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» декабря 2023 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по выполнению практических работ
по МДК.02.03 Кибербезопасность
ПМ.02 ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ

для специальности
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Санкт-Петербург
2023 г.

Методические рекомендации рассмотрены на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол № 2 от «29» ноября 2023 г.

Методические рекомендации одобрены на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий

Протокол № 4 от «21» ноября 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА 6

1 ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ ПО ТЕМАМ МДК.02.03. «КИБЕРБЕЗОПАСНОСТЬ» ПМ.02 «ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ» 9

2 ОПИСАНИЕ ПОРЯДКА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ 17

Практическое занятие № 1. Установка и настройка Windows Server 2019 17

Практическое занятие № 2. Установка контроллера домена. Использование Windows PowerShell для администрирования AD DS. 29

Практическая работа № 3 «Установка ролей сервера Windows Server 2012 R2» 56

Практическая работа № 4 «Подключение сетевых периферийных устройств через Групповую политику» 70

Практическая работа № 5 «Установка и настройка сервера времени и сервера лицензирования» 76

Практическая работа № 6 «Управление пользовательским рабочим столом через Групповую политику» 86

Практическая работа № 7 «Установка, настройка и устранение неполадок роли Сервер Сетевой политики» 92

Практическая работа № 8 «Применение технологии DirectAccess с помощью мастера начальной настройки» 99

Практическая работа № 9 «Развертывание расширенной инфраструктуры DirectAccess» 110

Практическая работа № 10 «Внедрение VPN» 118

Практическая работа № 11 «Настройка шифрования и расширенного аудита» 124

Практическая работа № 12 «Использование службы развертывания Windows для развертывания Windows Server 2012» 133

Практическая работа № 13 «Внедрение управления обновлениями. Мониторинг Windows Server 2012» 144

Практическое занятие №14. Настройка файлового сервера 164

Практическое занятие № 15. Настройка DHCP 165

Практическое занятие № 16. Настройка центра сертификации 166

Практическое занятие № 17. Настройка групповых политик 167

Практическое занятие № 18. Добавление рабочих станций в домен 167

Практическое занятие № 19. Установка сервера Debian. 167

Практическая работа № 15 «Установка и настройка веб-сервера на базе Nginx + PHP-FPM в Debian 179

Практическая работа № 16 «Настройка сервера DNS в ОС Debian 188

Практическая работа № 17 «Настройка сервера DHCP в ОС Debian» 191

Практическая работа № 18 «Настройка файловых серверов в ОС Debian» 194

Практическая работа № 19 «Настройка контейнеров Docker» 199
Практическая работа № 20 «Установка сервера CentOS» 205
Практическая работа № 21 «Настройка web-сервера в CentOS» 211
Практическая работа № 22 «Настройка сервера DNS в CentOS» 227
Практическая работа № 23 «Настройка сервера DHCP в CentOS» 248
Практическая работа № 24 «Установка и настройка OpenVPN» 250
Практическая работа № 25 «Применение протокола IP-sec и SSH.» 259
Практическая работа № 26 «Настройка регистрации действий» 271
Практическая работа № 27 «Установка и настройка OpenLDAP» 274
Практическая работа № 28 «Установка и настройка IPtables» 280
Практическое занятие № 34. Установка и базовая настройка Kali Linux 285
Практическое занятие № 35. Администрирование Kali Linux 285
Практическое занятие №36. Установка и настройка утилит в Kali Linux 285
Практическое занятие № 37. Поиск уязвимостей информационных систем 286
Практическое занятие № 38. Применение антивирусной защиты 293
Практическое занятие № 39. Настройка безопасности веб-браузеров 294
Практическое занятие № 40. Оценка рисков информационной безопасности сиспользованием классификации веб-угроз 294
Практическое занятие № 41. Сканирование системы с помощью IP-сканера 297
Практическое занятие № 42. Сканирование системы с помощью CFI LanGuard 300
Практическое занятие № 43. Поиск открытых портов 307
Практическое занятие № 44. Сканирование сети с помощью NetScan 308
Практическое занятие № 45. «Сканирование сети с помощью Nessus Tool 315
Практическое занятие № 46. Сканирование сети с помощью Colasoft Packet Builder 315
Практическое занятие № 47. Сканирование устройства в сети с помощью Dude. 316
Практическое занятие № 48. Отображение сети с помощью Friendly Pinger 317
Практическое занятие № 49. Анализ уязвимостей серверов 317
Практическое занятие № 50. Поиск и устранение неисправностей сети с помощью MegaPing 318
Практическое занятие № 51. Настройка межсетевого экрана 318
Практическое занятие № 52. Настройка параметров безопасности Windows. 318
Практическое занятие № 53. Составление рекомендаций по повышению уровня защищенности информационной инфраструктуры 319
Практическое занятие № 54. Выявление предпосылок и обстоятельств, приведших к возникновению компьютерного инцидента. 319
Практическое занятие № 55. Обнаружение события информационной безопасности. Оценка события информационной безопасности 322

Практическое занятие № 56. Исследование открытой информации в поисковых системах 329
Практическое занятие № 57. Поиск информации в социальных сетях.....329
Практическое занятие № 58. Поиск информации с помощью утилит 330

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Рабочая тетрадь для выполнения практических работ предназначена для организации работы на практических занятиях по темам МДК.02.03. «Кибербезопасность» ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» являющегося важной составной частью в системе подготовки специалистов среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

Практические занятия являются неотъемлемым этапом изучения тем МДК.02.03. «Кибербезопасность» 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 темам МДК.02.03. «Кибербезопасность» способствуют формированию следующих общих и профессиональных компетенций:

- ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
- ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
- ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.
- ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
- ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
- ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
- ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
- ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
- ОК 09. Использовать информационные технологии в профессиональной деятельности.

- ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.
- ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.
- *ПК.2.7. Администрирование компонентов ИТ-инфраструктуры*
- *ПК.2.8. Обеспечение мер по информационной безопасности сетевой инфраструктуры и ее компонентов*
- *ПК.2.9. Проведение анализа компонентов ИТ-инфраструктуры на наличие уязвимостей*
- *ПК.2.10. Проведение мониторинга и анализа инцидентов информационной безопасности*

В Рабочей тетради предлагаются к выполнению практические работы, предусмотренные рабочей программой ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами».

При разработке содержания практических работ учитывался уровень сложности освоения студентами соответствующей темы, общих и профессиональных компетенций, на формирование которых направлен ПМ.02.

Выполнение практических работ в рамках тем МДК.02.03. «Кибербезопасность» ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» позволяет получить опыт в поиске, анализе и предотвращении кибе-ратак, администрировании защищенных систем.

Рабочая тетрадь для выполнения практических заданий по МДК.02.03. «Кибербезопасность» ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» имеет практическую направленность и значимость. Формируемые в процессе их проведения умения могут быть использованы студентами в будущей профессиональной деятельности.

80-90 % заданий направлено на выполнение, моделирование обучающимися практических видов работ, связанных с будущей профессиональной деятельностью в условиях, приближенных к реальным производственным.

Рабочая тетрадь предназначена для студентов колледжа, изучающих темы МДК.02.03. «Кибербезопасность» ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» и может использоваться как на учебных занятиях, которые проводятся под руководством преподавателя, так и для самостоятельного выполнения практических работ, предусмотренных рабочей программой во внеаудиторное время.

Практические занятия проводятся в учебном кабинете, не менее двух академических часов, обязательным этапом является самостоятельная деятельность студентов.

Практические занятия в соответствии с требованием ФГОС включают такой обязательный элемент, как использование персонального компьютера.

Оценки за выполнение практических работ выставляются по пятибалльной системе. Оценки за практические работы являются обязательными текущими оценками по темам МДК.02.03. «Кибербезопасность» ПМ.02 «Защита информации в автоматизированных системах программными и программно-аппаратными средствами» и выставляются в журнале теоретического обучения.

1 ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ РАБОТ ПО ТЕМАМ МДК.02.03. «КИБЕРБЕЗОПАСНОСТЬ» ПМ.02 «ЗАЩИТА ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ»

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов	
				практических занятий	в форме практической подготовки
Тема 3.1	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7	Практическое занятие № 1. Установка и настройка Windows Server 2019	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7	Практическое занятие № 2. Установка контроллера домена. Использование Windows PowerShell для администрирования AD DS.	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7	Практическое занятие № 3. Установка ролей сервера Windows Server 2019	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 4. Подключение сетевых периферийных устройств через ГП	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 5. Установка и настройка сервера времени и сервера лицензирования	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 6. Управление пользовательским рабочим столом через ГП	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 7.Установка, настройка и устранение неполадок роли сервер	2	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов	
				практических занятий	в форме практической подготовки
Тема 3.2	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 8.Применение технологии DirectAccess с помощью мастера начальной настройки	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 9.Развертывание расширенной инфраструктуры DirectAccess	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 10. Внедрение VPN	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 11. Настройка шифрования и расширенного аудита	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 12. Использование службы развертывания	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 13. Внедрение управления обновлениями.	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие №14. Настройка файлового сервера	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 15. Настройка DHCP	2	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов	
				практических занятий	в форме практической подготовки
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 16. Настройка центра сертитификации	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 17. Настройка групповых политик	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 18. Добавление рабочих станций в домен	2	2
Тема 3.3.	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 19. Установка сервера Debian.	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 20. Настройка web-сервера в ОС Debian.	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 21. Настройка сервера DNS в ОС Debian.	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 22. Настройка сервера DHCP в ОС Debian.	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 23. Настройка файловых серверов в ОС Debian	2	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов	
				практических занятий	в форме практической подготовки
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 24. Настройка контейнеров Docker.	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 25. Установка сервера CentOS.	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 26. Настройка web-сервера в CentOS.	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 27. Настройка сервера DNS в CentOS.	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 28. Настройка сервера DHCP в CentOS.	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие №29. Установка и настройка OpenVPN	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие №30. Применение протокола IPsec и SSH.	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие №31. Настройка регистрации действий	2	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов	
				практических занятий	в форме практической подготовки
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 32. Установка и настройка OpenLDAP	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 33. Установка и настройка IPtables	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 34. Установка и базовая настройка Kali Linux	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 35. Администрирование Kali Linux	2	2
	З7, З11, З12 У11, У12, У13, У14	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие №36. Установка и настройка утилит в Kali Linux	2	2
Тема 3.4	З8-З11 У17-У19	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 37. Поиск уязвимостей информационных систем	2	2
	З8-З11 У17-У19	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 38. Применение антивирусной защиты	2	2
	З8-З11 У17-У19	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 39. Настройка безопасности веб-браузеров	2	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов	
				практических занятий	в форме практической подготовки
	З8-З11 У17-У19	ОК11-ОК11 ПК2.7, ПК 2.8	Практическое занятие № 40. Оценка рисков информационной безопасности с использованием классификации веб-угроз	2	2
Тема 3.5	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 41. Сканирование системы с помощью IP-сканера	2	2
	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 42. Сканирование системы с помощью CFI LanGuard	2	2
	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 43. Поиск открытых портов	2	2
	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 44. Сканирование сети с помощью NetScan	2	2
	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 45. «Сканирование сети с помощью Nessus Tool	2	2
	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 46. Сканирование сети с помощью Colasoft Packet Builder	2	2
	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 47. Сканирование устройства в сети с помощью Dude»	2	2

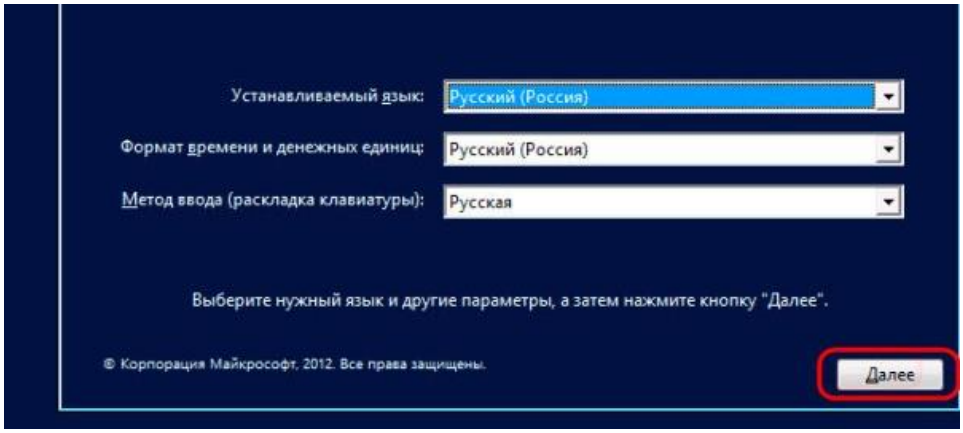
№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов	
				практических занятий	в форме практической подготовки
	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 48. Отображение сети с помощью Friendly Pinger	2	2
	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 49. Анализ уязвимостей серверов	2	2
	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 50. Поиск и устранение неисправностей сети с помощью MegaPing	2	2
Тема 3.6	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 51. Настройка межсетевого экрана	2	2
	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 52. Настройка параметров безопасности Windows.	2	2
	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 53. Составление рекомендаций по повышению уровня защищенности информационной инфраструктуры	2	2
Тема 3.7	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 54. Выявление предпосылок и обстоятельств, приведших к возникновению компьютерного инцидента.	2	2
	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 55. Обнаружение события информационной безопасности. Оценка события информационной безопасности	2	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов	
				практических занятий	в форме практической подготовки
Тема 3.8	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 56. Исследование открытой информации в поисковых системах	2	2
	З8-З11 У17-У19	ОК11-ОК11 ПК2.9, ПК 2.10	Практическое занятие № 57. Поиск информации в социальных сетях	2	2
	З8-З11 У17-У19	ОК11-ОК11 ПК2.8, ПК 2.10	Практическое занятие № 58. Поиск информации с помощью утилит	2	2

2 ОПИСАНИЕ ПОРЯДКА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

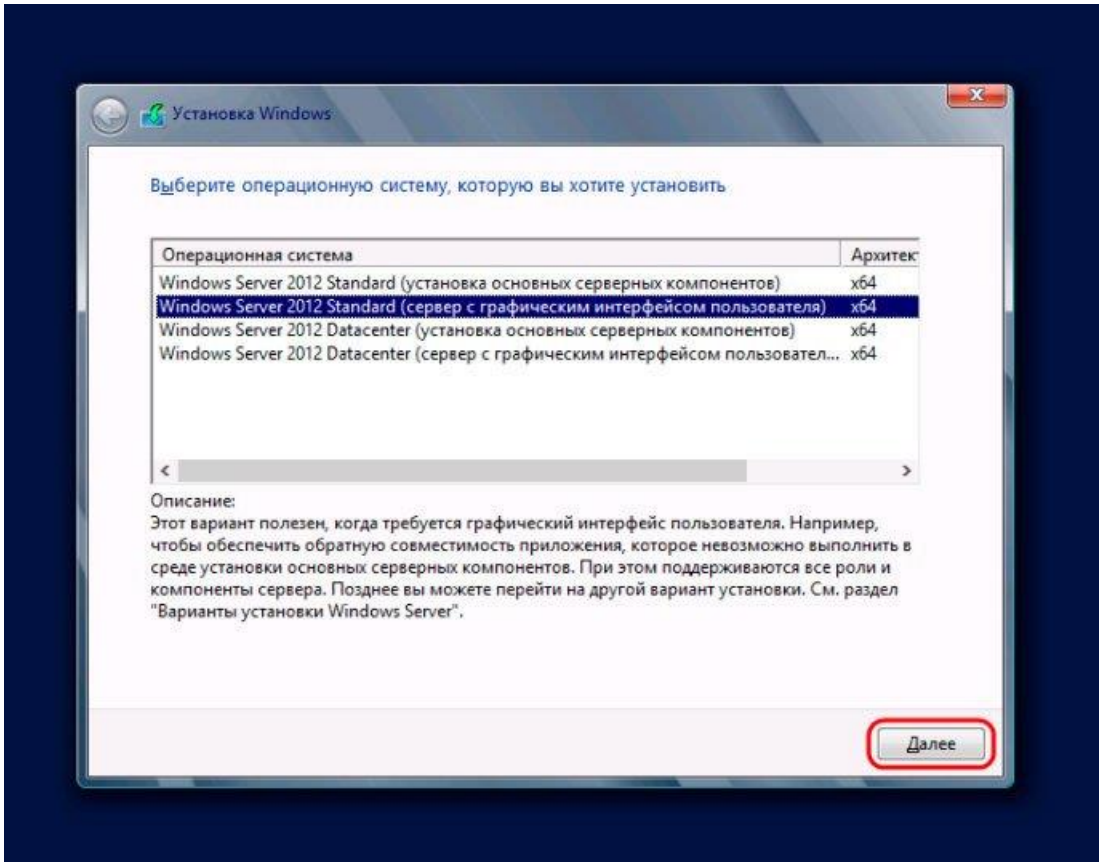
2.1 Практическое занятие № 1. Установка и настройка Windows Server 2019

Итак, загружаемся с нашего носителя. Видим такую табличку. В ней выбираем нужный язык. Потом жмем кнопку далее.

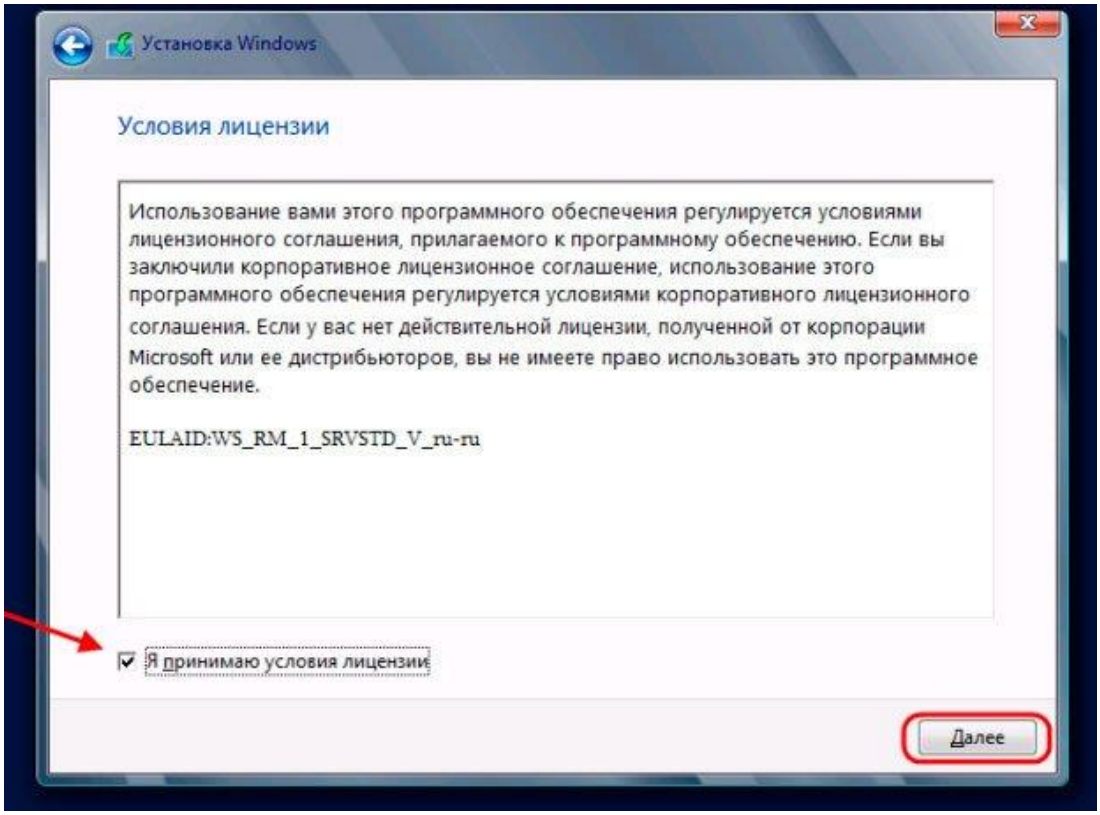


В следующем окне щелкаем кнопу установки.

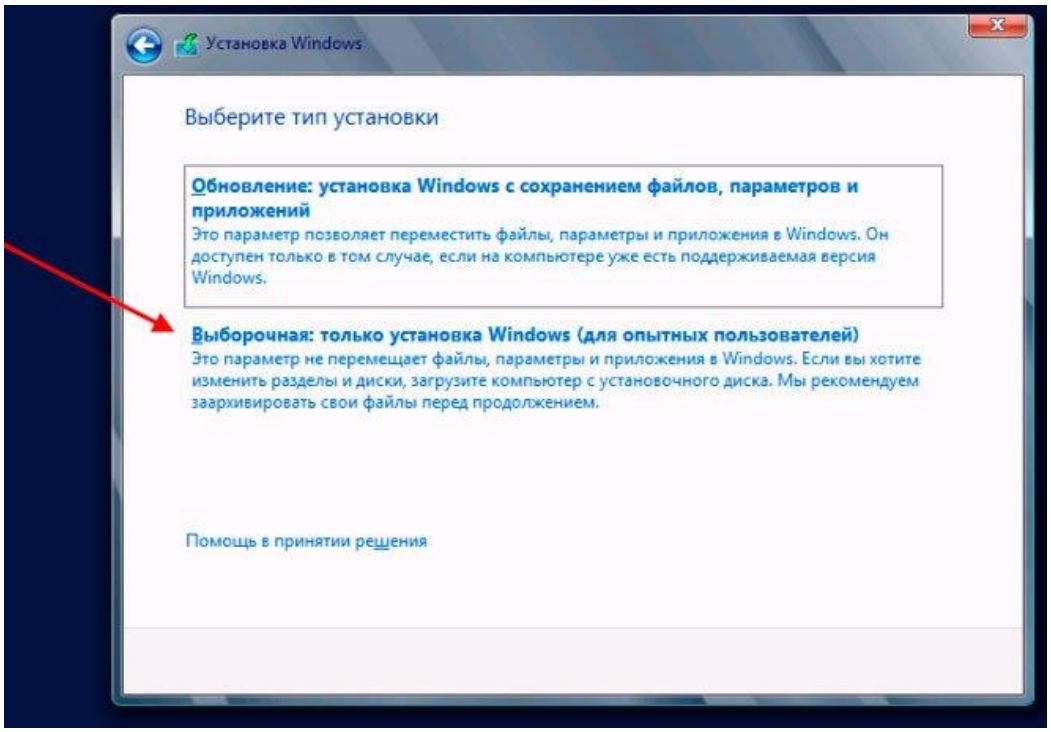
Теперь нужно определиться с разрядностью. Жмем далее.



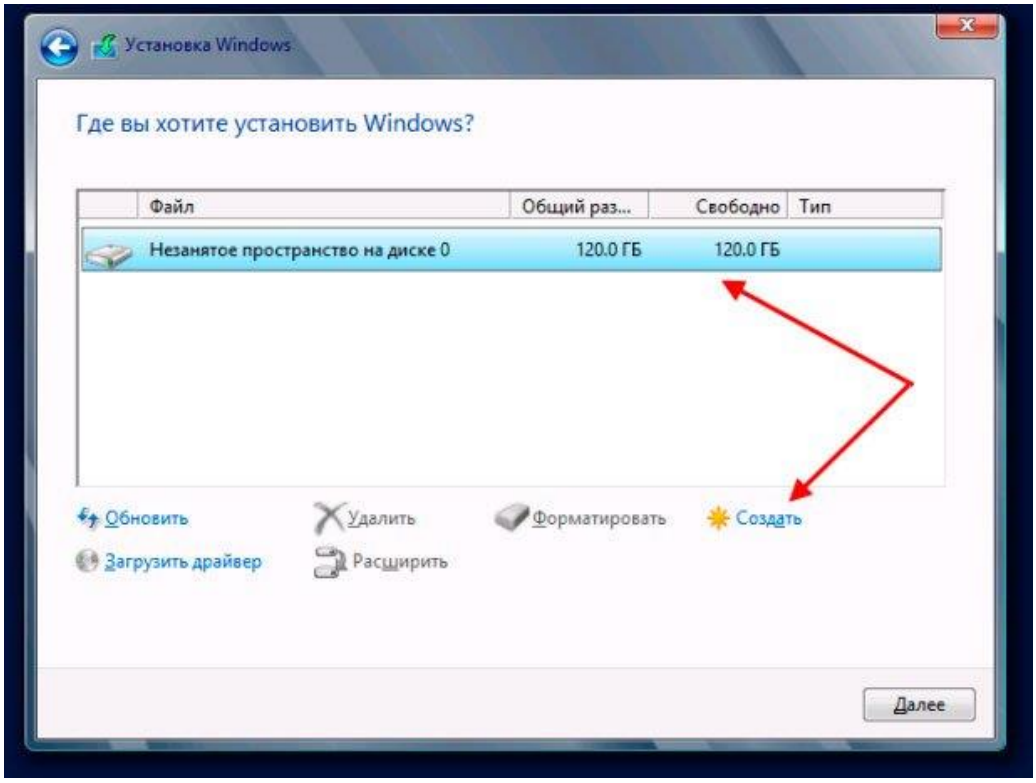
Теперь принимаем условия лицензии. Жмем на кнопку следующего этапа.



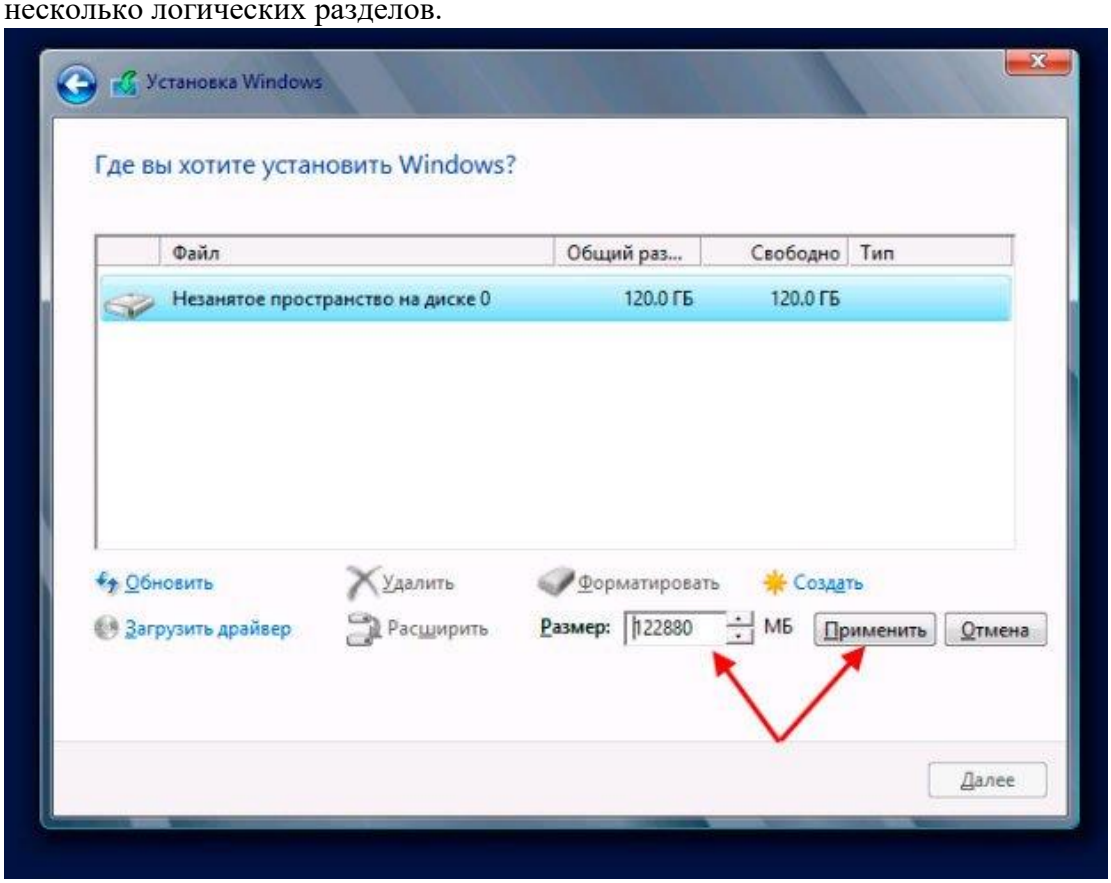
Далее, выбираем тип установки «Выборочная»



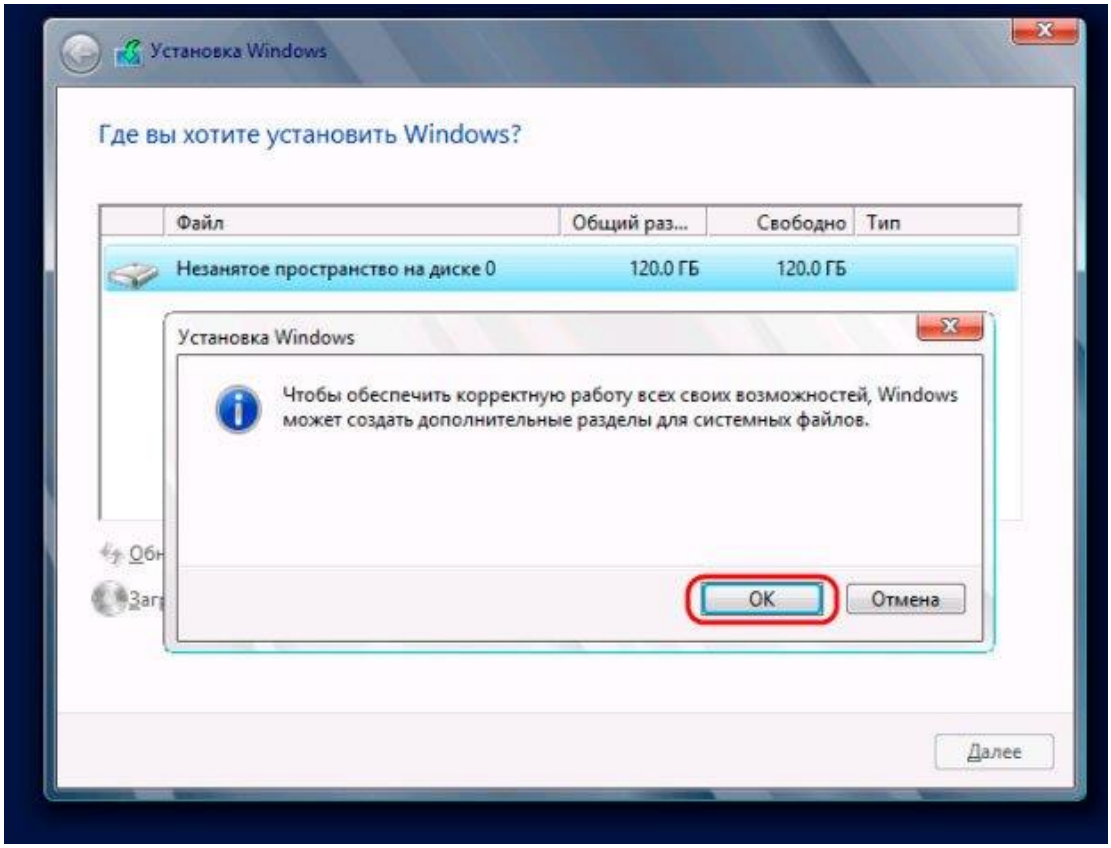
Теперь нужно разделиться диск. Изначально он будет выглядеть как полностью незанятое пространство. Выбираем его и жмем кнопку создать.



