МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт Факультет приборостроения, информационных технологий и электроники	Кафедра «Информационная безопасность систем и технологий»
Специальность 10.05.03 –	Информационная безопасность автоматизированных систем
Специализация -	Защищенные автоматизированные системы управления

ДИПЛОМНЫЙ ПРОЕКТ

на тему

ПРАКТИКУМ ПО ПОСТРОЕНИЮ И АДМИНИСТРИРОВАНИЮ СИСТЕМЫ ЗАЩИТЫ СРЕДЫ ВИРТУАЛИЗАЦИИ НА ОСНОВЕ МЕХАНИЗМОВ БЕЗОПАСНОСТИ ОС WINDOWS SERVER

Студент _____ Трушин Роман Николаевич

Руководитель _____ Фатеев А.Г.

Нормоконтролёр _____ Фатеев А.Г.

Рецензент ведущий инженер АО «ПНИЭИ» _____ Горячев Д.В.

Работа допущена к защите (протокол заседания кафедры от 15.06.20 № 13)

Заведующий кафедрой _____ С.Л. Зефиров

Работа защищена с отметкой отлично (протокол заседания ГЭК от 25.06.20 № 9)

Секретарь ГЭК _____ А.П. Иванов

Пенза 2020

Оглавление

Введение……...5
1 Общее описание платформы виртуализации……7
2 Встроенные механизмы, которые применяются для обеспечения безопасности гипервизора и виртуальной инфраструктуры в целом……..10
2.1 Общая характеристика особенностей обеспечения безопасности виртуальной инфраструктуры……..10
2.2 Описание механизмов безопасности виртуальных инфраструктур и гипервизора……13
3 Создание ВМ, входящих в состав стенда…….……....20
3.1 ВМ, входящие в состав стенда…….....20
3.2 Создание ВМ с установленной гостевой ОС Windows 2012 R2……...22
3.3 Создание ВМ с установленным гипервизором Hyper-V 2012 R2…….44
3.4 Установка компонентов Hyper-V на ВМ…….....54
3.5 Установка роли и компонентов управления Hyper-V на ВМ с гостевой ОС Windows Server 2012 R2……..……...56
3.6 Создание и конфигурирование локальной сети, состоящей из виртуальных машин …….……....61
3.7 Установка компонентов ОС Windows Server, реализующих механизмы защиты виртуальных инфраструктур и средства администрирования……...….75
4 Порядок выполнения практического задания по теме «Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»…93
5 Порядок выполнения практического задания по теме «Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора…179
6 Описание порядка выполнения заданий практикума и результатов выполнения
заданий……20517

6.1 Порядок выполнения заданий практикума и результатов выполнения заданий по теме «Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»…….…...217
6.2 Порядок выполнения заданий практикума и результатов выполнения заданий по теме «Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»……219
7 Описание структуры и содержания отчета о выполнении практических заданий……..221
7.1 Структура и содержания отчета о выполнении практических заданий……..221
7.2 Содержание отчета о выполнении практической работы по теме «Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»……...…….221
7.3 Содержание отчета о выполнении практической работы по теме «Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора» ……...……231
8 Определение порядка контроля выполнения практического задания……...233
9 Подготовка сценариев для автоматизированного развертывания ВМ……234
10 Вредные психофизиологические факторы, влияющие на опорно-двигательный аппарат специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие…….237
Заключение……...240
Список используемых источников……242
Приложение А Состав виртуального стенда, использующегося при выполнении практикума……...243
Приложение Б UML – диаграмма последовательности действий при выполнении практического задания по теме «Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»……..245

Приложение В UML – диаграмма последовательности действий при выполнении практического задания по теме «Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»……...247
Приложение Г Графическое представление структур отчетов о выполнении практических работ……....249
Приложение Д Контрольные экземпляры отчетов о выполнении практических работ……..251
Приложение Е Графическое представление порядка контроля выполнения заданий ……..…260
Приложение Ж Сценарии автоматизированного развертывания ВМ ……...262
Приложение И Протокол проверки на оригинальность……...…...265

Введение

Одна из технологий, которая находит все большее применение в IT сфере - виртуализация. Многие организации используют ее в той или иной степени. Она обеспечивает снижение стоимости обслуживания, позволяет проводить тестирование новых систем и повышает уровень безопасности.

Виртуализация — предоставление набора вычислительных ресурсов или их логического объединения, абстрагированное от аппаратной реализации, и обеспечивающее при этом логическую изоляцию друг от друга вычислительных процессов, выполняемых на одном физическом ресурсе.

Примером использования виртуализации является возможность запуска нескольких операционных систем на одном компьютере: при том каждый из экземпляров таких гостевых операционных систем работает со своим набором логических ресурсов (процессорных, оперативной памяти, устройств хранения), предоставлением которых из общего пула, доступного на уровне оборудования, управляет хостовая операционная система — гипервизор.

Помимо преимуществ, которые обеспечивает технология виртуализации, ее применение создает ряд задач обеспечения безопасности виртуальных инфраструктур. Для решения задач защиты виртуальных инфраструктур могут применяться механизмы безопасности, реализуемые ОС Windows Server. Эти механизмы защиты реализуют широкий набор функциональных возможностей, которые обеспечивают защиту виртуальной инфраструктуры на различных уровнях.

В настоящее время во многих отчетах, обзорах, прогнозах и аналитических статьях в сфере информационной безопасности отмечается то, что использование ОС Windows Server с использованием среды виртуализации будет увеличиваться.

Выпускная квалификационная работа посвящена построению и администрированию системы защиты среды виртуализации на основе

механизмов безопасности ОС Windows Server. Актуальность темы выпускной квалификационной работы обуславливается увеличением применения операционных систем на базе Windows Server с использованием среды виртуализации и увеличением применения средств защиты информации для защиты ПЭВМ, работающих на базе ОС.

Целью данной выпускной квалификационной работы является разработка практикума по построению и администрированию системы защиты среды виртуализации на основе механизмов безопасности ОС Windows Server.

В ВКР должны быть рассмотрены следующие вопросы:

– платформа виртуализации Hyper-V и ее применение для создания виртуальных инфраструктур;

– механизмы безопасности Windows Server, применяемые для защиты виртуальных инфраструктур;

– описание создания ВМ и подготовки лабораторного стенда, используемого при выполнении заданий;

– порядок выполнения практического задания по теме «Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»;

– порядок выполнения практического задания по теме «Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»;

– описание порядка выполнения заданий практикума и результатов выполнения заданий;

– описание структуры и содержания отчета о выполнении практических заданий;

– определение порядка контроля выполнения задания;

– описание сценариев для автоматизированного развертывания ВМ;

– вредные психофизиологические факторы, влияющие на опорно-двигательный аппарат специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие.

1 Общее описание платформы виртуализации

Платформа виртуализации Hyper-V - это платформа аппаратной виртуализации, обеспечивающая создание изолированных программных окружений для использования в качестве виртуальных машин, одновременно работающих на одном физическом сервере. Платформа обеспечивает возможность запуска в рамках созданной виртуальной машины различных операционных систем, способных взаимодействовать с аппаратной частью физического сервера посредством поддерживаемой самой платформой виртуализации оборудования.

Отдельная версия Hyper-V Server является бесплатной. Первая версия была выпущена 1 октября 2008. Является базовым («Server Core») вариантом Windows Server 2008, то есть включает в себя полную функциональность Hyper-V; прочие роли Windows 2008 Server отключены, также лимитированы службы Windows.

Установка гипервизора Hyper-V позволяет создать инфраструктуру для виртуализации серверов, сегментов сети, клиентских машин или отдельных приложений. Благодаря средствам виртуализации Hyper-V работа ИТ-инфраструктуры становится эффективнее, повышается защищенность и отказоустойчивость, снижаются расходы на содержание.

Преимущества, которые дает технология виртуализации Hyper-V:

- рациональное использование оборудования. Поддержка аппаратной виртуализации Hyper-V дает возможность сосредоточить серверы на меньшем количестве физических машин. Например, перенос сервера на виртуальную машину Hyper-V позволит развернуть на единственном физическом сервере одновременно сервер Active Directory, сервер терминалов и баз данных, соответственно, у заказчика получится сэкономить средства на покупку оборудования и его эксплуатацию;

- организация частной облачной среды предприятия. Система виртуализации Hyper-V поможет создать общедоступные облачные ресурсы компании и гибко управлять их использованием. Для большей безопасности и защиты виртуальных серверов Hyper-V существует технология экранирования виртуальных машин (Shielded virtual machines);

- безопасность данных компании. Например, при переносе физической машины в виртуальную среду Hyper-V, можно развернуть две виртуальные машины – рабочую и персональную. На рабочей виртуальной машине настроить все необходимые ограничения доступа и политики безопасности, а на персональной виртуальной машине можно делать, что угодно, при этом данные компании останутся в полном порядке, так как виртуальные машины изолированы друг от друга;

- установка и настройка Hyper-V Server 2012 и хоста виртуализации удаленных рабочих столов предоставит пользователям личные виртуальные рабочие столы – готовое рабочее окружение с доступом к нему из любой точки мира, позволит централизовать администрирование и контролировать все пользовательские потоки данных. А средства динамической миграции ВМ дадут возможность выполнять перенос виртуальных машин Hyper-V практически незаметно для пользователей;

- моделирование любых сред для задач разработки и тестирования приложений;

- можно использовать виртуализацию при помощи Hyper-V для имитации физических компьютерных сред, в которых должно функционировать приложение. При этом нет необходимости покупать и поддерживать все аппаратные комплектующие, которые понадобились бы, если бы среду воссоздавали физически, достаточно установить Windows Hyper-V и смоделировать все необходимые компоненты;

- непрерывность бизнес-процессов;

- виртуализация серверов с Windows Server Hyper-V поможет уменьшить влияние простоев, поскольку виртуальный сервер не привязан к физическому оборудованию, которое может отказать. В случае отказа его можно быстро и несложно запустить на дублирующем оборудовании (лучше всего, если выполнена настройка сети Hyper-V Windows и организован отказоустойчивый кластер серверов);

- гипервизор Hyper-V распространяется бесплатно, его можно скачать с сайта Microsoft, устанавливается он на любой Windows или Linux сервер. Им легко управлять и просто использовать.

Для удаленного управления настройками Hyper-V используется консоль "Диспетчер Hyper-V" (Hyper-V Manager). Диспетчер Hyper-V позволяет управлять небольшим количеством узлов Hyper-V, как удаленными, так и локальными.

Для локального управления Hyper-V серверами используются стандартная командная строка, окно скрипта sconfig.cmd, а также оболочка Windows Powershell.

Оболочка Windows Powershell— это в первую очередь командная оболочка с языком сценариев, изначально созданная на основе платформы .NET Framework, а позднее — на .NET Core. В отличие от принимающих и возвращающих текстовые данные оболочек, Windows PowerShell работает с классами .NET, у которых есть свойства и методы. PowerShell позволяет выполнять обычные команды, а также дает доступ к объектам COM, WMI и ADSI. В ней используются различные хранилища, вроде файловой системы или реестра Windows, для доступа к которым созданы поставщики (providers). Стоит отметить возможность встраивания исполняемых компонентов PowerShell в другие приложения для реализации различных операций, в том числе через графический интерфейс. Верно и обратное: многие приложения для Windows предоставляют доступ к своим интерфейсам управления через PowerShell.

2 Встроенные механизмы, которые применяются для обеспечения безопасности гипервизора и виртуальной инфраструктуры в целом

2.1 Общая характеристика особенностей обеспечения безопасности виртуальной инфраструктуры

Основным требованием, которое предъявляется к виртуальной инфраструктуре, является непрерывная работа и доступность ресурсов. Большинство механизмов ориентировано именно на это.

Объекты виртуальной инфраструктуры на которые может осуществляться воздействие:

– аппаратная платформа, на которой функционирует виртуальная инфраструктура (сервер виртуализации);

– системное ПО (гипервизор);

– система управления виртуальной инфраструктурой (серверные и клиентские программные компоненты, позволяющие локально или удаленно управлять настройками гипервизора и ВМ);

– ВМ, включающие файлы конфигурации и виртуальные жесткие диски, содержащие установленное в ВМ системное и прикладное программное обеспечение, а также информацию, хранящуюся и обрабатывающуюся в ВМ;

– сетевые ресурсы и СХД (включающая коммутационное оборудование и систему хранения) с размещаемыми образами ВМ и данными (сеть хранения данных может быть реализована на основе SAN, NAS, iSCSI).

Особенности обработки информации при использовании виртуальной инфраструктуры:

– информация обрабатывается в пределах ВМ. В рамках одного сервера может существовать множество виртуальных серверов, на каждом из которых может обрабатываться информация различных категорий, а сами серверы

могут входить в разные информационные системы (локальные сети). При этом «образ» сервера может находиться в отдельно стоящем хранилище данных;

– информация передается между ВМ внутри виртуальной инфраструктуры. Поскольку ВМ – это также файл, хранящийся в хранилище данных, то передача информации между ВМ предполагает, что информация передается из одной области хранилища данных, проходит сетевое оборудование, попадает на сервер с развернутой виртуальной инфраструктурой, а затем в обратном порядке возвращается в хранилище, но уже для другой ВМ;

– информация передается между виртуальной инфраструктурой и внешней средой (как реальной, так и виртуальной). При этом из сетевого интерфейса одного физического сервера может «выходить» информация, относящаяся к различным виртуальным серверам, что требует интеграции механизмов защиты виртуальной среды и внешних физических компонентов.

Основные проблемы обеспечения безопасности виртуальной инфраструктуры:

– наличие трафика между ВМ. В локальных сетях в случае, когда один узел (компьютер) сети заражен (скомпрометирован) и используется в качестве источника воздействия на другие узлы (компьютеры) сети, сетевой трафик между ними можно перехватить и проконтролировать. В виртуальной среде физический интерфейс может не использоваться. Поэтому обычные средства сетевой защиты могут быть неэффективны;

– «растягивание» или «расползание» (sprawl) ВМ. ВМ легко создавать, делать их копии, переносить на другие серверы. Кроме того под «растягиванием» понимается увеличение файла образа ВМ;

– мобильность. ВМ могут перемещаться с одного сервера на другой с различными механизмами защиты. При этом защищенность серверов может отличаться;

– удержание и сохранение ресурсов. Обеспечение ИБ требует затрат ресурсов. Для виртуальных инфраструктур требуется распределять ресурсы между ВМ и средствами обеспечения ИБ для обеспечения их работоспособности;

– отсутствие фиксированного периметра безопасности и перемещение информации. Обрабатываемая информация может перемещаться между ВМ и физическими серверами;

– зависимость от аппаратных средств и ресурсов физического сервера;

– наличие большого количества ВМ, часть которых может редко запускаться для обработки данных (спящие ВМ). При этом в таких ВМ устаревают защитные механизмы;

– различный уровень защищенности ВМ. У виртуальных машин может быть различный уровень защищенности по причине создания их в разное время, отсутствия своевременного обновления и др.;

– наличие «суперпользователя». Наличие учетной записи администратора, обладающего максимальными полномочиями управления виртуальной инфраструктурой;

– использование СХД. Несколько ВМ физически находятся в одном разделе в целях обеспечения миграции и отказоустойчивости. Таким образом, получив контроль над подобным хранилищем с виртуальными машинами, злоумышленник получает доступ сразу к группе виртуальных машин;

– использование процедур клонирования и развертывания ВМ из шаблонов. При наличии ошибок в конфигурации исходной ВМ или в шаблоне, они будут повторены в созданных ВМ. Также могут быть использованы устаревшие шаблоны ВМ, без необходимых обновлений;

– при миграции ВМ могут оставаться «старые» данные. Они могут содержать как фрагменты конфигурации ВМ, так и фрагменты информации, хранящейся в файле виртуального жесткого диска;

– представление ВМ в виде набора файлов, которые могут быть скопированы на съемный носитель;

– применение процедур миграции и репликации для обеспечения функционирования виртуальной инфраструктуры. При миграции или репликации передаваемые файлы ВМ могут быть перехвачены или перенаправлены на сервер, находящийся под управлением злоумышленника;

– применение процедуры мгновенных снимков. Снимки могут быть использованы для скрытия следов воздействия, а также для несанкционированного копирования информации.

Механизмами безопасности виртуальной инфраструктуры являются:

— установка и обновление приложений;
— установка SSL - сертификатов;
— политики безопасности;
— антивирусная защита;
— системный мониторинг;
— резервное копирование;
— оптимизация виртуальных жестких дисков;
— перенос виртуальных серверов из других систем;
— защита от намеренного подбора паролей к учетных записям.

2.2 Описание механизмов безопасности виртуальных инфраструктур и гипервизора

Установка и обновление приложений. Обычной проблемой в крупной инфраструктуре является размножение образов. Это размножение приводит к тому, что появляется огромное количество шаблонов виртуальных машин с одной и той же операционной системой, но с различными приложениями или ролями. Управлять таким количеством образов и обеспечивать их обновление

непросто, но такие продукты, как System Center Virtual Machine Manager позволяют сократить число образов и устанавливать приложения, роли и функции в виртуальных серверах при помощи пакетов приложений.

Установка SSL – сертификатов. Если организация разрабатывает или использует веб-приложения, расположенные в виртуальной инфраструктуре, то доступ к этим приложениям необходимо защищать при помощи шифрования. Доверенные сертификаты – единственное надежное решение для защиты веб-приложений. Провайдеры облачных услуг могут предложить выпуск доверенных сертификатов SSL из панели управления.

Политики безопасности. Виртуальная инфраструктура повышает степень интеграции ИТ-средств, при этом одновременно уменьшая количество физического оборудования. Но количество сетевых приложений, сервисов остается таким же и даже большим. Поэтому защищать виртуальную инфраструктуру нужно комплексно, комбинируя сетевые и локальные средства защиты.

Следует иметь в виду, что политика безопасности, привязанная к таким физическим атрибутам, как физический сервер, IP-адрес, MAC-адрес не работает в облаке, так как провайдер облачных услуг может их изменить. Политику безопасности следует привязать к логическим атрибутам. Становятся важными идентификация, групп или роль пользователей, а также чувствительность нагрузки.

Модель контроля доступа должна быть основана на пользователе. Контроль сетевого доступа (Network Access Control — NAC) определяет пользователей и к чему у пользователей есть доступ. Контроль доступа должен учитывать, что пользователи могут прийти из любого места в Интернет, в любое время, с любого устройства, а также запрашивать доступ одновременно с разных устройств.

Антивирусная защита. Технологии виртуализации порождают ряд новых рисков информационной безопасности. Типичным примером атаки на облачные

среды является «антивирусный шторм», который вызывает одновременный запуск множества антивирусов. Такой шторм может привести к нарушению работоспособности виртуальной машины. Высокая доступность виртуальных машин и приложений может создать множество возможностей для злоумышленников. При этом одна незащищённая или зараженная виртуальная машина может стать источником угрозы для всей виртуальной инфраструктуры.

Традиционные средства защиты, например, агентские антивирусы, не всегда применимы в условиях виртуализации. Стоит выделить три основных подхода к антивирусной защите виртуальной инфраструктуре:

- первый подход состоит в том, что виртуальная среда предоставляет специальный программный интерфейс для контроля виртуальных машин через гипервизор, а антивирус используется им, перенаправляя всю защиту на специализированную виртуальную машину. Это позволяет отказаться от использования антивирусных агентов на виртуальных машинах;

- второй подход заключается в работе по старой схеме с использованием антивирусных агентов, которые нужно обновлять и настраивать. Но вместе с тем производители антивирусов стараются предоставить новые возможности для оптимизации исполнения агентов в виртуальной среде;

- третий подход заключается в том, чтобы не отказываться от агентов полностью, делать их максимально легковесными и простыми для исполнения, но в то же время большую часть аналитики реализовывать на специализированной виртуальной машине. Этот более универсален, но в некоторых случаях может уступать первым и вторым подходам.

Системный мониторинг. Так как виртуальная машина работает с виртуальным аппаратным обеспечением, за которым нет необходимости следить также, как и за физическим, можно удалить все программы-агенты аппаратного обеспечения при переводе физического сервера на виртуальную платформу. Кроме того, виртуальные машины загружаются быстрее

физических, и из-за этого система мониторинга может не успеть обнаружить перезагрузку виртуальной машины, если ее интервал сбора данных окажется слишком большой.

Резервное копирование. Виртуализация усложняет задачу резервного копирования. С одной стороны, можно продолжать выполнять резервное копирование с помощью традиционных средств путем установки на каждую виртуальную машину агента, который будет копировать файлы в нужное место. Этот метод надежен, но в условиях виртуальной среды может работать некорректно. При одновременном запуске агентов на всех виртуальных машинах возникает «шторм», в ходе которого каждая виртуальная машина стремится захватить все ресурсы сервера для выполнения задачи резервного копирования.

Другой подход состоит в том, что резервное копирование может выполняться на уровне сервера виртуализации. В этом случае копирование данных из виртуальных машин может проходить гораздо быстрее.

Одной из основных задач системного администратора является резервное копирование данных, находящихся на рабочих станциях и ноутбуках. Ведь в случае хищения ноутбука данные могут попасть к злоумышленникам, а пользователи редко сами принимают шифрование.

Оптимизация виртуальных жестких дисков. Подобно тому, как на физических серверах необходимо производить дефрагментацию жестких дисков, в виртуальных машинах необходимо производить сжатие виртуальных дисков. Сжатие применяется к динамически расширяемым и разностным виртуальным жестким диска.

Перенос виртуальных серверов из других систем. Если уже есть виртуальная инфраструктура в облаке, но по каким-то причинам ее нужно перенести к другому провайдеру применяется копирование виртуальной машины с полным сохранением ее конфигурации.

Защита от намеренного подбора паролей к учетным записям. В технологиях виртуализации существует возможность задания количества неудачных попыток входа до блокировки учетной записи, времени автоматической разблокировки учетной записи, а также сброс счетчика неудачных попыток входа.

Платформа виртуализации Hyper-V добавляет еще несколько функций таких как репликация, миграция виртуальных машин, экспорт и импорт ВМ, дедупликация данных.

Репликация виртуальных машин — это процесс создания точной копии (реплики) виртуальной машины с последующей поддержкой реплики в синхронизированном состоянии с исходной машиной. Репликация критически важных машин позволяет всегда иметь копию этой машины в готовом к запуску состоянии.

Миграция виртуальных машин — перенос виртуальной машины с одного узла кластера на другой.

Миграция может быть полезна, когда требуется мигрировать виртуальную машину на небольшой промежуток времени без простоя, а также при проблемах с производительностью сервера.

Экспорт виртуальной машины заключается в собирании всех необходимых файлов в одну единицу — файлы виртуального жесткого диска, файлы конфигурации виртуальной машины и файлы контрольных точек. Это можно сделать на виртуальной машине, которая находится в запущенном или остановленном состоянии.

При импорте виртуальной машины она регистрируется на узле Hyper-V. Можно выполнить импорт в узел или на новый узел. При импорте в тот же узел не нужно сначала экспортировать виртуальную машину, так как Hyper-V пытается повторно создать виртуальную машину из доступных файлов. Импорт виртуальной машины регистрирует ее, чтобы ее можно было использовать на узле Hyper-V.

Дедупликация данных — это поиск и удаление дублирующихся данных. Найденные копии данных удаляются и заменяются ссылками на оригинал, что позволяет хранить только уникальный контент и высвобождает дисковое пространство. Цель дедупликации заключается в том, чтобы разместить большее количество данных на меньшем пространстве.

Настройка межсетевого экрана на Hyper-V происходит следующим образом: для того чтобы разрешить сетевой трафик, который необходим для доступа к Hyper-V, а также для управления им и ресурсами ВМ, при инсталляции Hyper-V конфигурируется несколько правил межсетевого экрана. При настройке правил настраиваются как входящие, так и исходящие правила межсетевого экрана.

При управлении доступом Hyper-V определяет набор операций, которые можно использовать для создания элементов управления доступом на базе ролей (role-based access controls, RBAC), которые не требуют непосредственной модификации разрешений для каждого отдельного объекта, а присваивают разрешения набору ресурсов (чтобы можно было выполнить требующиеся функции). При использовании RBAC, роль – это базовый модуль, который позволяет управлять разрешениями и присваиваниями. Разрешения предоставляются роли, а роль присваивается пользователям или группам. В отличие от списков контроля доступа к файлам или каталогам (ACL) (которые хранятся с объектом), определения ролей, задач и операций (а также присваивание ролей пользователям и группам) хранятся отдельно от объектов в хранилище авторизации (которым можно управлять при помощи оснастки Authorization Manager для MMC).

При помощи Менеджера авторизации сервер Hyper-V запрашивает на стадии выполнения политику авторизации (для подтверждения того, что пользователь авторизован для выполнения запрошенной операции с ресурсом Hyper-V).

По умолчанию Hyper-V определяет одну область действия, более 30 операций и одну роль. Допускается модификация политики авторизации Hyper-V по умолчанию (при помощи консоли Authorization Manager для MMC). Для использования этой оснастки необходимо использовать учетную запись, которая является членом группы администраторов родительского раздела.

В Hyper-V по умолчанию определена только одна роль – Administrator. Поскольку все операции Hyper-V присвоены роли Administrator, то она может просматривать и модифицировать все объекты Hyper-V (в том числе виртуальные машины, виртуальные жесткие диски с соответствующими списками ACL, виртуальные сети и настройки Hyper-V).

При установке по умолчанию Windows Server 2012 Hyper-V только членам группы администраторов (родительского раздела) предоставлен доступ к управлению конфигурацией Hyper-V, а также объектами ВМ, виртуальных жестких дисков и виртуальных сетей. Группа администраторов – это единственная группа, которой присвоена роль Administrator. Для предоставления другим пользователям или группам разрешений на доступ к ресурсам Hyper-V и управление ими необходимо создать и добавить дополнительные роли и присвоить владение этими ролями.

Часть этих механизмов рассматривается в практикуме с учетом возможности реализации на ВМ.

Таким образом, из перечисленных в параграфе защитных механизмов в рамках практических заданий рассмотрены такие как установка SSL – сертификатов, оптимизация виртуальных жестких дисков, перенос виртуальных серверов из других систем, настройка межсетевого экрана, репликация виртуальных машин, миграция виртуальных машин, экспорт виртуальной машины.

3 Создание ВМ, входящих в состав стенда

3.1 ВМ, входящие в состав стенда

Перечень виртуальных машин, входящих в состав стенда:

- виртуальная машина 1 с установленным гипервизором Hyper-V 2012, являющаяся локальным сервером виртуализации;

- виртуальная машина 2 с установленной гостевой ОС Windows 2012 R2, которая является контроллером домена;

- виртуальная машина 3 с установленным гипервизором Hyper-V 2012, являющаяся сервером виртуализации, входящим в состав среды виртуализации;

- виртуальная машина 4 с установленным гипервизором Hyper-V 2012, являющаяся сервером виртуализации, входящим в состав среды виртуализации.

Аппаратная конфигурация ВМ 1 включает:

– количество процессоров – 1;

– объем оперативной памяти – минимальный 1Гбайт, рекомендуемый 2 ГБайт;

– виртуальный жесткий диск, подключаемый с использованием интерфейса SATA. Объем виртуального жесткого диска – 20 ГБайт;

– привод оптических дисков, подключаемый с использованием интерфейса SATA;

– видеопамять объемом 128 Мбайт;

– общая папка обмена между гостевой и основной ОС.

Программная конфигурация ВМ 1 включает:

– гостевая ОС – гипервизор Hyper-V 2012 R2;

– роль ВМ – сервер виртуализации;

– компоненты гостевой ОС – Hyper-V, Hyper-V Management Tools, Windows PowerShell, модуль Hyper-V для Windows PowerShell.

Аппаратная конфигурация ВМ 2 должна включать:

– количество процессоров – 1;

– объем оперативной памяти – 2 ГБайт;

– виртуальный жесткий диск, подключаемый с использованием интерфейса SATA. Объем виртуального жесткого диска – 30 ГБайт;

– привод оптических дисков, подключаемый с использованием интерфейса SATA;

– видеопамять объемом 128 Мбайт;

– сетевой адаптер с типом подключения «внутренняя сеть» (intnet). Тип адаптера Intel PRO/1000;

– общая папка обмена между гостевой и основной ОС.

Программная конфигурация ВМ2 включает:

– гостевая ОС – Windows Server 2012 R2 (разрядность 64 бит);

– роли ВМ – контроллер домена, сервер службы разрешения доменных имен (DNS сервер), сервер Internet Information Services, включая web-сервер, сервер приложений, сервер электронной почты (SMTP-сервер) и компоненты гостевой ОС, центр сертификации Active Directory:

– компоненты гостевой ОС – компоненты Microsoft Active Directory, включая средства управления контроллером домена, средства управления Internet Information Services, сервером приложений, средства управления сервером DNS, средства управления службами сертификатов Active Directory, NET Framework 3.5 и 4.5.

Аппаратные конфигурации ВМ3 и ВМ4 включают:

– количество процессоров – 1;

– объем оперативной памяти – минимальный 1Гбайт, рекомендуемый 2 ГБайт;

– виртуальный жесткий диск, подключаемый с использованием интерфейса SATA. Объем виртуального жесткого диска – 30 ГБайт;

– привод оптических дисков, подключаемый с использованием интерфейса SATA;

– видеопамять объемом 128 Мбайт;

– сетевой адаптер с типом подключения «внутренняя сеть» (intnet). Тип адаптера Intel PRO/1000;

– общая папка обмена между гостевой и основной ОС.

Программные конфигурации ВМ3 и ВМ4 включают:

– гостевая ОС – гипервизор Hyper-V 2012 R2;

– роль ВМ – сервер виртуализации;

– компоненты гостевой ОС – Hyper-V, Hyper-V Management Tools, Windows PowerShell, модуль Hyper-V для Windows PowerShell, средства удаленного администрирования сервера, службы удаленных рабочих столов включая компоненты виртуализации рабочих столов.

3.2 Создание ВМ с установленной гостевой ОС Windows 2012 R2

Необходимо создать виртуальную машину (ВМ) с установленной гостевой ОС Windows Server R2. Для создания ВМ следует запустить программу Oracle VirtualBox Менеджер. Для создания ВМ нажать кнопку «Создать» на панели инструментов. На экране появится диалоговое окно мастера создания ВМ. На первом этапе создания ВМ следует указать имя ВМ, тип и версию гостевой ОС. В качестве значений этих параметров указаны следующие:

- имя – WS2012-DC;

- тип – Microsoft Windows;

- версия – Windows 2012 (64 bit).

Установленные параметры приведены на рисунке 1.

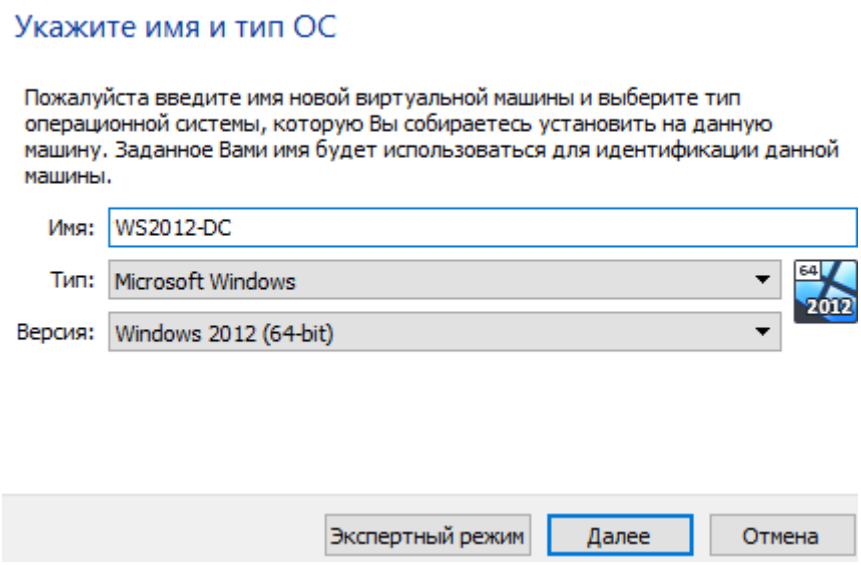


Рисунок 1-Настройка параметров виртуальной машины

Далее необходимо указать объем оперативной памяти для виртуальной машины - 2048 Мб (см. рисунок 2).

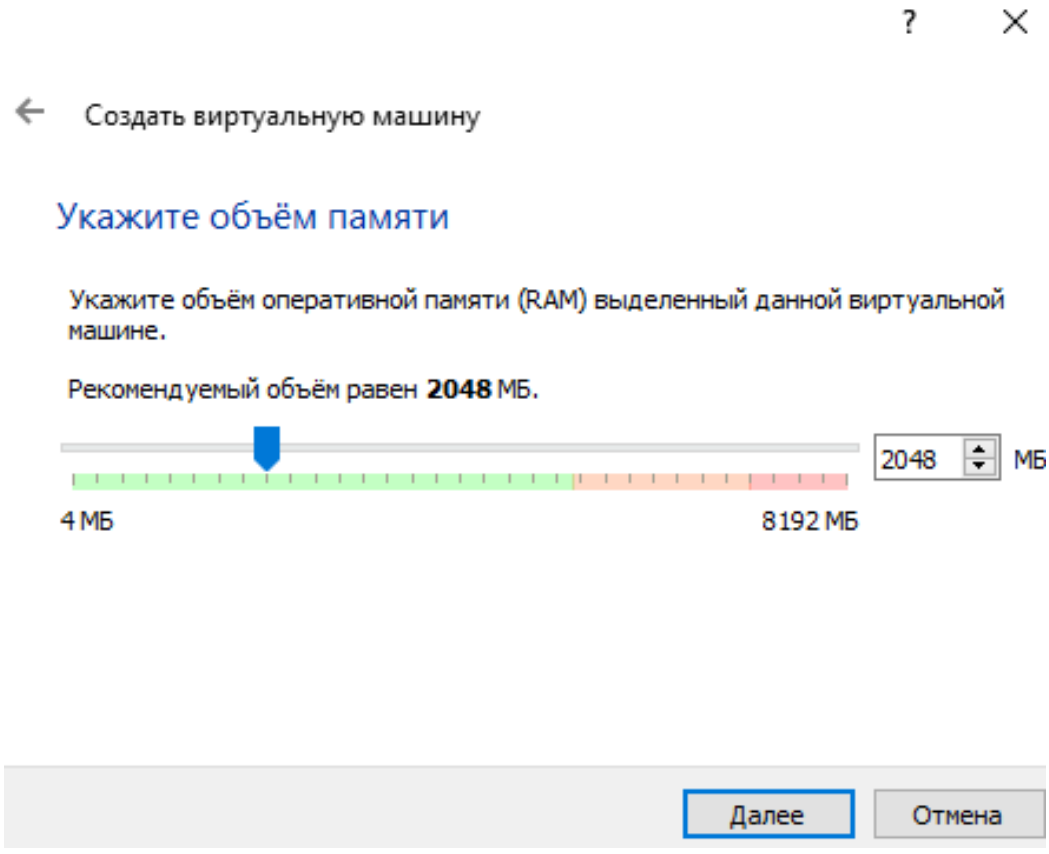


Рисунок 2-Настройка объема памяти

Затем необходимо создать новый виртуальный жесткий диск (см. рисунок 3).

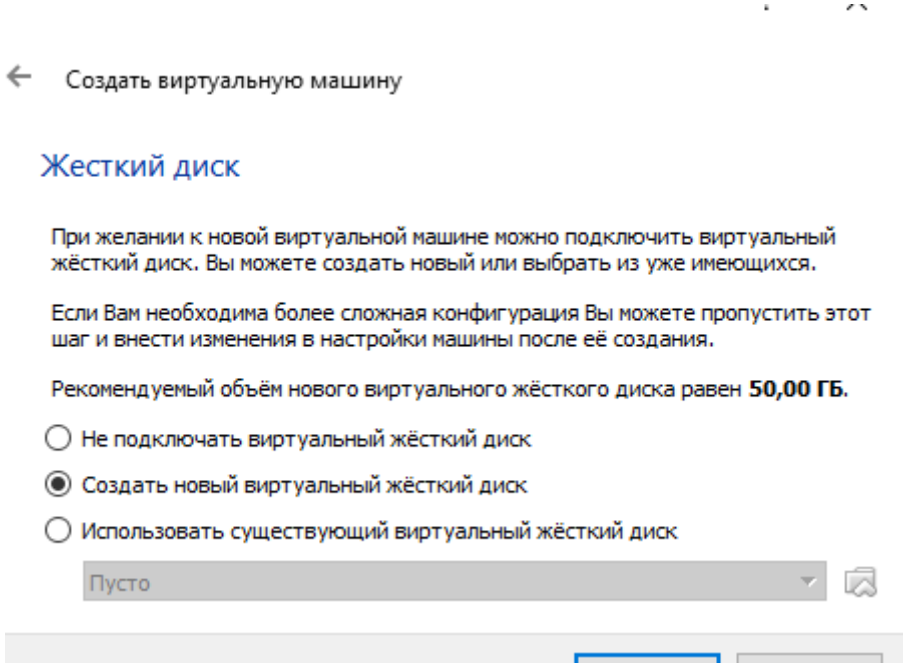


Рисунок 3-Настройка жесткого диска

Далее следует указать тип файла виртуального жесткого диска - VDI (см. рисунок 4).

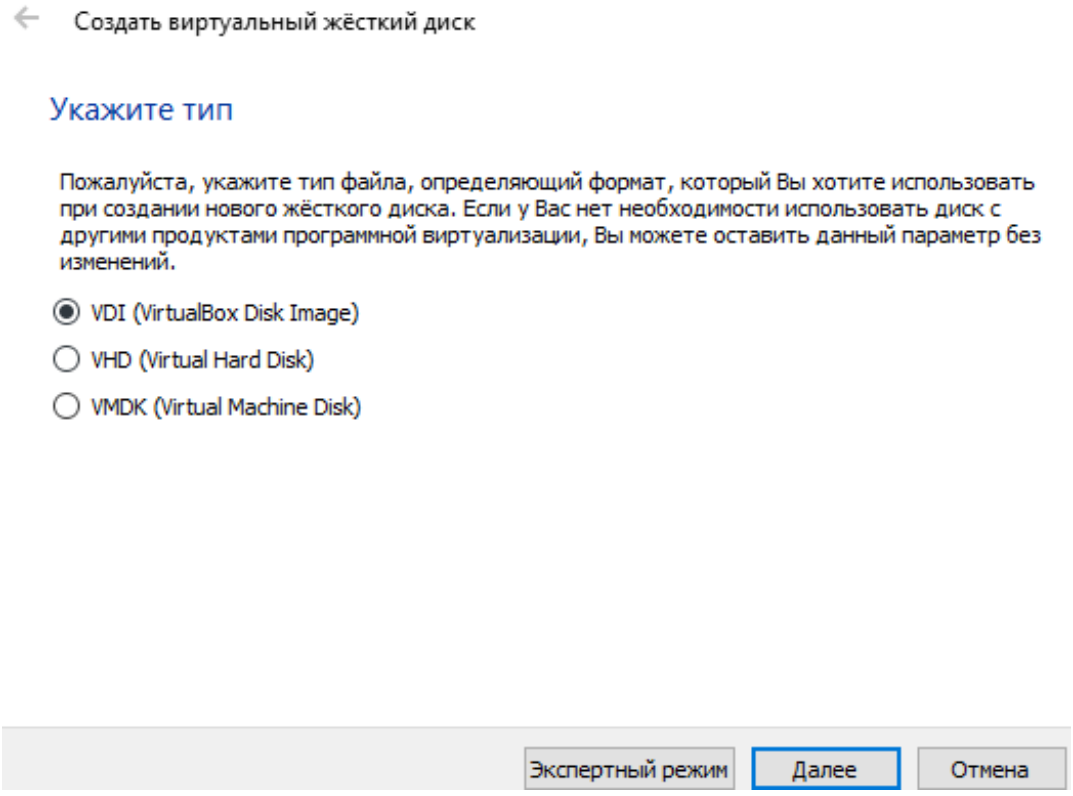


Рисунок 4 - Настройка типа виртуального жесткого диска

После этого необходимо указать формат хранения виртуального жесткого диска – динамический виртуальный жесткий диск (см. рисунок 5)

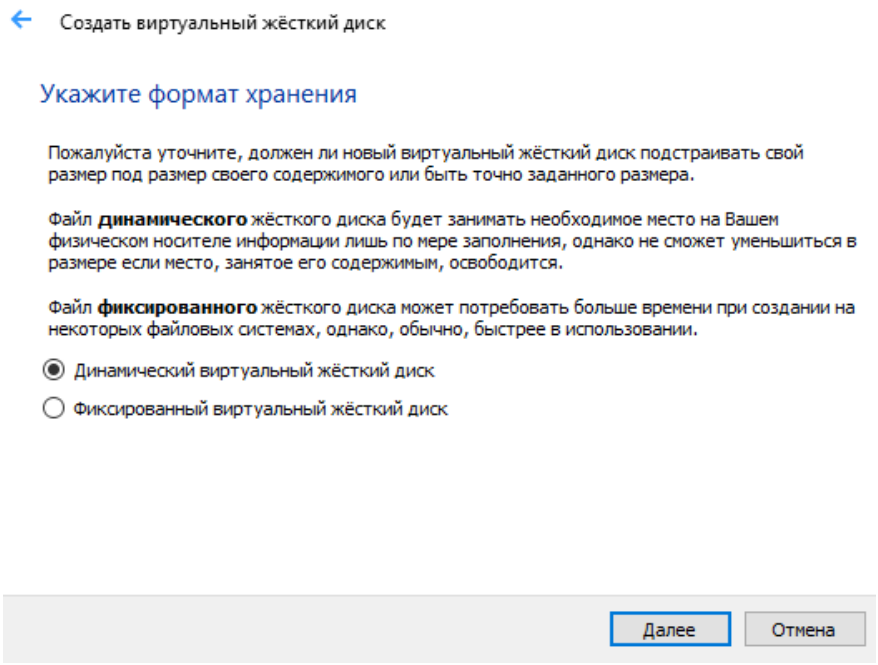


Рисунок 5 - Настройка формата хранения виртуального жесткого диска

Далее следует указать размер виртуального жесткого диска и указать каталог, в котором будет храниться соответствующий файл. Предельный размер файла динамического виртуального жесткого диска установлен 50 Гб, а имя файла соответствует имени ВМ (см. рисунок 6).

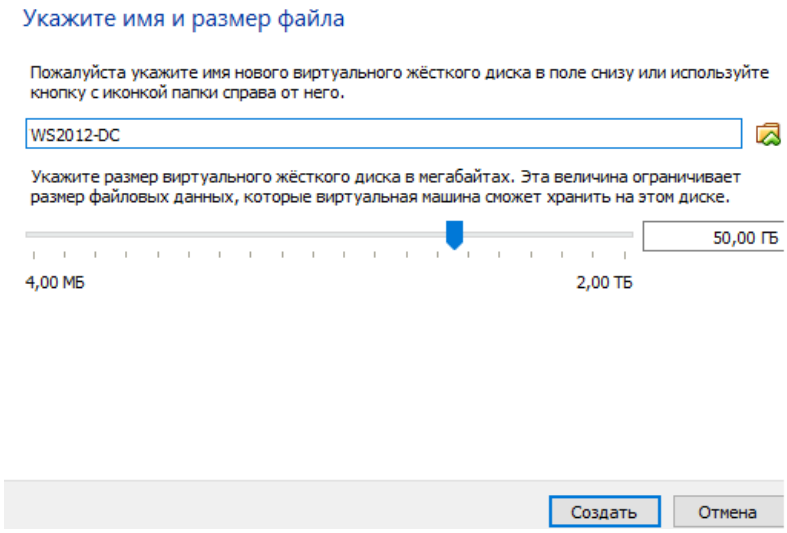


Рисунок 6 - Настройка имени и размера виртуального жесткого диска

После указания значений параметров надо нажать кнопку «Создать». На этом создание ВМ завершается. После создания ВМ необходимо настроить ее параметры с помощью Oracle VirtualBox Менеджер. Для настройки можно щелкнуть правой клавишей мыши по имени ВМ и в контекстном меню выбрать команду «Настроить». В диалоговом окне настроек перейти в раздел «Общие» и включить функции «Буфер обмена» и «Drag-n-Drop», установив значение параметра «Двунаправленный» (см. рисунок 7).

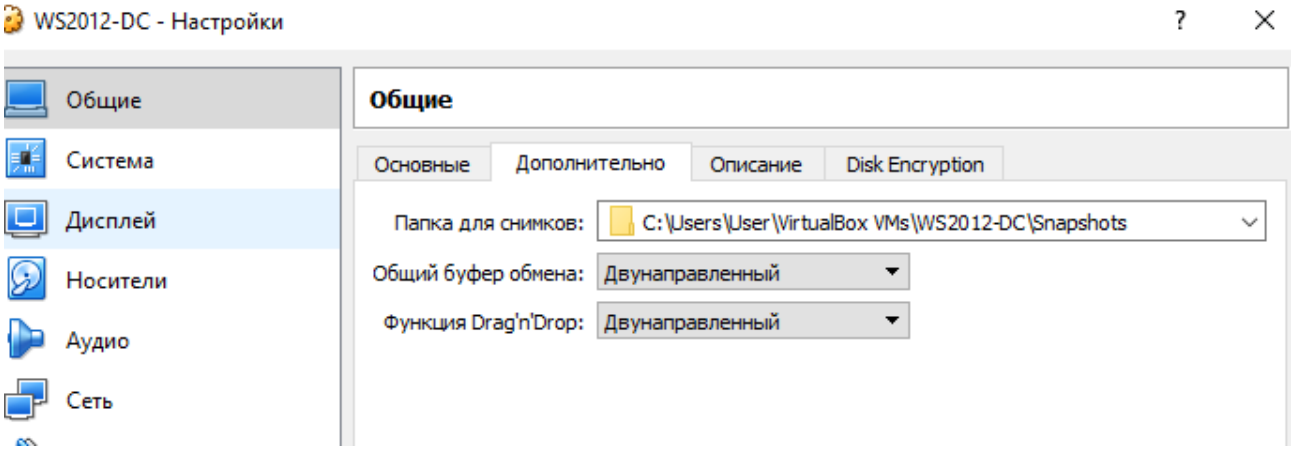


Рисунок 7 – Настройка функций «Буфер обмена» и «Drag-n-Drop»

Затем перейти в раздел «Система» и проверить настройки объема оперативной памяти. Установить порядок загрузки ВМ, так как указано на рисунке 8.

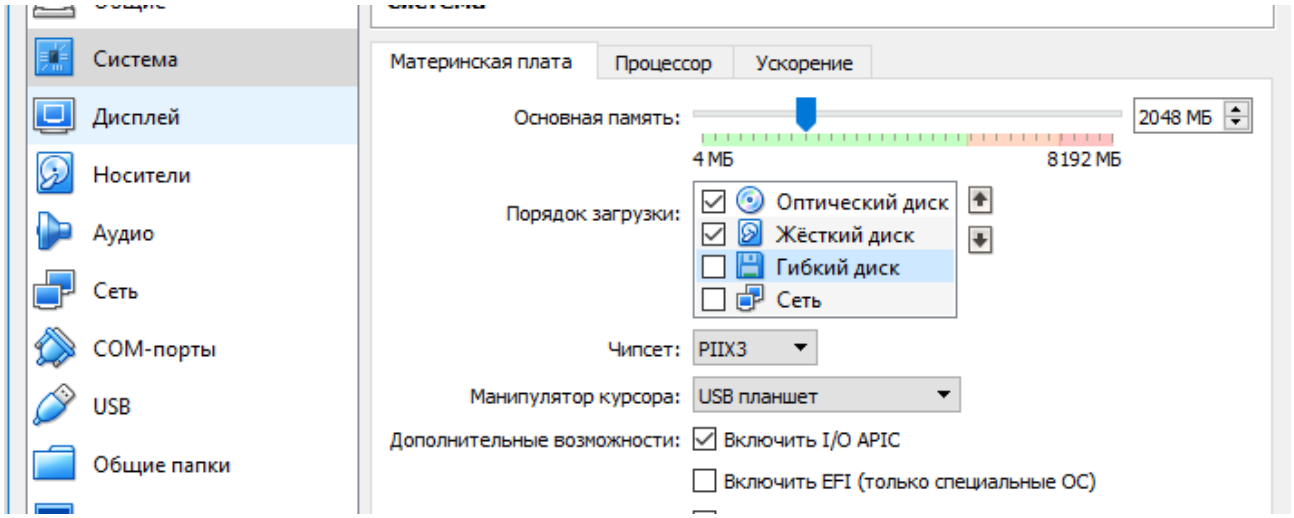


Рисунок 8 – Настройка системы виртуальной машины

Проверить носитель, подключенный к виртуальной машине. Для этого перейти в раздел «Носители» и проверить подключение выбранного жесткого диска (см. рисунок 9).

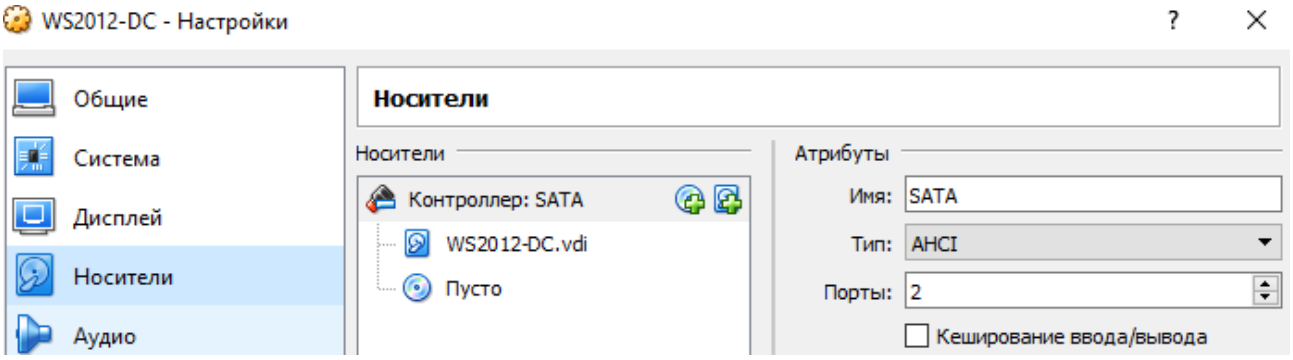


Рисунок 9 – Проверка настройки носителя, подключенного к виртуальной машине

Затем проверить настройки сети для включения ВМ в локальную сеть.

Выбрать следующие параметры и установить их значения: «Тип подключения: Внутренняя сеть», «Имя: intnet», тип адаптера оставить по умолчанию, «Неразборчивый режим: Разрешить все», MAC-адрес оставить по умолчанию, установить параметр «Подключить кабель» (см. рисунок 10).

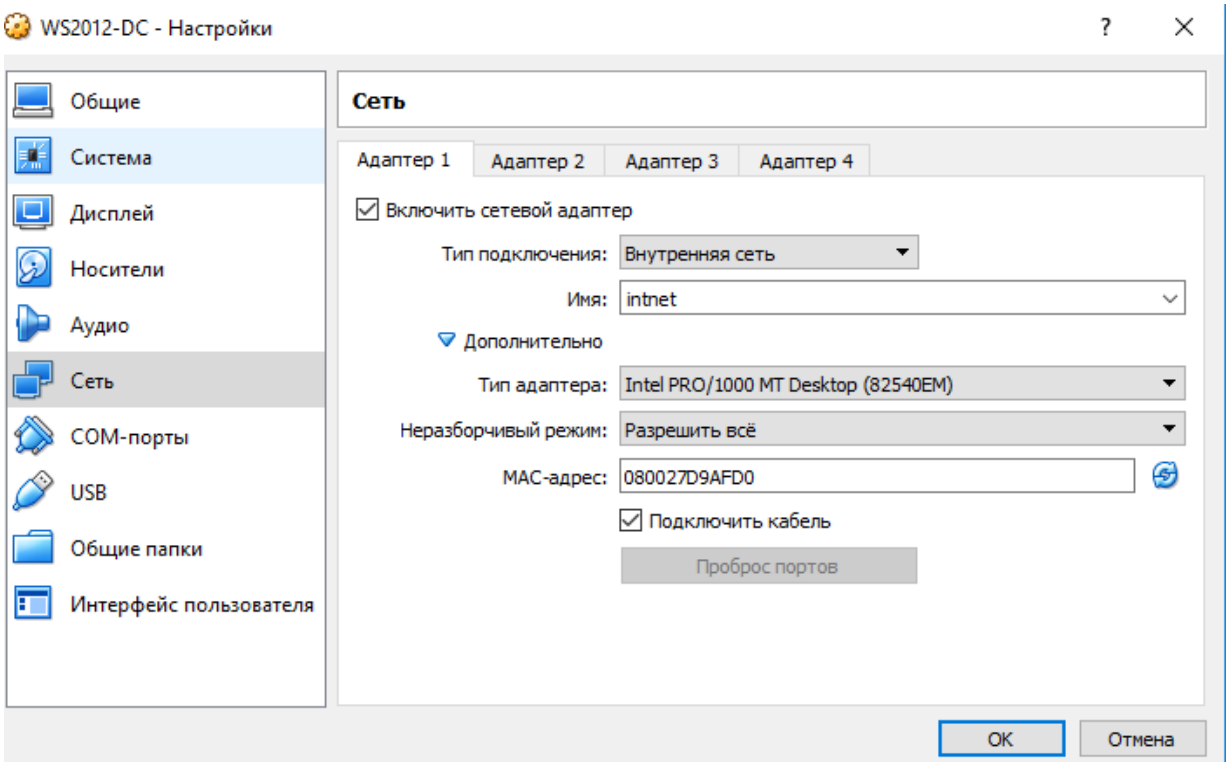


Рисунок 10 - Настройка сети виртуальной машины

После этого выбрать в настройках виртуальной машины раздел «Общие папки». Добавить общую папку, указав расположение данной папки, а также включить ее авто-подключение (см. рисунок 11).

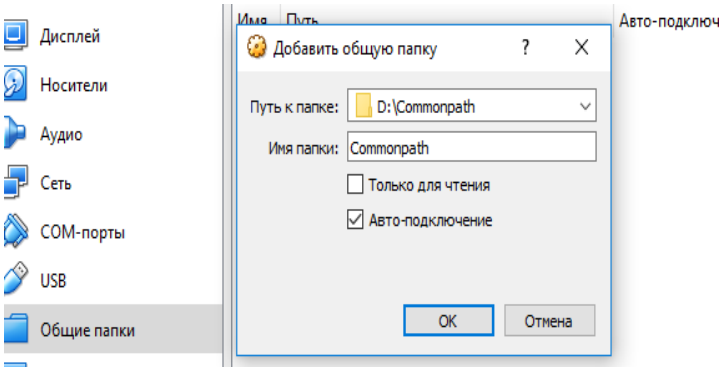


Рисунок 11 - Настройка общей папки виртуальной машины

После создания и настройки виртуальной машины с помощью Oracle VirtualBox Менеджер была выполнена установка гостевой ОС Windows Server 2012 R2. Она выполнялась в соответствии с документацией разработчика – компании Microsoft.

При установке гостевой ОС была создана учетная запись администратора гостевой ОС. Имя учетной записи – «Администратор», пароль – «P.ssw0rd».

При входе в операционную систему необходимо указать логин – «Администратор», пароль «P.ssw0rd».

Далее необходимо установить дополнения гостевой Oracle VirtualBox.

Для этого в строке меню виртуальной машины выбрать меню «Устройства», команду «Подключить образ диска Дополнений гостевой ОС» (см. рисунок 12).

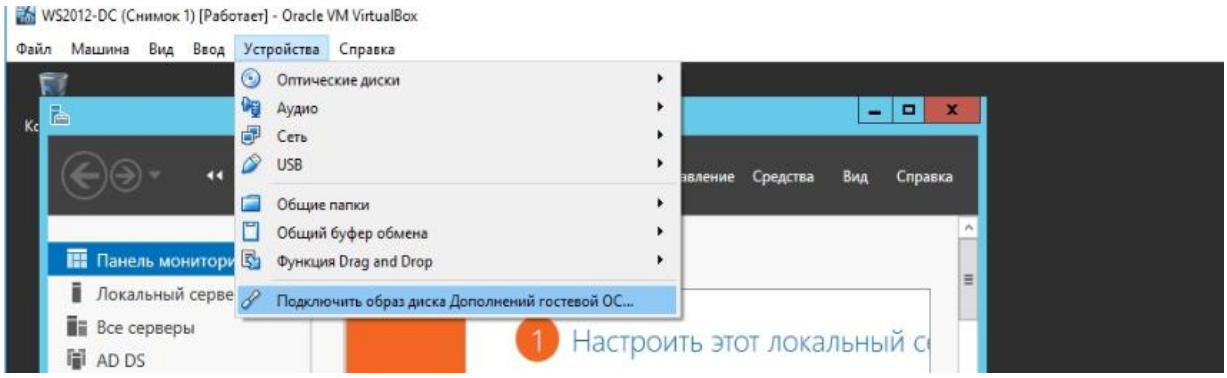


Рисунок 12 - Настройка дополнений гостевой ОС

Далее необходимо настроить гостевую ОС.

Настроить вид папок. Для этого необходимо открыть проводник «Этот компьютер», в панели быстрого доступа выбрать «Файл». В появившемся окне выбрать команду «Параметр». В верхней части появившегося окна выбрать раздел «Вид», выбрать пункт «Скрытые файлы и папки», установить отметку в поле «Не показывать скрытые файлы, папки и диски» (см. рисунок 13).

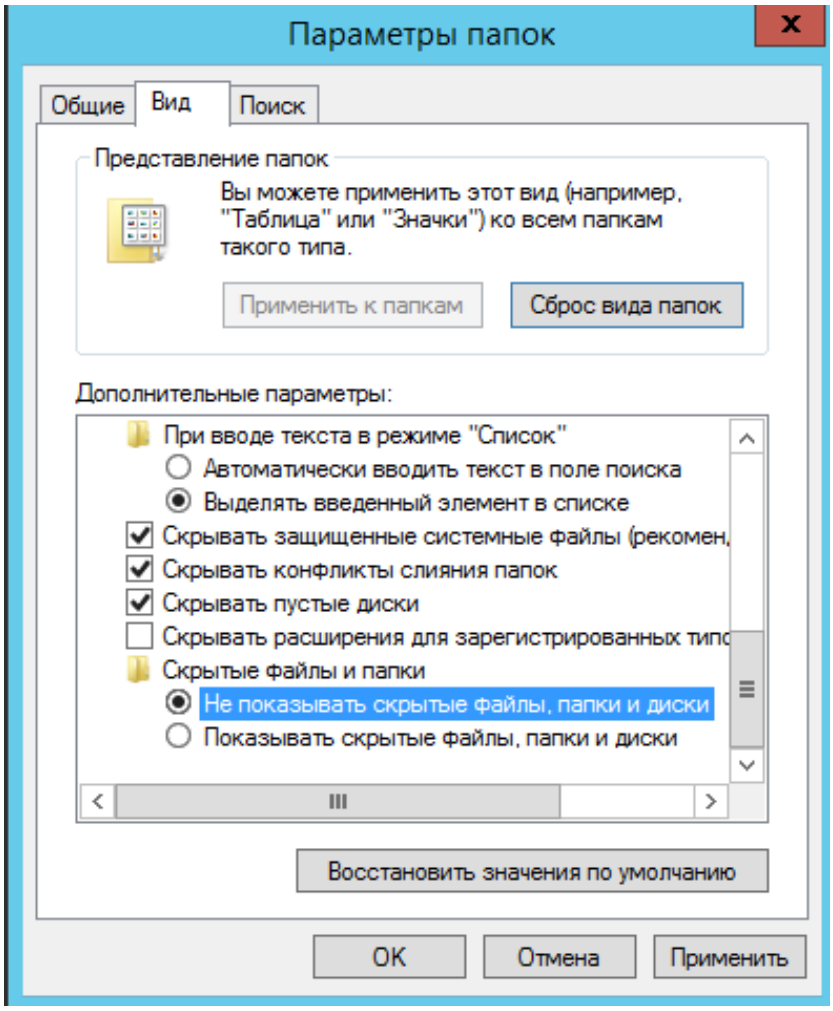


Рисунок 13 – Настройка вида папок

В нижней панели задач операционной системы Windows Server 2012 открыть консоль управления «Диспетчер серверов», открыть раздел «Локальный сервер», нажать на свойство «Имя компьютера». В появившемся окне нажать на команду «Изменить». После этого ввести имя сервера, совпадающее с именем виртуальной машины (см. рисунок 14). После этого ВМ необходимо перезагрузить.

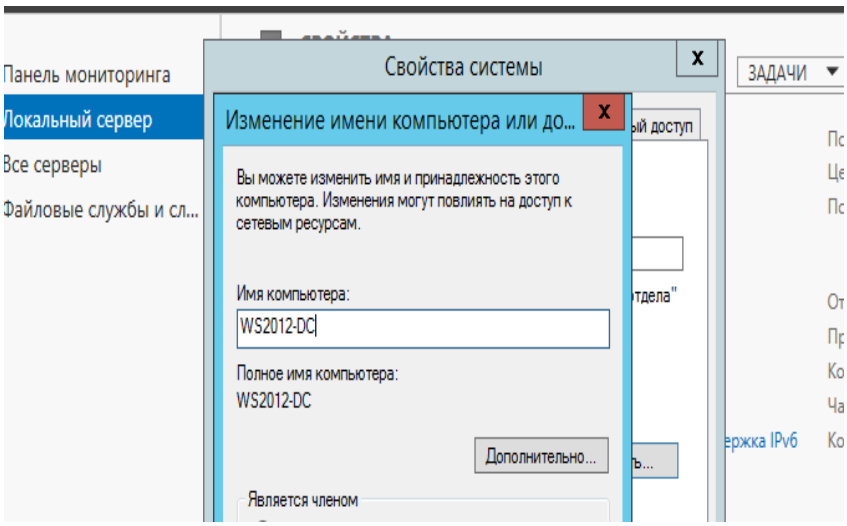


Рисунок 14 – Изменение имени сервера

В нижней панели задач операционной системы Windows Server 2012 открыть консоль управления «Диспетчер серверов», открыть раздел «Локальный сервер», нажать на гиперссылку «Ethernet». В появившемся окне щелкнуть правой кнопкой мыши по адаптеру рабочего стола, в контекстном меню выбрать команду «Свойства». В появившемся окне отключить параметр «Протокол интернет версии 6 (TCP/IPv6)». Выбрать в списке «Протокол интернет версии 4 (TCP/IPv4)», нажать на кнопку «Свойства». В появившемся окне включить параметр «Использовать следующий IP-адрес. Далее необходимо настроить сетевой адрес. Назначить IP-адрес «192.168.100.1», Маска подсети «255.255.255.0». В качестве шлюза по умолчанию указать адрес самого сервера (см. рисунок 15).

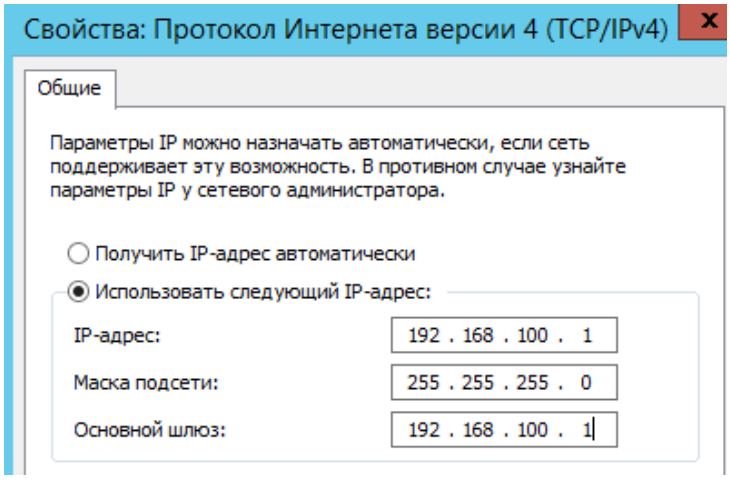


Рисунок 15 – Настройка сетевого адреса

Проверить текущие дату и время. Проверка даты и времени необходима для согласования даты и времени в домене. Дата и время на всех компьютерах домена должны совпадать. В системной области панели задач операционной системы щелкнуть один раз правой клавишей мыши по дате и времени и в контекстном меню выбрать команду «Настройка даты и времени», нажать на время и дату. В появившемся окне выбрать параметр «Изменение настроек даты и времени» (см. рисунок 16).

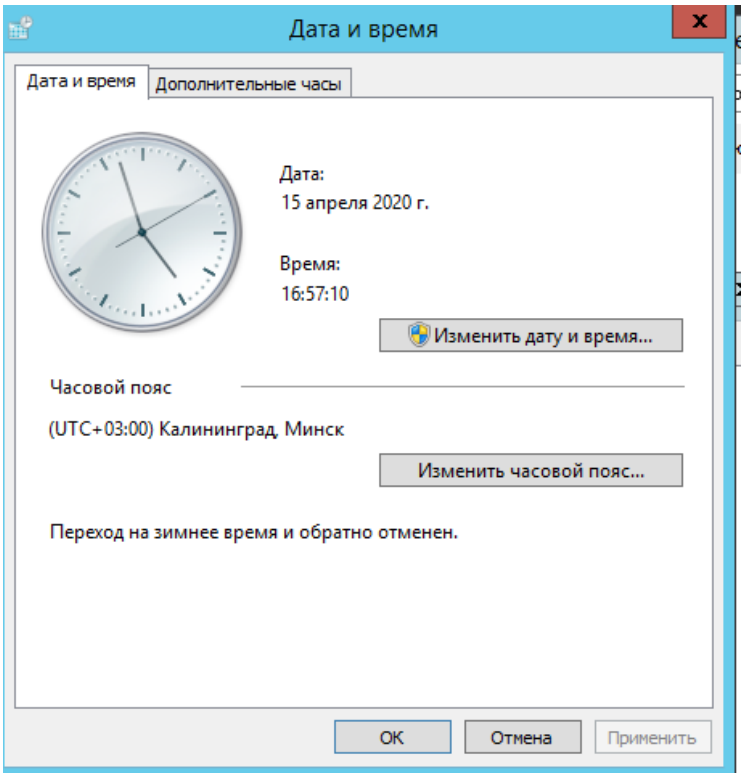


Рисунок 16 – Настройка времени и даты

Для учетной записи администратора установить параметр «Срок действия пароля не ограничен». Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», выбрать выпадающий список «Средства», далее консоль «Управление компьютером», в открывшемся окне открыть раздел «Локальные пользователи», раздел «Пользователи». Необходимо щелкнуть правой кнопкой мыши по учетной записи администратора, в контекстном меню выбрать команду «Свойства». Откроется

диалоговое окно «Свойства», на вкладке «Общие» надо установить параметр «Срок действия пароля не ограничен» (см. рисунок 17).

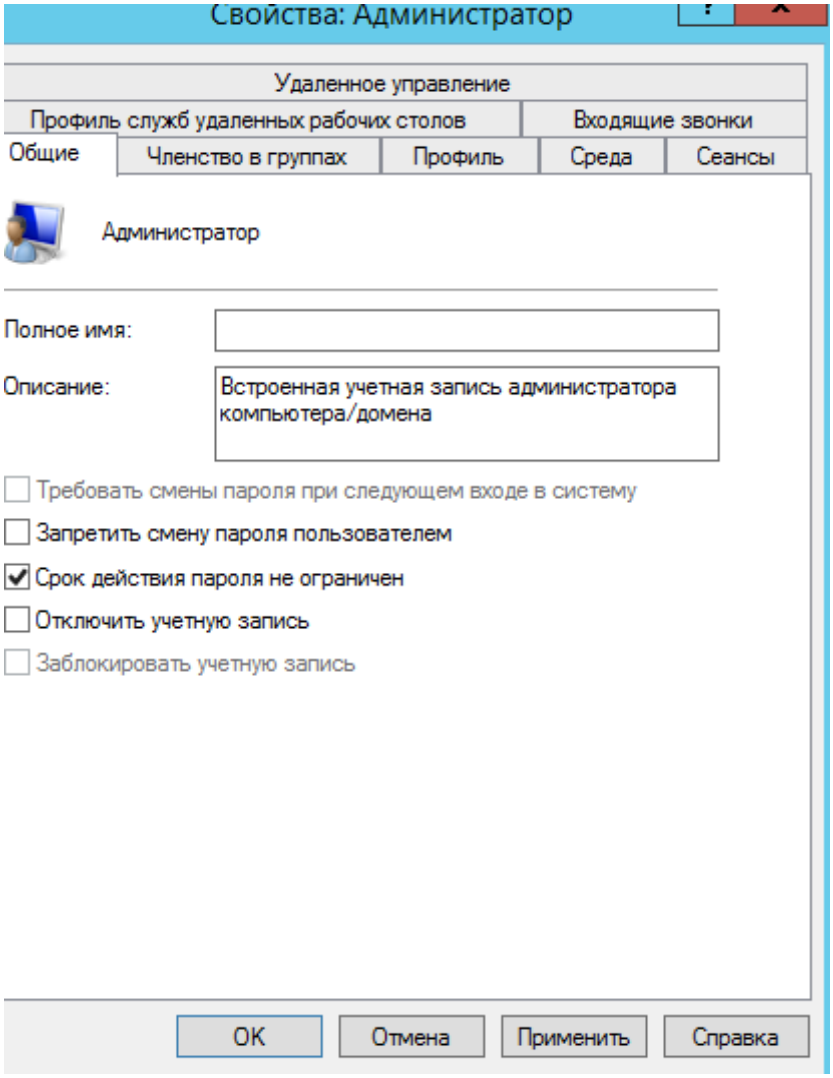


Рисунок 17 – Настройка параметра для учетной записи администратора

Установить роль DNS-сервера. Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», выбрать выпадающий список команд «Управление», далее выбрать команду «Добавить роли и компоненты». Будет запущен мастер добавления ролей и компонентов. В диалоговом окне надо нажать кнопку «Далее» до этапа «Роли сервера». Значения параметров на этапах «Тип установки» и «Выбор сервера» оставить по умолчанию. В этапе «Роли сервера» следует установить отметку в поле «DNS-сервер» (см. рисунок 18). После этого нажать команду «Установить» (см. рисунок 19). Если при установке выдается сообщение об

ошибке (отсутствует статический адрес), то виртуальную машину после настройки IP адреса надо перезагрузить. После перезагрузки заново запустить процесс установки ролей и компонентов.

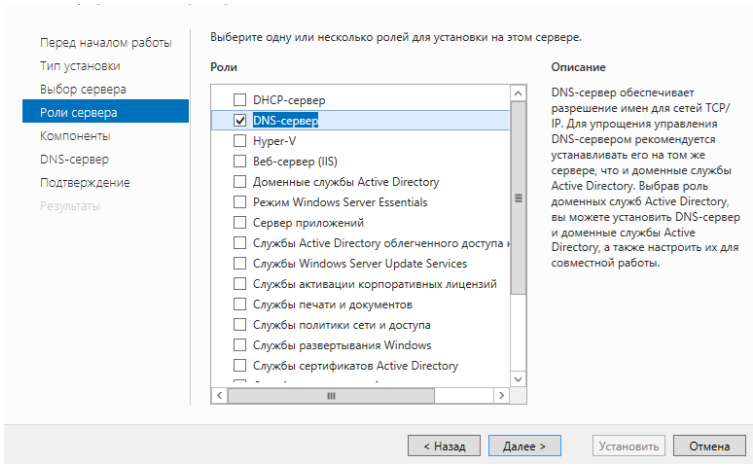


Рисунок 18 – Выбор ролей сервера

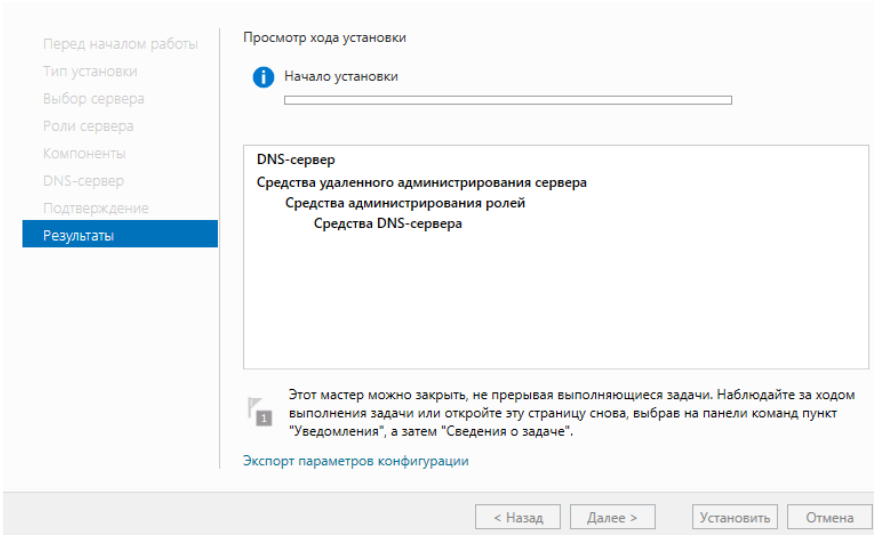


Рисунок 19 – Установка средств DNS-сервера

После установки выполнить его конфигурирование с помощью консоли DNS. Для этого необходимо в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», выбрать выпадающий список «Средства», далее команду «DNS». Откроется диспетчер DNS. В верхней панели инструментов выбрать меню «Действие», далее команду «Создать новую зону». Запустится мастер создания новой зоны, в диалоговом

окне которого нажать кнопку «Далее», установить в появившемся поле отметку «Основная зона», нажать «Далее» (см. рисунок 20).

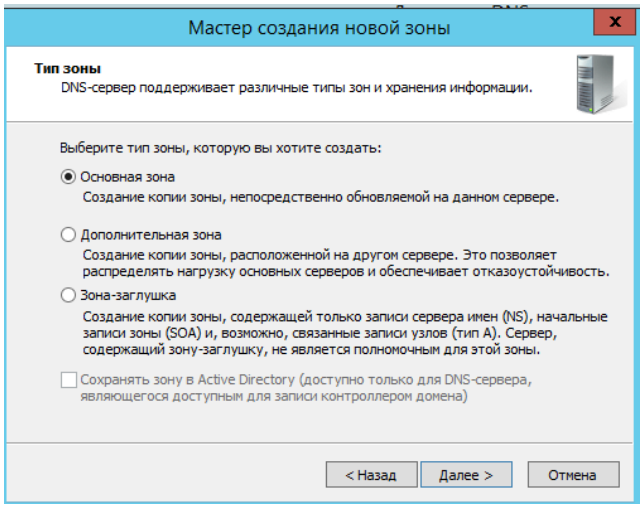


Рисунок 20 – Выбор типы зоны

В следующем окне указать имя зоны «WPS.PSU». Оно должно совпадать с именем домена для интеграции с AD, нажать кнопку «Далее» (см. рисунок 21).

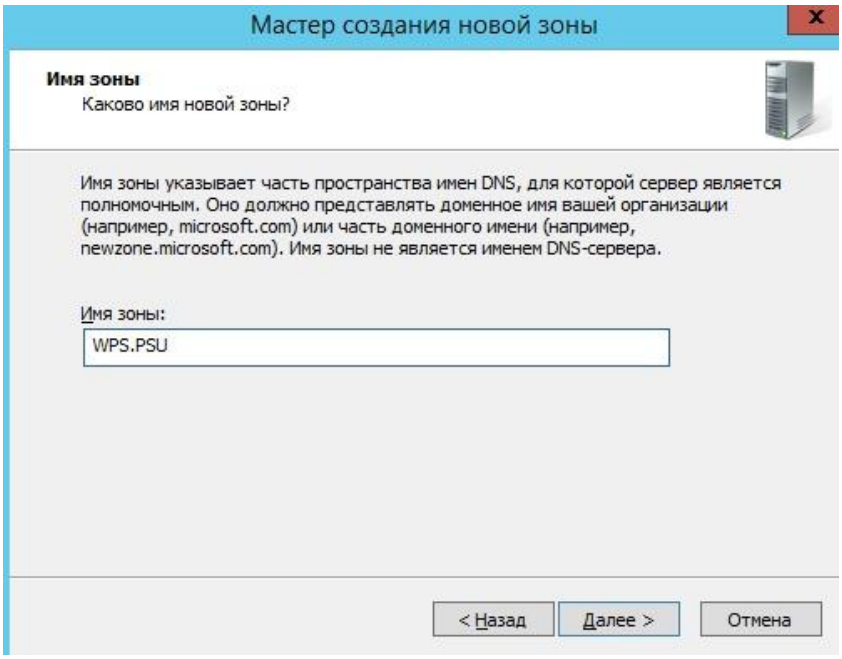


Рисунок 21 – Указание имя зоны

Установить отметку «Создать новый файл», указав название файла «WPS.PSU.dns», нажать кнопку «Далее». Установить отметку «Разрешить любые динамические обновления» (см. рисунок 22).

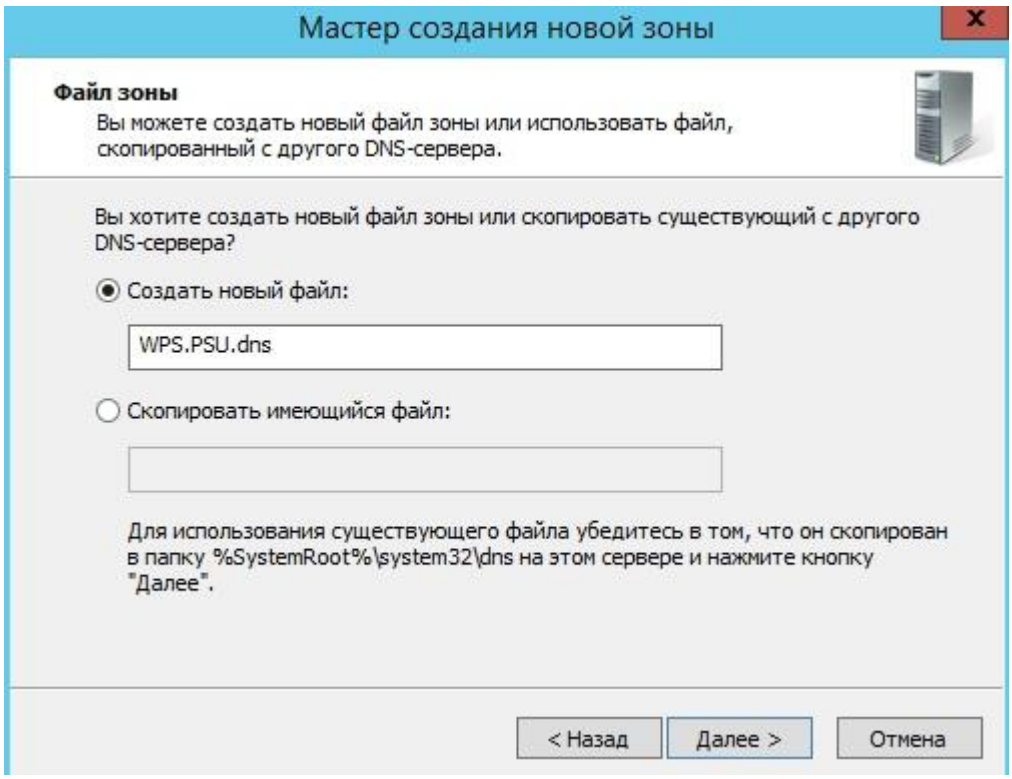


Рисунок 22 – Создание нового файла зоны

Нажать «Далее». На последнем этапе создания зоны DNS нажать кнопку «Готово» (см. рисунок 23).

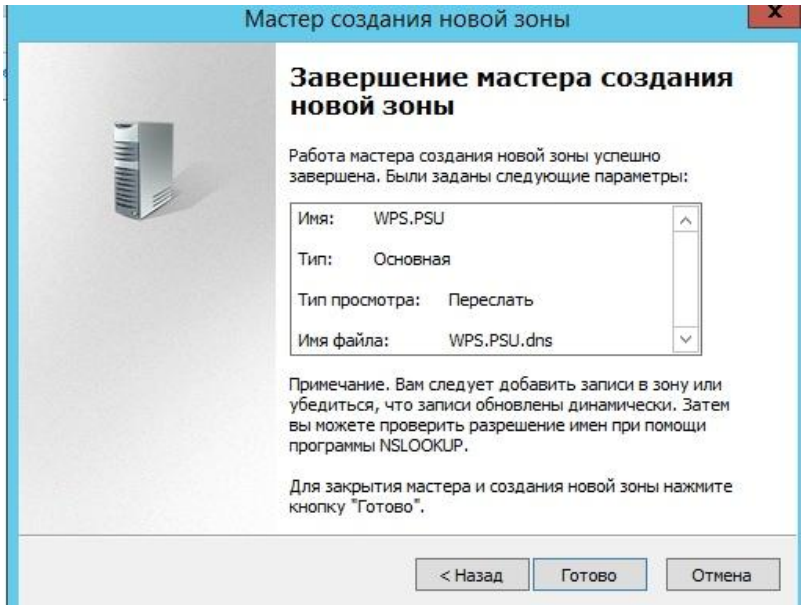


Рисунок 23 – Завершение мастера создания новой зоны

В нижней панели задач операционной системы Windows Server 2012 открыть консоль управления «Диспетчер серверов», выбрать выпадающий список команд «Локальный сервер», нажать на гиперссылку «Ethernet». В

появившемся окне щелкнуть правой кнопкой мыши по адаптеру рабочего стола, в появившемся окне нажать на кнопку «Свойство». Щелкнуть правой кнопкой мыши по параметру «Протокол интернет версии 4 (TCP/IPv4)», нажать на кнопку «Свойства». В появившемся окне поставить отметку в поле «Использовать следующие адреса DNS-серверов». Далее необходимо настроить предпочитаемый DNS-сервер и альтернативный DNS-сервер (см. рисунок 24).

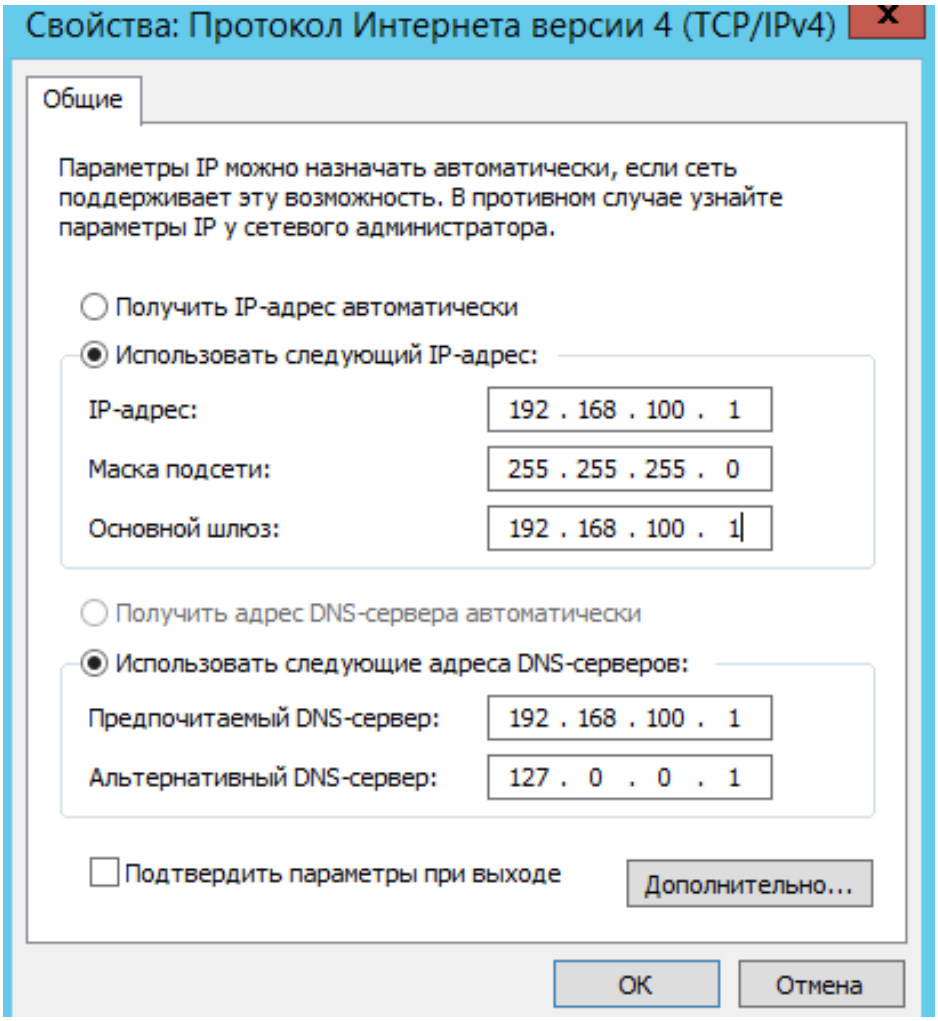


Рисунок 24 – Настройка DNS-серверов

В нижней панели задач операционной системы Windows Server 2012 открыть консоль управления «Диспетчер серверов». Нажав кнопку «Изменить» в разделе «Локальный параметр», перейти к настройке имени сервера. Затем нажать кнопку «Дополнительно» и в дополнительных настройках в строке «Основной DNS-суффикс этого компьютера» указать имя зоны прямого просмотра (см. рисунок 25).

