Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
_____ О.В. Фомичева
«26» _____ 2023г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по выполнению практических работ
по МДК.02.01 Администрирование сетевых операционных систем
ПМ.02 ОРГАНИЗАЦИЯ СЕТЕВОГО АДМИНИСТРИРОВАНИЯ ОПЕРАЦИОННЫХ СИСТЕМ

для специальности

09.02.06 Сетевое и системное администрирование

Санкт-Петербург
2023г.

Методические рекомендации рассмотрены на заседании методического совета СПб ГБПОУ «АУГСГиП»
Протокол № 2 от «22» 11 202 3 г.

Методические рекомендации одобрены на заседании цикловой комиссии информационных технологий
Протокол № 4 от «21» 11 202 3 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая тетрадь по выполнению практических работ предназначены для организации работы на практических занятиях по МДК.02.01 «Администрирование сетевых операционных систем», которая является важной составной частью в системе подготовки специалистов среднего профессионального образования по специальности 09.02.06 «Сетевое и системное администрирование».

Практические занятия являются неотъемлемым этапом изучения учебной дисциплины и проводятся с целью:

- формирования практических умений в соответствии с требованиями к уровню подготовки обучающихся, установленными рабочей программой учебной дисциплины;
- обобщения, систематизации, углубления, закрепления полученных теоретических знаний;
- готовности использовать теоретические знания на практике.

Практические занятия по МДК.02.01 «Администрирование сетевых операционных систем» способствуют формированию в дальнейшем при изучении профессиональных модулей, следующих общих и профессиональных компетенций:

ОК 1. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 2. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;

ОК 4. Эффективно взаимодействовать и работать в коллективе и команде;

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;

ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;

ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 2.1 Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.

ПК 2.2 Администрировать сетевые ресурсы в информационных системах.

В рабочей тетради предлагаются к выполнению практические работы, предусмотренные учебной рабочей программой по МДК.02.01 «Администрирование сетевых операционных систем».

При разработке содержания практических работ учитывался уровень сложности освоения студентами соответствующей темы, общих и профессиональных компетенций, на формирование которых направлена дисциплина.

Выполнение практических работ в рамках МДК.02.01 «Администрирование сетевых операционных систем» позволяет освоить комплекс работ по выполнению практических заданий по всем темам МДК.02.01 «Администрирование сетевых операционных систем».

Рабочая тетрадь по МДК.02.01 «Администрирование сетевых операционных систем» имеют практическую направленность и значимость. Формируемые в процессе практических занятий умения могут быть использованы студентами в будущей профессиональной деятельности.

Рабочая тетрадь предназначена для студентов колледжа, изучающих МДК.02.01 «Администрирование сетевых операционных систем».

Оценки за выполнение практических работ выставляются по пятибалльной системе. Оценки за практические работы являются обязательными текущими оценками по учебной дисциплине и выставляются в журнале теоретического обучения.

1. Перечень практических работ по МДК03.01 «Администрирование сетевых операционных систем»

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
Тема 2. Администрирование Windows Server	– администрировать локальные вычислительные сети; – принимать меры по устранению возможных сбоев;	ОК1-11 ПК 2.1 ПК 2.2.	Практическая работа № 1 Настройка и устранение неполадок службы DNS	2
			Практическая работа№ 2 Поддержка ADDS	2
			Практическая работа№ 3 Управление пользовательскими и служебными учетными записями	2
			Практическая работа№ 4 Внедрение инфраструктуры Групповых политик	2
			Практическая работа№ 5 Управление пользовательским рабочим столом через Групповую политику	2
			Практическая работа№ 6 Установка и настройка роли Сервер Сетевой политики	2
			Практическая работа№ 7 Применение защиты доступа к сети	2
			Практическая работа№ 8 Внедрение технологии DirectAccess с помощью мастера начальной настройки	2
			Практическая работа№ 9 Развертывание расширенной инфраструктуры DirectAccess	2
			Практическая работа№ 10 Внедрение VPN	2
			Практическая работа№ 11 Внедрение Web Application Proxy	2
			Практическая работа№ 12 Настройка Квот и файлового экранирования в FSRM	2
			Практическая работа№ 13 Применение DFS	2
			Практическая работа№ 14 Настройка шифрования и расширенного аудита	2
			Практическая работа№ 15 Использование службы развертывания Windows для развертывания WindowsServer	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
			Практическая работа№ 16 Внедрение управления обновлениями	2
			Практическая работа№ 17 Мониторинг WindowsServer	2
Тема 4. Администрирование Web-серверов	– устанавливать и настраивать web-сервер; – устанавливать и настраивать CMS; – обеспечивать защиту при подключении к информационно-телекоммуникационной сети "Интернет".	ОК1-11 ПК 2.1 ПК 2.2.	Практическая работа№ 18 Установка web-сервера Ubuntu	2
			Практическая работа№ 19 Установка web-сервера Arch Linux	2
			Практическая работа№ 20 Установка и настройка apache, php, mysql на web-сервер Ubuntu	2
			Практическая работа№ 21 Установка и настройка apache, php, mysql на web-сервер Arch Linux	2
			Практическая работа№ 22 Установка OpenSSL и создание сертификатов центра сертификации ОС Ubuntu	2
			Практическая работа№ 23 Установка OpenSSL и создание сертификатов центра сертификации ОС Arch Linux	2
			Практическая работа№ 24 Установка CMS wordpress на web-сервер	2
			Практическая работа№ 25 Создание web-ресурса на wordpress. Обеспечение доступа по HTTPS	2
			Практическая работа№ 26 Установка CMS joomla на web-сервер	2
			Практическая работа№ 27 Создание web-ресурса на joomla. Обеспечение доступа по HTTPS	2
			Практическая работа№ 28 Установка CMS Drupal на web-сервер	2
			Практическая работа№ 29 Создание web-ресурса на Drupal. Обеспечение доступа по HTTPS	2
			Практическая работа№ 30 Исследование безопасности сайтов на различных CMS	2
				60

,

2. Описание порядка выполнения практических работ

2.1. Практическая работа № 1
Настройка и устранение неполадок службы DNS

Задание:

Установка службы DNS
1 Зарегистрируйтесь на сервере server как Администратор.
2 Выполните команду Пуск -> Панель управления -» Установка и удаление программ. Выберите действие Установка компонентов Windows.
3 В появившемся окне Мастер компонентов Windows выберите Сетевые службы и нажмите на кнопку Состав.
4 В появившемся окне Сетевые службы установите флажок Domain Name Server (DNS) и нажмите ОК
5 Нажатием на кнопку Далее запустите установку службы DNS. Она не требует перезагрузки системы.
Настройка DNS
1 Выполните команду Пуск -» Панель управления -» Администрирование и выберите DNS. Откроется окно консоли с именем сервера server.
2 В левой части окна разверните объект сервера, щелкните правой кнопкой мыши по пункту Зоны прямого просмотра и выберите из контекстного меню Новая зона. Запустится Мастер создания зоны. На первом шаге нажмите кнопку Далее.
3 В диалоговом окне Тип зоны установите флажок Основная зона и нажмите Далее.
4 В поле Имя зоны введите study.local. Нажмите Далее.
5 В диалоговом окне Файл зоны установите флажок Создать новый файл и введите имя файла: study.local. dns. Нажмите Далее.
6 В окне Динамическое обновление установите флажок Разрешить любые динамические обновления и нажмите Далее.
7 Завершите установку нажатием кнопки Готово.
Настройка DNS на сервере “server”
1 В главном меню выберите Панель управления —» Сетевые подключения, а затем правой кнопкой мыши щелкните по пункту Подключение по локальной сети.
2 Из контекстного меню выберите Свойства.
3 В окне свойств подключения к локальной сети выберите пункт Протокол сети Интернет TCP/IP и нажмите на кнопку Свойства. Откроется окно свойств протокола TCP/IP.
4 В поле Предпочитаемый сервер DNS введите IP-адрес сервера server—192.168.2.51.
5 Последовательным нажатием на кнопку ОК закройте все окна.
6 В меню Пуск нажмите правой кнопкой мыши на меню Мой компьютер и выберите пункт Свойства.
7 В диалоговом окне Свойства системы откройте вкладку Имя компьютера и нажмите кнопку Изменить.
8 В диалоговом окне смены имени компьютера нажмите кнопку Дополнительно.
9 В диалоговом окне DNS-суффикс и NetBIOS-имя компьютера введите в поле Предпочитаемый DNS-суффикс имя зоны study.local. Нажатием ОК закройте окно.
10 Вы увидите в диалоговом окне Смена имени компьютера в поле Полное имя компьютера server.study, local —имя, состоящее из имени узла и суффикса DNS. Это имя должно быть уникальным в пределах сети. Диалоговое окно закройте нажатием ОК. После этого необходимо перезагрузить компьютер.
11 После перезагрузки компьютера снова откройте консоль DNS и в левой части окна выберите зону study.local. В правой части окна обратите внимание на созданный объект А (хост) сервера server

Настройка DNS на рабочей станции
1 Зарегистрируйтесь на компьютере pc1 как Администратор.
2 В главном меню выберите Панель управления -» Сетевые подключения, а затем правой кнопкой мыши щелкните по пункту Подключение по локальной сети.
3 Из контекстного меню выберите Свойства.
4 В окне Подключение по локальной сети — свойства выберите Протокол сети Интернет TCP/IP, нажмите на кнопку Свойства.
5 В поле Предпочитаемый DNS-сервер введите адрес сервера server —192.168.2.51. Затем нажмите ОК. Диалоговое окно свойств подключения закройте нажатием кнопки Закрыть.
6 В меню Пуск нажмите правой кнопкой мыши на меню Мой компьютер и выберите пункт Свойства.
7 В диалоговом окне Свойства системы откройте вкладку Имя компьютера и нажмите кнопку Изменить.
8 В диалоговом окне смены имени компьютера нажмите кнопку Дополнительно.
9 В диалоговом окне DNS-суффикс и NetBIOS-имя компьютера введите в поле Предпочитаемый DNS-суффикс имя зоны study.local. Нажатием ОК закройте окно.

2.2. Практическая работа № 2
Поддержка ADDS

Задание:
1. Настройка имени сервера и статического IP-адреса
   1. Откройте **Пуск > Компьютер (пр. кнопкой мыши) > Свойства** (Рис.1).

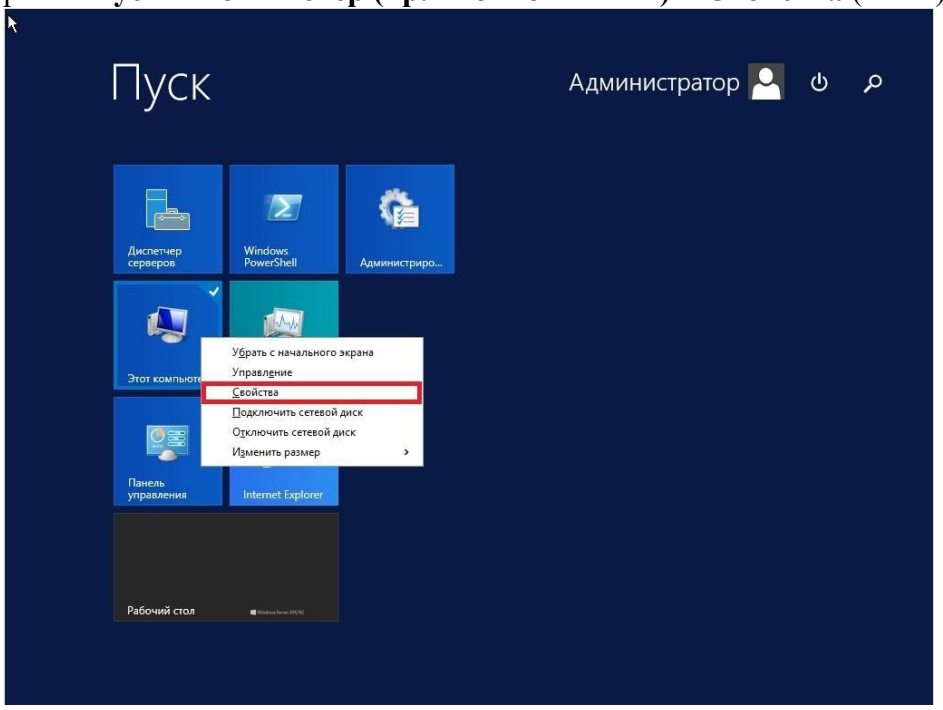


Рис. 12

2. В открывшемся окне выберите **Изменить параметры**.

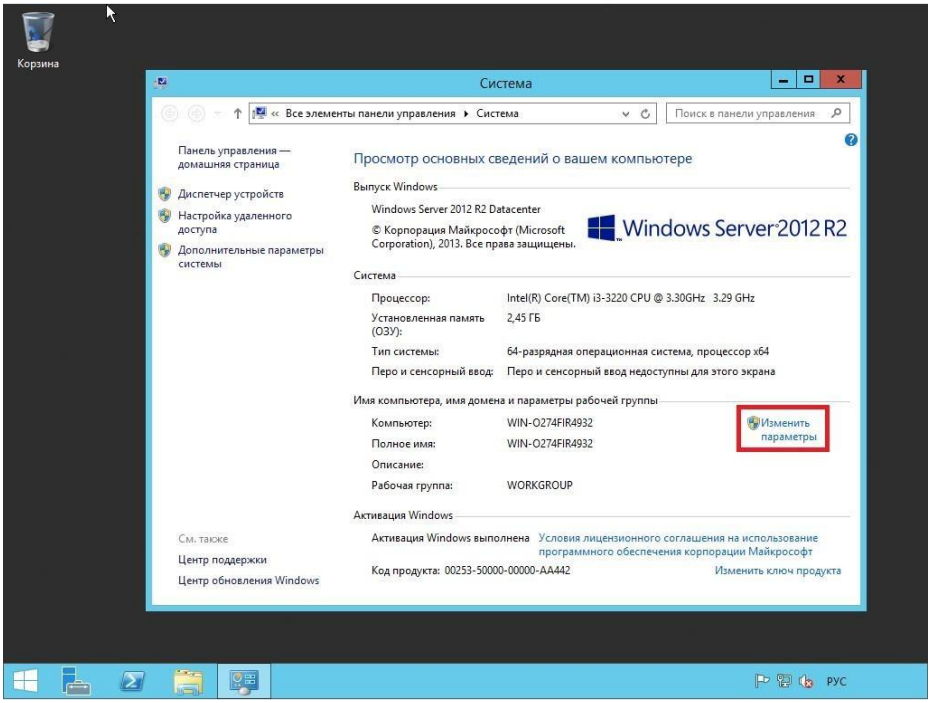


Рис. 13

3. В **Свойствах системы** выберите вкладку **Имя компьютера** и нажмите **Изменить…** . В появившемся окне укажите новое имя сервера в поле Имя компьютера (*прим. в данном руководстве это SERVER2012R2*), затем нажмите **ОК**.

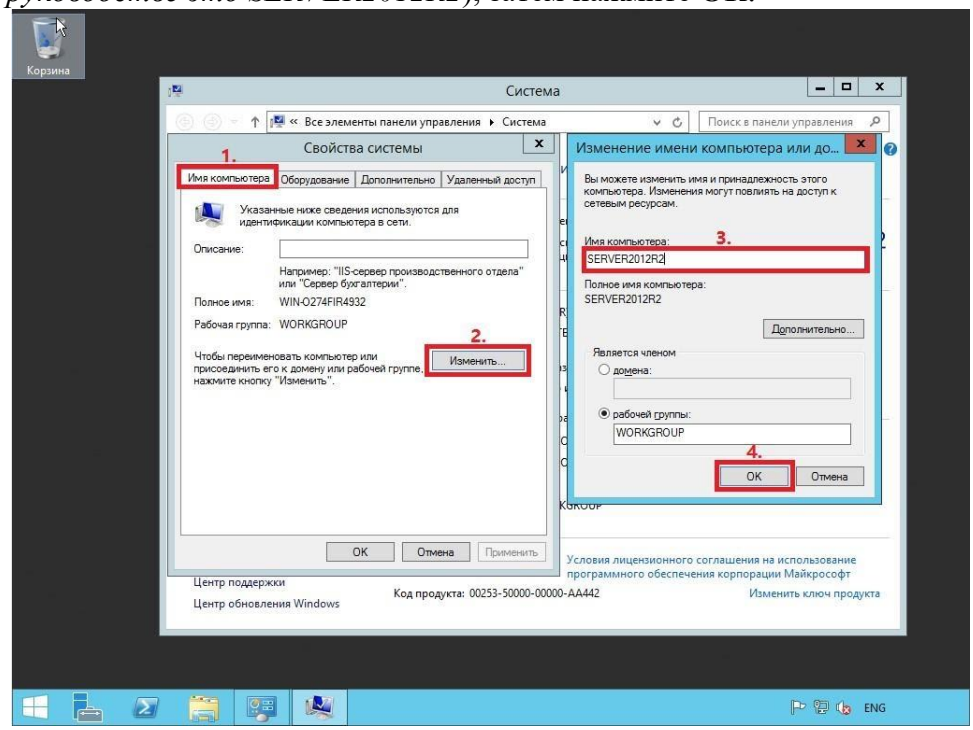


Рис. 14

4. Система предупредит о том, что для применения новых настроек необходимо перезагрузить сервер. Нажмите кнопку **ОК**

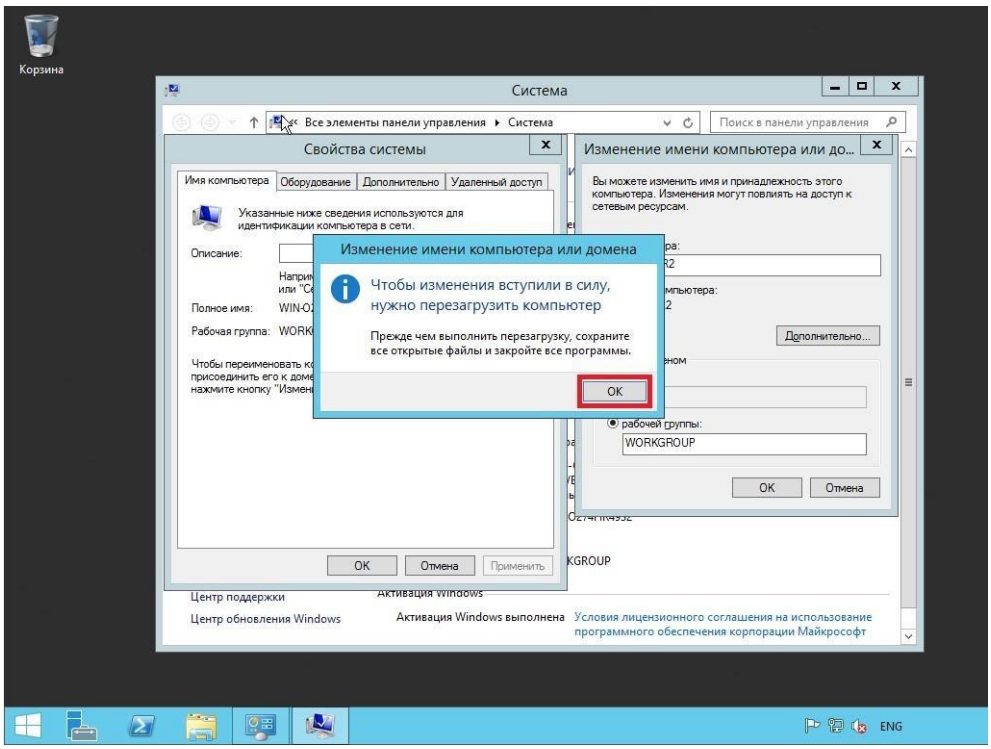
5. 

Рис. 15

6. После перезагрузки, в правом нижнем углу кликните (пр. кнопкой мыши) на иконке сетевого соединения. В открывшемся меню выберите **Центр управления сетями и общим доступом**

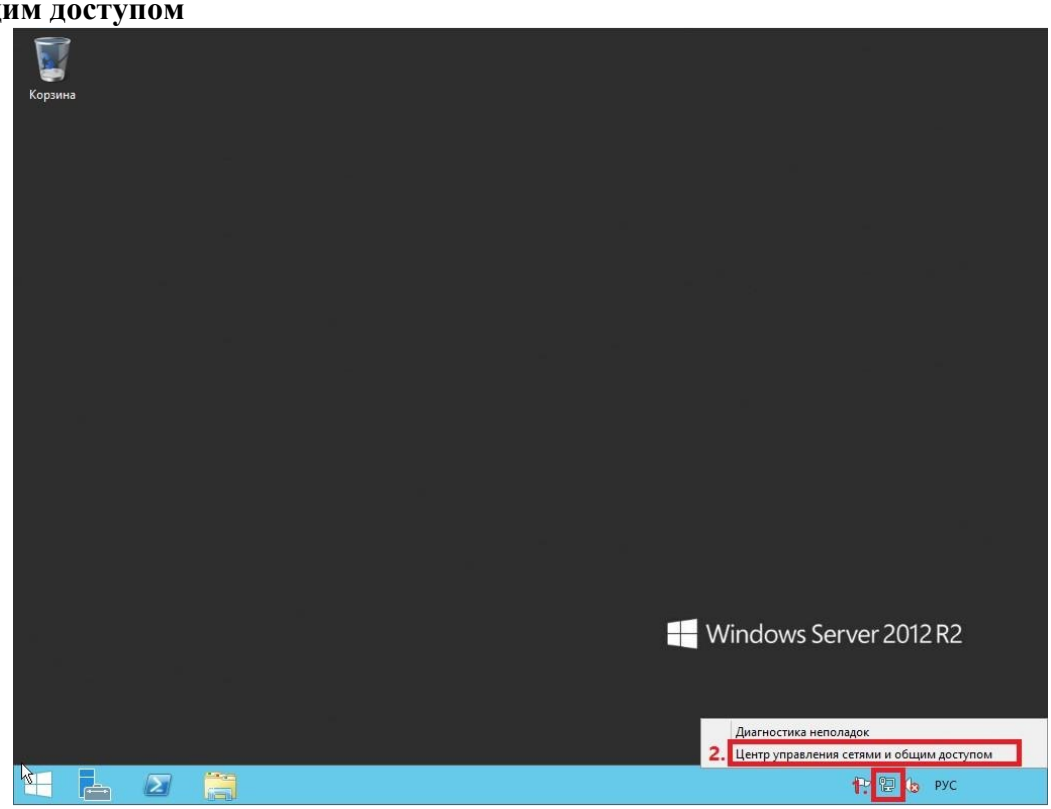


Рис. 16

7. В открывшемся окне выберите **Изменение параметров адаптера**

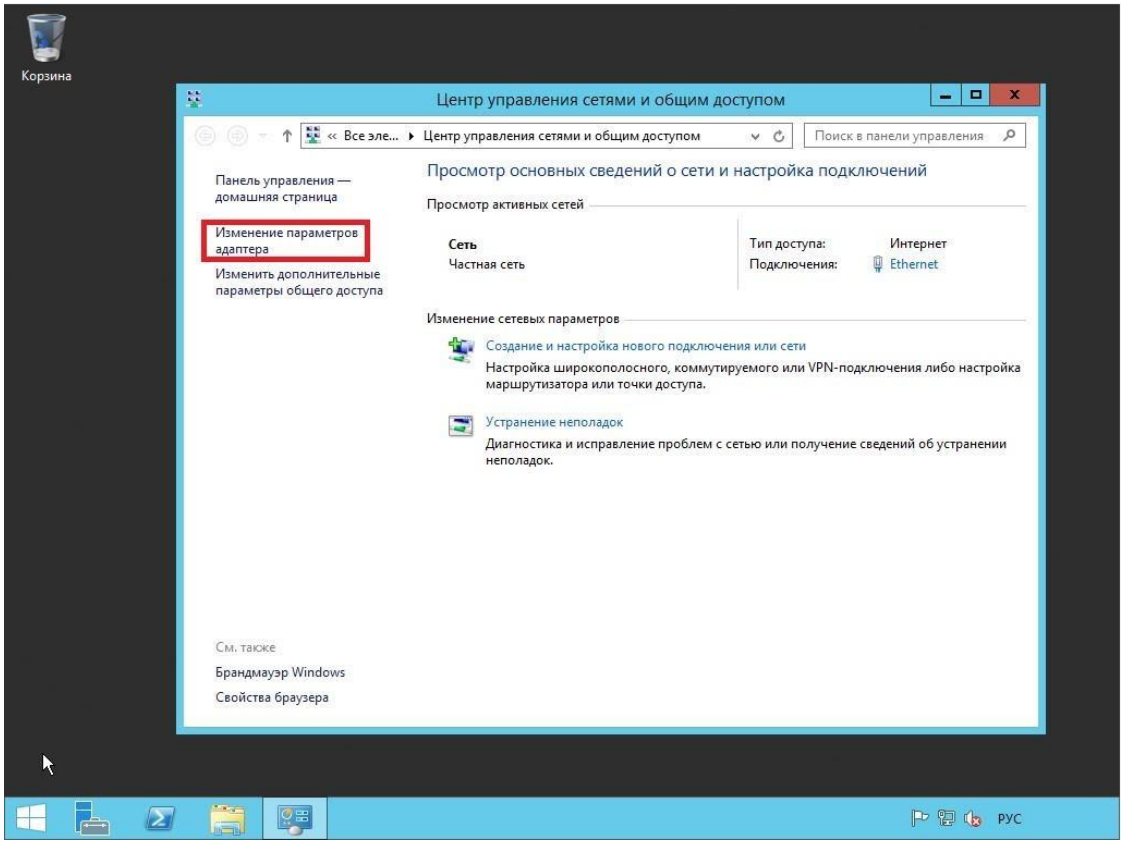


Рис. 17

8. В открывшемся окне Сетевые подключения нажмите правой кнопкой мыши на сетевом подключении и выберите пункт **Свойства**. В появившемся окне выделите **Протокол Интернета версии 4 (TCP/IPv4)** и нажмите **Свойства**

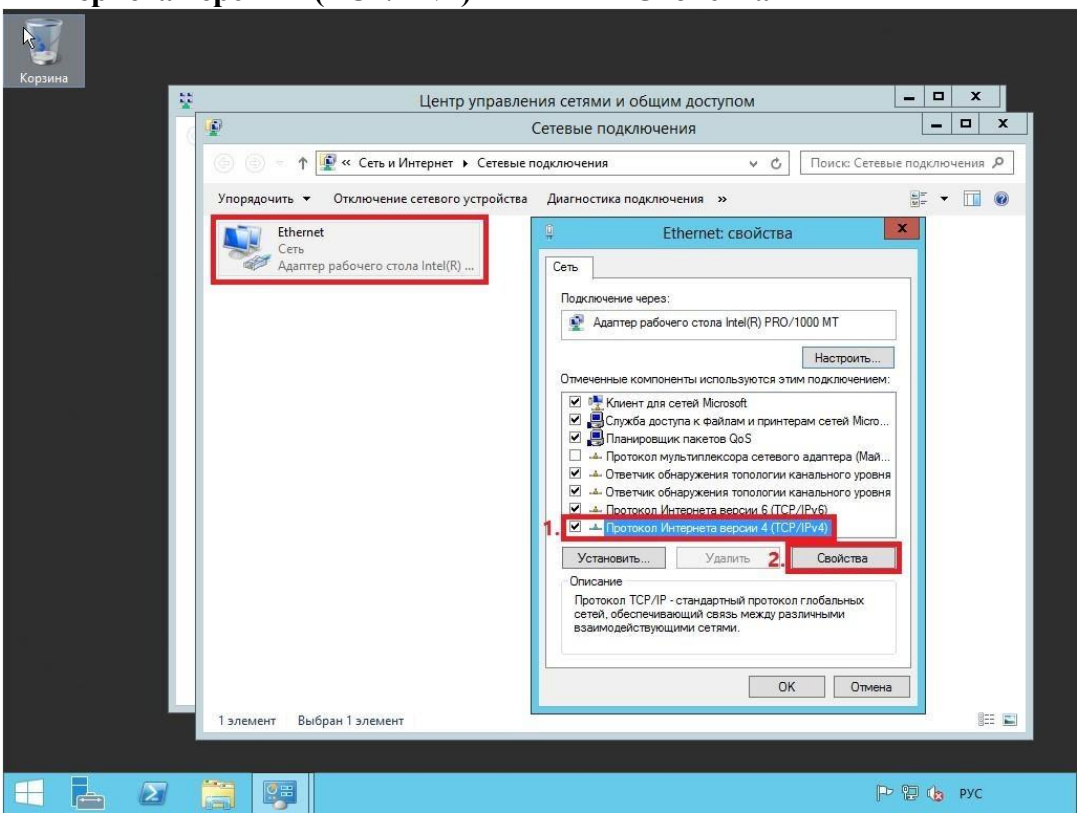


Рис. 18

9. В свойствах, на вкладке Общие выберите пункт **Использовать следующий IP-адрес**. В соответствующие поля введите **свободный IP-адрес**, **маску подсети** и **основ-**

ной шлюз. Затем выберите пункт **Использовать следующие адреса DNS-серверов**. В поле **предпочитаемый DNScервер** введите **IP-адрес сервера**, после чего нажмите **ОК**.

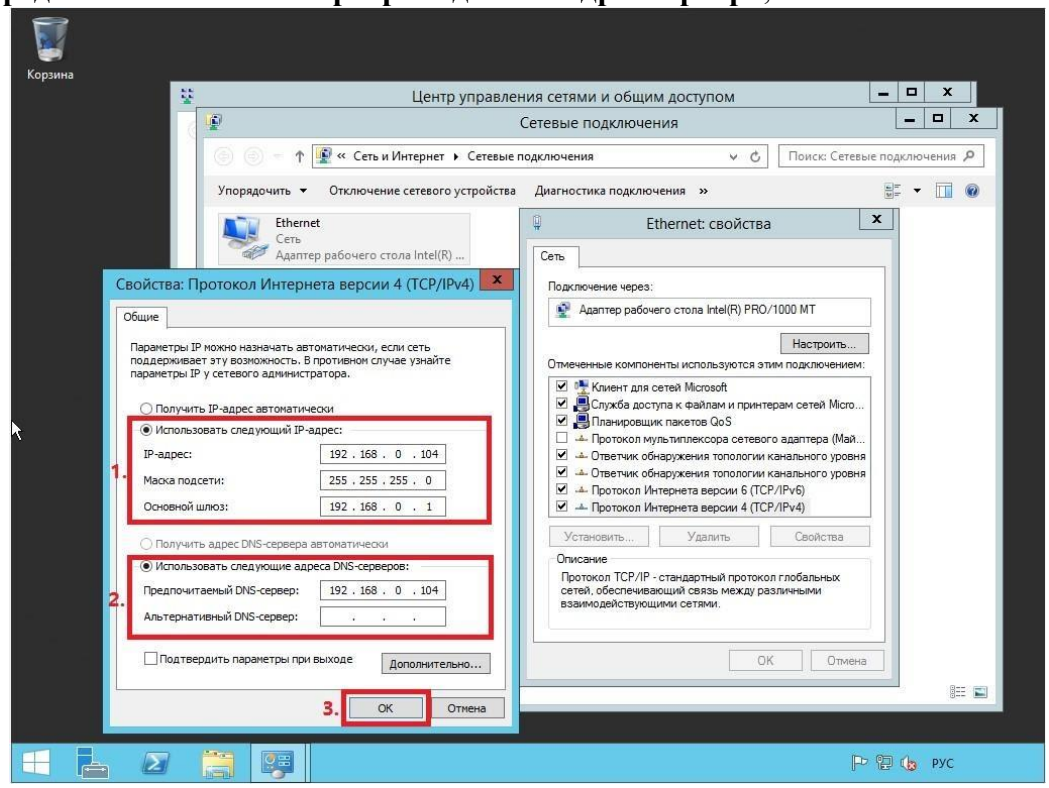


Рис. 19

Установка роли Active Directory Domain Services

1. Откройте окно диспетчера сервера и выберите пункт **Добавить роли и компоненты** (Рис.9).

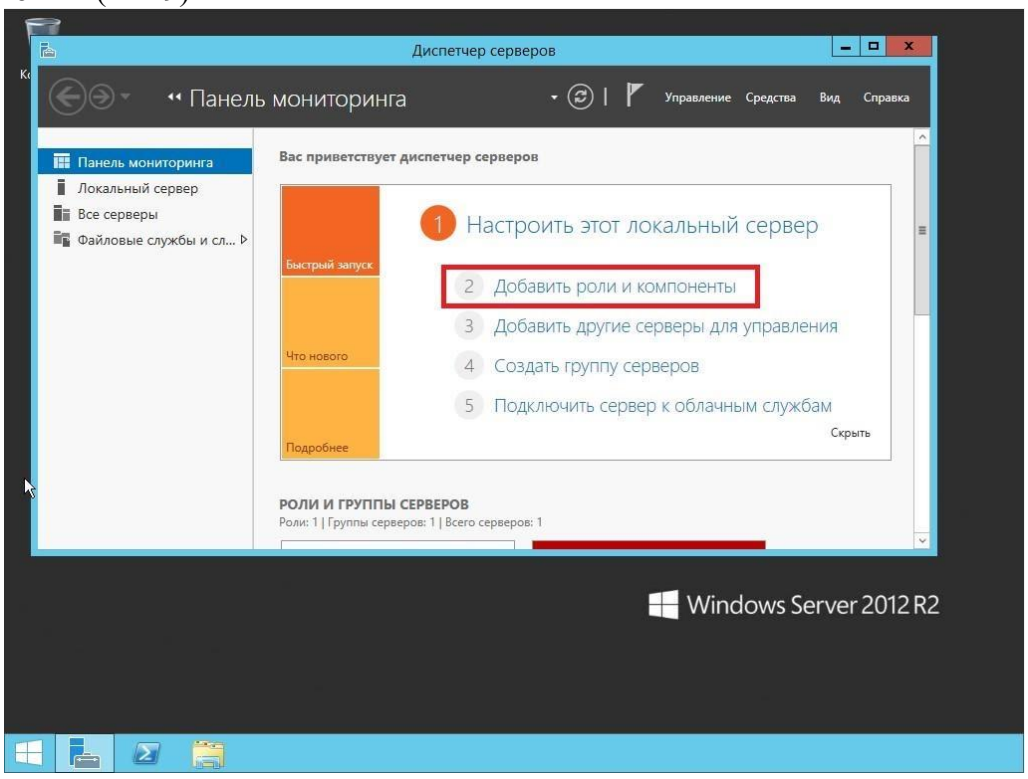


Рис. 20

2. В появившемся окне нажмите **Далее**

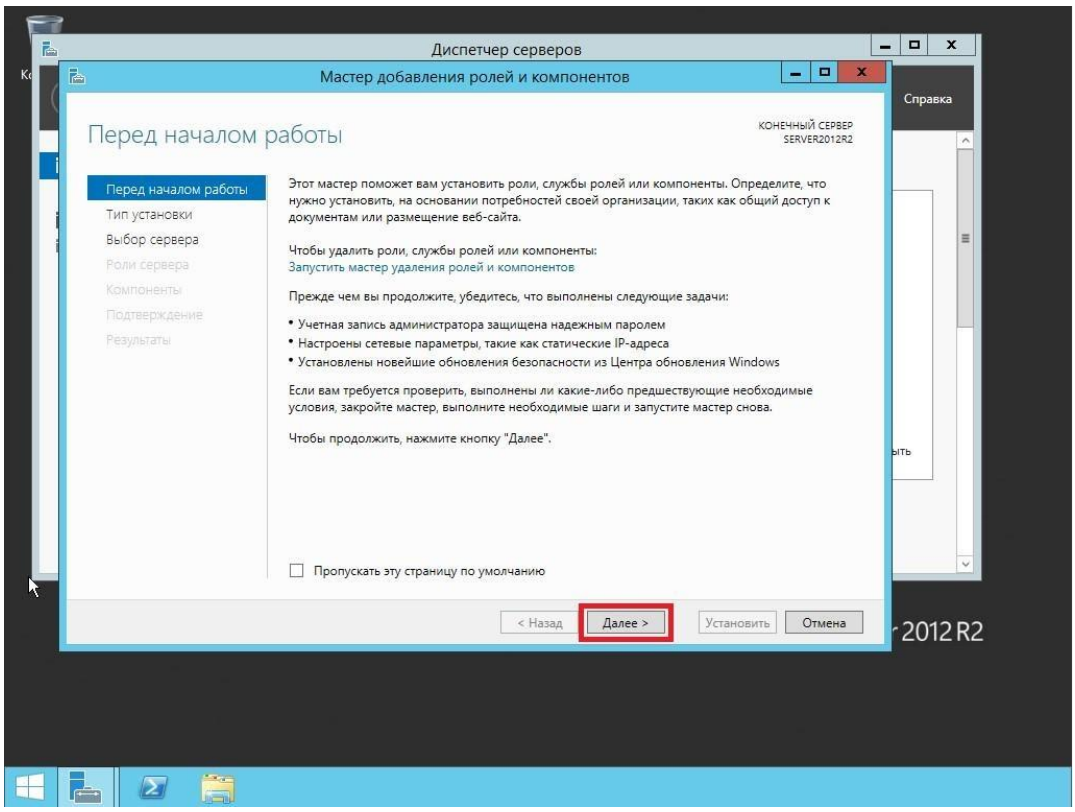


Рис. 21

3. Выберите пункт **Установка ролей и компонентов**, затем нажмите **Далее**

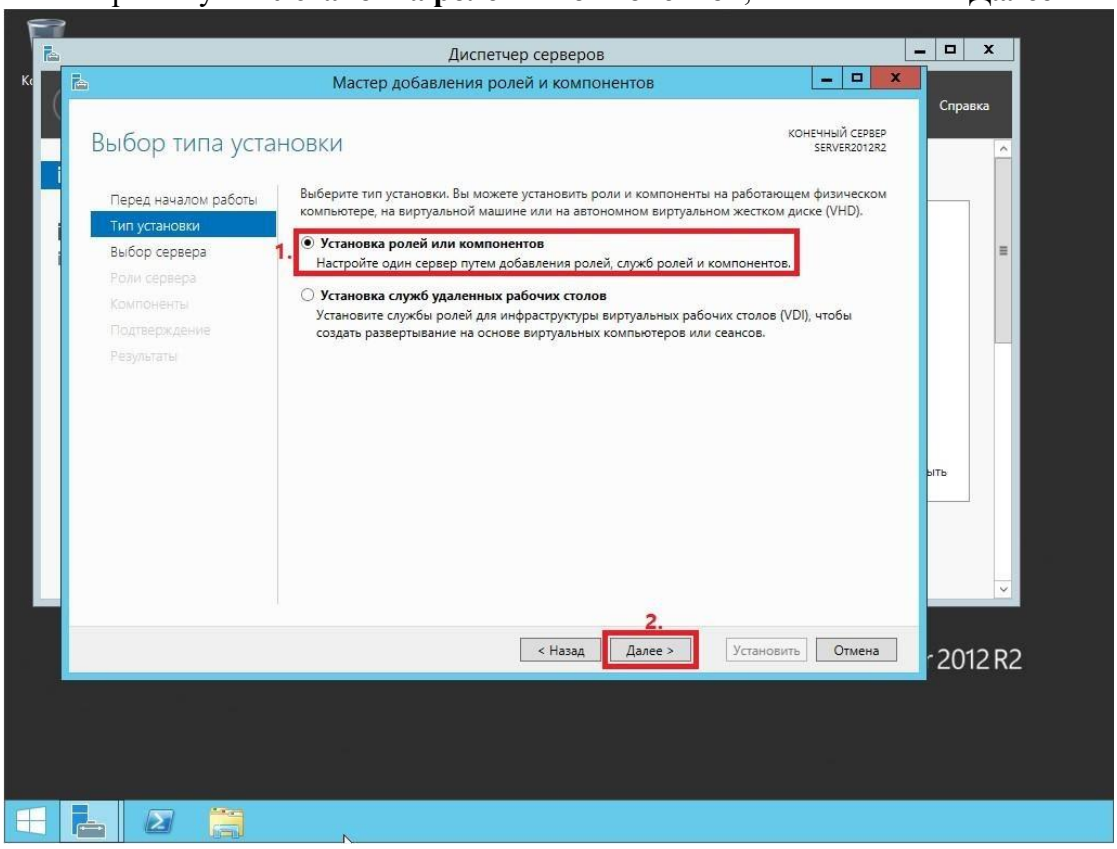


Рис. 22

4. Выберите сервер, на который будет производиться установка роли, затем нажмите **Далее**

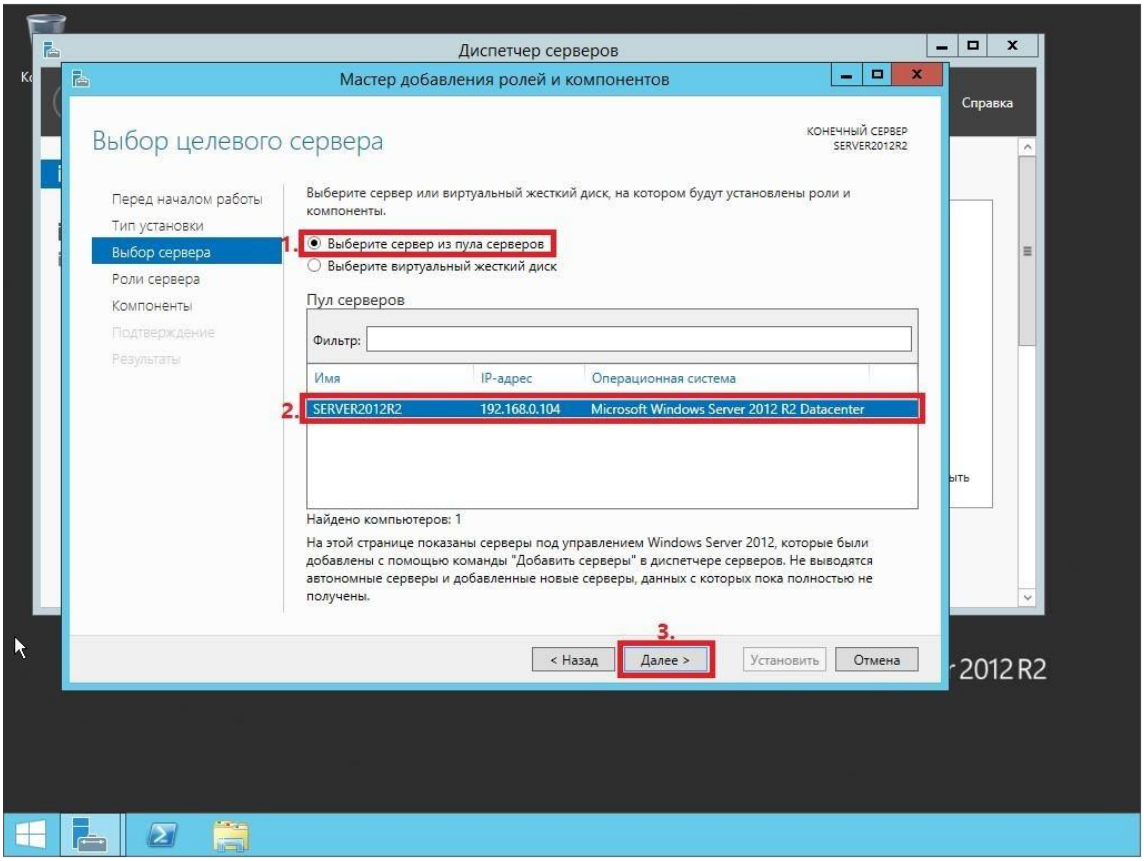


Рис. 23

5. Выберите роль **Доменные службы Active Directory**, на следующем этапе Мастер установки ролей предупредит, что для установки роли Доменные службы Active Directory нужно установить несколько компонентов. Нажмите **Добавить компоненты**

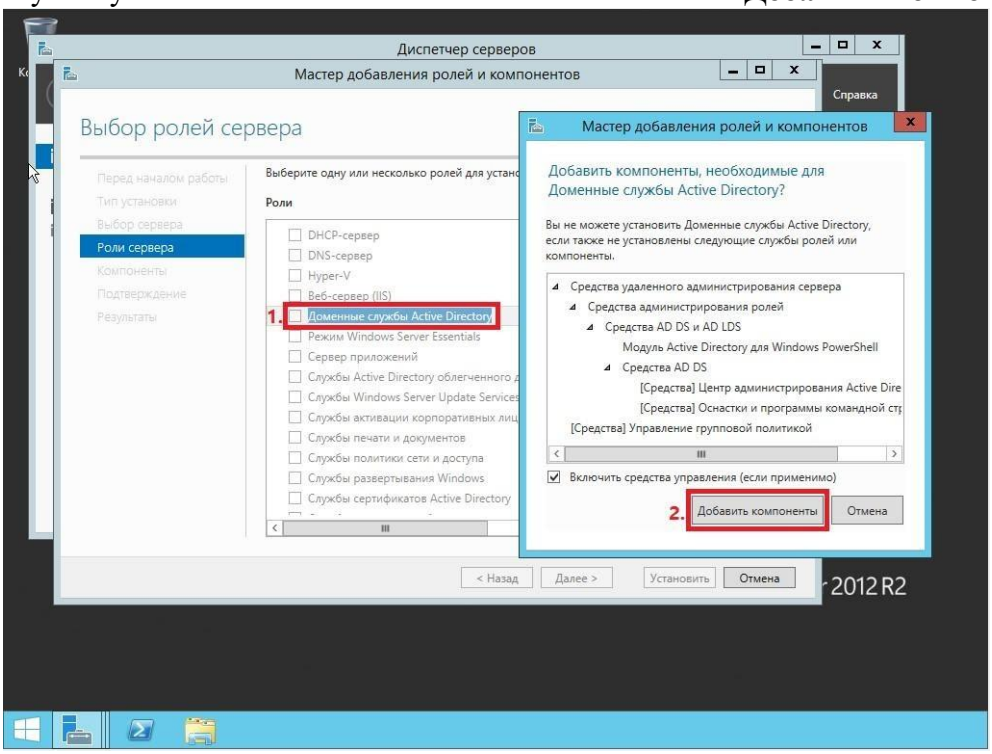


Рис. 24

6. Убедитесь, что после установки необходимых компонентов напротив **Доменные службы Active Directory** стоит галочка, затем нажмите **Далее**

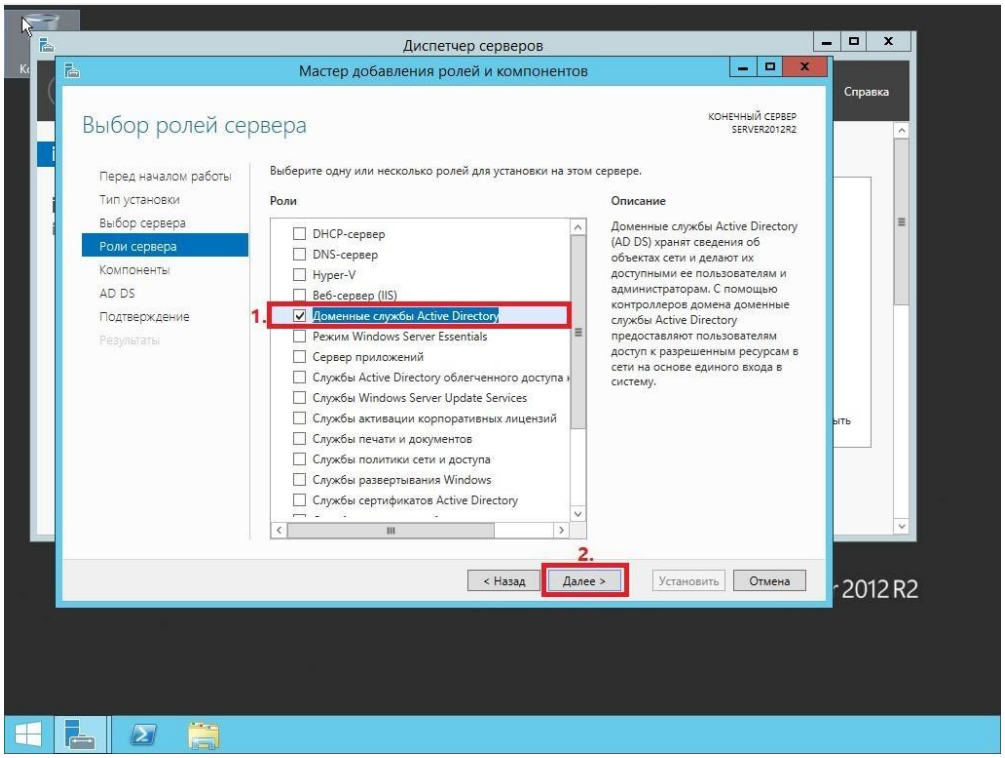


Рис. 25

7. На этапе добавления компонентов оставьте все значения по умолчанию и нажмите **Далее**

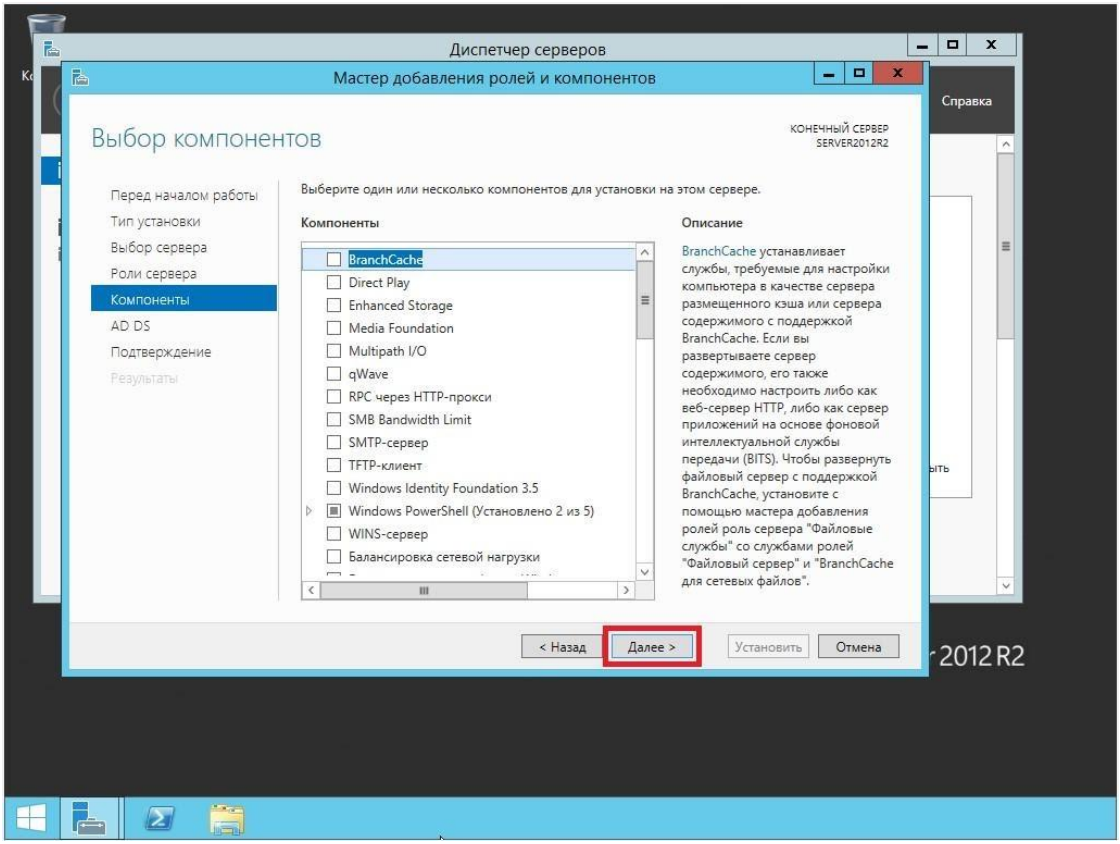


Рис. 26

8. Ознакомьтесь с дополнительной информацией касательно Доменных служб Active Directory, затем нажмите **Далее**

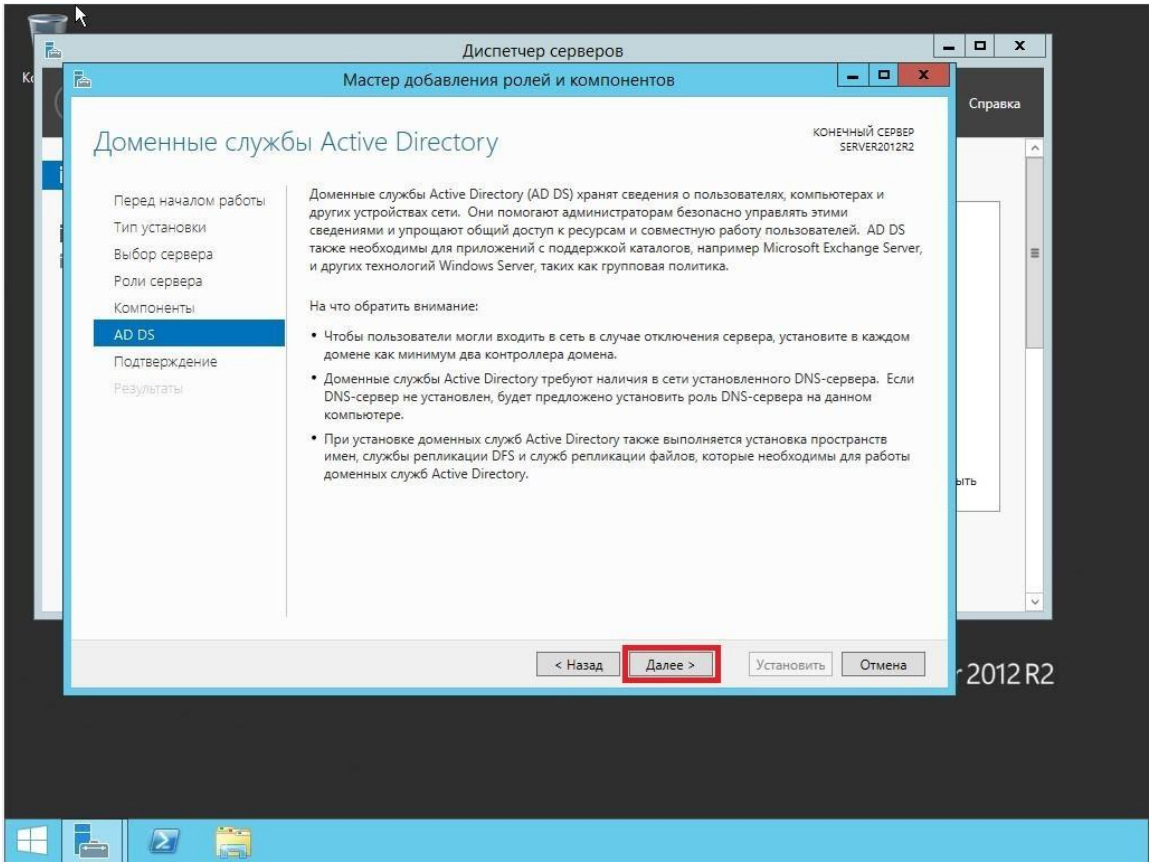


Рис. 27

9. Для начала установки роли нажмите **Установить**

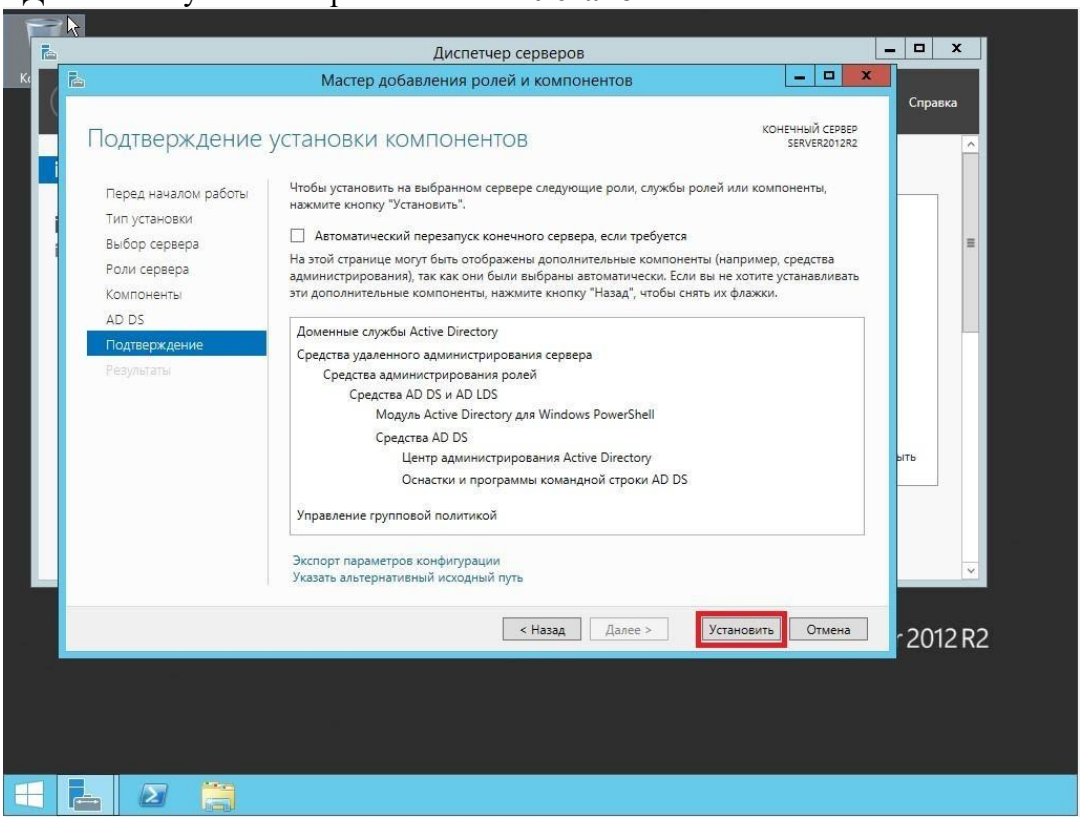


Рис. 28

10. После окончания установки нажмите **Повысить роль этого сервера до уровня контроллера домена**

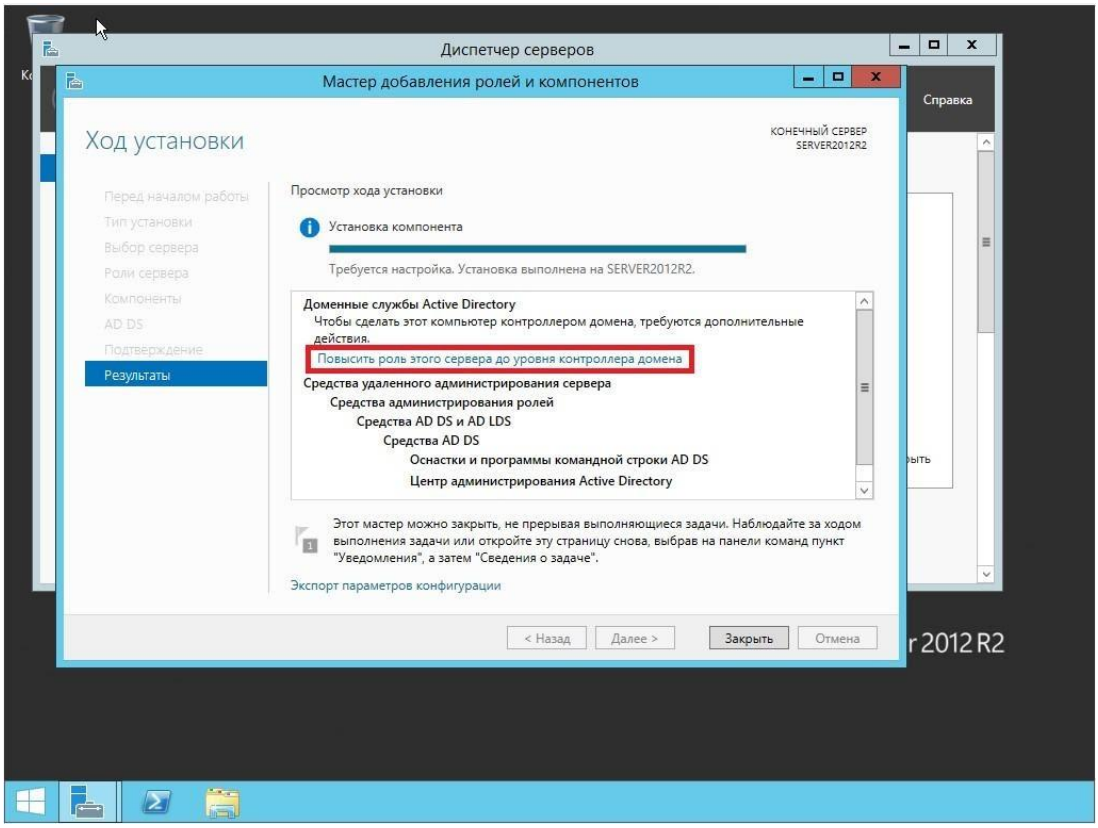


Рис. 29

11. Выберите пункт **Добавить новый лес**, затем в поле **Имя корневого домена** введите имя домена (*прим. в данном руководстве это example.local, Вы можете выбрать любое другое*), затем нажмите **Далее**

ВАЖНО! Домен вида .local или аналогичный можно использовать в качестве тестового, однако, он имеет ряд недостатков, а именно: 1) Вы никак не сможете подтвердить владение им для получения публичного SSL-сертификата; 2) Такое имя невозможно использовать из внешней сети; 3) Данный способ именования вступает в противоречие с глобальным DNS, так как не гарантирует его уникальность что приводит к потенциальным коллизиям.

Рекомендуется создавать согласованное пространство имен. Например имея домен wbsh.ru (который использует сайт), домен Active Directory делать суб-доменом, например: server. wbsh.ru. Либо использовать разные домены, например wbsh.ru — для сайта, а wbsh.net — для Active Directory.

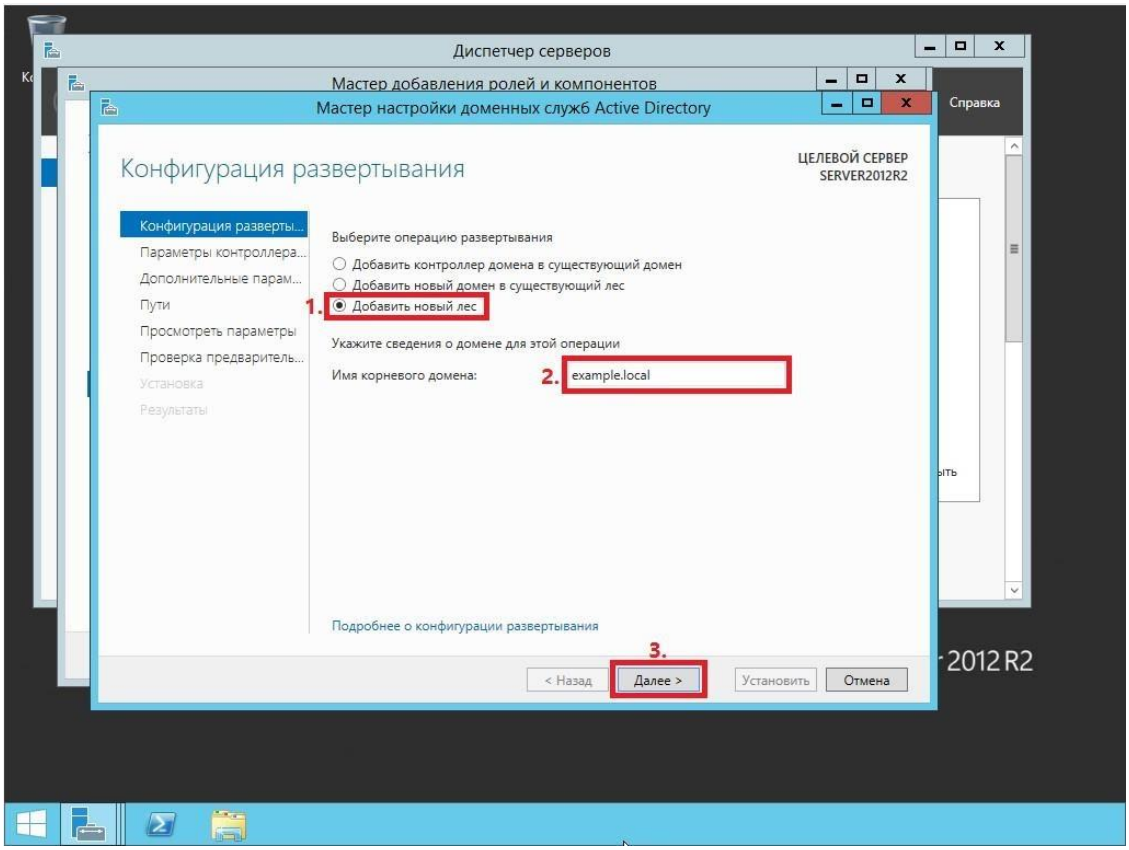


Рис. 30

12. На следующем шаге предлагается выбрать функциональный уровень нового леса и корневого домена. Если вы добавляете новый лес и планируете в дальнейшем использовать серверы на базе операционной системы Windows Server 2012 R2, то можете не менять функциональный уровень леса и корневого домена. Установите галочку напротив **DNS-сервер**, придумайте и введите пароль для режима восстановления служб каталогов в соответствующие поля, затем нажмите **Далее**

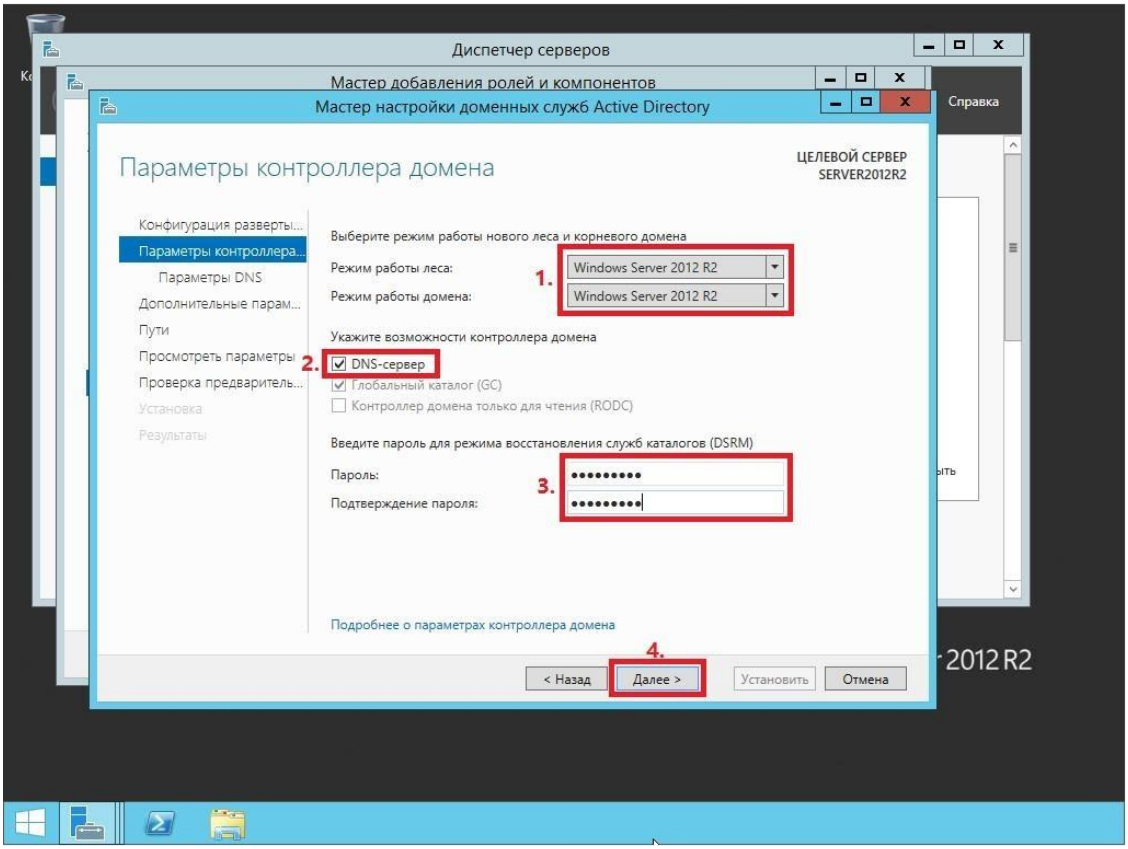


Рис. 31

13. Оставьте значение NetBIOS по умолчанию и нажмите **Далее**

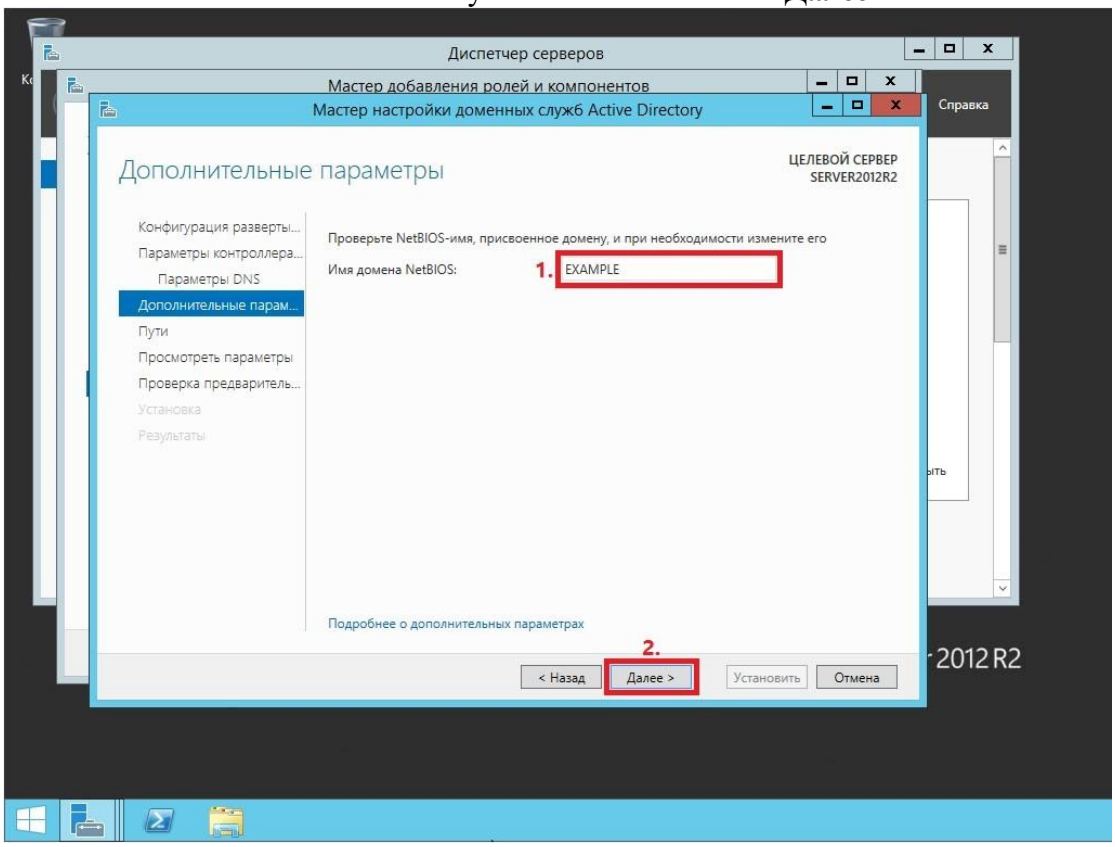


Рис. 32

14. Оставьте настройки по умолчанию и нажмите **Далее**

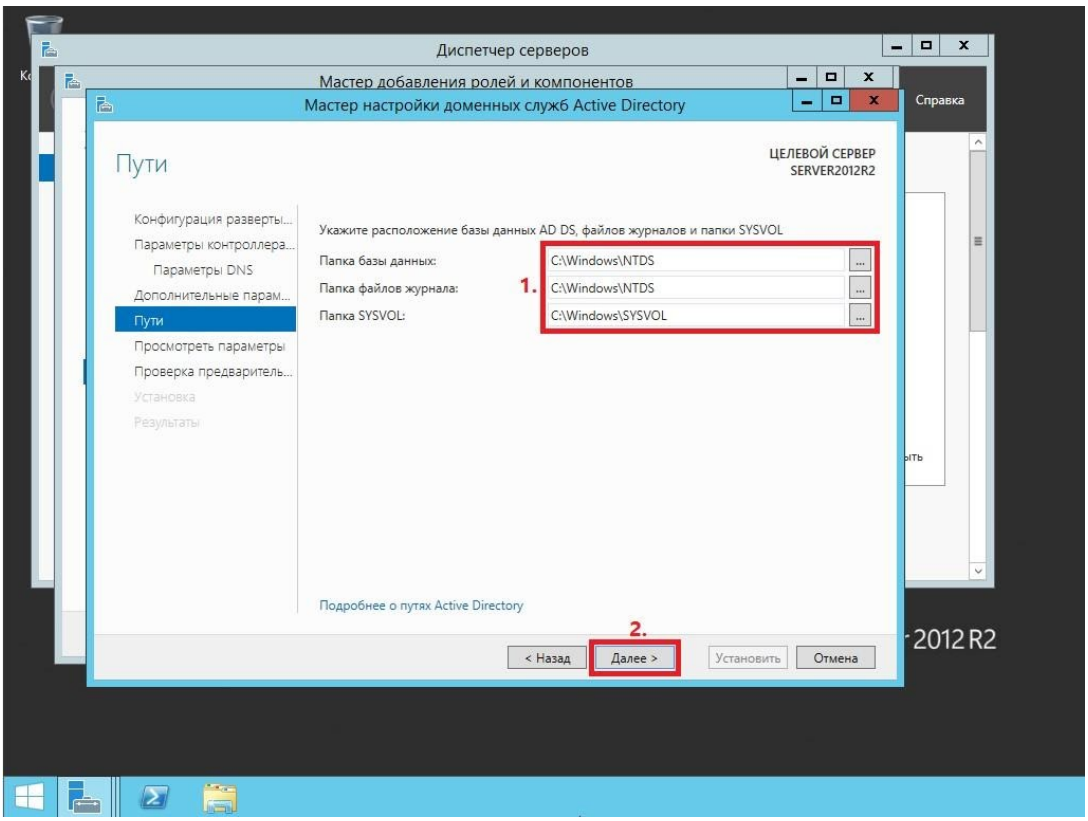


Рис. 33

15. В окне со сводной информацией по настройке сервера нажмите **Далее**

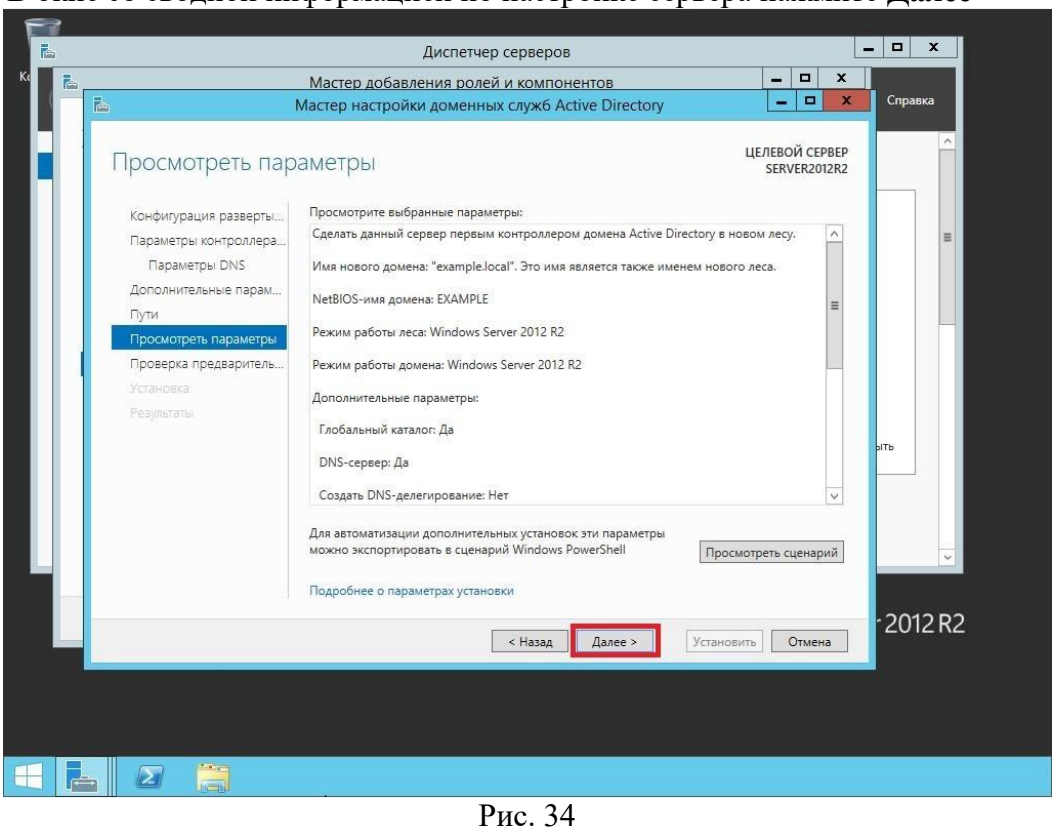


Рис. 34

16. Далее Мастер настройки доменных служб Active Directory проверит все ли предварительные требования соблюдены и выведет отчет. Нажмите **Установить** (Рис.24).

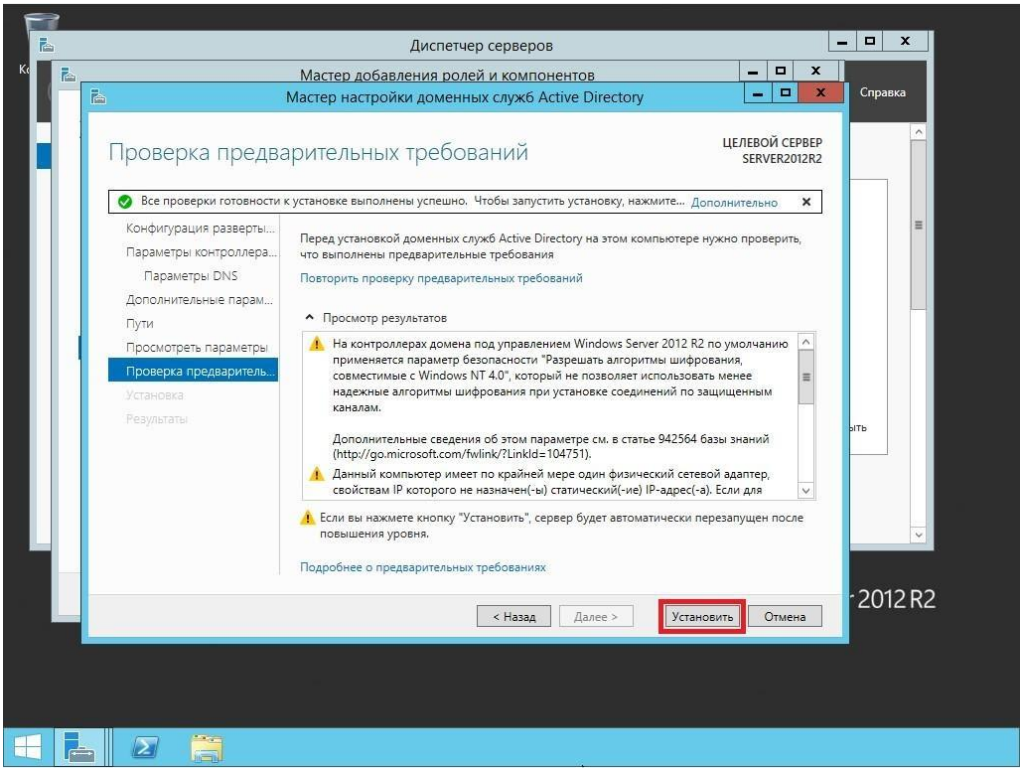


Рис. 35

17. После того как роль вашего сервера будет повышена до уровня контроллера домена, сервер автоматически перезагрузится. Перед тем как сервер начнет перезагружаться вы увидите предупреждение

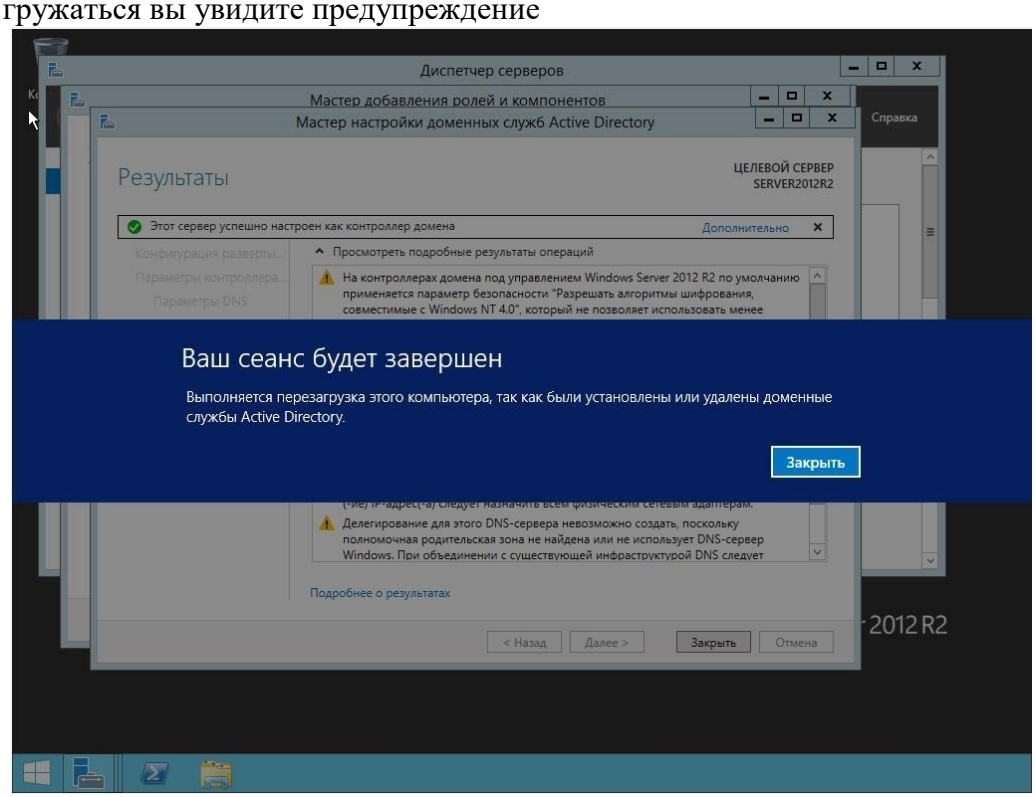


Рис. 36

18. После повышения роли сервера до уровня контроллера домена и перезагрузки — зайдите в систему под учетной записью с правами администратора домена

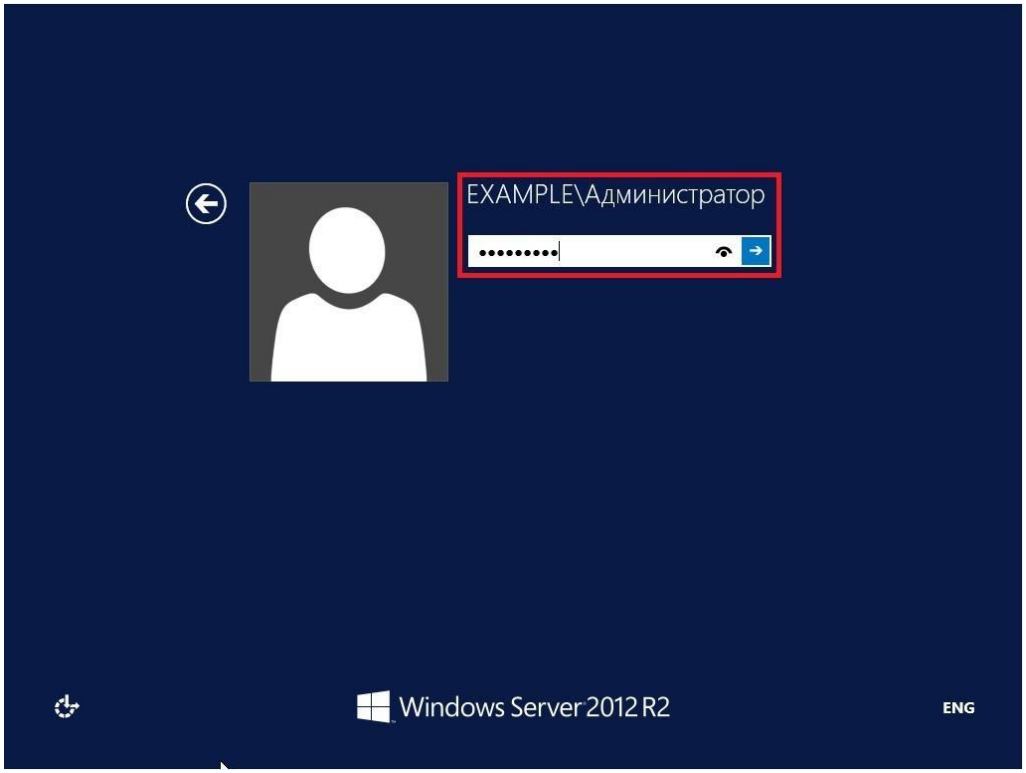


Рис. 37

Установка контроллера домена Active Directory в Windows Server 2012 R2 завершена!

Сделайте скриншоты (фотографии) процесса установки контроллера домена Active Directory и вставьте в отчёт.

2.3. Практическая работа № 3
Управление пользовательскими и служебными учетными записями

Задание:

Настройка политики паролей учетных записей в Active Directory

1. Что бы изменить политику паролей для пользователей, находящихся в домене, заходим в **«Диспетчер серверов»** далее в верхнем меню жмем **"Средства"** и переходим в раздел **"Управления групповой политикой"**

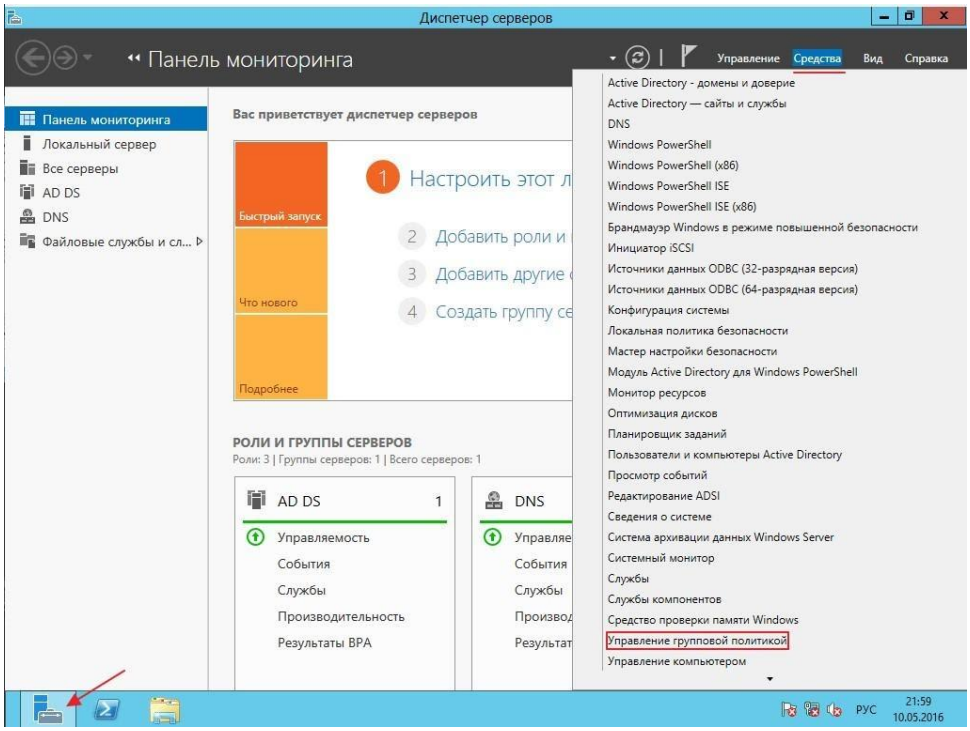


Рис. 38

2. Для того что бы изменить политику паролей необходимо изменить политику по умолчанию домена (Default Domain Police) для этого нажмите ПКМ по данной политике и нажмите на пункт **"Изменить"**

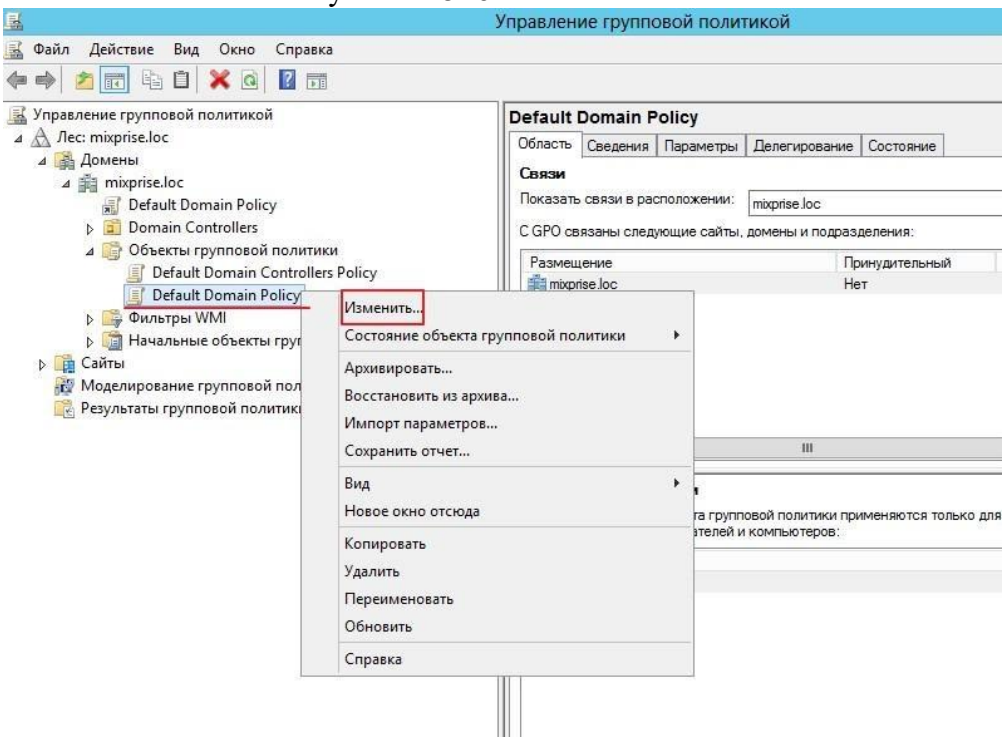


Рис. 39

3. В открывшимся окне открылся редактор, теперь необходимо найти где же изменять саму политику паролей, редактирование происходит в разделе **"Конфигурации компьютера"** далее разворачиваем папку **"Конфигурация Windows"** дальше открываем **"Параметры безопасности и политики учетных записей"**

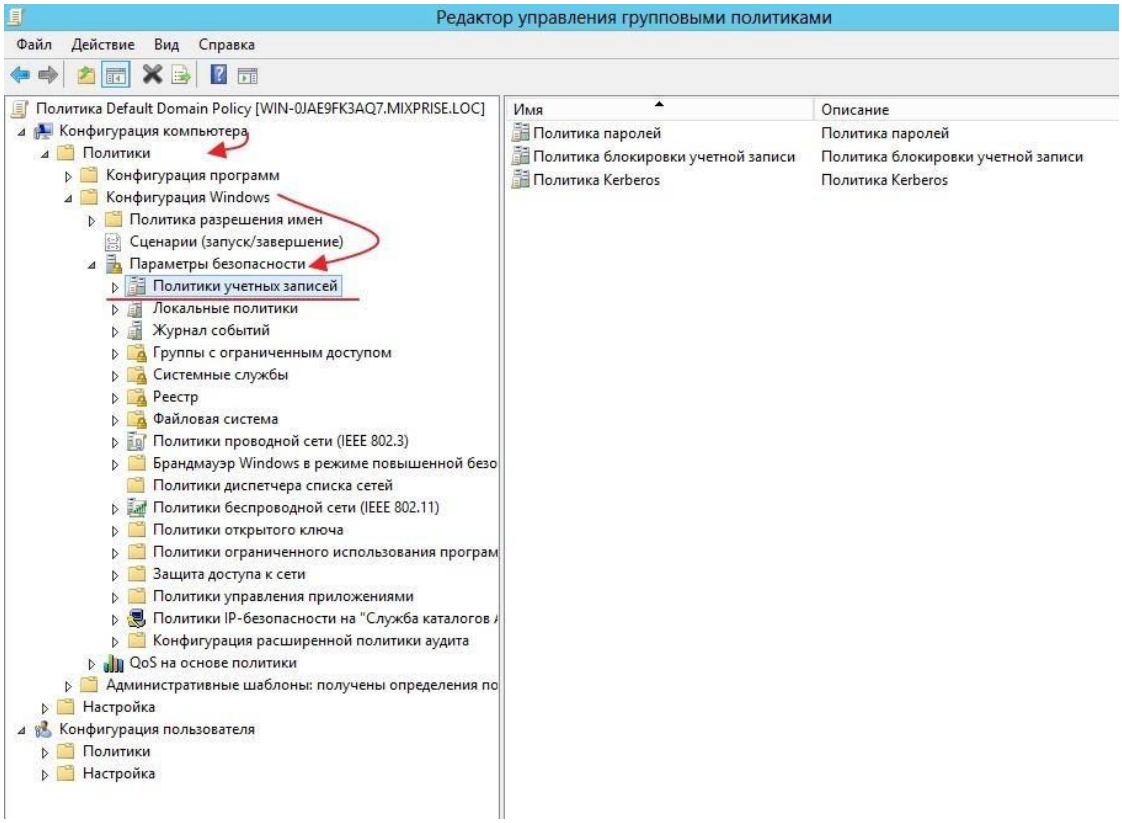


Рис. 40

Начнем настройку с первого раздела под названием **"Политика паролей"** открываем его

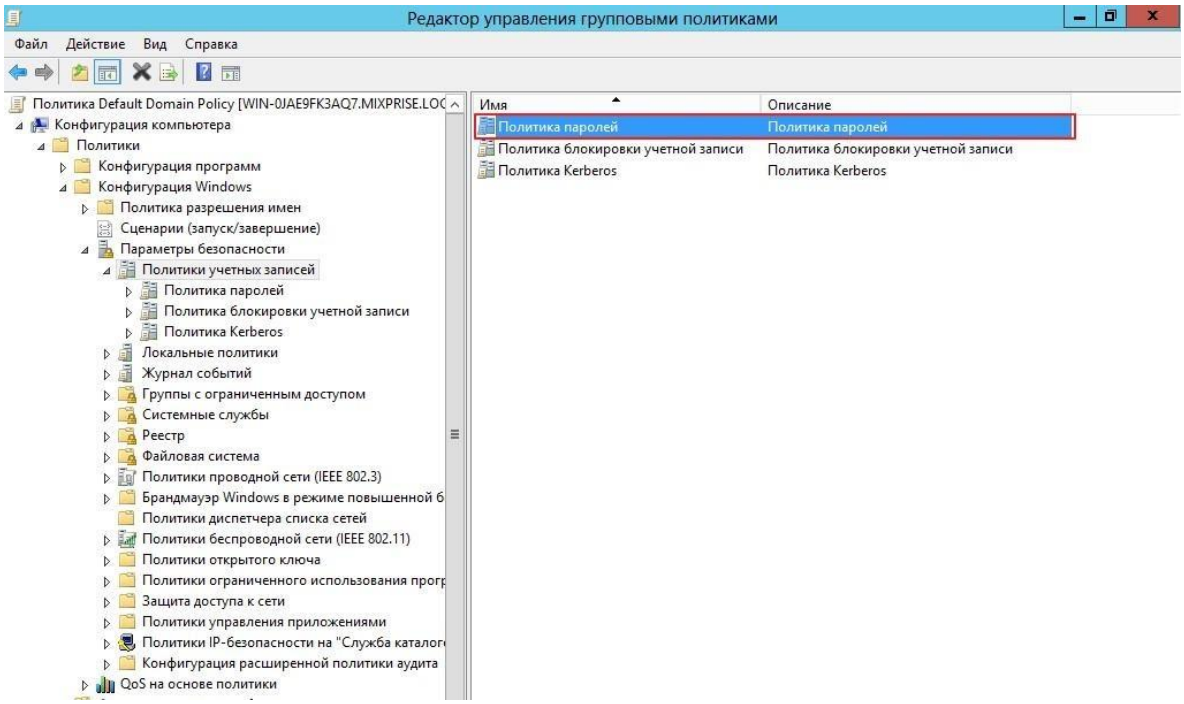


Рис. 41

В открывшимся окошке нам доступно для изменения 6 пунктов, каждый из них мы можем изменить, достаточно просто кликнуть на него.

