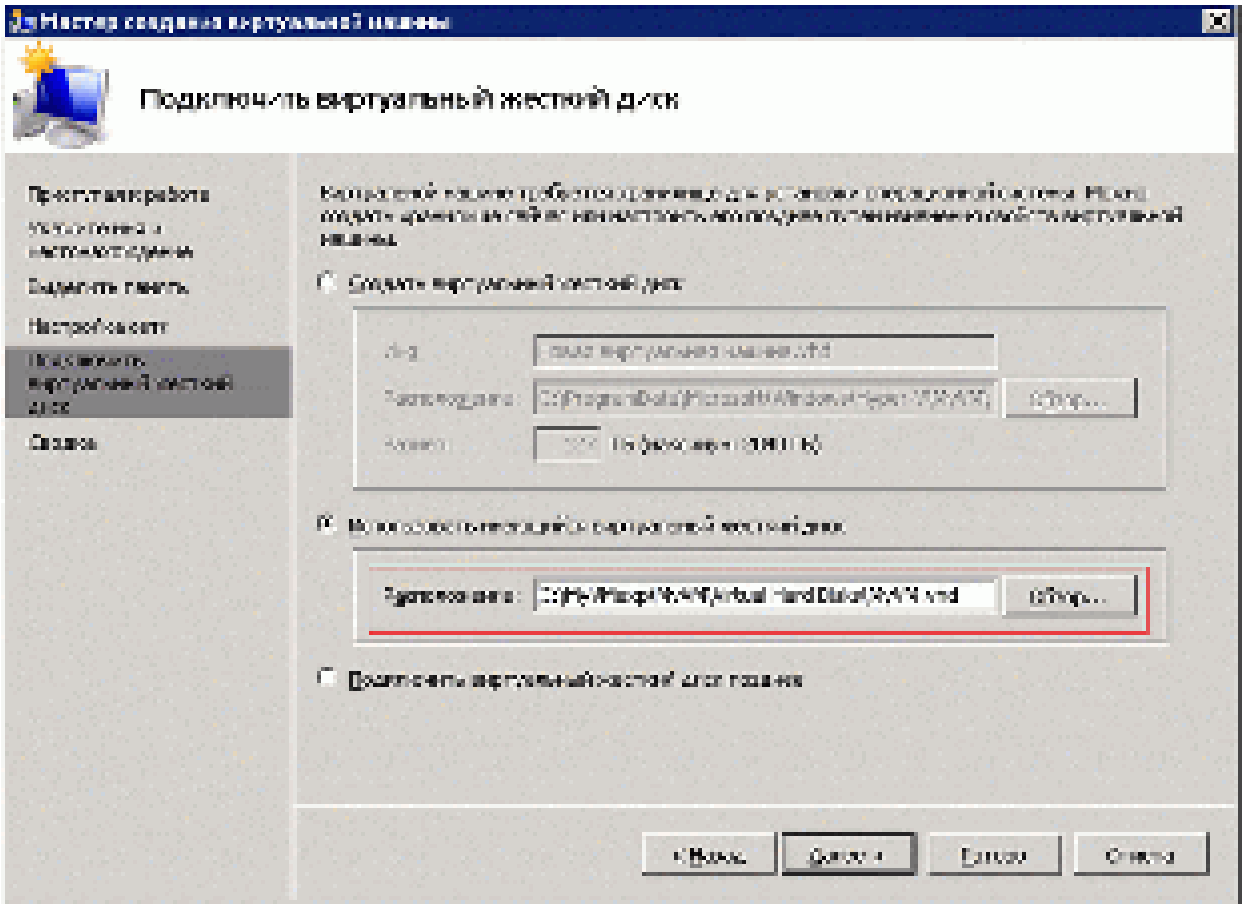
1. Выбрать пункт "Импорт виртуальной машины" меню Действие диспетчера Hyper -V.



2. В появившемся окне указать путь до папки, в которой располагаются файлы экспортированной виртуальной машины. Определить параметры импорта и нажать кнопку Далее.