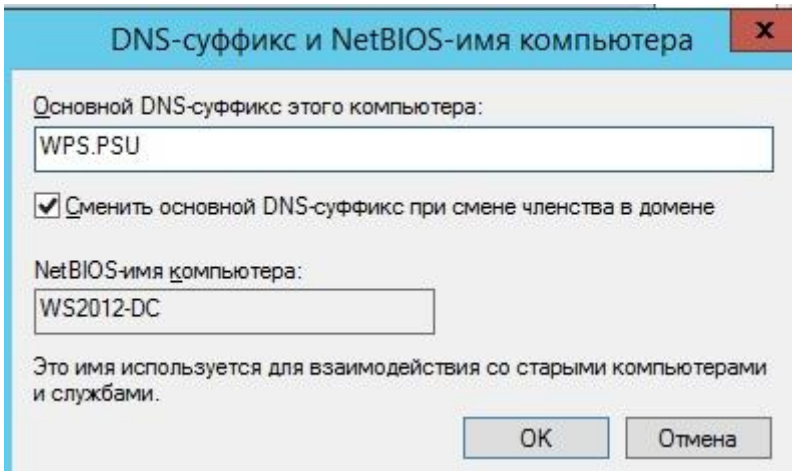


Рисунок 25 – Изменение DNS-суффикса

После указания суффикса потребуется перезагрузка ВМ.

Установить из списка компонентов NET Framework 3.5. Для этого необходимо запустить оболочку Powershell в нижней панели задач операционной системы. Далее в оболочке Powershell ввести командлет `Add-WindowsFeature Net-Framework-Core -Source d:\source\sxs`. (см. рисунок 26).

```
PS C:\Users\Администратор> Add-WindowsFeature Net-Framework-Core -Source d:\sources\sxs

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {.NET Framework 3.5 (включает .NET 2.0 и 3...
```

Рисунок 26 – Установка NET Framework 3.5

Для проверки в оболочке PowerShell нужно набрать командлет `Get-WindowsOptionalFeature -Online | Where FeatureName -Like "NetFx3"`. (см. рисунок 27).

```
PS C:\Users\Администратор> Get-WindowsOptionalFeature -Online | Where FeatureName -Like "NetFx3"

Feature Name : NetFx3
State        : Enabled
```

Рисунок 27 – Проверка установки компонента NET Framework 3.5

Установить роль Веб-сервер (IIS). Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», выбрать выпадающий список команд «Управление», далее выбрать команду «Добавить роли и компоненты». Будет запущен мастер добавления ролей и

компонентов, в диалоговом окне которого надо нажать кнопку «Далее» до этапа «Роли сервера». Этапы «Тип установки» и «Выбор сервера» оставить по умолчанию. На этапе «Роли сервера» установить отметку в поле «Веб-сервер (IIS)». Нажать кнопку «Далее». На этапе «Компоненты» оставить все без изменений. На этапе «Роль веб-сервера (IIS)» не отмечать такие роли, которые предполагают использование сертификатов, трассировку, перенаправление и публикацию, разработку приложений, сжатие динамического содержимого и расширяемость FTP. Остальные компоненты необходимо отметить для установки (см. рисунок 28).

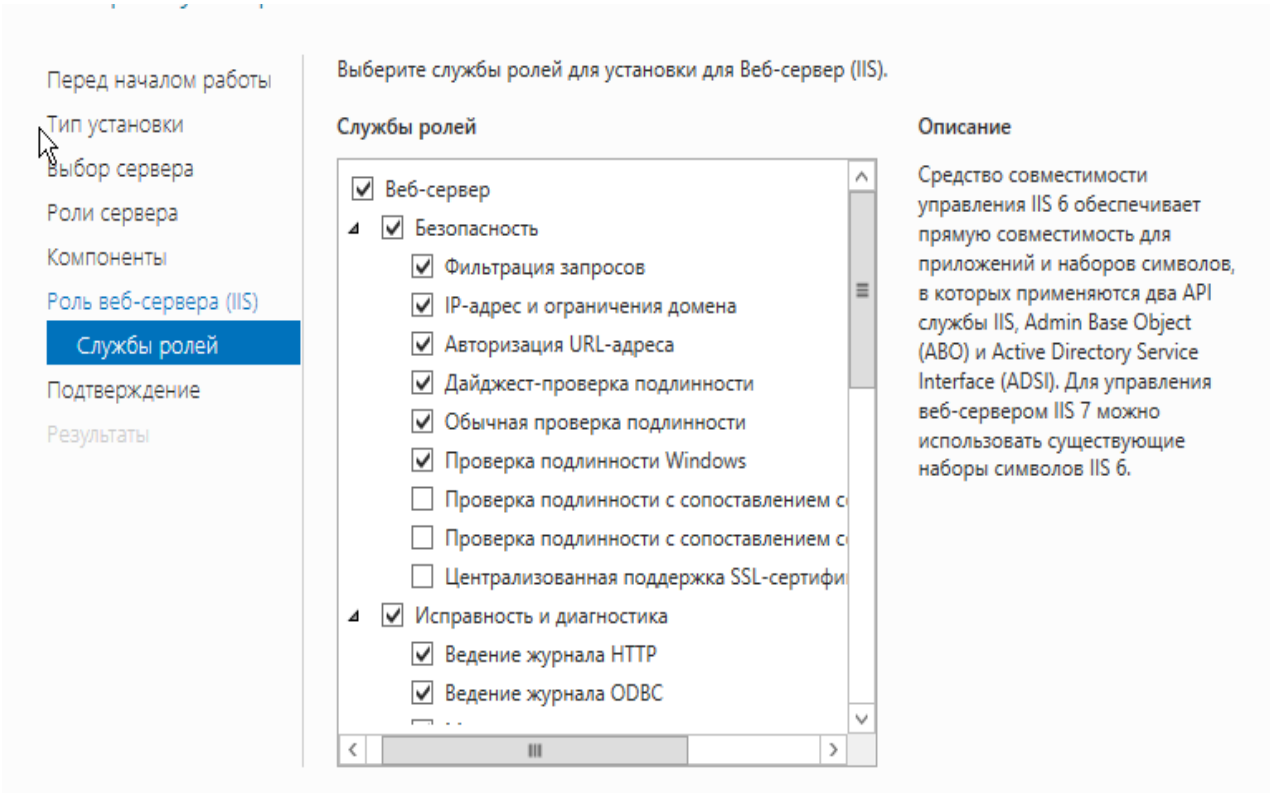


Рисунок 28 – Выбор службы ролей для установки для Веб-сервера

Затем установить роль сервера приложений. Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», выбрать выпадающий список команд «Управление», далее выбрать команду «Добавить роли и компоненты». Будет запущен мастер добавления ролей и компонентов, в диалоговом окне которого надо нажать кнопку «Далее» до этапа «Роли сервера». Этапы «Тип установки» и «Выбор сервера» оставить

по умолчанию. На этапе «Роли сервера» поставить отметку в поле «Сервер приложений» (см. рисунок 29).

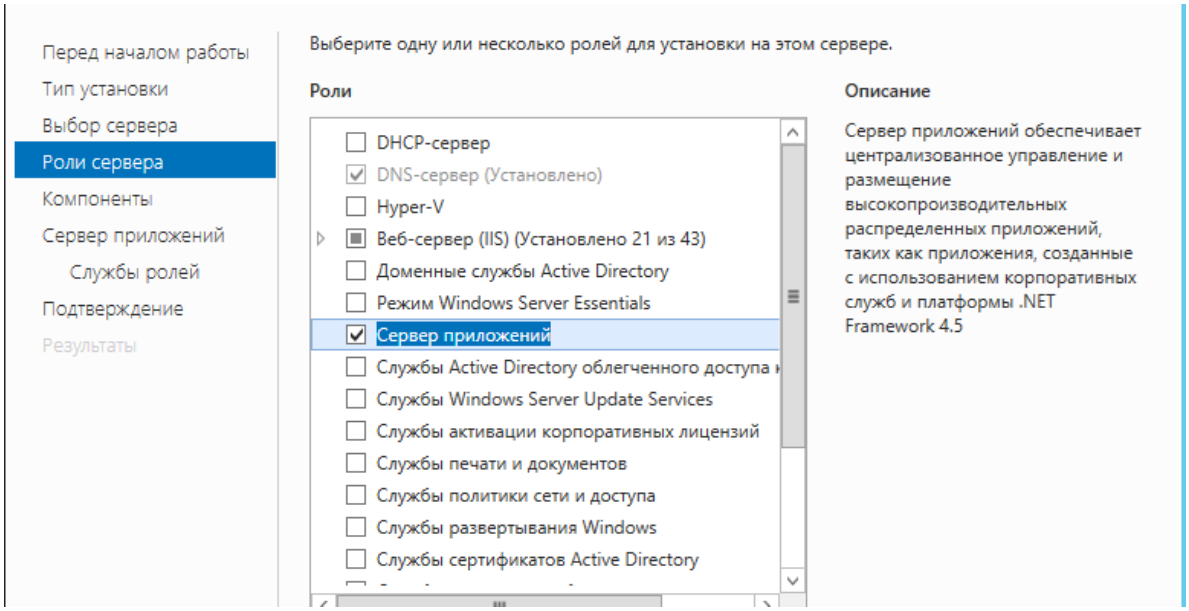


Рисунок 29 – Установка сервера приложений

При выборе компонентов необходимо выбрать все компоненты, кроме компонента распределенных транзакций (WS-Atomic) (см. рисунок 30).

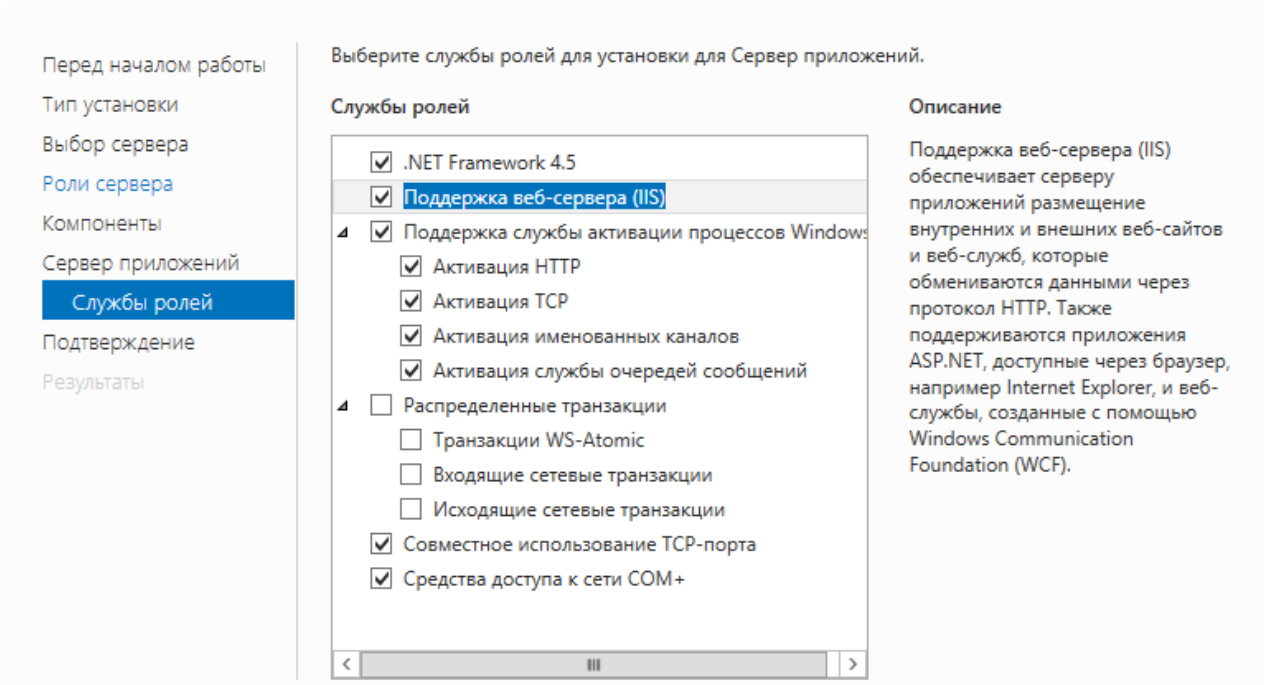


Рисунок 30 – Выбор службы для установки сервера приложений

Из списка компонентов в диспетчере серверов установить Средство просмотра XPS. Для этого в нижней панели задач операционной системы

открыть консоль управления «Диспетчер серверов», выбрать выпадающий список команд «Управление», далее выбрать команду «Добавить роли и компоненты». Будет запущен мастер добавления ролей и компонентов, в диалоговом окне которого надо нажать кнопку «Далее» до этапа «Компоненты». Настройки на этапах «Тип установки», «Выбор сервера» и «Роли сервера» оставить по умолчанию. На этапе «Компоненты» поставить отметку в поле «Средство просмотра XPS», далее нажать кнопку «Добавить компоненты», далее кнопку «Установить» (см. рисунок 31).

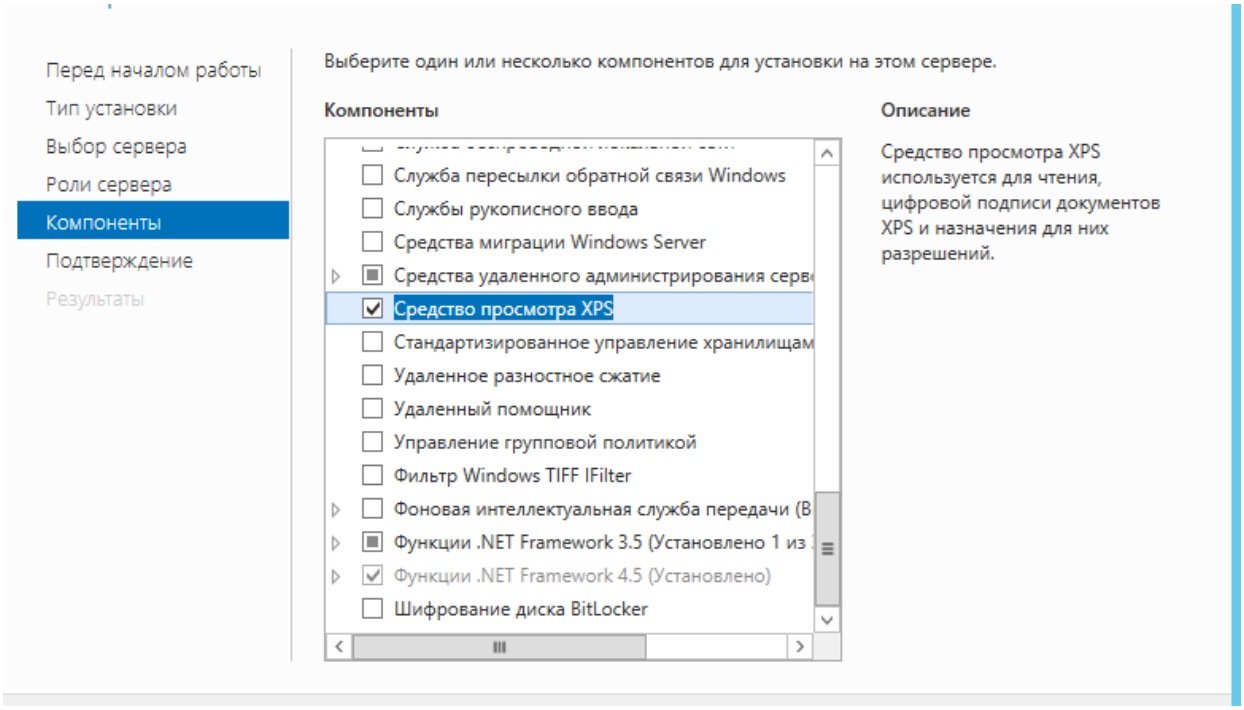


Рисунок 31 – Установка средства просмотра XPS

Из списка компонентов в диспетчере серверов установить SMTP-сервер. Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», выбрать выпадающий список команд «Управление», далее выбрать команду «Добавить роли и компоненты». Будет запущен мастер добавления ролей и компонентов, в диалоговом окне которого надо нажать кнопку «Далее» до этапа «Компоненты». Настройки на этапах «Тип установки», «Выбор сервера»

и «Роли сервера» оставить по умолчанию. На этапе «Компоненты» поставить отметку в поле «SMTP-сервер», нажать кнопку «Добавить компоненты», далее кнопку «Установить» (см. рисунок 32).

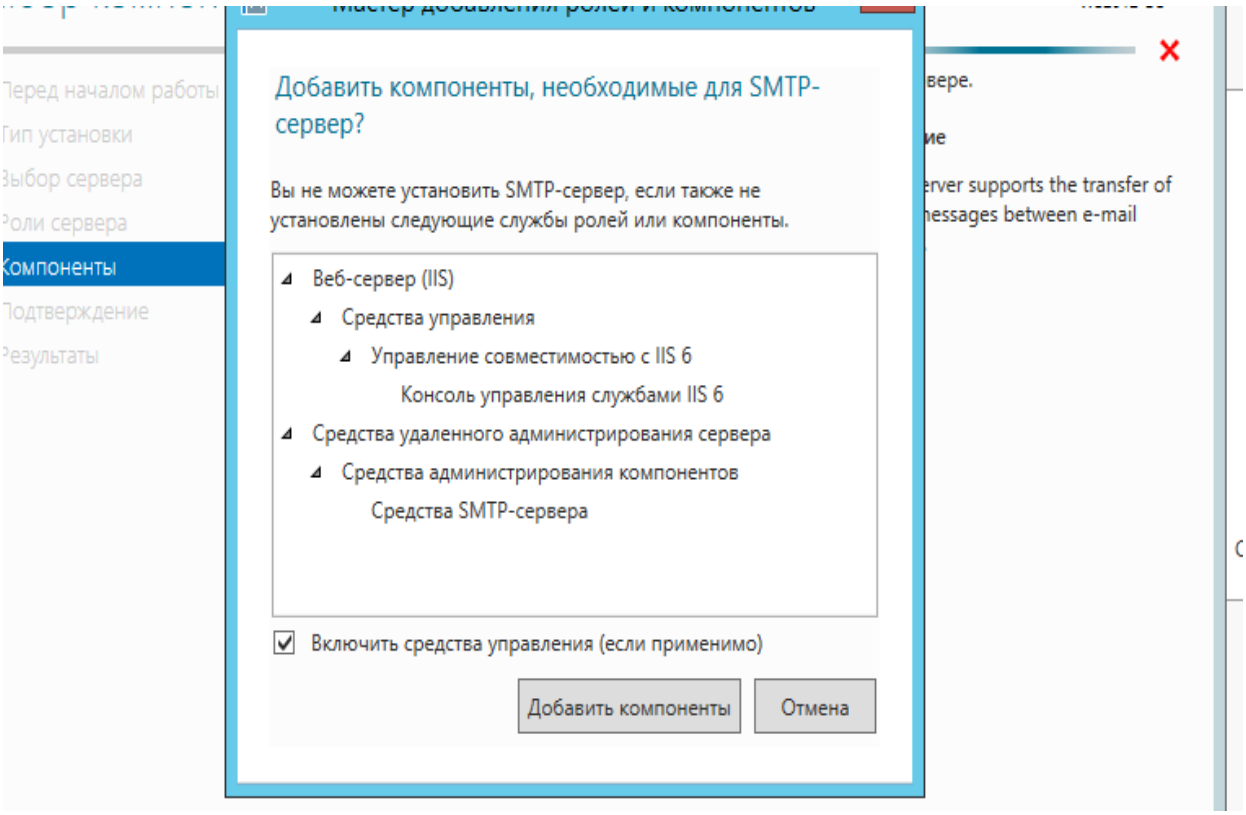


Рисунок 32 – Установка SMTP-сервера

Установить из списка компонентов компонент Фоновая интеллектуальная служба передачи (BITS). Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», выбрать выпадающий список команд «Управление», далее выбрать команду «Добавить роли и компоненты». Будет запущен мастер добавления ролей и компонентов, в диалоговом окне которого надо нажать кнопку «Далее» до этапа «Компоненты». Настройки на этапах «Тип установки», «Выбор сервера» и «Роли сервера» оставить по умолчанию. На этапе «Компоненты» поставить отметку в поле «Фоновая интеллектуальная

служба передачи (BITS)», нажать кнопку «Добавить компоненты», далее кнопку «Установить» (см. рисунок 33).

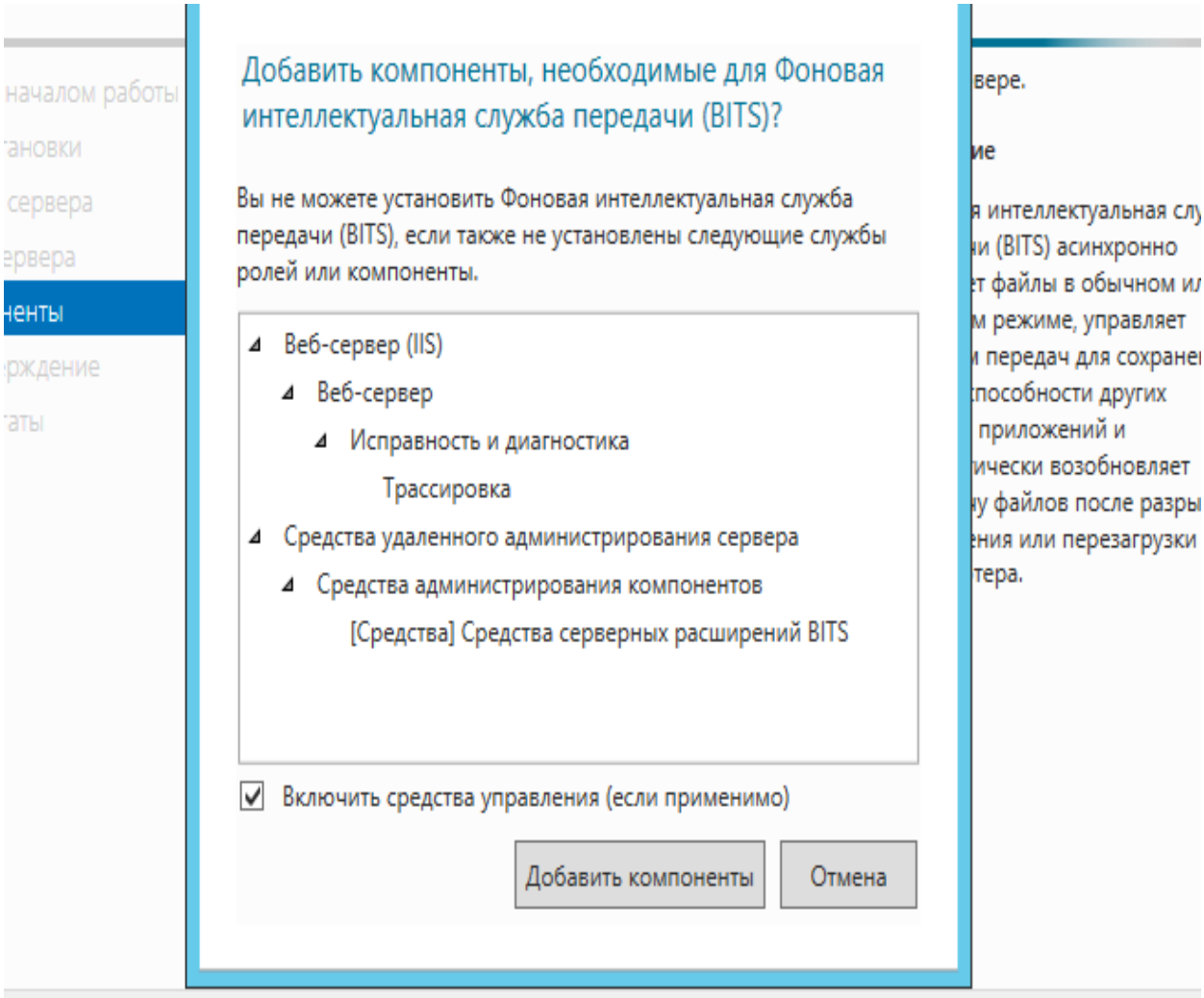


Рисунок 33 – Установка фоновой интеллектуальной службы передачи

При необходимости используя мастер добавления ролей и компонентов, можно установить сервер Telnet и клиент Telnet. Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», выбрать выпадающий список команд «Управление», далее выбрать команду «Добавить роли и компоненты». Будет запущен мастер добавления ролей и компонентов, в диалоговом окне которого надо нажать кнопку «Далее» до этапа «Компоненты». Настройки на этапах «Тип установки», «Выбор сервера» и «Роли сервера» оставить по

умолчанию. На этапе «Компоненты» поставить отметку в поле «Клиент Telnet», нажать кнопку «Добавить компоненты», далее кнопку «Установить» (см. рисунок 34).

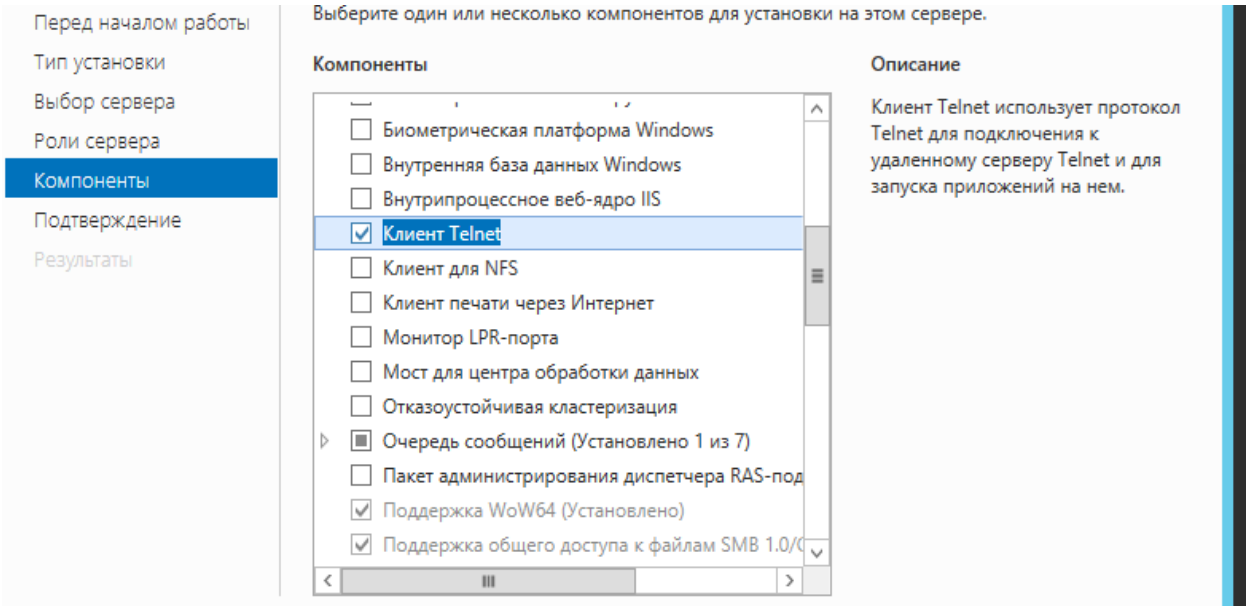


Рисунок 34 – Установка фоновой интеллектуальной службы передачи

Настроить локальные службы. Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», выбрать выпадающий список команд «Средства», параметр «Службы». Настроить тип запуска, указав тип «Автоматически» и запустить службы: Браузер компьютеров, Журналы и оповещения производительности, Обнаружение SSDP, Служба SSTP, Удаленный вызов процедур (RPC), Удаленный реестр, Узел универсальных PNP-устройств, Фоновая интеллектуальная служба передачи (BITS).

В Центре управления сетями и общим доступом надо настроить дополнительные параметры общего доступа. В нижней панели задач операционной системы Windows Server 2012 открыть консоль управления «Диспетчер серверов», выбрать раздел «Локальный сервер», нажать на свойство «Брандмауэр Windows». В появившемся окне выбрать раздел «Центр управления сетями и общим доступом». Выбрать команду «Изменить дополнительные параметры общего доступа». Для всех сетевых профилей

включить сетевое обнаружение и общий доступ к файлам и принтерам. В профиле «Все сети» отключить общий доступ с парольной защитой. Сохранить изменения. Затем еще раз проверить дополнительные параметры общего доступа. Они должны быть сохранены (см. рисунок 35).

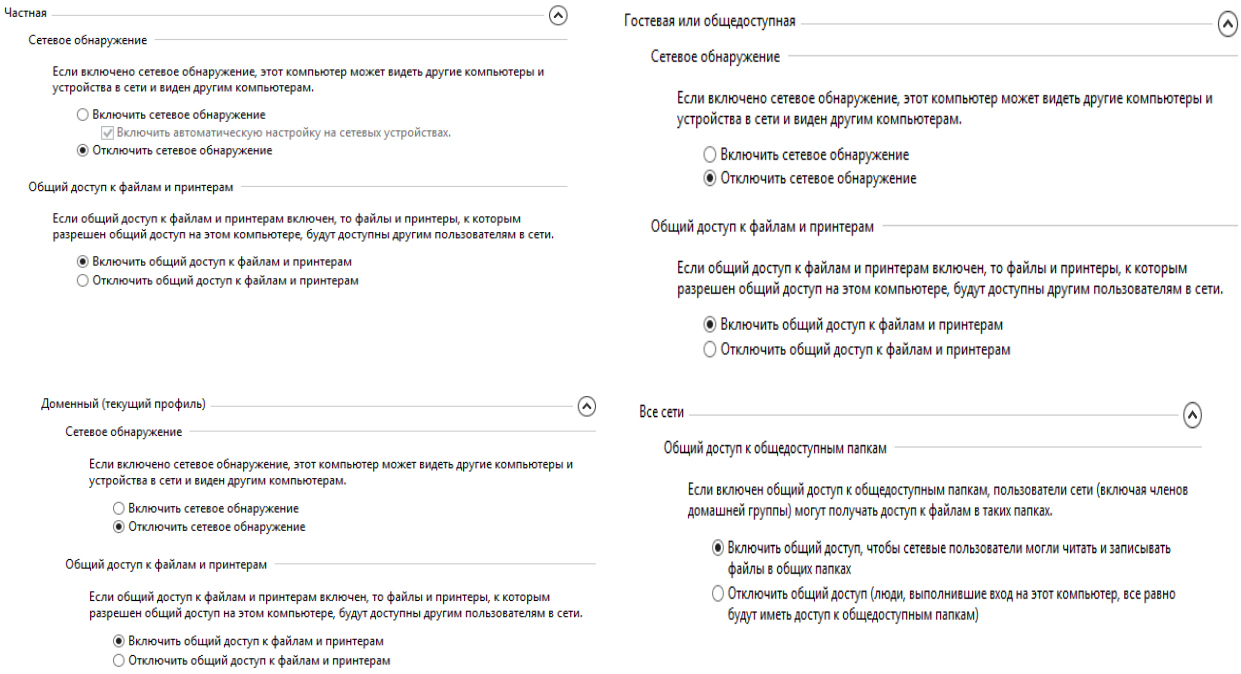


Рисунок 35 – Настройка дополнительных параметров общего доступа

В результате всех выполненных действий была создана виртуальная машина с установленной гостевой ОС Windows 2012 R2, настроен статический IP-адрес, добавлены необходимые для дальнейшей работы роли и компоненты.

3.3 Создание ВМ с установленным гипервизором Hyper-V 2012 R2

Необходимо создать виртуальную машину (ВМ) с установленной гостевой ОС, которой является гипервизор Microsoft Hyper-V Server 2012.

Для создания ВМ следует запустить программу Oracle VirtualBox Менеджер. Для создания ВМ нажать кнопку «Создать» на панели инструментов. На экране появиться диалоговое окно мастера создания ВМ. На

первом этапе создания ВМ следует указать имя ВМ, тип и версию гостевой ОС. В качестве значений этих параметров указаны следующие:

– имя – HS2012 - VS1;

– тип – Microsoft Windows;

– версия – Windows 2012 (64 bit).

Установленные параметры приведены на рисунке 36.

Рисунок 36 - Настройка параметров виртуальной машины

Далее необходимо указать объем оперативной памяти виртуальной машины (см. рисунок 37)

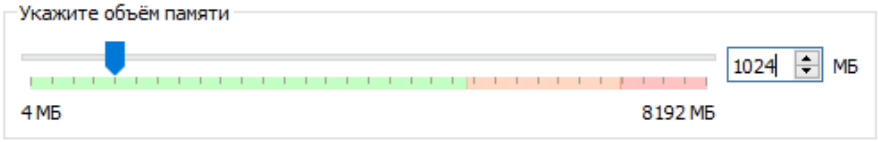


Рисунок 37 - Настройка объема оперативной памяти

Затем необходимо создать новый виртуальный жесткий диск (см. рисунок 38).

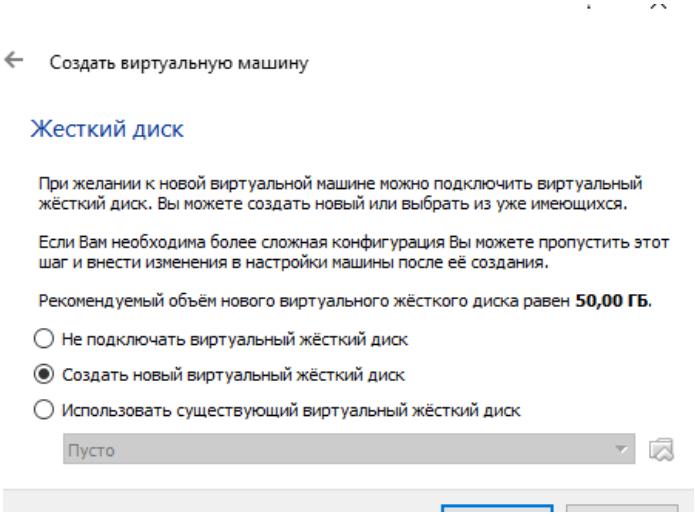


Рисунок 38 - Настройка жесткого диска

Затем необходимо создать новый виртуальный жесткий диск, указать размер виртуального жесткого диска – 30 Гб, указать тип – VDI, выбрать формат хранения - динамический виртуальный жесткий диск (см. рисунок 39).

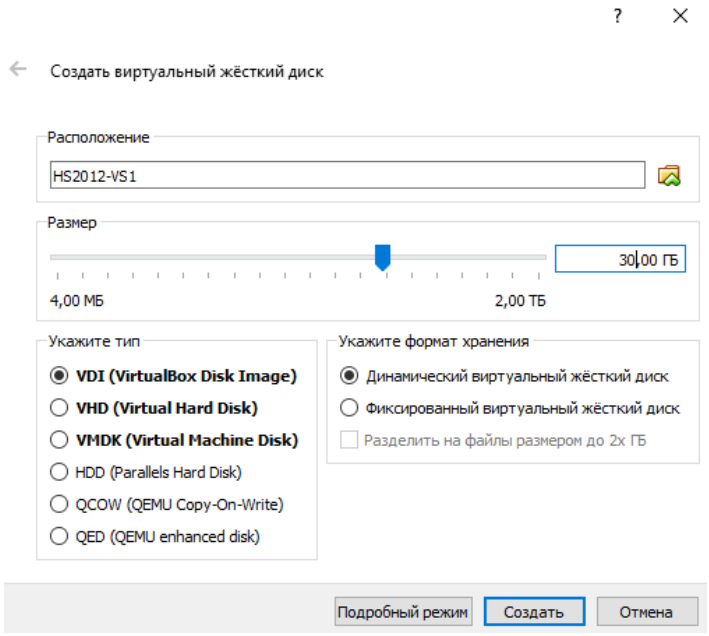


Рисунок 39-Настройка жесткого диска

После указания значений параметров надо нажать кнопку «Создать». На этом создание ВМ завершается. После создания ВМ необходимо настроить ее параметры с помощью Oracle VirtualBox Менеджер. Для настройки можно щелкнуть правой клавишей мыши по имени ВМ и в контекстном меню выбрать команду «Настроить». В диалоговом окне настроек перейти в раздел «Общие» и включить функции «Буфер обмена» и «Drag-n-Drop», установив значение «Двунаправленный» (см. рисунок 40).

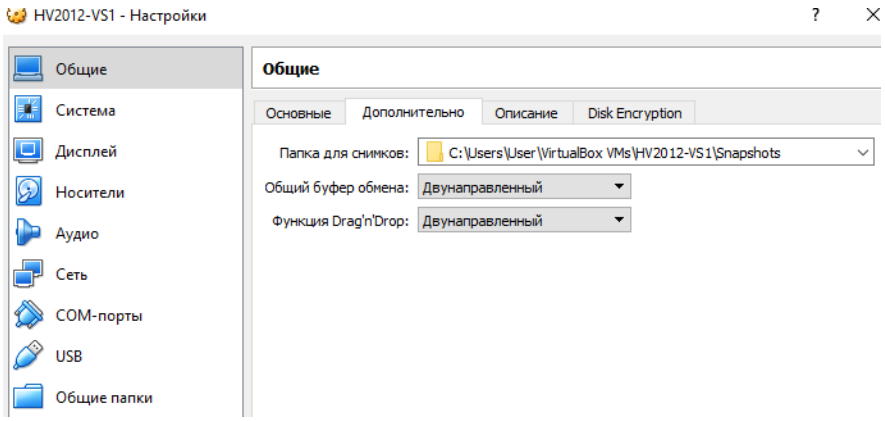


Рисунок 40 – Настройка функций «Буфер обмена» и «Drag-n-Drop»

Затем перейти в раздел «Система» и проверить настройки объема оперативной памяти. Установить порядок загрузки ВМ, так как указано на рисунке 41.

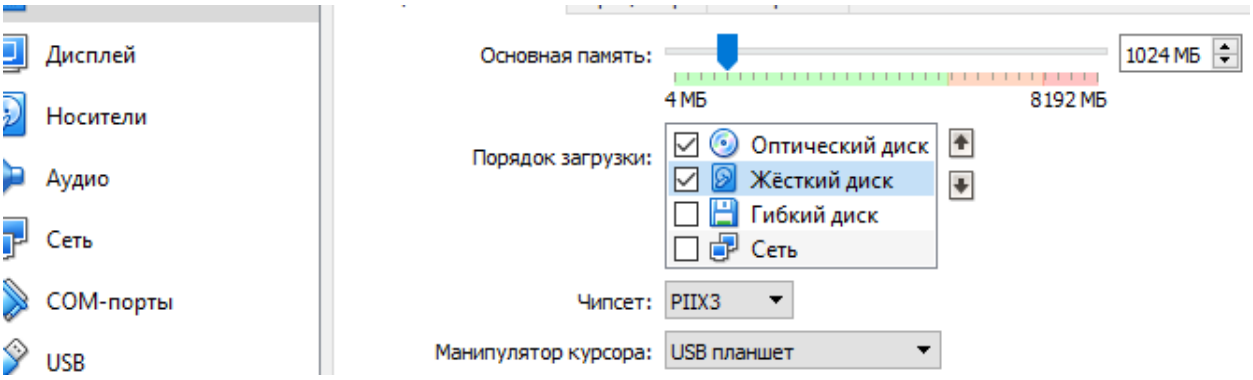


Рисунок 41 – Настройка объема оперативной памяти

Проверить носитель, подключенный к виртуальной машине. Для этого перейти в раздел «Носители» и проверить подключение выбранного жесткого диска (см. рисунок 42).

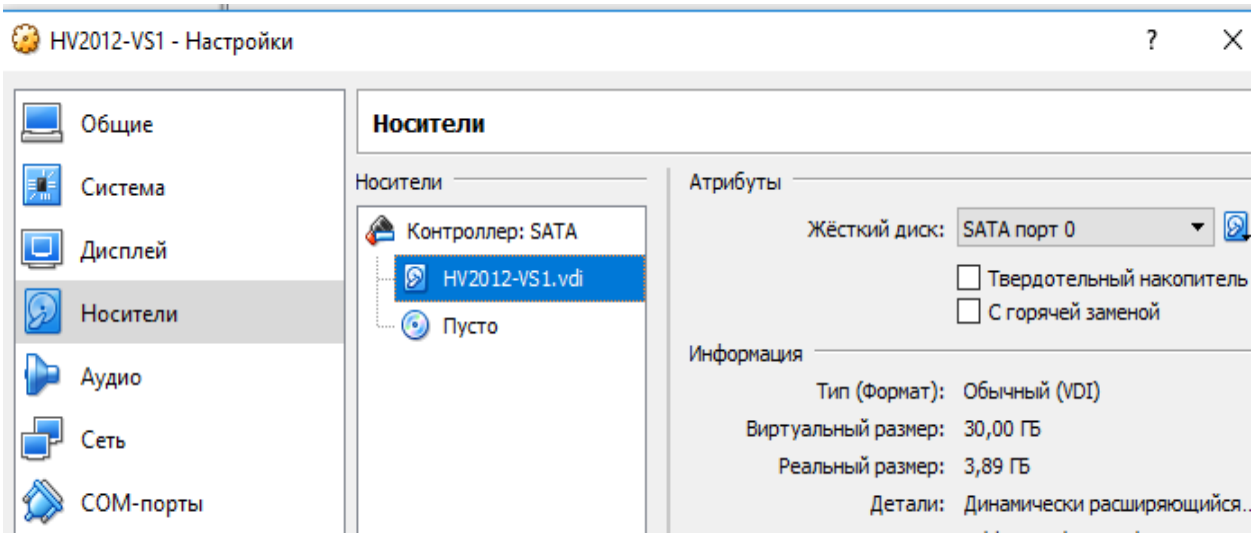


Рисунок 42 – Проверка настройки носителя, подключенного к виртуальной машине

Затем проверить настройки сети для включения ВМ в локальную сеть. Выбрать следующие параметры: «Тип подключения: Внутренняя сеть», «Имя: intnet», тип адаптера оставить по умолчанию, «Неразборчивый режим: Разрешить все», MAC-адрес оставить по умолчанию, поставить отметку в поле «Подключить кабель» (см. рисунок 43).

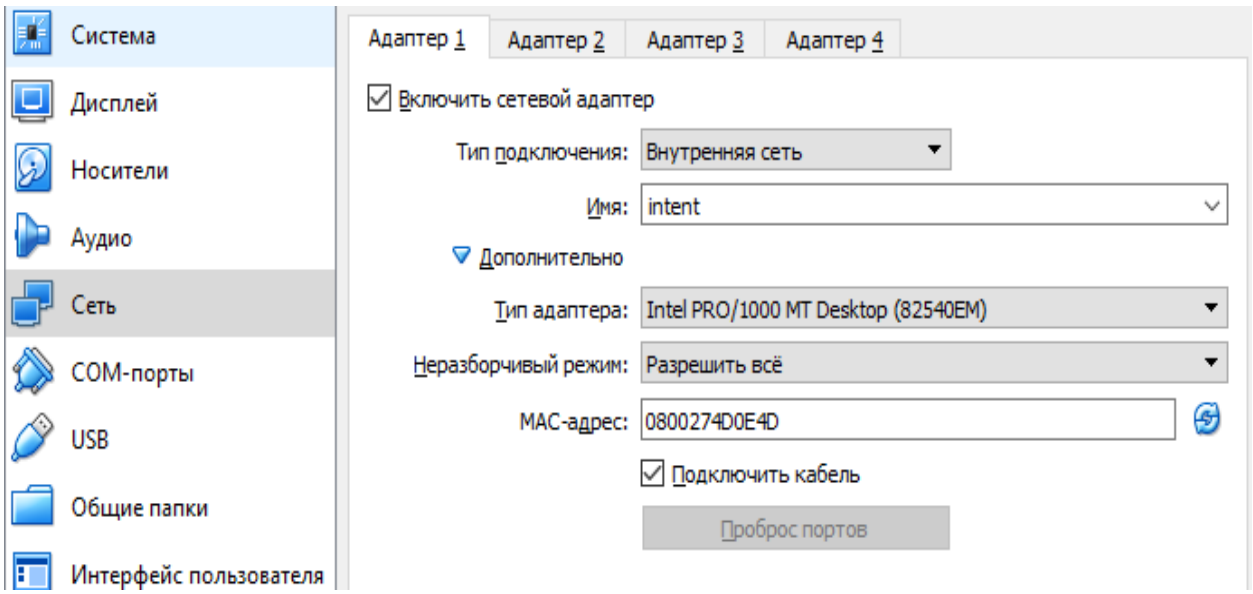


Рисунок 43 - Настройка сети виртуальной машины

После этого выбрать в настройках виртуальной машины раздел «Общие папки». Добавить общую папку, указав расположение данной папки, а также включить авто-подключение (см. рисунок 44).

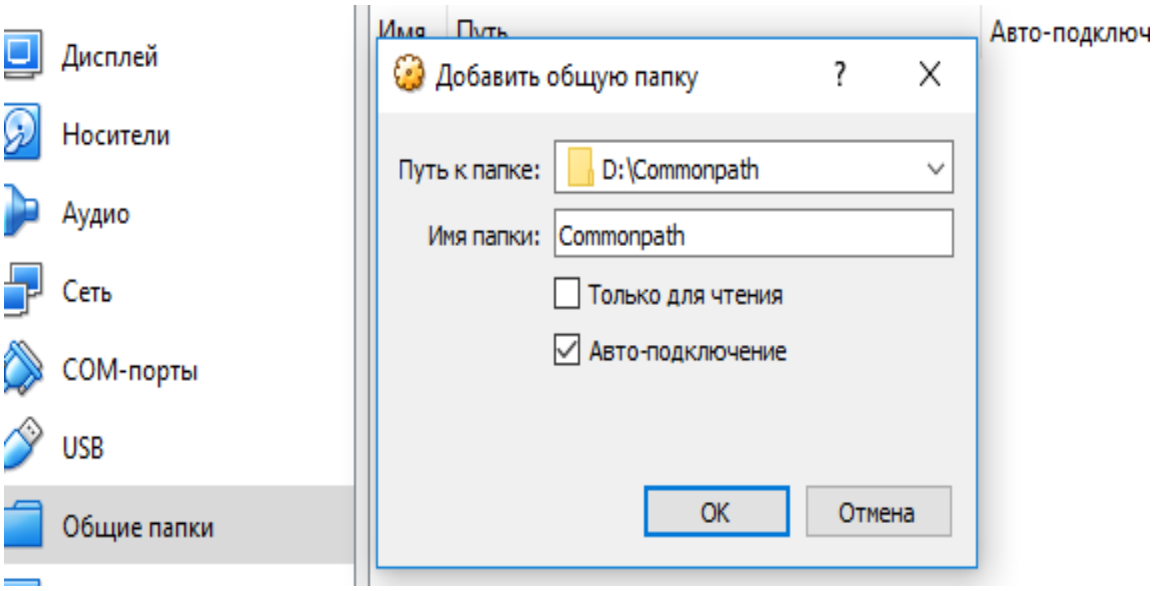


Рисунок 44 - Настройка общей папки виртуальной машины

После создания и настройки виртуальной машины с помощью Oracle VirtualBox Менеджер была выполнена установка гостевой ОС Microsoft Hyper Server 2012 R2. Она выполнялась в соответствии с документацией разработчика – компании Microsoft.

При установке гостевой ОС была создана учетная запись администратора гостевой ОС. Имя учетной записи – «Администратор», пароль – «P.ssw0rd».

При входе в операционной систему надо указать логин – «Администратор», пароль «P.ssw0rd».

Для создания других ВМ с гипервизором посредством клонирования необходимо в левом окне в Oracle VirtualBox Менеджер выбрать ВМ1 – HV2012-VS1. Далее в верхней панели Oracle VirtualBox Менеджер в разделе «Машина» выбрать параметр «Клонирование». В результате будет клонирован Hyper-V сервер HV2012-VS1. После этого откроется диалоговое окно «Клонировать виртуальную машину». Указать имя новой виртуальной машины - HV2012-VS2 (см.рисунок 45).

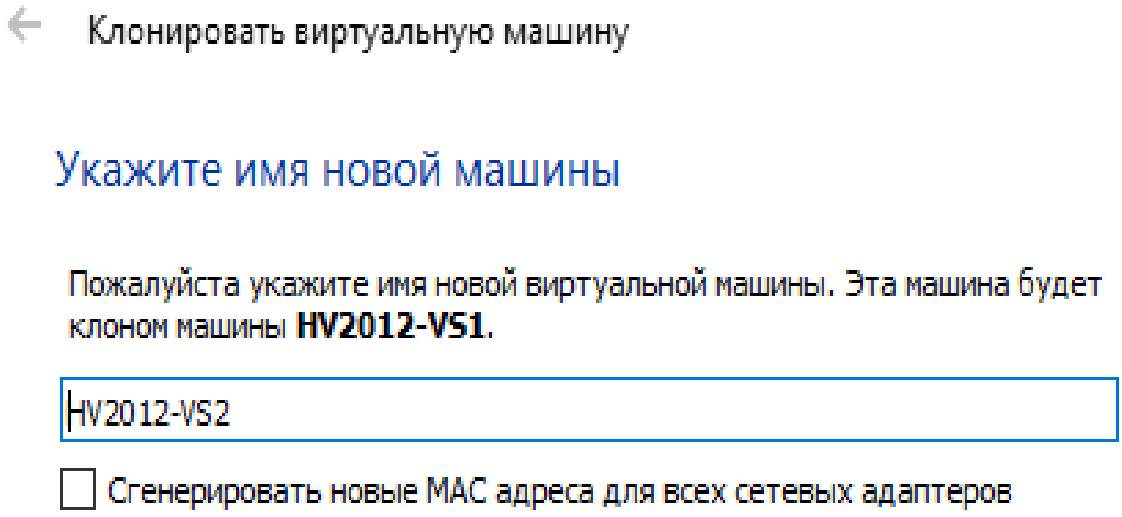


Рисунок 45 – Клонирование виртуальной машины

Аналогично клонировать ВМ3 и указать имя HV2012-VS3.

Далее необходимо настроить гостевую ОС.

Изменить имя Hyper-V сервера. Для этого необходимо запустить утилиту sconfig.exe. Для запуска этой утилиты из командной строки или оболочки PowerShell надо набрать команду sconfig. Будет выведен список параметров, отображающих конфигурацию сервера. Для смены имени надо выбрать номер параметра 2, который отображает имя компьютера. После нажатия параметра 2

надо ввести новое имя компьютера и нажать клавишу Enter. Затем перезагрузить сервер. После перезагрузки сервера и входа администратора с помощью утилиты sconfig проверить текущее имя сервера (см. рисунок 46).

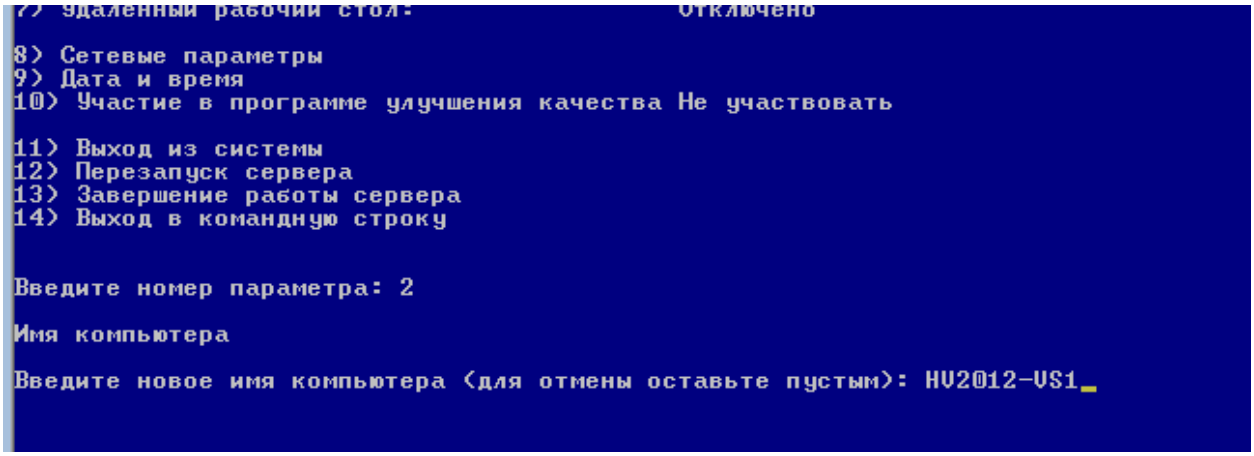


Рисунок 46 - Настройка имени в виртуальной машине

Проверить дату и время. Проверка даты и времени необходима для согласования даты и времени в домене. Дата и время на всех компьютерах домена должны совпадать. Для этого следует запустить утилиту sconfig.exe и выбрать параметр 9. После ввода его номера на экран выводится диалоговое окно настройки даты и времени (см. рисунок 47).

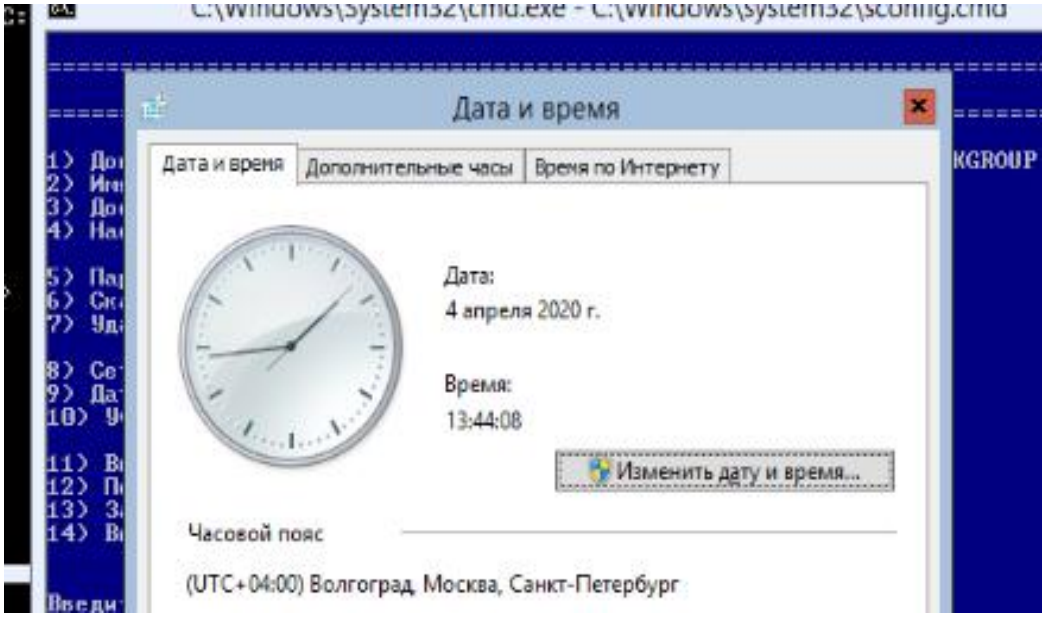


Рисунок 47 - Настройка времени в виртуальной машине

Настроить сетевые параметры гипервизора (см. рисунок 48). Для настройки сетевых параметров необходимо в командной строке ввести команду

netsh interface ip set address name="Ethernet 2" static 192.168.100.11 255.255.255.0 192.168.100.1, где:

- Ethernet - название сетевого интерфейса;

- 192.168.100.11 - сетевой адрес (ip address);

- 255.255.255.0 - сетевая маска (network mask);

- 192.168.100.1 - шлюз (default gateway).

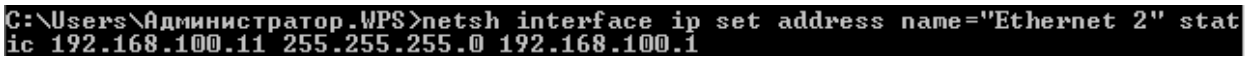


Рисунок 48 – Настройка сети

Проверить установленную конфигурацию сети с помощью команды ipconfig /all (см. рисунок 49).

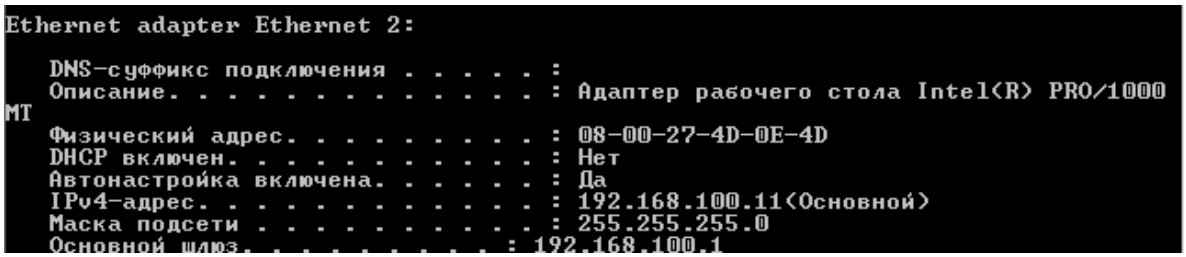


Рисунок 49 – Проверка настройки сети

Также необходимо настроить адрес DNS-сервера, используемого в локальной сети. Для этого в командной строке необходимо ввести команду «netsh interface ip set DNS "Ethernet 2" static 192.168.100.1» (см. рисунок 50).

Рисунок 50 – Настройка DNS-сервера

Проверить установленную конфигурацию сети с помощью команды ipconfig /all (см. рисунок 51).

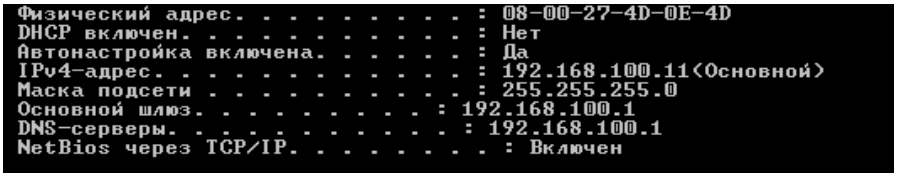


Рисунок 51 – Проверка настройки DNS-сервера

Далее необходимо отключить поддержку протокола IPv6. В командной строке ввести команду powershell, чтобы перейти в оболочку powershell. Далее

следует ввести команду «Disable-NetAdapterBinding –InterfaceAlias "Ethernet 2" –ComponentID ms_tcpip6» (см. рисунок 52).

Рисунок 52 – Отключение поддержки протокола IPv6

Для проверки отключения поддержки IPv6 надо еще раз получить сведения о сетевом адаптере. В перечне значений IPv6-адрес отображаться не должен. Для этого в командной строке ввести команду `ipconfig /all` (см. рисунок 53).

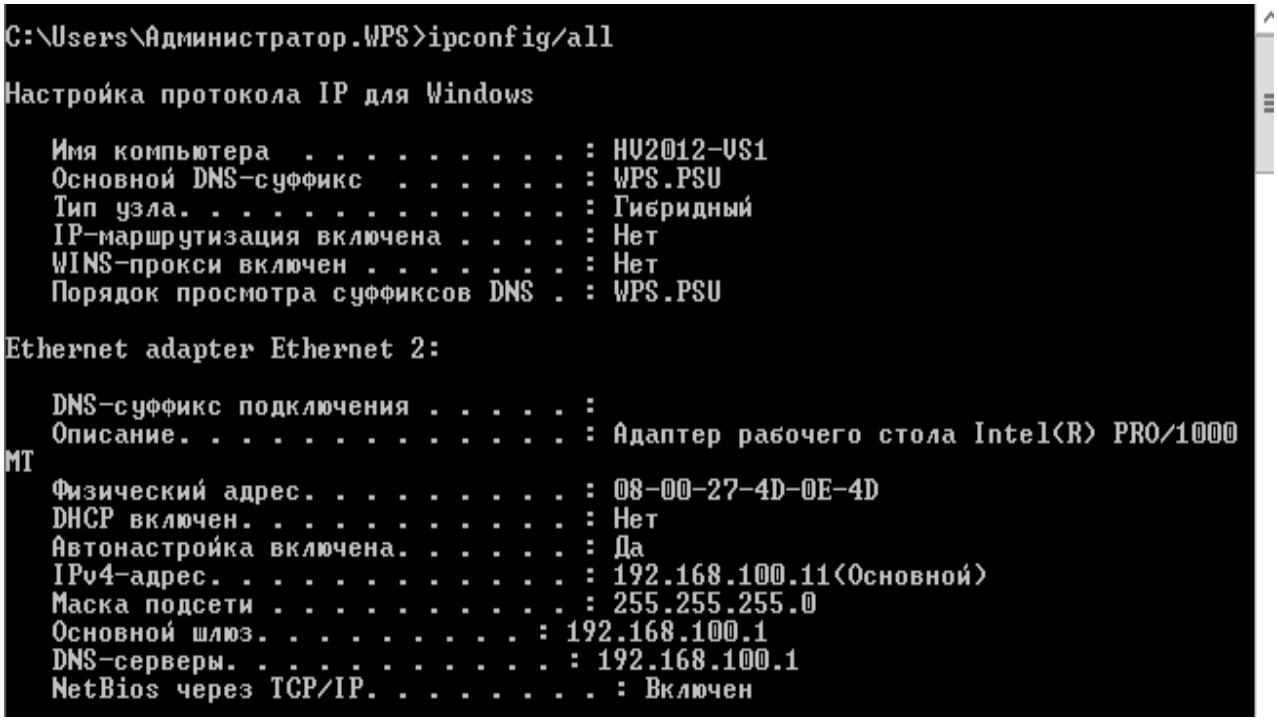


Рисунок 53 – Проверка отключение поддержки протокола IPv6

В результате описанных действий создана ВМ с гостевой ОС Hyper-V Server 2012 R2. Выполнена ее настройка с помощью Oracle VirtualBox Менеджер и настройка гостевой ОС. Эта ВМ после установки гостевой и до ее настройки использовалась для создания двух других ВМ с такой гостевой ОС посредством операции клонирования.

Для клонированной виртуальной машины HV2012-VS2 необходимо изменить имя на «HV2012-VS2»

Для этого необходимо запустить утилиту sconfig.exe. Для запуска этой утилиты из командной строки или оболочки PowerShell надо набрать команду sconfig. Будет выведен список параметров, отображающих конфигурацию сервера. Для смены имени надо выбрать номер параметра 2, который отображает имя компьютера. После нажатия параметра 2 надо ввести новое имя компьютера и нажать клавишу Enter. Затем перезагрузить сервер. После перезагрузки сервера и входа администратора с помощью утилиты sconfig проверить текущее имя сервера

Также необходимо изменить сетевой адрес. Использовать в командной строке команду «netsh interface ip set address name="Ethernet 2" static 192.168.100.12 255.255.255.0 192.168.100.1», где:

- Ethernet - название сетевого интерфейса;
- 192.168.100.12 - сетевой адрес (ip address);
- 255.255.255.0 - сетевая маска (network mask);
- 192.168.100.1 - шлюз (default gateway).

Остальные параметры такие как дата и время, настройка DNS-сервера, отключение поддержки протокола IPv6 такие же, что и на Hyper-V сервере HV2012-VS1 .

Далее для виртуальной машины HV2012-VS3 необходимо изменить имя на «HV2012-VS3». Изменить сетевой адрес. Для этого использовать в командной строке команду «netsh interface ip set address name="Ethernet 2" static 192.168.100.13 255.255.255.0 192.168.100.1», где:

- Ethernet - название сетевого интерфейса;
- 192.168.100.13 - сетевой адрес (ip address);
- 255.255.255.0 - сетевая маска (network mask);
- 192.168.100.1 - шлюз (default gateway).

Остальные параметры такие как дата и время, настройка DNS-сервера, отключение поддержки протокола IPv6 такие же, что и на Hyper-V сервере HV2012-VS1.

HV2012-VS1 и HV2012-VS2 являются серверами виртуализации, входящими в состав среды виртуализации, которая построена на основе домена Active Directory. ВМ являются компьютерами домена.

HV2012-VS3 является локальным сервером виртуализации.

3.4 Установка компонентов Hyper-V на ВМ

Установка компонентов Hyper-V гостевых ОС.

Для установки компонентов сначала надо проверить список компонентов для установки. Для этого необходимо открыть оболочку «Powershell», ввести командлет `Get-WindowsFeature *Hyper-V*` (см. рисунок 54).

Рисунок 54 – Проверка списка компонентов для установки

Список средств управления Hyper-V включает модуль Hyper-V для Windows PowerShell. Этот компонент надо установить, используя командлет Install-WindowsFeature с указанием параметра имени (Name) компонента. Имена отображаются в результатах работы команды Get-WindowsFeature *Hyper-V*. Для установки модуля Hyper-V для Windows Powershell необходимо в оболочке «Powershell» ввести командлет `Install-WindowsFeature Hyper-V-Powershell` (см. рисунок 55).

Рисунок 55 – Установка модуля Hyper-V для Windows PowerShell

Для проверки установки компонентов можно использовать командлет Get-WindowsFeature или команду Get-WindowsFeature *Hyper-V*. Компоненты для управления Hyper-V будут отмечены как установленные. Для этого в оболочке «Powershell» ввести командлет Get-WindowsFeture *Hyper-V* (см. рисунок 56).

Рисунок 56 – Проверка установки компонентов

Для получения модуля управления платформой Hyper-V к оболочке Windows PowerShell надо использовать командлет Get-Module. Для этого следует ввести в оболочке «Powershell» командлет Get-Module. Соответствующий модуль в списке будет отсутствовать (см. рисунок 57).

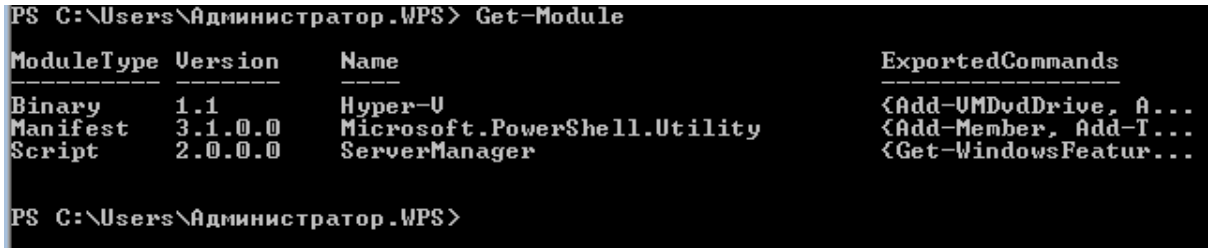


Рисунок 57 - Получение модуля управления платформой Hyper-V к оболочке Windows PowerShell

Для подключения модуля надо использовать командлет «Import-Module Hyper-V» (см. рисунок 58).

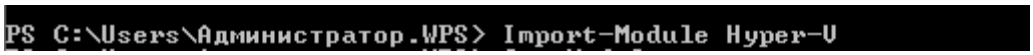


Рисунок 58 – Подключение модуля управления платформой Hyper-V к оболочке Windows PowerShell

Повторная проверка с помощью командлета Get-Module должна показать наличие модуля Hyper-V в списке подключенных.

Модуль Hyper-V содержит командлеты для управления компонентами среды виртуализации – виртуальными жесткими дисками, виртуальными

машинами и др. Для проверки доступности этих командлетов можно использовать командлет Get-Command *VM* или Get-Command *VHD*. Необходимо ввести в оболочке «Powershell» командлет «Get-Command *VM*» (см. рисунок 59).

Рисунок 59 – Выполнение командлета Get-Command *VM*

В результате их запуска будет выведен соответствующий список командлетов.

3.5 Установка роли и компонентов управления Hyper-V на ВМ с гостевой ОС Windows Server 2012 R2

Для управления средой виртуализации включая удаленное управление надо установить компоненты и роли Hyper-V. Так как гостевая ОС установлена в ВМ, созданной с помощью ПО Oracle VirtualBox, установки роли Hyper-V в ОС Windows Server 2012 R2 невозможна. Можно установить отдельные компоненты, которые в дальнейшем могут применяться для управления средой виртуализации.

Для установки компонентов сначала надо проверить список компонентов для установки. Для этого необходимо открыть оболочку «Powershell», в нижней панели вирутальной машины Windows Server 2012 R2 и ввести командлет `Get-WindowsFeature *Hyper-V*` (см. рисунок 60).

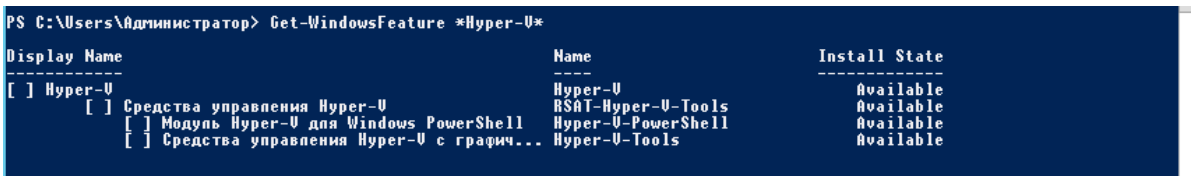


Рисунок 60 – Проверка списка компонентов для установки

Список средств управления Hyper-V включает модуль Hyper-V для Windows PowerShell и средства управления Hyper-V с графическим интерфейсом. Эти два компонента надо установить, используя командлет Install-WindowsFeature с указанием параметра имени (Name) компонента. Имена отображаются в результатах работы команды Get-WindowsFeature *Hyper-V*. Для установки модуля Hyper-V для Windows Powershell необходимо в оболочке «Powershell» ввести командлет `Install-WindowsFeature Hyper-V-Powershell` (см. рисунок 61).

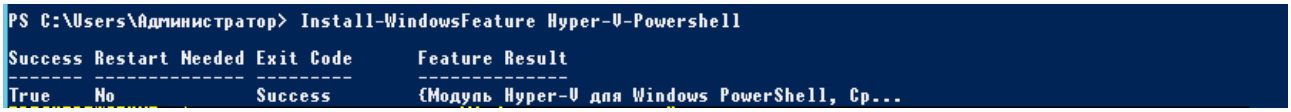


Рисунок 61– Установка модуля Hyper-V для Windows PowerShell

Для установки средства управления Hyper-V с графическим интерфейсом необходимо в оболочке «Powershell» ввести командлет `Install-WindowsFeature Hyper-V-Tools` (см. рисунок 62).

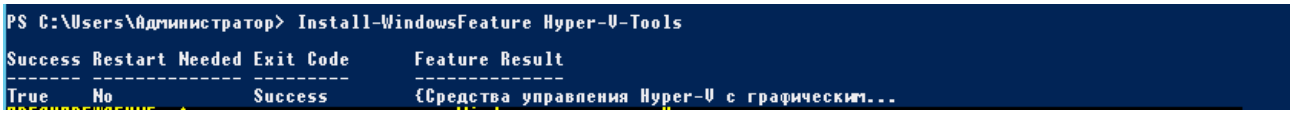


Рисунок 62– Установка средства управления Hyper-V с графическим интерфейсом

Для проверки установки компонентов можно использовать командлет Get-WindowsFeature или команду Get-WindowsFeature *Hyper-V*. Компоненты для управления Hyper-V будут отмечены как установленные. Для этого в оболочке «Powershell» ввести командлет Get-WindowsFeture *Hyper-V* (см. рисунок 63).

```
PS C:\Users\Администратор> Get-WindowsFeature *Hyper-V*

Display Name                                            Name                    Install State
------------                                            ----                    -------------
[ ] Hyper-V                                             Hyper-V                     Available
    [X] Средства управления Hyper-V                     RSAT-Hyper-V-Tools          Installed
        [X] Модуль Hyper-V для Windows PowerShell       Hyper-V-PowerShell          Installed
        [X] Средства управления Hyper-V с графич...     Hyper-V-Tools               Installed
```

Рисунок 63 – Проверка установки компонентов

Для получения модуля управления платформой Hyper-V к оболочке Windows PowerShell надо использовать командлет Get-Module. Для этого следует ввести в оболочке «Powershell» командлет Get-Module. Соответствующий модуль в списке будет отсутствовать (см. рисунок 64).

```
PS C:\Users\Администратор> Get-Module

ModuleType Version    Name                                ExportedCommands
---------- -------    ----                                ----------------
Manifest   3.1.0.0    Microsoft.PowerShell.Management     {Add-Computer, Add-Content, Checkpoint-Computer, Clear-Con...
Manifest   3.1.0.0    Microsoft.PowerShell.Utility        {Add-Member, Add-Type, Clear-Variable, Compare-Object...}
Script     2.0.0.0    ServerManager                       {Get-WindowsFeature, Install-WindowsFeature, Uninstall-Win...
```

Рисунок 64 - Получение модуля управления платформой Hyper-V к оболочке Windows PowerShell

Для подключения модуля надо использовать командлет «Import-Module Hyper-V» (см. рисунок 65).

```
PS C:\Users\Администратор> Import-Module Hyper-V
```

Рисунок 65 – Подключение модуля управления платформой Hyper-V к оболочке Windows PowerShell

Повторная проверка с помощью командлета Get-Module должна показать наличие модуля Hyper-V в списке подключенных (см. рисунок 66)

```
PS C:\Users\Администратор> Get-Module

ModuleType Version    Name                                ExportedCommands
---------- -------    ----                                ----------------
Binary     1.1        Hyper-V                             {Add-VMDvdDrive, Add-VMFibreChannelHba, Add-VMHardDiskDriv...
Manifest   3.1.0.0    Microsoft.PowerShell.Management     {Add-Computer, Add-Content, Checkpoint-Computer, Clear-Con...
Manifest   3.1.0.0    Microsoft.PowerShell.Utility        {Add-Member, Add-Type, Clear-Variable, Compare-Object...}
Script     2.0.0.0    ServerManager                       {Get-WindowsFeature, Install-WindowsFeature, Uninstall-Win...
```

Рисунок 66 – Повторная проверка с помощью командлета Get-Module

Модуль Hyper-V содержит командлеты для управления компонентами среды виртуализации – виртуальными жесткими дисками, виртуальными машинами и др. Для проверки доступности этих командлетов можно

использовать командлет Get-Command *VM* или Get-Command *VHD*. В оболочке «Powershell» надо ввести командлет «Get-Command *VM*» (см. рисунок 67).

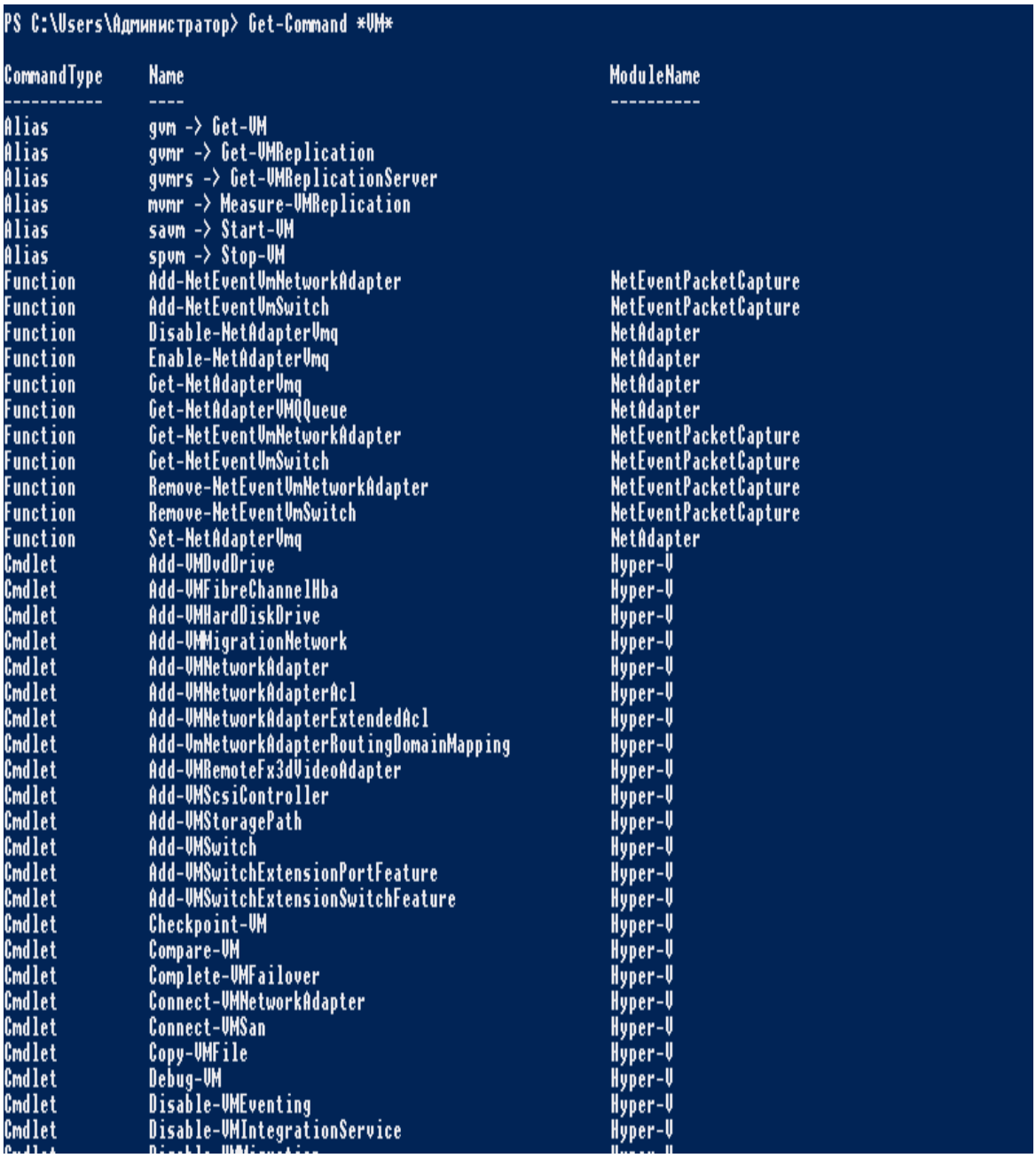


Рисунок 67 – Выполнение командлета Get-Command *VM*

В результате их запуска будет выведен соответствующий список командлетов.

Также необходимо проверить наличие консолей управления, которые предоставляют администратору графический интерфейс. Для запуска

графической консоли управления Менеджер Hyper-V можно с помощью команды «Выполнить» из меню «Пуск» запустить файл virtmgmt.msc. После запуска консоли Менеджер Hyper-V надо запустить один из подготовленных серверов виртуализации (ВМ с гипервизором) и в консоли выполнить подключение к этому серверу виртуализации. Для этого следует в верхней панели диспетчера Hyper-V открыть раздел «Действие», команду «Подключиться к серверу». Откроется диалоговое окно «Выбор компьютера». В этом диалоговом окне поставить отметку в пункте «Другой компьютер», щелкнуть левой кнопкой мыши по кнопке «Обзор». Откроется диалоговое окно «Выбор: "Компьютер "» После этого щелкнуть левой кнопкой мыши по кнопке «Дополнительно», в появившемся окне щелкнуть левой кнопкой мыши на кнопку «Поиск». В результатах поиска выбрать необходимую виртуальную машину для подключения к серверу виртуализации. Нажать кнопку «ОК» (см. рисунок 68).

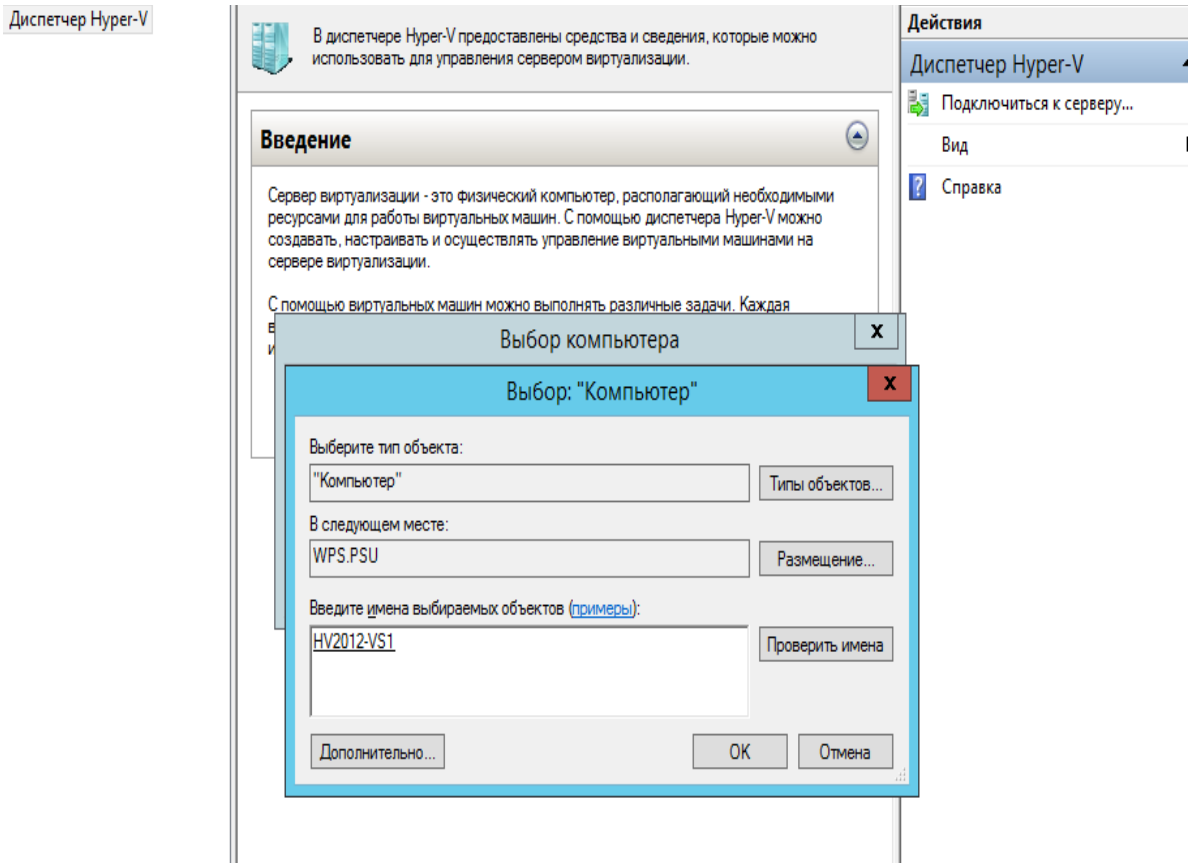


Рисунок 68 – Подключение виртуальной машины к серверу виртуализации

После подключения в правой части окна консоли будет отображен список ВМ, созданных на этом сервере (см. рисунок 69).