4. Открываем вкладку **"Вести журнал паролей"** с помощью нее определятся числовое значение новых паролей, которые применяются к пользователю прежде чем он сможет снова использовать предыдущий пароль, здесь я оставляем все по умолчанию.

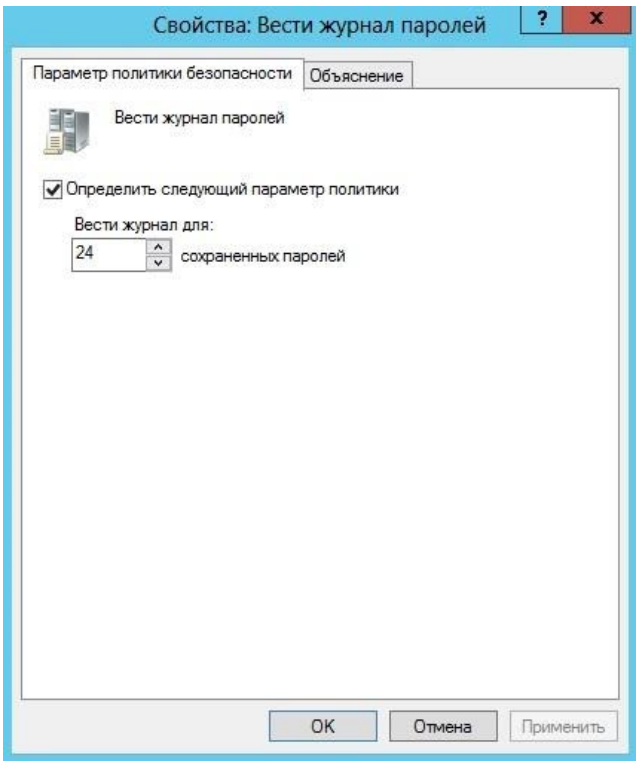


Рис. 42

5. Следующая вкладка **"Максимальный срок действия пароля"** по умолчанию это 42 дня, с помощью этой политики определяется временной интервал, в котором используется пароль прежде чем система вновь потребует от пользователя этот пароль поменять, убираем чекбокс и жмем **"Применить"**

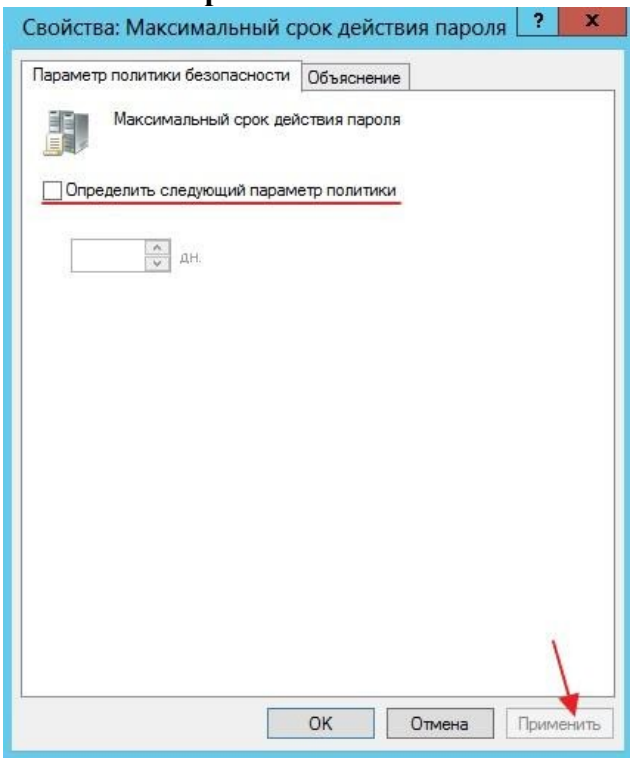


Рис. 43

Переходим на раздел **"Минимальная длина пароля"**. По умолчанию это 7-8 символов, выставляем как минимум 4 символа

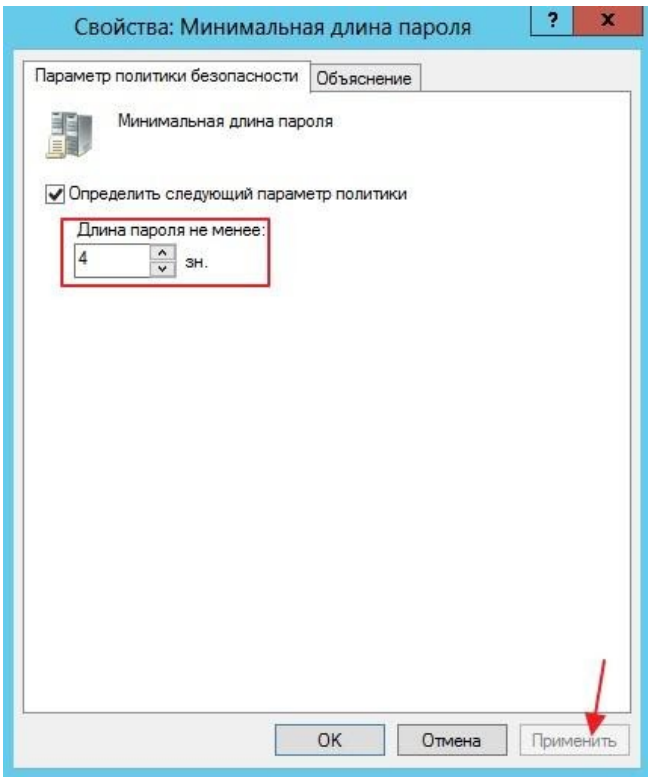


Рис. 44

6. Далее **"Минимальный срок действия пароля"** с помощью него определяется время, за которое пользователь не может изменить пароль по умолчанию значение ноль дней. Убираем галочку и применяем настройки

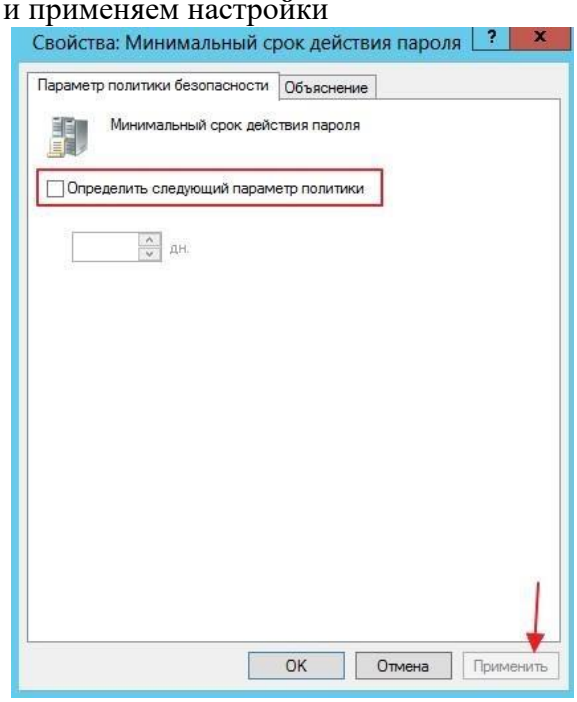


Рис. 45

7. Переходим к **"Пароль должен отвечать требованиям сложности"** это те требования, когда в пароле обязательно должны присутствовать английские буквы, верхнего и нижнего регистра, цифры, не алфавитные символы и т.д. Ставим **"Отключен"** и кликаем **"Применить".**

ВАЖНО! При настройке «живого» сервера эти параметры должны быть включены!

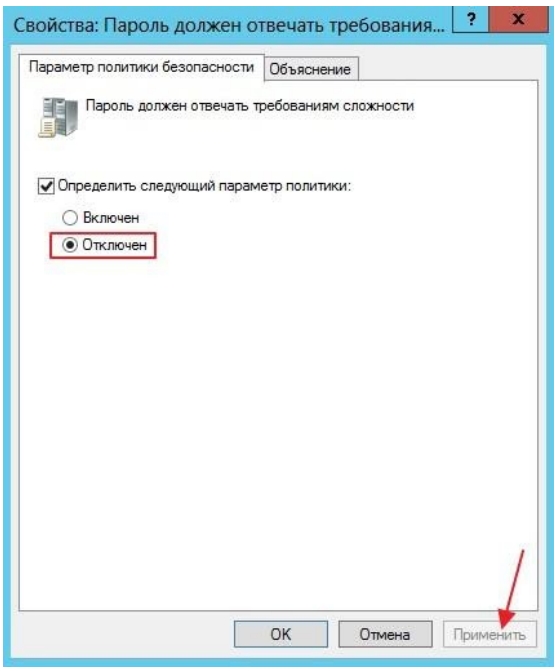


Рис. 46

8. Последняя политика **"Хранить пароли"**, скажем лишь то, что если в ее включить пароли ваших пользователей в системе будут храниться в открытом виде и если злоумышленник доберется до вашей сети, то он легко сможет получить доступ к файлам!

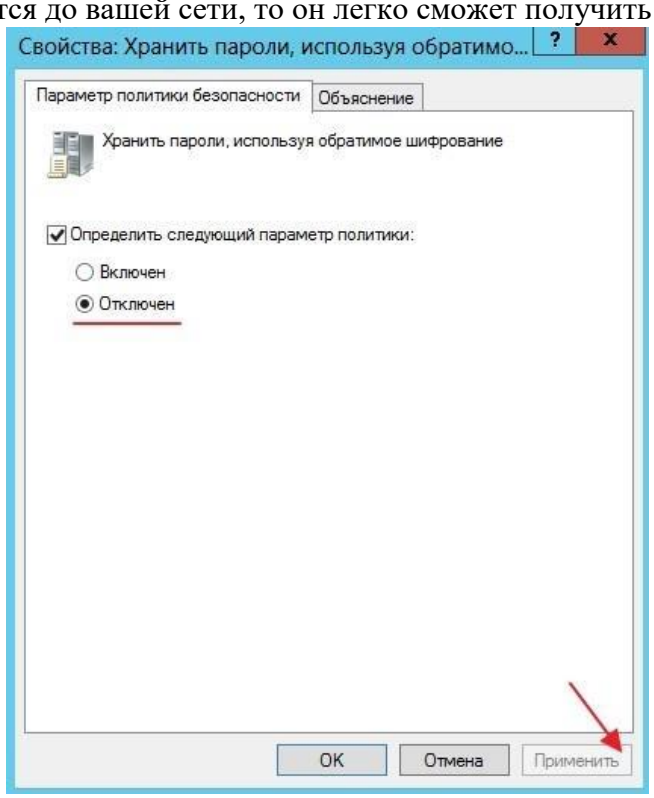


Рис. 47

9. Рассмотрим **"Политику блокировки учетной записи"**. В данной политике доступны 3 блока это: **"Время до сброса счетчика блокировки"** выставляете время блокировки аккаунта, в качестве примера поставим значение равное 30 мин

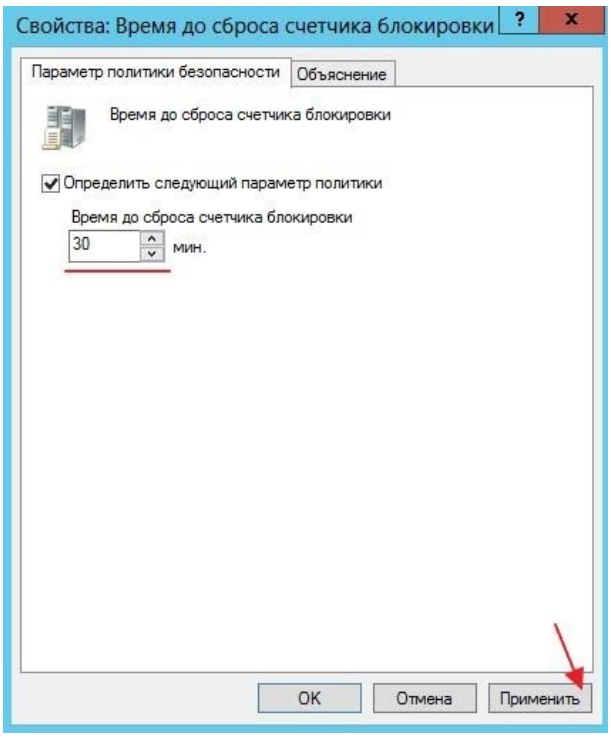


Рис. 48

"Пороговое значение блокировки» прежде, чем аккаунт будет заблокирован, грубо говоря выставляете попытки ввода неверного пароля, после чего наступит блокировка аккаунта пользователя, выставим в качестве примера 3 раза

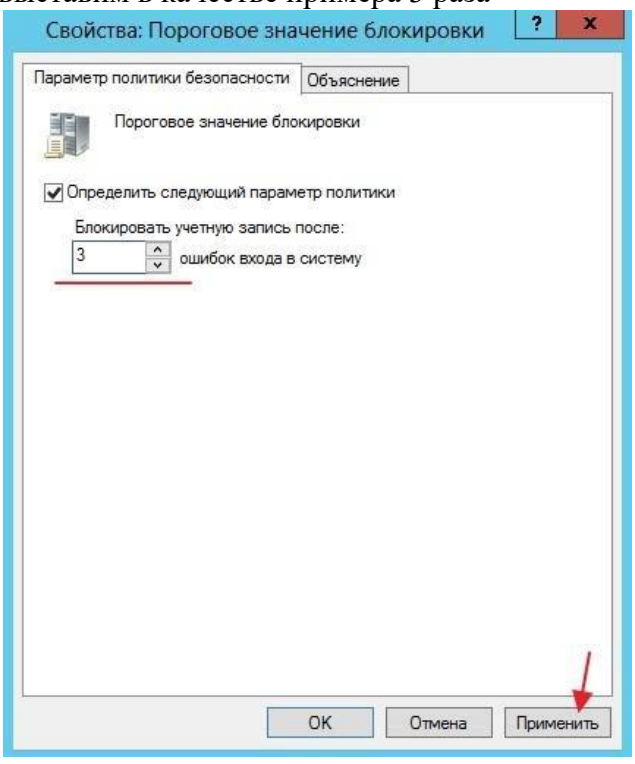


Рис. 49

"Продолжительность блокировки учетной записи" означает что если вы ввели скажем 4 раза неверный пароль, при такой настройке можете подождать 30 мин, и у вас снова будет доступно 3 попытки ввода пароля

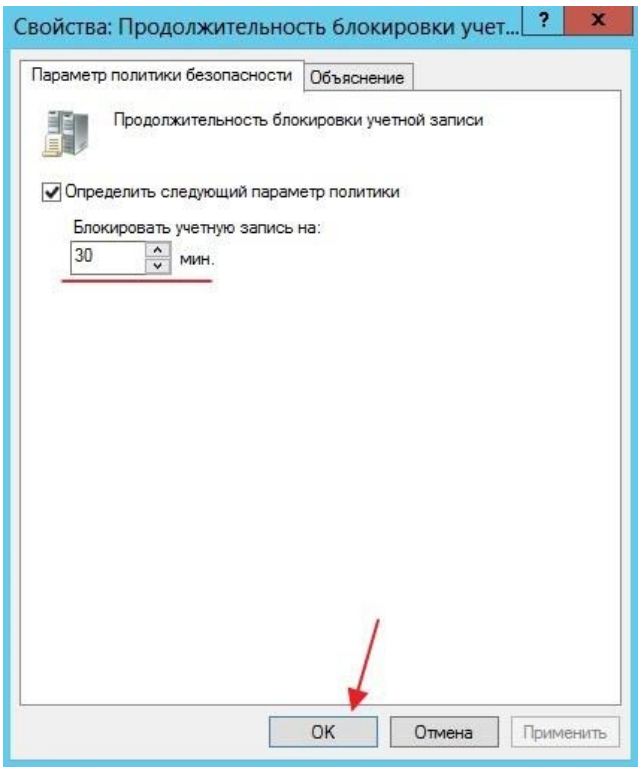


Рис. 50

10. Теперь что бы изменить пароль у пользователя заходим в **"Пользователи и компьютеры Active Directory"**

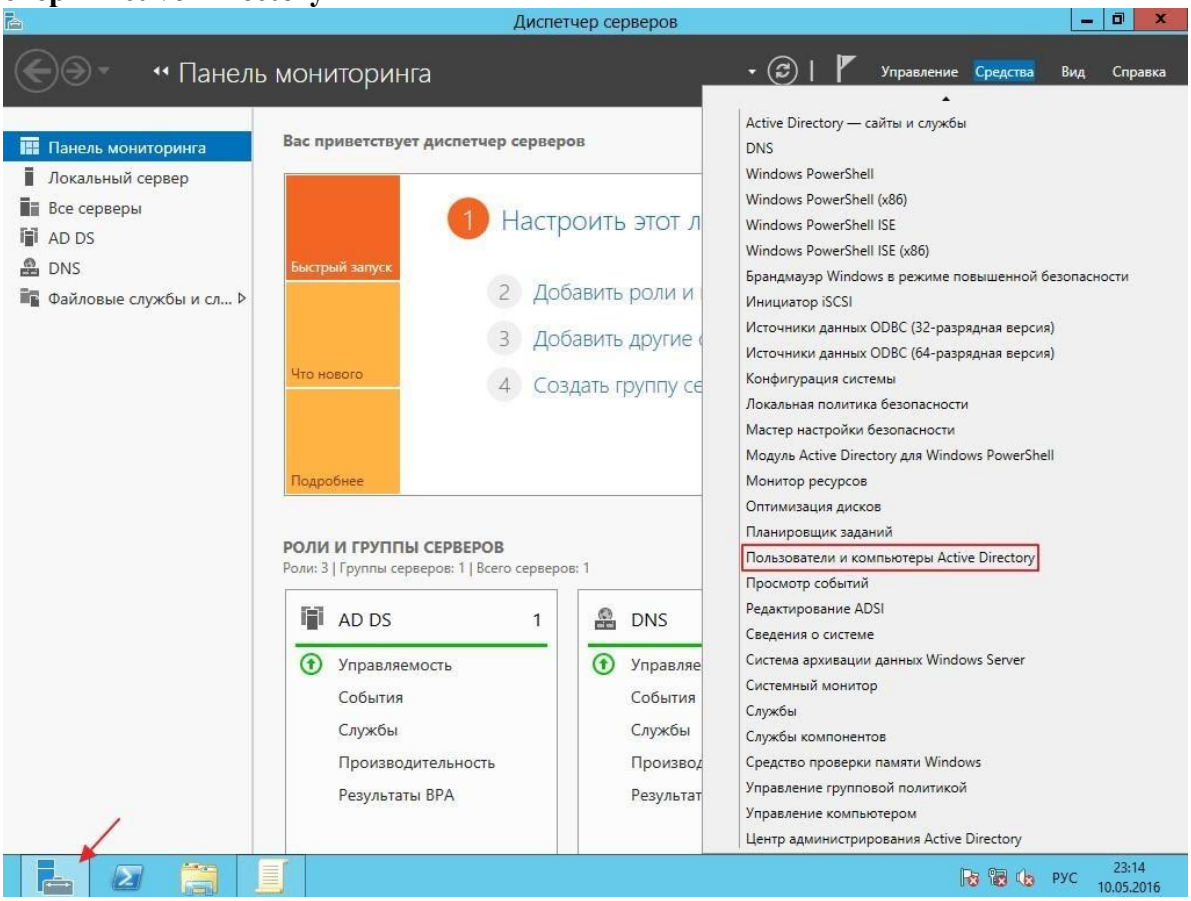


Рис. 51

Ищем учётную запись, для которой мы хотим изменить пароль, в нашем примере создайте учетную запись **«Admin».**

11. Теперь попробуем войти на сервер с новой учетной записью и новым паролем, для этого выполните **"Выход из системы"**

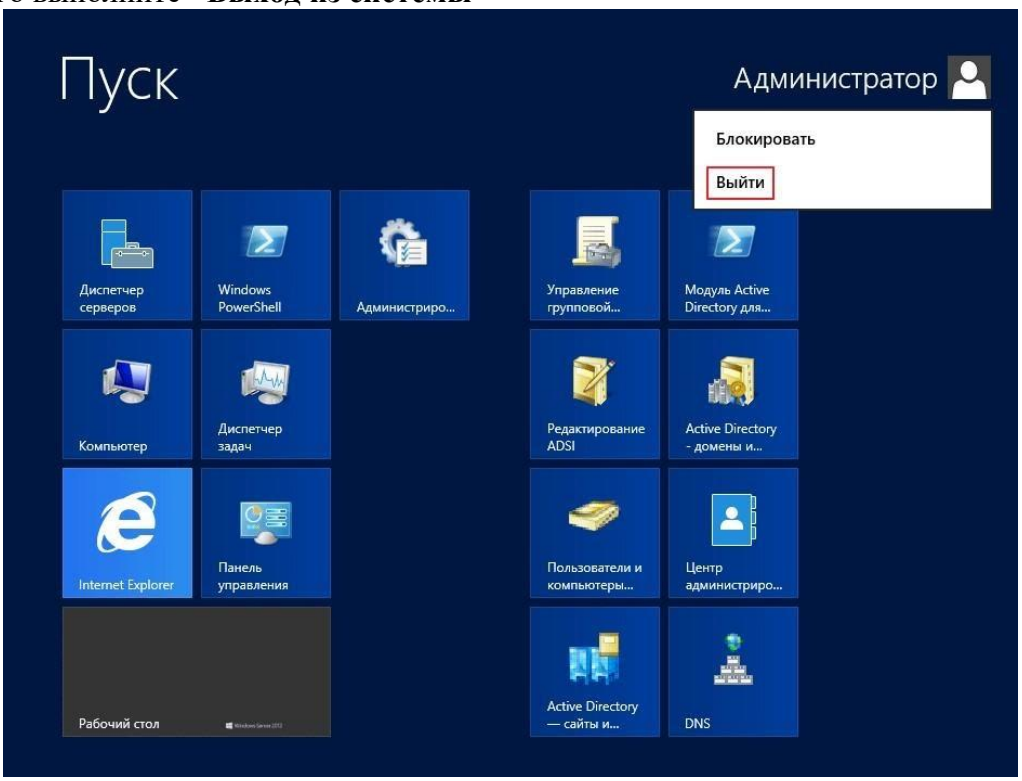


Рис. 52

Осуществляем вход с новой учетной записью

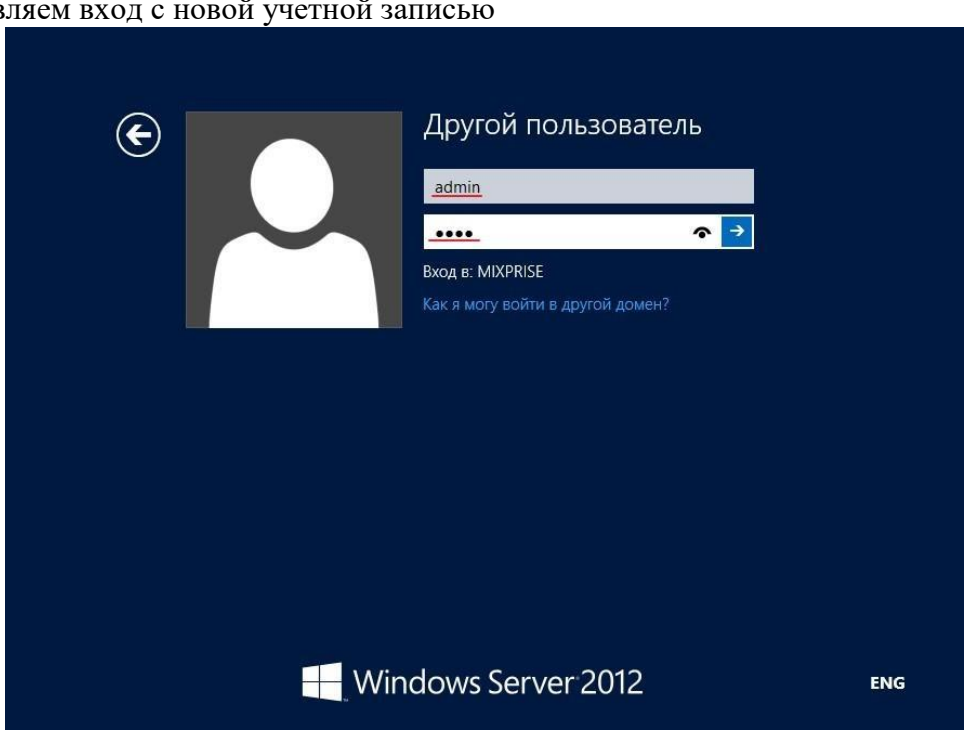


Рис. 53

Сделайте скриншоты (фотографии) процесса настройки контроллера домена Active Directory и вставьте в отчёт.

Создание пользователя в Powershell с параметрами New-ADUser

1. Итак, представим, что нам нужно срочно создать 50 однотипных учетных записей.

Пишем вот такой скрипт:

$org="OU=Students,DC=contoso,DC=com"
$username="student" $count=1..50 foreach ($i in $count)
{ New-AdUser -Name $username$i -Path $org -passThru }

Где:

- Name - логин
- GivenName - имя
- SurName - фамилия
- AccountPassword - пароль, который мы объявили в переменной
- Enbaled - делает пользователя активным

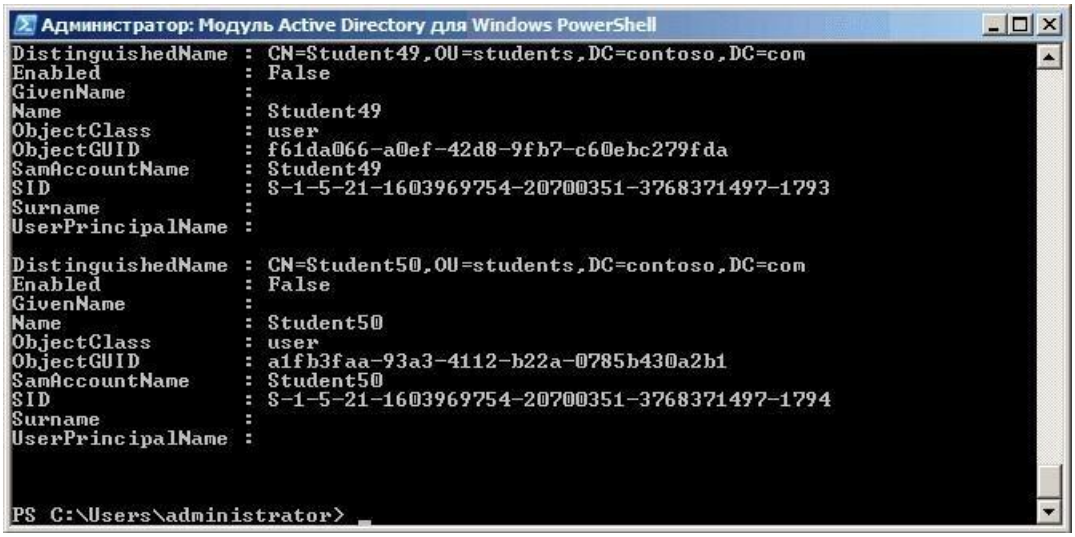


Рис. 54

Запускаем скрипт, и в подразделении Students создается 50 пользователей с именами student1-student50. По умолчанию учетки создаются отключенными, и пользователи все равно будут вынуждены к вам обращаться для их активации. Избежим этого:

$org="OU=Students,DC=contoso,DC=com"
$username="student" $count=1..50 foreach ($i in $count)
{ New-AdUser -Name $username$i -Path $org -Enabled $True -ChangePasswordAtLogon $true `
-AccountPassword (ConvertTo-SecureString «p@$$w0rd» -AsPlainText -force) -passThru }

Здесь создаем учетные записи уже активными и задаем *p@$$w0rd* как пароль по умолчанию, а также указываем сменить его при первом входе в систему. Чтобы не передавать пароль в открытом виде, используем командлет *ConvertTo-SecureString*, который переводит текстовую строку в защищенный формат.

2. Теперь сделаем наш скрипт чуть более гибким. Используя командлет *Read-Host* заставим наш скрипт запрашивать имя и количество пользователей:

$org="OU=Students,DC=contoso,DC=com"
$username=Read-Host "Enter name"

```
$number=Read-Host "Enter number"
$count=1..$number foreach ($i in $count)
{ New-AdUser -Name $username$i -Path $org -Enabled $True -ChangePasswordAtLogon
$true `
-AccountPassword (ConvertTo-SecureString "p@$$w0rd" -AsPlainText -force) -passThru }
```

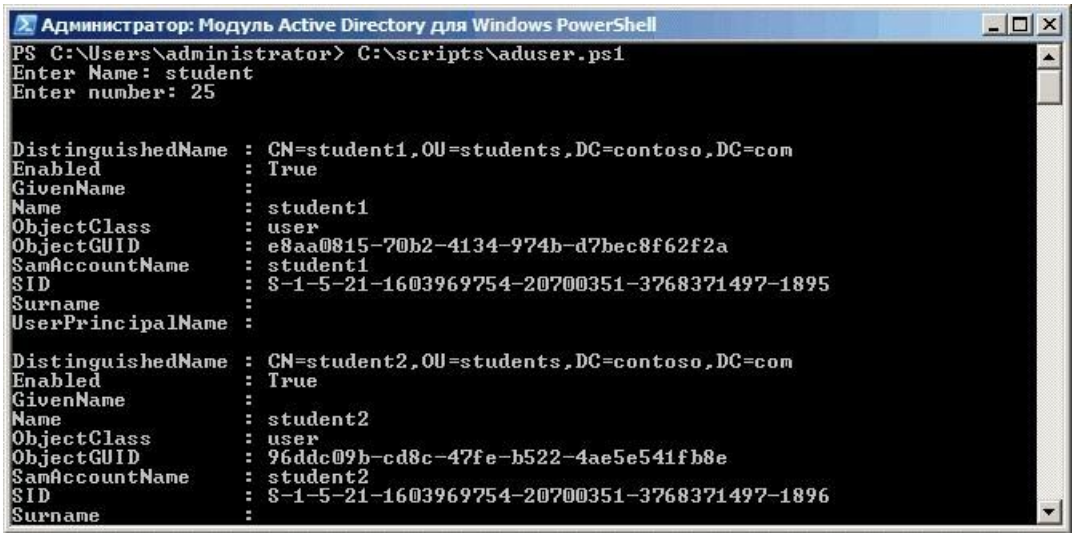


Рис. 55

Учетные записи созданы, пользователи могут заходить в систему и работать. Теперь их надо настроить — добавить в группы безопасности, прописать домашний каталог, сценарии входа и т.п. Сделать это можно с помощью шаблона. Проще говоря, создаем шаблонную учетную запись, полностью настраиваем ее, а затем делаем с нее нужное количество копий с помощью параметра *-Instance* :

```
$template = Get-AdUser -Identity "student"
$org="OU=Students,DC=contoso,DC=com"

$username=Read-Host "Enter name"
$number=Read-Host "Enter number"
$count=1..$number foreach ($i in $count)
{ New-AdUser -Name $username$i -UserPrincipalName $username$i -Path $org -Instance `
$template -Enabled $True -ChangePasswordAtLogon $true `
-AccountPassword (ConvertTo-SecureString "p@$$w0rd" -AsPlainText -force) -passThru }
```

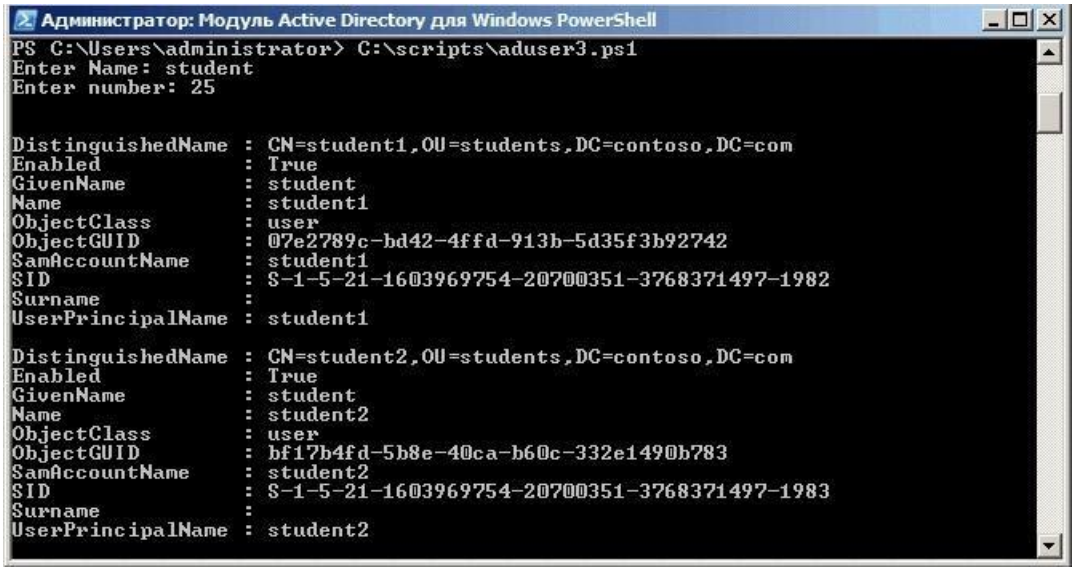
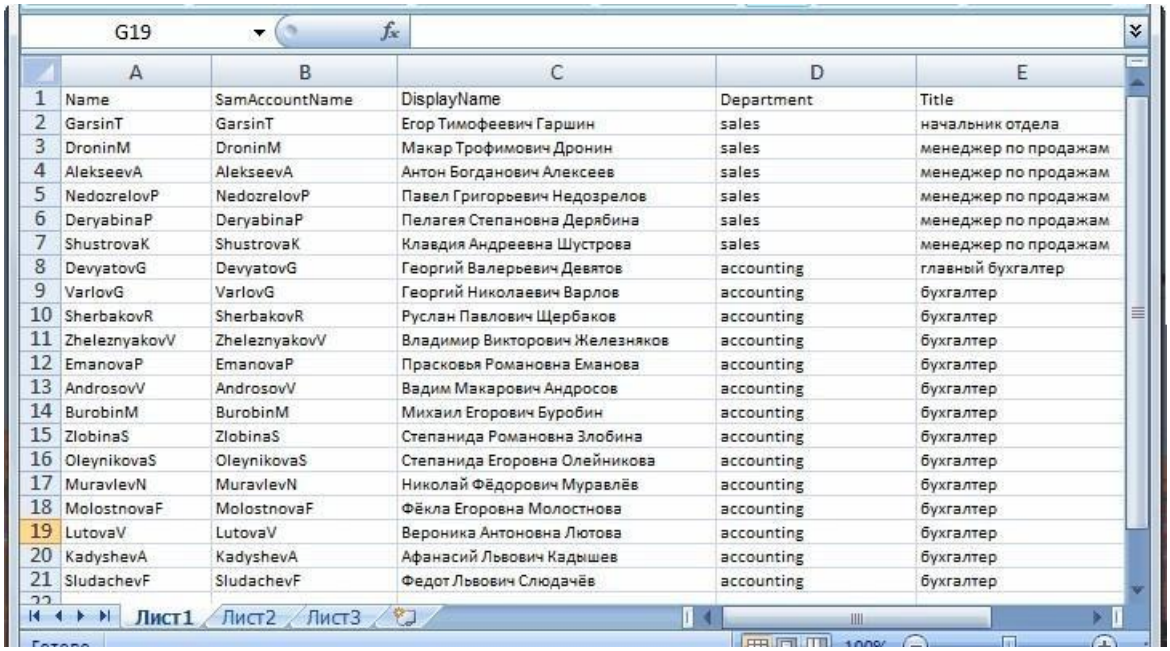


Рис. 56

3. Следующий способ автоматизировать создание учетных записей — импортировать их из CSV-файла. Этот способ подойдет в том случае, если вам предоставили список пользователей, и им надо завести учетные записи в соответствии с этим списком. Как правило, подобные списки создаются в Excel в виде таблицы со столбцами Имя, Должность, Отдел и т.п., примерно такого вида:



	A	B	C	D	E
1	Name	SamAccountName	DisplayName	Department	Title
2	GarsinT	GarsinT	Егор Тимофеевич Гаршин	sales	начальник отдела
3	DroninM	DroninM	Макар Трофимович Дронин	sales	менеджер по продажам
4	AlekseevA	AlekseevA	Антон Богданович Алексеев	sales	менеджер по продажам
5	NedozrelovP	NedozrelovP	Павел Григорьевич Недозрелов	sales	менеджер по продажам
6	DeryabinaP	DeryabinaP	Пелагея Степановна Дерябина	sales	менеджер по продажам
7	ShustrovaK	ShustrovaK	Клавдия Андреевна Шустрова	sales	менеджер по продажам
8	DevyatovG	DevyatovG	Георгий Валерьевич Девятов	accounting	главный бухгалтер
9	VarlovG	VarlovG	Георгий Николаевич Варлов	accounting	бухгалтер
10	SherbakovR	SherbakovR	Руслан Павлович Щербаков	accounting	бухгалтер
11	ZheleznyakovV	ZheleznyakovV	Владимир Викторович Железняков	accounting	бухгалтер
12	EmanovaP	EmanovaP	Прасковья Романовна Еманова	accounting	бухгалтер
13	AndrosovV	AndrosovV	Вадим Макарович Андросов	accounting	бухгалтер
14	BurobinM	BurobinM	Михаил Егорович Буробин	accounting	бухгалтер
15	ZlobinaS	ZlobinaS	Степанида Романовна Злобина	accounting	бухгалтер
16	OleynikovaS	OleynikovaS	Степанида Егоровна Олейникова	accounting	бухгалтер
17	MuravlevN	MuravlevN	Николай Фёдорович Муравлёв	accounting	бухгалтер
18	MolostnovaF	MolostnovaF	Фёкла Егоровна Молостнова	accounting	бухгалтер
19	LutovaV	LutovaV	Вероника Антоновна Лютова	accounting	бухгалтер
20	KadyshevA	KadyshevA	Афанасий Львович Кадышев	accounting	бухгалтер
21	SludachevF	SludachevF	Федот Львович Слюдачёв	accounting	бухгалтер

Рис. 57

Наша задача — сохранить его в формате CSV и затем указать в скрипте с помощью командлета *ImportCSV*. Если ваш CSV-файл содержит все необходимые столбцы, то *New-ADUser* автоматически свяжет их с правильными атрибутами пользователя :

```
$csv = Import-CSV -Path "C:\scripts\users.csv"
$csv | New-AdUser  -Path $org -Enabled $True -ChangePasswordAtLogon $true
`

-AccountPassword (ConvertTo-SecureString "p@$$w0rd" -AsPlainText -force) -passThru
```

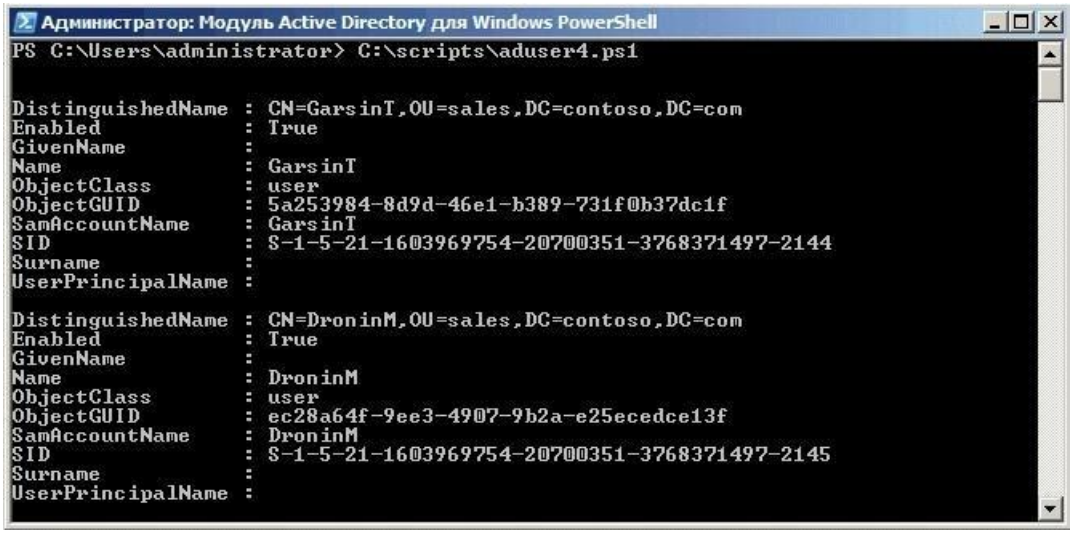


Рис. 58

Таким образом можно импортировать сотни новых пользователей за несколько секунд, но есть в этом методе и подводные камни:

- Названия столбцов должны **полностью** совпадать с названиями атрибутов пользователя, например Name (Имя), Organization (Организация), Title (должность), иначе ничего не получиться.
- В таблице **обязательно** нужно указать SamAccountName, в противном случае будет выдана ошибка о том, что учетная запись уже существует.
- Если атрибуты задаватьть в русской раскладке, как в нашем примере, то могут возникнуть проблемы с кодировкой. В решении этой проблемы мне помогло извлечение содержимго CSVфайла с помощью командлета *Get-Content* и сохранение его в другой CSV-файл: *Get-Content users.csv >> users1.csv*. После этого все русскоязычные атрибуты стали отображаться нормально.

Сделайте скриншоты (фотографии) процесса добавления пользователей домена Active Directory и вставьте в отчёт.

2.4. Практическая работа № 4
Внедрение инфраструктуры Групповых политик

Задание:

Установка принтеров пользователям домена AD с помощью групповых политик

Рассмотрим возможности автоматического подключения принтеров пользователям домена Active Directory с помощью групповых политик (GPO). Довольно удобно, когда при первом входе в систему у пользователя сразу устанавливаются и появляются в принтерах доступные ему устройства.

Рассмотрим следующую конфигурацию: в организации имеется 3 отдела, каждый отдел должен печатать документы на собственном цветном сетевом принтере. Ваша задача, как администратора, настроить автоматическое подключение сетевых принтеров пользователям в зависимости от отдела.

1. Подключение принтеров пользователям через GPO
1. Создайте три новые группы безопасности в AD (prn_HPColorSales, prn_HPColorIT, prn_HPColorManagers) и добавьте в нее пользователей отделов (наполнение групп пользователей можно автоматизировать по статье “Динамические группы в AD”). Вы можете создать группы в консоли ADUC, или с помощью командлета New-ADGroup:

```
New-ADGroup"prnHPColorSales"-path
'OU=Groups,OU=Moscow,DC=corp,dc=winitpro,DC=ru' -GroupScope Global –PassThru
```

2. Запустите консоль редактора доменных политик (GPMC.msc), создайте новую политику **prnt_AutoConnect** и прилинкуйте ее к OU с пользователями;

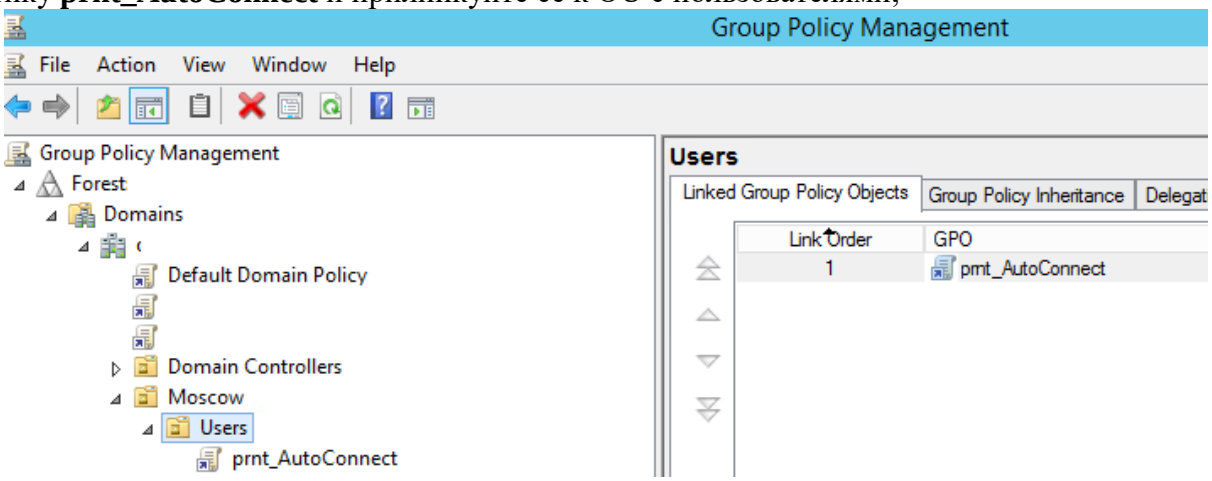


Рис. 74

Если у вас в домене используется небольшое количество сетевых принтеров (до 30-50), вы можете все их настраивать с помощью одной GPO. Если у вас сложная структура домена, есть сайты AD, используется делегирование прав администраторам филиалов, лучше создать несколько политик подключения принтеров, например по одной политике на сайт или OU.

3. Перейдите в режим редактирования политики и разверните секцию **User Configuration -> Preferences -> Control Panel Setting -> Printers**. Создайте новый элемент политики с именем **Shared Printer;**

Если вы хотите подключать принтер по IP адресу (не через принт-сервер, а напрямую), выберите пункт **TCP/IP Printer**.

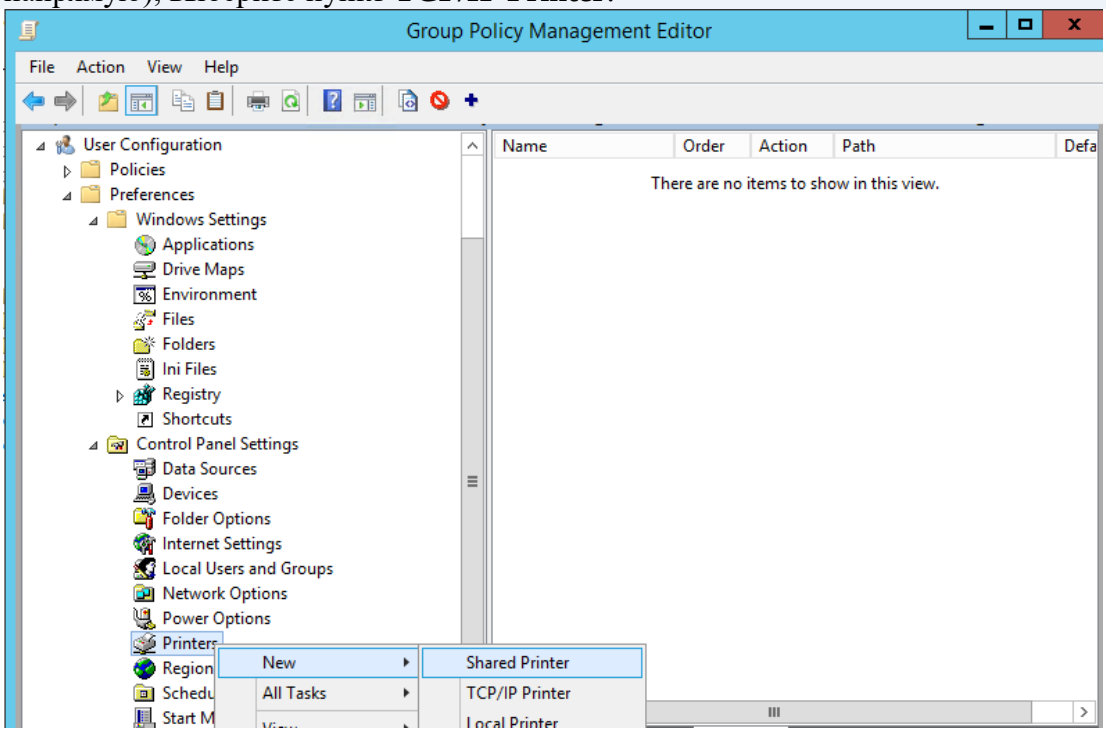


Рис. 75

4. Действие – **Update**. В поле **Shared Path** укажите UNC адрес принтера, например, \\msk-prnt\hpcolorsales (в моем примере все принтеры подключены к принт-серверу \\msk-prnt). Здесь же вы можете указать, нужно ли использовать этот принтер в качестве принтера по-умолчанию;

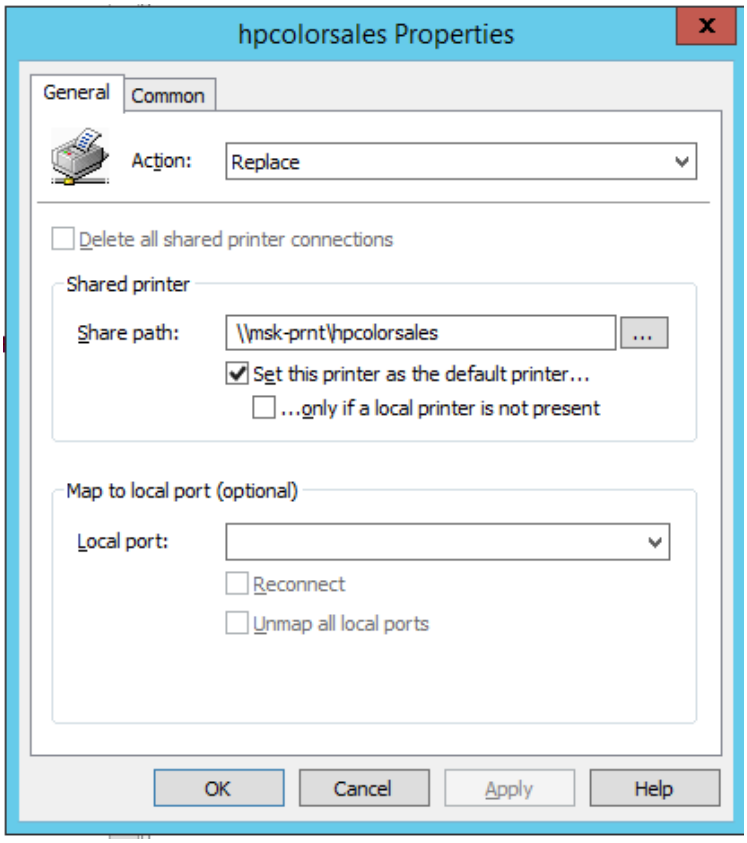


Рис. 76

5. Перейдите на вкладку **Common** и укажите, что принтер нужно подключать в контексте пользователя (опция **Run in logged-on user's security context**). Также выберите опцию **Item-level targeting** и нажмите на кнопку **Targeting**;
6. С помощью нацеливания GPP вам нужно указать, что данная политика подключения принтера применялась только для членов группы prn_HPColorSales. Для этого нажмите **New Item -> Security Group** -> в качестве имени группы укажите prn_HPColorSales;

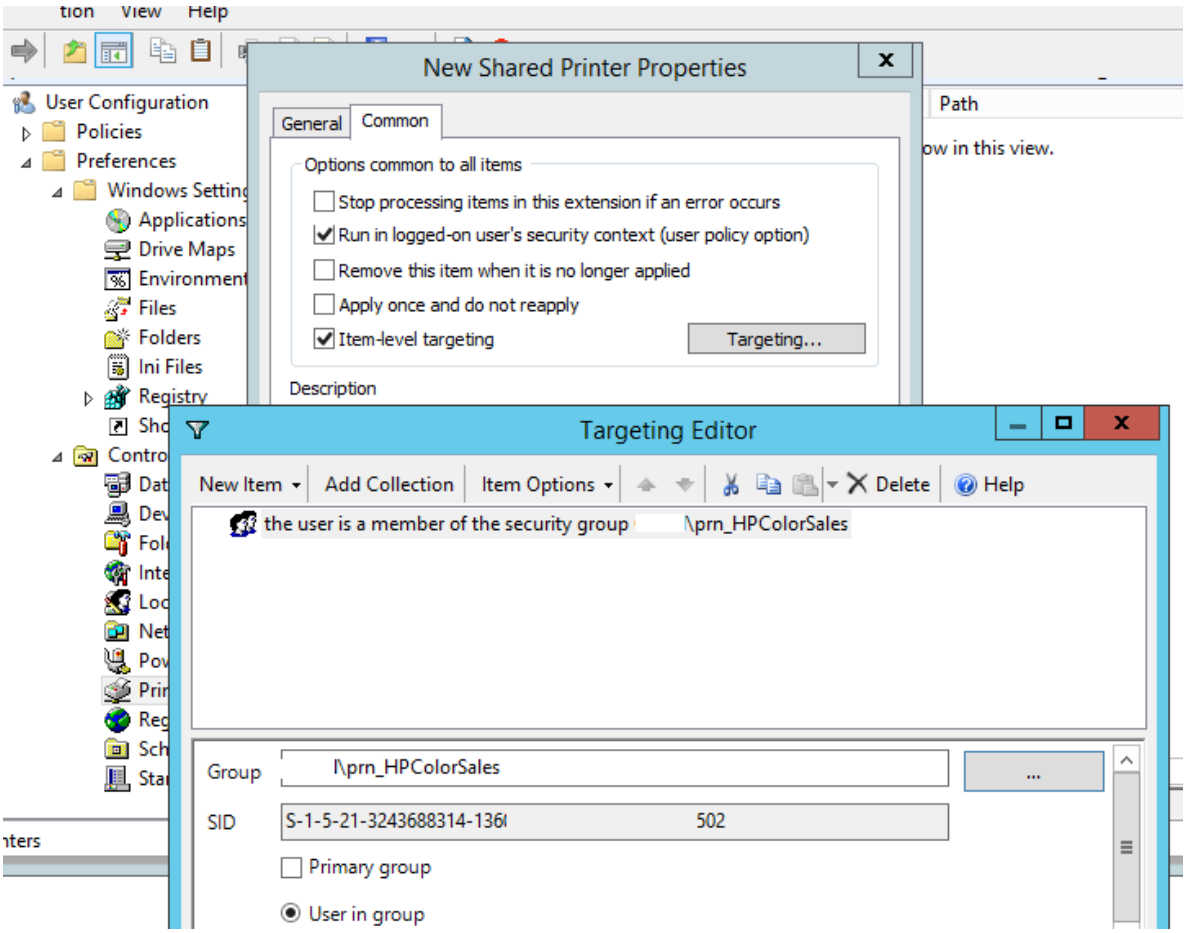


Рис. 77

Обратите внимание, что данное ограничение не запрещает любому пользователю домена подключить это принтер вручную в проводнике Windows. Чтобы ограничить доступ к принтеру, нужно изменить права доступа к нему на принт-сервере, ограничив возможность печати определенными группам.

7. Аналогичным образом создайте политики подключения принтеров для других групп пользователей.

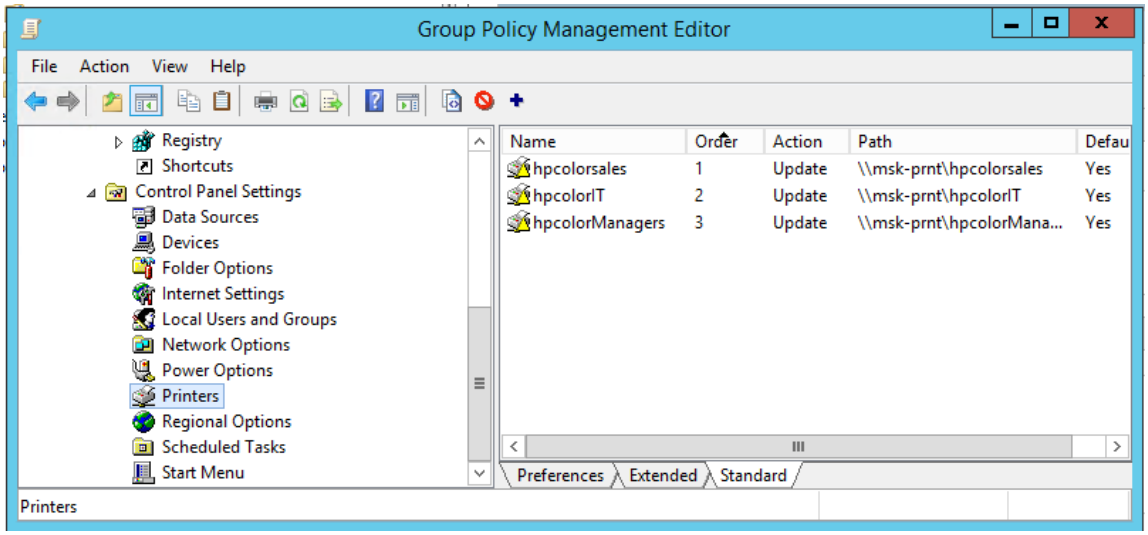


Рис. 78

Есть еще старый раздел политик для настройки принтеров — Computer Configuration -> Policies -> Windows Settings -> Deployed Printers, однако этот метод установки принтеров пользователям не такой гибкий, как рассмотренный ваше способ с помощью GPP.
При использовании такой групповой политики, новые принтера будут устанавливаться у пользователей, только если на их компьютере уже установлен соответствующий принтеру драйвер печати. Дело в том, что у обычных пользователей нет прав на установку драйверов.

2. Настройка политики подключения принтеров Point and Print Restrictions
   1. Для корректного подключения принтеров у любого пользователя, вам необходимо настроить политику Point and Print Restrictions и настроить адреса принт-серверов серверов, с которых пользователей разрешено устанавливать принтеры.

Если вы подключаете принтеры через пользовательский раздел политики, перейдите в раздел GPO **User Configuration -> Policy -> Administrative Templates -> Control Panel -> Printers -> Printer -> Point and Print Restriction**. Включите политику (Enabled) и настройте ее следующим образом:

- **Users can only point and print to these servers** –укажите список принт-серверов, с которых разрешено устанавливать драйвера (указываются FQDN имена, разделитель точка с запятой);
- **When installing driver for new connection** -> Do not show warning or elevation prompt
- **When installing driver for existing connection** -> Do not show warning or elevation prompt.

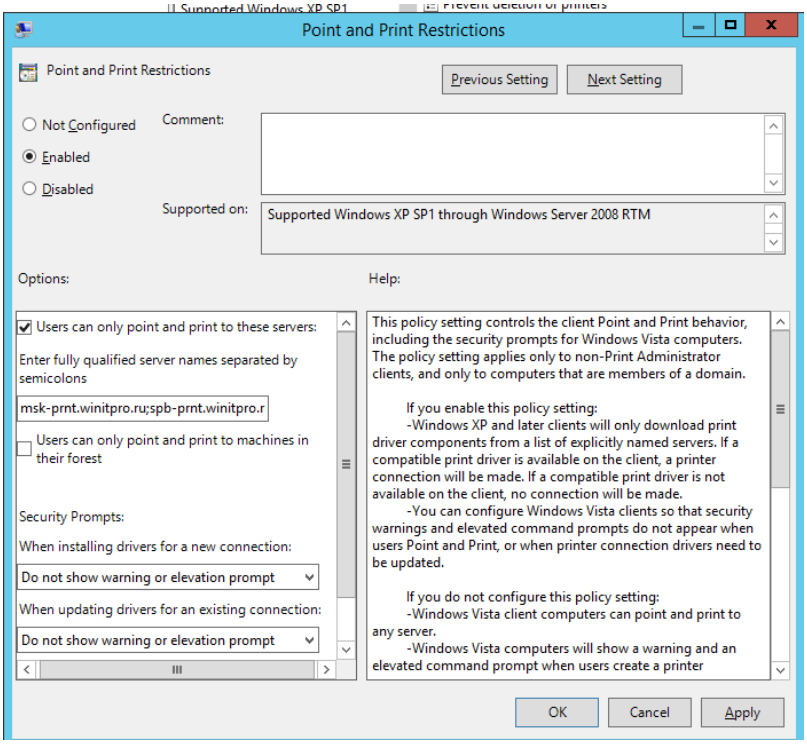


Рис. 79

Аналогичным образом нужно включить политику **Package Point and Print – Approved server** в разделе **User Configuration -> Policies -> Administrative Templates -> Printers** и задать в ней список доверенных принт-серверов.

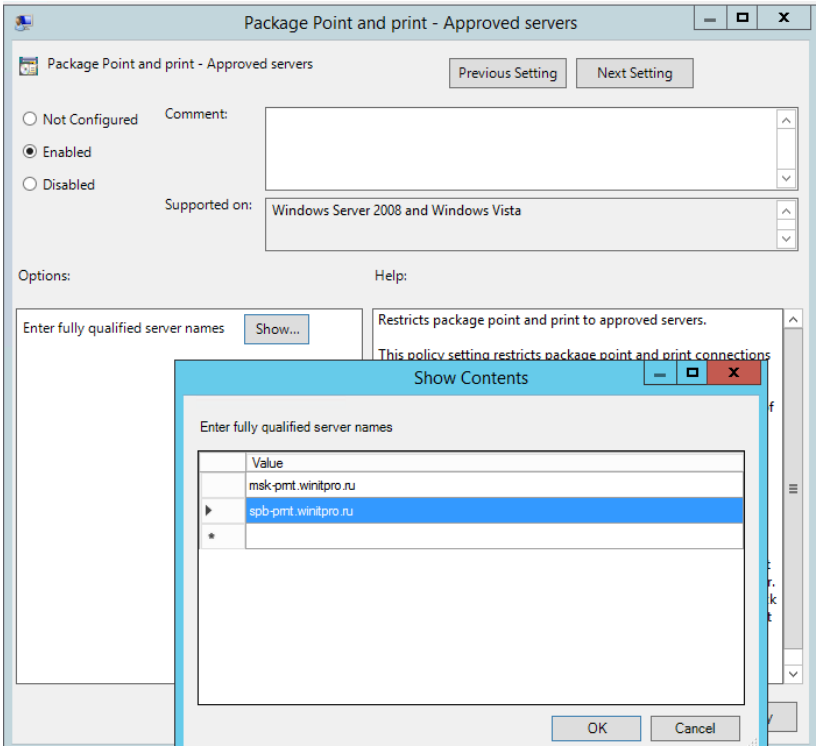


Рис. 80

Теперь после перезагрузки компьютера при входе пользователя у него будет автоматически подключаться назначенный ему сетевой принтер.

Сделайте скриншоты (фотографии) процесса подключения сетевого принтера и вставьте в отчёт.

2.5. Практическая работа № 5
Управление пользовательским рабочим столом через Групповую политику

Задание:

1. Установка фона (обоев) рабочего стола через групповые политики

Рассмотрим, как с помощью групповых политик можно установить одинаковый рисунок рабочего стола (обои) на всех компьютерах домена. Как правило, такое требование возникает в крупных организациях, требующих использовать на всех компьютерах одинаковый фон рабочего стола, выполненного в корпоративном стиле компании.

Нам понадобится, собственно файл с рисунком, который вы хотите использовать в качестве обоев. Это может быть файл формата bmp или jpg.

Если в компании используются мониторы различных форматов, нужно выбрать разрешение наименьшего монитора и использовать именно это разрешение для картинки обоев. Например, если минимальное разрешение монитора 1280 x 1024, именно это разрешение картинки нужно использовать. При этом фоновая картинка будет располагаться по центру экрана, и отображается в режиме заполнения (Fill).

Файл с изображением можно предварительно скопировать на все компьютеры, но на мой взгляд проще, чтобы клиенты автоматически брали jpg файл из сетевого каталога. Для этого можно использовать файл-сервер, каталог SYSVOL на контроллерах домена или DFS каталог. Для нашей распределенной сети мы выбрали второй вариант, ведь так как содержимое SYSVOL автоматически реплицируется между всеми DC, это уменьшит WAN — трафик между филиалами при получении клиентами файла с рисунком.

Скопируйте файл с изображением на любом контроллер домена в каталог **C:\Windows\SYSVOL\sysvol\winitpro.loc\scripts\Screen**. UNC путь к файлу будет выглядеть так: **\\winitpro.loc\SYSVOL\winitpro.loc\scripts\Screen\corp_wallpaper.jpg**.

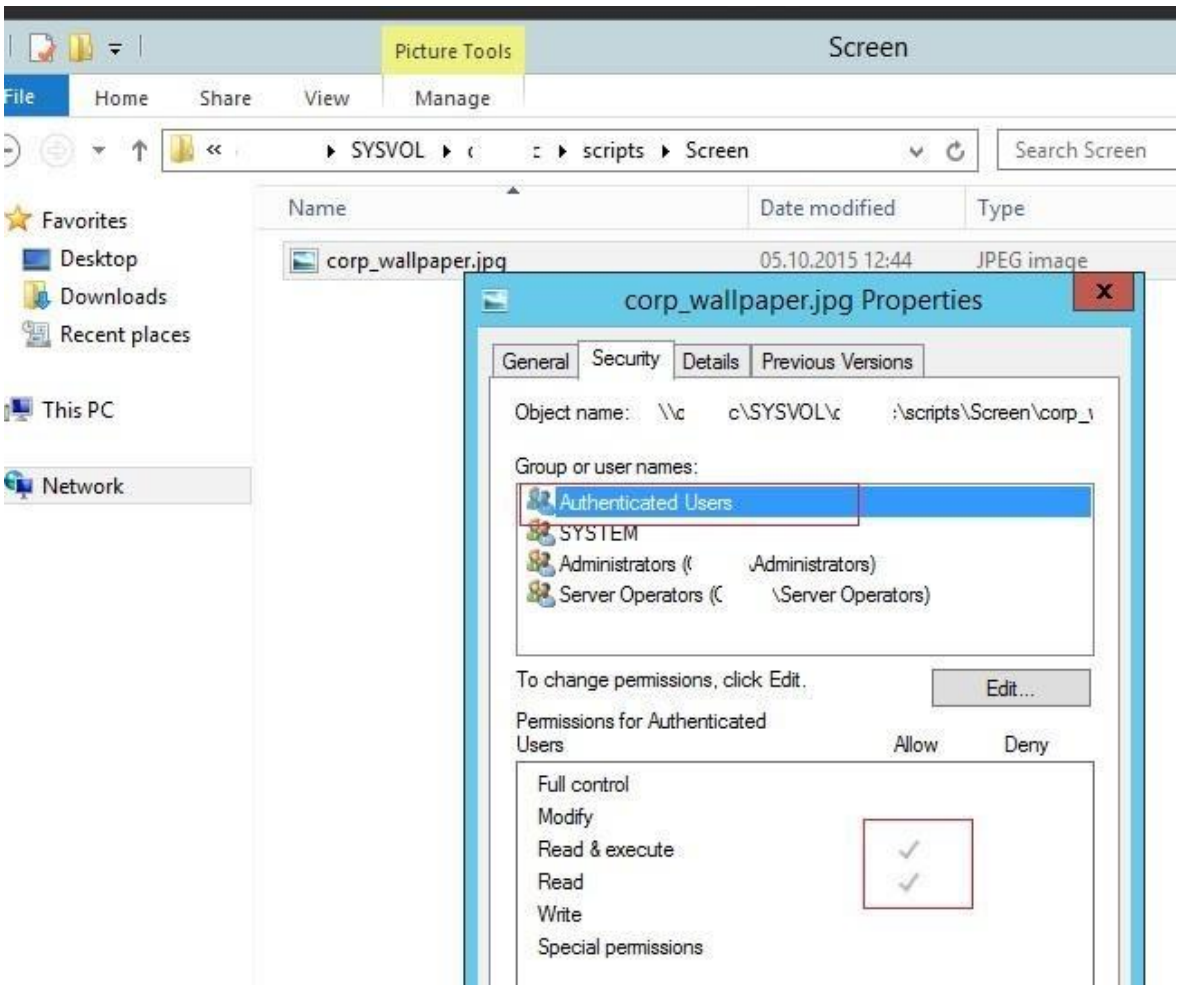


Рис. 96

Проверьте, что у пользователей домена есть права на чтение этого файла (проверьте NTFS разрешения, предоставив право **Read** группе **Domain Users** или **Authenticated Users**).

2. Настройка групповых политик управления фоном рабочего стола

Затем откройте консоль управления доменными GPO (**GPMC.msc**). Создайте новую политику и назначьте ее на нужный OU с пользователями (в нашем примере мы хотим, чтобы политика применялась на все компьютеры и сервера домена, поэтому мы просто отредактируем политику Default Domain Policy). Перейдите в режим редактирования политики.

Перейдите в секцию секции **User Configuration -> Policies -> Administrative Templates -> Desktop -> Desktop** (Конфигурация пользователя -> Административные шаблоны -> Рабочий стол -> Рабочий стол).

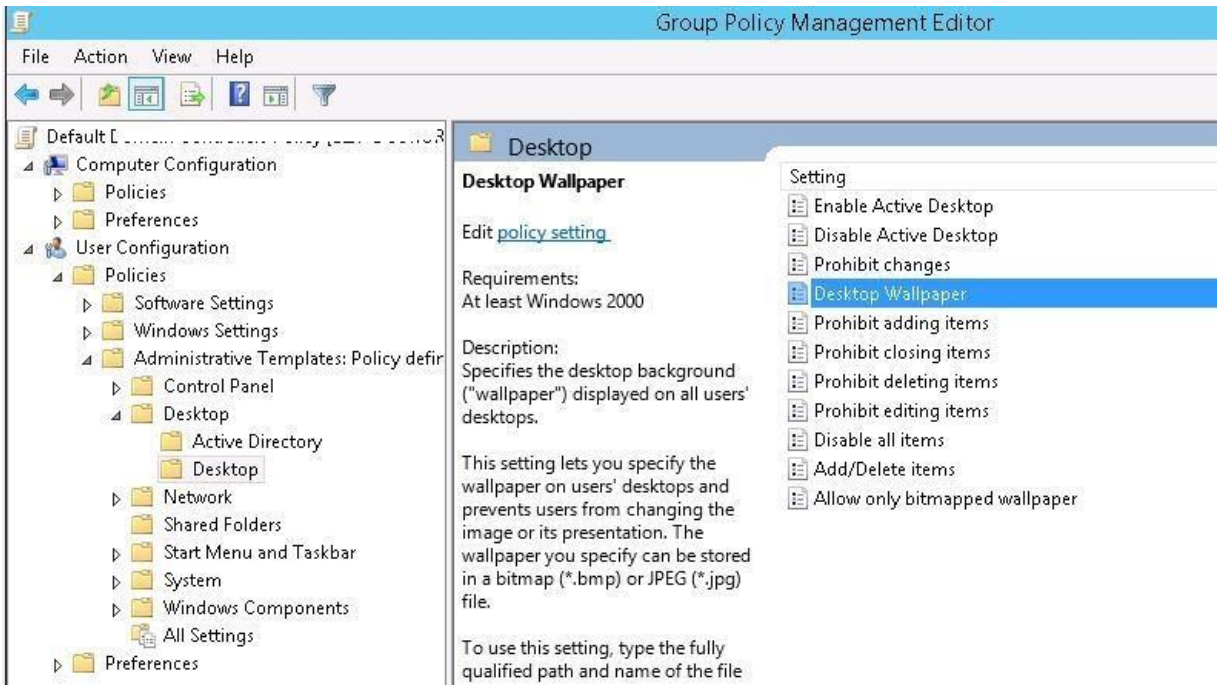


Рис. 97

Включите политику **Enable Active Desktop** (Включить Active Desktop).

Рис. 98

Затем включите политику **Desktop Wallpaper** (Фоновые рисунки рабочего стола). В параметрах политики укажите **UNC путь** к файлу с рисунком и выберите стиль фонового рисунка (Wallpaper Style) — **Fill** (Заполнение).

Совет. Как правило, стиль фонового рисунка “Fill” выглядит нормально почти на всех разрешениях экрана.

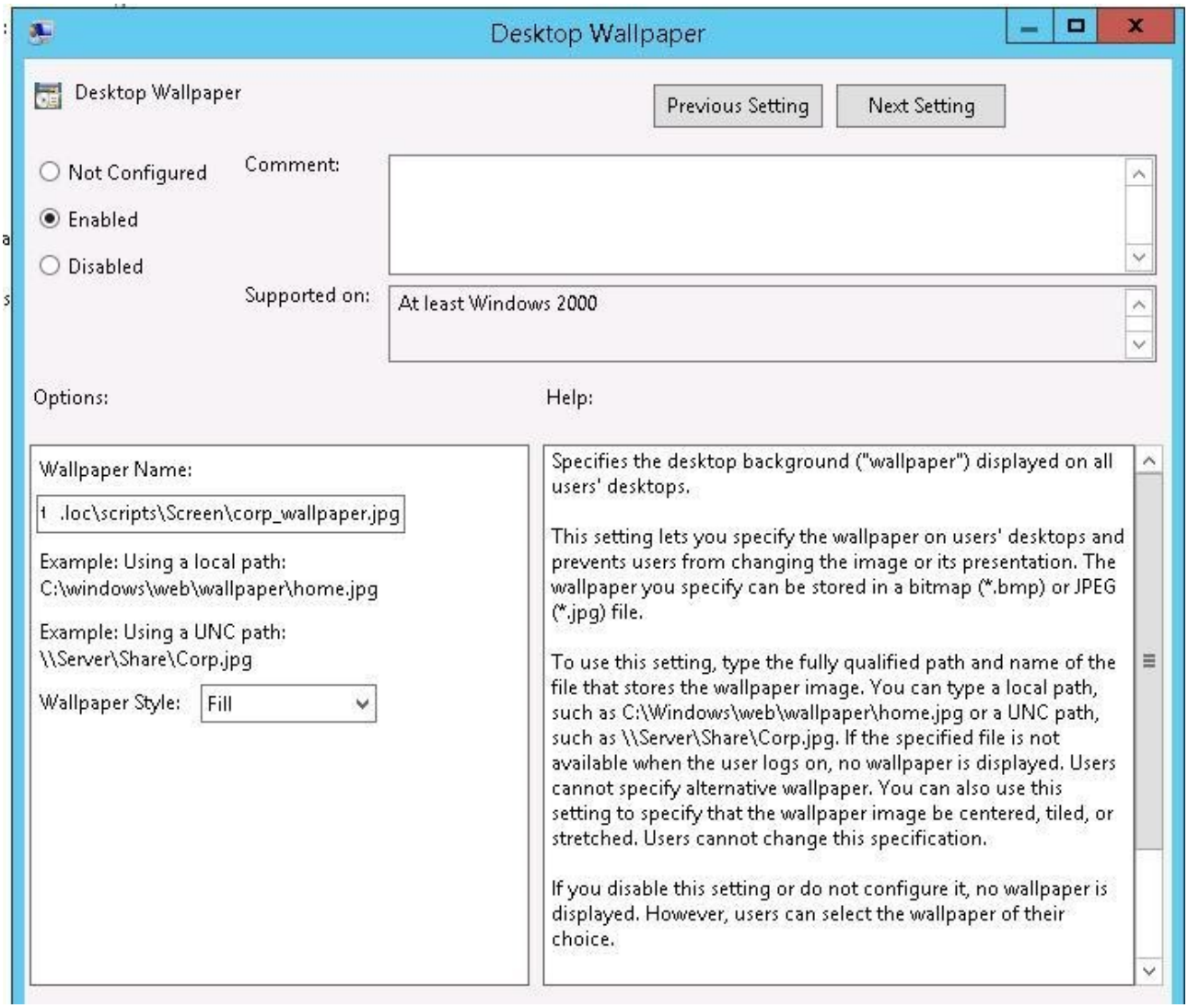


Рис. 99

Чтобы проверить работу политики на клиенте, выполните выход из системы (logoff) и зайдите в систему опять. На рабочем столе пользователя должны отобразиться заданные обои.

Если групповая политика не применяется на клиентах, выполнить диагностику назначения политики на конкретном клиенте можно с помощью команды gpresult (убедить что ваша политика отображается в секции Applied Group Policy Objects).

Если требуется **запретить пользователям менять фоновый рисунок рабочего стола**, включите политику **Prevent Changing Desktop Background** (Запрет изменения фона рабочего стола) в разделе **User Configuration -> Administrative Templates -> Control Panel -> Personalization**.

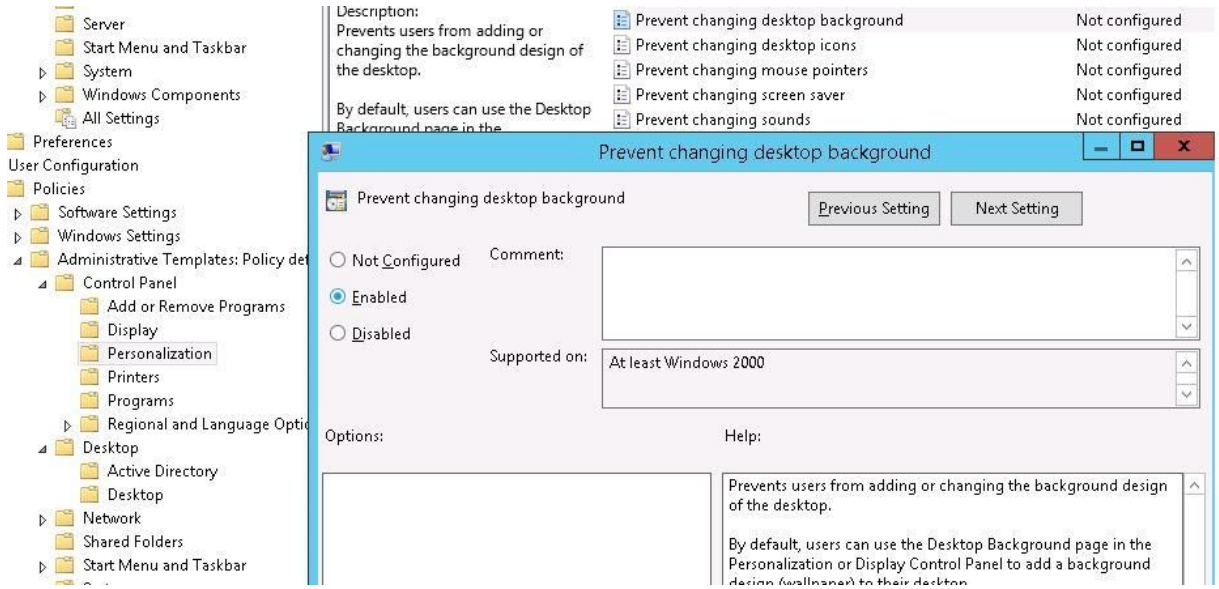


Рис. 100

Если вы хотите более точно нацеливать политику с обоями на клиентов, вы можете использовать WMI Фильтры GPO, например, чтобы применить обои только к десктопам с Windows 10, используйте следующий WMI фильтр:

```
select * from Win32_OperatingSystem where Version like “10.%”
```

3. Настройка фона рабочего стола через реестр и GPO

Вы можете задать параметры и файл фонового рисунка рабочего стола через реестра. Путь к файлу обоев хранится в строковом (REG_SZ) параметре реестра **Wallpaper** в ветке **HKEY_CURRENT_USER\Control Panel\Desktop** или **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System**. В этом параметре нужно указать UNC путь к вашей картинке.

В этой же ветке реестра параметром **WallpaperStyle** (REG_SZ) задается положение изображения на рабочем столе. Для растягивания изображения используется значение **2**.

Если вы хотите запретить пользователям менять фон рабочего стола, создайте в ветке ре-

естра **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop** параметр «NoChangingWallPaper»=dword:00000001

Эти настройки реестра можно распространить на компьютеры пользователей через расширение GPO – Group Policy Preferences. Для этого перейдите в раздел **User Configuration -> Preferences -> Windows Settings** и создайте два параметра реестра с режимом Update.

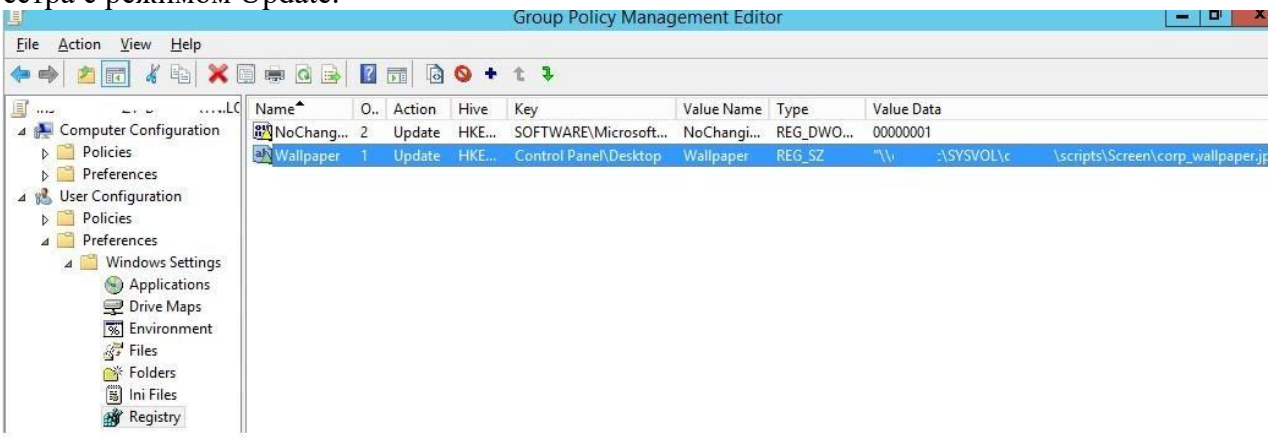


Рис. 101

С помощью Group Policy Preferences Item level Targeting вы можете более точно назначить политику обоев на клиентов. Например, в свойствах параметра реестра в политике

на вкладке **Common** включите **Item level Targeting**, нажмите кнопку **Targeting** и с помощью простого мастера укажите, что данные настройки политики фонового рисунка должны применяться только к компьютерам с Windows 10 и пользователям из определённой группы безопасности AD.

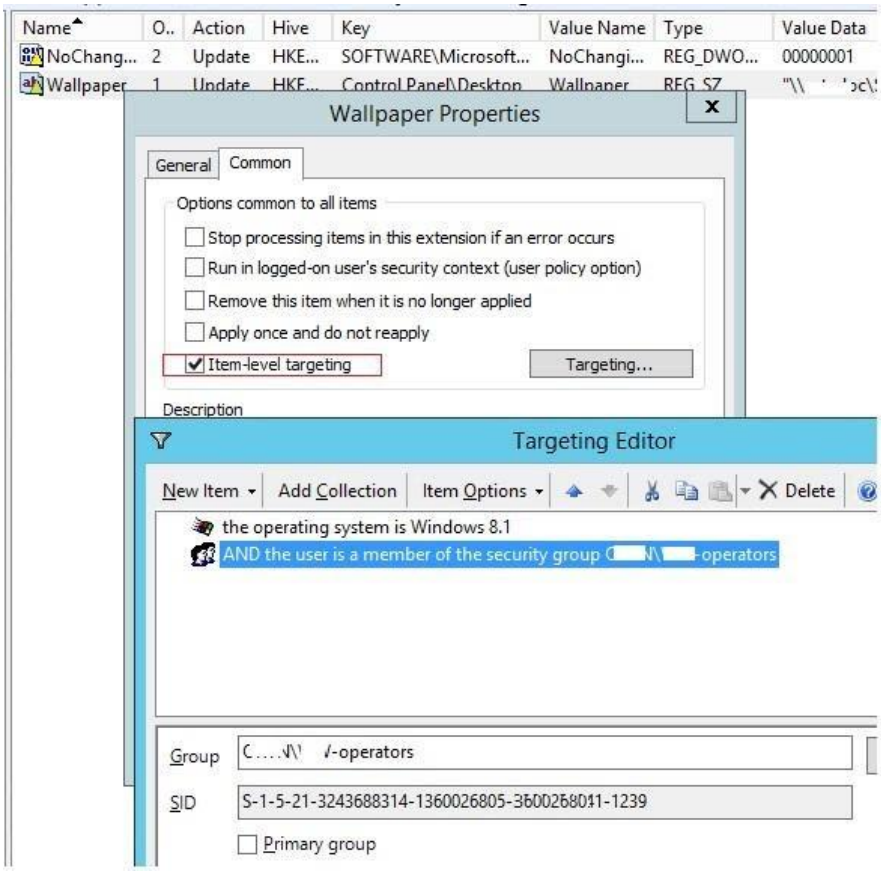


Рис. 102

Аналогичным образом вы можете сделать несколько разных файлов обоев для разных групп пользователей (или устройств). Добавив нужных пользователей в группы доступа вы можете задать различный фоновый рисунок рабочего стола для разных категорий сотрудников.

Дополнительно вы можете изменить картинку на экране входа в систему. Для этого можно использовать политику **Force a specific default lock screen image** в разделе GPO Computer Configuration -> Policies -> Administrative Templates -> Control Panel -> Personalization или через следующие параметры реестра:

- HKLM\Software\Policies\Microsoft\Windows\Personalization — LockScreenImage — путь к jpg изображению на экране блокировки;
- HKLM\Software\Policies\Microsoft\Windows\Personalization — LockScreenOverlaysDisabled = 1;
- HKLM\Software\Policies\Microsoft\Windows\System — DisableLogonBackgroundImage = 0.

Дополнительно вы можете настроить на компьютерах единый корпоративный скринсейвер в виде слайдшоу из набора jpeg картинок.

4. На Windows 10 не применяются обои рабочего стола через GPO

На компьютерах с Windows 10 политика обоев рабочего стола может применяться не с первого раза. Дело в том, что Windows 7 и Windows 10 по-разному используют кеш фонового рисунка рабочего стола. В Windows 7 при каждом входе пользователя в систему кэш фонового изображения обоев перегенерируется автоматически.

В Windows 10, если путь к картинке не изменился, не происходит обновление кэша, соответственно пользователь будет видеть старую картинку, даже если вы обновили ее в каталоге на сервере.
Поэтому для Windows 10 можно добавить дополнительный логоф скрипт, который очищает кэш изображения при выходе пользователя из системы. Это может быть bat файл **Clear_wallpaper_cache.bat** с кодом:

```
del /F /S /Q %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper
del /F /S /Q %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Themes\CachedFiles\*.*
```

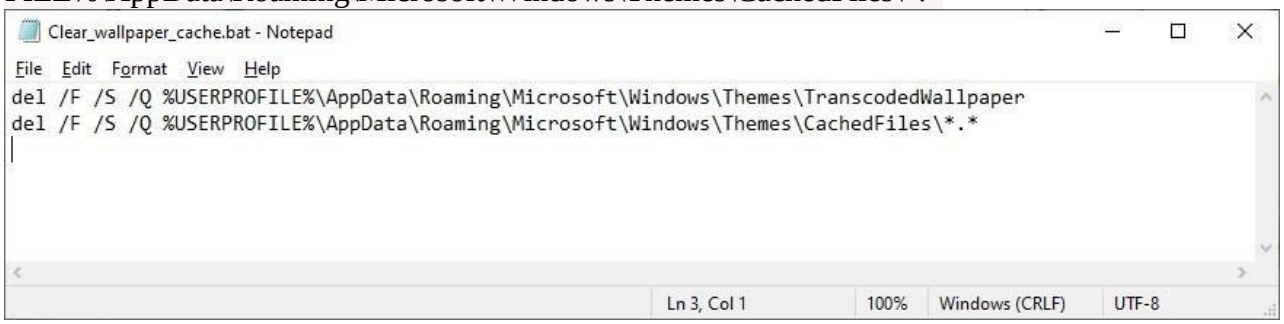


Рис. 103

В результате фон рабочего стола у пользователей Windows 10 станет применяться нормально.

Сделайте скриншоты (фотографии) процесса настройки пользовательского рабочего стола через Групповую политику и вставьте в отчёт.

2.6. Практическая работа № 6
Установка и настройка роли Сервер Сетевой политики

Задание:

1. Установка и настройка ADRMS на Windows Server 2012 R2
    1. Служба **Active Directory Right Management Services** – одна из стандартных ролей Windows Server, позволяющая организовать защиту пользовательских данных от несанкционированного использования. Защита информации реализуется за счет шифрования и подписывания документов, причем владелец документа или файла может сам определить, каким пользователям можно открывать, редактировать, распечатывать, пересылать и выполнять другие операции с защищенной информацией. Нужно понимать, что защита документов с помощью ADRMS возможно только в приложениях, разработанных с учетом этой службы (AD RMS-enabled applications). Благодаря AD RMS можно обеспечить защиту конфиденциальных данных как внутри, так и за пределами корпоративной сети.

    Несколько важных требования, которые нужно учесть при планировании и развертывании решения AD RMS:

- Желательно использовать выделенный сервер AD RMS. Не рекомендуется совмещать роль AD RMS с ролью контроллера домена, сервера Exchange, SharePoint Server или центра сертификации (CA)
- У пользователей AD должен быть заполнен атрибут email
- На компьютерах пользователей RMS сервер должен быть добавлен в зону доверенных сайтов IE (Trusted Sites). Проще всего это сделать с помощью групповой политики.

2. Прежде чем приступить непосредственно к развертыванию ADRMS, нужно выполнить ряд подготовительных шагов. В первую очередь необходимо создать в Active Directory отдельную сервисную запись для ADRMS с бессрочным паролем, например с именем svcadrms (для службы ADRMS можно создать и особую управляемую учетную запись AD — типа gMSA).

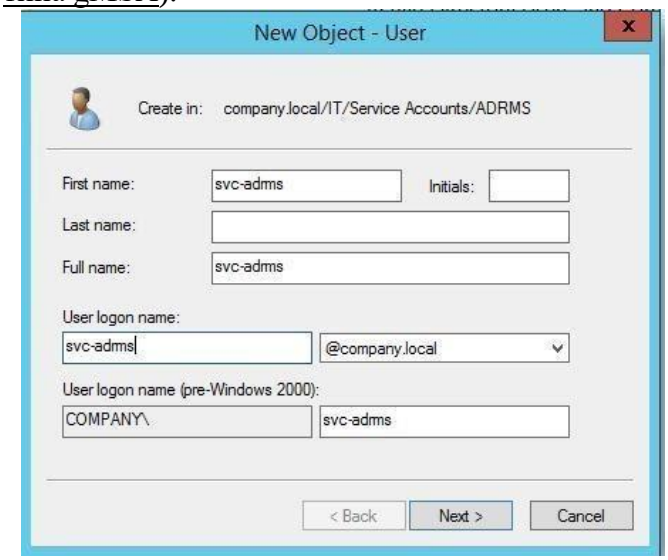


Рис. 59

3. В DNS-зоне создадим отдельную ресурсную запись, указывающую на AD RMS сервер. Допустим его имя будет – **adrms**.

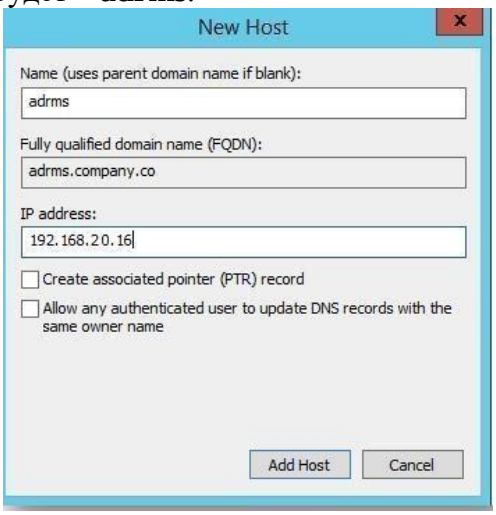


Рис. 60

4. Приступим к установке роли ADRMS на сервере с Windows Server 2012 R2. Откройте консоль Serve Manager и установите роль **Active Directory Rights Management Service** (здесь все просто – просто соглашайтесь с настройками и зависимостями по-умолчанию).