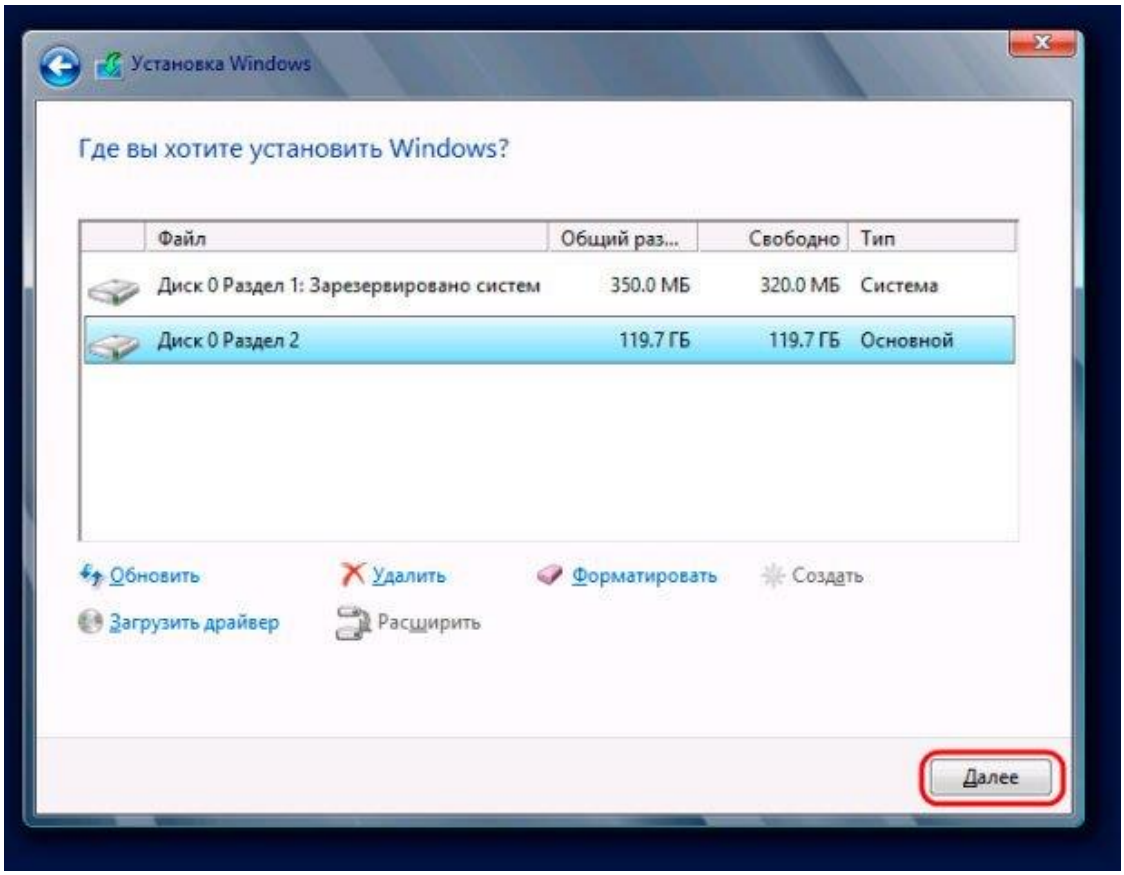
Ставим максимальный размер и создаем Локальный диск. Не стоит делить винчестер на несколько логических разделов.



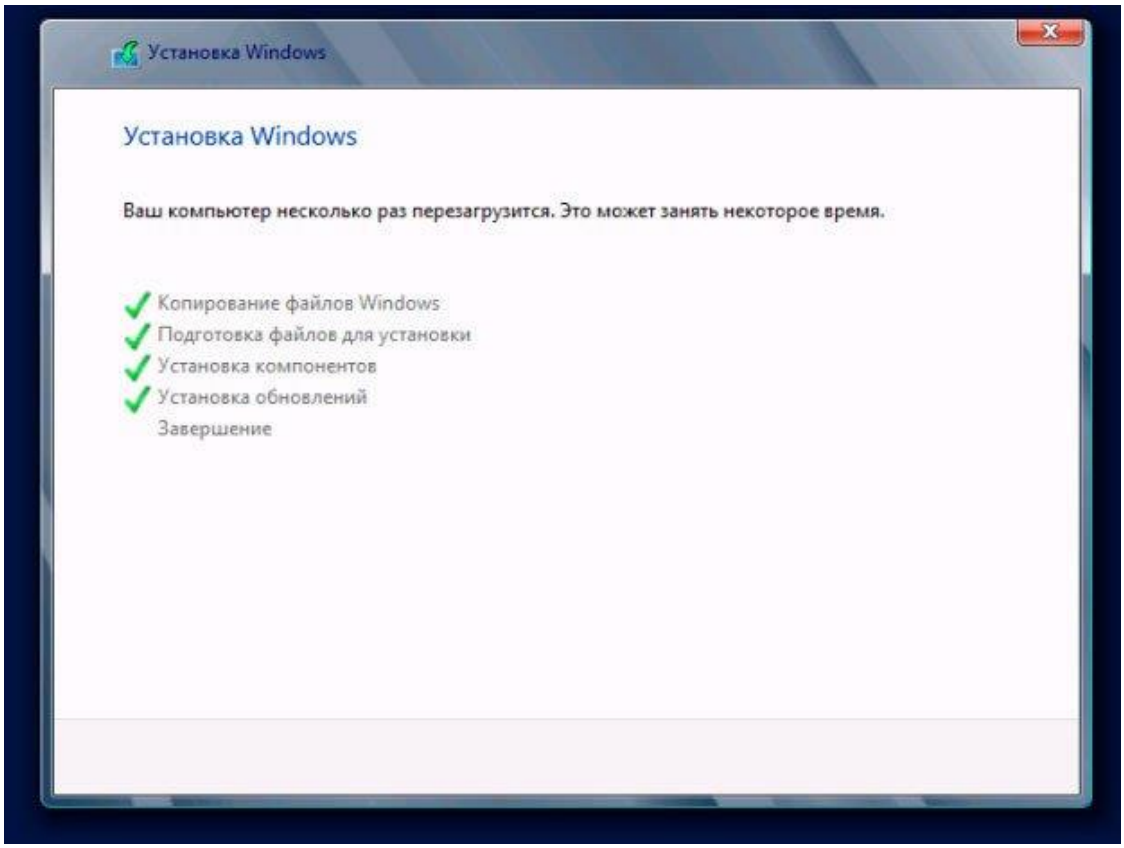
По завершению процесса выскочит табличка, в которой мы нажимаем ОК.



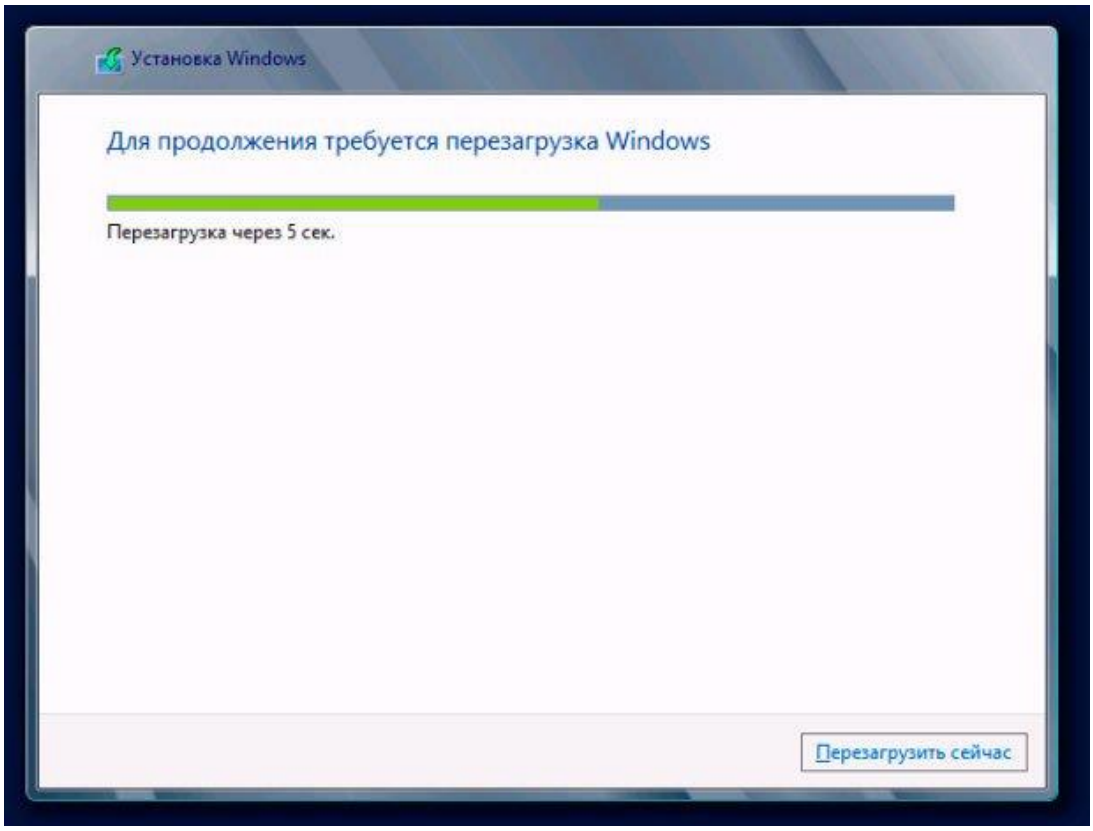
Опять жмем далее и переходим к следующему этапу.



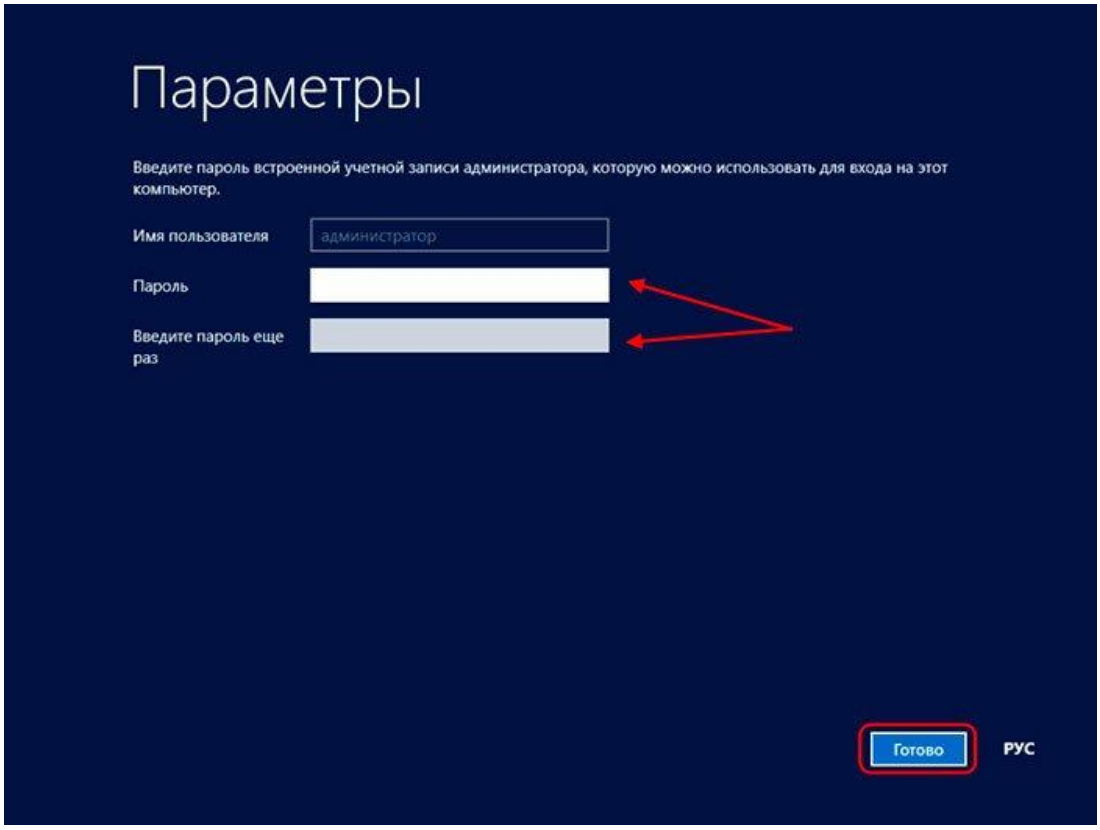
Дальше пойдет копирование файлов, их распаковка и установка. Дожидаемся окончания.



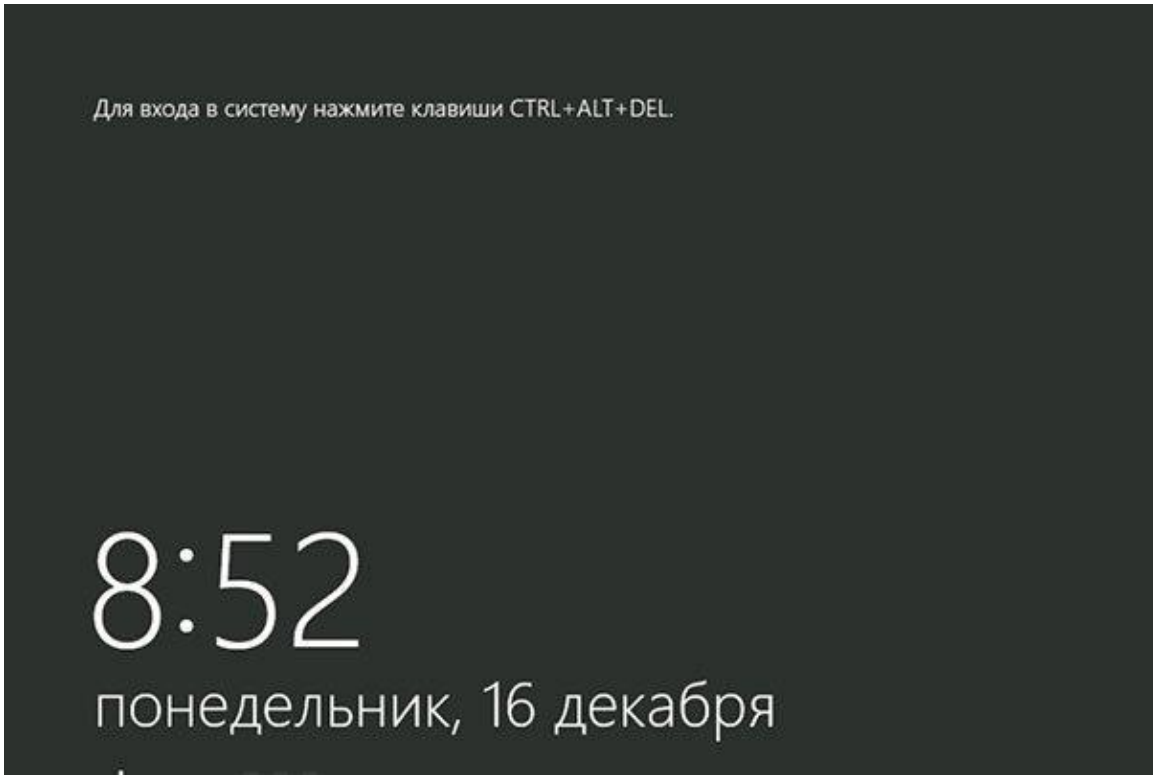
Появится таймер, компьютер уйдет в перезагрузку.



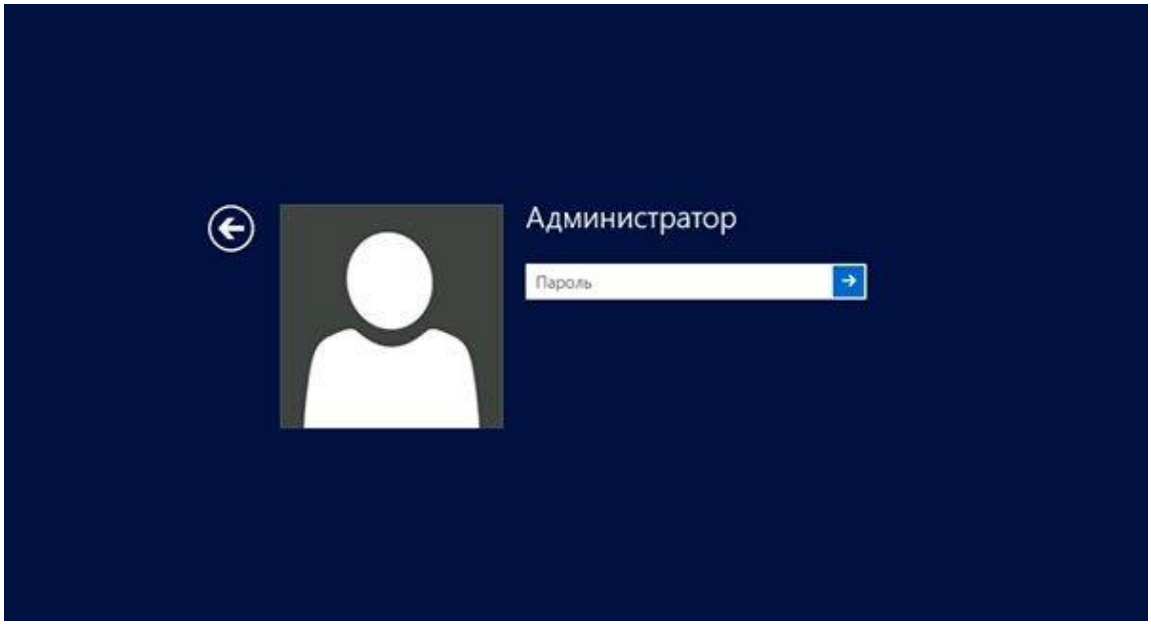
Дальше нам нужно назвать учетную запись и поставить пароль. После задания пароля нажмите на кнопку готово.



Следующие, что вы увидите – стартовое окно системы.



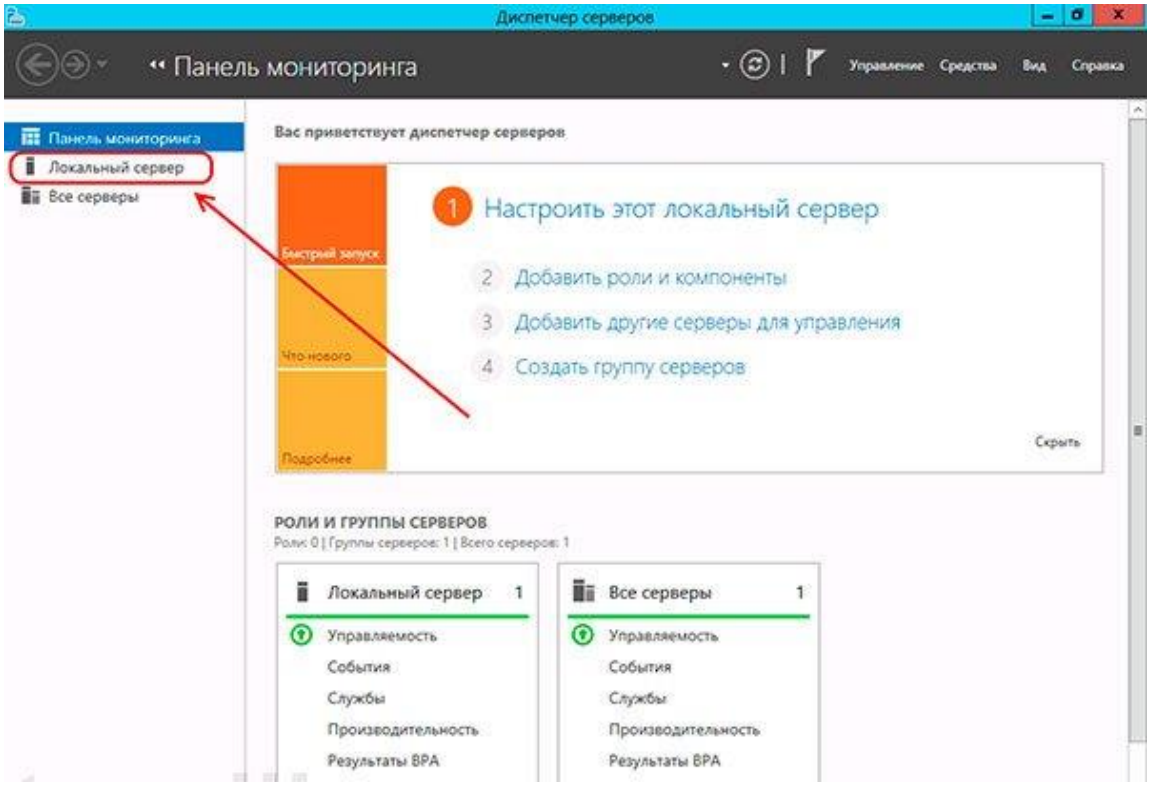
Вводим пароль, который устанавливали ранее. *Перепишите его в блокнот на всякий случай.*



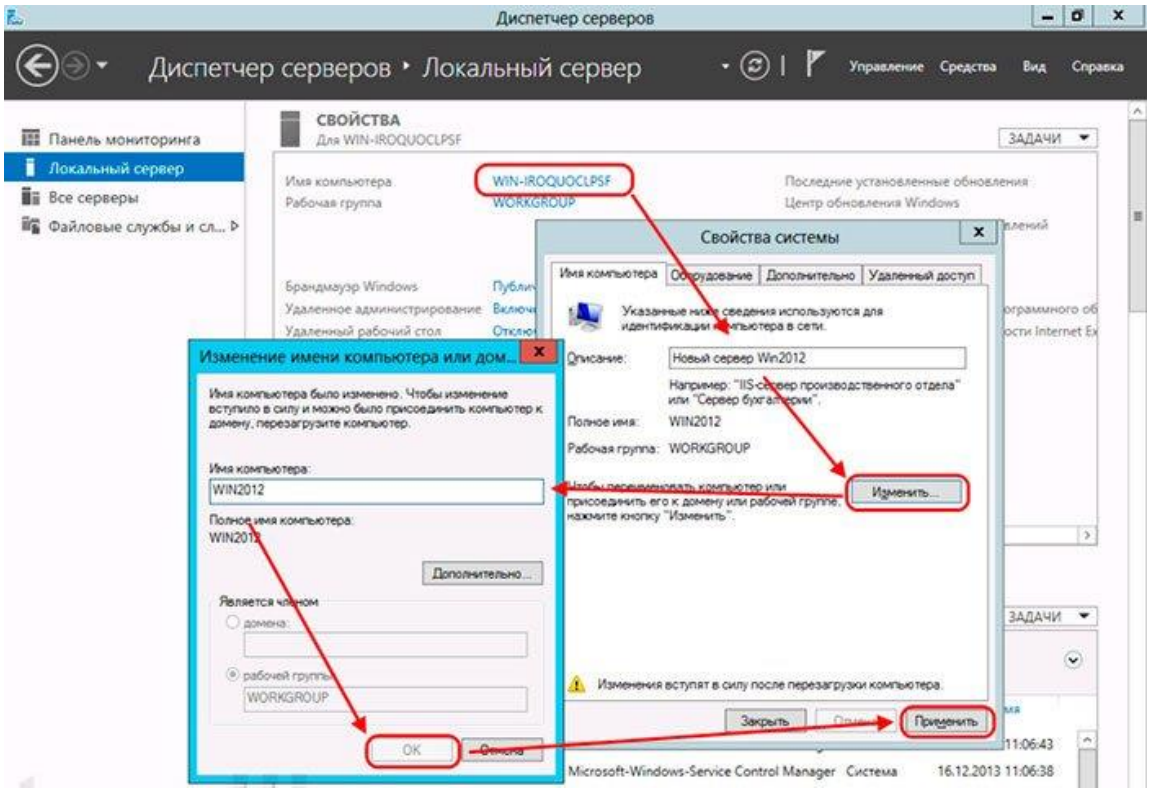
Установка завершена.