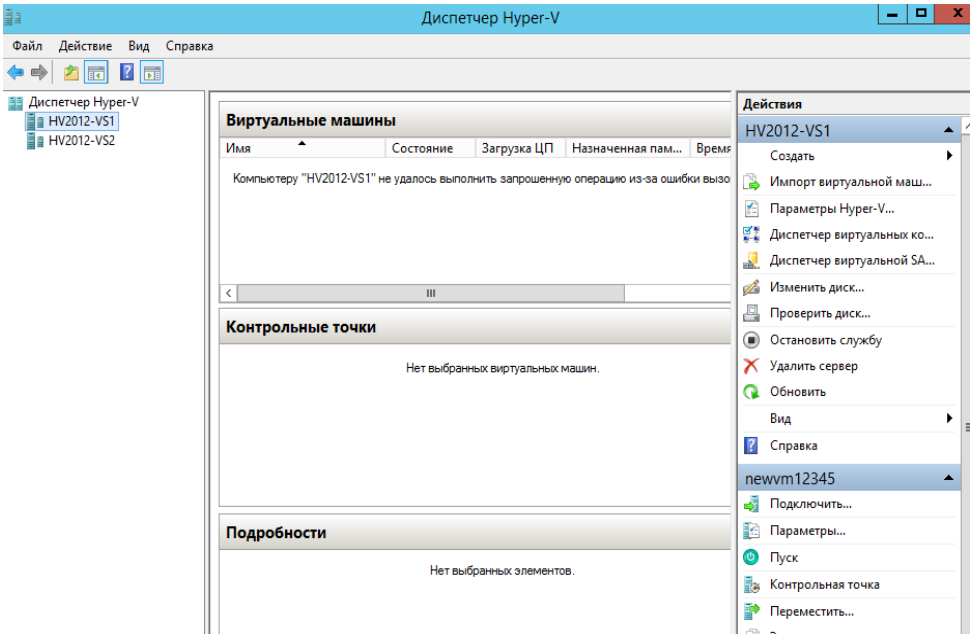


Рисунок 69 – Отображение списка ВМ, созданных на сервере

Таким образом, были созданы виртуальные машины, входящие в состав стенда: виртуальная машина с установленной гостевой ОС Windows 2012 и виртуальная машина с установленным гипервизором Hyper-V 2012 R2. Установлены компоненты Hyper-V на виртуальные машины.

Все виртуальные машины и компоненты Hyper-V 2012 R2 функционируют правильно.

3.6 Создание и конфигурирование локальной сети, состоящей из виртуальных машин

Для обеспечения возможности удаленного управления гипервизорами необходимо настроить средства удаленного управления и межсетевой экран на Hyper-V сервере.

Первоначально необходимо на Hyper-V сервере включить удаленное управление. Для этого надо использовать командлет «Enable-PSRemoting» (см. рисунок 70).

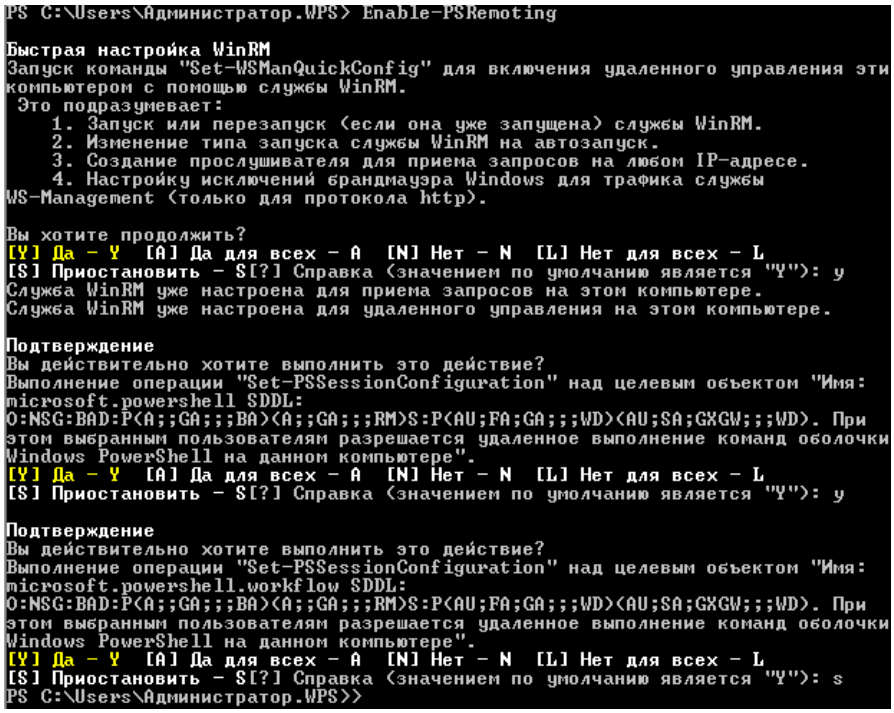


Рисунок 70 – Включение удаленного управления

После выполнения этого командлета надо проверить статус служб сервера, таких как WinRM, Winmgmt. Их статус должен быть Running. Для проверки надо использовать командлет Get-Service (см. рисунок 71).

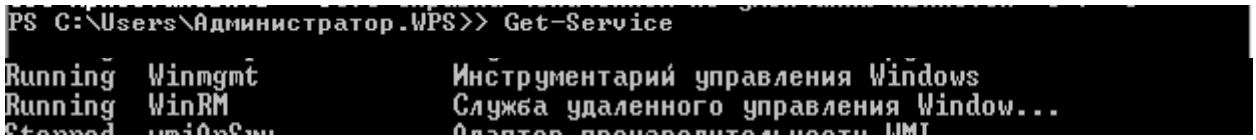


Рисунок 71 – Проверка статуса служб

Также надо проверить состояние службы «RemoteRegistry» (см. рисунок 72).

Рисунок 72 – Проверка статуса службы «RemoteRegistry»

Если состояние этой службы Stopped, то надо изменить тип запуска на «Автоматически» и затем запустить эту службу. Для настройки и запуска службы удаленного реестра надо использовать следующие команды:

— «Set-Service –Name RemoteRegistry –StartupType Auto»;

— «Start-Service –Name RemoteRegistry».

Кроме настройки удаленного управления надо настроить межсетевой экран на Hyper-V сервере. Настройка выполняется для межсетевого экрана в режиме повышенной безопасности. Она может быть выполнена с использованием утилиты командной строки «netsh».

Для настройки удаленного управления сервером виртуализации надо настроить следующие входящие правила межсетевого экрана в режиме повышенной безопасности. Сначала надо включить правило, позволяющее управлять логическими дисками (томами). Ввести команду «Netsh advfirewall firewall set rule group="Удаленное управление томами" new enable=yes» (см. рисунок 73).

Рисунок 73 – Включение правила, позволяющего управлять логическими дисками (томами)

Затем надо разрешить удаленное управление файерволом. Следует ввести команду «Netsh advfirewall firewall set rule group="Удаленное управление брандмауэром Windows" new enable=yes» (см. рисунок 74).

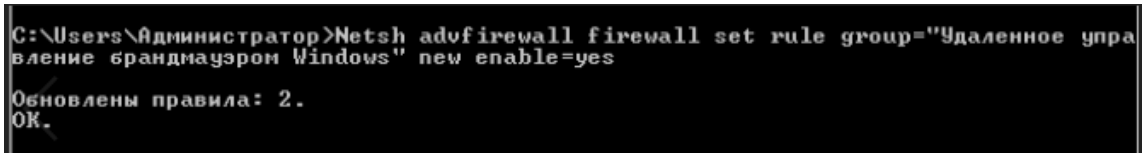


Рисунок 74 – Настройка разрешения удаленного управления файерволом

Для разрешения использовать «Windows Management Instrumentation (WMI)» надо применить следующую команду «netsh advfirewall firewall set rule

group="Инструментарий управления Windows (WMI)" new enable=yes» (см. рисунок 75).

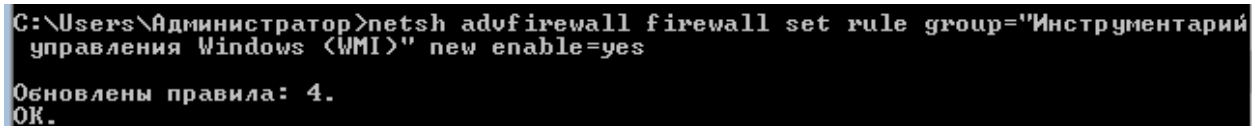


Рисунок 75 – Настройка разрешения инструментария управления Windows

Затем необходимо разрешить icmp-протокол. Ввести команду «netsh firewall set icmpsetting 8» (см. рисунок 76).

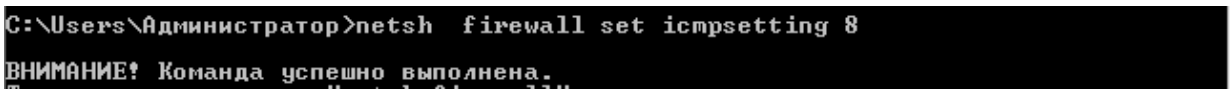


Рисунок 76 – Настройка разрешения icmp – протокола

Следующая группа правил, которую необходимо включить – Журналы и оповещения производительности. Ввести команду «netsh advfirewall firewall set rule group=" Журналы и оповещения производительности" new enable=yes» (см. рисунок 77).

Рисунок 77 – Настройка правил, содержащих журналы и оповещения производительности

Затем необходимо разрешить удаленное управление Windows. Ввести команду «netsh advfirewall firewall set rule group="Удаленное управление Windows" new enable=yes» (см. рисунок 78).

Рисунок 78– Настройка разрешения удаленного управления Windows

Следующая группа правил, которую необходимо включить – Удаленное управление журналом событий. Ввести команду «netsh advfirewall firewall set

rule group="Удаленное управление журналом событий" new enable=yes» (см. рисунок 79).

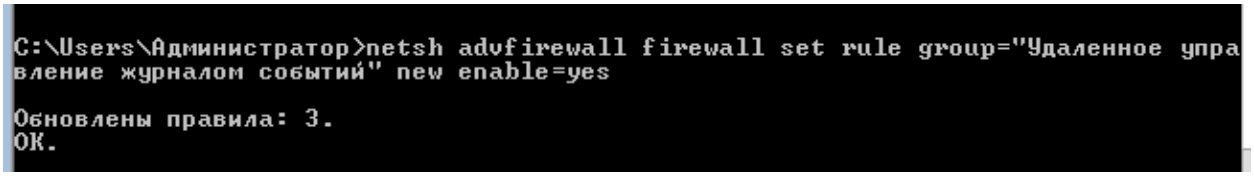


Рисунок 79 – Настройка разрешения удаленного управления журналом событий

Для разрешения использовать «Наблюдение за виртуальной машиной» надо применить следующую команду «netsh advfirewall firewall set rule group="Наблюдение за виртуальной машиной" new enable=yes» (см. рисунок 80).

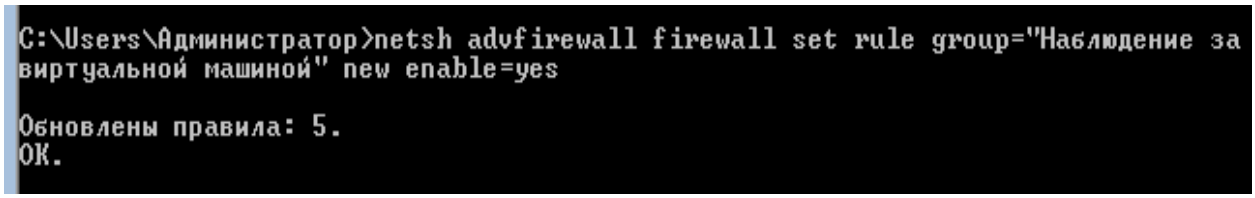


Рисунок 80 – Настройка разрешения наблюдения за виртуальной машиной

Затем необходимо разрешить дистанционное управление рабочим столом. Ввести команду «netsh advfirewall firewall set rule group="Дистанционное управление рабочим столом" new enable=yes» (см. рисунок 81).

Рисунок 81 – Настройка разрешения дистанционного управления рабочим столом

Провести те же действия с сервером виртуализации HV2012-VS2.

После создания и настройки ВМ1, ВМ2 и ВМ3 входят в рабочую группу. Перед созданием домена Active Directory необходимо проверить соединение виртуальных машин HV2012-VS1 и HV2012-VS2 с контроллером домена сервером WS2012-DC по сетевому адресу и DNS имени.

Проверка соединения с Hyper-V сервера HS2012-WS1 на сервер контроллера домена WS2012-DC осуществляется с использованием команд «ping 192.168.100.1» и «ping WS2012-DC» (см. рисунок 82).

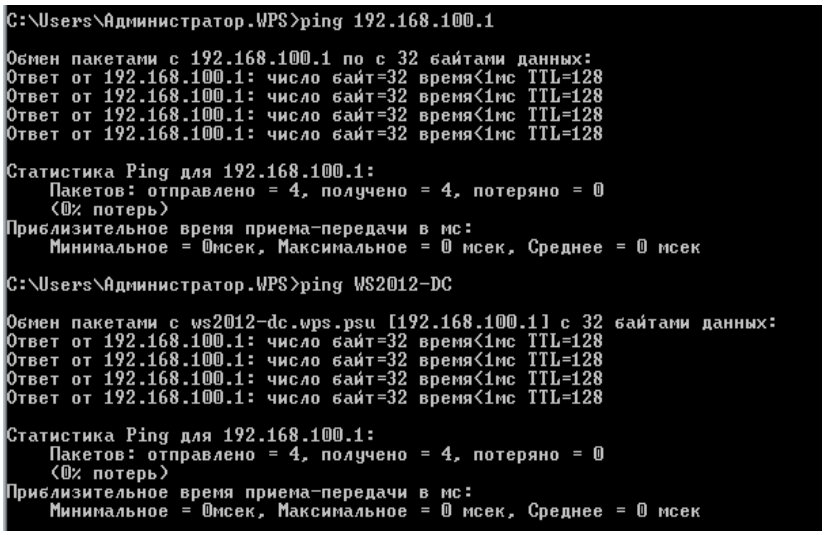


Рисунок 82 – Проверка соединения с Hyper-V сервера HV2012-VS1 на сервер контроллера домена WS2012-DC

Проверка соединения с Hyper-V сервера HS2012-WS2 на сервер контроллера домена WS2012-DC осуществляется с использованием команд «ping 192.168.100.1» и «ping WS2012-DC» (см. рисунок 83).

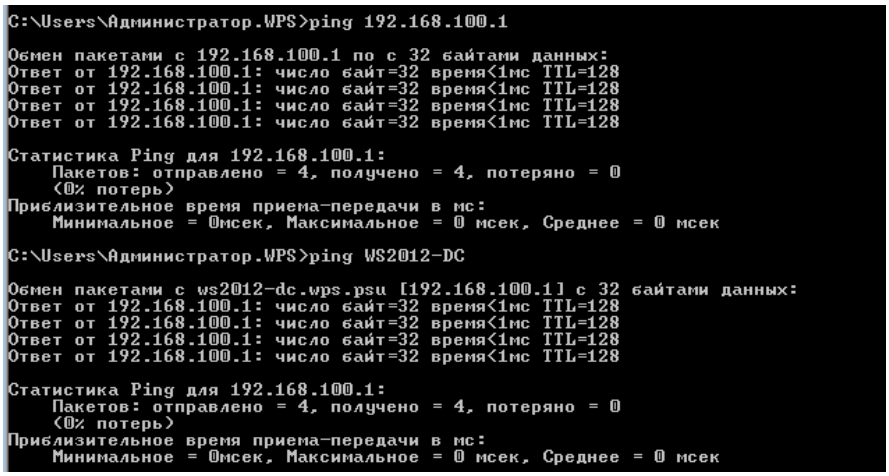


Рисунок 83 – Проверка соединения с Hyper-V сервера HV2012-VS2 на сервер контроллера домена WS2012-DC

Проверка соединения с сервера контроллера домена WS2012-DC на Hyper-V сервера HV2012-VS1 и HV2012-VS2 осуществляется с

использованием команд «ping 192.168.100.11», «ping 192.168.100.12» и «ping HS2012-VS1», «ping HS2012-VS2» (см. рисунок 84).

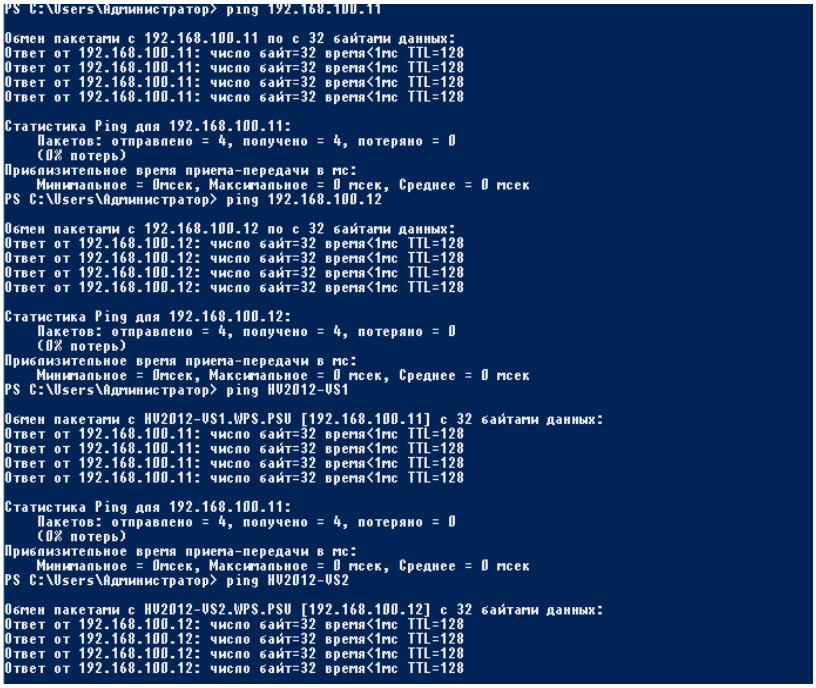


Рисунок 84 – Проверка соединения с сервера контроллера домена WS2012-DC на Hyper-V сервера HV2012-VS1 и HV2012-VS2

В результате проверки можно сделать вывод, что соединение между Hyper-V серверами и контроллером домена осуществляется, пакеты отправляются, что показывает правильность сетевых настроек с помощью Oracle VirtualBox Менеджер и настроек гостевой ОС.

Далее необходимо создать домен Active Directory с контроллером домена WS2012-DC и включить в него ВМ1, ВМ2 и ВМ3. Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», выбрать выпадающий список команд «Управление», далее выбрать команду «Добавить роли и компоненты». Будет запущен мастер добавления ролей и компонентов, в диалоговом окне которого надо нажать кнопку «Далее» до этапа «Роли сервера». Все настройки на этапах «Тип установки» и «Выбор сервера» оставить по умолчанию. На этапе «Роли сервера» поставить отметку в поле «Доменные службы Active Directory», нажать «Добавить компоненты», «Установить» (см. рисунок 85)

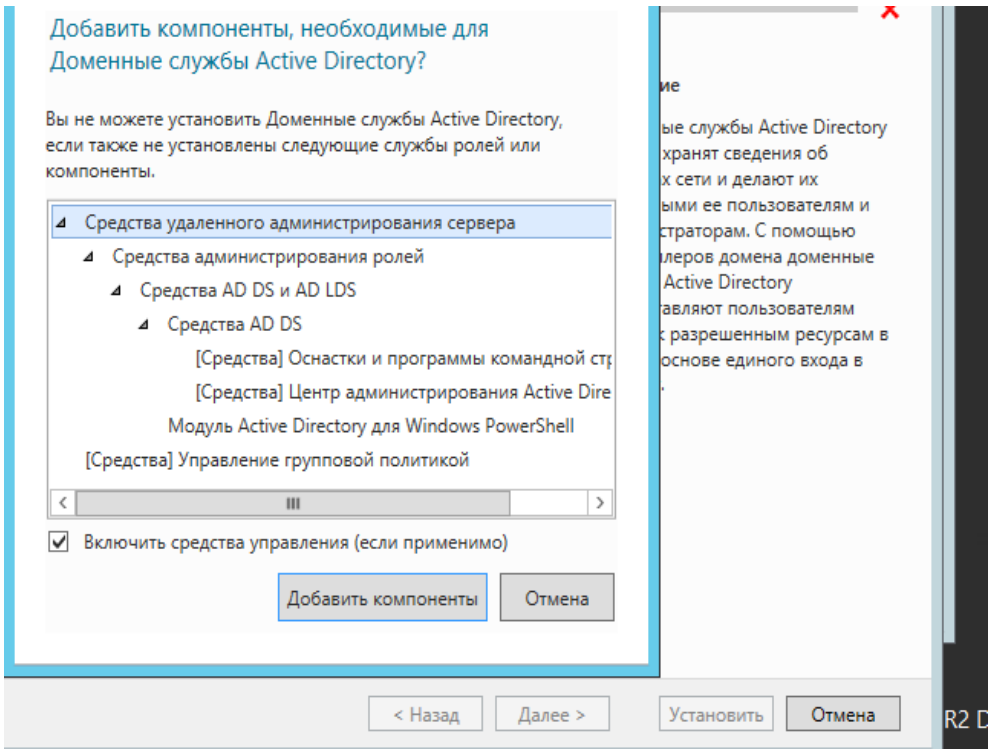


Рисунок 85 – Установка компонента «Доменные службы Active Directory »

После установки на ВМ WS2012-DC служб Active Directory необходимо настроить сервер, повысив его роль до роли контроллера домена. Для этого в диспетчере сервера следует щелкнуть на флажок и выбрать команду «Повысить роль этого сервера до уровня контроллера домена» (см. рисунок 86).

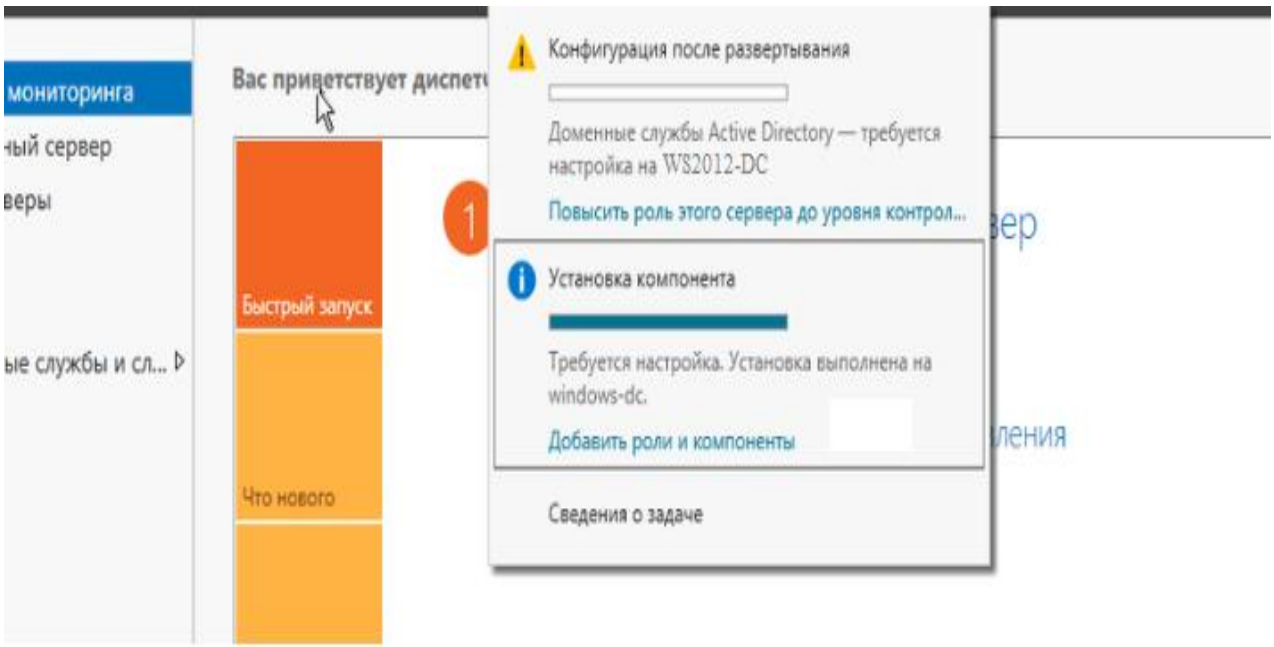


Рисунок 86 – Повышение сервера до роли контроллера домена

При этом надо выбрать вариант создания нового леса, в качестве имени корневого домена надо указать имя зоны прямого просмотра DNS (см. рисунок 87).

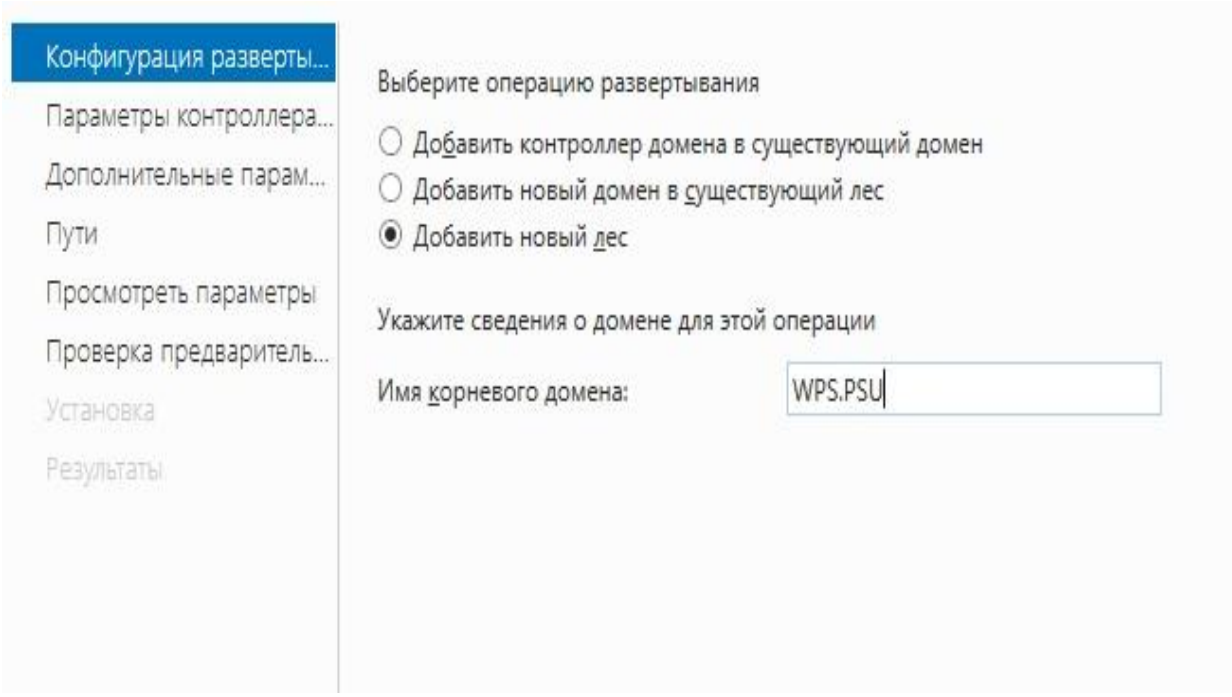


Рисунок 87 – Настройка конфигурации развертывания

В качестве пароля для режима восстановления служб каталогов (DSRM) указать пароль администратора сервера. Остальные параметры оставить без изменений (см.рисунок 88).

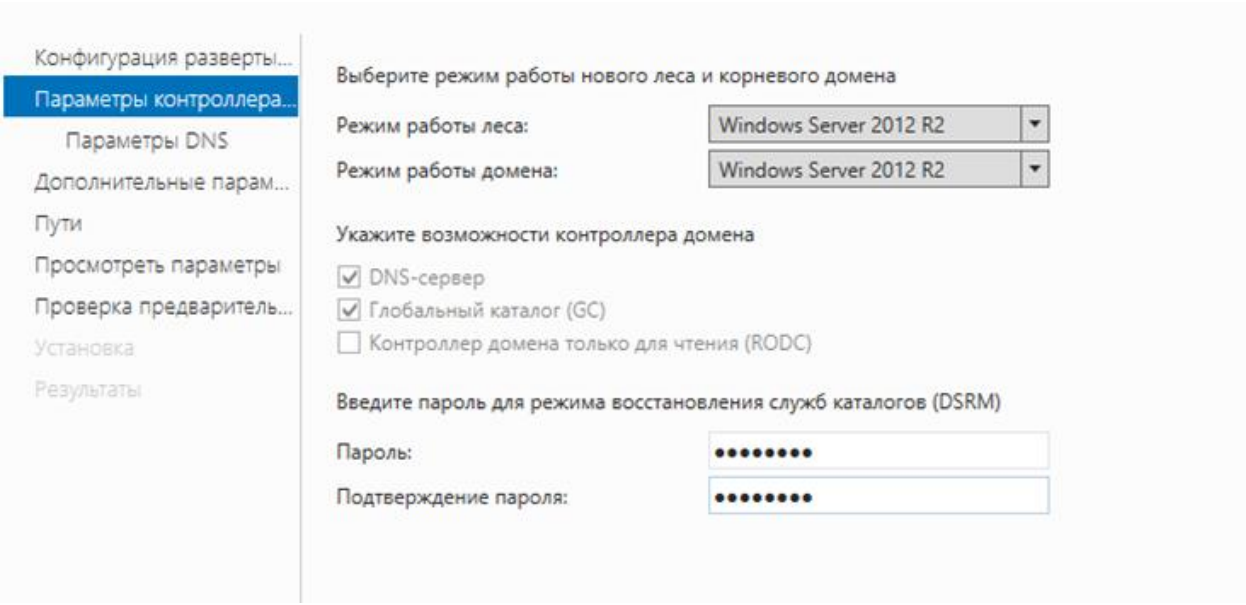


Рисунок 88 – Настройка параметров контроллера домена

При настройке делегирования DNS надо указать имя и пароль администратора сервера (рисунок 89).

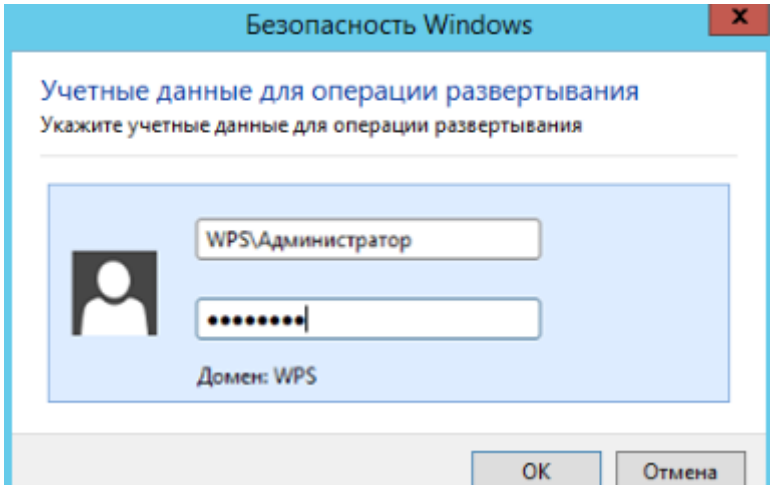


Рисунок 89 – Настройка параметров DNS

В качестве имени домена NetBIOS надо указать имя домена (зоны прямого просмотра) без точки и имени домена первого уровня. Остальные параметры оставить без изменения (см. рисунок 90).

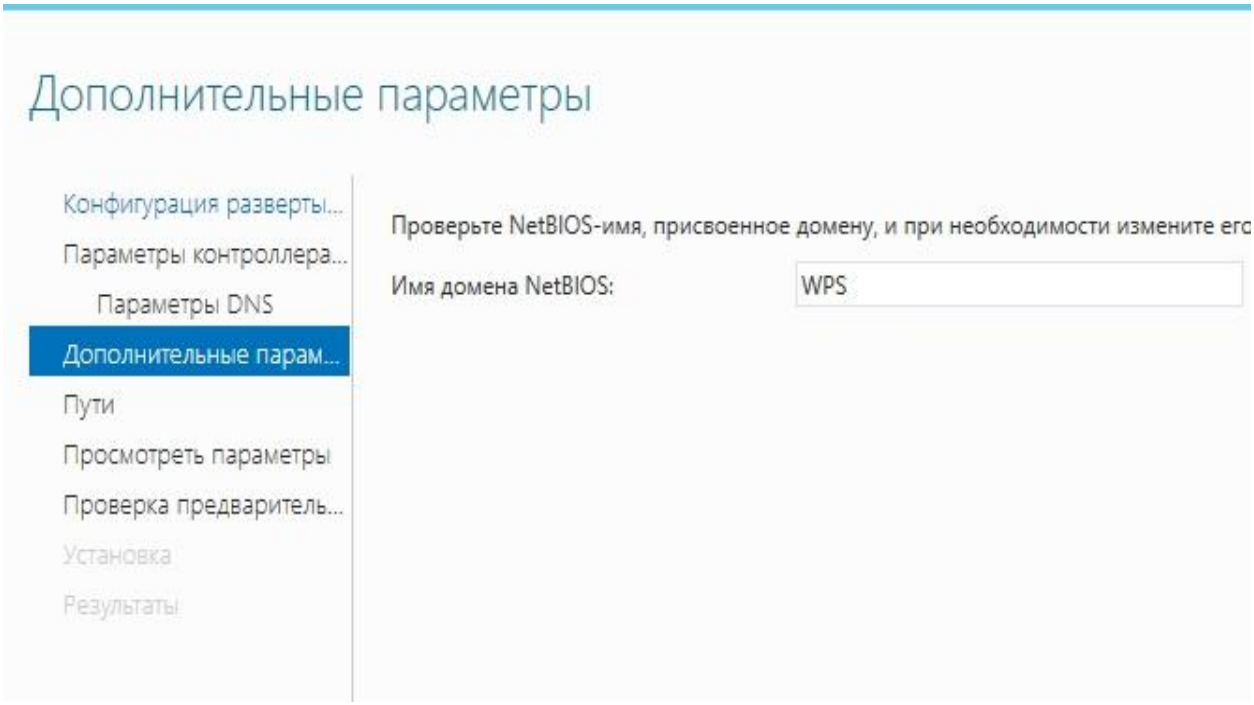


Рисунок 90– Настройка параметров DNS

Интегрировать зону прямого просмотра DNS и Active Directory. Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», в разделе «Средства» выбрать параметр «DNS». В

открывшемся окне нажать на раздел «Зона прямого просмотра», открыть правой кнопкой мыши кнопку «Свойство» сервера и на вкладке «Общие» нажать кнопку «Изменить». Установить параметр «Хранить зону в Active Directory». Сохранить изменения, нажав кнопку «ОК» (см. рисунок 91).

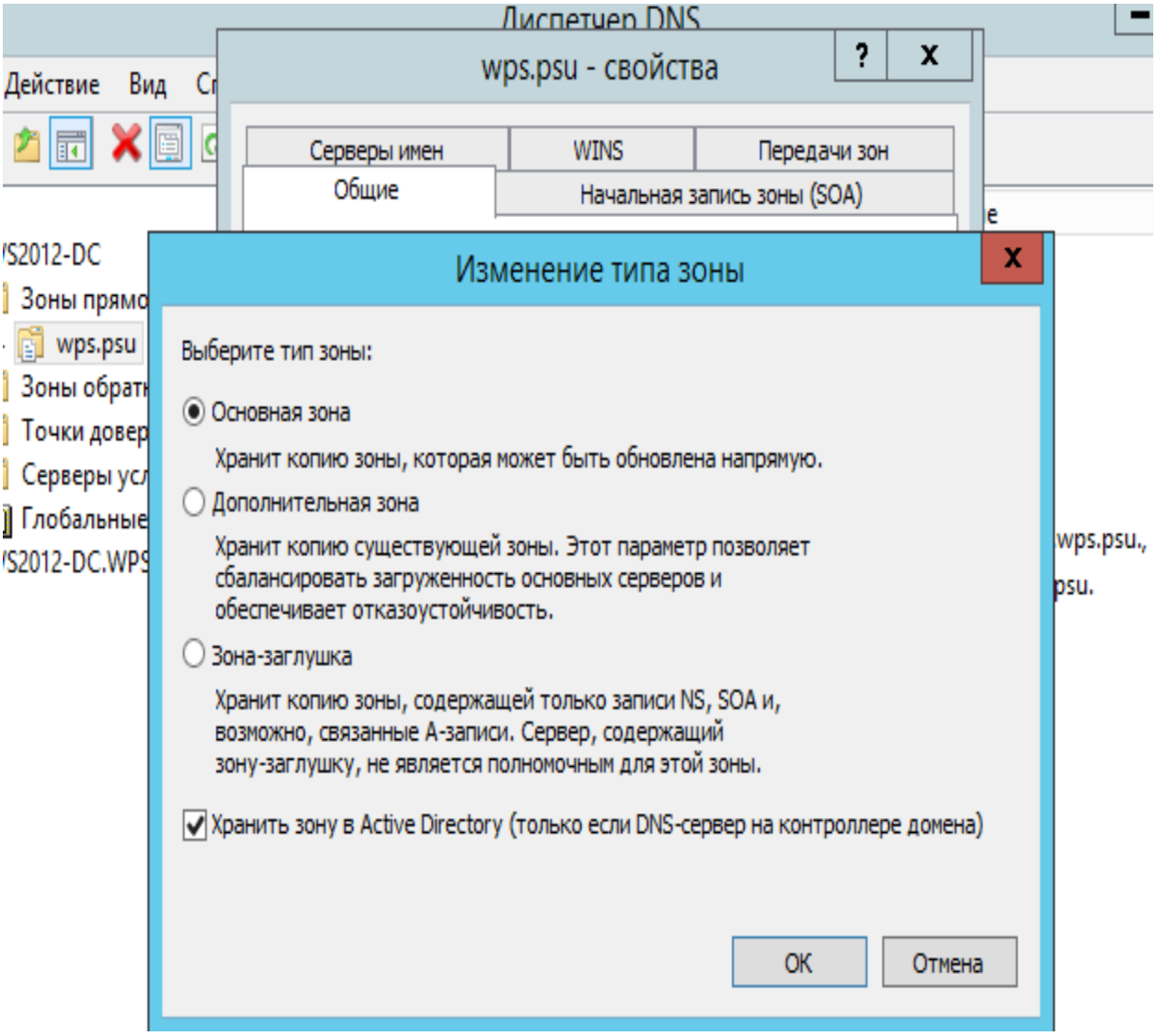


Рисунок 91 – Интегрирование зоны прямого просмотра

Добавить гипервизор HV2012-VS1 в домен. Для этого первоначально необходимо изменить его основной DNS-суффикс, ввести в оболочке powershell командлет «reg add HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters /v ‘Domain’ /d ‘имя_DNS_зоны’». Проверить изменение основного DNS-суффикса имени сервера можно с помощью командной строки, используя команду ipconfig /all.

Для параметра Основной DNS-суффикс будет указано имя зоны прямого просмотра DNS (см. рисунок 92).

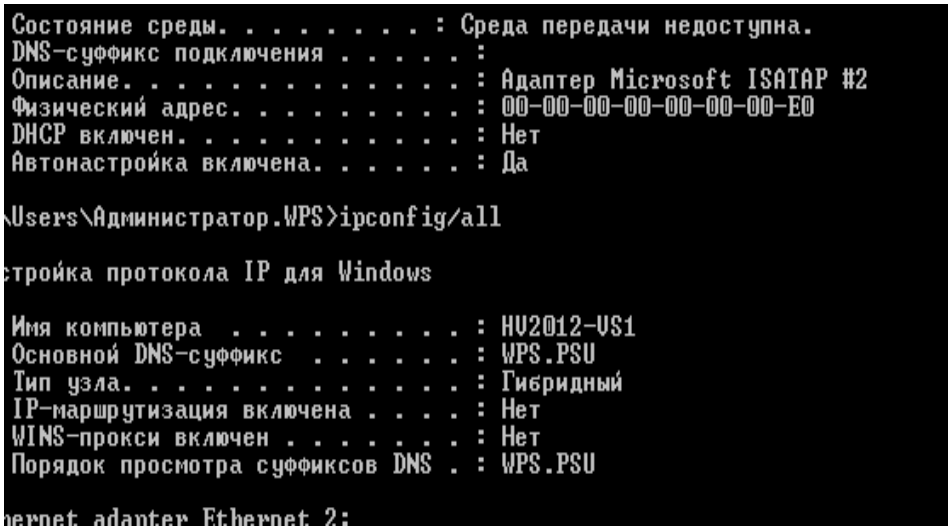


Рисунок 92 – Изменение DNS-суффикса Hyper-V сервера

Также для проверки на контроллере домена надо запустить консоль DNS, отобразить содержимое зоны прямого просмотра. Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», в выпадающем списке команд «Средства» выбрать параметр «DNS». В открывшемся окне нажать на раздел «Зона прямого просмотра», щелкнуть на имя сервера.

При необходимости содержимое зоны прямого просмотра обновить. В списке узлов типа А должно быть указано два узла – контроллер домена, который является DNS-сервером, и сервер Hyper-V. В строке с именем каждого узла указывается его IP-адрес (см. рисунок 93).

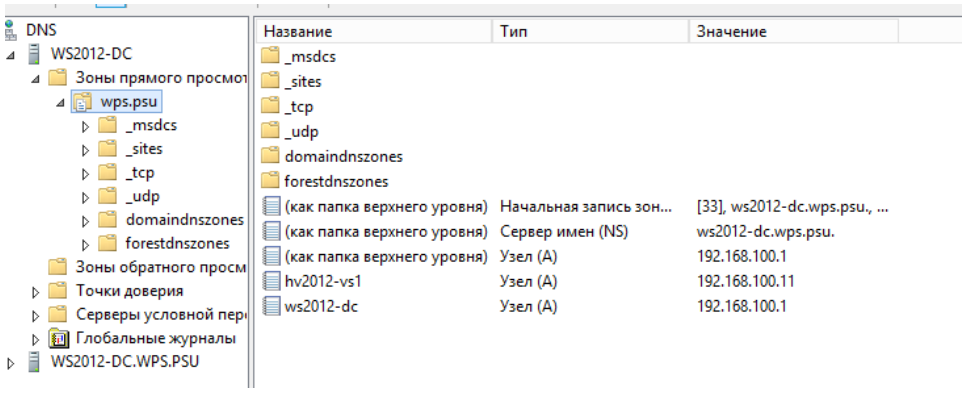


Рисунок 93 – Проверка Hyper-V сервера на контроллере домена

Необходимо проверить работу DNS-сервера. Для этого надо на сервере Hyper-V в командной строке запустить команду ping. В качестве параметра первоначально необходимо указать IP-адрес контроллера домена, затем его имя. Контроллер домена должен быть доступен (см. рисунок 94).

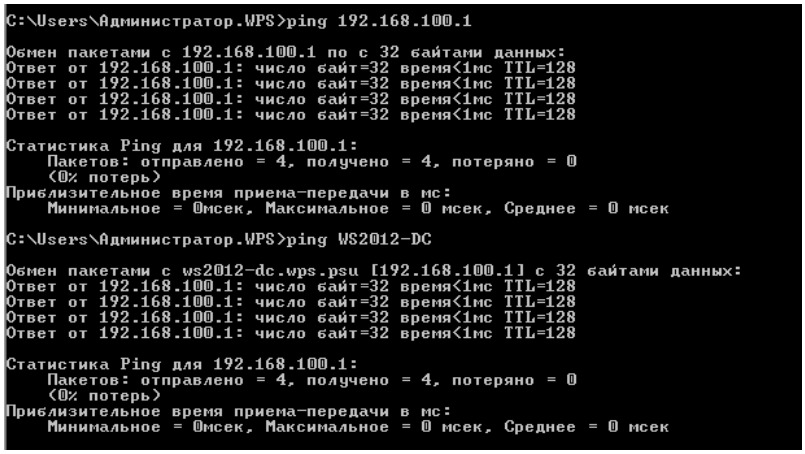


Рисунок 94 – Проверка работы DNS-сервера

Добавить сервер Hyper-V в домен, используя оболочку PowerShell. Для добавления надо выполнить команду «add-computer –domainname %DomainName% -cred %DomainName%\%UserName%». После выполнения этой команды появится диалоговое окно, в котором надо ввести пароль доменного администратора. Можно не использовать параметр –cred и вводить имя и пароль доменного администратора в диалоговом окне, которое появится после ввода команды (см. рисунок 95).

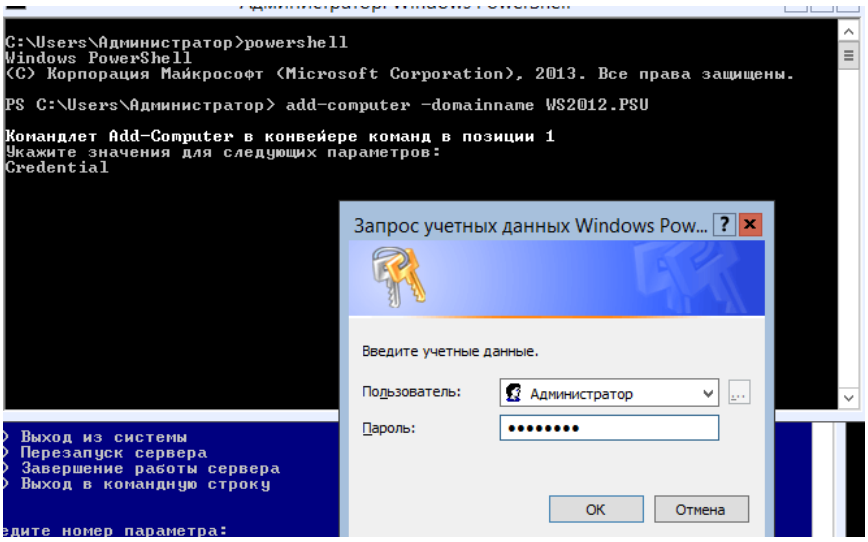


Рисунок 95 – Добавление сервера Hyper-V в домен

После завершения добавления сервера потребуется его перезагрузка. Для перезагрузки надо использовать командлет «restart-computer».

Для проверки надо запустить утилиту sconfig в командной строке. В качестве значения параметра 1 будет указано имя домена (см. рисунок 96).

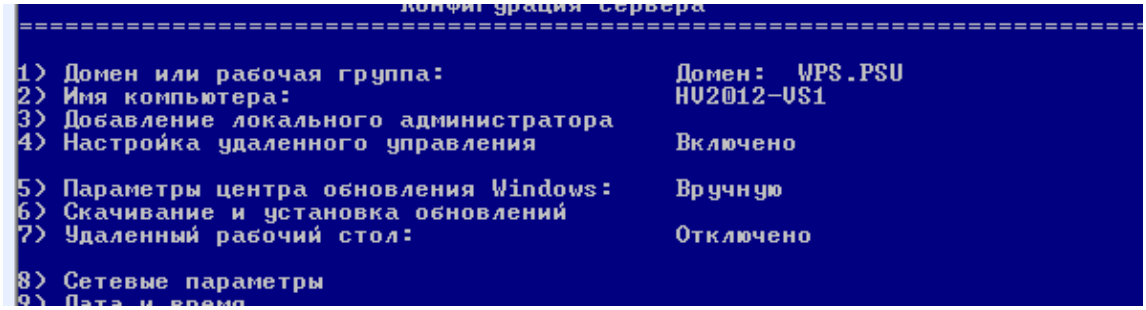


Рисунок 96 – Проверка сервера Hyper-V в домене с помощью утилиты sconfig

Для добавления второго гипервизора (ВМ) выполняются аналогичные действия.

Проверить возможность управления гипервизорами с контроллера домена. Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», выбрать выпадающий список команд «Средства», далее параметр «Active Directory – пользователи и компьютеры». В открывшемся окне выбрать пункт «Computers», далее нажать правой кнопкой мыши по серверу виртуализации HV2012-VS1, далее нажать на параметр «Управление» (см. рисунок 97).

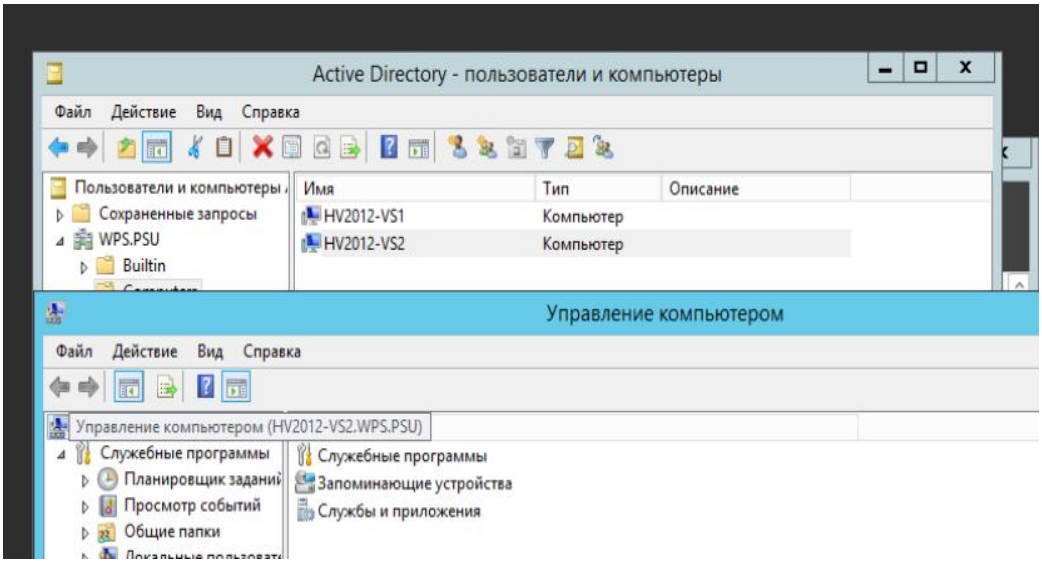


Рисунок 97 – Проверка управления гипервизора с контроллером домена

Аналогично проверить для сервера виртуализации HV2012-VS2 (см. рисунок 98).

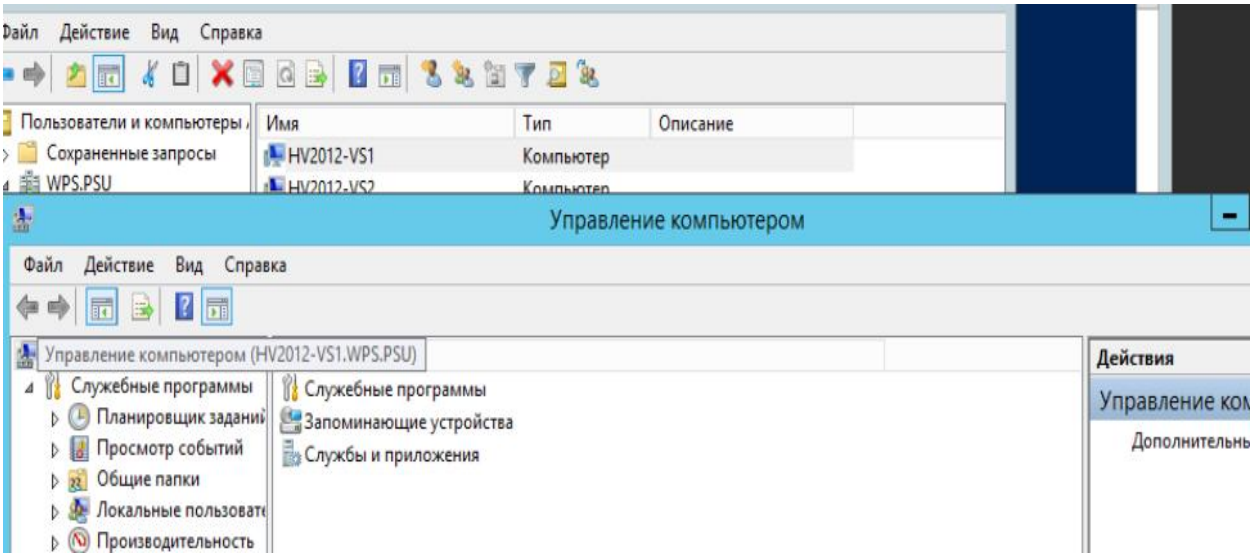


Рисунок 98 – Проверка управления гипервизора с контроллером домена

Таким образом, на контроллере домена WS2012-DC был создан домен Active Directory. ВМ1, ВМ2, ВМ3 были включены в этот домен. Все действия были выполнены успешны.

3.7 Установка компонентов ОС Windows Server, реализующих механизмы защиты виртуальных инфраструктур и средства администрирования

Установка роли управления сертификатами Active Directory. Установка этой роли выполняется только на компьютере (ВМ), которая является контроллером домена. Для установки роли необходимо запустить Диспетчер серверов и на панели мониторинга выбрать команду «Добавить роли и компоненты». Из списка ролей выбрать роль «Службы сертификатов Active Directory». На этапе выбора компонентов роли надо отметить только три компонента – Центр сертификации, Веб-служба политик регистрации сертификатов и Веб-служба регистрации сертификатов. Остальные компоненты не отмечать.

Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», выбрать выпадающий список команд «Управление», далее выбрать команду «Добавить роли и компоненты». Будет запущен мастер добавления ролей и компонентов. Нажать кнопку «Далее» до этапа «Роли сервера». Этапы «Тип установки» и «Выбор сервера» оставить по умолчанию. В этапе «Роли сервера» следует установить отметку в поле «Службы сертификатов Active Directory» (см. рисунок 99).

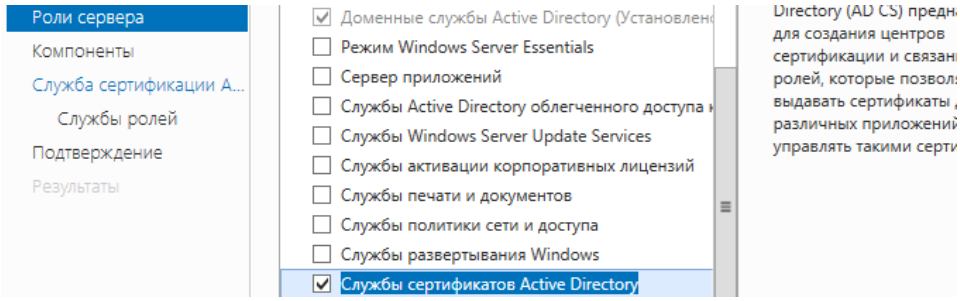


Рисунок 99 – Установка роли сервера «Службы сертификатов Active Directory»

Нажать кнопку «Далее» до этапа «Службы ролей». Этапы «Компоненты» и «Службы сертификации» оставить без изменений. На этапе «Служб ролей» поставить отметки в полях «Центр сертфиикации», «Веб-служба политик регистрации сертификатов», «Веб-служба регистрации сертификатов». Остальные компоненты не отмечать (см. рисунок 100).

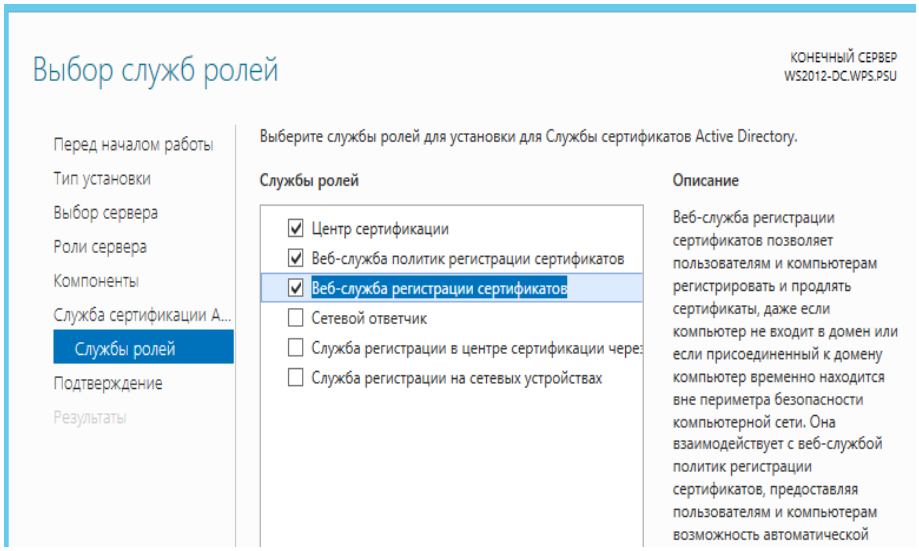


Рисунок 100 – Установка службы ролей Active Directory

После завершения установки отмеченных компонентов перейти по гиперссылке «Настроить службы сертификатов Active Directory на конечном сервере», которая активная на завершающем этапе установке компонентов (см. рисунок 101).

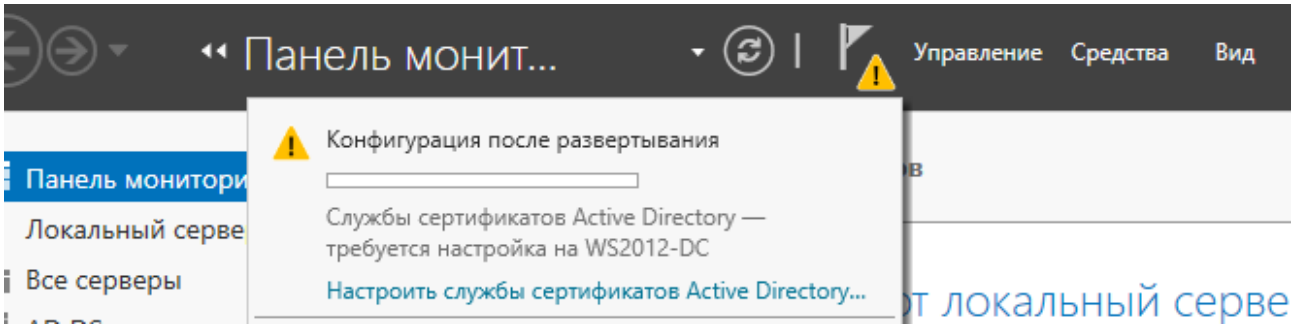


Рисунок 101 – Переход по гиперссылке «Настроить службы сертификатов Active Directory на конечном сервере»

Откроется диалоговое окно «Конфигурация службы сертификатов Active Directory».

Настройка выполняется следующим образом. На этапе «Учетные данные» все параметры надо оставить без изменения (см. рисунок 102).

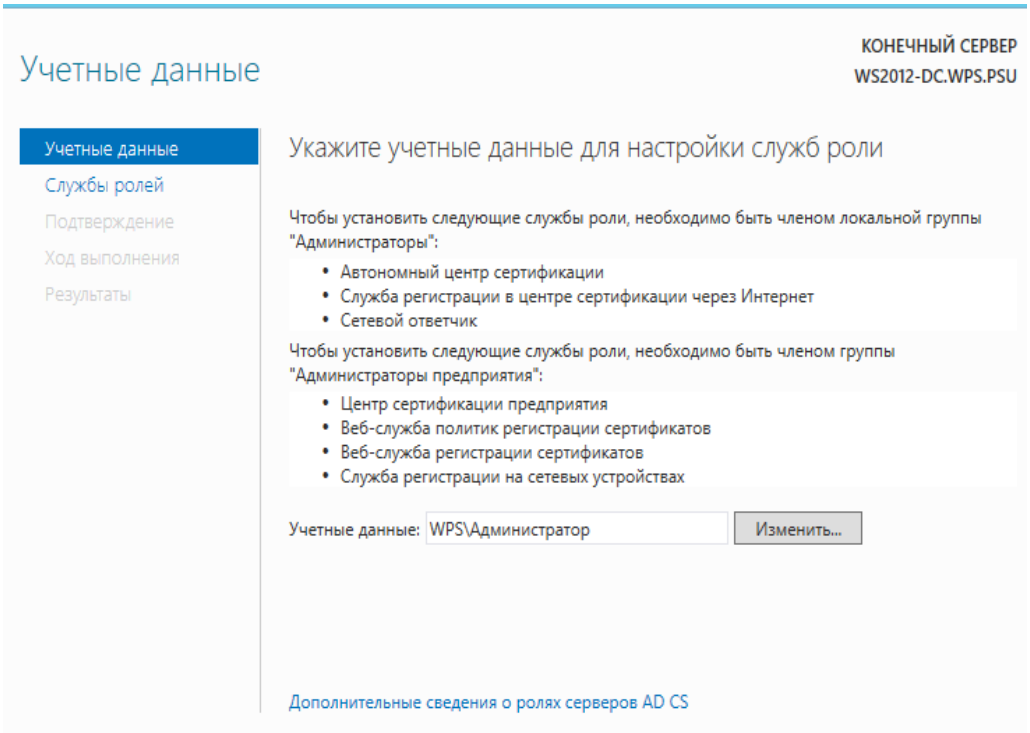


Рисунок 102 – Настройка учетных данных

На этапе «Службы ролей» надо отметить только службу Центр сертификации (см. рисунок 103).

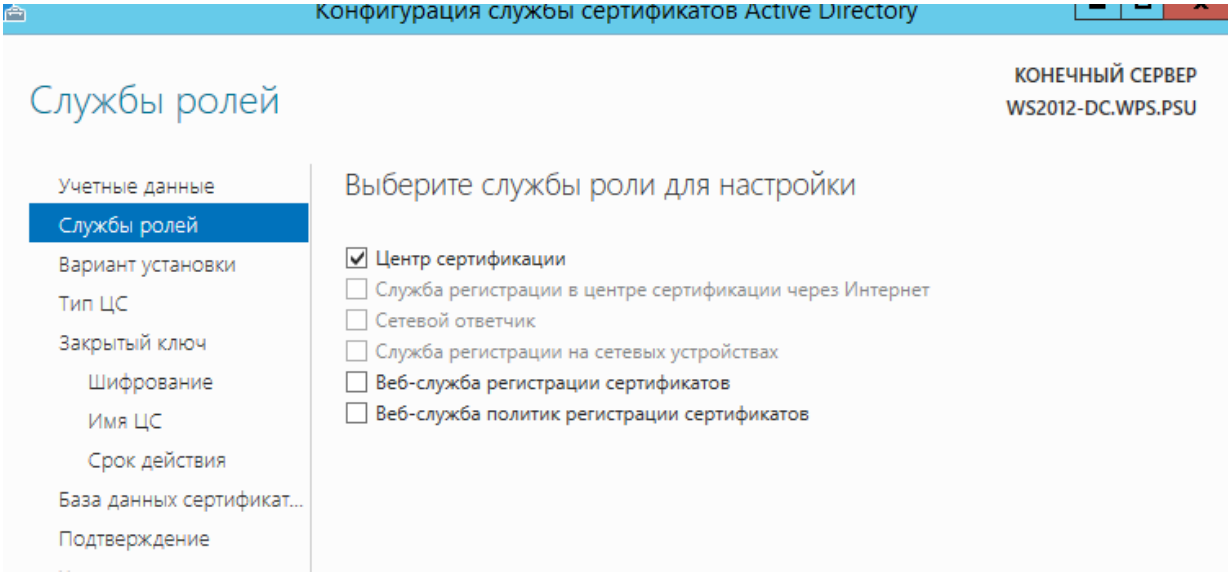


Рисунок 103 – Настройка службы ролей

На этапе «Вариант установки» надо выбрать ЦС предприятия (см. рисунок 104).

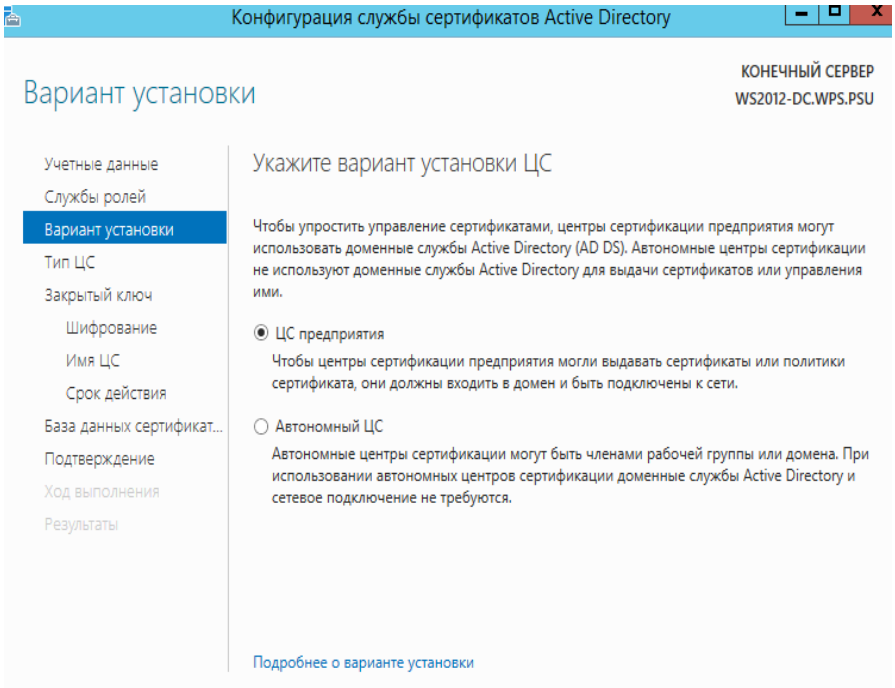


Рисунок 104 – Настройка варианта установки

На этапе «Тип ЦС» надо выбрать тип «Корневой ЦС» (см. рисунок 105).

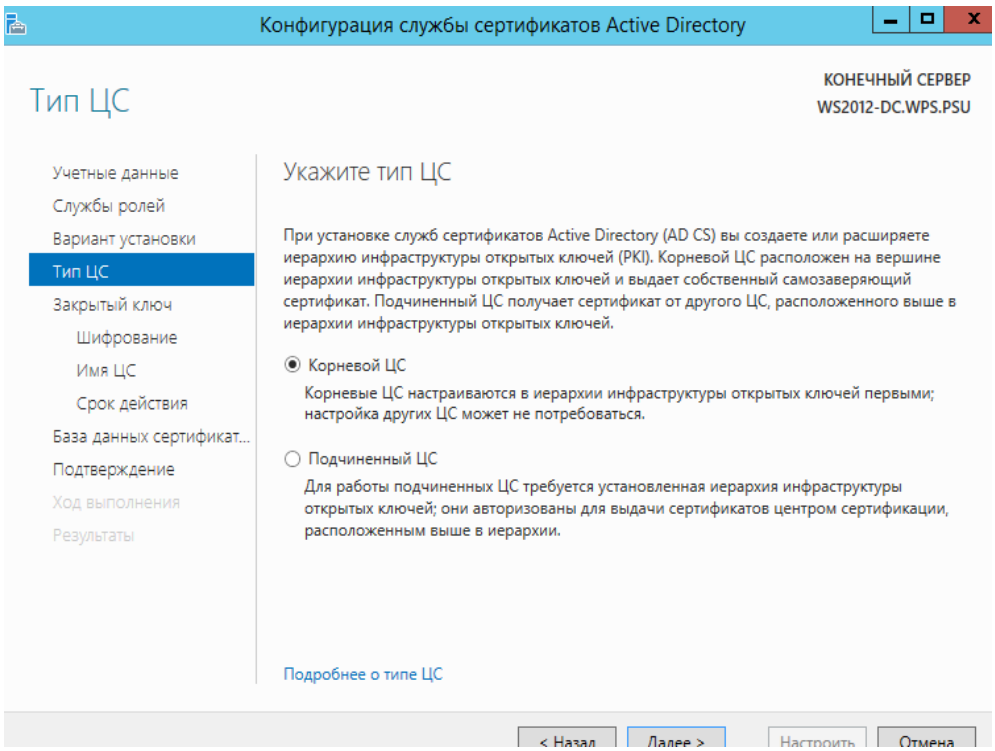


Рисунок 105 – Настройка типа ЦС

На этапе «Закрытый ключ» надо выбрать вариант настройки «Создать новый закрытый ключ» (см. рисунок 106).

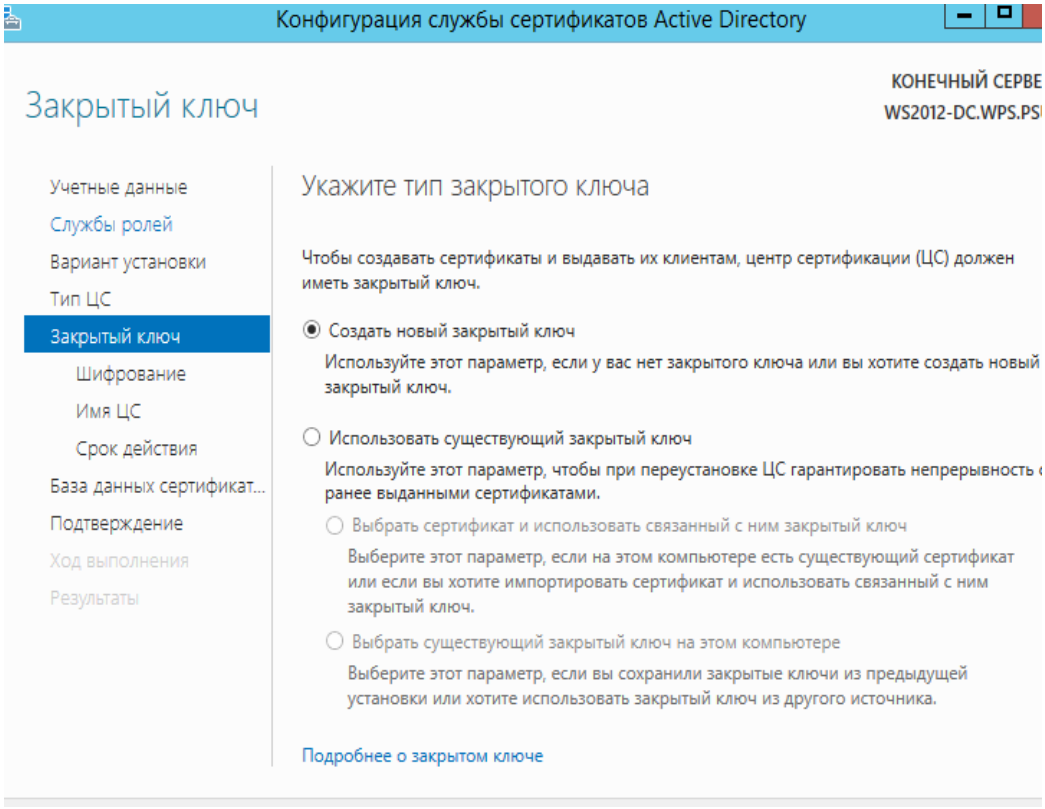


Рисунок 106 – Настройка закрытого ключа

На этапе «Шифрование для ЦС» оставить значения всех параметров без изменения (см. рисунок 107).

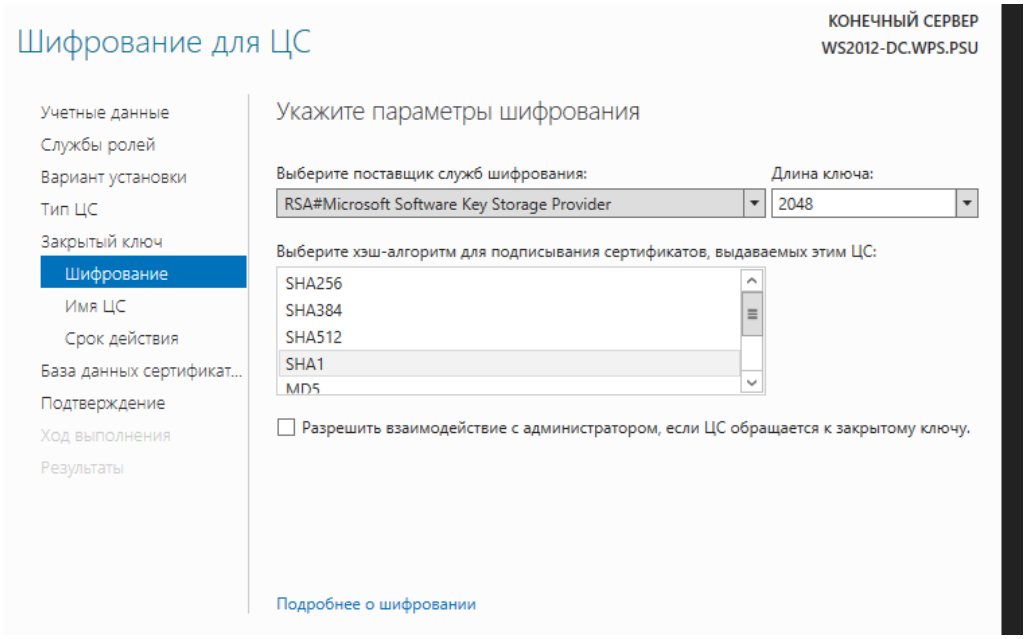


Рисунок 107 – Настройка шифрования для ЦС

На этапе «Имя ЦС» также значения всех параметров оставить без изменения (см. рисунок 108).

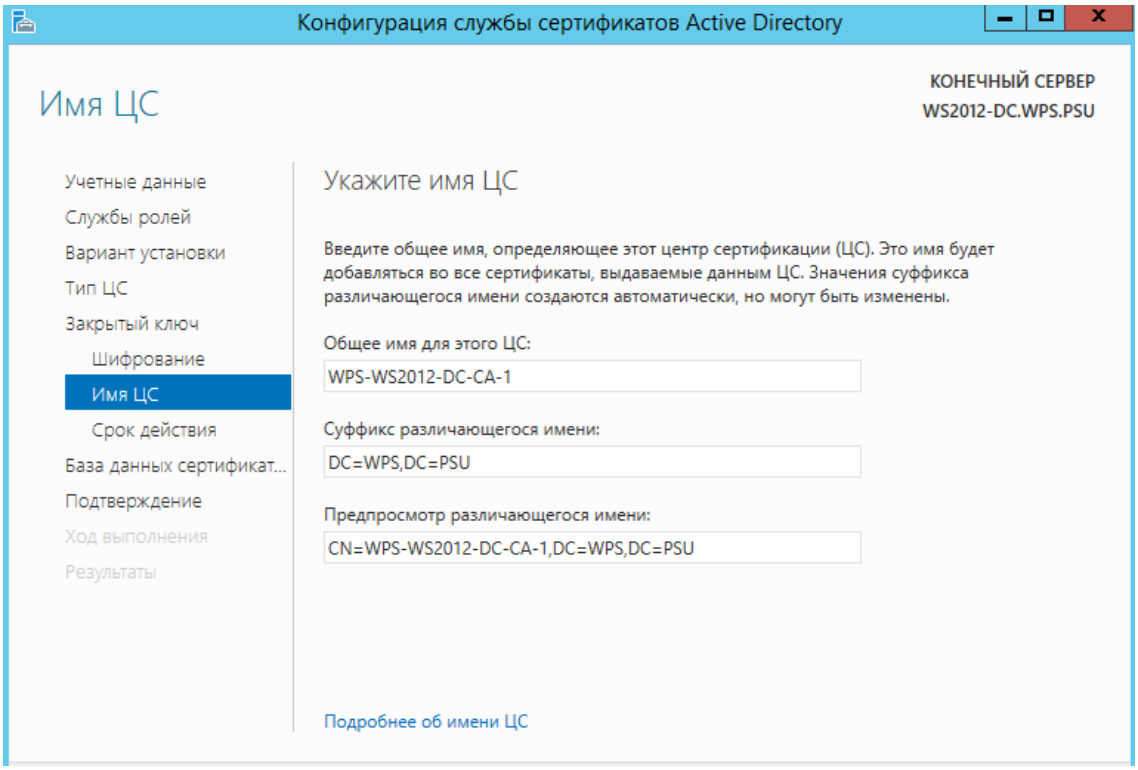


Рисунок 108 – Настройка имени ЦС

На этапе «Срок действия» все оставить без изменения (см. рисунок 109).

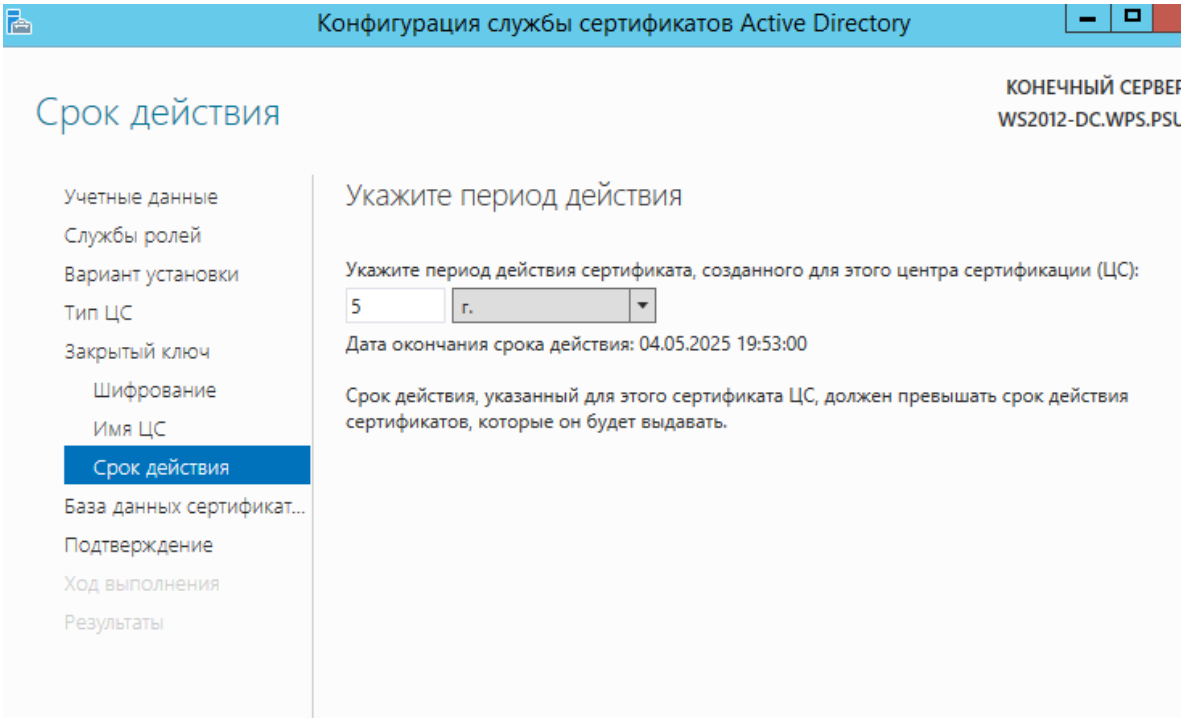


Рисунок 109 – Настройка срок действия сертификата

На этапе «База данных сертификатов» все параметры оставить без изменения (см. рисунок 110).

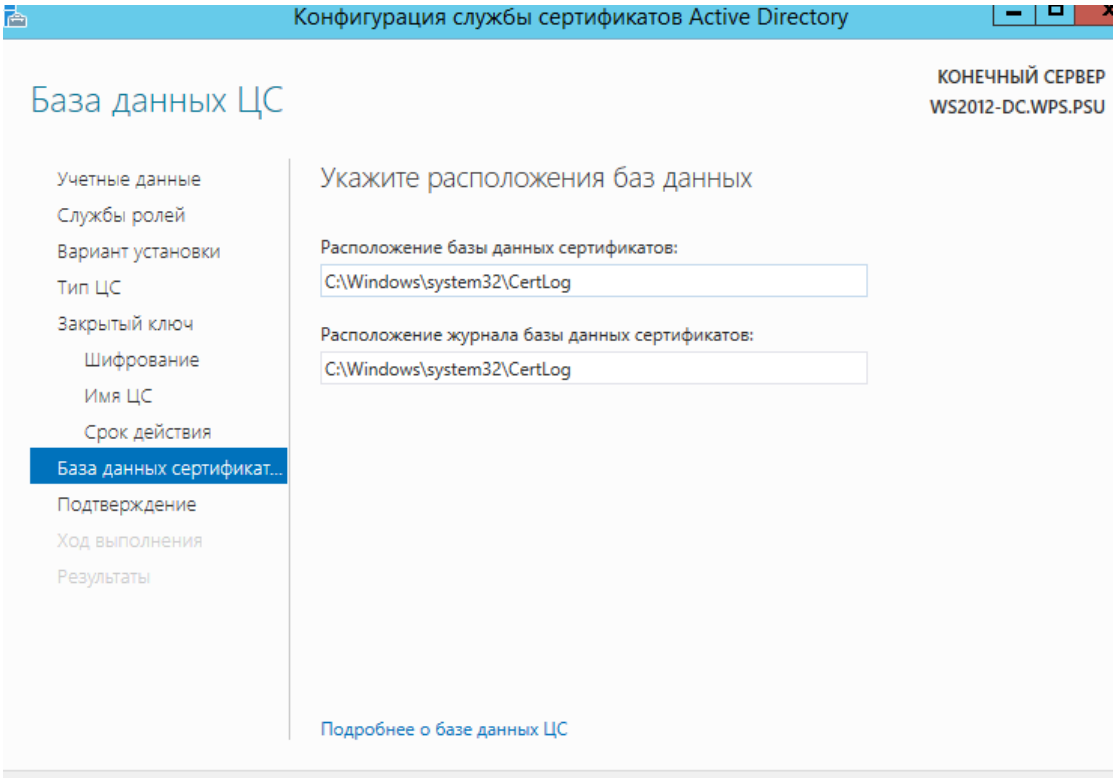


Рисунок 110 – Настройка базы данных сертификатов

На этапе «Подтверждение» нажать кнопку «Настроить» (см. рисунок 111).

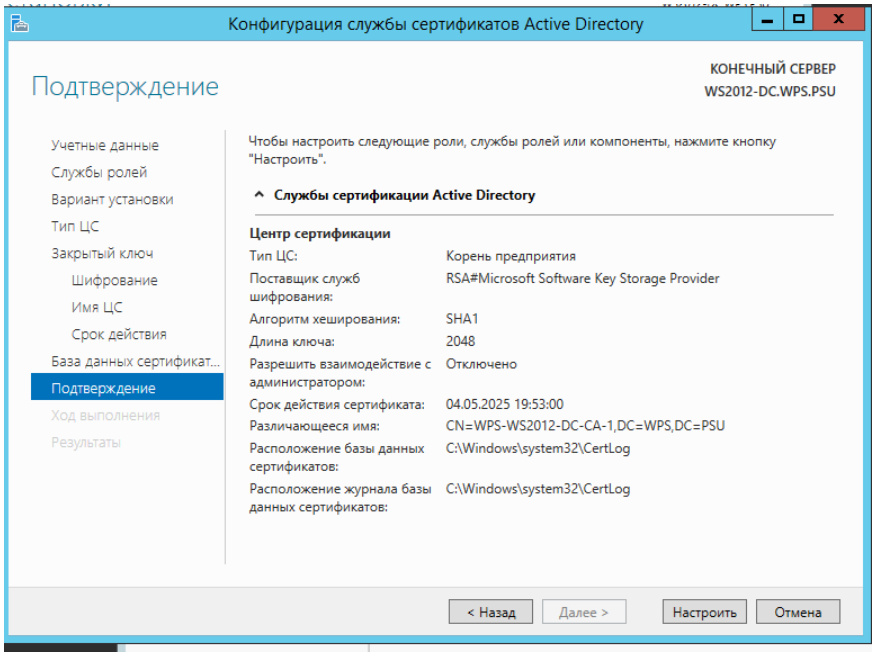


Рисунок 111 – Подтверждение настройки ролей или компонентов

После завершения настройки нажать кнопку «Завершить» и в запросе на настройку дополнительных служб ролей нажать кнопку «Да» (см. рисунок 112).