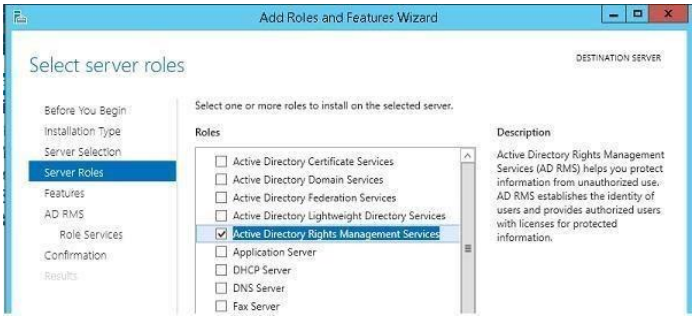


Рис. 61

5. После того, как установка роли ADRMS и сопутствующих ей ролей, и функций закончится, чтобы перейти в режим настройки роли ADRMS, щелкните по ссылке **Perform additional configuration**.

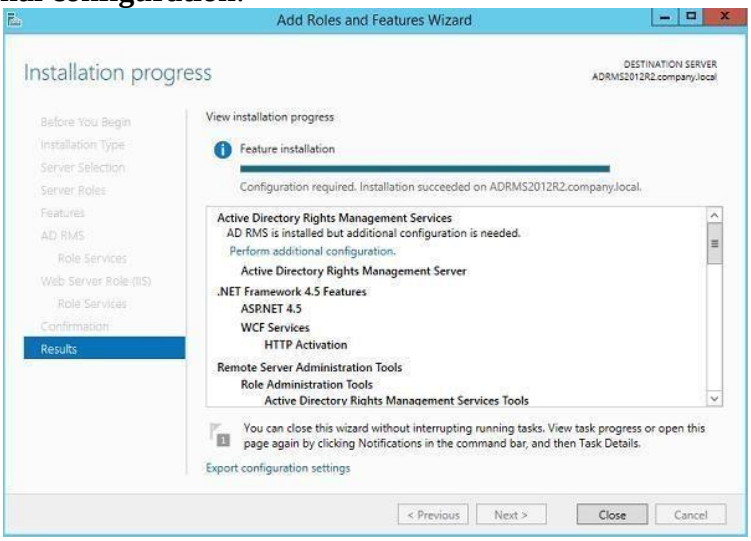


Рис. 62

6. В мастере настройки выберем, что мы создаем новый корневой кластер AD RMS (**Create a new AD RMS root cluster**).

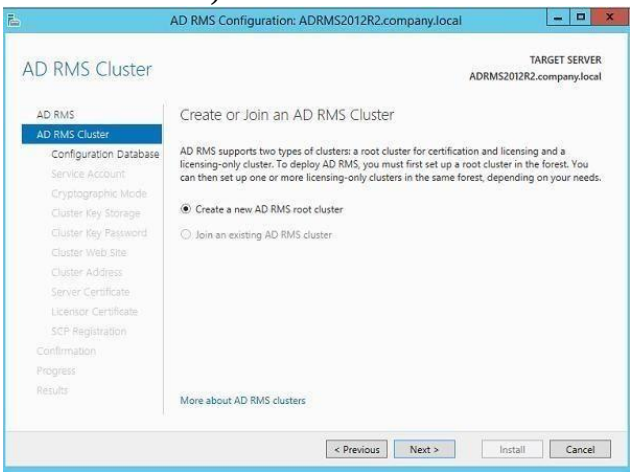
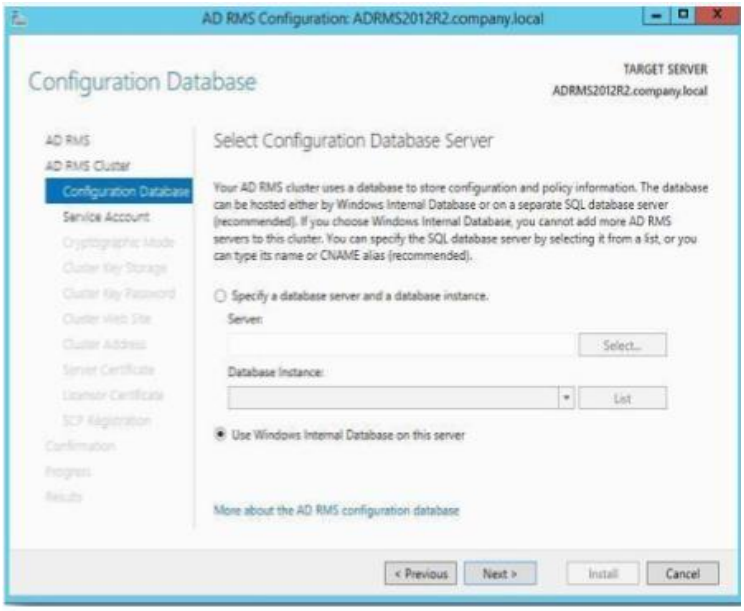
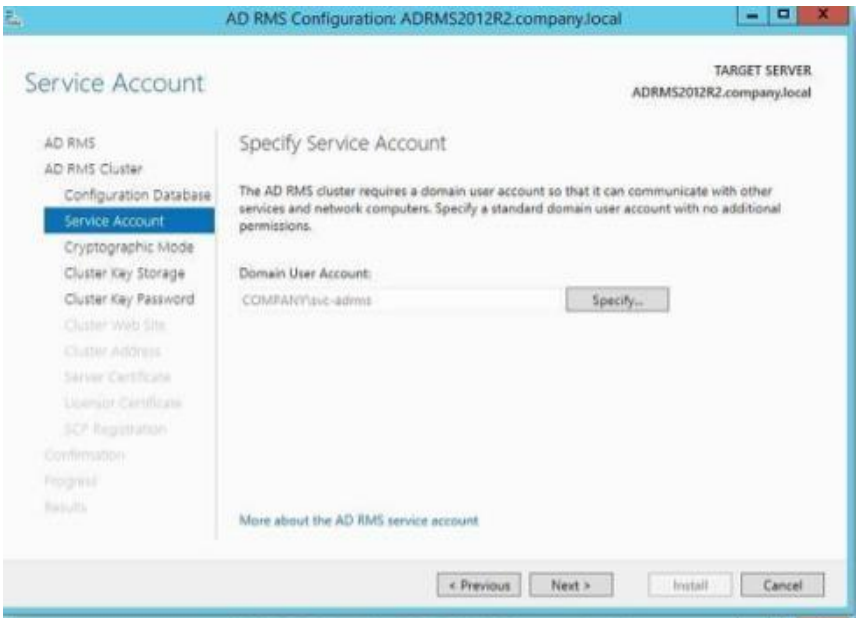


Рис. 63

7. В качестве базы данных RMS будем использовать внутреннюю базу данных Windows (**Use Windows Internal Database on this server).**



8. Затем укажем созданную ранее сервисную учетную запись (svc-adrms), используемый криптографический алгоритм, метод хранения ключа кластера RMS и его пароль.


AD RMS Configuration: ADRMS2012R2.company.local
Service Account
TARGET SERVER
ADRMS2012R2.company.local
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Specify Service Account
The AD RMS cluster requires a domain user account so that it can communicate with other services and network computers. Specify a standard domain user account with no additional permissions.
Domain User Account:
COMPANY\svc-adrms
Specify...
More about the AD RMS service account
< Previous
Next >
Install
Cancel


AD RMS Configuration: ADRMS2012R2.company.local
Cryptographic Mode
TARGET SERVER
ADRMS2012R2.company.local
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Specify Cryptographic Mode
AD RMS can operate under two modes which differ on the basis of the cryptographic key length and the strength of signature hashes. Cryptographic mode 2 is recommended for new cluster deployments where you have ensured that all AD RMS client computers have been updated to support it. As cryptographic mode 2 cannot be undone, if you are unsure of full support within this cluster or any other clusters that it will share a trusted user domain (TUD) relationship with, select cryptographic mode 1 instead.
Cryptographic Mode 2 (RSA 2048-bit keys/SHA-256 hashes)
Cryptographic Mode 1 (RSA 1024-bit keys/SHA-1 hashes)
More about the AD RMS cryptographic mode
< Previous
Next >
Install
Cancel

9. Задайте веб-адрес кластера AD RMS, к которому будут обращаться RMS-клиенты (рекомендуется использовать защищенное SSL соединение).

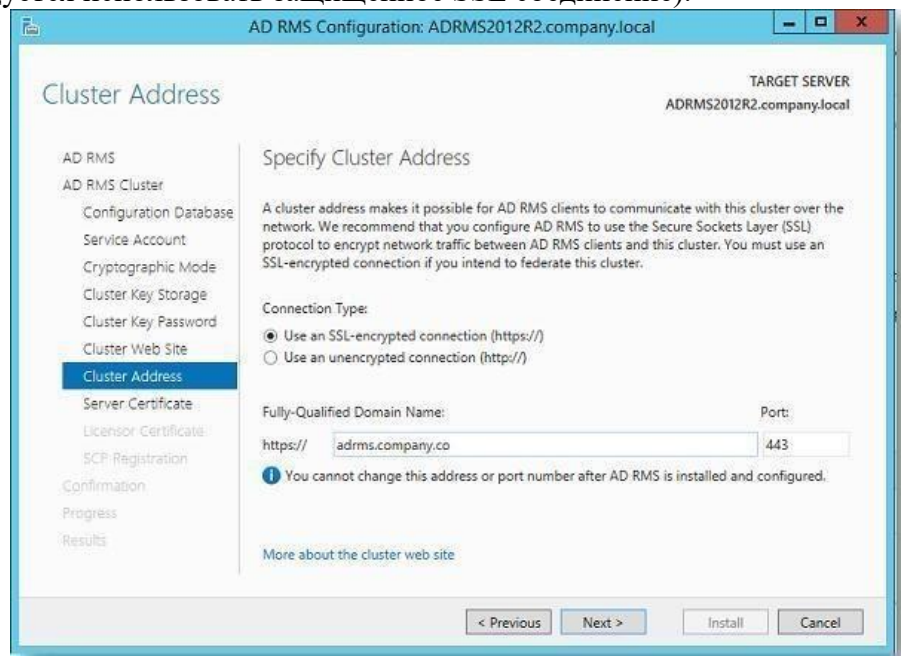
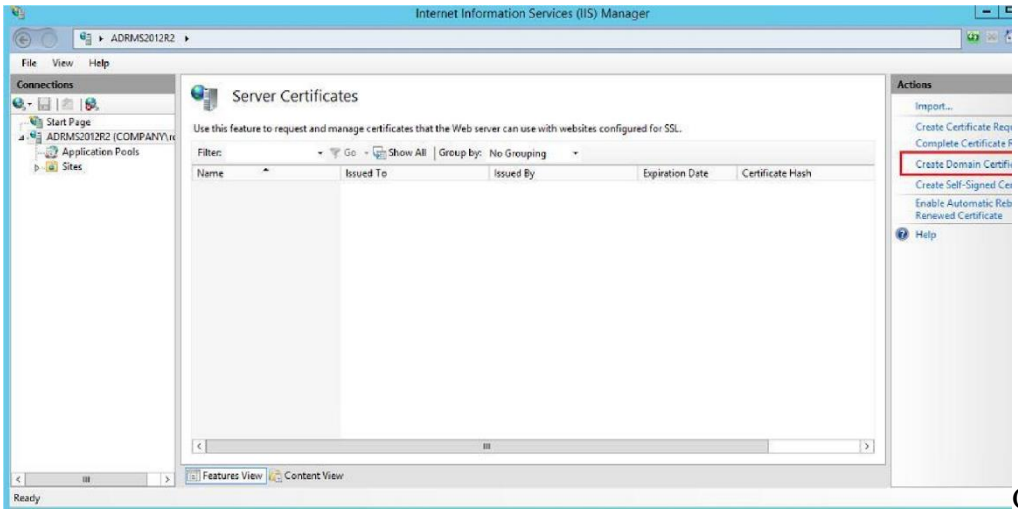


Рис. 64

Не закрывайте мастер настройки AD RMS!

10. Установка SSL-сертификата на сайт IIS. Сертификат может быть самоподписаным (в дальнейшем его нужно будет добавить в доверенные на всех клиентах), или выданным корпоративным/внешним центром сертификации (CA). Сформируем сертификат с помощью уже имеющегося корпоративного CA. Для этого откройте консоль IIS Manager (**inetmgr**) и перейдите в раздел Server Certificates. В правом столбце щелкните по ссылке **Create Domain Certificate** (создать сертификат домена).



Сгенерируйте новый сертификат с помощью мастера и привяжите его к серверу IIS.

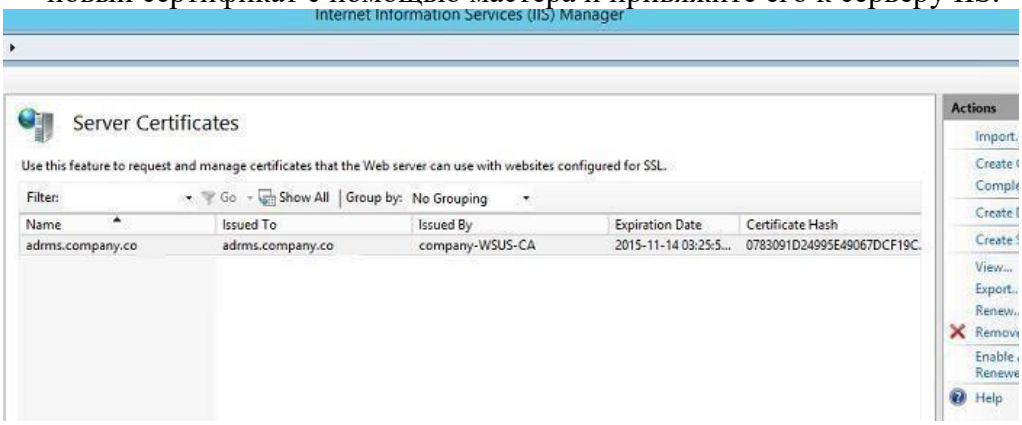


Рис. 65

11. Вернитесь в окно настройки роли AD RMS и выберите сертификат, который планируется использовать для шифрования трафика AD RMS.

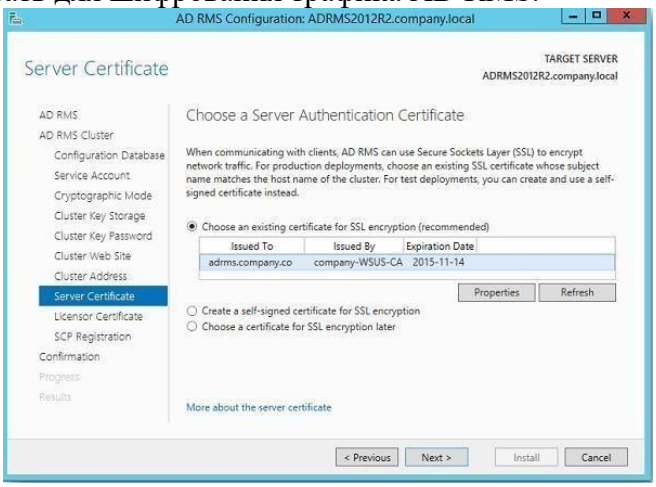


Рис. 66

12. Отметьте, что точку SCP нужно зарегистрировать в AD немедленно (**Register the SCP now**).

Примечание. Для регистрации точки SCP в Active Directory нужно обладать правами Enterprise Admins.

13. Запустите консоль ADRMS.

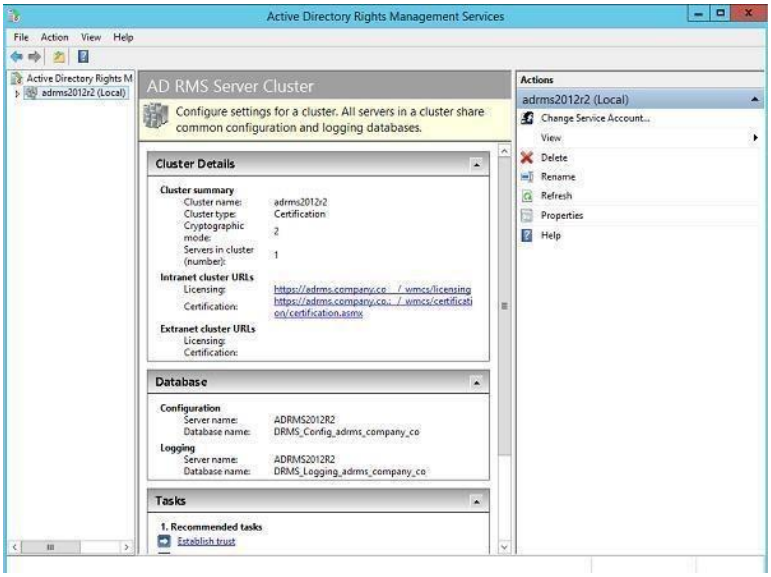


Рис. 67

Для примера создадим новый шаблон политики RMS. Предположим мы хотим создать шаблон RMS, позволяющий владельцу документа разрешить всем просмотр защищенных этим шаблоном писем без прав редактирования/пересылки. Для этого перейдем в раздел **Rights Policy Templates** и щелкнем по кнопке **Create Distributed Rights Policy Template**.

Нажав кнопку **Add**, добавим языки, поддерживаемые этим шаблоном и имя политики для каждого из языков.

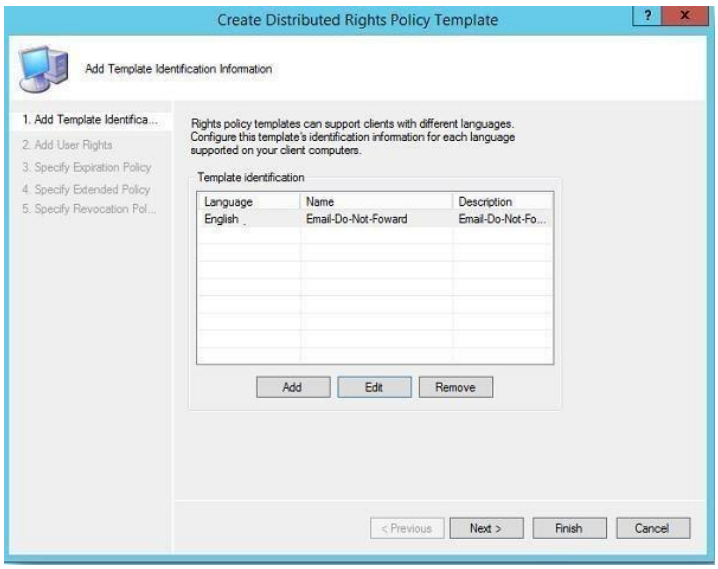


Рис. 68

14. Укажем, что все (**Anyone**) могут просматривать (**View**) содержимое защищенного автором документа.

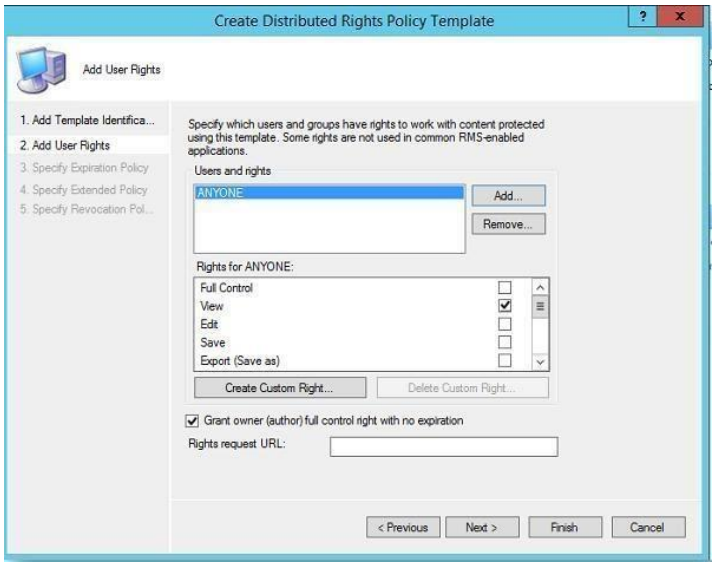


Рис. 69

15. Укажем, что срок окончания действия политики защиты не ограничен (**Never expires**).

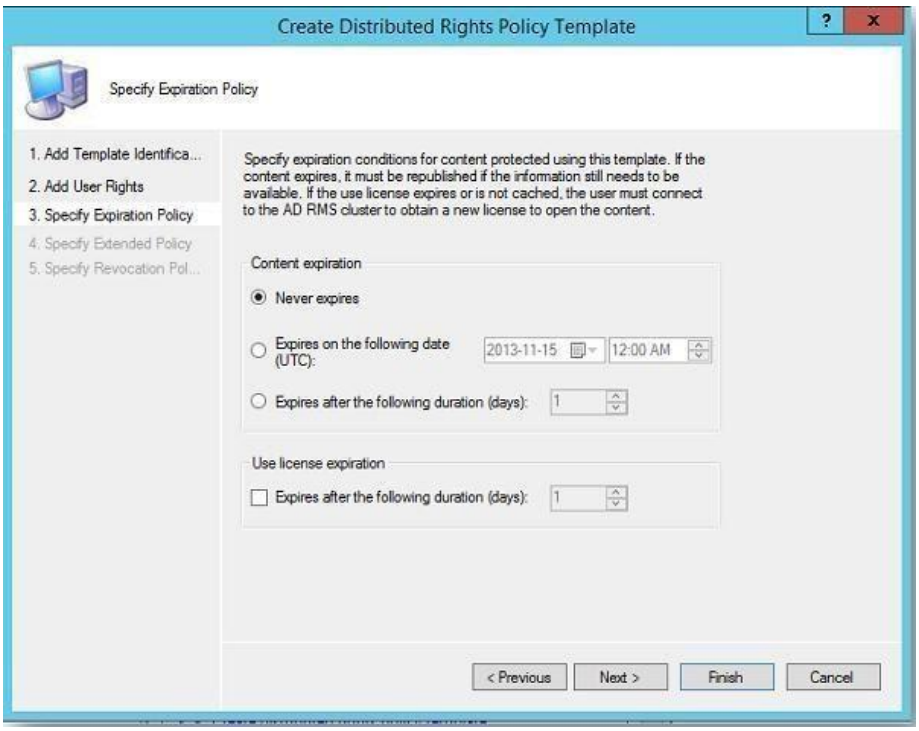


Рис. 70

16. На следующем шаге укажем, что защищенное содержимое можно просматривать в браузере с помощью расширений IE (**Enable users to view protected content using a browser add-on**).

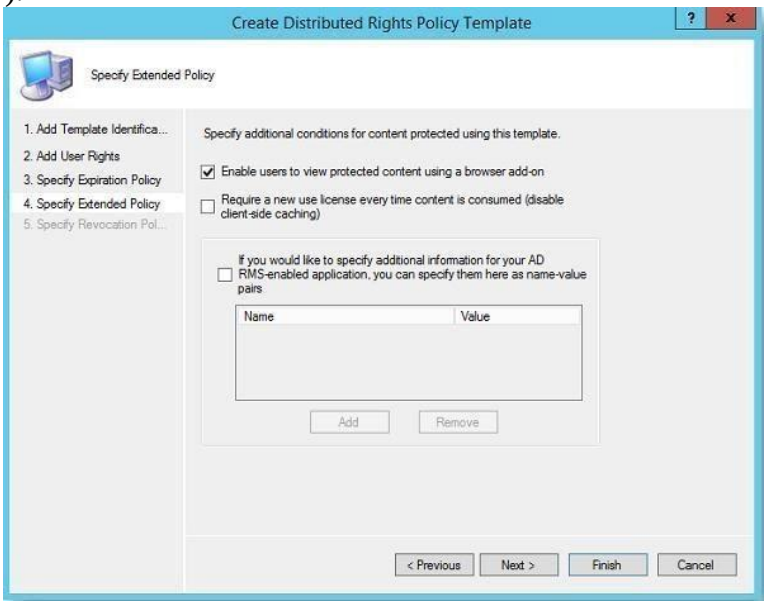
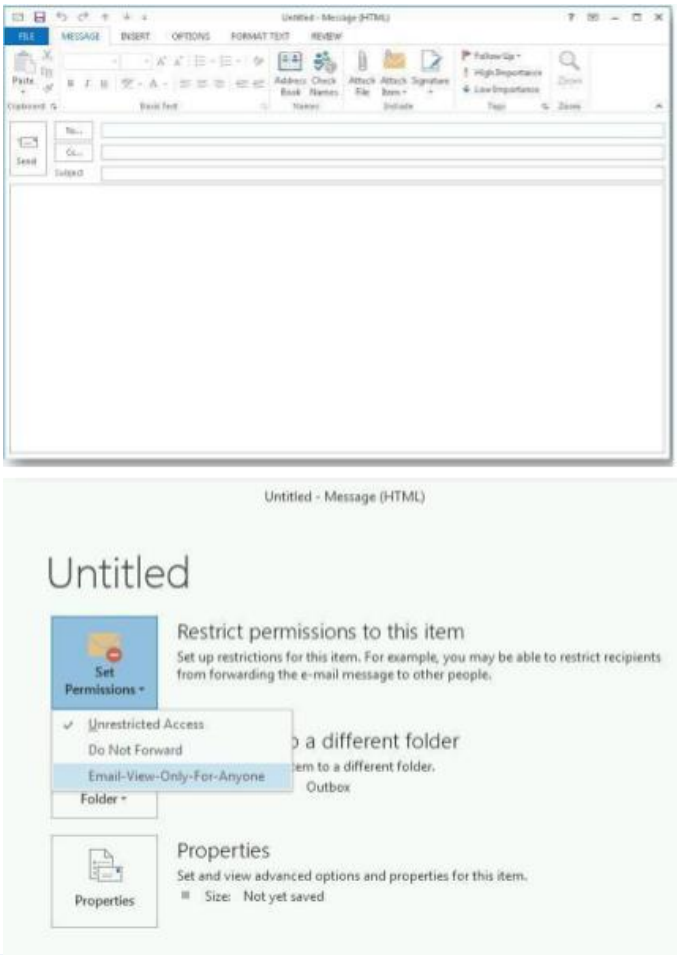


Рис. 71

Протестируем созданный шаблон RMS в **Outlook Web App**, для чего создадим новое пустое письмо, в свойствах которого нужно щелкнуть по кнопке **Set Permissions**. В выпадающем меню выберите имя шаблона (**Email-View-Onl-For-Anyone**).



Примечание. Если список шаблонов RMS открывается с ошибкой, или созданные шаблоны отсутствуют, проверьте что адрес сайта AD RMS относится к зоне Local Intranet /Trusted zone , а текущий пользователь может авторизоваться на IIS сервера RMS.

Отправим письмо, защищенное RMS, другому пользователю.

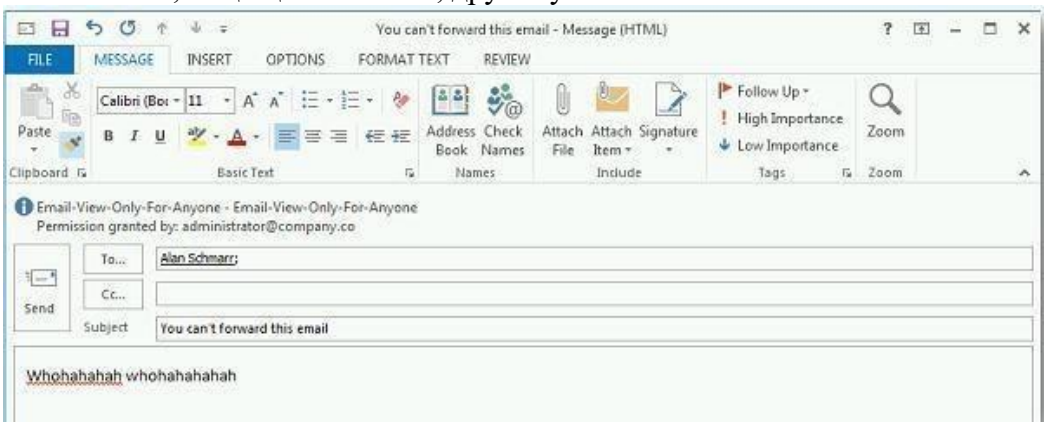


Рис. 72

17. Посмотрим, как выглядит защищенное письмо в ящике получателя.

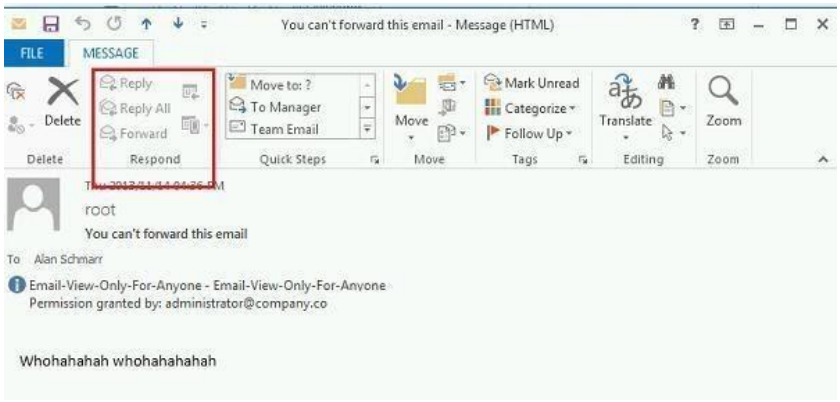


Рис. 73

Как мы видим, кнопки Ответить и Переслать недоступны, а в информационной панели указан используемый шаблон защиты документа и его владелец.

Сделайте скриншоты (фотографии) процесса настройки ADRMS и вставьте в отчёт.

2.7. Практическая работа № 7
Применение защиты доступа к сети

Задание:

1. Настраиваем доменную аутентификацию на сетевом оборудовании

При обслуживании больших сетей системные администраторы часто сталкиваются с проблемами аутентификации на сетевом оборудовании. В частности, довольно сложно организовать нормальную работу нескольких сетевых администраторов под индивидуальными учетными записями на большом количестве оборудования (приходится вести и поддерживать в актуальном состоянии базу локальных учетных записей на каждом устройстве). Логичным решение было бы использовать для авторизации уже существующей базы учетных записей — Active Directory. В этой статье мы разберемся, как настроить **доменную (Active Directory) аутентификацию на активном сетевом оборудовании** (коммутаторы, маршрутизаторы).

Не все сетевое оборудование популярных вендоров (CISCO, HP, Huawei) поддерживает функционал для непосредственного обращения к каталогу LDAP, и такое решение не будет универсальным. Для решения нашей задачи подойдет протокол **AAA (Authentication Authorization and Accounting)**, фактически ставший стандартом де-факто для сетевого оборудования. Клиент AAA (сетевое устройство) отправляет данные авторизующегося пользователя на сервер **RADIUS** и на основе его ответа принимает решение о предоставлении / отказе доступа.

Протокол **Remote Authentication Dial In User Service (RADIUS)** в Windows Server 2012 R2 включен в роль **NPS (Network Policy Server)**. В первой части статьи мы установим и настроим роль Network Policy Server, а во второй покажем типовые конфигурации сетевого устройств с поддержкой RADUIS на примере **коммутаторов HP Procurve** и **оборудования Cisco**.

2. Установка и настройка сервера с ролью Network Policy Server

Как правило, сервер с ролью NPS рекомендуется устанавливать на выделенном сервере (не рекомендуется размещать эту роль на контроллере домена). В данном примере роль NPS мы будем устанавливать на сервере с Windows Server 2012 R2.

Откройте консоль **Server Manager** и установите роль **Network Policy Server** (находится в разделе **Network Policy and Access Services**).

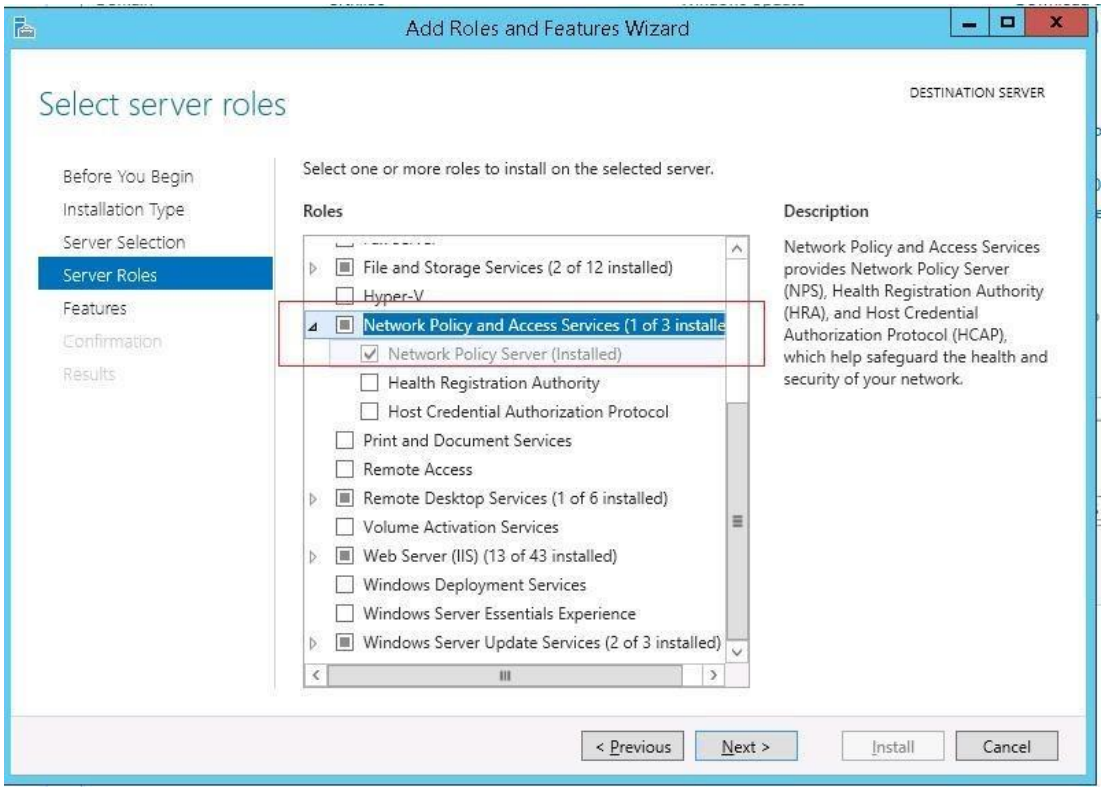


Рис. 104

После окончания установки запустите mmc-консоль управления Network Policy Server. Нас интересуют три следующих раздела консоли:

1. **RADIUS Clients** — содержит список устройств, которые могут аутентифицироваться на сервере
2. **Connection Request Policies** – определяет типы устройств, которые могут аутентифицироваться
3. **Network Polices** – правила аутентификации

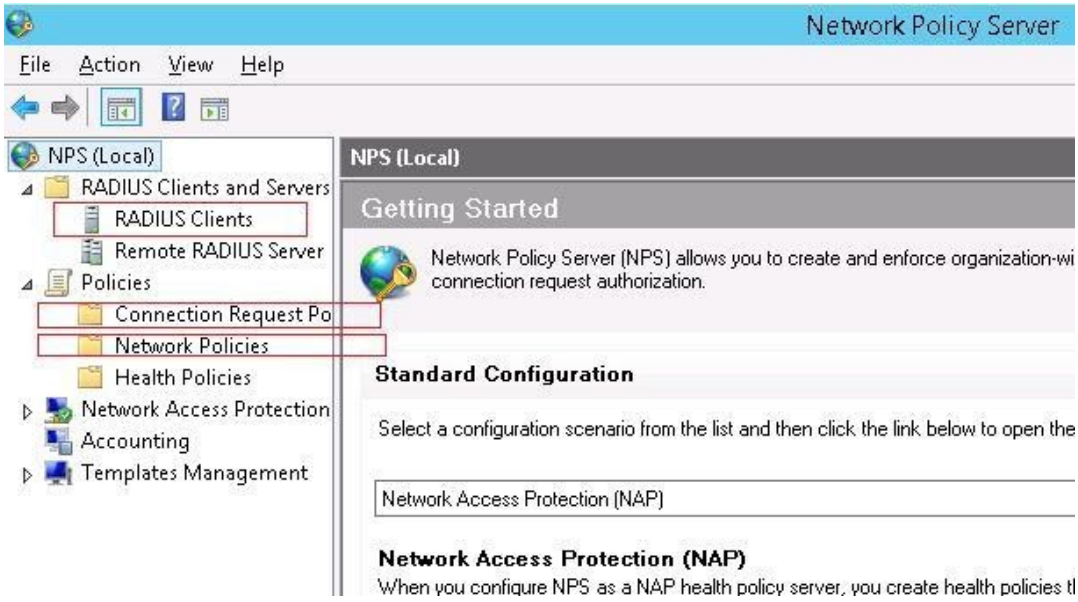


Рис. 105

Добавим нового клиента RADIUS (это будет коммутатор HP ProCurve Switch 5400zl), щелкнув ПКМ по разделу **RADIUS Clients** и выбрав **New**. Укажем:

- **Friendly Name**:sw-HP-5400-1

- **Address (IP or DNS)**: 10.10.10.2
- **Shared secret** (пароль/секретный ключ): пароль можно указать вручную (он должен быть достаточно сложным), либо сгенерировать с помощью специальной кнопки (сгенерированный пароль необходимо скопировать, т.к. в дальнейшем его придется указать на сетевом устройстве).

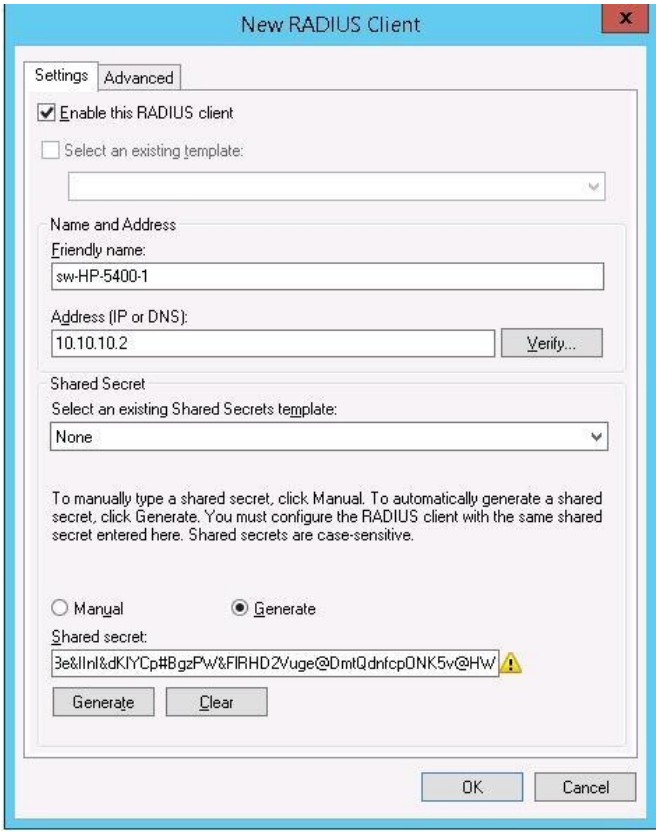


Рис. 106

Отключим стандартную политику (**Use Windows authentication for all users**) в разделе Connection Request Policies, щелкнув по ней ПКМ и выбрав **Disable**.

Создадим новую политику с именем **Network-Switches-AAA** и нажимаем далее. В разделе **Condition** создадим новое условие. Ищем раздел **RADIUS Client Properites** и выбираем **Client Friendly Name**.

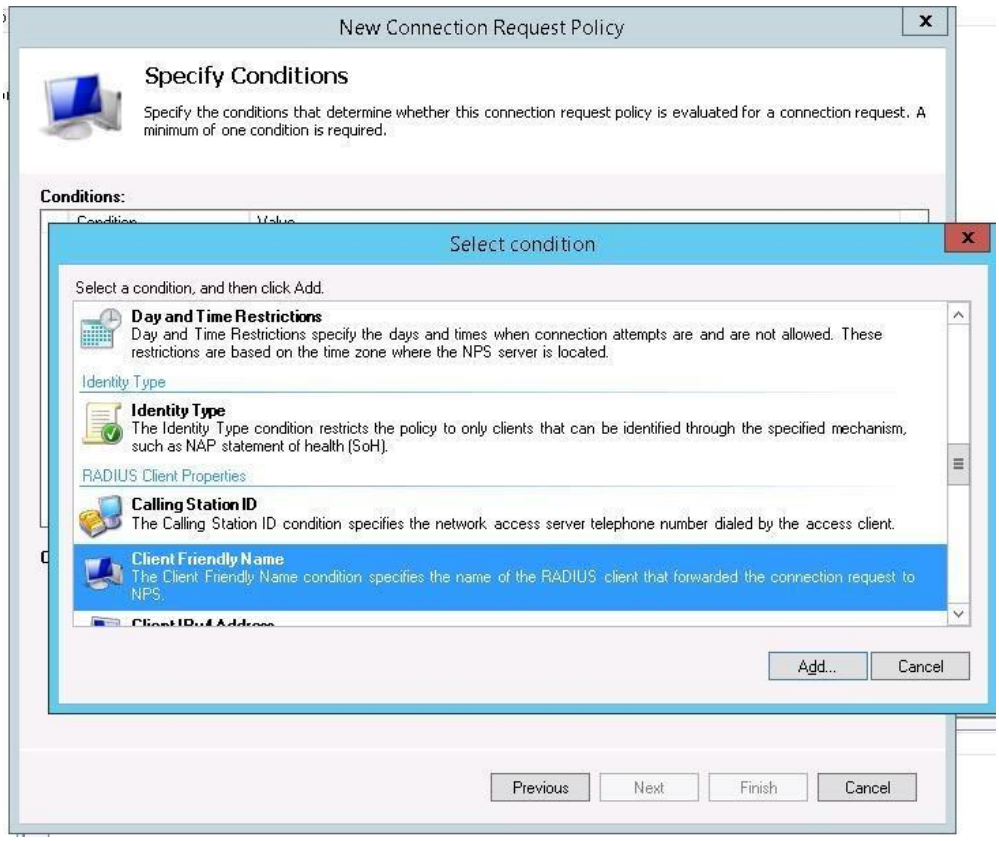


Рис. 107

В качестве значения укажем **sw-?**. Т.е. условие будет применяться для всех клиентов RADIUS, начинающийся с символов :"sw-". Жмем Next->Next-> Next, соглашаясь со всеми стандартными настройками.

Далее в разделе **Network Policies** создадим новую политику аутентификации. Укажите ее имя, например **Network Switch Auth Policy for Network Admins**. Создадим два условия: в первом условии **Windows Groups**, укажем доменную группу, члены которой могут аутентифицироваться (учетные записи сетевых администраторов в нашем примере включены в группу AD Network Admins) Второе условие **Authentication Type**, выбрав в качестве протокола аутентификации PAP.

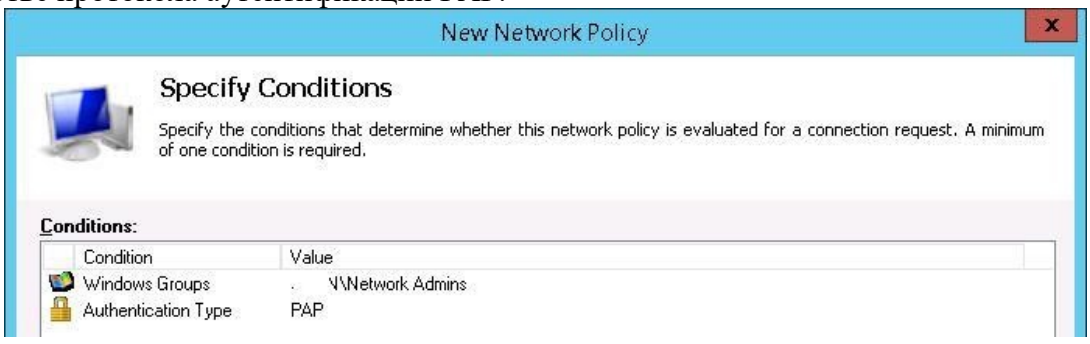


Рис. 108

Далее в окне Configure Authentication Methods снимаем галки со всех типов аутентификации, кроме **Unencrypted authentication (PAP. SPAP)**.

В окне **Configure Settings** изменим значение атрибута **Service-Type** на **Administrative**.

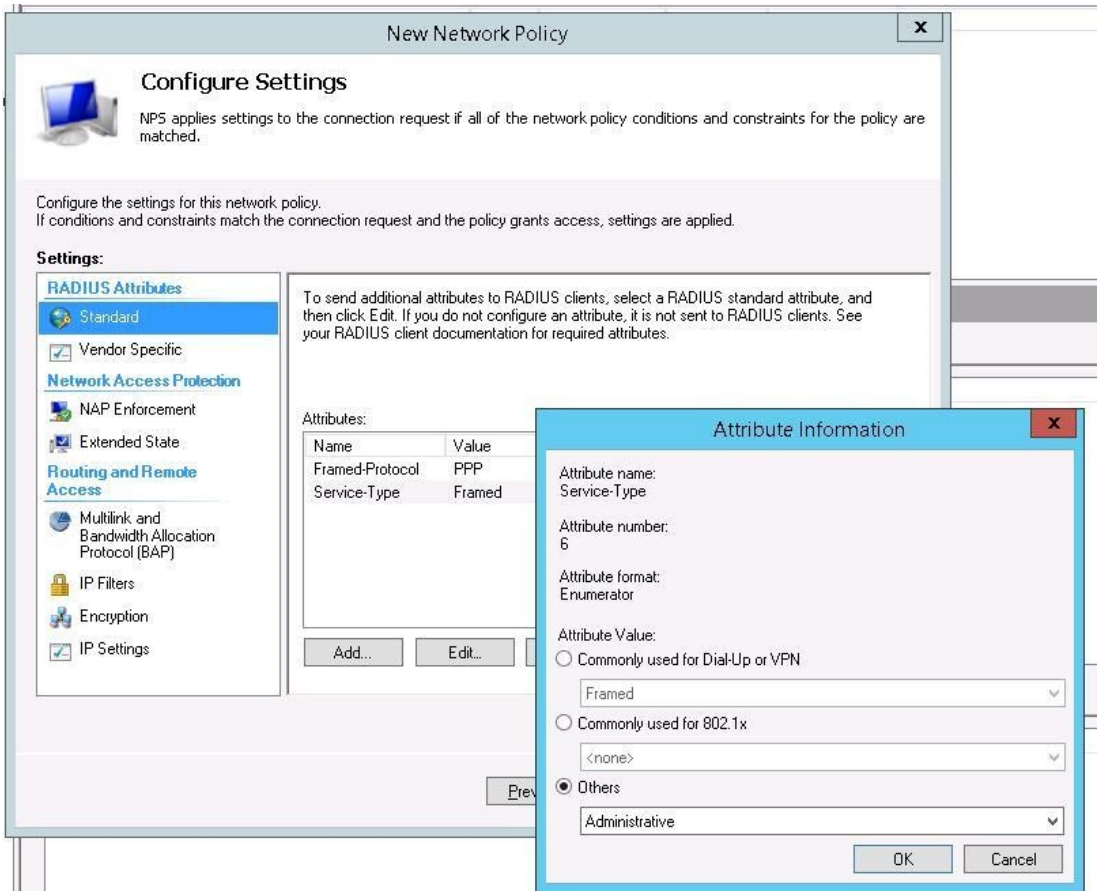


Рис. 109

В остальных случаях соглашаемся со стандартными настройками и завершаем работу с мастером.

И, напоследок, переместим новую политику на первое место в списке политик.

Рис. 110

3. Настройка сетевого оборудования для работы с сервером RADUIS

Осталось настроить наше сетевое оборудование для работы с сервером Radius. Подключимся к нашему коммутатору HP ProCurve Switch 5400 и внесем следующе изменение в его конфигурацию (измените ip адрес сервера Raduis и пароль на свои).

```
aaa authentication console enable radius local
aaa authentication telnet login radius local
aaa authentication telnet enable radius local
aaa authentication ssh login radius local

aaa authentication ssh enable radius local
aaa authentication login privilege-mode
radius-server key YOUR-SECRET-KEY
radius-server host 10.10.10.44 YOUR-SECRET-KEY auth-port 1645 acct-port 1646
```

```
radius-server host 10.10.10.44 auth-port 1645
radius-server host 10.10.10.44 acct-port 1646
```

Совет. Если в целях безопасности вы запретили подключаться к сетевому оборудованию через telnet, эти строки нужно удалить из конфига:

```
aaa authentication telnet login radius local
aaa authentication telnet enable radius local
```

Не закрывая консольное окно коммутатора (**это важно!**, иначе, если что-то пойдет не так, вы более не сможете подключиться к своему коммутатору), откройте вторую telnet-сессию. Должно появиться новое окно авторизации, в котором будет предложено указать имя и пароль учетной записи. Попробуйте указать данные своей учетной записи в AD (она должна входить в группу Network Admins). Если подключение установлено – вы все сделали правильно!

Рис. 111

Для коммутатора Cisco конфигурация, предполагающая использование доменных учетных записей для аутентификации и авторизации, может выглядеть так:

Примечание. В зависимости от модели сетевого оборудования Cisco и версии IOS конфигурация может несколько отличаться.

```
aaa new-model
radius-server host 10.10.10.44 auth-port 1645 acct-port 1646 key YOUR-SECRET-KEY
aaa authentication login default group radius local
aaa authorization exec default group radius local
ip radius source-interface Vlan421
line con 0
line vty 0 4
line vty 5 15
```

Примечание. В такой конфигурации для аутентификации сначала используется сервер RADIUS, а если он не доступен – локальная учетная запись.

Для Cisco ASA конфигурация будет выглядеть так:

```
aaa-server RADIUS protocol radius
```

```
aaa-server RADIUS host 10.10.10.44 key YOUR-SECRET-KEY
radius-common-pw YOUR-SECRET-KEY
aaa authentication telnet console RADIUS LOCAL
aaa authentication ssh console RADIUS LOCAL
aaa authentication http console RADIUS LOCAL
aaa authentication http console RADIUS LOCAL
```

Сделайте скриншоты (фотографии) процесса установки, настройки и устранения неполадок роли Сервер Сетевой политики и вставьте в отчёт.

2.8. Практическая работа № 8
Внедрение технологии DirectAccess с помощью мастера начальной настройки

Задание:

1. Установка роли Remote Access

Запустим консоль Server Manager и с помощью мастера Add Roles and Features установим роль Remote Access.

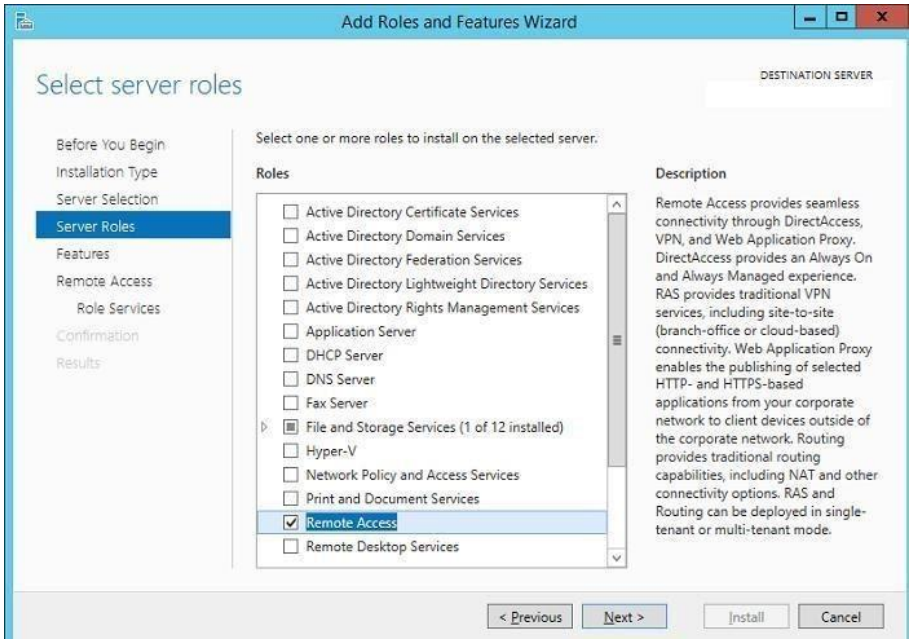


Рис. 112

В составе роли Remote Access нужно установить службу **DirectAccess and VPN (RAS).**

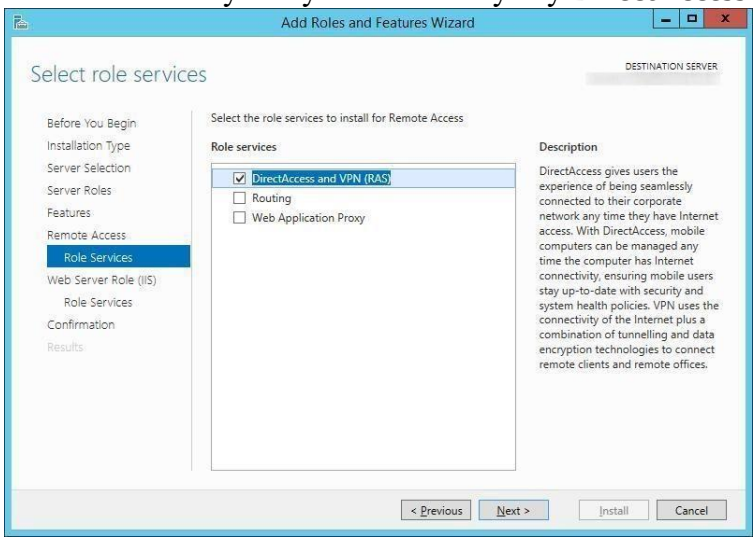


Рис. 113

Все остальные зависимости оставляем по умолчанию.

2. Настройка службы Direct Access в Windows Server 2012 R2

После окончания установки службы Remote Access, откройте оснастку **Tools -> Remote Access Management**.

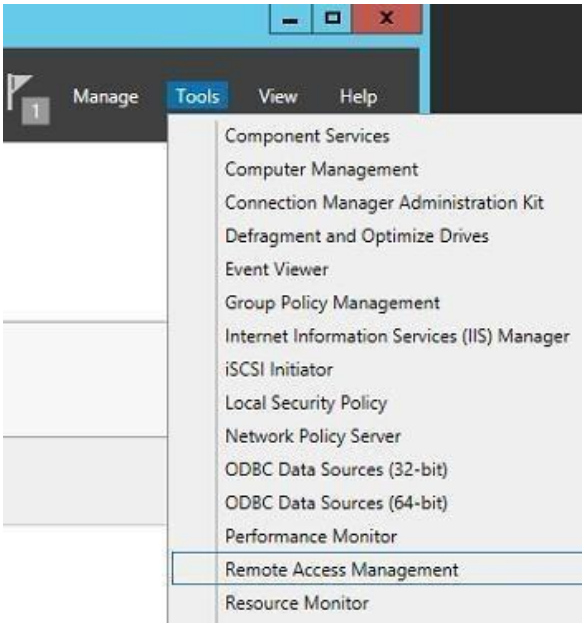


Рис. 114

Запустится мастер настройки роли удаленного доступа. Укажем, что нам нужно установить только роль DA — **Deploy DirectAccess only.**

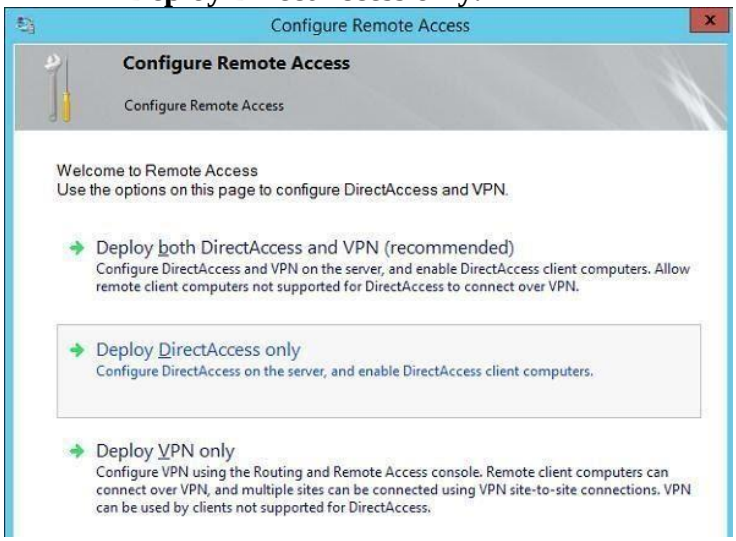


Рис. 115

После этого должно открыться окно, в правой половине которого в графическом виде показаны четыре этапа (Step 1 – 4) настройки службы DA.

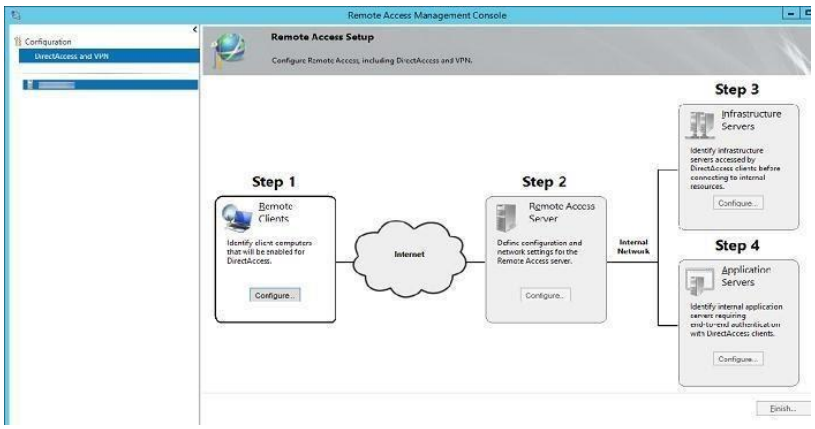


Рис. 116

Первый этап (Step 1: Remote Clients).

Укажем, что мы разворачиваем полноценный DirectAccess сервер с возможностью доступа клиентов и их удаленного управления **Deploy full DirectAccess for client access and remote management**.

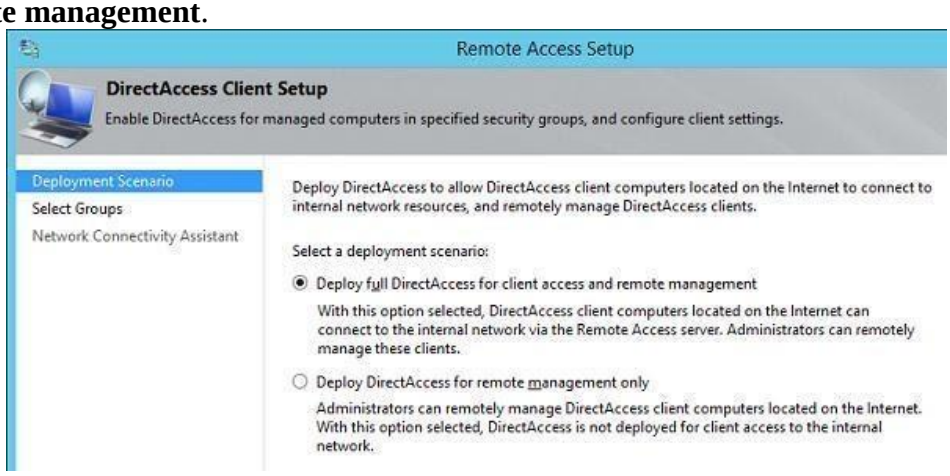


Рис. 117

Далее, нажав кнопкуAdd нужно указать группы безопасности AD, в которой будут находиться учетные записи компьютеров, которым разрешено подключаться к корпоративной сети через Direct Access (в нашем примере это группа DirectAccessComputers).

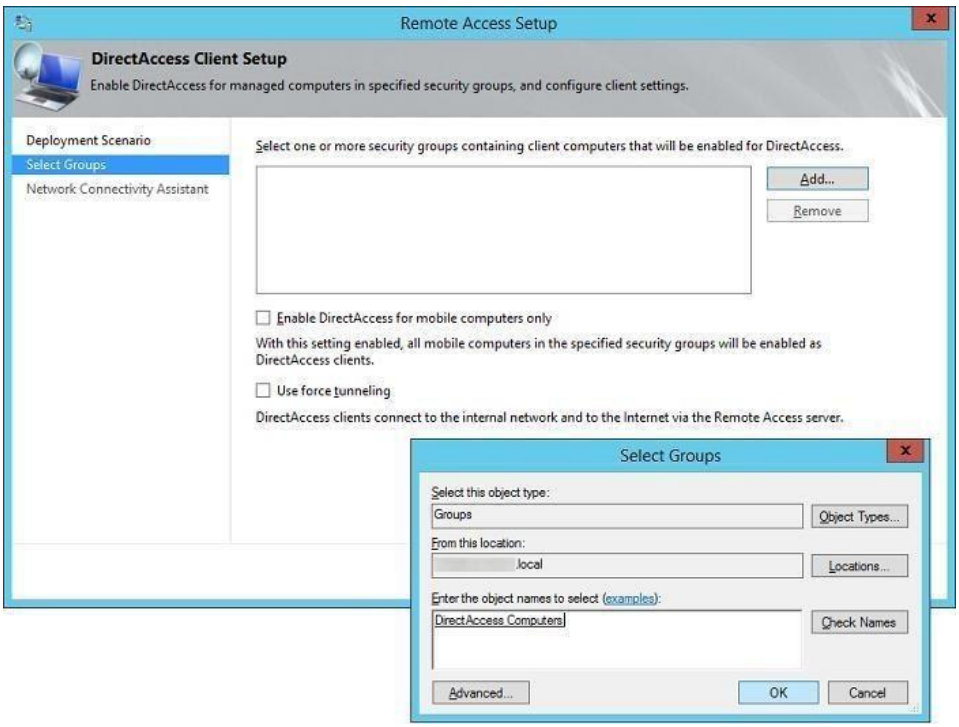


Рис. 118

Примечание. Опция Enable DirectAccess for mobile only – позволяет ограничить подключение через DA только для мобильных устройств (ноутбуки, планшеты). Реализуется функция за счет опроса клиентов по WMI. Опция Use force tunneling – означает, что удаленные клиенты при доступе к любым удаленным ресурсам (в том числе обычным вебсайтам) всегда использовать сервера DA (т.е. весь внешний трафик клиента проходит через корпоративный шлюз).

Следующий шаг – нужно указать список внутренних сетевых имен или URLадресов, с помощью которых клиент может проверить (Ping или HTTP запрос), что он подключен к корпоративной сети. Здесь же можно указать контактный email службы helpdesk и наименование подключения DirectAccess (так оно будет отображаться в сетевых подключениях на клиенте). В случае необходимости можно включить опцию Allow DirectAccess clients to use local name resolution, позволяющую разрешить клиенту использовать внутренние DNS-сервера компании (адреса DNS серверов могут получаться по DHCP).

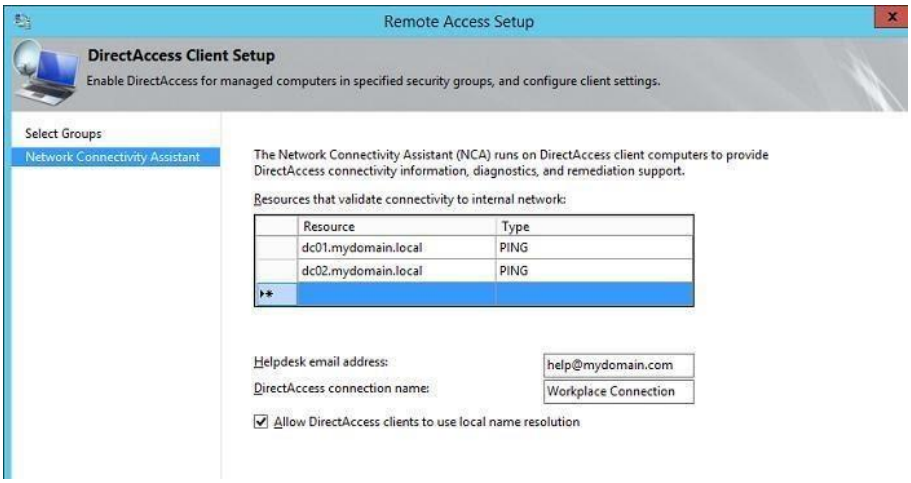


Рис. 119

-

Второй этап (Step 2: Remote Access Server)

Следующий шаг — настройка сервера Remote Access. Указываем, что наш сервер удаленного доступа представляет собой конфигурацию с двумя сетевыми картами — **Behind an edge device (with two network adapters)**, одна их которых находится в корпоративной сети, а вторая подключена напрямую в Internet или DMZ-подсеть. Здесь же нужно указать внешнее DNS имя или IP адрес в Интернете (именно с этого адреса пробрасывается 443 порт на внешний интерфейс сервера DirectAccess), к которому должны подключаться клиенты DA.

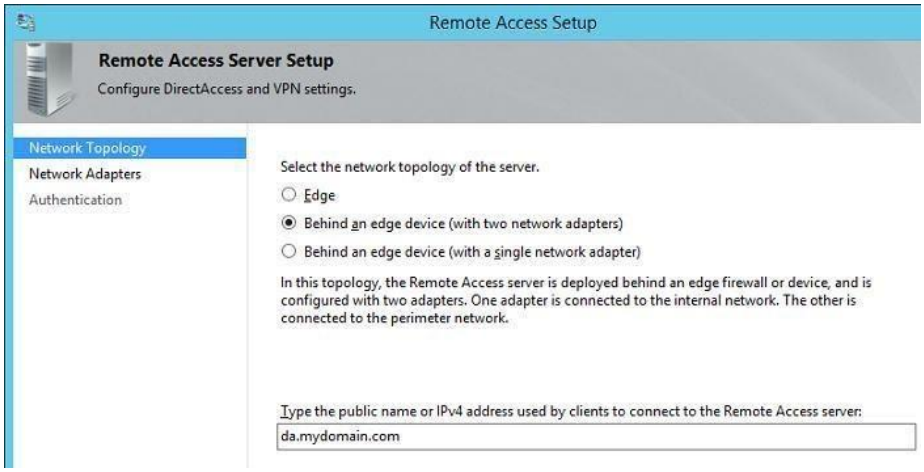


Рис. 120

Затем нужно указать какая сетевая карта будет считаться внутренней (**Internal – LAN)**, а какая внешней (**External – DMZ).**

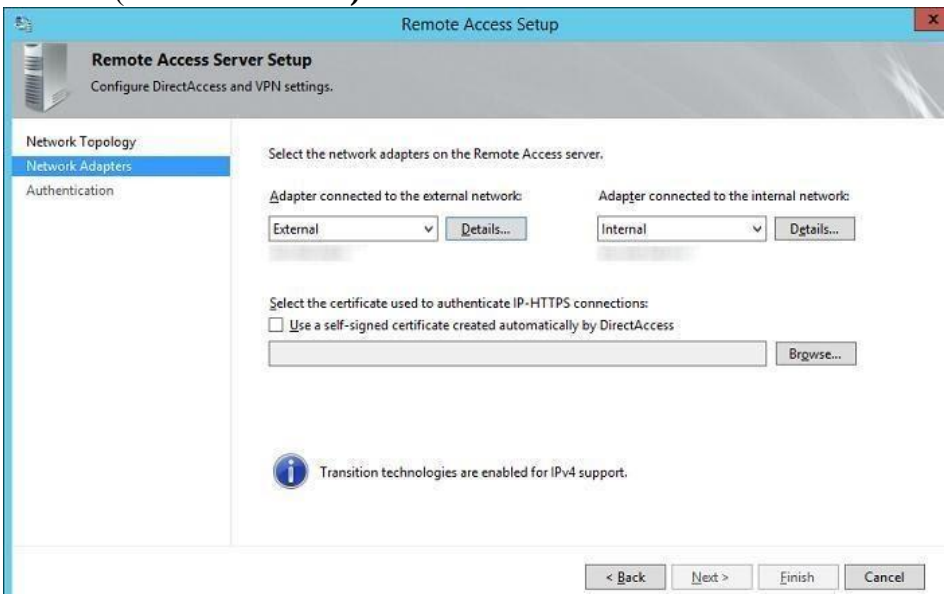


Рис. 121

Свернем пока мастер настройки сервера Direct Access и сгенерируем сертификат сервера DA. Для этого создадим новую оснастку mmc, в которую добавим консоль **Certificates,** управляющую сертификатами локального компьютера (**Computer Account**)

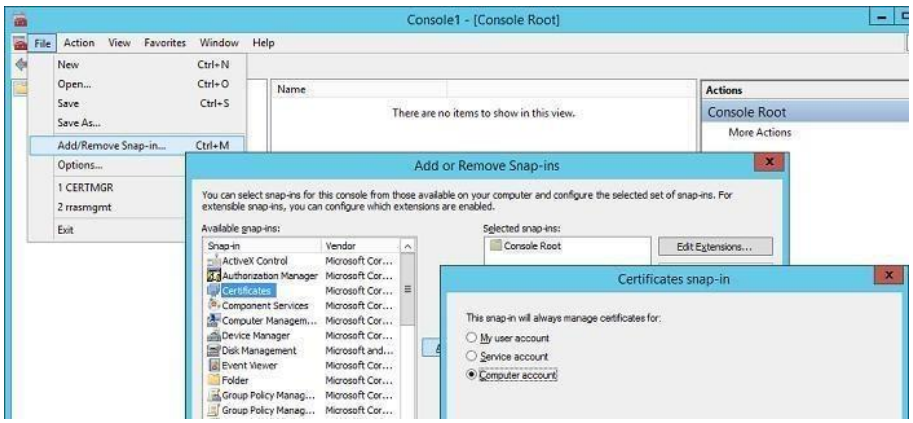


Рис. 122

В консоли управления сертификатами запросим новый персональный сертификат, щелкнув ПКМ по разделу **Certificates (Local Computer) -> Personal -> Certificates** и выбрав в меню **All Tasks-> Request New Certificate**

Запросим сертификат через политику **Active Directory Enrollment Policy**. Нас интересует сертификат на основе шаблона **WebServers**.

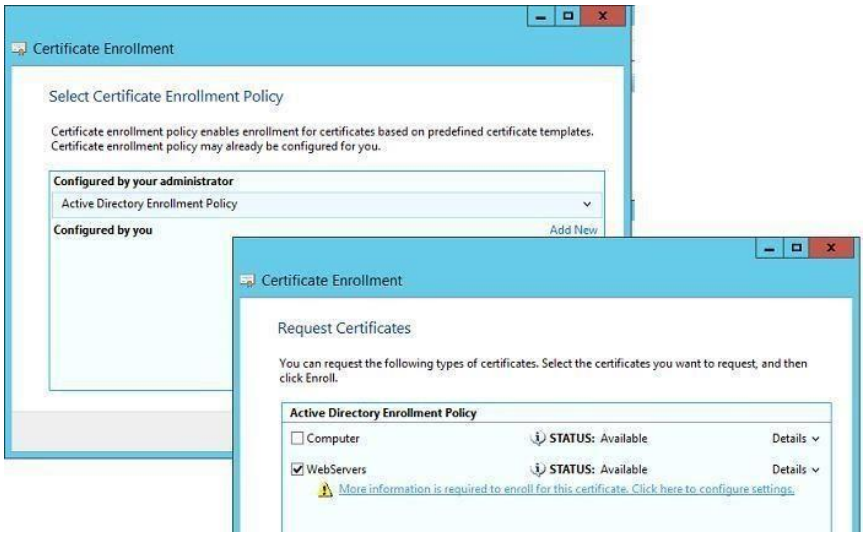


Рис. 123

В настройках запроса нового сертификата на вкладке **Subject** заполним поля, идентифицирующие нашу компанию, а на вкладке Private Key укажем, что закрытый ключ сертификата можно экспортировать (**Make private key exportable**).

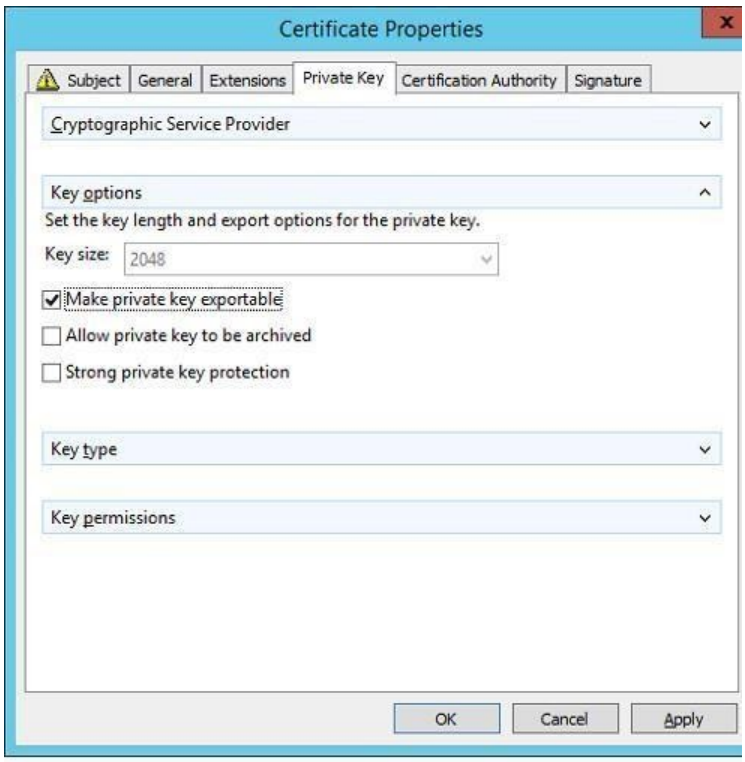


Рис. 124

Сохраним изменения и запросим новый сертификат у CA.

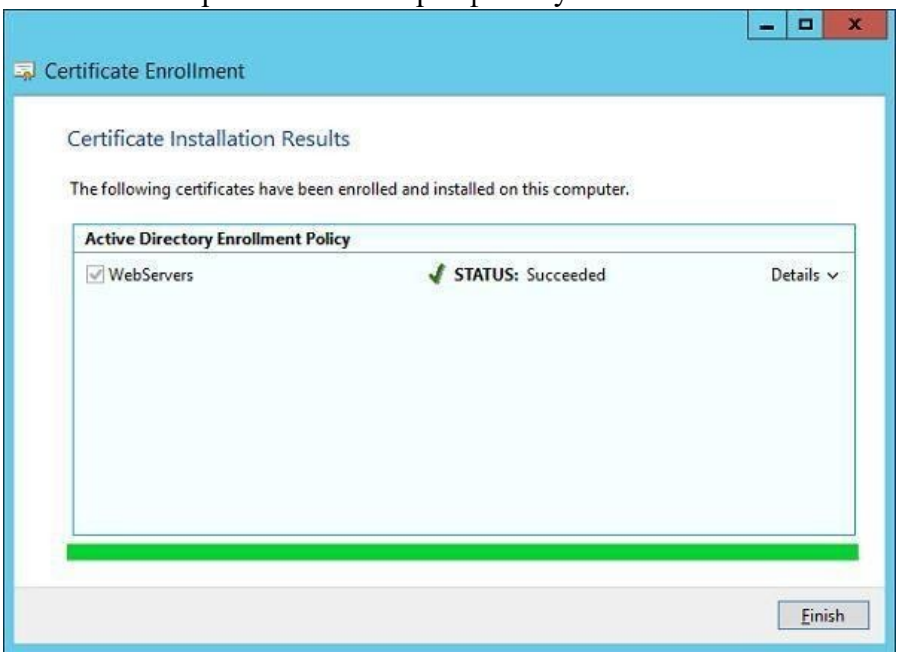


Рис. 125

Вернемся в окно настроек сервера DirectAccess и, нажав кнопку Browse, выберем сгенерированный сертификат.

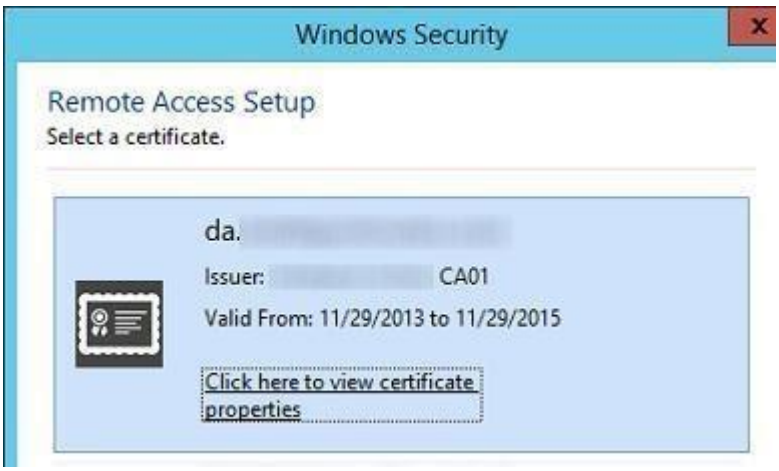


Рис. 126

На следующем шаге мастера выберем способ аутентификации клиентов Direct Access. Укажем, что используется аутентификация по логину и паролю AD (Active Directory credentials – username/password). Отметим чекбокс Use computer certificates (Использовать сертификаты компьютеров) и Use an intermediate certificate. Нажав кнопку Browse, нужно указать центр сертификации, который будет отвечать за выдачу сертификатов клиентов.

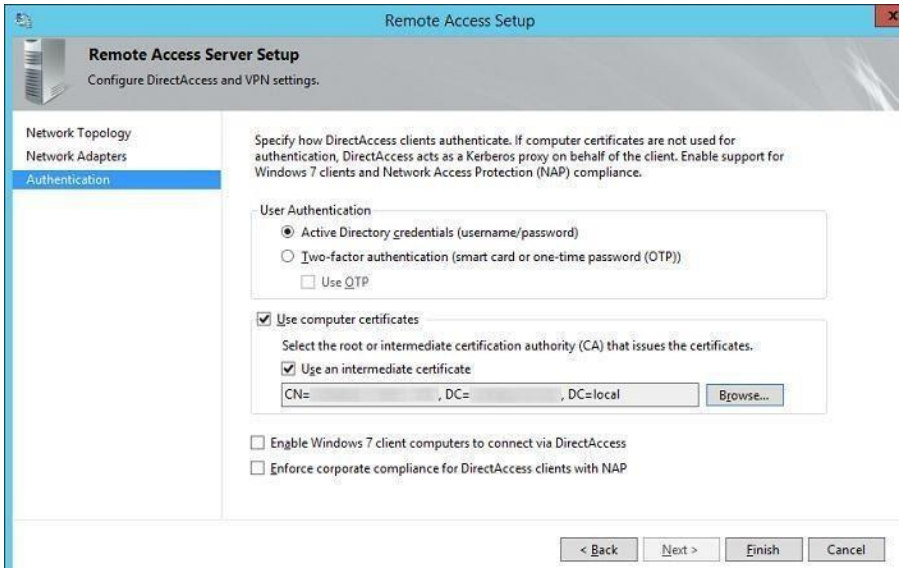


Рис. 127

Третий этап (Step 3: Infrastructure Servers)

Третий этап – настройка инфраструктурных серверов. Нам будет предложено указать адрес сервера Network Location Server, находящегося внутри корпоративной сети. **Network Location Server** — это сервер, с помощью которого клиент может определить, что он находится во внутренней сети организации, т.е. не требуется использовать DA для подключения. NLS – сервером может быт любой внутренний веб-сервер (даже с дефолтной страничкой IIS), основное требование – сервер NLS не должен быть доступен снаружи корпоративной сети.

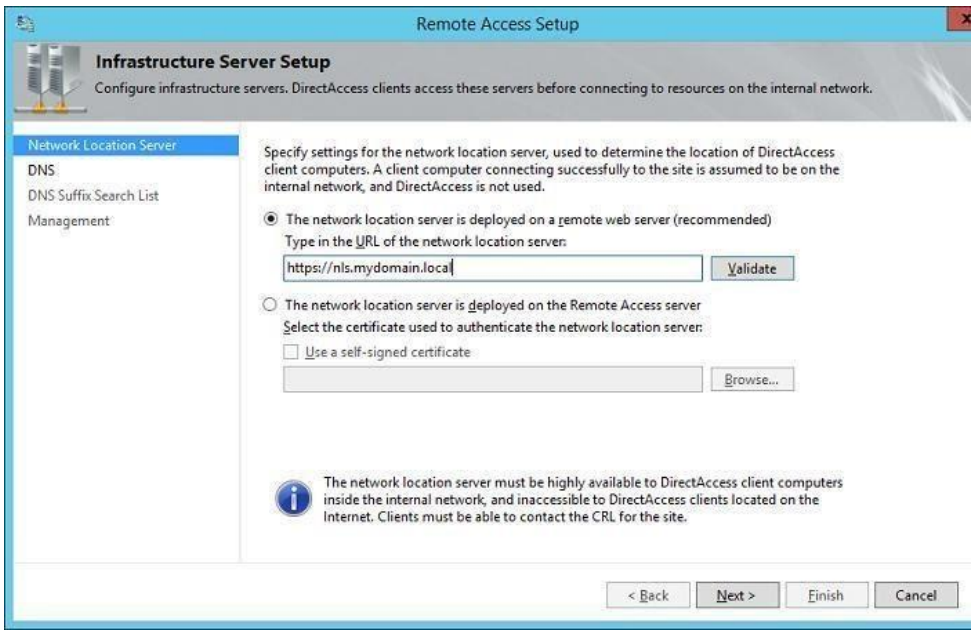


Рис. 128

Далее укажем список DNS серверов для разрешения имен клиентами. Рекомендуется оставить опцию **Use local name resolution if the name does not exist in DNS or DNS servers are unreachable when the client computer is on a private network (recommended).**

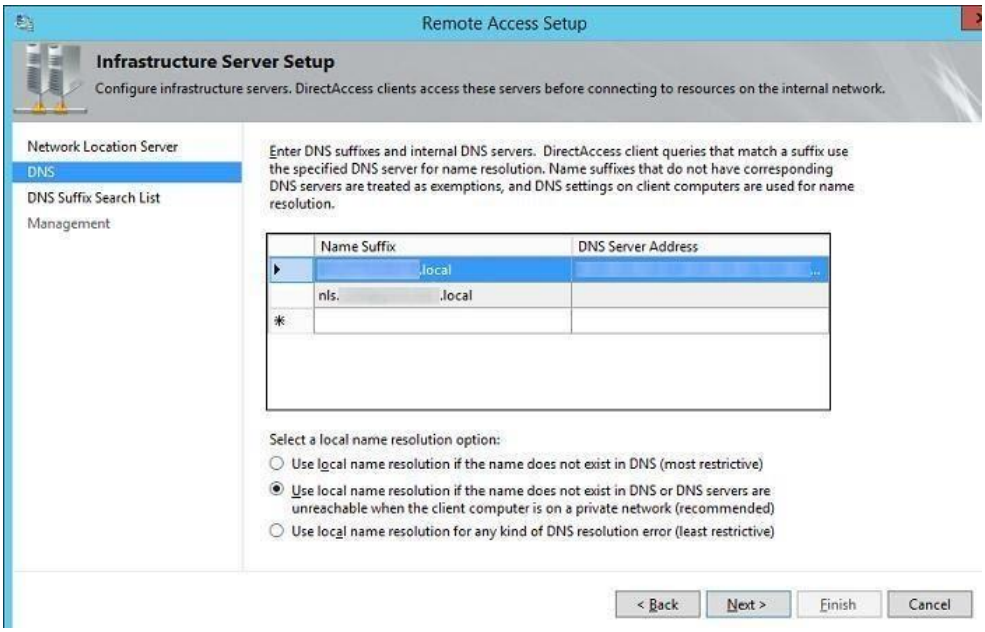


Рис. 129

Затем укажем DNS-суффиксы внутренних доменов в порядке приоритета их использования.

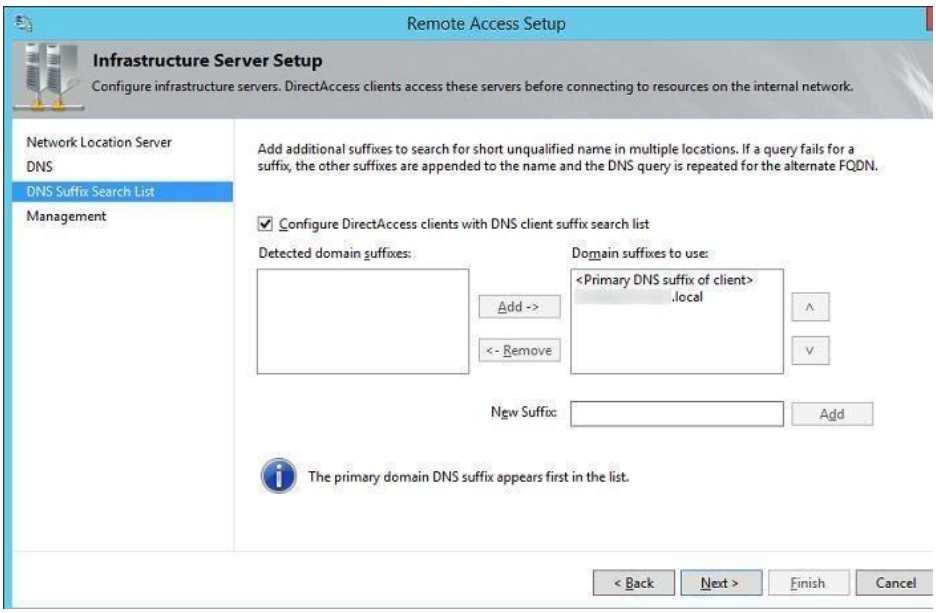


Рис. 130

В окне настройки Management ничего указывать не будем. Четвертый этап (Step 4: Application Servers)

Этап настройки серверов приложений. На этом этапе можно настроить дополнительную аутентификацию и шифрование трафика между внутренними серверами приложений и клиентами DA. Нам это не требуется, поэтому оставим опцию **Do not extend authentication to application servers.**

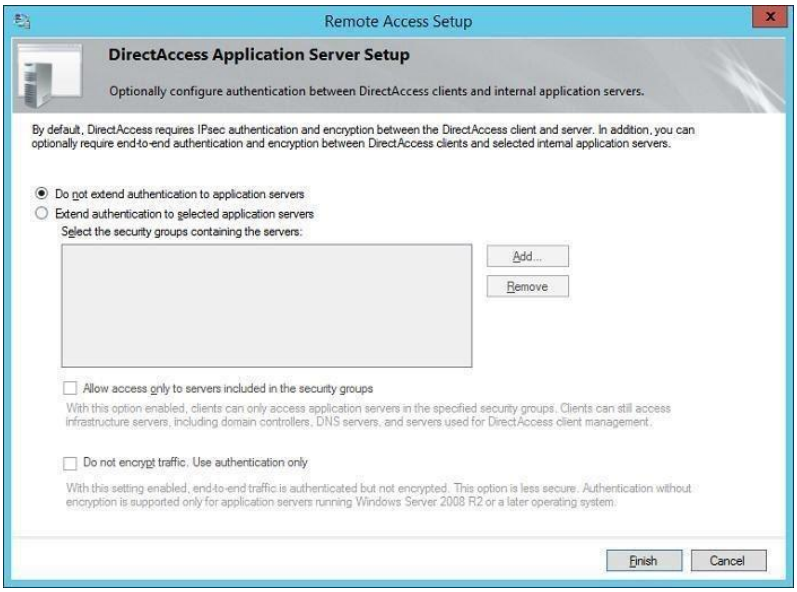


Рис. 131

На этом мастер настройки роли Remote Access завершен, нам осталось сохранить изменения.

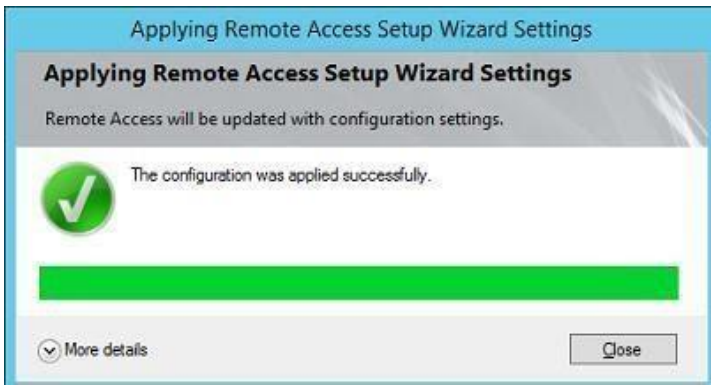


Рис. 132

Сделайте скриншоты (фотографии) процесса настройки технологии DirectAccess и вставьте в отчёт.

2.9. Практическая работа № 9
Развертывание расширен-ной инфраструктуры DirectAccess

Задание:

1. Установка сертификата IP-HTTPS из внутреннего ЦС
1. На сервере DirectAccess: на **начальном** экране введите **mmc.exe**и нажмите клавишу ВВОД.
2. В консоли MMC в меню **Файл** выберите **Добавить или удалить оснастку**.
3. В диалоговом окне **Добавление или удаление оснасток** щелкните **Сертификаты**, нажмите кнопку **Добавить**, выберите **Учетная запись компьютера**, нажмите кнопку **Далее**, щелкните **Локальный компьютер** и последовательно нажмите кнопки **Готово** и **ОК**.
4. В дереве консоли оснастки "Сертификаты" откройте раздел **Сертификаты (локальный компьютер)\Личные\Сертификаты**.

5. Щелкните правой кнопкой **Сертификаты**, наведите указатель на элемент **Все задачи**, а затем щелкните **Запрос нового сертификата**.
6. Щелкните дважды **Далее**.
7. На странице **запрос сертификатов** установите флажок для созданного ранее шаблона сертификата (Дополнительные сведения см. в разделе 1.5.2 configure Certificate Templates). При необходимости щелкните **Требуется больше данных для регистрации этого сертификата**.
8. В диалоговом окне **Свойства сертификата** на вкладке **Субъект** в области **Имя субъекта** в поле **Тип** выберите **Общее имя**.
9. В поле **Значение** укажите IPv4-адрес внешнего сетевого адаптера сервера DirectAccess или полное доменное имя URL-адреса IPHTTPS, а затем нажмите кнопку **Добавить**.
10. В области **Альтернативное имя** в поле **Тип** выберите **DNS**.
11. В поле **Значение** укажите IPv4-адрес внешнего сетевого адаптера сервера DirectAccess или полное доменное имя URL-адреса IPHTTPS, а затем нажмите кнопку **Добавить**.
12. На вкладке **Общие** в поле **Понятное имя** можно ввести имя, которое упростит идентификацию сертификатов.
13. На вкладке **Расширения** щелкните стрелку рядом с элементом **Расширенное использование ключа** и убедитесь, что элемент **Проверка подлинности сервера** есть в списке **Выбранные параметры**.
14. Нажмите кнопку **ОК**, щелкните **Зарегистрировать** и нажмите кнопку **Готово**.

15. В области сведений оснастки "Сертификаты" убедитесь, что новый сертификат был зарегистрирован с целью проверки подлинности сервера.

2. Настройка DNS-сервера

Необходимо вручную настроить запись DNS для веб-сайта сервера сетевых расположений внутренней сети в вашем развертывании. **Создание сервера сетевых расположений**

- На DNS-сервере внутренней сети: на **начальном** экране введите **днсмгмт. Msc** и нажмите клавишу ВВОД.
- В левой области консоли **Диспетчер DNS** разверните зону прямого просмотра для вашего домена. Щелкните домен правой кнопкой и выберите **Новый узел (A или AAAA)**.
- В диалоговом окне **Новый узел** в поле **IP-адрес**:

В поле **Имя (если оставить пустым, будет использован родительский домен)** введите DNS-имя для веб-сайта сервера сетевых расположений (это имя клиенты DirectAccess могут использовать для подключения к серверу сетевых расположений).

Введите IPv4- или IPv6-адрес сервера сетевых расположений, нажмите кнопку **Добавить узел** и нажмите **ОК**.

- В диалоговом окне **Новый узел**:

В поле Имя (если оставить пустым, будет использован родительский домен) введите DNS-имя для веб-пробы (имя вебпробы по умолчанию — directaccess-webprobehost).

В поле IP-адрес введите IPv4- или IPv6-адрес веб-пробы и нажмите кнопку Добавить узел.

Повторите этот процесс для directaccesscorpconnectivityhost и вручную созданных средств проверки.

- В диалоговом окне **DNS** нажмите кнопку **ОК**, а затем — **Готово**.

Следующие командлеты Windows PowerShell выполняют ту же функцию, что и предыдущая процедура. Вводите каждый командлет в одной строке несмотря на то, что здесь они могут отображаться разбитыми на несколько строк из-за ограничений форматирования.

Add-DnsServerResourceRecordA -Name <network_location_server_name>
-ZoneName <DNS_zone_name> -IPv4Address
<network_location_server_IPv4_address> Add-DnsServerResourceRecordAAAA -Name
<network_location_server_name> -ZoneName <DNS_zone_name> -IPv6Address
<network_location_server_IPv6_address>

Также следует настроить записи DNS для следующих компонентов:

- **Сервер IP-HTTPS**

У клиентов DirectAccess должна быть возможность разрешения DNS-имени сервера DirectAccess из Интернета.

- **Проверка отзыва CRL**

DirectAccess использует проверку отзыва сертификатов для подключения IP-HTTPS между клиентами DirectAccess и сервером DirectAccess, а также для HTTPS-подключений между клиентом DirectAccess и сервером сетевых расположений. В обоих случаях у клиентов DirectAccess должна быть возможность разрешения расположения точки распространения CRL и доступа к ней.