1. **Настройка**

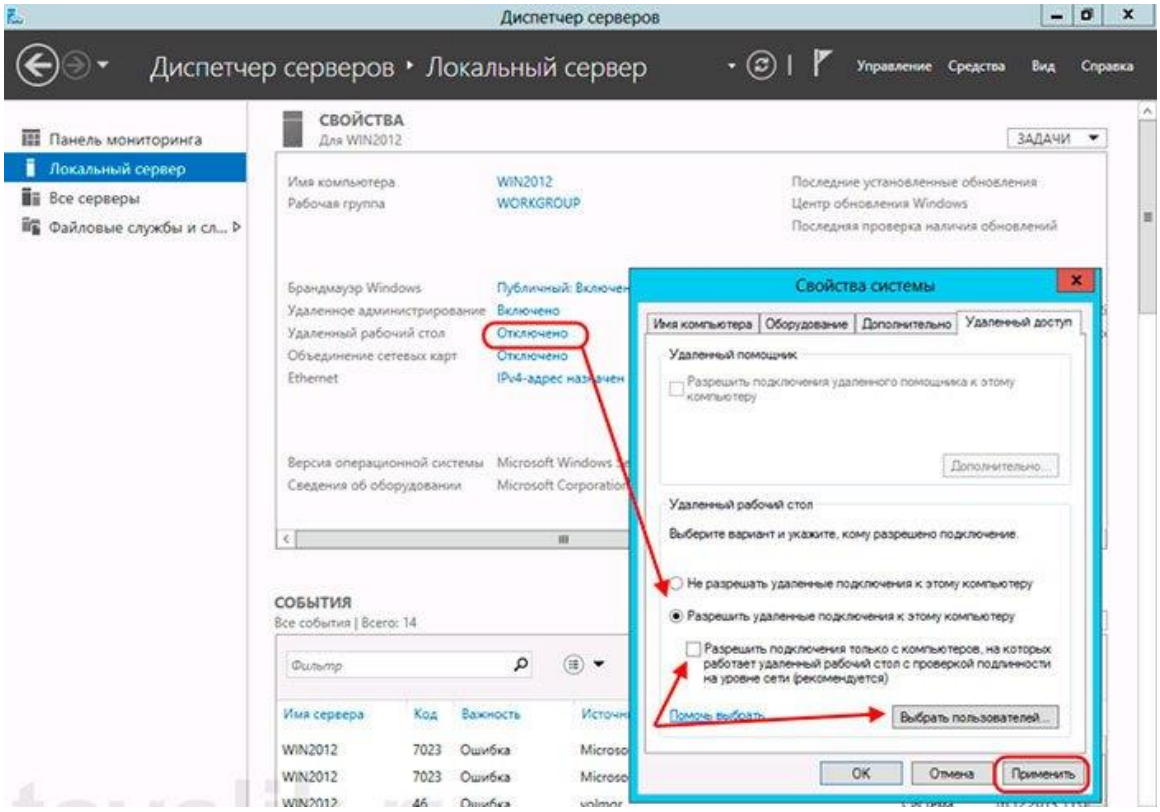
Проведем оптимизацию и настройку. Заходим в панель монитора и выбираем там локальный сервер.



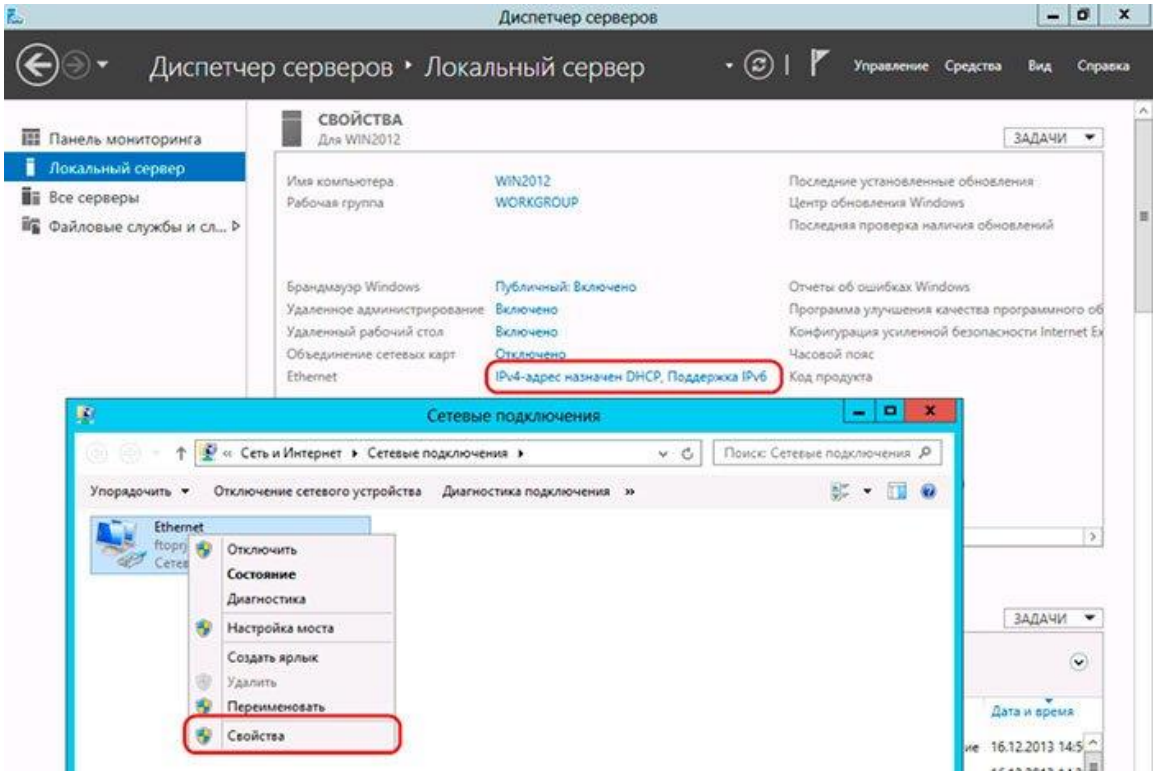
Нажимаем на имя компьютера, в самом верху. В открывшейся табличке меняем его. Далее нажимаем кнопку Изменить. В открывшемся окне вписываем новое имя, затем нажимаем ОК и жмем Применить.



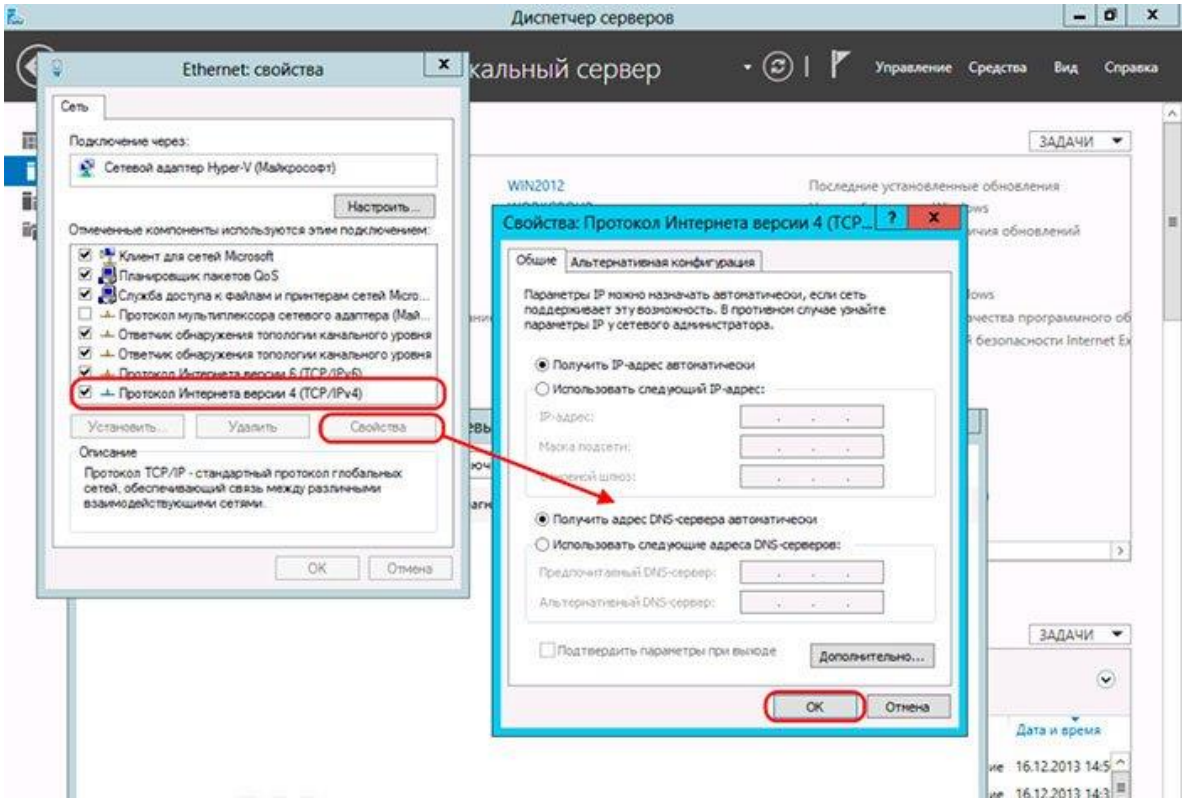
Теперь, в строчке удаленного рабочего стола нажимаем на параметр отключено, в новом окне выбираем **Разрешить удаленные подключения к этому компьютеру**. Дальше ставим галочку снизу, далее выбираем пользователя, которому разрешено удаленное подключение, и нажимаем кнопку Применить.



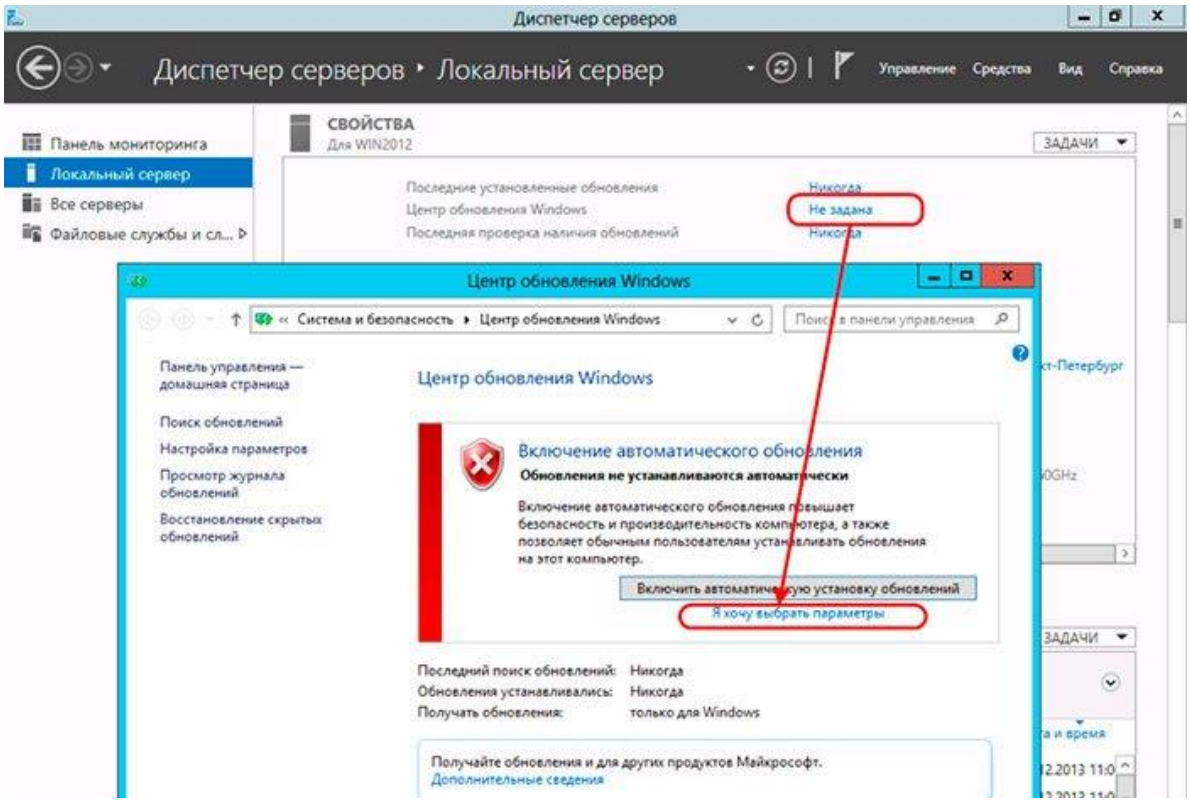
Теперь идем в параметры сетевых подключений. На адаптере жмем правой кнопкой мыши и открываем Свойства.



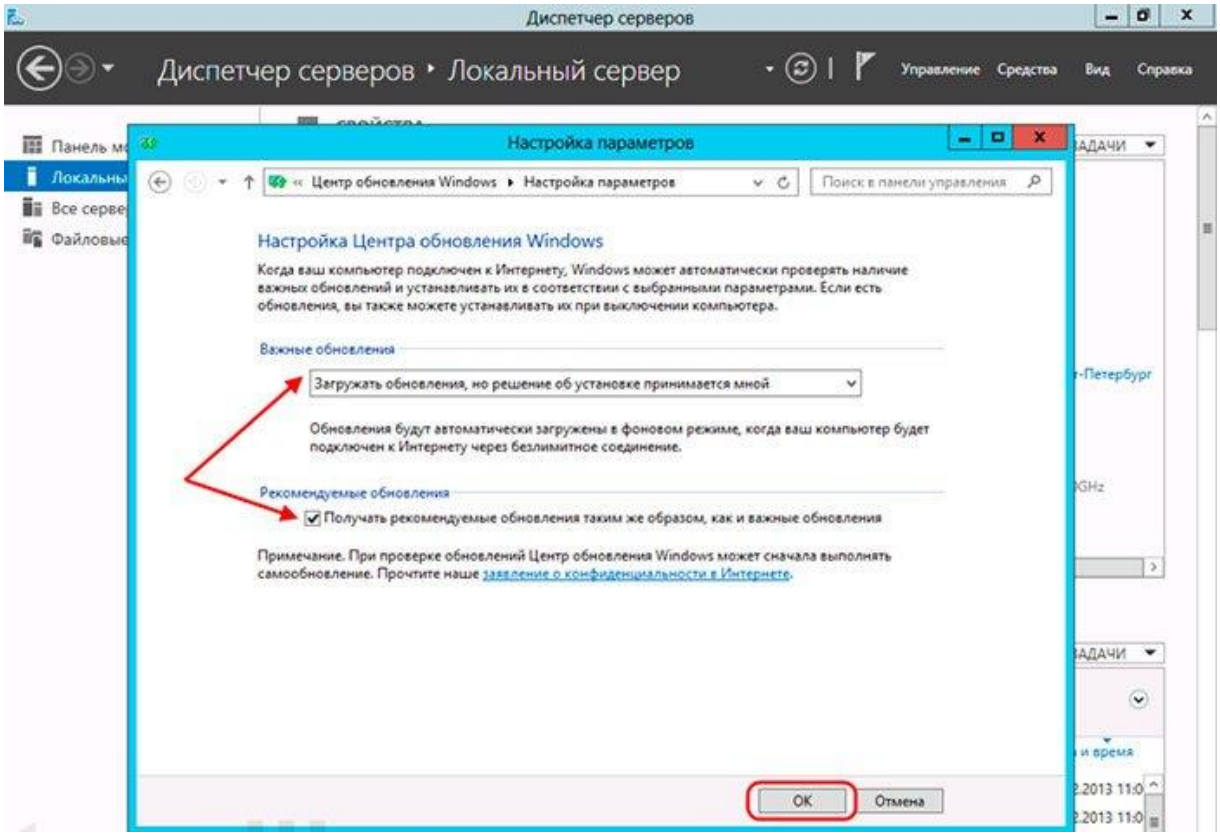
В строке протокола интернета четвертой версии ставим галку, нажимаем Свойства и выставляем параметры под автоматическое получение всех необходимых параметров.



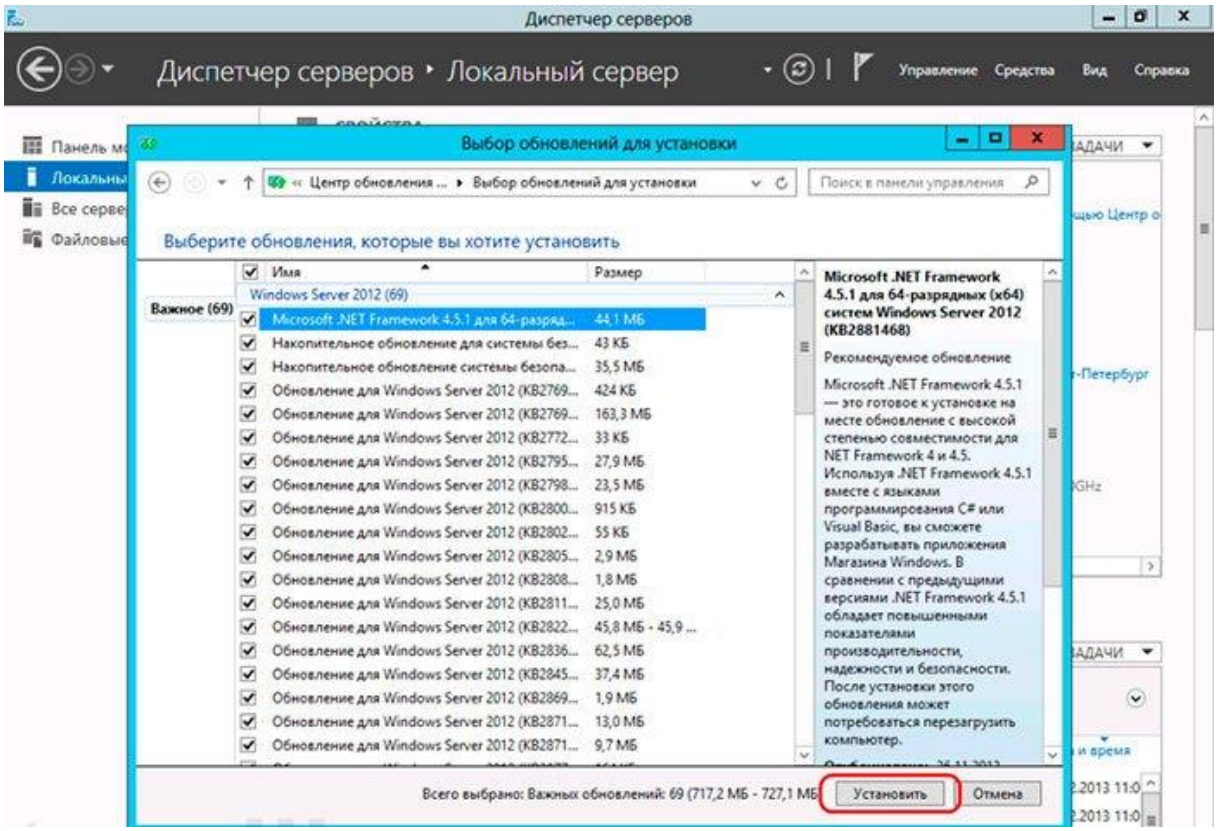
Далее, в предыдущем главном окне видим строчку центра обновления с отключенными параметрами. Щелкаем на синюю ссылку, переходим в сам центр и включаем функцию.



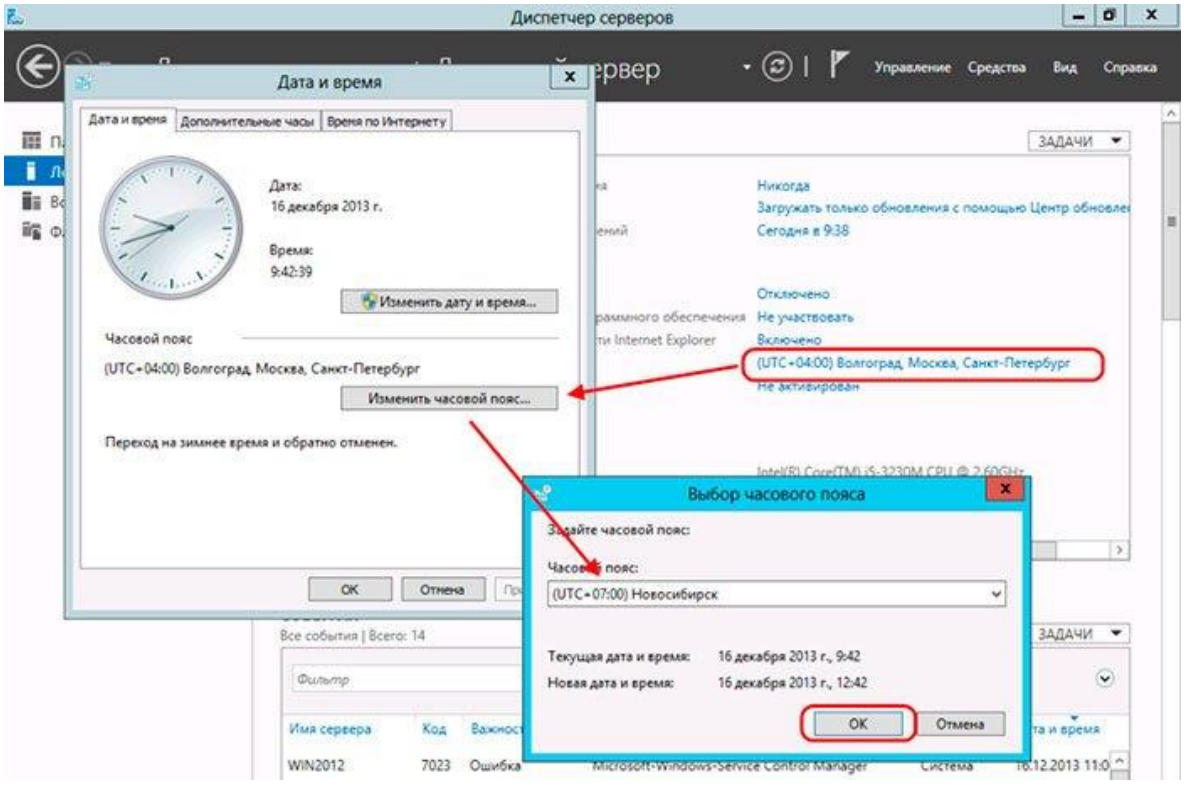
Выставляем на загрузку всех данных с уведомлением пользователя, ниже ставим галку как на рисунке и жмем ОК.



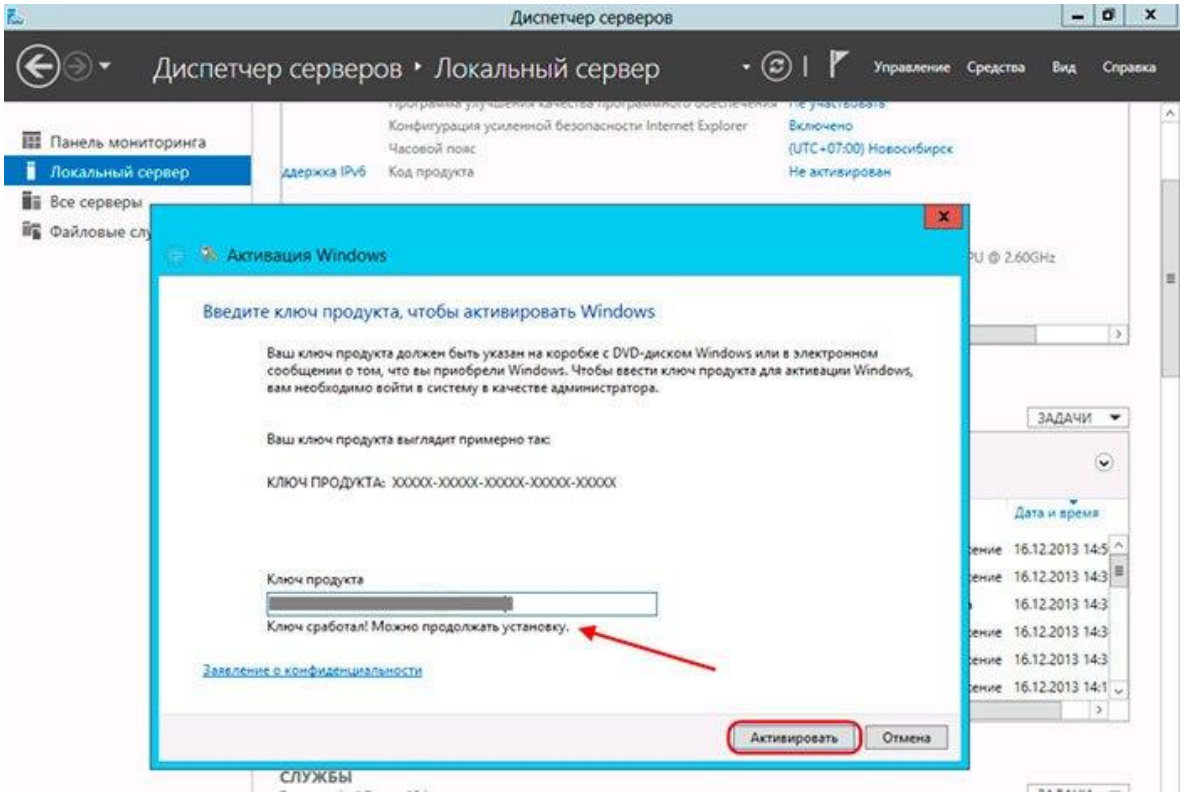
Как только система скачает обновления, она выведет их список.



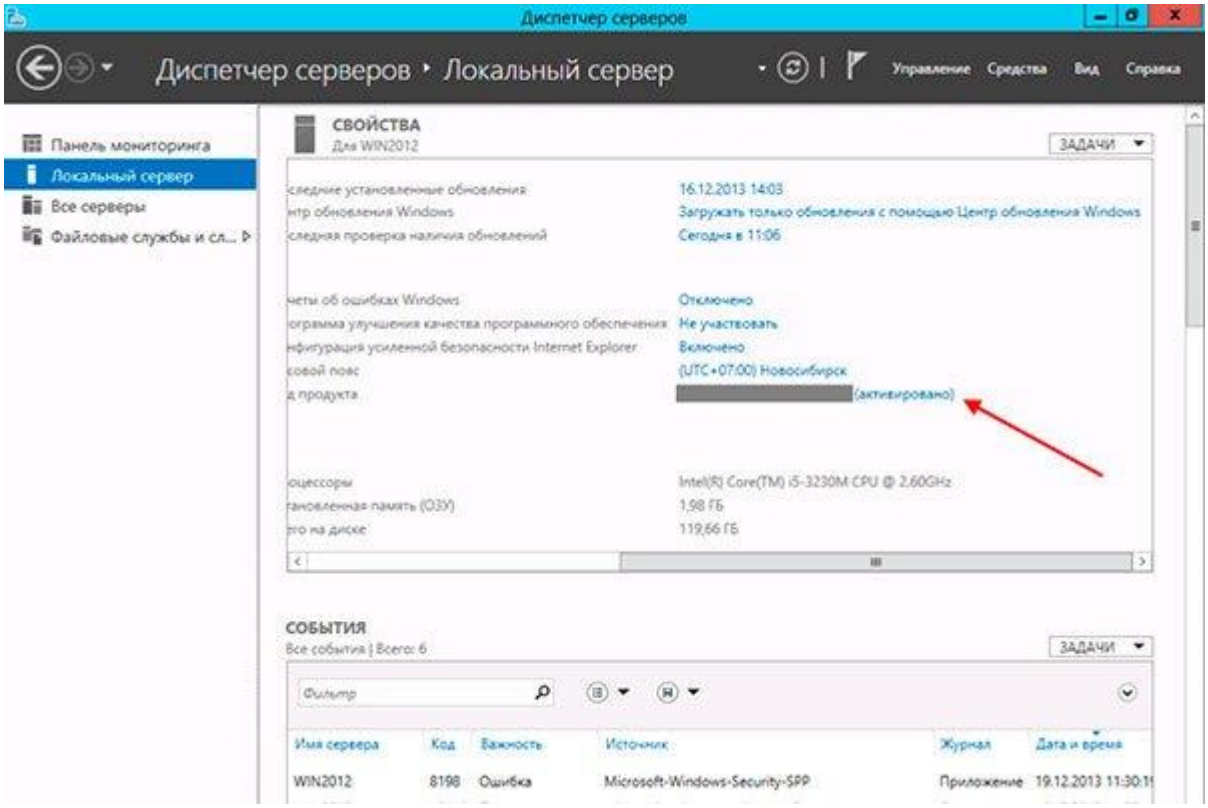
Теперь, в поле с часовым поясом нажимаем левой кнопкой мыши и настраиваем часы. Как только все готово – жмем ОК.



Далее вбиваем ключ продукта.



После активации должна появиться вот такая вот надпись.



Наша операционная система полностью готова к использованию.

Практическое занятие № 2. Установка контроллера домена. Использование Windows PowerShell для администрирования AD DS.

Задание: установить контроллер домена, настроить базовые параметры

1. Настройка имени сервера и статического IP-адреса

1.1 Откройте **Пуск > Компьютер (пр. кнопкой мыши) > Свойства** (Рис.1).