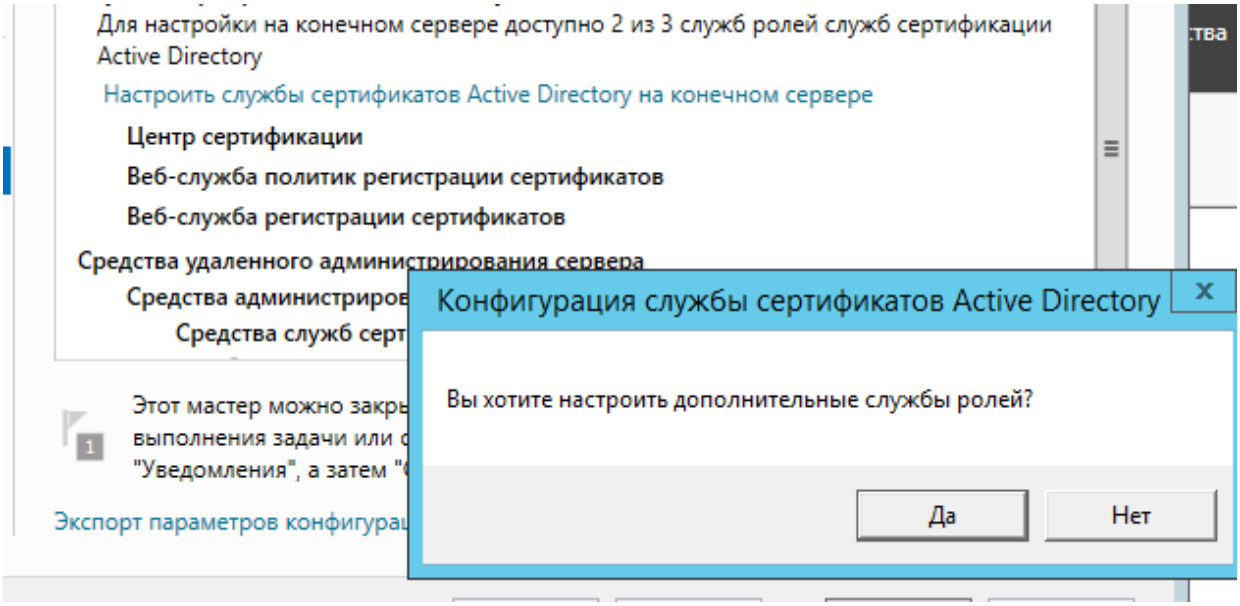


Рисунок 112 – Настройка дополнительных служб ролей

На следующем этапе настраиваются веб-службы. На этапе настройки учетных данных все параметры оставить без изменения (см. рисунок 113).

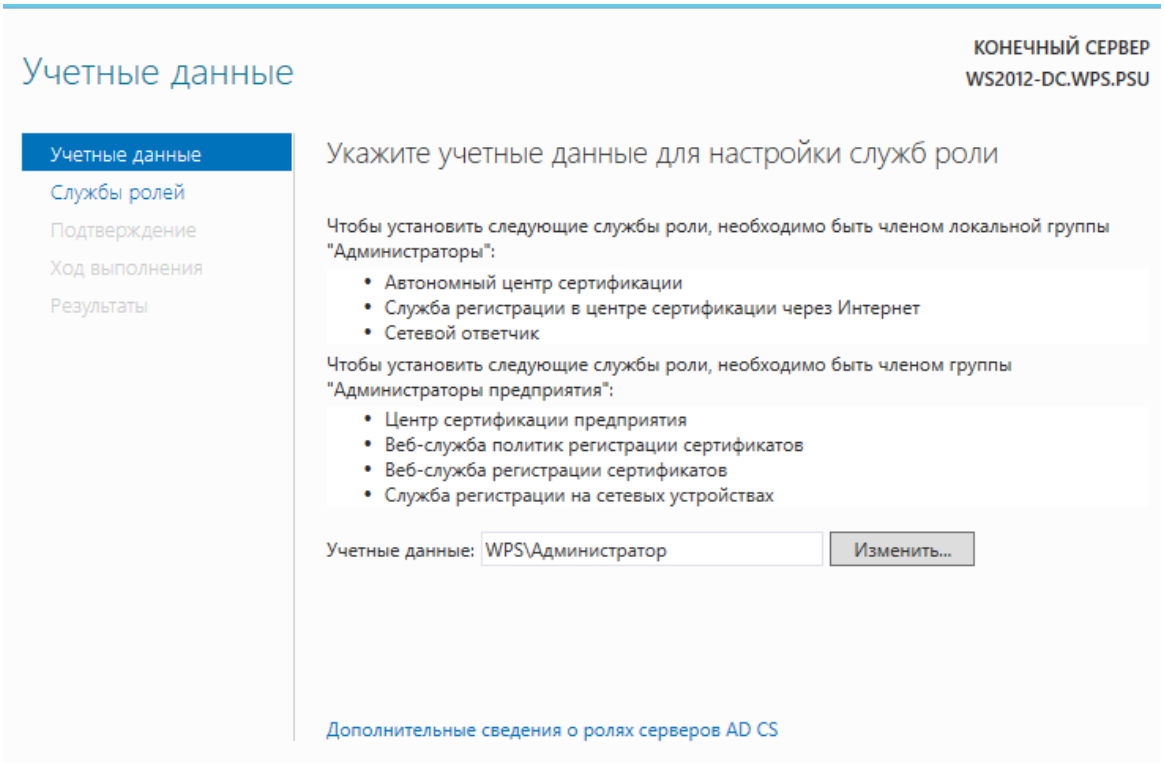


Рисунок 113 – Настройка учетных данных

На этапе «Службы ролей» отметить две службы – Веб-служба политик регистрации сертификатов и Веб-служба регистрации сертификатов (см. рисунок 114).

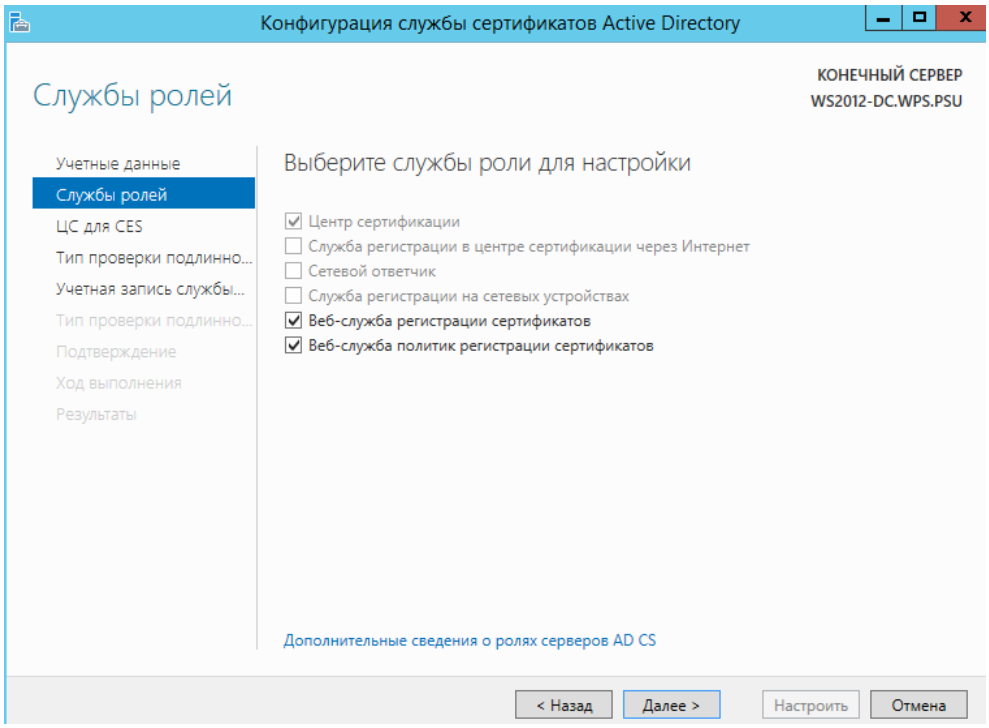


Рисунок 114 – Настройка службы ролей

На этапе ЦС для CES значения параметров оставить без изменения (см. рисунок 115).

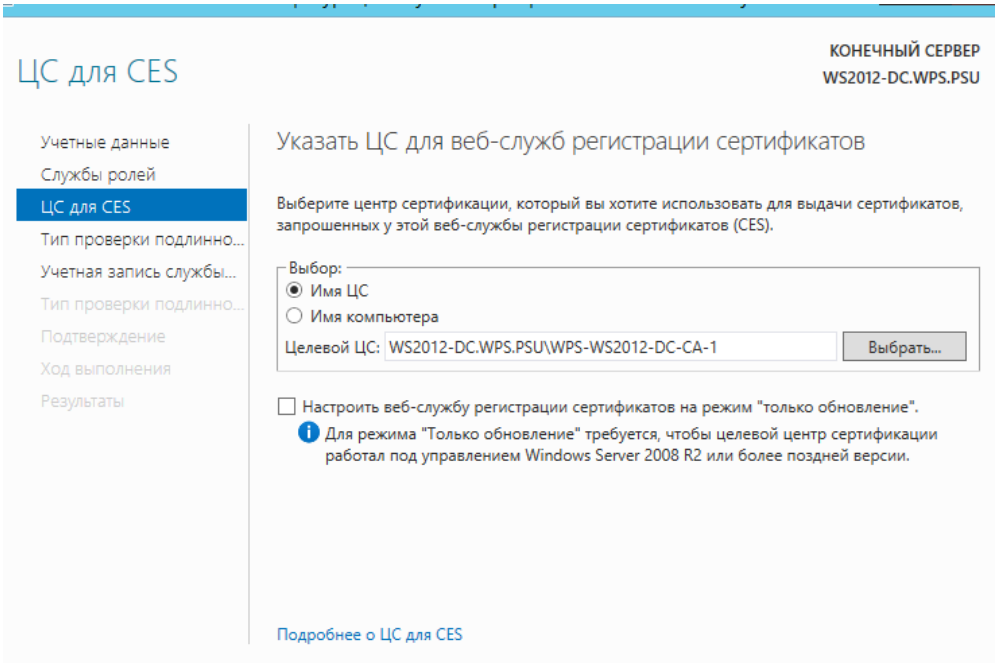


Рисунок 115 – Настройка ЦС для CES

На этапе Тип проверки подлинности для службы CES выбрать вариант Встроенная проверка подлинности Windows (см. рисунок 116).

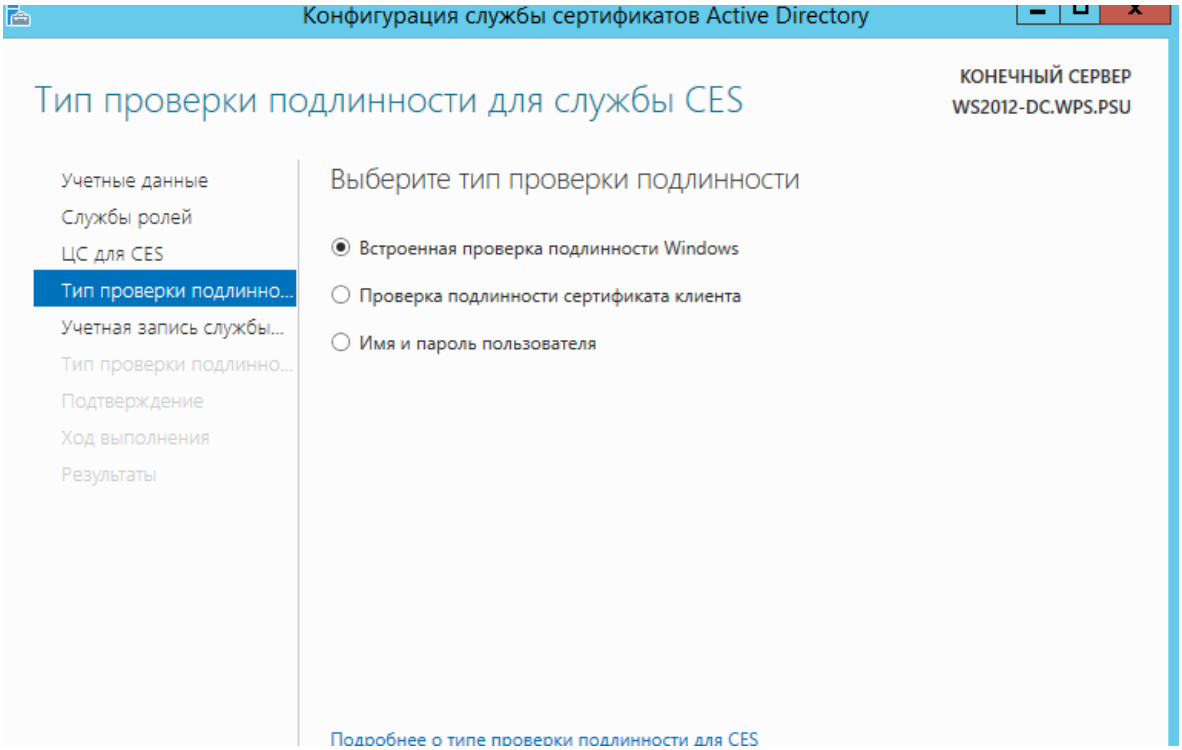


Рисунок 116 – Настройка типа проверки подлинности для службы CES

На этапе Учетная запись службы CES надо указать имя учетной записи доменного администратора. Предварительно его учетную запись надо включить в группу IIS_IUSRS. Для этого в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», выбрать выпадающий список команд «Средства», далее выбрать команду «Пользователи компьютеры Active Directory». Открыть домен в левой панели. Раскроется список контейнеров. Нажать на контейнер «Users», выбрать учетную запись доменного администратора, щелкнув правой клавишей мыши. В контекстном меню выбрать команду «Добавить в группу…». В диалоговом окне «Выбор: «Группы»» нажать кнопку «Дополнительно», затем кнопку «Поиск». В списке групп надо выбрать группу IIS_IUSRS и нажать кнопку «ОК» для подтверждения выбора (см. рисунок 117).

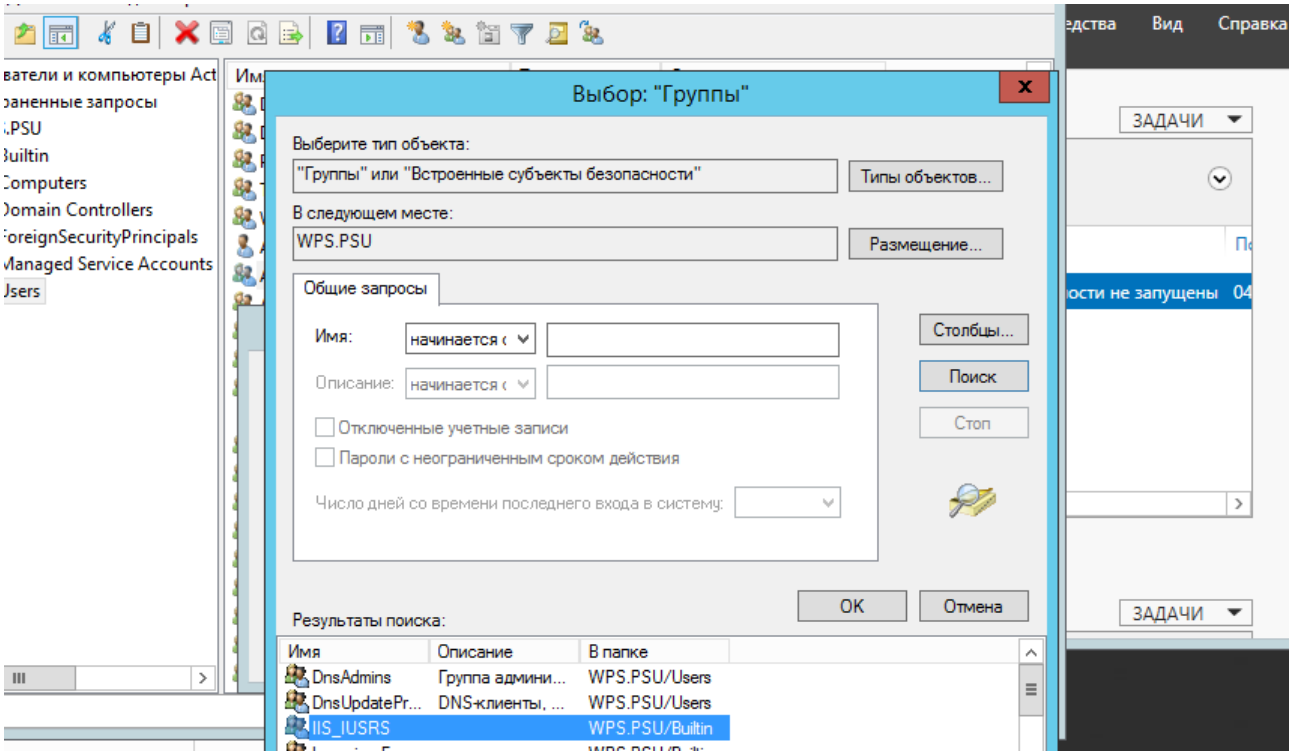


Рисунок 117 – Добавление доменного администратора в группу

Затем еще раз нажать кнопку «ОК» для добавления в группу учетной записи доменного администратора. Появится сообщение об успешном добавлении учетной записи в группу (см. рисунок 118).

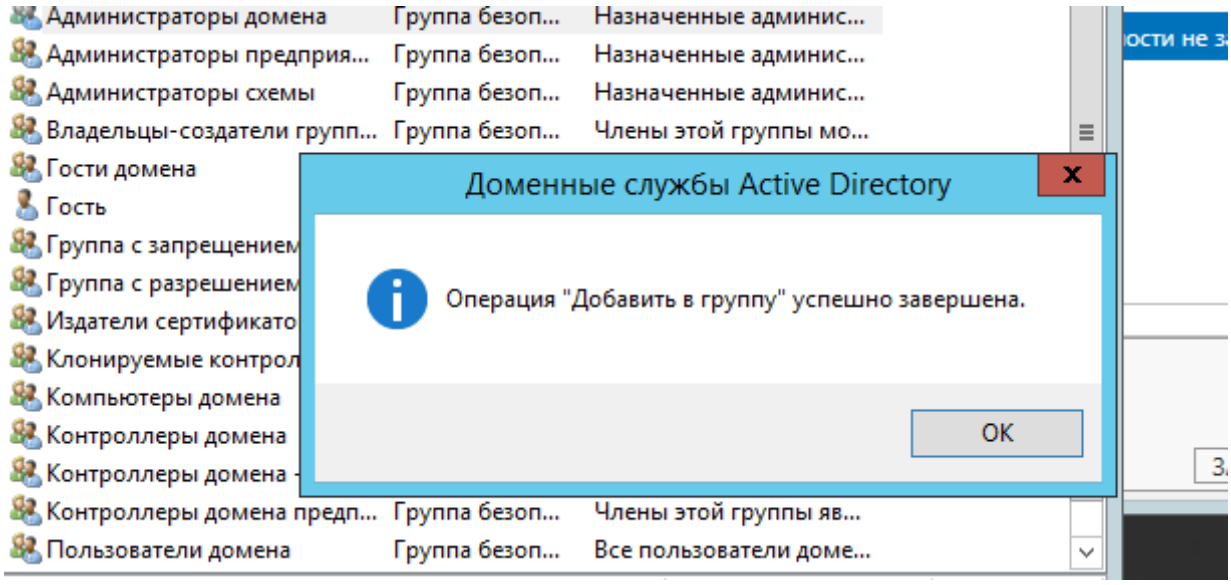


Рисунок 118 – Завершение добавления доменного администратора в группу

После добавления учетной записи доменного администратора в группу IIS_IUSRS закрыть консоль Пользователи компьютеры Active Directory.

После добавления учетной записи доменного администратора в группу IIS_IUSRS закрыть консоль «Пользователи компьютеры Active Directory». На этапе «Учетная запись службы CES» надо нажать кнопку «Выбрать». В диалоговом окне «Безопасность Windows» ввести имя учетной записи доменного администратора, например, WPS\Администратор и его пароль. После появления имени учетной записи доменного администратора в соответствующей строке нажать кнопку «Далее» (см. рисунок 119).

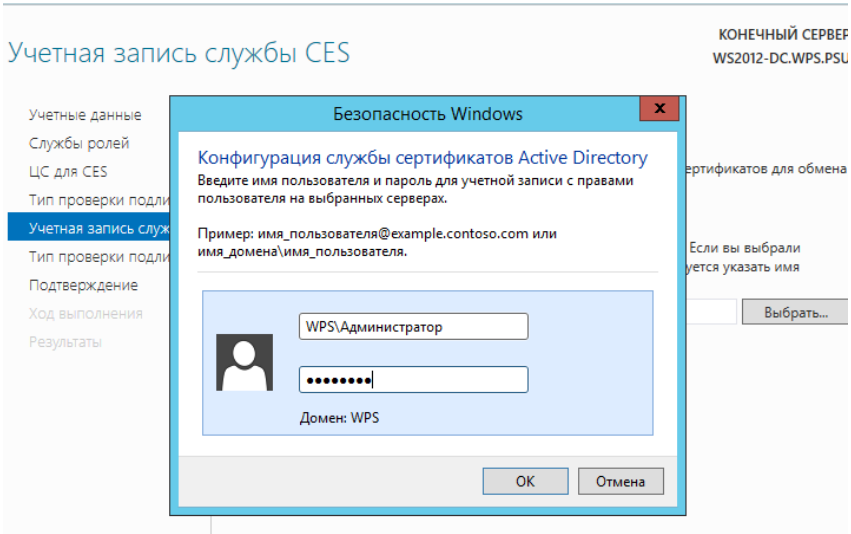


Рисунок 119 Настройка учетной записи службы CES

На этапе Тип проверки подлинности для службы CEP выбрать вариант Встроенная проверка подлинности Windows (см. рисунок 120).

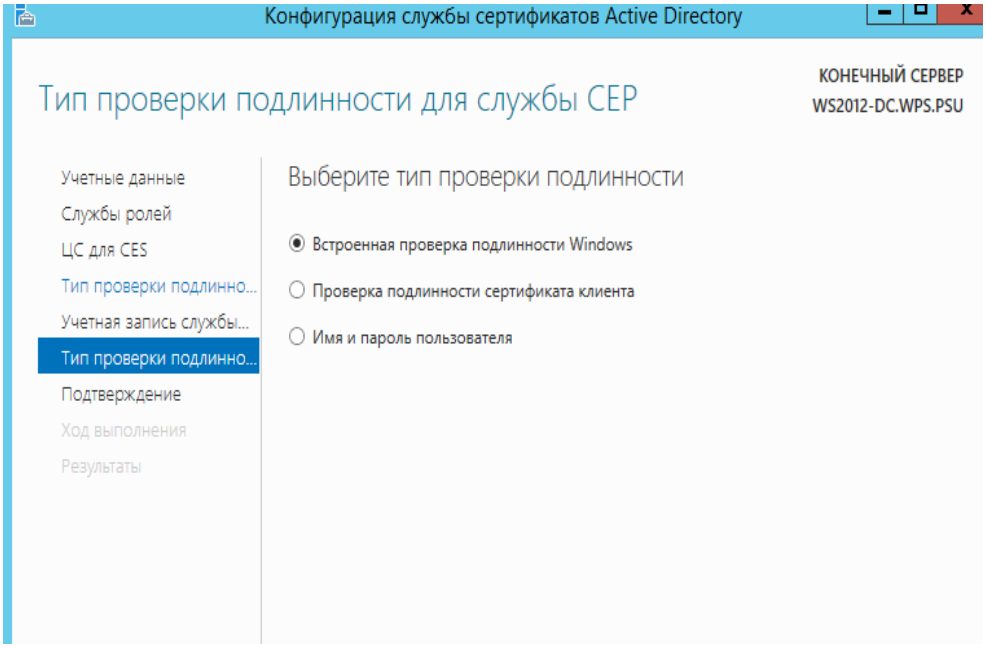


Рисунок 120 Настройка типа проверки подлинности для службы CEP

На этапе Сертификат сервера выбрать вариант «Выбрать существующий сертификат для шифрования SSL (рекомендуется)». В списке сертификатов выбрать тот, у которого срок действия 5 лет. Обычно он первый в списке.

На этапе «Подтверждение» нажать кнопку «Настроить». После завершения настройки закрыть это диалоговое окно и окно мастера добавления ролей и компонентов.

Далее в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», выбрать выпадающий список команд «Управление», далее выбрать команду «Добавить роли и компоненты». Будет запущен мастер добавления ролей и компонентов. Нажать кнопку «Далее» до этапа «Роли сервера». Этапы «Тип установки» и «Выбор сервера» оставить по умолчанию. На этапе добавления ролей выбрать роль «Службы сертификатов Active Directory (Установлено 3 из 6)», щелкнув левой клавишей мыши по отметке слева для раскрытия списка компонентов и отметить оставшиеся три компонента – «Сетевой ответчик», «Служба регистрации в центре

сертификации через Интернет», «Служба регистрации на сетевых устройствах» (см. рисунок 121).

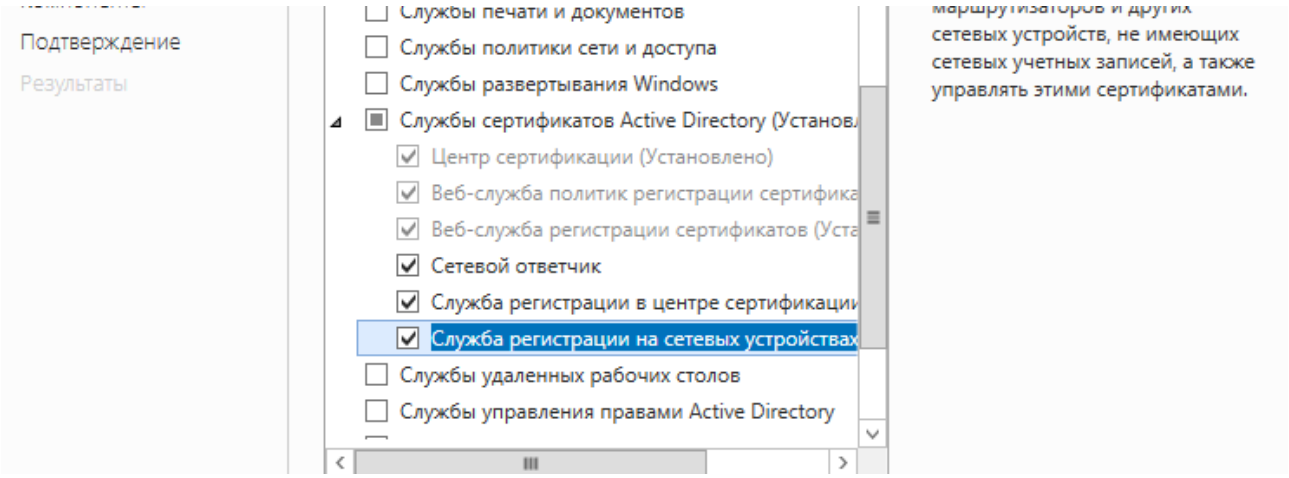


Рисунок 121 - Настройка службы сертификатов

При появлении диалогового окна добавления компонентов нажать кнопку «Добавить компоненты». На этапе «Подтверждение» мастера установки ролей и компонентов нажать кнопку «Установить».

После завершения установки компонентов роли требуется их настройка. Для настройки надо перейти по гиперссылке «Настроить службы сертификатов Active Directory на конечном сервере», которая отображается в диалоговом окне хода установке на этапе «Результаты» (см. рисунок 122).

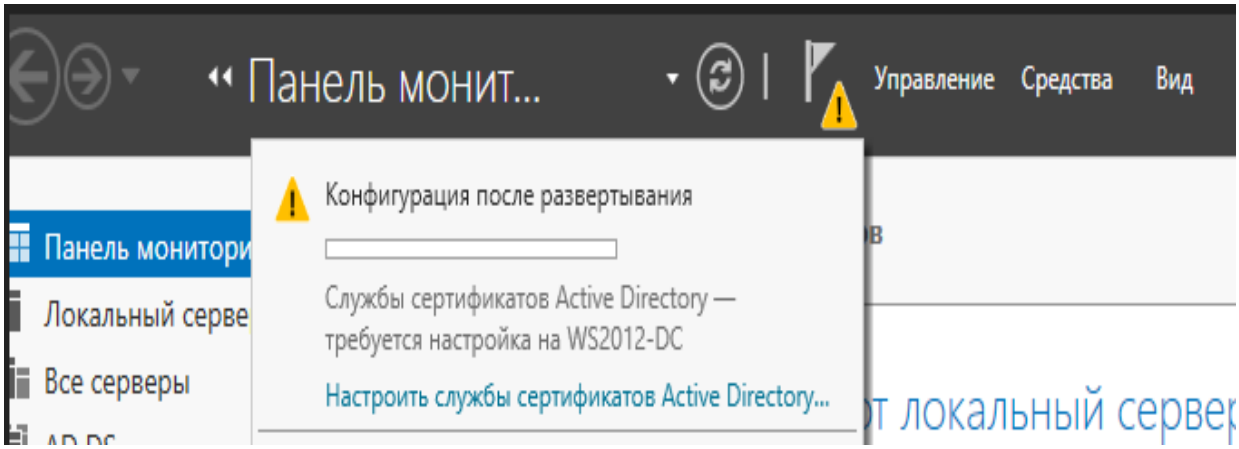


Рисунок 122 - Переход по гиперссылке «Настроить службы сертификатов Active Directory на конечном сервере»

Настройка выполняется следующим образом. На этапе настройки учетных данных все параметры надо оставить без изменения (см. рисунок 123).

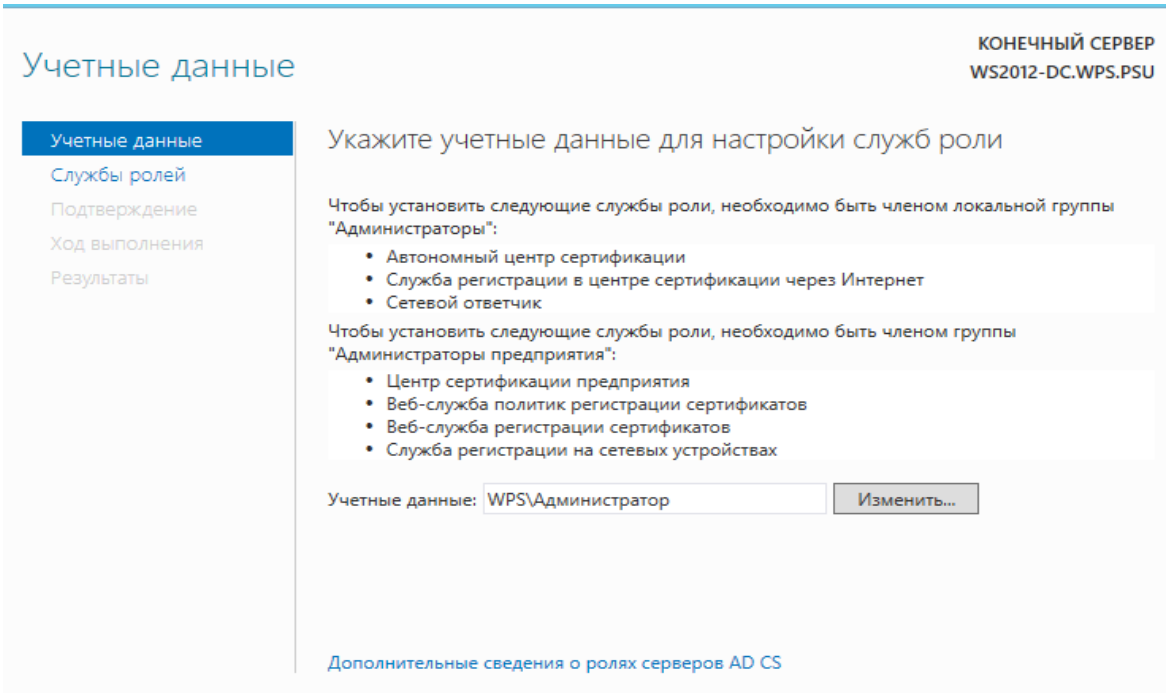


Рисунок 123 – Настройка учетных данных

На этапе Службы ролей надо отметить службы: «Служба регистрации в центре сертификации через Интернет», «Сетевой ответчик», «Служба регистрации на сетевых устройствах» (см. рисунок 124).

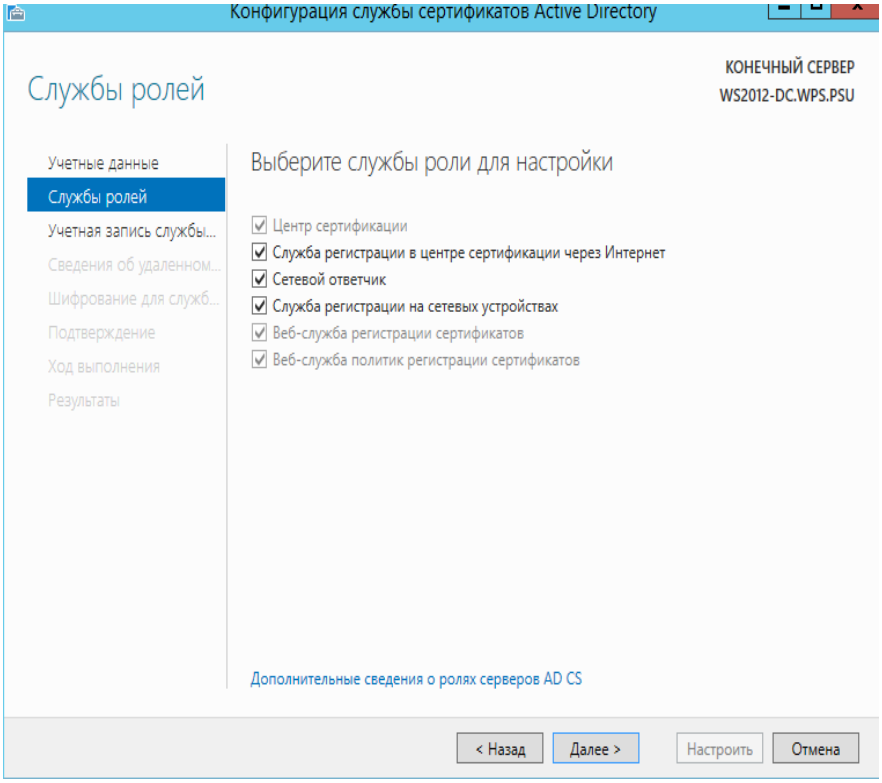


Рисунок 124 – Настройка службы ролей

На этапе «Учетная запись службы NDES» нажать кнопку «Выбрать» и выбрать учетную запись доменного администратора, так как она входит в группу IIS_IUSRS, указав имя учетной записи и ее пароль (см. рисунок 125).

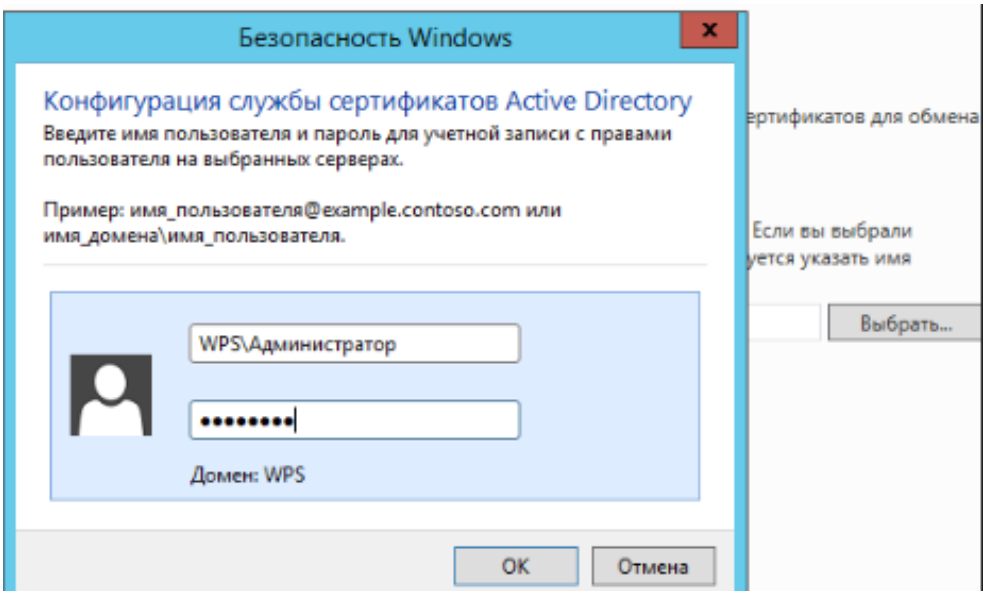


Рисунок 125 – Настройка учетной записи службы NDES

На этапе «Сведения об удаленном помощнике» обязательные сведения оставить без изменения. Необязательные можно не заполнять (см. рисунок 126).

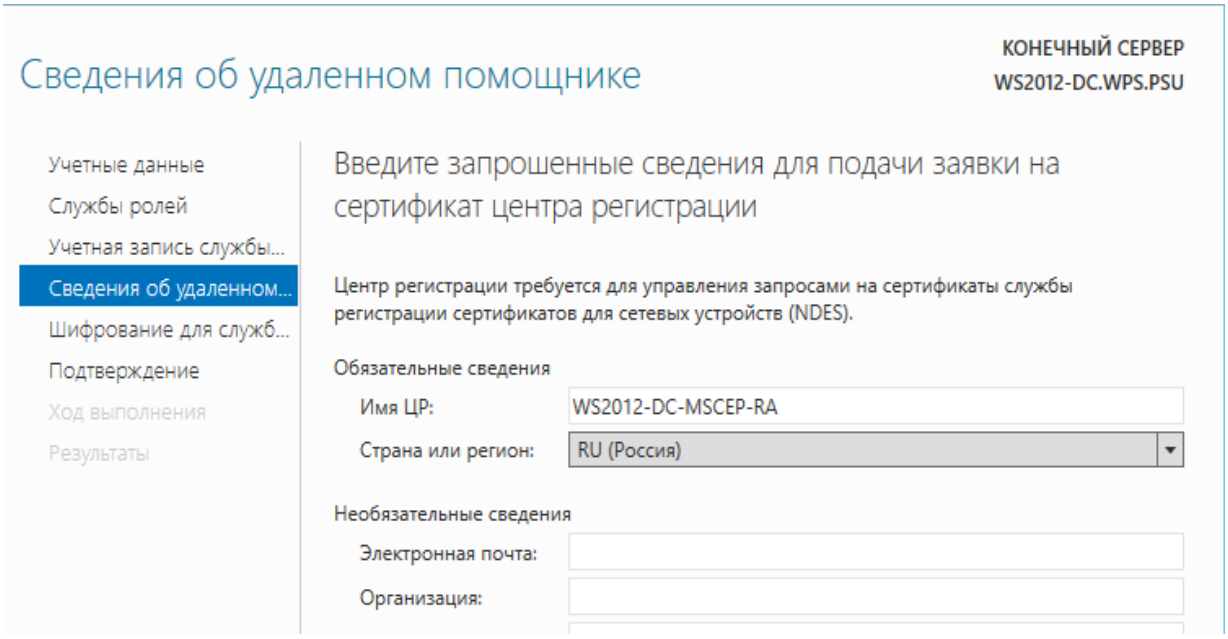


Рисунок 126 – Настройка сведений об удаленном помощнике

На этапе «Шифрование для службы NDES» значения всех параметров оставить без изменения (см. рисунок 127).

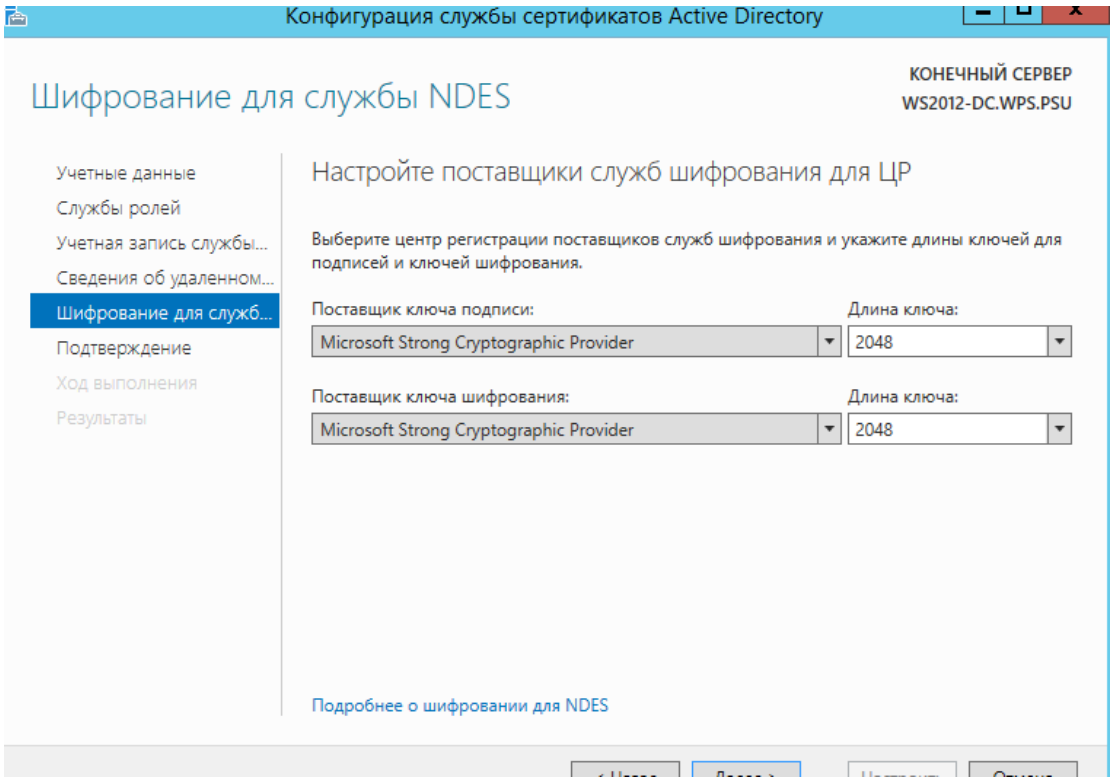


Рисунок 127 – Настройка шифрования для службы NDES

На этапе «Подтверждение» нажать кнопку «Настроить». На этапе «Результаты» нажать кнопку «Закрыть» и также закрыть мастер установки ролей и компонентов нажав кнопку «Закрыть» (см.рисунок 128).

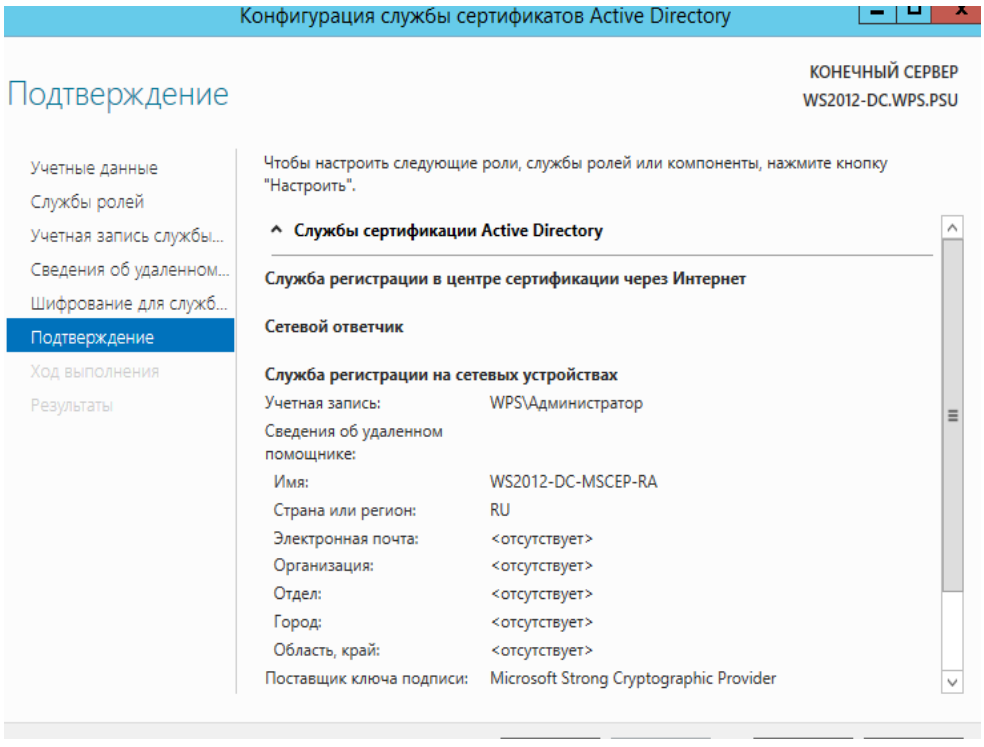


Рисунок 128 – Настройка ролей, службы ролей и компонентов

После установки роли Службы сертификатов Active Directory в диспетчере задач на панели инструментов нажать кнопку «Средства» и в выпадающем списке программ управления выбрать программу «Центр сертификации». Отобразится работающий центр сертификации. Надо открыть его структуру и выбрать раздел «Выданные сертификаты». В правой части окна консоли должен отобразиться список созданных сертификатов (см. рисунок 129).

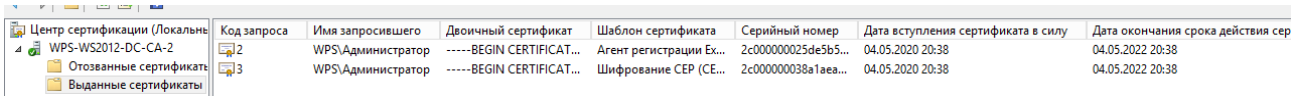


Рисунок 129 – Список созданных сертификатов

Таким образом, были установлены компоненты ОС Windows Server, реализующих механизмы защиты виртуальных инфраструктур и средства администрирования. Была установлена роль управления сертификатами Active Directory, которая необходима для надежной аутентификации, создания SSL-соединений. К ней относится установка центра сертификации - компонента глобальной службы каталогов, отвечающего за управление криптографическими ключами пользователей. Установлены веб-службы регистрации сертификатов и веб-службы политик регистрации сертификатов, которые позволяют запрашивать сертификаты пользователями без участия администратора, а также предоставлять по требованию сертификат корневого центра сертификации. Установлена служба регистрации в центре сертификации через Интернет, позволяющая получать сертификаты через веб-браузер. Установлен сетевой ответчик - доверенный сервер, получающий от отдельных клиентов запросы состояния сертификата и отвечающего на них. Установлена служба регистрации сетевых устройств, с помощью которого программное обеспечение на маршрутизаторах и других сетевых устройствах, работающих без использования учетных данных домена, может получать сертификаты на основе протокола SCEP.

4 Порядок выполнения практического задания по теме «Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»

Настройка гипервизора. Для того, чтобы узнать на каком узле запущена виртуальная машина используется командлет `Get-VMHost`. Для этого необходимо запустить командлет `Get-VMHost` в оболочке Powershell. Для того чтобы перейти в эту оболочку нужно ввести команду «Powershell» в командной строке (см. рисунок 130).

Рисунок 130– Проверка запуска виртуальной машины на определенном узле

Для просмотра установленной роли Hyper-V на виртуальной машине нужно использовать параметр `-ComputerName` командлета `GetVMHost`. Например, если необходимо посмотреть установлена ли роль Hyper-V на виртуальной машине HV2012-VS2, то необходимо выполнить команды, указанные на рисунке 131.

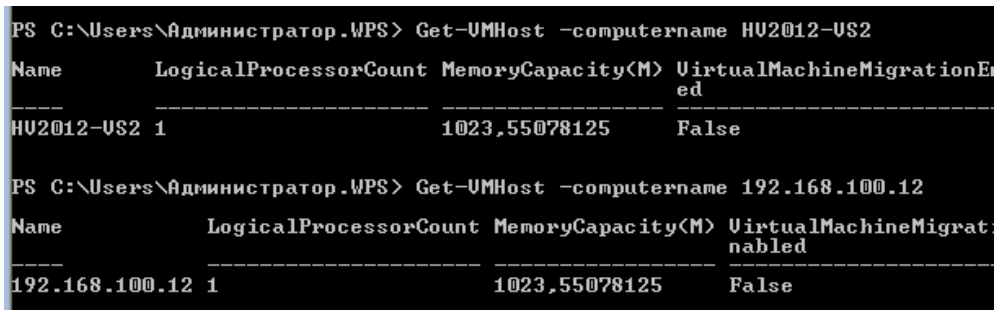


Рисунок 131 – Проверка установки роли Hyper-V на виртуальной машине HV2012-VS2

Основными параметрами командлета `Get-VMHost` являются следующие:

– ComputerName – определяет один или более серверов Hyper-V на которых создаются виртуальные жесткие диски. В качестве значения параметра можно указывать имена NetBIOS, IP адреса или полностью определенные доменные имена (FQDN, fully qualified domain name). По умолчанию значением параметра является имя локального компьютера. Для явного определения локального компьютера можно использовать значение localhost или точку (.);

– Credential – определяет одну или более учетных записей пользователей, которые имеют разрешение на выполнение этого действия. По умолчанию это учетная запись текущего пользователя;

– CimSession – запускает командлет на выполнение в удаленной сессии или на удаленном компьютере. Надо ввести имя компьютера или объекта сессии, такого как результат выполнения командлетов New-CimSession или Get-CimSession. По умолчанию используется текущая сессия на локальном компьютере.

Для того, что настроить хост Hyper-V используется командлет Set-VMHost.

Пример команды, которая настраивает локальный хост Hyper-V, чтобы разрешить 10 одновременных миграций в реальном времени и миграцию хранилища (см. рисунок 132).

Рисунок 132 – Настройка локального хоста Hyper-V с разрешением 10 одновременных миграций в реальном времени и миграцию хранилища

Значение параметра –MaximumVirtualMachineMigrations задает максимальное количество динамических миграций, которые могут быть выполнены одновременно на хосте Hyper-V, значение параметра -MaximumStorageMigrations задает максимальное количество миграций хранилища, которое может быть выполнено одновременно на хосте Hyper-V.

Пример команды, которая разрешает использование любой сети для входящих миграций в реальном времени на локальном хосте Hyper-V (см. рисунок 133).

Рисунок 133 – Настройка использования любой сети для входящих миграций в реальном времени на локальном хосте Hyper-V

Значение параметра `-UseAnyNetworkForMigrations` определяет, как сети выбираются для входящего трафика прямой миграции.

В этом примере задаются новые расположения по умолчанию для виртуальных жестких дисков и виртуальных машин на локальном узле Hyper-V. (см. рисунок 134).

Рисунок 134 – Задание новых расположений по умолчанию для виртуальных жестких дисков и виртуальных машин на локальном узле Hyper-V

Значение параметра `-VirtualHardDiskPath` указывает папку по умолчанию для хранения виртуальных жестких дисков на хосте Hyper-V, значение параметра –VirtualMachinePath указывает папку по умолчанию для хранения файлов конфигурации виртуальной машины на хосте Hyper-V.

В этом примере настраиваются параметры хоста Fibre Channel на локальном хосте Hyper-V (см. рисунок 135).

Рисунок 135 – Настройка параметров хоста Fibre Channel на локальном хосте Hyper-V

Значение параметра `-FibreChannelWwnn` указывает значение по умолчанию для имени узла на хосте Hyper-V, значение параметра `-FibreChannelWwpnMaximum` задает максимальное значение, которое можно использовать для создания глобальных имен портов на хосте Hyper-V, значение параметра `-FibreChannelWWpnMinimum` задает минимальное

значение, которое можно использовать для генерации глобальных имен портов на хосте Hyper-V.

В этом примере отключается связывание NUMA на локальном хосте Hyper-V (см. рисунок 136).

Рисунок 136 – Отключение связывания NUMA на локальном хосте Hyper-V

Значение параметра `-NumaSpanningEnabled` указывает, могут ли виртуальные машины на хосте Hyper-V использовать ресурсы из более чем одного узла NUMA.

В этом примере настраивается локальный хост Hyper-V для сохранения данных, которые отслеживают потребление ресурсов каждые полтора часа (см. рисунок 137).

Рисунок 137 – Настройка локального хоста Hyper-V для сохранения данных, которые отслеживают потребление ресурсов каждые полтора часа

Значение параметра `-ResourceMeteringSaveInterval` указывает, как часто хост Hyper-V сохраняет данные, которые отслеживают использование ресурсов.

В этом примере настраивается локальный хост Hyper-V для использования Kerberos, который является сетевым протоколом аутентификации, который предлагает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними для проверки подлинности входящих миграций (см. рисунок 138).

Рисунок 138 – Настройка локального хоста Hyper-V для использования Kerberos для проверки подлинности входящих миграций

Параметр `-VirtualMachineMigrationAuthenticationType` определяет тип аутентификации, который будет использоваться. Допустимые значения для этого параметра: Kerberos и CredSSP.

Основными параметрами командлета `Set-VMHost` являются следующие:

– CimSession – запускает командлет на выполнение в удаленной сессии или на удаленном компьютере. Надо ввести имя компьютера или объекта сессии, такого как результат выполнения командлетов New-CimSession или Get-CimSession. По умолчанию используется текущая сессия на локальном компьютере;

– ComputerName – определяет один или более серверов Hyper-V на которых создаются новые ВМ. В качестве значения параметра можно указывать имена NetBIOS, IP адреса или полностью определенные доменные имена (FQDN, fully qualified domain name). По умолчанию значением параметра является имя локального компьютера. Для явного определения локального компьютера можно использовать значение localhost или точку (.);

– Credential – определяет одну или более учетных записей пользователей, которые имеют разрешение на выполнение этого действия. По умолчанию это учетная запись текущего пользователя;

– Confirm – необходимо подтвердить выполнение командлета, введя соответствующие символы;

– EnableEnhancedSessionMode - указывает, могут ли пользователи использовать расширенный режим при подключении к виртуальным машинам на этом сервере с помощью подключения к виртуальной машине;

– FibreChannelWwnn - указывает значение по умолчанию для имени узла на хосте Hyper-V;

– FibreChannelWWpnMaximum - задает максимальное значение, которое можно использовать для создания глобальных имен портов на хосте Hyper-V;

– FibreChannelWWpnMinimum - задает минимальное значение, которое можно использовать для генерации глобальных имен портов на хосте Hyper-V;

– MacAddressMaximum - задает максимальный MAC-адрес с использованием действительного шестнадцатеричного значения;

– MacAddressMinimum - задает минимальный MAC-адрес с использованием действительного шестнадцатеричного значения;

– MaximumStorageMigrations - задает максимальное количество миграций хранилища, которое может быть выполнено одновременно на хосте Hyper-V;

– MaximumVirtualMachineMigrations - задает максимальное количество динамических миграций, которые могут быть выполнены одновременно на хосте Hyper-V;

– NumaSpanningEnabled - указывает, могут ли виртуальные машины на хосте Hyper-V использовать ресурсы из более чем одного узла NUMA;

– Passthru - указывает, что файл Microsoft.HyperV.PowerShell.Host должен передаваться в конвейер, представляющий настраиваемый хост Hyper-V;

– ResourceMeteringSaveInterval - указывает, как часто хост Hyper-V сохраняет данные, которые отслеживают использование ресурсов. Диапазон составляет от 1 часа до 24 часов. Время в этом диапазоне может быть указано с использованием формата чч: мм: сс, где чч обозначает часы, мм обозначает минуты, а сс обозначает секунды. Также можно использовать объект Timespan для указания интервала;

– UseAnyNetworkForMigration - определяет, как сети выбираются для входящего трафика прямой миграции. Если установлено значение $ True, любая доступная сеть на хосте может использоваться для этого трафика. Если установлено значение $ False, входящий трафик прямой миграции передается только в сетях, указанных в свойстве MigrationNetworks хоста. Командлет Get-VMMigrationNetwork возвращает список сетей, которые можно использовать для миграции трафика;

– VirtualHardDiskPath - указывает папку по умолчанию для хранения виртуальных жестких дисков на хосте Hyper-V;

–VirtualMachineMigrationAuthenticationType - определяет тип аутентификации, который будет использоваться для миграций. Допустимые значения для этого параметра: Kerberos и CredSSP;

– VirtualMachineMigrationPerformanceOption - определяет параметр производительности, используемый для динамической миграции;

– VirtualMachinePath - указывает папку по умолчанию для хранения файлов конфигурации виртуальной машины на хосте Hyper-V;

– WhatIf – показывает, что произойдет, если командлет будет выполнен.

Проверка установки роли сервера виртуализации и компонента Hyper-V. Командлет Install-WindowsFeature устанавливает одну или несколько ролей, служб ролей или компонентов на локальном или указанном удаленном сервере под управлением Windows Server 2012 R2.

Для того, чтобы проверить какие компоненты установлены необходимо ввести командлет `Get-WindowsFeature *Hyper-V*` в оболочке Powershell (см. рисунок 139).

Рисунок 139 – Проверка установленных компонентов Hyper-V

Для установки модуля Hyper-V для Windows Powershell необходимо в оболочке «Powershell» ввести командлет `Install-WindowsFeature` Hyper-V-Powershell (см. рисунок 140).

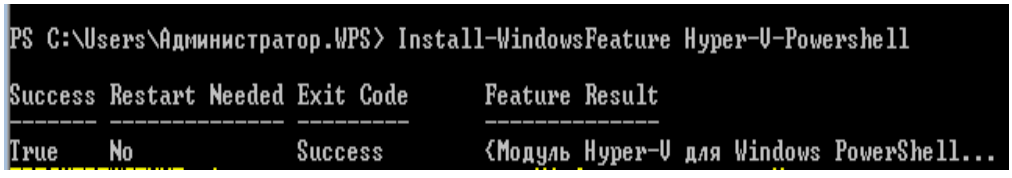


Рисунок 140 – Установка модуля Hyper-V для Windows PowerShell

Для проверки установки компонентов можно использовать командлет `Get-WindowsFeature` или команду `Get-WindowsFeature *Hyper-V*`. Компоненты для управления Hyper-V будут отмечены как установленные. Для этого в оболочке «Powershell» ввести командлет `Get-WindowsFeture *Hyper-V*` (см. рисунок 141).

```
PS C:\Users\Администратор.WPS> Get-WindowsFeature *Hyper-V*

Display Name                                            Name
------------                                            ----
[X] Hyper-V                                             Hyper-V
        [X] Hyper-V Management Tools                    RSAT-Hyper-V-Tools
            [X] Модуль Hyper-V для Windows PowerShell   Hyper-V-PowerShell
```

Рисунок 141 – Проверка установки компонентов

Получение списка команд для управления Hyper-V. Чтобы получить сведений о командлетах, применяемых для управления Hyper-V необходимо в оболочке Powershell ввести командлет `Get-Command –Module hyper-V` (см. рисунок 142).

```
PS C:\Users\Администратор.WPS> Get-Command -Module hyper-V

CommandType     Name                                               ModuleName
-----------     ----                                               ----------
Cmdlet          Add-VMDvdDrive                                     Hyper-V
Cmdlet          Add-VMFibreChannelHba                              Hyper-V
Cmdlet          Add-VMHardDiskDrive                                Hyper-V
Cmdlet          Add-VMMigrationNetwork                             Hyper-V
Cmdlet          Add-VMNetworkAdapter                               Hyper-V
Cmdlet          Add-VMNetworkAdapterAcl                            Hyper-V
Cmdlet          Add-VMNetworkAdapterExtendedAcl                    Hyper-V
Cmdlet          Add-VmNetworkAdapterRoutingDomainMapping           Hyper-V
Cmdlet          Add-VMRemoteFx3dVideoAdapter                       Hyper-V
Cmdlet          Add-VMScsiController                               Hyper-V
Cmdlet          Add-VMStoragePath                                  Hyper-V
Cmdlet          Add-VMSwitch                                       Hyper-V
Cmdlet          Add-VMSwitchExtensionPortFeature                   Hyper-V
Cmdlet          Add-VMSwitchExtensionSwitchFeature                 Hyper-V
Cmdlet          Checkpoint-VM                                      Hyper-V
```

Рисунок 142 – Получение сведений о командлетах, применяемых для управления Hyper-V

Создание виртуальных жестких дисков. Для получения списка всех командлетов PowerShell, которые могут применяться для управления виртуальными жесткими дисками, можно использовать командлет `Get-Command *VHD*` (см. рисунок 143).

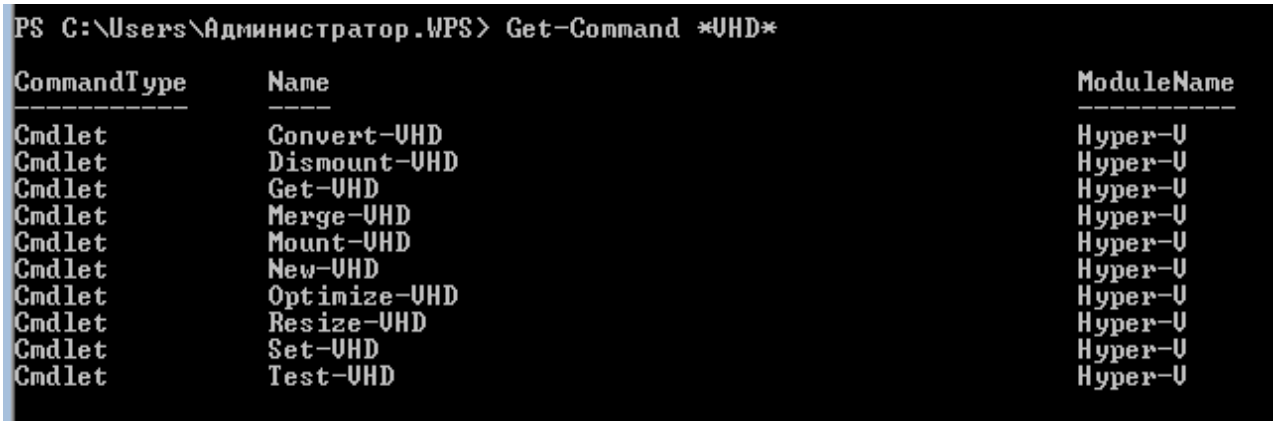


Рисунок 143 – Получение списка всех командлетов PowerShell, которые могут применяться для управления виртуальными жесткими дисками

Командлет `New-VHD` создает один или несколько новых виртуальных жестких дисков в формате VHD или более новом формате VHDX. Указанное расширение имени файла определяет формат.

VHD – формат файла, содержащий полную структуру и содержание, сходные с жёстким диском. Используется для хранения виртуальных операционных систем, программ и других файлов в одном файле-образе, который можно открыть разными программами виртуализации. Максимальный размер памяти до 2 ТБ, нет возможности сжимать и расширять диск при работающей машине.

VHDX — это формат диска, в котором по сравнению с VHD форматом диска были внесены ряд изменений: появился специальный внутренний журнал, снижающий вероятность повреждения данных, увеличилась емкость до 64 ТБ.

В этом примере создается динамический виртуальный жесткий диск в формате VHDX размером 10 ГБ (см. рисунок 144).

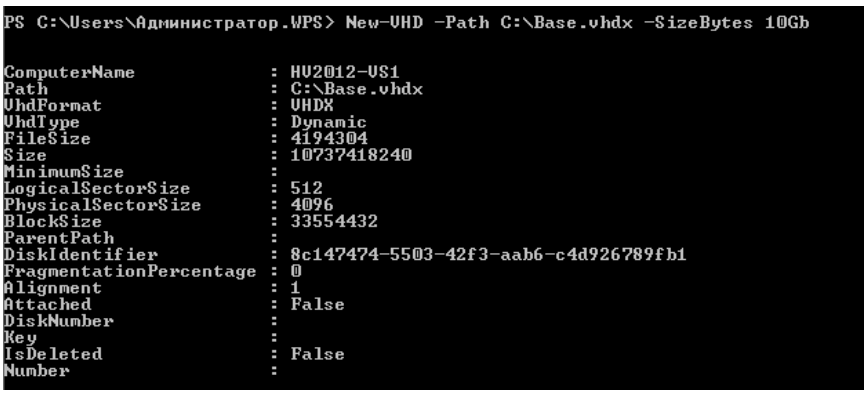


Рисунок 144 – Создание динамического виртуального жесткого диска в формате VHDX размером 10 ГБ

Значение параметра -Path определяет путь к новому файлу (файлам) виртуального жесткого диска, который создается в результате выполнения команды, значение параметра `-SizeBytes` означает максимальный размер создаваемого виртуального жесткого диска в байтах.

В этом примере создается разностный виртуальный жесткий диск формата VHDX с родительским путем c:\Base.vhdx (см. рисунок 145).

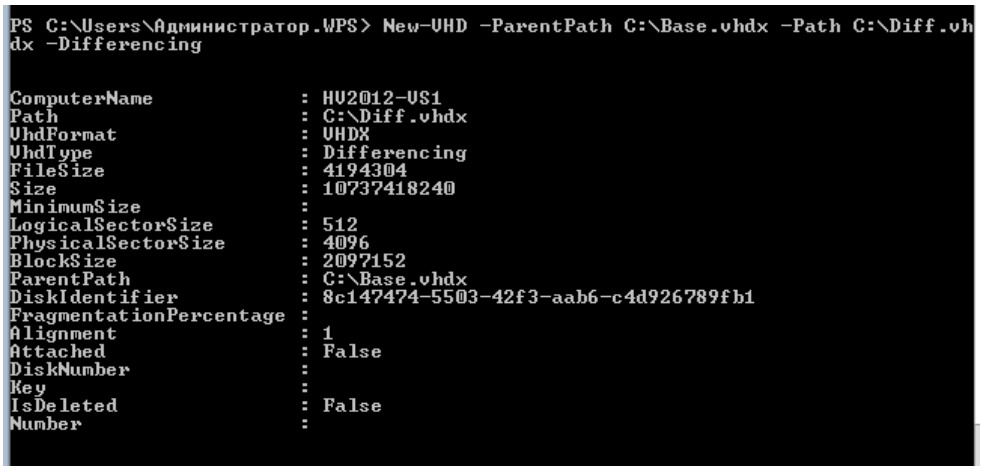


Рисунок 145 – Создание разностного виртуального жесткого диска формата VHDX с родительским путем c:\Base-да.VHDX-файлы

Значение параметра -ParentPath указывает путь к родительскому элементу создаваемого разностного диска (этот параметр может быть указан только для создания разностного диска), значение параметра `–Differencing` указывает, что необходимо создать разностный виртуальный жесткий диск.

В этом примере создается фиксированный виртуальный жесткий диск формата VHD объемом 5 GB по указанному пути (см. рисунок 146).

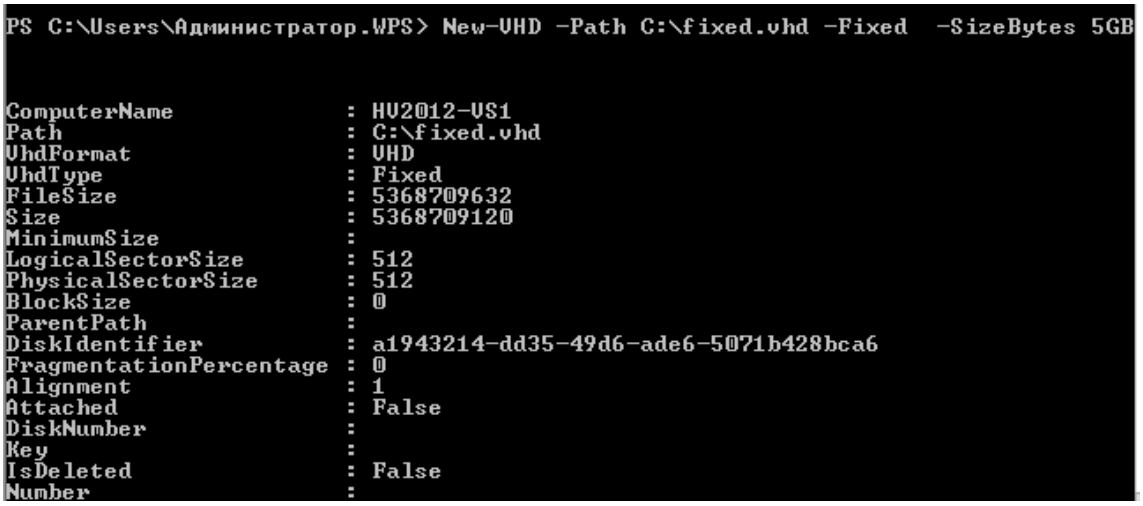


Рисунок 146 – Создание фиксированного виртуального жесткого диска формата VHD объемом 5 GB по указанному пути

Значение параметра `-Fixed` указывает, что необходимо создать фиксированный виртуальный жесткий диск.

В этом примере создается новый динамический виртуальный жесткий диск формата VHDX объемом 5MB по указанному пути с размером блока 128 МБ и размером логического сектора 4 КБ (рисунок 147).

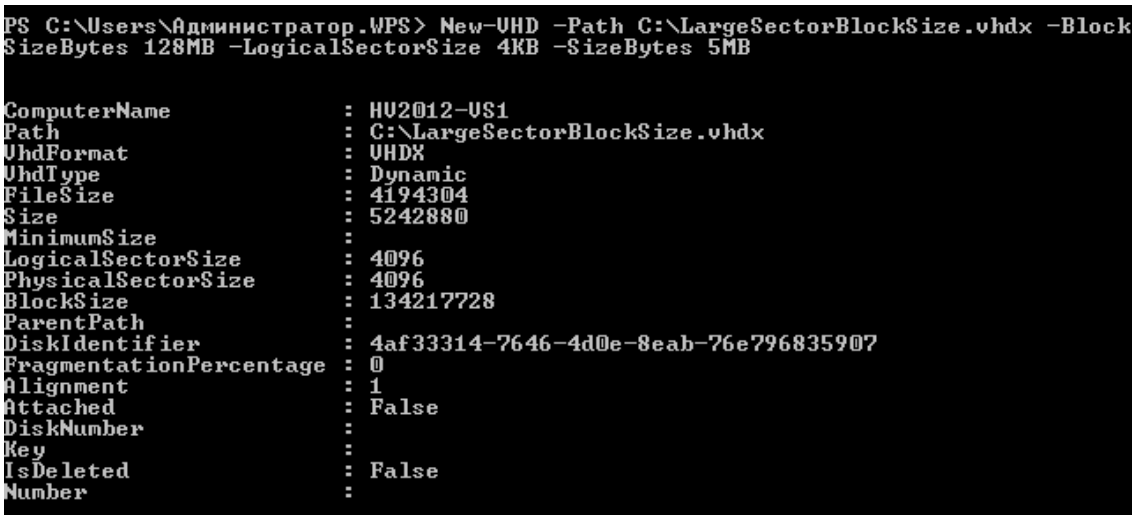


Рисунок 147– Создание фиксированного виртуального жесткого диска формата VHDX объемом 5MB по указанному пути с размером блока 128 МБ и размера сектора логического диска 4КВ.

Значение параметра –LogicalSectorSizeBytes задает размер логического сектора в байтах создаваемого виртуального жесткого диска

Основными параметрами командлета New-VHD являются следующие:

– AsJob – запускает командлет в качестве фонового задания;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых должны быть созданы файлы виртуального жесткого диска. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Необходимо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– Confirm – запрашивает подтверждение перед запуском командлета;

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– Differencing – указывает, что необходимо создать разностный виртуальный жесткий диск;

– Dynamic – указывает, что должен быть создан динамический виртуальный жесткий диск;

– Fixed – указывает, что необходимо создать фиксированный виртуальный жесткий диск;

– LogicalSectorSizeBytes – задает размер логического сектора в байтах создаваемого виртуального жесткого диска. Допустимые значения - 512 и 4096;

– ParentPath – указывает путь к родительскому элементу создаваемого разностного диска (Этот параметр может быть указан только для создания разностного диска);

– Path – путь к новому файлу (файлам) виртуального жесткого диска, который создается в результате выполнения команды. Если указано имя файла или относительный путь, то новый путь виртуального жесткого диска вычисляется относительно текущего рабочего каталога;

– PhysicalSectorSizeBytes – задает размер физического сектора в байтах. Допустимые значения - 512 и 4096;

– SizeBytes – Максимальный размер создаваемого виртуального жесткого диска в байтах;

– SourceDisk – указывает физический диск, который будет использоваться в качестве источника для создания виртуального жесткого диска;

– WhatIf – показывает, что произойдет, если командлет будет выполнен.

Преобразование виртуальных жестких дисков. Командлет `Convert-VHD` преобразует файл виртуального жесткого диска путем копирования данных из исходного файла виртуального жесткого диска в новый файл виртуального жесткого диска заданного формата и типа версии. Формат также определяется расширением имени файла указанных файлов .vhdx или .VHD-файл. Преобразование - это автономная операция; виртуальный жесткий диск не должен быть подключен при запуске операции.

В данном примере командлет `Convert-VHD` преобразует исходный VHD в конечный VHDX. Поскольку формат определяется расширением имени файла, а тип по умолчанию определяется исходным виртуальным жестким диском, если тип не указан, конечный виртуальный жесткий диск будет представлять собой диск формата VHDX того же типа, что и исходный виртуальный жесткий диск (см. рисунок 148).

Рисунок 148 – Преобразование исходного VHD в конечный VHDX

Значение параметра `-DestinationPath` указывает путь к преобразованному виртуальному жесткому диску.

Основными параметрами командлета `Convert-VHD` являются следующие:

– BlockSizeBytes – определяет размер блока в байтах для виртуального жесткого диска после его преобразования;

– CimSession – запускает командлет на выполнение в удаленной сессии или на удаленном компьютере. Надо ввести имя компьютера или объекта сессии, такого как результат выполнения командлетов New-CimSession или Get-CimSession. По умолчанию используется текущая сессия на локальном компьютере.

– Credential – определяет одну или более учетных записей пользователей, которые имеют разрешение на выполнение этого действия. По умолчанию это учетная запись текущего пользователя;

– Confirm – необходимо подтвердить выполнение командлета, введя соответствующие символы;

– ComputerName – определяет один или более серверов Hyper-V на которых преобразуются виртуальные жесткие диски. В качестве значения параметра можно указывать имена NetBIOS, IP адреса или полностью определенные доменные имена (FQDN, fully qualified domain name). По умолчанию значением параметра является имя локального компьютера. Для явного определения локального компьютера можно использовать значение localhost или точку (.);

– DeleteSource – указывает на то, что исходный виртуальный жесткий диск должен быть удален после конвертирования;

– DestinationPath – указывает путь к преобразованному виртуальному жесткому диску;

– ParentPath – определяет родительский путь для назначения – файла

разностного виртуального жесткого диска;

– Passthru – определяет, что объект, который должен передаваться по конвейеру, представляет собой преобразованный виртуальный жесткий диск;

– Path – указывает путь к виртуальному жесткому диску, который должен быть преобразован. Если определены имя файла или относительный путь, то путь к преобразованному виртуальному жесткому диску вычисляется относительно текущего рабочего каталога;

– VHDType – определяет тип преобразованного виртуального жесткого диска. Допускаются такие значения как Fixed (фиксированный), Dynamic (динамический) и Differencing (разностный). По умолчанию определяется типом исходного виртуального жесткого диска;

– WhatIf – показывает, что произойдет, если командлет будет выполнен. При этом сразу после запуска командлет не выполняется.

Изменение размера виртуальных жестких дисков. Командлет `Resize-VHD` изменяет максимальный физический размер виртуального жесткого диска. Он позволяет расширить как файлы с расширением .vhd так и .vhdx, но уменьшать может только файлы формата .vhdx. Операция уменьшения закончится неудачно, если уменьшать виртуальный жесткий диск до размера меньше чем его минимально допустимый размер (доступен как значение свойства MinimumSize объекта VHDX).

Если файл виртуального жесткого диска подключен к ВМ с помощью интерфейса IDE, нельзя изменить размер виртуального жесткого диска во время работы ВМ. Если файл виртуального жесткого диска подключен к ВМ с помощью интерфейса SCSI, можно изменить размер виртуального жесткого диска во время работы ВМ.

Командлет `Resize-VHD` не удаляет пустые блоки из динамически расширяемых файлов виртуальных жестких дисков. Для этого необходимо использовать командлет `Optimize-VHD`.

Следующий пример показывает изменение размера виртуального жесткого диска в формате .vhdx до 10Гбайт. Если он был больше, то командлет успешно выполнится только в том случае, когда параметр MinimumSize меньше чем или равен 10Гбайт (см. 149).

Рисунок 149 – Изменение размера виртуального жесткого диска в формате vhdx до 10 Гбайт

Основными параметрами командлета `Resize-VHD` являются следующие:

– CimSession – запускает командлет на выполнение в удаленной сессии или на удаленном компьютере. Надо ввести имя компьютера или объекта сессии, такого как результат выполнения командлетов New-CimSession или Get-CimSession. По умолчанию используется текущая сессия на локальном компьютере;

– Credential – определяет одну или более учетных записей пользователей, которые имеют разрешение на выполнение этого действия. По умолчанию это учетная запись текущего пользователя;

– Confirm – необходимо подтвердить выполнение командлета, введя соответствующие символы;

– ComputerName – определяет один или более серверов Hyper-V на которых изменяется размер виртуальных жестких дисков. В качестве значения параметра можно указывать имена NetBIOS, IP адреса или полностью определенные доменные имена (FQDN, fully qualified domain name). По умолчанию значением параметра является имя локального компьютера. Для явного определения локального компьютера можно использовать значение localhost или точку (.);

– Passthru – определяет, что объект, который должен передаваться по конвейеру, представляет собой виртуальный жесткий диск, размер которого изменяется;

– Path – указывает путь к виртуальному жесткому диску, размер которого изменяется;

– SizeBytes – определяет размер, который должен быть установлен для виртуального жесткого диска;

– ToMinimumSize – определяет, что размер виртуального жесткого диска изменяется до минимально возможного;

– WhatIf – показывает, что произойдет, если командлет будет выполнен. При этом сразу после запуска командлет не выполняется.

Проверка виртуальных жестких дисков. Командлет `Test-VHD` проверяет виртуальный жесткий диск на наличие любых проблем, которые могут сделать его неиспользуемым.

Пример команды, которая показывает выполнение проверки того, находится ли цепочка виртуальных жестких дисков в используемом состоянии, которая начинается с виртуального жесткого диска, ассоциированного с диском Fixed.vhdx (см. рисунок 150).

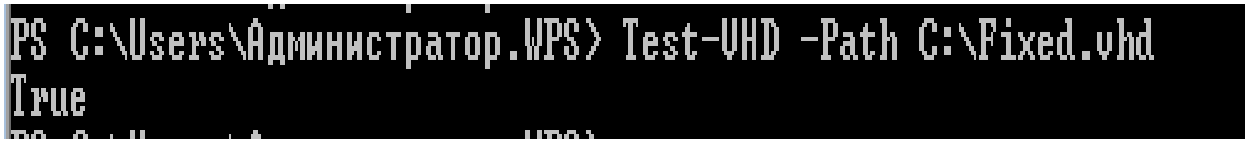


Рисунок 150 – Проверка цепочки виртуального жесткого диска

Основными параметрами командлета Test-VHD являются следующие:

– CimSession – запускает командлет на выполнение в удаленной сессии или на удаленном компьютере. Надо ввести имя компьютера или объекта сессии, такого как результат выполнения командлетов New-CimSession или Get-CimSession. По умолчанию используется текущая сессия на локальном компьютере;

– ComputerName – определяет один или более серверов Hyper-V на которых проводится проверка виртуальных жестких дисков. В качестве значения параметра можно указывать имена NetBIOS, IP адреса или полностью определенные доменные имена (FQDN, fully qualified domain name). По

умолчанию значением параметра является имя локального компьютера. Для явного определения локального компьютера можно использовать значение localhost или точку (.);

– Credential – определяет одну или более учетных записей пользователей, которые имеют разрешение на выполнение этого действия. По умолчанию это учетная запись текущего пользователя;

– Path – указывает путь к виртуальному жесткому диску, который проверяется. Если определены имя файла или относительный путь, то путь к новому виртуальному жесткому диску вычисляется относительно текущего рабочего каталога;

– SupportPersistentReservations – указывает, что командлет тестирует семантику поддержки постоянного резервирования SCSI. Этот параметр определяется при тестировании или виртуального жесткого диска или пути, который поддерживает общие виртуальные жесткие диски.

Оптимизация виртуальных жестких дисков. Командлет `Optimize-VHD` оптимизирует распределение пространства в одном или более виртуальных жестких дисках, за исключением виртуальных жестких дисков фиксированного типа. Для оптимизации файлов используется операция Compact. Эта операция отмечает неиспользуемые блоки, а также переупорядочивает блоки для более эффективной упаковки, что сокращает размер файла виртуального жесткого диска. Для использования командлета `Optimize-VHD` виртуальный жесткий диск не должен быть присоединен к ВМ или присоединен в режиме «только чтение» (read-only).

Операция Compact может быть выполнена успешно без сокращения размера файла в том случае, если оптимизация невозможна.

Далее приведен пример выполнения операции компактности в полном режиме. Если файл виртуального жесткого диска в формате .vhdx не

прикреплен как доступный только для чтения до начала операции, он по умолчанию будет в режиме Prezeroed (см. рисунок 151).

Рисунок 151 – Выполнения операции компактности в полном режиме

Значение параметра `-Mode` – определяет режим, в котором может быть оптимизирован виртуальный жесткий диск.

Следующий пример показывает выполнение операции компактности в режиме `Retrim`. Если файл виртуального жесткого диска в формате .vhdx не подключен как доступный только для чтения до начала операции, выполнение командлета вернет ошибку (см. рисунок 152).

Рисунок 152 – Выполнения операции компактности в Retrim режиме

Следующий пример – выполнение операции компактности в быстром режиме. Если файл виртуального жесткого диска в формате .vhdx не прикреплен как доступный только для чтения до начала операции, он по умолчанию будет в режиме `Pretrimmed` (см. рисунок 153).

Рисунок 153 – Выполнения операции компактности в быстром режиме

Основными параметрами командлета `Optimize-VHD` являются следующие:

– CimSession – запускает командлет на выполнение в удаленной сессии или на удаленном компьютере. Надо ввести имя компьютера или объекта сессии, такого как результат выполнения командлетов New-CimSession или Get-CimSession. По умолчанию используется текущая сессия на локальном компьютере;

– ComputerName – определяет один или более серверов Hyper-V на которых проводится оптимизация виртуальных жестких дисков. В качестве

значения параметра можно указывать имена NetBIOS, IP адреса или полностью определенные доменные имена (FQDN, fully qualified domain name). По умолчанию значением параметра является имя локального компьютера. Для явного определения локального компьютера можно использовать значение localhost или точку (.);

– Credential – определяет одну или более учетных записей пользователей, записей пользователей, которые имеют разрешение на выполнение этого действия. По умолчанию это учетная запись текущего пользователя;

– Confirm – необходимо подтвердить выполнение командлета, введя соответствующие символы;

– Mode – определяет режим в котором может быть оптимизирован виртуальный жесткий диск. Для виртуального жесткого диска в формате .vhd режимом по умолчанию является полный режим. Для виртуального жесткого диска в формате .vhdx режимом по умолчанию является быстрый режим. Возможны следующие режимы:

– полный режим (Full) заключается в сканировании для поиска нулевых блоков и освобождения неиспользуемых блоков. Доступен только в том случае, если виртуальный жесткий диск подключен только для чтения;

– режим Pretrimmed реализуется также как и быстрый (Quick)режим, но требует, чтобы виртуальный жесткий диск был подключен только для чтения. Определение неиспользуемого пространства менее эффективно чем в быстром (Quick) режиме (в котором виртуальный жесткий диск подключается только для чтения) потому, что при сканировании невозможно получить информацию о свободном пространстве виртуального жесткого диска с файловой системой NTFS. Полезен, когда файл виртуального жесткого диска в формате .vhdx используется ОС по крайней мере Windows 8 или Windows Server 2012, или когда этот командлет для файла в формате .vhdx в режиме Retrim;

– режим Prezeroed реализуется также как и быстрый режим, но не требует чтобы виртуальный жесткий диск был подключен только для чтения. Определение неиспользуемого пространства будет менее эффективным чем, если бы виртуальный жесткий диск был подключен только для чтения, так как при сканировании невозможно получить информацию о свободном пространстве виртуального жесткого диска с файловой системой NTFS. Полезно, если инструмент был запущен ранее, чтобы обнулить все свободное пространство на виртуальном диске, так как этот режим сжатия может затем освободить это пространство для последующих распределений блоков. Этот режим также может быть полезен при работе с виртуальным жестким диском с файловой системой, отличающейся от NTFS;

– быстрый режим (Quick) освобождает неиспользуемые блоки, но не сканирует нулевые блоки. Допускается, если виртуальный жесткий диск подключен только для чтения;

– режим Retrim отправляет повторные попытки без сканирования нулевых блоков или возврата неиспользованных блоков. Допускается, если виртуальный жесткий диск подключен только для чтения;

– Passthru – определяет, что объект, который должен передаваться по конвейеру, представляет собой виртуальный жесткий диск, который оптимизируется;

– Path – указывает один или более путей к динамическому или разностному виртуальному жесткому диску, который оптимизируется;

– WhatIf – показывает, что произойдет, если командлет будет выполнен. При этом сразу после запуска командлет не выполняется.