- **ISATAP**

Протокол ISATAP использует туннелирование, чтобы позволить клиентам DirectAccess подключаться к серверу DirectAccess по IPv4интернету, инкапсулируя паке-

ты IPv6 в заголовке IPv4. Служба удаленного доступа использует ISATAP для установки IPv6подключений к узлам ISATAP в интрасети. В сетевой среде без встроенной поддержки IPv6 сервер DirectAccess автоматически настраивается как маршрутизатор ISATAP. Требуется поддержка разрешения имени ISATAP.

3. Настройка Active Directory

Сервер DirectAccess и все клиентские компьютеры DirectAccess должны быть присоединены к домену Active Directory. Клиентские компьютеры DirectAccess должны быть членом домена одного из следующих типов:

- домена в том же лесу, что и сервер DirectAccess;
- домены в лесах с двусторонним отношением доверия с лесом сервера DirectAccess;
- домену с двусторонним отношением доверия с доменом сервера DirectAccess.

Присоединение сервера DirectAccess к домену

- В диспетчере серверов щелкните **Локальный сервер**. В области сведений перейдите по ссылке **Имя компьютера**.
- В диалоговом окне **Свойства системы** щелкните **Имя компьютера**, а затем **Изменить**.
- В поле **Имя компьютера** введите имя компьютера, если вы меняете имя компьютера при присоединении сервера к домену. В разделе **Член групп** выберите **Домен** и введите имя домена, к которому нужно присоединить сервер, например corp.contoso.com, а затем нажмите **ОК**.
- При появлении предложения ввести имя пользователя и пароль введите имя и пароль пользователя с правами присоединения компьютеров к домену, а затем нажмите **ОК**.
- При появлении диалогового окна с приветствием домена нажмите кнопку **ОК**.
- При появлении запроса на перезагрузку компьютера нажмите кнопку **ОК**.
- В диалоговом окне **Свойства системы** нажмите кнопку **Закрыть**.
- При появлении запроса на перезагрузку компьютера нажмите кнопку **Перезагрузить сейчас**.

Присоединение клиентских компьютеров к домену

- На **начальном** экране введите**explorer.exe**и нажмите клавишу ВВОД.
- Щелкните правой кнопкой значок компьютера и выберите **Свойства**.
- На странице **Система** щелкните **Дополнительные параметры системы**.
- В диалоговом окне **Свойства системы** на вкладке **Имя компьютера** щелкните **Изменить**.
- В поле **Имя компьютера** введите имя компьютера, если вы меняете имя компьютера при присоединении сервера к домену. В разделе **Член групп** выберите **Домен** и введите имя домена, к которому нужно присоединить сервер, например corp.contoso.com, а затем нажмите **ОК**.
- При появлении предложения ввести имя пользователя и пароль введите имя и пароль пользователя с правами присоединения компьютеров к домену, а затем нажмите **ОК**.
- При появлении диалогового окна с приветствием домена нажмите кнопку **ОК**.
- При появлении запроса на перезагрузку компьютера нажмите кнопку **ОК**.
- В диалоговом окне **Свойства системы** нажмите кнопку **Закрыть**.
- При появлении запроса на перезагрузку компьютера нажмите кнопку **Перезагрузить сейчас**.

Следующие командлеты Windows PowerShell выполняют ту же функцию, что и предыдущая процедура. Вводите каждый командлет в одной строке, несмотря на то, что

здесь они могут отображаться разбитыми на несколько строк из-за ограничений форматирования.

Примечание

При вводе следующей команды **Add-Computer** следует указать учетные данные домена.

Add-Computer -DomainName <domain_name> Restart-Computer

4. Настройка объектов групповой политики

Для развертывания удаленного доступа требуется не менее двух групповая политика объектов:

- один содержит параметры для сервера DirectAccess;
- другой содержит параметры для клиентских компьютеров DirectAccess.

При настройке удаленного доступа мастер автоматически создает необходимые групповая политика объекты. Но если организация принудительно применяет соглашение об именовании, вы можете ввести имя в диалоговом окне "Объект групповой политики" в консоли управления удаленным доступом. Дополнительные сведения см. в разделе 2.7. Сводка конфигурации и альтернативные объекты групповой политики. Если у вас есть разрешения на создание, будет создан GPO. Если у вас нет требуемых разрешений для создания GPO, их необходимо настроить до настройки службы удаленного доступа.

Сведения о создании групповая политика объектов см. в разделе Создание и изменение объекта Групповая политика.

Важно!

Администраторы могут вручную связать объекты групповая политика DirectAccess с подразделением (OU), выполнив следующие действия.

- Перед настройкой DirectAccess свяжите созданные GPO с соответствующими подразделениями.
- Во время настройки DirectAccess укажите группу безопасности для клиентских компьютеров.
- Возможно, администратор удаленного доступа не имеет разрешений на связывание объектов групповая политика с доменом. В любом из этих случаев объекты групповой политики будут настроены автоматически. Если объекты групповой политики уже привязаны к подразделению, связи не будут удалены и эти GPO не будут привязаны к домену. Для объекта групповой политики сервера подразделение должно включать объект-компьютер сервера. В противном случае объект групповой политики будет связан с корневым каналом домена.
- Если вы не создали связь с подразделением до запуска мастера DirectAccess, то после завершения настройки администратор домена сможет связать объекты групповая политика DirectAccess с требуемыми подразделениями. Связь с доменом можно удалить. Дополнительные сведения см. в разделе **Связывание объекта групповой политики.**

5. Настройка объектов групповой политики удаленного доступа с ограниченными разрешениями

В развертывании с использованием промежуточных и производственных объектов групповой политики администратор домена должен выполнить следующие действия.

- Получить список GPO, необходимых для развертывания службы удаленного доступа, у администратора удаленного доступа.

- Для каждого GPO, запрошенного администратором удаленного доступа, создайте пару GPO с разными именами. Первый из них будет использовать как промежуточный GPO, а второй — как производственный.

Сведения о создании групповая политика объектов см. в разделе Создание и изменение объекта Групповая политика.

- Инструкции по связыванию производственных GPO см. в разделе Связывание объекта групповой политики.
- Предоставьте администратору удаленного доступа разрешение **Изменение параметров, удаление и изменение разрешений безопасности** для всех промежуточных GPO. Дополнительные сведения см. в разделе Делегирование разрешений для группы или пользователя в объекте групповой политики.
- Запретите администратору удаленного доступа связывание объектов групповой политики во всех доменах (или убедитесь, что администратор удаленного доступа не имеет таких разрешений). Дополнительные сведения см. в разделе Делегирование разрешений для связывания объектов групповой политики.

Когда администраторы удаленного доступа настраивают службу удаленного доступа, они всегда должны указывать только промежуточные GPO (а не производственные). Это справедливо для начальной настройки удаленного доступа и для выполнения дополнительных операций настройки, для которых требуются дополнительные GPO, например при добавлении точек входа в развертывание на нескольких сайтах или активации клиентских компьютеров в дополнительных доменах.

После внесения изменений в конфигурацию удаленного доступа администратором удаленного доступа администратор домена должен проверить настройки в промежуточных GPO и с их в производственные GPO с помощью следующей процедуры.

6. Копирование параметров в производственные объекты групповой политики

- Убедитесь, что все промежуточные GPO в развертывании службы удаленного доступа были реплицированы во все контроллеры домена в используемом домене. Это необходимо для импорта последней конфигурации в производственные GPO. Дополнительные сведения см. в разделе Проверка статуса инфраструктуры групповой политики.
- Экспортируйте параметры, создав резервную копию всех промежуточных GPO в развертывании удаленного доступа. Дополнительные сведения см. в разделе Резервное копирование объекта групповой политики.
- Для каждого производственного GPO измените фильтры безопасности в соответствии с фильтрами соответствующего промежуточного GPO. Дополнительные сведения см. в разделе Фильтрация с использованием групп безопасности.

Примечание

Это необходимо, потому что команда **Импорт параметров** не копирует фильтр безопасности исходного GPO.

- Для каждого производственного GPO импортируйте параметры из резервной копии соответствующего промежуточного GPO следующим образом:
- В консоль управления групповыми политиками (GPMC) разверните узел объекты групповая политика в лесу и домене, который содержит объект рабочего групповая политика, в который будут импортированы параметры.
- Щелкните правой кнопкой GPO и выберите команду **Импорт параметров**.
- В **мастере импорта параметров** на странице **приветствия** нажмите кнопку **Далее**.

- На странице **Архивирование объекта групповой политики** нажмите кнопку **Резервное копирование**.
- В диалоговом окне **Архивация объекта групповой политики** в поле **Расположение** введите путь расположения, где будут сохранены резервные копии GPO, или нажмите кнопку **Обзор**, чтобы выбрать папку.
- В поле **Описание** введите описание производственного GPO и нажмите кнопку **Резервное копирование**.
- После завершения резервного копирования нажмите кнопку **ОК**, а затем на странице **Архивирование объекта групповой политики** нажмите **Далее**.
- На странице **Расположение архива** в поле **Папка архива** введите путь, в которой была сохранена резервная копия соответствующего промежуточного GPO на шаге 2, или нажмите кнопку **Обзор**, выберите папку и нажмите **Далее**.
- На странице **Исходный объект GPO** установите флажок **Показывать только последние версии объекта групповой политики**, чтобы скрыть старые резервные копии, и выберите соответствующий промежуточный GPO. Нажмите кнопку **Просмотр параметров**, чтобы просмотреть параметры удаленного доступа перед их применением к производственному GPO, а затем нажмите кнопку **Далее**.
- На странице **Проверка архива** нажмите кнопку **Далее**, а затем кнопку **Готово**.

Следующие командлеты Windows PowerShell выполняют ту же функцию, что и предыдущая процедура. Вводите каждый командлет в одной строке, несмотря на то, что здесь они могут отображаться разбитыми на несколько строк из-за ограничений форматирования.

- Чтобы создать резервную копию GPO промежуточного клиента "Параметры клиента DirectAccess — промежуточное хранение" в домене

"corp.contoso.com" в папку резервного копирования "C:\Backups" :

$backup = Backup-GPO "Name 'DirectAccess Client Settings - Staging' "Domain 'corp.contoso.com' "Path 'C:\Backups\'

- Чтобы просмотреть фильтр безопасности объекта групповой политики промежуточного клиента "Параметры клиента DirectAccess — промежуточное хранение" в домене "corp.contoso.com":

Get-GPPermission "Name 'DirectAccess Client Settings - Staging' "Domain 'corp.contoso.com' "All | ?{ $_.Permission "eq 'GpoApply'}

- Добавление группы безопасности "Corp. contoso. Ком\директакцесс Clients" в фильтр безопасности объекта групповой политики "Параметры клиента DirectAccess" Production "в домене" corp.contoso.com ":

Set-GPPermission "Name 'DirectAccess Client Settings - Production'
"Domain 'corp.contoso.com' "PermissionLevel GpoApply "TargetName
'corp.contoso.com\DirectAccess clients' "TargetType Group

- Импорт параметров из резервной копии в объект групповой политики "Параметры клиента DirectAccess" рабочей среды в домене "corp.contoso.com":

Import-GPO "BackupId $backup.Id "Path $backup.BackupDirectory
"TargetName 'DirectAccess Client Settings - Production' "Domain
'corp.contoso.com'

7. Настройка групп безопасности

Параметры DirectAccess, содержащиеся в объекте групповая политика клиентского компьютера, применяются только к компьютерам, входящим в группы безопасности, указанные при настройке удаленного доступа. Кроме того, если вы используете группы

безопасности для управления серверами приложений, необходимо создать группу безопасности для этих серверов.

Создание группы безопасности для клиентов DirectAccess

- На **начальном** экране введите**DSA. msc**и нажмите клавишу ВВОД. В консоли **Active Directory — пользователи и**

компьютеры разверните в левой области домен, к которому будет принадлежать группа безопасности, щелкните правой кнопкой мыши **Пользователи**, выберите **Новые**, после чего щелкните **Группа**.

- В диалоговом окне **Создание объекта — группа** в поле **Имя группы** введите имя группы безопасности.
- В разделе **Область группы** щелкните **Глобальная**, а в разделе **Тип группы** щелкните **Безопасность** и нажмите кнопку **ОК**.
- Дважды щелкните группу безопасности клиентских компьютеров DirectAccess и в диалоговом окне свойств откройте вкладку **Члены**.
- На вкладке **Члены группы** щелкните **Добавить**.
- В диалоговом окне **Выбор пользователей, контактов, компьютеров или учетных записей служб** выберите клиентские компьютеры, которые необходимо активировать для DirectAccess, а затем нажмите кнопку **ОК**.

Следующие командлеты Windows PowerShell выполняют ту же функцию, что и предыдущая процедура. Вводите каждый командлет в одной строке несмотря на то, что здесь они могут отображаться разбитыми на несколько строк из-за ограничений форматирования.

```
New-ADGroup -GroupScope global -Name
<DirectAccess_clients_group_name>
Add-ADGroupMember -Identity DirectAccess_clients_group_name -Members
<computer_name>
```

8. Настройка сервера сетевых расположений

Сервер сетевых расположений должен обладать высоким уровнем доступности и действительным SSL-сертификатом, которому доверяют клиенты DirectAccess. Для сервера сетевых расположений можно использовать один из следующих типов сертификатов:

- **Частный сертификат**

Этот сертификат основан на созданном вами шаблоне сертификата. для этого следуйте инструкциям в разделе 1.5.2 Настройка шаблонов сертификатов.

- **Самозаверяющий сертификат**

Примечание

Самозаверяющие сертификаты не могут использоваться в развертываниях на нескольких сайтах.

Для каждого типа сертификата требуется создать следующие элементы, если они еще не существуют:

- Сертификат веб-сайта, используемый для сервера сетевых расположений. Субъектом этого сертификата должен быть URL-адрес сервера сетевых расположений.
- Точка распространения CRL с высоким уровнем доступности из внутренней сети.

Установка сертификата сервера сетевых расположений из внутреннего ЦС

- На сервере, где будет размещаться веб-сайт сервера сетевого расположения: на **начальном** экране введите**mmc.exe**и нажмите клавишу ВВОД.

- В консоли MMC в меню **Файл** выберите **Добавить или удалить оснастку**.
- В диалоговом окне **Добавление или удаление оснасток** щелкните **Сертификаты**, нажмите кнопку **Добавить**, выберите **Учетная запись компьютера**, нажмите кнопку **Далее**, щелкните **Локальный компьютер** и последовательно нажмите кнопки **Готово** и **ОК**.
- В дереве консоли оснастки "Сертификаты" откройте

раздел **Сертификаты (локальный компьютер)\Личные\Сертификаты**.

- Щелкните правой кнопкой **Сертификаты**, наведите указатель на элемент **Все задачи**, а затем щелкните **Запрос нового сертификата**.
- Щелкните дважды **Далее**.
- На странице **запрос сертификатов** установите флажок для созданного шаблона сертификата, выполнив инструкции в разделе Настройка шаблонов сертификатов 1.5.2. При необходимости щелкните **Требуется больше данных для регистрации этого сертификата**.
- В диалоговом окне **Свойства сертификата** на вкладке **Субъект** в области **Имя субъекта** в поле **Тип** выберите **Общее имя**.
- В поле **Значение** укажите полное доменное имя для вебсайта сервера сетевых расположений и щелкните **Добавить**.
- В области **Альтернативное имя** в поле **Тип** выберите **DNS**.
- В поле **Значение** укажите полное доменное имя для вебсайта сервера сетевых расположений и щелкните **Добавить**.
- На вкладке **Общие** в поле **Понятное имя** можно ввести имя, которое упростит идентификацию сертификатов.
- Нажмите кнопку **ОК**, щелкните **Зарегистрировать** и нажмите кнопку **Готово**.
- В области сведений оснастки "Сертификаты" убедитесь, что новый сертификат был зарегистрирован с целью проверки подлинности сервера.

Настройка сервера сетевых расположений

- Настройте веб-сайт на сервере с высоким уровнем

доступности. Для него контент не требуется, но для проверки вы можете определить страницу по умолчанию, с сообщением, которое видят клиенты при подключении.

Примечание

Это действие не требуется, если веб-сайт сервера сетевых расположений размещен на сервере DirectAccess.

- Привяжите сертификат HTTPS-сервера к веб-сайту. Общее имя сертификата должно совпадать с именем сайта сервера сетевых расположений. Убедитесь, что клиенты DirectAccess доверяют ЦС, выдающему сертификат.

Примечание

Это действие не требуется, если веб-сайт сервера сетевых расположений размещен на сервере DirectAccess.

- Настройте сайт CRL с высоким уровнем доступности из внутренней сети.

Точки распространения CRL можно получить с помощью:

Веб-серверы с помощью URL-адреса на основе HTTP, например: https://crl.corp.contoso.com/crld/corp-APP1-CA.crl о Файловые серверы, доступ к которым осуществляется по UNC-пути, например \ \crl.Corp.contoso.com\crld\corp-APP1-CA.CRL

Если внутренняя точка распространения CRL доступна только по IPv6, необходимо настроить правило безопасности брандмауэра Windows в режиме повышенной безопасности, чтобы исключить защиту

IPsec IPv6-адреса интрасети для IPv6-адресов точек распространения CRL.

- Убедитесь, что клиенты DirectAccess во внутренней сети могут разрешить имя сервера сетевых расположений. Убедитесь, что это имя не разрешается клиентами DirectAccess в Интернете.

Сделайте скриншоты (фотографии) процесса развертывания расширенной инфраструктуры DirectAccess и вставьте в отчёт.

2.10. Практическая работа № 10
Внедрение VPN

Задание:

1. Установить роль удаленного доступа.

Для этого в оснастке Server Manager запускаем мастер добавления ролей и выбираем роль «Remote Access» со всеми дополнительными фичами.

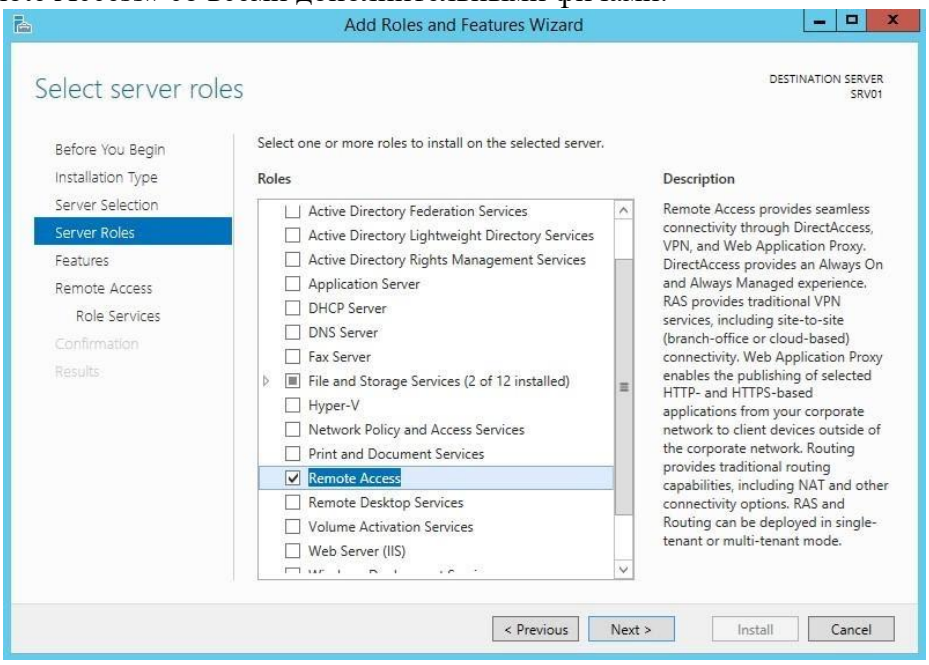


Рис. 133

И затем в списке сервисов для данной роли выбираем «DirectAccess and VPN (RAS)».

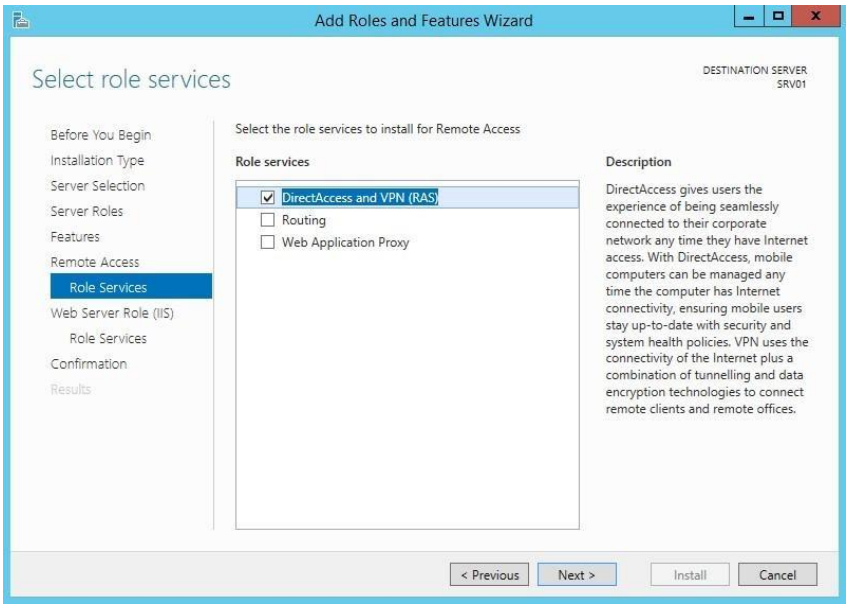


Рис. 134

Кроме роли удаленного доступа и инструментов управления будут дополнительно установлены web-сервер IIS и внутренняя база данных Windows. Полный список

устанавливаемых компонентов можно просмотреть в финальном окне мастера, перед подтверждением запуска установки.

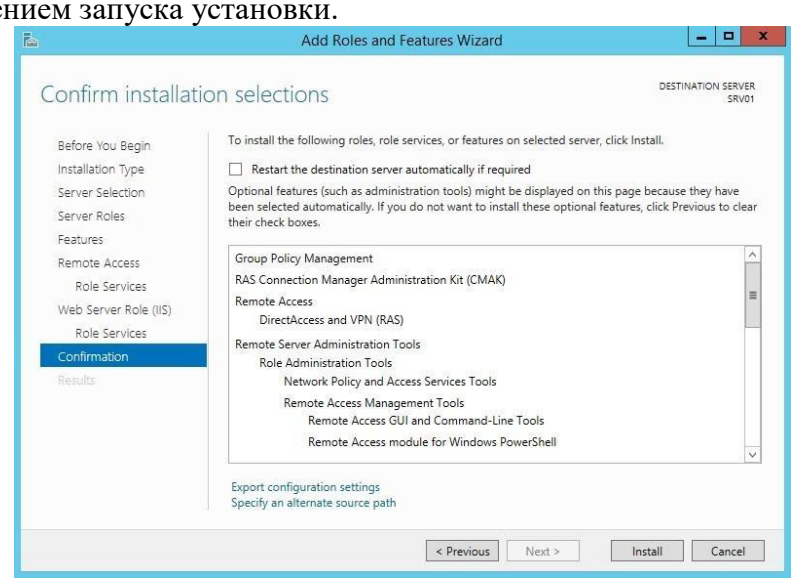


Рис. 135

Все то же самое, только гораздо быстрее, можно проделать с помощью PowerShell. Для этого надо открыть консоль и выполнить команду:

Install-WindowsFeature -Name Direct-Access-VPN -IncludeAllSubFeature IncludeManagementTools

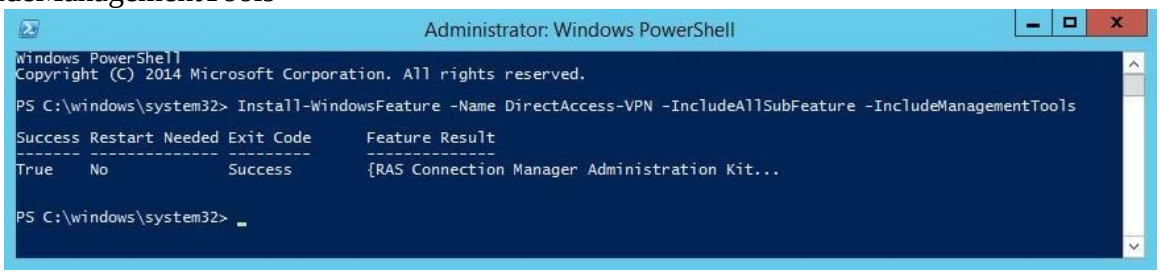


Рис. 136

После установки роли нам потребуется включить и настроить службу с помощью оснастки «Routing and Remote Access». Для ее открытия жмем **Win+R** и вводим команду **rrasmgmt.msc.**

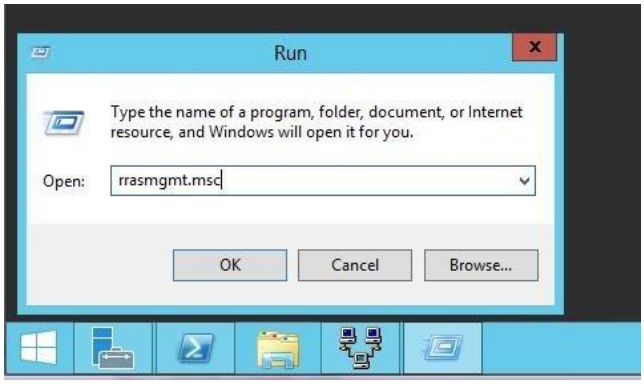


Рис. 137

В оснастке выбираем имя сервера, жмем правой клавишей мыши и в открывшемся меню выбираем пункт «Configure and Enable Routing and Remote Access».

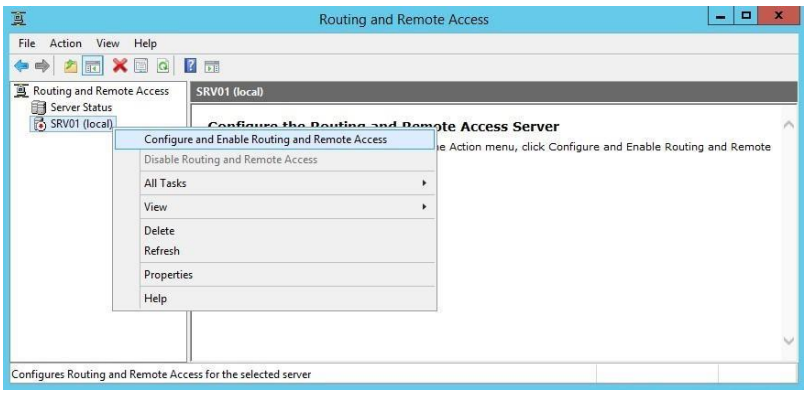


Рис. 138

В окне мастера настройки выбираем пункт «Custom configuration».

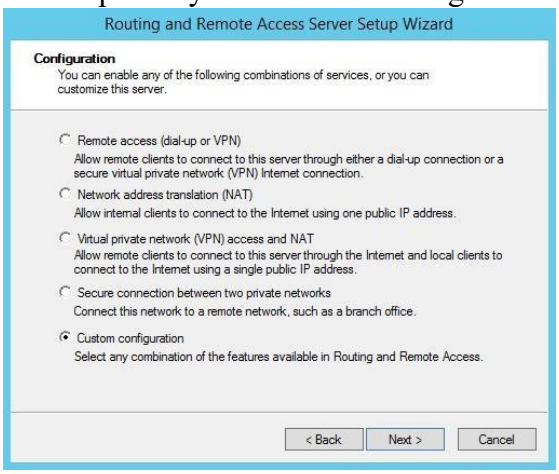


Рис. 139

И отмечаем сервис «VPN access».

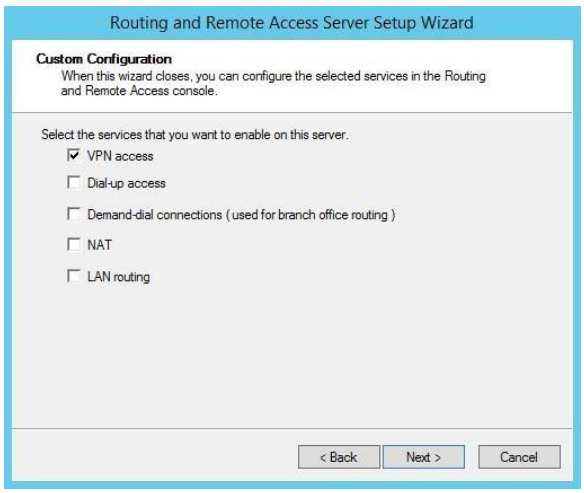


Рис. 140

В завершение настройки стартуем сервис удаленного доступа.

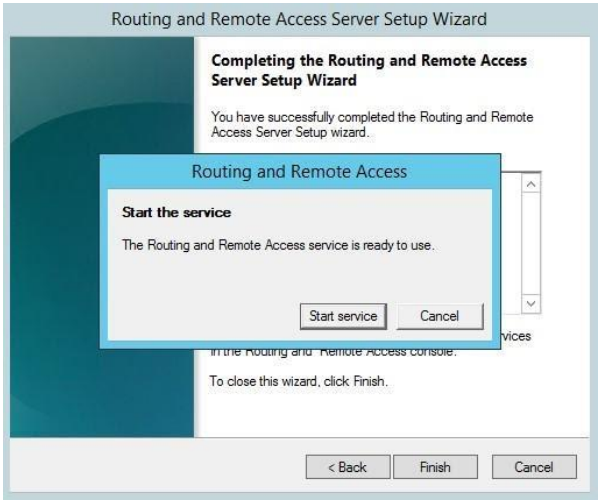


Рис. 141

Сервис VPN установлен и включен, теперь необходимо сконфигурировать его нужным нам образом. Опять открываем меню и выбираем пункт «Properties».

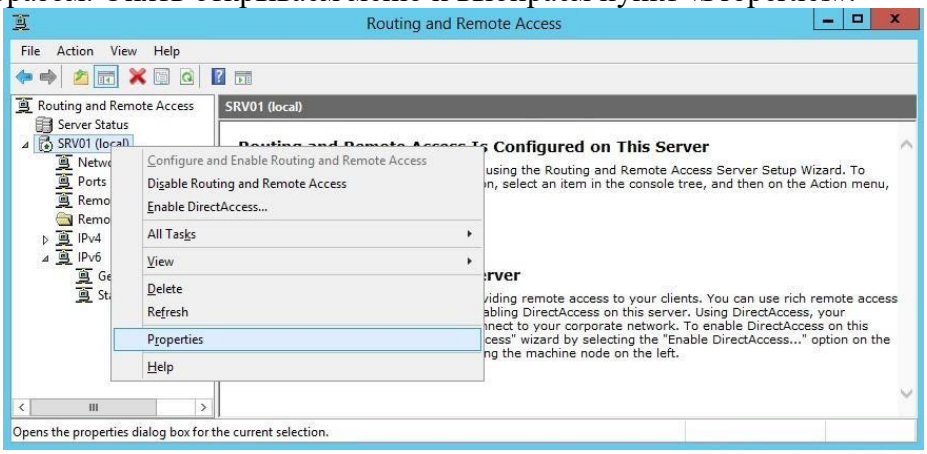


Рис. 142

Переходим на вкладку IPv4. Если у вас в сети нет DHCP сервера, то здесь надо задать диапазон IP адресов, которые будут получать клиенты при подключении к серверу.

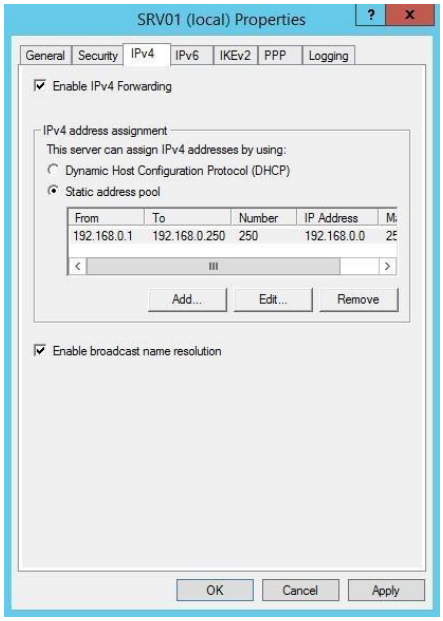


Рис. 143

Дополнительно на вкладке «Security» можно настроить параметры безопасности — выбрать тип аутентификации, задать предварительный ключ (preshared key) для L2TP или выбрать сертификат для SSTP.

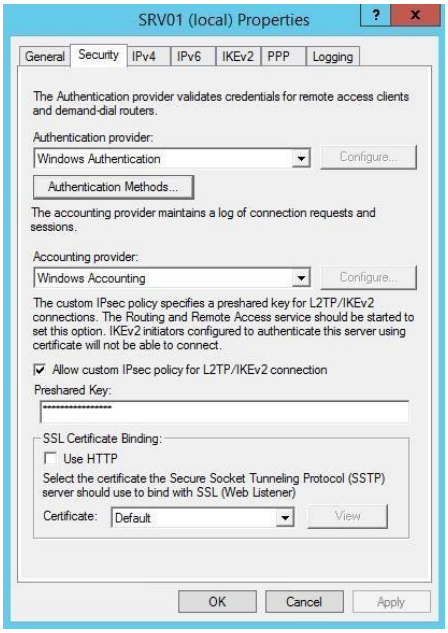


Рис. 144

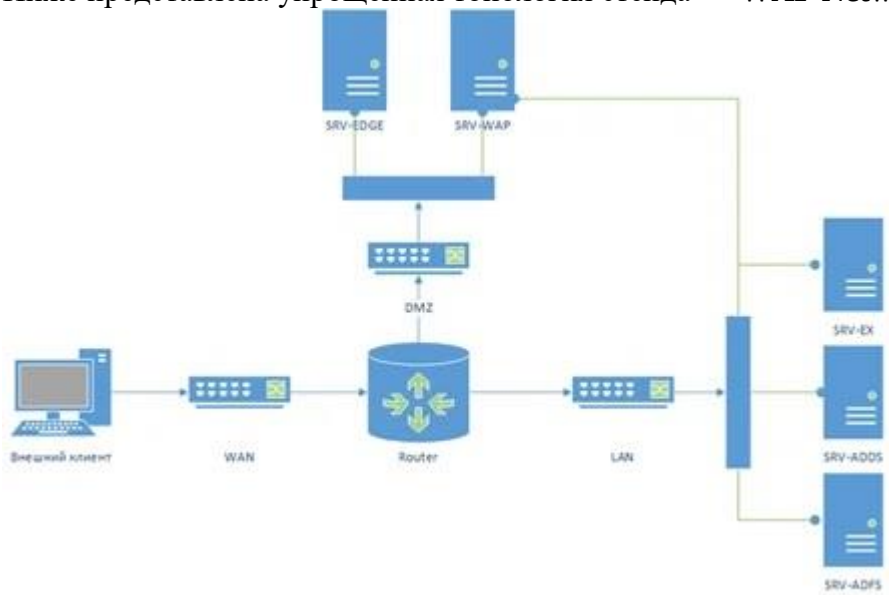
Сделайте скриншоты (фотографии) процесса внедрения VPN и вставьте в отчёт.

2.11. Практическая работа № 11
Внедрение Web Application Proxy

Задание:

Исследование **WAP** будет выполнено на лабораторном стенде, работающем под управлением **Windows Server 2012 R2 Datacenter** с установленной ролью Hyper-V. На сервере создано 3 виртуальных коммутатора: **WAN**, **LAN** и **DMZ**.

Ниже представлена упрощенная топология стенда — **WAP Network**



В качестве маршрутизатора использовался Endian Firewall community, основанный на Linux. Маршрутизатор реализует «трехногую» конфигурацию, образовывая 2 частных сети DMZ и LAN.

Адресное пространство DMZ — 192.168.1.0/24, а для LAN — 172.16.20.0/24.
Подготовка сервера под ADFS

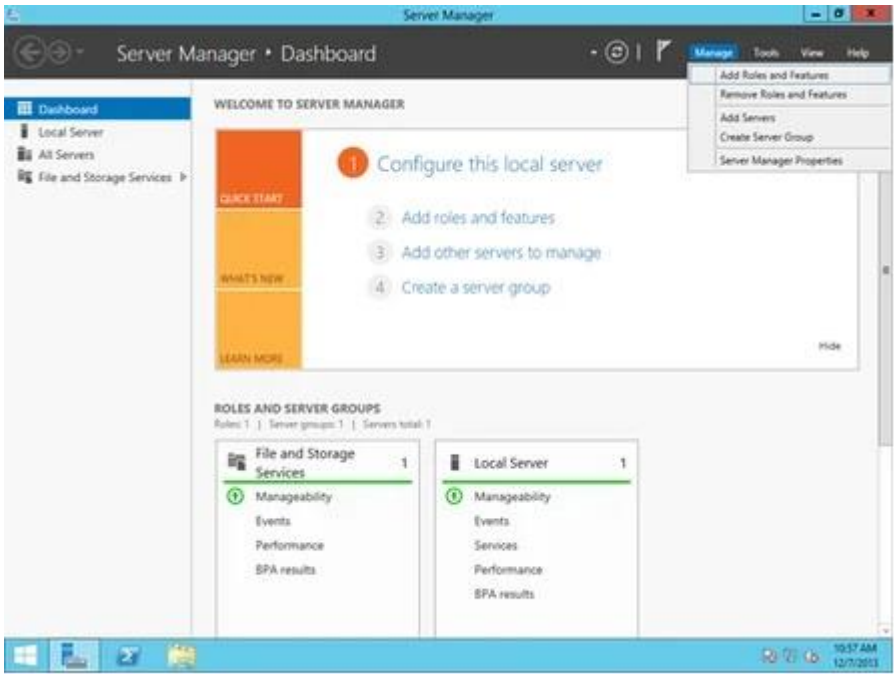
Службы федерации будут размещается на виртуальной машине SRV-ADFS которая является членом домена office365.local. Характеристики виртуальной машины:
ОС: **Server 2012 R2 Standard** с 2-я виртуальными процессорами и 2-я ГБ ОЗУ
IP адрес сервера: 172.16.20.14 /24

Требования к публикации

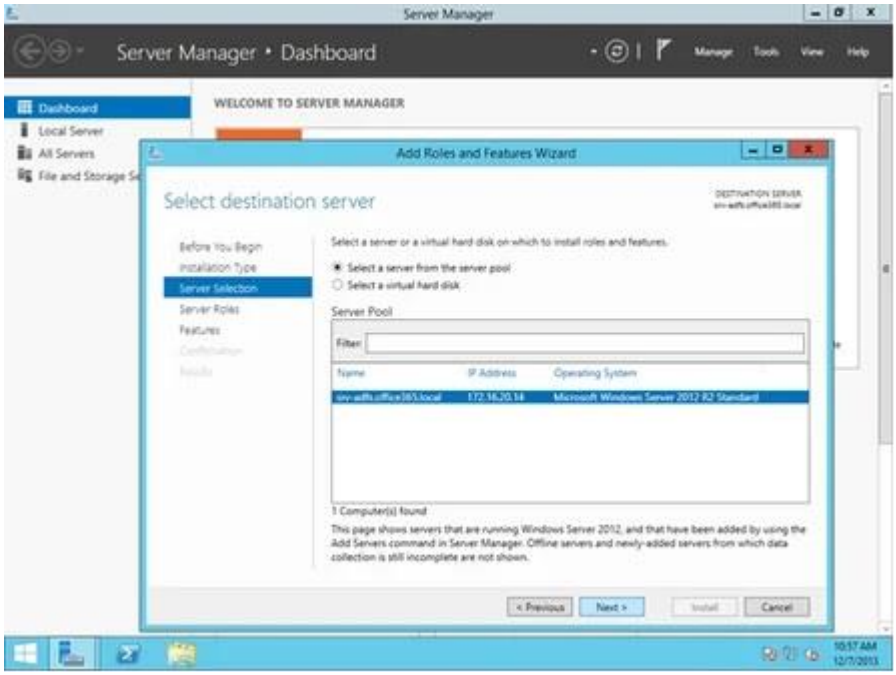
Говоря о требованиях к публикации, нужно продумать два важных момента:
1) Под каким внешним DNS именем будут доступны службы ADFS нашей организации для клиентов
2) Какими техническими характеристиками должен обладать SSL сертификат публикуемый сервере ADFS
Думаю, с первым пунктом вопросов не должно возникнуть. Во внешней DNS зоне создаем запись типа A которая будет указывать на IP адрес WAP сервера. Ну а вот относительного второго пункта возможно возникнут вопросы, давайте разбираться.
В процессе развертывания необходимо использовать SSL сертификат в поле **Subject Alternative Name** которого содержится DNS имя публикуемой службы ADFS. Сам он может быть импортирован заранее или добавлен во время работы мастера конфигурации ADFS. В качестве удостоверяющего CA допускается использование либо внутреннего CA, либо внешнего третьей стороны. Различия будет лишь в том, что если сертификат не от третьей стороны, за доставку корневого сертификата ответственны будете лишь вы.
В случае моего демо-стенда, будет использовать коммерческий Wildcard сертификат выписанный под доменное имя *.office365.kiev.ua Наличие именно коммерческого сертификата не является обязательным требованием.

Развертывание роли ADFS

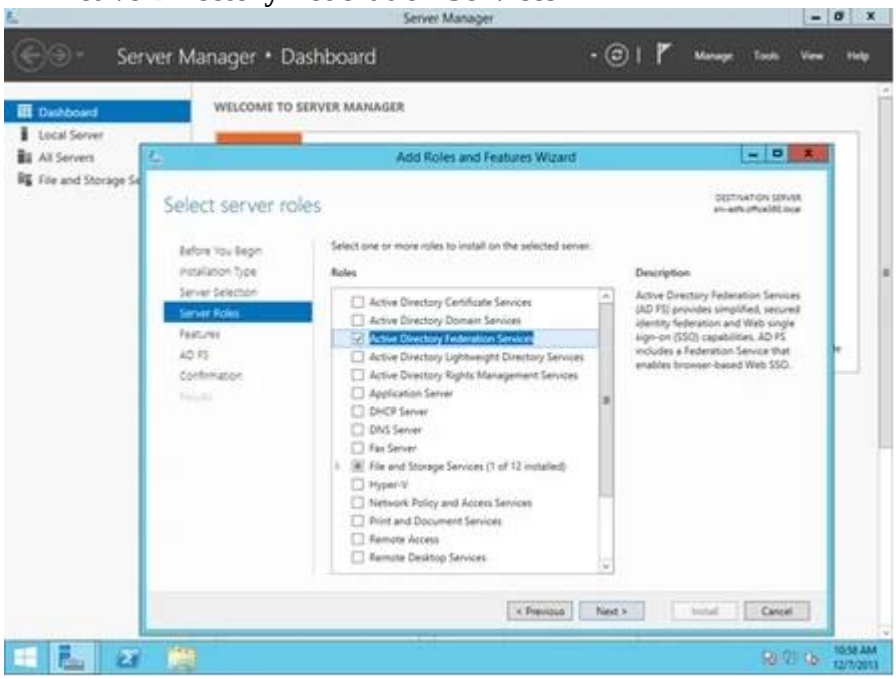
На сервере SRV-ADFS.office365.local и запустим **Server Manager.** В меню **Manage,** открываем **Add Roles and Features**



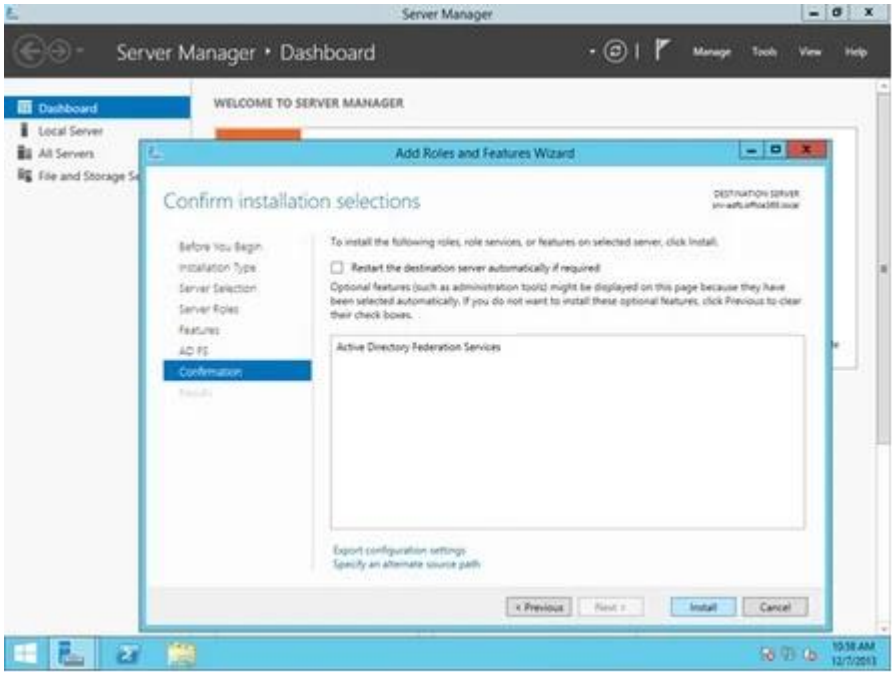
Доходим до шага выбора сервера для инсталляции и продолжаем



Выбираем роль **Active Directory Federation Services**

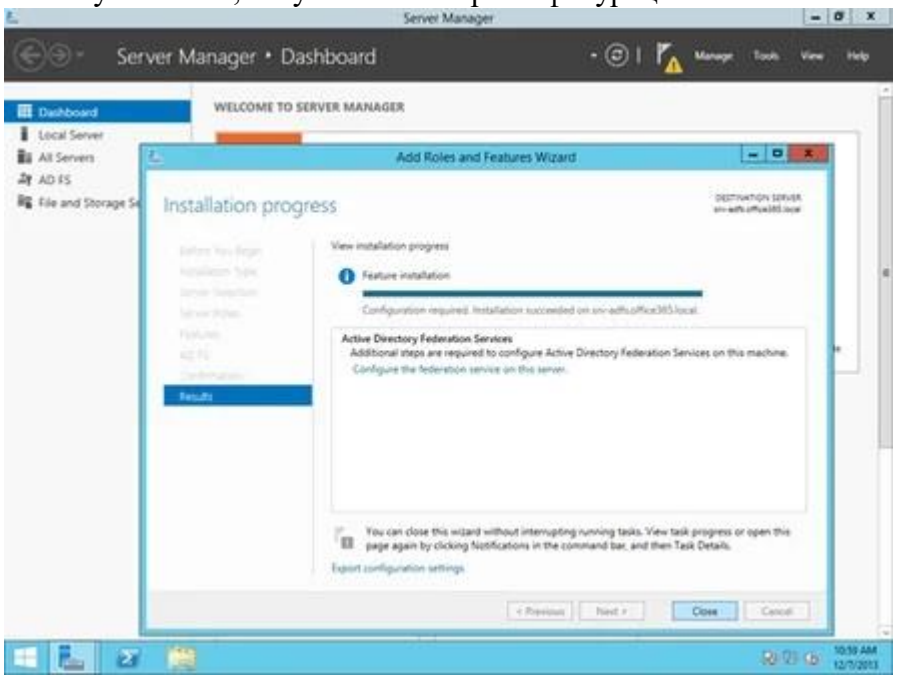


В следующем окне нажимаем **Install** дожидаясь до конца установки роли.

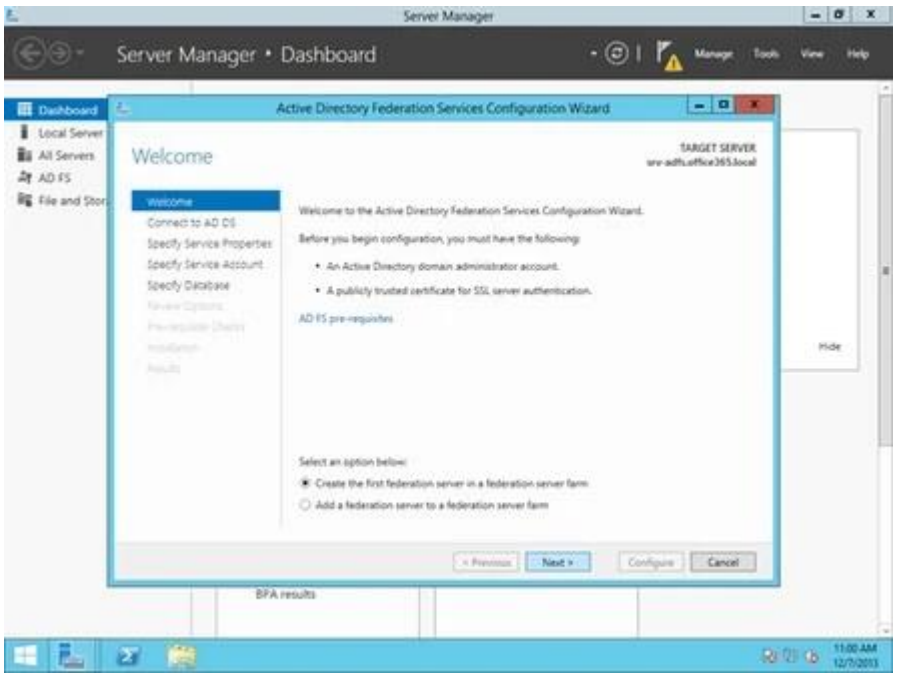


Конфигурирование службы ADFS

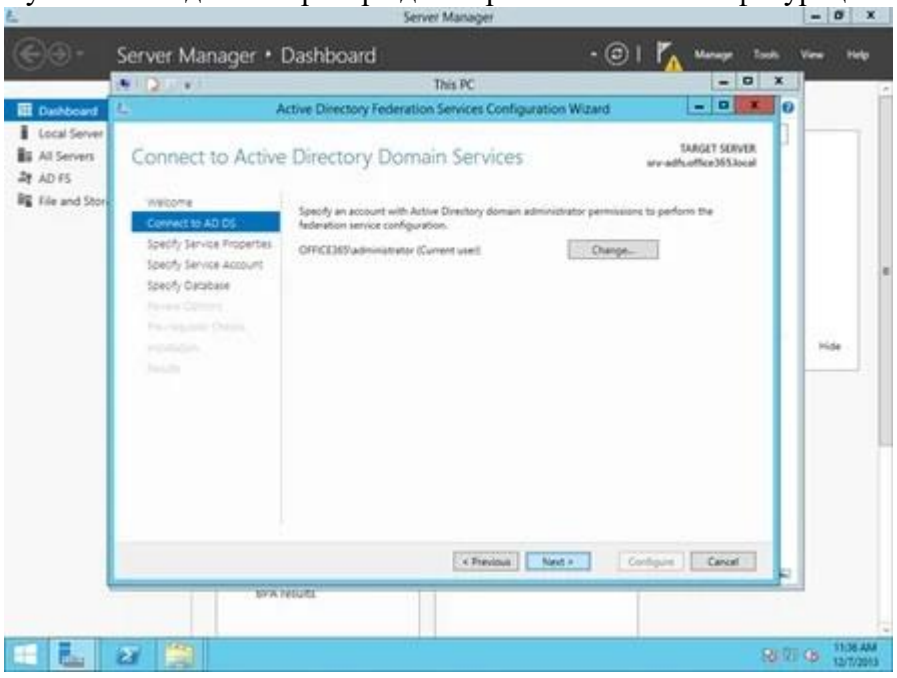
После завершения установки, запускаем мастер конфигурации



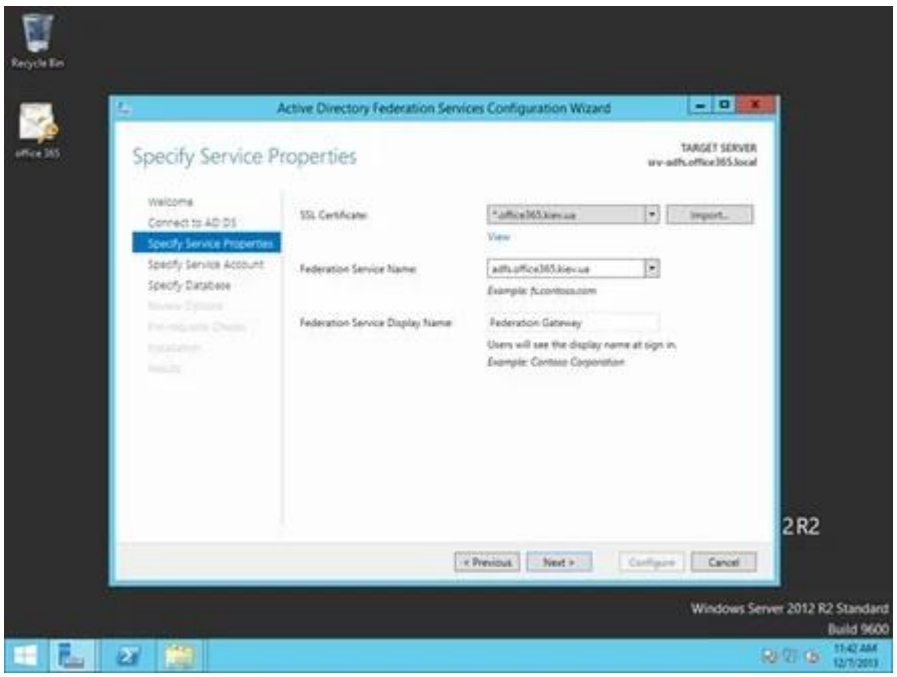
В мастере выставляем радио-бокс на против **Create the first server in a federation farm** тем самым создавая первый сервер федерации в новой ферме ADFS.



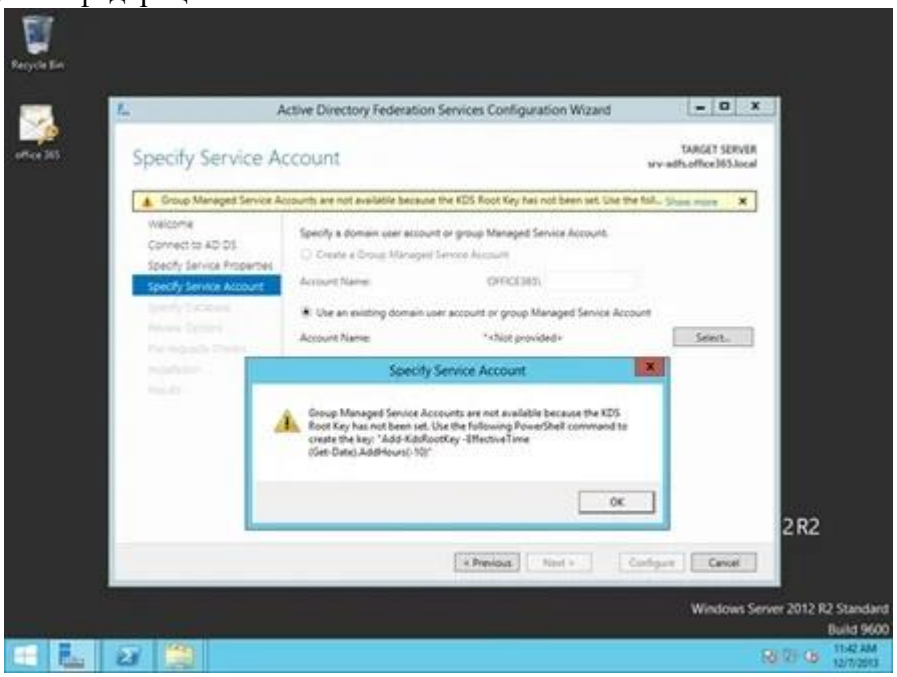
Вводим учетную запись администратора для первоначальной конфигурации служб.



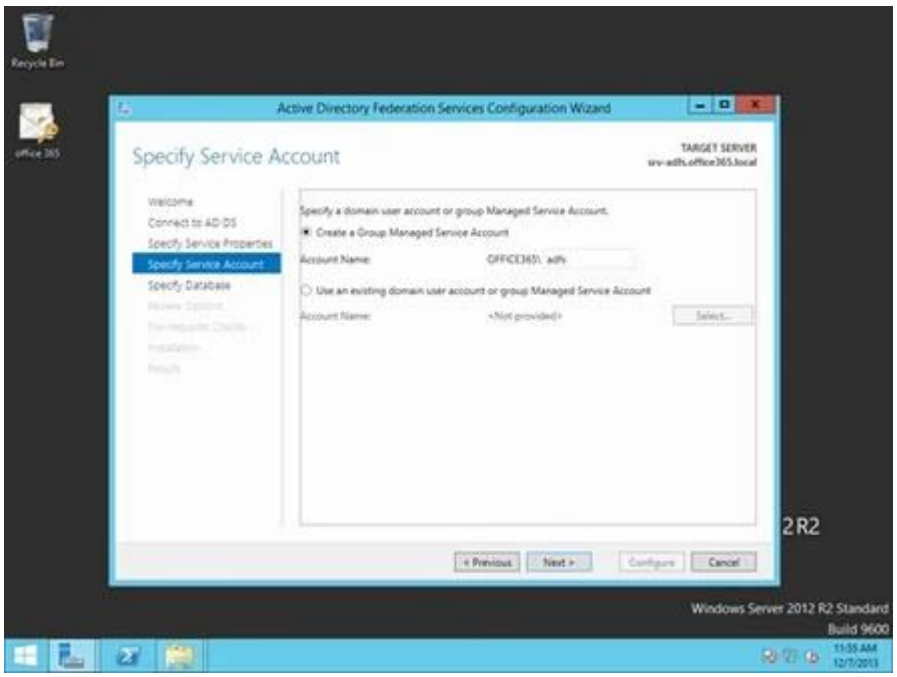
Следующий шаг, попросит указать SSL сертификат для настройки ADFS. Заранее я произвел его импорт на сервер, после этого мастер дал возможность его выбрать из списка SSL сертификатов. В поле **Federation Service Name** будет указано внешнее DNS имя adfs.office365.kiev.ua а в **Federation Service Display Name —** отображаемое имя служб федерации для клиентов.



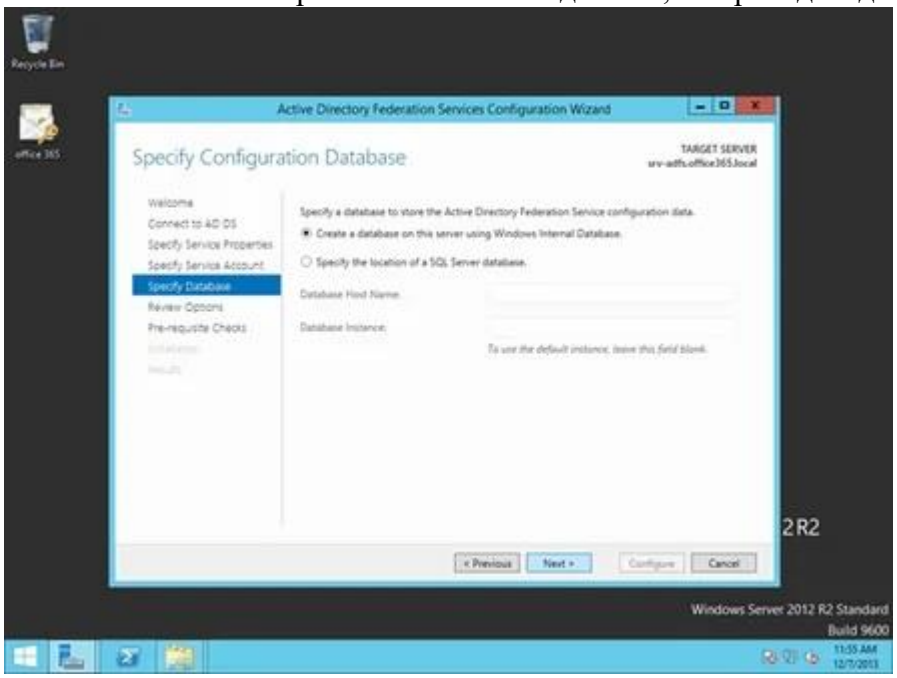
На следующем шаге, необходимо определить учетную запись, из под прав которой будут работать службы федерации.



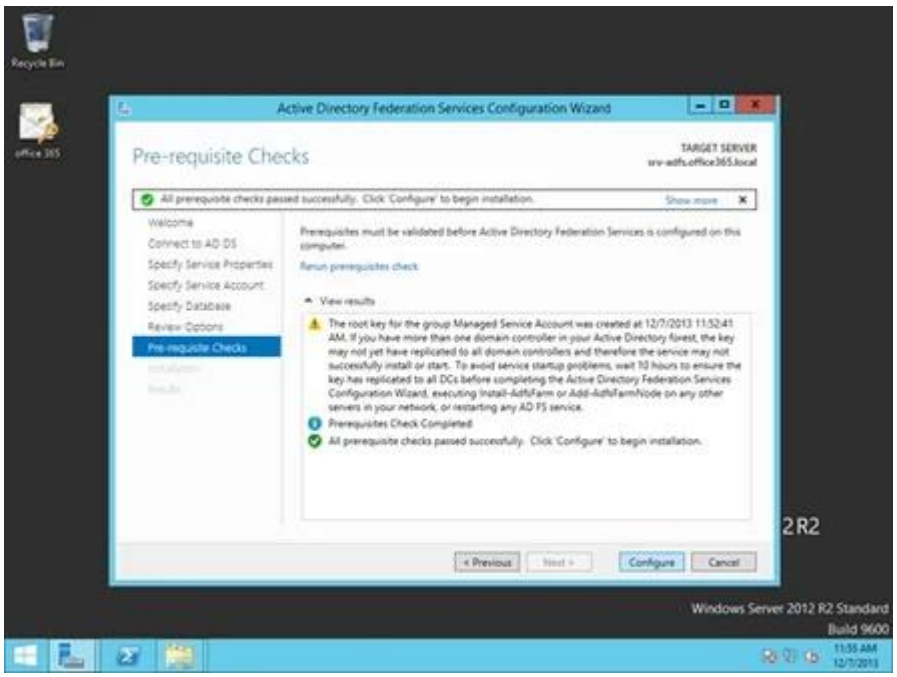
Окно предупреждения выдало ошибку:
Group Management Service Account are not available because the KDS root key not been set…
Это произошло, потому что предварительно не был создан **Microsoft Key Distribution Service root key** который необходим для функционирования **Group Managed Service Account.** На TechNet описана полная процедура создания.
В своем примере я воспользовался подсказкой в предупреждении и выполнил командлет
Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10))
на контроллере домена.
После выполнение вернутся на один шаг назад и заново перешел к выбору **Service Account** После исчезновения окна предупреждения, в качестве учетной записи было выбрано имя **adfs**



Оставляем без изменений место хранения базы базы данных, и переходим далее.



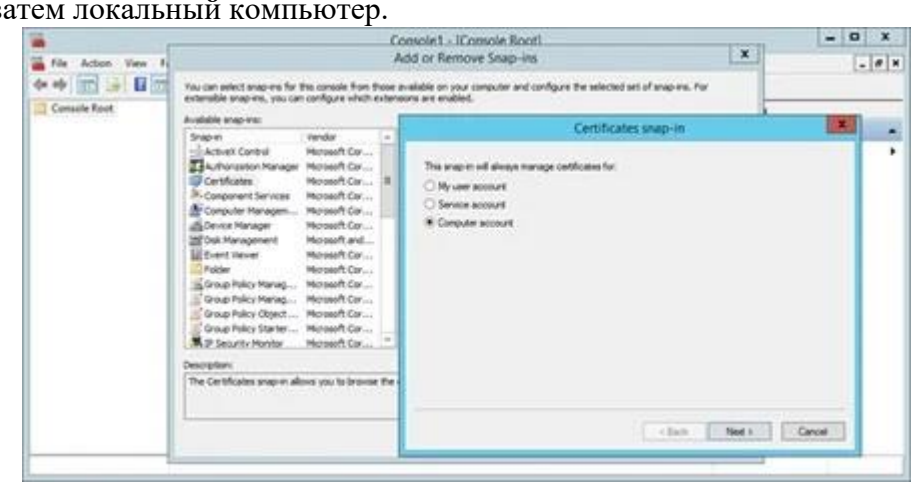
Нажимаем **Configure** и дожидаемся до окончания завершения конфигурации служб ADFS.



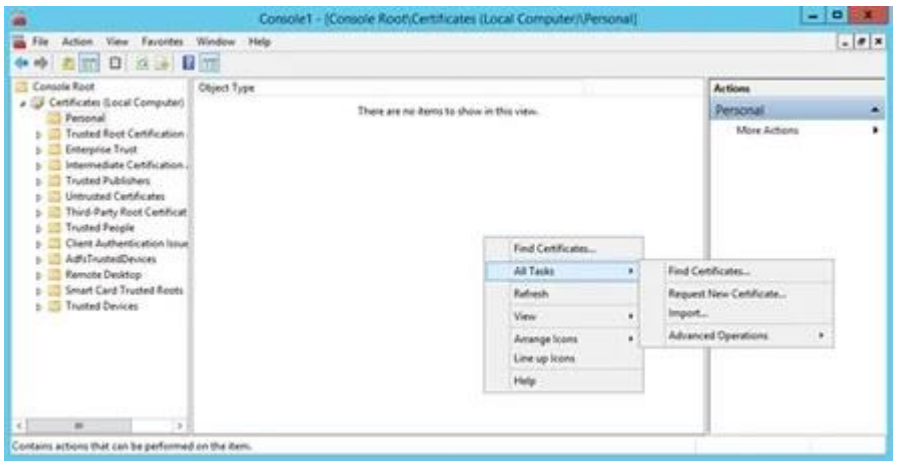
Импортирование SSL сертификата для WAP

В качестве сертификата для публикации WAP, я использовал тот же сертификат, который задействовал в предыдущей статье для конфигурирования ADFS. Предварительно нужно его импортировать на локальный сервер. Для этого запустим от имени администратора консоль mmc

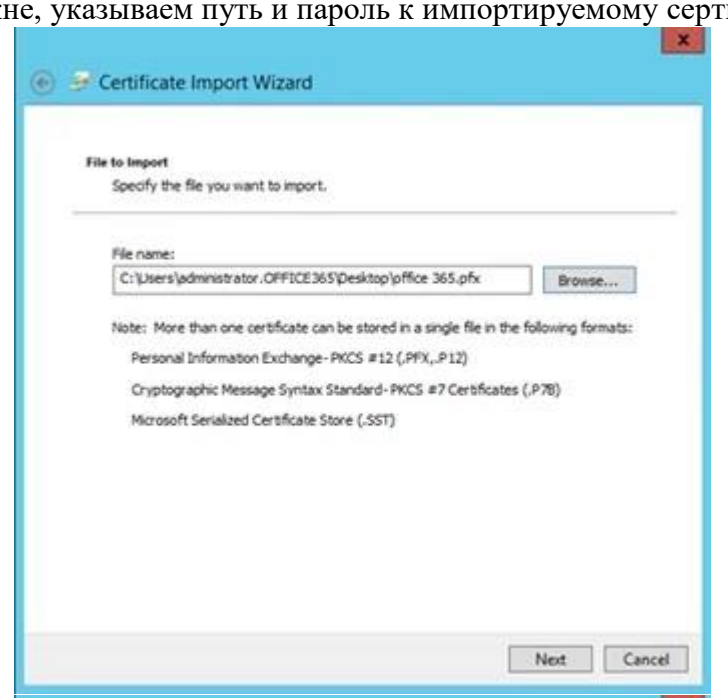
Нажав <Ctrl> + <M> добавим оснастку Certificates, выбрав в качестве управления компьютер, а затем локальный компьютер.



Открываем вкладку Personal и через меню All Task выбираем Import

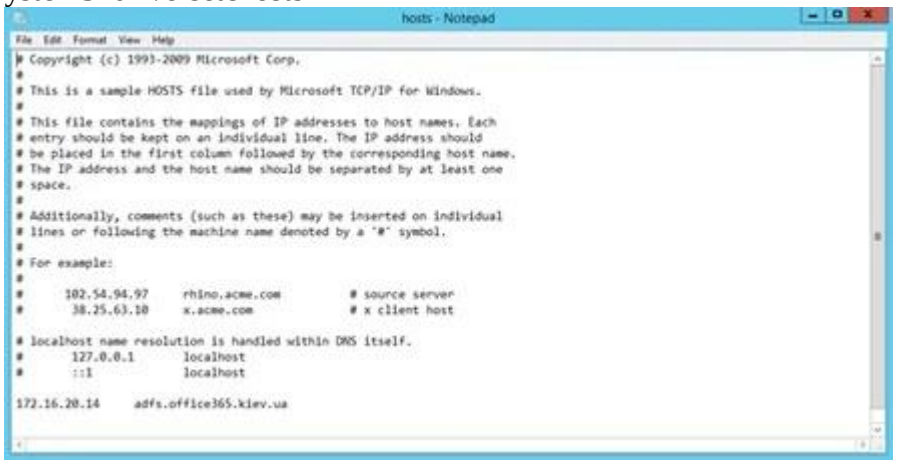


В открывшемся окне, указываем путь и пароль к импортируемому сертификату.



После импорта нужно так же настроим файл Host для возможности разрешения сервера ADFS. Это важный шаг – если данная настройка не будет выполнена, мастер конфигурирования WAP не сможет завершить конфигурацию с службами ADFS.

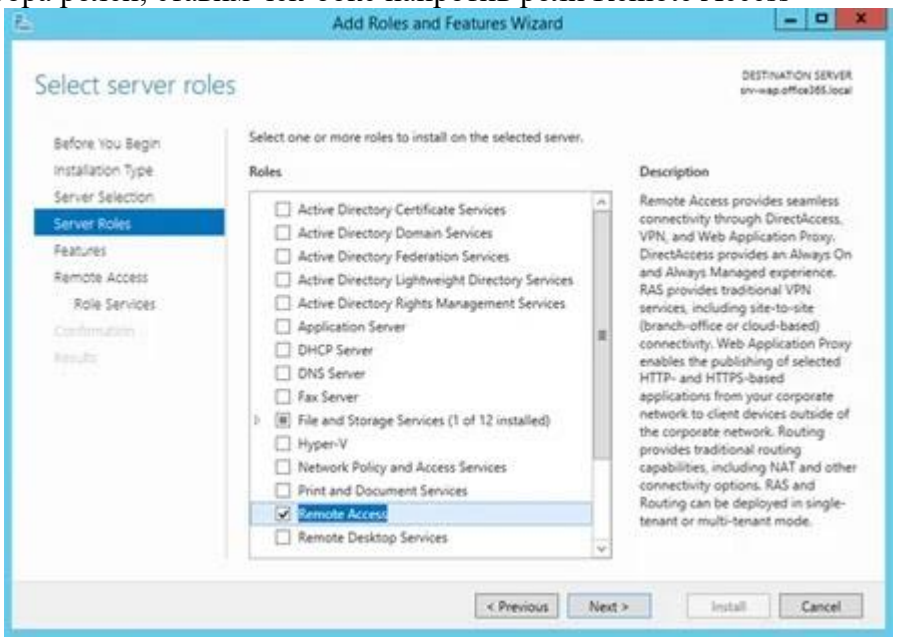
Для этого, от имени администратора вызываем Notepad. Открываем файл Host по указанному пути:
C:WindowsSystem32driversetchosts



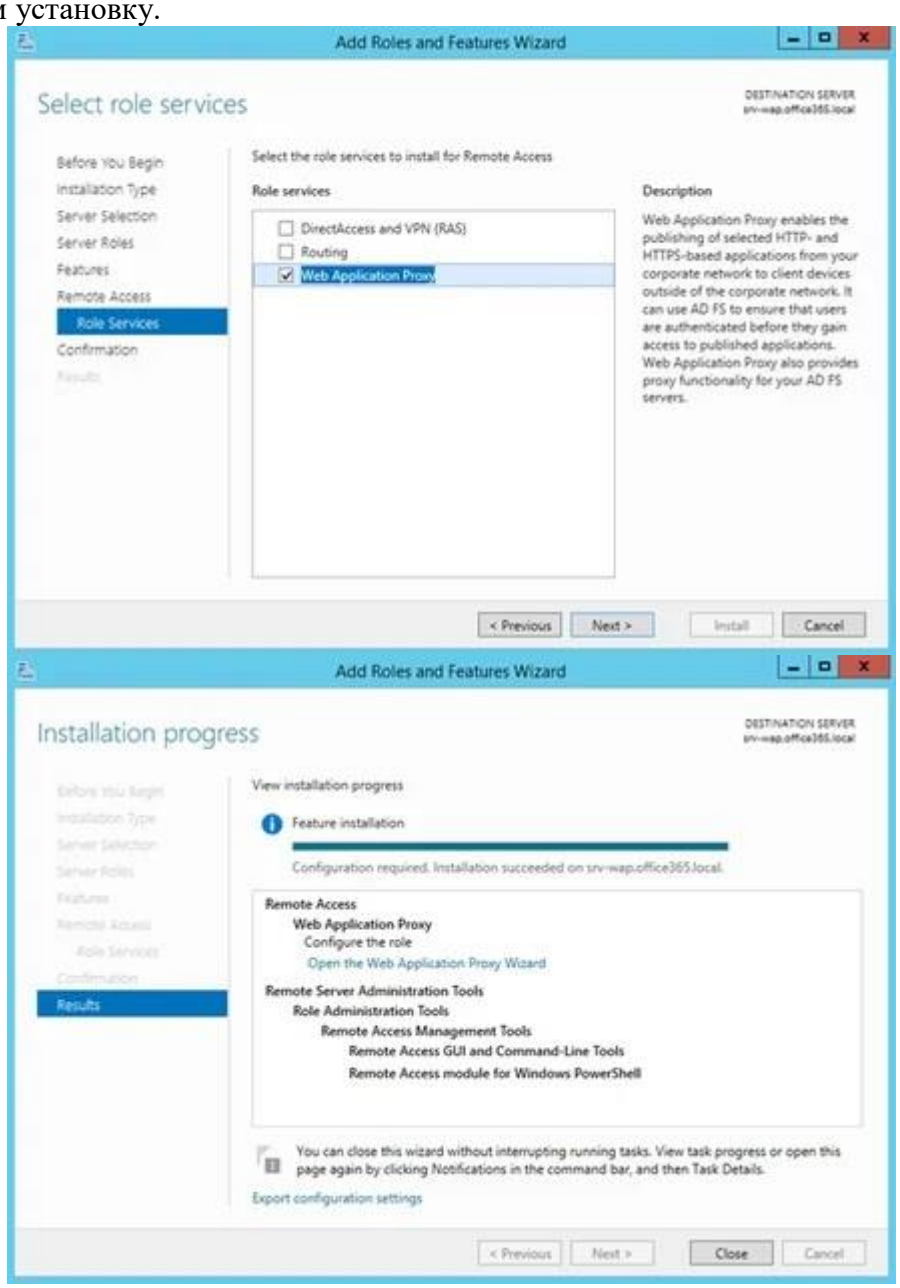
Произведем изменения, добавив в качестве новой строки: IP адрес сервера ADFS и его FQDN. В моем случае, данные выглядят так:
172.16.20.14 adfs.office365

Развертывание WAP
Запустил Server Manager, меню Manage откроем Add Roles and Features

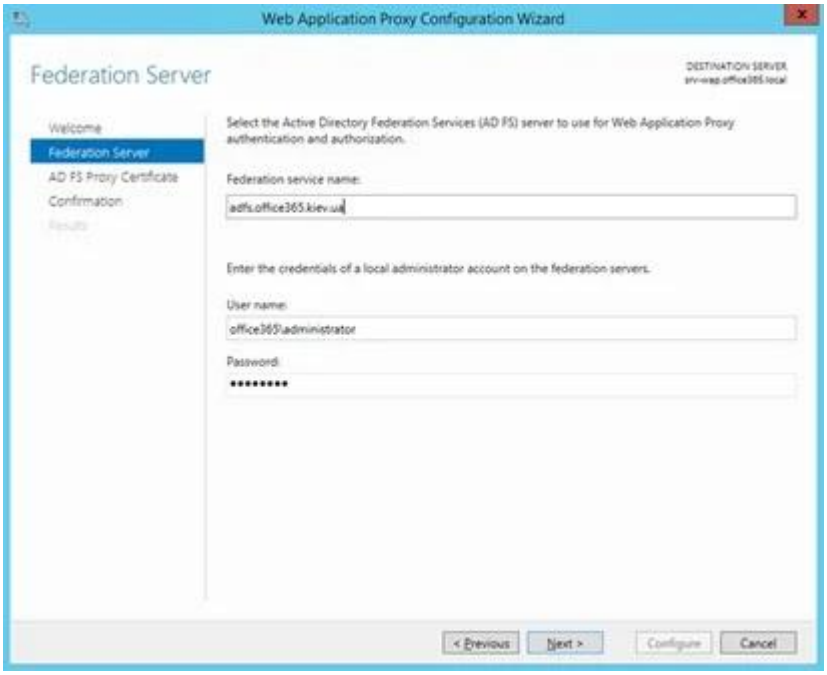
На шаге выбора ролей, ставим чек-бокс напротив роли Remote Access



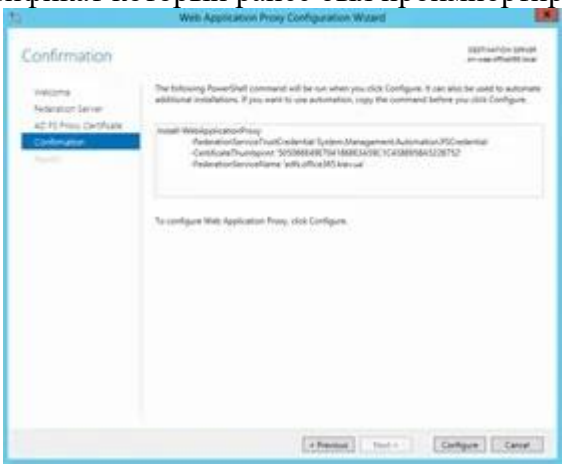
При конфигурировании службы ролей, ставим чек-бокс напротив Web Application Proxy и завершаем установку.



После завершения, открываем мастер конфигурации WAP

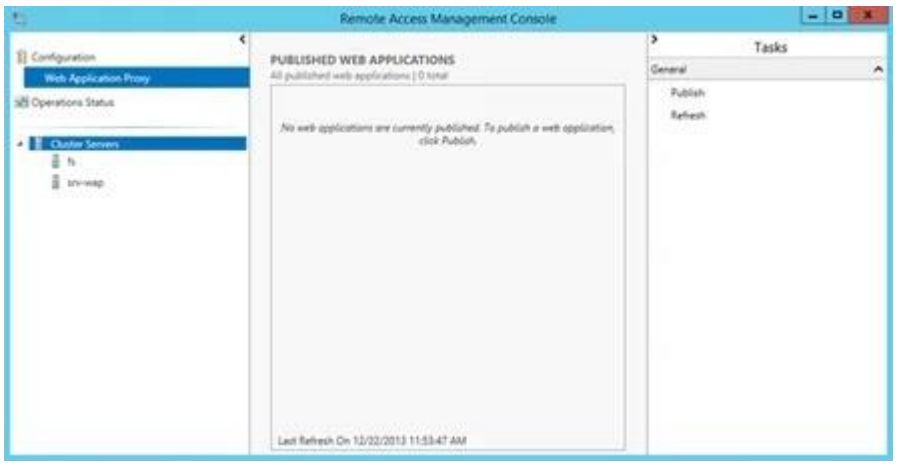


В поле Federation service name укажем расположение сервера федерации Active Directory, в поле User name — аккаунт локального администратора. На следующем шаге необходимо выбирать SSL сертификат который ранее был проимпортирован на сервер.



Результатом работы мастера будет создание PowerShell коммандлета который произведет конфигурацию WAP.

Конфигурация завершена. В процессе конфигурирования, на стороне служб ADFS, была создана подписка на WAP сервер. Для проверки работоспособности подписки, откроем консоль Remote Access Management Console и перейдем Web Application Proxy. Примером успешной конфигурации будет служить возможность произвести публикацию приложения выбрав Publish. Именно этим я займусь в будущей статье, когда будет производится публикация приложений Exchange Sevrer.

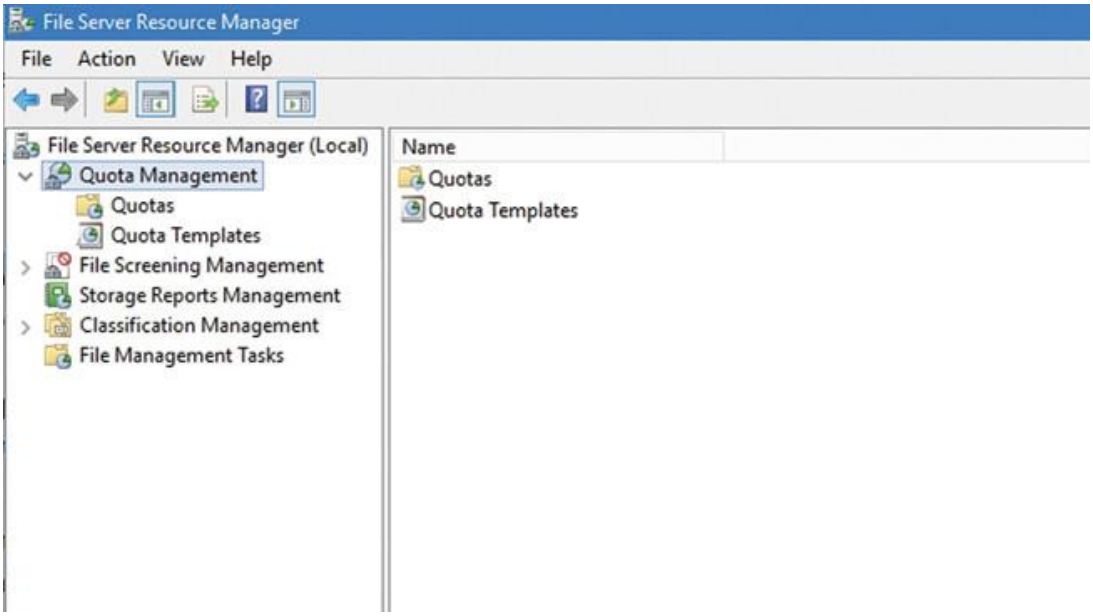


2.12. Практическая работа № 12
Настройка Квот и файлового экранирования в FSRM

Задание:

Чтобы создать квоту, откройте диспетчер ресурсов файлового сервера, выбрав его из списка инструментов диспетчера серверов. После того как консоль откроется, разверните контейнер Quota Management («Управление квотами»).

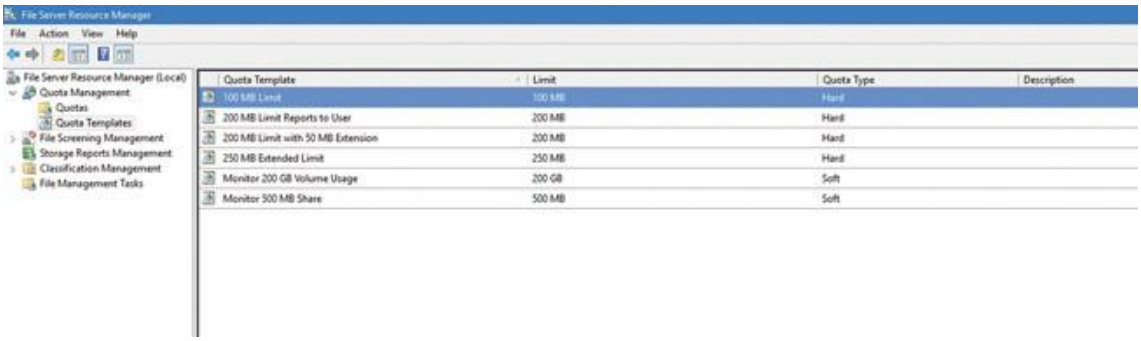
На экране 1 показаны два вложенных контейнера в контейнере Quota Management. Один из них называется Quotas («Квоты»), а другой — Quota Templates («Шаблоны квот»).



Экран 1. Создание квот и управление ими из консоли диспетчера ресурсов файлового сервера

Квоты основаны на шаблонах квот. Шаблон квоты определяет предельный размер и действия, которые совершаются при достижении предела. С другой стороны, квоты применяют шаблон квоты к конкретному пути. Учитывая это, рассмотрим анатомию шаблона квот.

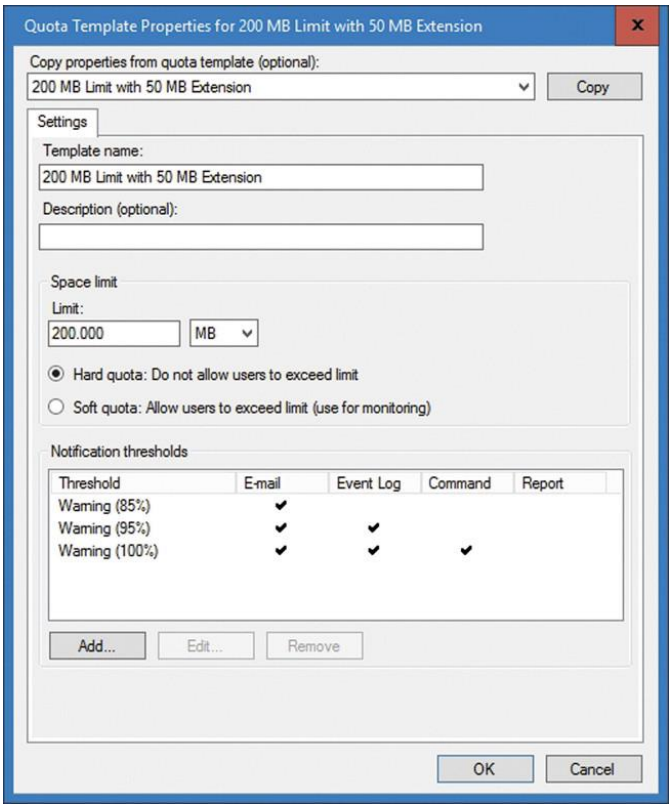
Если взглянуть на экран 2, можно увидеть несколько шаблонов квот, существующих по умолчанию. Эти шаблоны квот можно использовать в изначальном виде или изменить в соответствии со своими нуждами. Конечно, возможно и создание дополнительных шаблонов квот.



Экран 2. Существует несколько встроенных шаблонов квот

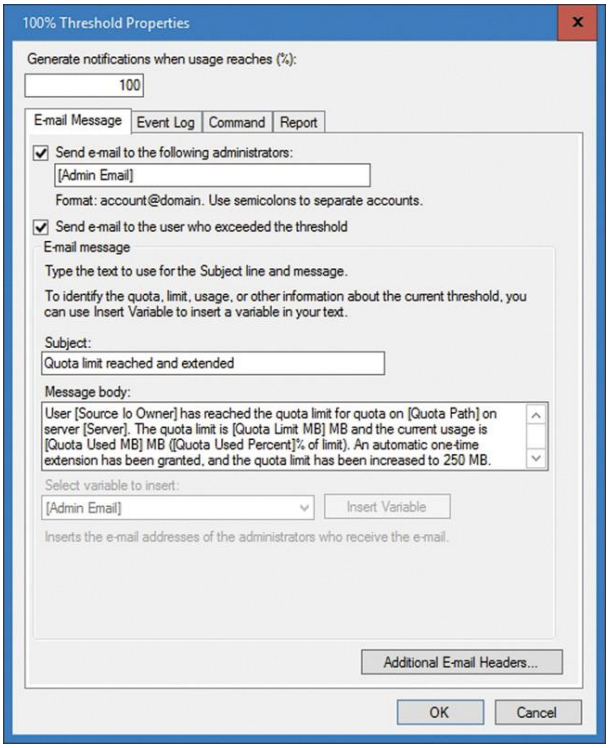
Обратите внимание на несколько особенностей этого экрана. Во-первых, квоты определяются как жесткая или мягкая квота. Жесткие квоты применяются принудительно, а мягкие используются в основном для тестирования или в информационных целях. Во-вторых, один из шаблонов квот определен как имеющий предел 200 Мбайт с расширением 50 Мбайт. В сущности, это шаблон для 200 Мбайт жесткой квоты. Однако, после того как квота исчерпана, шаблон квоты может инструктировать Windows предпринять какие-либо действия, например отправить сообщение по электронной почте или выполнить команду. Шаблон использует такую команду для автоматического расширения квоты. Это происходит следующим образом.

Если щелкнуть по шаблону квоты правой кнопкой мыши и выбрать команду Edit Template Properties («Изменить свойства шаблона») из контекстного меню, откроется окно, представленное на экране 3. Обратите внимание, что шаблон квоты не только задает предельный размер, но и определяет действия, предпринимаемые в том случае, если пользователь приближается к пределу квоты. Предупреждающее сообщение по электронной почте отправляется, когда использовано 85% пространства. Второе предупреждение отправляется пользователю, когда израсходовано 95% пространства. Кроме того, в журнал событий вносится соответствующая запись. Когда лимит квоты окончательно исчерпан, отправляется еще одно сообщение по электронной почте и вносится запись в журнал событий. Однако на этот раз, помимо прочего, выполняется команда. Все эти действия настраиваемые.

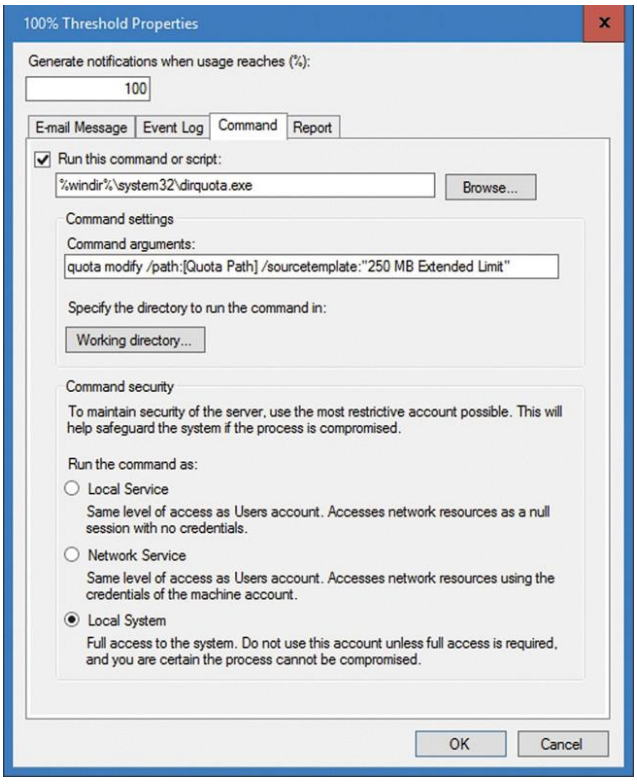


Экран 3. Вид шаблона квоты

Если выбрать вариант Warning 100% («Предупреждение 100%») и нажать кнопку Edit («Изменить»), то откроется диалоговое окно, показанное на экране 4. В этом диалоговом окне можно управлять действиями, выполняемыми после достижения предела. Здесь показан текст электронного сообщения, которое будет отправлено. Однако, взглянув на вкладку Command («Команда»), можно увидеть, что этот шаблон квоты настроен на автоматическое увеличение квоты путем применения другого шаблона квоты (экран 5).



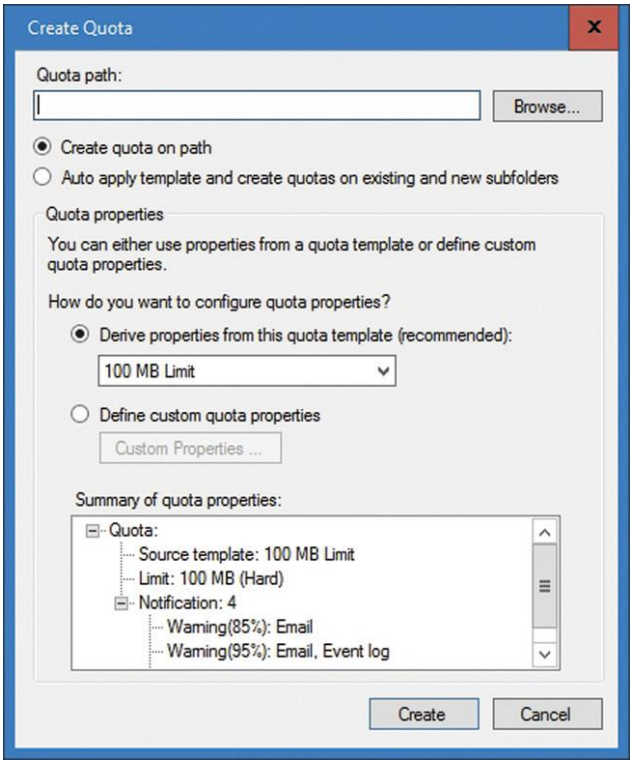
Экран 4. Настройка электронного сообщения, отправляемого при достижении предела квоты



Экран 5. Вкладка Command настраивается для выполнения команды расшире-

ния при достижении предела квоты

Как отмечалось выше, шаблоны квот просто определяют поведение операционной системы. С другой стороны, квоты привязывают шаблон квоты к пути к файлу. Можно создать квоту, щелкнув правой кнопкой мыши на контейнере Quotas и выбрав команду Create Quota («Создать квоту») из контекстного меню. Как показано на экране 6, в открывающемся в результате диалоговом окне Create Quotas («Создание квот») содержится приглашение ввести путь к квоте и выбрать шаблон квоты.



Экран 6. Квоты применяют шаблон квоты в соответствии с путем к файлу

После того как в диалоговом окне Create Quotas введены все необходимые файлы, можно воспользоваться разделом сводки внизу, чтобы проверить параметры квоты, прежде чем нажать кнопку Create («Создать»).