В случае возникновения ошибки импорта, для продолжения работы с виртуальной машиной необходимо создать новую, и на этапе подключения виртуального жесткого диска указать файл жесткого диска импортируемой машины.

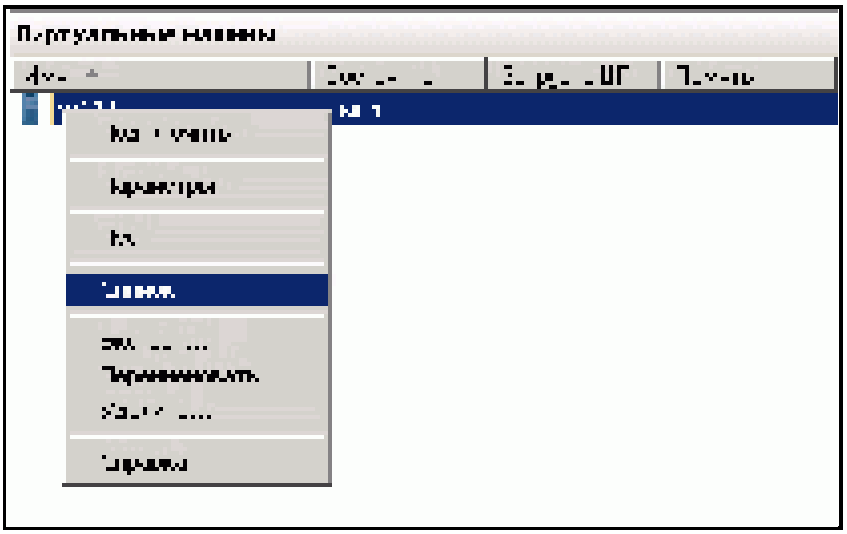



**Снимки виртуальной машины (snapshot)**

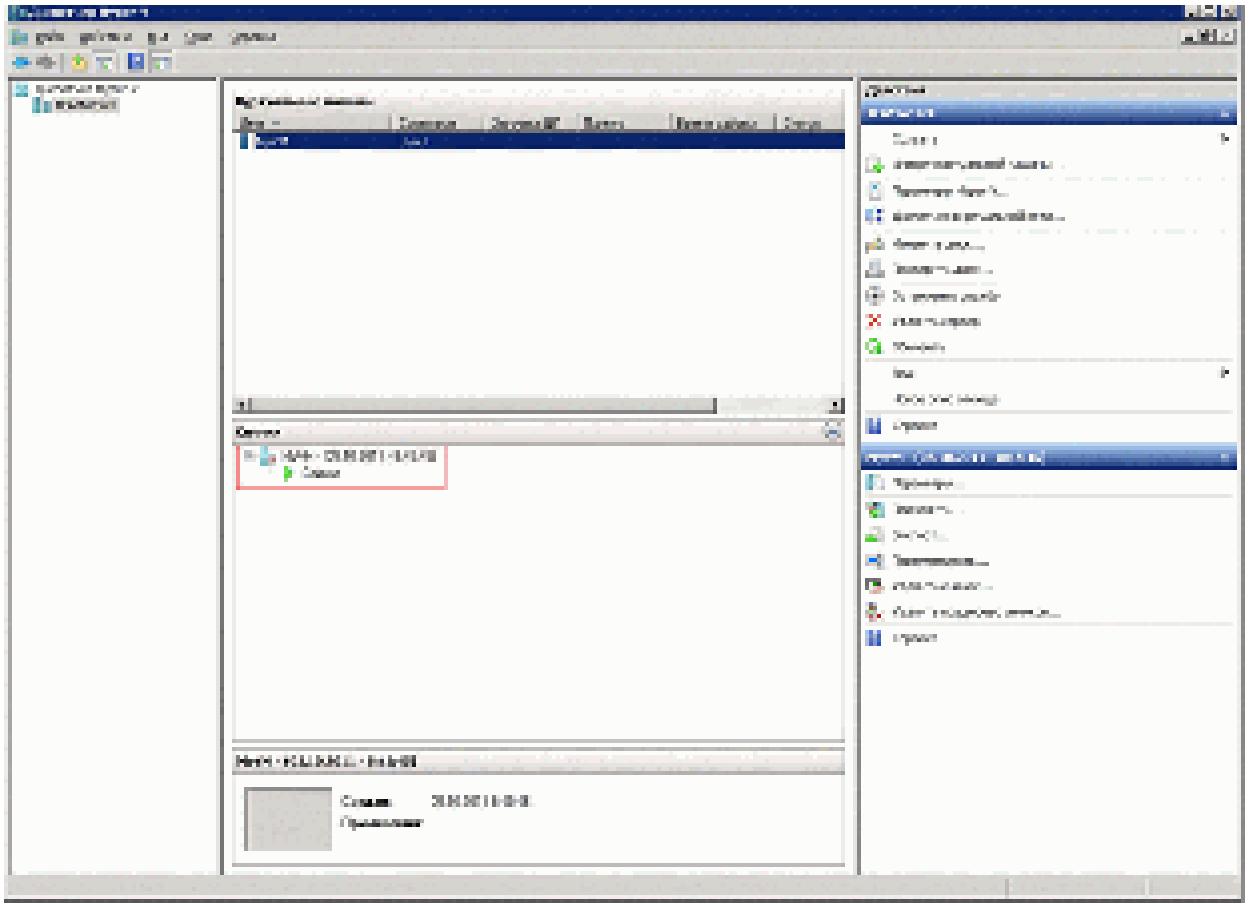
Снимком называется состояние виртуальной машины на определенный момент времени. Снимки используются для хранения информации о состояниях и возврата к ним, в случае необходимости (отмена внесенных изменений с момента создания снимка).