Создание нескольких виртуальных жестких дисков различного типа и объема.

Примеры создания виртуальных жестких дисков различного типа и объема (см. рисунки с 154 по 158)

```
PS C:\Users\Администратор.WPS> New-VHD -Path C:\Disk1.vhdx -SizeBytes 2GB


ComputerName            : HV2012-VS1
Path                    : C:\Disk1.vhdx
VhdFormat               : VHDX
VhdType                 : Dynamic
FileSize                : 4194304
Size                    : 2147483648
MinimumSize             :
LogicalSectorSize       : 512
PhysicalSectorSize      : 4096
BlockSize               : 33554432
ParentPath              :
DiskIdentifier          : 0b976027-9078-46b8-a9b4-db6c06f15ba1
FragmentationPercentage : 0
Alignment               : 1
Attached                : False
DiskNumber              :
Key                     :
IsDeleted               : False
Number                  :
```

Рисунок 154 – Создание виртуального жесткого диска формата VHDX размером 2GB

```
PS C:\Users\Администратор.WPS> New-VHD -Path C:\Disk2.vhdx -SizeBytes 3GB


ComputerName            : HV2012-VS1
Path                    : C:\Disk2.vhdx
VhdFormat               : VHDX
VhdType                 : Dynamic
FileSize                : 4194304
Size                    : 3221225472
MinimumSize             :
LogicalSectorSize       : 512
PhysicalSectorSize      : 4096
BlockSize               : 33554432
ParentPath              :
DiskIdentifier          : 3e471fcd-bd98-499f-b131-b3b419a4e6c2
FragmentationPercentage : 0
Alignment               : 1
Attached                : False
DiskNumber              :
Key                     :
IsDeleted               : False
Number                  :
```

Рисунок 155 – Создание виртуального жесткого диска формата VHDX размером 3GB

```
PS C:\Users\Администратор.WPS> New-VHD -Path C:\Disk3.vhdx -SizeBytes 4GB


ComputerName            : HV2012-VS1
Path                    : C:\Disk3.vhdx
VhdFormat               : VHDX
VhdType                 : Dynamic
FileSize                : 4194304
Size                    : 4294967296
MinimumSize             :
LogicalSectorSize       : 512
PhysicalSectorSize      : 4096
BlockSize               : 33554432
ParentPath              :
DiskIdentifier          : 354d8c4e-9539-413f-90e5-55dc37ad6556
FragmentationPercentage : 0
Alignment               : 1
Attached                : False
DiskNumber              :
Key                     :
IsDeleted               : False
Number                  :
```

Рисунок 156 – Создание виртуального жесткого диска формата VHDX размером 4GB

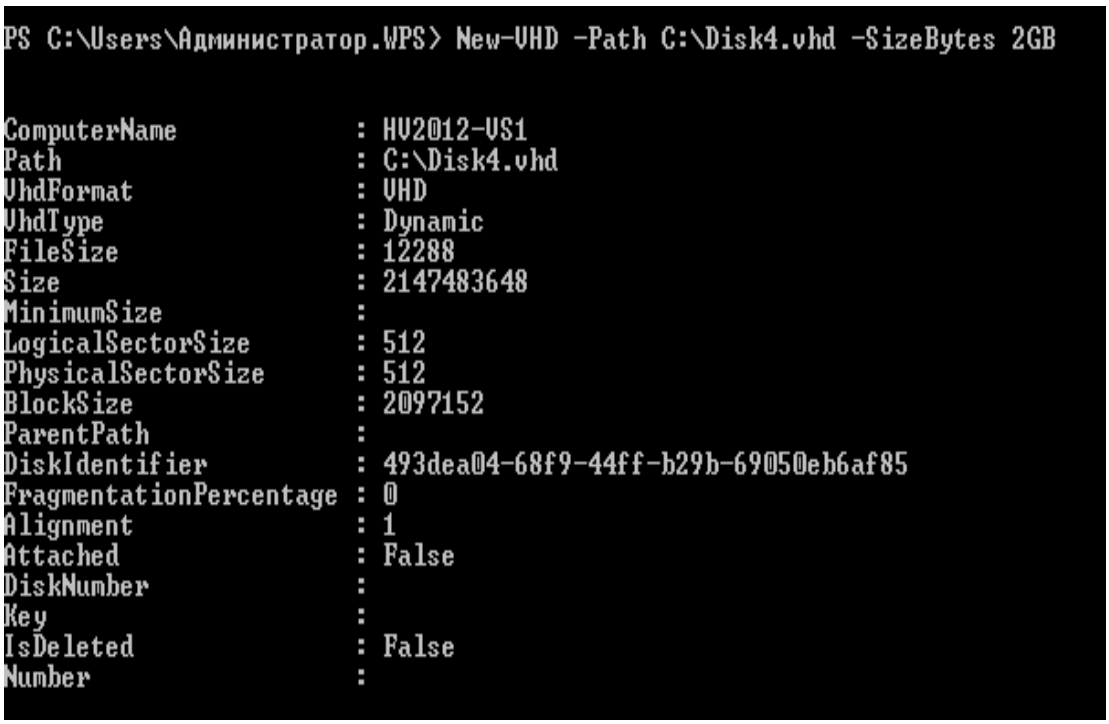


Рисунок 157 – Создание виртуального жесткого диска формата VHD размером 2GB

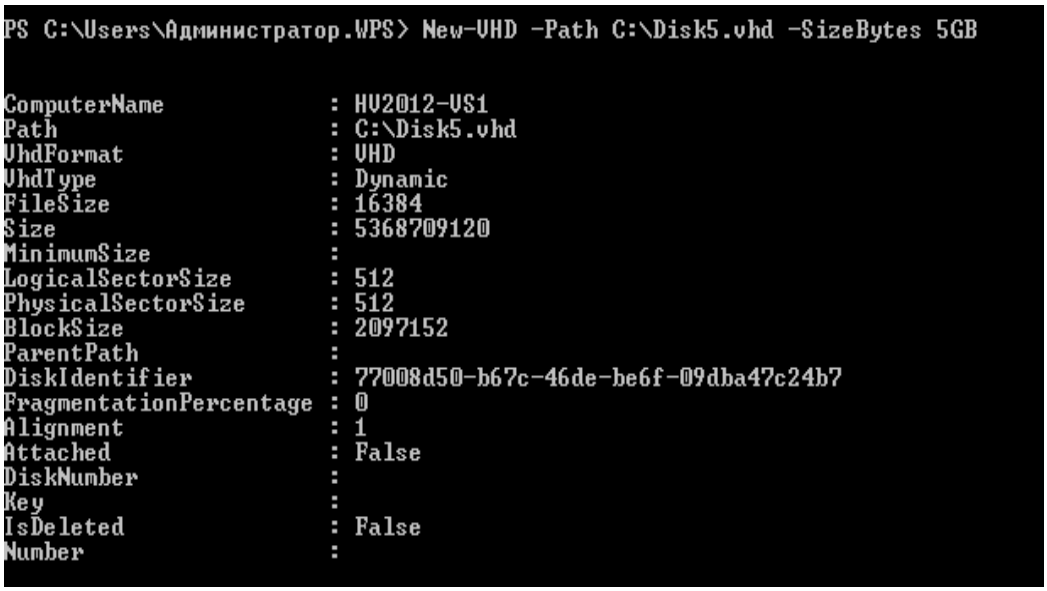


Рисунок 158 – Создание виртуального жесткого диска формата VHD размером 5GB

Создание виртуальных машин. Для получения списка всех командлетов PowerShell, которые могут применяться для управления виртуальными машинами, можно использовать командлет `Get-Command *VM*` (см. рисунок 159).

Рисунок 159 – Получение списка всех командлетов PowerShell, которые могут применяться для управления виртуальными машинами

Для того, что создать новую виртуальную машину используется командлет New-VM

В этом примере с помощью командлета `New-VM` создается новая виртуальная машина с именем wm23, имеющая 512 МБ памяти (см. рисунок 160).

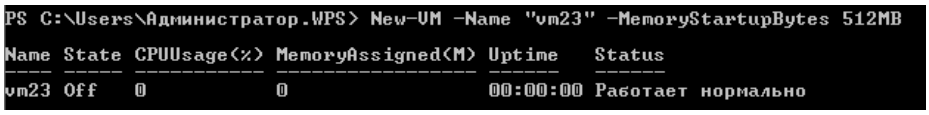


Рисунок 160 – Создание виртуальной машины с объемом памяти 512 МБ

Значение параметра `-Name` задает имя новой виртуальной машины, значение параметра `-MemoryStartupBytes` задает объем памяти в байтах для назначения виртуальной машине.

В этом примере создается виртуальная машина с именем newm12345, имеющая 512 МБ памяти и подключенная к новому 800-Мбайтному виртуальному жесткому диску, использующему формат VHDX (см.рисунок 161).

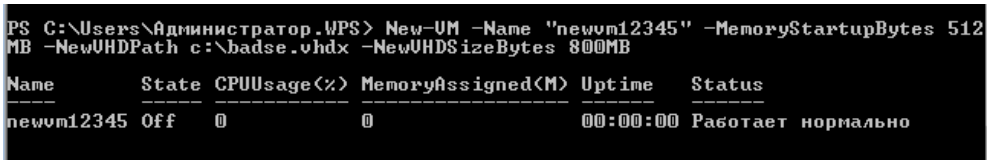


Рисунок 161 – Создание виртуальной машины с именем newm12345, имеющая 512 МБ памяти и подключенная к новому 800-Мбайтному виртуальному жесткому диску, использующему формат VHDX

В этом примере создается виртуальная машина с именем vm512, которая имеет 512 МБ памяти и подключается к существующему виртуальному жесткому диску, использующему формат VHDX (см. рисунок 162).

Рисунок 162 – Создание виртуальной машины с именем vm512, которая имеет 512 МБ памяти и подключается к существующему виртуальному жесткому диску, использующему формат VHDX

Основными параметрами командлета `Add-VMNetworkAdapter` являются следующие:

– AsJob– запускает командлет в качестве фонового задания;

– BootDevice – указывает устройство, которое будет использоваться в качестве загрузочного устройства для новой виртуальной машины компьютера можно использовать значение localhost или точку (.);

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых должна быть создана виртуальная машина;

– Confirm – запрашивает подтверждение перед запуском командлета;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– Generation – задает генерацию в виде целого числа для виртуальной машины;

– MemoryStartupBytes – задает объем памяти в байтах для назначения виртуальной машине;

– Name – задает имя новой виртуальной машины;

– NewVHDPath – создает новый виртуальный жесткий диск с указанным путем и подключает его к новой виртуальной машине;

– NewVHDSizeBytes – задает размер динамического виртуального жесткого диска, который создается и присоединяется к новой виртуальной машине;

– NoVHD – создает виртуальную машину без подключения каких-либо виртуальных жестких дисков;

– Path – указывает каталог для хранения файлов для новой виртуальной машины;

– SwitchName – задает понятное имя виртуального коммутатора, если требуется подключить новую виртуальную машину к существующему виртуальному коммутатору для обеспечения подключения к сети;

– VHDPath – указывает путь к файлу виртуального жесткого диска;

– WhatIf – показывает, что произойдет, если командлет будет запущен.

Подключение к ВМ контроллеров IDE и SCSI.

IDE — параллельный интерфейс подключения накопителей (гибких дисков, жёстких дисков и оптических дисководов) к компьютеру.

SCSI представляет собой набор стандартов для физического подключения и передачи данных между компьютерами и периферийными устройствами.

Командлет `Add-VMScsiController` добавляет контроллер SCSI в виртуальную машину.

Пример добавления контроллера SCSI в виртуальную машину (см. рисунок 163).

Рисунок 163 – Добавление контроллера SCSI в виртуальную машину

Пример добавления виртуального жесткого диска к контроллеру SCSI номер 0 при тестировании виртуальной машины (см. рисунок 164).

Рисунок 164 – Добавление виртуального жесткого диска к контроллеру SCSI

Значение параметра `-ControllerType` указывает тип контроллера, к которому должен быть добавлен жесткий диск.

Пример добавления виртуального жесткого диска с номером контроллера IDE 1 на тестовой виртуальной машине (см. рисунок 165).

Рисунок 165 – Добавление виртуального жесткого диска к контроллеру IDE

Значение параметра `-ControllerNumber` указывает номер контроллера, к которому должен быть добавлен жесткий диск.

Основными параметрами командлета `Add-VMScsiController` являются следующие:

– CimSession – запускает командлет на выполнение в удаленной сессии или на удаленном компьютере. Надо ввести имя компьютера или объекта сессии, такого как результат выполнения командлетов New-CimSession или Get-CimSession. По умолчанию используется текущая сессия на локальном компьютере.

– Credential – определяет одну или более учетных записей пользователей, которые имеют разрешение на выполнение этого действия. По умолчанию это учетная запись текущего пользователя;

– Confirm – необходимо подтвердить выполнение командлета, введя соответствующие символы;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых должен быть добавлен контроллер SCSI. В качестве значения параметра можно указывать имена NetBIOS, IP адреса или полностью определенные доменные имена (FQDN, fully qualified domain name). По

умолчанию значением параметра является имя локального компьютера. Для явного определения локального компьютера можно использовать значение localhost или точку (.);

– Passthru – определяет, что объект, который должен передаваться по конвейеру, представляет собой преобразованный виртуальный жесткий диск;

– WhatIf – показывает, что произойдет, если командлет будет выполнен. При этом сразу после запуска командлет не выполняется;

– VMName – задает имя виртуальной машины, на которую будет добавлен сетевой адаптер.

Включение служб интеграции для ВМ. Службы интеграции Hyper-V отвечают за эффективное взаимодействие виртуальных машин и гипервизора посредством установки дополнительных сервисов в гостевую.

Для получение работающих служб используется командлет `Get-VMIntegrationService` (см. рисунок 166).

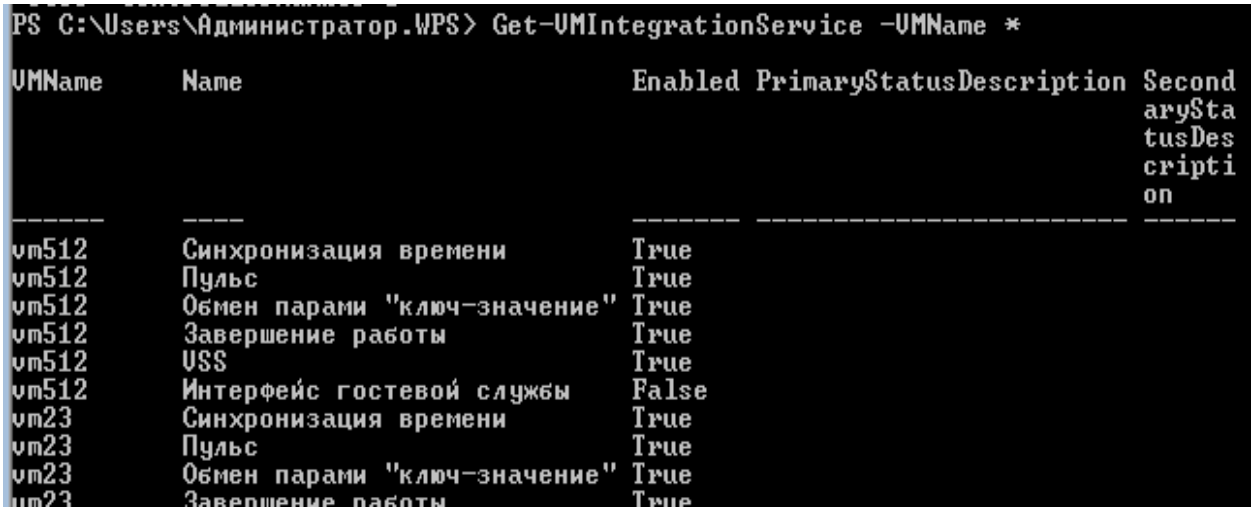


Рисунок 166 – Получение работающих служб

Пример включение службы «Интерфейс гостевой службы» (см. рисунок 167).

Рисунок 167 – Включение службы «Интерфейс гостевой службы»

Значение параметра –Name указывает имя извлекаемой службы интеграции.

Чтобы убедиться, что служба включена используется командлет Get-VMIntegrationService (см. рисунок 168).

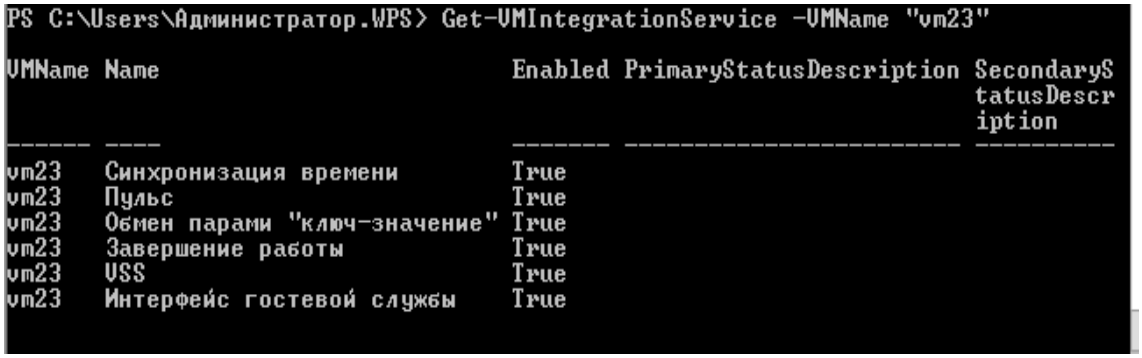


Рисунок 168 – Проверка включения службы «Интерфейс гостевой службы»

Основными параметрами командлета Get-VMIntegrationService являются следующие:

– CimSession – запускает командлет на выполнение в удаленной сессии или на удаленном компьютере. Надо ввести имя компьютера или объекта сессии, такого как результат выполнения командлетов New-CimSession или Get-CimSession. По умолчанию используется текущая сессия на локальном компьютере;

– Credential – определяет одну или более учетных записей пользователей, которые имеют разрешение на выполнение этого действия. По умолчанию это учетная запись текущего пользователя;

– ComputerName – определяет один или более серверов Hyper-V на которых преобразуются виртуальные жесткие диски. В качестве значения параметра можно указывать имена NetBIOS, IP адреса или полностью определенные доменные имена (FQDN, fully qualified domain name). По умолчанию значением параметра является имя локального компьютера. Для явного определения локального компьютера можно использовать значение localhost или точку (.);

– VMName – задает имя виртуальной машины, на которую будет добавлен сетевой адаптер;

– Name – указывает имя извлекаемой службы интеграции;

– VMSnapshot – указывает моментальный снимок, из которого должны быть извлечены службы integration services.

Настройка BIOS виртуальной машины поколения 1. Командлет `Set-VMBios` настраивает BIOS виртуальной машины поколения 1. Этот командлет не работает с виртуальной машиной 2 поколения. При попытке выполнения командлет выдает ошибку.

В этом примере ключ `NumLock` по умолчанию отключается на виртуальной машине vm23 (см. рисунок 169).

Рисунок 169 – Отключение ключа NumLock на виртуальной машине

Значение параметра `-DisableNumLock` указывает, что `NumLock` должен быть отключен в BIOS настраиваемой виртуальной машины.

В этом примере виртуальная машина vm23 настраивается для проверки наличия загрузочного устройства в следующем порядке: дискета, сеть, CD-дисковод, жесткий диск (см. рисунок 170).

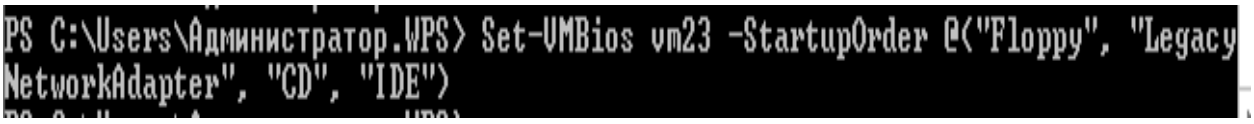


Рисунок 170– Настройка виртуальной машины для проверки наличия загрузочного устройства в следующем порядке: дискета, сеть, CD-дисковод, жесткий диск

Значение параметра `-StartupOrder` задает массив загрузочных устройств, представляющих порядок загрузки в BIOS виртуальной машины.

Основными параметрами командлета `Set-VMBios` являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Введите имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– ComputerName – указывает один или несколько узлов Hyper-V, для которых должен быть настроен BIOS. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– VMName – задает имя виртуальной машины, для которой должна быть настроена BIOS;

– VM – указывает виртуальную машину, для которой необходимо настроить BIOS;

– VMBios – задает массив объектов BIOS. Командлет настраивает BIOS, указанный для виртуальных машин. Чтобы получить объект BIOS, надо использовать командлет Get-VMBios;

– DisableNumLock – указывает, что NumLock должен быть отключен в BIOS настраиваемой виртуальной машины;

– EnableNumLock – указывает, что NumLock должен быть включен в BIOS настраиваемой виртуальной машины;

– StartupOrder – задает массив загрузочных устройств, представляющих порядок загрузки в BIOS виртуальной машины. Загрузочные устройства задаются как члены перечисления BootDevices (CD, IDE, LegacyNetworkAdapter, Floppy);

– WhatIf – показывает, что произойдет, если командлет будет запущен.

Задание конфигурации микропрограммного обеспечения виртуальной машины. Командлет `Set-VMFirmware` задает конфигурацию микропрограммного обеспечения виртуальной машины поколения 2.

Этот пример включает функцию безопасной загрузки на виртуальной машине "Virtmachine" (см. рисунок 171).

Рисунок 171 – Включение функции безопасной загрузки на виртуальной машине

Значение параметра `-EnableSecureBoot` указывает, следует ли включить безопасную загрузку.

В этом примере виртуальная машина "Virtmachine" загружается с объекта сетевого адаптера виртуальной машины, хранящегося в файле $vmNetworkAdapter. Этот объект был получен с помощью командлета `Get-VMNetworkAdapter` (см. рисунок 172).

Рисунок 172 – Загрузка виртуальной машины с объекта сетевого адаптера виртуальной машины

Значение параметра `-FirstBootDevice` указывает устройство, с которого будет предпринята первая попытка загрузки.

Основными параметрами командлета `Set-VMFirmware` являются следующие:

– BootOrder – задает массив устройств. Порядок загрузки определяет порядок устройств, с которых будет производиться загрузка;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– ComputerName – задает имена узлов Hyper-V, конфигурацию микропрограммного обеспечения которых требуется изменить;

– VM – указывает виртуальную машину, для которой необходимо настроить BIOS;

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– DisableNumLock – указывает, что NumLock должен быть отключен в BIOS настраиваемой виртуальной машины;

– Confirm – запрашивает подтверждение перед запуском командлета;

– StartupOrder – задает массив загрузочных устройств, представляющих порядок загрузки в BIOS виртуальной машины. Загрузочные устройства задаются как члены перечисления BootDevices (CD, IDE, LegacyNetworkAdapter, Floppy);

– EnableSecureBoot – указывает, следует ли включить безопасную загрузку;

– FirstBootDevice – указывает устройство, с которого будет предпринята первая попытка загрузки;

– PauseAfterBootFailure – задает поведение виртуальной машины после сбоя запуска. При значении On, если виртуальная машина не запускается правильно с устройства, виртуальная машина приостанавливается;

– PreferredNetworkBootProtocol – указывает версию протокола IP для использования во время сетевой загрузки;

– SecureBootTemplate – задает имя шаблона безопасной загрузки. Если включена безопасная загрузка, то для запуска гостевой операционной системы необходимо иметь действительный шаблон безопасной загрузки;

– SecureBootTemplateId – задает идентификатор шаблона безопасной загрузки;

– VM – указывает объекты виртуальной машины, для которых требуется изменить конфигурацию микропрограммного обеспечения. Чтобы получить объект виртуальной машины, используйте командлет Get-VM;

– VMFirmware – задает массив конфигураций микропрограммного обеспечения виртуальной машины. Командлет задает заданные конфигурации микропрограммного обеспечения;

– VMName – задает массив имен виртуальных машин,для которых требуется изменить конфигурацию микропрограммного обеспечения;

– WhatIf – показывает, что произойдет, если командлет будет запущен.

Подключение к ВМ привода оптических дисков. Командлет `Add-VMDvdDrive` добавляет DVD-диск в виртуальную машину.

DVD-диск - оптический носитель информации, выполненный в форме диска, для хранения различной информации в цифровом виде.

В этом примере с помощью командлета Add-VMDvdDrive добавляется виртуальный DVD-диск с использованием файла D:\Commonpath\Windows.iso для тестирования виртуальной машины (см. рисунок 173).

Рисунок 173 – Добавление виртуального DVD-диска для тестирования виртуальной машины

Основными параметрами командлета `Add-VMDvdDrive` являются следующие:

– AllowUnverifiedPaths – указывает, что никакая ошибка не должна возникать, если указанный путь не проверен как доступный для кластера. Этот параметр применим к кластеризованным виртуальным машинам;

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– ComputerName – указывает один или несколько узлов Hyper-v, на которых должен быть добавлен DVD-привод. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– Confirm – запрашивает подтверждение перед запуском командлета;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– ControllerLocation – указывает номер места на контроллере, в котором должен быть добавлен DVD-привод. Если это не указано, то используется номер первого доступного местоположения на контроллере;

– VM – указывает виртуальную машину, к которой должен быть добавлен дисковод DVD;

– Path – указывает полный путь к файлу виртуального жесткого диска или тому физического жесткого диска для добавленного DVD-диска;

– ResourcePoolName – задает понятное имя пула ресурсов ISO, с которым должен быть связан этот DVD-привод;

– VMName – указывает имя виртуальной машины, к которой будет добавлен DVD-привод;

– WhatIf – показывает, что произойдет, если командлет будет запущен.

Переименование виртуальной машины. Для того чтобы переименовывать виртуальную машину используется командлет `Rename-VM`.

В этом примере с помощью командлета `Rename-VM` изменяется название виртуальной машины vm11 (см. рисунок 174).

```
PS C:\Users\Администратор.WPS> Rename-VM vm1 -NewName vm11
```

Рисунок 174 – Переименование виртуальной машины

Значение параметра -NewName указывает имя, на которое должна быть переименована виртуальная машина.

В этом примере с помощью командлета Rename-VM изменяется название виртуальной машины vm11 и отображается новое имя с помощью командлета Get-VM (см. рисунок 175).

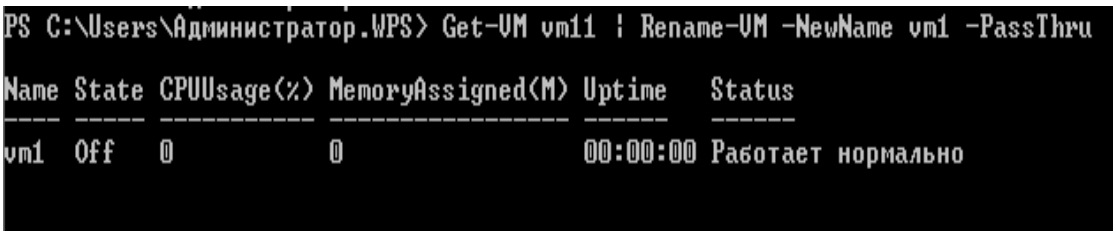


Рисунок 175 - Переименование виртуальной машины и отображение нового имени виртуальной машины

Значение параметра -Passthru указывает, что объект должен быть передан в конвейер, представляющий виртуальную машину, подлежащую переименованию.

Основными параметрами командлета Rename-VM являются следующие:

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых работает этот командлет. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– Confirm – запрашивает подтверждение перед запуском командлета;

– Passthru – указывает, что объект должен быть передан в конвейер, представляющий виртуальную машину, подлежащую переименованию;

– Confirm – запрашивает подтверждение перед запуском командлета;

– Name – указывает имя виртуальной машины, которая будет переименована;

– NewName – указывает имя, на которое должна быть переименована виртуальная машина;

– VM – указывает виртуальную машину, которую необходимо переименовать;

– VMName – задает массив имен виртуальных машин, для которых требуется изменить конфигурацию микропрограммного обеспечения;

– WhatIf – показывает, что произойдет, если командлет будет запущен.

Удаление виртуальной машины. Для удаление виртуальной машины используется командлет `Remove-VM`. При выполнении этого командлета удаляется файл конфигурации виртуальной машины, но не удаляются никакие виртуальные жесткие диски. Если виртуальная машина имеет какие-либо моментальные снимки, они удаляются и объединяются в файлы виртуального жесткого диска после удаления виртуальной машины.

В этом примере с помощью командлета `Remove-VM` удаляется виртуальная машина vm2 (см. рисунок 176)

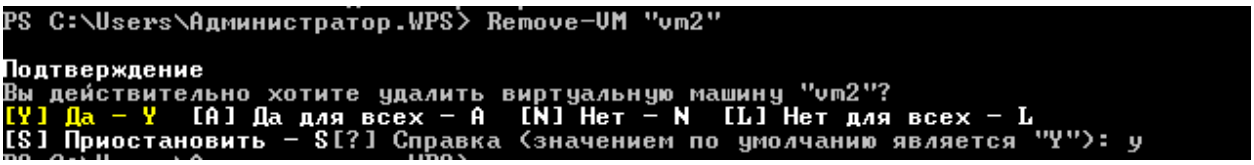


Рисунок 176 – Удаление виртуальной машины

При выполнение командлета `Remove-VM` необходимо нажать кнопку «Y» для подтверждения удаления виртуальной машины.

Основными параметрами командлета `Remove-VM` являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например

выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– ComputerName – указывает один или несколько узлов Hyper-V, с которых должна быть удалена виртуальная машина. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– Force – указывает, что запросы подтверждения должны подавляться во время удаления виртуальной машины;

– Name – указывает имя удаляемой виртуальной машины;

– ResourcePoolName – указывает имя пула ресурсов, из которого должен быть удален коммутатор;

– VM – указывает виртуальную машину, подлежащую удалению;

– WhatIf – показывает, что произойдет, если командлет будет запущен;

– Passthru – указывает, что объект должен быть передан в конвейер, представляющий удаляемую виртуальную машину.

Подключение к ВМ сетевых адаптеров. Добавление виртуального сетевого адаптера к виртуальной машине. Командлет `Add-VMNetworkAdapter` добавляет виртуальный сетевой адаптер к виртуальной машине.

В этом примере добавляется виртуальный сетевой адаптер с именем Test1 на виртуальную машину с именем vm23 (см. рисунок 177).

```
PS C:\Users\Администратор.WPS> Add-VMNetworkAdapter -VMName vm23 -Name "Test1"
```

Рисунок 177 – Добавление виртуального сетевого адаптера на виртуальную машину

Значение параметра `-VMName` задает имя виртуальной машины, на которую будет добавлен сетевой адаптер, значение параметра `-Name` задает имя для нового виртуального сетевого адаптера.

В этом примере добавляется второй виртуальный сетевой адаптер в операционную систему управления (см. рисунок 178).

Рисунок 178 – Добавление второго виртуального сетевого в операционную систему управлению

Значение параметра `-ManagementOS` определяет операционную систему управления.

Основными параметрами командлета `Add-VMNetworkAdapter` являются следующие:

– CimSession – запускает командлет на выполнение в удаленной сессии или на удаленном компьютере. Надо ввести имя компьютера или объекта сессии, такого как результат выполнения командлетов New-CimSession или Get-CimSession. По умолчанию используется текущая сессия на локальном компьютере;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых должен быть добавлен виртуальный сетевой адаптер. В качестве значения параметра можно указывать имена NetBIOS, IP адреса или полностью определенные доменные имена (FQDN, fully qualified domain name). По умолчанию значением параметра является имя локального компьютера. Для явного определения локального компьютера можно использовать значение localhost или точку (.);

– Credential – определяет одну или более учетных записей пользователей, которые имеют разрешение на выполнение этого действия. По умолчанию это учетная запись текущего пользователя;

– Confirm – необходимо подтвердить выполнение командлета, введя соответствующие символы;

– DynamicMacAddress – назначает динамически генерируемые MAC-адрес виртуального сетевого адаптера;

–VirtualMachinePath – указывает папку по умолчанию для хранения файлов конфигурации виртуальной машины на хосте Hyper-V;

– ManagementOS – определяет операционную систему управления;

– IsLegacy – указывает, является ли виртуальный сетевой адаптер устаревшим типом;

– WhatIf – показывает, что произойдет, если командлет будет выполнен. При этом сразу после запуска командлет не выполняется;

– Name – задает имя для нового виртуального сетевого адаптера. Значение по умолчанию - " сетевой адаптер";

– Passthru – указывает, что объект должен быть передан в конвейер, представляющий добавляемый сетевой адаптер;

– ResourcePoolName – задает понятное имя пула ресурсов;

– StaticMacAddress – назначает конкретный MAC-адрес новому виртуальному сетевому адаптеру;

– SwitchName – задает имя виртуального коммутатора для подключения к новому сетевому адаптеру. Если имя коммутатора не является уникальным, то операция завершается неудачей;

– VMName – задает имя виртуальной машины, на которую будет добавлен сетевой адаптер.

Возращение виртуальных сетевых адаптеров указанной виртуальной машины, моментального снимка или операционной системы управления. Для возращения виртуальных сетевых адаптеров указанной виртуальной машины, моментального снимка или операционной системы управления используется командлет `Get-VMNetworkAdapter`.

В этом примере с помощью командлета `Get-VMNetworkAdapter` выводятся виртуальные сетевые адаптеры со всех виртуальных машин на локальном узле Hyper-V (см. рисунок 179).

```
PS C:\Users\Администратор.WPS> Get-VMNetworkAdapter -VMName vm1

Name           IsManagementOs VMName SwitchName MacAddress   Status IPAddresse
                                                                    s
----           -------------- ------ ---------- ----------   ------ ----------
Сетевой адаптер False         vm1               000000000000       {}
```

Рисунок 179 – Вывод сетевых адаптеров на виртуальной машине vm1

В этом примере возвращаются виртуальные сетевые адаптеры в `ManagementOS` (т. е. локальный узел Hyper-V) (см. рисунок 180).

```
PS C:\Users\Администратор.WPS> Get-VMNetworkAdapter -ManagementOS

Name      IsManagementOs VMName SwitchName MacAddress   Status IPAddresses
----      -------------- ------ ---------- ----------   ------ -----------
NewSwitch True                  NewSwitch  0800274D0E4D Ok     
```

Рисунок 180 – Возвращение виртуальных сетевых адаптеров в ManagementOS

В этом примере с помощью командлета `Get-VMNetworkAdapter` отображаются виртуальные сетевые адаптеры со всех виртуальных машин на локальном узле Hyper-V (см. рисунок 181).

```
PS C:\Users\Администратор.WPS> Get-VMNetworkAdapter -All

Name           IsManagementOs VMName      SwitchName MacAddress   Status IPAdd
                                                                        resse
                                                                        s
----           -------------- ------      ---------- ----------   ------ -----
NewSwitch      True                       NewSwitch  0800274D0E4D Ok     
Сетевой адаптер False         newvm12345              000000000000       {}
Сетевой адаптер False         newvm12345              000000000000       {}
Сетевой адаптер False         newvm12345              000000000000       {}
Сетевой адаптер False         Virtmachine             000000000000       {}
Сетевой адаптер False         vm1                     000000000000       {}
Сетевой адаптер False         vm23                    000000000000       {}
Test1          False          vm23                    000000000000       {}
Сетевой адаптер False         vm512                   000000000000       {}
```

Рисунок 181 - Получение виртуальных сетевых адаптеров со всех виртуальных машин на локальном узле Hyper-V

Основными параметрами командлета Get-VMNetworkAdapter являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– ComputerName – указывает, что необходимо извлечь один или несколько узлов Hyper-V на виртуальных сетевых адаптерах. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– All – указывает все виртуальные сетевые адаптеры в системе, независимо от того, находится ли виртуальный сетевой адаптер в операционной системе управления или в виртуальной машине;

– ManagementOS – задает операционную систему управления, т. е. операционную систему узла виртуальной машины;

– IsLegacy – надо указать $true, чтобы извлекать только традиционные сетевые адаптеры, или $false для получения только в Hyper-V-удельный сетевые адаптеры. Если этот параметр не указан, то извлекаются виртуальные сетевые адаптеры обоих типов;

– Name – указывает имя извлекаемого сетевого адаптера;

– SwitchName – задает имя виртуального коммутатора, сетевые адаптеры которого должны быть извлечены. (этот параметр доступен только для виртуальных сетевых адаптеров в операционной системе управления);

–VMSnapshot – указывает моментальный снимок, сетевые адаптеры которого должны быть извлечены;

– VM – указывает виртуальную машину, виртуальные сетевые адаптеры которой должны быть извлечены. Звездочка " * " - это подстановочный знак. Если он указан, командлет возвращает виртуальные сетевые адаптеры с каждой виртуальной машины в системе;

– VMName - указывает имя виртуальной машины, сетевые адаптеры которой должны быть извлечены.

Переименование виртуального сетевого адаптера на виртуальной машине или в операционной системе управления. Для того чтобы переименовывать виртуальную машину используется командлет `Rename-VMNetworkAdapter`.

В этом примере все виртуальные сетевые адаптеры виртуальной машины vm1 переименовываются в CoreNet (см. рисунок 182).

Рисунок 182– Переименование всех сетевых адаптеров виртуальной машины

Значение параметра `–VMName` задает имя виртуальной машины, имеющей виртуальный сетевой адаптер, который требуется переименовать, значение параметра `–NewName` задает новое имя для виртуального сетевого адаптера.

В этом примере виртуальный сетевой адаптер CoreNet переименовывается в Ethernet 5 в виртуальной машине vm1 (см. рисунок 183).

Рисунок 183 – Переименование сетевого адаптера виртуальной машины

Значение параметра `–Name` указывает существующее имя виртуального сетевого адаптера.

Основными параметрами командлета `Rename-VMNetworkAdapter` являются:

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых должен быть переименован виртуальный сетевой адаптер. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– Confirm – запрашивает подтверждение перед запуском командлета;

– Passthru – указывает, что объект должен быть передан в конвейер, представляющий виртуальный сетевой адаптер, подлежащий переименованию;

– Name – указывает существующее имя виртуального сетевого адаптера;

– ManagementOS – указывает, что требуется переименовать виртуальный сетевой адаптер, принадлежащий операционной системе управления;

– NewName – задает новое имя для виртуального сетевого адаптера;

– VM – указывает виртуальную машину, имеющую виртуальный сетевой адаптер, который требуется переименовать;

– VMName – задает имя виртуальной машины, имеющей виртуальный сетевой адаптер, который требуется переименовать;

– VMNetworkAdapter – указывает виртуальный сетевой адаптер, который необходимо переименовать;

– WhatIf – показывает, что произойдет, если командлет будет запущен.

Удаление виртуального сетевого адаптера. Для того, чтобы удалить один или несколько виртуальных сетевых адаптеров из конфигурации виртуальной машины используется командлет `Remove-VMNetworkAdapter`.

В этом примере показано удаление виртуального сетевого адаптера с виртуальной машины (см. рисунок 184).

Рисунок 184 – Удаление виртуального сетевого адаптера

Значение параметра `–VMNetworkAdapter` указывает сетевой адаптер виртуальной машины, который необходимо удалить, значение параметра означает `–VMNetworkAdapter` указывает сетевой адаптер виртуальной машины, который необходимо удалить.

Основными параметрами командлета `Remove-VMNetworkAdapter` являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых должен быть удален виртуальный сетевой адаптер. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– Credential указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– Confirm – запрашивает подтверждение перед запуском командлета;

– ManagementOS – указывает операционную систему управления удаляемым виртуальным сетевым адаптером;

– Name – указывает имя удаляемого виртуального сетевого адаптера;

– SwitchName – указывает имя виртуального коммутатора, подключенного к удаляемому виртуальному сетевому адаптеру;

– VM – указывает виртуальную машину, подлежащую удалению;

– VMName – указывает имя виртуальной машины, на которой установлен виртуальный сетевой адаптер, который требуется удалить;

– VMNetworkAdapter – указывает сетевой адаптер виртуальной машины, который необходимо удалить;

– WhatIf – показывает, что произойдет, если командлет будет запущен;

– Passthru – указывает, что объект, который должен быть передан в конвейер, представляющий сетевой адаптер виртуальной машины, подлежащий удалению.

Создание нового виртуального коммутатора на одном или нескольких узлах виртуальной машины. В Hyper-V есть три типа виртуальных коммутаторов:

– внешний (External) – тип сети, который позволяет виртуальным машинам взаимодействовать с внешними сетями и хостом;

– внутренний (Internal) – тип сети, предназначенный для подключения виртуальных машин и хоста и не предусматривает соединения с внешними сетями;

– частный (Private) – тип сети, где виртуальный коммутатор может быть подключен только к виртуальным машинам и изолирован от хоста.

Командлет `New-VMSwitch` создает новый виртуальный коммутатор на одном или нескольких узлах виртуальной машины.

В этом примере создается новый коммутатор Switch1, который привязывается к сетевому адаптеру под названием Ethernet 3(см. рисунок 185).

Рисунок 185 – Создание внешнего коммутатора

Значение параметра `-NetAdapterName` Задает имя сетевого адаптера, который будет привязан к создаваемому коммутатору.

Для того, чтобы настроить виртуальный коммутатор командлет `Set-VMSwitch`.

В этом примере выполняется преобразование виртуального коммутатора по имени Switch1 к внутреннему коммутатору (см. рисунок 186).

Рисунок 186 – Преобразование внешнего виртуального коммутатора во внутренней

Значение параметра `-SwitchType` указывает тип создаваемого коммутатора.

Создание виртуального внешнего коммутатора и преобразование его в частный показано далее (см рисунок 187 и 188).

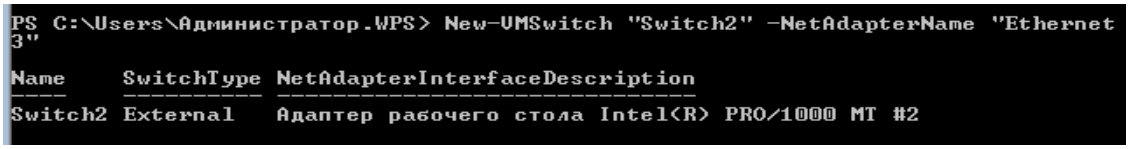


Рисунок 187 – Создание внешнего виртуального коммутатора

Рисунок 188 – Преобразование внешнего коммутатора в частный

Создать виртуальный внешний коммутатор (см. рисунок 189).

Рисунок 189 – Создание внешнего виртуального коммутатора

Основными параметрами командлета `New-VMSwitch` являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых должен быть создан виртуальный коммутатор. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– Confirm – запрашивает подтверждение перед запуском командлета;

– EnableEmbeddedTeaming – указывает, позволяет ли этот командлет объединять команды для виртуального коммутатора;

– ManagementOS – определяет операционную систему управления;

– EnableIov – указывает, что виртуализация ввода-вывода должна быть включена на создаваемом виртуальном коммутаторе;

– WhatIf – показывает, что произойдет, если командлет будет выполнен. При этом сразу после запуска командлет не выполняется;

– NetAdapterInterfaceDescription – задает описание интерфейса сетевого адаптера, который будет привязан к создаваемому коммутатору;

– Notes – указывает примечание, которое должно быть связано с создаваемым коммутатором;

– EnablePacketDirect – указывает, включает ли этот командлет прямой

путь к пакету через виртуальный коммутатор. Значение по умолчанию – $False;

– MinimumBandwidthMode – указывает, как должна быть настроена минимальная пропускная способность на виртуальном коммутаторе;

– NetAdapterName – задает имя сетевого адаптера, который будет привязан к создаваемому коммутатору;

– SwitchType – указывает тип создаваемого коммутатора. Допустимые значения являются внутренними и частными. Чтобы создать внешний виртуальный коммутатор, укажите либо NetAdapterInterfaceDescription, либо параметр NetAdapterName, который неявно устанавливает тип виртуального коммутатора в External;

– Name – задает имя создаваемого коммутатора.

Основными параметрами командлета `Set-VMSwitch` являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых должен быть настроен виртуальный коммутатор. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– Confirm – запрашивает подтверждение перед запуском командлета;

– AllowManagementOS – указывает, может ли операционная система управления использовать физический сетевой адаптер, привязанный к внешнему виртуальному коммутатору;

– DefaultFlowMinimumBandwidthAbsolute – Задает минимальную пропускную способность в битах в секунду, которая выделяется для специальной категории, называемой "поток по умолчанию". Любой трафик, отправленный виртуальным сетевым адаптером, который подключен к этому виртуальному коммутатору и не имеет минимальной выделенной полосы пропускания, фильтруется в эту категорию;

– WhatIf – показывает, что произойдет, если командлет будет выполнен. При этом сразу после запуска командлет не выполняется;

– Extensions – задает упорядоченный список сетевых расширений, используемых для изменения порядка Привязок на виртуальном коммутаторе;

– Name – задает имя настраиваемого виртуального коммутатора;

– NetAdapterInterfaceDescription – задает описание интерфейса физического сетевого адаптера, к которому должен быть привязан внешний виртуальный коммутатор. Если задать этот параметр для преобразования виртуального коммутатора, внешний виртуальный коммутатор будет настроен таким образом, чтобы позволить операционной системе управления совместно использовать доступ к физическому сетевому адаптеру. Чтобы переопределить это поведение, надо включить в команду AllowManagementOs $false;

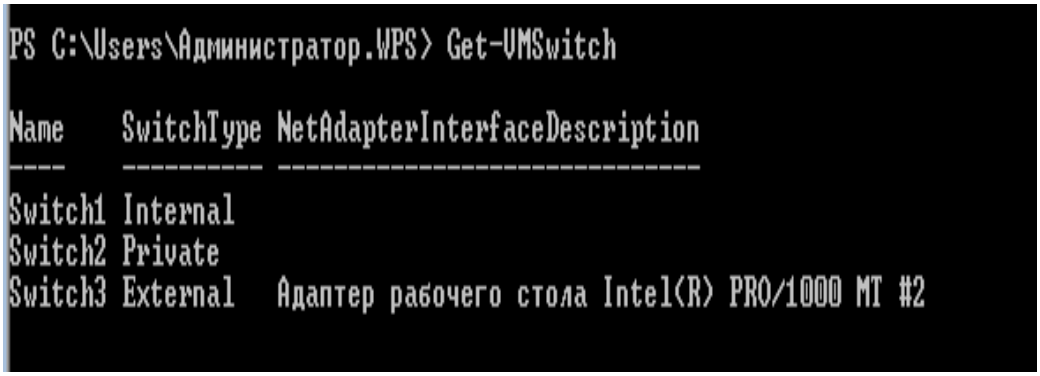
– NetAdapterName – задает имя физического сетевого адаптера, к которому должен быть привязан внешний виртуальный коммутатор. Если задать этот параметр для преобразования виртуального коммутатора, внешний виртуальный коммутатор будет настроен таким образом, чтобы позволить операционной системе управления совместно использовать доступ к физическому сетевому адаптеру. Чтобы переопределить это поведение, надо включить в команду AllowManagementOs $false;

– SwitchType – указывает тип создаваемого коммутатора. Допустимые значения являются внутренними и частными. Чтобы создать внешний виртуальный коммутатор, надо указать либо NetAdapterInterfaceDescription, либо параметр NetAdapterName, который неявно устанавливает тип виртуального коммутатора в External;

– VMSwitch – указывает виртуальный коммутатор, который необходимо настроить.

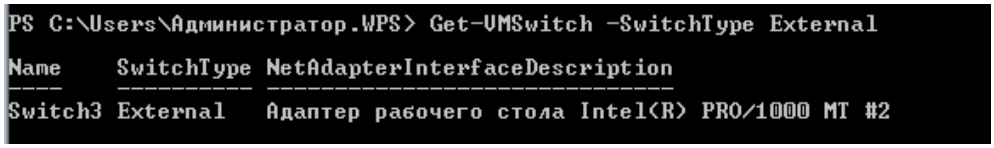
Получение виртуальных коммутаторов от одного или нескольких виртуальных узлов Hyper-V. Для получения виртуальных коммутаторов с узла Hyper-V используется командлет `Get-VMSwitch`. Если параметры не заданы, этот командлет возвращает все виртуальные коммутаторы с локального узла Hyper-V.

В этом примере с помощью командлета `Get-VMSwitch` отображаются все виртуальные коммутаторы с локального узла Hyper-V (см. рисунок 190).



Пример 190 – Получение виртуальных коммутаторов с локального узла Hyper-V

В этом примере отображаются все виртуальные коммутаторы, подключенные к внешней сети. (см. рисунок 191).



Пример 191 – Получение виртуальных коммутаторов, подключенных к внешней сети

Основными параметрами командлета `Set-VMSwitch` являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– ComputerName – указывает один или несколько узлов Hyper-V, с которых должны быть получены виртуальные коммутаторы. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– Id – задает уникальный идентификатор извлекаемого виртуального коммутатора;

– Name – задает имя извлекаемого виртуального коммутатора;

– SwitchType – указывает тип извлекаемых виртуальных коммутаторов. Допустимые значения - внешние, внутренние и частные;

– ResourcePoolName – указывает пул ресурсов, из которого должны быть извлечены виртуальные коммутаторы.

Переименование виртуального коммутатора. Для того чтобы переименовать виртуальный коммутатор используется командлет `Rename-VMSwitch`.

В этом примере с помощью командлета `Rename-VMSwitch` переименовывается виртуальный коммутатор Switch1 (см. рисунок 190).

Рисунок 192 – Изменение названия виртуального коммутатора

Основными параметрами командлета `Rename-VMSwitch` являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых виртуальный коммутатор должен быть переименован. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– Id – задает уникальный идентификатор извлекаемого виртуального коммутатора;

– Name – задает имя виртуального коммутатора, который будет переименован;

– NewName – задает имя, на которое будет переименован виртуальный коммутатор;

– VMSwitch – указывает виртуальный коммутатор, который будет переименован;

– WhatIf показывает, что произойдет, если командлет будет запущен.

Удаление виртуального коммутатора. Для того, чтобы удалить виртуальный коммутатор используется командлет `Remove-VMSwitch`.

В этом примере с помощью командлета `Remove-VMSwitch` удаляется виртуальный коммутатор Switch1 (см. рисунок 193).

Рисунок 193 – Удаление виртуального коммутатора

Основными параметрами командлета `Remove-VMSwitch` являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых виртуальный коммутатор должен быть удален. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– Force – принудительно запускает команду, не запрашивая подтверждения пользователя;

– Name – указывает имя виртуального коммутатора, подлежащего удалению;

– ResourcePoolName – указывает имя пула ресурсов, из которого должен быть удален коммутатор;

– VMSwitch – указывает виртуальный коммутатор, подлежащий удалению;

– WhatIf – показывает, что произойдет, если командлет будет запущен.

Создание и подключение виртуальных машин к виртуальному коммутатору к внутренней сети. В этом примере создаются три виртуальные машины с помощью командлета New-VM (см. рисунок 194).

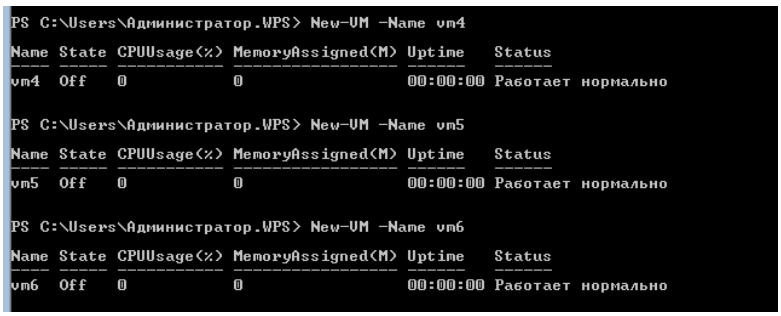


Рисунок 194 – Создание виртуальных машин

Значение параметра `-Name` задает имя виртуальной машины.

Для того чтобы проверить, что виртуальные машины созданы необходимо ввести в оболочке «Powershell» командлет `Get-VM` (см. рисунок 195).

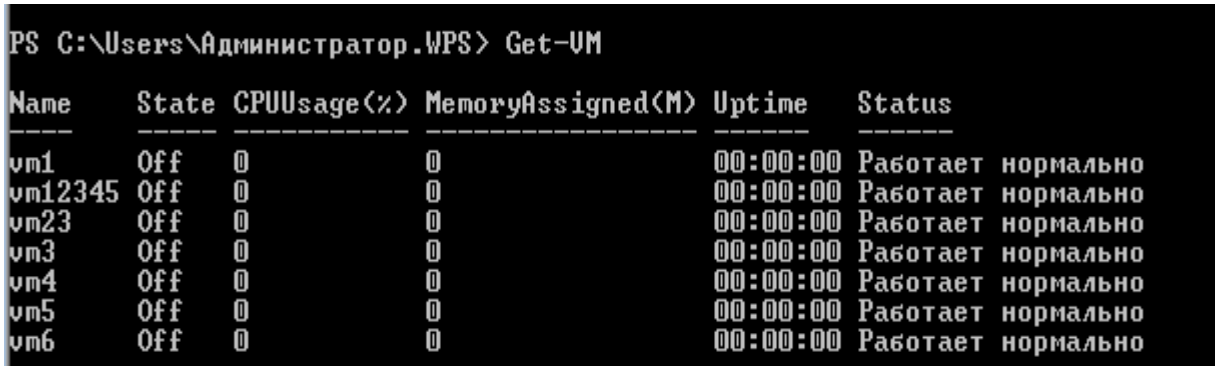


Рисунок 195 – Проверка создания виртуальных машин

Для создания виртуального коммутатора используется командлет `New-VMSwitch`.

В этом примере с помощью командлета `New-Switch` создается виртуальные коммутатор Switch4 с внутреннем типом сети (см. рисунок 196).

Рисунок 196 – Создание виртуального коммутатора с внутренним типом сети

Для того чтобы подключить виртуальные машины к виртуальному коммутатору используется командлет `Add-VMNetworkAdapter`.

В этом примере с помощью командлета `Add-VMNetworkAdapter` виртуальные машины vm4, vm5, vm6 подключаются к виртуальному коммутатору (см. рисунок 197).

```
PS C:\Users\Администратор.WPS> Add-VMNetworkAdapter -VMName vm4 -SwitchName Swit
ch4
PS C:\Users\Администратор.WPS> Add-VMNetworkAdapter -VMName vm5 -SwitchName Swit
ch4
PS C:\Users\Администратор.WPS> Add-VMNetworkAdapter -VMName vm6 -SwitchName Swit
ch4
```

Рисунок 197 – Подключение виртуальных машин к виртуальному коммутатору

Значение параметра `-SwitchName` задает понятное имя виртуального коммутатора, если требуется подключить новую виртуальную машину к существующему виртуальному коммутатору для обеспечения подключения к сети, значение параметра `-VMName` задает имя виртуальной машины.

Для того, чтобы проверить, что виртуальные машины подключены к виртуальному коммутатору необходимо использовать командлет `Get-VMNetworkAdapter`.

В этом примере проверяется подключение виртуальных машин к виртуальному коммутатору с помощью командлета `Get-VMNetworkAdapter` (см. рисунок 198).

```
PS C:\Users\Администратор.WPS> Get-VmNetworkAdapter -VMName vm4

Name            IsManagementOs VMName SwitchName MacAddress   Status IPAddresse
                                                                     s
----            -------------- ------ ---------- ----------   ------ ----------
Сетевой адаптер False          vm4                000000000000        {}
Сетевой адаптер False          vm4    Switch4     000000000000        {}

PS C:\Users\Администратор.WPS> Get-VmNetworkAdapter -VMName vm5

Name            IsManagementOs VMName SwitchName MacAddress   Status IPAddresse
                                                                     s
----            -------------- ------ ---------- ----------   ------ ----------
Сетевой адаптер False          vm5                000000000000        {}
Сетевой адаптер False          vm5    Switch4     000000000000        {}

PS C:\Users\Администратор.WPS> Get-VmNetworkAdapter -VMName vm6

Name            IsManagementOs VMName SwitchName MacAddress   Status IPAddresse
                                                                     s
----            -------------- ------ ---------- ----------   ------ ----------
Сетевой адаптер False          vm6                000000000000        {}
Сетевой адаптер False          vm6    Switch4     000000000000        {}
```

Рисунок 198 – Проверка подключения виртуальных машин к виртуальному коммутатору

Далее необходимо поменять названия сетевого адаптера у виртуальных машин, чтобы они отличались.

Для этого необходимо использовать командлет `Rename-VMNetworkAdapter`.

В этом пример переименовываются сетевые адаптеры виртуальных машин vm4, vm5, vm6 (см. рисунок 199).

```
PS C:\Users\Администратор.WPS> Rename-VMNetworkAdapter -VMName vm4 -Name "Сетево
й адаптер" -NewName SetAdapter1
PS C:\Users\Администратор.WPS> Rename-VMNetworkAdapter -VMName vm5 -Name "Сетево
й адаптер" -NewName SetAdapter2
PS C:\Users\Администратор.WPS> Rename-VMNetworkAdapter -VMName vm6 -Name "Сетево
й адаптер" -NewName SetAdapter3
```

Рисунок 199 - Изменение имен сетевых адаптеров виртуальных машин

Значение параметра `-Name` задает название сетевого адаптера.

Проверить изменение имен сетевых адаптеров виртуальных машин (см. рисунок 200).

```
PS C:\Users\Администратор.WPS> Get-VmNetworkAdapter -VMName vm4

Name         IsManagementOs VMName SwitchName MacAddress   Status IPAddresses
----         -------------- ------ ---------- ----------   ------ ------------
SetAdapter1 False          vm4                000000000000        {}
SetAdapter1 False          vm4    Switch4     000000000000        {}

PS C:\Users\Администратор.WPS> Get-VmNetworkAdapter -VMName vm5

Name         IsManagementOs VMName SwitchName MacAddress   Status IPAddresses
----         -------------- ------ ---------- ----------   ------ ------------
SetAdapter2 False          vm5                000000000000        {}
SetAdapter2 False          vm5    Switch4     000000000000        {}

PS C:\Users\Администратор.WPS> Get-VmNetworkAdapter -VMName vm6

Name         IsManagementOs VMName SwitchName MacAddress   Status IPAddresses
----         -------------- ------ ---------- ----------   ------ ------------
SetAdapter3 False          vm6                000000000000        {}
SetAdapter3 False          vm6    Switch4     000000000000        {}
```

Рисунок 200 – Проверка изменений сетевых адаптеров

Далее необходимо добавить виртуальные сетевые адаптеры виртуальных машин vm4, vm5, vm6 в операционную систему управления.

Для этого используется командлет `Add-VMNetworkAdapter`.

В этом примере виртуальные сетевые адаптеры виртуальных машин vm4, vm5, vm6 добавляются в операционную систему управления (см. рисунок 201).

```
PS C:\Users\Администратор.WPS> Add-VMNetworkAdapter -ManagementOS -Name SetAdapt
er1
PS C:\Users\Администратор.WPS> Add-VMNetworkAdapter -ManagementOS -Name SetAdapt
er2
PS C:\Users\Администратор.WPS> Add-VMNetworkAdapter -ManagementOS -Name SetAdapt
er3
```

Рисунок 201 – Добавление виртуальных сетевых адаптеров в операционную систему управления

Значение параметра `-ManagementOS` определяет операционную систему управления.

Далее настроить внутреннюю сеть. Внутренняя сеть предназначена для подключения виртуальных машин и хоста и не предусматривает соединения с внешними сетями.

Для настройки IP-адреса сети и маски на каждом виртуальном сетевом адаптере виртуальных машин vm4, vm5, vm6 и хоста используется командлет `New-NetIPAddress`.

В этом примере с помощью командлета `New-NetIPAddress` настраиваются конфигурации сети виртуальных машин vm4, vm5, vm6 и хоста Hyper-V (см. рисунки с 202 по 205).

```
PS C:\Users\Администратор.WPS> New-NetIPAddress -InterfaceAlias "vEthernet (Set
dapter1)" -IPAddress "192.168.200.10" -PrefixLength 24


IPAddress         : 192.168.200.10
InterfaceIndex    : 136
InterfaceAlias    : vEthernet (SetAdapter1)
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 192.168.200.10
InterfaceIndex    : 136
InterfaceAlias    : vEthernet (SetAdapter1)
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore
```

Рисунок 202 - Настройка сети виртуальной машины vm4

```
PS C:\Users\Администратор.WPS> New-NetIPAddress -InterfaceAlias "vEthernet (SetA
dapter2)" -IPAddress "192.168.200.11" -PrefixLength 24


IPAddress         : 192.168.200.11
InterfaceIndex    : 156
InterfaceAlias    : vEthernet (SetAdapter2)
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 192.168.200.11
InterfaceIndex    : 156
InterfaceAlias    : vEthernet (SetAdapter2)
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore
```

Рисунок 203 – Настройка сети виртуальной машины vm5

```
PS C:\Users\Администратор.WPS> New-NetIPAddress -InterfaceAlias "VEthernet (SetA
dapter3)" -IPAddress "192.168.200.12" -PrefixLength 24


IPAddress         : 192.168.200.12
InterfaceIndex    : 176
InterfaceAlias    : vEthernet (SetAdapter3)
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 192.168.200.12
InterfaceIndex    : 176
InterfaceAlias    : vEthernet (SetAdapter3)
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore
```

Рисунок 204 – Настройка сети виртуальной машины vm6

```
PS C:\Users\Администратор.WPS> New-NetIPAddress -InterfaceAlias "VEthernet (Swit
ch4)" -IPAddress "192.168.200.13" -PrefixLength 24


IPAddress         : 192.168.200.13
InterfaceIndex    : 129
InterfaceAlias    : vEthernet (Switch4)
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 192.168.200.13
InterfaceIndex    : 129
InterfaceAlias    : vEthernet (Switch4)
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore
```

Рисунок 205 – Настройка сети хоста Hyper-V

Значение параметра `-InterfaceAlias` задает псевдоним сетевого интерфейса, значение параметра `-IPAddress` назначает сетевой адрес виртуальной машины, значение параметра `-PrefixLength` задает длину

префикса. Этот параметр определяет размер локальной подсети и также известен как маска подсети.

Создание и подключение виртуальных машин к виртуальному коммутатору к частной сети. Для создания виртуального коммутатора используется командлет `New-VMSwitch`.

В этом примере с помощью командлета `New-Switch` создается виртуальные коммутатор Switch5 с частным типом сети (см. рисунок 206).

```
PS C:\Users\Администратор.WPS> New-VMSwitch "Switch5" -SwitchType Private

Name    SwitchType NetAdapterInterfaceDescription
----    ---------- ----------------------------
Switch5 Private
```

Рисунок 206 – Создание виртуального коммутатора с частным типом сети

Для того чтобы подключить виртуальные машины к виртуальному коммутатору используется командлет `Add-VMNetworkAdapter`.

В этом примере с помощью командлета `Add-VMNetworkAdapter` виртуальные машины vm4, vm5, vm6 подключаются к виртуальному коммутатору (см. рисунок 207).

```
PS C:\Users\Администратор.WPS> Add-VMNetworkAdapter -VMName vm4 -SwitchName Swit
ch5
PS C:\Users\Администратор.WPS> Add-VMNetworkAdapter -VMName vm5 -SwitchName Swit
ch5
PS C:\Users\Администратор.WPS> Add-VMNetworkAdapter -VMName vm6 -SwitchName Swit
ch5
```

Рисунок 207 – Подключение виртуальных машин к виртуальному коммутатору

Для того, чтобы проверить, что виртуальные машины подключены к виртуальному коммутатору необходимо использовать командлет `Get-VMNetworkAdapter`.

В этом примере проверяется подключение виртуальных машин к виртуальному коммутатору с помощью командлета `Get-VMNetworkAdapter` (см. рисунок 208).

```
PS C:\Users\Администратор.WPS> Get-VmNetworkAdapter -VMName vm4

Name            IsManagementOs VMName SwitchName MacAddress   Status IPAddresse
                                                                     s
----            -------------- ------ ---------- ----------   ------ ----------
SetAdapter1     False          vm4                000000000000        {}
SetAdapter1     False          vm4    Switch4     000000000000        {}
Сетевой адаптер False          vm4    Switch5     000000000000        {}


PS C:\Users\Администратор.WPS> Get-VmNetworkAdapter -VMName vm5

Name            IsManagementOs VMName SwitchName MacAddress   Status IPAddresse
                                                                     s
----            -------------- ------ ---------- ----------   ------ ----------
SetAdapter2     False          vm5                000000000000        {}
SetAdapter2     False          vm5    Switch4     000000000000        {}
Сетевой адаптер False          vm5    Switch5     000000000000        {}


PS C:\Users\Администратор.WPS> Get-VmNetworkAdapter -VMName vm6

Name            IsManagementOs VMName SwitchName MacAddress   Status IPAddresse
                                                                     s
----            -------------- ------ ---------- ----------   ------ ----------
SetAdapter3     False          vm6                000000000000        {}
SetAdapter3     False          vm6    Switch4     000000000000        {}
Сетевой адаптер False          vm6    Switch5     000000000000        {}
```

Рисунок 208 – Проверка подключения виртуальных машин к виртуальному коммутатору

Далее необходимо поменять названия сетевого адаптера у виртуальных машин, чтобы они отличались.

Для этого необходимо использовать командлет `Rename-VMNetworkAdapter`.

В этом пример переименовываются сетевые адаптеры виртуальных машин vm4, vm5, vm6 (см. рисунок 209).

```
PS C:\Users\Администратор.WPS> Rename-VMNetworkAdapter -VMName vm4 -Name "Сетево
й адаптер" -NewName SetAdapter4
PS C:\Users\Администратор.WPS> Rename-VMNetworkAdapter -VMName vm5 -Name "Сетево
й адаптер" -NewName SetAdapter5
PS C:\Users\Администратор.WPS> Rename-VMNetworkAdapter -VMName vm6 -Name "Сетево
й адаптер" -NewName SetAdapter6
```

Рисунок 209 - Изменение имен сетевых адаптеров виртуальных машин

Проверить изменение имен сетевых адаптеров виртуальных машин (см. рисунок 210).

```
PS C:\Users\Администратор.WPS> Get-VmNetworkAdapter -VMName vm4

Name         IsManagementOs VMName SwitchName MacAddress   Status IPAddresses
----         -------------- ------ ---------- ----------   ------ ----------
SetAdapter1 False          vm4                000000000000        {}
SetAdapter1 False          vm4    Switch4     000000000000        {}
SetAdapter4 False          vm4    Switch5     000000000000        {}


PS C:\Users\Администратор.WPS> Get-VmNetworkAdapter -VMName vm5

Name         IsManagementOs VMName SwitchName MacAddress   Status IPAddresses
----         -------------- ------ ---------- ----------   ------ ----------
SetAdapter2 False          vm5                000000000000        {}
SetAdapter2 False          vm5    Switch4     000000000000        {}
SetAdapter5 False          vm5    Switch5     000000000000        {}


PS C:\Users\Администратор.WPS> Get-VmNetworkAdapter -VMName vm6

Name         IsManagementOs VMName SwitchName MacAddress   Status IPAddresses
----         -------------- ------ ---------- ----------   ------ ----------
SetAdapter3 False          vm6                000000000000        {}
SetAdapter3 False          vm6    Switch4     000000000000        {}
SetAdapter6 False          vm6    Switch5     000000000000        {}
```

Рисунок 210 – Проверка изменений сетевых адаптеров

Далее необходимо добавить виртуальные сетевые адаптеры виртуальных машин vm4, vm5, vm6 в операционную систему управления.

Для этого используется командлет `Add-VMNetworkAdapter`.

В этом примере виртуальные сетевые адаптеры виртуальных машин vm4, vm5, vm6 добавляются в операционную систему управления (см. рисунок 211).

```
PS C:\Users\Администратор.WPS> Add-VMNetworkAdapter -ManagementOS -Name SetAdapt
er4
PS C:\Users\Администратор.WPS> Add-VMNetworkAdapter -ManagementOS -Name SetAdapt
er5
PS C:\Users\Администратор.WPS> Add-VMNetworkAdapter -ManagementOS -Name SetAdapt
er6
```

Рисунок 211 – Добавление виртуальных сетевых адаптеров в операционную систему управления

Далее надо настроить частную сеть. Частная сеть - тип сети, где виртуальный коммутатор может быть подключен только к виртуальным машинам и изолирован от хоста.

Для настройки IP-адреса сети и маски на каждом виртуальном сетевом адаптере виртуальных машин vm4, vm5, vm6 и хоста используется командлет `New-NetIPAddress`.

В этом примере с помощью командлета `New-NetIPAddress` настраиваются конфигурации сети виртуальных машин vm4, vm5, vm6 (см. рисунки с 212 по 214).

```
PS C:\Users\Администратор.WPS> New-NetIPAddress -InterfaceAlias "VEthernet (SetA
dapter4)" -IPAddress "192.168.200.14" -PrefixLength 24


IPAddress         : 192.168.200.14
InterfaceIndex    : 199
InterfaceAlias    : vEthernet (SetAdapter4)
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 192.168.200.14
InterfaceIndex    : 199
InterfaceAlias    : vEthernet (SetAdapter4)
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore
```

Рисунок 212 - Настройка сети виртуальной машины vm4

```
PS C:\Users\Администратор.WPS> New-NetIPAddress -InterfaceAlias "VEthernet (SetA
dapter5)" -IPAddress "192.168.200.15" -PrefixLength 24


IPAddress         : 192.168.200.15
InterfaceIndex    : 226
InterfaceAlias    : vEthernet (SetAdapter5)
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 192.168.200.15
InterfaceIndex    : 226
InterfaceAlias    : vEthernet (SetAdapter5)
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore
```

Рисунок 213 – Настройка сети виртуальной машины vm5

```
PS C:\Users\Администратор.WPS> New-NetIPAddress -InterfaceAlias "VEthernet (SetA
dapter6)" -IPAddress "192.168.200.17" -PrefixLength 24


IPAddress         : 192.168.200.17
InterfaceIndex    : 251
InterfaceAlias    : vEthernet (SetAdapter6)
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 192.168.200.17
InterfaceIndex    : 251
InterfaceAlias    : vEthernet (SetAdapter6)
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore
```

Рисунок 214 – Настройка сети виртуальной машины vm6

Создание стандартных списков контроля доступа. Для создания стандартных списков доступа используется командлет `Add-VMNetworkAdapterAcl`, который создает ACL для применения к трафику через сетевой адаптер виртуальной машины. Когда создается виртуальный сетевой адаптер, на нем нет ACL. Учитывая список записей ACL на основе IP, которые должны быть применены к трафику в том же направлении, самое длинное правило соответствия решает, какая из записей является наиболее подходящей для применения к определенному пакету.

В этом примере с помощью командлета Add-VMNetworkAdapterAcl создается стандартный список контроля доступа, чтобы разрешить виртуальной машине vm5 отправлять и получать трафик из IP-подсети 192.168.200.11 (см. рисунок 215).

```
PS C:\Users\Администратор.WPS> Add-VMNetworkAdapterAcl -VMName vm5 -RemoteIPAddr
ess 192.168.200.11 -Direction Both -Action Allow
```

Рисунок 215 – Создание стандартного списка контроля доступа для разрешения виртуальной машине отправлять и получать трафик

Значение параметра `–VMName` задает имя виртуальной машины, к которой должен применяться ACL, значение параметра `–RemoteIPAddress` указывает удаленный IP-адрес, к которому должен применяться этот ACL, значение параметра `-Direction` Задает направление сетевого трафика, к которому должен применяться ACL.

В этом примере с помощью командлета `Add-VMNetworkAdapterAcl` создается стандартный список контроля, который запрещает виртуальной машине vm6 отправлять трафик IPv4 или IPv6 в любое место и получать такой трафик из любого места, значение параметра `–Action` задает действие для ACL. Допустимые значения: разрешить, запретить и счетчик. `–Name` указывает имя удаляемого виртуального сетевого адаптера (см. рисунок 216).

Рисунок 216 - Создание стандартного списка контроля доступа, который запрещает виртуальной машине отправлять трафик IPv4 или IPv6 в любое место и получать такой трафик из любого места

Основными параметрами командлета `Add-VMNetworkAdapterAcl` являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых должен быть создан ACL;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия;

– Confirm – запрашивает подтверждение перед запуском командлета;

– Action – задает действие для ACL. Допустимые значения: разрешить, запретить и счетчик;

–Name – указывает имя удаляемого виртуального сетевого адаптера;

– Direction – задает направление сетевого трафика, к которому должен применяться ACL. Допустимые значения-входящие, исходящие или оба вместе;

– LocalIPAddress – указывает локальный IP-адрес, к которому должен применяться ACL;

– LocalMacAddress – указывает локальный MAC-адрес, к которому должен применяться ACL;

– ManagementOS – указывает, что ACL должен применяться в операционной системе управления;

– RemoteIPAddress – указывает удаленный IP-адрес, к которому должен применяться этот ACL;

– RemoteMacAddress – указывает удаленный MAC-адрес, к которому должен применяться этот ACL;

– Passthru – указывает, что объект должен быть передан в конвейер, представляющий добавляемый ACL;

– VM – указывает виртуальную машину, к которой должен применяться ACL;

– VMName – задает имя виртуальной машины, к которой должен применяться ACL;

– VMNetworkAdapter – указывает сетевой адаптер виртуальной машины, который необходимо удалить;

– WhatIf – показывает, что произойдет, если командлет будет запущен;

– VMNetworkAdapter – указывает сетевой адаптер виртуальной машины, к которому должен применяться ACL;

– VMNetworkAdapterName – задает имя сетевого адаптера виртуальной машины, к которому должен применяться ACL.

Обеспечение безопасности компонентов виртуальной инфраструктуры. Для того чтобы создать учетную запись на гипервизоре необходимо в консольном окне ввести команду `Net user /Add` (см. рисунок).

В этом примере с помощью команды `Net user /Add` создается учетная запись пользователя на гипервизоре (см. рисунок 217).

Рисунок 217 – Создание учетной записи на гипервизоре

В этом примере с помощью командлета New-VHD проверяется возможность создания вирутального жесткого диска с объемом памяти 5 Гб (см. рисунок 218).

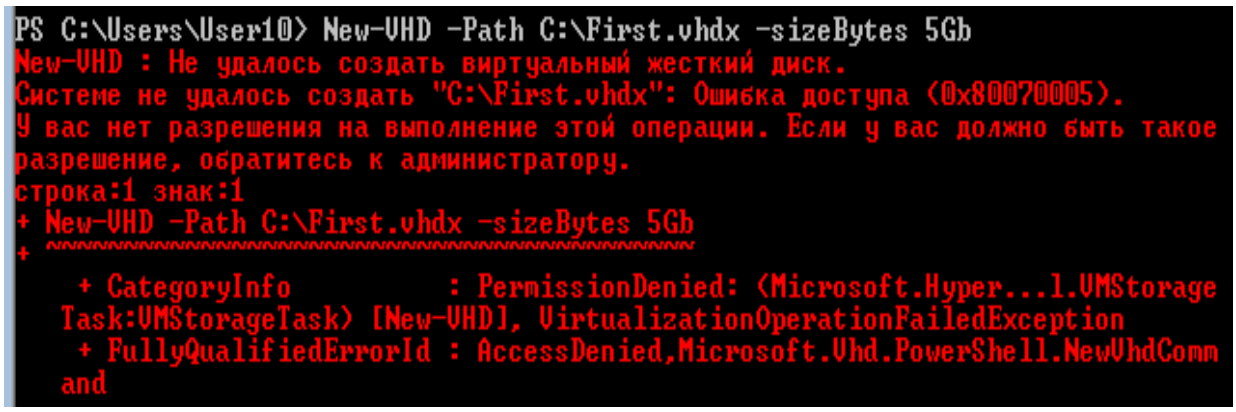


Рисунок 218 - Проверка возможность создания вирутального жесткого диска с объемом памяти 5 Гб

Так как у учетной записи пользователя User10 нет разрешения на выполнение этой операции командлет не выполняется.

Чтобы добавить пользователя в группу локальных администраторов необходимо ввести команду `Net local group /add` (см. рисунок 219).

Рисунок 219 – Добавление пользователя в группу локальных администраторов

В этом примере с помощью командлета New-VHD проверяется возможность создания вирутального жесткого диска с объемом памяти 5 Гб на учетной записи пользователя User10 (см. рисунок 220).

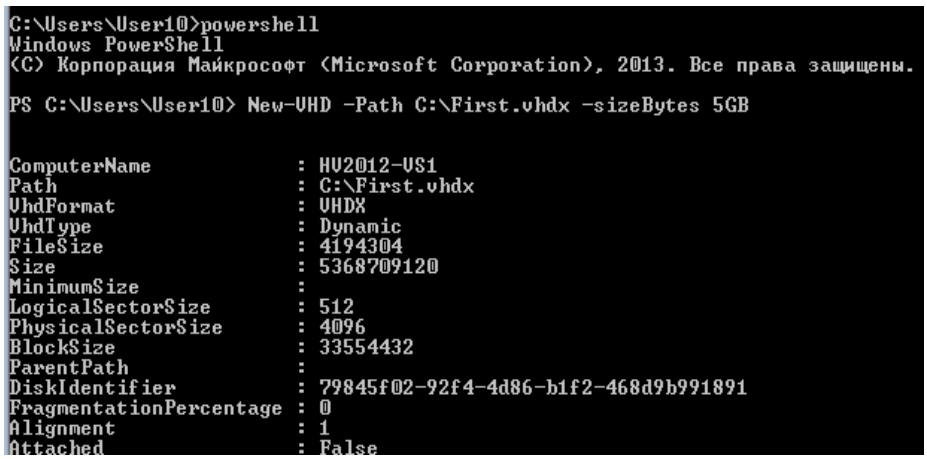


Рисунок 220 - Проверка возможность создания вирутального жесткого диска с объемом памяти 5 Гб

В этом примере с помощью командлета New-VHD проверяется возможность создания вирутальной машины с объемом памяти 512 MB на учетной записи пользователя User10.

Так как пользователь User10 был добавлен в список локальных администраторов, ему разрешены все права (см. рисунок 221).

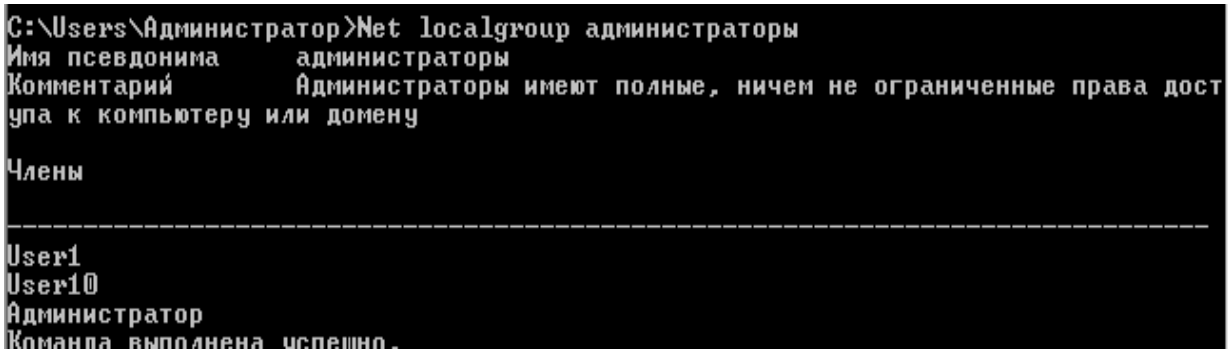


Рисунок 221 – Добавление пользователя User10 в список локальных администраторов

Для того, чтобы создать доменную учетную запись на контроллере домена WS2012-DC необходимо в нижней панели задач операционной системы открыть консоль управления «Диспетчер серверов», выбрать выпадающий список команд «Средства», далее выбрать команду «Пользователи и компьютеры Active Directory». Откроется диалоговое окно «Active Directory – пользователи и компьютеры». В верхней части панели нажать на раздел «Создание нового пользователя в текущем контейнере» (см. рисунок 222).

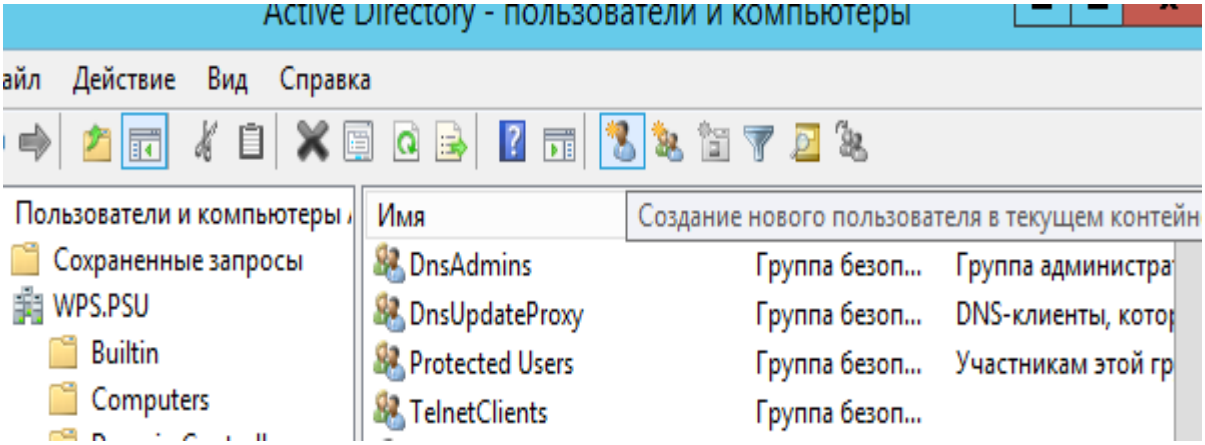


Рисунок 222 – Создание нового пользователя

Откроется диалоговое окно «Новый объект - Пользователь». В поле «Имя» ввести имя учетной записи доменного пользователя. В поле «Имя входа пользователя» надо ввести имя пользователя при входе в систему. Нажать кнопку «Далее». Остальные поля оставить без изменений (см. рисунок 223).

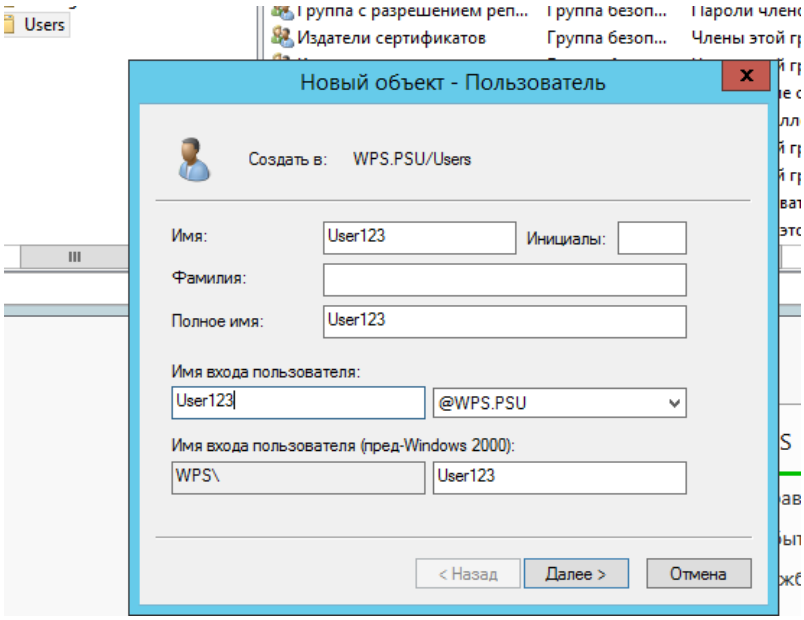


Рисунок 223– Создание учетной записи доменного пользователя

В поле «Пароль» ввести пароль нового пользователя, в поле «Подтверждение» ввести подтверждение этого пароля. Нажать кнопку Далее. (см. рисунок 224).