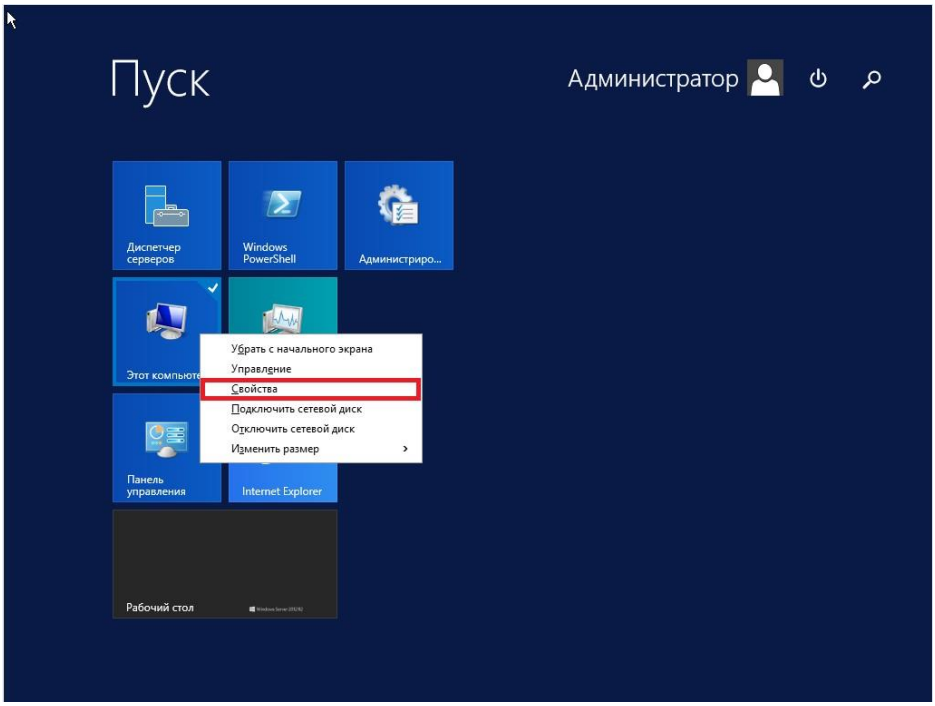


Рис. 1

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

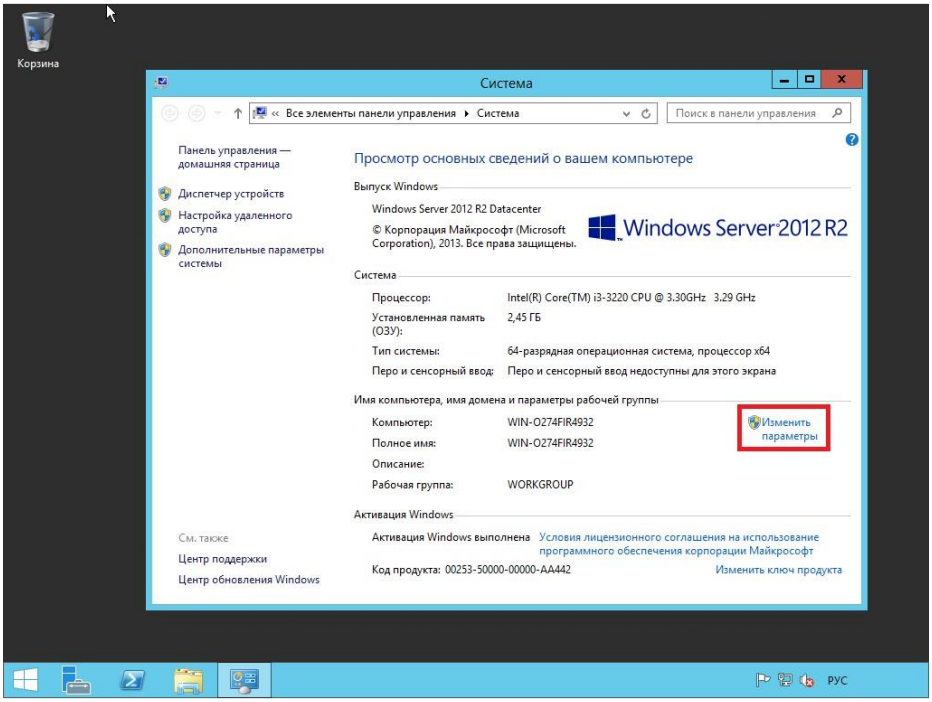


Рис. 2

1.3 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**.

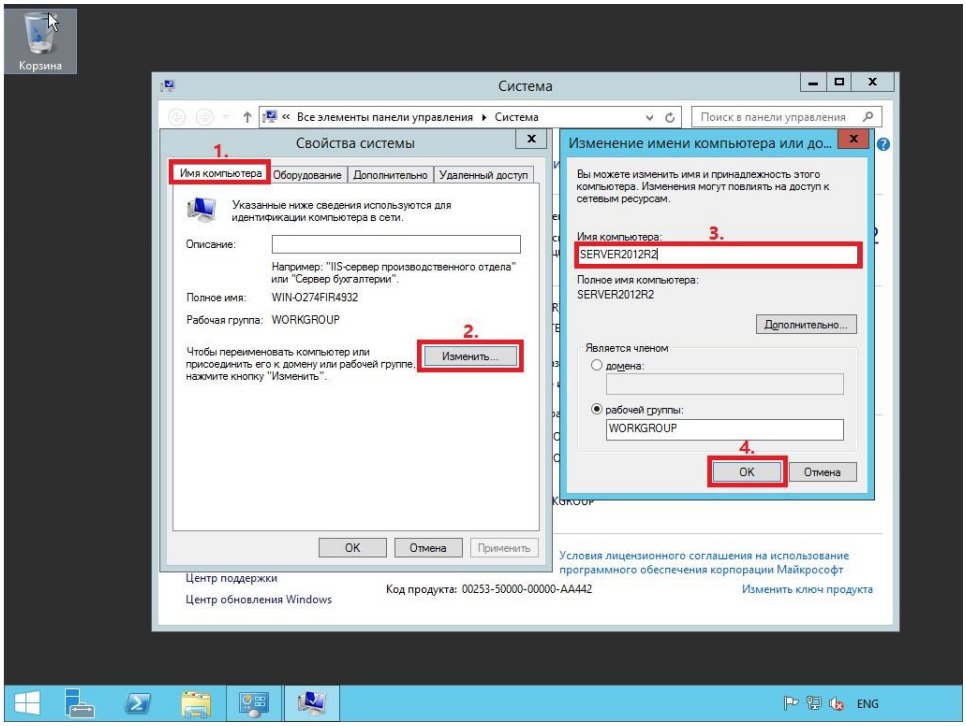
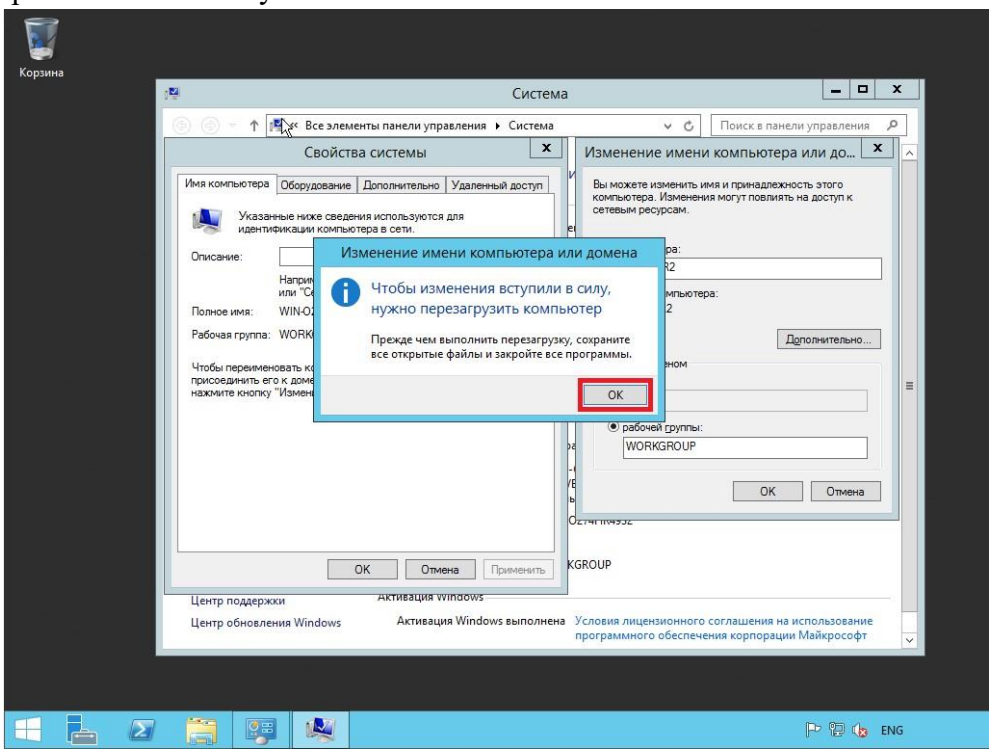


Рис. 3

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



1.5

Рис. 4

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

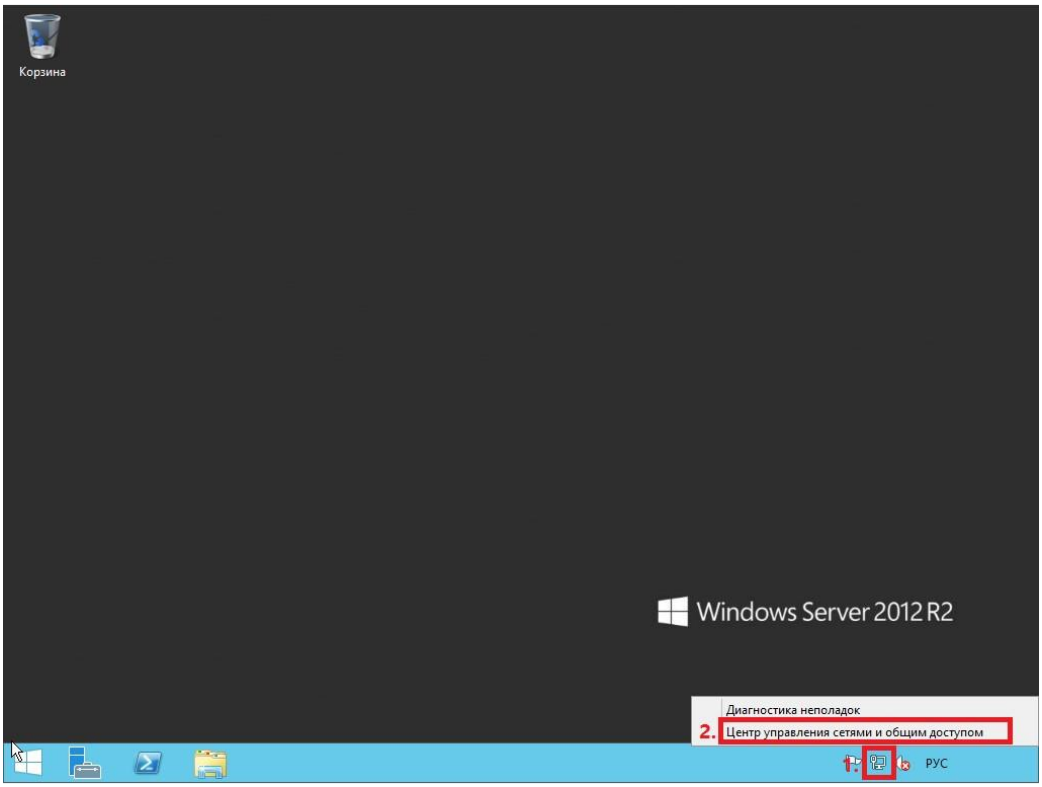


Рис. 5

1.7 В открывшемся окне выберите **Изменение параметров адаптера**

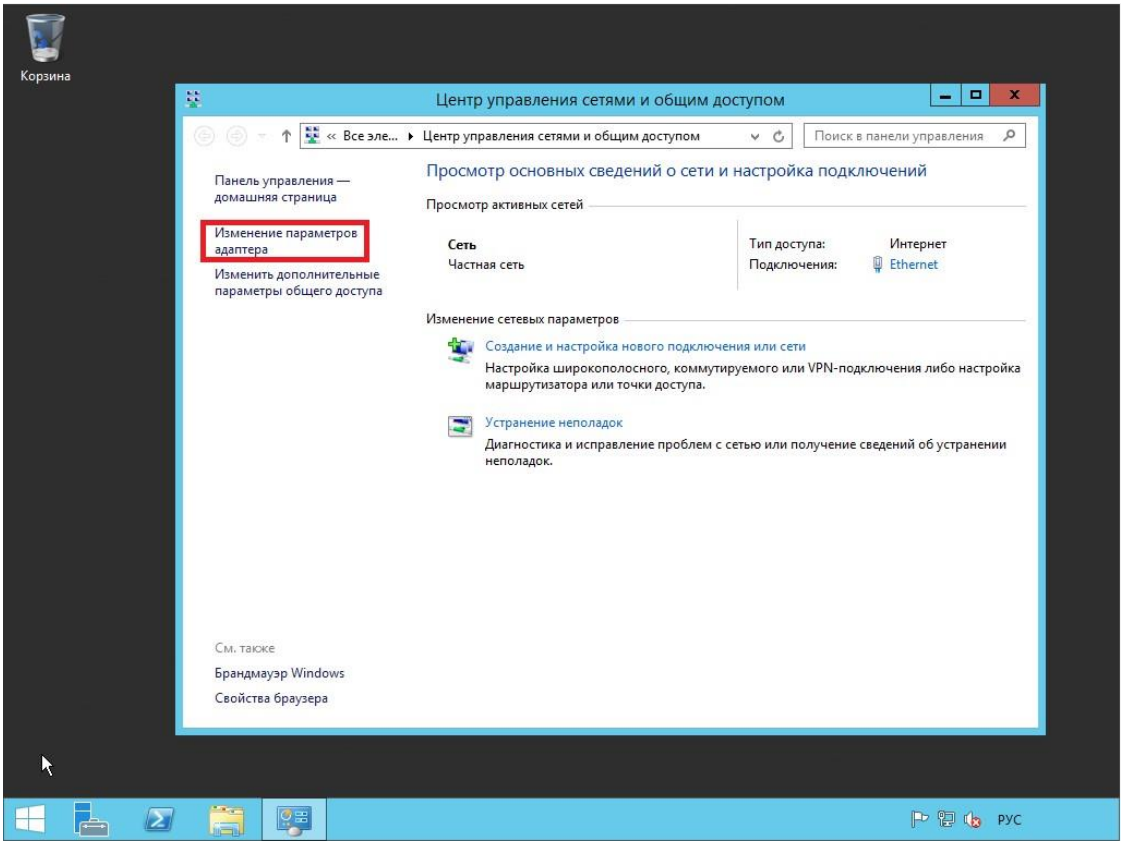


Рис. 6

1.8 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**

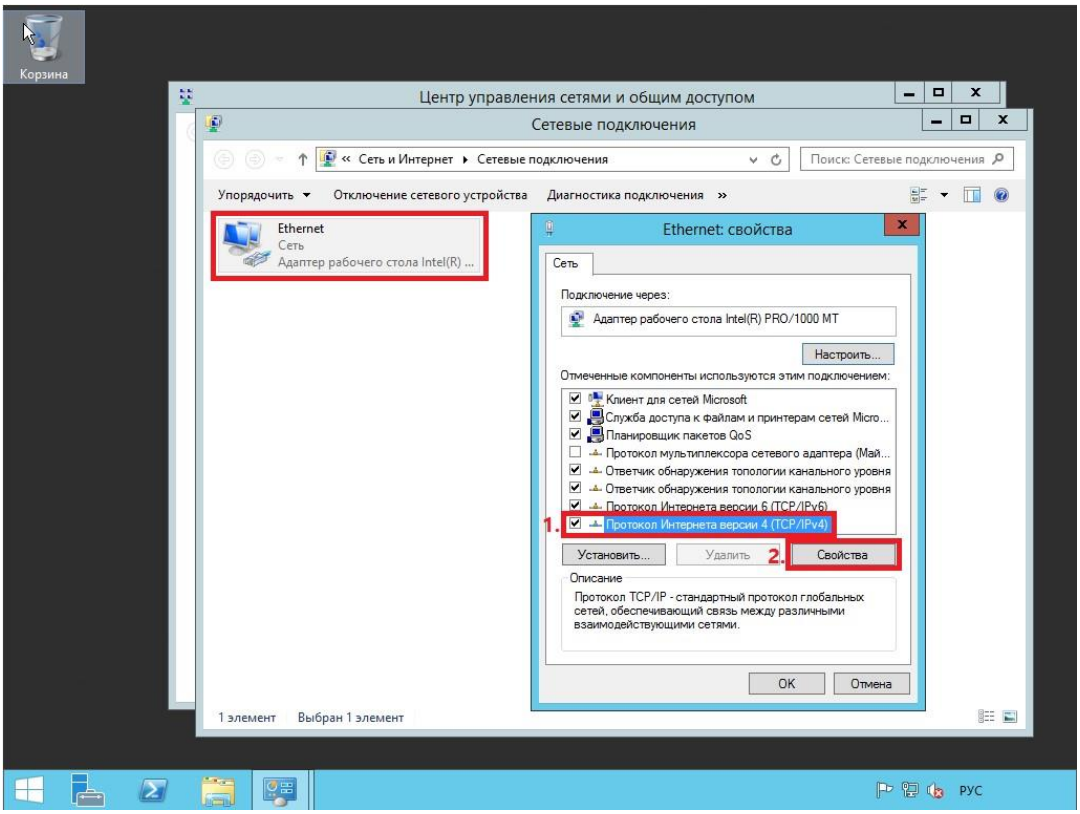


Рис. 7

1.9 В свойствах, на вкладке Общие выберите пункт **Использовать следующий IP-адрес**. В соответствующие поля введите **свободный IP-адрес**, **маску подсети** и **основной шлюз**. Затем выберите пункт **Использовать следующие адреса DNS-серверов**. В поле **предпочитаемый DNSсервер** введите **IP-адрес сервера**, после чего нажмите **ОК**.