Нельзя создать снимок приостановленной виртуальной машины. При создании нескольких снимков может образоваться их хронологическая последовательность - дерево снимков.

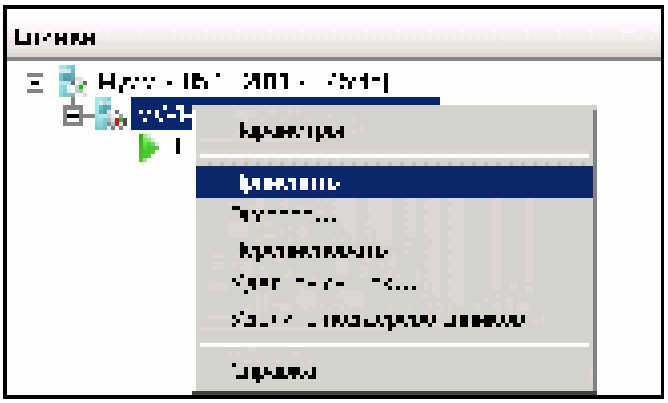
Для создания снимка необходимо выбрать пункт Снимок выпадающего меню.



После создания снимка появится соответствующий значок на панели "Снимки" диспетчера Hyper-V.



Для возврата виртуальной машины к состоянию снимка, необходимо применить его к виртуальной машине.



Доступны следующие действия работы со снимками:

- **Применить** - скопировать состояние виртуальной машины из выбранного снимка в активную виртуальную машину. При этом виртуальная машина возвращается к состоянию, описанному в выбранном снимке. Все несохраненные данные в активной виртуальной машине будут потеряны.
- **Переименовать** - команда позволяет изменения имени моментального снимка.
- **Удалить снимок** - команда удаления файлов, связанных с выбранным снимком, файлы других снимков затронуты не будут. При удалении текущее состояние активной виртуальной машины не меняется.
- **Удалить дерево снимков** - позволяет удалить выбранный моментальный снимок и все снимки, иерархически подчиненные ему. При удалении текущее состояние активной виртуальной машины не меняется.

Функции экспорта и импорта используются для переноса виртуальной машины с одного Hyper-V сервера на другой.

Снимки состояний, как правило, используются в процессе разработки, тестирования и развертки приложений. Снимки позволяют вернуть состояние виртуальной машины к моменту их создания, при этом все внесенные с этого времени изменения будут потеряны.