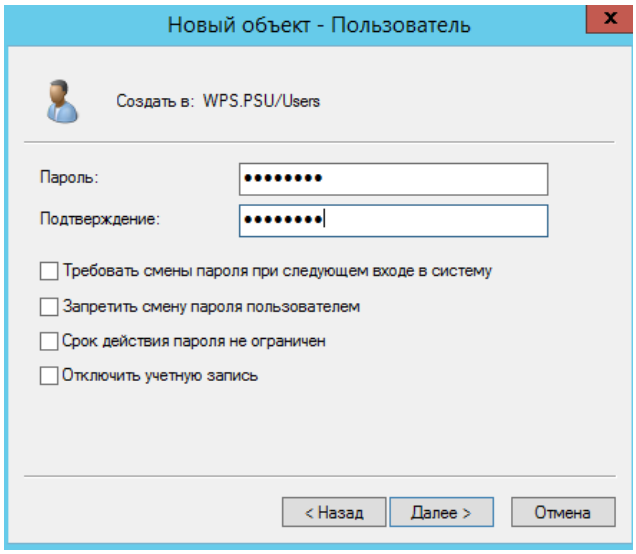


Рисунок 224 – Создание пароля нового пользователя

После этого нажать кнопку «Готово» (см. рисунок 225).

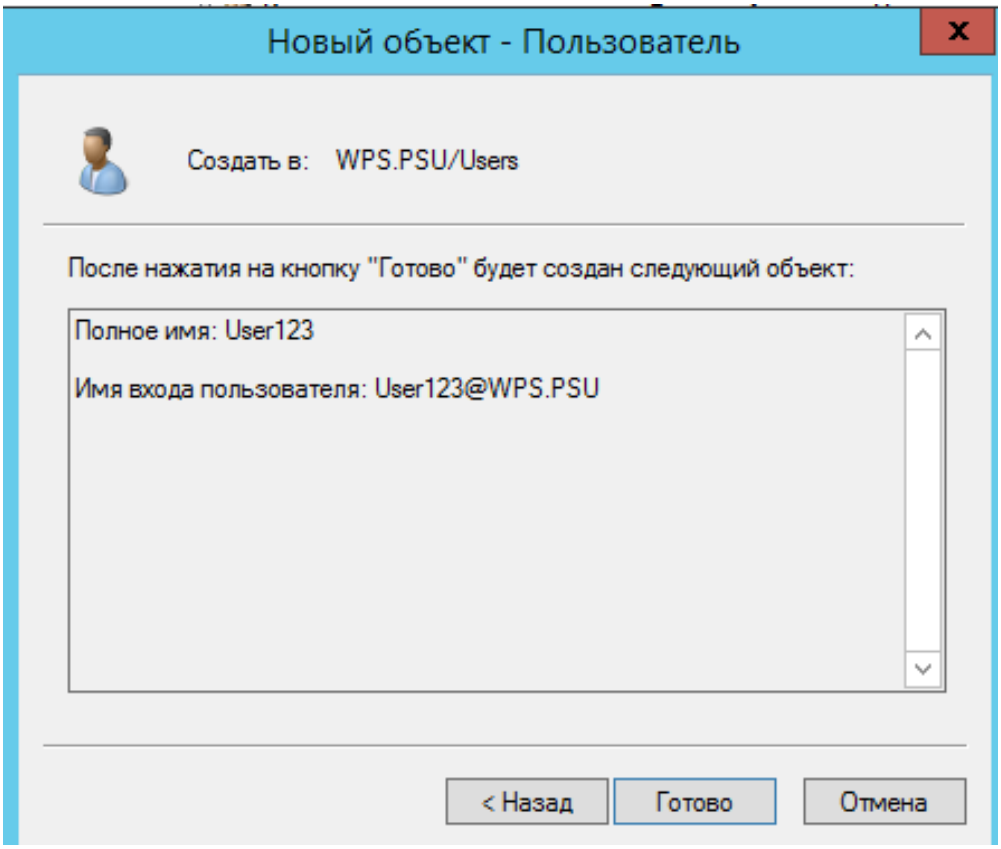


Рисунок 225 – Завершение создание доменного пользователя

Далее необходимо зайти в систему на контролере домена под учетной записи нового пользователя. При попытке входа выйдет предупреждение «Этот метод вход запрещено использовать…» (см. рисунок 226).

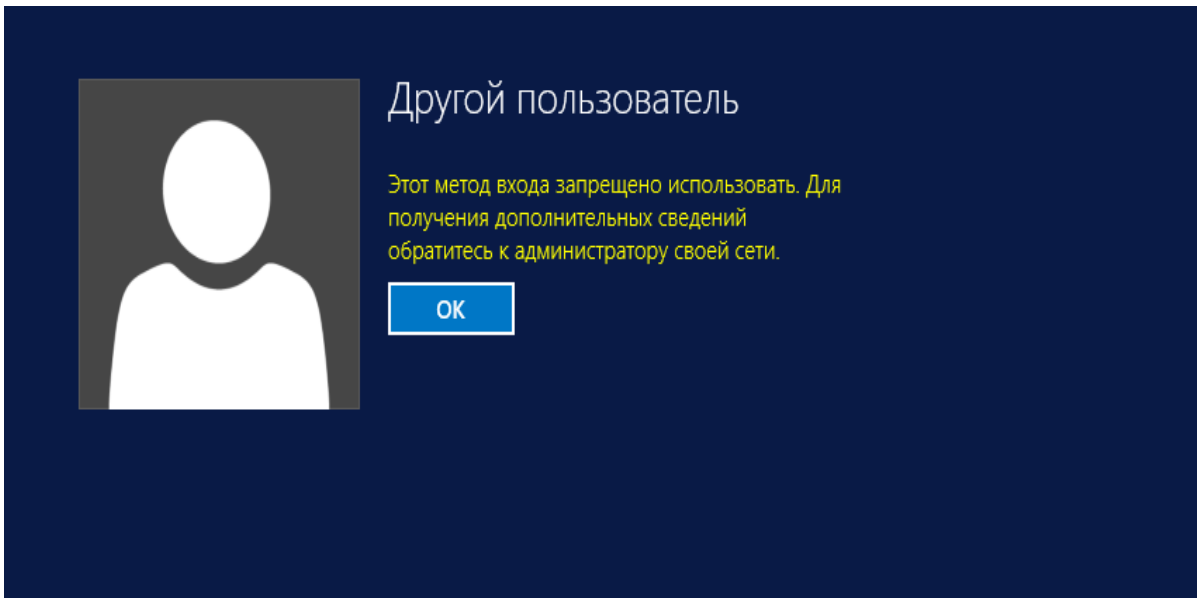


Рисунок 226 – Попытка входа на учетную запись User12345

Таким образом, под доменной учетной записью User12345 зайти в систему нельзя.

Создание пула ресурсов. Пул ресурсов — это логическое объединение серверов управления или серверов шлюзов, которые распределяют между собой рабочие нагрузки и принимают на себя рабочие нагрузки в случае сбоя одного из членов.

Командлет `New-VMResourcePool` создает пул ресурсов.

В этом примере создается новый пул ресурсов виртуального жесткого диска, связанный с одним путем (см. рисунок 227).

Рисунок 227 – Создание нового пула ресурсов виртуального жесткого диска

Основными параметрами командлета `New-VMResourcePool` являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– Credential – определяет одну или более учетных записей пользователей, которые имеют разрешение на выполнение этого действия. По умолчанию это учетная запись текущего пользователя;

– ParentName – задает имя родительского пула ресурсов для нового пула ресурсов;

– Confirm – запрашивает подтверждение перед запуском командлета;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых должен быть создан пул ресурсов. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный

компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– ResourcePoolType – указывает тип ресурса пула ресурсов;

– WhatIf – показывает, что произойдет, если командлет будет выполнен. При этом сразу после запуска командлет не выполняется;

– Paths – задает массив путей, связанных с новым пулом ресурсов хранения;

– Name – указывает имя пула ресурсов.

Возврат контрольных точек, связанных с виртуальной машиной или контрольной точкой. Контрольные точки гипервизоров, в отличие от точек восстановления или резервных копий, хранят в себе информацию не только о состоянии гостевой ОС. В гипервизорах контрольные точки предусматривают фиксацию и состояния установленной операционной системы, и конфигурации оборудования виртуальной машины.

Командлет `Get-VMSnapshot` возвращает контрольные точки, связанные с виртуальной машиной или контрольной точкой.

В этом примере с помощью командлета `Get-VMSnapsot` отображаются контрольные точки виртуальной машины vm1 (см. рисунок 228).

```
PS C:\Users\Администратор.WPS> Get-VMSnapshot -VMName vm1

VMName Name       SnapshotType CreationTime        ParentSnapshotName
------ ----       ------------ ------------        ------------------
vm1    kontrpoint Standard     09.05.2020 16:29:47
```

Рисунок 228 – Отображение контрольных точек виртуальной машины

В этом примере отображаются все стандартные контрольные точки виртуальной машины vm1 (см. рисунок 229).

```
PS C:\Users\Администратор.WPS> Get-VM -Name vm1 | Get-VMSnapshot -SnapshotType S
tandard

VMName Name       SnapshotType CreationTime        ParentSnapshotName
------ ----       ------------ ------------        ------------------
vm1    kontrpoint Standard     09.05.2020 16:29:47
```

Рисунок 229 – Отображение стандартных контрольных точек виртуальной машины

Значение параметра `-SnapshotType` указывает тип контрольных точек.

Основными параметрами командлета `Get-VMSnapshot` являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

–ParentName – задает имя родительского пула ресурсов для нового пула ресурсов;

– Confirm – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых должны быть получены контрольные точки. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– ChildOf – указывает контрольную точку, дочерние контрольные точки которой должны быть извлечены;

– WhatIf – показывает, что произойдет, если командлет будет выполнен. При этом сразу после запуска командлет не выполняется;

– Id – указывает уникальный идентификатор виртуальной машины, контрольные точки которой должны быть получены;

– Name – указывает имя контрольной точки, которая будет получена;

– ParentOf – указывает контрольную точку, непосредственная родительская контрольная точка которой должна быть получена;

– SnapshotType – указывает тип контрольных точек;

– VMName – указывает имя виртуальной машины, контрольные точки которой должны быть получены;

– VM – указывает виртуальную машину, контрольные точки которой должны быть получены;

– Path – указывает путь к папке, в которую будет экспортирована контрольная точка.

Экспорт контрольной точки виртуальной машины на диск. Экспортированные контрольные точки можно использовать для резервного копирования. Экспорт объединяет контрольные точки в пакет как виртуальную машину, так что контрольную точку можно переместить в новое место.

Командлет `Export-VMSnapshot` экспортирует контрольную точку виртуальной машины на диск.

В этом примере осуществляется экспорт контрольной точки «kontrpoint» виртуальной машины vm1 на диск C (см. рисунок 230).

Рисунок 230– Экспорт контрольной точки

Основными параметрами командлета `Export-VMSnapshot` являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых будет экспортироваться контрольная точка виртуальной машины. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– Confirm – запрашивает подтверждение перед запуском командлета;

– WhatIf – показывает, что произойдет, если командлет будет выполнен. При этом сразу после запуска командлет не выполняется;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– Name – указывает имя контрольной точки, которая будет получена;

– VMSnapshot – указывает контрольную точку, подлежащую экспорту;

– SnapshotType – указывает какой тип контрольных точек должен быть получен;

– VMName – указывает имя виртуальной машины, из которой будет экспортироваться контрольная точка;

– VM – указывает виртуальную машину, из которой будет экспортироваться контрольная точка.

Возврат процессора виртуальной машины или моментальный снимок. Командлет Get-VMProcessor возвращает процессор виртуальной машины (рисунок 231).

Рисунок 231 – Отображение процессора виртуальной машины

Основными параметрами командлета Get-VMProcessor являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых должен быть получен процессор виртуальной машины или моментальный снимок. Допустимы имена NetBIOS, IP-адреса и полные

доменные имена. По умолчанию используется локальный компьютер. Надо ввести localhost или точку (.) чтобы явно указать локальный компьютер;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– VMSnapshot – указывает моментальный снимок, процессор которого должен быть извлечен;

– VMName – задает имя виртуальной машины, процессор которой должен быть извлечен;

– VM – указывает виртуальную машину, процессор которой должен быть извлечен.

Настройка параметров для виртуальных процессоров виртуальной машины. Для того, чтобы настроить параметры для виртуальных процессоров виртуальной машины используется командлет `Set-VMProcessor`. Настройки применяются равномерно ко всем виртуальным процессорам, принадлежащим виртуальной машине.

В этом примере настраивается виртуальная машина vm1 с одним виртуальным процессором, резервом 10%, пределом 75% и приоритет распределения вычислительной мощности физического компьютера 200 (см. рисунок 232).

Рисунок 232 – Настройка виртуальной машины с одним виртуальным процессором, резервом 10%, пределом 75% и приоритет распределения вычислительной мощности физического компьютера 200

Значение параметра `-Count` задает количество виртуальных процессоров для виртуальной машины, значение параметра `-Reserve` указывает процент ресурсов процессора, зарезервированных для этой виртуальной машины, значение параметра `-Maximum` задает максимальный процент ресурсов,

доступных для конфигурируемого процессора виртуальной машины, значение параметра -RelativeWeight задает приоритет распределения вычислительной мощности физического компьютера для этой виртуальной машины относительно других.

В этом примере настраивается виртуальная машина vm1, включая совместимость процессоров для динамической миграции (см. рисунок 233).

Рисунок 233 – Настройка виртуальной машины, включая совместимость процессоров для динамической миграции

Значение параметра -CompatibilityForMigrationEnabled указывает, следует ли ограничивать возможности виртуального процессора для обеспечения совместимости при переносе виртуальной машины на другой узел.

Настраивает виртуальной машины vm1, обеспечивая совместимость для запуска более старых операционных систем(см. рисунок 234).

Рисунок 234 – Настройка виртуальной машины, включая совместимость для запуска более старых операционных систем

Параметр -CompatibilityForOlderOperatingSystemsEnabled указывает, следует ли ограничить возможности виртуального процессора для обеспечения совместимости со старыми операционными системами.

Основными параметрами командлета Set-VMProcessor являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере. Надо ввести имя компьютера или объект сеанса, например

выходные данные командлета New-CimSession или Get-CimSession. По умолчанию используется текущий сеанс на локальном компьютере;

– CompatibilityForMigrationEnabled – указывает, следует ли ограничивать возможности виртуального процессора для обеспечения совместимости при переносе виртуальной машины на другой узел;

– CompatibilityForOlderOperatingSystemsEnabled – указывает, следует ли ограничить возможности виртуального процессора для обеспечения совместимости со старыми операционными системами;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых должны быть настроены процессоры. Допустимы имена NetBIOS, IP-адреса и полные доменные имена. По умолчанию используется локальный компьютер. Надо использовать localhost или точку (.) чтобы явно указать локальный компьютер;

– Confirm – запрашивает подтверждение перед запуском командлета;

– Count – задает количество виртуальных процессоров для виртуальной машины;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия. По умолчанию используется текущий пользователь;

– VMName задает – имя виртуальной машины, процессор которой должен быть извлечен;

– EnableHostResourceProtection – указывает, следует ли включить защиту ресурсов узла на виртуальной машине. Если этот параметр включен, узел будет применять ограничения на некоторые аспекты деятельности виртуальной машины, предотвращая чрезмерное потребление вычислительных ресурсов узла. Действия виртуальной машины, управляемые этим параметром, включают сообщения канала VMbus, связанные с подмножеством виртуальных устройств виртуальной машины, и перехваты, генерируемые виртуальной машиной.

Затронутые виртуальные устройства включают видео, клавиатуру, мышь и динамическую память VDEVs;

– ExposeVirtualizationExtensions – указывает, должен ли гипервизор предоставлять виртуальной машине доступ к наличию расширений виртуализации, что обеспечивает поддержку вложенной виртуализации;

– HwThreadCountPerCore – задает количество виртуальных потоков SMT, доступных для виртуальной машины. Установка этого значения в 0 означает, что виртуальная машина унаследует количество потоков узла на одно ядро. Этот параметр не может превышать количество потоков на одном ядре хоста;

– Maximum – задает максимальный процент ресурсов, доступных для конфигурируемого процессора виртуальной машины. Допустимые значения варьируются от 0 до 100;

– MaximumCountPerNumaNode – задает максимальное число процессоров на узле NUMA, которое должно быть настроено для виртуальной машины;

–MaximumCountPerNumaSocket – указывает максимальное количество сокетов на узел NUMA, которое должно быть настроено для виртуальной машины;

– Perfmon – указывает аппаратное обеспечение, которое должно быть предоставлено для мониторинга производительности;

– RelativeWeight – задает приоритет распределения вычислительной мощности физического компьютера для этой виртуальной машины относительно других. Допустимые значения варьируются от 1 до 10000;

– Reserve – указывает процент ресурсов процессора, зарезервированных для этой виртуальной машины. Допустимые значения варьируются от 0 до 100;

– ResourcePoolName – указывает имя используемого пула ресурсов процессора;

– VM – указывает виртуальную машину, на которой должен быть настроен процессор;

– VMName – задает имя виртуальной машины, на которой должен быть настроен процессор;

– VMProcessor – указывает, что необходимо настроить параметры виртуальной машины для виртуальных процессоров;

– WhatIf – показывает, что произойдет, если командлет будет запущен.

Создание расширенных списков контроля доступа. Командлет `Add-VMNetworkAdapterExtendedAcl` создает расширенный список управления доступом (ACL) для виртуального сетевого адаптера. ACL разрешает или запрещает доступ к сетевому адаптеру виртуальной машины для сетевых пакетов на основе IP-адреса источника, IP-адреса назначения, протокола, порта источника и порта назначения.

В этом примере с помощью командлета `Add-VMNetworkAdapterExtendedAcl` создается расширенный список контроля доступа, который позволяет отправлять исходящие пакеты на удаленное устройство с помощью протокола TCP (см. рисунок 235).

```
PS C:\Users\Администратор.WPS> Add-VMNetworkAdapterExtendedAcl -VMName vm4 -Acti
on Allow -Direction Outbound -RemotePort "80" -Protocol "TCP" -Weight 100
```

Рисунок 235 – Создание расширенного контроля доступа для разрешения виртуальной машине отправлять исходящие пакеты на удаленное устройство с помощью протокола TCP

Значение параметра `–VMName` задает массив имен виртуальных машин. Командлет добавляет список управления доступом для указанных виртуальных машин, значение параметра `–Action` задает действие для ACL, значение параметра `–Direction` задает направление сетевого трафика, к которому должен применяться ACL, значение параметра `–RemotePort` указывает удаленный порт для ACL., значение параметра `–Protocol` указывает протокол, к которому применяется ACL, значение параметра `–Weight` предназначено для определения порядка, в котором виртуальный коммутатор Hyper-V обрабатывает правила.

В этом примере с помощью командлета Add-VMNetworkAdapterExtendedAcl создается расширенный список контроля доступа, который позволяет удаленному устройству подключаться к виртуальной машине по порту 3389, который является портом для протокола удаленного рабочего стола (см. рисунок 236).

Рисунок 236 - Создание расширенного списка контроля доступа, который позволяет удаленному устройству подключаться к виртуальной машине по порту 3389, который является портом для протокола удаленного рабочего стола

Значение параметра –LocalPort задает локальный порт для ACL.

Основными параметрами командлета Add-VMNetworkAdapterExtendedAcl являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере;

– ComputerName – задает массив узлов Hyper-V;

– Credential – указывает одну или несколько учетных записей пользователей, имеющих разрешение на выполнение этого действия;

– Confirm – запрашивает подтверждение перед запуском командлета;

– Action – задает действие для ACL;

– Direction – задает направление сетевого трафика с точки зрения виртуальной машины,к которой применяется ACL;

– LocalIPAddress – задает локальный IP-адрес для ACL;

– IdleSessionTimeout – задает период ожидания в секундах для сеансов простоя;

– ManagementOS – указывает, что ACL должен применяться в операционной системе управления;

– RemoteIPAddress – задает локальный IP-адрес для ACL.-IsolationID. Задает идентификатор виртуальной подсети;

– RemotePort – указывает удаленный порт для ACL;

– Passthru – указывает, что объект должен быть передан в конвейер, представляющий добавляемый ACL;

– Stateful – указывает, применяется ли ACL к пакетам в обоих направлениях одного и того же сеанса;

– VM – задает массив объектов виртуальной машины. Командлет добавляет список управления доступом для указанных виртуальных машин;

– VMName – задает имя виртуальной машины, к которой должен применяться ACL;

– VMName – задает массив имен виртуальных машин. Командлет добавляет список управления доступом для указанных виртуальных машин;

– VMNetworkAdapter – командлет добавляет ACL к указанным адаптерам;

– VMNetworkAdapterName – задает имя виртуального сетевого адаптера;

– LocalPort – задает локальный порт для ACL. Для входящего пакета TCP или UDP локальный порт является портом назначения. Для исходящего пакета локальный порт является исходным портом;

– Weight – предназначен для определения порядка, в котором виртуальный коммутатор Hyper-V обрабатывает правила;

– Protocol – указывает протокол, к которому применяется ACL;

– WhatIf – показывает, что произойдет, если командлет будет запущен.

Настройка параметров виртуальной локальной сети для трафика через виртуальный сетевой адаптер. Для настройки параметров виртуальной локальной сети для трафика через виртуальный сетевой адаптер используется командлет `Set-VMNetworkAdapterVlan`.

В этом примерес помощью командлета `Set-VMNetworkAdapterVlan` устанавливает виртуальный сетевой адаптер в виртуальной машине vm4 в

режим доступа. Трафик, отправляемый этой виртуальной машиной, помечается идентификатором VLAN 55 (см. рисунок 237).

Рисунок 237 – Установка виртуального сетевого адаптера в виртуальной машине в режим доступа

Значение параметра `-VMName` задает имя виртуальной машины, значение параметра `-Access` задает направление сетевого трафика с точки зрения виртуальной машины, к которой применяется ACL, значение параметра `-VlanId` задает идентификатор виртуальной локальной сети сетевого адаптера виртуальной машины.

В этом примере с помощью командлета `Set-VMNetworkAdapterVlan` устанавливается виртуальный сетевой адаптер в виртуальной машине vm4 в режим магистрали. Любой трафик, помеченный одним из идентификаторов VLAN в списке разрешенных VLAN, будет разрешен к отправке или приему VLAN. Если трафик не помечен тегами, он будет обработан так, как если бы он был на VLAN 10 (см. рисунок 238).

Рисунок 238 - Установка виртуального сетевого адаптера в виртуальной машине в режим магистрали

Значение параметра `-Trunk` задает режим магистрали для сетевого адаптера виртуальной машины, значение параметра `-AllowedVlanIdList` задает список виртуальных локальных сетей, разрешенных для сетевого адаптера виртуальной машины, значение параметра `-NativeVlanID` задает собственный идентификатор виртуальной локальной сети для сетевого адаптера виртуальной машины.

Основными параметрами командлета `Set-VMNetworkAdapterVlan` являются следующие:

– CimSession – запускает командлет в удаленном сеансе или на удаленном компьютере;

– ComputerName – указывает один или несколько узлов Hyper-V, на которых должны быть настроены параметры виртуальной локальной сети на сетевом адаптере виртуальной машины;

– Isolated – задает изолированный режим для настройки сетевого адаптера виртуальной машины;

– AllowedVlanIdList – задает список виртуальных локальных сетей, разрешенных для сетевого адаптера виртуальной машины;

– Access – задает направление сетевого трафика с точки зрения виртуальной машины,к которой применяется ACL;

– NativeVlanId – задает собственный идентификатор виртуальной локальной сети для сетевого адаптера виртуальной машины;

– PrimaryVlanId – задает основной идентификатор виртуальной локальной сети для виртуального сетевого адаптера в режиме сообщества, изолированного или беспорядочного доступа;

– ManagementOS – указывает, что ACL должен применяться в операционной системе управления;

– Promiscuous – задает неразборчивый режим для сетевого адаптера виртуальной машины;

– SecondaryVlanId – задает вторичный идентификатор виртуальной локальной сети для виртуального сетевого адаптера в режиме сообщества или изолированного режима;

– SecondaryVlanIdList – задает список частных виртуальных локальных сетей вторичных виртуальных локальных сетей на сетевом адаптере виртуальной машины;

– Trunk – задает режим магистрали для сетевого адаптера виртуальной машины;

– Untagged – задает режим без тегов для сетевого адаптера виртуальной машины;

– VM – указывает виртуальную машину;

– VMName – задает имя виртуальной машины;

–VMNetworkAdapter – указывает сетевой адаптер виртуальной машины;

– VMNetworkAdapterName – задает имя сетевого адаптера виртуальной машины;

– VlanId – задает идентификатор виртуальной локальной сети сетевого адаптера виртуальной машины.

Практическое задание предусматривает базовый и повышенный уровни сложности. Базовому уровню заданий соответствуют задачи по настройке гипервизора, проверке установки роли сервера виртуализации, компонента Hyper-V, получению списка команд для управления Hyper-V, созданию виртуальных жестких дисков, преобразованию виртуальных жестких дисков, изменению размера виртуальных жестких дисков, проверке виртуальных жестких дисков, оптимизации виртуальных жестких дисков, созданию виртуальных машин, подключению к ВМ контроллеров IDE и SCSI, включению служб интеграции для ВМ, настройке BIOS виртуальной машины поколения, заданию конфигурации микропрограммного обеспечения виртуальной машины, подключению к ВМ привода оптических дисков, переименованию виртуальной машины, удалению виртуальной машины, созданию виртуальных сетевых адаптеров, возвращению виртуальных сетевых адаптеров виртуальной машины, моментального снимка, операционной системы управления или виртуальной машины и операционной системы управления, переименованию виртуального сетевого адаптера на виртуальной машине или в операционной системе управления, удалению виртуального сетевого адаптера, созданию нового виртуального коммутатора на одном или нескольких узлах виртуальной машины, получению виртуальных коммутаторов от одного или нескольких виртуальных узлов Hyper-V, переименованию

виртуального коммутатора, удалению виртуального коммутатора, созданию и подключению виртуальных машин к виртуальному коммутатору к внутренней сети, созданию и подключению виртуальных машин к виртуальному коммутатору к частной сети, созданию стандартных списков контроля доступа, обеспечению безопасности компонентов виртуальной инфраструктуры.

Повышенному уровню сложности соответствуют задачи по созданию пула ресурсов, возврату контрольных точек, связанных с виртуальной машиной или контрольной точкой, экспорту контрольной точки виртуальной машины на диск, настройке параметров для виртуальных процессоров виртуальной машины, созданию расширенных списков контроля доступа, настройке параметров виртуальной локальной сети для трафика через виртуальный сетевой адаптер.

5 Порядок выполнения практического задания по теме «Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»

Создание жестких дисков. Для того, чтобы создать виртуальные жесткий диск необходимо запустить графическую консоль управления «Менеджер Hyper-V». Ее можно запустить на выполнение с помощью команды «Выполнить» из меню Пуск, введя имя файла консоли virtmgmt.msc. После запуска консоли «Менеджер Hyper-V» надо запустить подготовленный сервер виртуализации (ВМ с гипервизором) и в консоли выполнить подключение к этому серверу виртуализации. Для этого следует в верхней панели диспетчера Hyper-V открыть раздел «Действие», команду «Подключиться к серверу». Откроется диалоговое окно «Выбор компьютера». В этом диалоговом окне поставить отметку в пункте «Другой компьютер», щелкнуть левой кнопкой мыши по кнопке «Обзор». Откроется диалоговое окно «Выбор: "Компьютер"» После этого щелкнуть левой кнопкой мыши по кнопке «Дополнительно», в появившемся окне щелкнуть левой кнопкой мыши на кнопку «Поиск». В результатах поиска выбрать необходимый сервер виртуализации для подключения к контроллеру домена WS2012-DC. Нажать кнопку «ОК» (см. рисунок 239).

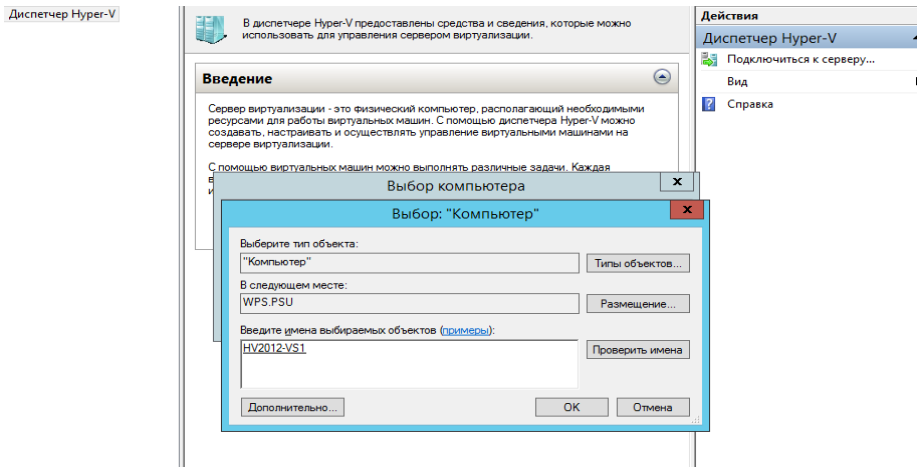


Рисунок 239 – Подключение сервера виртуализации к контроллеру домена

После подключения в правой части окна консоли будет отображен список ВМ, созданных на этом сервере (см. рисунок 240).

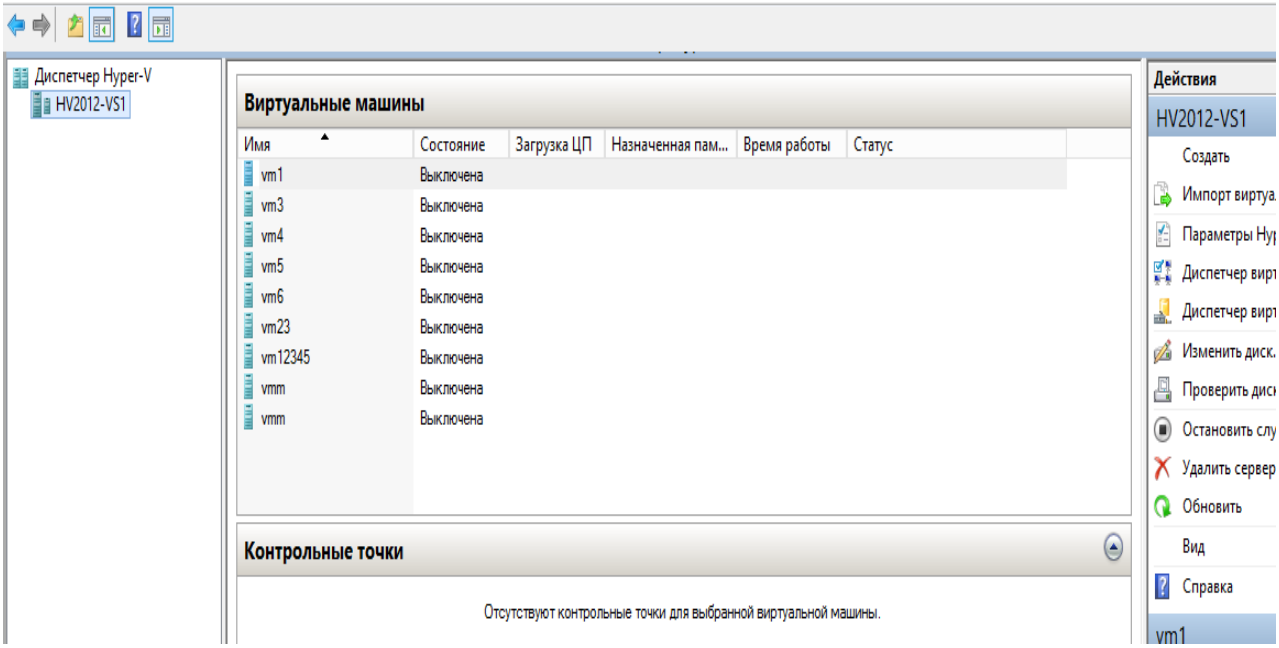


Рисунок 240 – Отображение списка ВМ, созданных на сервере

В левой панели диспетчера Hyper-V щелкнуть правой кнопкой мыши на подготовленный гипервизор. Нажать кнопку «Создать», далее нажать кнопку «Жесткий диск» (см. рисунок 241).

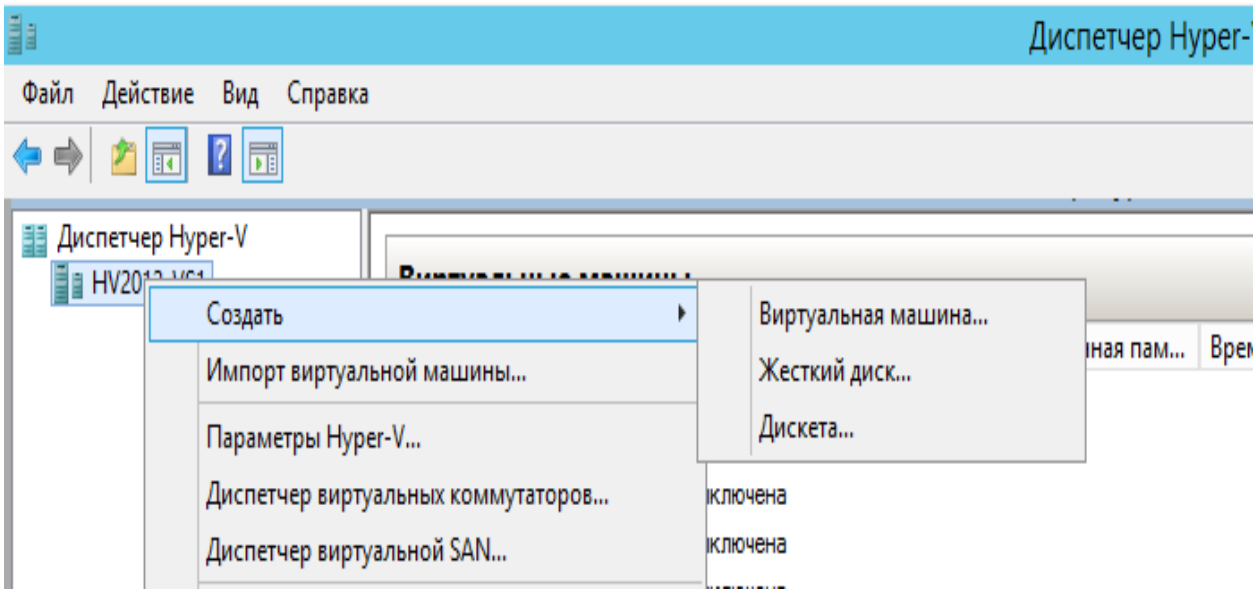


Рисунок 241 – Создание виртуального жесткого диска

Откроется окно «Мастер создания виртуального жесткого диска» (см. рисунок 242).

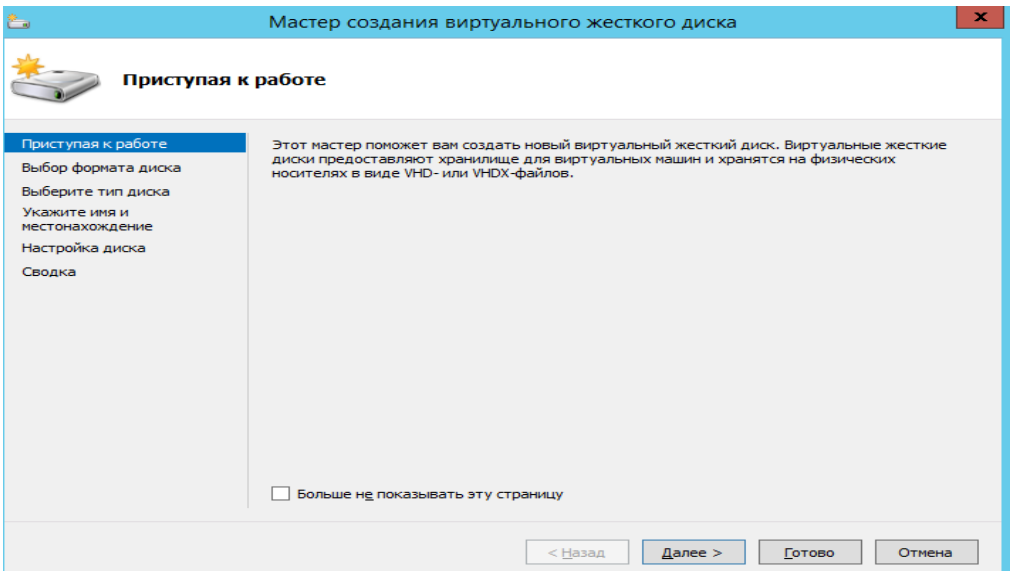


Рисунок 242 – Открытие диалогового окна «Мастер создания виртуального жесткого диска»

Нажать кнопку «Далее». На этапе «Выбор формата диска» поставить отметку в поле «VHDX» (см. рисунок 243).

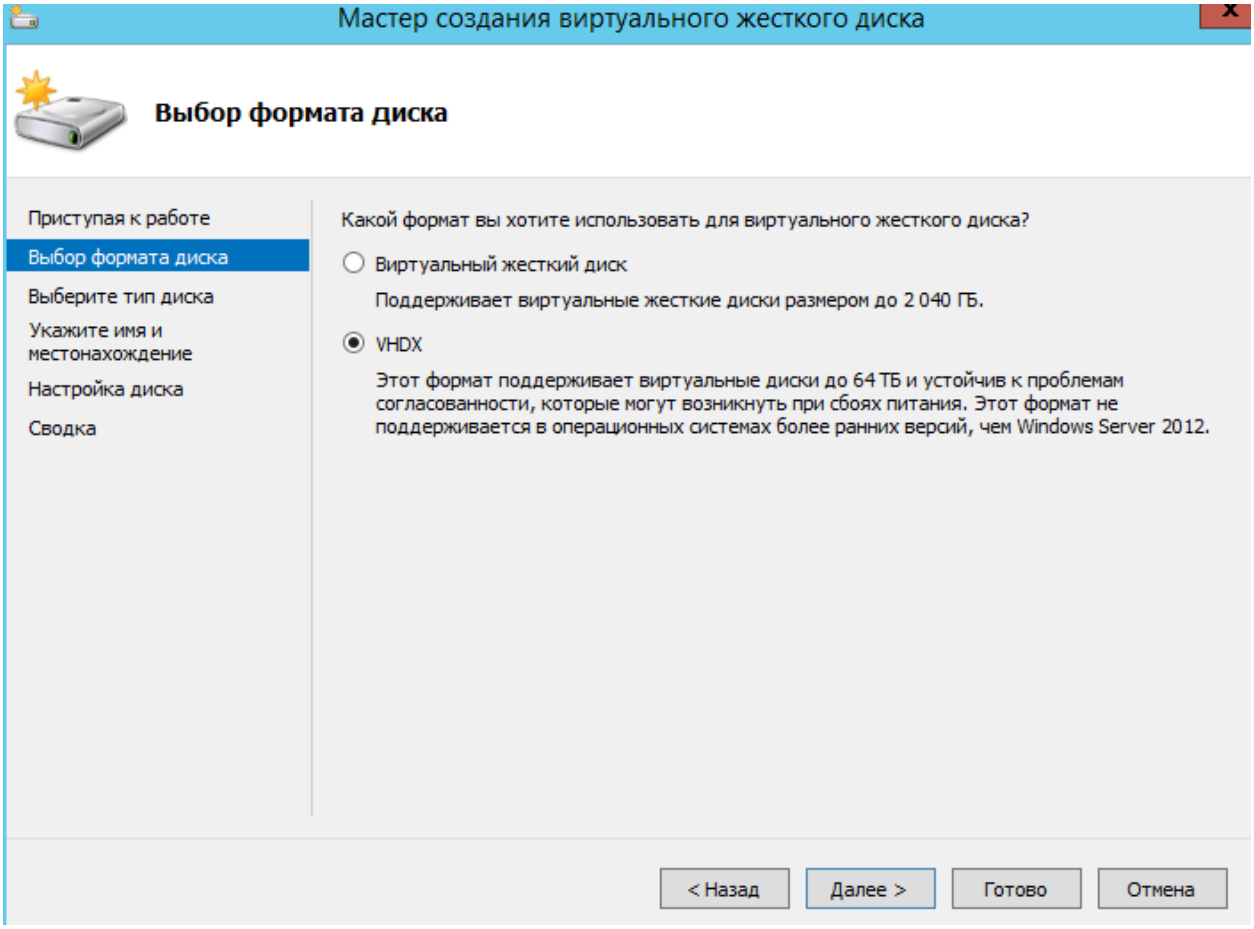


Рисунок 243 – Выбор формата диска

На этапе «Выберите тип диска» поставить отметку в поле «Динамически расширяемый». Нажать кнопку «Далее» (см. рисунок 244).

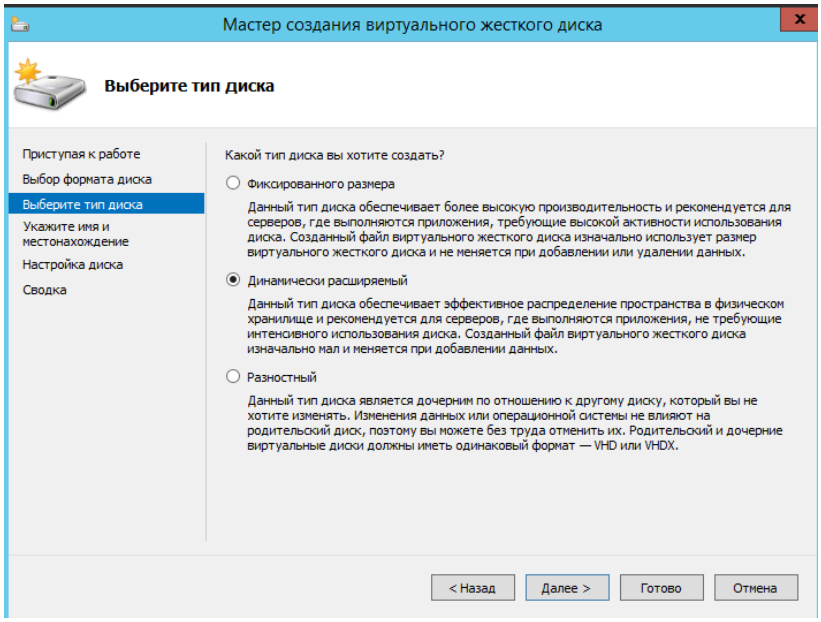


Рисунок 244 – Выберите тип диска

На этапе «Укажите имя и местонахождение» необходимо указать имя виртуального жесткого диска и указать путь сохранения виртуального жесткого диска. Нажать кнопку «Далее» (см. рисунок 245).

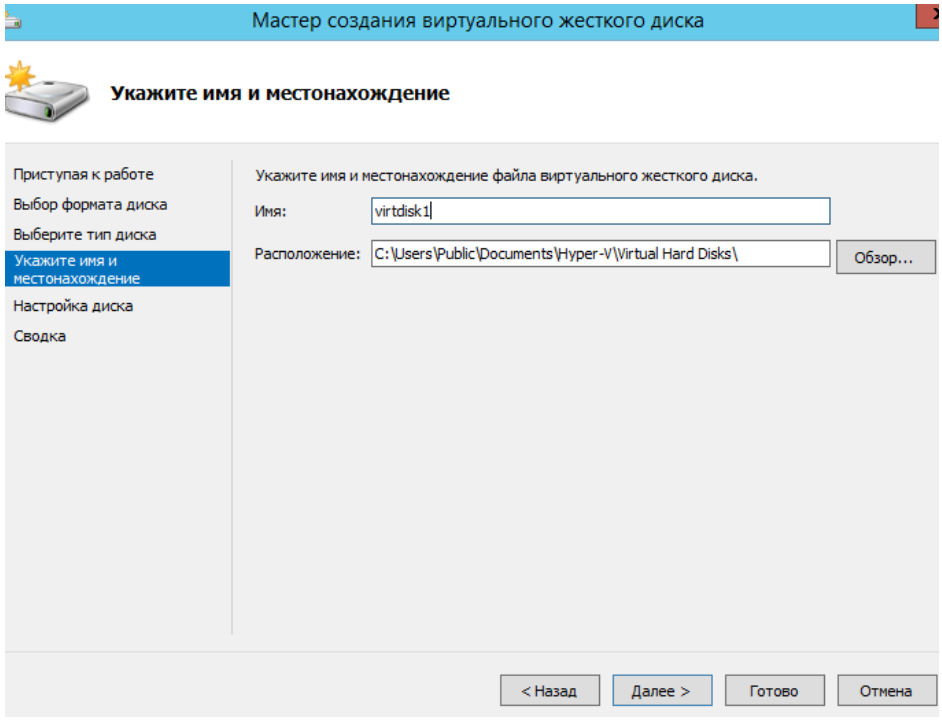


Рисунок 245 – Указание имени и местонахождения виртуальной машины

На этапе «Настройка диска» поставить отметку в поле «Создать пустой виртуальный жесткий диск». Нажать кнопку «Далее» (см. рисунок 246).

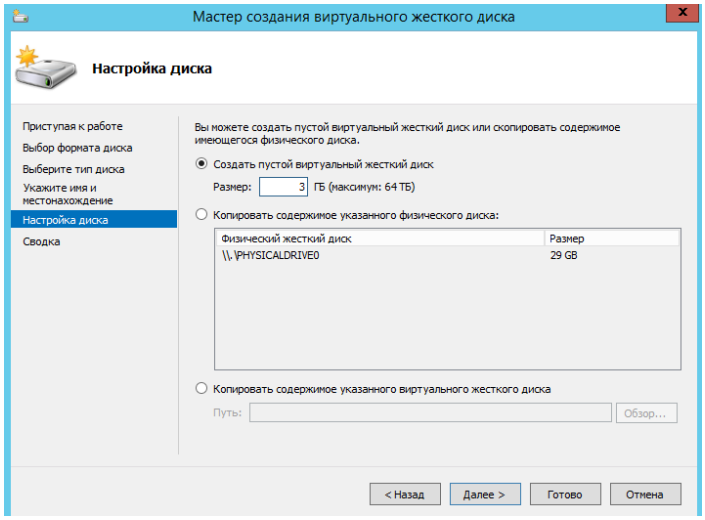


Рисунок 246 – Настройка диска

На этапе «Сводка» нажать кнопку «Готово» (см. рисунок 247).

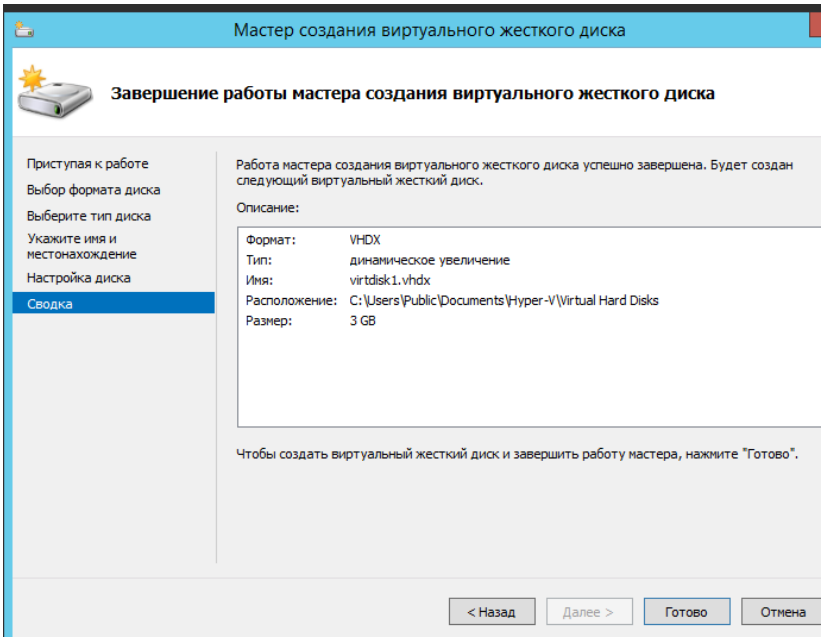


Рисунок 247 – Завершение работы мастера создания виртуального жесткого диска

Чтобы убедиться, что виртуальный жесткий диск создан успешно, необходимо в левой панели диспетчера Hyper-V щелкнуть правой кнопкой мыши по гипервизору, на котором создавался виртуальный жесткий диск. В выпадающем списке нажать кнопку «Проверить диск». В полученном

диалоговом окне должен отобразиться созданный виртуальный жесткий диск (см. рисунок 248).

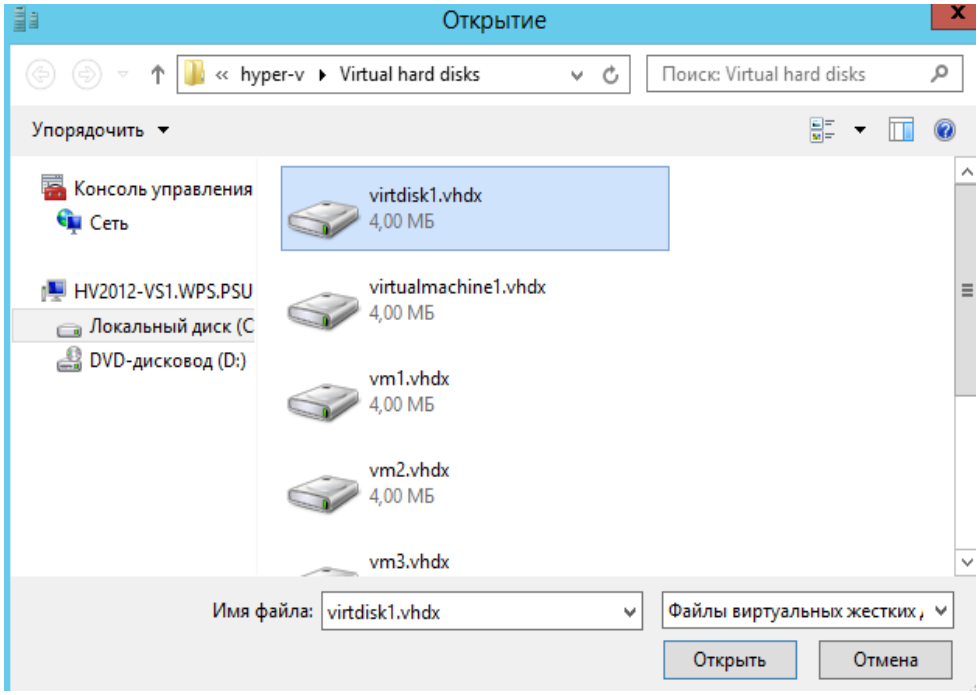


Рисунок 248 – Проверка созданного виртуального жесткого диска

Создание виртуальной машины. Для того чтобы создать виртуальную машину необходимо запустить графическую консоль управления «Менеджер Hyper-V». Его можно запустить на выполнение с помощью команды «Выполнить» из меню Пуск, введя имя файла консоли virtmgmt.msc. После запуска консоли «Менеджер Hyper-V» надо запустить подготовленной сервер виртуализации (ВМ с гипервизором) и в консоли выполнить подключение к этому серверу виртуализации. Для этого следует в верхней панели диспетчера Hyper-V открыть раздел «Действие», команду «Подключиться к серверу». Откроется диалоговое окно «Выбор компьютера». В этом диалоговом окне поставить отметку в пункте «Другой компьютер», щелкнуть левой кнопкой мыши по кнопке «Обзор». Откроется диалоговое окно «Выбор: "Компьютер"» После этого щелкнуть левой кнопкой мыши по кнопке «Дополнительно», в появившемся окне щелкнуть левой кнопкой мыши на кнопку «Поиск». В результатах поиска выбрать необходимый сервер виртуализации для

подключения к контроллеру домена WS2012-DC. Нажать кнопку «ОК» (см. рисунок 249).

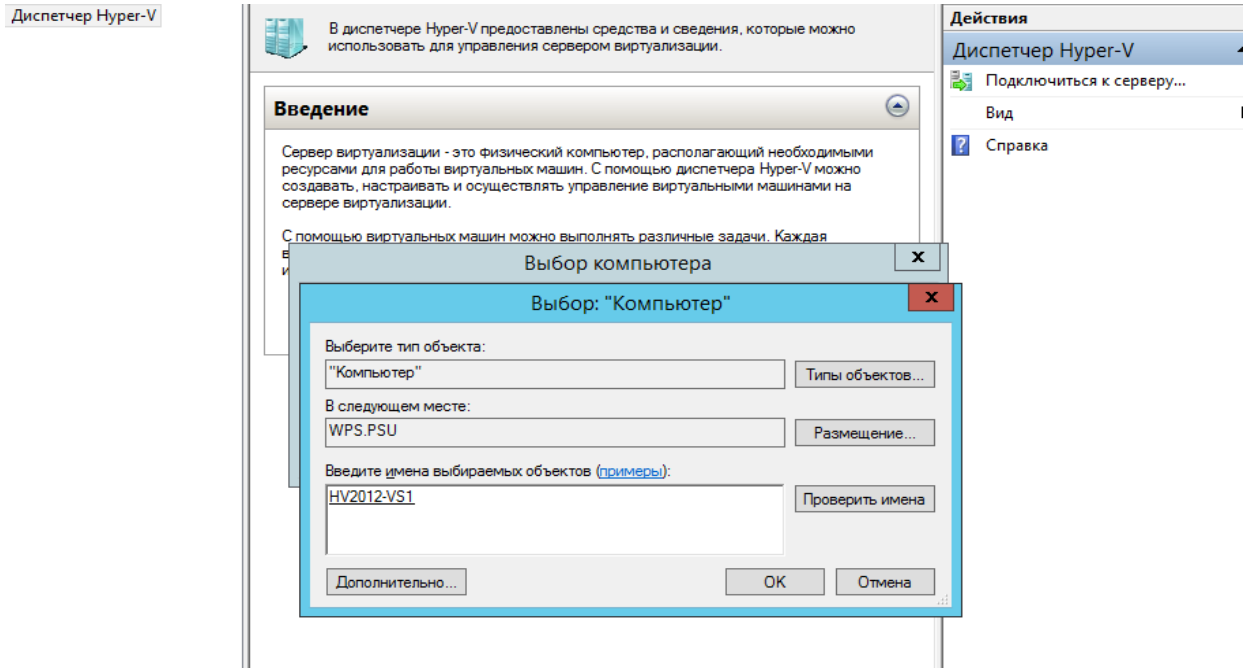


Рисунок 249 – Подключение сервера виртуализации к контроллеру домена

После подключения в правой части окна консоли будет отображен список ВМ, созданных на этом сервере (см. рисунок 250).

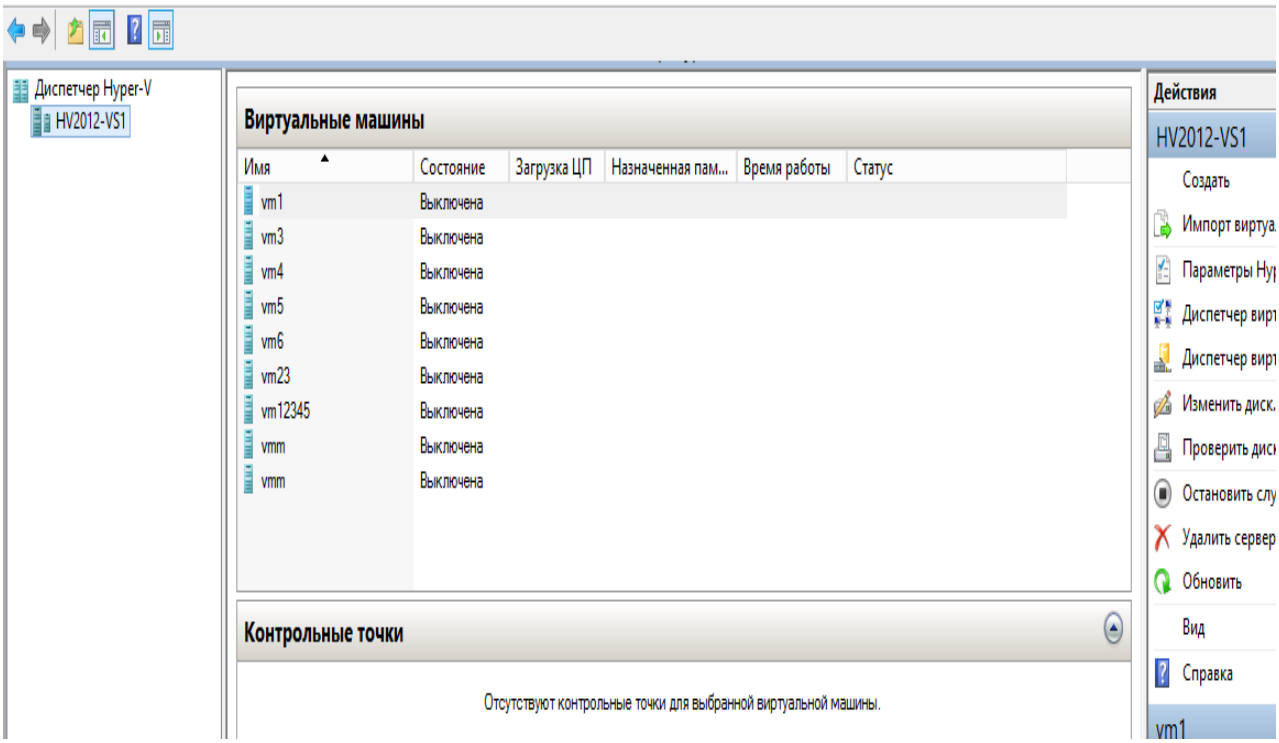


Рисунок 250 – Отображение списка ВМ, созданных на сервере

В левой панели диспетчера Hyper-V щелкнуть правой кнопкой мыши на подготовленный гипервизор. Нажать кнопку «Создать», далее нажать кнопку «Виртуальная машина» (см. рисунок 251).

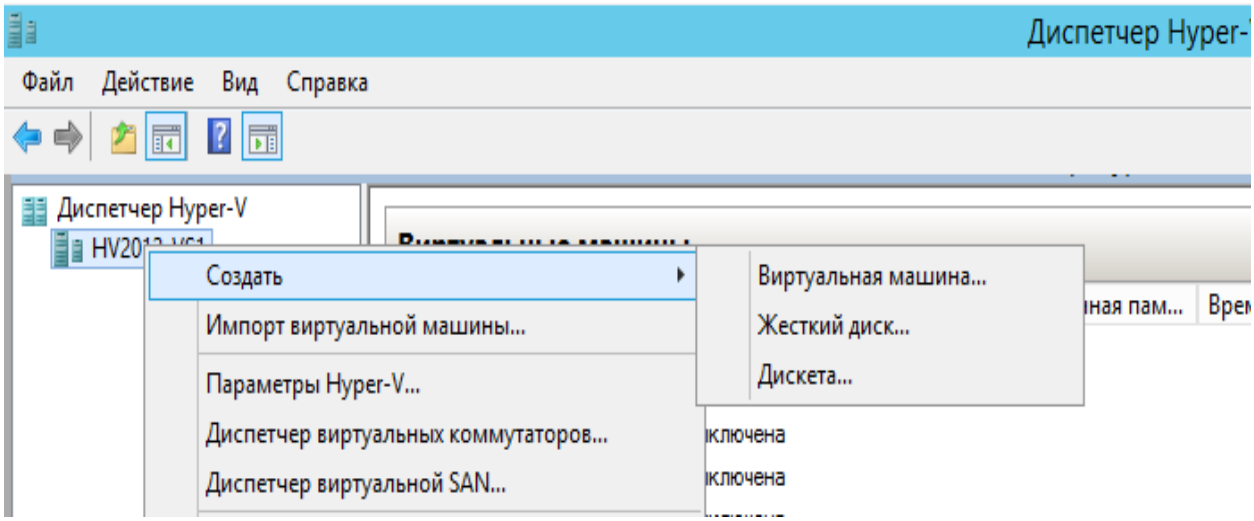


Рисунок 251– Создание виртуальной машины

Откроется окно «Мастер создания виртуальной машины». Нажать кнопку «Далее» (см. рисунок 252).

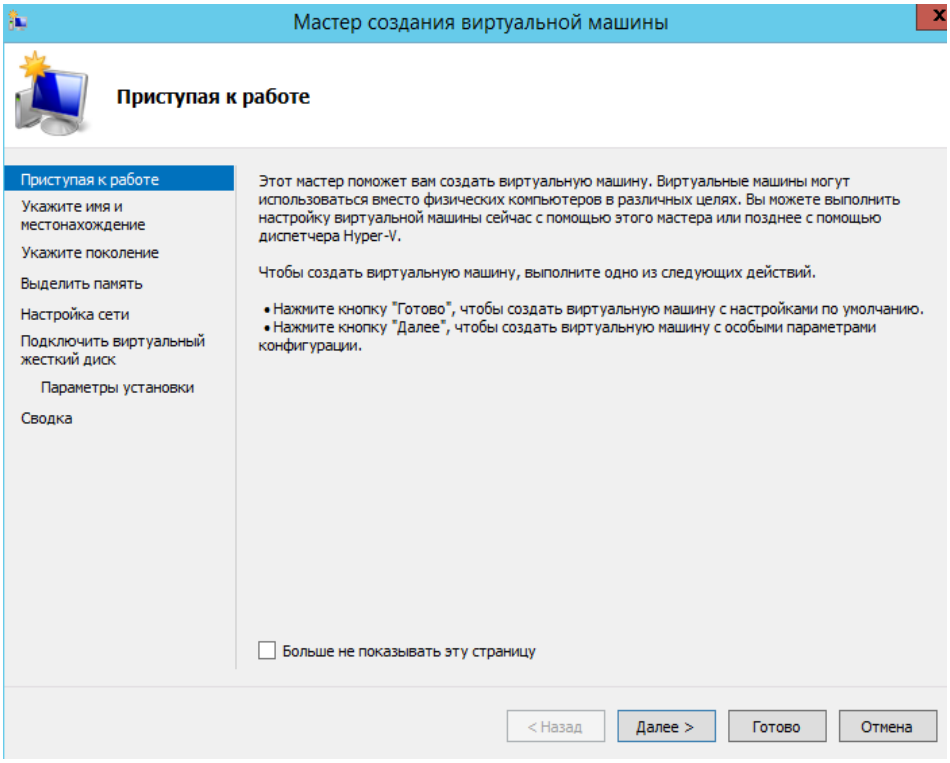


Рисунок 252 – Открытие диалогового окна «Мастер создания виртуальной машины»

На этапе «Укажите имя и местонахождение» указать имя новой виртуальной машины и местонахождение. Нажать кнопку «Далее» (см. рисунок 253).

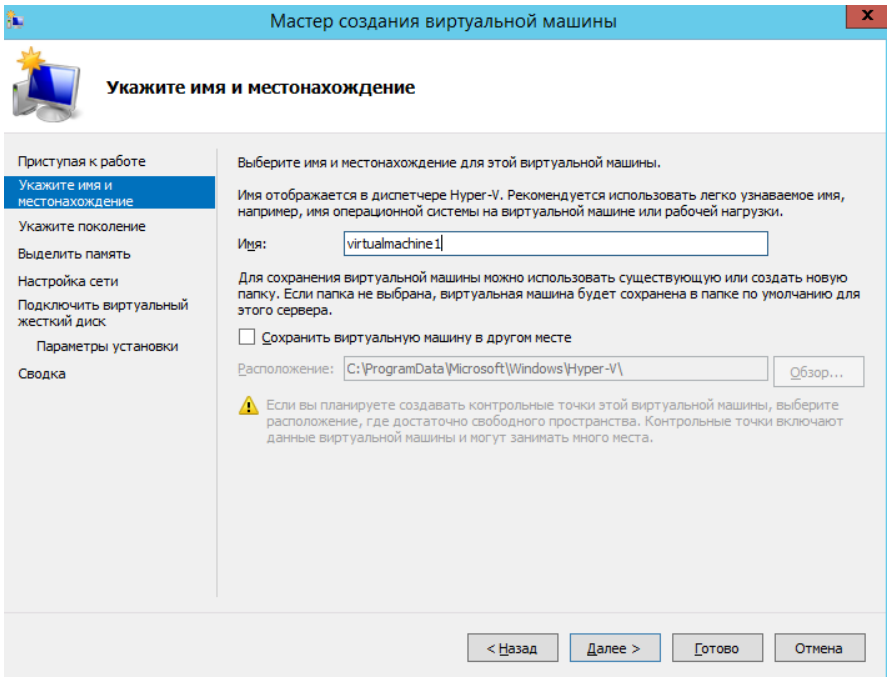


Рисунок 253 – Указание имени и местонахождения виртуальной машины

На этапе «Укажите поколение» поставить отметку в поле «Поколение 1» Нажать кнопку «Далее» (см. рисунок 254).

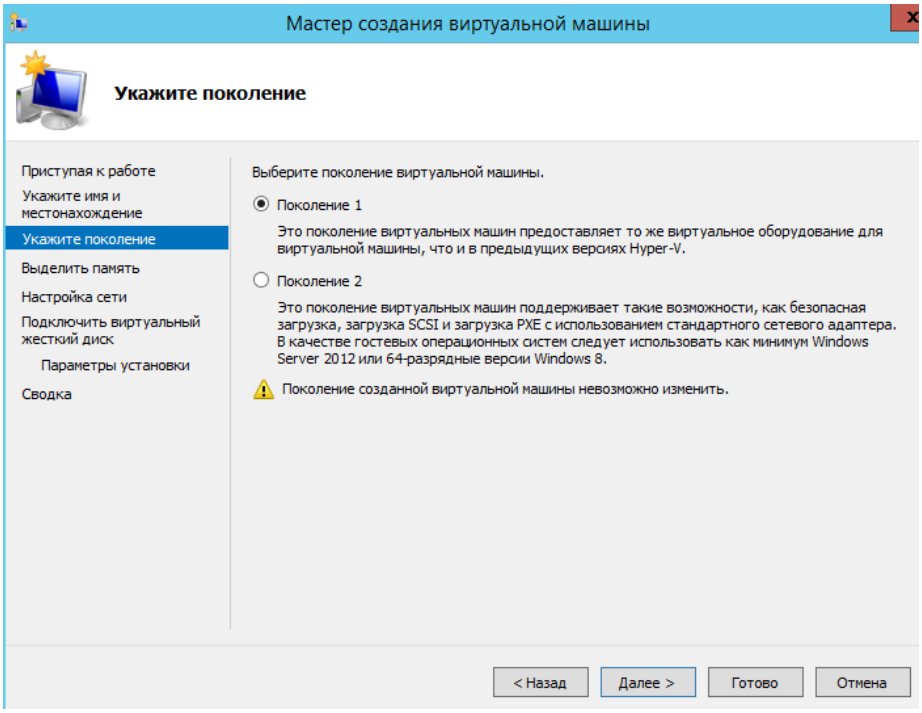


Рисунок 254 – Указание поколения виртуальной машины

На этапе «Выделите память» назначить память, выделенную при запуске 32 МБ. Нажать кнопку «Далее» (см. рисунок 255).

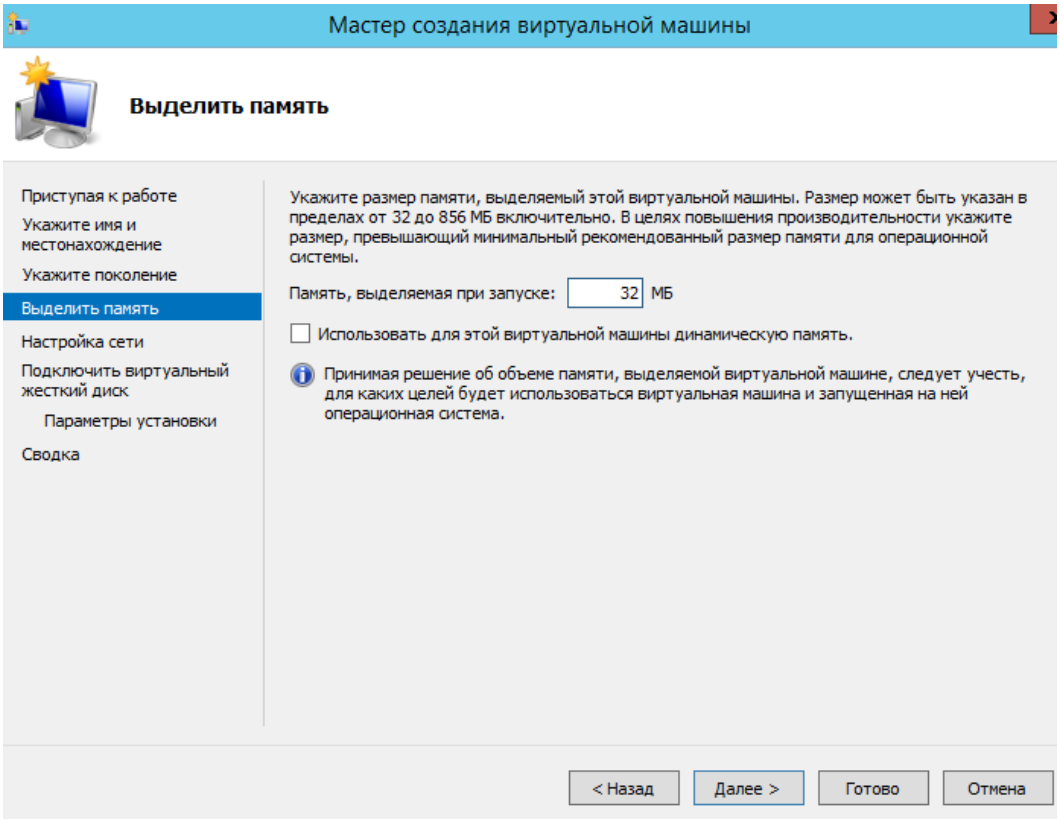


Рисунок 255 – Выделение памяти для виртуальной машины

На этапе «Настройка сети» оставить все без изменений. Нажать кнопку «Далее» (см. рисунок 256).

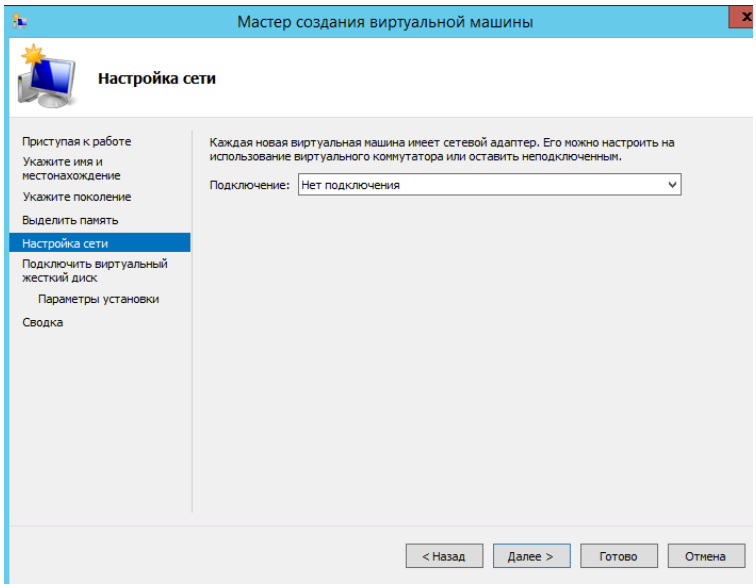


Рисунок 256 – Настройка сети

На этапе «Подключить виртуальный жесткий диск» поставить отметку в поле «Создать виртуальный жесткий диск», в разделе «Размер», назначить размер виртуального жесткого диска 3 ГБ. Остальные настройки оставить без изменений. Нажать кнопку «Далее» (см. рисунок 257)

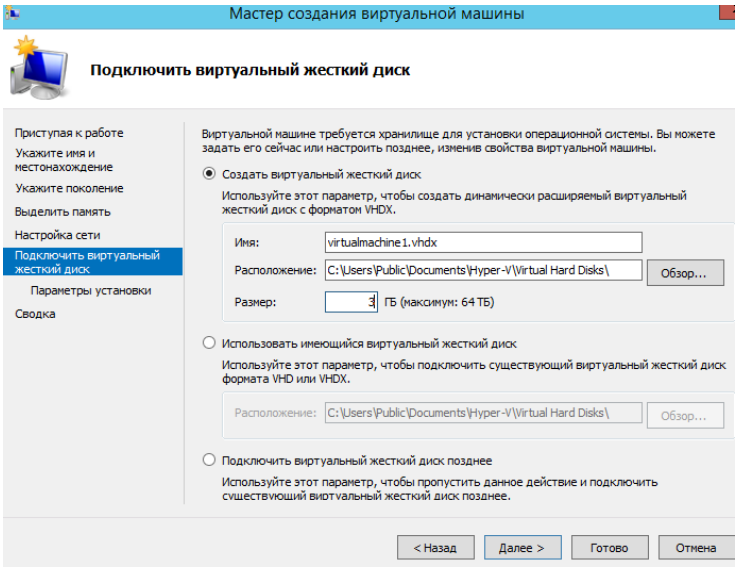


Рисунок 257– Подключение виртуального жесткого диска

На этапе «Параметры установки» поставить отметку в поле «Установить операционную систему позднее». Нажать кнопку «Далее» (см. рисунок 258).

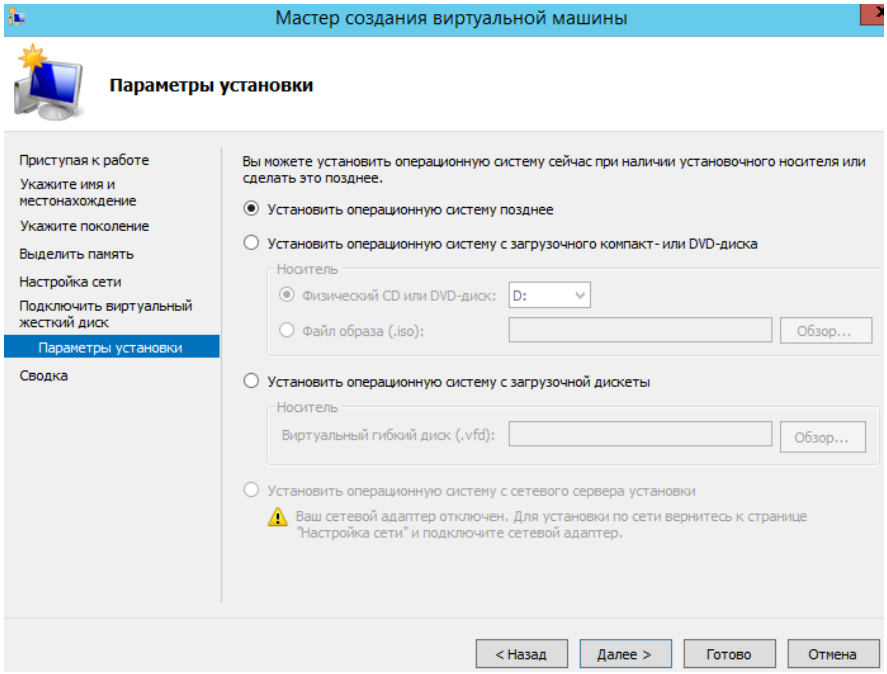


Рисунок 258– Настройка параметров установки

На этапе «Сводка» нажать кнопку «Готово» (см. рисунок 259).

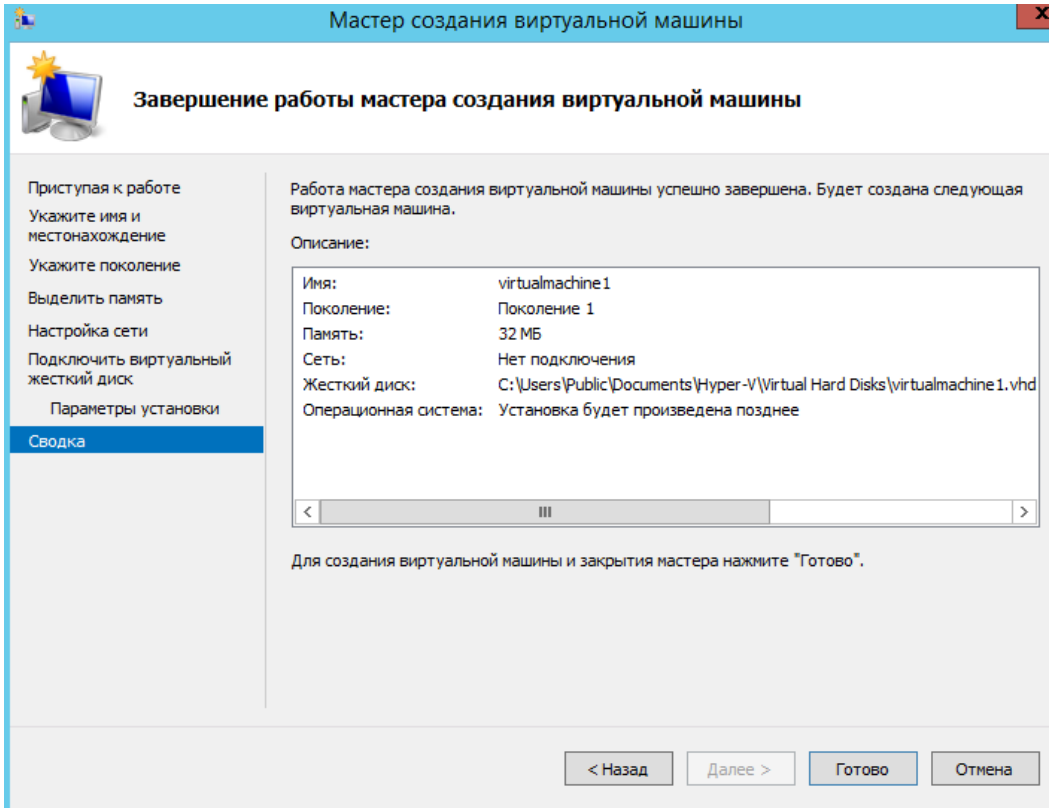


Рисунок 259– Завершение работы мастера создания виртуальной машины

Для того, чтобы убедиться, что виртуальная машина создана необходимо в левой панели диспетчера Hyper-V щелкнуть левой кнопкой мыши по гипервизору, на котором создалась виртуальная машина. В разделе «Виртуальные машины» отобразятся все виртуальные машины, созданные на гипервизоре (см. рисунок 260).

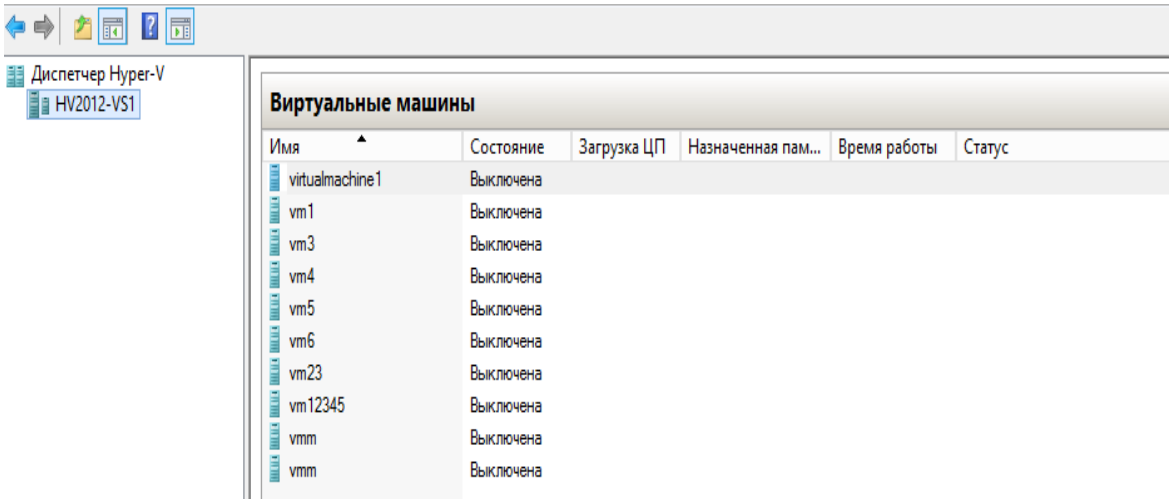


Рисунок 260 – Проверка созданных виртуальных машин

Создание виртуальных коммутаторов. Для того чтобы создать виртуальные коммутаторы необходимо запустить графическую консоль управления «Менеджер Hyper-V». Ее можно запустить на выполнение с помощью команды «Выполнить» из меню Пуск, введя имя файла консоли virtmgmt.msc. После запуска консоли «Менеджер Hyper-V» надо запустить подготовленной сервер виртуализации (ВМ с гипервизором) и в консоли выполнить подключение к этому серверу виртуализации. Для этого следует в верхней панели диспетчера Hyper-V открыть раздел «Действие», команду «Подключиться к серверу». Откроется диалоговое окно «Выбор компьютера». В этом диалоговом окне поставить отметку в пункте «Другой компьютер», щелкнуть левой кнопкой мыши по кнопке «Обзор». Откроется диалоговое окно «Выбор: "Компьютер "» После этого щелкнуть левой кнопкой мыши по кнопке «Дополнительно», в появившемся окне щелкнуть левой кнопкой мыши на кнопку «Поиск». В результатах поиска выбрать необходимый сервер виртуализации для подключения к контроллеру домена WS2012-DC. Нажать кнопку «ОК» (см. рисунок 261).

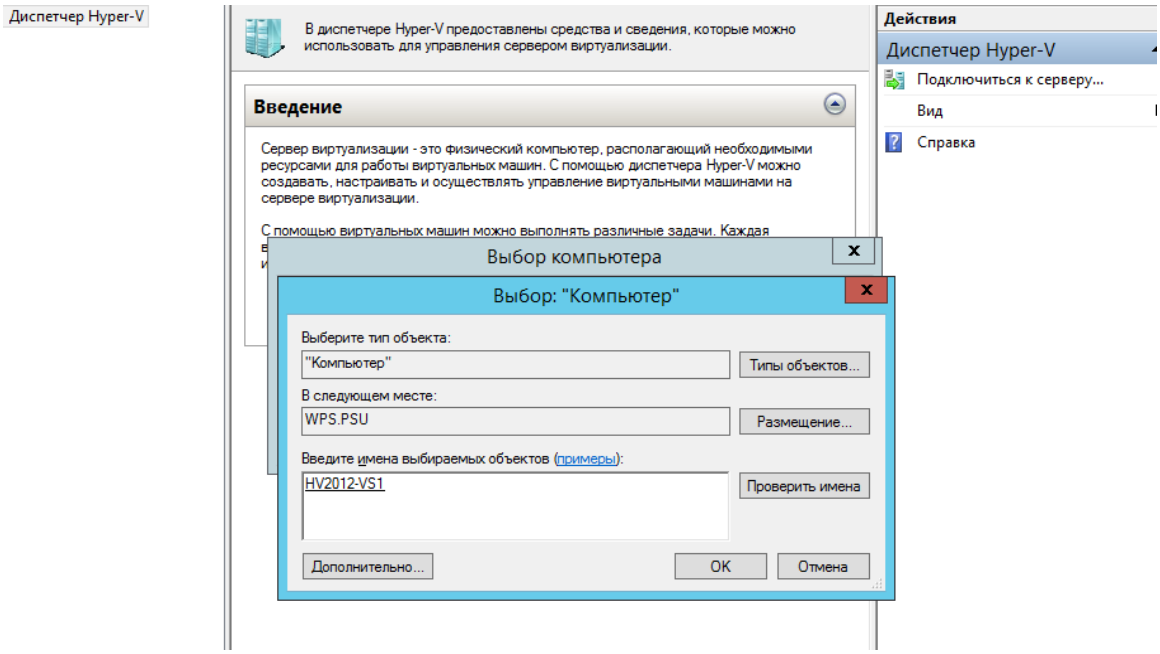


Рисунок 261 – Подключение сервера виртуализации к контроллеру домена

После подключения в правой части окна консоли будет отображен список ВМ, созданных на этом сервере (см. рисунок 262).