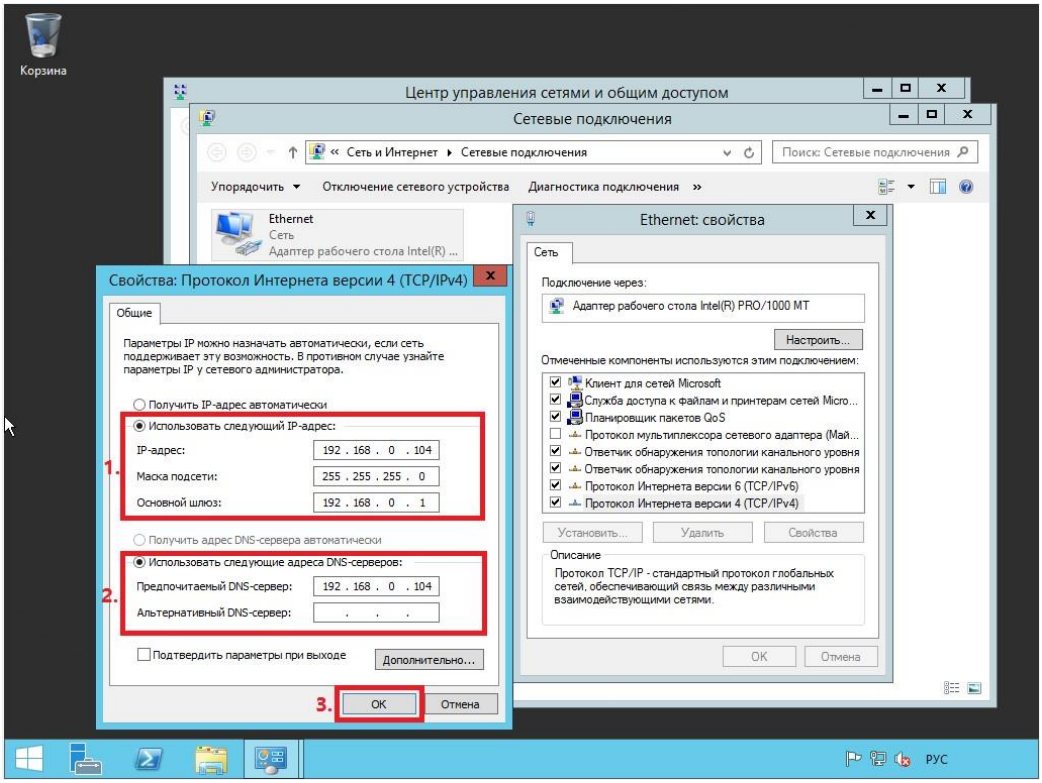


Рис. 8

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

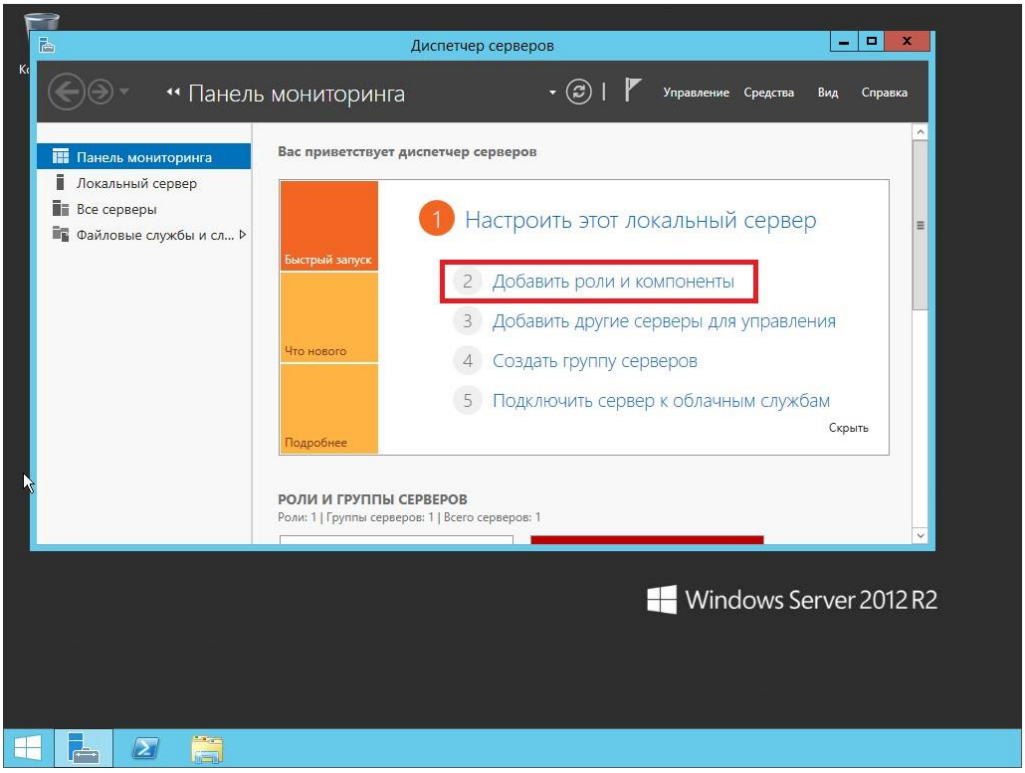


Рис. 9

2.2 В появившемся окне нажмите **Далее**

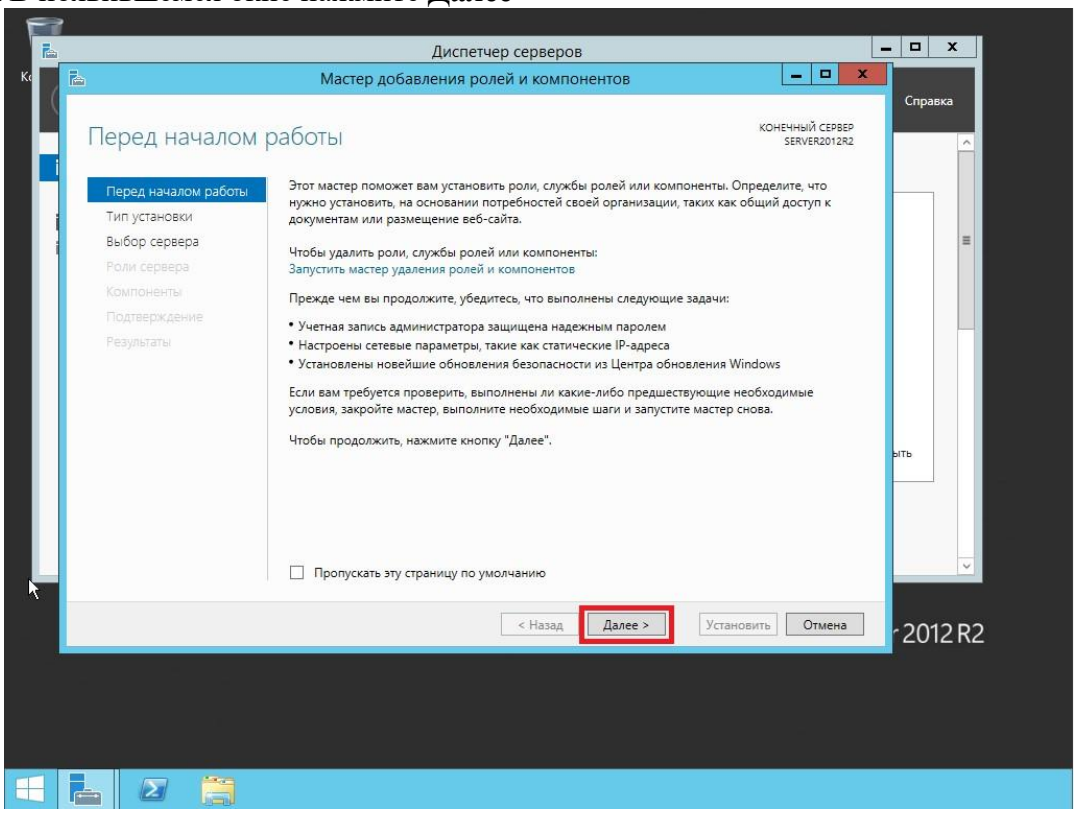


Рис. 10

2.3 Выберите пункт **Установка ролей и компонентов**, затем нажмите **Далее**

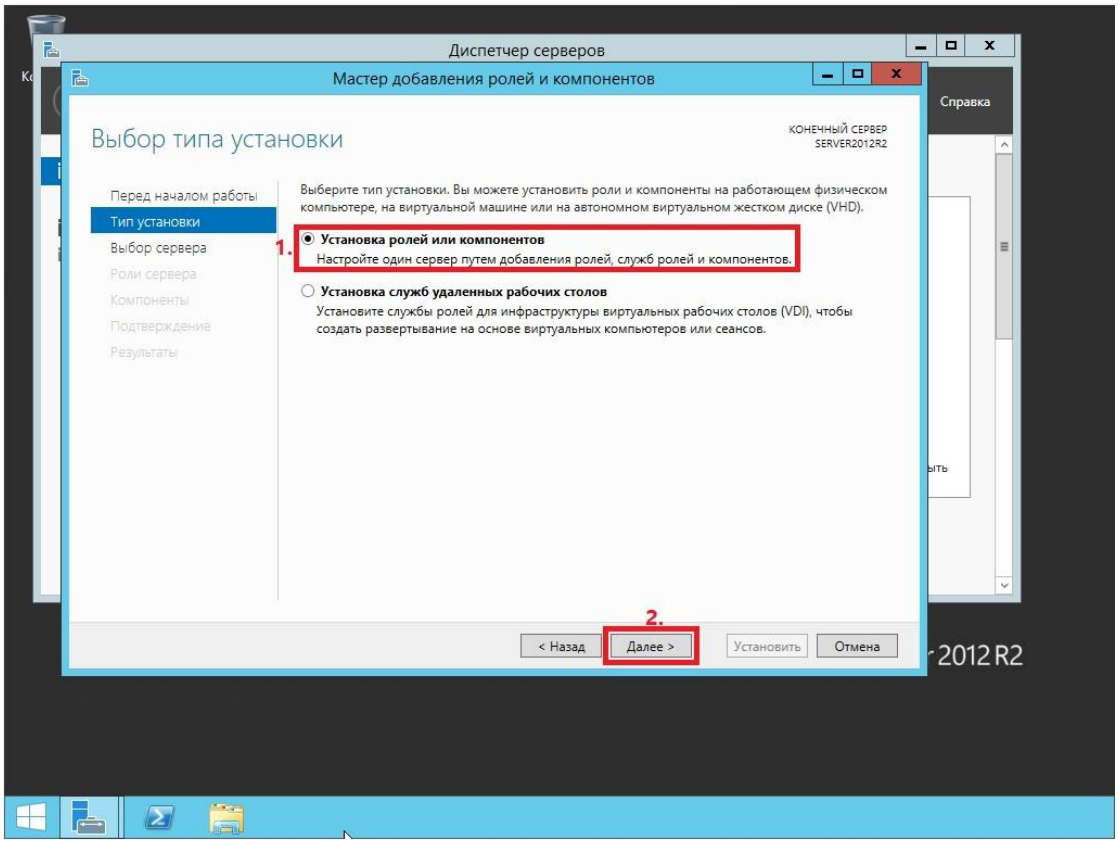


Рис. 11

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

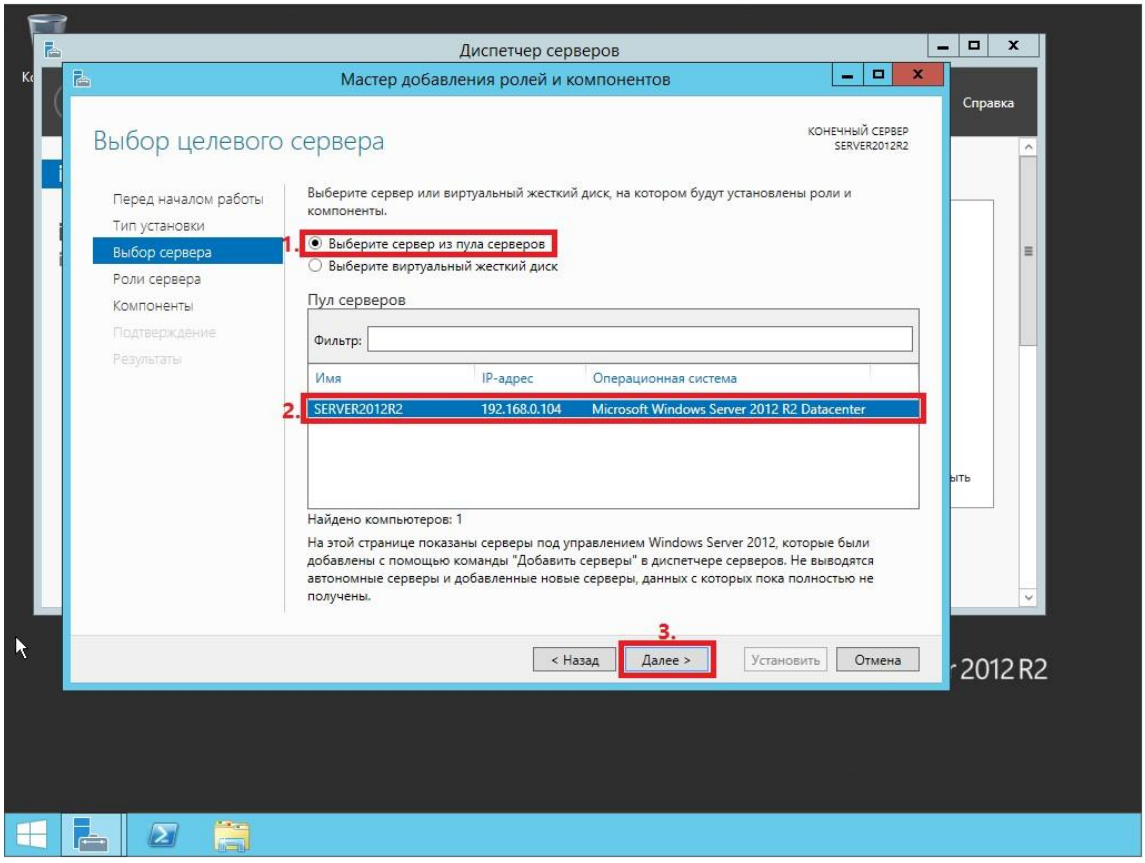


Рис. 12

2.5 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**

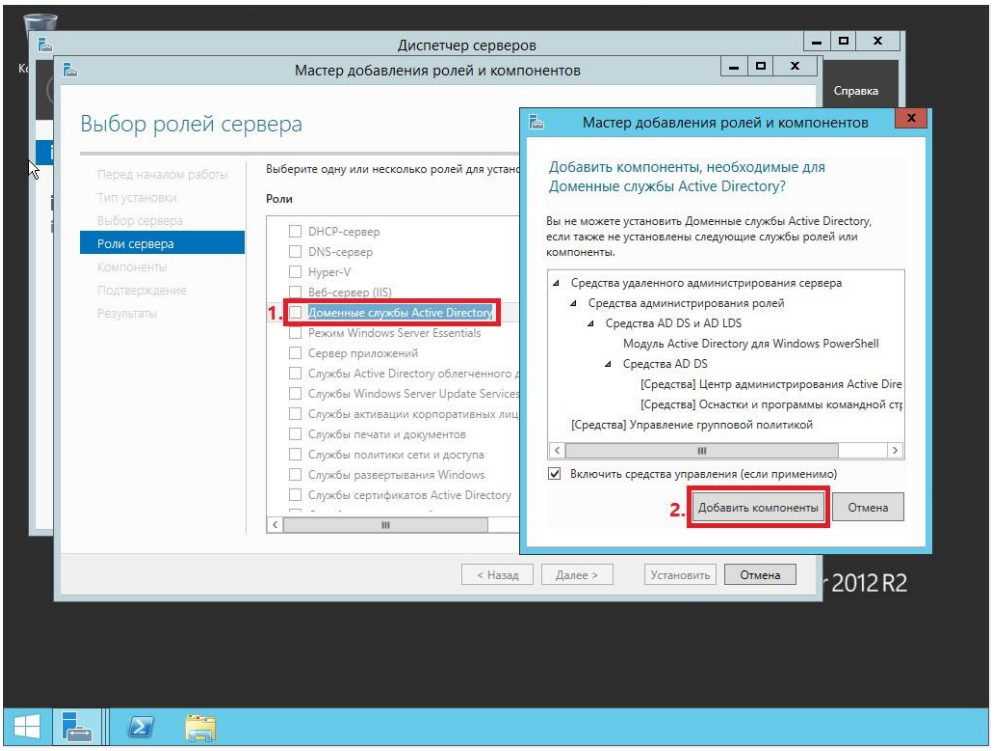


Рис. 13

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

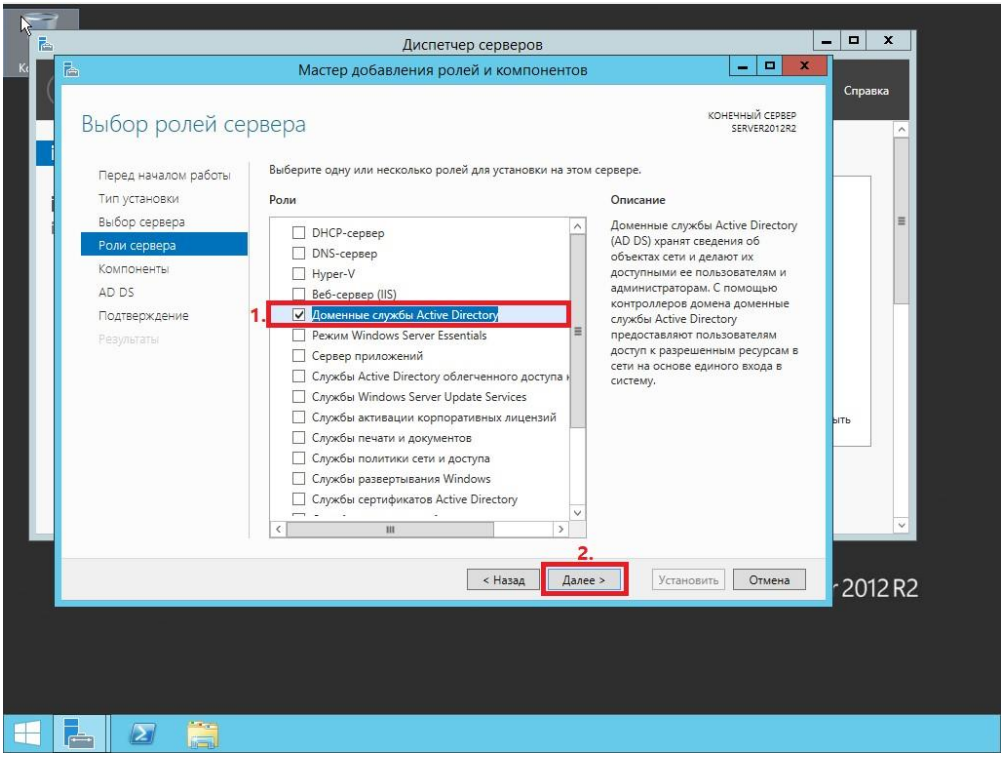


Рис. 14

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

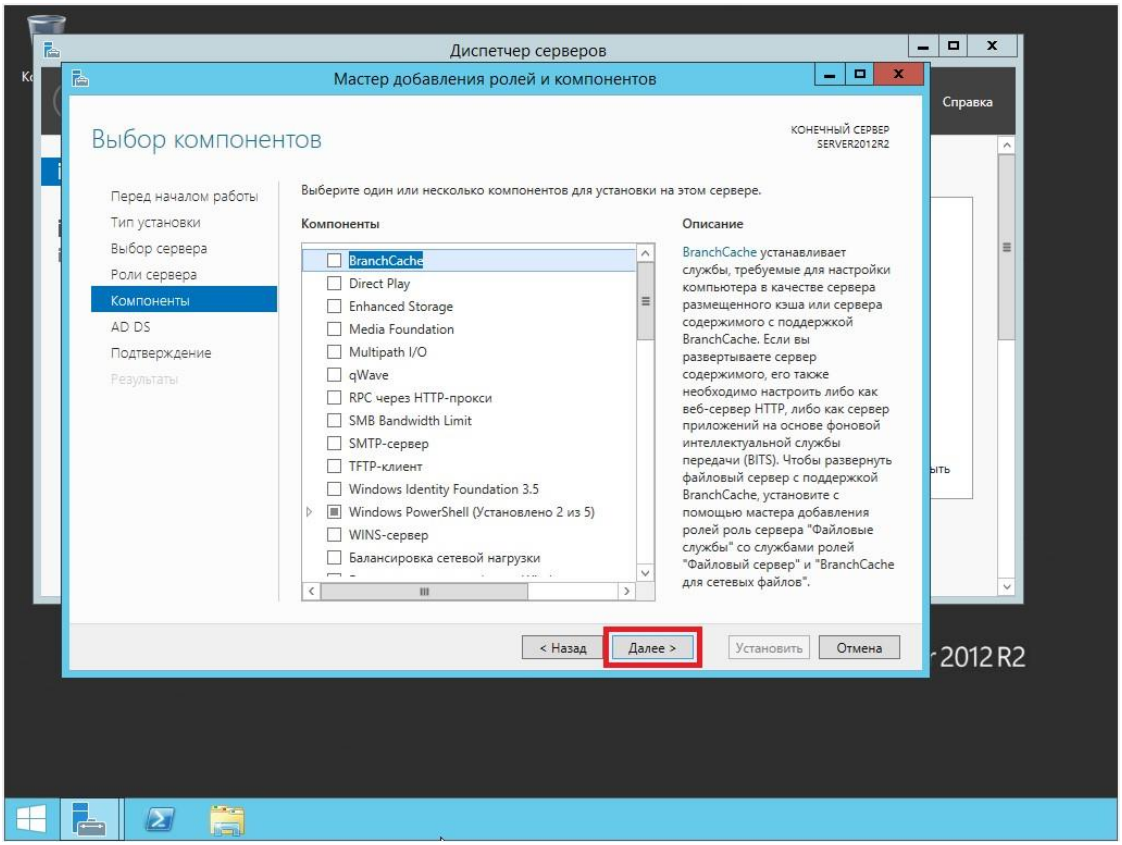


Рис. 15

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

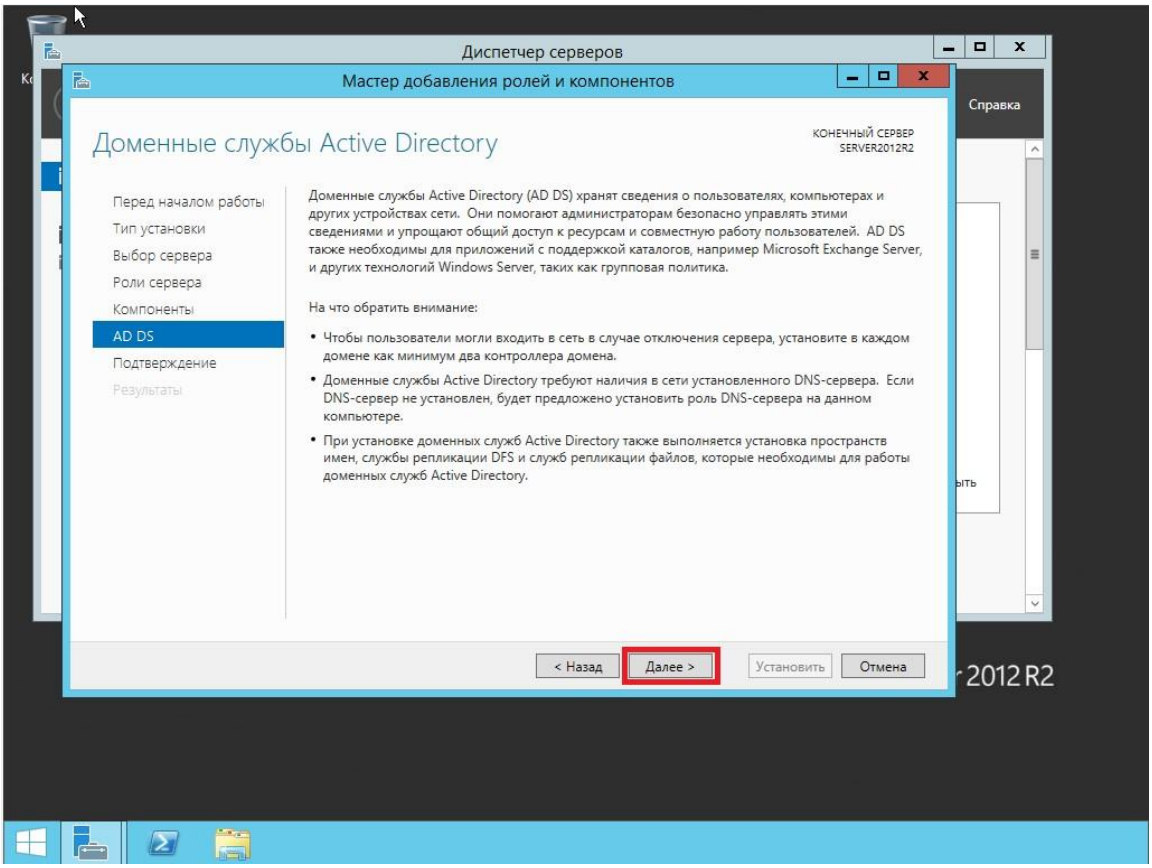


Рис. 16

2.9 Для начала установки роли нажмите **Установить**

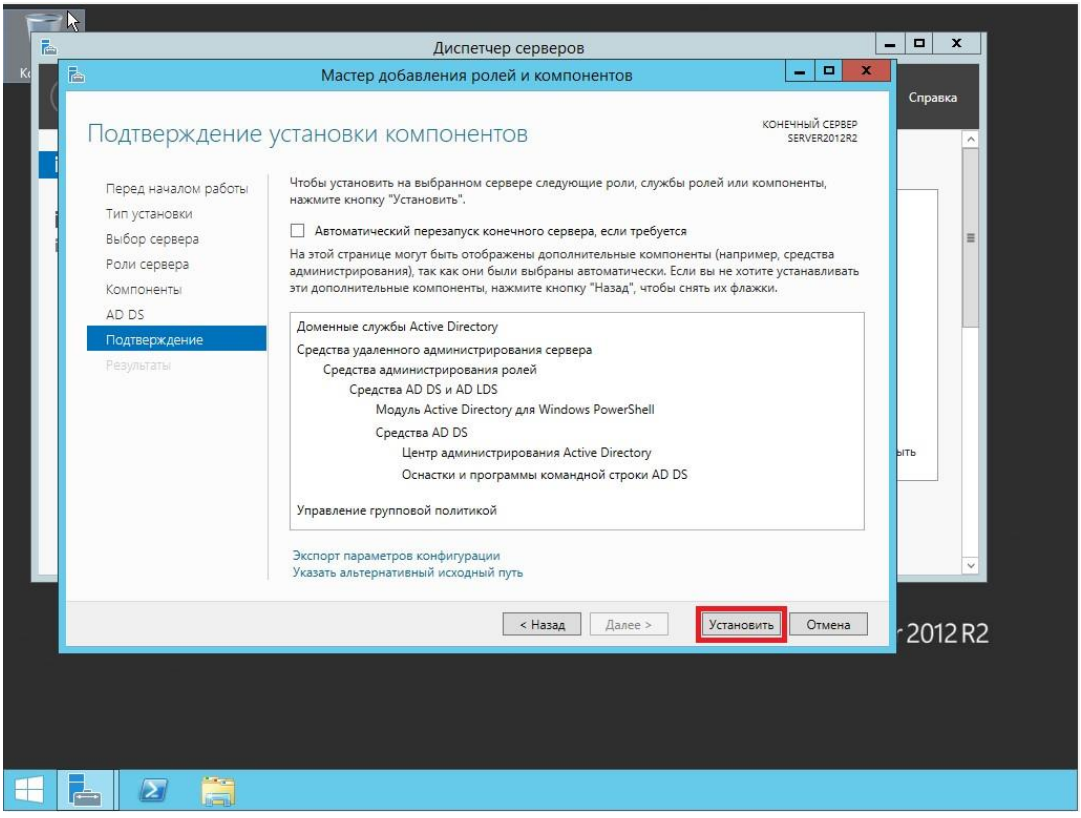


Рис. 17

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

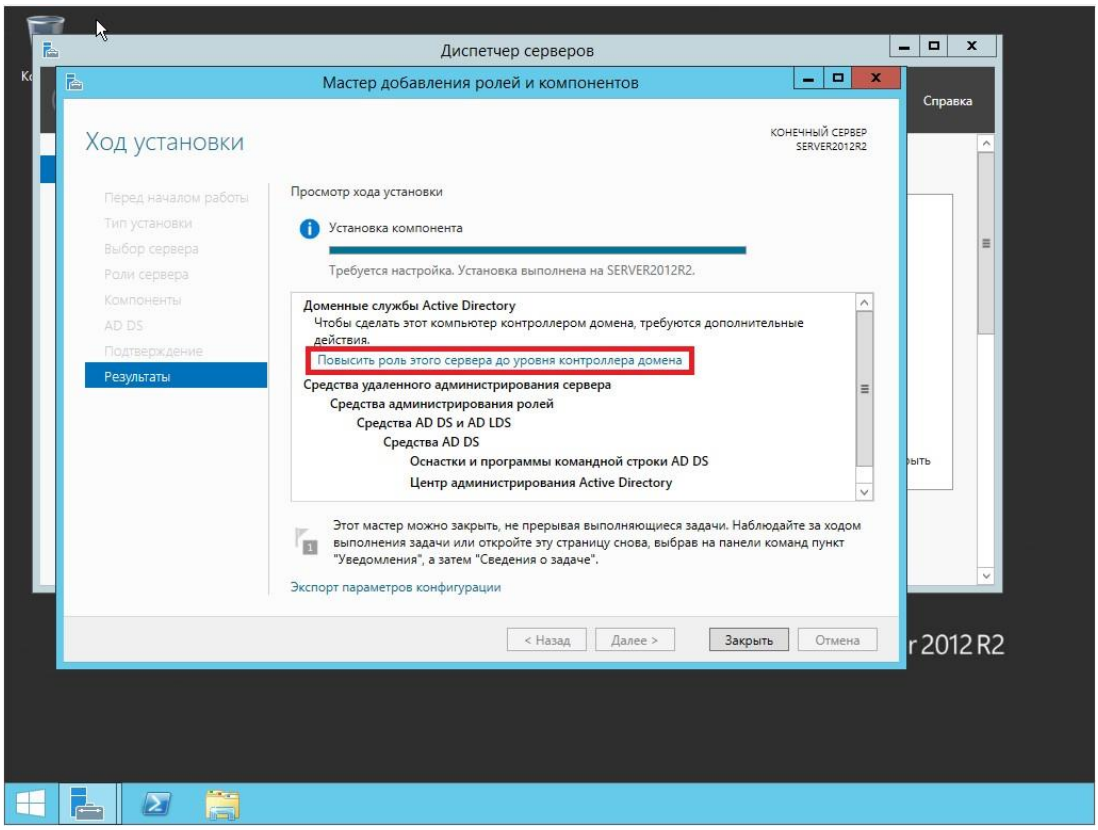


Рис. 18

2.11 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.