2.13. Практическая работа № 13
Применение DFS

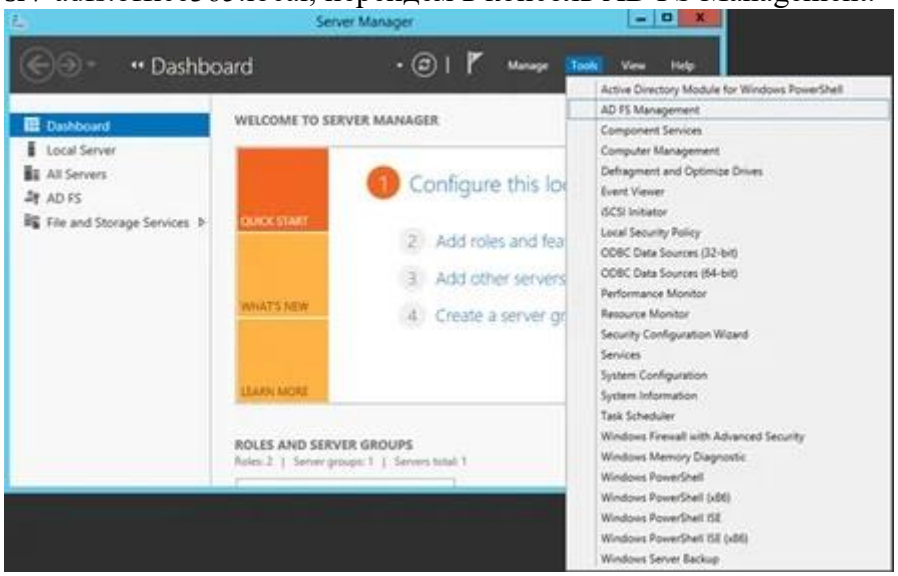
Задание:

Конфигурирование ADFS

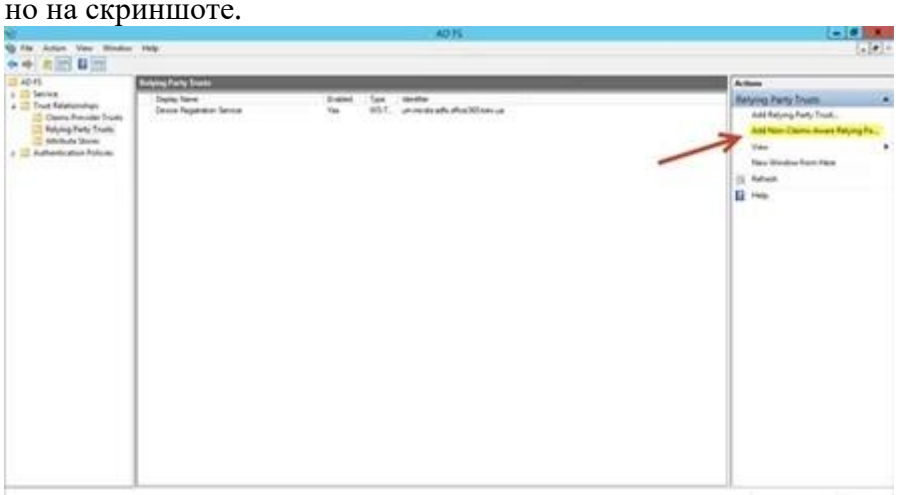
Active Directory Federation Services (ADFS) – впервые появились с релизом обновления R2 2003 сервера. Основное назначение служб федерации — это возможности по части аутентификации клиентов на различных веб приложения через сеть интернет, а так же предоставления SSO. Сама же аутентификация будет работать на основании цифровых удостоверений (Claims) В данном ключе, Claims стоит рассматривать как некоторое удостоверение которое выдано третьей доверенной стороной, которой доверяют все участники процесса. В отличии от доменных служб Active Directory, в службах федерации не применяется протокол Kerberos. Это связано с тем, что протокол разрабатывался для применения в локальных сетях, но никак в сети интернет. Основные же протоколы, использующиеся в ADFS — Security Assertion Markup Language (SAML) и Simple Web Token (SWT) Оба протокола XML ориентированы и в качестве транспорта используют SSL 3.0 или TSL 1.0

В ADFS различают два важных понятия: поставщик аутентификации (Claims Provider Trust) и поставщик ресурсов (Relying Party Trusts)

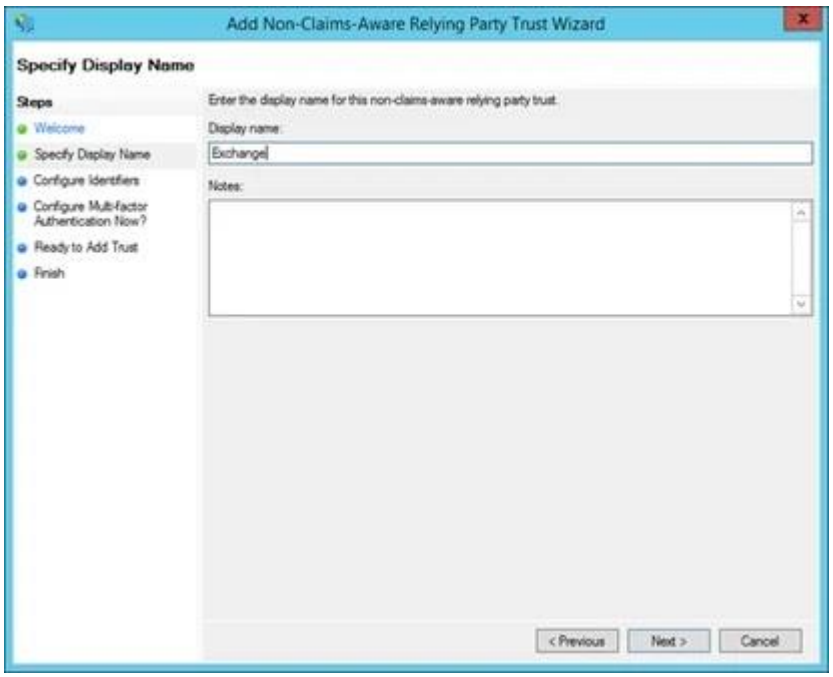
Claims Provider Trust – это организация, которая создает и управляет учетными записями ресурсов. Примером могут послужить те же самые службы ADDS, либо другие LDAP хранилища.
Relying Party Trusts — предоставляет доступ к ресурсам и управляет этим доступом. Например это может быть стороннее веб приложение расположенное вне пределах организации но настроенное на взаимодействие с поставщиком аутентификации.
В различной литературе, иногда оба понятия называют островами. В зависимости от задачи, которую будут решать службы федерации, острова могут находится в различных организациях либо в рамках одной. Задача же ADFS как раз и будет состоять в объединении этих островов.
Вернемся в рамки нашей текущей задачи. Для Claims Provider Trust будут использоваться доменные службы Active Directory, а в качестве Claims Provider Trust я создам нового поставщика услуг для Exchnage сервера.
Для этого на сервере с установленными службами ADFS, в моем демо-стенде это сервер srv-adfs.office365.local, перейдем в консоль AD FS Management.



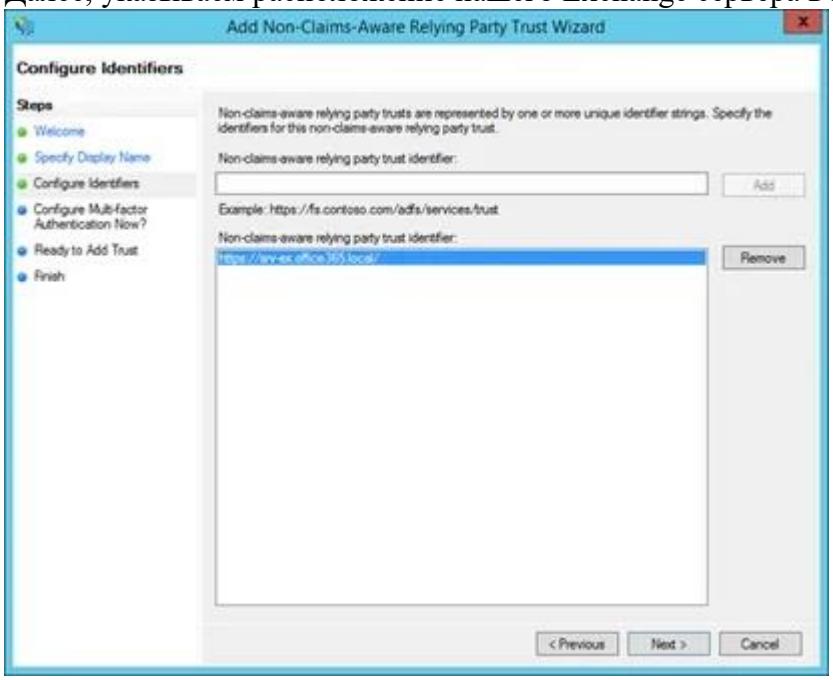
Далее, в Trustrelationship выберем Add Non-Claims-Aware Relying Party trust, как показано на скриншоте.



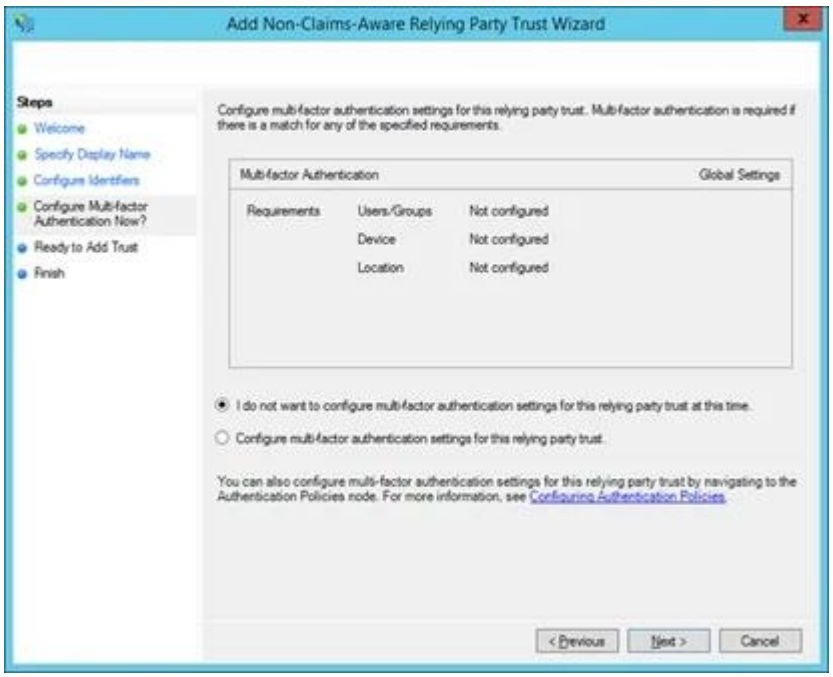
В качестве имени, выберем Exchange.



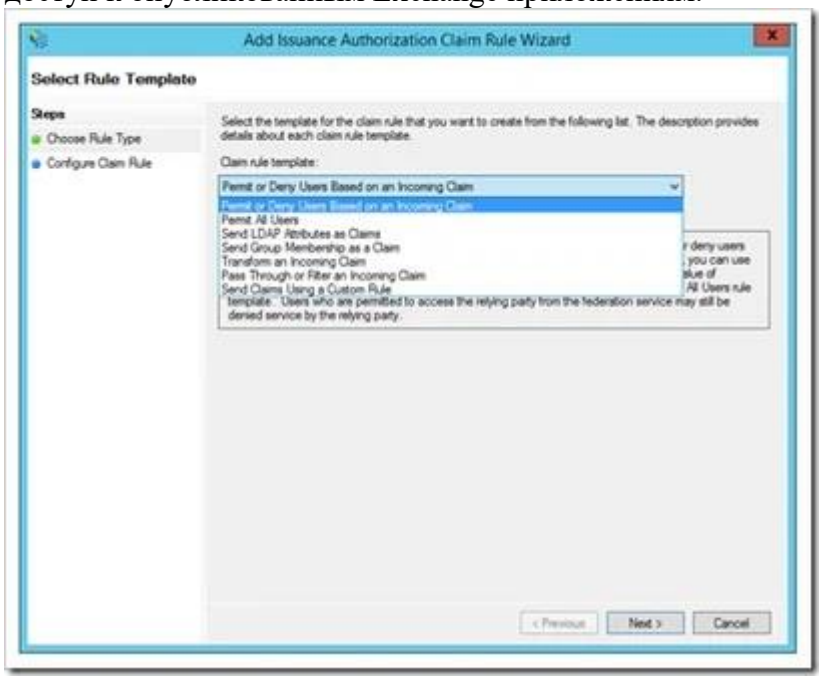
Далее, указываем расположение нашего Exchange сервера в интрасети



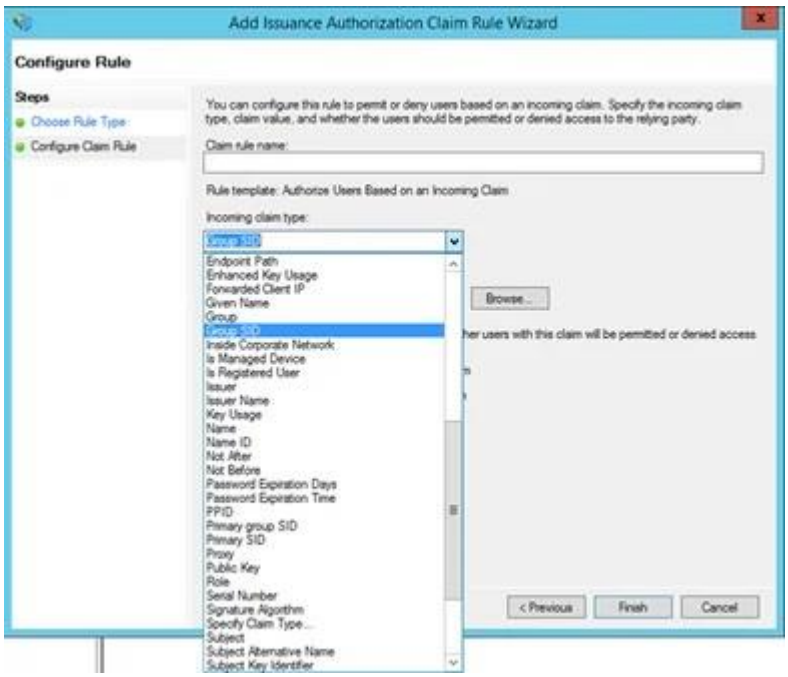
На следующем шаге мы не будем настраивать мульти-факторную аутентификацию.



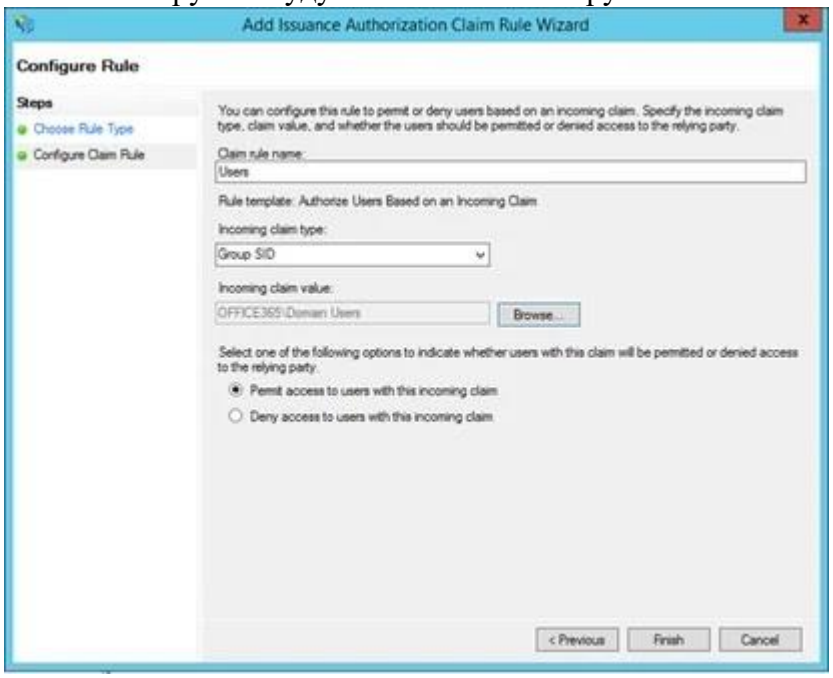
После завершения работы мастера, мы настроили нового поставщика услуг для Exchange теперь нужно создать авторизационные правила, по которым будет регламентироваться доступ к опубликованным Exchange приложениям.



В качестве примера, я создам правило которое будет действовать на основе атрибута SID группы объектов Active Directory.



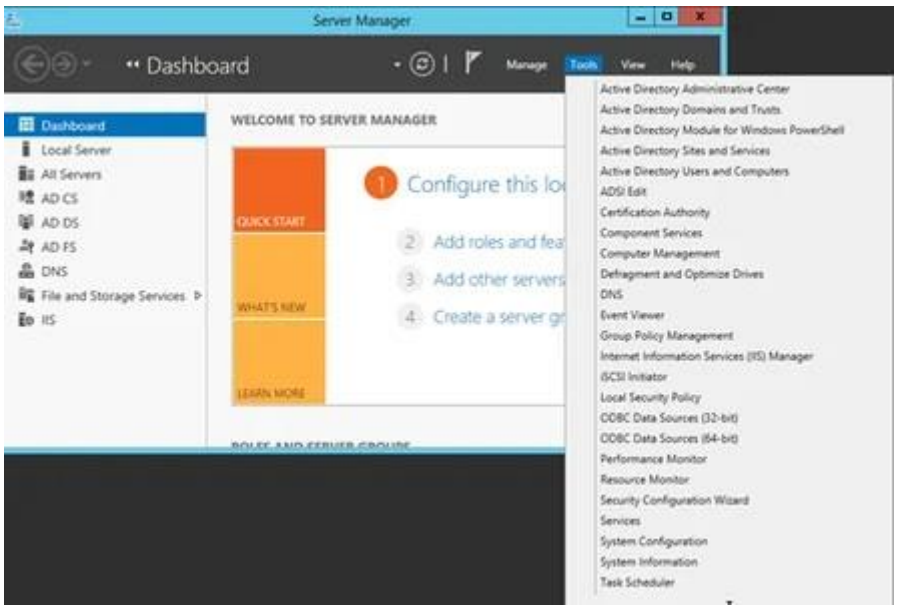
В качестве группы будут использоваться группа domain users.



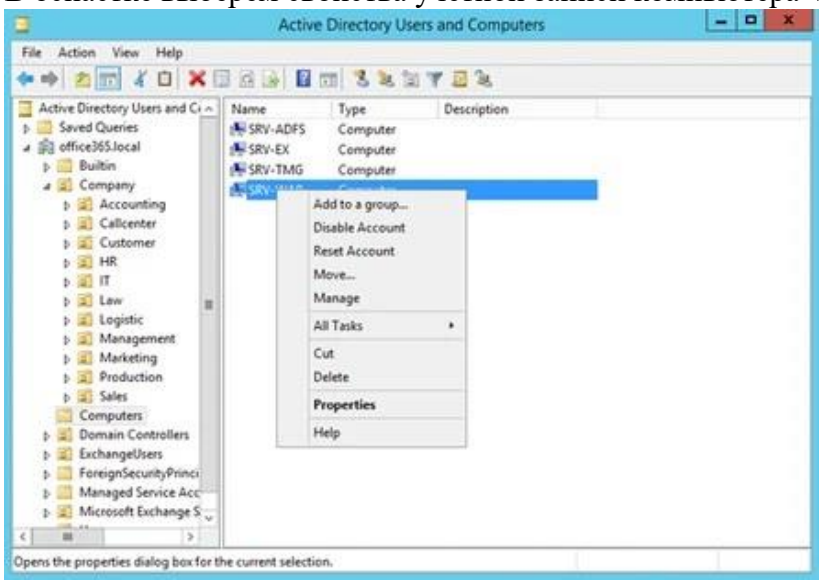
По завершению мастера, у меня получилось простое правило разрешающее всем пользователям домена получать доступ к опубликованным приложениям Exchange. В производственной среде вы можете комбинировать различные правила, тем самым довольно точно регламентировать конечный доступ к приложения.

Конфигурирование ADDS

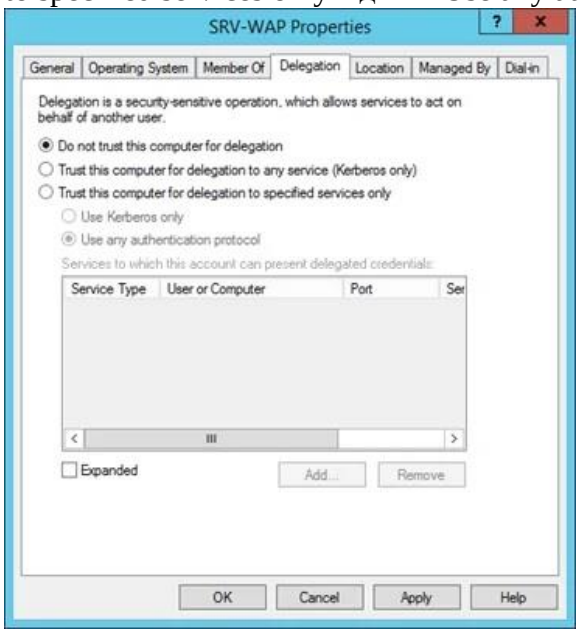
Со стороны ADDS, нам нужно настроить делегирование на учетной записи компьютера сервера WAP. Данный шаг нам необходим, так как поставщик ресурсов для Exchnage Server будет использовать встроенную проверку подлинности Windows в процессе аутентификации. Для этого с Server Manager запустим оснастку Active Directory Users and Computers.



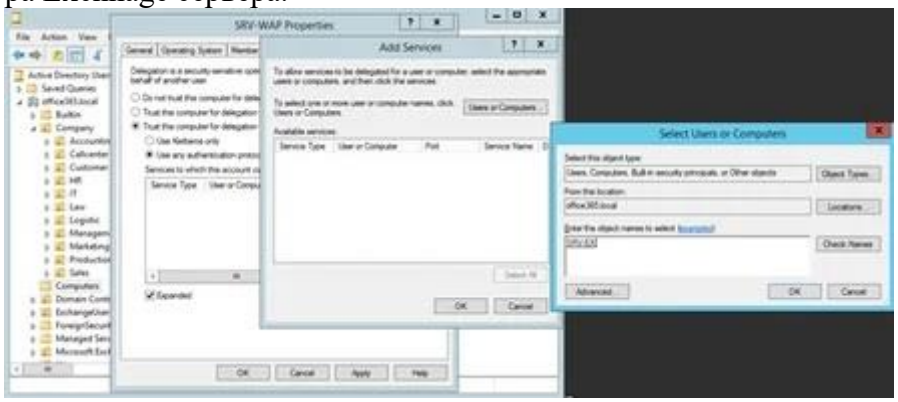
В оснастке выберем свойства учетной записи компьютера WAP сервера.



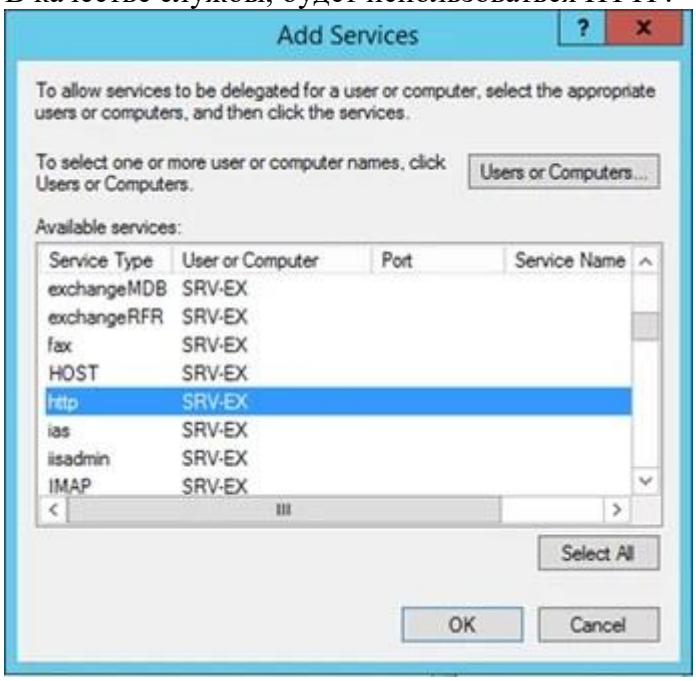
Во вкладке Delegation, выставляем радиобокс напротив Trust this computer for delegation to specified services only а далее Use any authentication protocol.



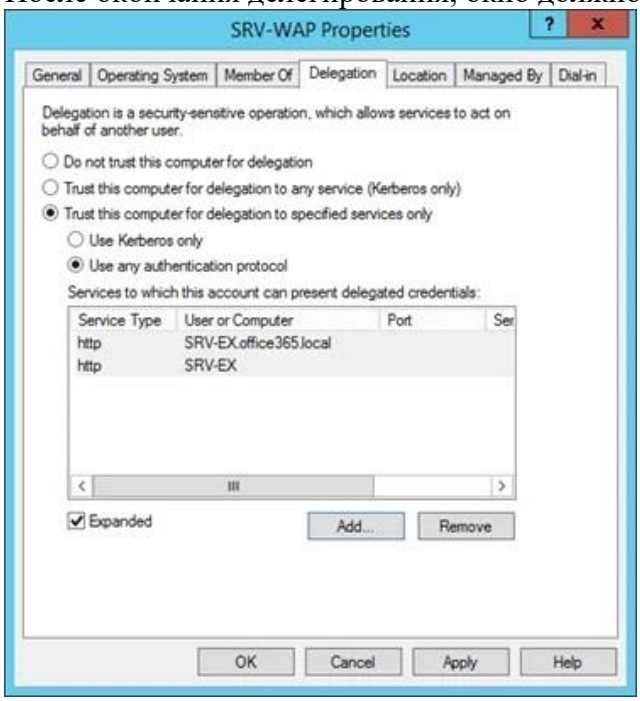
Далее, как показано на скриншоте, нужно выбрать доменную учетную запись компьютера Exchnage сервера.



В качестве службы, будет использоваться HTTP.

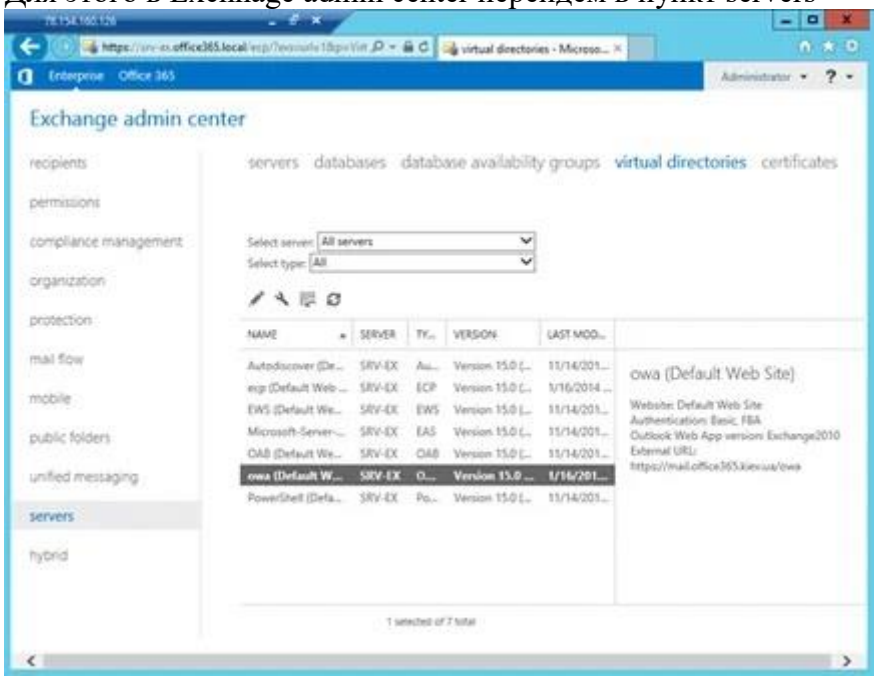


После окончания делегирования, окно должно иметь следующий вид



Конфигурирование Exchange Server

На стороне Exchange Server нам нужно лишь поменять методы аутентификации на веб каталогах OWA и ECP с FBA на встроенную проверку подлинности Windows.
Для этого в Exchnage admin center перейдем в пункт servers



И выставим соответствующие настройки на веб каталогах после чего следует перезапустить IIS сервер.

2.14. Практическая работа № 14
Настройка шифрования и расширенного аудита

Задание:

1. Установка BitLocker с помощью диспетчера серверов

- Откройте Диспетчер серверов, выбрав значок Диспетчер серверов или выполняющий servermanager.exe.
- Нажмите кнопку **Управление** на панели **навигации диспетчера серверов** и выберите пункт **Добавить роли и функции** , чтобы запустить **Мастер добавления ролей и компонентов.**
- После открытия **мастера добавления ролей и компонентов** нажмите кнопку **Далее** на **начальной** странице (если она отображается).
- На панели " **тип установки** " **мастера "Добавить роли и компоненты** " выберите установку на основе **ролей или компонентов** и нажмите кнопку **Далее** , чтобы продолжить.
- Выберите в области **выбора сервера** пункт **выбрать сервер из пула серверов** и подтвердите, что у вас установлен компонент BitLocker.
- Серверные роли и компоненты устанавливаются с помощью одного и того же мастера в диспетчере серверов. Нажмите кнопку **Далее** в области **роли сервера** мастера **Добавить роли и компоненты** , чтобы перейти к области **функции** .
- Установите флажок рядом с **компонентом Шифрование диска BitLocker** в окне "компоненты" **мастера "Добавить роли и компоненты**". Мастер отобразит дополнительные функции управления, доступные для BitLocker. Если вы не хотите устанавливать эти компоненты, снимите флажок **включить средства управления** и нажмите кнопку **Добавить компоненты**. После завершения выбора дополнительных функций нажмите кнопку **Далее** , чтобы продолжить работу с мастером.

Примечание. Функция **Enhanced Storage** является обязательной функцией для включения BitLocker. Эта функция обеспечивает поддержку зашифрованных жестких дисков в системах, поддерживающих шифрование.

- На панели **подтверждения мастера добавления ролей и компонентов** нажмите кнопку **установить** , чтобы начать установку компонентов BitLocker. Для завершения работы средства BitLocker требуется перезагрузка. При установке флажка **автоматически перезапускать сервер назначения** после завершения установки на панели **подтверждения** будет принудительно перезапустить компьютер.
- Если параметр **автоматически перезагружает сервер назначения, если** он не установлен, в **области результатов мастера добавления ролей и компонентов** будет отображено сообщение об успешном завершении установки компонента BitLocker. При необходимости в тексте результатов будет выводиться уведомление о дополнительных действиях, необходимых для завершения установки компонента (например, перезагрузка компьютера).

2. Установка BitLocker с помощью Windows PowerShell

Windows PowerShell позволяет администраторам еще одним вариантом для установки компонентов BitLocker. Windows PowerShell устанавливает функциональные возможности с помощью servermanager модуля "или" dism , однако servermanager модули не dism всегда имеют функцию "контроль четности". Поэтому перед установкой рекомендуется подтвердить имя компонента или роли.

Примечание. Для завершения установки BitLocker необходимо перезапустить сервер.

3. Настройка расширенного аудита.

Шаг 1

Мы открываем наш Диспетчер серверов или Диспетчер серверов. Мы нажимаем на **Инструменты** и выбираем опцию **Управление групповой политикой.**

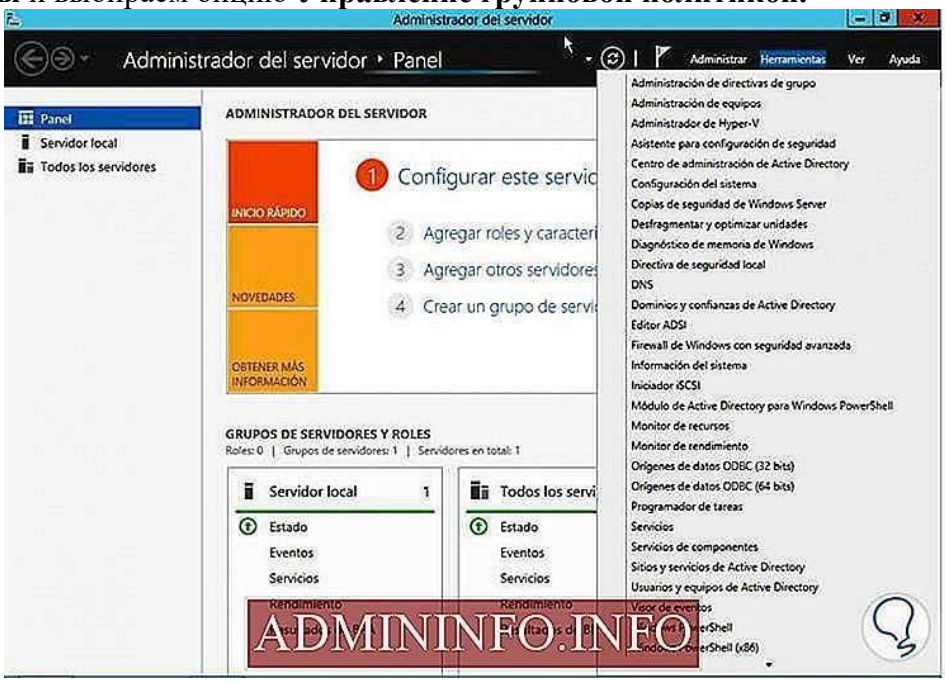


Рис. 145

Это отобразит меню GPO, мы должны отобразить текущий домен и щелкнуть правой кнопкой мыши по **Политике домена** по **умолчанию.**

Рис. 146

Шаг 2
Мы выбираем опцию **Изменить,** и **будет** отображаться **редактор управления групповой политикой.**

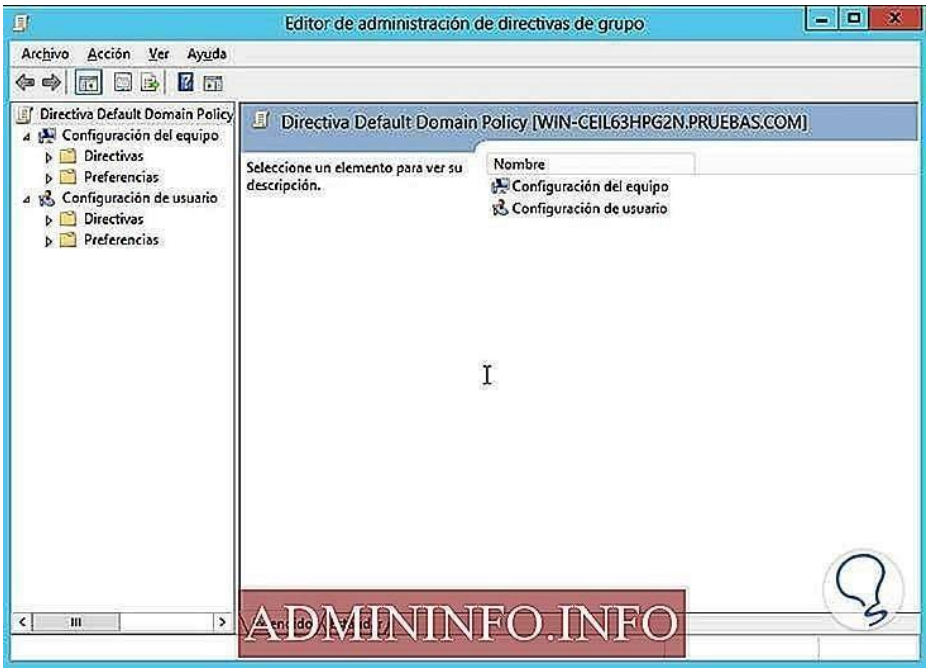


Рис. 147

Мы развернем следующий маршрут:

- Конфигурация оборудования
- Директивы
- Настройки Windows
- Настройки безопасности

- Местные директивы
- Директива об аудите

Рис. 148

Шаг 3

Мы увидим окно с различными **параметрами для аудита**:

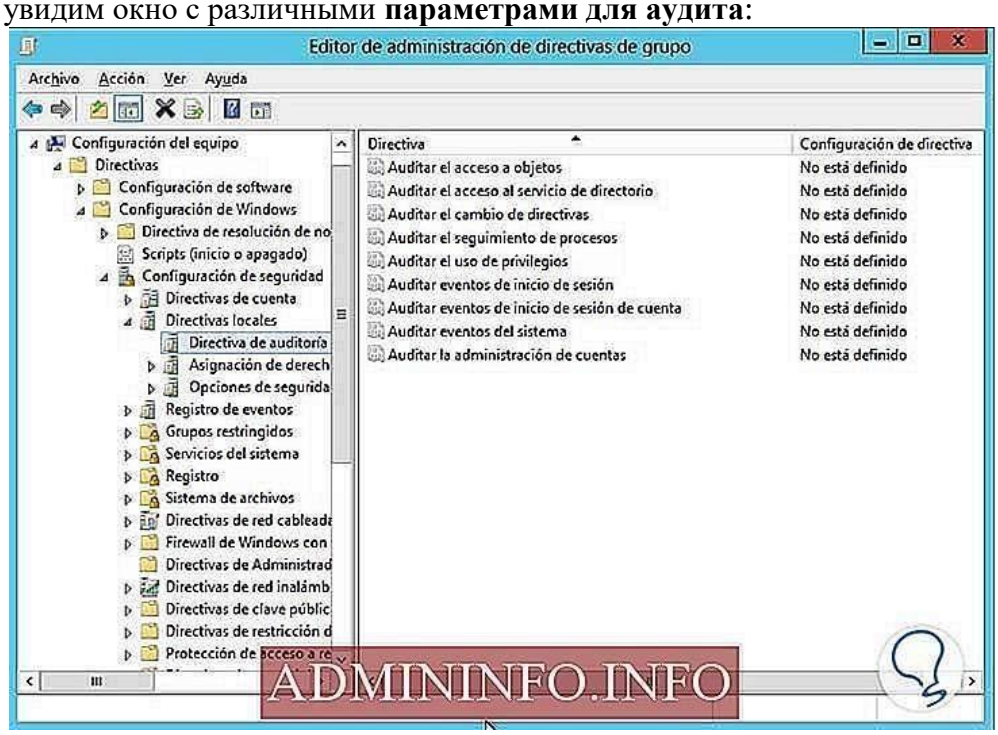


Рис. 149

Дважды щелкните опцию **Аудит событий входа в систему**, и мы увидим, что окно свойств указанного аудита открыто.

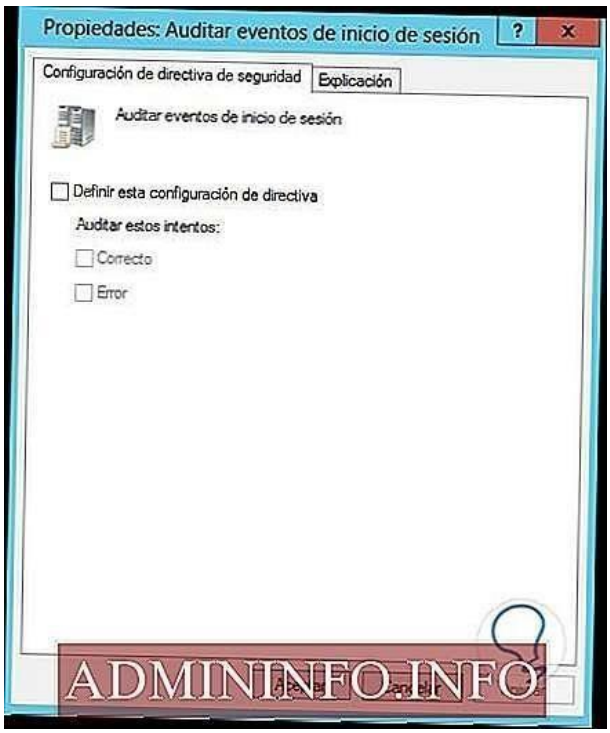


Рис. 150

Установите флажок **Определите этот параметр политики,** чтобы включить эту политику, **установите** оба флажка (Исправить и Ошибка) и нажмите **Применить** и, наконец, **ОК,** чтобы сохранить изменения.

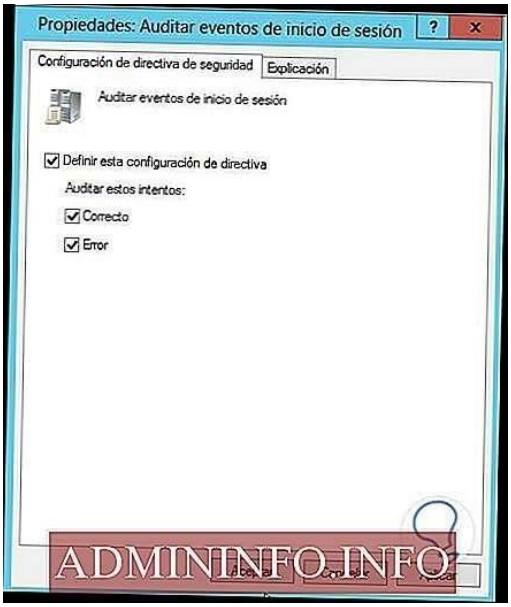


Рис. 151

Мы увидим изменения, отраженные в нашем аудите:

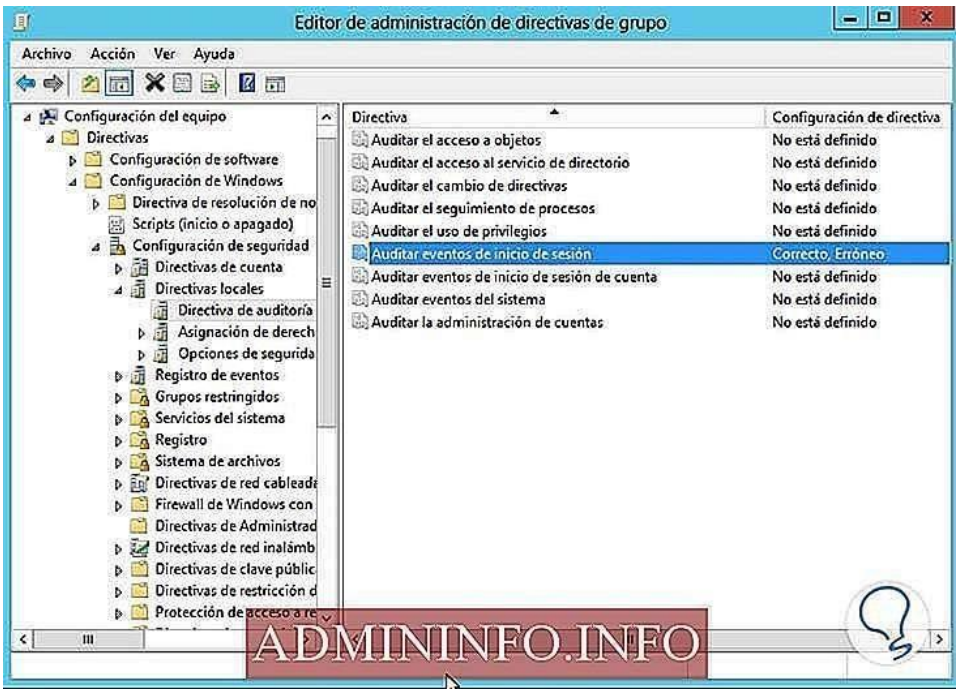


Рис. 152

4. **Внедрить политику аудита (файл или папка)**

Мы можем добавить тип аудита к определенному файлу или папке, для этого мы выполним следующий процесс:

Шаг 1

Мы щелкаем **правой кнопкой мыши** по папке, которую хотим назначить аудиту, и выбираем опцию **«Свойства».**

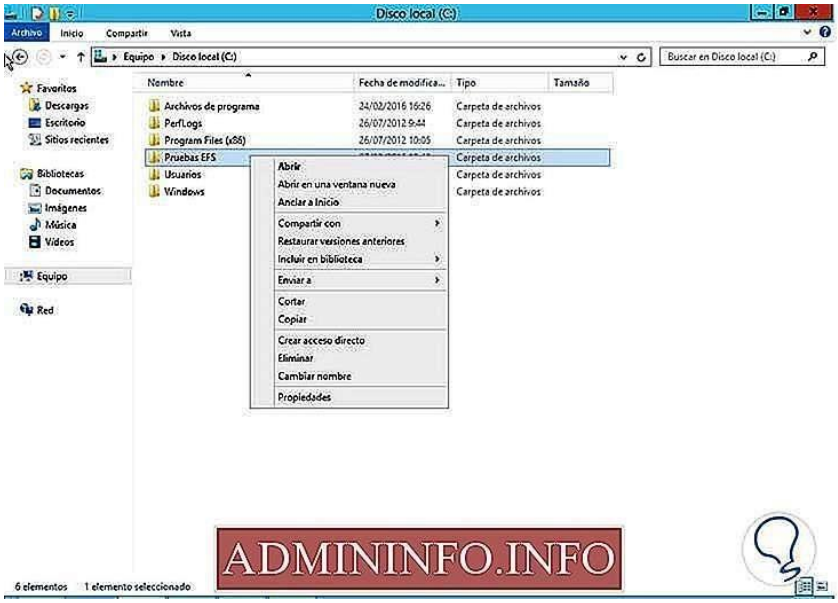


Рис. 153

В окне « **Свойства»** выбираем вкладку « **Безопасность** » **.**

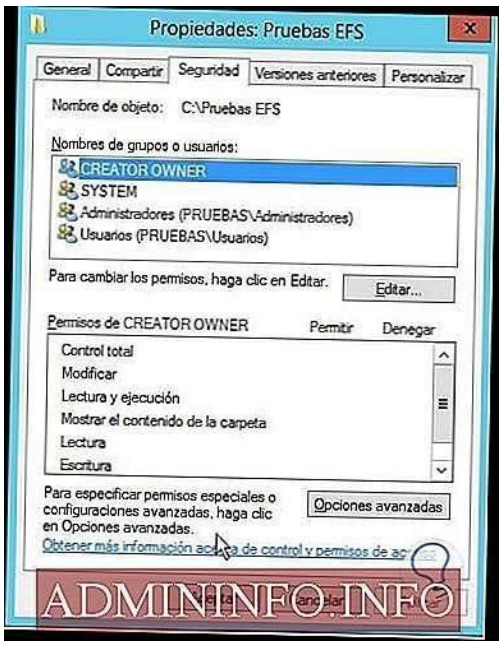


Рис. 154

Шаг 2
Мы нажимаем на Дополнительные параметры, и появится следующее окно:

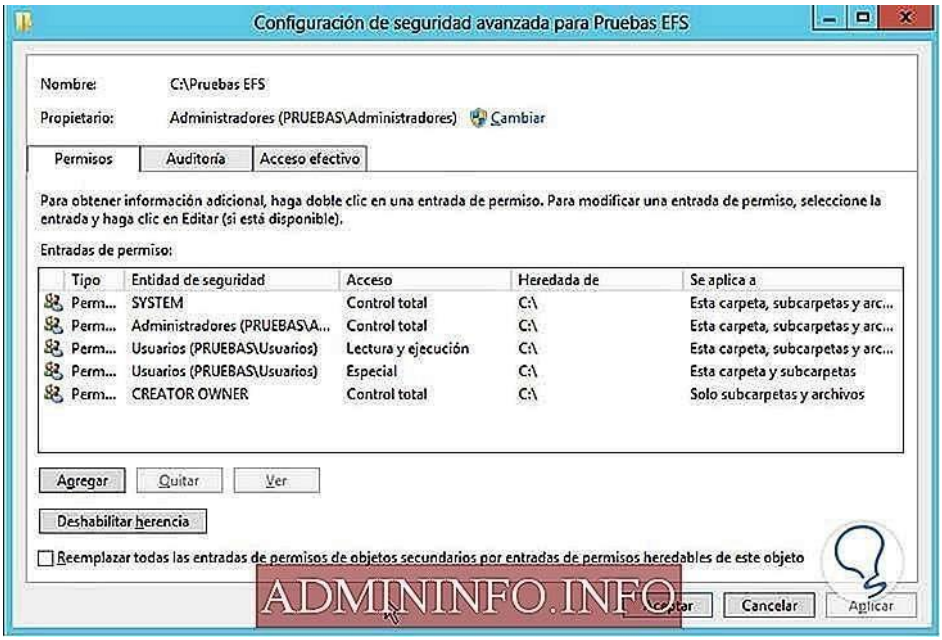


Рис. 155

Мы нажимаем на опцию **Аудит,** а затем на **Добавить.**

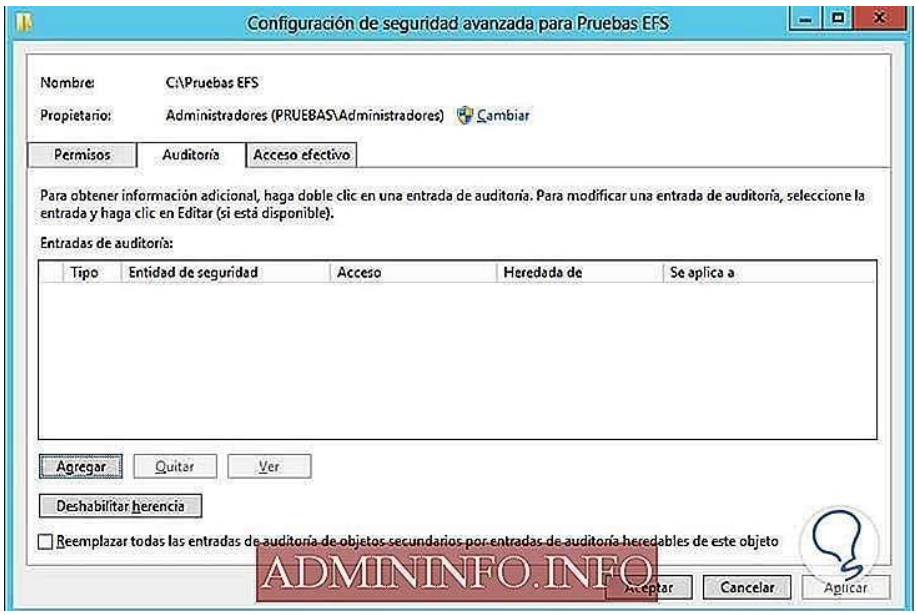


Рис. 156

Шаг 3

В открывшемся окне мы выбираем опцию **Выберите объект безопасности,** чтобы найти, какую политику добавить.

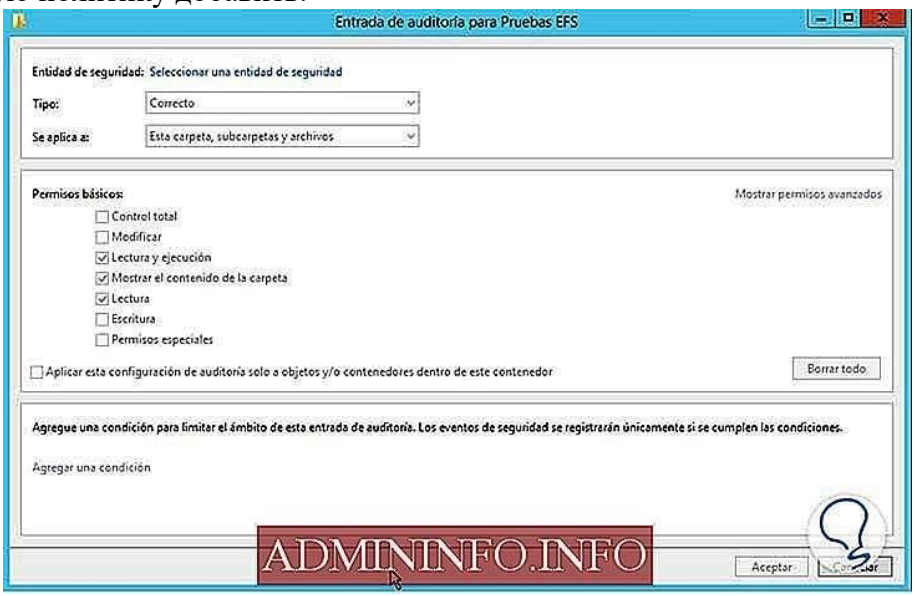


Рис. 157

Рис. 158

Мы выбираем **объект для применения аудита** :

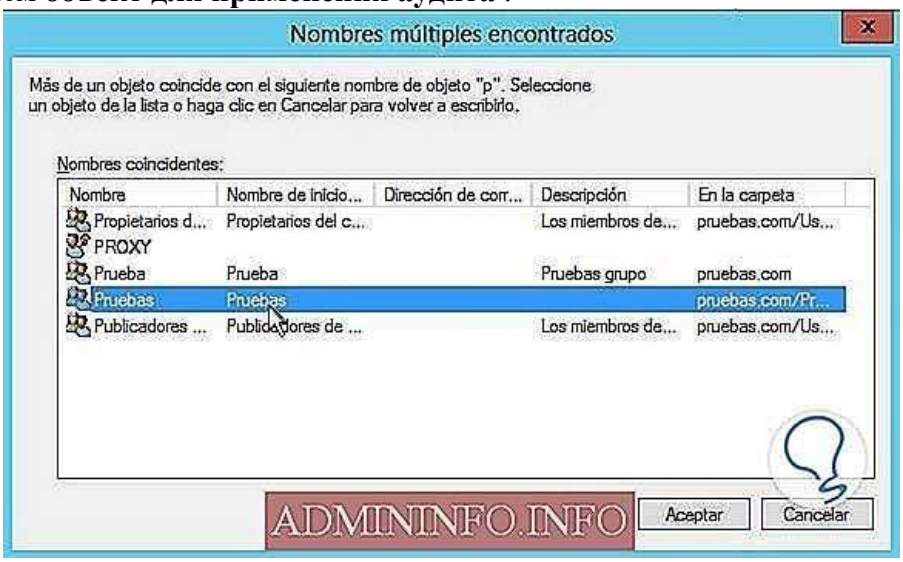


Рис. 159

Наконец, мы указываем параметры аудита (чтение, запись и т. Д.), Нажимаем **ОК,** чтобы сохранить изменения.

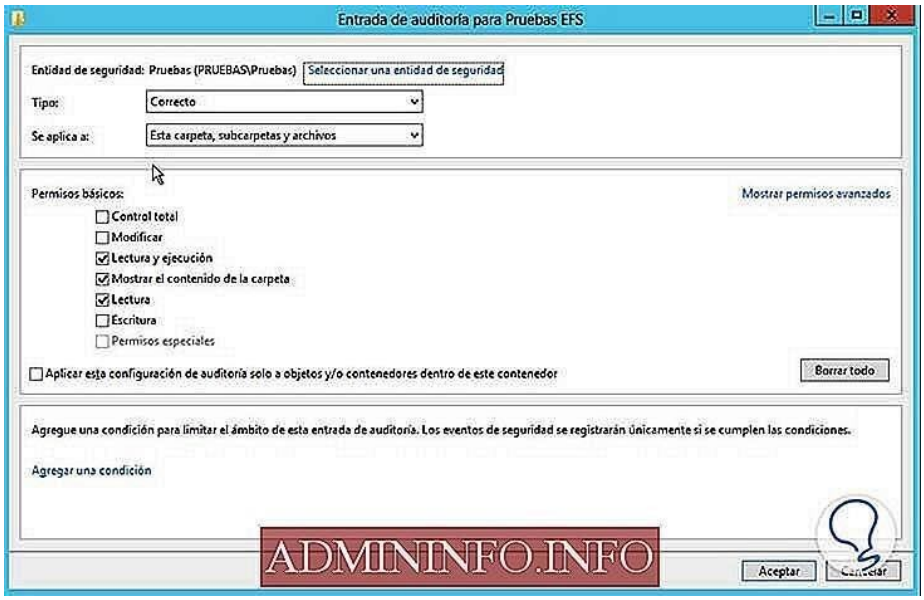


Рис. 160

Сделайте скриншоты (фотографии) процесса настройки шифрования и расширенного аудита и вставьте в отчёт.

2.15. Практическая работа № 15
Использование службы развертывания Windows для развертывания WindowsServer

Задание:

1. Заходим в диспетчер серверов, выбираем **Добавить роли и компоненты**

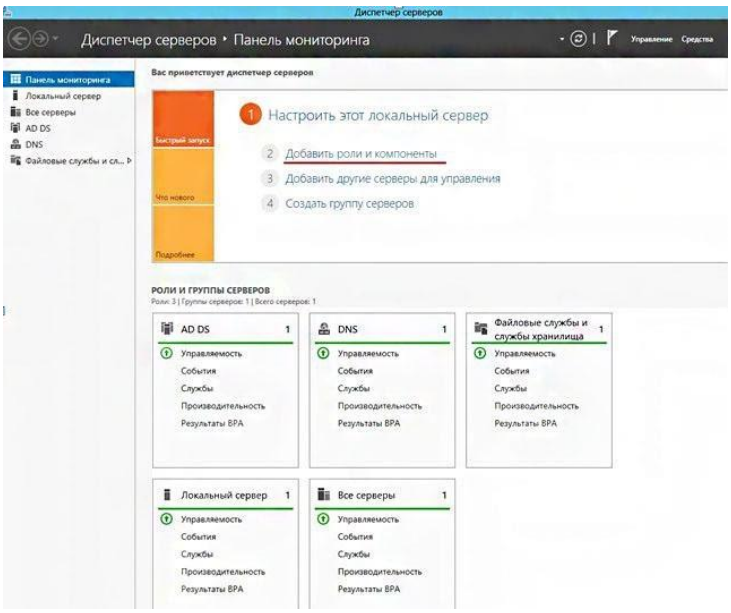


Рис. 161

Далее

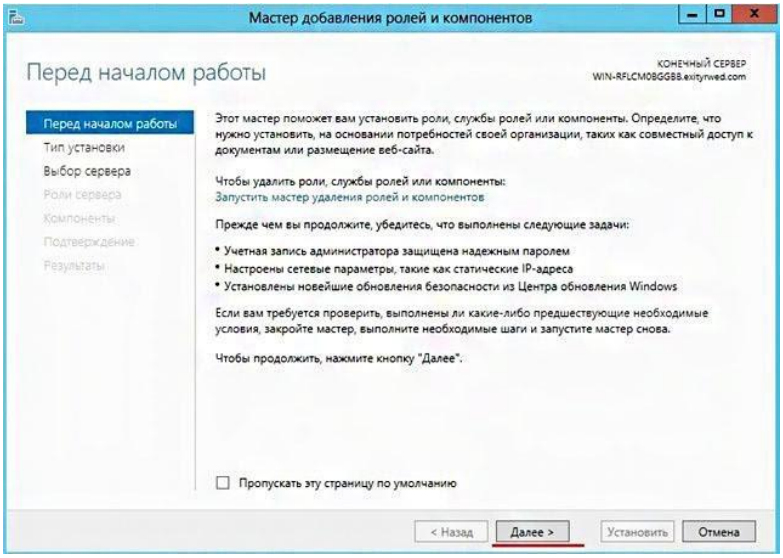


Рис. 162

Выбираем **Установка ролей или компонентов**

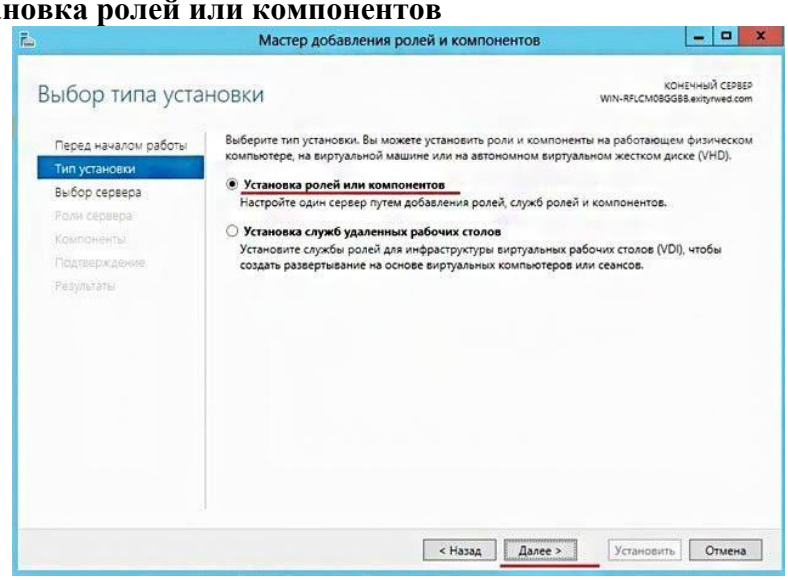


Рис. 163

Выбираем **целевой сервер**, далее

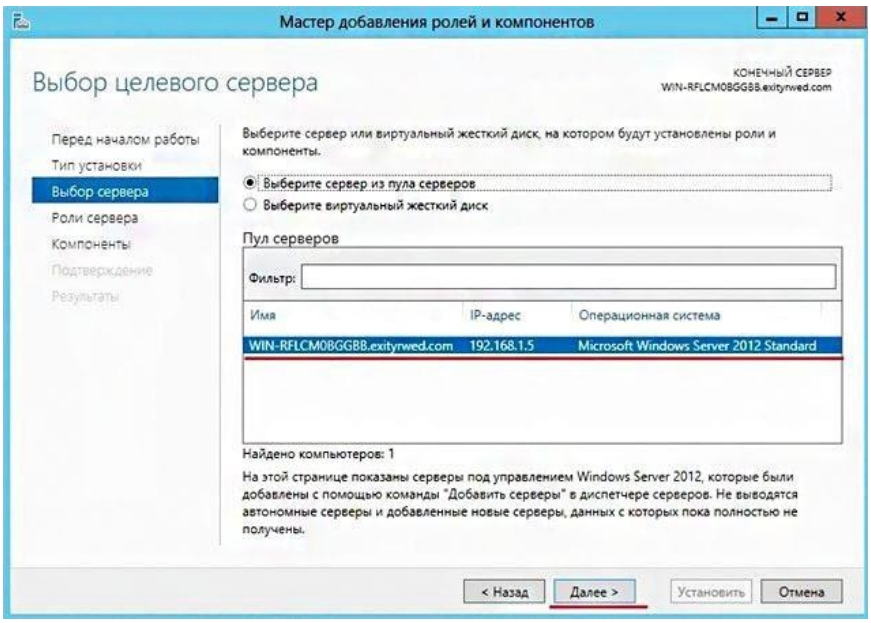


Рис. 164

Выбираем **службы развертывания Windows**, добавить компоненты

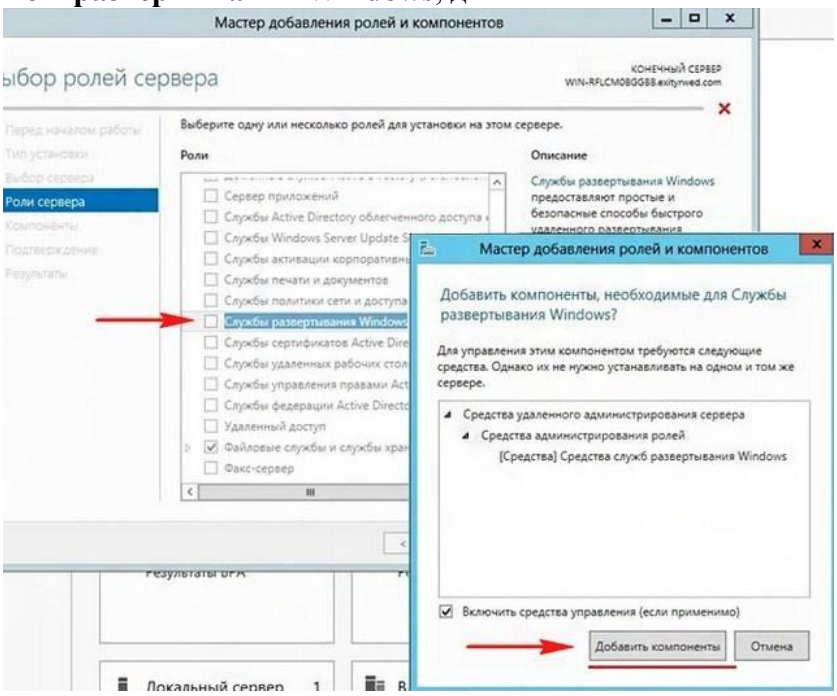


Рис. 165

Далее

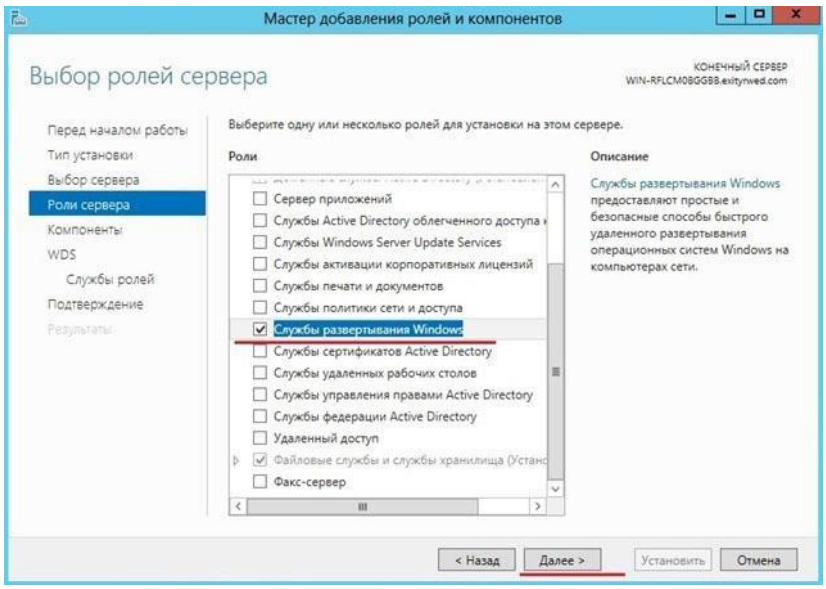


Рис. 166

Из компонентов ничего не нужно выбирать, далее

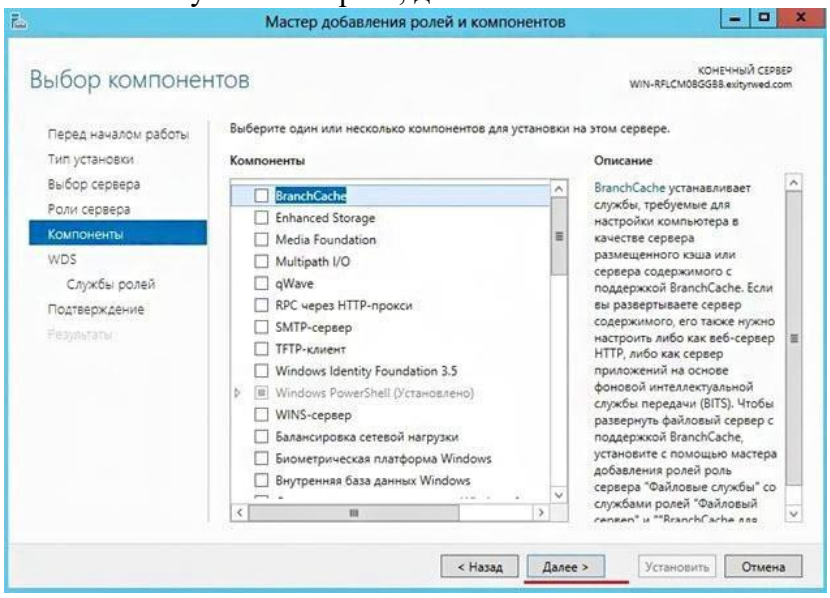


Рис. 167

Далее

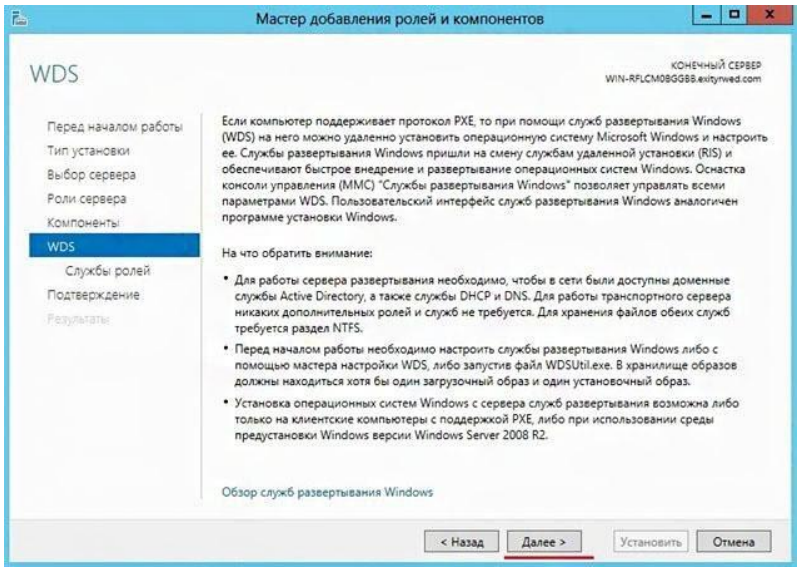


Рис. 168

Ставим галочки **Сервер развертывания** и **Транспортный сервер**. Далее

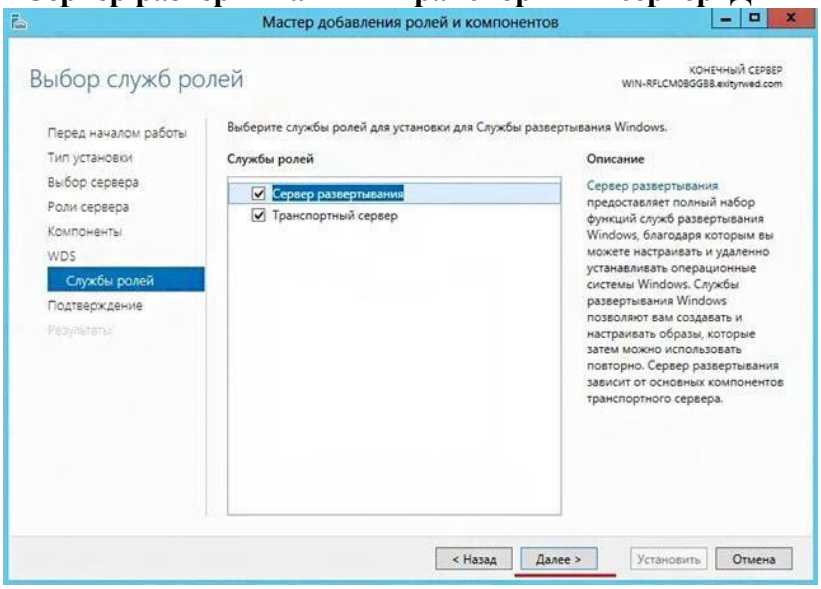


Рис. 169

Установить

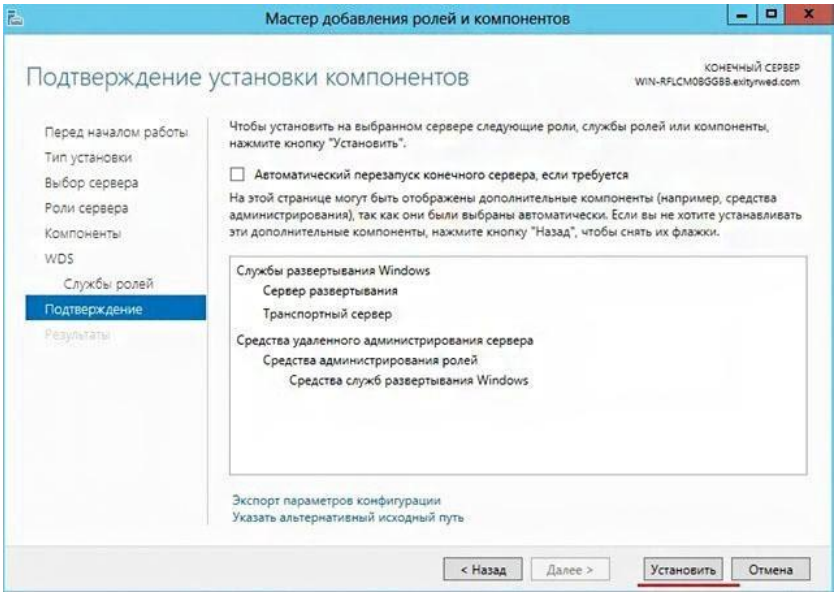


Рис. 170

Идет установка

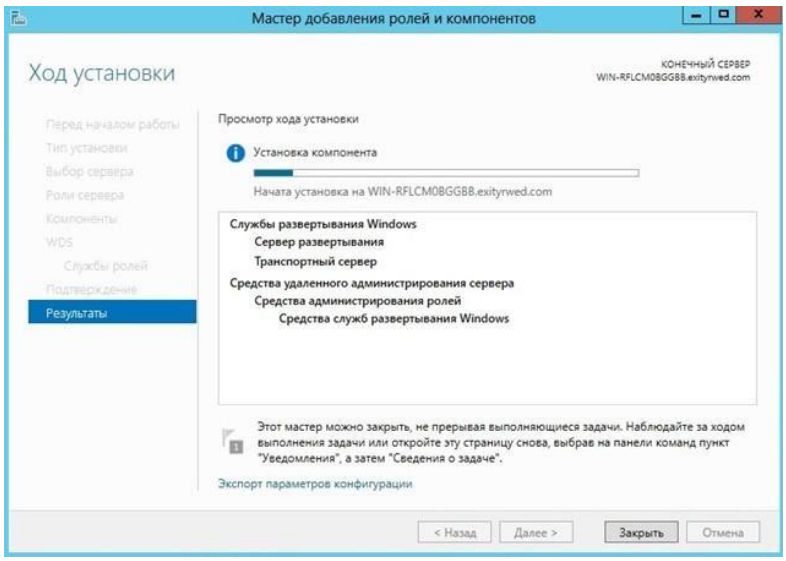


Рис. 171

Установка завершена

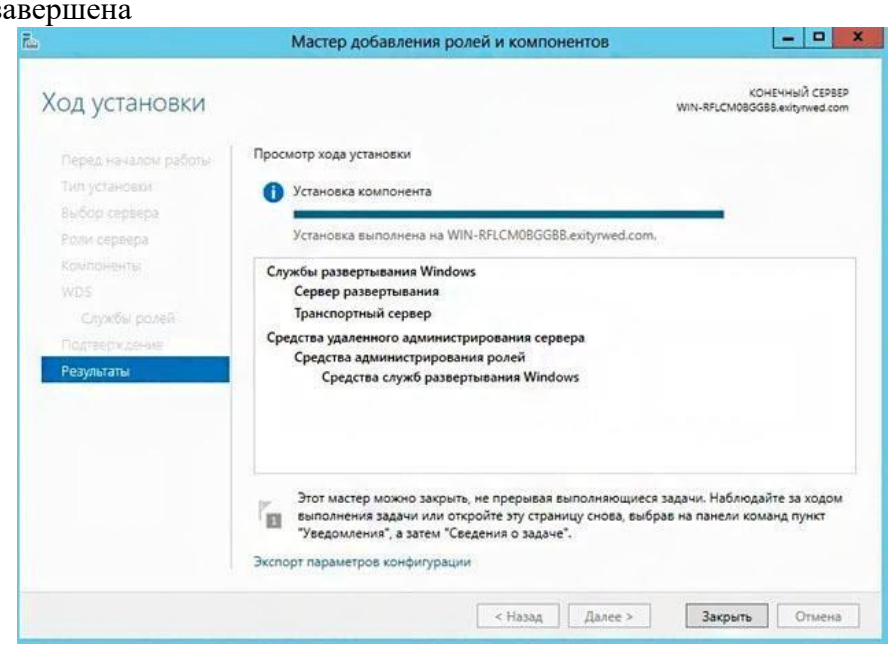


Рис. 172

Появился наш WDS

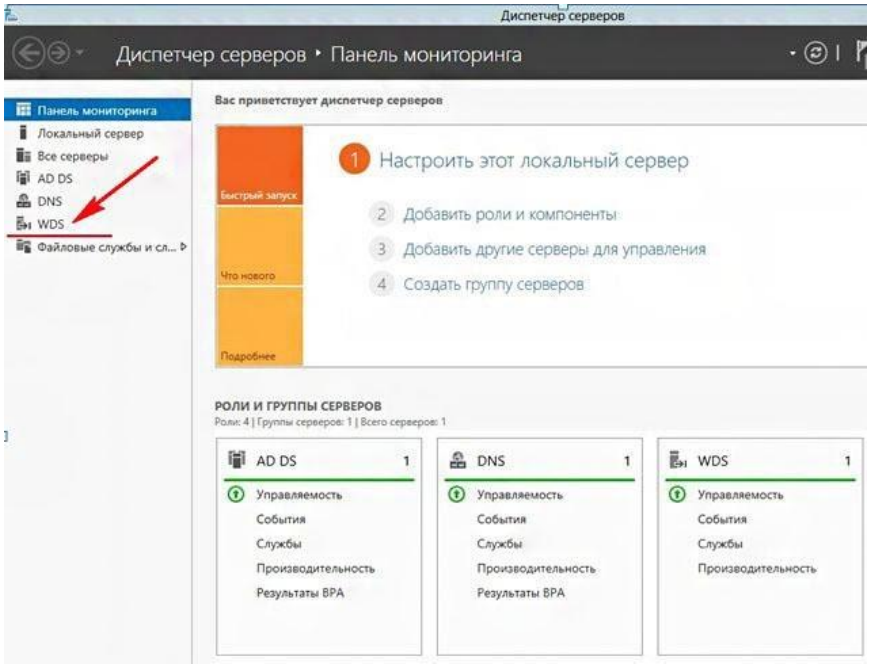


Рис. 173

Нажимаем на WDS, выбираем наш сервер WIN-RFLCMOBGGBB, щелкаем по нему правой кнопкой мыши тем самым вызвав контекстное меню и выбираем **Консоль управления службами развертывания Windows**

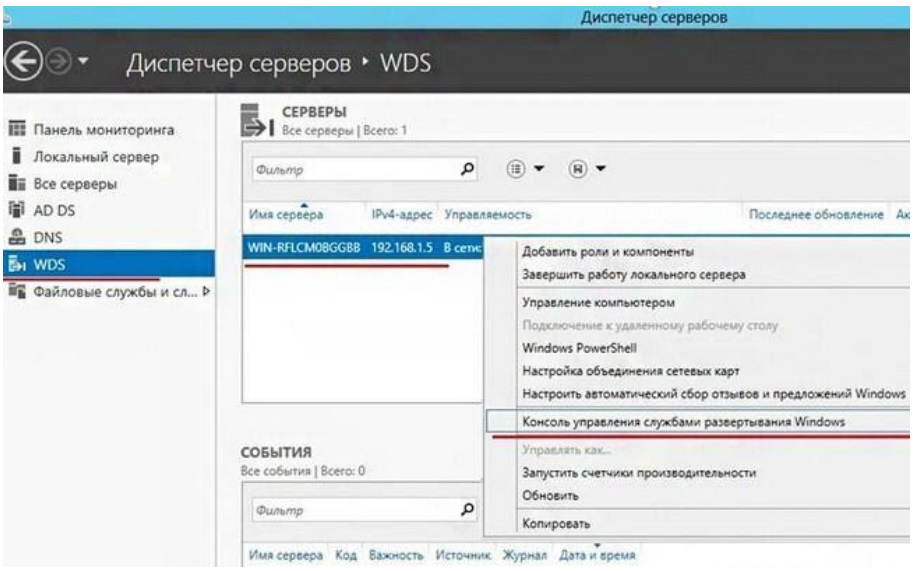


Рис. 174

Откроется окно консоли управления службами развертывания Windows. Как видим возле нашего сервера есть желтый значок в виде треугольника с восклицательным знаком, это значит что наш сервер требует настройки.

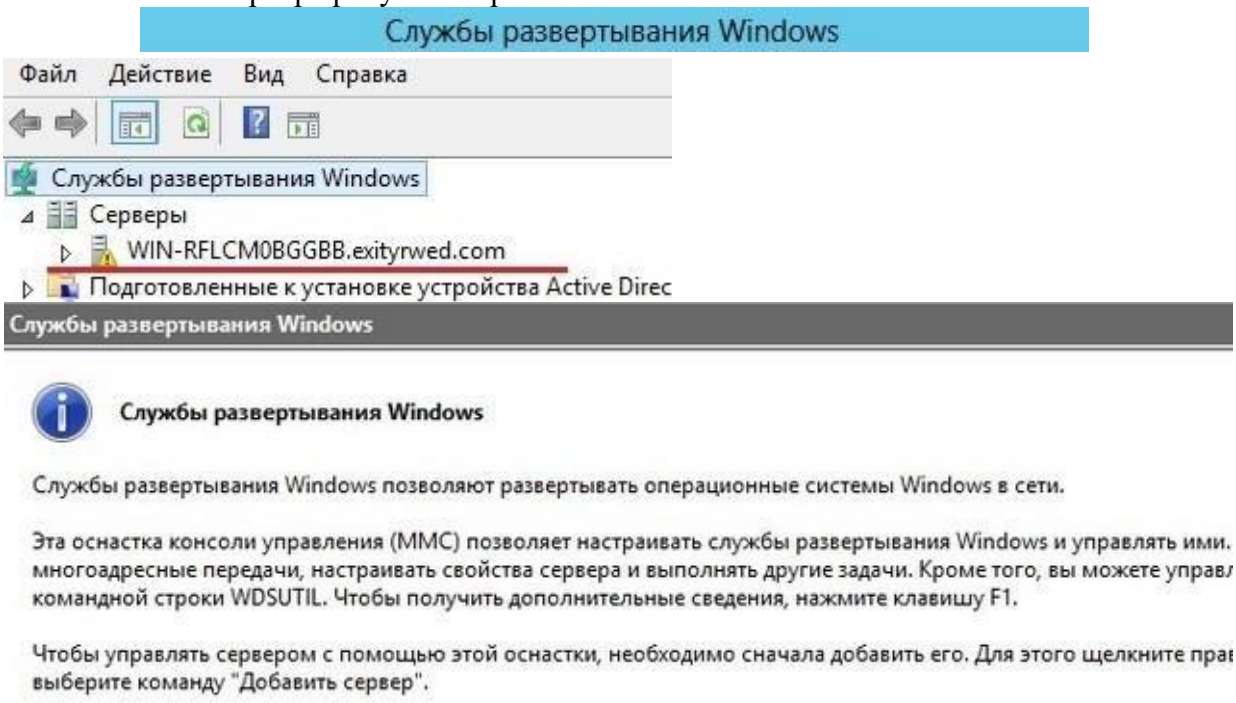


Рис. 175

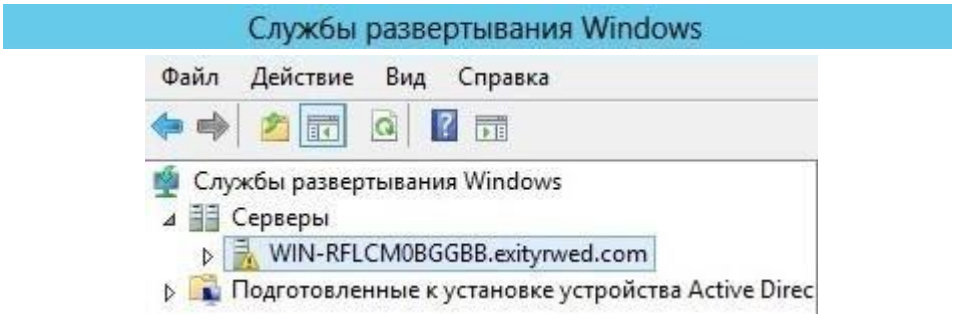
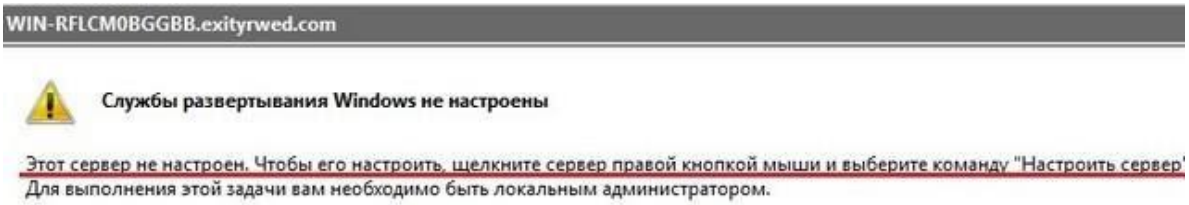


Рис. 176



Выбираем **Настроить сервер**

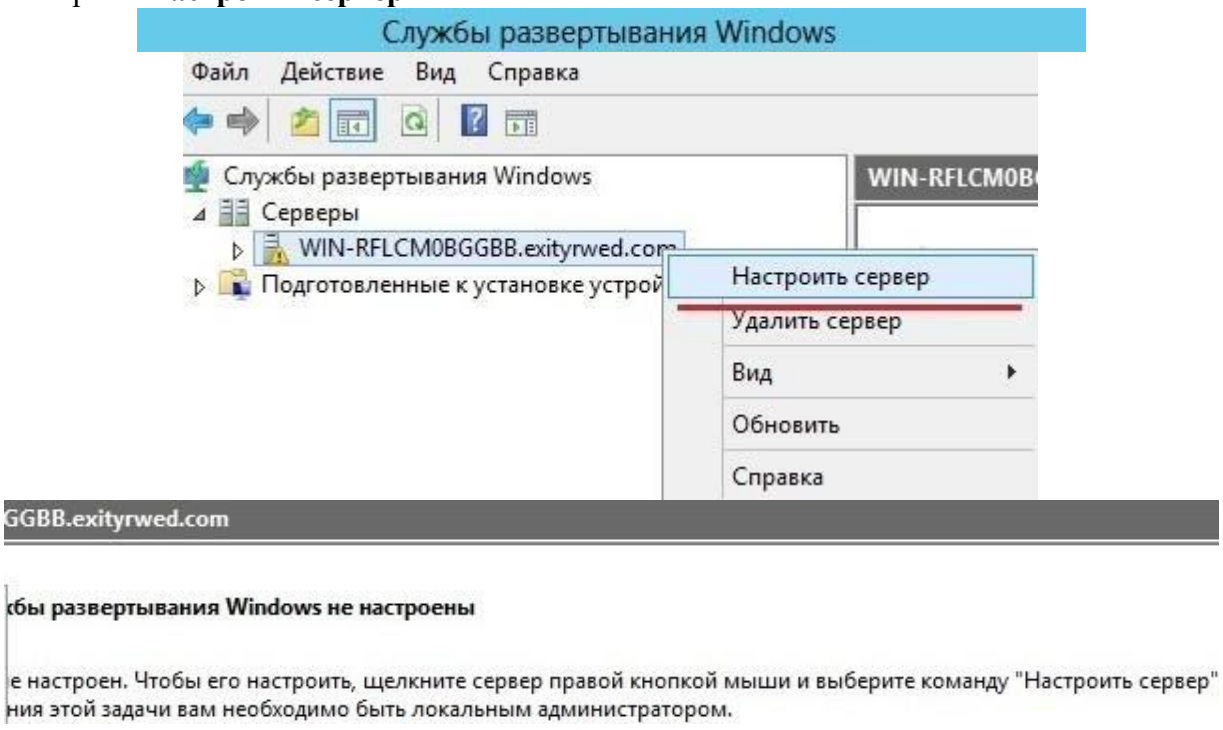


Рис. 177

Далее

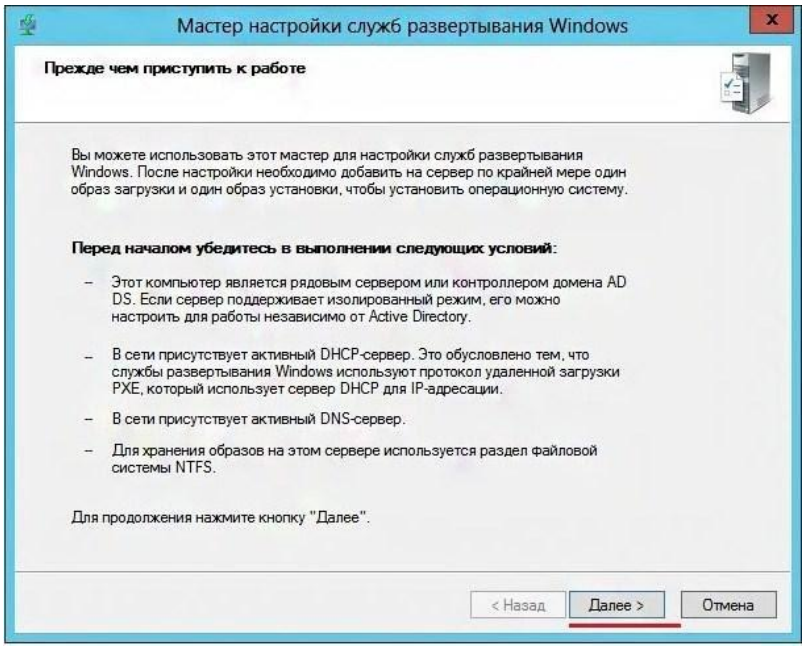


Рис. 178

Выбираем **Интеграция с доменными службами Active Directory**, далее

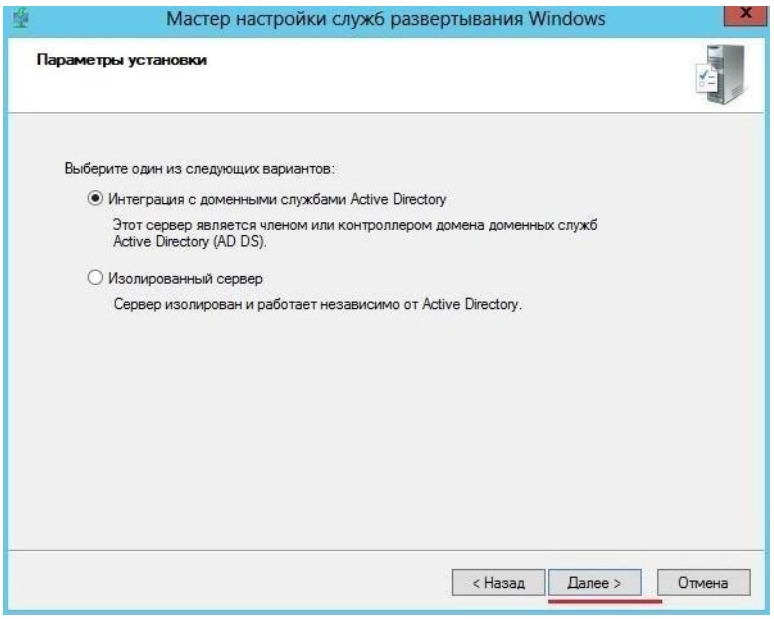


Рис. 179

Выбираем раздел для хранения загрузочных и установочных образов

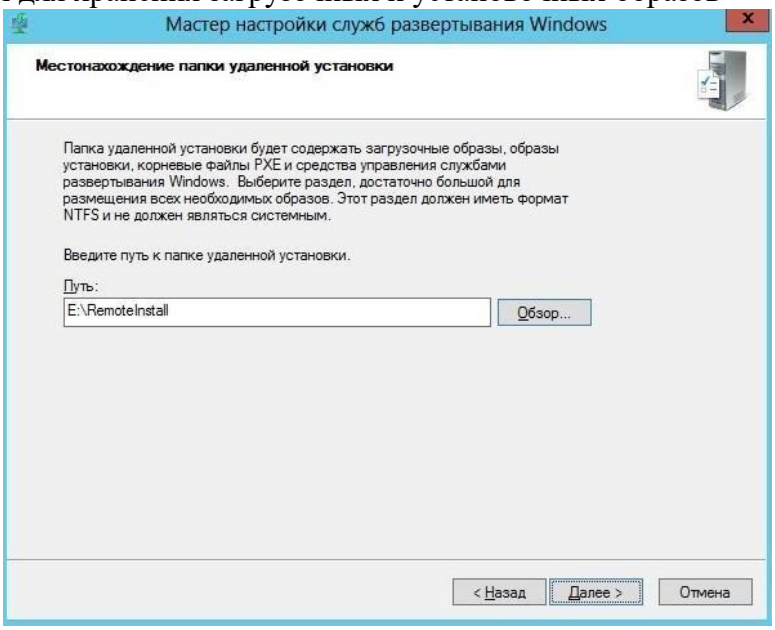


Рис. 180

Так как по умолчанию предлагается загрузочные и установочные образы хранить на системном диске (что не рекомендуется), то создадим на разделе E: папку RemoteInstall, которая и была указана мастеру настройки сервера

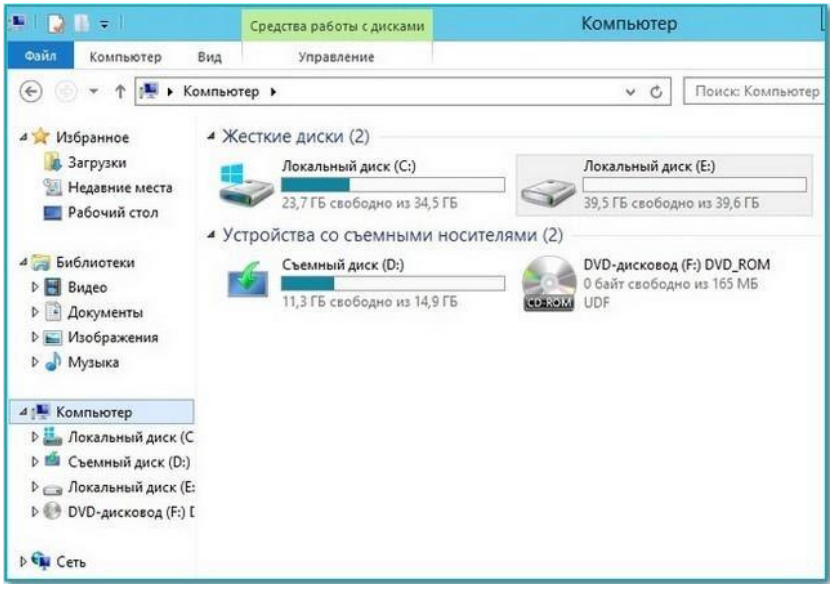


Рис. 181

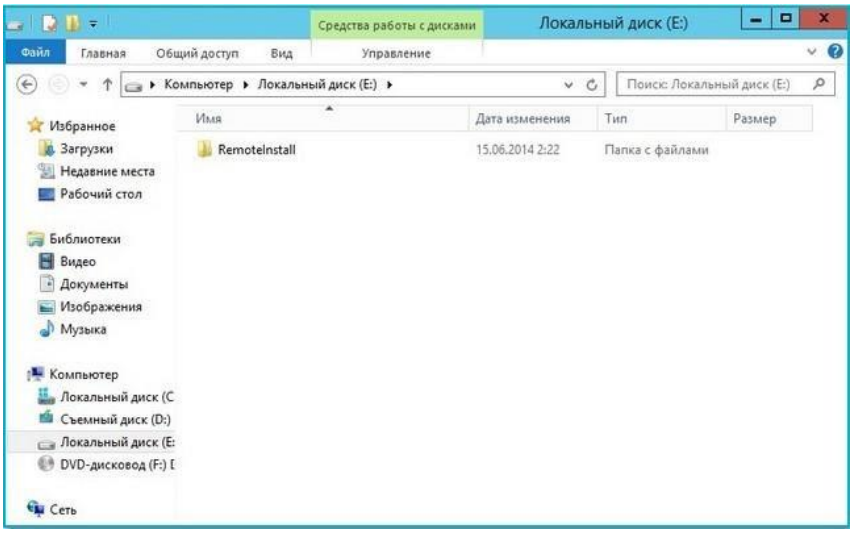


Рис. 182

Выбираем один из нескольких параметров (для начала можно выбрать **Не отвечать никаким клиентским компьютерам**). Далее

Далее

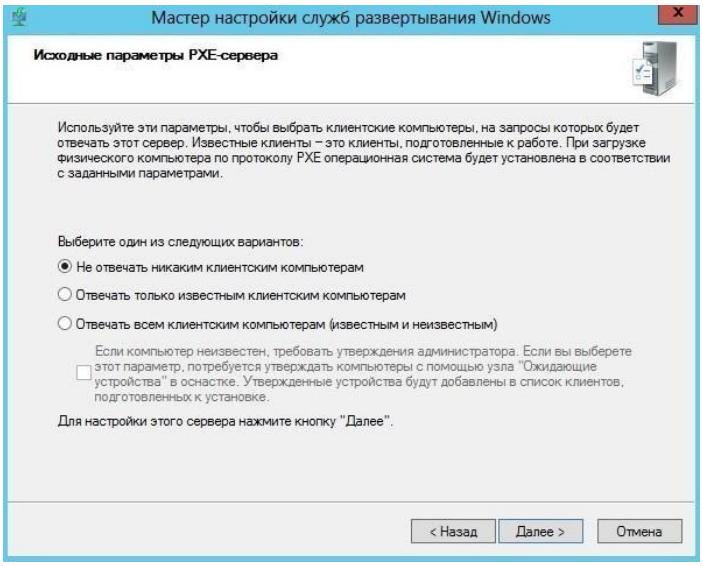


Рис. 183

Запуск служб развертывания Windows

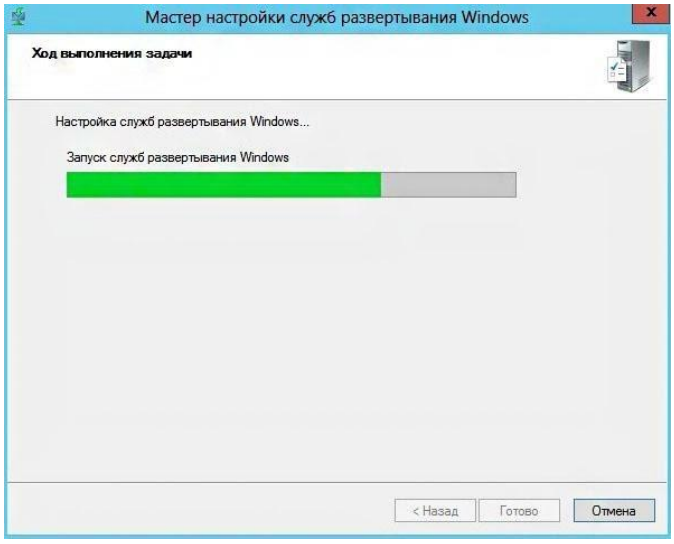


Рис. 184

Службы развертывания успешно настроены. Готово

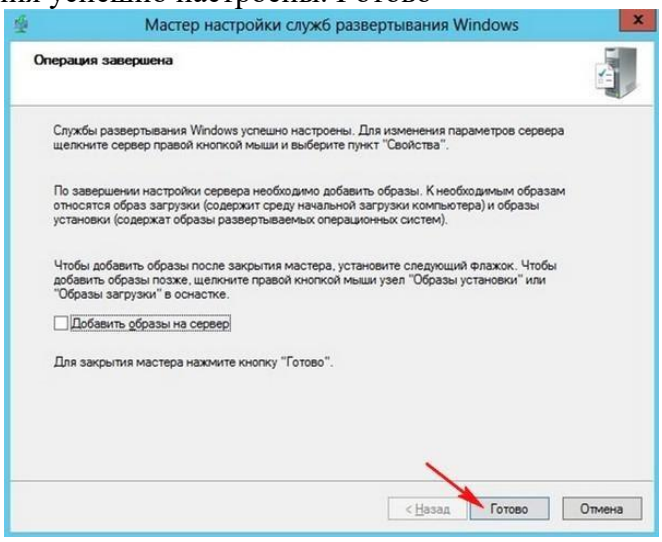


Рис. 185

Как видим, значок желтого треугольника с восклицательным знаком внутри исчез. Сервер настроен.