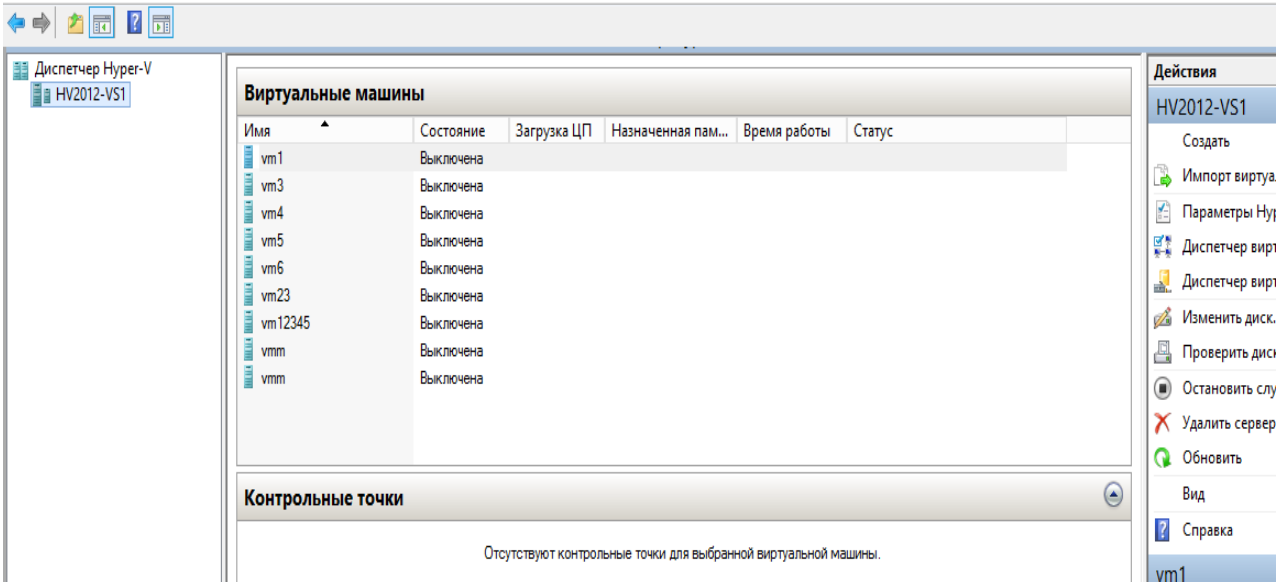


Рисунок 262 – Отображение списка ВМ, созданных на сервере

В левой панели диспетчера Hyper-V щелкнуть правой кнопкой мыши по гипервизору. В выпадающем списке нажать кнопку «Диспетчер виртуальных коммутаторов» (см. рисунок 263).

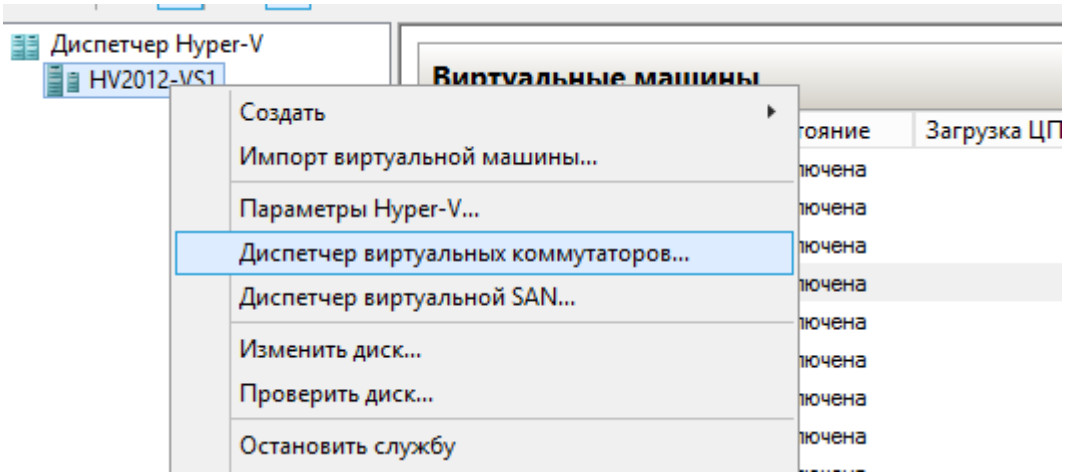


Рисунок 263– Открытие диспетчера виртуальных коммутаторов

Откроется диалоговое окно «Диспетчер виртуальных коммутаторов». В левой панели этого окна выбрать раздел «Создать виртуальный сетевой коммутатор».

В разделе «Создать виртуальный коммутатор» выбрать тип виртуального коммутатора «Внутренняя». Далее нажать кнопку «Создать виртуальный коммутатор» (см. рисунок 264).

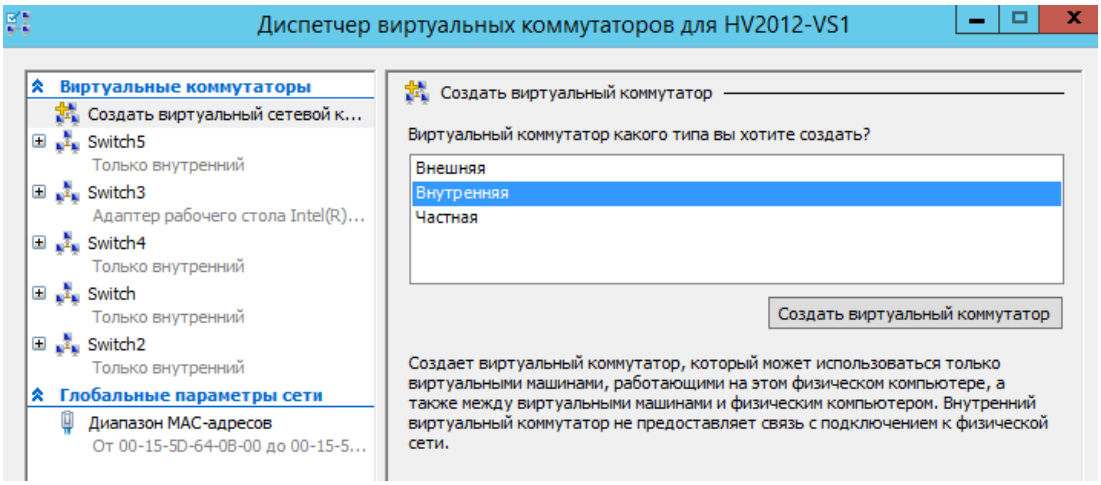


Рисунок 264 – Выбор типа виртуального коммутатора

Откроется раздел «Свойства виртуального коммутатора». В поле «Имя» указать имя виртуального коммутатора, в поле «Тип подключения» поставить отметку в поле «Внутренняя сеть» (см. рисунок 265).

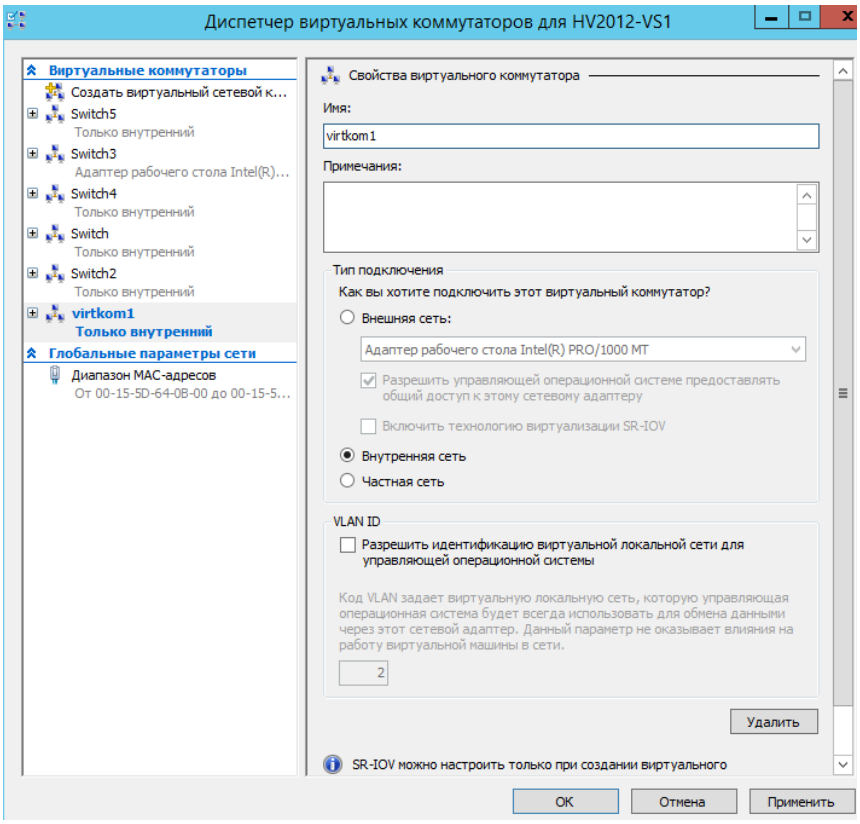


Рисунок 265– Настройка свойств виртуального коммутатора

В левой панели диспетчера виртуальных коммутаторов отображается список созданных виртуальных коммутаторов.

Подключение виртуальной машины к виртуальному коммутатору. Для того чтобы подключить виртуальный коммутатор к виртуальной машине необходимо в необходимо запустить графическую консоль управления «Менеджер Hyper-V». Ее можно запустить на выполнение с помощью команды «Выполнить» из меню Пуск, введя имя файла консоли virtmgmt.msc. После запуска консоли «Менеджер Hyper-V» надо запустить подготовленной сервер виртуализации (ВМ с гипервизором) и в консоли выполнить подключение к этому серверу виртуализации. Для этого следует в верхней панели диспетчера Hyper-V открыть раздел «Действие», команду «Подключиться к серверу». Откроется диалоговое окно «Выбор компьютера». В этом диалоговом окне поставить отметку в пункте «Другой компьютер», щелкнуть левой кнопкой мыши по кнопке «Обзор». Откроется диалоговое окно «Выбор: "Компьютер "» После этого щелкнуть левой кнопкой мыши по кнопке «Дополнительно», в появившемся окне щелкнуть левой кнопкой мыши на кнопку «Поиск». В результатах поиска выбрать необходимый сервер виртуализации для подключения к контроллеру домена WS2012-DC. Нажать кнопку «ОК» (см. рисунок 266).

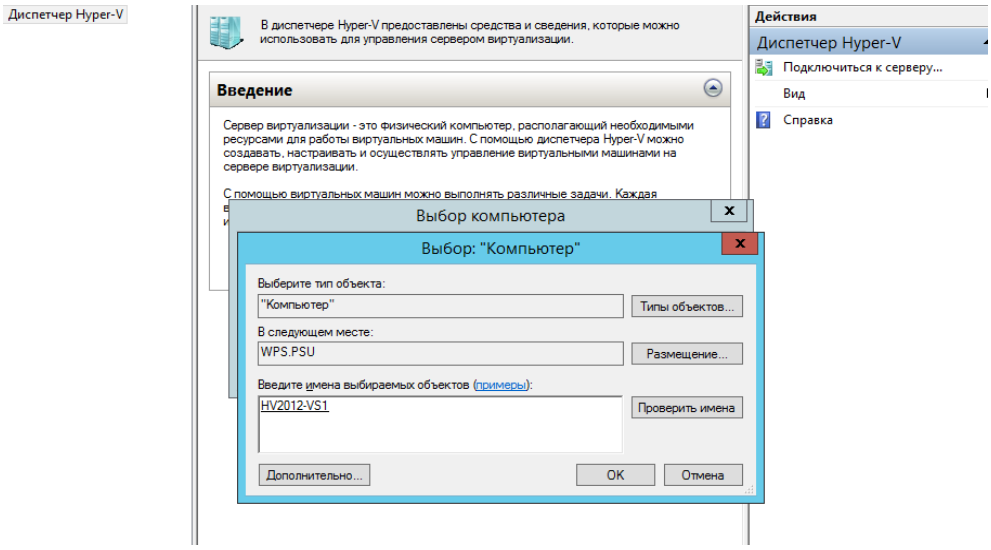


Рисунок 266 – Подключение сервера виртуализации к контроллеру домена

После подключения в правой части окна консоли будет отображен список ВМ, созданных на этом сервере (см. рисунок 267).

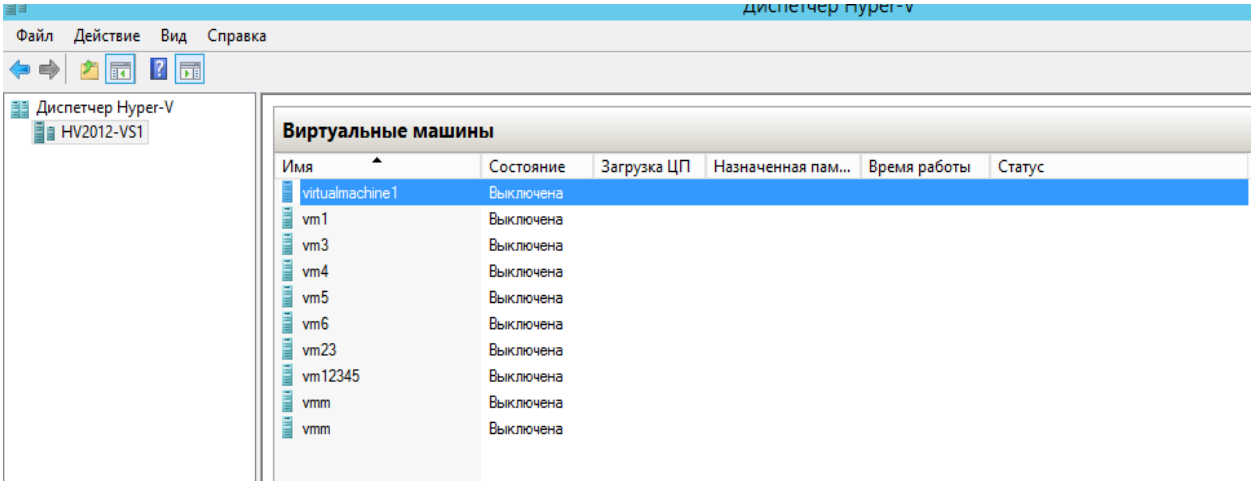


Рисунок 267 – Отображение списка ВМ, созданных на сервере

Щелкнуть левой кнопкой мыши по виртуальной машине, к которой необходимо подключить виртуальный коммутатор. В выпадающем списке нажать кнопку «Параметры» (см. рисунок 268).

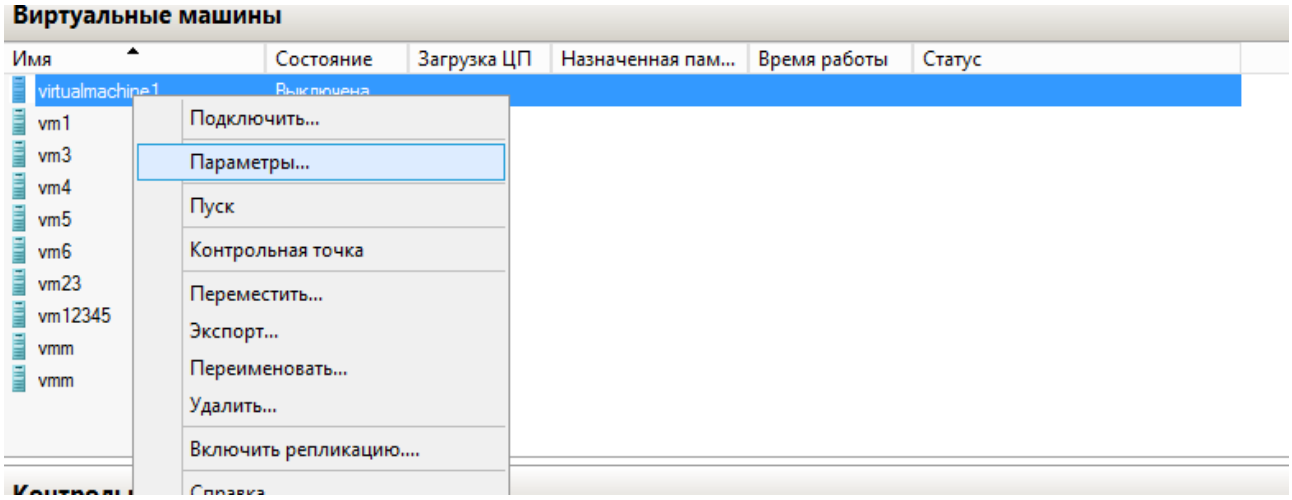


Рисунок 268 – Открытие параметров виртуальной машины

Откроется диалоговое окно параметров виртуальной машины. В левой панели этого окна щелкнуть по разделу «Сетевой адаптер». Далее в поле «Виртуальный коммутатор» выбрать виртуальный коммутатор, к которому нужно подключить виртуальную машину. Далее нажать кнопку «Применить». После этого кнопку «ОК» (см. рисунок 269).

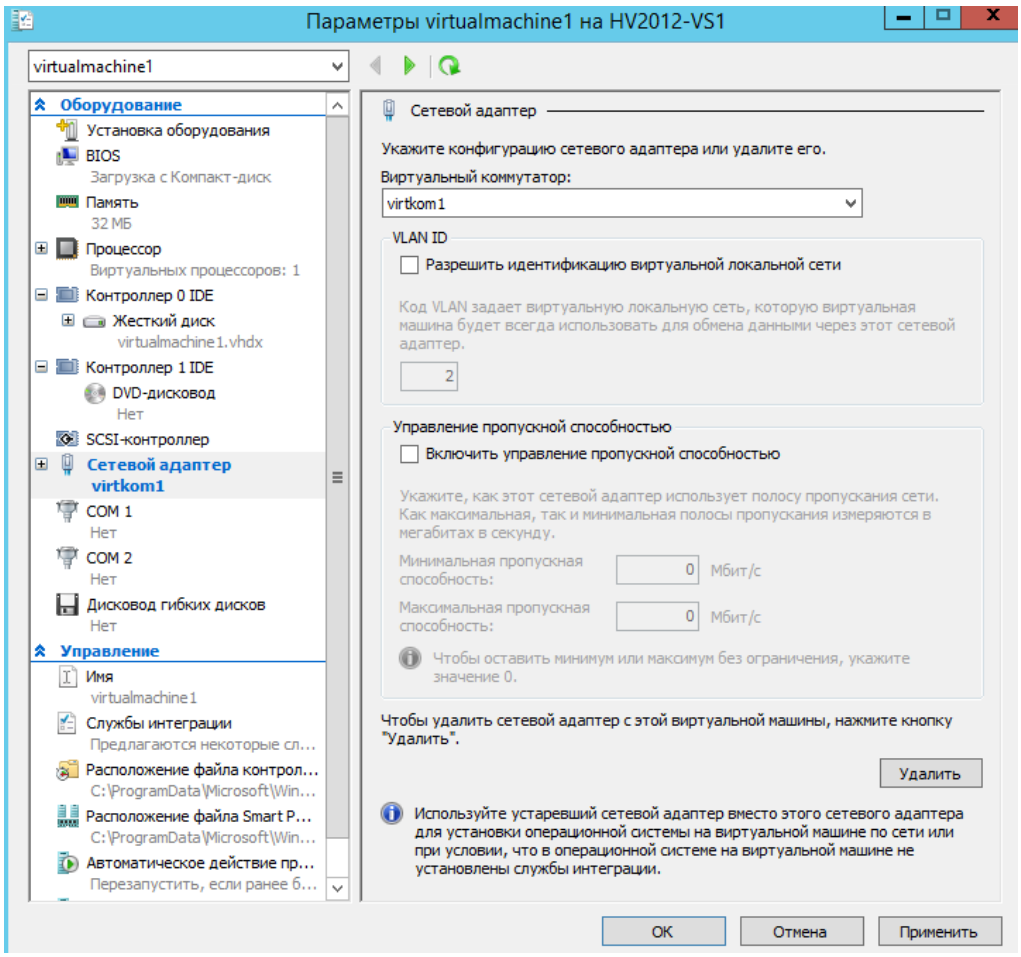


Рисунок 269 - Подключение виртуальной машины к виртуальному коммутатору

В левой части панели параметров виртуальной машины в разделе «Сетевой адаптер» должно отображаться имя виртуального коммутатора.

Репликация виртуальной машины. Реплика Hyper-V является неотъемлемой частью роли Hyper-V. Она влияет на стратегию аварийного восстановления путем репликации виртуальных машин с одного сервера узла Hyper-V на другой для поддержания доступности рабочих нагрузок. Реплика Hyper-V создает копию активной виртуальной машины в автономной виртуальной машине реплики.

Для того, чтобы провести репликацию виртуальной машины с гипервизора изначально следует создать правило для разрешения входящего подключения через порт 80. Для этого следует нажать кнопки «Win+R». Откроется диалоговое окно «Выполнить». В пустой строке набрать команду «mmc». В полученном диалоговом окне в верхнем меню нажать на раздел

«Файл», нажать кнопку «Добавить или удалить оснастку». Откроется диалоговое окно «Добавление и удаление оснасток». В левой панели меню «Доступные оснастки» нажать левой кнопкой мыши на оснастку «Брандмауэр Windows в режиме повышенной безопасности» и нажать кнопку «Добавить». Откроется диалоговое окно «Выберите компьютер». Поставить отметку в поле «Другой компьютер», нажать на кнопку «Обзор». Нажать кнопку «Типы объектов». В полученном диалоговом окне убрать отметку в поле «Встроенные субъекты безопасности». Нажать кнопку «ОК». В нижней панели диалогового окна «Выбор: "Компьютер"» нажать на кнопку «Дополнительно». В полученном окне нажать кнопку «Поиск». В разделе «Результаты поиска» будет выведен список виртуальных машин. Выбрать ВМ HV2012-VS2, нажать 2 раза кнопку «ОК», затем кнопку «Готово. Далее в диалоговом окне «Добавление и удаление оснасток» нажать на кнопку «ОК». В левой панели полученного диалогового окна в разделе «Корень консоли» раскрыть пункт «Брандмауэр Windows в режиме повышенной безопасности» (см. рисунок 270).

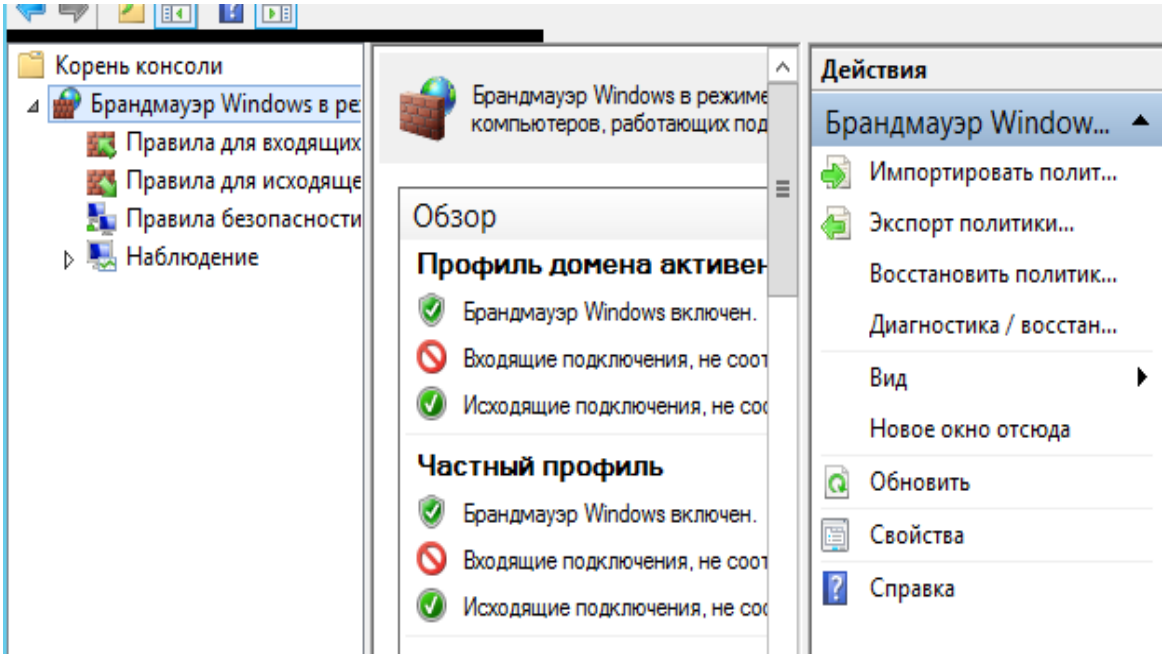


Рисунок 270 – Настройка брандмауэра Windows

Далее следует нажать на команду «Правила для входящих подключений». В правой панели в разделе «Действия» нажать на кнопку «Создать правило».

Откроется диалоговое окно «Мастер создания правила для нового входящего подключения». На шаге «Тип правила» поставить отметку в поле «Для порта» и нажать кнопку «Далее» (см. рисунок 271).

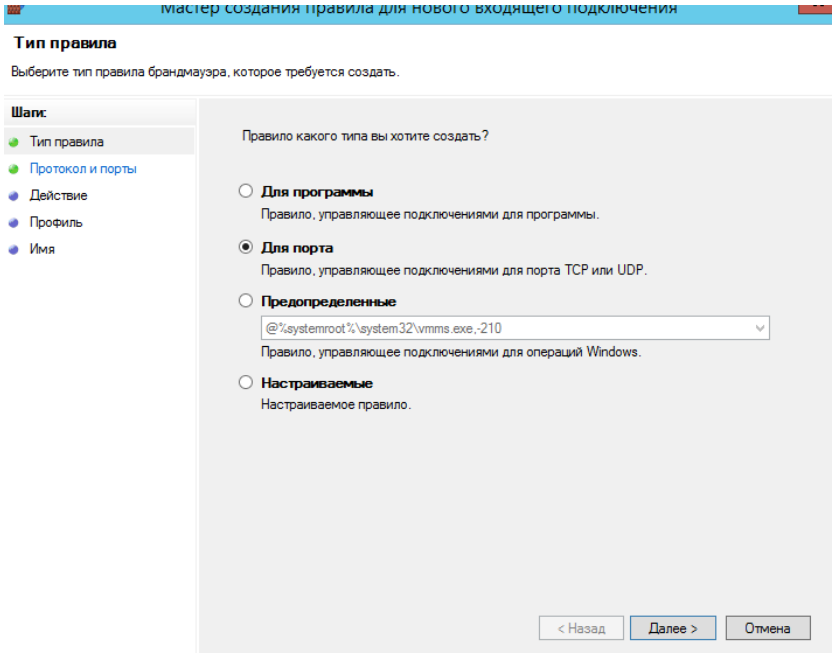


Рисунок 271 – Выбор типа правила для нового входящего подключения

На шаге «Протокол и порты» необходимо поставить отметку в поле «Протокол TCP» и в поле «Определенные локальные порты». В пустой строке ввести значение порта 80 (см. рисунок 272).

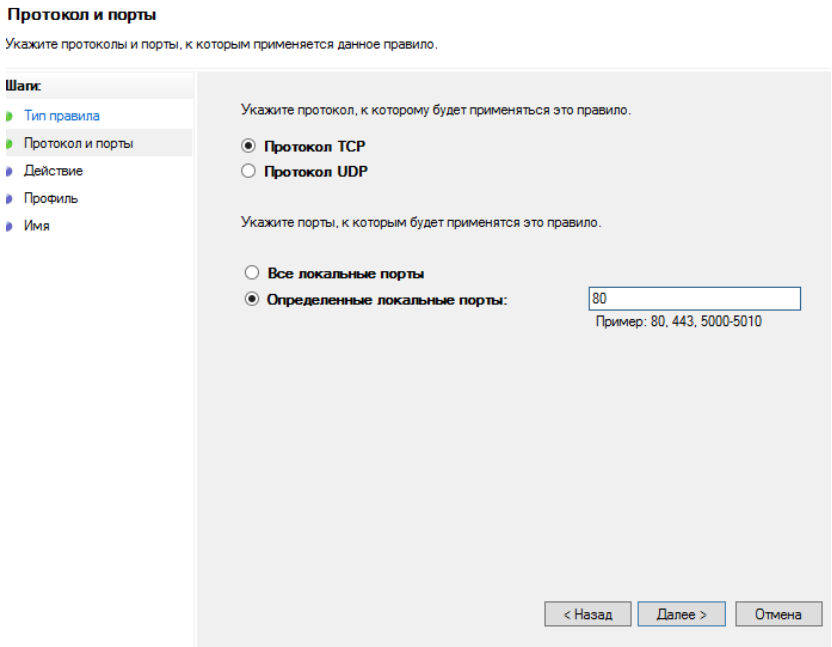


Рисунок 272 – Указание протокола и порта для нового входящего подключения

На шаге «Действие» поставить отметку в поле «Разрешить подключение» (см. рисунок 273).

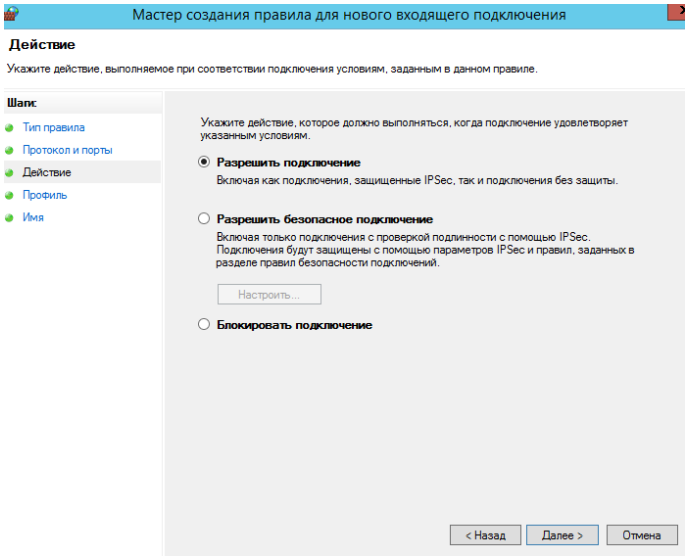


Рисунок 273 – Указание действия, которое должно выполняться, когда подключение удовлетворяет указанному условию

На шаге «Профиль» оставить все по умолчанию (см. рисунок 274).

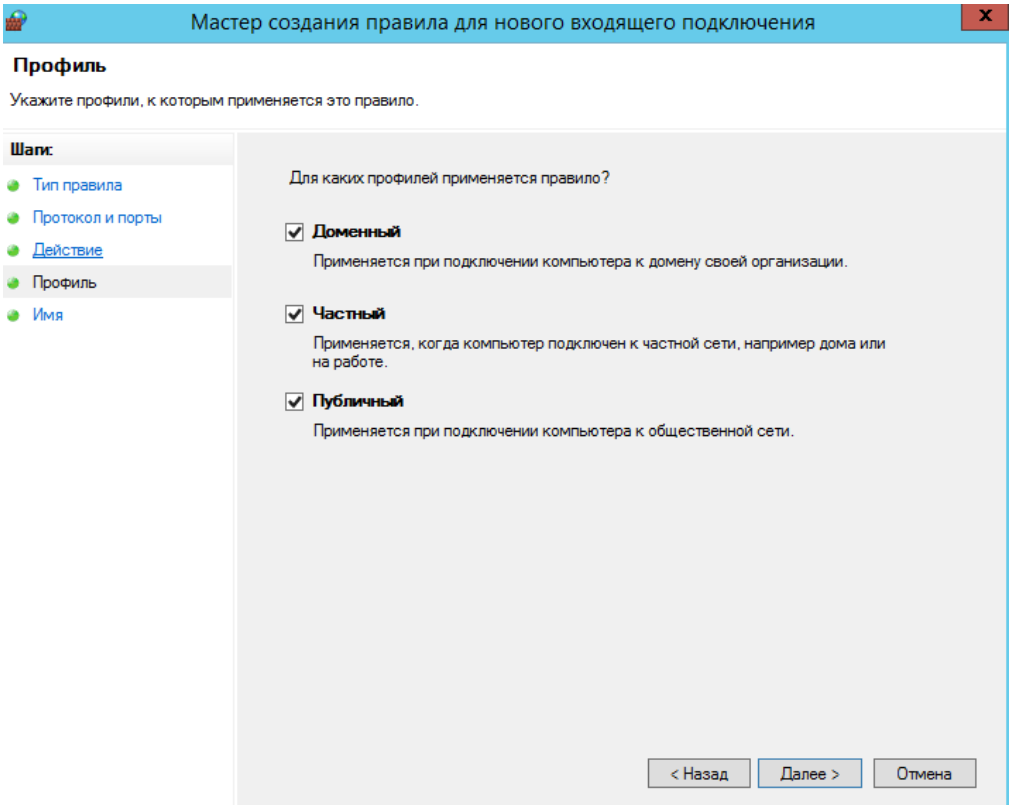


Рисунок 274 – Указание профиля, к которому применяется правило

На шаге «Имя» в пустой строке ввести имя правила. Описание необязательно. Нажать кнопку «Готово» (см. рисунок 275).

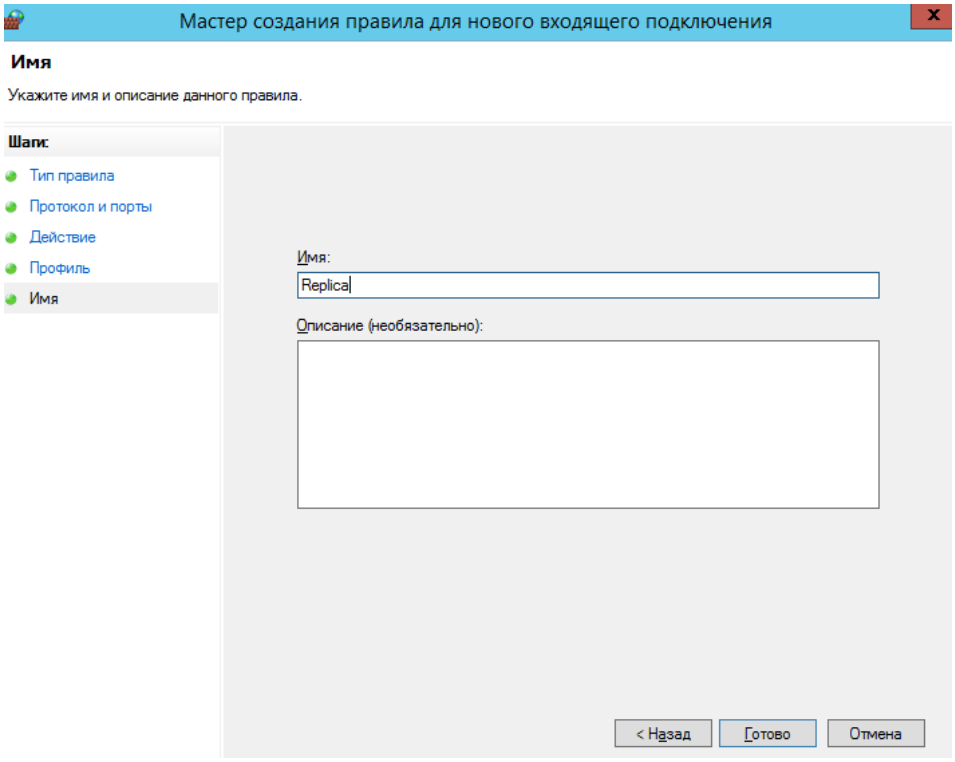


Рисунок 275 – Указание имени правила

Далее следует открыть консоль «Менеджер Hyper-V». Ее можно запустить на выполнение с помощью команды «Выполнить» из меню Пуск, введя имя файла консоли virtmgmt.msc. После запуска консоли «Менеджер Hyper-V» надо запустить два подготовленных сервера виртуализации (ВМ с гипервизором) и в консоли выполнить подключение к этим серверам виртуализации. Для того, что провести репликацию виртуальной машины с гипервизора HV2012-VS1 на гипервизор HV2012-VS2 необходимо в меню «Диспетчер Hyper-V» щелкнуть правой кнопкой мыши по сервере HV2012-VS2, нажать на кнопку «Параметр Hyper-V». Откроется диалоговое окно «Параметр Hyper-V для HV2012-VS2». Далее в разделе «Сервер» щелкнуть левой кнопкой мыши по пункту «Конфигурация репликации. Настроен как сервер-реплика». В полученном диалоговом окне поставить отметку в поле «Включить компьютер как сервер-реплику», «Использовать встроенную

проверку подлинности (Windows (HTTP):» и поставить отметку в поле «Разрешить репликацию с любого прошедшего проверку сервера» и нажать кнопку «Применить», а затем кнопку «ОК» (см. рисунок 276).

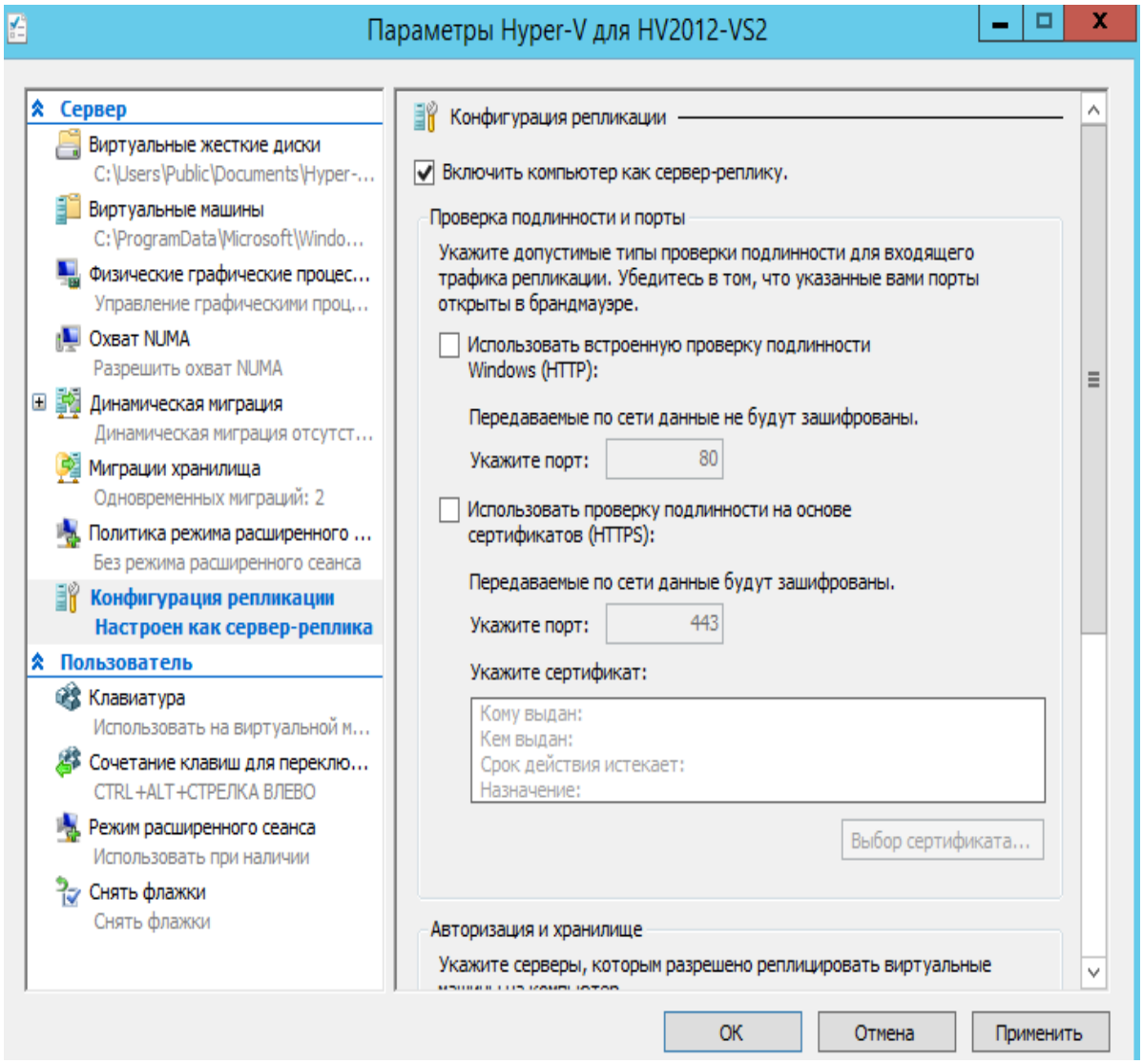


Рисунок 276 – Конфигурация репликации Hyper-V сервера HV2012-VS2

Далее в верхней панели «Диспетчер Hyper-V» в меню «Виртуальные машины» щелкнуть правой кнопкой мыши по виртуальной машине, на которой следует включить репликацию, нажать на команду «Включить репликацию». Откроется диалоговое «Включение репликации… ». На этапе «Перед началом работу» нажать кнопку «Далее». На этапе «Указать сервер-реплику» нажать на кнопку «Обзор». В полученном диалоговом окне нажать на кнопку «Дополнительно». В новом диалогов окне в правой панели нажать команду

«Поиск». В нижней панели в разделе «Результаты поиска:» выбрать гипервизор, который будет являться сервером репликации, нажать кнопку «ОК», затем кнопку «Далее» (см. рисунок 277).

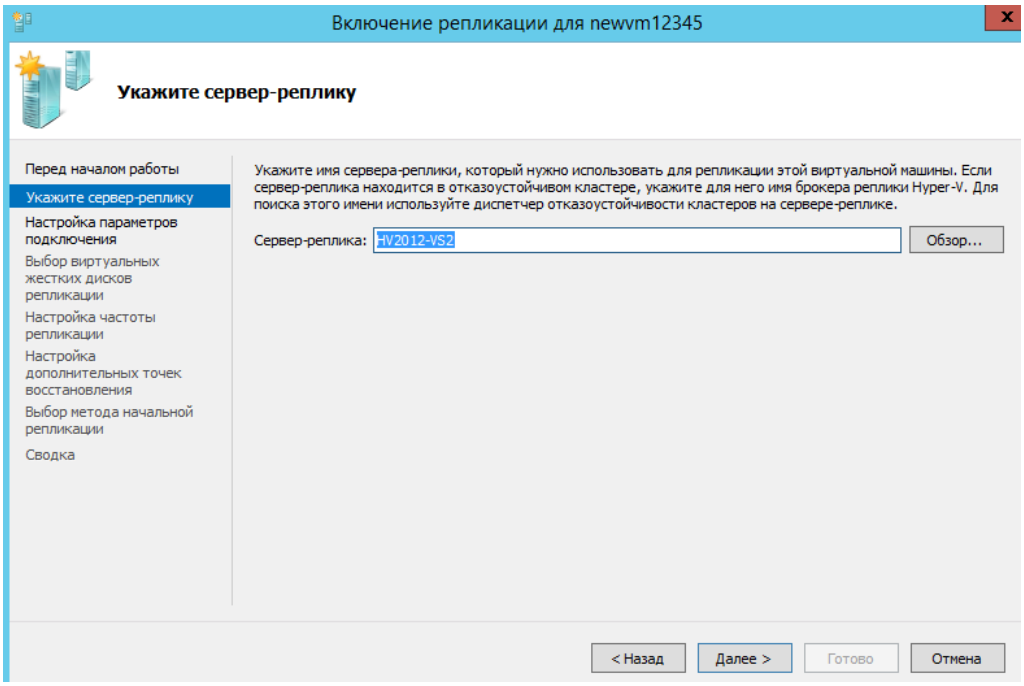


Рисунок 277 – Указание сервера репликации

На этапе «Настройка параметров подключения» в поле «Порт на сервер-реплике:» присвоить значение 80, в разделе «Тип проверки подлинности» поставить отметку в поле «Использовать проверку подлинности Kerberos (HTTP)», нажать кнопку «Далее» (см. рисунок 278).

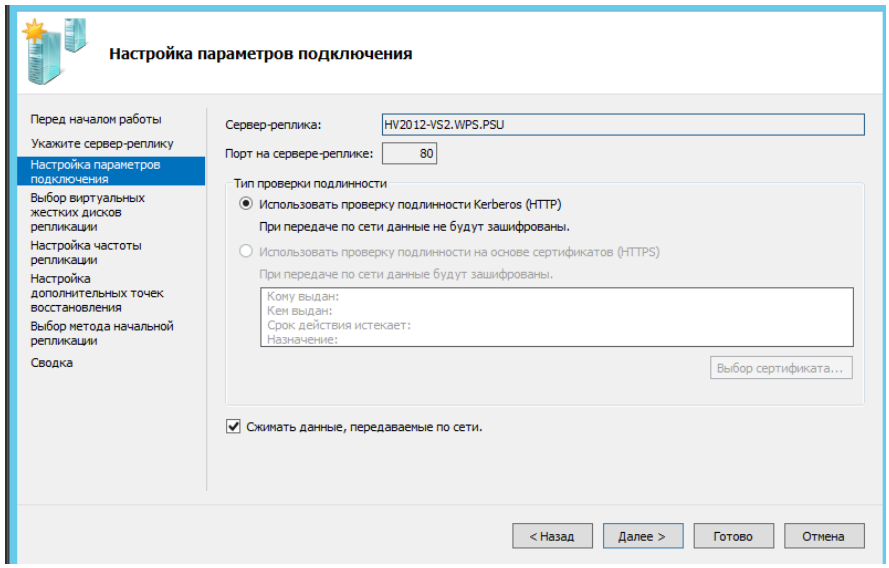


Рисунок 278 – Настройка параметров подключения

На этапе «Выбор виртуальных жестких дисков репликации» все оставить без изменений и нажать кнопку «Далее».

На этапе «Настройка частоты репликации» в разделе «Выберите частоту отправки изменений на сервер-реплику» 5 минут, нажать кнопку «Далее» (см. рисунок 279).

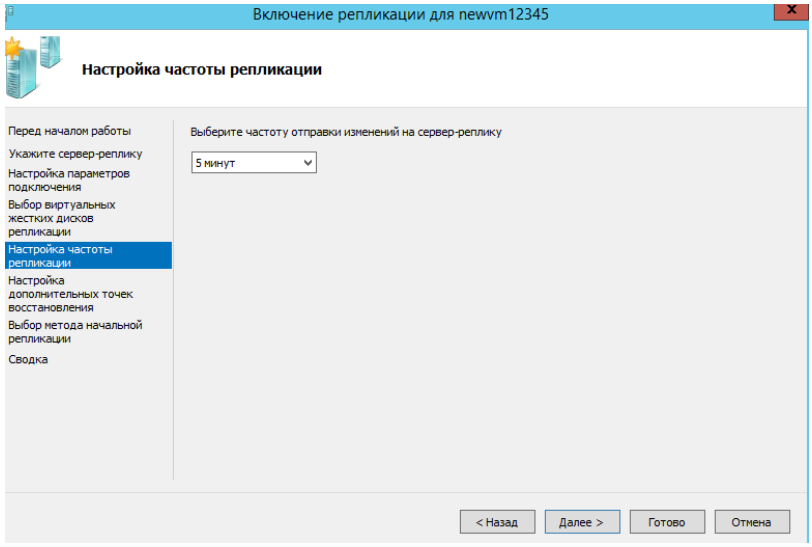


Рисунок 279 – Настройка частоты репликации

На этапе «Настройка дополнительных точек восстановления» в разделе «Настройка дополнительных точек восстановления для этой виртуальной машины» поставить отметку в поле «Хранить только последнюю точку восстановления» и нажать кнопку «Далее» (см. рисунок 280).

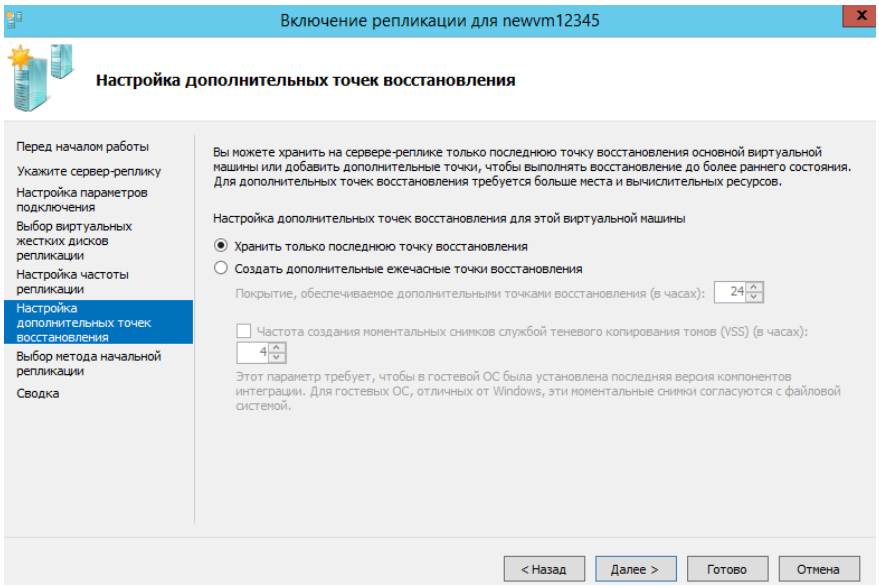


Рисунок 280 – Настройка дополнительных точек восстановления

На этапе «Выбор метода начальной репликации» в разделе «Метод начальной репликации» поставить отметку в поле «Передать начальную копию по сети». В разделе «Планирование начальной репликации» поставить отметку в поле «Запустить репликацию немедленно». Нажать кнопку «Далее» (см. рисунок 281).

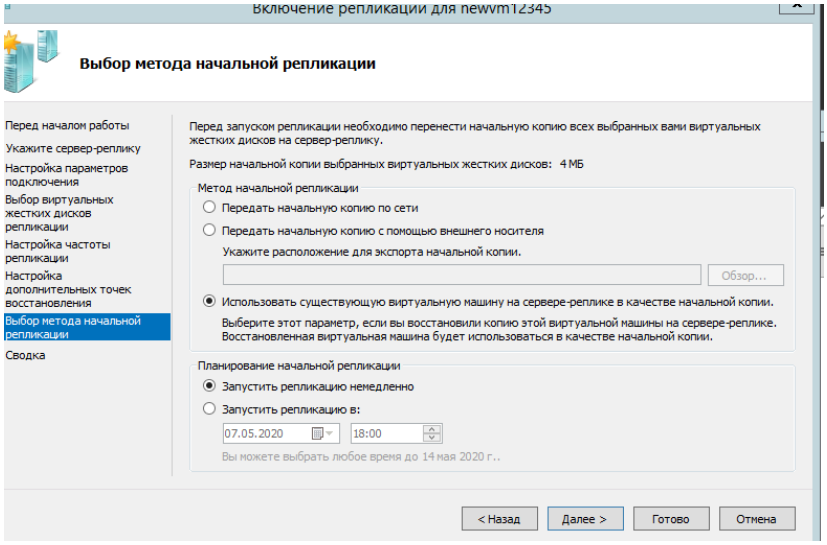


Рисунок 281 – Выбор метода начальной репликации

На этапе «Сводка» нажать кнопку «Готово» (см. рисунок 282).

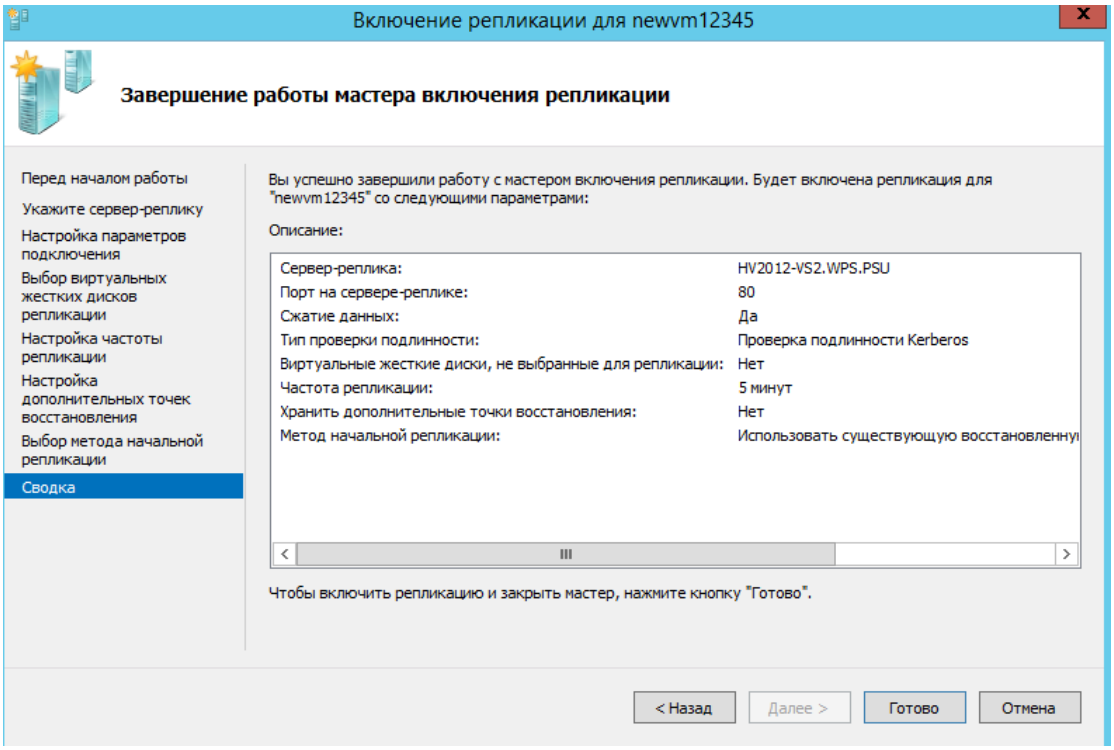


Рисунок 282 – Завершение работы мастера включения репликации

Для проверки репликации следует в левой панели «Диспетчер Hyper-V» нажать левой кнопкой мыши по гипервизору HV2012-VS2. В списке виртуальных машин должна отобраться ВМ добавленная с помощью репликации (см. рисунок 283).

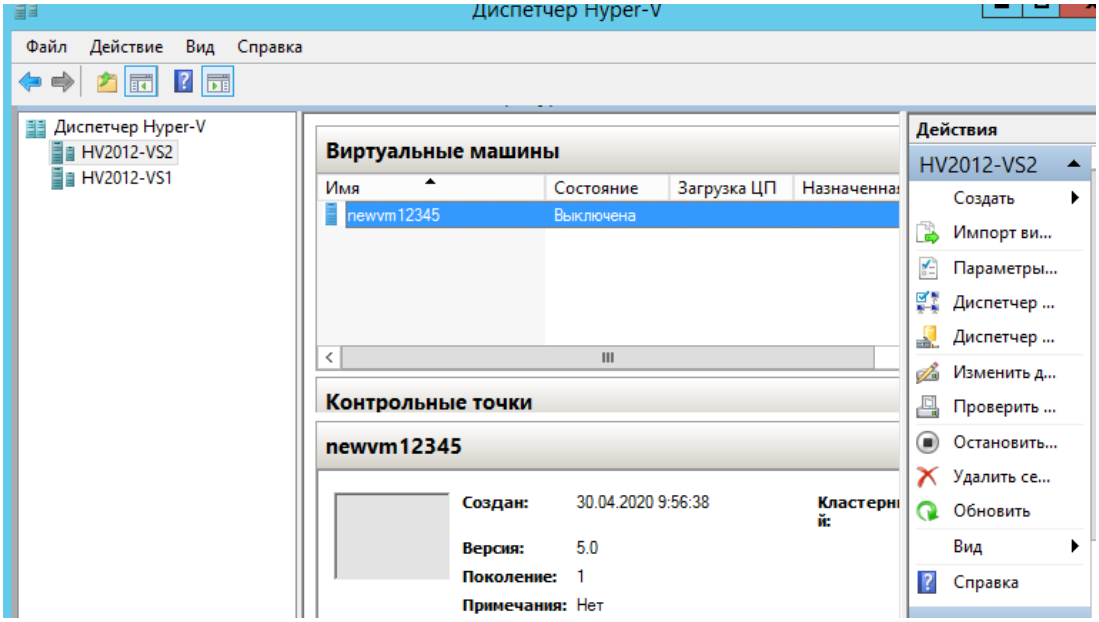


Рисунок 283 – Проверка репликации ВМ

К нему же добавить описание миграции ВМ и пояснить, что полностью этой действие не реализуется из-за того, что гипервизор работает на ВМ.

Экспорт виртуальной машины. Экспорт собирает все необходимые файлы в одну единицу — файлы виртуального жесткого диска, файлы конфигурации виртуальной машины и файлы контрольных точек. Это можно сделать на виртуальной машине, которая находится в запущенном или остановленном состоянии.

Для этого запустить графическую консоль управления «Менеджер Hyper-V». Ее можно запустить на выполнение с помощью команды «Выполнить» из меню Пуск, введя имя файла консоли virtmgmt.msc. После запуска консоли «Менеджер Hyper-V» надо запустить два подготовленных сервера виртуализации (ВМ с гипервизором) и в консоли выполнить подключение к этим серверам виртуализации. Для этого следует в верхней панели диспетчера Hyper-V открыть раздел «Действие», команду «Подключиться к серверу».

Откроется диалоговое окно «Выбор компьютера». В этом диалоговом окне поставить отметку в пункте «Другой компьютер», щелкнуть левой кнопкой мыши по кнопке «Обзор». Откроется диалоговое окно «Выбор: "Компьютер "» После этого щелкнуть левой кнопкой мыши по кнопке «Дополнительно», в появившемся окне щелкнуть левой кнопкой мыши на кнопку «Поиск». В результатах поиска выбрать необходимый сервер виртуализации для подключения к контроллеру домена WS2012-DC. Нажать кнопку «ОК» (см. рисунок 284).

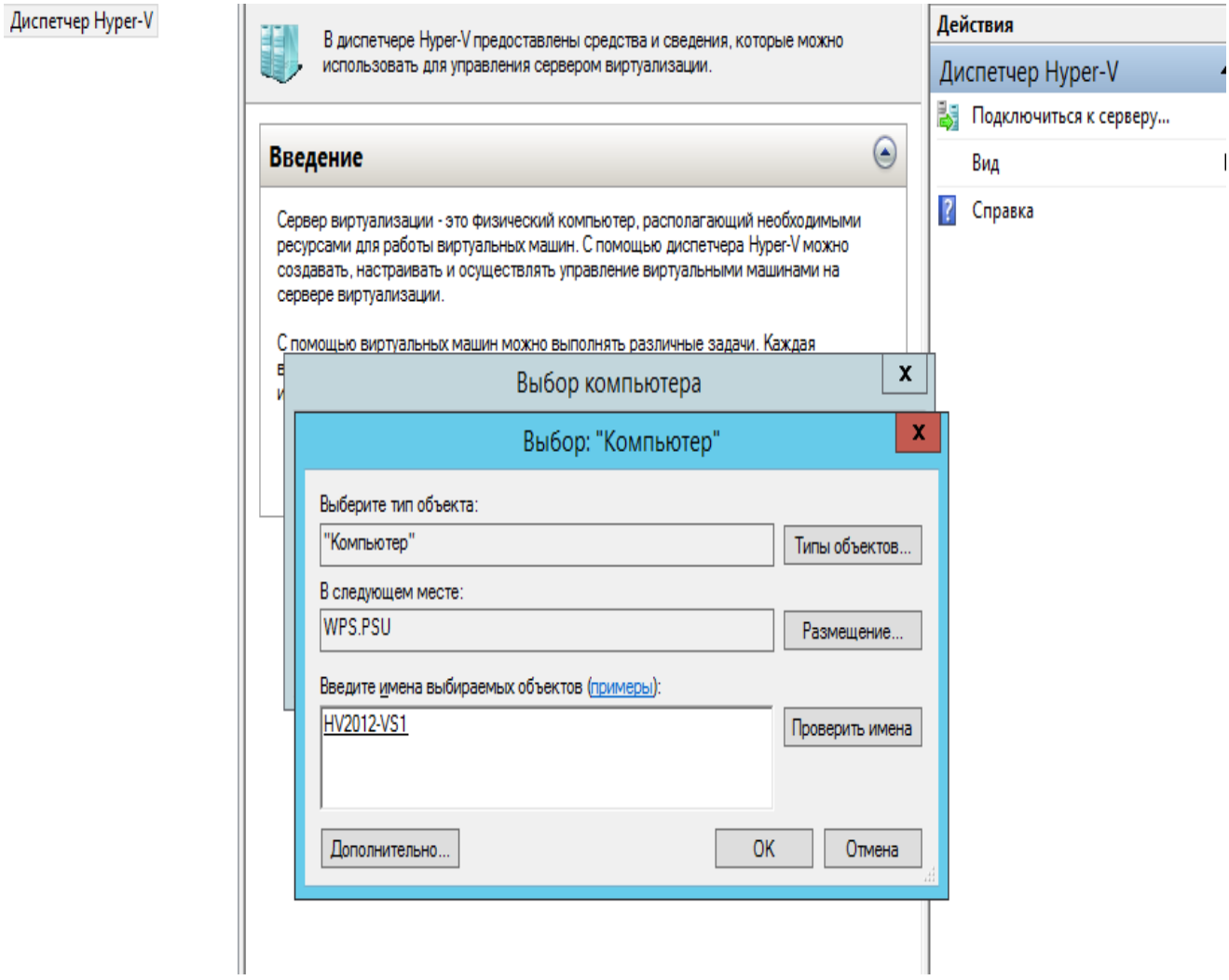


Рисунок 284 – Подключение сервера виртуализации к контроллеру домена

После подключения в правой части окна консоли будет отображен список ВМ, созданных на этом сервере (см. рисунок 285).

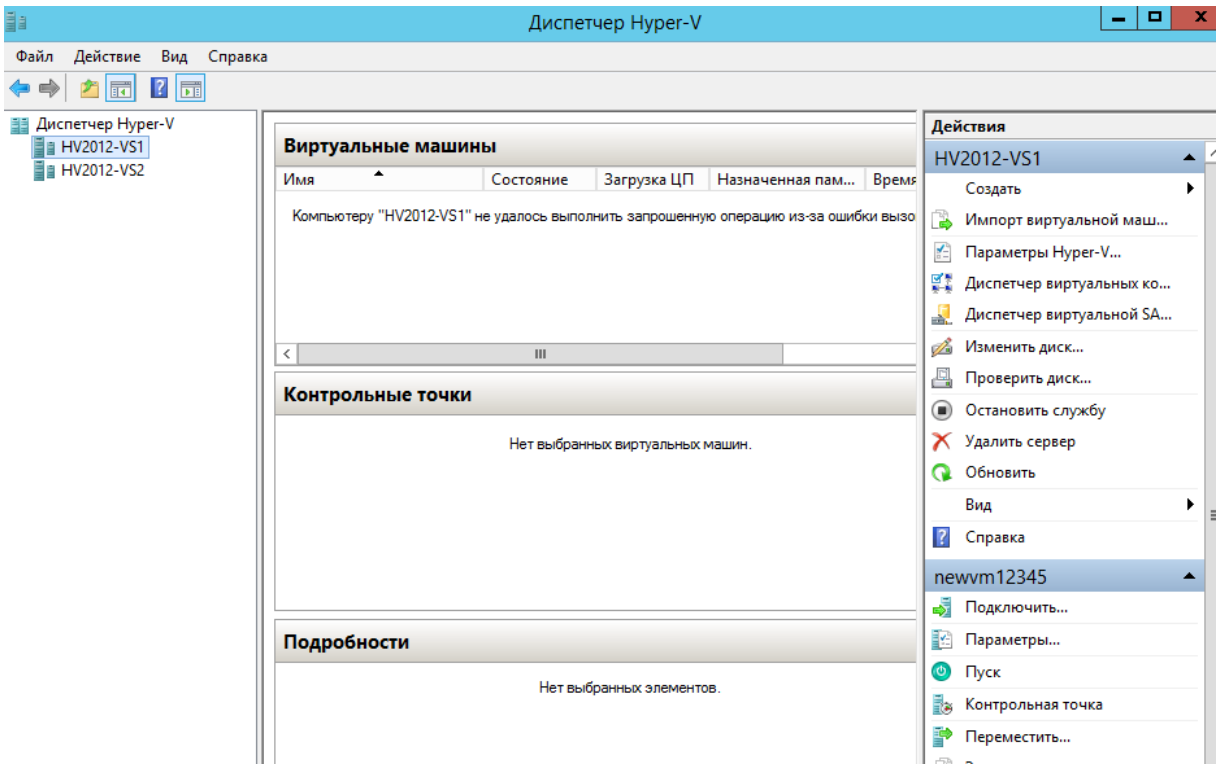


Рисунок 285 – Отображение списка ВМ, созданных на сервере

Чтобы экспортировать виртуальную машину необходимо правой кнопкой мыши щелкнуть по выбранной виртуальной машине и выбрать команду «Экспорт». Далее надо выбрать место хранения экспортируемых файлов и нажать кнопку «Экспорт» (см. рисунок 286).

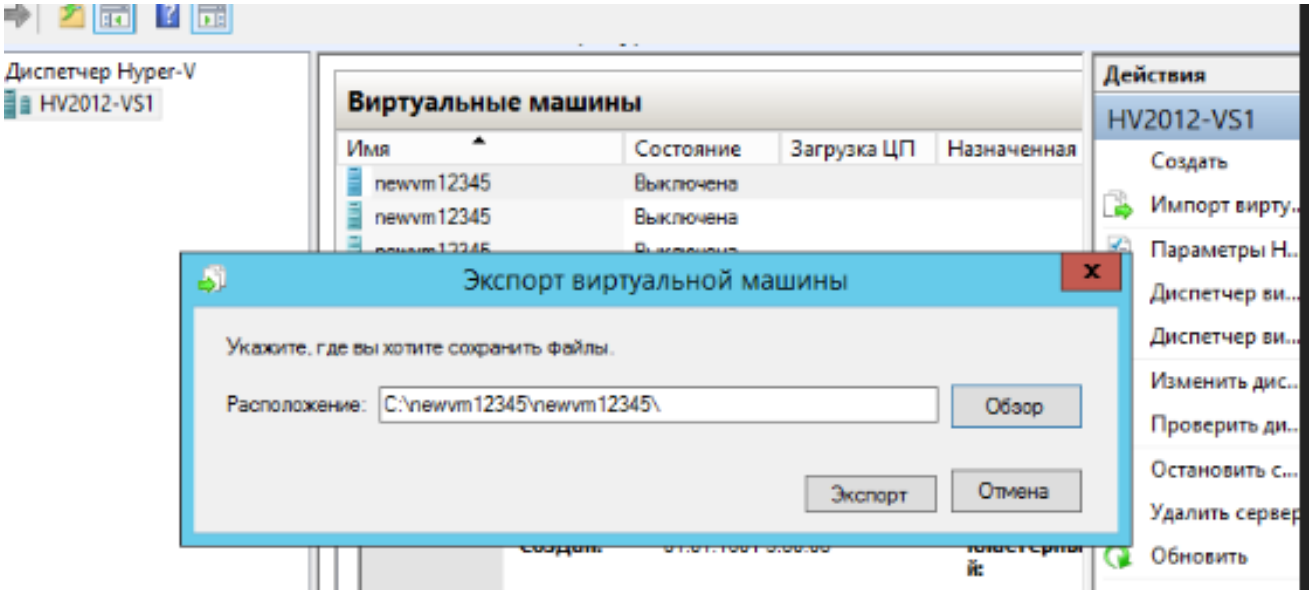


Рисунок 286 – Экспорт виртуальной машины

Импорт виртуальной машины. При импорте виртуальной машины она регистрируется на узле Hyper-V. Можно выполнить импорт в узел или на новый узел. При импорте в тот же узел не нужно сначала экспортировать виртуальную машину, так как Hyper-V пытается повторно создать виртуальную машину из доступных файлов. Импорт виртуальной машины регистрирует ее, чтобы ее можно было использовать на узле Hyper-V.

Мастер импорта виртуальных машин также помогает устранить несовместимости, которые могут существовать при переходе с одного узла на другой. Обычно это различие в физическом оборудовании, таком как память, виртуальные коммутаторы и виртуальные процессоры.

Чтобы импортировать виртуальную машину следует в левом меню «Диспетчер Hyper-V» выбрать виртуальную машину, щелкнуть правой кнопкой мыши на команду «Импорт виртуальной машины». На этапе «Перед началом работы» нажать кнопку «Далее». На этапе «Выбор папки» выбрать папку, содержащую экспортированные файлы, и нажмите кнопку «Далее» (см. рисунок 287).

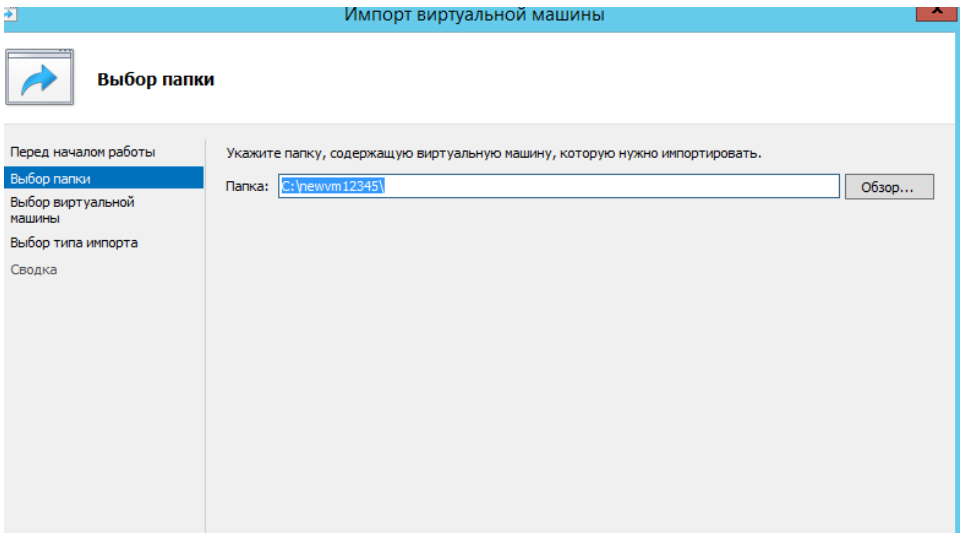


Рисунок 287 - Выбор папки, содержащей виртуальную машину, которую нужно импортировать

На этапе «Выбор виртуальной машины» нажать кнопку «Далее» (см. рисунок 288).

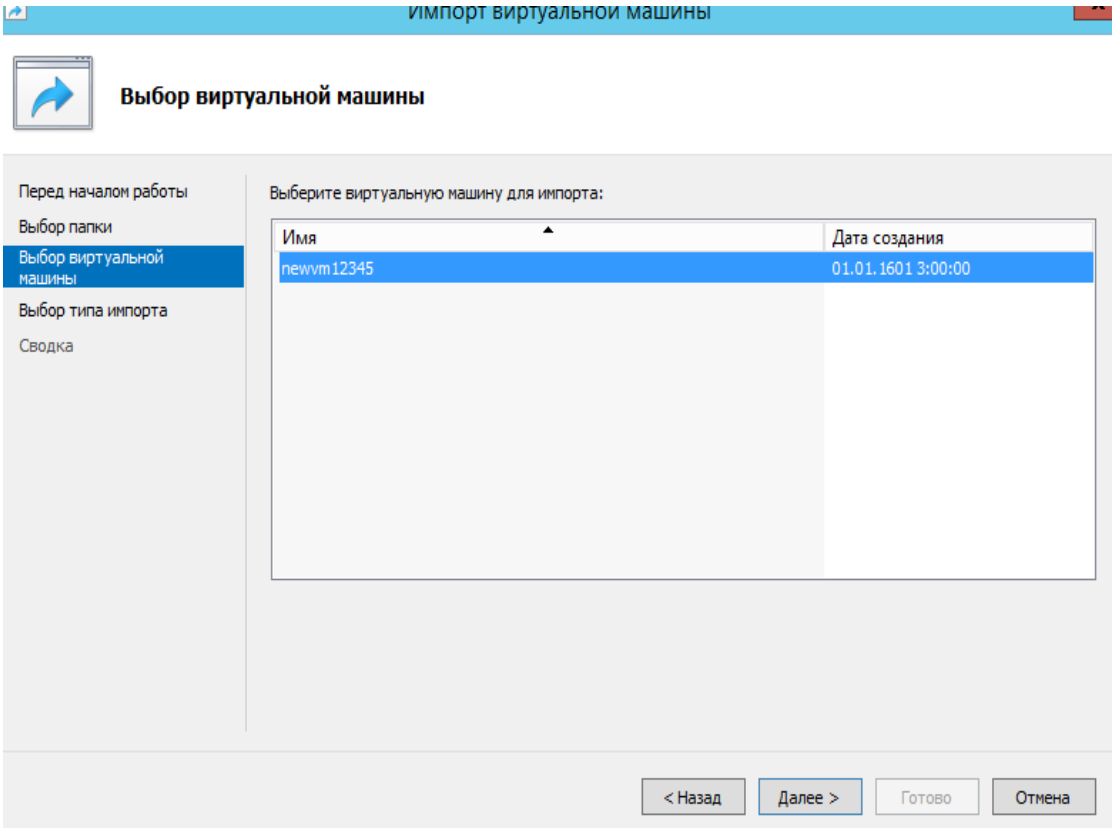


Рисунок 288 – Выбор виртуальной машины для импорта

На этапе «Выбор типа импорта» поставить отметку в пункте «Копировать виртуальную машину (создать новый уникальный идентификатор)» и нажать кнопку «Далее» (см. рисунок 289).

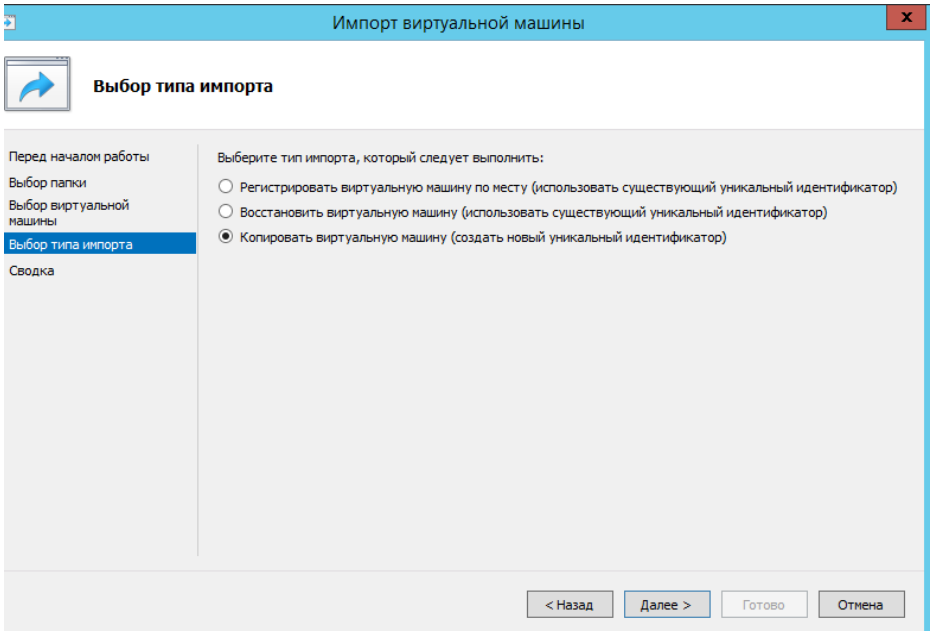


Рисунок 289 – Выбор типа импорта

На этапе «Выбор назначения» оставить все без изменений (см. рисунок 290).

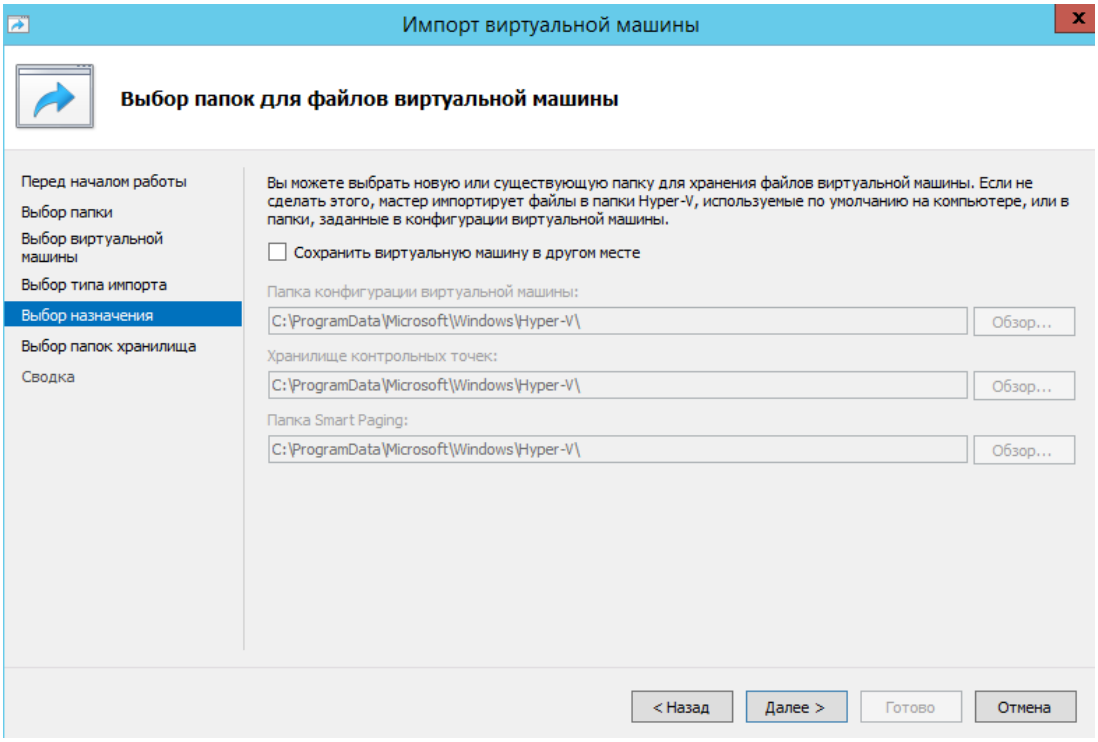


Рисунок 290 – Выбор назначения

На этапе «Выбор папок хранилища» выбрать папку, где следует хранить импортированные виртуальные жесткие диски для виртуальной машины и нажать кнопку «Далее» (см. рисунок 291).

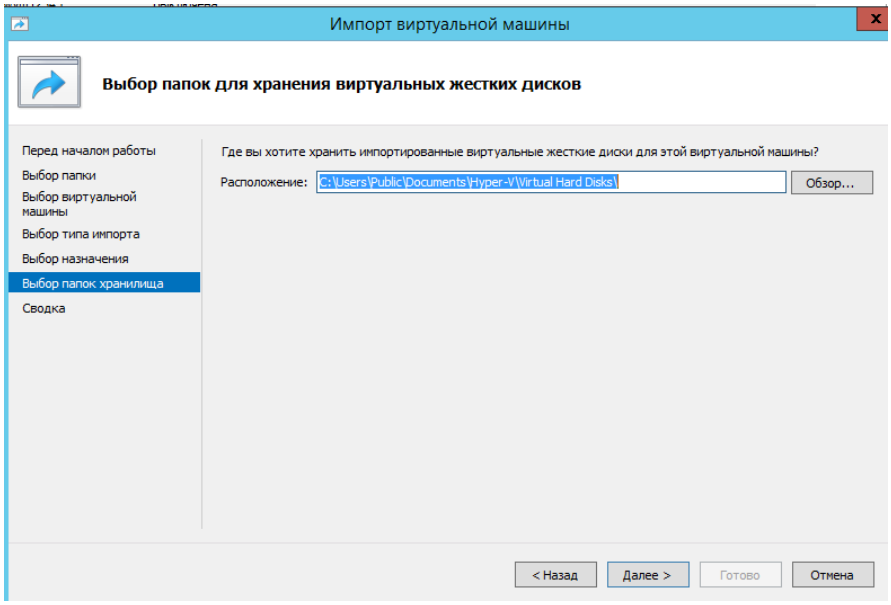


Рисунок 291 – Выбор папок хранилища

На этапе «Настройка памяти» указать количества ОЗУ для запуска и нажать кнопку «Далее» (см. рисунок 292).

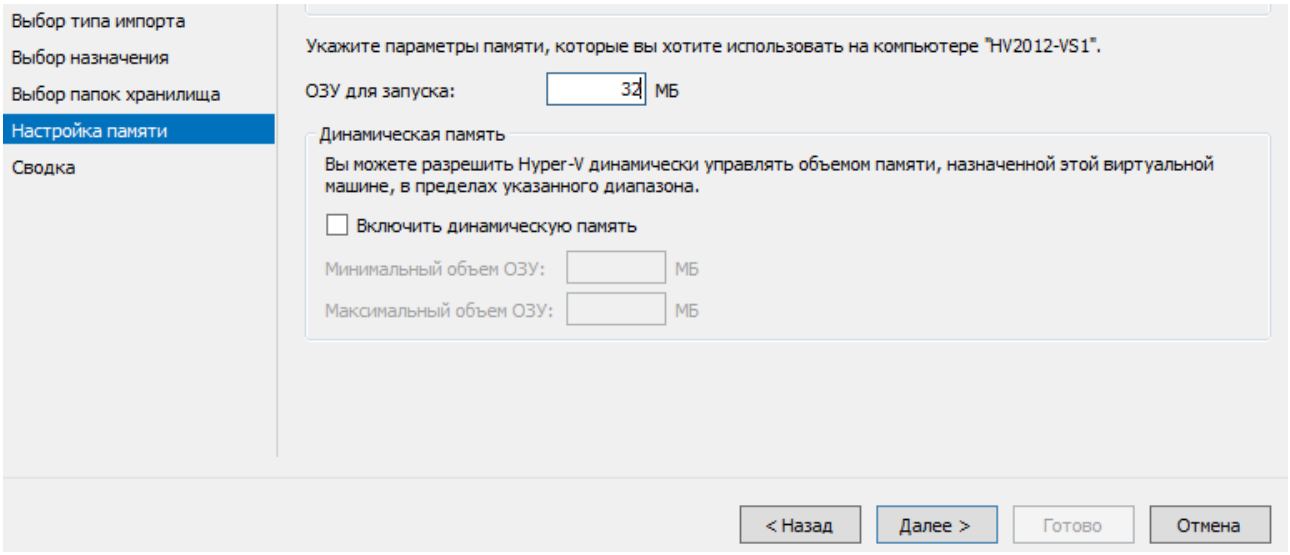


Рисунок 292 – Настройка памяти

На этапе «Сводка» нажать кнопку «Готово» (см. рисунок 293).