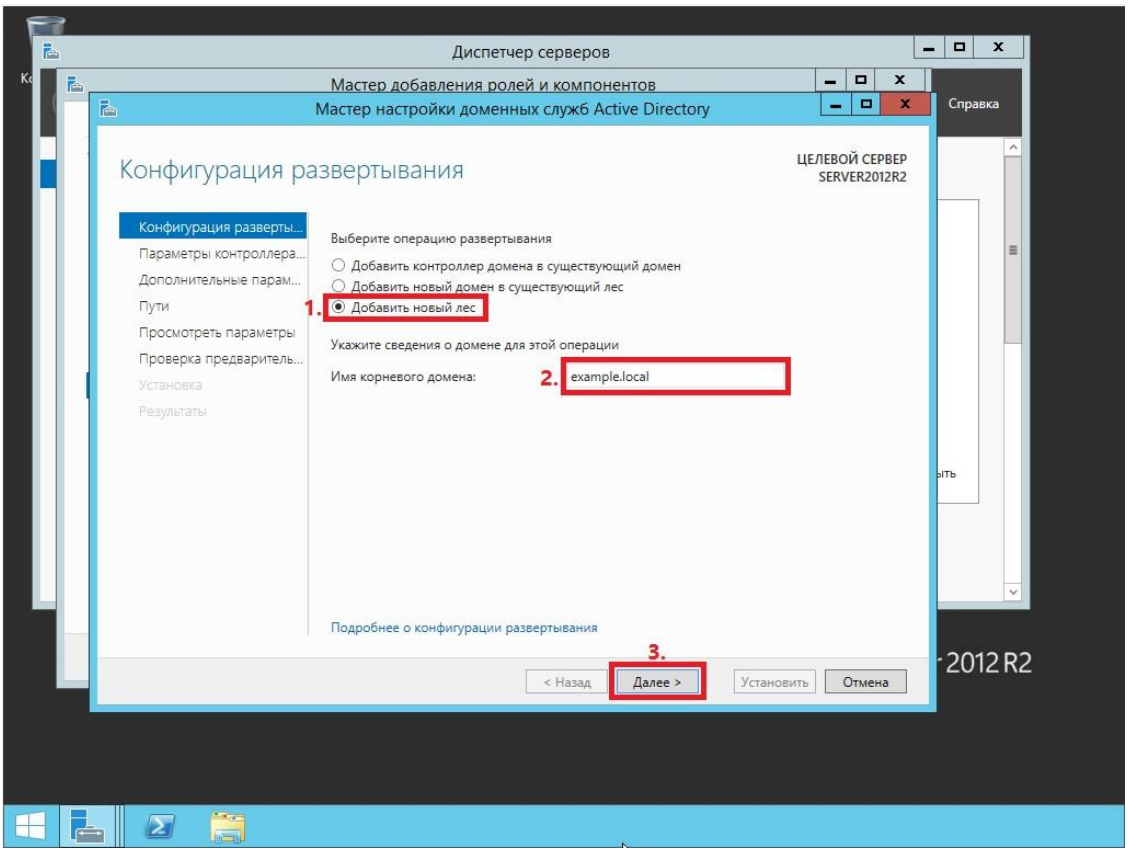


Рис. 19

2.12 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**

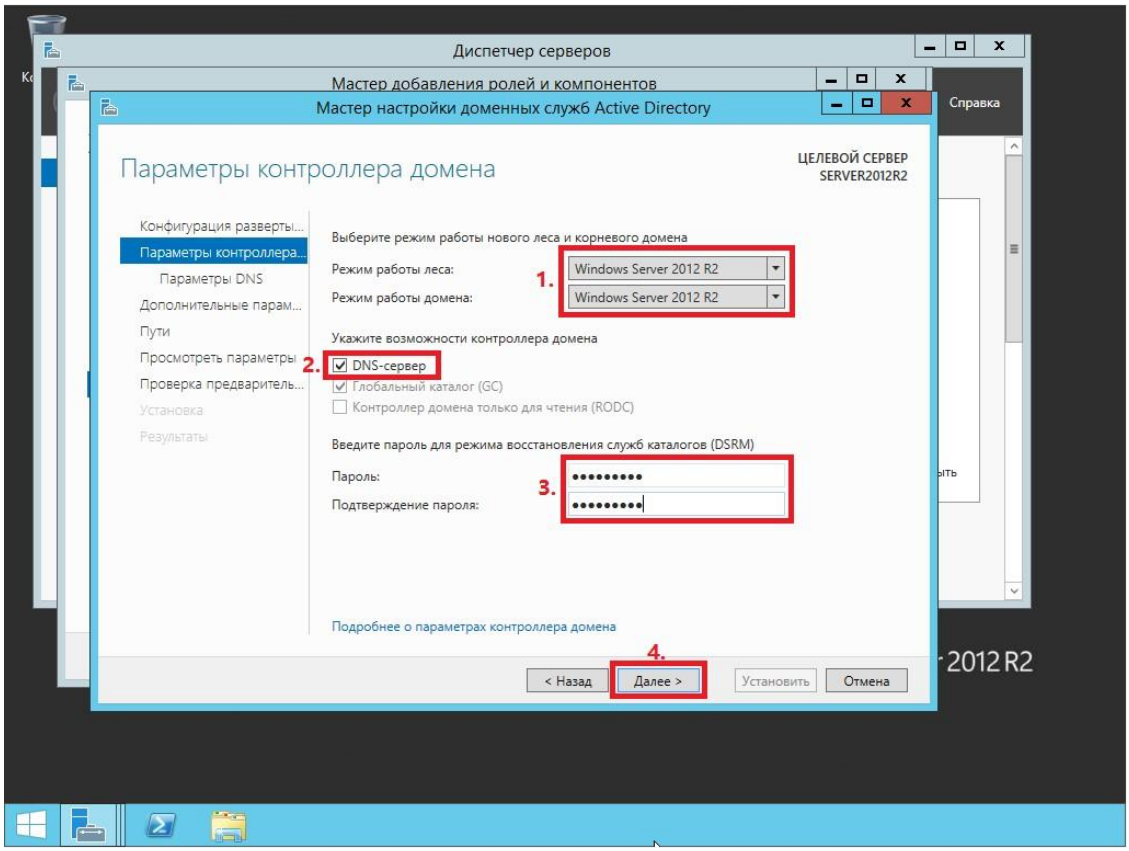


Рис. 20

2.13 Оставьте значение NetBIOS по умолчанию и нажмите **Далее**

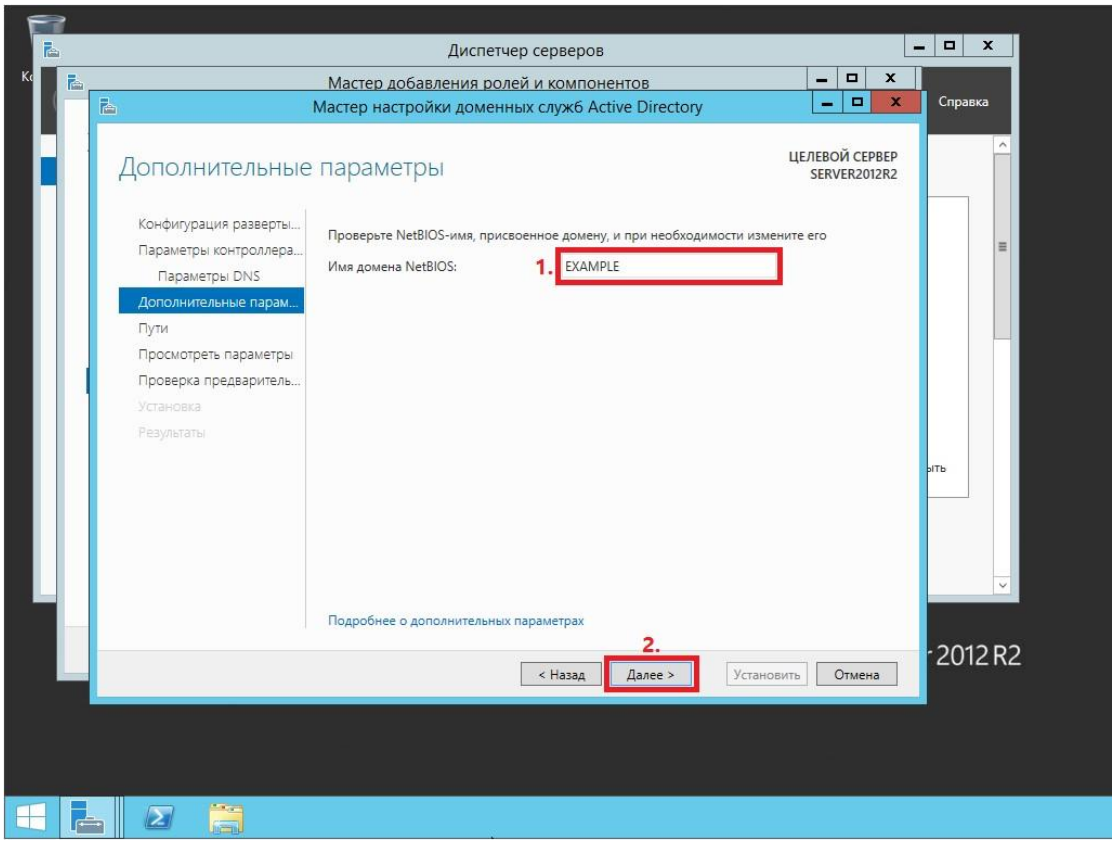


Рис. 21

2.14 Оставьте настройки по умолчанию и нажмите **Далее**

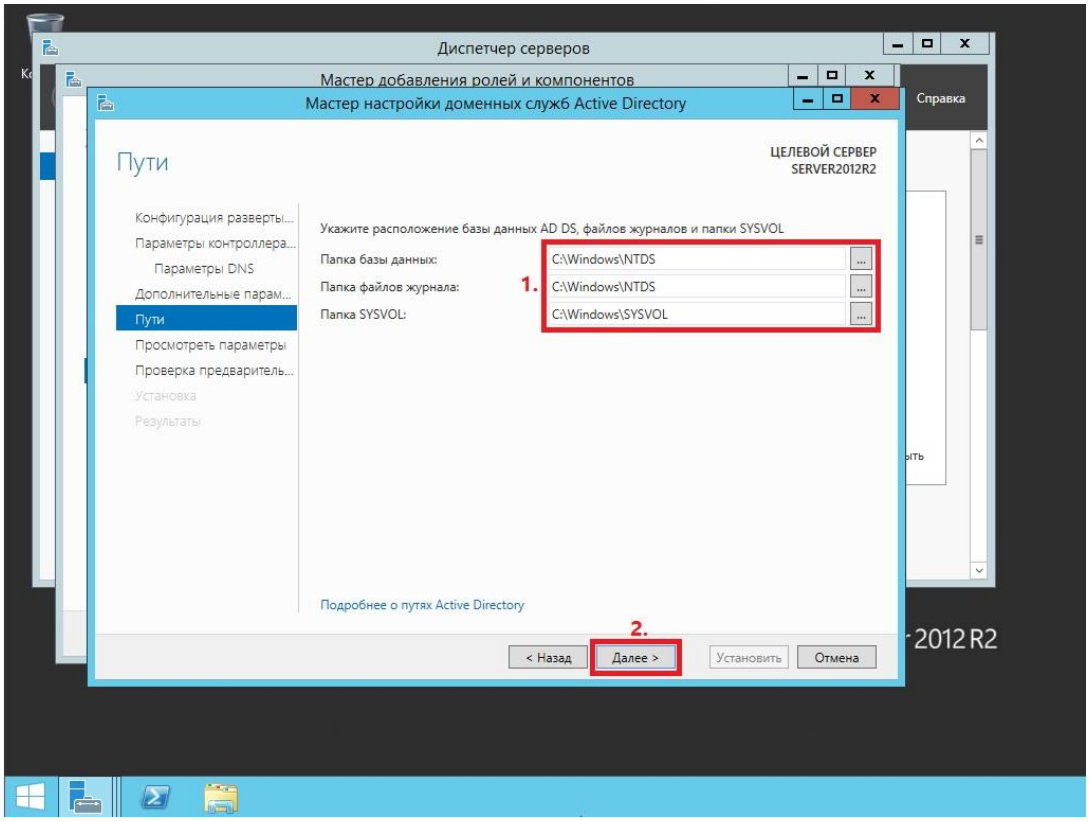


Рис. 22

2.15 В окне со сводной информацией по настройке сервера нажмите **Далее**

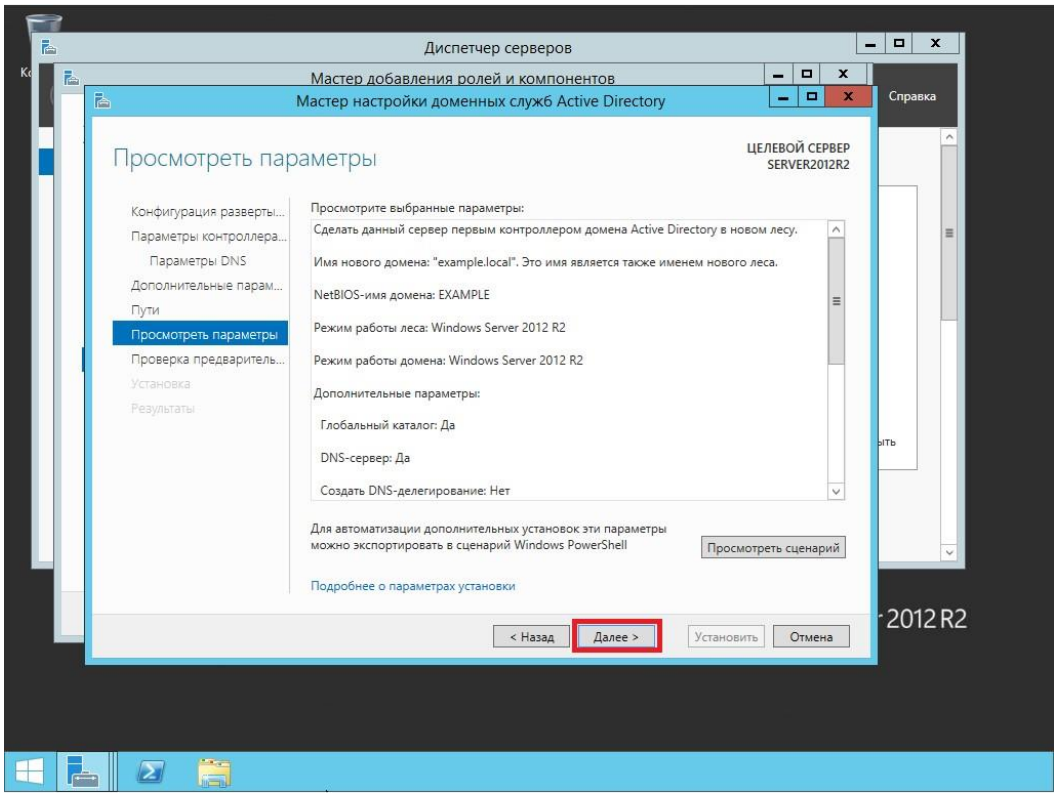


Рис. 23

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

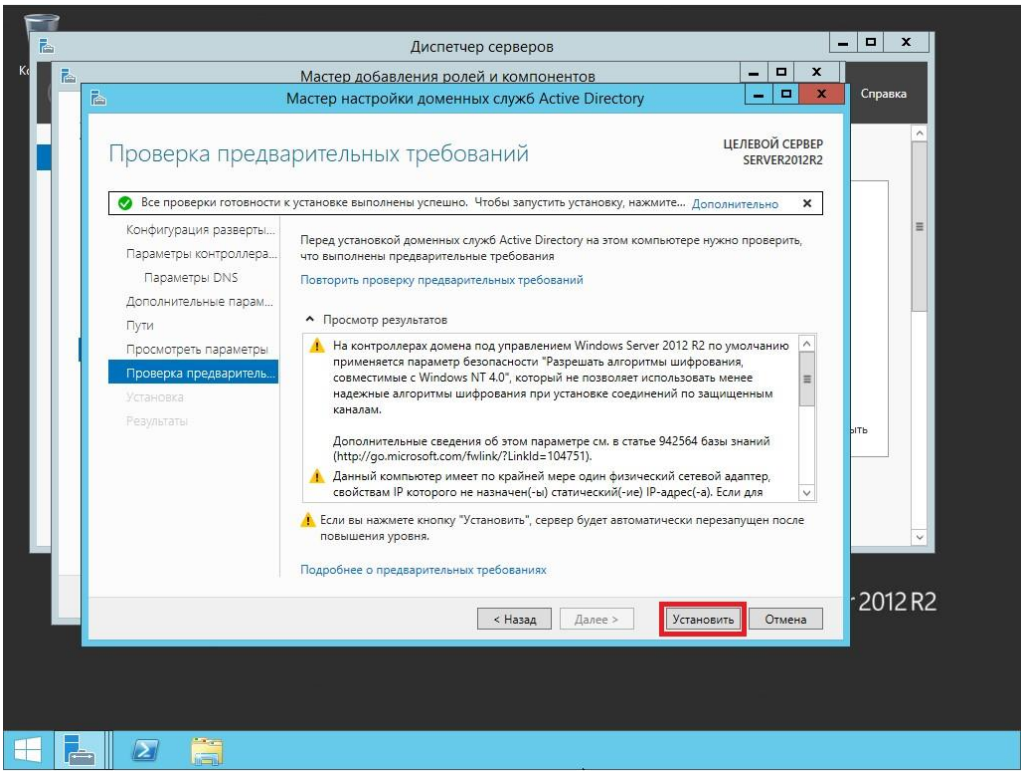


Рис. 24

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

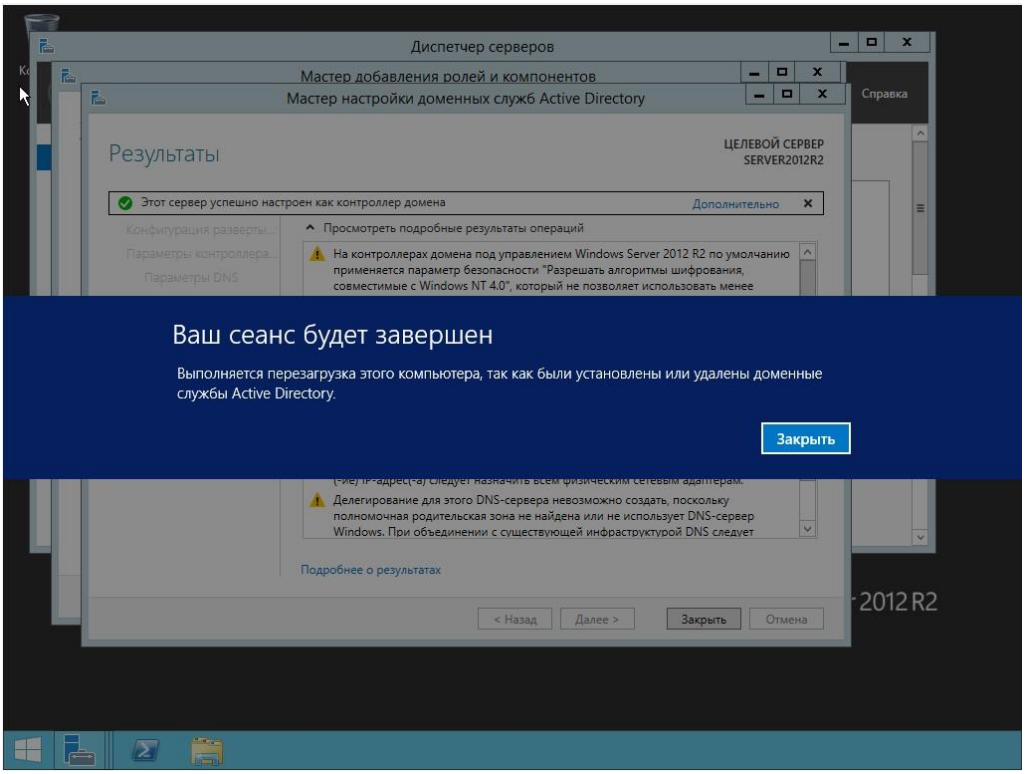


Рис. 25

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

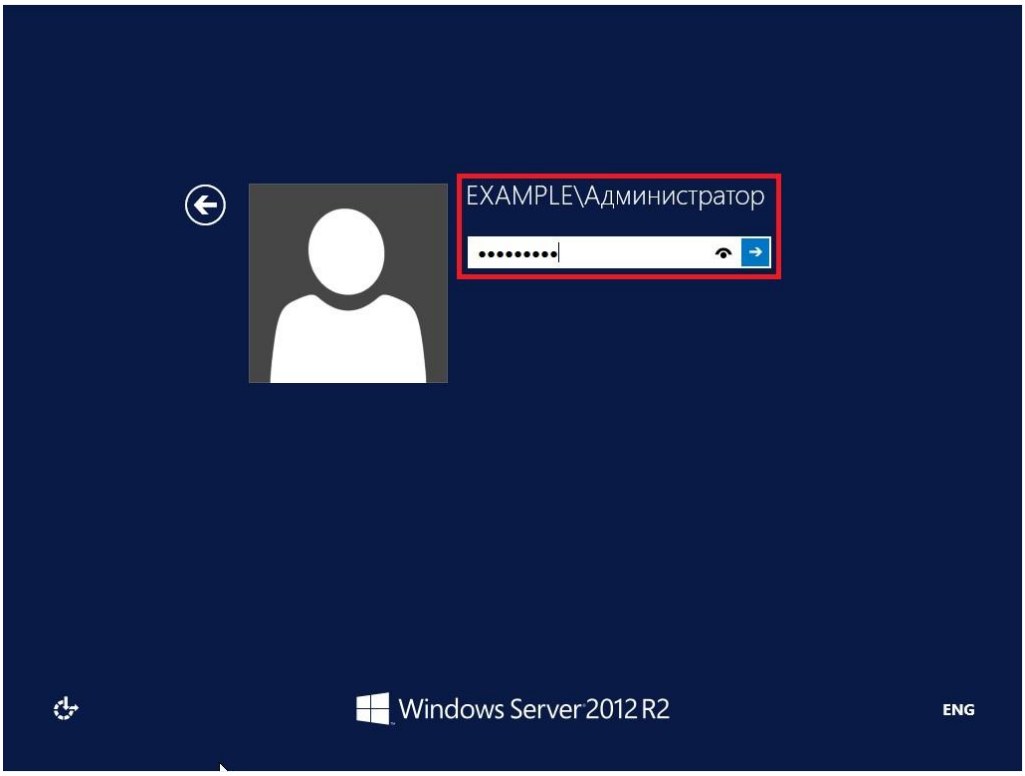


Рис. 26

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

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

Настройка политики паролей учетных записей в Active Directory

3.1 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"**

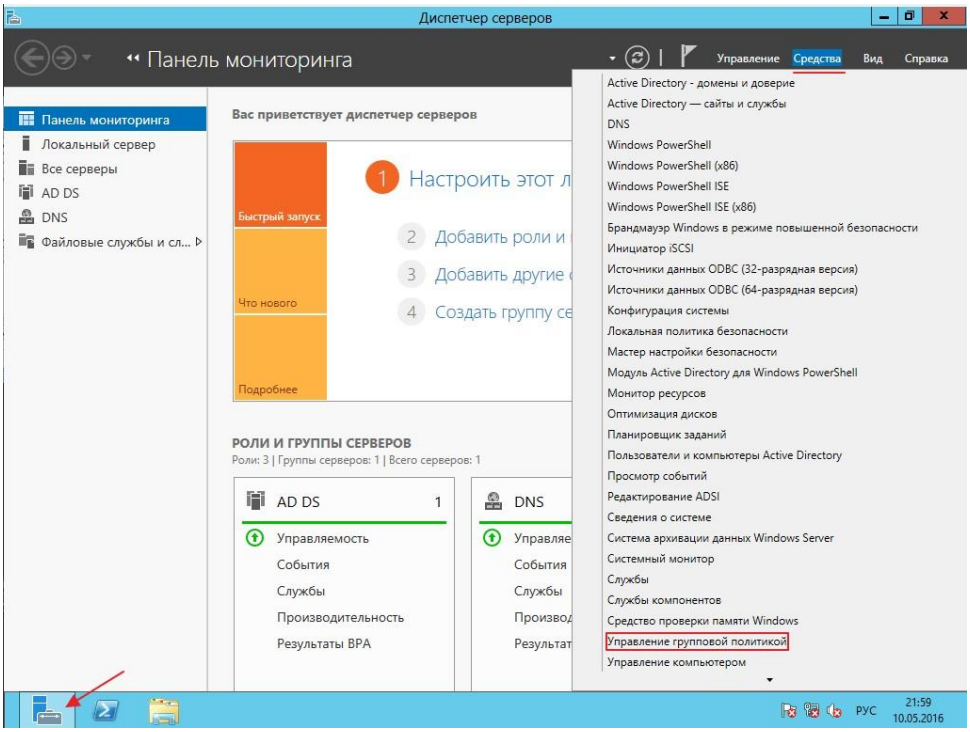


Рис. 27

3.2 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"**

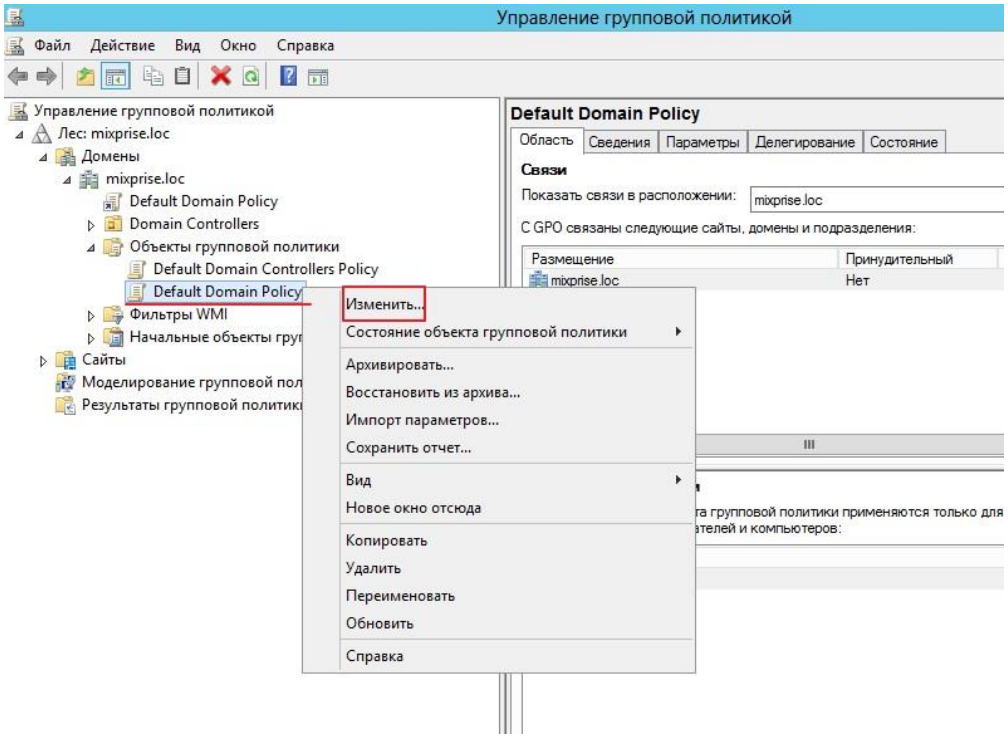


Рис. 28

3.3 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"**

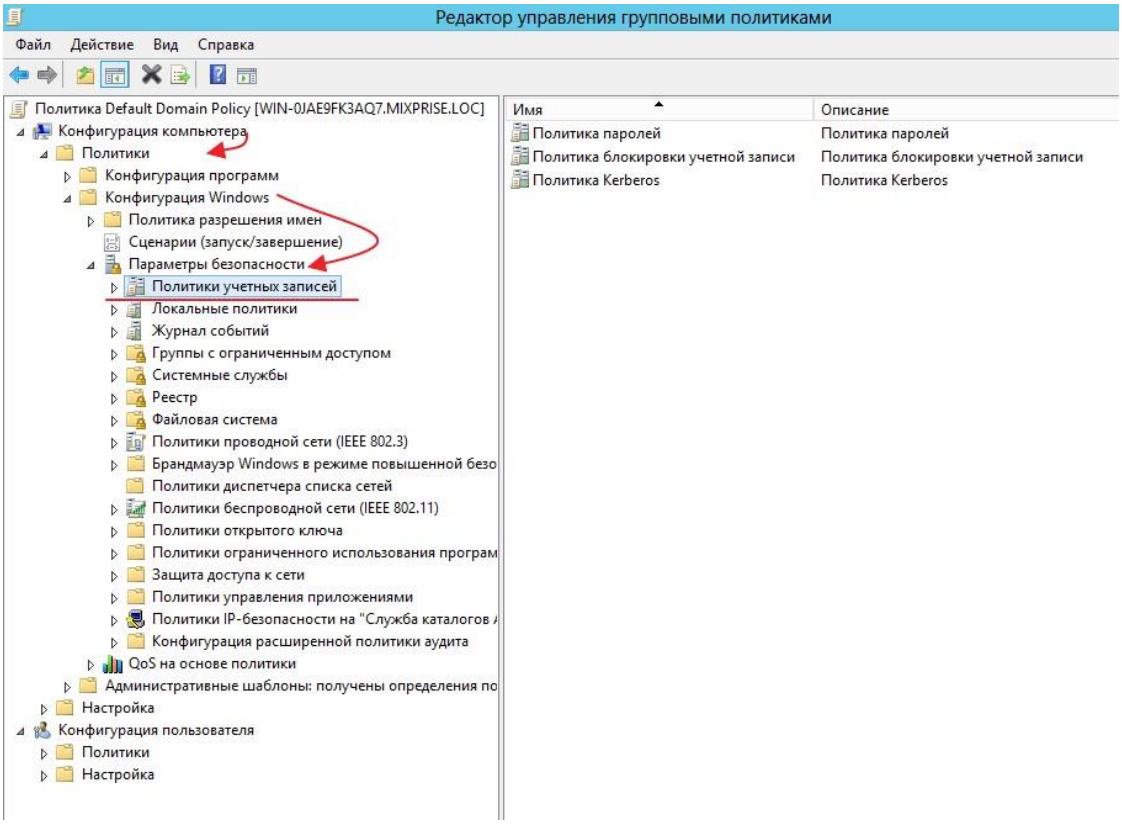


Рис. 29

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

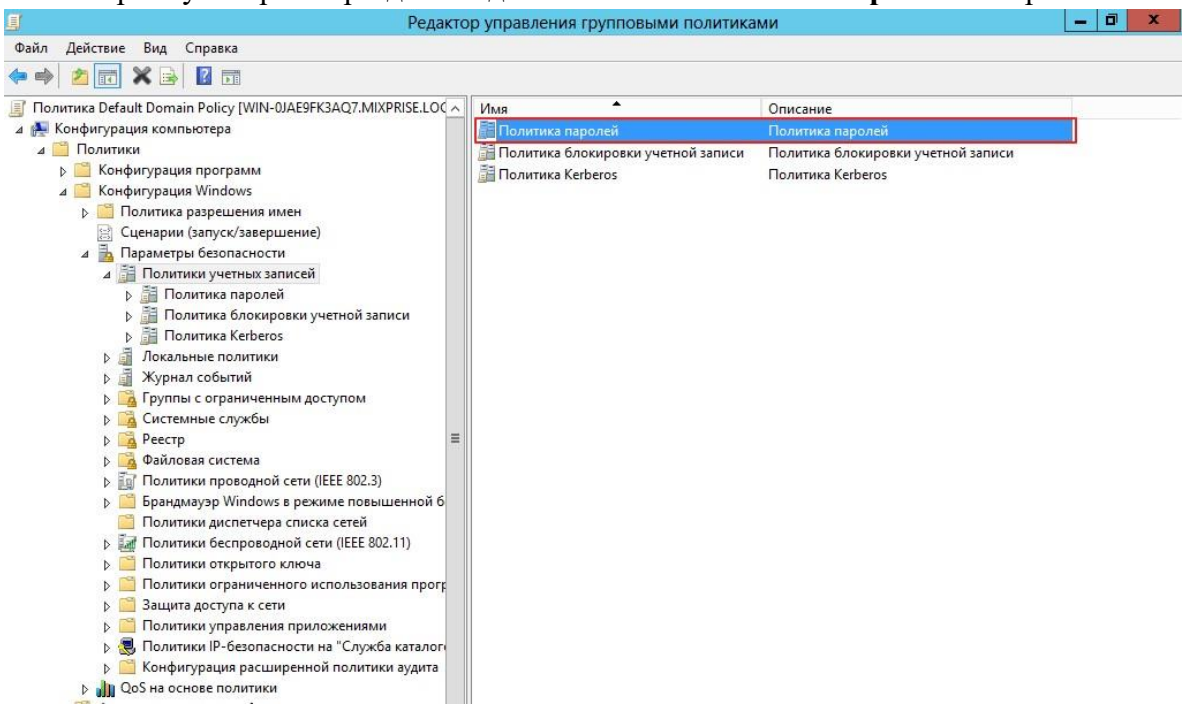


Рис. 30

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

3.4 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.