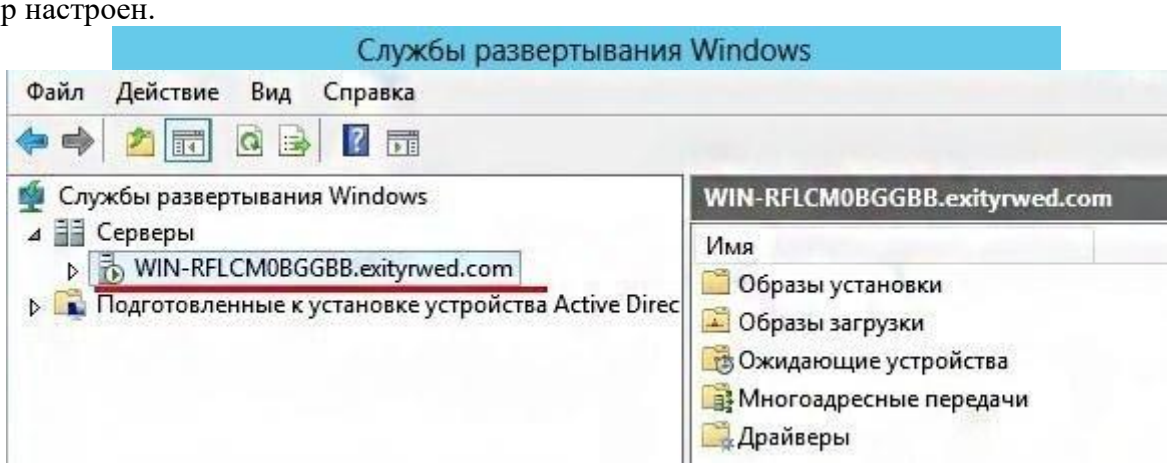


Рис. 186

Сделайте скриншоты (фотографии) процесса использования службы развертывания Windows и вставьте в отчёт.

2.16. Практическая работа № 16
Внедрение управления обновлениями

Задание:

1. Установка роли WSUS на Windows Server 2012 R2 / 2016

Еще в Windows Server 2008 сервис WSUS был выделен в отдельную роль, которую можно было установить через консоль управления сервером. В Windows Server 2012 / R2 этот момент не поменялся. Откройте консоль Server Manager и отметьте роль **Windows Server Update Services** (система автоматически выберет и предложит установить необходимые компоненты веб сервера IIS).

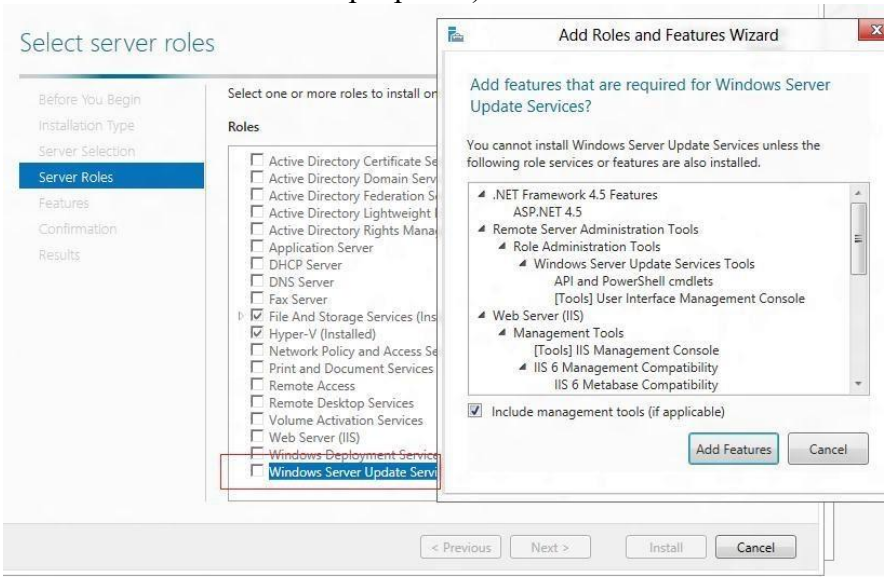


Рис. 187

Отметьте опцию WSUS Services, далее необходимо выбрать тип базы данных, которую будет использовать WSUS.

В Windows Server 2012 R2 поддерживаются следующие типы SQL баз данных для WSUS сервера:

- Windows Internal Database (WID);
- Microsoft SQL Server 2008 R2 SP1, 2012, 2014, 2016 в редакциях Enterprise / Standard / Express Edition;
- Microsoft SQL Server 2012 Enterprise / Standard / Express Edition.

Соответственно вы можете использовать встроенную базу данных Windows WID (Windows Internal database), которая является бесплатной и не требует дополнительного лицензирования. Либо вы можете использовать выделенную локальная или удаленную (на другом сервере) базу данных на SQL Server для хранения данных WSUS.

База WID по умолчанию называется **SUSDB.mdf** и хранится в каталоге **windir%\wid\data\.** Эта база поддерживает только Windows аутентификацию (но не SQL). Инстанс внутренней (WID) базы данных для WSUS называется **server_name\Microsoft##WID**. В базе данных WSUS хранятся настройки сервера обновлений, метаданные обновлений и сведения о клиентах сервера WSUS.

Внутреннюю базу Windows (Windows Internal Database) рекомендуется использовать, если:

- Организация не имеет и не планирует покупать лицензии на SQL Server;
- Не планируется использовать балансировку нагрузки на WSUS (NLB WSUS);

- Если планируется развернуть дочерний сервер WSUS (например, в филиалах). В этом случае на вторичных серверах рекомендуется использовать встроенную базу WSUS.

Базу WID можно администрировать через SQL Server Management Studio (SSMS), если указать в строке подключения \\.\pipe\MICROSOFT##WID\tsql\query.
Отметим, что в бесплатных редакциях SQL Server 2008/2012 Express имеет ограничение на максимальный размер БД – 10 Гб. Скорее всего это ограничение достигнуто не будет (например, размер базы WSUS на 2500 клиентов – около 3 Гб). Ограничение Windows Internal Database – 524 Гб.
В случае, установки роли WSUS и сервера БД на разных серверах, существует ряд ограничений:

- SQL сервер с БД WSUS не может быть контроллером домена;
- Сервер WSUS не может быть одновременно сервером терминалов с ролью Remote Desktop Services;

Если вы планируете использовать встроенную базу данных (это вполне рекомендуемый и работоспособный вариант даже для больших инфраструктур), отметьте опцию **WID Database**.

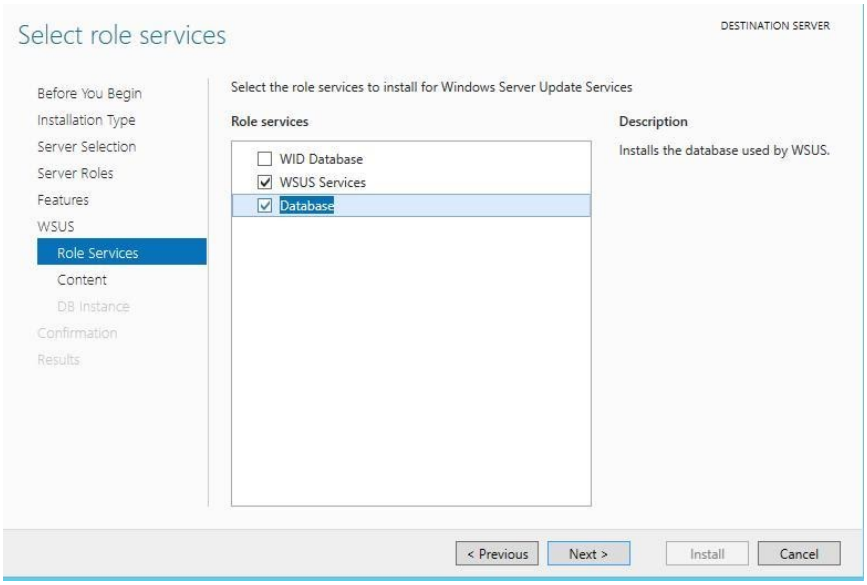


Рис. 188

Затем нужно указать каталог, в котором будут храниться файлы обновлений (рекомендуется, чтобы на выбранном диске было как минимум 10 Гб свободного места).
Размер базы данных WSUS сильно зависит от количества продуктов и ОС Windows, которое вы планируете обновлять. В большой организации размер файлов обновлений на WSUS сервере может достигать сотни Гб. Например, у меня каталог с обновлениями WSUS занимает около 400 Гб (хранятся обновления для Windows 7, 8.1, 10, Windows Server 2008 R2, 2012 / R2/ 2016, Exchange 2013, Office 2010 и 2016, SQL Server 2008/2012/2016). Имейте это в виду, планируя место для размещения файлов WSUS.

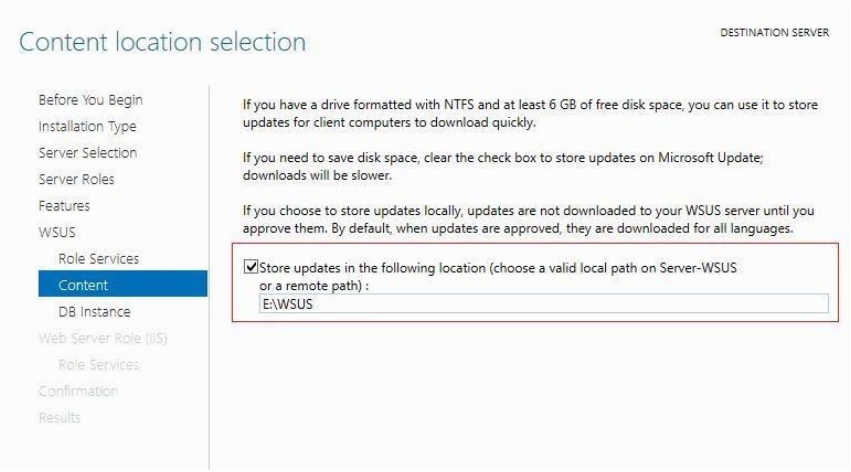


Рис. 189

В том случае, если ранее было выбрано использование отдельной выделенной БД SQL, необходимо указать имя сервера СУБД, инстанса БД и проверить подключение.

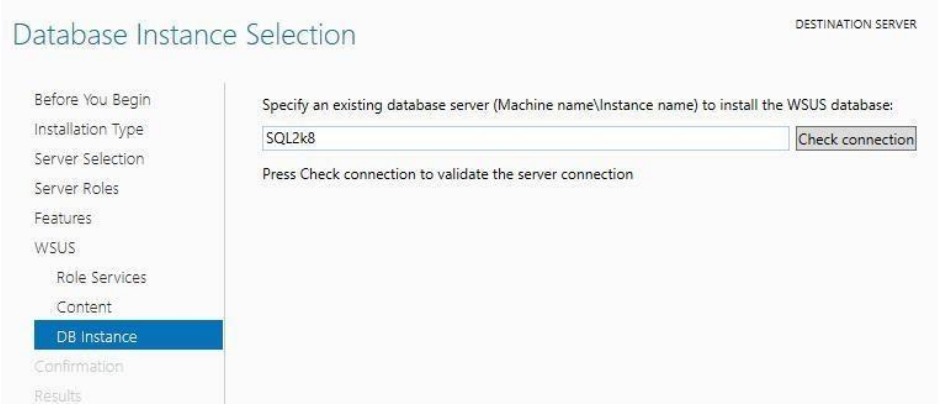


Рис. 190

Далее запустится установка роли WSUS и всех необходимых компонентов, после окончания которых запустите консоль управления WSUS в консоли Server Manager.

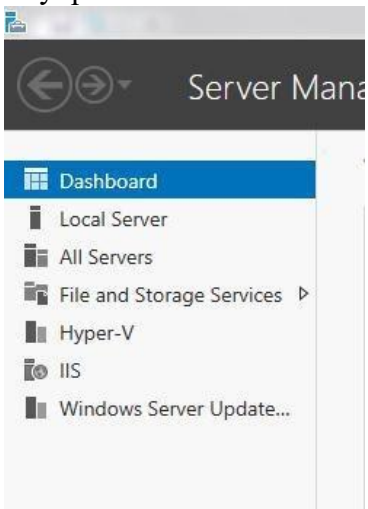


Рис. 191

Вы также можете установить сервер WSUS со внутренней базой данных с помощью следующей команды PowerShell:

```
Install-WindowsFeature -Name Updateservices,UpdateServices-WidDB,UpdateServices-services –IncludeManagementTools
```

2. Начальная настройка сервера обновлений WSUS в Windows Server 2012 R2 / 2016

При первом запуске консоли WSUS автоматически запустится мастер настройки сервера обновлений. Рассмотрим основные шаги настройки сервера WSUS с помощью мастера.

Укажите, будет ли сервер WSUS брать обновления с сайта Microsoft Update напрямую или он должен качать его с вышестоящего WSUS сервера (обычно этот вариант используется в крупных сетях для настройки WSUS сервера большого регионального подразделения, который берет обновления с WSUS центрального офиса, чем существенно снижается нагрузка на каналы связи между центральным офисом и филиалом).

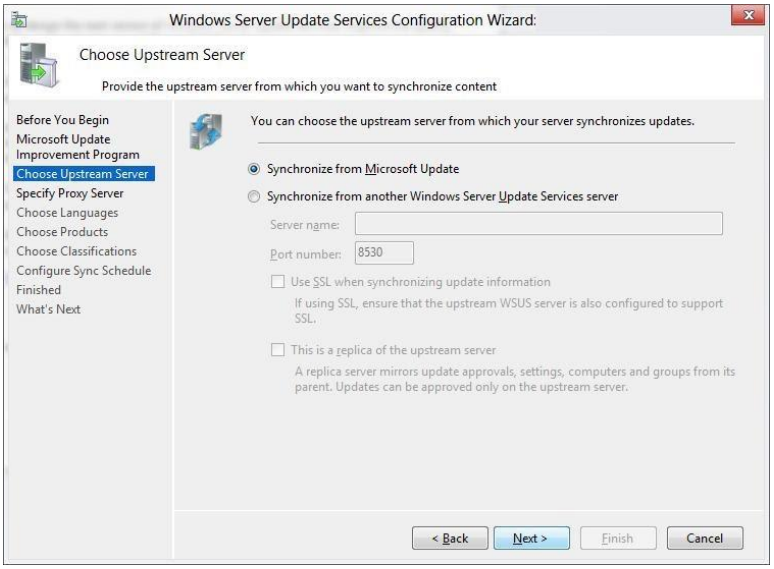


Рис. 192

Если ваш сервер WSUS сам должен загружать обновления с серверов Windows Update, и доступ в Интернет у вас осуществляется через прокси-сервер, вы должны указать адрес прокси сервера, порт и логин/пароль для авторизации на нем.

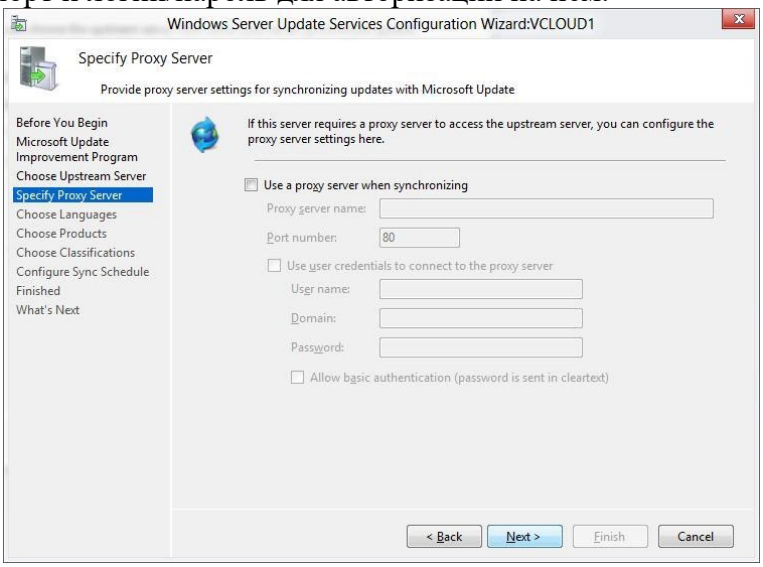


Рис. 193

Далее проверяется связь с вышестоящим сервером обновления. Нажмите кнопку **Start Connecting**.

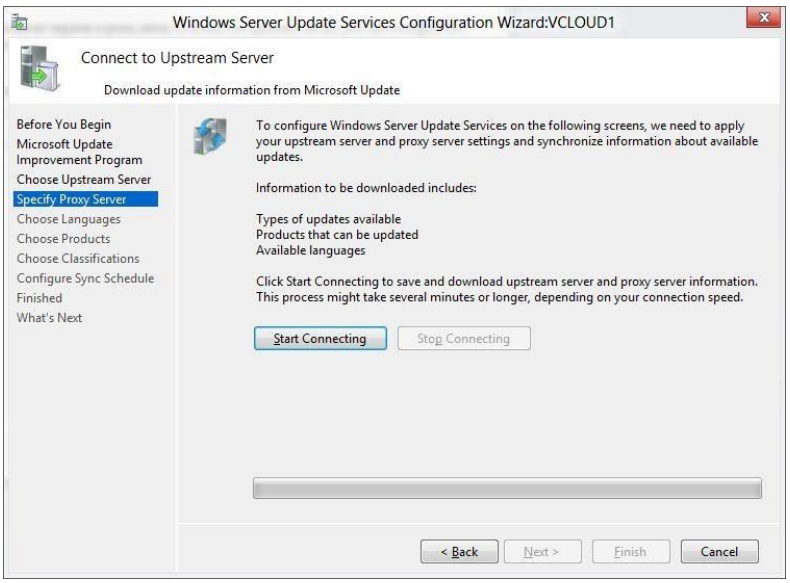


Рис. 194

Затем необходимо выбрать языки, для которых WSUS будет скачивать обновления. Мы укажем **English** и **Russian** (список языков может быть в дальнейшем изменен из консоли WSUS).

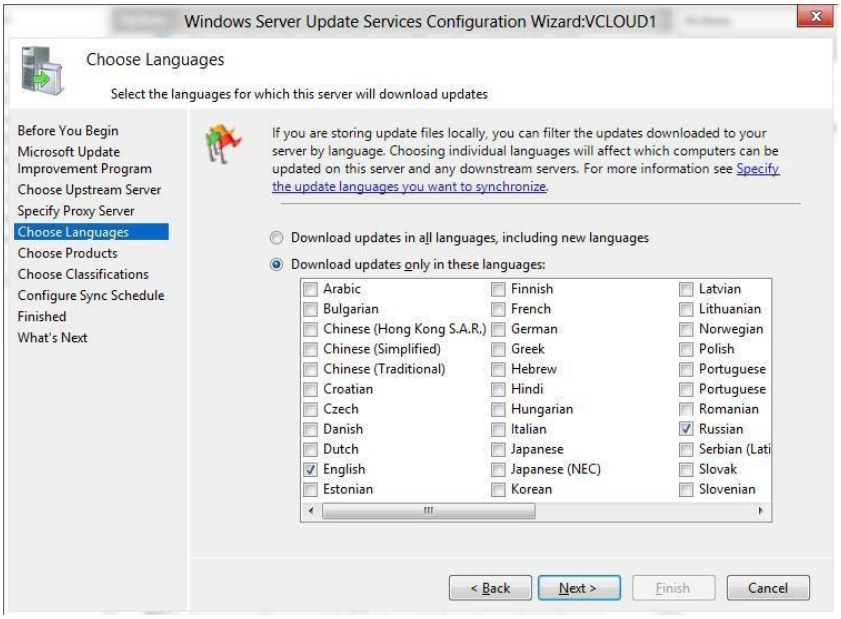


Рис. 195

Затем указывается список продуктов, для которых WSUS должен скачивать обновления. Необходимо выбрать все продукты Microsoft, которые используются в Вашей корпоративной сети. Имейте в виду, что все обновления занимают дополнительное место на диске, поэтому лишние продукты отмечать не следует. Если вы точно уверены, что в вашей сети не осталось компьютеров с Windows XP или Windows 7, не выбирайте эти опции. Тем самым вы сэкономите существенно место на диске WSUS сервера.

В случае необходимости вы сможете вручную импортировать любые обновления из каталога Microsoft Update Catalog на свой сервер WSUS.

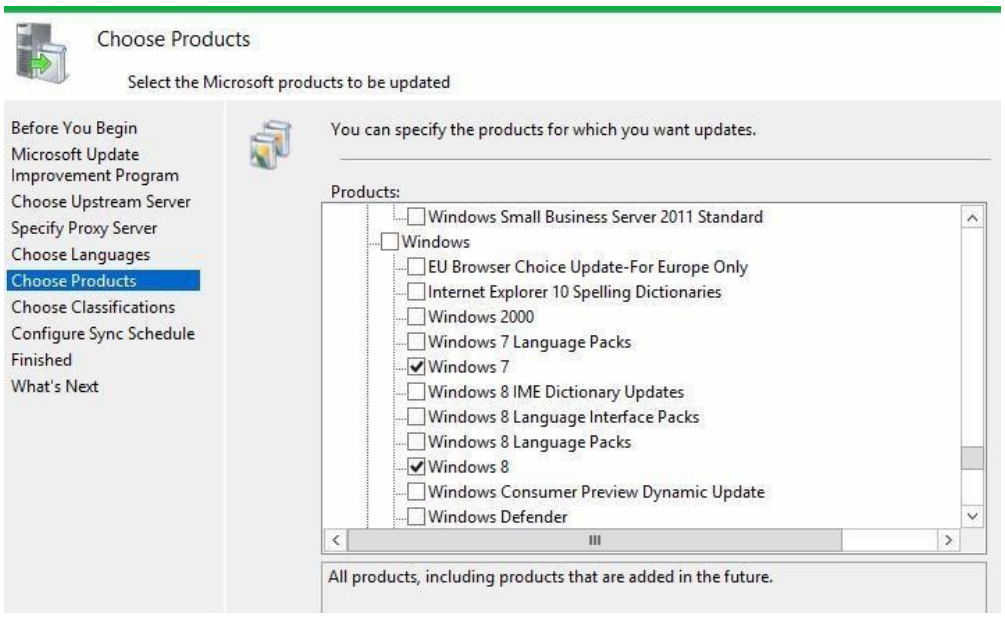


Рис. 196

На странице **Classification Page**, нужно указать типы обновлений, которые будут распространяться через WSUS. Рекомендуется обязательно указать: Critical Updates, Definition Updates, Security Packs, Service Packs, Update Rollups, Updates.

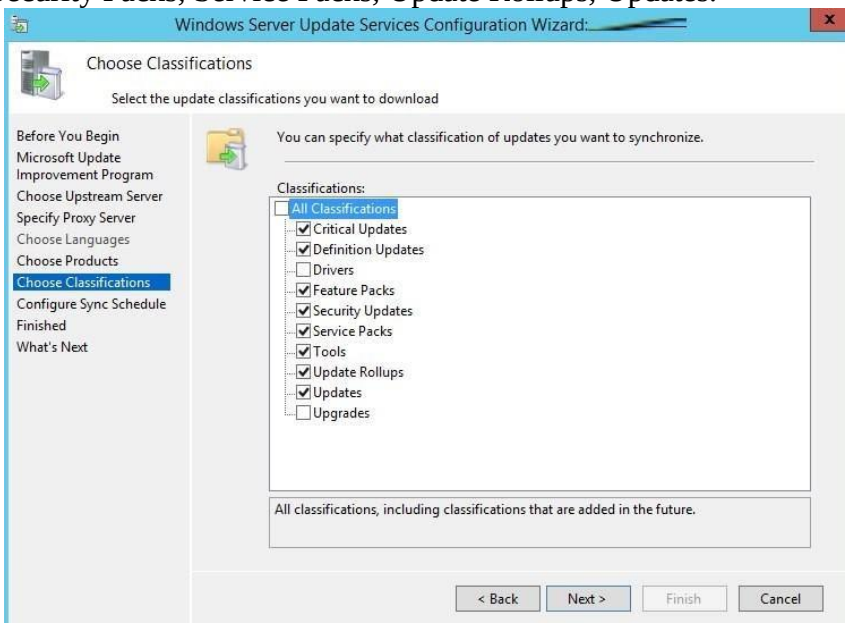


Рис. 197

Далее необходимо указать расписание синхронизации обновлений – рекомендуется использовать автоматическую ежедневную синхронизацию сервера WSUS с серверами обновлений Microsoft Update. Имеет смысл выполнять синхронизацию в ночные часы, чтобы не загружать канал доступа в Интернет в рабочее время.

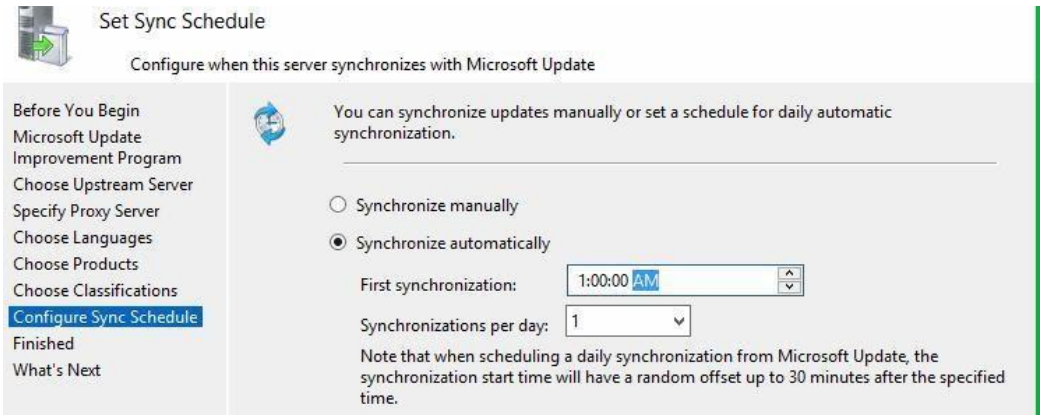


Рис. 198

Первоначальная синхронизация сервера WSUS с вышестоящим сервером обновлений может занят несколько дней, в зависимости от количества продуктов, которое вы выбрали ранее и скорости доступа в Интернет.

После окончания работы мастер запустится консоль WSUS.

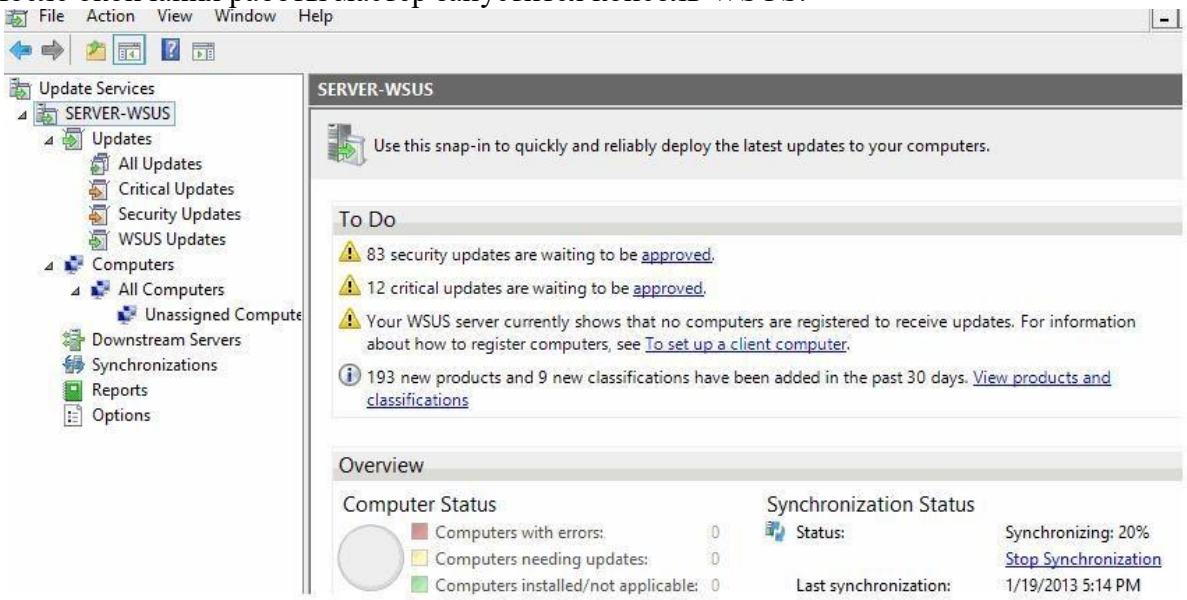


Рис. 199

С целью повышения производительности сервера WSUS на Windows Server рекомендуется исключить следующие папки из области проверки антивируса:

- \WSUS\WSUSContent;
- %windir%\wid\data;
- \SoftwareDistribution\Download.

Клиенты теперь могут получать обновления, подключившись к WSUS серверу по порту 8530 (в Windows Server 2003 и 2008 по умолчанию использоваться 80 порт).

2. Настройка клиентов WSUS с помощью групповых политик

После того, как вы настроили сервер, нужно настроить Windows-клиентов (сервера и рабочие станции) на использование сервера WSUS для получения обновлений, чтобы клиенты получали обновления с внутреннего сервера обновлений, а не с серверов Microsoft Update через Интернет. В этой статье мы рассмотрим процедуру настройки клиентов на использование сервера WSUS с помощью групповых политик домена Active Directory.

Групповые политики AD позволяют администратору автоматически назначить компьютеры в различные группы WSUS, избавляя его от необходимости ручного

перемещения компьютеров между группами в консоли WSUS и поддержки этих групп в актуальном состоянии. Назначение клиентов к различным целевым группам WSUS основывается на метке в реестре на клиенте (метки задаются групповой политикой или прямым редактированием реестра). Такой тип соотнесения клиентов к группам WSUS называется **client side targeting** (Таргетинг на стороне клиента).

Предполагается, что в нашей сети будут использоваться две различные политики обновления — отдельная политика установки обновлений для серверов (**Servers**) и для рабочих станций (**Workstations**). Эти две группы нужно создать в консоли WSUS в секции All Computers.

Совет. Политика использования сервера обновлений WSUS клиентами во многом зависит от организационной структуры OU в Active Directory и правил установки обновлении в организации. В этой статье мы рассмотрим всего лишь частный вариант, позволяющий понять базовые принципы использования политик AD для установки обновлений Windows.

В первую очередь необходимо указать правило группировки компьютеров в консоли WSUS (targeting). По умолчанию в консоли WSUS компьютеры распределяются администратором по группам вручную (server side targeting). Нас это не устраивает, поэтому укажем, что компьютеры распределяются в группы на основе client side targeting (по определенному ключу в реестре клиента). Для этого в консоли WSUS перейдите в раздел **Options** и откройте параметр **Computers**. Поменяйте значение на **Use Group Policy or registry setting on computers** (Использовать на компьютерах групповую политику или параметры реестра).

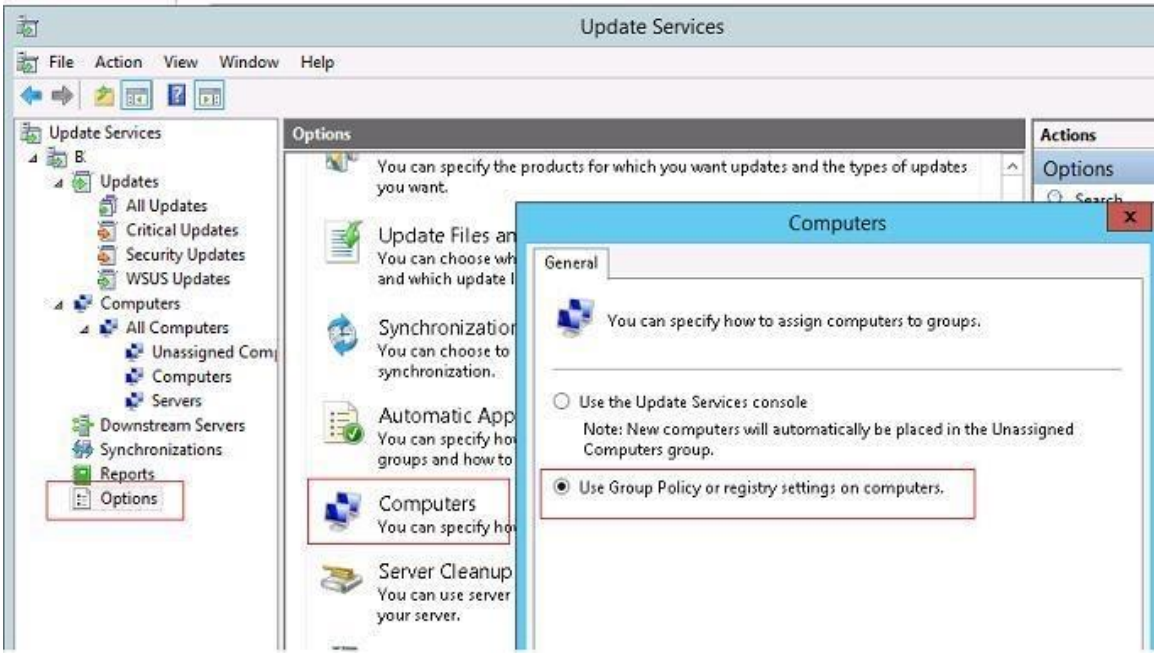


Рис. 200

Теперь можно создать GPO для настройки клиентов WSUS. Откройте доменную консоль управления групповыми политиками (Group Policy Management) и создайте две новые групповые политики: ServerWSUSPolicy и WorkstationWSUSPolicy.

3. Групповая политика WSUS для серверов Windows

Начнем с описания серверной политики **ServerWSUSPolicy**.

Настройки групповых политик, отвечающих за работу службы обновлений Windows, находятся в разделе GPO: **Computer Configuration** -> **Policies**-> **Administrative templates**-> **Windows Component**-> **Windows Update** (Конфигурация компьютера -> Административные шаблоны -> Компоненты Windows -> Центр обновления Windows).

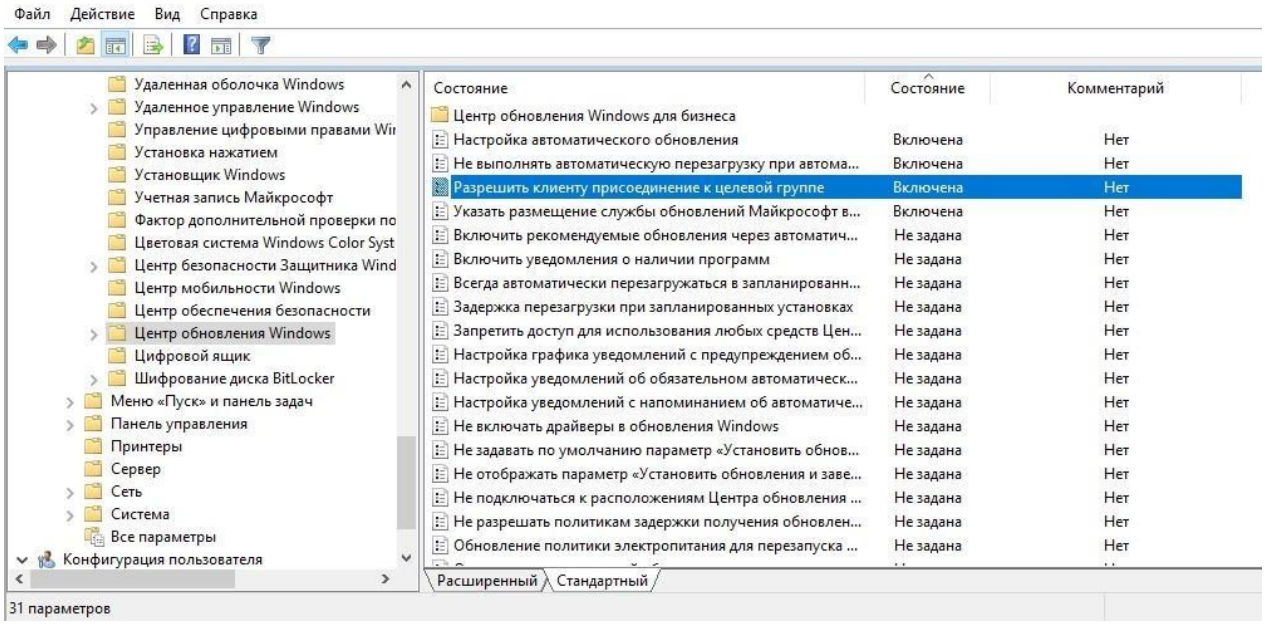


Рис. 201

В нашей организации мы предполагаем использовать данную политику для установки обновлений WSUS на сервера Windows. Предполагается, что все попадающие под эту политику компьютеры будут отнесены к группе Servers в консоли WSUS. Кроме того, мы хотим запретить автоматическую установку обновлений на серверах при их получении. Клиент WSUS должен просто скачать доступные обновления на диск, отобразить оповещение о наличии новых обновлений в системном трее и ожидать запуска установки администратором (ручной или удаленной с помощью модуля PSWindowsUpdate) для начала установки. Это значит, что продуктивные сервера не будут автоматически устанавливать обновления и перезагружаться без подтверждения администратора (обычно эти работы выполняются системным администратором в рамках ежемесячных плановых регламентных работ). Для реализации такой схемы зададим следующие политики:

- **Configure Automatic Updates** (Настройка автоматического обновления): *Enable. 3 – Auto download and notify for install (Автоматически загружать обновления и уведомлять об их готовности к установке)* – клиент автоматически скачивает новые обновлений и оповещает об их появлении;
- **Specify Intranet Microsoft update service location** (Указать размещение службы обновлений Майкрософт в интрасети): *Enable*. Set the intranet update service for detecting updates (Укажите службу обновлений в интрасети для поиска обновлений): *http://srv-wsus.winitpro.ru:8530*, Set the intranet statistics server (Укажите сервер статистики в интрасети): *http://srv-wsus.winitpro.ru:8530* – здесь нужно указать адрес вашего сервера WSUS и сервера статистики (обычно они совпадают);
- **No auto-restart with logged on users for scheduled automatic updates installations** (Не выполнять автоматическую перезагрузку при автоматической установке обновлений, если в системе работают пользователя): *Enable* – запретить автоматическую перезагрузку при наличии сессии пользователя;
- **Enable client-side targeting (**Разрешить клиенту присоединение к целевой группе): *Enable*. Target group name for this computer (Имя целевой группу для данного компьютера): *Servers* – в консоли WSUS отнести клиенты к группе Servers.

4. Политика установки обновлений WSUS для рабочих станций

Мы предполагаем, что обновления на клиентские рабочие станции, в отличии от серверной политики, будут устанавливаться автоматически ночью сразу после получения обновлений. Компьютеры после установки обновлений должны перезагружаться автоматически (предупреждая пользователя за 5 минут).

В данной GPO (WorkstationWSUSPolicy) мы указываем:

- **Allow Automatic Updates immediate installation** (Разрешить немедленную установку автоматических обновлений): *Disabled* — запрет на немедленную установку обновлений при их получении;
- **Allow non-administrators to receive update notifications** (Разрешить пользователям, не являющимся администраторами, получать уведомления об обновлениях): *Enabled* — отображать не-администраторам предупреждение о появлении новых обновлений и разрешить их ручную установку;
- **Configure Automatic Updates:** *Enabled*. Configure automatic updating: *4 — Auto download and schedule the install*. Scheduled install day: *0 — Every day*. Scheduled install time: *05:00* – при получении новых обновлений клиент скачивает в локлаьный кэш и планирует их автоматическую установку на 5:00 утра;
- **Target group name for this computer:** *Workstations* – в консоли WSUS отнести клиента к группе Workstations;
- **No auto-restart with logged on users for scheduled automatic updates installations:** *Disabled* — система автоматически перезагрузится через 5 минут после окончания установки обновлений;
- **Specify Intranet Microsoft update service location**: Enable. Set the intranet update service for detecting updates: *http://srv-wsus.winitpro.ru:8530,* Set the intranet statistics server: *http://srv-wsus.winitpro.ru:8530* –адрес корпоративного WSUS сервера.

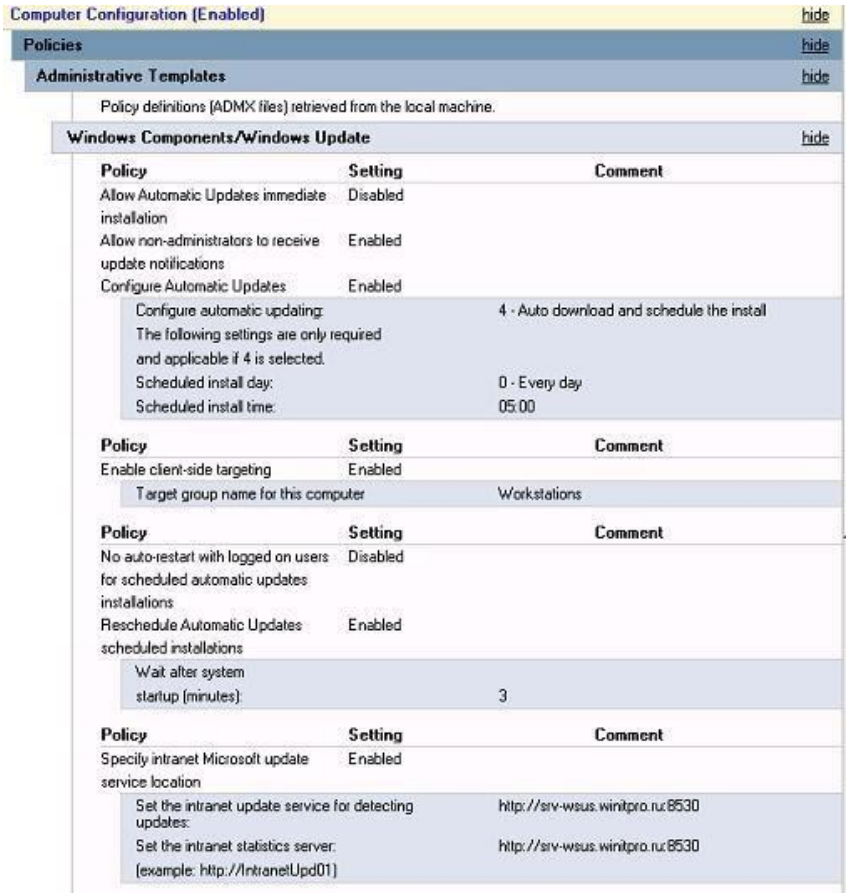


Рис. 202

Do not allow update deferral policies to cause scans against Windows Update (ссылка).

Совет. Чтобы улучшить «уровень пропатченности» компьютеров в организации, в обоих политиках можно настроить принудительный запуск службы обновлений (wuauserv) на клиентах. Для этого в разделе **Computer Configuration -> Policies-> Windows Setings -> Security Settings -> System Services** найдите службу Windows Update и задайте для нее автоматический запуск (**Automatic**).

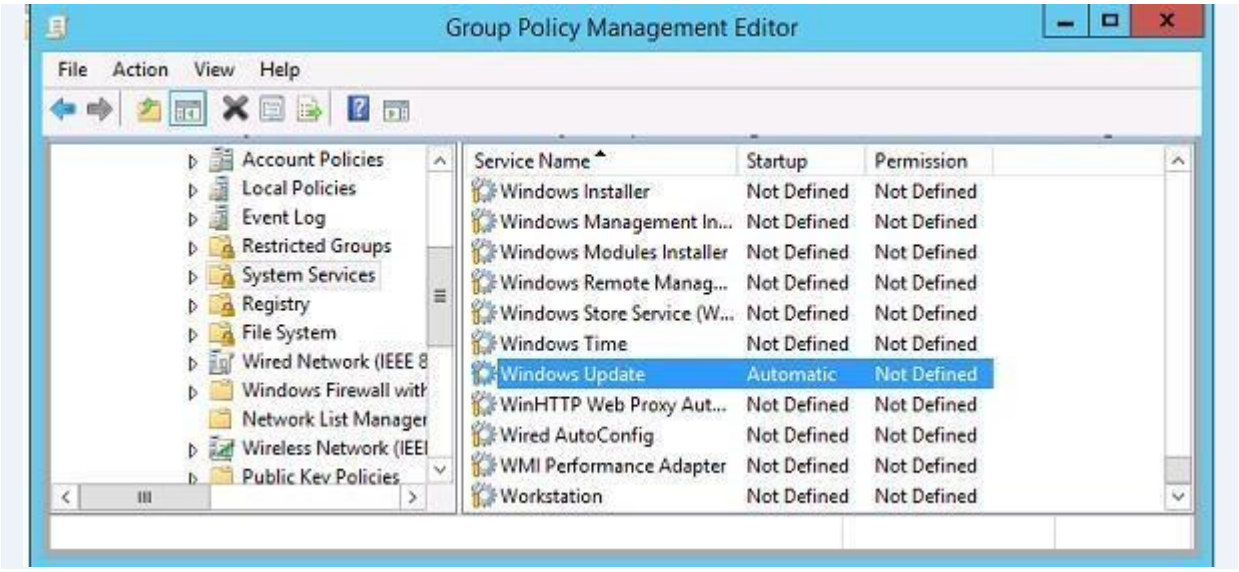


Рис. 203

5. Назначаем политики WSUS на OU Active Directory

Следующий шаг – назначить созданные политики на соответствующие контейнеры (OU) Active Directory. В нашем примере структура OU в домене AD максимально простая: имеются два контейнера – Servers (в нем содержаться все сервера организации, помимо контроллеров домена) и WKS (Workstations –компьютеры пользователей).

Совет. Мы рассматриваем лишь один довольно простой вариант привязки политик WSUS к клиентам. В реальных организациях возможно привязать одну политику WSUS на все компьютеры домена (GPO с настройками WSUS вешается на корень домена), разнести различные виды клиентов по разным OU (как в нашем примере – мы создали разные политики WSUS для серверов и рабочих станций), в больших распределенных доменах можно привязывать различные WSUS сервера к сайтам AD, или же назначать GPO на основании фильтров WMI, или скомбинировать перечисленные способы.

Чтобы назначить политику на OU, щелкните в консоли управления групповыми политиками по нужному OU, выберите пункт меню **Link as Existing GPO** и выберите соответствующую политику.

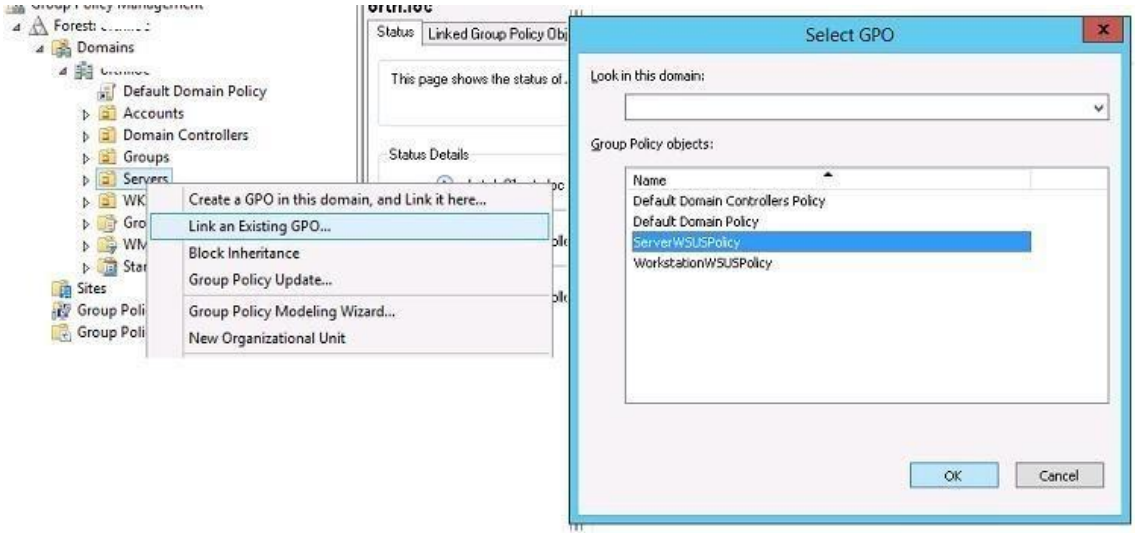


Рис. 204

Точно таким же способом нужно назначить политику WorkstationWSUSPolicy на контейнер AD WKS, в котором находятся рабочие станции Windows.

Осталось обновить групповые политики на клиентах для привязки клиента к серверу WSUS:

```
gpupdate /force
```

Все настройки системы обновлений Windows, которые мы задали групповыми политиками должны появится в реестре клиента в ветке **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate**.

Данный reg файл можно использовать для переноса настроек WSUS на другие компьютеры, на которых не удается настроить параметры обновлений с помощью GPO (компьютеры в рабочей группе, изолированных сегментах, DMZ и т.д.)