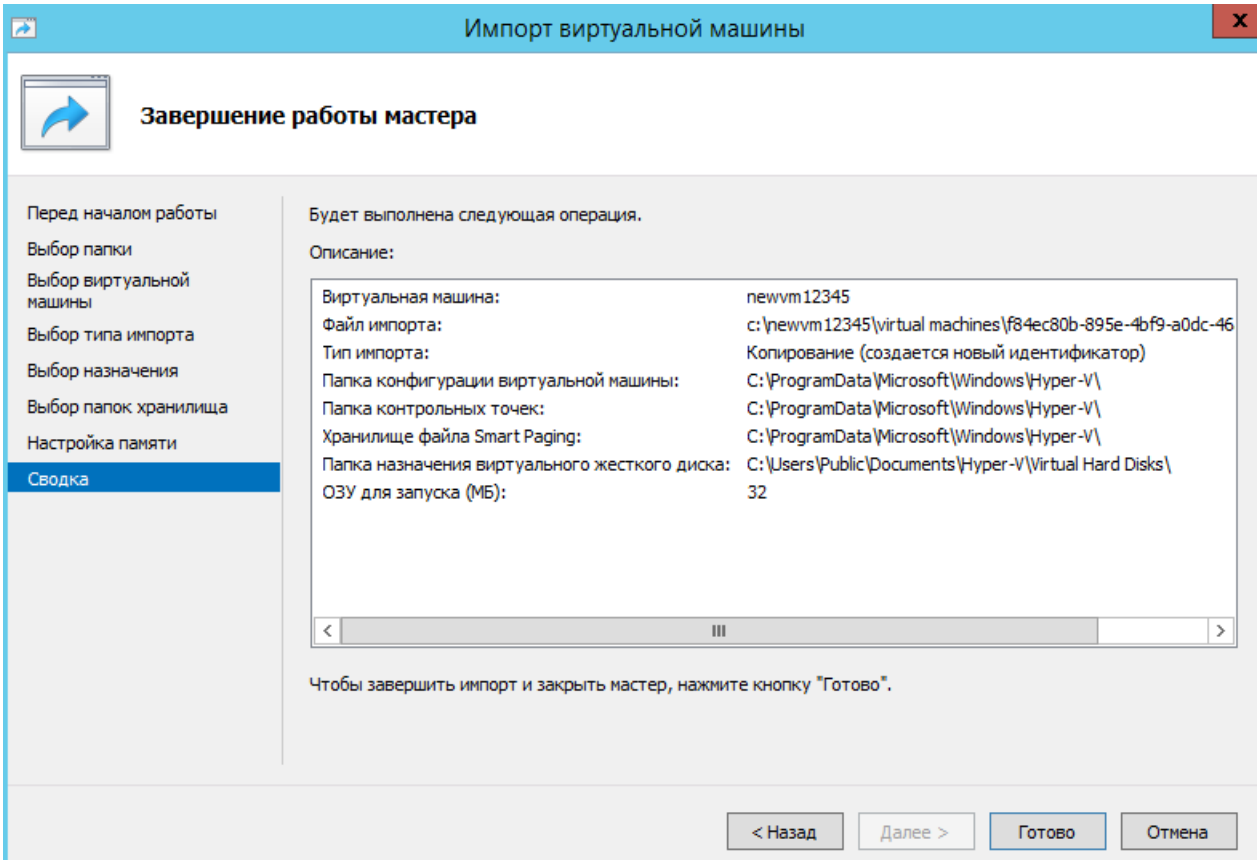


Рисунок 293 – Завершение импорта

Миграция виртуальной машины. Миграция виртуальной машины - это перенос виртуальной машины с одного физического сервера на другой без прекращения работы виртуальной машины и остановки сервисов.

Чтобы мигрировать виртуальную машину следует в левом меню «Диспетчер Hyper-V» выбрать хост Hyper-V, на который необходимо мигрировать виртуальную машину, щелкнуть правой кнопкой мыши и выбрать команду «Параметры Hyper-V». Откроется диалоговое окно «Параметры Hyper-V…». В левой части интерфейса выбрать раздел «Динамическая миграция». Поставить галочку в поле «Включить входящие и исходящие миграции». Поставить отметку в разделе «Входящие динамические миграции» в поле «Использовать любую доступную сеть для динамической миграции» (см. рисунок 294).

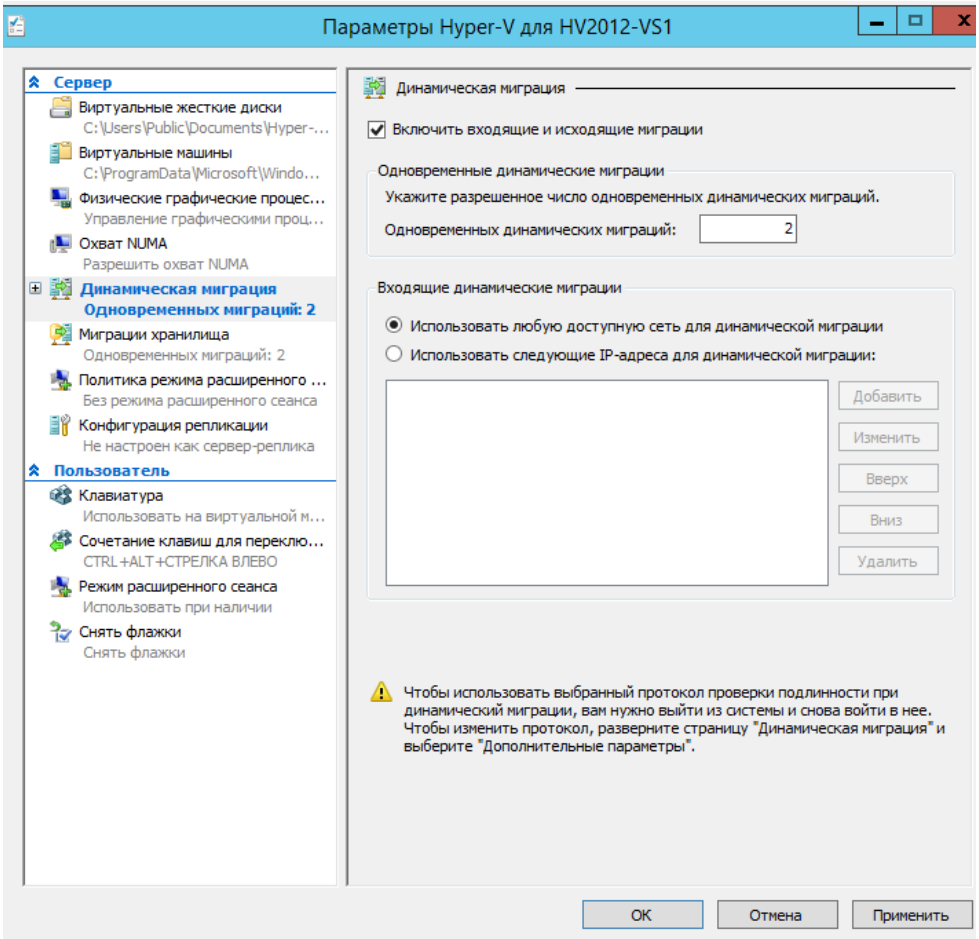


Рисунок 294 – Настройка динамической миграции

Затем нажать на плюсик у настройки раздела «Динамическая миграция», перейти в раздел «Дополнительные параметры». Поставить отметку в поле «Использовать Kerberos» и в поле «Сжатие» (см. рисунок 295).

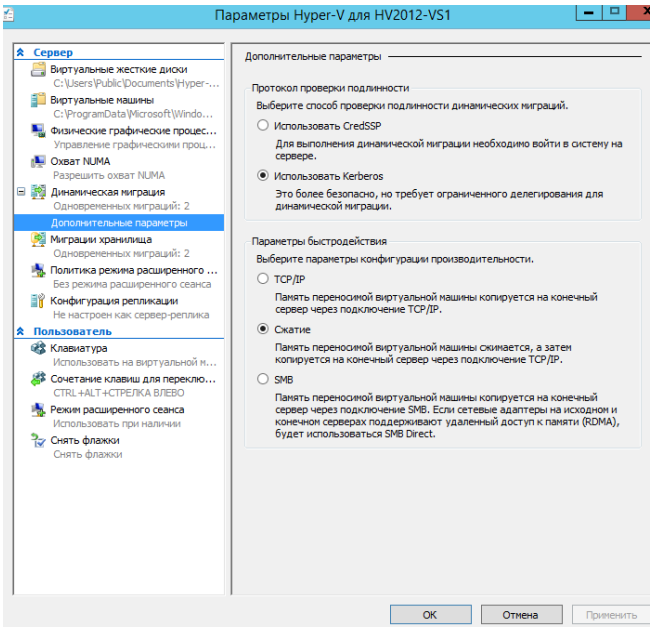


Рисунок 295 – Настройка дополнительных настроек динамической миграции

Затем щелкнуть правой кнопкой мыши по хосту Hyper-V, из которого необходимо мигрировать виртуальную машину. Далее щелкнуть правый кнопкой мыши по виртуальной машине, которую необходимо мигрировать, нажать на команду «Переместить». Откроется диалоговое окно «Мастер перемещения…». Нажать кнопку «Далее» (см. рисунок 296).

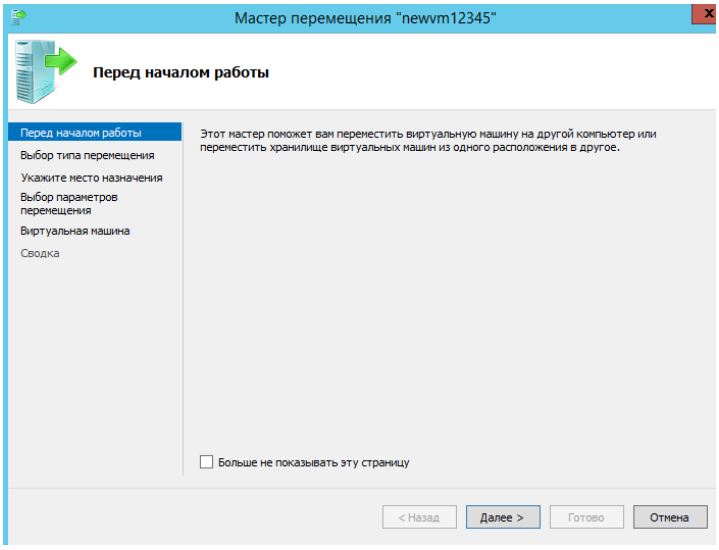


Рисунок 296 – Открытие мастера перемещения

На этапе «Выбор типа перемещения» поставить отметку в поле «Переместить виртуальную машину» (см. рисунок 297).

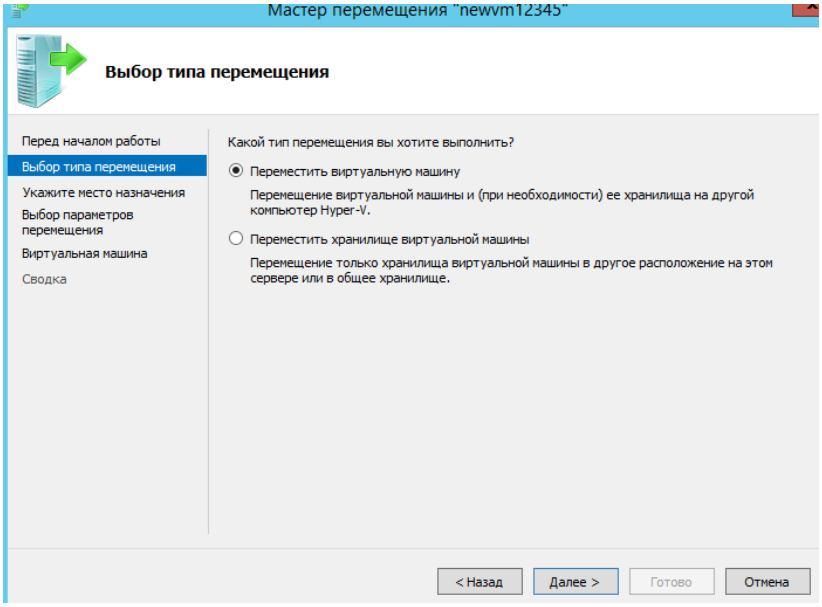


Рисунок 297 – Выбор типа перемещения

На этапе «Укажите место назначения» необходимо указать на какой хост Hyper-V нужно мигрировать виртуальную машину. Нажать кнопку «Обзор». В новом диалоговом окне в разделе «Выберите тип объекта» выбрать тип «Компьютер». Далее нажать на кнопку «Дополнительно». Затем нажать на кнопку «Поиск» и выбрать хост Hyper-V на который нужно переместить виртуальную машину (см. рисунок 298).

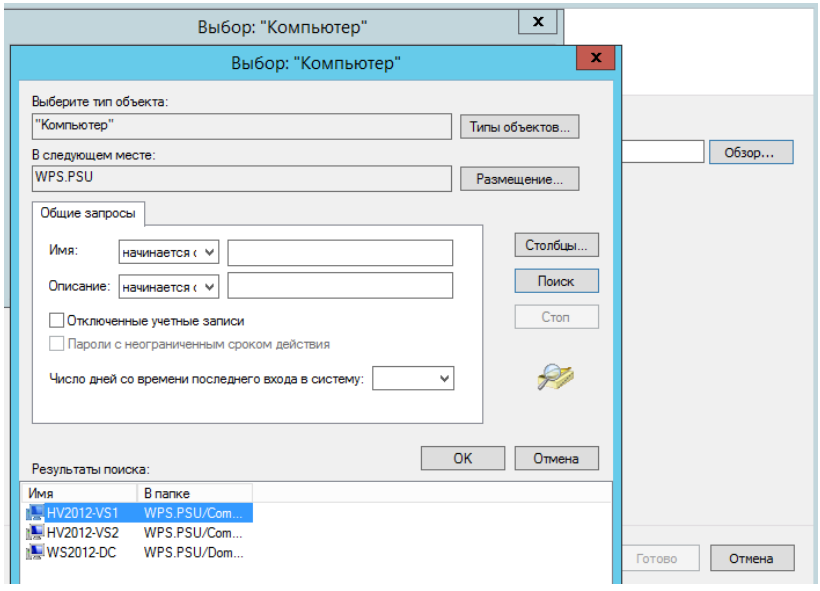


Рисунок 298 - Указание места перемещения

На этапе «Выбор параметров перемещения» поставить отметку в поле «Переместить данные виртуальной машины в одно расположение» (см. рисунок 299).

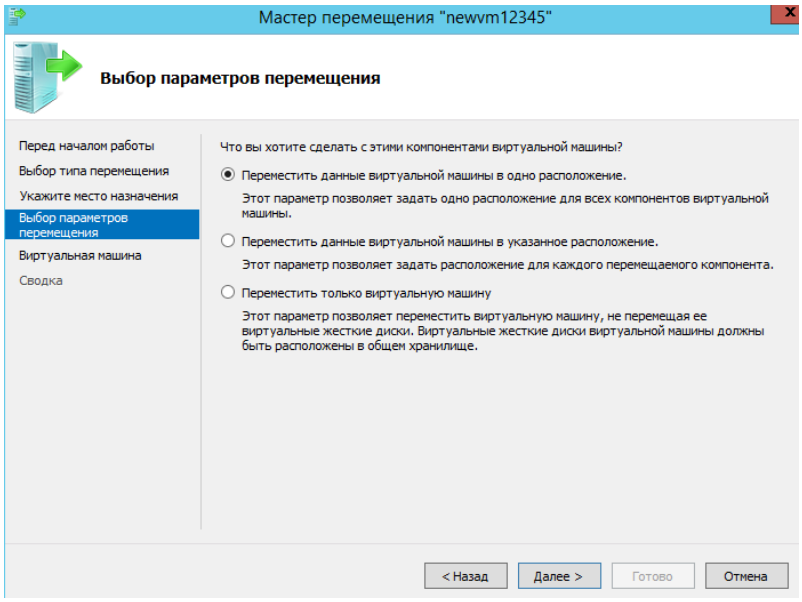


Рисунок 299 – Выбор параметров перемещения

На этапе «Виртуальная машина» указать расположение для элементов виртуальной машины. Нажать кнопку «Обзор» и выбрать нужную папку (см. рисунок 300).

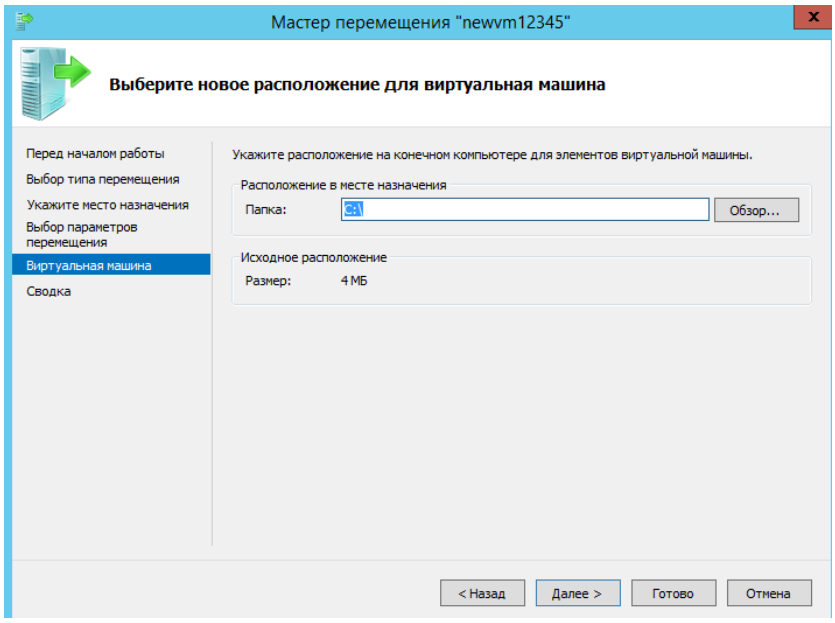


Рисунок 300 – Указание нового расположения для виртуальной машины

На этапе «Сводка» нажать кнопку «Готово» (см. рисунок 299).

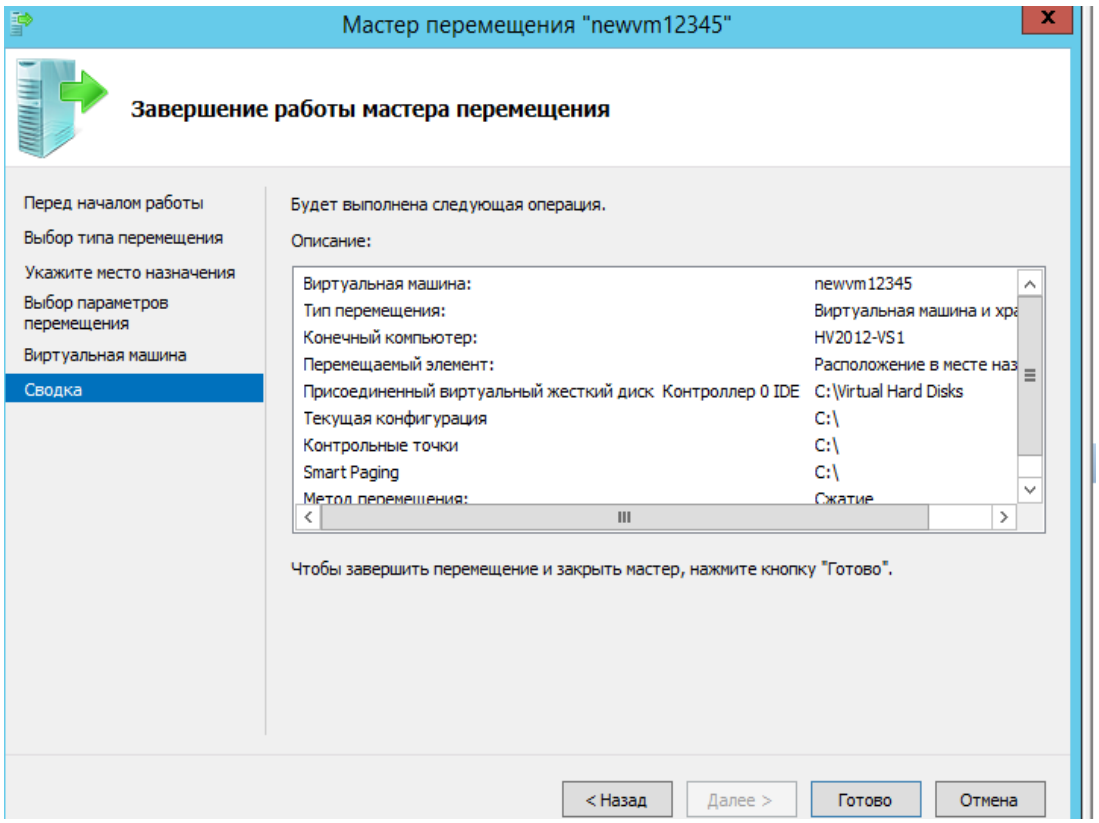


Рисунок 301 – Завершение работы мастера перемещения

В результате выполненных действий виртуальная машина произведет перемещение с одного хоста гипервизора HV2012-VS2 на другой хост гипервизора HV2012-VS1.

Практическое задание предусматривает базовый и повышенный уровни сложности. Базовому уровню сложности соответствуют задачи по созданию виртуальных жестких дисков, созданию виртуальной машины, созданию виртуального коммутатора, подключению виртуального коммутатора к виртуальной машине, репликации виртуальной машины. Повышенному уровню заданий соответствуют задачи экспорту виртуальной машины, импорту виртуальной машины, миграции виртуальной машины.

6 Описание порядка выполнения заданий практикума и результатов выполнения заданий

6.1 Порядок выполнения заданий практикума и результатов выполнения заданий по теме «Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»

Этапы выполнения заданий по теме «Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора» с использованием лабораторного стенда включают в себя:

– ознакомление с теоретическим материалом;

– запуск клиентской виртуальной машины, выполняющей роль рабочей станции;

– выполнение пунктов задания;

– подготовка, формирование и защита отчета о проделанной работе.

В ходе выполнения заданий по теме «Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора» с использованием лабораторного стенда необходимо:

– осуществить вход в систему гипервизора, используя учетную запись администратора домена;

– приступить к выполнению задания практикума;

В завершении выполнения задний с использованием лабораторного стенда необходимо сформулировать вывод по проделанной работе и сформировать отчет.

Выполнение задания осуществляется с помощью описаний выполнения заданий практикума по теме «Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора» которое приведено в главе 4 данного отчета.

В результате выполнения практикума «Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора» будет осуществлено знакомство с порядком работы администратора по локальному управлению сервером виртуализации и функциями безопасности гипервизора, будут получены практические и теоретические навыки по настройке и администрированию гипервизора, созданию, преобразованию, оптимизации, изменению виртуальных жестких дисков, созданию виртуальных машин, подключению к виртуальным машинам привода оптических дисков, созданию виртуальных сетевых адаптеров, подключению к ВМ контроллеров IDE и SCSI, включению службы интеграции для виртуальных машин, настройке BIOS виртуальной машины, заданию конфигурации микропрограммного обеспечения виртуальной машины, созданию пула ресурсов, экспорту контрольных точек, настройки параметров для виртуальных процессоров виртуальной машины, переименованию виртуальных машин, переименованию виртуального сетевого адаптера, созданию нового виртуального коммутатору, переименованию виртуального коммутатора, переименованию виртуальной машины, удалению виртуального коммутатора, удалению виртуальной машины, удалению виртуального сетевого адаптера, обеспечению безопасности компонентов виртуальной машины, подключению виртуальных машин к виртуальному к коммутатору к частной сети и к внутренней сети, созданию стандартных и расширенных списков контроля доступа, настройке параметров виртуальной локальной сети для трафика через виртуальный сетевой адаптер.

UML - диаграмма последовательности действий выполнения практического задания по локальному управлению сервером виртуализации Hyper-V и функциями безопасности гипервизора приведена в приложении Б.

6.2 Порядок выполнения заданий практикума и результатов выполнения заданий по теме «Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»

Этапы выполнения заданий по теме «Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора» с использованием лабораторного стенда:

– изучение теоретического материала;

– запуск виртуальной машины, выполняющей роль контроллера домена и роль рабочей станции.

– убедиться в наличии подключения к внутренней локальной сети;

– выполнение пунктов, предусмотренных заданием;

– подготовка, формирование и защита отчета о проделанной работе.

В ходе выполнения заданий по теме «Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора» с использованием лабораторного стенда необходимо:

– осуществить вход в систему гипервизора, используя учетную запись администратора домена;

– осуществить вход в систему контроллера домена, используя учетную запись администратора домена;

– приступить к выполнению задания практикума;

В завершении выполнения задний с использованием лабораторного стенда необходимо сформулировать вывод по проделанной работе и сформировать отчет.

Выполнение задания осуществляется с помощью описаний выполнения заданий практикума по теме «Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора» которое приведено в главе 5 данного отчета.

В результате выполнения практикума «Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора» будут закреплены теоретические и практические навыки по созданию виртуальных жестких дисков, виртуальной машины, виртуального коммутатора, подключению виртуального коммутатора к виртуальной машине, экспорту виртуальной машины, импорту виртуальной машины, репликации виртуальной машины.

UML - диаграмма последовательности действий выполнения практического задания по удаленному управлению сервером виртуализации Hyper-V и функциями безопасности гипервизора приведена в приложении В.

7 Описание структуры и содержания отчета о выполнении практических заданий

7.1 Структура и содержания отчета о выполнении практических заданий

Отчет о выполнении практических заданий включает следующие разделы:

– титульный лист отчета о выполнении практического задания;

– цель практического задания;

– задание практикума;

– описание выполнения задания практикума, иллюстрируемое снимками экрана, создаваемыми в соответствии с заданием;

– вывод по результатам выполнения задания практикума;

– снимки построенных в соответствии с заданием отчетов.

7.2 Содержание отчета о выполнении практической работы по теме «Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»

Базовый уровень сложности при выполнении заданий практической работы по теме «Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора» предполагает выполнение пунктов «7.2.1-7.2.28».

7.2.1 Настройка гипервизора.

В виде снимков экрана отразить результаты проведения запуска виртуальной машины на определенном узле и установки роли Hyper-V на виртуальной машине HV2012-VS3.

В виде снимков экрана отразить результаты настройки локального хоста Hyper-V с разрешением 10 одновременных миграций в реальном времени и миграцию хранилища.

В виде снимков экрана отразить результаты настройки использования любой сети для входящих миграций в реальном времени на локальном хосте Hyper-V.

В виде снимков экрана отразить результаты задания новых расположений по умолчанию для виртуальных жестких дисков и виртуальных машин на локальном узле Hyper-V.

В виде снимков экрана отразить результаты настройки параметров хоста Fibre Channel на локальном хосте Hyper-V.

В виде снимков экрана отразить результаты отключения связывания NUMA на локальном хосте Hyper-V.

В виде снимков экрана отразить результаты настройки локального хоста Hyper-V для сохранения данных, которые отслеживают потребление ресурсов каждые полтора часа.

В виде снимков экрана отразить результаты настройки локального хоста Hyper-V для использования Kerberos для проверки подлинности входящих миграций.

7.2.2 Проверка установки роли сервера виртуализации и компонента Hyper-V.

В виде снимков экрана отразить результаты проверки установленных компонентов Hyper-V.

В виде снимков экрана отразить результаты установки модуля Hyper-V для Windows PowerShell.

В виде снимков экрана отразить проверку установки компонентов.

7.2.3 Получение списка команд для управления Hyper-V.

Отразить в отчете в виде снимков экрана результаты получения сведений о командлетах, применяемых для управления Hyper-V.

7.2.4 Создание виртуальных жестких дисков.

В виде снимков экрана отразить результаты получения списка всех командлетов PowerShell, которые могут применяться для управления виртуальными жесткими дисками.

В виде снимков экрана отразить результаты создания динамического виртуального жесткого диска в формате VHDX размером 10 ГБ.

В виде снимков экрана отразить результаты создание разностного виртуального жесткого диска формата VHDX с родительским путем c:\Base-да.VHDX-файлы.

В виде снимков экрана отразить результаты создание фиксированного виртуального жесткого диска формата VHDX объемом 5MB по указанному пути с размером блока 128 МБ и размера сектора логического диска 4КВ.

7.2.5 Преобразование виртуальных жестких дисков.

В виде снимков экрана отразить результаты преобразования исходного VHD в конечный VHDX.

7.2.6 Изменение размера виртуальных жестких дисков.

В виде снимков экрана отразить изменение размера виртуального жесткого диска в формате .vhdx до 10Гбайт.

7.2.7 Проверка виртуальных жестких дисков.

В виде снимков экрана отразить результаты преобразования цепочки виртуального жесткого диска.

7.2.8 Оптимизация виртуальных жестких дисков.

В виде снимков экрана отразить результаты выполнение операции компактности в полном режиме.

В виде снимков экрана отразить результаты выполнение операции компактности в Retrim режиме.

В виде снимков экрана отразить результаты выполнение операции компактности в быстром режиме.

7.2.9 Создание виртуальных машин.

В виде снимков экрана отразить результаты получения списка всех командлетов PowerShell, которые могут применяться для управления виртуальными машинами.

В виде снимков экрана отразить результаты создания виртуальной машины с объемом памяти 512 МБ.

В виде снимков экрана отразить результаты создания виртуальной машины с именем newm12345, имеющей 512 МБ памяти и подключенной к новому 800-Мбайтному виртуальному жесткому диску, использующему формат VHDX.

В виде снимков экрана отразить результаты создания Создание виртуальной машины с именем vm512, которая имеет 512 МБ памяти и подключается к существующему виртуальному жесткому диску, использующему формат VHDX.

7.2.10 Подключение к ВМ контроллеров IDE и SCSI.

В виде снимков экрана отразить результаты добавления контроллера SCSI в виртуальную машину.

В виде снимков экрана отразить результаты добавления виртуального жесткого диска к контроллеру SCSI.

В виде снимков экрана отразить результаты добавления виртуального жесткого диска к контроллеру IDE.

7.2.11 Включение служб интеграции для ВМ.

В виде снимков экрана отразить результаты получения работающих служб.

В виде снимков экрана отразить результаты включения службы «Интерфейс гостевой службы».

В виде снимков экрана отразить результаты проверки включения службы «Интерфейс гостевой службы».

7.2.12 Настройка BIOS виртуальной машины поколения 1.

В виде снимков экрана отразить результаты отключения ключа NumLock на виртуальной машине.

В виде снимков экрана отразить результаты настройки виртуальной машины для проверки наличия загрузочного устройства в следующем порядке: дискета, сеть, CD-дисковод, жесткий диск.

7.2.13 Задание конфигурации микропрограммного обеспечения виртуальной машины.

В виде снимков экрана отразить результаты включения функции безопасной загрузки на виртуальной машине.

В виде снимков экрана отразить результаты загрузки виртуальной машины с объекта сетевого адаптера виртуальной машины.

7.2.14 Подключение к ВМ привода оптических дисков.

В виде снимков экрана отразить результаты добавления виртуального DVD-диска для тестирования виртуальной машины.

7.2.15 Переименование виртуальной машины.

В виде снимков экрана отразить результаты переименования виртуальной машины.

2 В виде снимков экрана отразить переименование виртуальной машины и отображение нового имени виртуальной машины.

7.2.16 Удаление виртуальной машины.

В виде снимков экрана отразить результаты удаления виртуального машины.

7.2.17 Создание виртуальных сетевых адаптеров.

В виде снимков экрана отразить результаты добавления виртуального сетевого адаптера на виртуальную машину.

В виде снимков экрана отразить результаты добавления второго виртуального сетевого в операционную систему управлению.

7.2.18 Возвращение виртуальных сетевых адаптеров виртуальной машины, моментального снимка, операционной системы управления или виртуальной машины и операционной системы управления

В виде снимков экрана отразить результаты получения виртуальные сетевые адаптеры со всех виртуальных машин на локальном узле Hyper-V.

В виде снимков экрана отразить результаты возвращения виртуальных сетевых адаптеров в ManagementOS.

В виде снимков экрана отразить результаты получения виртуальных сетевых адаптеров со всех виртуальных машин на локальном узле Hyper-V.

7.2.19 Переименование виртуального сетевого адаптера на виртуальной машине или в операционной системе управления.

В виде снимков экрана результаты переименования всех сетевых адаптеров виртуальной машины.

В виде снимков экрана отразить результаты переименования сетевого адаптера виртуальной машины.

7.2.20 Удаление виртуального сетевого адаптера.

В виде снимков экрана отразить результаты удаления виртуального сетевого адаптера.

7.2.21 Создание нового виртуального коммутатора на одном или нескольких узлах виртуальной машины.

В виде снимков экрана отразить результаты создания внешнего коммутатора.

В виде снимков экрана отразить результаты – преобразования внешнего виртуального коммутатора во внутренней.

В виде снимков экрана отразить результаты создания внешнего виртуального коммутатора.

В виде снимков экрана отразить результаты преобразования внешнего коммутатора в частный.

В виде снимков экрана отразить результаты преобразования внешнего коммутатора во внутренний.

7.2.22 Получение виртуальных коммутаторов от одного или нескольких виртуальных узлов Hyper-V.

В виде снимков экрана отразить результаты получения виртуальных коммутаторов с локального узла Hyper-V.

В виде снимков экрана отразить результаты получения виртуальных коммутаторов, подключенных к внешней сети.

7.2.23 Переименование виртуального коммутатора.

В виде снимков экрана отразить результаты изменения названия виртуального коммутатора.

7.2.24 Удаление виртуального коммутатора.

В виде снимков экрана отразить результаты удаления виртуального коммутатора.

7.2.25 Создание и подключение виртуальных машин к виртуальному коммутатору к внутренней сети.

В виде снимков экрана отразить результаты создания виртуальных машин.

В виде снимков экрана отразить результаты проверки создания виртуальных машин.

В виде снимков экрана отразить результаты создания виртуального коммутатора с частным типом сети.

В виде снимков экрана отразить результаты подключения виртуальных машин к виртуальному коммутатору.

В виде снимков экрана отразить результаты проверки подключения виртуальных машин к виртуальному коммутатору.

В виде снимков экрана отразить результаты изменения имен сетевых адаптеров виртуальных машин.

В виде снимков экрана отразить проверки изменений сетевых адаптеров.

В виде снимков экрана отразить результаты добавления виртуальных сетевых адаптеров в операционную систему управления.

В виде снимков экрана отразить результаты настройка сети виртуальных машин.

7.2.26 Создание и подключение виртуальных машин к виртуальному коммутатору к частной сети.

В виде снимков экрана отразить результаты создания виртуального коммутатора с частным типом сети.

В виде снимков экрана отразить результаты подключения виртуальных машин к виртуальному коммутатору.

В виде снимков экрана отразить результаты проверки подключения виртуальных машин к виртуальному коммутатору.

В виде снимков экрана отразить результаты изменения имен сетевых адаптеров виртуальных машин.

В виде снимков экрана отразить проверки изменений сетевых адаптеров.

В виде снимков экрана отразить результаты добавления виртуальных сетевых адаптеров в операционную систему управления.

В виде снимков экрана отразить результаты настройка сети виртуальных машин.

7.2.27 Создание стандартных списков контроля доступа.

В виде снимков экрана отразить результаты создания стандартного списка контроля доступа для разрешения виртуальной машине отправлять и получать трафик.

В виде снимков экрана отразить результаты создания стандартного списка контроля доступа, который запрещает виртуальной машине отправлять трафик IPv4 или IPv6 в любое место и получать такой трафик из любого места.

7.2.28 Обеспечение безопасности компонентов виртуальной инфраструктуры.

В виде снимков экрана отразить результаты создания учетной записи на гипервизоре.

В виде снимков экрана отразить результаты проверки возможности создания вирутального жесткого на новой учетной записи на гипервизоре.

В виде снимков экрана отразить результаты добавления нового пользователя в группу локальных администраторов.

В виде снимков экрана отразить результаты проверки возможности создания вирутального жесткого на нвоой учетной записи, добавленной в группу локальных администраторов.

В виде снимков экрана отразить результаты создания учетной записи доменного пользователя.

В виде снимков экрана отразить результаты попытки входа на новую учетную запись.

Повышенной уровень сложности при выполнении заданий практической работы №1 предполагает выполнение пунктов «7.3.1-7.3.6».

7.3.1 Создание пула ресурсов.

В виде снимков экрана отразить результаты создания нового пула ресурсов виртуального жесткого диска.

7.3.2 Возврат контрольных точек, связанных с виртуальной машиной или контрольной точкой.

В виде снимков экрана отразить результаты отображения контрольных точек виртуальной машины.

В виде снимков экрана отразить результаты отображения Отображение стандартных контрольных точек виртуальной машины.

7.3.3 Экспорт контрольной точки виртуальной машины на диск.

В виде снимков экрана отразить результаты экспорта контрольной точки.

Возврат процессора виртуальной машины или моментальный снимок.

В виде снимков экрана отразить результаты отображения процессора виртуальной машины.

7.3.4 Настройка параметров для виртуальных процессоров виртуальной машины.

В виде снимков экрана отразить результаты настройки виртуальной машины с одним виртуальным процессором, резервом 10%, пределом 75% и приоритет распределения вычислительной мощности физического компьютера 200.

В виде снимков экрана отразить результаты настройки виртуальной машины, включая совместимость процессоров для динамической миграции.

В виде снимков экрана отразить результаты настройки виртуальной машины, включая совместимость для запуска более старых операционных систем.

7.3.5 Создание расширенных списков контроля доступа.

В виде снимков экрана отразить результаты создания расширенного контроля доступа для разрешения виртуальной машине отправлять исходящие пакеты на удаленное устройство с помощью протокола TCP.

В виде снимков экрана отразить результаты создания расширенного списка контроля доступа, который позволяет удаленному устройству подключаться к виртуальной машине по порту 3379, который является портом для протокола удаленного рабочего стола.

7.3.6 Настройка параметров виртуальной локальной сети для трафика через виртуальный сетевой адаптер

В виде снимков экрана отразить результаты установки виртуального сетевого адаптера в виртуальной машине в режим доступа.

В виде снимков экрана отразить результаты установки виртуального сетевого адаптера в виртуальной машине в режим магистрали.

7.3 Содержание отчета о выполнении практической работы по теме «Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»

Базовый уровень сложности при выполнении заданий практической работы по теме «Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора» предполагает выполнение пунктов «7.3.1 - 7.3.7».

7.3.1 Создание виртуальных жестких дисков.

В виде снимков экрана отразить результаты создания жестких дисков.

7.3.2 Создание виртуальной машины.

В виде снимков экрана отразить результаты создания виртуальной машины.

7.3.3 Создание виртуальных коммутаторов.

В виде снимков экрана отразить результаты создания виртуальных коммутаторов.

7.3.4 Подключение виртуального коммутатора к виртуальной машине.

В виде снимков экрана отразить результаты подключения виртуального коммутатора к виртуальной машине.

7.3.5 Репликация виртуальной машины.

В виде снимков экрана отразить результаты репликации виртуальной машины

Повышенной уровень сложности при выполнении заданий практической работы предполагает выполнение пунктов «7.3.5-7.3.7».

7.3.5 Экспорт виртуальной машины.

В виде снимков экрана отразить результаты экспорта виртуальной машины.

7.3.6 Импорт виртуальной машины.

В виде снимков экрана отразить результаты импорта виртуальной машины.

7.3.7 Миграция виртуальной машины.

В виде снимков экрана отразить результаты миграции виртуальной машины.

Графическое представление структуры отчета о выполнении практических работ приведено в приложении Г.

Контрольные экземпляры отчетов о выполнении практических работ приведены в приложении Д.

8 Определение порядка контроля выполнения практического задания

Порядок контроля выполнения практического задания выполняется одинаково для двух заданий и предусматривает следующие этапы контроля:

– проверка даты выполнения и сроков формирования отчетов;

– проверка правильности оформления отчета установленным требованиям;

– проверка правильности оформления отчета установленным требованиям;

– проверка правильности порядка выполнения заданий базового уровня, согласно описанию выполнения заданий;

– проверка наличия и правильности выполнения заданий повышенного уровня сложности;

– проверка наличия всех необходимых снимков экрана;

– проверка составленных отчетов;

– проверка сделанных выводов о результатах выполнения практического задания.

Графическое представление порядка контроля выполнения практического задания приведено в приложении Е.

9 Подготовка сценариев для автоматизированного развертывания ВМ

VBoxManage – утилита командной строки, позволяющая контролировать все возможности VirtualBox. Утилита VBoxManage позволяет изменять свойства созданных виртуальных машин. Большинство возможностей, которые утилита позволяет использовать, соответствуют возможностям, которые доступны в пользовательском графическом интерфейсе Oracle VM VirtualBox, которые отображены в диалоговом окне настроек при создании ВМ, однако большинство сложных настроек доступны только с использованием утилиты VBoxManage. К таким настройкам относится разработка сценариев автоматизированного развертывания ВМ.

Сценарий это – система взаимодействия, которая обрабатывает и перенаправляет инструкции (команды), выполняемые над объектом, от контролирующего к контролируемому.

Сценарий представляет собой набор команд которые включают в себя элементы приложения доступные для обработки, методы обращения, и ссылочный файл (элемент файловой системы).

Для автоматизации развертывания ВМ входящих в состав стенда разработаны сценарии, определяющие конфигурацию ВМ после их создания, и режимы их работы в момент их использования.

В качестве управления используется набор команд. Некоторые часто используемые наборы команд:

– `#VBoxManage list vms` - просмотр перечня гостевых операционных систем;

– `#VBoxManage showvminfo` - просмотр подробной информации о конкретной виртуальной ОС;

– `#VBoxManage startvm "WS2012-DC"` - запуск гостевой ОС;

– `#VBoxManage startvm " WS2012-DC " --type=headless` - запуск гостевой ОС в фоне (например через ssh-туннель);

– `#VBoxManage controlvm " WS2012-DC " savestate` - выключение гостевой ОС.

Сценарии определяют аппаратную конфигурацию виртуальной машины, которая определяется при создании ВМ.

Аппаратная конфигурация гипервизора включает в себя следующие параметры:

– количество процессоров – 1;

– объем оперативной памяти – минимальный 1Гбайт, рекомендуемый 2 ГБайт;

– виртуальный жесткий диск, подключаемый с использованием интерфейса SATA. Объем виртуального жесткого диска – 20 ГБайт;

– привод оптических дисков, подключаемый с использованием интерфейса SATA;

– видеопамять объемом 128 Мбайт;

– общая папка обмена между гостевой и основной ОС.

Аппаратная конфигурация контроллера домена включает в себя следующие параметры:

– количество процессоров – 1;

– объем оперативной памяти – 2 ГБайт;

– виртуальный жесткий диск, подключаемый с использованием интерфейса SATA. Объем виртуального жесткого диска – 30 ГБайт;

– привод оптических дисков, подключаемый с использованием интерфейса SATA;

– видеопамять объемом 128 Мбайт;

– сетевой адаптер с типом подключения «внутренняя сеть» (intnet). Тип адаптера Intel PRO/1000;

– общая папка обмена между гостевой и основной ОС.

В сценариях был задан режим работы виртуальных машин, автоматически возвращающий их в исходное состояние при закрытии, который называется «immutable». Любые изменения в immutable диске актуальны ровно до тех пор, пока виртуальная машина работает. После отключения виртуальной машины все изменения пропадают.

Было подготовлено три сценария для автоматизированного развертывания виртуальных машин. Разработанные сценарии приведены в приложении Ж.

10 Вредные психофизиологические факторы, влияющие на опорно-двигательный аппарат специалиста по защите информации. Методы и средства физической культуры, снижающие их воздействие

Работа специалиста по защите информации предполагает работу с различными техническими средствами, которые могут негативно воздействовать на организм специалиста. К таким воздействиям относятся:

— электромагнитные излучения и радиоизлучения;

— высокочастотные звуковые сигналы;

— вибрация;

— ненормированный уровень шума;

— ненормированная яркость изображения на экране мониторов и дисплеев.

Также негативное влияние на здоровье специалиста по защите информации оказывают внешние факторы, такие как:

— вид трудовой активности;

— микроклимат помещений;

— освещенность рабочего места;

— расположение органов управления и технических средств на рабочем месте по отношению к специалисту.

Воздействие вредных факторов на опорно-двигательный аппарат специалиста зависит в первую очередь от его двигательной активности в период рабочего времени. Сфера его деятельности может включать:

— длительное нахождение в помещении с высоким уровнем вибрации;

— работу, связанную с частым переносом тяжелого оборудования;

— длительное пребывание в сидячем положении.

Так, при постоянном выполнении работ в помещениях с высоким уровнем вибрации у специалиста страдает мышечная система, хрящи и связки. При постоянной вибрации появляется мышечная усталость, их сила снижается, происходит атрофия мышц. Хрящевая ткань от вибраций становится грубее и затрудняет движения в суставах, о чем может свидетельствовать боль и отеки. Связки также становятся грубее и менее прочными, что приводит к их растяжению и разрыву.

Во время поднятия, приёма, переноса или перестановки тяжелого оборудования создается большая нагрузка на мышцы, а при неразвитой мускулатуре или поднятии очень большого веса, всю нагрузку берет на себя позвоночник. Вследствие этого возможно растяжение и разрыв мышц спины, смещение, протрузии, грыжи межпозвоночных дисков.

Если же рабочая деятельность подразумевает постоянное нахождение в сидячем положении при работе на компьютере, это может привести к развитию тоннельного синдрома запястного канала, искривлению позвоночника, остеохондрозу позвоночника шейного, грудного и поясничного отделов, застоя венозной крови в органах малого таза и ногах, что может привести к варикозу и тромбозу.

Во избежание получения травм во время работы необходимо поддерживать правильное положение тела, как показано на рисунках 302 и 303.

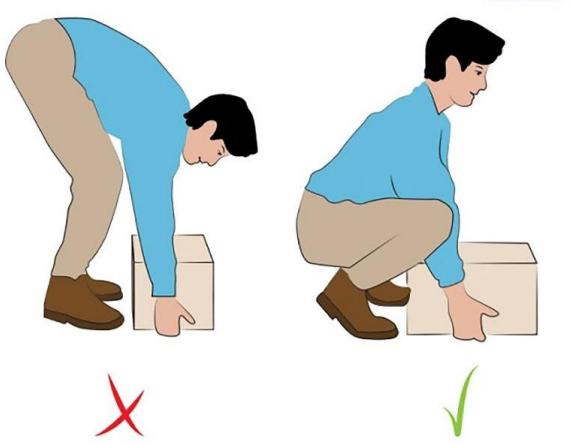


Рисунок 302 — Правильный и неправильный подъем груза

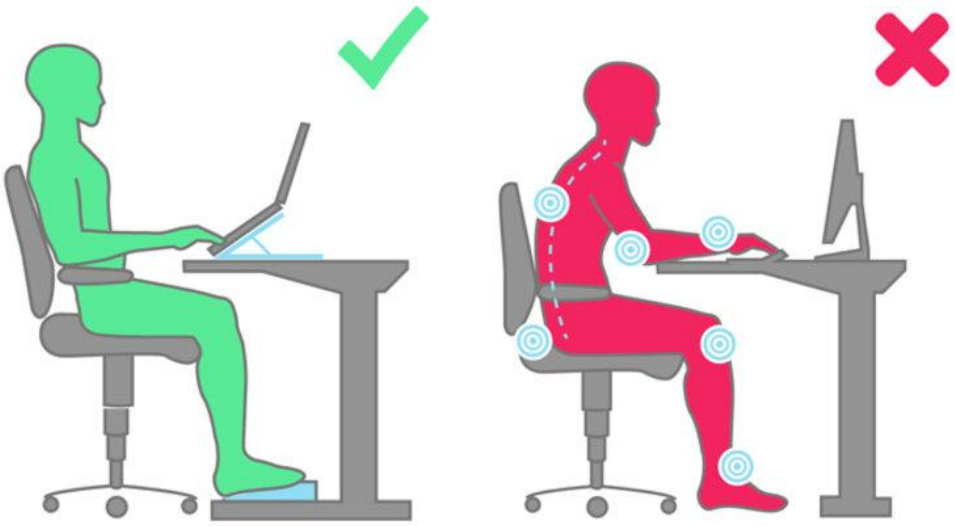


Рисунок 303 — Неправильное и правильное положение сидя

Также, помимо соблюдения правильного положения тела, для профилактики негативных воздействий, влияющих на опорно-двигательный аппарат специалиста по защите информации рекомендуется выполнять следующие действия, направленные на разгрузку и поддержание в тонусе опорно-двигательного аппарата:

— ежедневная утренняя зарядка;

— ежедневная ходьба в среднем темпе в течение 40 минут;

— занятие активными видами спорта;

— делать небольшой перерыв через каждые 2 или 3 часа постоянной работы, во время которого осуществлять разминку опорно-двигательного аппарата;

— массаж.

Заключение

В результате выполнения выпускной квалификационной работы был разработан лабораторный стенд, обеспечивающий изучение механизмов безопасности операционной системы (ОС) Windows Server, используемых для обеспечения безопасности компонентов среды виртуализации.

Лабораторный стенд обеспечивает выполнение следующих заданий:

– локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора;

– удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора.

В ходе дипломного проектирования был проведен обзор механизмов безопасности Windows Server, применяемых для защиты виртуальных инфраструктур. После чего в ходе написания отчета о ВКР был описан процесс создания новой виртуальной машины с помощью средства виртуализации Oracle VM Virtual Box и процесс настройки ВМ с помощью программы Oracle VM Virtual Box Менеджер. Произведено описание процесса установки гостевой операционной системы на виртуальную машину в полном объеме. Произведена установка компонентов Hyper-V. Произведена настройка общей папки обмена основной и гостевой ОС. Реализовано конфигурирование локальной сети, состоящей из виртуальных машин. Была выполнена установка компонентов ОС Windows Server, реализующей механизмы защиты виртуальных инфраструктур и средства администрирования. Разработано описание порядка выполнения практических заданий с использованием разработанного лабораторного стенда для подготовки специалистов по ИБ.

В результате выполнения составленных заданий студенты получат навыки по локальному и удаленному управлению сервером виртуализации Hyper-V и функциями безопасности гипервизора.

Таким образом, все пункты технического задания на выпускную квалификационную работу выполнены в полном объеме.

В процессе выполнения выпускной квалификационной работы была подготовлена статья на тему «Обзор функциональных возможностей операционной системы Windows Server, применяемых для защиты виртуальных инфраструктур» и опубликована в сборнике VII Ежегодной всероссийской межвузовской научно-практической конференции «Информационные технологии в науке и образовании. Проблемы и перспективы»[5].

Протокол проверки отчета ВКР в системе «Антиплагиат» приведен в приложении И.

Список используемых источников

1 Microsoft-официальная страница [Электронный ресурс]. Режим доступа: https://www.microsoft.com/ru-ru, (свободный).

2 VirtualBox-официальная страница [Электронный ресурс]. Режим доступа https://www.virtualbox.org, (свободный).

3 Справочник командлетов Windows PowerShell [Электронный ресурс]. Режим доступа: http://prolibra.ru/article/administration/windows/46-spravochnik-komandletov-windows-powershell, (свободный).

4 Механизмы в Windows Server для защиты виртуальных инфраструктур. [Электронный ресурс]. Режим доступа: http://www.oszone.net/18743/ (свободный).

5 Трушин Р.Н., Фатеев А.Г. «Обзор функциональных возможностей операционной системы Windows Server, применяемых для защиты виртуальных инфраструктур». Сборник статей по материалам VII Всероссийской межвузовской научно-практической конференции. [Электронный ресурс]// Режим доступа: https://www.elibrary.ru/item.asp?id=42821624/ (свободный).

Приложение А

(обязательное)

Состав виртуального стенда, использующегося при выполнении практикума

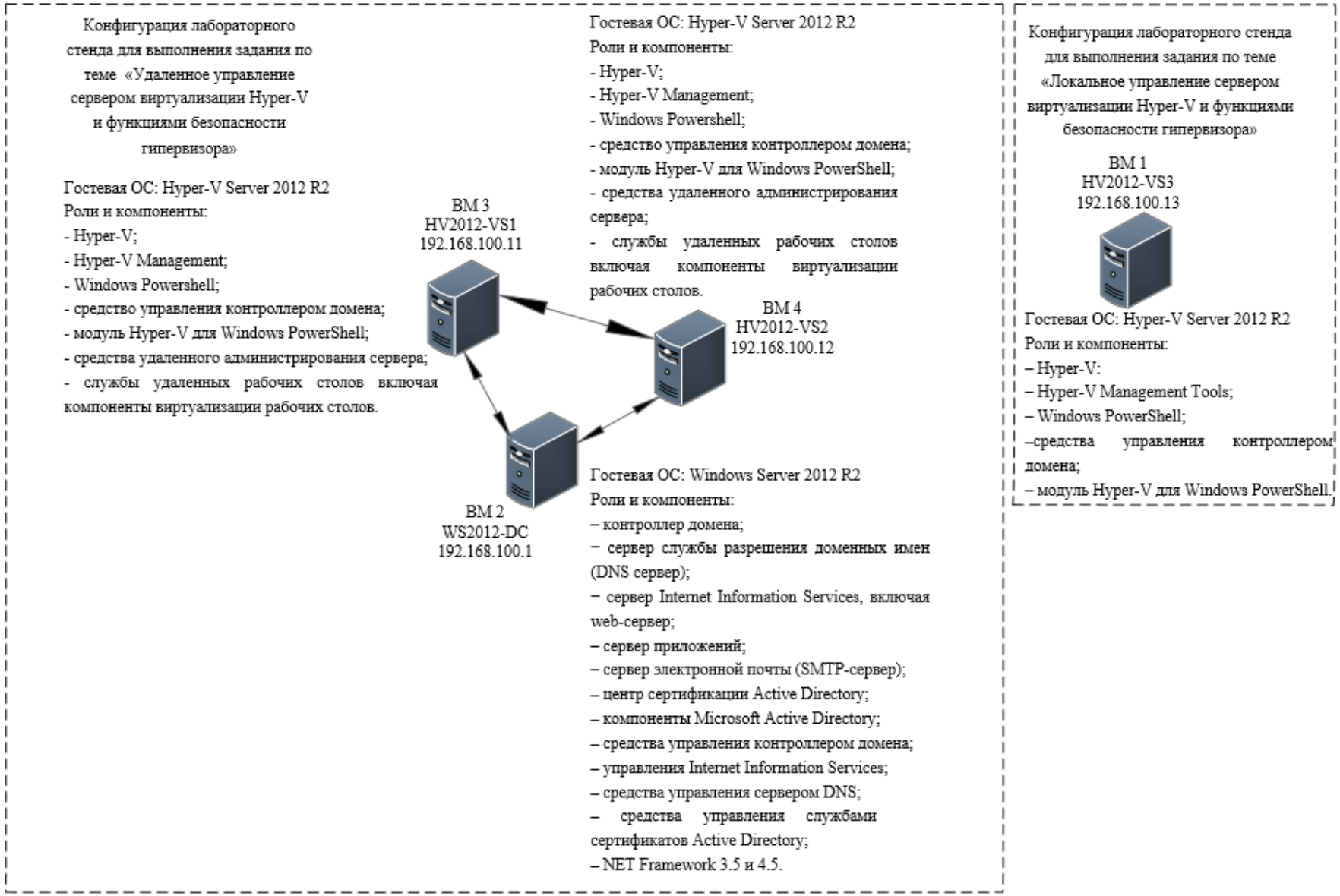


Рисунок А.1 - Состав виртуального стенда, использующегося при выполнении практикума

Приложение Б

(обязательное)

UML – диаграмма последовательности действий при выполнении практического задания по теме «Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора

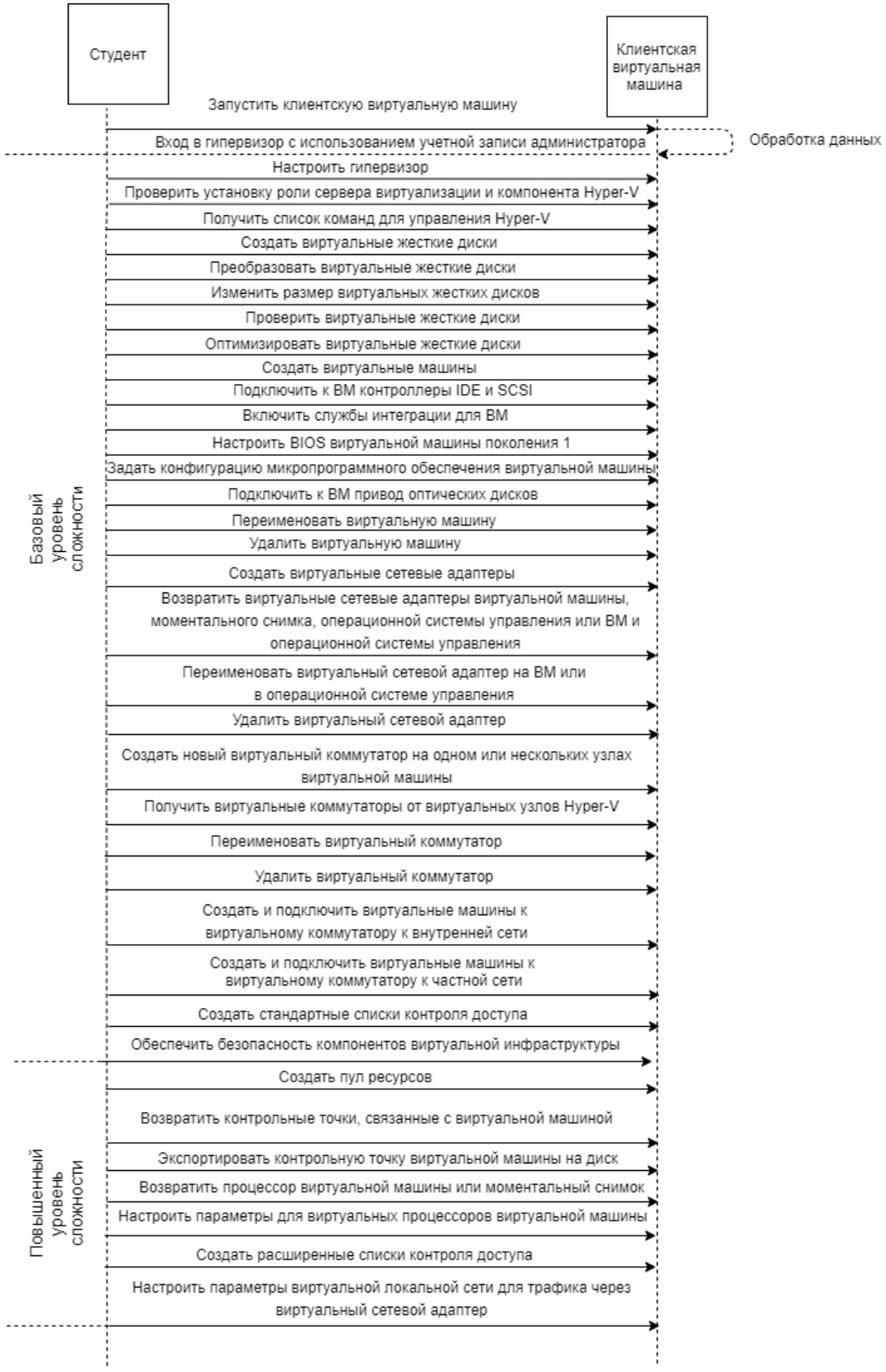


Рисунок Б.1 - UML – диаграмма последовательности действий выполнения практического задания по локальному управлению сервером виртуализации Hyper-V и функциями безопасности гипервизора

Приложение В

(обязательное)

UML – диаграмма последовательности действий при выполнении практического задания по теме «Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора

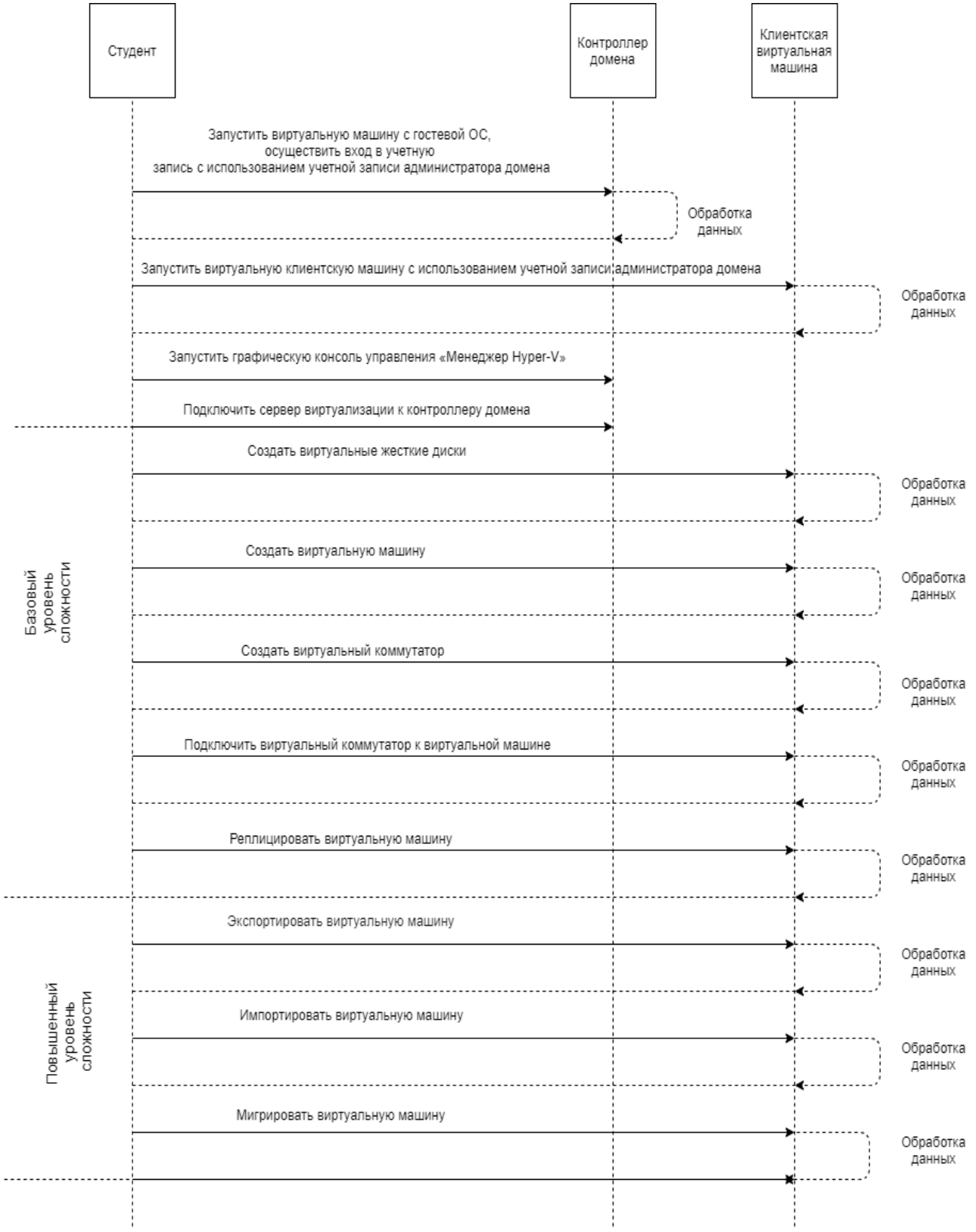


Рисунок В.1 - UML – диаграмма последовательности действий выполнения практического задания по удаленному управлению сервером виртуализации Hyper-V и функциями безопасности гипервизора

Приложение Г

(обязательное)

Графическое представление структур отчетов о выполнении практических работ

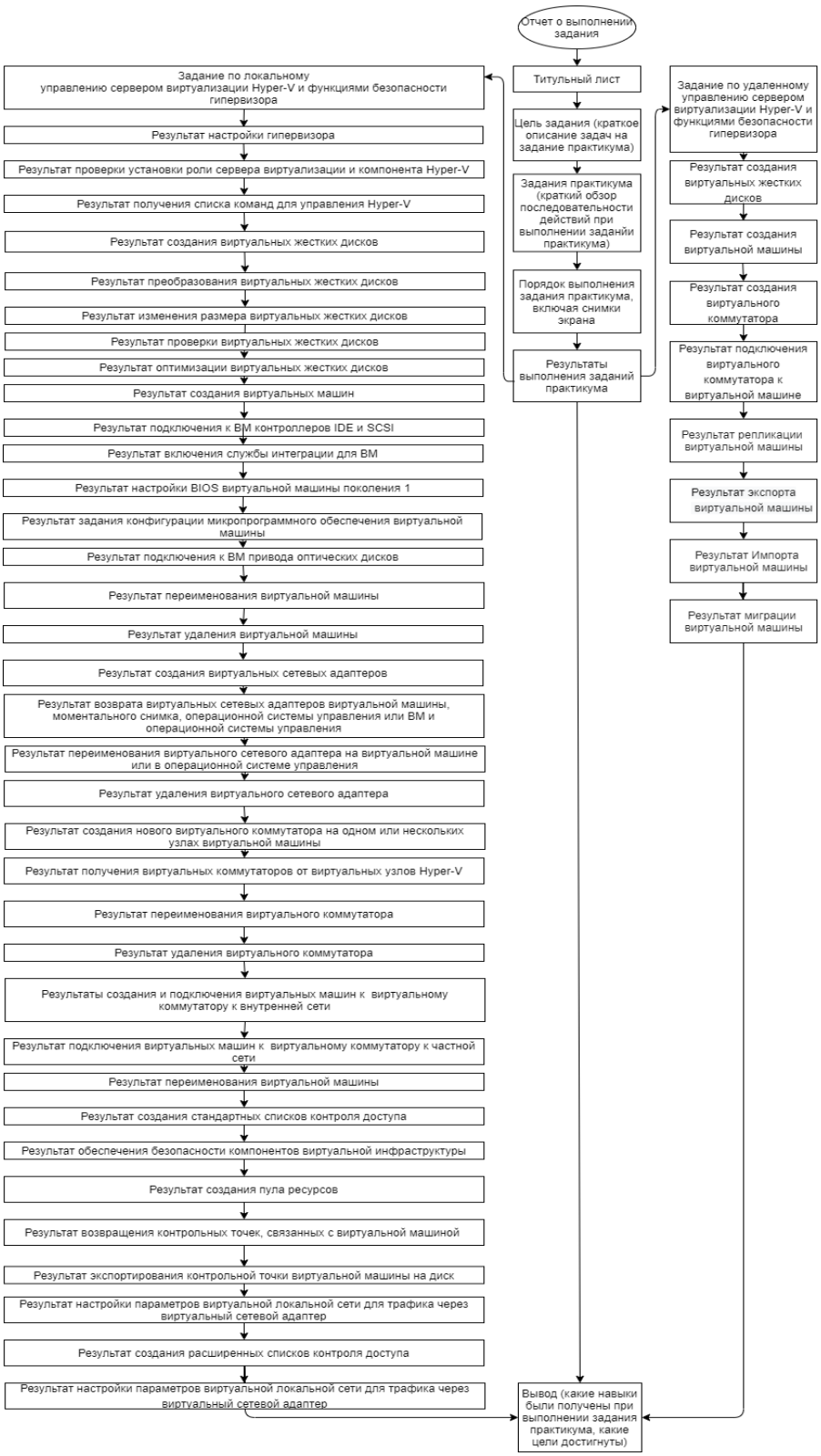


Рисунок Г.1 – Структура и содержание отчета о выполнении практических заданий по теме «Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора» и заданий по теме «Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»

Приложение Д

(обязательное)

Контрольные экземпляры отчетов о выполнении практических работ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Кафедра «Информационная безопасность систем и технологий»

ОТЧЕТ

о выполнении практической работы

«Локальное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»

Дисциплина:

Группа:

Выполнил:

Количество баллов:

Дата сдачи:

Принял:

2020

Цель работы – получить навыки по локальному управлению сервером виртуализации Hyper-V и функциями безопасности гипервизора.

Задание на лабораторный практикум включает в себя:

– настройка гипервизора;

– проверка установки роли сервера виртуализации, компонента Hyper-V;

– получение списка команд для управления Hyper-V;

– создание виртуальных жестких дисков;

– преобразование виртуальных жестких дисков;

– изменение размера виртуальных жестких дисков;

– проверка виртуальных жестких дисков;

– оптимизация виртуальных жестких дисков;

– создание виртуальных машин;

– подключение к ВМ контроллеров IDE и SCSI;

– включение служб интеграции для ВМ;

– настройка BIOS виртуальной машины поколения;

– задание конфигурации микропрограммного обеспечения виртуальной машины;

– подключение к ВМ привода оптических дисков;

– переименование виртуальной машины;

– удаление виртуальной машины;

– создание виртуальных сетевых адаптеров;

– возвращение виртуальных сетевых адаптеров виртуальной машины, моментального снимка, операционной системы управления или виртуальной машины и операционной системы управления;

– переименование виртуального сетевого адаптера на виртуальной машине или в операционной системе управления;

– удаление виртуального сетевого адаптера;

– создание нового виртуального коммутатора на одном или нескольких узлах виртуальной машины;

– получение виртуальных коммутаторов от одного или нескольких виртуальных узлов Hyper-V;

– переименование виртуального коммутатора;

– удаление виртуального коммутатора;

– создание и подключение виртуальных машин к виртуальному коммутатору к внутренней сети;

– создание и подключение виртуальных машин к виртуальному коммутатору к частной сети;

– создание стандартных списков контроля доступа;

– обеспечение безопасности компонентов виртуальной инфраструктуры;

– создание пула ресурсов;

– возврат контрольных точек, связанных с виртуальной машиной или контрольной точкой;

– экспорт контрольной точки виртуальной машины на диск;

– настройка параметров для виртуальных процессоров виртуальной машины;

– создание расширенных списков контроля доступа;

– настройка параметров виртуальной локальной сети для трафика через виртуальный сетевой адаптер.

Порядок выполнения задания.

Показать в виде снимков экрана результаты настройки гипервизора.

Показать в виде снимков экрана результаты проверки установки роли сервера виртуализации, компонента Hyper-V.

Показать в виде снимков экрана результаты получения списка команд для управления Hyper-V.

Показать в виде снимков экрана результаты создания виртуальных жестких дисков.

Показать в виде снимков экрана результаты преобразование виртуальных жестких дисков.

Показать в виде снимков экрана результаты изменения размера виртуальных жестких дисков.

Показать в виде снимков экрана результаты проверки виртуальных жестких дисков.

Показать в виде снимков экрана результаты оптимизации виртуальных жестких дисков.

Показать в виде снимков экрана результаты создания виртуальных машин.

Показать в виде снимков экрана результаты подключения к ВМ контроллеров IDE и SCSI.

Показать в виде снимков экрана результаты включения службы интеграции для ВМ.

Показать в виде снимков экрана результаты настройки BIOS виртуальной машины поколения 1.

Показать в виде снимков экрана результаты задания конфигурации микропрограммного обеспечения виртуальной машины.

Показать в виде снимков экрана результаты подключения к ВМ привода оптических дисков.

Показать в виде снимков экрана результаты переименования виртуальной машины.

Показать в виде снимков экрана результаты удаления виртуальной машины.

Показать в виде снимков экрана результаты создания виртуальных сетевых адаптеров.

Показать в виде снимков экрана результаты возврата виртуальных сетевых адаптеров виртуальной машины, моментального снимка, операционной системы управления или ВМ и операционной системы управления.

Показать в виде снимков экрана результаты переименования виртуального сетевого адаптера на виртуальной машине или в операционной системе управления.

Показать в виде снимков экрана результаты удаления виртуального сетевого адаптера.

Показать в виде снимков экрана результаты создания нового виртуального коммутатора на одном или нескольких узлах виртуальной машины.

Показать в виде снимков экрана результаты получения виртуальных коммутаторов от виртуальных узлов Hyper-V.

Показать в виде снимков экрана результаты переименования виртуального коммутатора.

Показать в виде снимков экрана результаты удаления виртуального коммутатора.

Показать в виде снимков экрана результаты создания и подключения виртуальных машин к виртуальному коммутатору к внутренней сети.

Показать в виде снимков экрана результаты подключения виртуальных машин к виртуальному коммутатору к частной сети.

Показать в виде снимков экрана результаты переименования виртуальной машины.

Показать в виде снимков экрана результаты создания стандартных списков контроля доступа.

Показать в виде снимков экрана результаты обеспечения безопасности компонентов виртуальной инфраструктуры.

Показать в виде снимков экрана результаты создания пула ресурсов.

Показать в виде снимков экрана результаты возвращения контрольных точек, связанных с виртуальной машиной или контрольной точкой.

Показать в виде снимков экрана результаты экспортирования контрольной точки виртуальной машины на диск.

Показать в виде снимков экрана результаты настройки параметров виртуальной локальной сети для трафика через виртуальный сетевой адаптер.

Показать в виде снимков экрана результаты создания расширенных списков контроля доступа.

Показать в виде снимков экрана результаты настройки параметров виртуальной локальной сети для трафика через виртуальный сетевой адаптер.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
Кафедра «Информационная безопасность систем и технологий»

ОТЧЕТ

о выполнении практической работы

«Удаленное управление сервером виртуализации Hyper-V и функциями безопасности гипервизора»

Дисциплина:

Группа:

Выполнил:

Количество баллов:

Дата сдачи:

Принял:

2020

Цель работы – получить навыки по удаленному управлению сервером виртуализации Hyper-V и функциями безопасности гипервизора.

Задание на лабораторный практикум включает в себя:

– создание виртуальных жестких дисков;

– создание виртуальной машины;

– создание виртуального коммутатора;

– подключение виртуального коммутатора к виртуальной машине;

– репликация виртуальной машины;

– экспорт виртуальной машины;

– импорт виртуальной машины;

– миграция виртуальной машины.

Порядок выполнения заданий.

Показать в виде снимков экрана результаты создания виртуальных жестких дисков.

Показать в виде снимков экрана создание виртуальной машины.

Показать в виде снимков экрана результаты создания виртуального коммутатора.

Показать в виде снимков экрана результаты подключения виртуального коммутатора к виртуальной машине.

Показать в виде снимков экрана результаты репликации виртуальной машины.

Показать в виде снимков экрана результаты экспорта виртуальной машины.

Показать в виде снимков экрана результаты импорта виртуальной машины.

Показать в виде снимков экрана результаты миграции виртуальной машины.

Приложение Е

(обязательное)

Графическое представление порядка контроля выполнения заданий

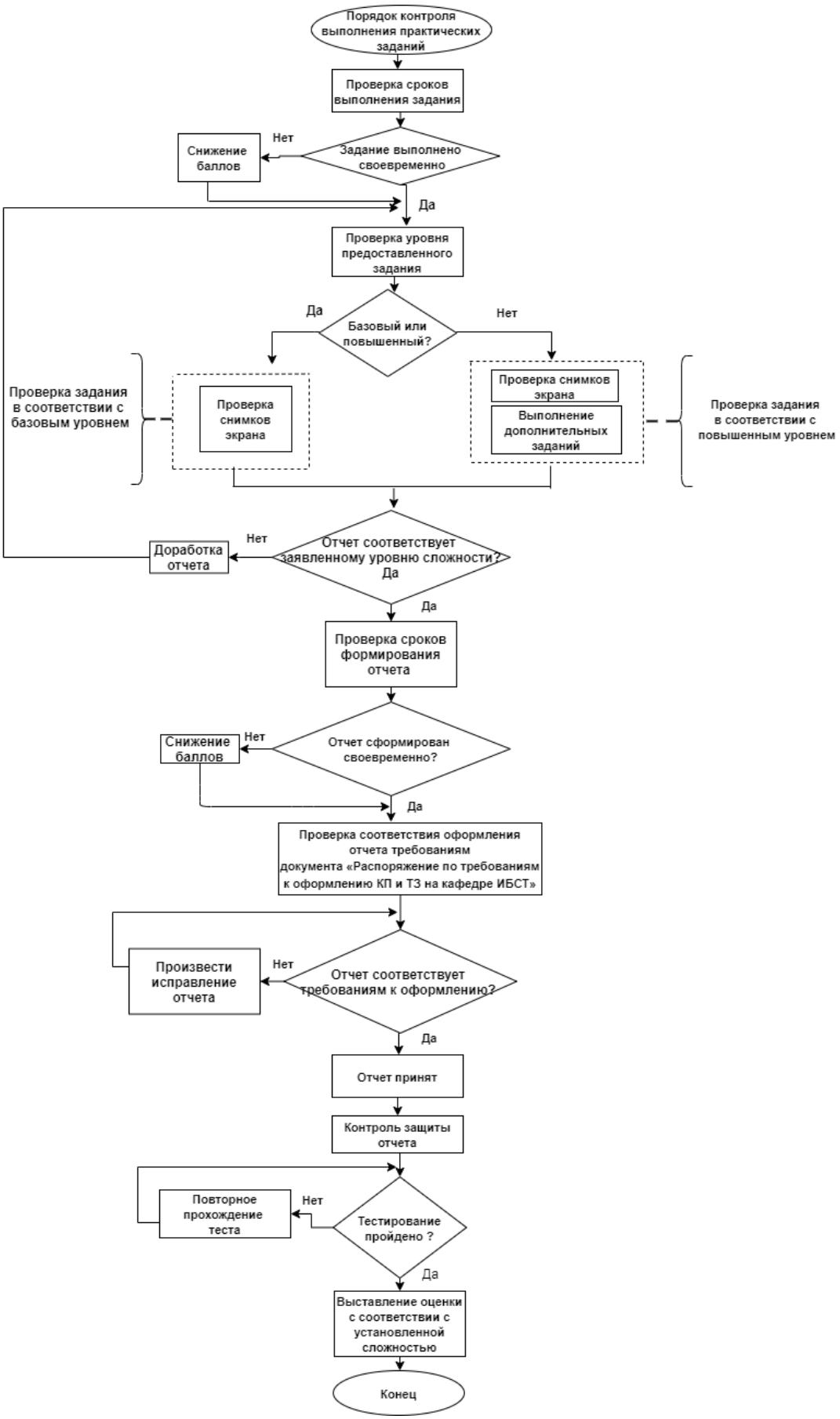


Рисунок Д.1 - Порядок контроля выполнения практических заданий

Приложение Ж

(обязательное)

Сценарии автоматизированного развертывания ВМ

Сценарий автоматизированного развертывания ВМ, которая является контроллером домена под управлением ОС Windows Server 2012 R2.

```
@echo off
rem *****************************************************
rem Universal script for VMs
rem *****************************************************
set VHDTYPE="immutable"
set VHDPATH="C:\\WS2012-DC.vdi"
set VMNAME=" WS2012-DC "
set OS_TYPE="Windows2012_64"
REM set OS_TYPE="Windows"
set MEMORY="2048"
set VIDEO="128"
set _ACPI="on"
set _IOAPIC="on"
set _PAE="on"
set _HWVIRTEX="on"
set _VTXVID="on"
set netadapter="Intel PRO/1000 MT Server (82540EM)"
set SHAREPATH="D:\share"
REM if == 0 -> not shared folders
set VBOXM="%programfiles%\Oracle\VirtualBox\vboxmanage"
%VBOXM% createvm --name %VMNAME% --ostype %OS_TYPE% --register
%VBOXM% storagectl %VMNAME% --add ide --controller PIIX4 --name
"PIIX4"
```

```
%VBOXM% storageattach %VMNAME% --storagectl PIIX4 --port 0 --device 0 --type hdd --medium %VHDPATH% --mtype %VHDTYPE%
%VBOXM% storageattach %VMNAME% --storagectl PIIX4 --port 0 --device 1 --type dvddrive --medium "emptydrive"
%VBOXM% modifyvm %VMNAME% --memory %MEMORY% --vram %VIDEO% --acpi %_ACPI% --ioapic %_IOAPIC% --pae %_PAE% --hwvirtex %_HWVIRTEX% --vtxvpid %_VTXVID% --audio none
%VBOXM% modifyvm %VMNAME% --usb on --usbehci on
%VBOXM% modifyvm %VMNAME% --clipboard bidirectional
%VBOXM% modifyvm %VMNAME% --nic1 intnet
if not %SHAREPATH%=="0" %VBOXM% sharedfolder add %VMNAME% --name share --hostpath %SHAREPATH%
@pause
```

Сценарий автоматизированного развертывания ВМ, являющейся локальным сервером виртуализации под управлением ОС Hyper-V Windows Server 2012 R2.

```
@echo off
rem ******************************************************
rem Universal script for VMs
rem ******************************************************
set VHDTYPE="immutable"
set VHDPATH="C:\\ HV2012-VS3.vdi"
set VMNAME=" HV2012-VS3"
set OS_TYPE="HyperVWindows2012_64"
REM set OS_TYPE="Windows"
set MEMORY="1024"
set VIDEO="128"
set _ACPI="on"
set _IOAPIC="on"
set _PAE="on"
```

```
set _HWVIRTEX="on"
set _VTXVID="on"
set netadapter="Intel PRO/1000 VT Desktop (82540EM)"
set SHAREPATH="D:\share"
REM if == 0 -> not shared folders
set VBOXM="%programfiles%\Oracle\VirtualBox\vboxmanage"
%VBOXM% createvm --name %VMNAME% --ostype %OS_TYPE% --register
%VBOXM% storagectl %VMNAME% --add ide --controller PIIX4 --name "PIIX4"
%VBOXM% storageattach %VMNAME% --storagectl PIIX4 --port 0 --device 0 --type hdd --medium %VHDPATH% --mtype %VHDTYPE%
%VBOXM% storageattach %VMNAME% --storagectl PIIX4 --port 0 --device 1 --type dvddrive --medium "emptydrive"
%VBOXM% modifyvm %VMNAME% --memory %MEMORY% --vram %VIDEO% --acpi %_ACPI% --ioapic %_IOAPIC% --pae %_PAE% --hwvirtex %_HWVIRTEX% --vtxvpid %_VTXVID% --audio none
%VBOXM% modifyvm %VMNAME% --usb on --usbehci on
%VBOXM% modifyvm %VMNAME% --clipboard bidirectional
%VBOXM% modifyvm %VMNAME% --nic1 intnet
if not %SHAREPATH%=="0" %VBOXM% sharedfolder add %VMNAME% --name share --hostpath %SHAREPATH%
@pause
```

Приложение И

(обязательное)

Протокол проверки на оригинальность

Протокол

Проверки на оригинальность в системе «Антиплагиат» отчета ВКР на тему «Практикум по построению и администрированию системы защиты среды виртуализации на основе механизмов безопасности ос Windows Server» студента Трушина Р.Н. специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализации «Защищенные автоматизированные системы».

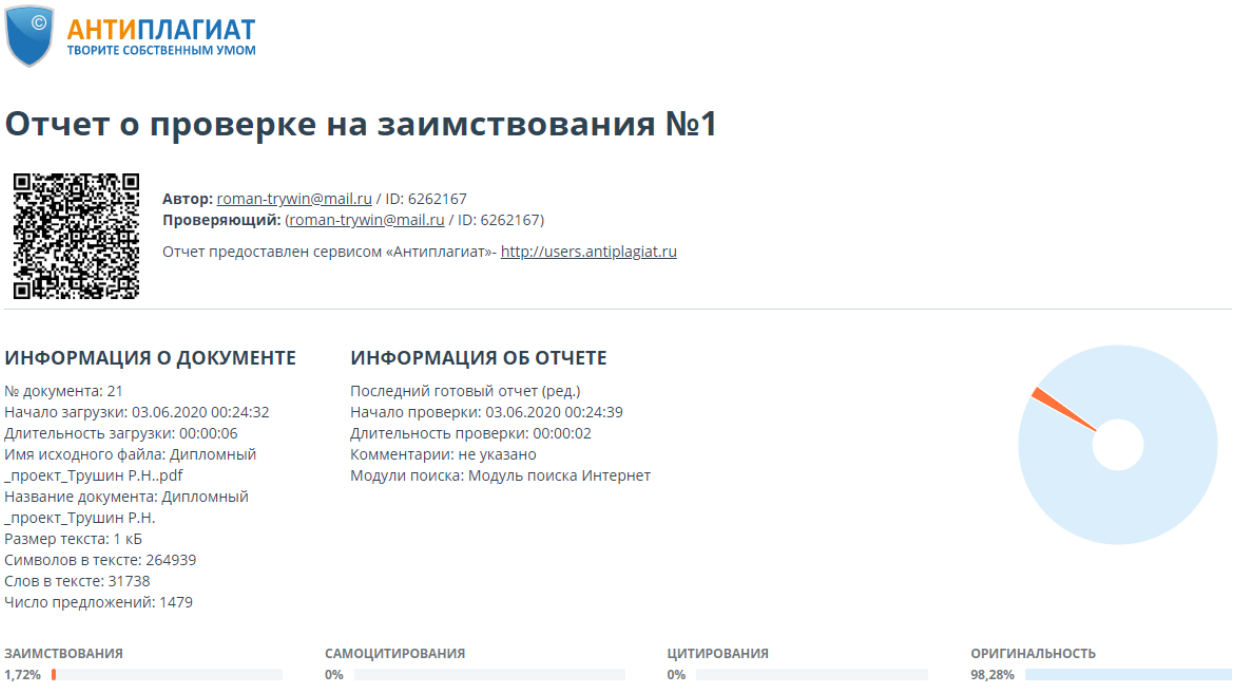


Рисунок И.1 - Протокол проверки на оригинальность