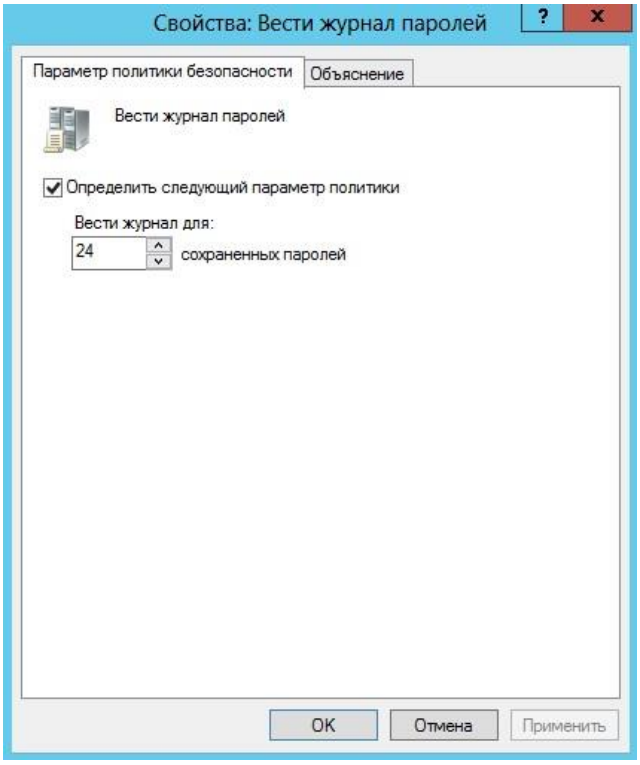


Рис. 31

3.5 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"**

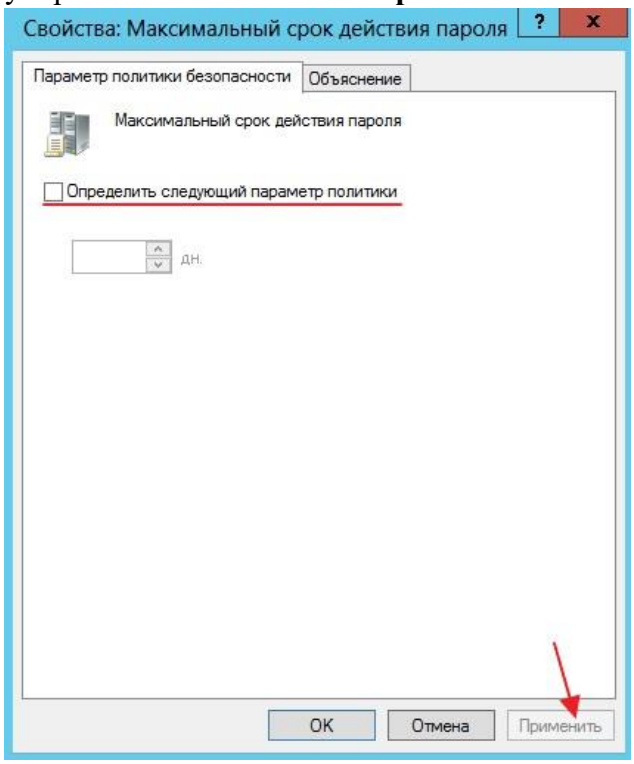


Рис. 32

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

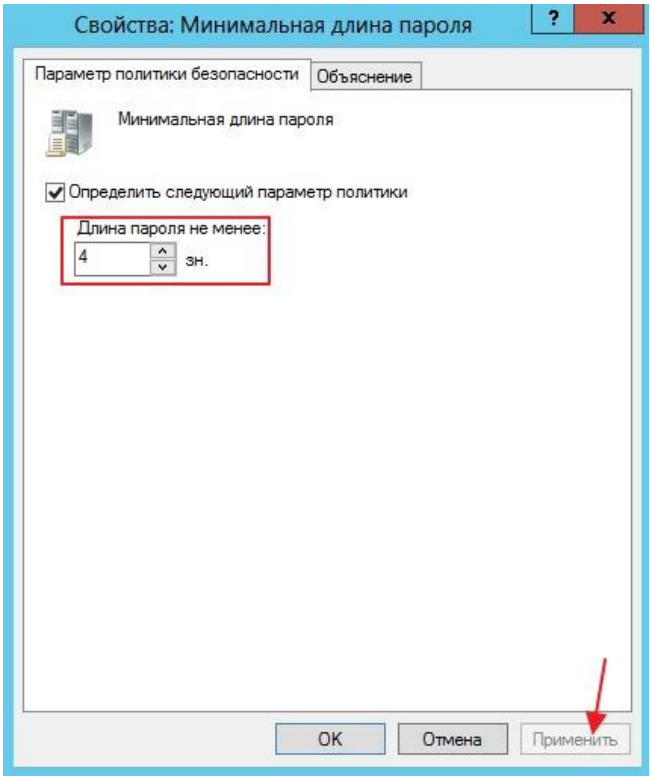


Рис. 33

3.6 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

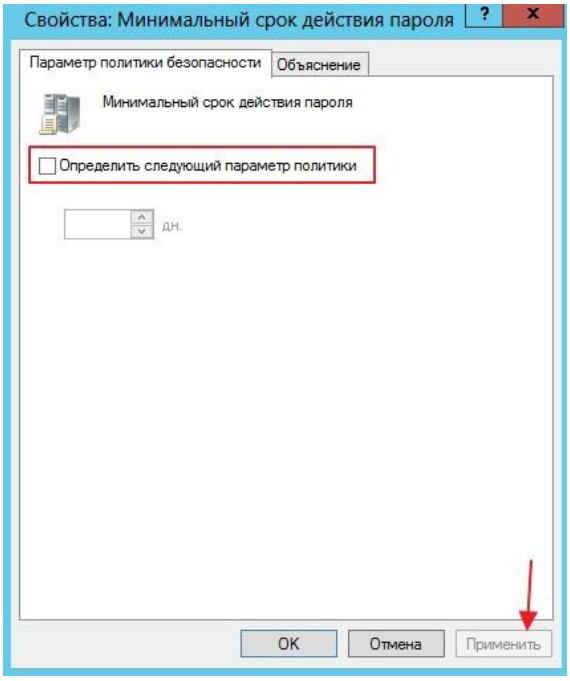


Рис. 34

3.7 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!

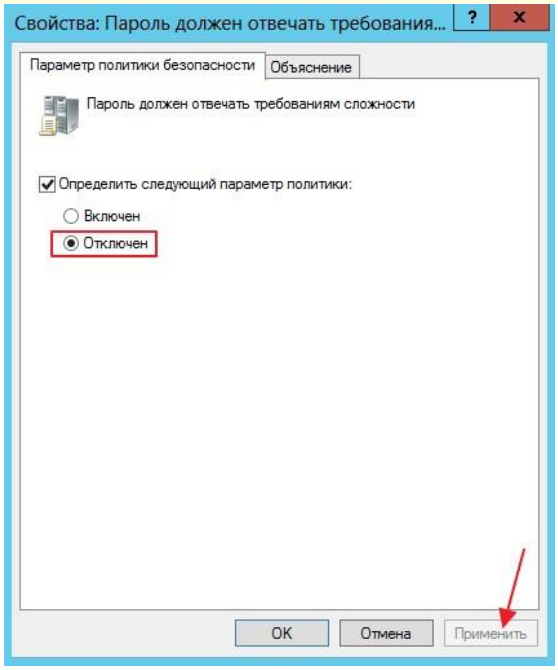


Рис. 35

3.8 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!

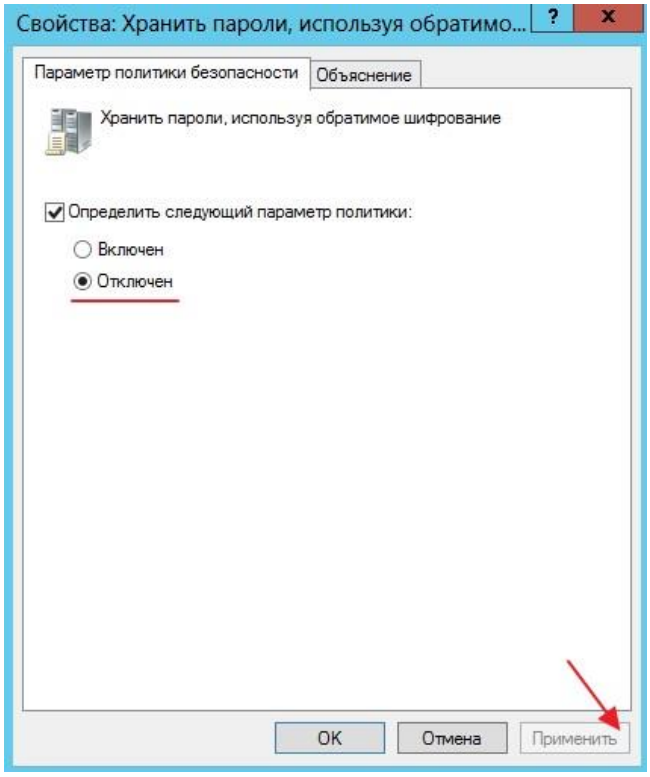


Рис. 36

3.9 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

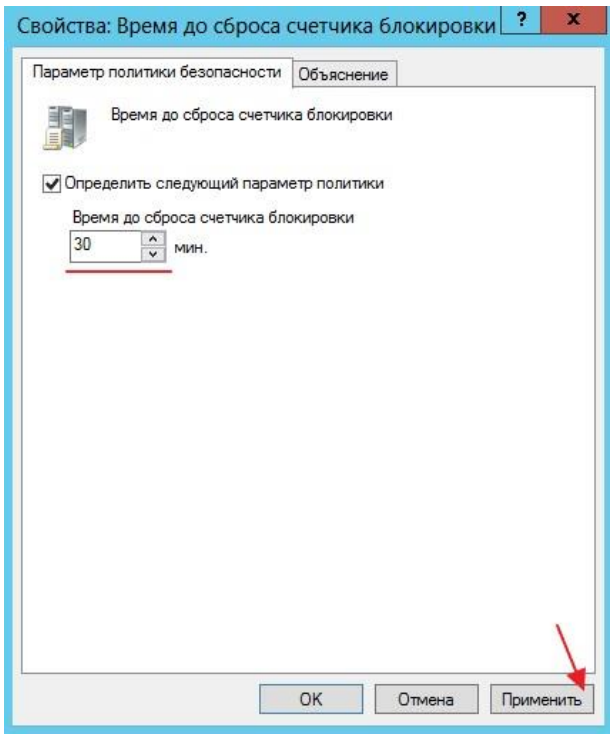


Рис. 37

"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

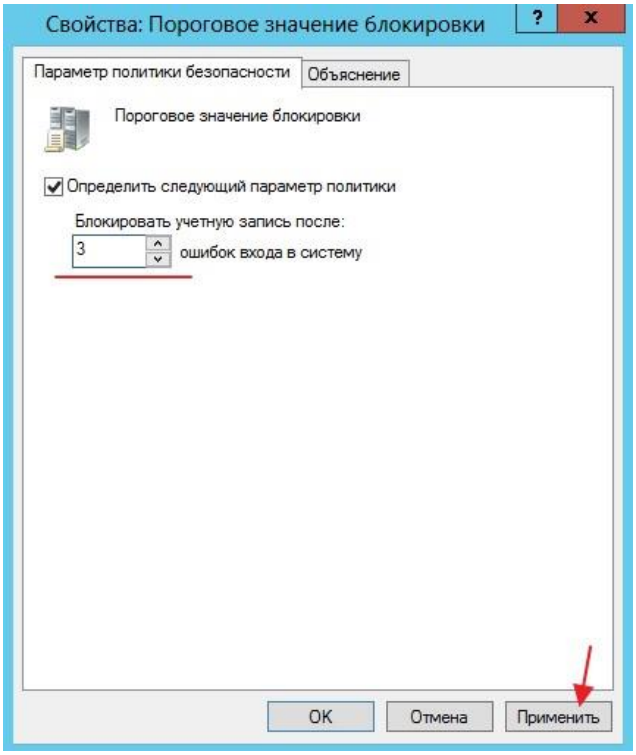


Рис. 38

"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

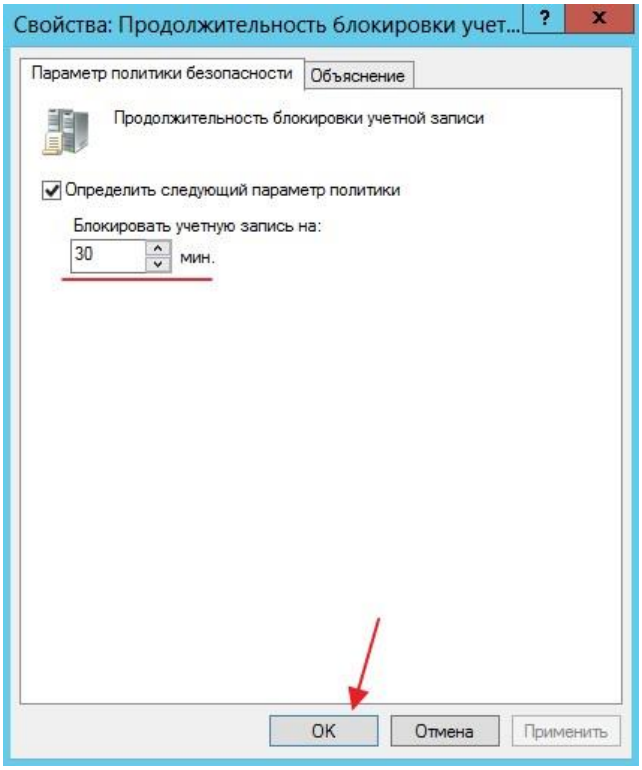


Рис. 39

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

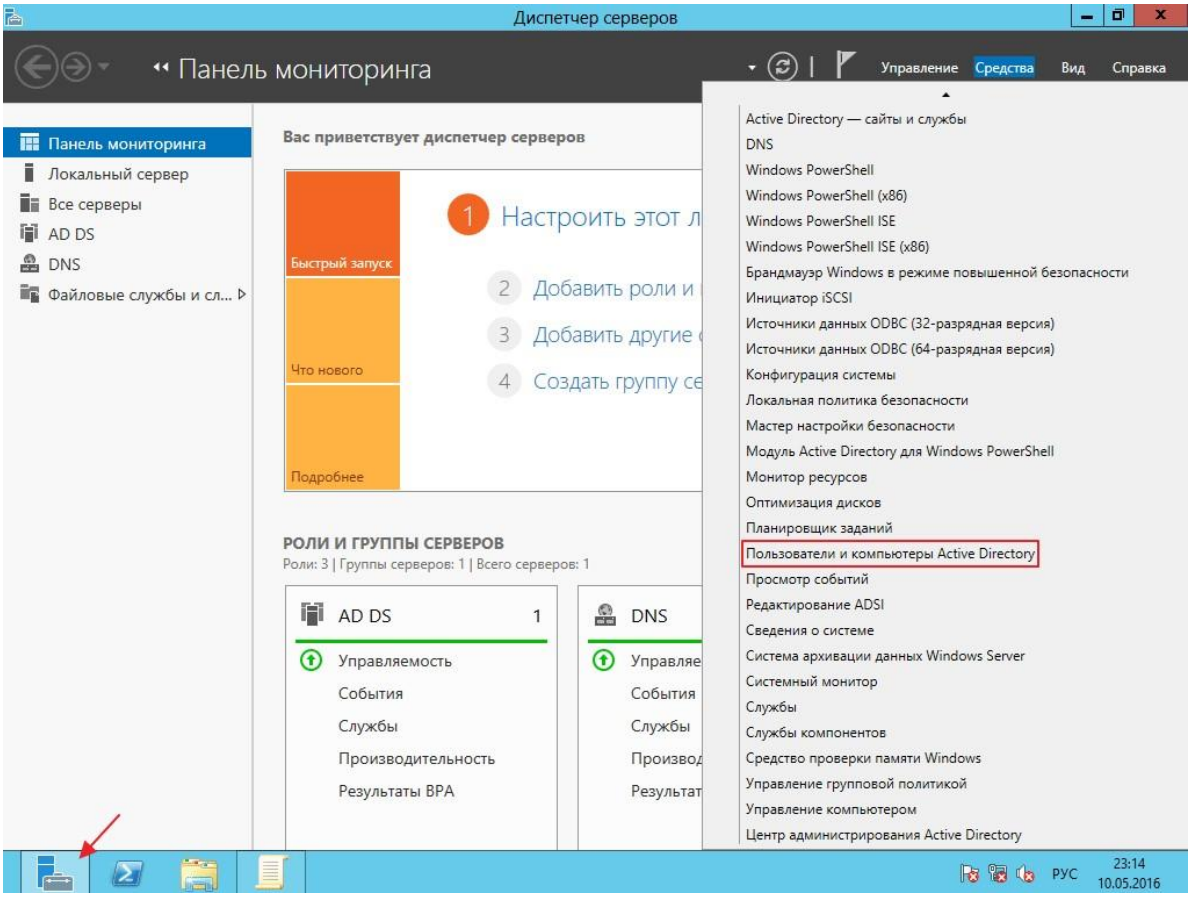


Рис. 40

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

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

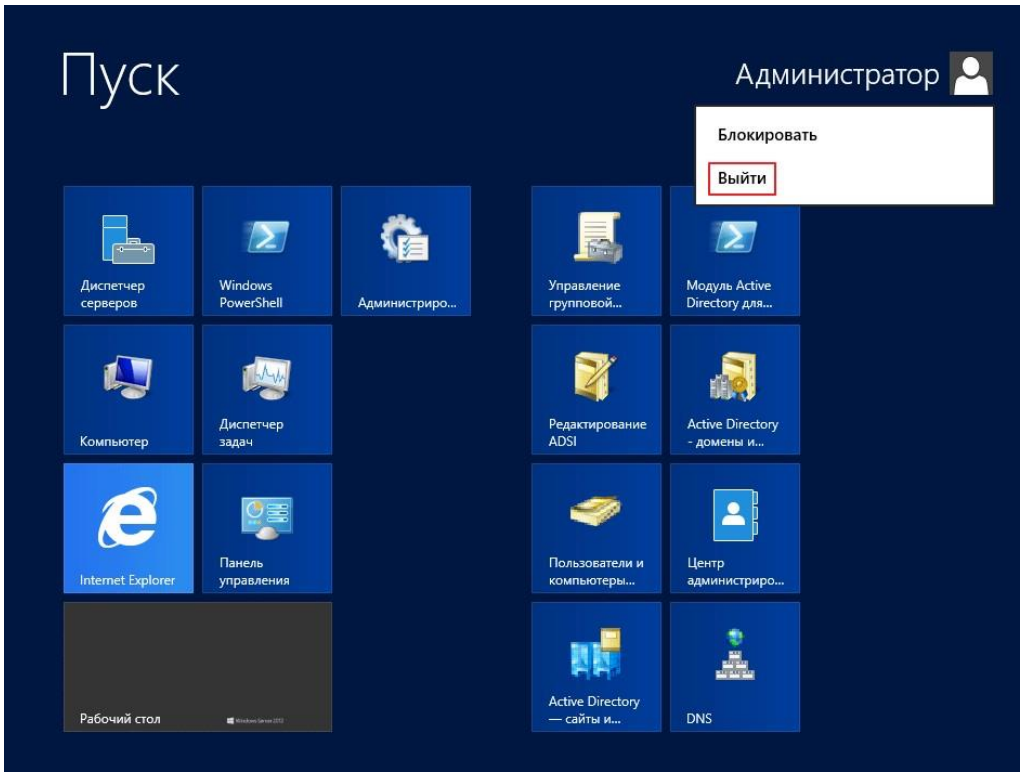


Рис. 41

Осуществляем вход с новой учетной записью

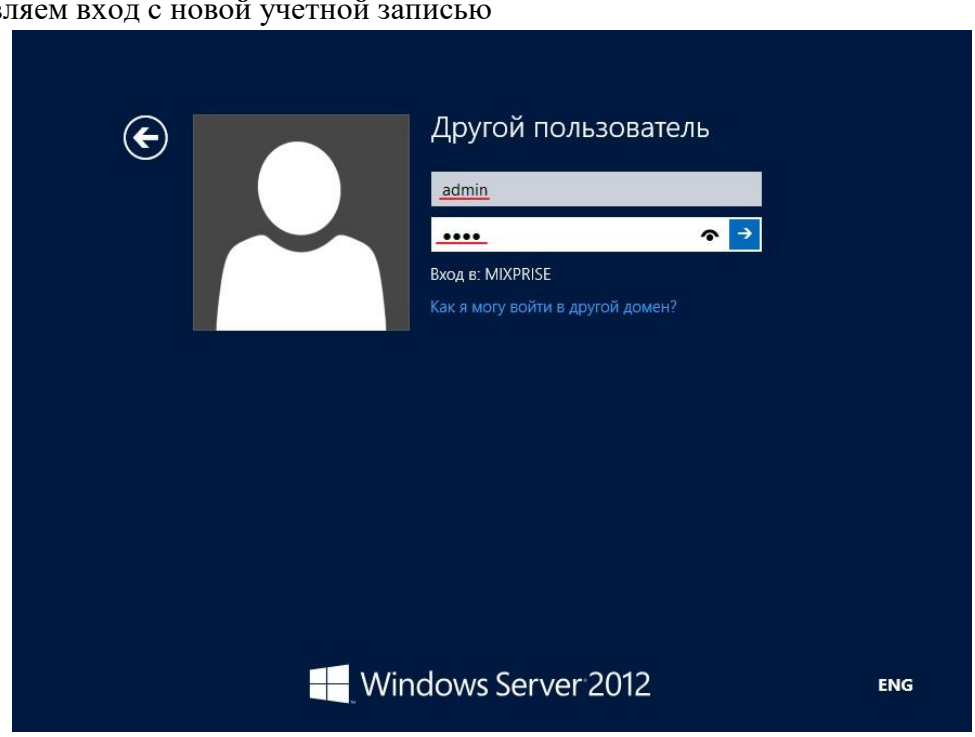


Рис. 42

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

Создание пользователя в Powershell с параметрами New-ADUser

4.1 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

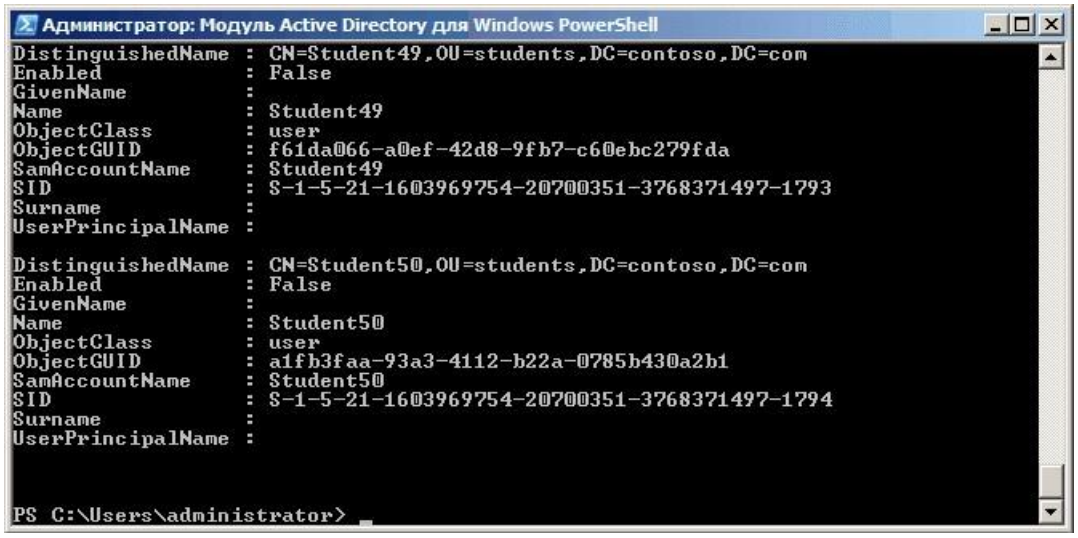


Рис. 43

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.

4.2 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 }
```

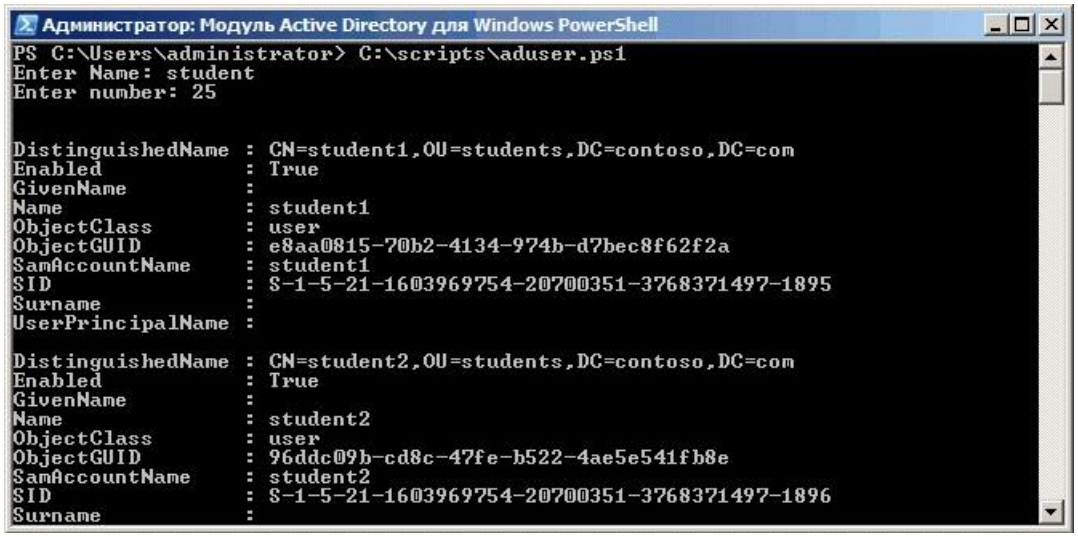


Рис. 44

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 }
```

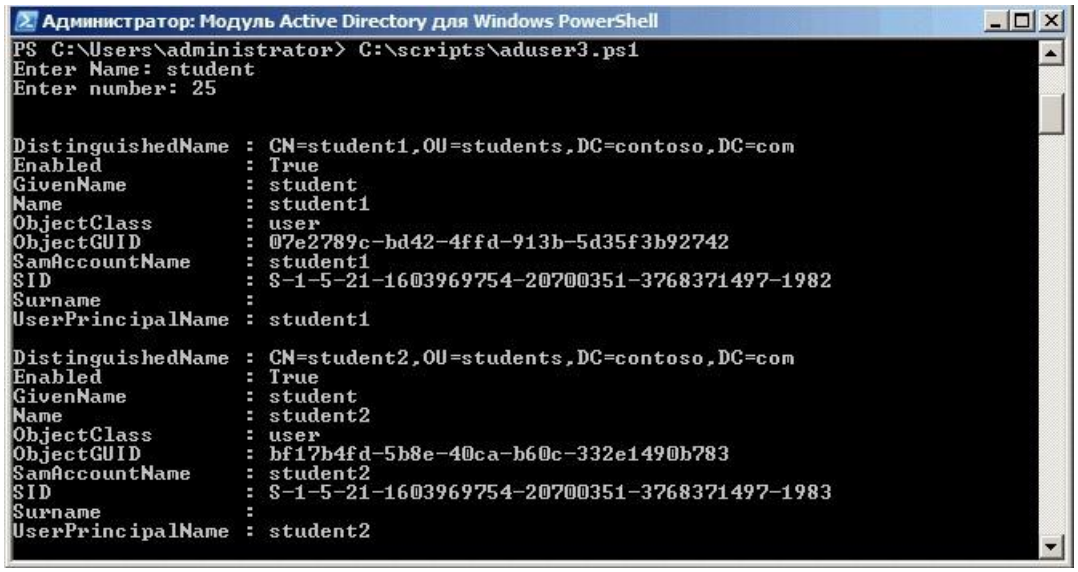
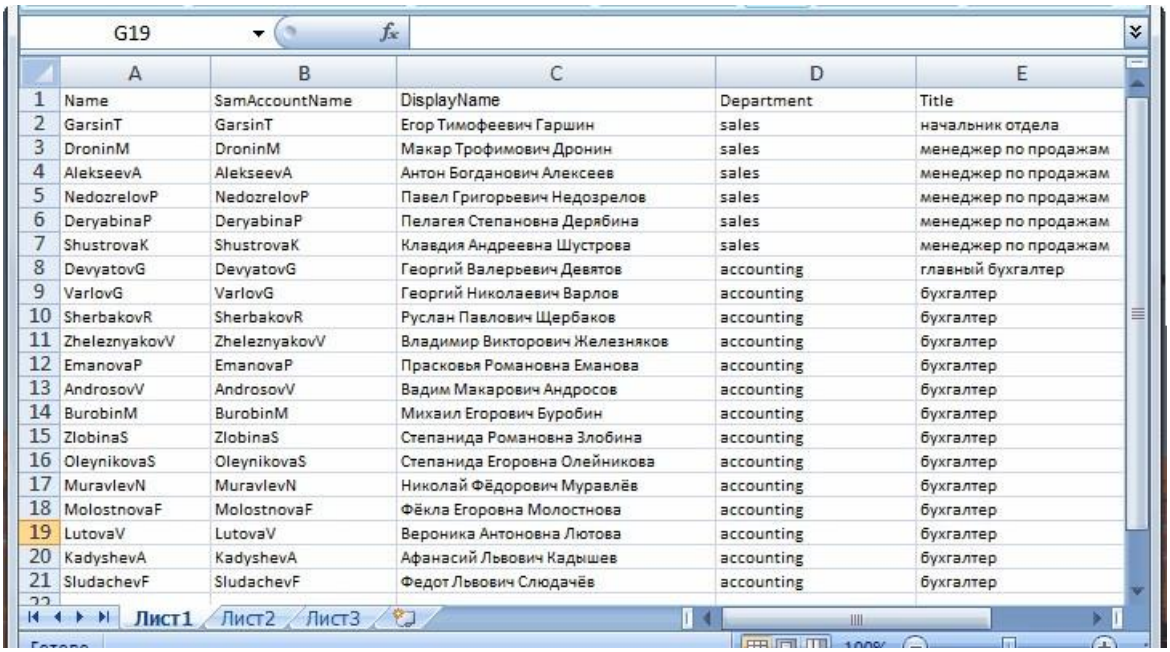