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]
"WUServer"="http://srv-wsus.winitpro.ru:8530"
"WUStatusServer"="http://srv-wsus.winitpro.ru:8530"
"UpdateServiceUrlAlternate"=""
"TargetGroupEnabled"=dword:00000001
"TargetGroup"="Servers"
"ElevateNonAdmins"=dword:00000000
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
]
"NoAutoUpdate"=dword:00000000
"AUOptions"=dword:00000003
"ScheduledInstallDay"=dword:00000000
"ScheduledInstallTime"=dword:00000003
"ScheduledInstallEveryWeek"=dword:00000001
"UseWUServer"=dword:00000001
"NoAutoRebootWithLoggedOnUsers"=dword:00000001
```

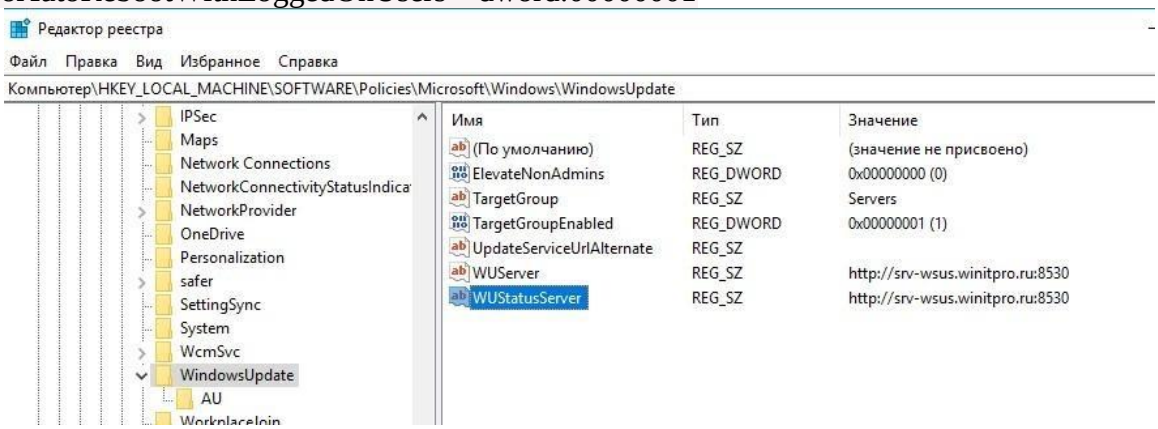


Рис. 205

Также удобно контролировать применённые настройки WSUS на клиентах с помощью rsop.msc.

И через некоторое время (зависит от количества обновлений и пропускной способности канала до сервера WSUS) нужно проверить в трее наличие всплывающего оповещений о наличии новых обновлений. В консоли WSUS в соответствующих группах должны появиться клиенты (в табличном виде отображается имя клиента, IP, ОС, процент их «пропатченности» и дата последнего обновлений статуса). Т.к. мы политиками привязали компьютеры и серверы к различным группам WSUS, они будут получать только обновления, одобренные к установке на соответствующие группы WSUS.

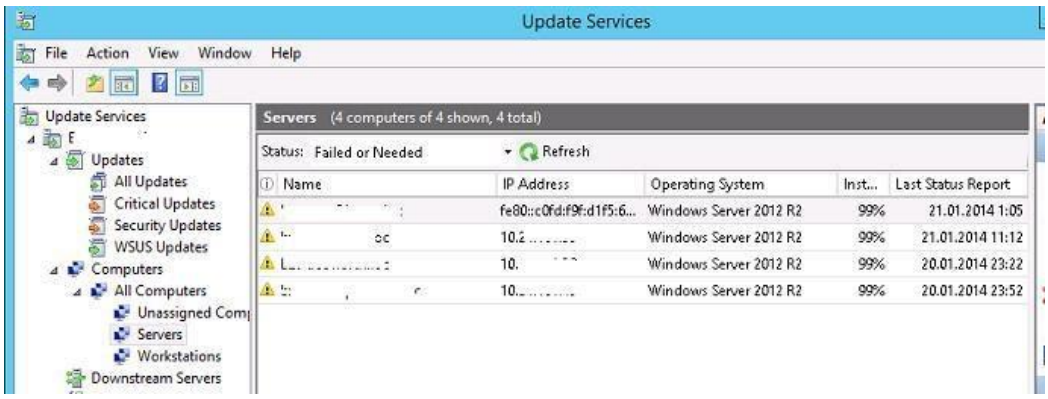


Рис. 206

Одобрение обновлений на WSUS в Windows Server 2012 R2/2016

Одна из основных задач администратора WSUS является управление обновлениями, одобренными для установки на компьютерах и сервера Windows. Сервер WSUS после установки и настройки начинает регулярно скачивать обновления для выбранных продуктов с серверов Microsoft Update.

Целевые группы компьютеров WSUS

После того, как обновления попали в базу данных WSUS, они могут быть установлены на компьютеры. Но, прежде чем компьютеры начнут качать и ставить новые обновления, их должен одобрить (или отклонить) администратор WSUS. Важно иметь в виду, что в большинстве случаев перед установкой обновлений на продуктивные системы их нужно обязательно тестировать на нескольких типовых рабочих станциях и серверах.

Для организации процесса тестирования и установки обновления на компьютерах и серверах домена администратор WSUS должен создать группы компьютеров. В зависимости от задач бизнеса, типов рабочих мест пользователей и категорий серверов можно создавать различные группы компьютеров. В общем случае в консоли WSUS в разделе **Computers** -> **All computers** имеет смысл создать следующие группы на WSUS:

1. Test_Srv_WSUS — группа с тестовыми серверами (некритичные для бизнеса сервера и выделенные сервера с тестовой средой, идентичной продуктивной);
2. Test_Wks_WSUS — тестовые рабочие станции;
3. Prod_Srv_WSUS — продуктивные сервера Windows;
4. Prod_Wks_WSUS — все рабочие станции пользователей.

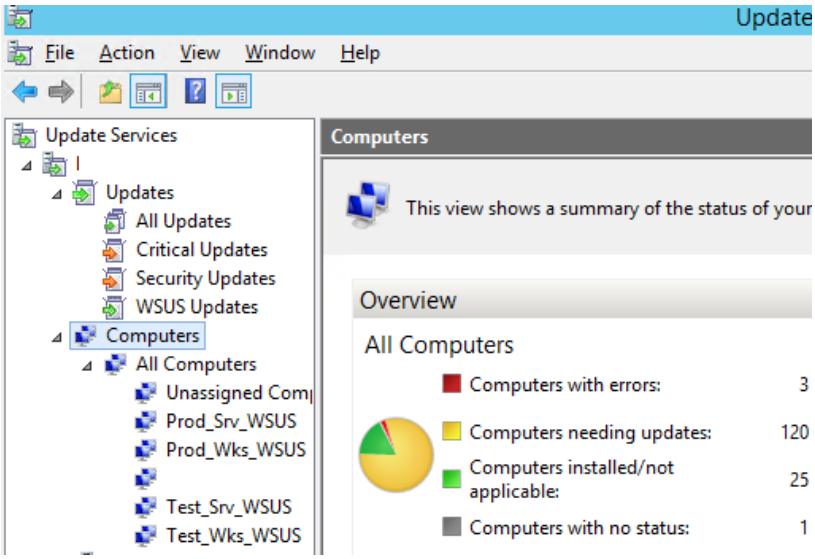


Рис. 207

Данные группы компьютеров можно наполнить серверами вручную (обычно это имеет смысл для тестовых групп) либо вы можете привязать компьютеры и сервера к груп-

пам WSUS с помощью групповой политики **Enable client-side targeting (**Разрешить клиенту присоединение к целевой группе).

После того, как группы созданы, вы можете одобрить для них обновления. Есть два способа утверждения обновлений для установки на компьютерах: ручное и автоматическое обновление.

Ручное одобрение и установка обновлений через WSUS

Откройте консоль управления WSUS (Update Services) и выберите секцию **Updates**. В ней отображается результирующий отчет о доступных обновлениях. В этом разделе по-умолчанию присутствую 4 подраздела: **All Updates**, **Critical Updates**, **Security Updates** и **WSUS Updates**. Вы можете одобрить конкретное обновление к установке, найдя его в одном из этих разделов (вы можете воспользоваться поиском по имени KB в консоли поиска обновлений или номеру бюллетеня безопасности Microsoft), или же можно отсортировать обновления по дате выпуска, или номерам.

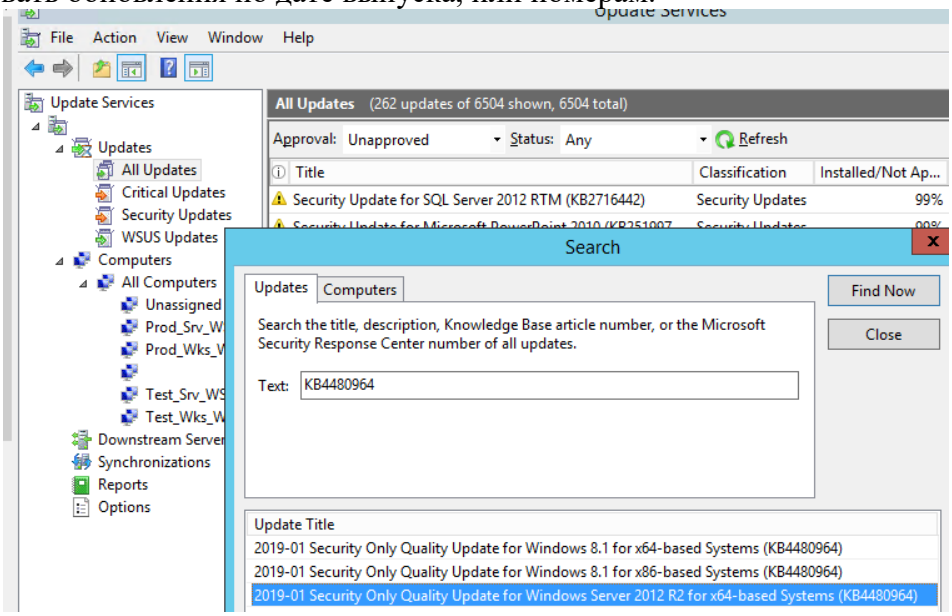


Рис. 208

Выведите список еще не утвержденных обновлений (фильтр — Approval=Unapproved). Найдите нужное обновление, щелкните по нему ПКМ и выберите в меню пункт **Approve**.

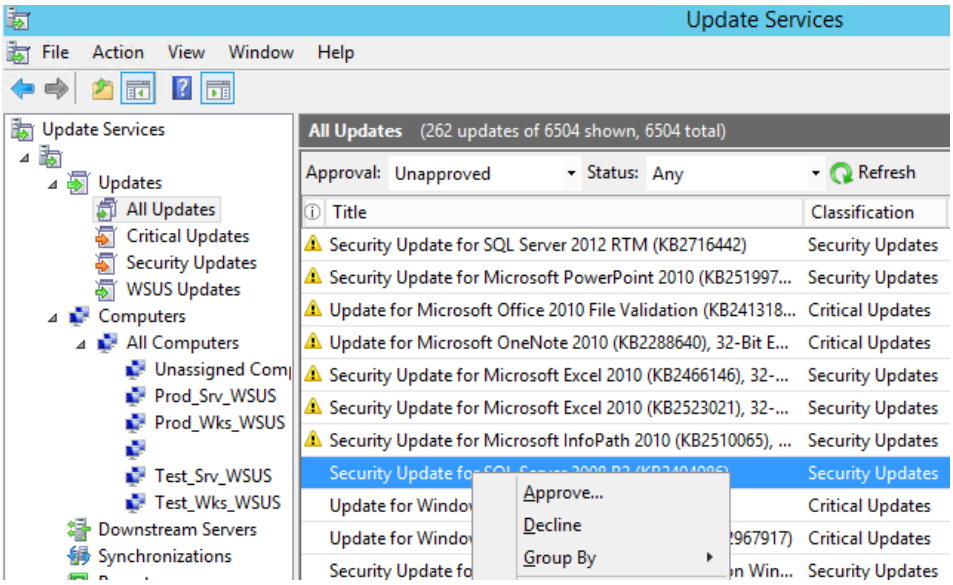


Рис. 209

В появившемся окне выберите группу компьютеров WSUS, для которых нужно одобрить установку данного обновления (например, Test_Srv_WSUS). Выберите пункт **Approve**

for Install. Можно одобрить обновление сразу для всех групп компьютеров, выбрав пункт **All Computers**, либо для каждой группы индивидуально. Например, сначала вы можете одобрить установку обновлений на группе тестовых компьютеров, а через 4-7 дней, если проблем не выявлено, одобрите установку обновления на все компьютеры.

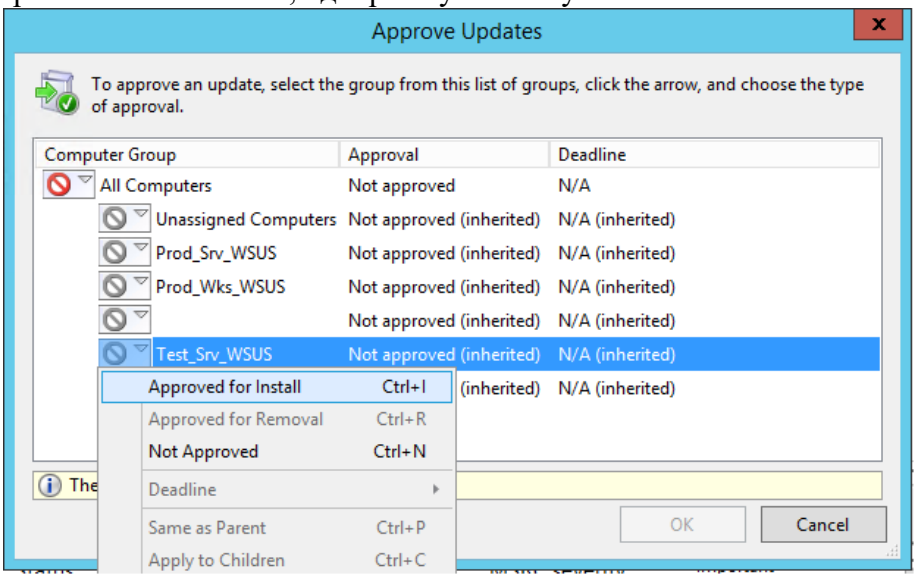


Рис. 210

Появится окошко с результатами процесса утверждения обновления. Если обновление успешно одобрено, появится надпись **Success**. Закройте это окно.

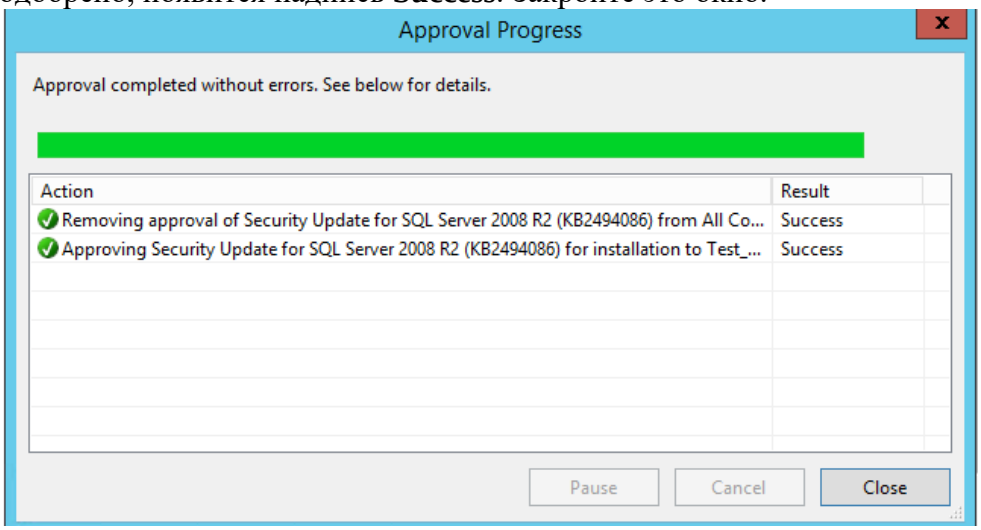


Рис. 211

Как вы поняли, это ручная схема одобрения конкретных обновлений. Она достаточно трудоемка, т.к. каждое обновление нужно одобрять индивидуально. Если вы не хотите одобрять обновления вручную, вы можете создать правила автоматического одобрения обновлений (auto-approval).

Настройка правил автоматического одобрения обновлений на WSUS

Автоматическое одобрение позволяет сразу, без вмешательства администратора, одобрить новые обновления, которые появились на сервере WSUS и назначить их для установки на клиентов. Автоматическое одобрение обновлений WSUS основано на правилах одобрения.

В консоли управления WSUS откройте раздел **Options** и выберите **Automatic Approvals**.

В появившемся окне на вкладке **Update Rules** указано только одно правило с именем **Default Automatic Approval Rule** (по умолчанию оно отключено).

Чтобы создать новое правило, нажмите на кнопку **New Rule**.

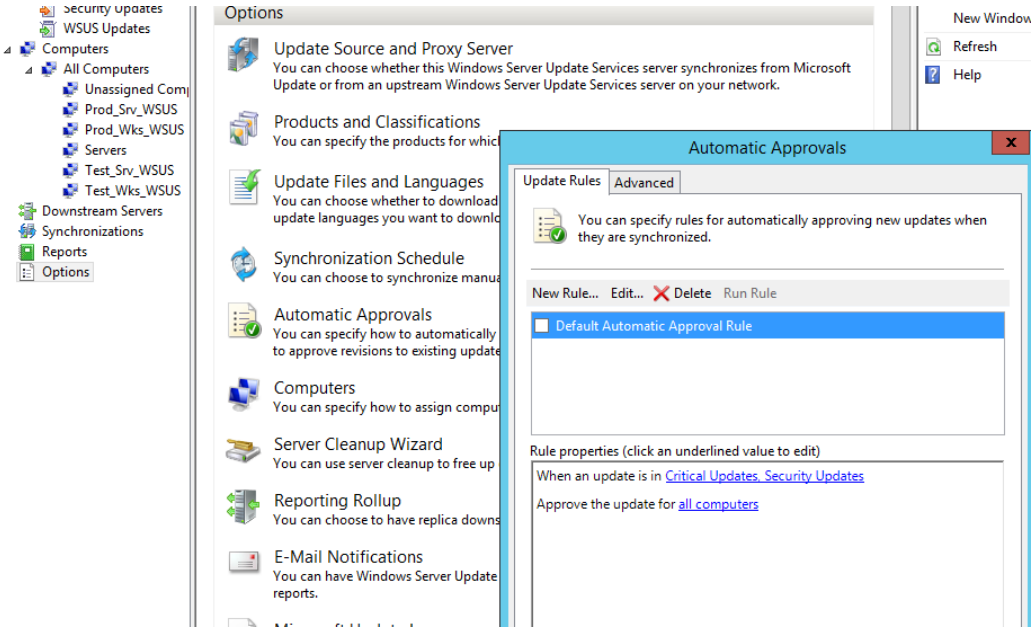


Рис. 212

Правило состоит из 3 шагов. Вам нужно выбрать необходимые свойства обновления, выбрать на какие группы компьютеров WSUS нужно одобрить обновление и имя правила.

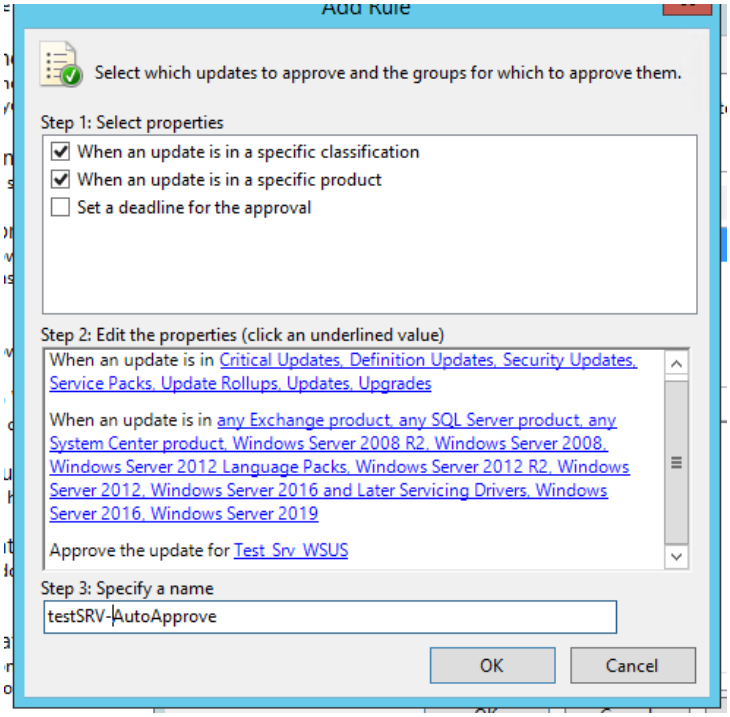


Рис. 213

Щелкая на каждую синюю ссылку, откроется соответствующее окно свойств.

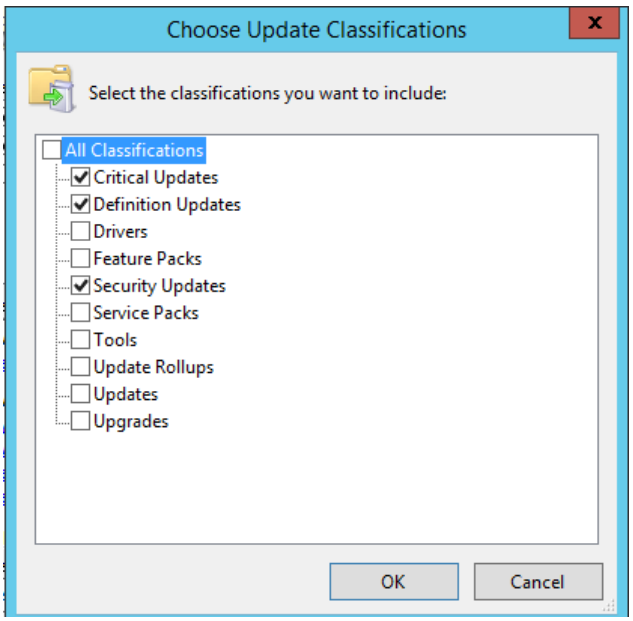


Рис. 214

Например, вы можете включить автоматическое одобрение обновлении безопасности для тестовых серверов. Для этого в секции Choose Update Classifications выберите пункт Critical Updates, Security Updates, Definition Updates (остальные галки снимите). Затем в диалоге Approve the update for выберите группу WSUS с именем Test_Srv_WSUS.

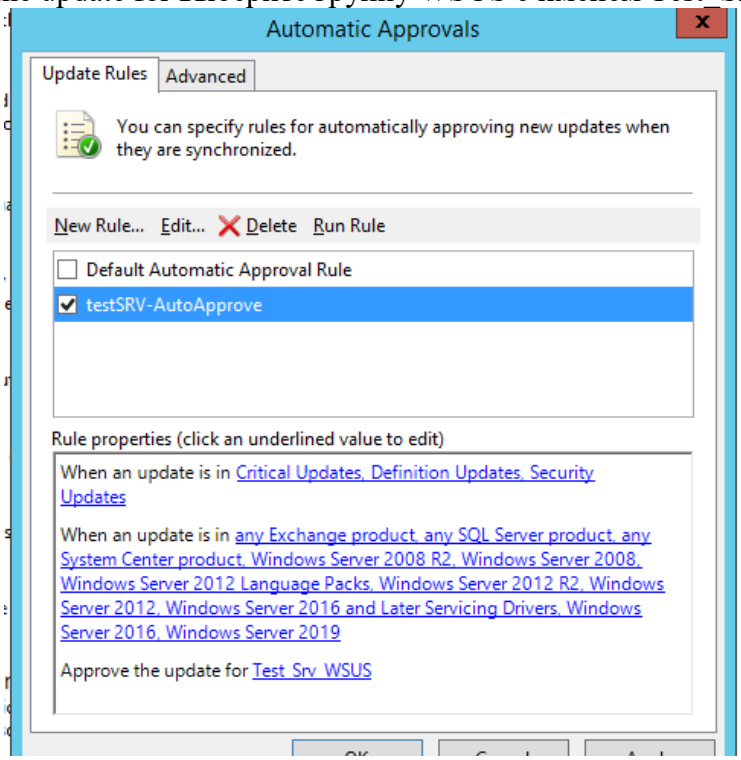


Рис. 215

На вкладке **Advanced** вы можете выбрать, нужно ли автоматически одобрять обновления для самой службы WSUS и нужно ли дополнительно одобрять обновления, которые были изменены Microsoft. Обычно все галки на этой вкладке включены.

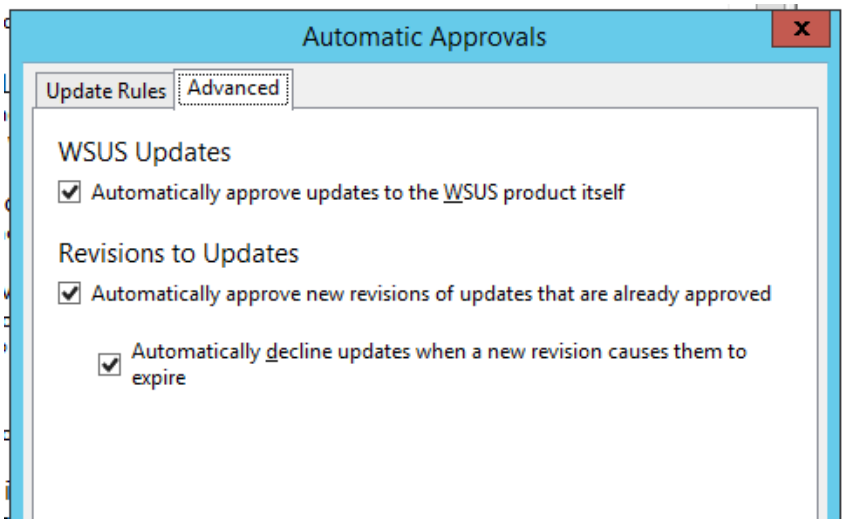


Рис. 216

Теперь, когда в очередной второй вторник месяца ваш сервер WSUS закачает новые обновления (или при ручном импорте обновлений), они будут одобрены для автоматической установки на тестовой группе. Клиенты Windows по умолчанию выполняют сканирование новых обновлений на сервере WSUS каждые 22 часа. Чтобы критичные компьютеры получали новые обновления как можно скорее, вы можете изменить частоту таких синхронизаций с помощью политики Automatic Update detection frequency до нескольких часов (также вы можете выполнить сканирование обновлений вручную с помощью модуля PSWindowsUpdate). При большом количестве клиентов на сервере WSUS (более 2000 компьютеров), производительность сервера обновлений со стандартными настройками может оказаться недостаточной, поэтому ее необходимо оптимизировать (см. статью).

Отзыв установленных обновлений на WSUS

Если одно из одобренных обновлений оказалось проблемным и вызывает ошибки на компьютерах или серверах, администратор WSUS может его отозвать. Для этого нужно найти обновление в консоли WSUS и выбрать **Decline**. Затем укажите

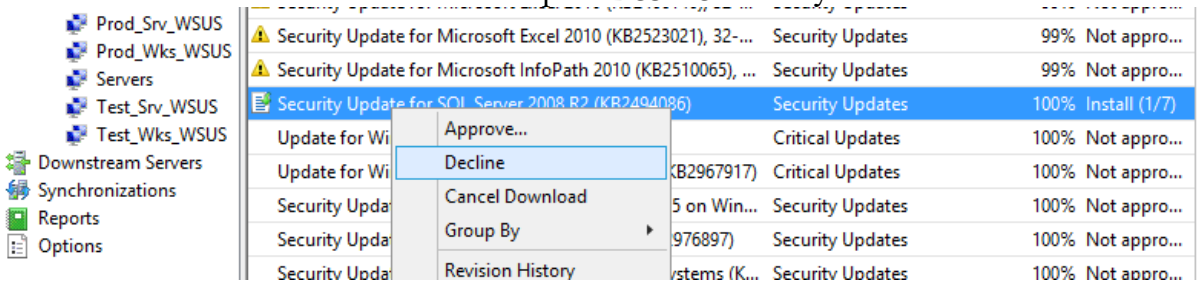


Рис. 217

Теперь выберите группу WSUS, для которой нужно отменить установку и выбрать **Approved for Removal.** Через некоторое время обновление будет удалено на клиенте

Сделайте скриншоты (фотографии) процесса внедрения управления обновлениями и вставьте в отчёт.

2.17. Практическая работа № 17
Мониторинг WindowsServer

Задание:

Чаще всего для мониторинга работоспособности, доступности, загруженности серверов используются сторонние продукты. Если вам нужно получать информацию о производительности приложений либо железа только с одного-двух Windows-серверов, либо когда

это нужно на непостоянной основе, либо возник более сложный случай, требующий глубокого траблшутинга производительности, то можно воспользоваться встроенным функционалом **Windows Performance Monitor**.

Performance Monitor имеет огромное количество счётчиков для получения информации о железе, операционной системе, установленном ПО в виде конкретных цифр. Performance Monitor может вести наблюдение за показателями производительности сервера в реальном времени или записывать историю.

Основные возможности Performance Monitor, которые можно использовать отдельно или совместно с другими сторонними системами мониторинга (типа Zabbix, Nagios, Cacti и другие):

- система мониторинга при выводе информации о производительности сначала обращается к Performance Monitor;
- главной задачей системы мониторинга является оповещение о наступлении тревожного момента, аварии, а у Performance Monitor – собрать и предоставить диагностические данные.

Текущие значения производительности Windows можно получить из Task Manager, но Performance Monitor умеет несколько больше:

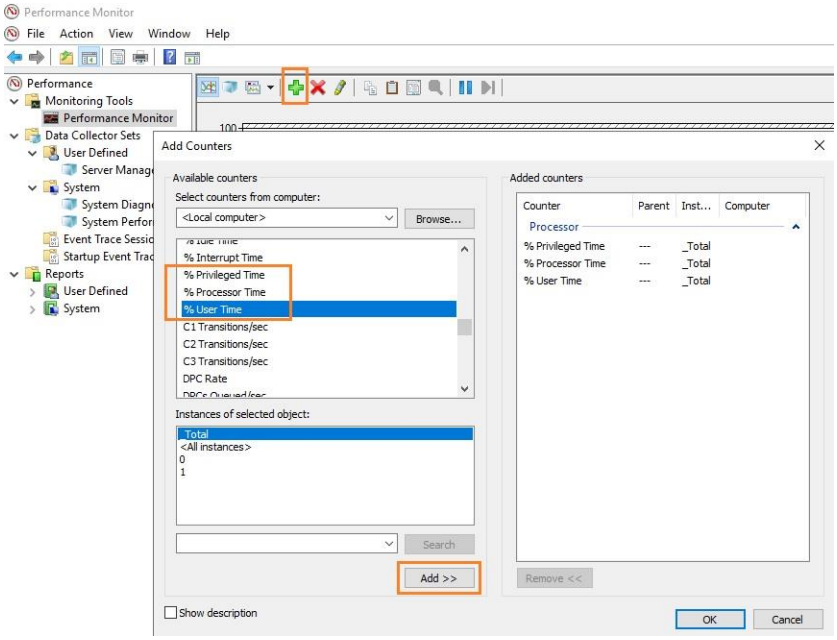
- Task Manager работает только в реальном времени и только на конкретном (локальном) хосте;
- в Performance Monitor можно подключать счётчики с разных серверов, вести наблюдение длительное время и собранную информацию сохранять в файл;
- в Task Manager очень мало показателей производительности.

Мониторинг производительности процессора с Perfomance Monitor

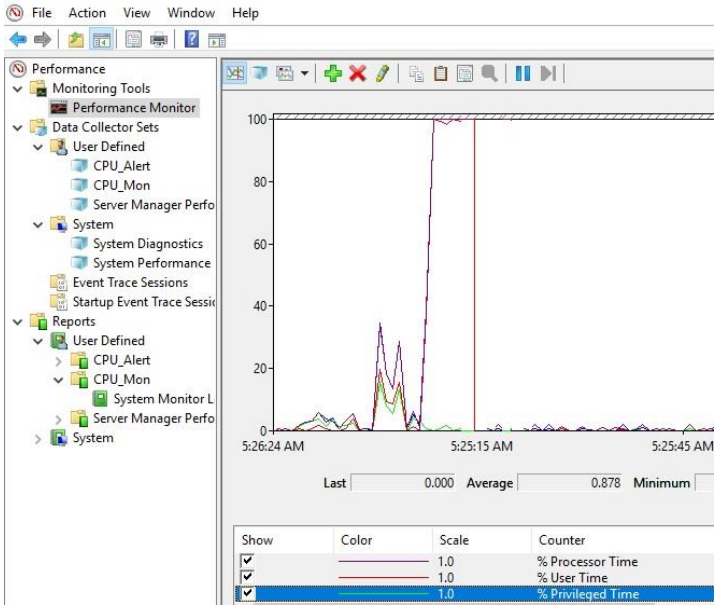
Для снятия данных о производительности процессора воспользуемся несколькими основными счётчиками:

- **\Processor\% Processor Time** — определяет уровень загрузки ЦП, и отслеживает время, которое ЦП затрачивает на работу процесса. Уровень загрузки ЦП в диапазоне в пределах 80-90 % может указывать на необходимость добавления процессорной мощности.
- **\Processor\%Privileged Time** — соответствует проценту процессорного времени, затраченного на выполнение команд ядра операционной системы Windows, таких как обработка запросов ввода-вывода SQL Server. Если значение этого счетчика постоянно высокое, и счетчики для объекта *Физический диск* также имеют высокие значения, то необходимо рассмотреть вопрос об установке более быстрой и более эффективной дисковой подсистемы
- **\Processor\%User Time** — соответствует проценту времени работы CPU, которое он затрачивает на выполнение пользовательских приложений.

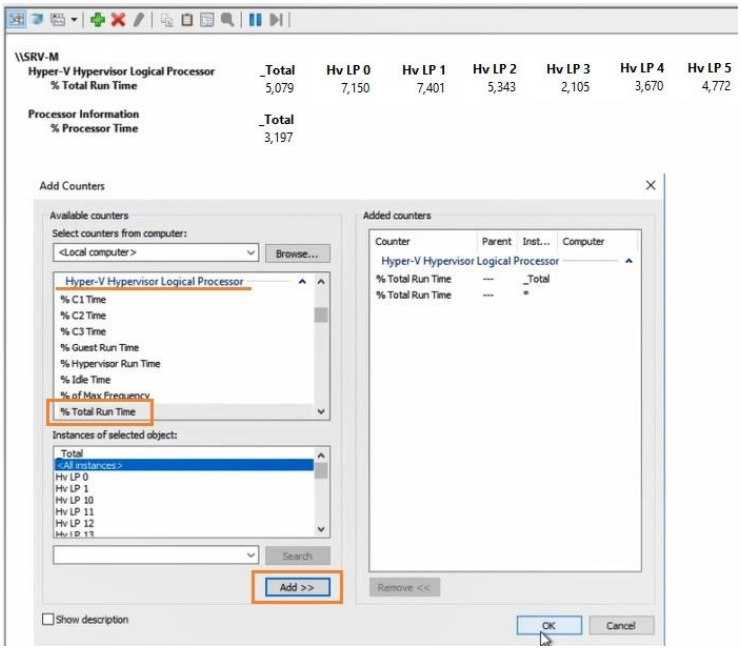
Запустите Performance Monitor с помощью команды **perfmon**. *В* разделе **Performance Monitor** отображается загрузкой CPU в реальном времени с помощью графика (параметр *Line*), с помощью цифр (параметр *Report*), с помощью столбчатой гистограммы (параметр *Histogram bar*) (вид выбирается в панели инструментов). Чтобы добавить счетчики, нажмите кнопку “+” (Add Counters).



Слева направо двигается линия в реальном времени и отображает график загрузки процессора, на котором можно увидеть, как всплески, так и постоянную нагрузку.



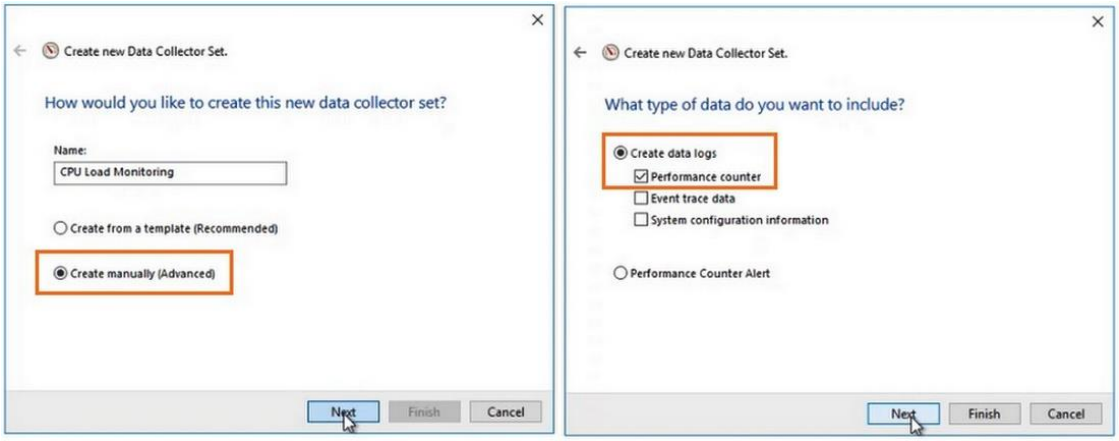
Например, вам нужно посмотреть загрузку процессора виртуальными машинами и самим Hyper-V. Выберите группу счетчиков **Hyper-V Hypervisor Logical Processor**, выберите счетчик **% Total Run Time**. Вы можете показывать нагрузку по всем ядрам CPU (Total), либо по конкретным (HV LP №), либо всё сразу (All Instances). Выберем *Total* и *All Instances*.



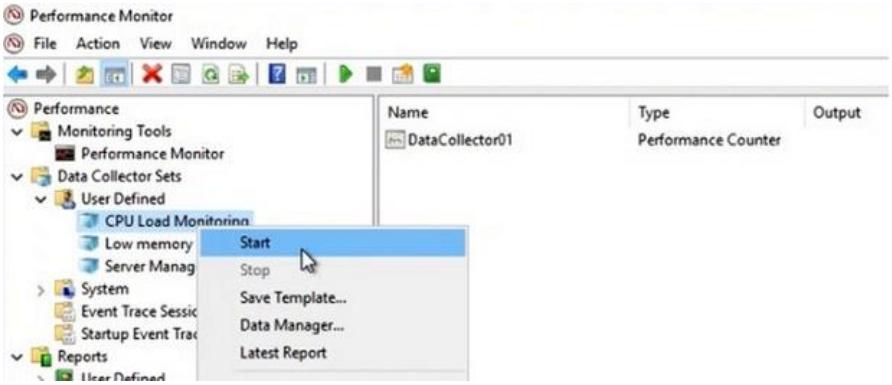
Группы сборщиков данных в PerfMon

Чтобы не сидеть целый за наблюдением движения линии, создаются группы сбор данных (**Data Collector Set**), задаются для них параметры и периодически просматриваются.

Чтобы создать группу сбора данных, нужно нажать на разделе **User Defined** правой кнопкой мыши, в меню выбрать **New** -> **Data Collector Set**. Выберите **Create manually (Advanced)** -> **Create Data Logs** и включите опцию **Performance Counter**. Нажмите **Add** и добавите счётчики. В нашем примере **% Total Run Time** из группы Hyper-V Hypervisor Logical Processor и **Available MBytes** из Memory. Установите интервал опроса счётчиков в 3 секунды.



Далее вручную запустите созданный Data Collector Set, нажав на нём правой кнопкой мыши и выбрав в меню пункт **Start**.



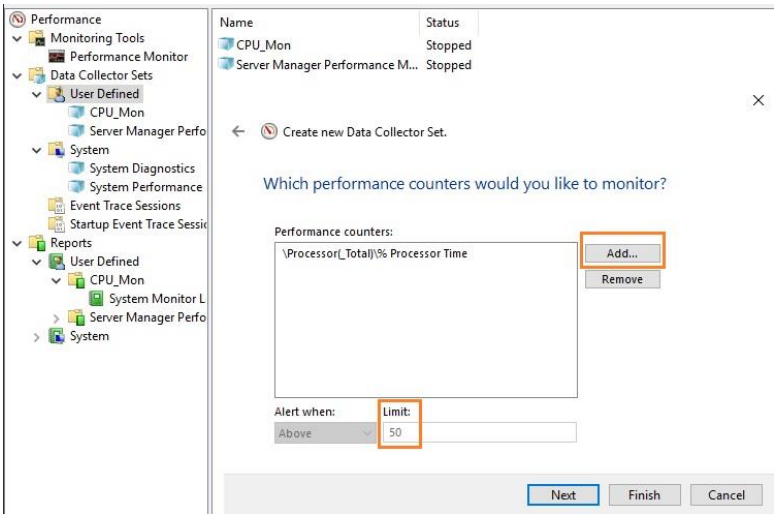
Через некоторое время можно просмотреть отчёт. Для этого в контекстном меню группы сбора данных нужно выбрать пункт **Latest Report**. *Вы можете* посмотреть и проанализировать отчёт производительности в виде графика. Отчёт можно скопировать и переслать. Он хранится в C:\PerfLogs\Admin\CPU_Mon и имеет расширение **.blg**.

Если нужно на другом сервере запустить такой же набор счётчиков, как на первом, то их можно переносить экспортом. Для этого в контекстном меню группы сбора данных выберите пункт **Save Template**, укажите имя файла (расширение .xml). Скопируйте xml файл на другой сервер, создайте новую группу сбора данных, выберите пункт **Create from a template** и укажите готовый шаблон.

Создание Alert для мониторинга загрузки CPU

В определённый критический момент в Performance Monitor могут срабатывать алерты, которые помогают ИТ-специалисту прояснить суть проблемы. В первом случае алерт может отправить оповещение, а во втором – запустить другую группу сбора данных.

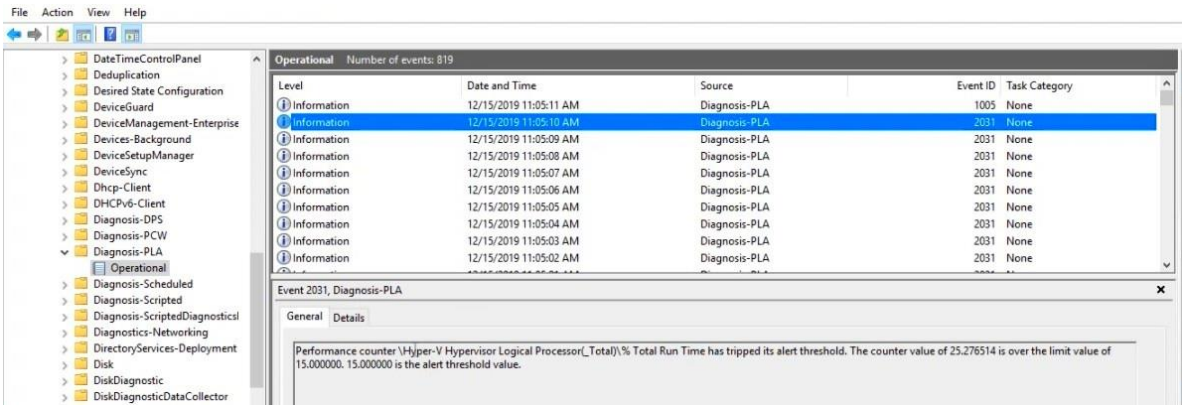
Чтобы создать алерт в PerfMon, нужно создать ещё один Data Collector Set. Укажите его имя CPU_Alert, выберите опцию Create **manually (Advanced)**, а затем — **Performance Counter Alert**. Добавьте счётчик **% Total Run Time** из Hyper-V Hypervisor Logical Processor, укажите границу загрузки 50 %, при превышении которой будет срабатывать алерт, установите интервал опроса счётчика в 3 секунды.



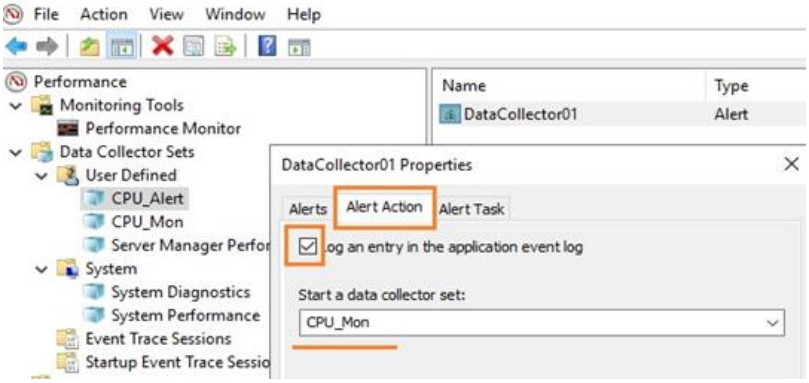
Далее нужно зайти в свойства данной группы сбора информации, перейти на вкладку *Alert Action*, включить опцию **Log an entry in the application event log** и запустить группу сбора данных. Когда сработает алерт, в журнале (в консоли Event Viewer в разделе

Applications and Services Logs\Microsoft\Windows\Diagnosis-PLA\Operational) появится запись:

"*Performance counter \Processor(_Total)\% Processor Time has tripped its alert threshold. The counter value of 100.000000 is over the limit value of 50.000000. 50.000000 is the alert threshold value*".

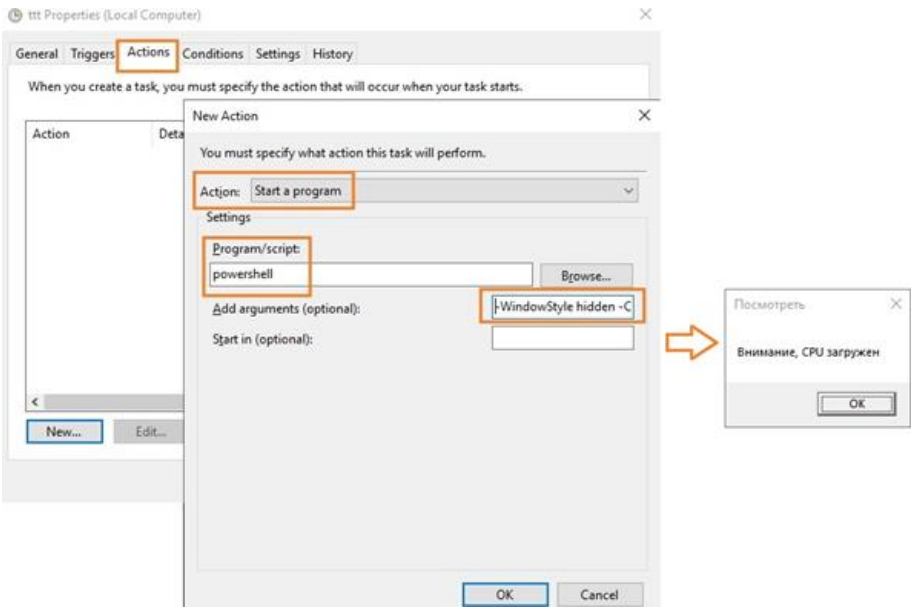


Здесь же рассмотрим и второй случай, когда нужно запустить другую группу сбора данных. Например, алерт срабатывает при достижении высокой загрузки CPU, делает запись в лог, но вы хотите включить сбор данных с других счётчиков для получения дополнительной информации. Для этого необходимо в свойствах алерта в меню **Alert Action** в выпадающем списке **Start a data collector set** выбрать ранее созданную группу сбора, например, CPU_Mon. Рядом находится вкладка **Alert Task**, в которой можно указать разные аргументы либо подключить готовую задачу из консоли Task Scheduler, указав её имя в поле **Run this task when an alert is triggered**. Будем использовать второй вариант.



С помощью Task Scheduler можно выполнить какие-то действия: выполнить команду, отправить письмо или вывести сообщение на экран (сейчас последниед ве функции не поддерживаются, считаются устаревшими (deprecated)). Для вывода на уведомления на экран можно использовать скриптом PowerShell. Для этого в консоли Task Scheduler создайте новую задачу, на вкладке **Triggers** выберите **One time**, на вкладке **Actions** в выпадающем поле **Action** выбирите параметр **Start a program**, в поле Program/Script укажите **powershell.exe**, а в поле Add arguments (optional) следующий код:

-WindowStyle hidden -Command "& {[System.Reflection.Assembly]::LoadWithPartialName('System.Windows.Forms'); [System.Windows.Forms.MessageBox]::Show('Внимание, CPU загружен', 'Посмотреть')}"



Для отправки письма вы можете воспользоваться командлетом PowerShell Send-MailMessage или стороннюю утилиту mailsend.exe.. Для этого создайте аналогичное задание в Task Scheduler, в поле **Program/Script** укажите полный путь к утилите (у нас *C:\Scripts\Mail\mailsend.exe)*, а в поле **Add arguments (optional)** через параметры нужно передать значения: электронный адрес, адрес и номер порта SMTP-сервера, текст письма и заголовка, пароль:

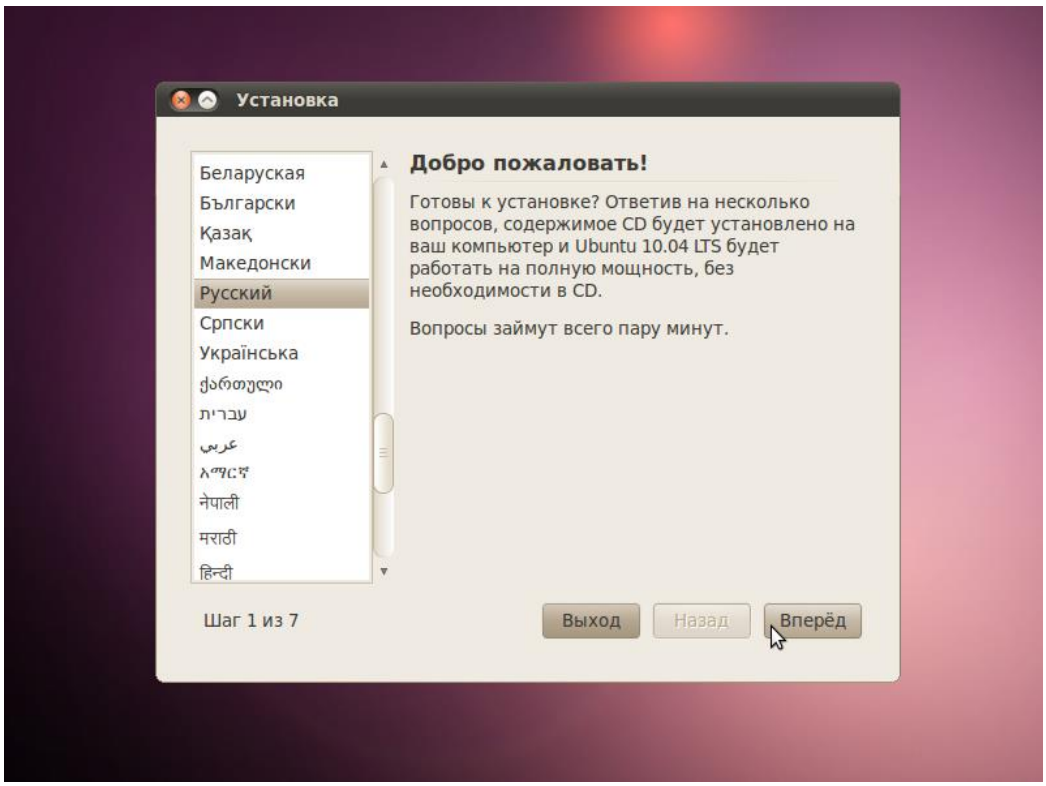
-to dep.it@ddd.com -from dep.it@ddd.com -ssl -port 465 -auth -smtp smtp.ddd.com -sub Alarm -v -user dep.it@ddd.com +cc +bc -M "Alarm, CPU, Alarm" -pass "it12345"

где *+cc* означает не запрашивать копию письма, *+bc* — не запрашивать скрытую копию письма.

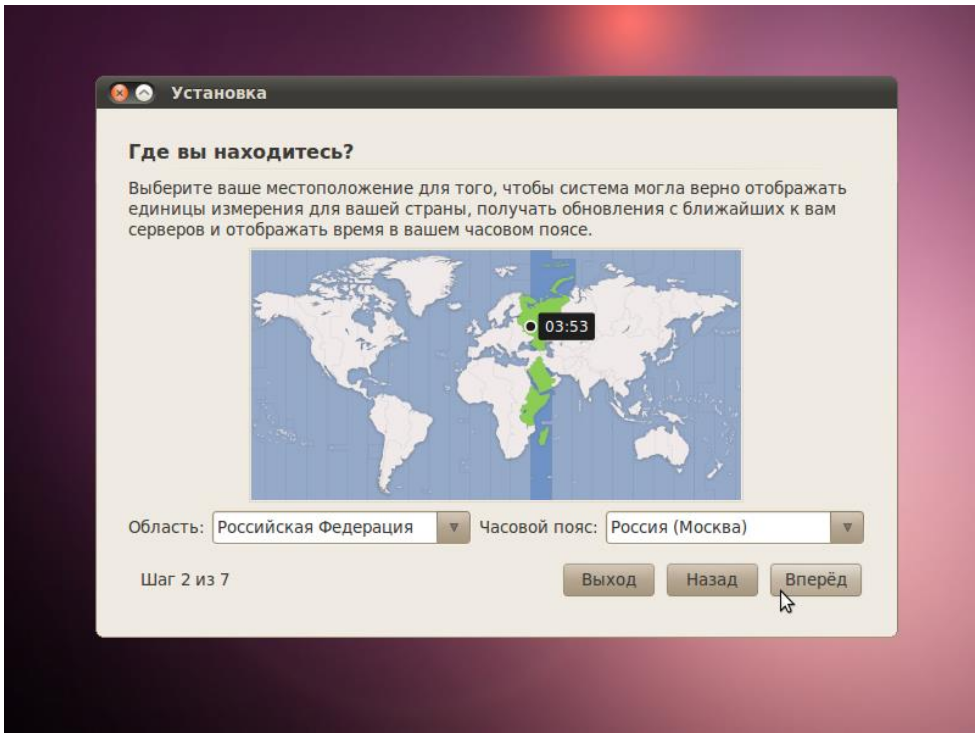
2.18. Практическая работа № 18
Установка web-сервера Ubuntu

Задание:
Запускаем VirtualBox и создаем виртуальную машину с именем Ubuntu -serv_1

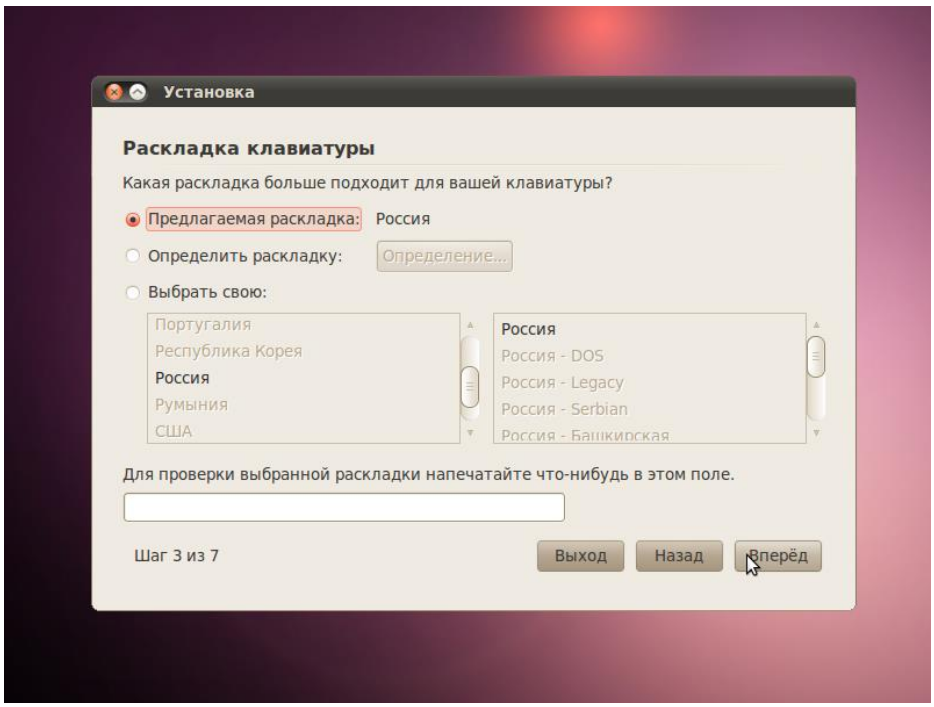
Шаг 1 в графическом мастере установки подразумевает выбор языка для новой операционной системы. Выбрав язык на левой панели, нажмите кнопку «Вперед».



Далее нужно будет выбрать ваш часовой пояс. Можно либо просто щёлкнуть в нужном месте на карте, либо выбрать регион или крупный город, находящийся в вашем часовом поясе. Установив часовой пояс, нажмите кнопку *Вперед*.

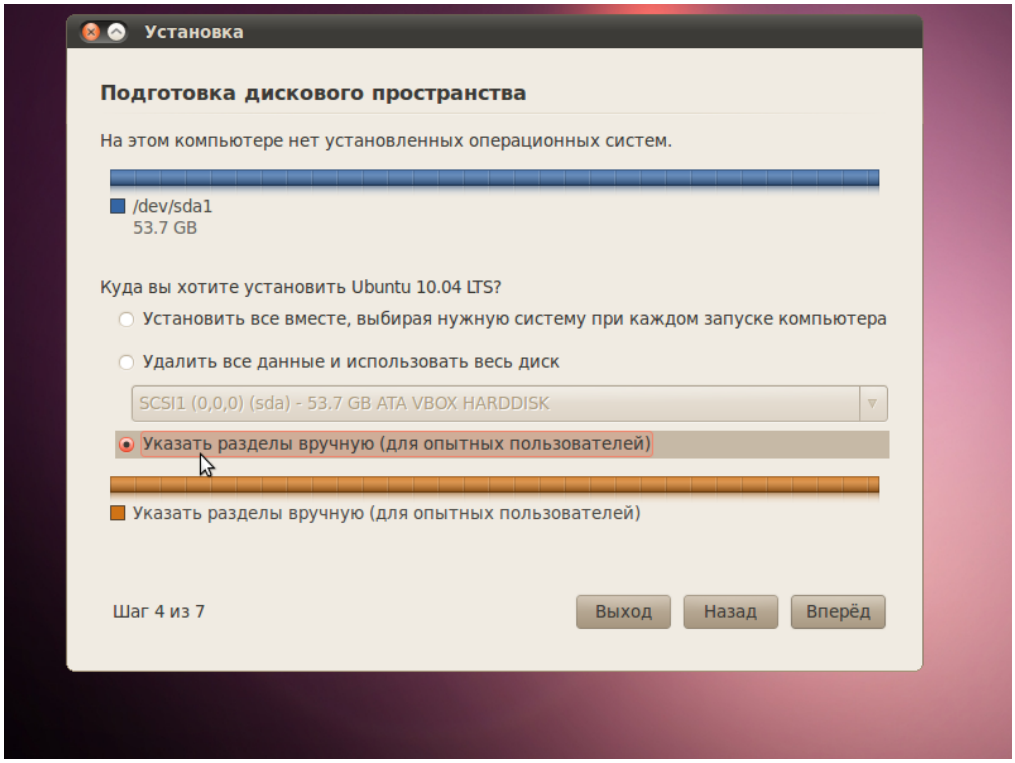


Третий шаг связан с настройкой клавиатуры. Можно оставить опцию *Предлагаемая раскладка* или выбрать собственные настройки, указав язык клавиатуры на левой панели и раскладку клавиатуры на правой панели. Определившись с выбором, нажмите кнопку *Вперед*.



Данный шаг подразумевает выполнение двух задач: во-первых, подготовка, которая заключается в освобождение места под разделы Linux, а во-вторых, создание разделов Linux.

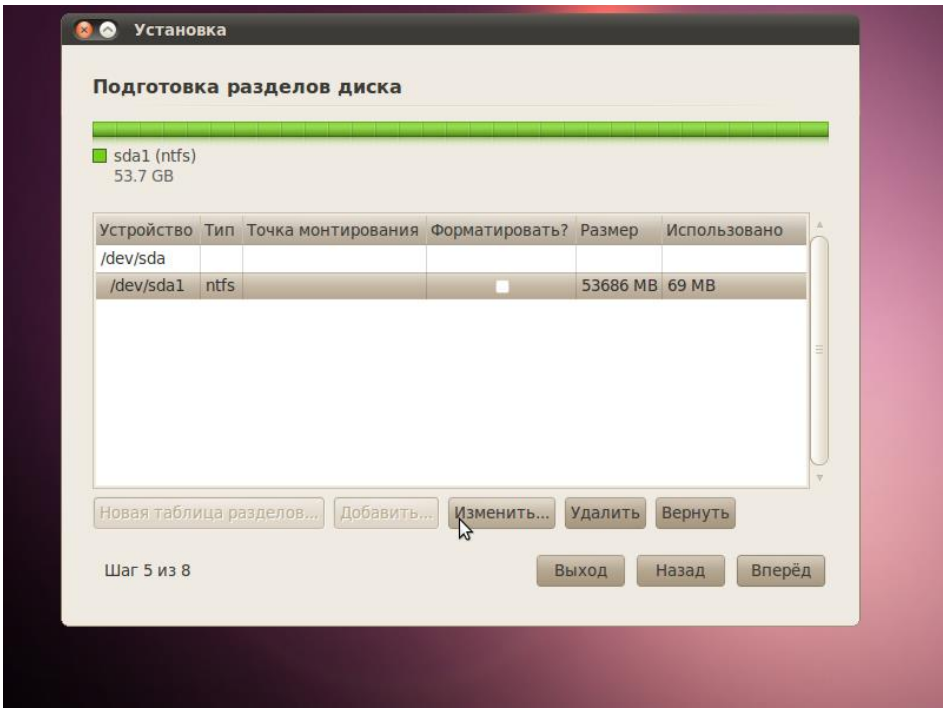
Для начала вам будет предложено несколько опций, в зависимости от того, что в данный момент находится на вашем жёстком диске. Выберите *Задать разделы вручную* и нажмите *Вперед*, не обращая внимания на то, что сейчас есть на диске.



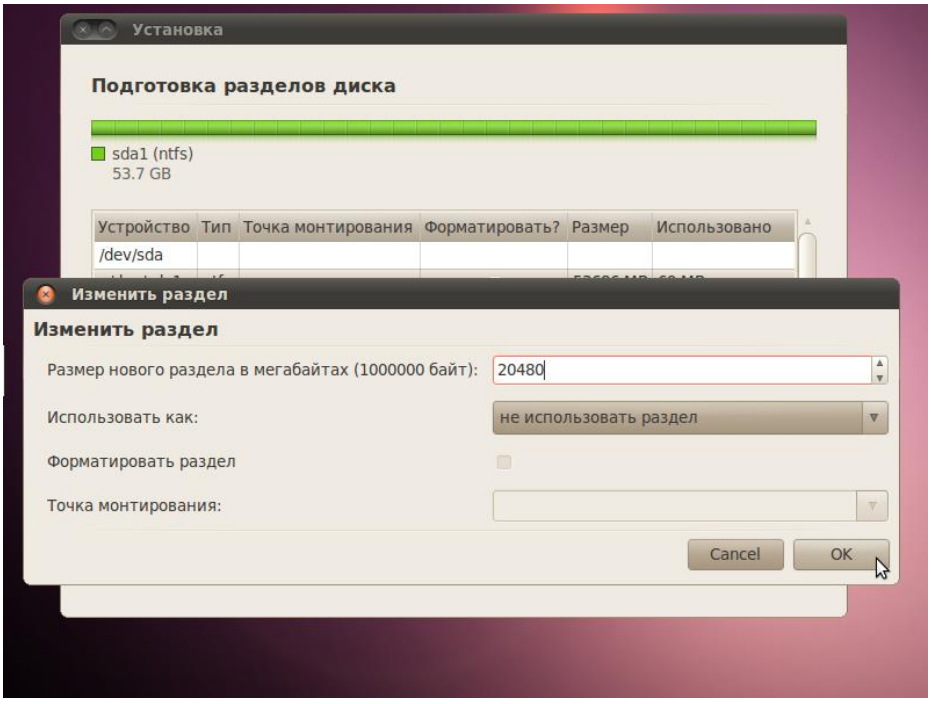
- Если весь диск полностью размечен под Windows, выполняйте указания Части A.
- Если диск совершенно пустой или вы хотите установить Ubuntu на второй жёсткий диск, а Windows оставить на первом, выполняйте указания Части B.

- Если на диск установлена операционная система Windows, и есть неразмеченное свободное дисковое пространство, выполняйте указания Части С.

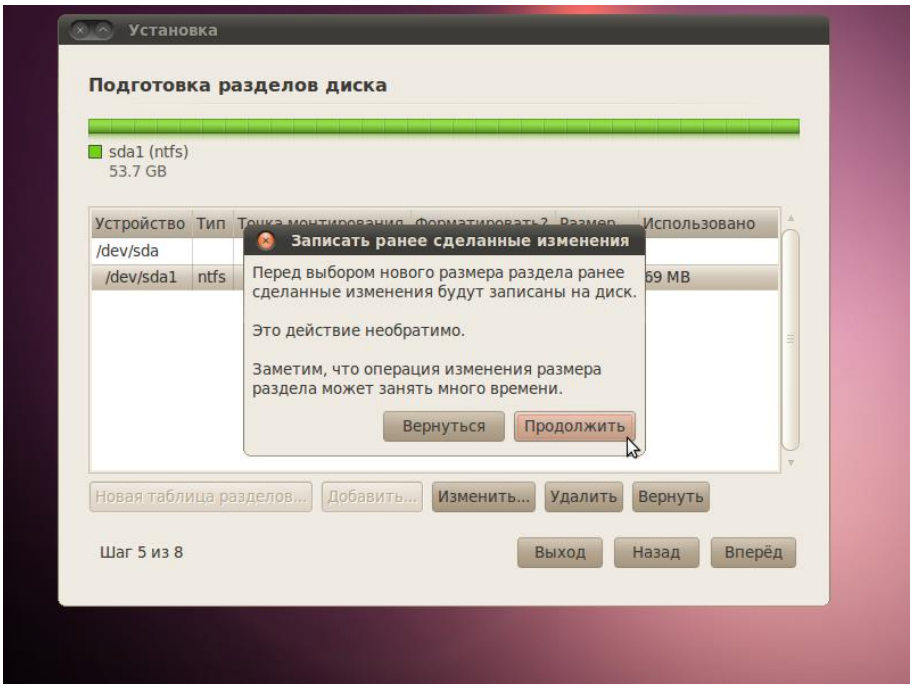
1. Если весь диск полностью размечен под Windows, выберите свой раздел Windows и нажмите кнопку *Изменить…*.



2. В появившемся диалоговом окне вам нужно сократить размер раздела Windows, чтобы появилось свободное место для Ubuntu. В первое поле введите размер (в мегабайтах), до которого вы хотите уменьшить раздел Windows, а во втором поле выберите «не использовать раздел». Нажмите *OK*.



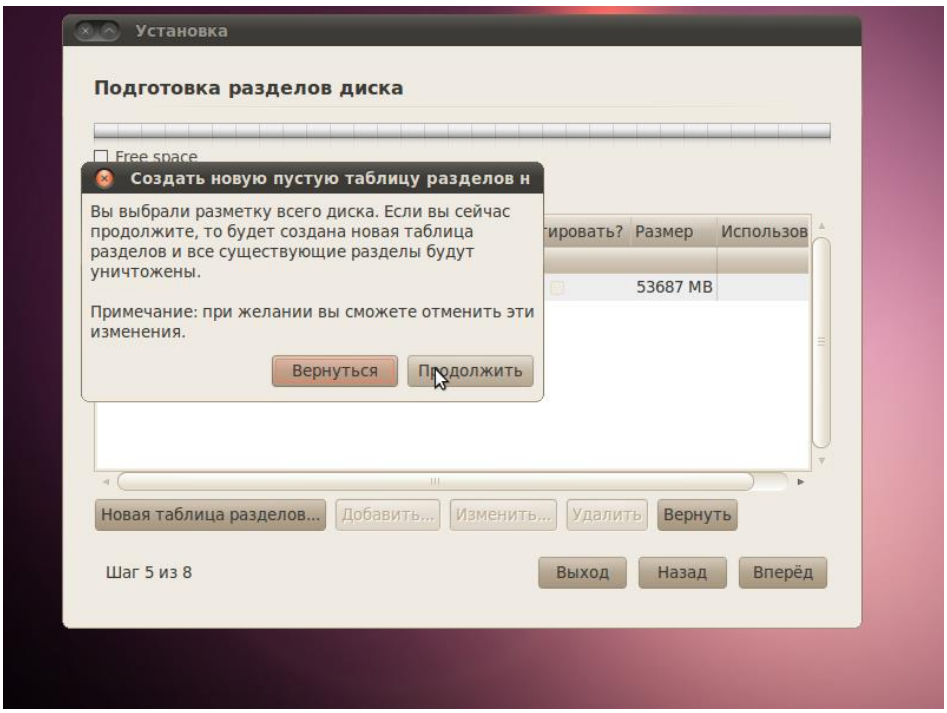
3. Появится диалоговое окно с просьбой подтвердить изменения. Это ваш последний шанс всё отменить, прежде чем изменения вступят в силу. Если вы готовы, нажмите *Продолжить*.



4. Таким образом вы получили свободное пространство для установки.

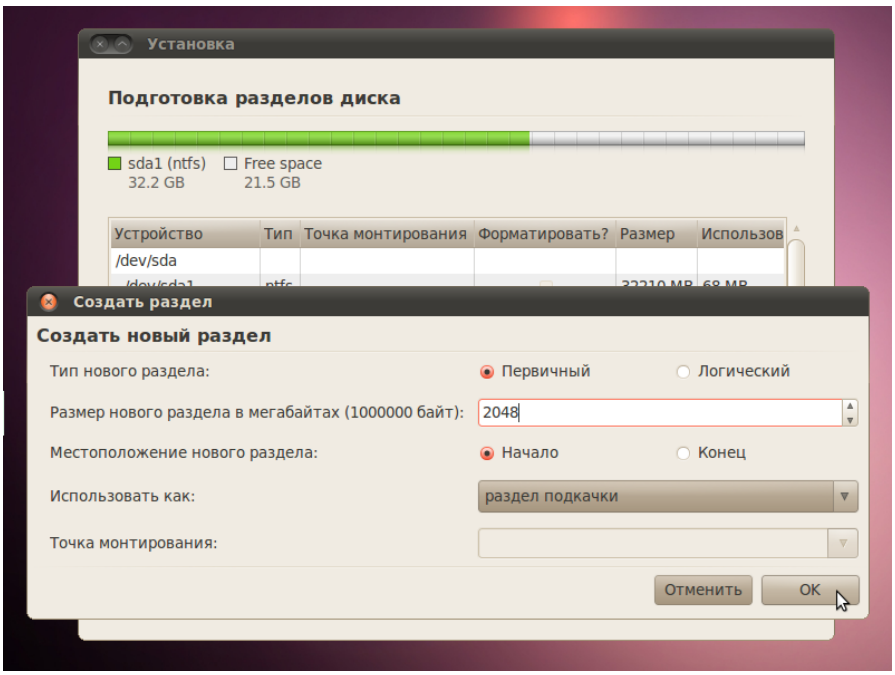
   Далее следуйте пунктам 2 и 3 Части B.

1. Если у вас один жёсткий диск, и он совершено пустой, то первым делом нужно будет создать новую таблицу разделов. Для этого выберите свой пустой диск, который обычно обозначается как HDA (для IDE) или SDA (для SATA, SCSI и USB), и нажмите кнопку *Новая таблица разделов*. Если вы устанавливаете Ubuntu на второй жёсткий диск, а на первом у вас установлена Windows, то второй диск, скорее всего, будет обозначен «HDB» или «SDB» (или наоборот, второй диск будет HDA или SDA). Появится предупреждение о возможной потере данных. Если у вас несколько дисков, убедитесь, что вы выбрали нужный, и нажмите «Продолжить».

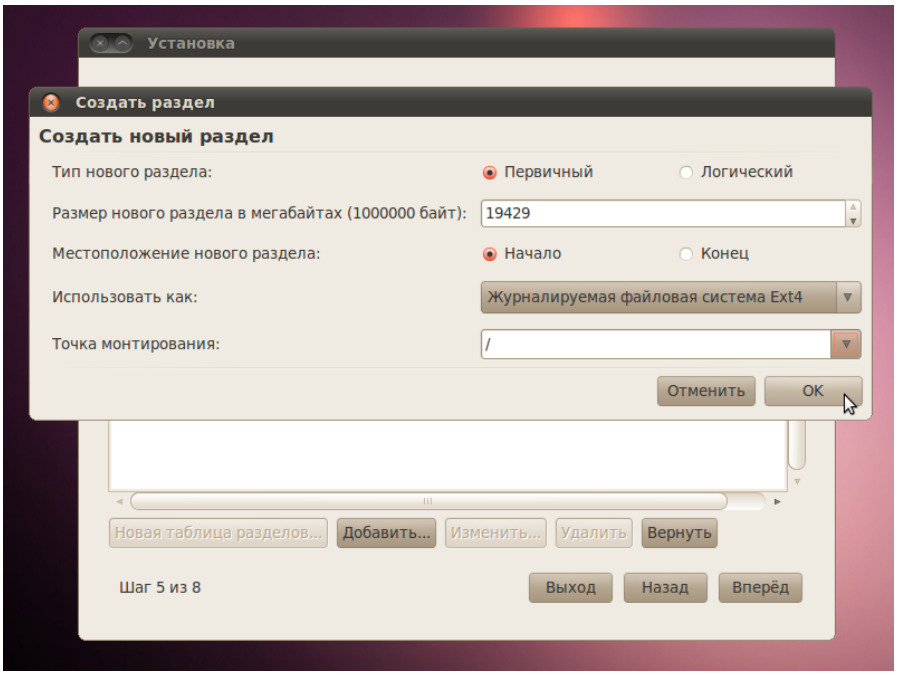


Получится новая таблица - свободное пространство без разделов.

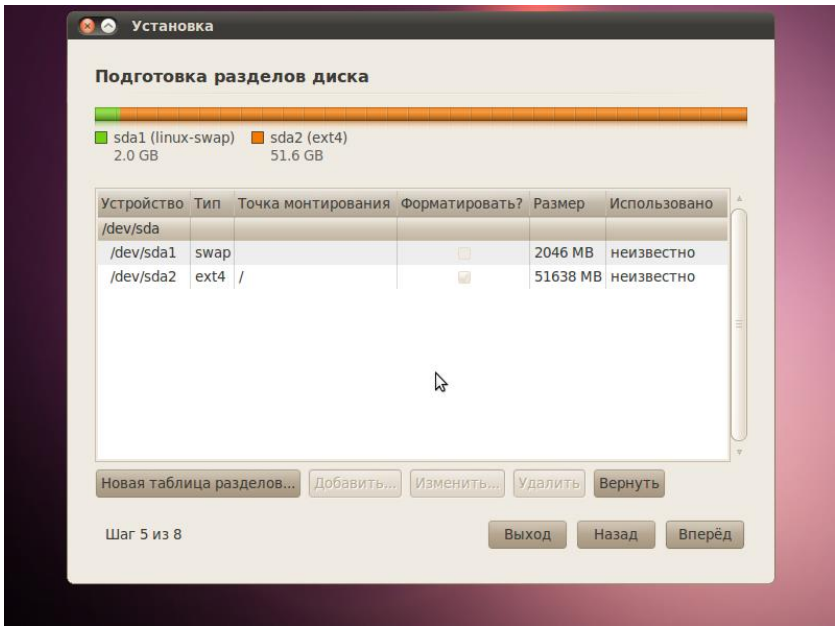
2. Как и в случае с местом, предназначенным для файлов подкачки в Windows, существуют разные мнения по поводу того, каким должен быть размер раздела «swap». Для простоты выделяем под «swap» место, равное объёму оперативной памяти системы. Если у вас 512 Мбайт памяти, то раздел «swap» должен иметь размер 512 Мбайт. Если у вас 4 Гбайт памяти, то и раздел «swap» будет на 4 Гбайт. Будет ли раздел первичным (primary) или логическим (logical), зависит от того, сколько операционных систем вы планируете поставить на этот диск. Максимальное число первичных разделов – четыре на диск. Хотя есть определённая выгода от расположения раздела «swap» в начале или в конце жёсткого диска, в значительной степени это зависит от индивидуальных спецификаций винчестера. Выберите пункт *свободное пространство* и нажмите кнопку *Добавить…*. Заполните все поля, кроме «Точка монтирования» и нажимите *OK*.



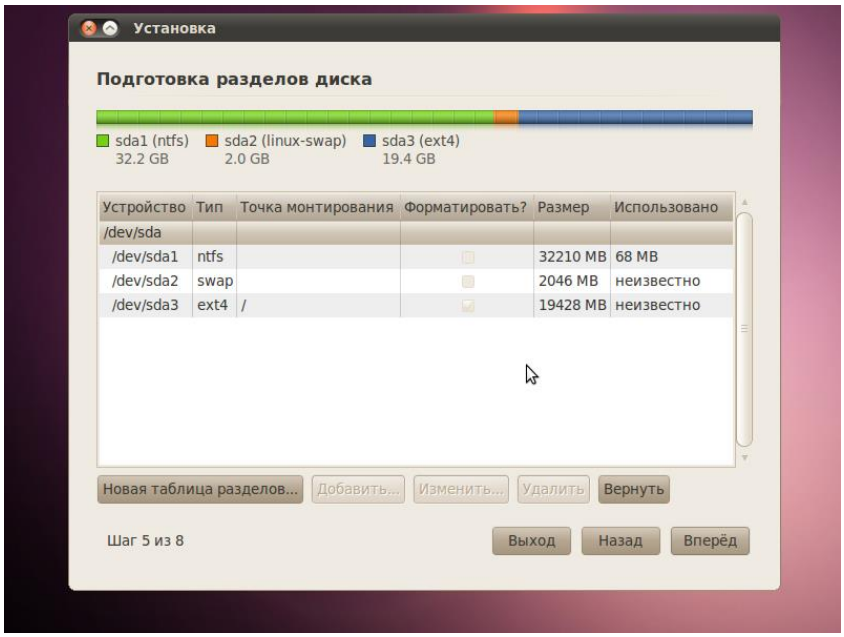
3. Далее нужно создать корневой раздел (/). Выберите пункт *свободное пространство* и нажмите кнопку *Добавить*…. Поскольку корневой раздел будет содержать все точки монтирования, вы должны выделить для него место. Минимум для корневого раздела (/) - 4 Гбайт, и этого будет достаточно, если большинство ваших приложений находятся в онлайне (в облаке). Однако если вы планируете установить много приложений локально или приложения будут большими, то нужно выделить для корневого раздела (/) больше места. Рекомендуется выделить под корневой раздел от 15 Гбайт и более, в зависимости от того, сколько у вас доступно места. В отличие от Windows, системные файлы Ubuntu можно установить как на первичный, так и на логический раздел. Для данного раздела выберите *Журналируемая файловая система Ext4*, точку монтирования - /, затем нажмите *OK*.



Для тех кто в начале следовал Части B. разметка диска должна выглядеть так:



Для тех кто в начале следовал Части A. и Части C. разметка диска должна выглядеть так:



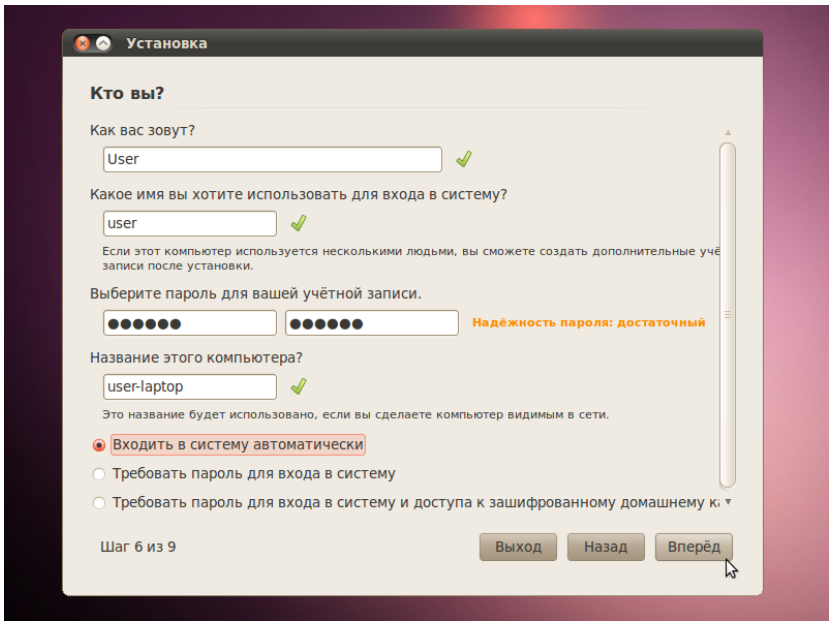
Теперь, когда разделы созданы, нажмите кнопку *Вперед*, чтобы продолжить установку. Перейдите к

Если на диск установлена операционная система Windows, и есть неразмеченное свободное дисковое пространство, то это должно выглядеть примерно так:

Далее следуйте пунктам 2 и 3

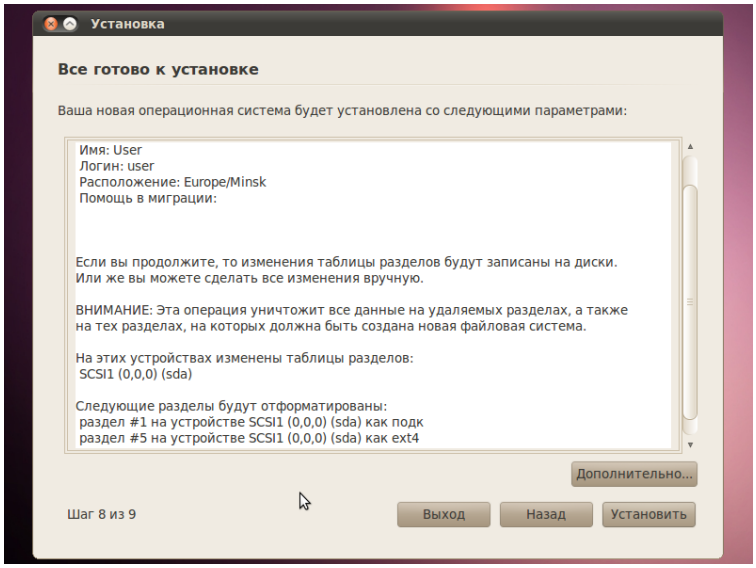
Этот этап процесса установки очень простой, но очень важно записать или запомнить те данные, которые вы здесь вводите! В верхнее поле введите своё имя. Во втором поле появится имя пользователя, образованное от вашего имени, которое вы указали выше.

Здесь вы можете изменить имя пользователя, если вас не устраивает предложенный вариант. Главное – не забыть то имя пользователя, которое вы ввели! Имя пользователя и пароль вам понадобятся не только для входа в систему.



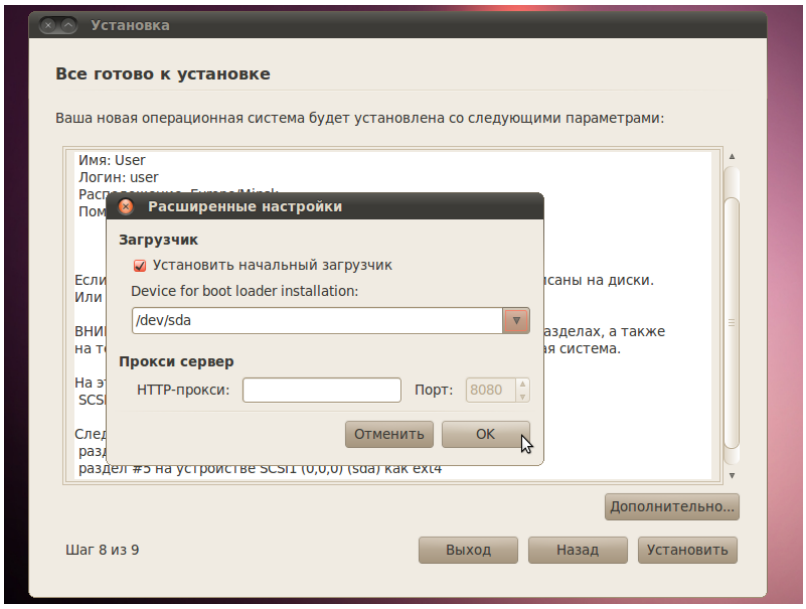
Следующий шаг называется *Перенос настроек из других операционных систем* – это мастер для переноса вспомогательных файлов и настроек. Этот шаг будет пропущен, если на вашем компьютере не установлено других операционных систем. Если Ubuntu является единственной операционной системой, то вы сразу перейдёте к последнему шагу. Если же у вас уже установлена операционная система Windows, то вам будет предложено перенести в Ubuntu файлы и настройки из пользовательских учётных записей Windows.

На последнем шаге выводится окно, в котором подытожены все выбранные вами изменения и настройки.

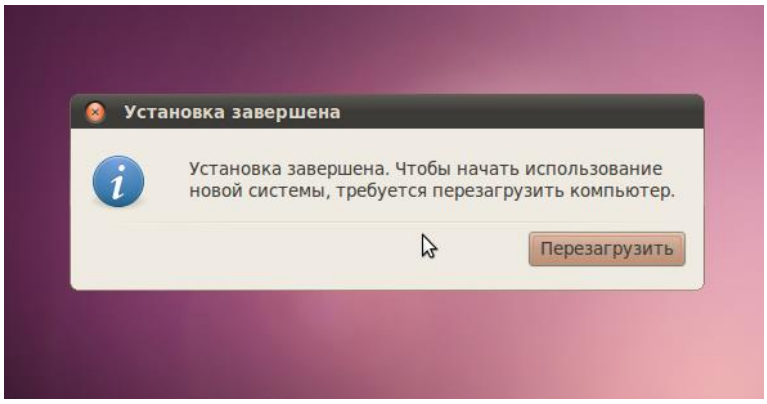


Кнопка *Дополнительно…* вызывает окно с расширенными опциями для начального загрузчика GRUB, а также с настройками прокси-сервера и предложением поучаствовать в опросе пользователей. Если у вас несколько жёстких дисков, убедитесь, что начальный

загрузчик будет установлен на тот жёсткий диск, который будет загружаться первым. Значение по умолчанию обычно указывает на первый жёсткий диск в очереди загрузки. Подтвердите свой выбор кнопкой *OK*. Если вы готовы нажмите *Установить*, чтобы начать копировать файлы на жёсткий диск.



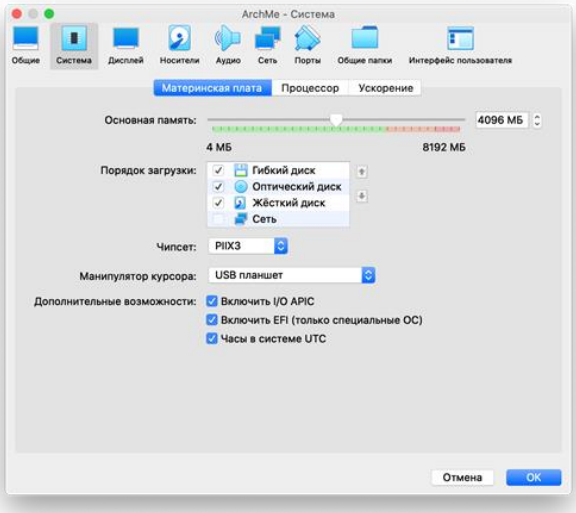
В зависимости от конфигурации вашей системы, копирование файлов может занять какое-то время. По завершении процесса вам будет предложено перезагрузить компьютер, нажав кнопку *Перезагрузить*.



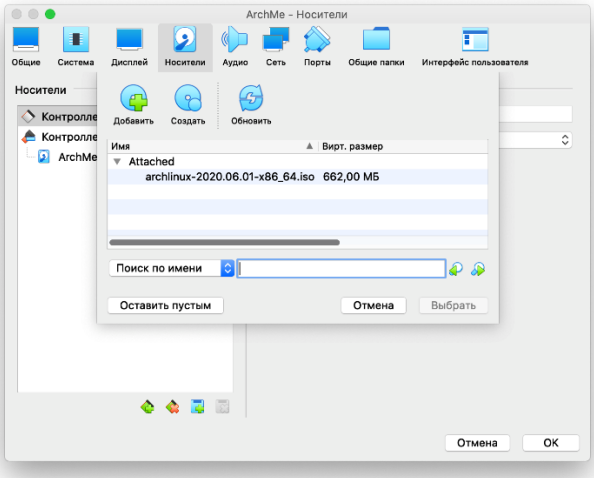
Сделайте скриншоты (фотографии) процесса установки сервера и вставьте в отчёт.

2.19. Практическая работа № 19
Установка web-сервера Arch Linux

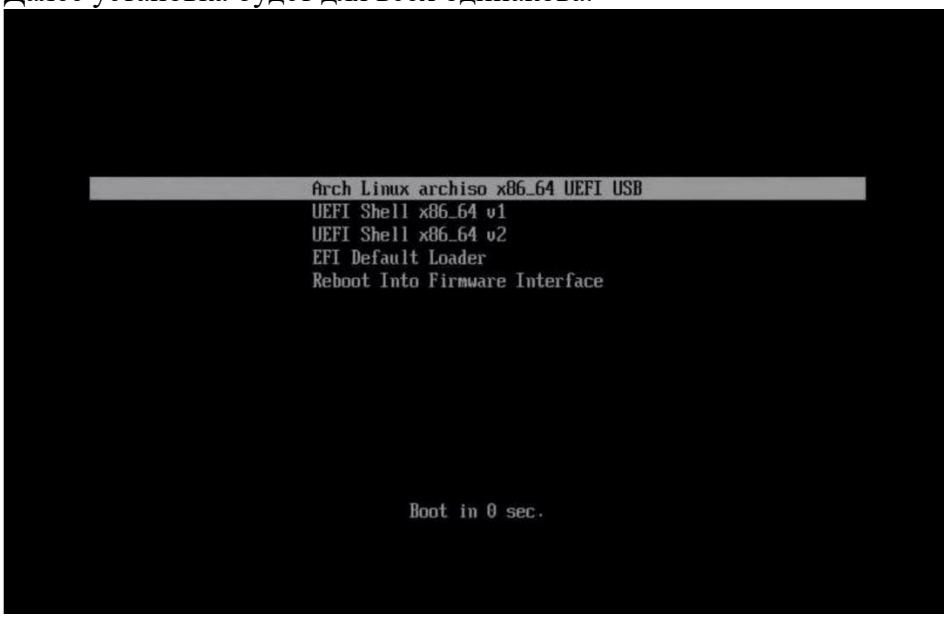
Задание:
Настроим VirtualBox, если вы используете её, то выполните следующие действия
1.Идём в настройки машины:
2.Во вкладке система ставим галочку около пункта "Включить EFI"



3.Далее идём во вкладку носители, там добавляем контроллер IDE и выбираем наш дистрибутив

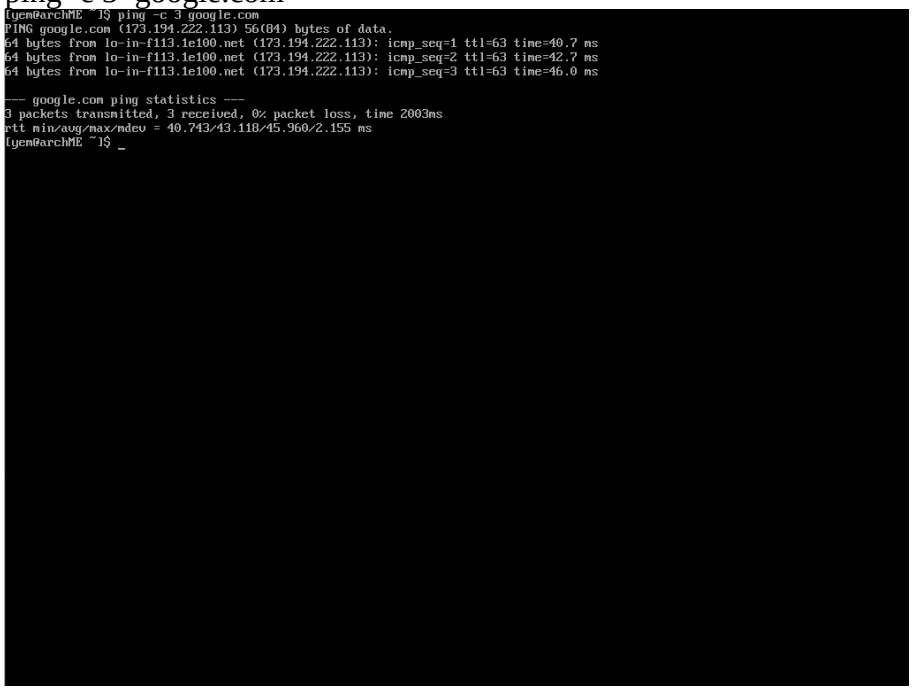


Далее установка будет для всех одинакова.

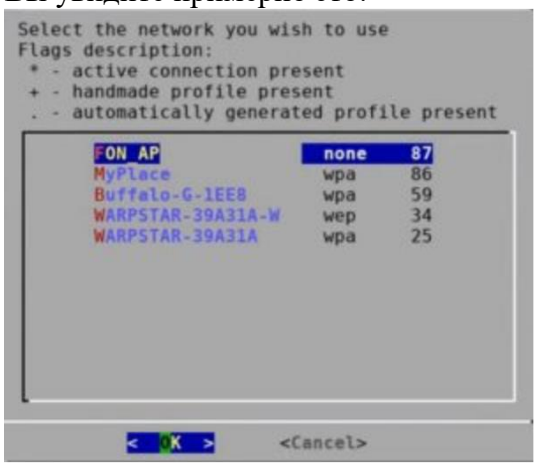


Выбираем первую строку и жмём Enter
Проверим соединение с интернетом:

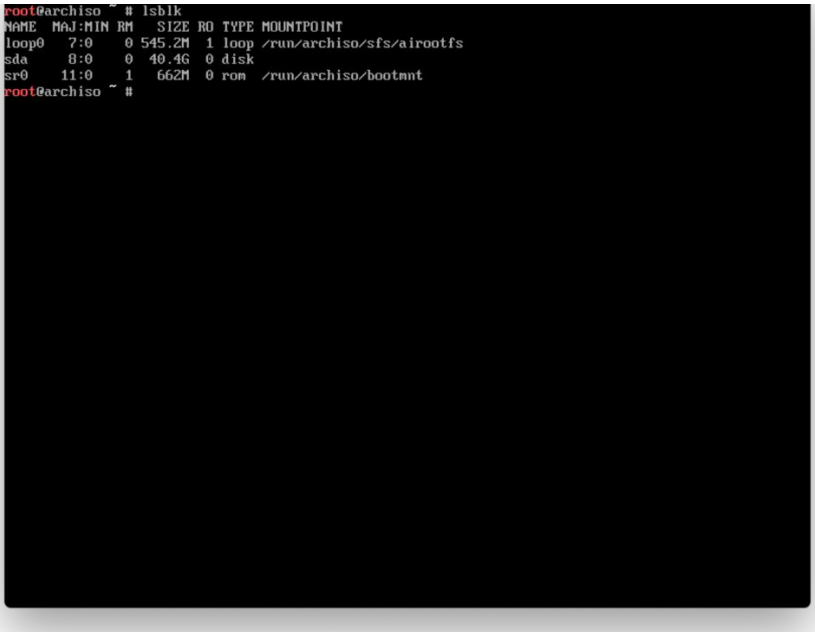
Это нужно, потому что Arch требует интернет для своей установки.
Такой командой можно проверить своё соединение и увидеть время ответа сайта.
ping -c 3 google.com



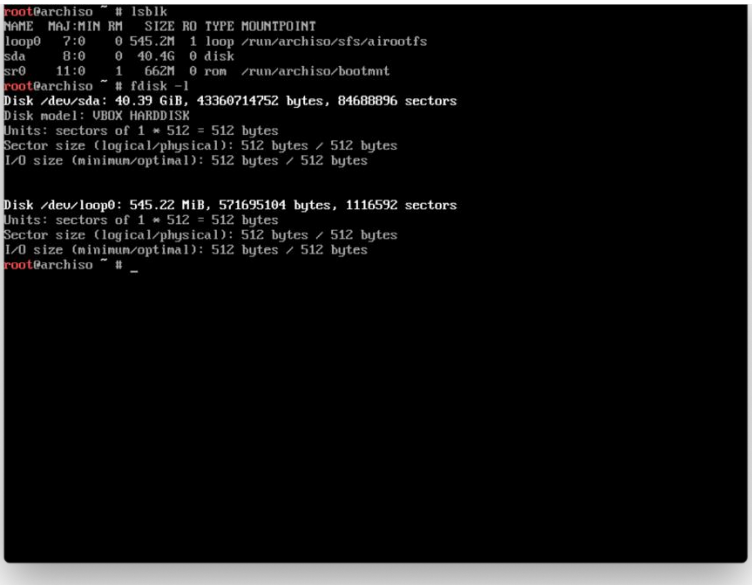
Если вы используете wifi на своём ПК, то используйте утилиту :
wifi-menu
Вы увидите примерно это:



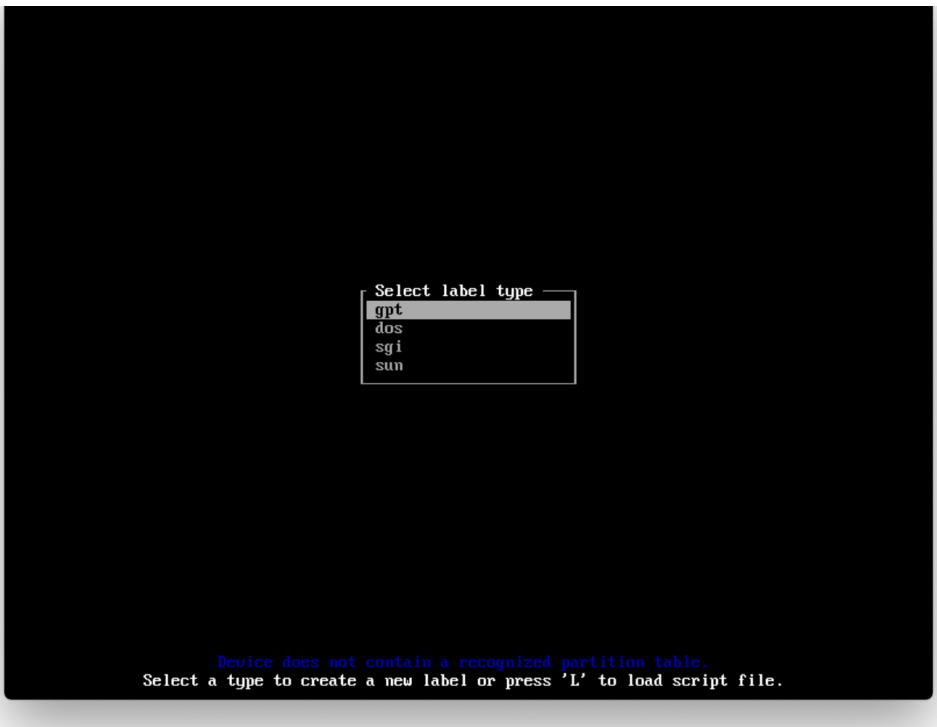
Разделы диска
Для того, чтоб разбить наш диск на разделы, можно сначала узнать какие диски подключены. Скорее всего у вас будет USB флешка и HDD\SSD вашего ПК.
Команда для просмотра разделов (понадобится нам ещё много раз):
lsblk



Если у вас несколько дисков, а вы хотите установить на какой-то конкретный, то можно посмотреть диски по размерам.
fdisk -l



Время размечать наш диск. Используем команду *cfdisk* для этого и выбираем *gpt* формат
cfdisk /dev/sda



Важно! если во время использования команды *lsblk* и *fdisk* вы увидели что sda является не тем диском, что нужен вам, то вы дописываете в конец название другого диска, например *sdb*.
Используя стрелочки создаём 3 раздела на диске:
/dev/sda1 # размером 1G места под UEFI
/dev/sda2 # размером примерно 10-15 GB под root
/dev/sda3 # всё оставшееся место под директорию home
PS: Если вы решили переделать разметку диска, то через эту утилиту можно и удалять разделы
Для проверки используем *lsblk* снова. Если всё норм, что */dev/sda* будет содежать в себе 3 раздела.
Далее форматируем наши разделы.
Форматируем тот раздел, который мы выделили под UEFi
mkfs.fat -F32 /dev/sda1
Раздел root
mkfs.ext4 /dev/sda2
Раздел home
mkfs.ext4 /dev/sda3
Монтируем *root* и создаём папку *home*:
mount /dev/sda2 /mnt
mkdir /mnt/home
mount /dev/sda3 /mnt/home

И снова *lsblk* для проверки

```
root@archiso ~ # mount /dev/sda2 /mnt
root@archiso ~ # mkdir /mnt/home
root@archiso ~ # mount /dev/sda3 /mnt/home
root@archiso ~ # lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0  463M  1 loop /run/archiso/sfs/airootfs
sda      8:0    0   20G  0 disk
├─sda1   8:1    0  512M  0 part
├─sda2   8:2    0   10G  0 part /mnt
└─sda3   8:3    0  9.5G  0 part /mnt/home
sr0     11:0    1  574M  0 rom  /run/archiso/bootmnt
root@archiso ~ # _
```

Установка

Начинается самая долгая часть, потому что нужно будет много скачать. Устанавливаем все основные пакеты, а также *nano*, чтоб редачить файлы системы. Если вдруг вы знакомы с vim можете скачать и его (дописать в конец).

pacstrap -i /mnt base linux linux-firmware sudo nano

Вам предложат что установить выбирайте *all* и далее *yes*. Встречался с проблемой, что можно было скачать *первый* или *второй* вариант, можно просто выполнить команду дважды выбирая вначале один пакет, а затем второй.

Создадим fstab файл

genfstab -U -p /mnt >> /mnt/etc/fstab

Настраиваем установленную систему

Chroot

Chroot (change root) нужен нам, чтобы мы могли сменить root пользователя (как и сказано в названии команды).

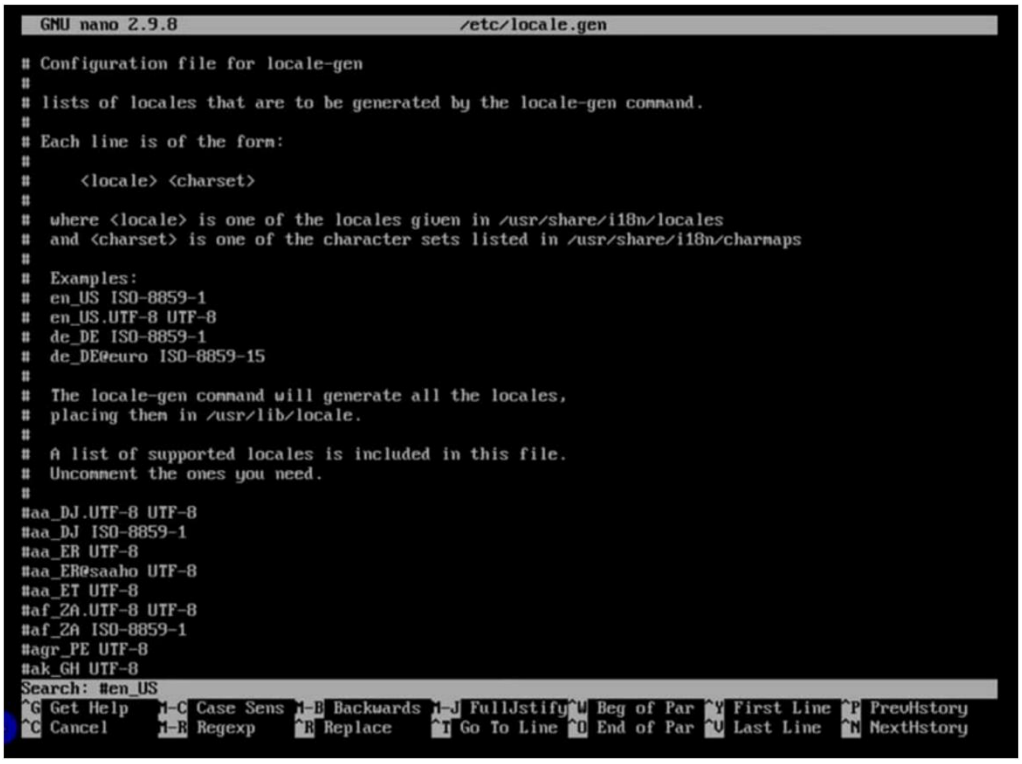
arch-chroot /mnt /bin/bash

```
root@archiso ~ # genfstab -U -p /mnt >>/mnt/etc/fstab
root@archiso ~ # genfstab --help
usage: genfstab [options] root

  Options:
    -L            Use labels for source identifiers (shortcut for -t LABEL)
    -p            Exclude pseudofs mounts (default behavior)
    -P            Include pseudofs mounts
    -t TAG        Use TAG for source identifiers
    -U            Use UUIDs for source identifiers (shortcut for -t UUID)

    -h            Print this help message

genfstab generates output suitable for addition to an fstab file based on the
devices mounted under the mountpoint specified by the given root.

root@archiso ~ # arch-chroot /mnt /bin/bash
[root@archiso /]# _
```

Настройка файла локали

Для начала идём в файл локали, чтоб настроить язык

nano /etc/locale.gen



Находим там *#en_US.UTF-8* и стираем #, с русским языком так же. PS: можно использовать Ctrl + W для поиска языка в файле.

Чтобы всё сохранить Ctrl + O, затем Enter и Ctrl + X, затем Enter

Далее пишем команды, которые сгенерируют локаль и создаём *locale.conf* с нужными настройками языка.

locale-gen

echo "LANG=en_US.UTF-8" > /etc/locale.conf

Настраиваем временную зону

ln -sf /usr/share/zoneinfo/

Далее жмём 2 раза на *Tab* и видим список регионов, после городов.

В моём случае было так:

ln -sf /usr/share/zoneinfo/Europe/Kaliningrad /etc/localtime

Задаём время

Тут 2 команды. Одна ставит время для системы, а другая его показывает.

hwclock --systohc --utc

date

Имя хоста и адрес

назвать ПК ArchMe, поэтому используем следующую команду:

echo ArchMe > /etc/hostname

Далее идём в файл *localhosts* и записываем ip. Если у вас ip статический, используйте свой.

nano /etc/hosts

127.0.1.1 localhost.localdomain ArchMe

Сетевой менеджер

Качаем и включаем.

pacman -S networkmanager

systemctl enable NetworkManager

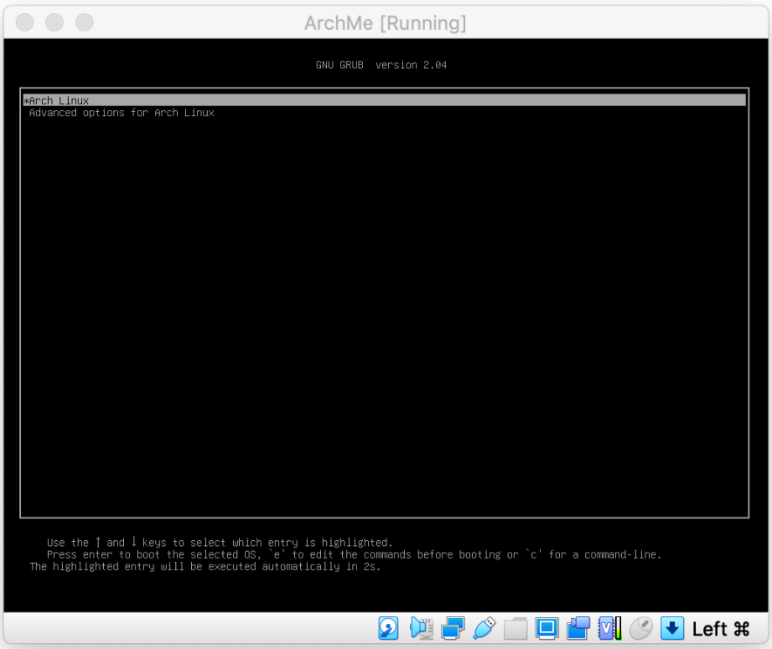
Установка GRUB

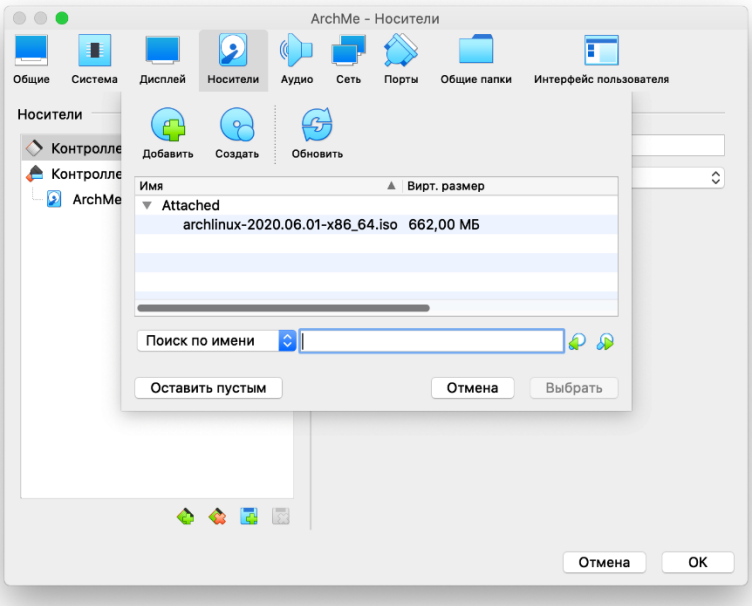
Для начала сменим пароль *root* пользователя :

passwd

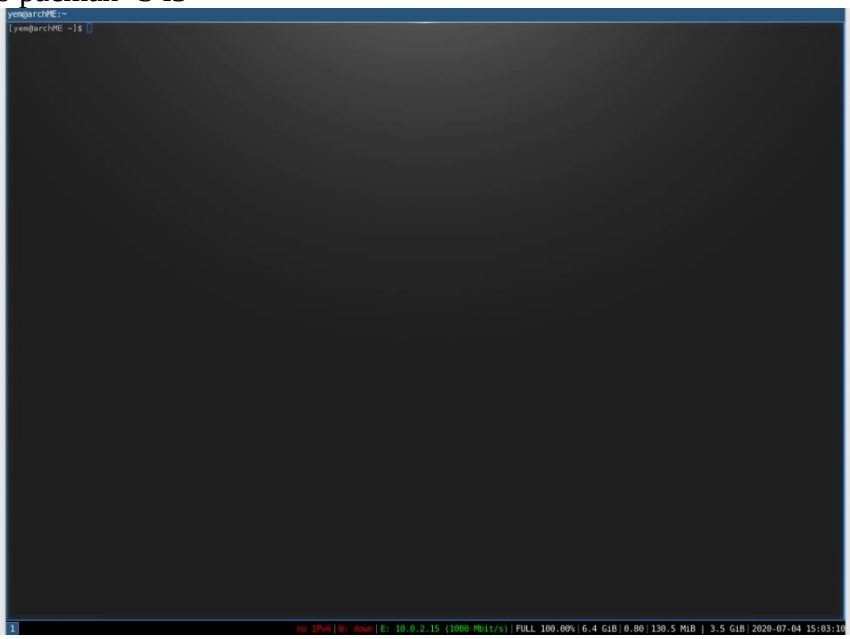
GRUB — это загрузчик, который нужен, чтоб запускать нашу установленную систему (в режиме EFI). Далее будет куча команд, которые нужно выполнить.

pacman -S grub efibootmgr
mkdir /boot/efi
mount /dev/sda1 /boot/efi
lsblk # для проверки всё ли норм смонтировано
grub-install --target=x86_64-efi --bootloader-id=GRUB --efi-directory=/boot/efi --removable
grub-mkconfig -o /boot/grub/grub.cfg
Перезагрузка
Чтобы без потерь перезагрузить нашу систему используем эти команды:
exit
umount -R /mnt
reboot
После перезагрузки вы увидите следующее. Если это так, то наш *GRUB* установился правильно





Входим в root аккаунт и создаём *swapfile* (что-то вроде доп оперативки) и задаём ему размер как у вашей **ОЗУ**
fallocate -l 3G /swapfile
Далее выполняем следующие команды:
chmod 600 /swapfile
mkswap /swapfile
swapon /swapfile
echo '/swapfile none swap sw 0 0' >> /etc/fstab
И проверяем, работает ли *swap*:
free -m
Добавим пользователя и окружение
useradd -m -g users -G wheel -s /bin/bash username
passwd username
username замените на то имя, что хотите вы)
Также нужно дать ему права суперюзера:
EDITOR=nano visudo
там ищем и убираем #, а дальше **Ctrl + O**, затем **Enter** и **Ctrl + X**, затем **Enter**
%wheel ALL=(ALL) ALL
pacman -S pulseaudio pulseaudio-alsa xorg xorg-xinit xorg-server
Вам будет предложен выбор, выбирайте исходя из своей графики.
Окружение
Вначале покажу как поставить довольно простое — **XFCE**
pacman -S xfce4 lightdm lightdm-gtk-greeter
echo "exec startxfce4" > ~/.xinitrc
systemctl enable lightdm
И моё любимое i3, там выбираем пакеты 2 4 5. Возможно вы увидите квадраты вместо символов, но это нормально, вам просто нужно будет скачать шрифт dejavu (pacman -S ttf-dejavu). Список горячих клавиш можно посмотреть тут
echo "exec i3" > ~/.xinitrc
sudo pacman -S i3



Если вы решите поменять своё окружение, то нужно будет менять запись в файле **xinitrc**.
Для запуска вашего окружения используйте
Startx

2.20. Практическая работа № 20
Установка и настройка apache, php, mysql на web-сервер Ubuntu

Задание:

Шаг 1. Установка Apache
Ubuntu 18.04 имеет огромный репозиторий пакетов, которые вы можете установить всего одной командой *apt* из консоли. Для инсталяции Apache, запустите в консоли следующую команду:
$ sudo apt install apache2
Чтобы подтвердить установку, нажмите «Y».
Чтобы убедиться в работоспособности установленного сервера, введите в адресной строке браузера IP-адрес вашего VPS. Если все в порядке, то увидите подобную страницу:

Шаг 2. Установка MySQL
Для установки сервера MySQL запустите в терминале команду:
$ sudo apt install mysql-server
Нажмите «Y» для подтверждения установки.
Настройки безопасности MySQL
Настройки по умолчанию не обеспечивают должной безопасности MySQL. Чтобы защититься от элементарных атак, нужно поменять конфигурацию. Делается это всего одной командой:
$ sudo mysql_secure_installation
Вам будет последовательно задано несколько вопросов по параметрам MySQL, которые нужно изменить. Нужно будет установить пароль для root-пользователя, настроить политику паролей, удалить доступ анонимным пользователям, тестовую базу и отключить

возможность удаленного подключения к базе. В терминале это будет выглядеть примерно так:
VALIDATE PASSWORD PLUGIN can be used to test passwords and improve security. It checks the strength of password and allows the users to set only those passwords which are secure enough. Would you like to setup VALIDATE PASSWORD plugin?

Press y|Y for Yes, any other key for No: Y

There are three levels of password validation policy:

LOW Length >= 8

MEDIUM Length >= 8, numeric, mixed case, and special characters

STRONG Length >= 8, numeric, mixed case, special characters and dictionary file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2

Please set the password for root here.

New password:

Re-enter new password:

Estimated strength of the password: 100

Do you wish to continue with the password provided?(Press y|Y for Yes, any other key for No) : Y

By default, a MySQL installation has an anonymous user, allowing anyone to log into MySQL without having to have a user account created for them. This is intended only for testing, and to make the installation go a bit smoother. You should remove them before moving into a production environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : Y

Success.

Normally, root should only be allowed to connect from 'localhost'. This ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : Y

Success.

By default, MySQL comes with a database named 'test' that anyone can access. This is also intended only for testing, and should be removed before moving into a production environment.

Remove test database and access to it? (Press y|Y for Yes, any other key for No) : Y

 - Dropping test database...

Success.

- Removing privileges on test database...

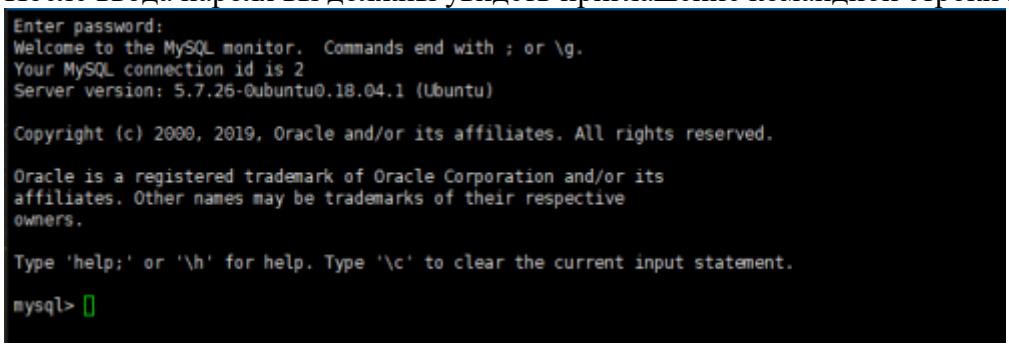
Success.

Reloading the privilege tables will ensure that all changes made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : Y

Success.

All done!
Проверяем работу MySQL-сервера
Чтобы убедиться в работоспособности вашего сервера баз данных, попробуйте подключиться к нему консольным клиентом. Делается это так:
$ sudo mysql -u root -p
После ввода пароля вы должны увидеть приглашение командной строки mysql.



Чтобы добавить новую базу данных, введите:
create database <dbname>
, где вместо <*dbname*> укажите нужное вам имя базы.

Шаг 3. Установка PHP
Чтобы установить PHP на Ubuntu 18.04, запустите в консоли команду:
$ sudo apt install php libapache2-mod-php
Проверка работоспособности PHP
Чтобы проверить работу PHP и посмотреть файл с информацией о нем, создайте тестовый скрипт в корневой директории вашего сайта:
$ sudo nano /var/www/html/info.php
Затем в открывшемся текстовом редакторе наберите указанный ниже код, нажмите CTR+X для выхода и «Y» для сохранения.

```
<?php

  phpinfo();

?>
```

Перезапуск Apache
Чтобы все изменения применились, необходимо перезапустить web-сервер:
$ sudo systemctl restart apache2
Затем нужно указать в браузере путь до вашего файла PHPinfo. Путь будет выглядеть так:
x.x.x.x/info.php

, где вместо *«x.x.x.x»* укажите IP-адрес вашего сервера.
В результате в браузере вы должны увидеть примерно такую страницу:

2.21. Практическая работа № 21
Установка и настройка apache, php, mysql на web-сервер Arch Linux

Задание:

1: Установка Apache
Apache – это свободное открытое программное обеспечение, обеспечивающее работу 50% веб-серверов в мире.
Перед установкой любой программы LAMP необходимо обновлять менеджер пакетов.
sudo pacman -Syu
Завершив обновление, можно приступать к установке Apache:
sudo pacman -S apache
Установив Apache, нужно внести пару изменений в настройки.
Откройте конфигурационный файл Apache:
sudo nano /etc/httpd/conf/httpd.conf
Раскомментируйте unique_id_module (для быстрого поиска используйте ctrl w):
#LoadModule unique_id_module modules/mod_unique_id.so
Перезапустите Apache:
sudo systemctl restart httpd
При перезапуске Apache может появиться следующее сообщение:
httpd: apr_sockaddr_info_get() failed for droplet1
httpd: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1 for ServerName
[DONE]
Хотя это предупреждение не помешает запуску Apache, его можно легко устранить, внеся в конфигурации имя хоста.
Откройте файл hosts:
sudo nano /etc/hosts
Добавьте имя хоста в конец строки, которая начинается с 127.0.0.1:
127.0.0.1 localhost.localdomain localhost droplet1
В дальнейшем при перезагрузке Apache больше не будет отображать это сообщение.
Веб-сервер Apache установлен! Направьте браузер на IP-адрес сервера (http://11.22.33.444), это откроет каталог авто-индекса. Теперь можно быстро создать пробную страницу, добавив файл index.html в root-каталог Arch, расположенный в srv/http:

```
sudo nano /srv/http/index.html
<html>
<title>Welcome</title>
<body>
<h2>Hello, Welcome to Arch</h2>
</body>
</html>
```

Теперь можно посетить страницу местозаполнителя, перейдя на IP-адрес сервера в браузере.

Как узнать IP-адрес сервера

Запустите следующую команду, чтобы узнать IP-адрес сервера.

```
curl -s icanhazip.com
```

2: Установка MySQL

MySQL – это мощная система управления базами данных (СУБД), которая используется для организации и поиска информации.

Примечание: с марта 2013 года MariaDB стала реализацией MySQL в репозиториях Arch. При установке пакет MySQL автоматически заменяется пакетом MariaDB.

Чтобы установить MySQL, откройте терминал и введите данную команду:

```
sudo pacman -S mysql
```

При появлении каких-либо извещений или вопросов просто нажмите enter (чтобы принять настройки по умолчанию).

По завершении установки запустите MySQL.

```
sudo systemctl start mysqld
```

В завершение нужно запустить настроечный скрипт MySQL.

```
sudo mysql_secure_installation
```

На данном этапе программа спросит текущий root-пароль MySQL (не путать с root-паролем сервера). Поскольку он еще не установлен, просто нажмите клавишу enter.

При запросе «Set root password?» введите Y, а затем наберите новый root-пароль MySQL. После этого проще всего ответить Yes на все появившиеся вопросы. В завершение MySQL перезагрузится и активирует все изменения.

```
By default, a MySQL installation has an anonymous user, allowing anyone
to log into MySQL without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.
Remove anonymous users? [Y/n] y
... Success!
Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.
Disallow root login remotely? [Y/n] y
... Success!
By default, MySQL comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.
Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!
Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.
Reload privilege tables now? [Y/n] y
```

... Success!
Cleaning up...
Готово! После инсталляции MySQL осталось только установить PHP.

3: Установка PHP

PHP – это скриптовый язык с открытым исходным кодом, который широко используется для создания динамических веб-страниц.
Для установки PHP нужно открыть терминал и набрать команду:
sudo pacman -S php php-apache
Кроме того, PHP нужно также внести в настройки apache:
sudo nano /etc/httpd/conf/httpd.conf
Внесите в конфигурационный файл следующий блок кода:
Use for PHP 5.x:
LoadModule php5_module   modules/libphp5.so
AddHandler php5-script php
Include conf/extra/php5_module.conf

4: Тестирование установки LAMP stack

Завершив установку всех компонентов LAMP stack, можно проверить работу ПО и просмотреть данные PHP, создав быструю страницу php info.
Итак, создайте новый файл:
sudo nano /srv/http/info.php
Внесите в него строки:
<?php
phpinfo();
?>
Сохраните и закройте файл.
Затем перезапустите apache, чтобы активировать изменения.
sudo systemctl restart httpd
Посетите страницу php info, введя http://11.22.33.444/info.php (и заменив пример ip-адреса настоящим).
Чтобы закрыть установку LAMP, откройте конфигурационный файл Arch по имени innitscripts и внесите Apache и MySQL в список программ, автоматически запускаемых при старте сервера:
sudo systemctl enable mysqld httpd

2.22. Практическая работа № 22
Установка OpenSSL и создание сертификатов центра сертификации ОС Ubuntu

Задание:

1: Установка Easy-RSA

Для начала нужно установить набор сценариев easy-rsa на ваш сервер ЦС. Пакет easy-rsa – это инструмент управления центрами сертификации, который вы будете использовать для создания закрытого ключа и открытого сертификата; позже они понадобятся для подписи запросов от клиентов и серверов, которые будут обращаться к вашему ЦС.

Войдите на свой сервер ЦС как пользователь sudo (не root) и выполните следующие команды:

```
sudo apt update
sudo apt install easy-rsa
```

Нажмите y, чтобы подтвердить, что вы хотите установить пакет.

Теперь у вас есть все, что вам нужно для настройки Easy-RSA. На следующем этапе мы создадим инфраструктуру открытых ключей, а затем начнем создавать ЦС.

2: Подготовка инфраструктуры открытых ключей

Теперь пора создать инфраструктуру открытых ключей (PKI) на сервере ЦС. Убедитесь, что вы работаете как пользователь sudo, и создайте каталог easy-rsa. Использовать sudo для запуска следующих команд не нужно, поскольку ваш обычный пользователь должен управлять и взаимодействовать с ЦС без повышенных привилегий.

```
mkdir ~/easy-rsa
```

Эта команда создаст в домашнем каталоге новый каталог по имени easy-rsa. Мы будем использовать его для создания символических ссылок (симлинков), указывающих на файлы пакета easy-rsa, которые мы установили на предыдущем этапе. Эти файлы находятся в папке /usr/share/easy-rsa.

Создайте симлинки с помощью команды ln:

```
ln -s /usr/share/easy-rsa/* ~/easy-rsa/
```

Примечание: В других мануалах вы можете прочесть, что вам нужно скопировать файлы easy-rsa в каталог PKI. Но в данном мануале используется метод символических ссылок. Это удобно, потому что в результате любые обновления пакета easy-rsa будут автоматически отражаться в скриптах вашей PKI.

Чтобы ограничить доступ к новому каталогу PKI, убедитесь, что он заблокирован для всех, кроме владельца:

```
chmod 700 /home/8host/easy-rsa
```

Теперь инициализируйте PKI в каталоге easy-rsa:

```
cd ~/easy-rsa
./easyrsa init-pki
init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /home/8host/easy-rsa/pki
```

Теперь у вас есть каталог, содержащий все файлы, необходимые для создания центра сертификации. Далее мы создадим закрытый ключ и открытый сертификат для ЦС.

3: Создание центра сертификации

Прежде чем вы сможете создать закрытый ключ и сертификат ЦС, вам нужно создать файл по имени vars и заполнить его некоторыми значениями по умолчанию. Перейдите в каталог easy-rsa, затем создайте и отредактируете файл vars с помощью nano или другого текстового редактора:

```
cd ~/easy-rsa
nano vars
```

Вставьте следующие строки в файл и отредактируйте все значения, чтобы отразить информацию о вашей организации. Здесь важно убедиться, что вы не оставили пустых значений:

```
~/easy-rsa/vars
set_var EASYRSA_REQ_COUNTRY    "US"
set_var EASYRSA_REQ_PROVINCE   "NewYork"
set_var EASYRSA_REQ_CITY       "New York City"
set_var EASYRSA_REQ_ORG        "MyOrganization"
set_var EASYRSA_REQ_EMAIL      "admin@example.com"
set_var EASYRSA_REQ_OU         "Community"
set_var EASYRSA_ALGO           "ec"
set_var EASYRSA_DIGEST         "sha512"
```

Когда вы закончите, сохраните и закройте файл. В nano для этого нужно нажать Ctrl + X, затем Y и Enter. Теперь вы готовы собрать свой ЦС.

Чтобы создать пару открытого и закрытого ключей для вашего центра сертификации, снова введите команду ./easy-rsa, но на этот раз с параметром build-ca:

```
./easyrsa build-ca
```

В выводе вы увидите несколько строк о версии OpenSSL. Также вам будет предложено ввести парольную фразу для вашей пары ключей. Обязательно выберите надежную фразу и сохраните ее в безопасном месте (или запомните). Эту фразу вам нужно ввести, чтобы получить доступ к своему ЦС (например, для подписи или отзыва сертификата).

Также вам будет предложено подтвердить Common Name (CN) для вашего ЦС. Common Name – это имя, используемое для обозначения этого компьютера в контексте центра сертификации. Вы можете ввести любую строку символов, но проще всего принять имя по умолчанию, нажав Enter.

```
. . .
Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
. . .
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:
CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/home/8host/easy-rsa/pki/ca.crt
```

Примечание: Если вы не хотите, чтобы при каждом взаимодействии с вашим ЦС запрашивался пароль, вы можете запустить команду build-ca с параметром nopass:

```
./easyrsa build-ca nopass
```

Теперь у вас есть два важных файла – ~/easy-rsa/pki/ca.crt и ~/easy-rsa/pki/private/ca.key – открытый и закрытый компонент центра сертификации.

- ca.crt – открытый файл сертификата ЦС. Пользователи, серверы и клиенты будут использовать его для проверки того, что они являются частью одной сети доверия. Каждый пользователь и сервер, который обращается к вашему ЦС, должен иметь копию этого файла. Все стороны будут полагаться на открытый сертификат, чтобы посторонние не могли выдавать себя за вашу систему (это предотвратит атаки посредника).

- ca.key – это закрытый ключ, который ЦС использует для подписи сертификатов серверов и клиентов. Если злоумышленник получит доступ к вашему ЦС и, в свою очередь, к вашему файлу ca.key, вам нужно будет уничтожить ваш ЦС. И поэтому ваш файл ca.key должен находиться только на вашем компьютере ЦС (в идеале компьютер ЦС должен оставаться в оффлайн, если вы не подписываете запросы на сертификат в качестве дополнительной меры безопасности).

После этого ваш центр сертификации будет готов. Его можно использовать для подписи запросов и для отзыва сертификатов.

4: Распространение открытого сертификата ЦС

Теперь ваш ЦС настроен и готов выступать корнем доверия для любых систем, которые вы хотите настроить для его поддержки. Вы можете добавить сертификат ЦС на свои серверы OpenVPN, веб-серверы, почтовые серверы и т. д. Любой пользователь или сервер, которому необходимо проверить подлинность другого пользователя или сервера в вашей сети, должен иметь копию файла ca.crt, импортированного в хранилище сертификатов своей операционной системы.

Чтобы импортировать открытый сертификат ЦС во вторую систему Linux (например, на другой сервер или локальный компьютер), сначала получите копию файла ca.crt с вашего сервера ЦС. Вы можете использовать команду cat, чтобы вывести файл в терминал, а затем скопировать и вставить его в файл на втором компьютере (на который нужно импортировать сертификат). Также для передачи файла между системами вы можете использовать такие инструменты, как scp, rsync. Мы скопируем и вставим сертификат с помощью nano, поскольку это будет работать во всех системах.

Выполните следующую команду на сервере ЦС:

```
cat ~/easy-rsa/pki/ca.crt
```

В терминале появится такой вывод:

```
-----BEGIN CERTIFICATE-----
MIIDSzCCAjOgAwIBAgIUcR9Crsv3FBEujrPZnZnU4nSb5TMwDQYJKoZIhvcNAQEL
BQAwFjEUMBIGA1UEAwwLRWFzeS1SU0EgQ0EwHhcNMjAwMzE4MDMxNjI2WhcNMzAw
. . .
. . .
-----END CERTIFICATE-----
```

Скопируйте все, включая строки ——BEGIN CERTIFICATE—— и ——END CERTIFICATE——.

На второй машине откройте файл /tmp/ca.crt:

```
nano /tmp/ca.crt
```

Вставьте код, который вы только что скопировали с сервера ЦС, в редактор. Когда вы закончите, сохраните и закройте файл.

Теперь, когда у вас есть копия файла ca.crt во второй системе Linux, пора импортировать сертификат в хранилище сертификатов данной операционной системы.

В системах на основе Debian и Ubuntu для импорта сертификата выполните следующие команды:

```
cp /tmp/ca.crt /usr/local/share/ca-certificates/
update-ca-certificates
```

Чтобы импортировать сертификат в системы на основе CentOS, Fedora или RedHat, скопируйте сертификат в /etc/pki/ca-trust/source/anchors/ и запустите команду update-ca-trust.

```
sudo cp /tmp/ca.crt /etc/pki/ca-trust/source/anchors/
update-ca-trust
```

Теперь вторая ваша система Linux будет доверять сертификатам, подписанным вашим ЦС.

Примечание: Если вы используете свой ЦС для веб-серверов и работаете с браузером Firefox, вам необходимо импортировать публичный сертификат ca.crt прямо в Firefox. Браузер Firefox не использует хранилище сертификатов локальной операционной системы. Подробную информацию о том, как добавить сертификат ЦС в Firefox, вы найдете в этой статье от Mozilla.

Если вы используете свой ЦС для интеграции со средой Windows или настольными компьютерами, ознакомьтесь с документацией по использованию certutil.exe.

Если вы знаете, как подписывать и отзывать сертификаты, вы уже можете закончить работу с мануалом. Если же вы хотите научиться подписывать и отзывать сертификаты, далее мы подробно опишем каждый процесс.

Опционально: Создание запросов на подпись и отзыв сертификатов

Следующие разделы данного мануала выполнять не обязательно. Если вы выполнили все предыдущие разделы, у вас уже есть полностью готовый центр сертификации, который можно использовать (например, в качестве основы для выполнения других мануалов). Вы можете импортировать файл ca.crt вашего ЦС и проверить сертификаты, которые были им подписаны.

Если вы хотите попрактиковаться или узнать больше о том, как подписывать запросы и как отзывать сертификаты, следуйте этим дополнительным разделам.

Создание и подпись запроса на сертификат

Теперь, когда у вас есть готовый центр сертификации, вы можете попрактиковаться в создании секретного ключа и запроса сертификата, чтобы ознакомиться с процессами подписания и распространения.

Запрос на подпись сертификата (CSR) состоит из трех частей: это открытый ключ, определение данных о запрашивающей системе и подпись запроса (создается с помощью закрытого ключа запрашивающей стороны). Закрытый ключ следует хранить в секрете, поскольку он будет использоваться для шифрования информации, расшифровать которую сможет только пользователь с подписанным открытым сертификатом.

Следующие действия нужно выполнять на вашей второй системе (Linux Debian, Ubuntu или дистрибутиве, который является производным от любой из этих систем). Это может

быть другой удаленный сервер или локальная машина Linux – например, ноутбук или компьютер. Поскольку команда easy-rsa не доступна по умолчанию во всех системах, мы используем инструмент openssl для создания личного ключа и сертификата.

Пакет openssl по умолчанию предустановлен в большинстве дистрибутивов Linux, но если вы не уверены в этом, запустите такую команду:

```
sudo apt update
sudo apt install openssl
```

По запросу введите y, чтобы продолжить установку. Теперь вы готовы создать тестовый запрос с помощью openssl.

Первое, что необходимо сделать для создания CSR, – это создать закрытый ключ с помощью openssl. Давайте создадим каталог practice-csr, а затем сгенерируем в нем ключ. Мы создадим этот запрос для условного сервера 8host-server (не для идентификации пользователя или другого ЦС).

```
mkdir ~/practice-csr
cd ~/practice-csr
openssl genrsa -out 8host-server.key
Generating RSA private key, 2048 bit long modulus (2 primes)
. . .
. . .
e is 65537 (0x010001)
```

Теперь, когда у вас есть закрытый ключ, вы можете создать соответствующий запрос с помощью утилиты openssl. Вам будет предложено заполнить несколько полей. Вы можете ввести точку (.), если хотите оставить поле пустым, но учтите, что в настоящих запросах на сертификаты так лучше не делать, в них следует использовать действительные данные о вашем местоположении и организации.

```
openssl req -new -key 8host-server.key -out 8host-server.req
. . .
-----
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:New York
Locality Name (eg, city) [Default City]:New York City
Organization Name (eg, company) [Default Company Ltd]:MyOrganization
Organizational Unit Name (eg, section) []:Community
Common Name (eg, your name or your server's hostname) []:8host-server
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Если вы хотите автоматически добавить эти значения прямо в вызов команды openssl (чтобы не вводить их через интерактивные окна), передайте аргумент -subj. Обязательно отредактируйте условные значения, указав вместо них свои.

```
openssl req -new -key 8host-server.key -out server.req -subj \
/C=US/ST=New\ York/L=New\ York\ City/O=MyOrganization/OU=Community/CN=8host-
server
```

Чтобы проверить содержимое вашего запроса, вы можете просмотреть файл запроса:

```
openssl req -in 8host-server.req -noout -subject
subject=C = US, ST = New York, L = New York City, O = MyOrganization, OU =
Community, CN = 8host-server
```

Если вы довольны вашим тестовым запросом на сертификат, скопируйте файл 8host-server.req на свой сервер ЦС, используя утилиту scp:

```
scp 8host-server.req 8host@your_ca_server_ip:/tmp/8host-server.req
```

Вы создали запрос на подпись сертификата для условного сервера 8host-server. В реальном сценарии запрос может быть предназначен для промежуточного веб-сервера или сервера разработки, который нуждается в TLS сертификате для целей тестирования. Также запрос может исходить от сервера OpenVPN, которому нужен сертификат, чтобы пользователи могли подключаться к VPN. Далее мы перейдем к подписанию запроса с помощью закрытого ключа сервера ЦС.

Подпись запроса на сертификат

На предыдущем этапе вы создали пробный запрос сертификата и ключ. Вы скопировали его в каталог /tmp на своем сервере ЦС (такой же процесс вы бы использовали, если бы у вас были реальные клиенты или серверы, отправляющие вам CSR-запросы, которые необходимо подписать).

Далее сервер ЦС должен импортировать тестовый сертификат и подписать его. Как только запрос сертификата будет подтвержден ЦС и передан обратно на сервер, клиенты, которые доверяют данному ЦС, также будут доверять только что выданному сертификату.

Поскольку на сервере ЦС доступна утилита easy-rsa, она будет использоваться на этапах подписания, чтобы упростить задачу (и не использовать openssl, как мы это делали в предыдущем разделе).

Первым делом для подписания запроса сертификата нужно импортировать этот запрос с помощью скрипта easy-rsa:

```
cd ~/easy-rsa
./easyrsa import-req /tmp/8host-server.req 8host-server
. . .
The request has been successfully imported with a short name of: 8host-
server
You may now use this name to perform signing operations on this request.
```

Теперь вы можете подписать запрос, запустив скрипт easyrsa с параметром sign-req, за которым указывается тип запроса и значение Common Name, включенное в запрос. Запрос может использовать один из следующих типов: client, server или ca. Поскольку наш тестовый сертификат предназначен для вымышленного сервера, используйте тип server.

```
./easyrsa sign-req server 8host-server
```

В выводе вам будет предложено подтвердить, что запрос поступил из надежного источника. Введите yes, затем нажмите Enter:

```
You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this re-
quest
```

```
has not been cryptographically verified. Please be sure it came from a
trusted
source or that you have verified the request checksum with the sender.
Request subject, to be signed as a server certificate for 3650 days:
subject=
commonName                = 8host-server
Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
. . .
Certificate created at: /home/8host/easy-rsa/pki/issued/8host-server.crt
```

Если вы зашифровали ключ ЦС, сейчас вам будет предложено ввести пароль.

Итак, вы подписали запрос сертификата 8host-server.req, используя закрытый ключ сервера ЦС из файла /home/8host/easy-rsa/pki/private/ca.key. Полученный файл 8host-server.crt содержит открытый ключ шифрования для нашего условного сервера, а также новую подпись от сервера ЦС. Смысл подписи заключается в том, чтобы сообщить всем, кто доверяет данному ЦС, что они также могут доверять сертификату сервера 8host-server.

Если бы этот запрос относился к реальному серверу (например, к веб- или VPN-серверу), сервер ЦС должен был бы передать новые файлы 8host-server.crt и ca.crt на удаленный сервер, который сделал запрос сертификата:

```
scp pki/issued/8host-server.crt 8host@your_server_ip:/tmp
scp pki/ca.crt 8host@your_server_ip:/tmp
```

После этого выданный сертификат можно использовать с веб-серверами, VPN, инструментами управления конфигурацией, системами баз данных или для аутентификации клиента.

Отзыв сертификата

У вас может возникнуть потребность отозвать подписанный сертификат, чтобы пользователь или сервер больше не могли его использовать: например, если ноутбук, для которого вы подписали сертификат, был украден, веб-сервер с вашим сертификатом взломали, сотрудник покинул вашу организацию и так далее.

Общий процесс отзыва сертификата состоит из таких этапов:

1. Отзыв сертификата с помощью команды ./easyrsa revoke client_name.
2. Создание нового запроса на сертификат с помощью команды ./easyrsa gen-crl.
3. Перенос обновленного файла crl.pem на сервер или серверы, которые зависят от вашего ЦС; копирование файла в требуемый каталог или каталоги в этих системах для программ, которые к нему обращаются.
4. Перезапуск всех сервисов, которые используют ваш ЦС и файл запроса.

Вы можете использовать этот процесс для отзыва любых ранее выданных сертификатов. Ниже мы подробно рассмотрим каждый шаг, начиная с команды revoke.

Чтобы отозвать сертификат, перейдите в каталог easy-rsa на вашем сервере ЦС:

```
cd ~/easy-rsa
```

Затем запустите скрипт easyrsa с опцией revoke, после нее укажите имя клиента, сертификат которого вы хотите отозвать. Следуя нашему примеру, Common Name сертификата – это 8host-server:

```
./easyrsa revoke 8host-server
```

Команда попросит вас подтвердить отзыв, введя yes:

```
Please confirm you wish to revoke the certificate with the following sub-
ject:
subject=
commonName                = 8host-server
Type the word 'yes' to continue, or any other input to abort.
Continue with revocation: yes
. . .
Revoking Certificate 8348B3F146A765581946040D5C4D590A
. . .
```

Обратите внимание на значение в строке Revoking Certificate. Оно представляет собой уникальный серийный номер отзываемого сертификата. Если вы хотите проверить список отозванных сертификатов (об этом чуть ниже), чтобы убедиться, что в нем есть этот сертификат, вам понадобится это значение.

После подтверждения действия ЦС отзовет сертификат. Однако удаленные системы, которые используют ваш ЦС, не могут проверить, были ли отозваны какие-либо сертификаты. Пользователи и серверы по-прежнему смогут использовать отозванный сертификат до тех пор, пока список отзыва сертификатов ЦС (Certificate Revocation List, CRL) не будет распространен на все системы, использующие ваш ЦС.

Давайте создадим CRL или обновим существующий файл crl.pem.

Обновив список отзыва, вы сможете указать, какие пользователи и системы имеют действительные сертификаты в вашем ЦС.

Чтобы создать CRL, запустите команду easy-rsa с параметром gen-crl, находясь в каталоге ~/easy-rsa:

```
./easyrsa gen-crl
```

Если при создании файла ca.key вы использовали парольную фразу, вам будет предложено ввести ее. Команда gen-crl создаст файл crl.pem, содержащий обновленный список отозванных сертификатов для этого ЦС.

Затем вам нужно будет передать обновленный файл crl.pem на все серверы и клиенты, которые используют ваш ЦС. В противном случае клиенты и системы будут по-прежнему иметь доступ к сервисам и системам, которые используют ваш ЦС, поскольку они не будут знать об аннулированном статусе сертификата.

Чтобы передать файл на серверы, которые доверяют вашему ЦС, вы можете использовать команду scp.

Примечание: В этом мануале показано, как создавать и распространять CRL вручную. Но существуют и более надежные, автоматизированные методы для распространения и проверки списков отзыва, например OCSP-Stapling.

Убедитесь, что вы вошли на сервер ЦС как пользователь sudo, и запустите следующую команду, указав свой IP-адрес или DNS-имя своего сервера вместо your_server_ip:

```
scp ~/easy-rsa/pki/crl.pem 8host@your_server_ip:/tmp
```

Теперь, когда файл находится в удаленной системе, нам остается только обновить все сервисы, чтобы предоставить им новую копию списка отзыва. Мы не будем подробно останавливаться на этом этапе. В общих чертах: вам нужно скопировать файл crl.pem в то место, где сервис будет его искать, а затем перезапустить сервис с помощью systemctl.

Как только сервисы получат новый файл crl.pem, они смогут отклонять соединения от клиентов или серверов, которые используют отозванный сертификат.

Если вы хотите проверить файл CRL (например, чтобы просмотреть список отозванных сертификатов), используйте следующую команду openssl в каталоге easy-rsa на вашем сервере ЦС:

```
cd ~/easy-rsa
openssl crl -in pki/crl.pem -noout -text
```

Вы также можете запустить эту команду на любом сервере или системе, где установлен инструмент openssl с копией файла crl.pem. Например, если вы перенесли файл crl.pem в вашу вторую систему и хотите убедиться, что сертификат 8host-server отозван, вы можете использовать команду openssl, как показано ниже (но укажите свой серийный номер отзыва сертификата):

```
openssl crl -in /tmp/crl.pem -noout -text |grep -A 1
8348B3F146A765581946040D5C4D590A
Serial Number: 8348B3F146A765581946040D5C4D590A
Revocation Date: Apr  1 20:48:02 2020 GMT
```

Обратите внимание: команда grep используется для проверки уникального серийного номера, который вы получили при отзыве. Теперь вы можете проверить свой список отозванных сертификатов в любой системе, которая использует его для ограничения доступа пользователей и сервисов.

2.23. Практическая работа № 23
Установка OpenSSL и со-здание сертификатов центра сертификации ОС Arch Linux

Задание:

1: Откройте конфигурационный каталог Apache

Для начала нужно перейти в главный каталог конфигураций Apache. Все последующие действия следует выполнять в этом каталоге.

```
cd /etc/httpd/conf
```

2: Создайте самоподписанный SSL-сертификат

Создайте 1024-битный закрытый ключ RSA. Опция -des3 указывает на необходимость парольной фразы. Парольная фраза обеспечивает более высокий уровень безопасности,

однако при перезапуске Apache она может стать причиной некоторых проблем. В случае сбоя или перезапуска Apache ее придется постоянно повторно вводить.

```
sudo openssl genrsa -des3 -out server.key 1024
```

Теперь нужно создать запрос на подпись сертификата (англ. certificate-signing request, или CSR). Если в предыдущем шаге была создана парольная фраза, на данном этапе она будет запрошена.

```
sudo openssl req -new -key server.key -out server.csr
```

Эта команда выведет на экран форму, которую нужно заполнить. Самое важное поле в ней – Common Name; внесите в него официальный домен или IP-адрес сервера.

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:New York
Locality Name (eg, city) []:NYC
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Awesome Inc
Organizational Unit Name (eg, section) []:Dept of Merriment
Common Name (e.g. server FQDN or YOUR name) []:example.com
Email Address []:webmaster@awesomeinc.com
```

Удалите фразовый пароль:

```
sudo cp server.key server.key.org
sudo openssl rsa -in server.key.org -out server.key
```

Теперь нужно задать срок действия сертификата; для этого измените значение опции –days, которая указывает количество дней, в течение которых сертификат будет действителен. Например, нижеприведенная команда задает срок действия в 1 год.

```
sudo openssl x509 -req -days 365 -in server.csr -signkey server.key -out
server.crt
```

3: Завершающие действия

Готово! Теперь сертификат создан и подписан. Осталось только включить его в настройки Apache. Откройте главный конфигурационный файл Apache:

```
sudo nano /etc/httpd/conf/httpd.conf
```

В нем раскомментируйте строку:

```
Include conf/extra/httpd-ssl.conf
```

Перезапустите Apache, чтобы изменения вступили в с

2.24. Практическая работа № 24
Установка CMS wordpress на web-сервер

Задание:

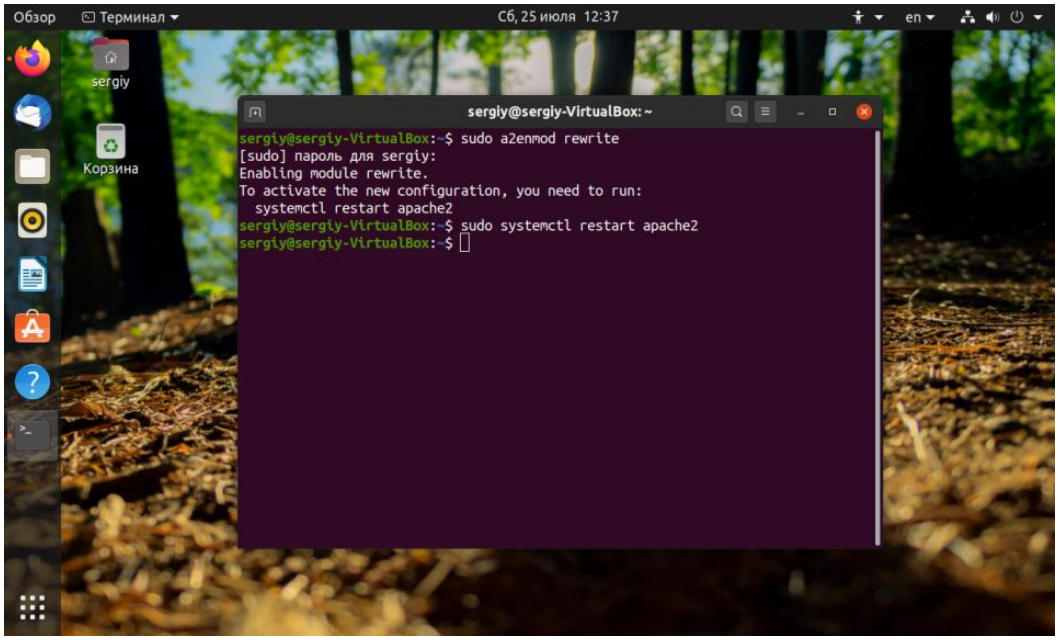
1.

Для корректной работы WordPress нужно, чтобы был активирован модуль Apache mod_rewrite. Для его включения выполните:

```
sudo a2enmod mod_rewrite
```

Затем перезагрузите веб-сервер:

```
sudo systemctl restart apache2
```



Установка WordPress в Ubutnu

Теперь все готово и мы можем перейти непосредственно к теме статьи. Сначала загрузите последнюю версию системы управления контентом из официального сайта:

```
wget -c http://wordpress.org/latest.tar.gz
```

Распакуйте содержимое архива в текущую папку:

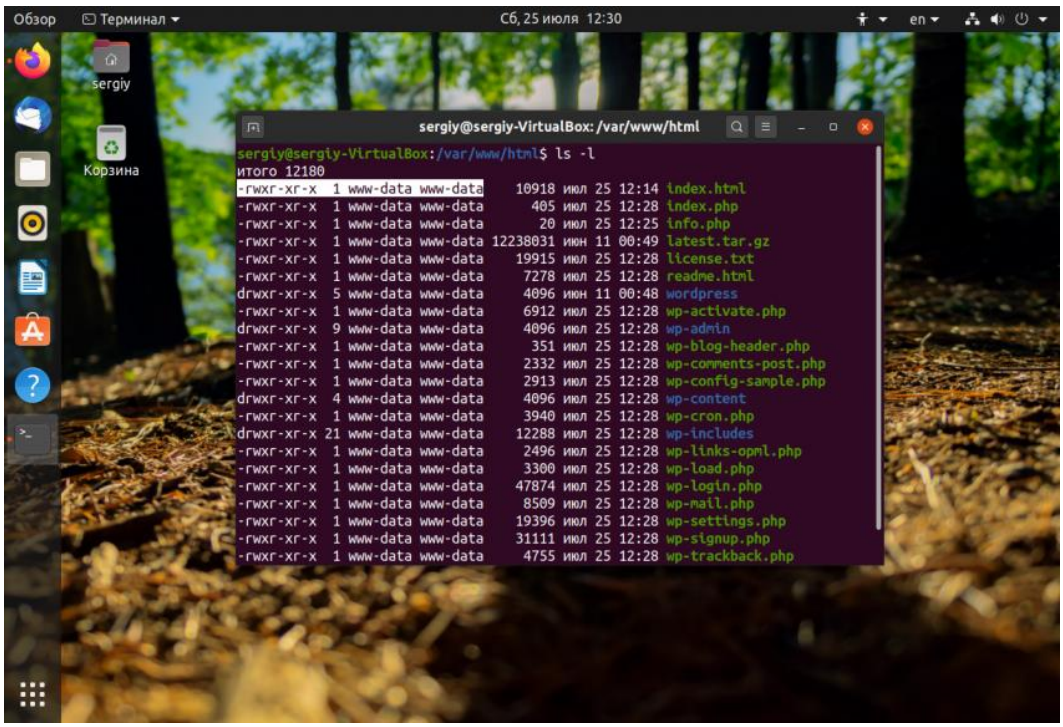
```
tar -xzvf latest.tar.gz
```

Скопируйте файлы WordPress из текущей папки в папку /var/www/html/:

```
sudo rsync -av wordpress/* /var/www/html/
```

Для того чтобы веб-сервер мог правильно работать с этими файлами нужно установить для них правильные права, а именно пользователь и группа www-data:

```
sudo chown -R www-data:www-data /var/www/html/
sudo chmod -R 755 /var/www/html/
```



Фактически установка WordPress на Ubuntu 20.04 завершена, но осталось еще настроить соединение с базой данных. Чтобы по умолчанию открывался WordPress файл index.html можно удалить:

```
sudo rm /var/www/html/index.html
```

Создание базы данных

Чтобы создать базу данных сначала войдите в интерфейс управления mysql, для этого выполните:

```
sudo mysql -u root -p
```

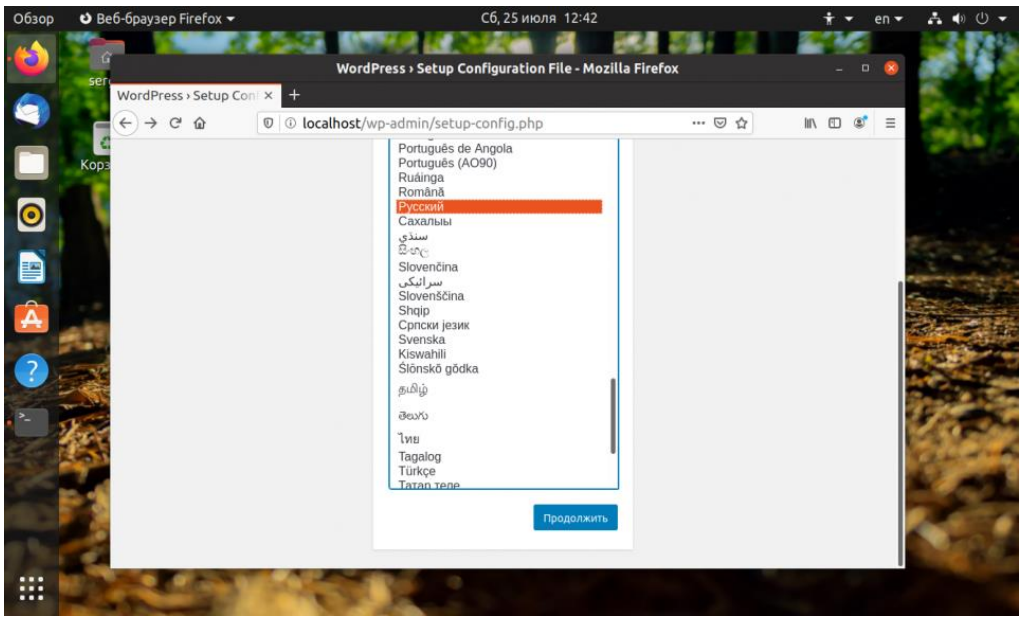
Введите пароль суперпользователя, а затем по очереди выполняйте такие команды для создания базы данных, пользователя и установки для них правильных привилегий:

```
mysql> CREATE DATABASE wp_database;
mysql> CREATE USER 'wp_user'@'localhost' IDENTIFIED BY 'password';
mysql> GRANT ALL PRIVILEGES ON wp_database.* TO 'wp_user'@'localhost';
mysql> FLUSH PRIVILEGES;
mysql> EXIT;
```

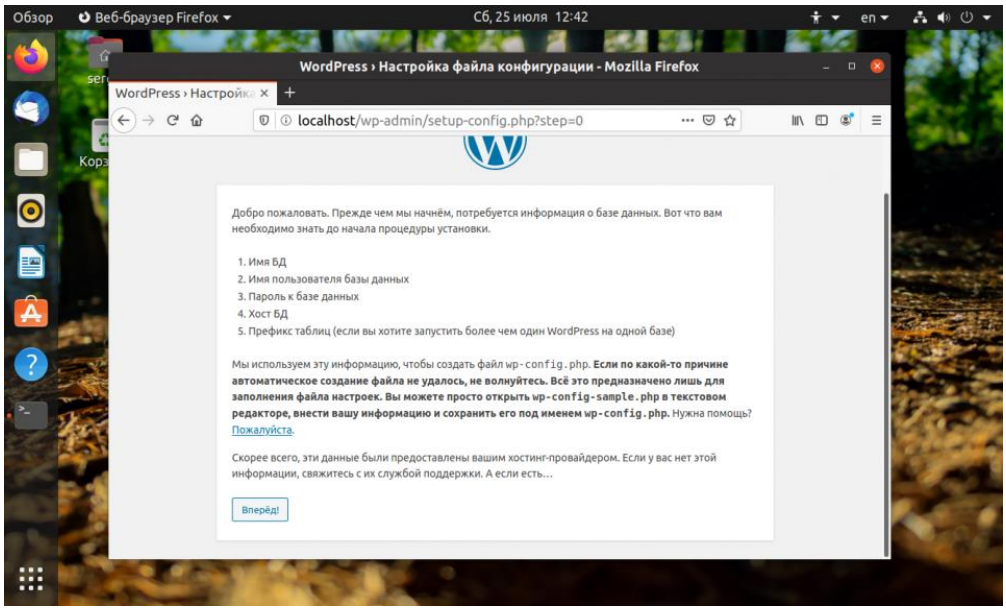
Замените wp_database на желаемое имя базы данных, wp_user - имя пользователя, а password на нужный пароль. Модификатор localhost означает, что к этой базе смогут подключиться только с локальной машины.

Настройка WordPress в Ubuntu

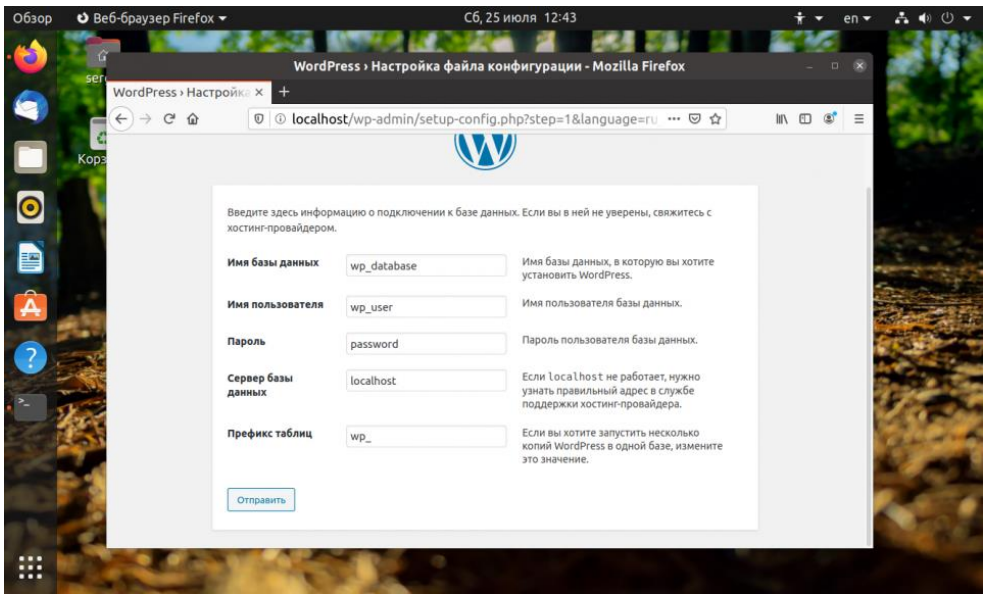
Всё готово для настройки WordPress. Откройте адрес сервера, на котором устанавливали WordPress или localhost, если программа была установлена на локальном компьютере. В первом окне программа предложит вам выбрать язык:



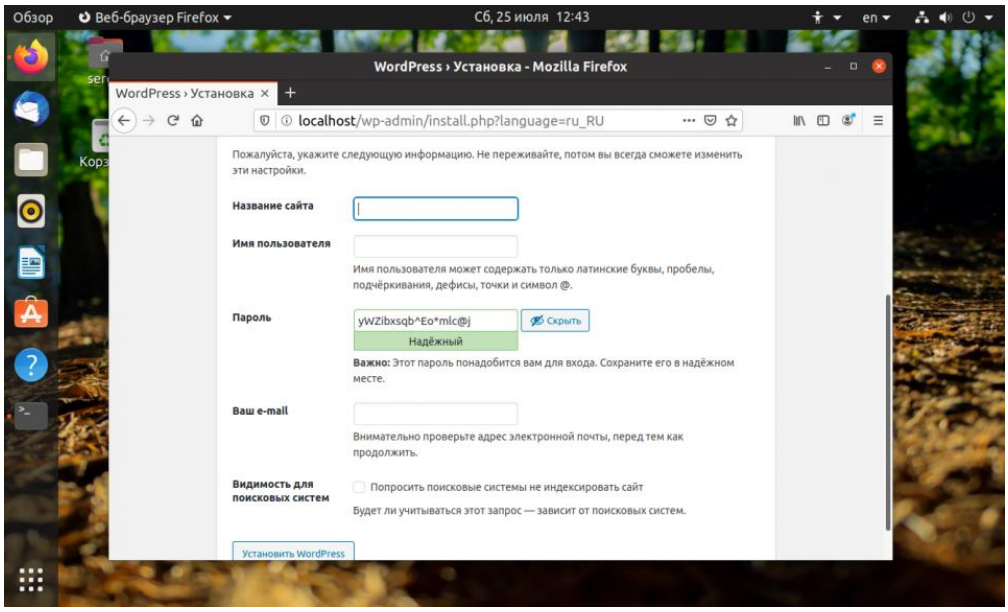
На следующем шаге нажимайте **Вперед**:



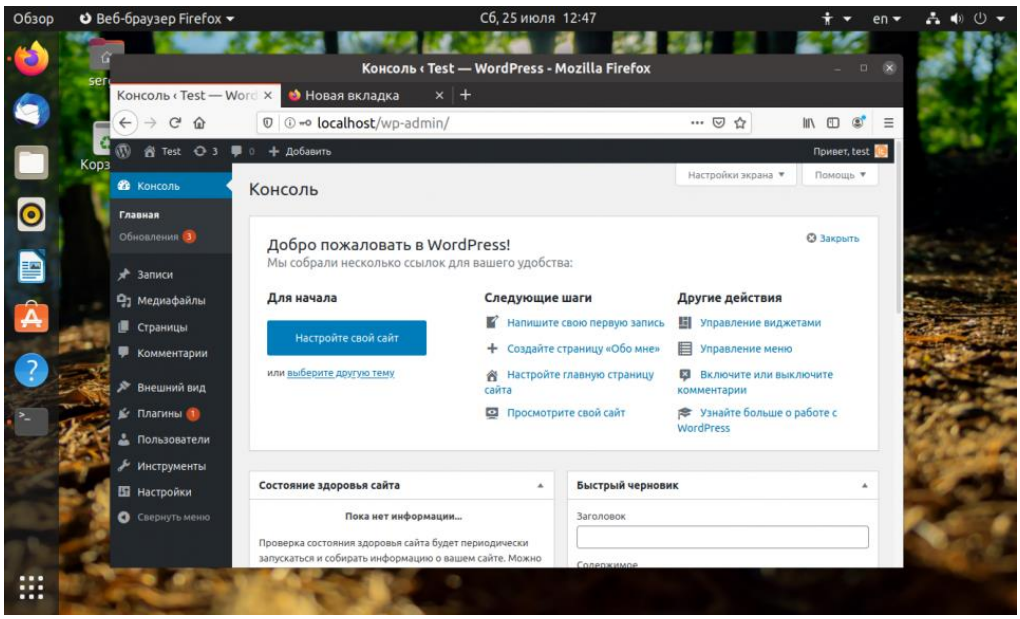
Далее введите имя базы данных, имя пользователя и пароль, которые использовали при создании базы.



Осталось выбрать название сайта, логин администратора, а также ввести пароль администратора. Можно оставить пароль, который предлагает система.



Затем останется только авторизоваться и можно пользоваться только что настроенной системой управления контентом.



2.

Убедитесь, что на сервере установлена утилита wget:

```
sudo pacman -S wget
```

Загрузить WordPress можно с сайта проекта:

```
wget http://wordpress.org/latest.tar.gz
```

Эта команда загрузит сжатый пакет WordPress в домашний каталог пользователя. Чтобы распаковать полученный файл, используйте:

```
tar -xzvf latest.tar.gz
```

2: Создание базы данных и пользователя WordPress

Распакованные файлы WordPress будут помещены в подкаталог wordpress домашнего каталога.

Теперь нужно создать БД и пользователя для WordPress.

Откройте оболочку MySQL:

```
mysql -u root -p
```

Введите root-пароль MySQL, а затем создайте БД, пользователя для БД и пароль для этого пользователя.

Примечание: Все команды MySQL должны оканчиваться символом точки с запятой.

Сначала создайте БД (в данном руководстве для простоты назовём её wordpress):

```
CREATE DATABASE wordpress;
Query OK, 1 row affected (0.00 sec)
```

Затем создайте нового пользователя. Замените условные имя пользователя, БД и пароль своими данными:

```
CREATE USER wordpressuser@localhost;
Query OK, 0 rows affected (0.00 sec)
```

Чтобы создать пароль, введите:

```
SET PASSWORD FOR wordpressuser@localhost= PASSWORD("password");
Query OK, 0 rows affected (0.00 sec)
```

В завершение передайте все права на БД новому пользователю. Без этого инсталлятор WordPress не сможет начать свою работу.

```
GRANT ALL PRIVILEGES ON wordpress.* TO wordpressuser@localhost IDENTIFIED BY
'password';
Query OK, 0 rows affected (0.00 sec)
```

Обновите MySQL:

```
FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
```

Закройте оболочку MySQL:

```
exit
```

3: Настройка WordPress

Скопируйте образец конфигурационного файла WordPress, который находится в каталоге wordpress, в новый файл для создания пользовательских настроек:

```
cp ~/wordpress/wp-config-sample.php ~/wordpress/wp-config.php
```

Откройте конфигурационный файл:

```
sudo nano ~/wordpress/wp-config.php
```

Найдите в нем следующий раздел и укажите в нем имя БД, пользователя и пароль:

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');
/** MySQL database username */
define('DB_USER', 'wordpressuser');
/** MySQL database password */
define('DB_PASSWORD', 'password');
```

Затем сохраните и закройте файл.

4: Копирование файлов

Загрузка WordPress на сервер почти завершена. Осталось только переместить распакованные файлы WordPress в root-каталог сайта.

```
sudo cp -r ~/wordpress/* /srv/http/
```

Убедитесь, что PHP может подключаться к MySQL. Откройте файл php.ini:

```
sudo nano /etc/php/php.ini
```

Найдите следующую строку и раскомментируйте её, удалив символ точки с запятой:

```
;extension=mysql.so
```

Теперь строка должна выглядеть так:

```
extension=mysql.so
```

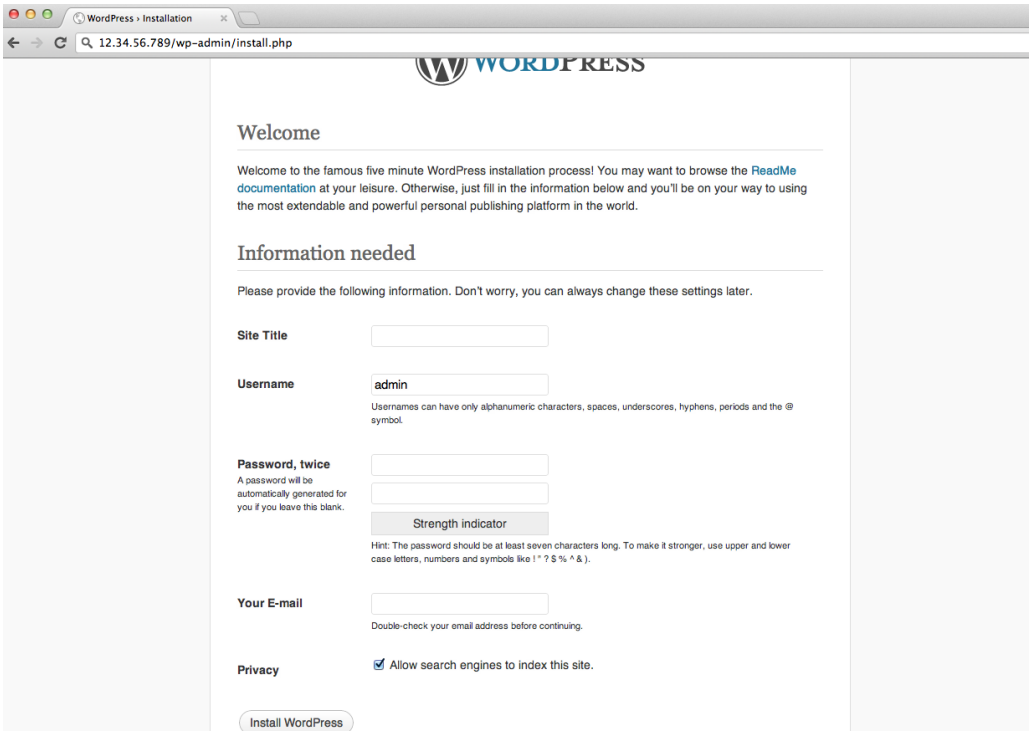
Перезапустите Apache:

```
sudo systemctl restart httpd
```

Теперь в браузере доступна простая онлайн-установка WordPress.

5: Онлайн-установка WordPress

Итак, теперь откройте страницу установки WordPress. Для этого перейдите на домен_или_IP_сервера/wp-admin/install.php (например, example.com/wp-admin/install.php) и заполните короткую форму, которая имеет такой вид:



2.25. Практическая работа № 25
Создание web-ресурса на wordpress. Обеспечение доступа по HTTPS

Задание:
Настройка Apache на сервере Ubuntu и Arch Linux

Для начала необходимо активировать `mod_ssl`:

```
sudo a2enmod ssl
```

А затем включить настройки HTTPS сайта по умолчанию:

```
sudo a2ensite default-ssl
```

Теперь необходимо отредактировать файл с настройками HTTPS сайта по умолчанию, указав в нём пути к вашим сертификатам. Сам файл называется `/etc/apache2/sites-enabled/default-ssl` (или `/etc/apache2/sites-enabled/default-ssl.conf`).

В этом файле рекомендуется после директивы

```
SSLEngine on
```

добавить строчку

```
SSLProtocol all -SSLv2
```

дабы запретить использование устаревшего протокола SSLv2.

Дальше вам необходимо отредактировать параметры, ответственные за сертификаты.

```
# Публичный сертификат сервера
SSLCertificateFile    /etc/ssl/certs/server.pem
# Приватный ключ сервера
SSLCertificateKeyFile /etc/ssl/private/server.key
```

Теперь просто перезагрузите Apache:

```
sudo service apache2 restart
```

И если все параметры указаны верно, ваши сайты станут доступны по HTTPS.

Протокол HTTPS работает по 443 порту, поэтому если сервер находится за шлюзом, то необходимо на нём пробросить данный порт.

Перенаправление HTTP запросов на HTTPS

Если вы хотите запретить использование HTTP, то самым разумным будет перенаправлять все HTTP запросы к страницам на их HTTPS адрес. Сделаем это с помощью `mod_alias`. Если он не включён — включаем:

```
sudo a2enmod alias
sudo service apache2 restart
```

Затем изменяем файл `/etc/apache2/sites-enabled/000-default`, отвечающий за виртуальный хост по умолчанию для HTTP запросов. В этот файл добавляем директиву

```
Redirect / https://example.com/
```

При этом все настройки директорий можно удалить, поскольку по HTTP на ваши сайты всё равно будет не попасть.

Всё, теперь ещё раз перезапустите Apache и убедитесь, что при заходе по HTTP вы автоматически перенаправляетесь на HTTPS страницу.

2.26. Практическая работа № 26
Установка CMS joomla на web-сервер

Задание:

1. **Ubuntu**

Создание базы данных MySQL

Joomla может хранить свои данные, такие как статьи, категории, пользователи, расширения и настройки тем, в базе данных MySQL, PostgreSQL или MS SQL.

Мы будем использовать MySQL как внутреннюю базу данных. Если на вашем сервере Ubuntu не установлен MySQL, вы можете установить его, набрав:

```
sudo apt-get updatesudo apt-get install mysql-server
```

Войдите в консоль MySQL, набрав:

```
sudo mysql
```

Из оболочки MySQL запустите следующий оператор SQL, чтобы создать базу данных :

```
CREATE DATABASE joomla CHARACTER SET utf8mb4 COLLATE utf8mb4_general_ci;
```

Затем создайте нового пользователя MySQL и предоставьте ему привилегии в новой базе данных:

```
GRANT ALL ON joomla.* TO 'joomlauser'@'localhost' IDENTIFIED BY 'change-
with-strong-password';
```

После этого выйдите из консоли mysql, набрав:

```
EXIT
```

Скачивание Joomla

На момент написания этой статьи последней версией Joomla была версия 3.9.4.

Перед загрузкой архива Joomla сначала создайте каталог, в котором будут храниться файлы Joomla, и перейдите к нему:

```
sudo mkdir -p /var/www/example.comcd /var/www/example.com
```

Затем загрузите текущую версию Joomla со страницы загрузок Joomla, используя следующую команду wget :

```
sudo wget https://downloads.joomla.org/cms/joomla3/3-9-4/Joomla_3-9-4-
Stable-Full_Package.zip
```

После завершения загрузки распакуйте архив и переместите файлы в корневой каталог документов домена:

```
sudo unzip Joomla_3-9-4-Stable-Full_Package.zip
```

Измените владельца каталога на `www-data` с помощью команды chown, чтобы веб-сервер имел полный доступ к файлам и каталогам сайта:

```
sudo chown -R www-data: /var/www/example.com
```

Настройка Apache

К настоящему времени у вас уже должен быть установлен Apache с сертификатом SSL в вашей системе, если нет, проверьте предварительные требования для этого руководства.

Следующим шагом является редактирование конфигурации виртуальных хостов Apache:

```
sudo nano /etc/apache2/sites-available/example.com.conf
```

Следующая конфигурация Apache [перенаправляет HTTP на HTTPS] и www на версию вашего домена без www и включает HTTP2. Не забудьте заменить `example.com` своим доменом Joomla и указать правильный путь к файлам сертификатов SSL.

/etc/apache2/sites-available/example.com.conf

```
<VirtualHost *:80>
  ServerName example.com
  ServerAlias www.example.com

  Redirect permanent / https://example.com/
</VirtualHost>

<VirtualHost *:443>
  ServerName example.com
  ServerAlias www.example.com

  Protocols h2 http/1.1

  <If "%{HTTP_HOST} == 'www.example.com'">
    Redirect permanent / https://example.com/
  </If>

  DirectoryIndex index.html index.php
  DocumentRoot /var/www/example.com

  ErrorLog ${APACHE_LOG_DIR}/example.com-error.log
  CustomLog ${APACHE_LOG_DIR}/example.com-access.log combined

  SSLEngine On
  SSLCertificateFile /etc/letsencrypt/live/example.com/cert.pem
  SSLCertificateKeyFile /etc/letsencrypt/live/example.com/privkey.pem
  SSLCertificateChainFile /etc/letsencrypt/live/example.com/chain.pem

  <Directory /var/www/example.com>
      Options FollowSymLinks
      AllowOverride All
      Require all granted
  </Directory>

</VirtualHost>
```

Если не включен, включите виртуальный хост для домена. Эта команда создаст символическую ссылку с `sites-available` на каталог `sites-enabled` :

```
sudo a2ensite example.com
```

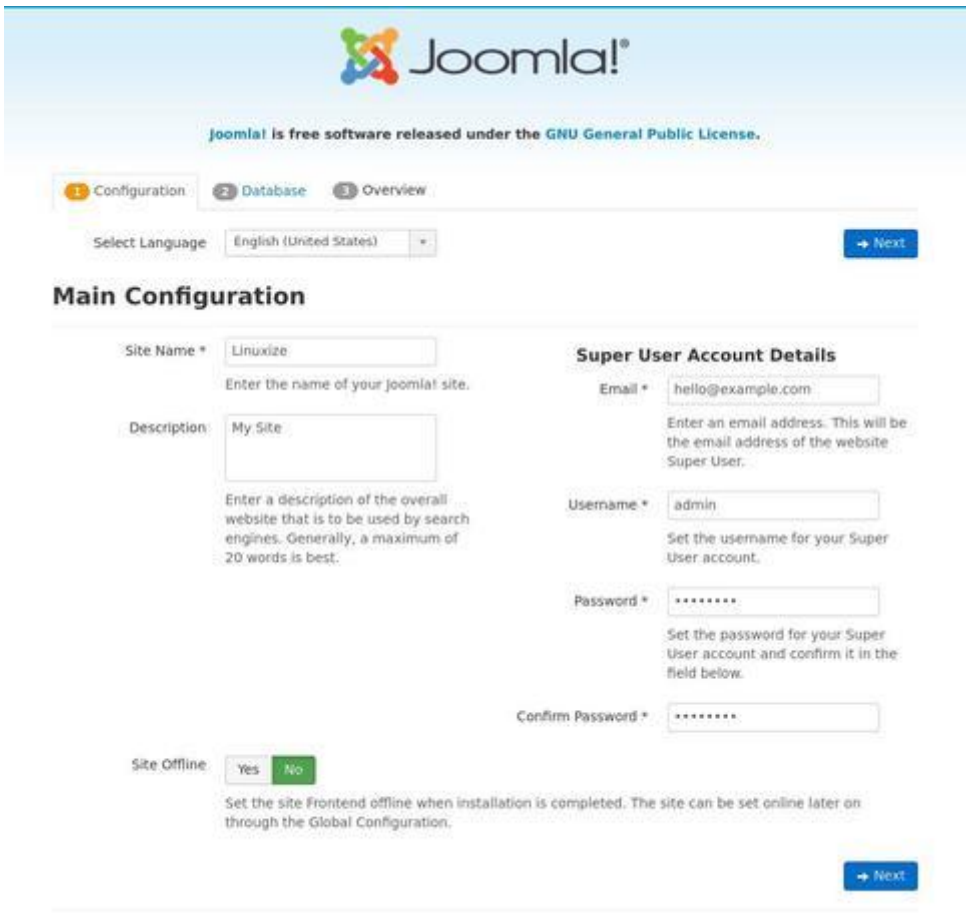
Чтобы новая конфигурация вступила в силу, перезапустите службу Apache, набрав:

```
sudo systemctl restart apache2
```

Завершение установки Joomla

Теперь, когда Joomla загружена и настройка сервера завершена, пора завершить установку Joomla с помощью веб-интерфейса.

Откройте браузер, введите свой домен, и появится экран, подобный следующему:



Выберите язык, который вы хотите использовать, и введите следующую информацию:

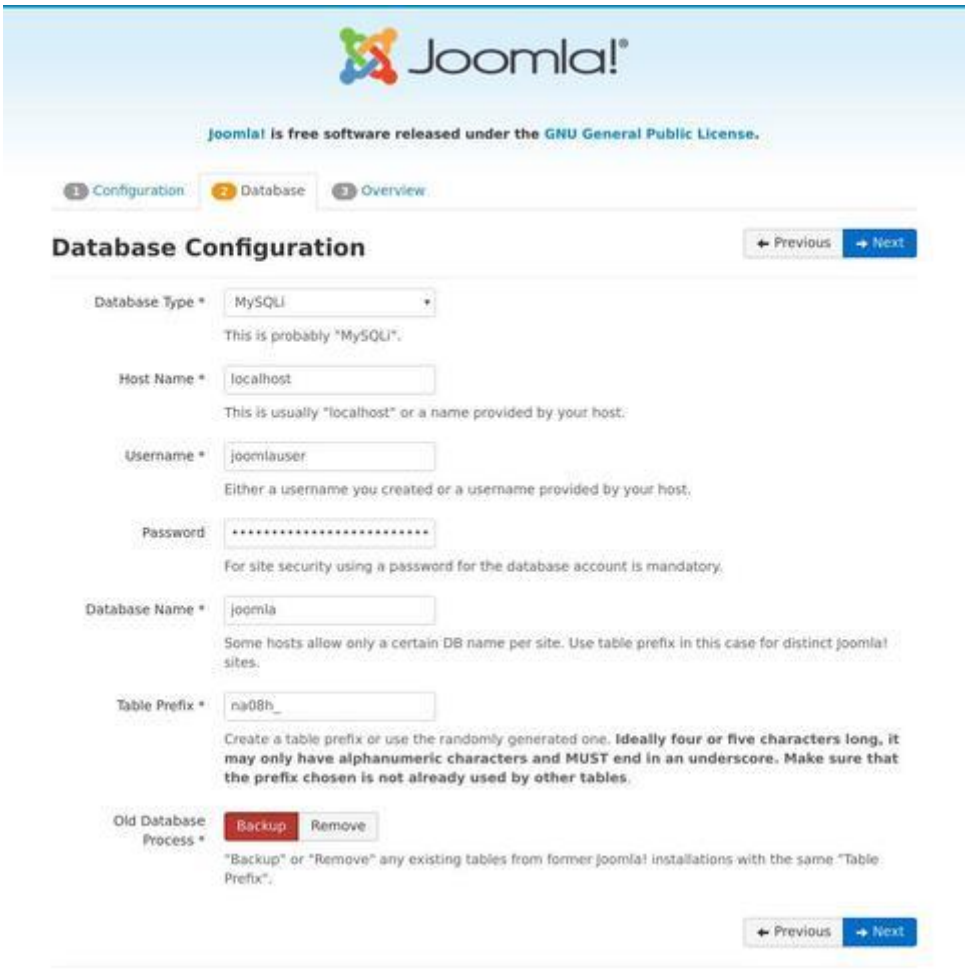
- **Имя сайта** — имя вашего нового веб-сайта Joomla.
- **Описание** — Описание сайта. Это резервное метаописание, которое будет использоваться на каждой странице без конкретного описания.
- **Адрес** электронной почты администратора — адрес электронной почты администратора. Используйте действующий адрес электронной почты. Если вы забудете свой пароль, вы получите ссылку для изменения пароля на этот адрес электронной почты.
- **Имя пользователя администратора** — имя пользователя с правами администратора. В целях безопасности установите для имени пользователя другое значение, кроме «admin».
- **Пароль администратора** — **пароль** администратора. Убедитесь, что вы используете надежный пароль. Введите тот же пароль в поле **Подтверждение пароля администратора** .

- **Сайт не в сети** — оставьте значение по умолчанию «Нет». Если вы выберете «Да», после завершения установки веб-сайт отобразит «Сайт не в сети».

Когда закончите, нажмите кнопку «Далее».

На следующем экране мастер настройки попросит вас ввести данные подключения к базе данных.

- **Тип базы данных** — оставьте значение по умолчанию «MySQLi».
- **Имя хоста** — оставьте значение по умолчанию «localhost». Если это руководство, база данных находится на том же сервере.
- **Имя пользователя** , **пароль** , **имя базы данных** — введите данные пользователя MySQL и базы данных, которые вы создали ранее.
- **Префикс таблицы** — оставьте автоматически созданный префикс.
- **Старый процесс базы данных** — оставьте параметр по умолчанию «Резервное копирование».



После нажатия кнопки «Далее» вы будете перенаправлены на страницу обзора:

Здесь вы можете выбрать установку демонстрационных данных и убедиться, что все проверки пройдены. Нажмите на кнопку « `Install` , и после завершения установки вы попадете на страницу, информирующую вас о том, что Joomla установлена.

Если вы хотите установить дополнительные языки, нажмите кнопку «Дополнительные шаги: Установить языки».

По соображениям безопасности вам необходимо удалить каталог установки. Для этого вернитесь в терминал и выполните следующую команду `rm` :

```
sudo rm -rf /var/www/example.com/installation
```

Чтобы получить доступ к вашей серверной части Joomla, нажмите кнопку « `Adminstrator` . Отсюда вы можете начать настройку вашей установки Joomla, установив новые темы и плагины.

2. Arch Linux

Аналогично провидите установку CMS Joomla на сервер с Arch Linux

2.27. Практическая работа № 27
Создание web-ресурса на joomla. Обеспечение доступа по HTTPS

Задание:

Настройка Apache на сервере Ubuntu и Arch Linux

Для начала необходимо активировать `mod_ssl`:

```
sudo a2enmod ssl
```

А затем включить настройки HTTPS сайта по умолчанию:

```
sudo a2ensite default-ssl
```

Теперь необходимо отредактировать файл с настройками HTTPS сайта по умолчанию, указав в нём пути к вашим сертификатам. Сам файл называется `/etc/apache2/sites-enabled/default-ssl` (или `/etc/apache2/sites-enabled/default-ssl.conf`).

В этом файле рекомендуется после директивы

```
SSLEngine on
```

добавить строчку

```
SSLProtocol all -SSLv2
```

дабы запретить использование устаревшего протокола SSLv2.

Дальше вам необходимо отредактировать параметры, ответственные за сертификаты.

```
# Публичный сертификат сервера
SSLCertificateFile    /etc/ssl/certs/server.pem
# Приватный ключ сервера
SSLCertificateKeyFile /etc/ssl/private/server.key
```

Теперь просто перезагрузите Apache:

```
sudo service apache2 restart
```

И если все параметры указаны верно, ваши сайты станут доступны по HTTPS.

Протокол HTTPS работает по 443 порту, поэтому если сервер находится за шлюзом, то необходимо на нём пробросить данный порт.

Перенаправление HTTP запросов на HTTPS

Если вы хотите запретить использование HTTP, то самым разумным будет перенаправлять все HTTP запросы к страницам на их HTTPS адрес. Сделаем это с помощью `mod_alias`. Если он не включён — включаем:

```
sudo a2enmod alias
sudo service apache2 restart
```

Затем изменяем файл `/etc/apache2/sites-enabled/000-default`, отвечающий за виртуальный хост по умолчанию для HTTP запросов. В этот файл добавляем директиву

```
Redirect / https://example.com/
```

При этом все настройки директорий можно удалить, поскольку по HTTP на ваши сайты всё равно будет не попасть.

Всё, теперь ещё раз перезапустите Apache и убедитесь, что при заходе по HTTP вы автоматически перенаправляетесь на HTTPS страницу.

2.29. Практическая работа № 29
Установка CMS Drupal на web-сервер

Задание:

Загрузка Drupal

Первое, что нам нужно сделать, это загрузить архив приложения на ваш виртуальный сервер. С помощью утилиты wget скачиваем стабильную версию ПО с официального сайта разработчика:

```
cd ~
wget http://ftp.drupal.org/files/projects/drupal-8.3.4.tar.gz
```

С помощью команды tar распакуйте файлы:

```
tar xzvf drupal*
```

В итоге содержимое каталога будет следующим:

```
root@Ubuntu1604x64:~# ls
drupal-8.3.4  drupal-8.3.4.tar.gz  nohup.out
```

Скопируйте файлы в каталог с помощью команд: `cd drupal-8.3.4`
`rsync -avz . /var/www/html`

Настройка Drupal для обеспечения безопасности

Сценарий установки требует внесения некоторых изменений в каталог Drupal, чтобы закончить процесс правильно. Сначала сделайте нужный подкаталог подкаталог:

```
cd /var/www/html/sites/default/
mkdir files
```

Далее мы должны скопировать файл настроек по умолчанию в файл, который Drupal использует для активной конфигурации:

```
cp /var/www/html/sites/default/default.settings.php
/var/www/html/sites/default/settings.php
```

Этот активный файл настроек временно требует дополнительных разрешений во время процедуры установки. Необходимо предоставить разрешения на запись владельцу группы:

```
chmod 664 /var/www/html/sites/default/settings.php
```

Нужно предоставить групповое владение файлами веб-пользователю, которым является www-data:

```
cd /var/www
chown www-data:www-data -R ./*
```

Настройка Базы данных

Создайте новую БД для MySQL для Drupal, для этого заходим в MySQL-оболочку:

```
mysql -u root -p
```

Войдите в СУБД, используя пароль суперпользователя MySQL. Затем нужно создать базу данных, нового пользователя в этой базе данных и предоставить ему привилегии.

Создаем базу данных:

```
CREATE DATABASE drupal;
```

Создаем нового пользователя:

```
CREATE USER duser@localhost;
```

Устанавливаем пароль для нового пользователя, указав вместо <пароль> ваш пароль:

```
SET PASSWORD FOR duser@localhost= PASSWORD("<пароль>");
```

Завершите настройку, предоставив все привилегии новому пользователю. Без привилегий CMS не сможет полноценно использовать базу данных:

```
GRANT ALL PRIVILEGES ON drupal.* TO duser IDENTIFIED BY '<пароль>';
```

Затем обновите MySQL:

```
FLUSH PRIVILEGES;
```

На этом этапе можно выйти из оболочки MySQL:

```
exit
```

Дополнительные модули PHP

Для работы данной CMS необходимо установка специальных модулей php. С помощью последующих действий установите их:

```
apt-get update
apt-get install php7.0-gd
```

Далее сделаем несколько небольших изменений в файле конфигурации PHP. Откройте файл конфигурации Apache PHP в текстовом редакторе, например vi:

```
vi /etc/php/7.0/apache2/php.ini
```

Откройте директивы **expose_php** и **allow_url_fopen** и установите оба значения в "Off".

Примечание: в текстовом редакторе vi поиск можно осуществить следующем образом - нажмите "/", введите слово для поиска, далее Enter. Перебор соответствий можно осуществить с помощью клавиши "n".

```
; Decides whether PHP may expose the fact that it is installed on the server
; (e.g. by adding its signature to the Web server header).  It is no security
; threat in any way, but it makes it possible to determine whether you use PHP
; on your server or not.
; http://php.net/expose-php
expose_php = Off
```

```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-fopen
allow_url_fopen = Off
```

Настройка Apache

Чтобы перейти к настройке Drupal в браузере, необходимо отредактировать файл конфигурации apache:

```
vi /etc/apache2/sites-enabled/000-default.conf
```

Пример:

```
<VirtualHost *:80>
    ServerName  185.158.152.201
    DocumentRoot /var/www/html
    ErrorLog /var/log/apache2/error_185.158.152.201
    CustomLog /var/log/apache2/access_log_185.158.152.201 combined
    <Directory /var/www/html>
        AllowOverride All
    </Directory>
</VirtualHost>
```

Примечание: если у вас несколько сайтов на сервере используйте документацию на Apache.

Настройка FireWall для возможности удаленного доступа (проброс порта):

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables-save
```

Примечание: после перезапуска сервера порт опять будет необходимо открыть.

Выполните перезапуск сервера Apache для проделанных изменений:

```
service apache2 restart
```

Настройка Drupal

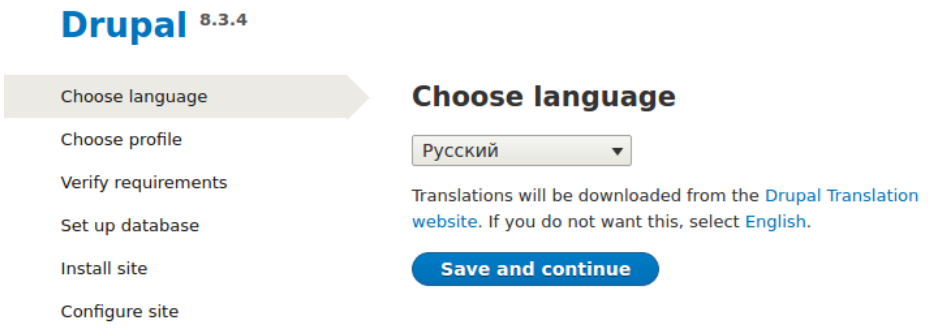
В адресной сроке браузера перейдите по ссылке, указав ваш АйПи-адрес:

```
<ip-адрес>
```

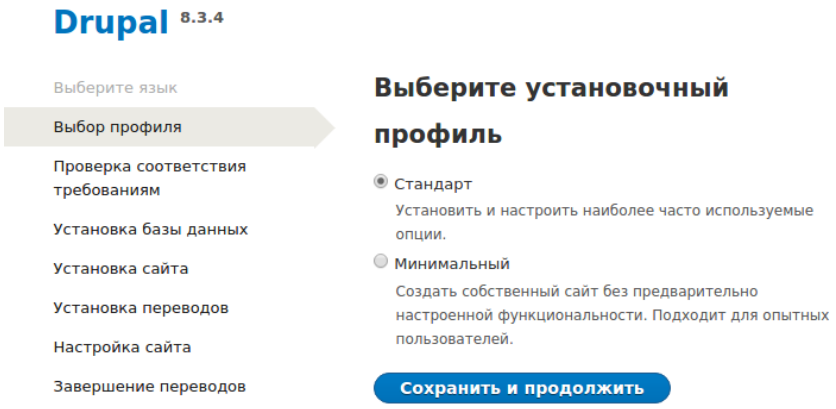
Например:

```
185.125.46.12
```

Выберете язык.

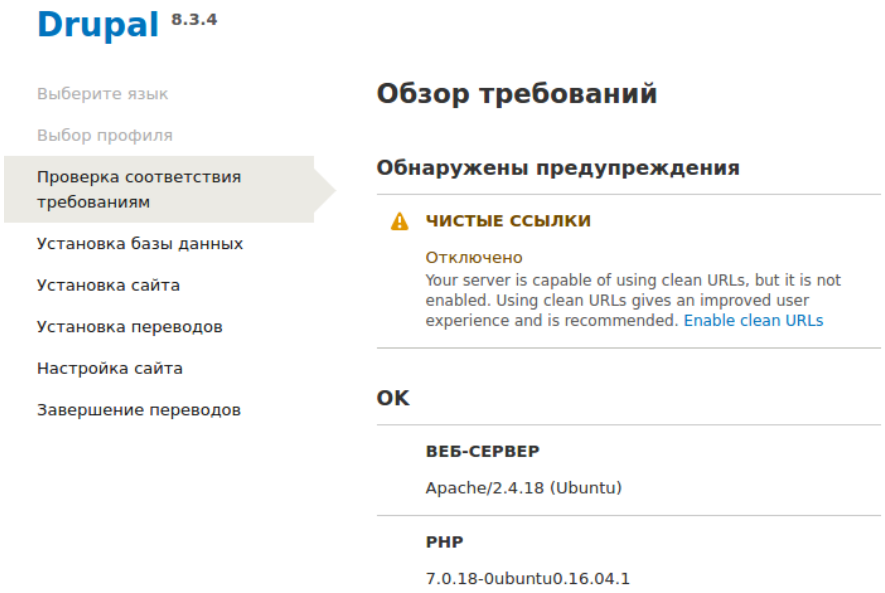


В окне установке выберете профиль **Стандарт** и нажмите **Сохранить и продолжить**.



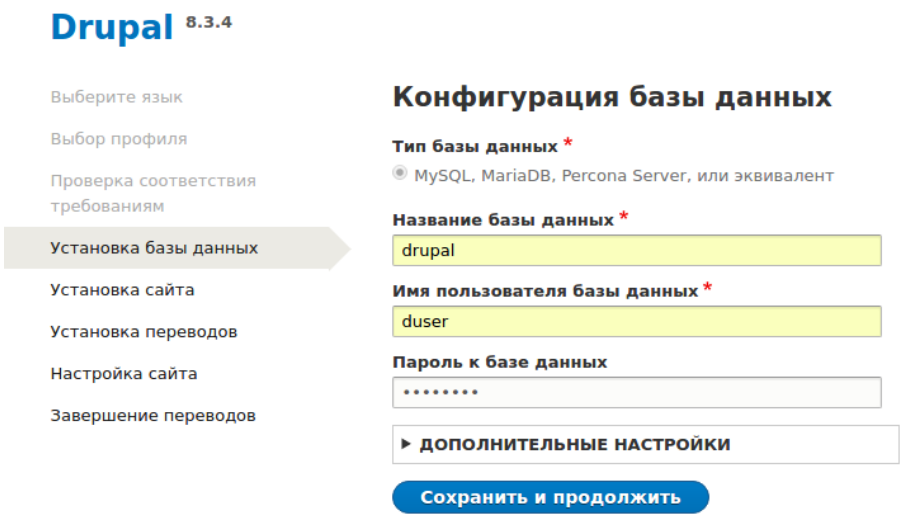
В следующем окне при возникновении ошибок установите недостающие модули.

Для продолжения перейдите по ссылке внизу страницы.

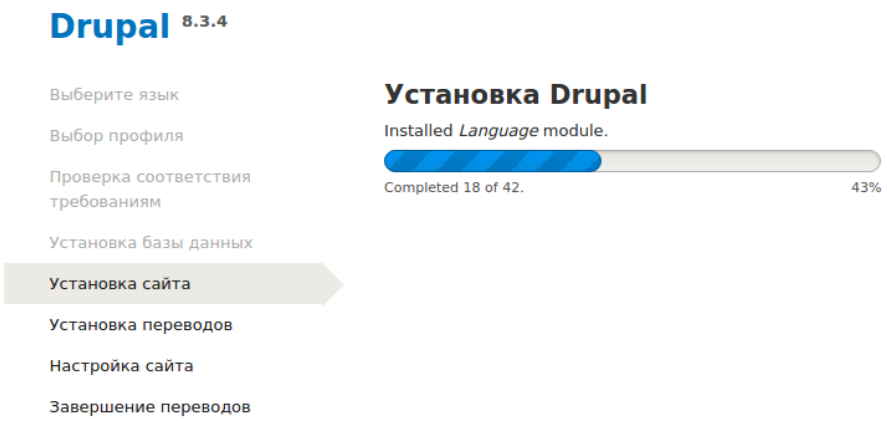


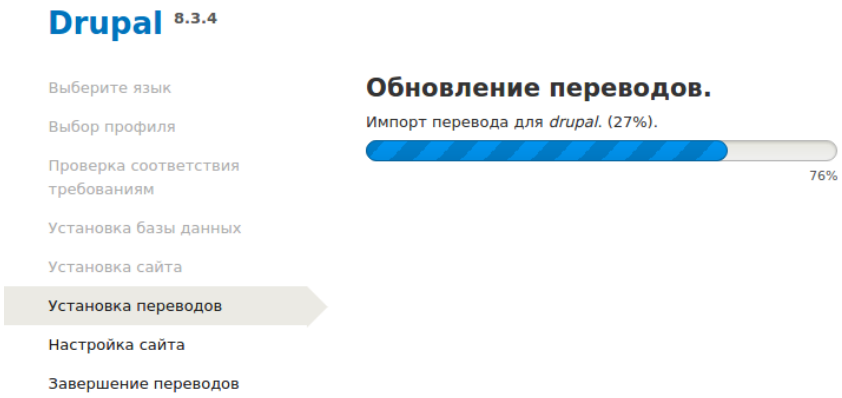
На следующем шаге введите созданного MySQL-пользователя, пароль и имя базы.

*Примечание: когда вы нажмите **Save and continue**, есть вероятность, что вы будете перенаправлены обратно на ту же страницу конфигурации базы данных. Если это произойдет, просто обновите страницу. База данных будет настроена, и профиль будет установлен.*



Как правило установка занимает некоторое время.

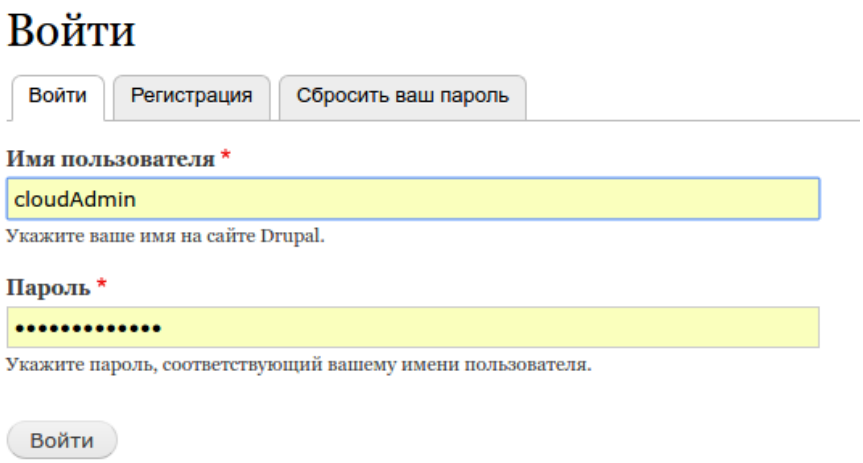




Далее введите личную информацию, такую как домен вашего сайта, электронную почту, и остальные сведения. При настройке Вам будут даны рекомендации по уровню сложности пароля и созданию имени администратора.

По завершению установки вы попадете в панель управления сайтом.

При переходе на сайт или ip-адрес для входа в CMS используйте созданные на последнем шаге логин и пароль.



2.29. Практическая работа № 29
Создание web-ресурса на Drupal. Обеспечение доступа по HTTPS

Задание:
Настройка Apache на сервере Ubuntu и Arch Linux

Для начала необходимо активировать `mod_ssl`:

```
sudo a2enmod ssl
```

А затем включить настройки HTTPS сайта по умолчанию:

```
sudo a2ensite default-ssl
```

Теперь необходимо отредактировать файл с настройками HTTPS сайта по умолчанию, указав в нём пути к вашим сертификатам. Сам файл называется `/etc/apache2/sites-enabled/default-ssl` (или `/etc/apache2/sites-enabled/default-ssl.conf`).

В этом файле рекомендуется после директивы

```
SSLEngine on
```

добавить строчку

```
SSLProtocol all -SSLv2
```

дабы запретить использование устаревшего протокола SSLv2.

Дальше вам необходимо отредактировать параметры, ответственные за сертификаты.

```
# Публичный сертификат сервера
SSLCertificateFile    /etc/ssl/certs/server.pem
# Приватный ключ сервера
SSLCertificateKeyFile /etc/ssl/private/server.key
```

Теперь просто перезагрузите Apache:

```
sudo service apache2 restart
```

И если все параметры указаны верно, ваши сайты станут доступны по HTTPS.

Протокол HTTPS работает по 443 порту, поэтому если сервер находится за шлюзом, то необходимо на нём пробросить данный порт.

Перенаправление HTTP запросов на HTTPS

Если вы хотите запретить использование HTTP, то самым разумным будет перенаправлять все HTTP запросы к страницам на их HTTPS адрес. Сделаем это с помощью `mod_alias`. Если он не включён — включаем:

```
sudo a2enmod alias
sudo service apache2 restart
```

Затем изменяем файл `/etc/apache2/sites-enabled/000-default`, отвечающий за виртуальный хост по умолчанию для HTTP запросов. В этот файл добавляем директиву

```
Redirect / https://example.com/
```

При этом все настройки директорий можно удалить, поскольку по HTTP на ваши сайты всё равно будет не попасть.

Всё, теперь ещё раз перезапустите Apache и убедитесь, что при заходе по HTTP вы автоматически перенаправляетесь на HTTPS страницу.

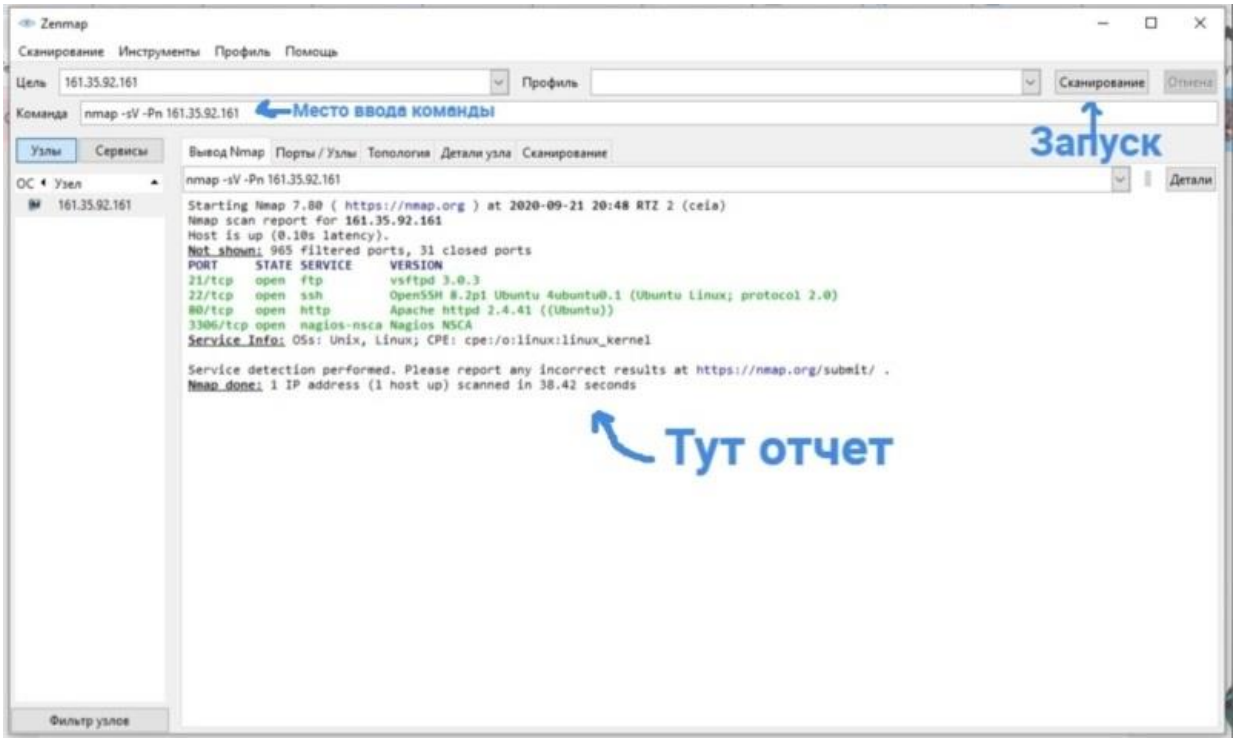
2.30. Практическая работа № 30
Анализ безопасности сайтов на различных CMS

Задание:

1. Проверить сетевую инфраструктуру.

Установка на Windows 10
Перейдите по ссылке загрузки nmap и загрузите последнюю стабильную версию. На данный момент (16.09.2020) эта версия 7.80. Скачать ее можно по этой ссылке с официального сайта. Дальше запустите nmap-7.80-setup.exe от имени администратора. Программа установки по умолчанию предложит установить все компоненты, галочки можно не снимать. Описывать шаги далее подробно (Примите лицензионное соглашение и тд) не буду, там все изи.
Запуск nmap на Windows
Запускать nmap можно как в режиме графического интерфейса, так и через командную строку.
Для запуска графической оболочки введите в строку поиска nmap и в результатах выберите nmap - Zenmap GUI

Для дальнейшей работы вы можете вводить нужные команды в поле "Команда", а затем нажимать на кнопку Сканирование. Результаты сканирования в виде текстового отчета вы можете посмотреть в окне, которое я старательно подписал "Отчет"



Устанавливаем скрипты

Также нам надо установить скрипт nmap_vulners, который будет проводить проверку на то, содержатся ли уязвимости в ПО, которое мы используем. Для его установки нужно скачать файлы скрипта и перенести файлы **http-vulners-regex.nse** и **vulners.nse** в *C:\Program Files (x86)\Nmap\scripts*.

Если у вас Mac OS, то перенести файлы скрипта нужно в папку
/usr/local/Cellar/nmap/<version>/share/nmap/scripts/

Начинаем проверку

Для начала запускаем сканирование своего сервера командой ниже, чтобы выяснить какие порты используются и для чего. Команда выглядит так (подставьте свой ip или домен). Команду нужно вводить в окне консоли, либо если вы используете Zenmap GUI, то в поле "Команда" (пример я привел выше):

nmap -sV -Pn -p- -T5 161.35.92.161

Параметр **T5** отвечает за скорость анализа сервера. Скорость можно менять от **T0** до **T5**, где T0 - очень медленная скорость анализа, а T5 - очень быстрая. Если вы не хотите сильно нагружать сервер, то используйте T2.

Параметр **-p-** означает, что мы будем проверять весь диапазон портов ('это займет около 10 минут) . Его можно убрать и тогда скрипт просканирует не все порты, а только 1000 первых (самые распространенные).

Ответ будет выглядеть примерно так:

nmap -sV -Pn 161.35.92.161 Starting Nmap 7.80 (https://nmap.org) at 2020-09-16 20:03 RTZ 2 (ceia) Nmap scan report for 161.35.92.161 Host is up (0.085s latency). Not shown: 965 filtered ports, 31 closed ports PORT STATE SERVICE VERSION 21/tcp open ftp vsftpd 3.0.3 22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0) 80/tcp open http Apache httpd 2.4.41 ((Ubuntu)) 3306/tcp open mysql MySQL 5.5.5-10.2.24-MariaDB Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 32.39 seconds

Из отчета мы видим, что nmap отобразил нам порты (под колонкой PORT), которые активны. В данном случае у нас используются:

- Порт 21 занят под FTP
- Порт 22 занят под SSH.
- Порт 80 прослушивается сервером Apache.
- Порт 3306 используется MySQL

Теперь запускаем наш скрипт, который проверит уязвимости в нашем ПО на сервере. Для этого запускаем следующую команду с указанием портов, которые мы будем проверять. Вам нужно будет заменить список портов на свои .

nmap -T5 -sV -Pn 161.35.92.161 --script=vulners.nse -p22,80,443,8080,8443,3306,20,21,23

Пример отчета. Ссылки на описание уязвимости идут после строки *vulners* (пример такой строки со ссылкой в отчете: *CVE-2014-9278 4.0 https://vulners.com/cve/CVE-2014-9278*)

Starting Nmap 7.80 (https://nmap.org) at 2020-09-16 20:50 RTZ 2 (ceia) Nmap scan report for 161.35.92.161 Host is up (0.094s latency). PORT STATE SERVICE VERSION 20/tcp closed ftp-data 21/tcp open ftp vsftpd 3.0.3 22/tcp open ssh OpenSSH 8.2p1 Ubuntu

4ubuntu0.1 (Ubuntu Linux; protocol 2.0) | vulners: | cpe:/a:openbsd:openssh:8.2p1: |_ CVE-2014-9278 4.0 https://vulners.com/cve/CVE-2014-9278 23/tcp filtered telnet 80/tcp open http Apache httpd 2.4.41 ((Ubuntu)) |_http-server-header: Apache/2.4.41 (Ubuntu) | vulners: | cpe:/a:apache:http_server:2.4.41: | CVE-2020-11984 7.5 https://vulners.com/cve/CVE-2020-11984 | CVE-2020-11984 7.5 https://vulners.com/cve/CVE-2020-11984 | CVE-2020-1927 5.8 https://vulners.com/cve/CVE-2020-1927 | CVE-2020-1927 5.8 https://vulners.com/cve/CVE-2020-1927 | CVE-2020-9490 5.0 https://vulners.com/cve/CVE-2020-9490 | CVE-2020-1934 5.0 https://vulners.com/cve/CVE-2020-1934 | CVE-2020-1934 5.0 https://vulners.com/cve/CVE-2020-1934 |_ CVE-2020-11993 4.3 https://vulners.com/cve/CVE-2020-11993 443/tcp closed https 3306/tcp open mysql MySQL 5.5.5-10.2.24-MariaDB 8080/tcp filtered http-proxy 8443/tcp filtered https-alt Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 24.23 seconds

Как видите из отчета, скрипт проанализировал активное ПО нашего сервера и любезно предоставил ссылки с описанием каждой найденной уязвимости. Что согласитесь, очень удобно как для нас, так и для злоумышленников.

Также можно записать результат анализа в файл, который потом можно скинуть ответственному разработчику или системному администратору. Сам файл результатов будет находиться в каталоге, из которого вы запускаете скрипт. Пример такой команды ниже:

nmap -T5 -sV -Pn 161.35.92.161 --script=vulners.nse -p22,80,443,8080,8443,3306,20,21,23 > result.txt

Чтобы избавиться от подобных проблем обычно достаточно обновить используемое ПО до последних версий, где уязвимости старых версий, как правило, уже исправлены.

2. Проверить устойчивость к перебору.

SSH

Вводим следующую команду (напомню, что вводить нужно либо в консоль, либо в поле "Команда" программы Zenmap GUI.

nmap --script ssh-brute -p22 161.35.92.161 --script-args userdb=users.lst,passdb=passwords.lst

В случае успеха (процесс не быстрый) скрипт выведет подобранный пароль и логин . Подобранные пары логин\пароль будут выведены после строчки *Accounts:*

22/ssh open ssh ssh-brute: Accounts username:password Statistics Performed 32 guesses in 25 seconds.

Кроме того, можно расширить стандартные списки паролей и пользователей от nmap, заменив файлы users.lst и passwords.lst . Различные базы для брутфорса можно найти в этом gitbub репозитории. Файлы с базой паролей можно разместить в папке *nmap/nselib/data*

FTP

Теперь проверяем FTP порт следующей командой:

nmap -d --script ftp-brute -p 21 161.35.92.161

Аналогично, сервис выведет подобранные пары логинов и паролей:

PORT STATE SERVICE 21/tcp open ftp | ftp-brute: | Accounts | root:root - Valid credentials |_ Statistics: Performed 864 guesses in 544 seconds, average tps: 4.8

MySQL

Проверяем доступен ли анонимный вход.

nmap -sV --script=mysql-empty-password <target>

В случае успеха:

3306/tcp open mysql | mysql-empty-password: | anonymous account has empty password |_ root account has empty password

Пытаемся подобрать пару логин\пароль для входа в базу данных mysql.

nmap --script mysql-brute -p 3306 <target> --script-args userdb=users.lst, passdb=passwords.lst

Также если у вас используются CMS (WordPress, Joomla, Drupal, Bitrix) и другие базы данных (Mongo, Postgres, Redis), то можно найти готовые скрипты для проверки устойчивости ваших паролей и форм. Ищите по ключевым словам <name_of_CMS_or_DB> brute force nmap

Проверяем формы авторизации

Найти формы авторизации можно с помощью такой команды (вместо <target> - подставьте домен вашего сайта):

nmap -p80 --script http-auth-finder <target>

После того, как нашли страницы с авторизацией, можно попробовать подобрать пароль и логин для входа в админку сайта.

Параметры

- **http-brute.hostname** - имя хоста
- **http-form-brute.path** - адрес страницы с формой или адрес с API
- **http-brute.method** - тип метода**,** по умолчанию **POST**
- **http-form-brute.uservar** - устанавливает имя переменной, которая отвечает за username. Если не установлено, то скрипт возьмет имя поля из формы
- **http-form-brute.passvar** - устанавливает имя переменной, которая отвечает за пароль. Если не установлено, то скрипт возьмет имя поля из формы

Параметры нужно перечислять через запятую после -script-args.

nmap -p-80 --script=http-form-brute --script-args=http-form-brute.path=/login <target>

Если скрипт успешно сработает, то выведет примерно вот такой результат.

Подобранные данные для входа будут отображены после строчки *Accounts.* В нашем случае скрипт подобрал логин user с паролем secret. В реальном приложении подбор может также занять продолжительное время, зависит от того насколько стойкий пароль используется.

PORT STATE SERVICE REASON 80/tcp open http syn-ack | http-form-brute: | Accounts | user:secret - Valid credentials | Statistics |_ Perfomed 60023 guesses in 467 seconds, average tps: 138

Если ваша формы авторизации использует cookies параметры или csrf-token, то в этом случае выдаст ошибку. (И это хорошо, значит базовую защиту вы предусмотрели).

В качестве защиты стоит использовать стойкие пароли, а также ограничивать количество запросов с одного IP-адреса (Rate limiting).

3. Поиск скрытых папок и файлов

Часто разработчики или системные администраторы довольно халатно относятся к правам доступа и забывают закрыть доступ к системным и другим важным папкам. Проверить есть у нас на сервере такие папки можно также с помощью утилиты nmap. Команды будет выглядеть так (вместо <target> нужно подставить IP-адрес сервера или домен сайта) :

nmap -sV -p 80 -T5 --script http-enum <target>

В результате в отчете нам покажут доступные для просмотра папки, интересные файлы - файлы паролей, резервные копии базы данных и тд. (Если такие существуют). Дальше уже вам нужно самостоятельно решить какие папки и файлы нужно закрыть от просмотра, а какие оставить как есть.

Пример небольшого отчета.

Host is up (0.024s latency). Not shown: 993 closed ports PORT STATE SERVICE 80/tcp open http | http-enum: | /robots.txt: Robots file | /css/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)' | /images/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)' |_ /js/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)'

4. Проверка на SQL инъекции

Так повелось, что большинство современных веб-приложений в той или иной мере используют SQL базы данных. Обычно параметры веб-страницы или какие-либо пользовательские данные подставляются в SQL запросы и результаты запроса отображаются на веб-странице. Если передаваемые параметры плохо фильтруются, то веб-сервис становится уязвимым для **SQL инъекций.**

Если сайт уязвим и выполняет такие инъекции, то по сути есть возможность творить с БД (чаще всего это MySQL) что угодно. Именно таким образом чаще всего воруют базы пользователей и их личные данные.

Далее я покажу как с помощью скриптов быстро и эффективно проверить есть в вашем продукте подобные уязвимости. Часто даже довольно опытные разработчики забывают о мерах предосторожности, поэтому даже серьезные продукты имеют подобные проблемы. Попробуем проверить наш тестовый веб-сервис на наличие таких проблем с помощью инструмента sqlmap.

Установка sqlmap.

Sqlmap - это кроссплатформенный сканер с открытым исходным кодом, который позволяет в автоматическом режиме тестировать веб-сервисы на наличие SQL инъекций, а затем использовать их для получения контроля над базой данных.

В данной статье я рассмотрю только способы как можно находить уязвимые для SQL инъекций страницы, API и формы без подробностей о том, как использовать найденные уязвимости для нанесения вреда. (Владельцы сайтов тут облегченно вздохнули). Для использования необходим python версии 2.7 и старше.

Установка на Windows

Для начала работы нам необходимо установить Python. Установщик Python для Windows можно найти на официальном сайте.

На сайте две ветки - 2.x и 3.x, но скачать и установить лучше ветку 3.x. Sqlmap корректно работают с каждой из этих версий, но в дальнейшем нам потребуется версия 3.x.

Загрузить последнюю версию sqlmap можно здесь. Распакуйте архив в любую удобную папку (чтобы было проще ее найти можно распаковать в папку C:\Users\<имя вашего пользователя>)

Для запуска вначале нужно открыть командную строку. Нажмите Win+R, в появившемся окне введите cmd и нажмите enter. Пример запуска:

C:\Users\Admin\sqlmap>python ./sqlmap.py -u http://161.35.92.161/page.php?id=2
Начинаем проверку

В моем тестируемом сервисе я специально подготовил sql уязвимости. Попробуем найти их следующей командой. Параметр **--dbs** означает, что нам интересны имена баз данных. В случае успеха и наличия уязвимости, после определения баз данных можно перейти к поиску таблиц и получения нужных данных. Команду необходимо вводить в консоль.

python sqlmap.py -u http://161.35.92.161/page.php?id=2 --dbs -o -random-agent

Через некоторое время скрипт может попросить нас уточнить некоторые данные. В данном случае выбираю "нет", чтобы скрипт прогнал все тесты.

[01:14:57] [INFO] fetched random HTTP User-Agent header value 'Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0; YComp 5.0.2.6; MSIECrawler)' from file 'C:\Users\Acer\sqlmap\data\txt\user-agents.txt' [01:15:04] [INFO] testing connection to the target URL [01:15:04] [INFO] checking if the target is protected by some kind of WAF/IPS [01:15:05] [INFO] testing NULL connection to the target URL [01:15:05] [INFO] NULL connection is supported with GET method ('Range') [01:15:05] [INFO] testing if the target URL content is stable [01:15:05] [INFO] target URL content is stable [01:15:05] [INFO] testing if

GET parameter 'id' is dynamic [01:15:05] [INFO] GET parameter 'id' appears to be dynamic [01:15:06] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable [01:15:06] [INFO] testing for SQL injection on GET parameter 'id' [01:15:06] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause' [01:15:06] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable [01:15:07] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'CrateDB' it looks like the back-end DBMS is 'CrateDB'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n

Скрипт выводит отчет:

[01:15:29] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' [01:15:29] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause' [01:15:29] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)' [01:15:30] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)' [01:15:30] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)' [01:15:30] [INFO] testing 'Generic inline queries' [01:15:30] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)' [01:15:30] [WARNING] time-based comparison requires larger statistical model, please wait..... (done) [01:15:32] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)' [01:15:32] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)' [01:15:32] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' [01:15:43] [INFO] GET parameter 'id' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable [01:15:43] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns' [01:15:43] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found [01:15:45] [INFO] target URL appears to be UNION injectable with 4 columns [01:15:46] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y

После продолжения анализа нас в первую очередь интересует строчка в конце: *GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]*.

Как можно видеть, скрипт определил, что параметр id уязвим и предлагает протестировать другие параметры. В нашем конкретном случае других параметров нет, но в реальных веб-приложениях таких параметров может быть десятки, так что иногда имеет смысл проверить все.

Итоговый отчет:

sqlmap identified the following injection point(s) with a total of 74 HTTP(s) requests: --- Parameter: id (GET) Type: boolean-based blind Title: AND boolean-based blind - WHERE or HAVING clause Payload: id=2 AND 9795=9795 Type: time-based blind Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP) Payload: id=2 AND (SELECT 7989 FROM (SELECT(SLEEP(5)))geJr) Type: UNION query Title: Generic UNION query (NULL) - 4 columns Payload: id=2 UNION ALL SELECT NULL,CONCAT(0x716a6a6b71,0x736654714b69505a4f6f64434776566d7a43455179446561434f7a46434241555449574d6759575a,0x7162627171),NULL,NULL-- - --- [INFO] the back-end DBMS is MySQL web server operating system: Linux Ubuntu web application technology: Apache 2.4.41 back-end DBMS: MySQL >= 5.0.12 [INFO] fetching database names available databases [2]: [*] information_schema [*] vc_test [INFO] fetched data logged to text files under 'C:\Users\Admin\AppData\Local\sqlmap\output\161.35.92.161'

В итоге скрипт не только определил, что параметр **id** является уязвимым, но и версию СУБД, а также получил название используемой базы данных на сервере - **vc_test**, в которой содержится контент сайта. Эту информацию можно найти в конце сгенерированного отчета.

5. Проверка на XSS уязвимости.

Межсайтовый скриптинг (XSS) – это уязвимость, которая заключается во внедрении злоумышленником своего Javascript кода в веб-страницу, которая отображается в браузере пользователя.
После такого внедрения злоумышленник фактически захватывает веб-страницу и может манипулировать данными пользователя, когда он находится на странице. В случае успеха злоумышленник может:

- Внедрять свои скрипты в веб-страницу
- Отправлять на свой сервер пользовательские данные - банковские карты, идентификаторы сессий, пароли и тд.
- Совершать действия от имени пользователя - рассылать спам, совершать денежные переводы

Уязвимость возникает из-за недостаточной фильтрации данных, которые выводятся при отображении страницы.
Такие уязвимости довольно часто встречаются даже в крупных продуктах, поэтому стоит обязательно тестировать свои веб-приложения на наличие XSS уязвимостей.
В данном случае для тестирования мы воспользуемся утилитой **XSStrike**
XSStrike - это довольно продвинутый сканер для поиска XSS уязвимостей с открытым исходным кодом. Он написано на Python3 и довольно прост в начальной настройке и использования.
Установка
Для установки необходимо скачать архив по ссылке и распаковать в удобную вам папку. После этого необходимо открыть консоль (ранее я уже показывал как это сделать в Mac и Windows) и перейти в распакованную папку. Затем нужно выполнить команды в консоле:
pip3 install pygame
Установим необходимые для корректной работы библиотеки:
pip3 install -r requirements.txt
Теперь мы готовы к тестированию. Пример простого запуска, вместо моего url укажите адрес страницы, которую хотите протестировать:
python xsstrike.py -u "http://161.35.92.161/index.php?page=2" --blind
Очень быстро скрипт обнаруживает, что параметр page является уязвимым (строчка *Reflections found*) и через него можно передать js код, который будет исполнен на странице. Пример такого кода приводится в строчке *Payload*. Такой тип XSS уязвимостей называется reflected XSS.
[~] Checking for DOM vulnerabilities [+] WAF Status: Offline [!] Testing parameter: page [!] Reflections found: 1 [~] Analysing reflections [~] Generating payloads [!] Payloads generated: 3072 ---------- [+] Payload: <HTmL%0aONmOuSEoVeR+=+(prompt)``%0dx// [!] Efficiency: 100 [!] Confidence: 10 [?] Would you like to continue scanning? [y/N] n
Кроме того, можно проверять и формы. Отправим на проверку форму, которая отправляет сообщение в наш сервис. Чтобы передать список POST параметров используем опцию **--data**.
python xsstrike.py -u "http://161.35.92.161/index.php" --data "name=&message=" --blind
Результат: параметр name уязвим.

[~] Checking for DOM vulnerabilities [+] WAF Status: Offline [!] Testing parameter: name [!] Reflections found: 3 [~] Analysing reflections [~] Generating payloads [!] Payloads generated: 4608 ---------- [+] Payload: <A%0aOnmOUSeOVEr%0d=%0d(prompt)``%0dx>v3dm0s [!] Efficiency: 100 [!] Confidence: 10 [?] Would you like to continue scanning? [y/N]

Как выглядит ответ, когда скрипт не находит уязвимых параметров:

[~] Checking for DOM vulnerabilities [+] WAF Status: Offline [!] Testing parameter: name [-] No reflection found [!] Testing parameter: message [-] No reflection found

Кроме того, в XSStrike поддерживает возможность передавать http заголовки, в том числе и cookies и проверять страницы для открытия которых нужна авторизация. Для этого используется опция **--headers**

python xsstrike.py -u "http://161.35.92.161/index.php" --data "name=&message=" --headers "Authorization: Bearer <token> Cookie: zmname\=none" --blind

Также можно запустить обход по всему сайту. Нужно указать стартовую страницу и сканер начнет обход всех найденных страниц. Запись **-l 100** отвечает за количество страниц обхода.

python xsstrike.py -u "http://161.35.92.161" --blind --crawl -l 100

Скрипт покажет страницы, на которых были найдены уязвимые параметры. Найденные страницы можно уже исследовать подробнее.

[~] Crawling the target [++] Vulnerable webpage: http://161.35.92.161/index.php [++] Vector for message: <htMl%09oNMOuseoVER%0d=%0dconfirm()// [++] Vulnerable webpage: http://161.35.92.161/index.php [++] Vector for page: <hTMl%0donPointereNter%0a=%0a[8].find(confirm)> [++] Vulnerable webpage: http://161.35.92.161/index.php [++] Vector for name: <D3v/+/oNMoUSeoveR%0a=%0a(confirm)()%0dx>v3dm0s !] Progress: 3/3

Также полезная функция - обход url страниц, которые указаны в файле с помощью опции **--seeds**. Можно также использовать вместе с опцией **--headers.**

python xsstrike.py -u "http://example.com" -l 3 --seeds urls.txt

Таким образом можно достаточно тщательно проверить свое веб-приложение на XSS уязвимости. Также хорошим ходом будет написать простой bash скрипт для объединения всех проверок XSS в один скрипт, специально заточенный под ваш проект.

Его задачей будет тестировать ваше веб-приложение после каждого изменения исходного кода и не пускать коммит в ветку master, если страницы и формы содержат XSS уязвимости .

Для борьбы с XSS уязвимости нужно также тщательно фильтровать данные, которые показываются пользователю.