Рис. 45

4.3 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. 46

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
```

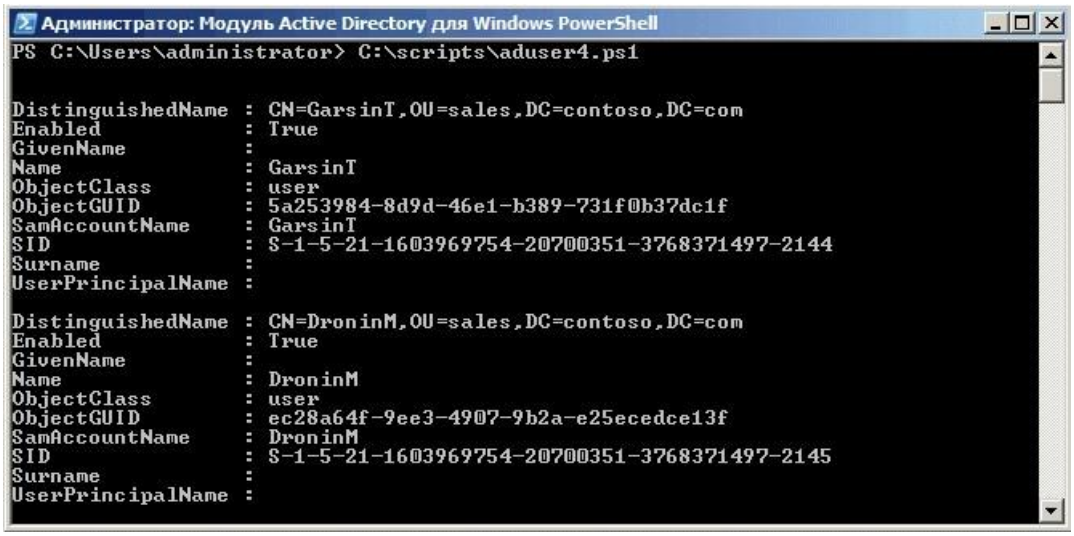


Рис. 47

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.

2.3. Практическая работа № 3 «Установка ролей сервера Windows Server 2012 R2»

Задание:

1. Установка и настройка ADRMS на Windows Server 2012 R2

1.1 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.

1.2 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).

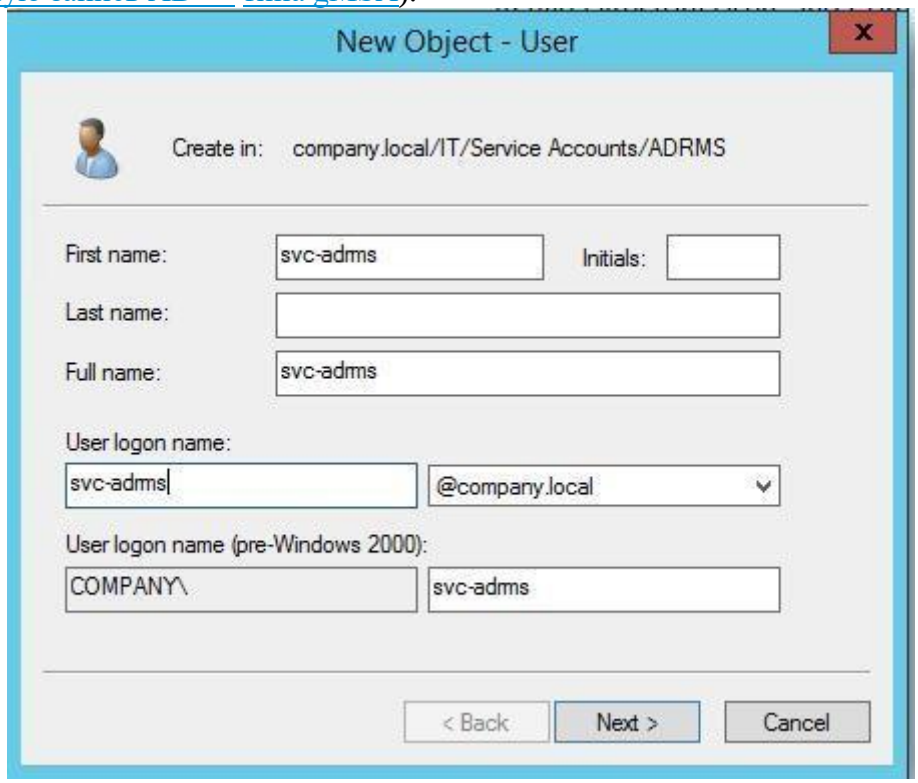


Рис. 48

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

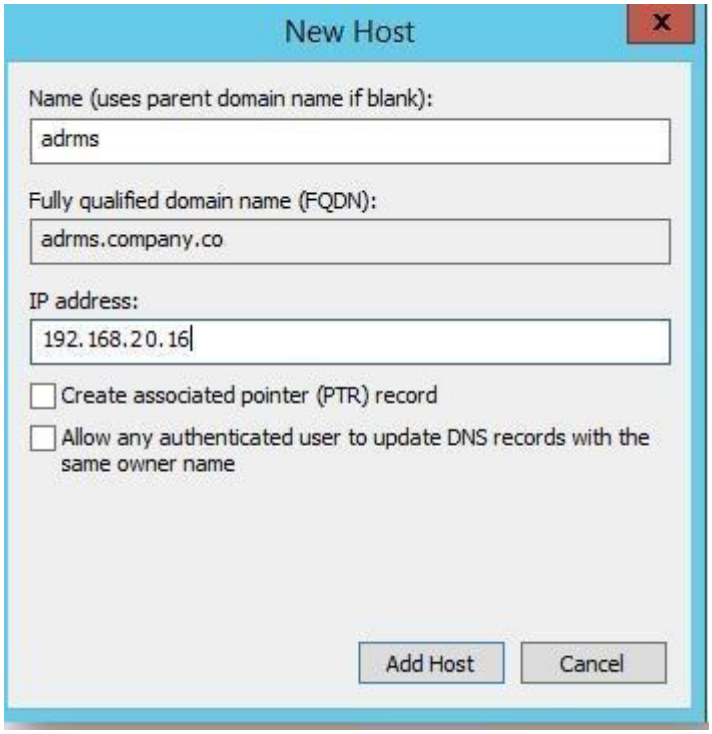


Рис. 49

1.4 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 поумолчанию).

Рис. 50

1.5 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**.

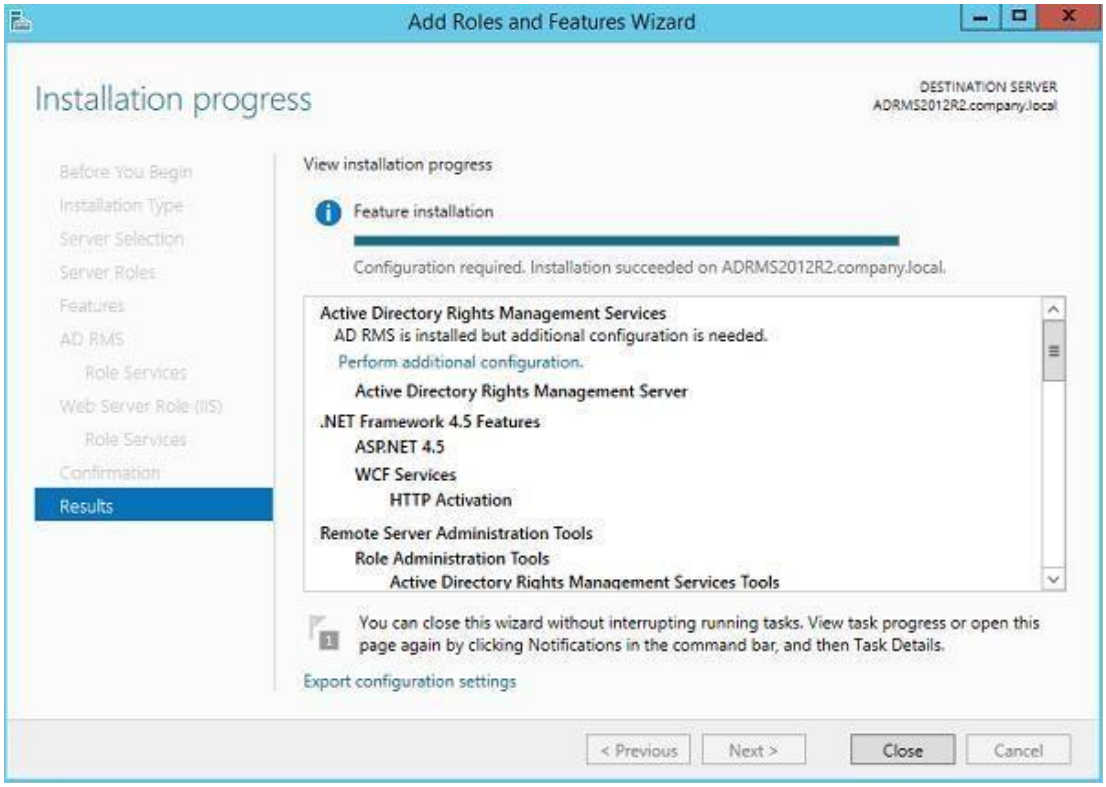


Рис. 51

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

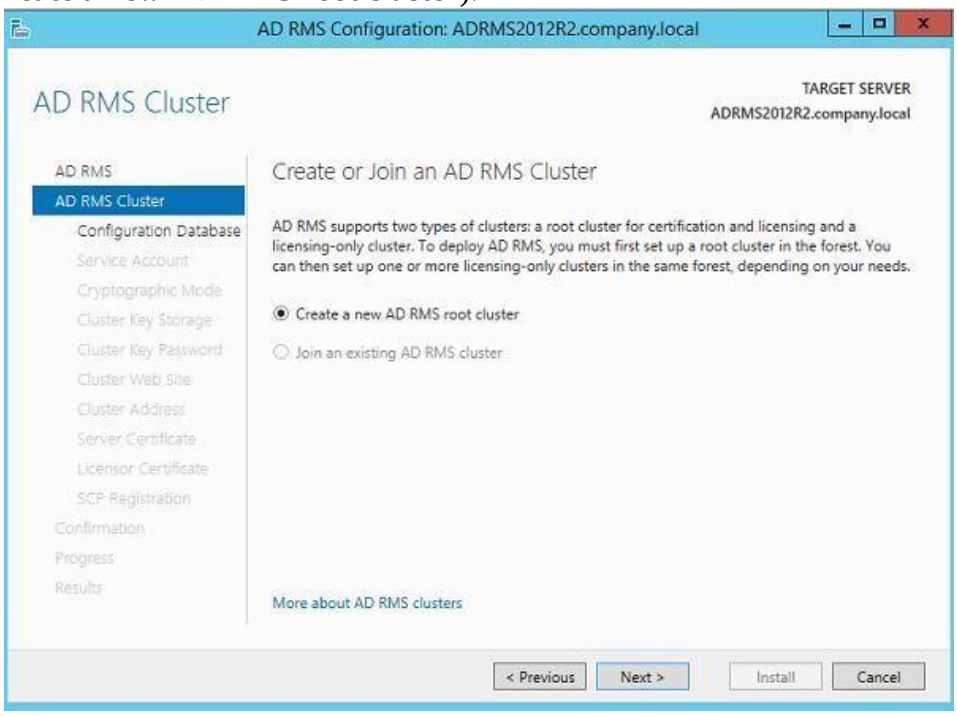
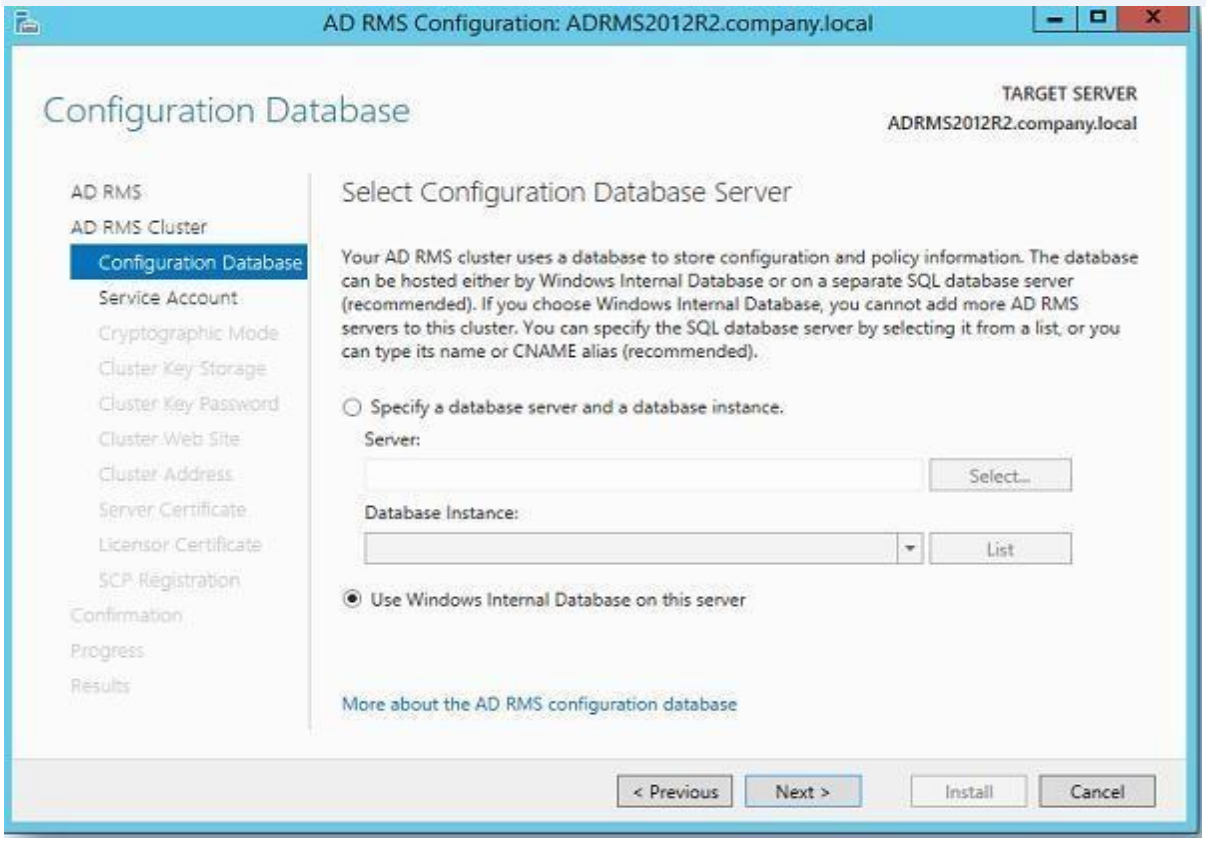


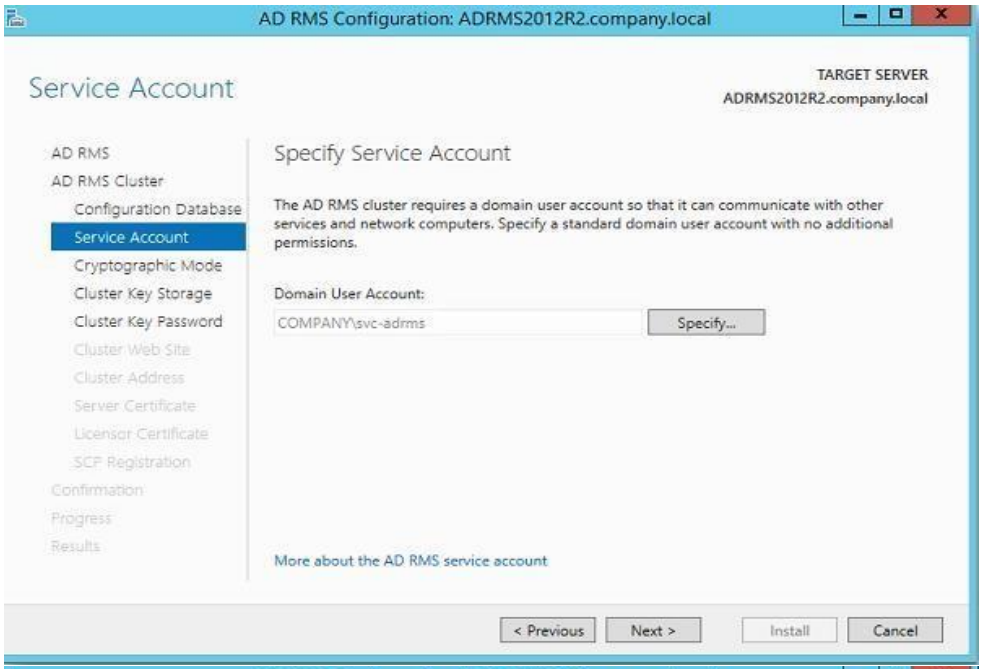
Рис. 52

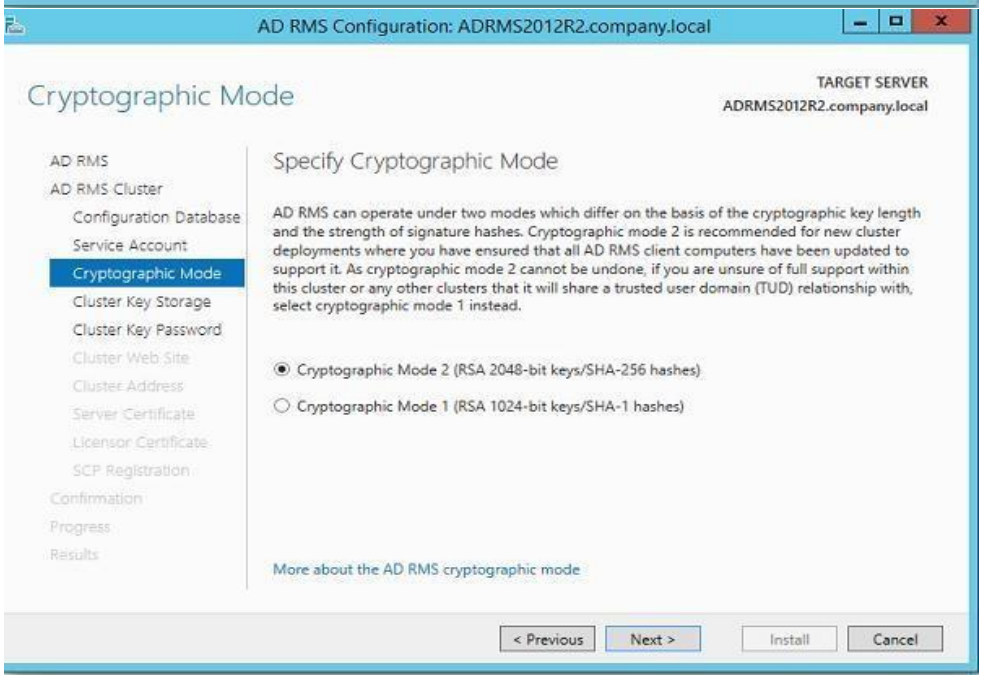
1.7 В качестве базы данных RMS будем использовать внутреннюю базу данных Windows (**Use Windows Internal Database on this server).**

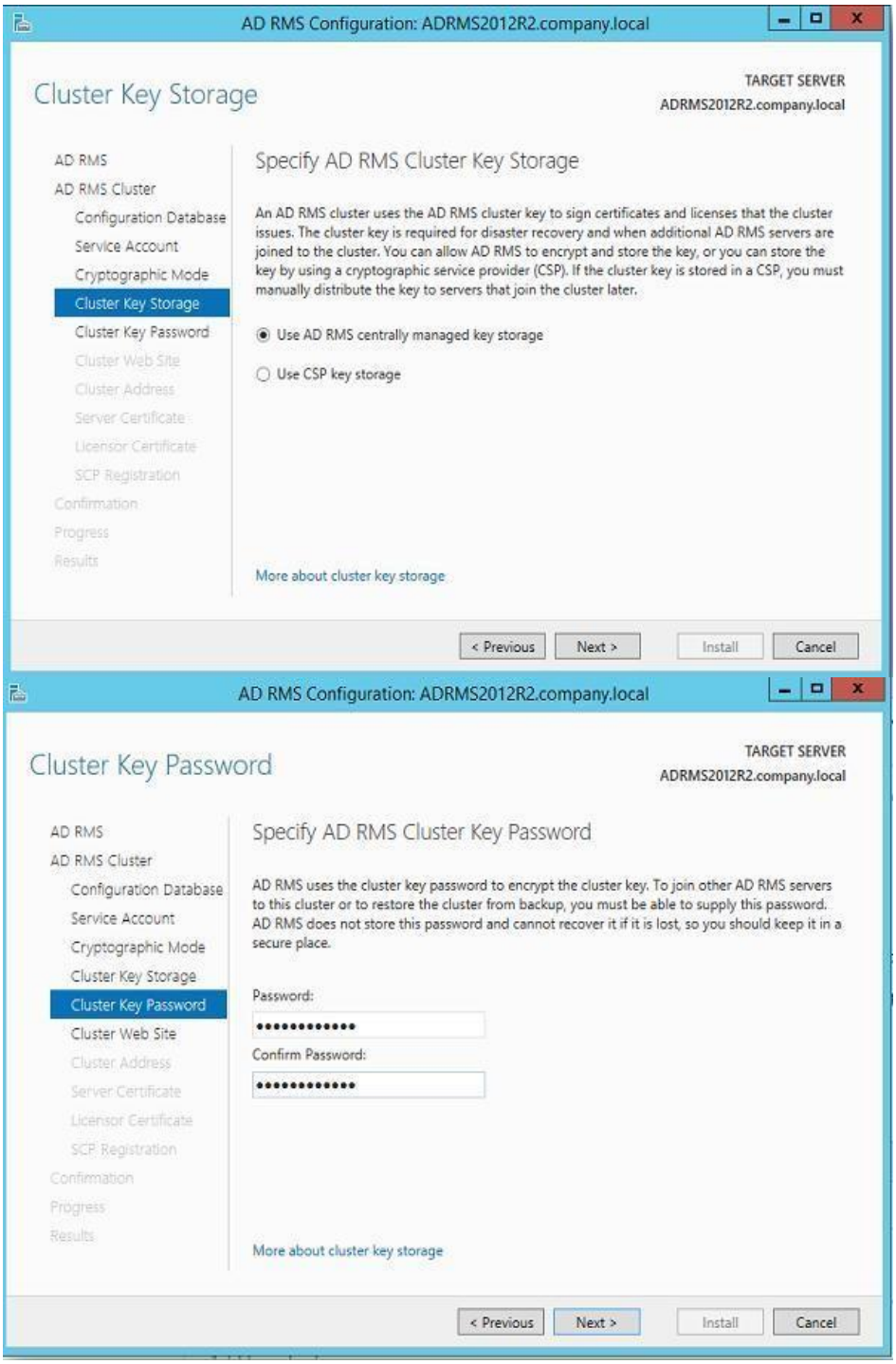
Совет. Подробнее про WID. В продуктивной среде рекомендуется для размещения БД RMS рекомендуется использовать отдельный инстанс Microsoft SQL Server. Связано это с тем, что внутренняя база Windows не поддерживает удаленные подключения, а это означает, что



1.8 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



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

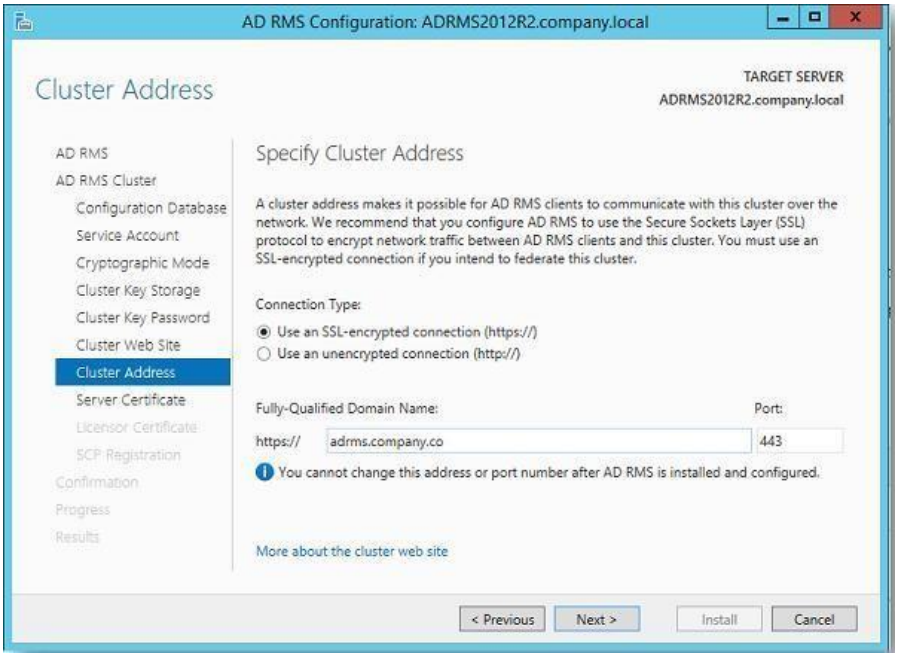
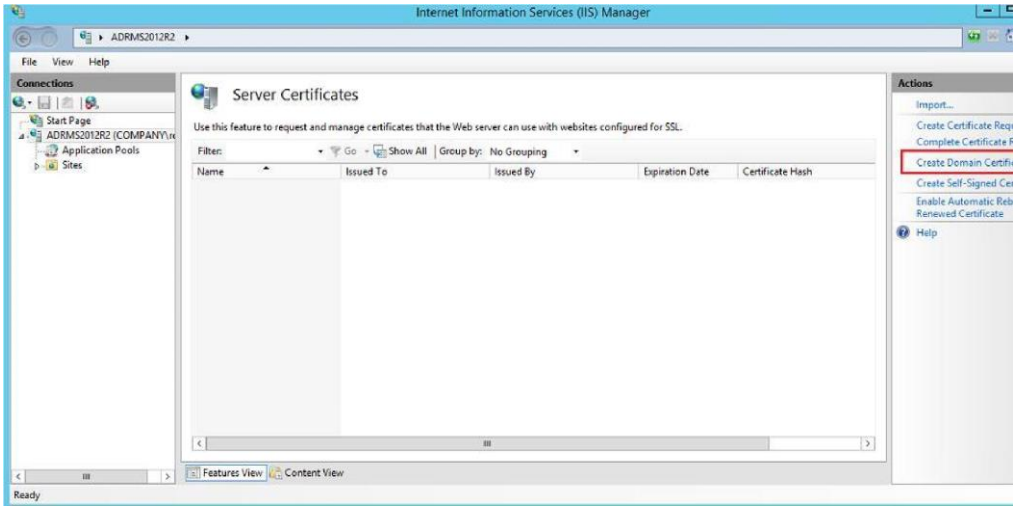


Рис. 53

Не закрывайте мастер настройки AD RMS!

1.10 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.



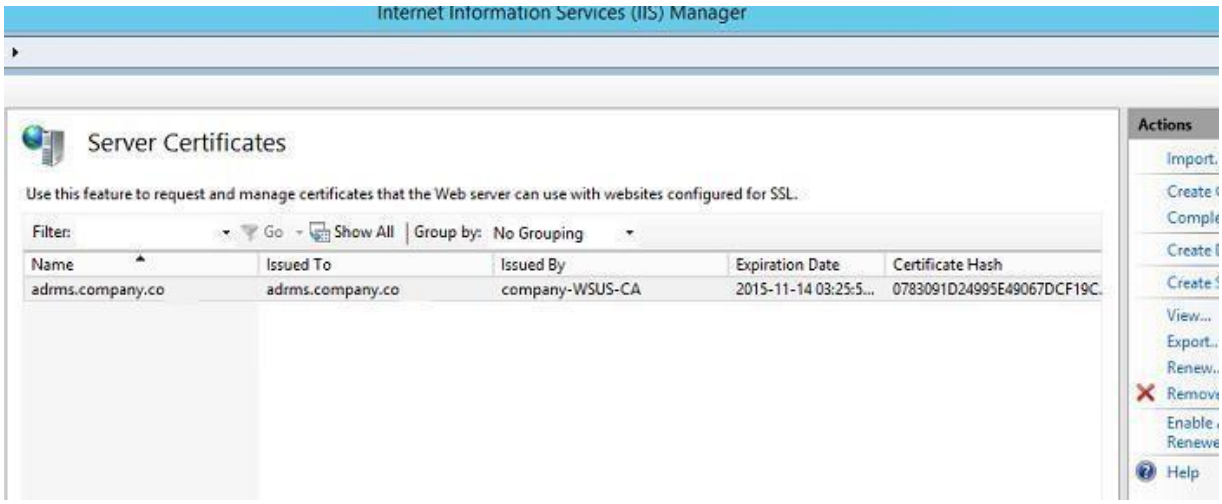


Рис. 54

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

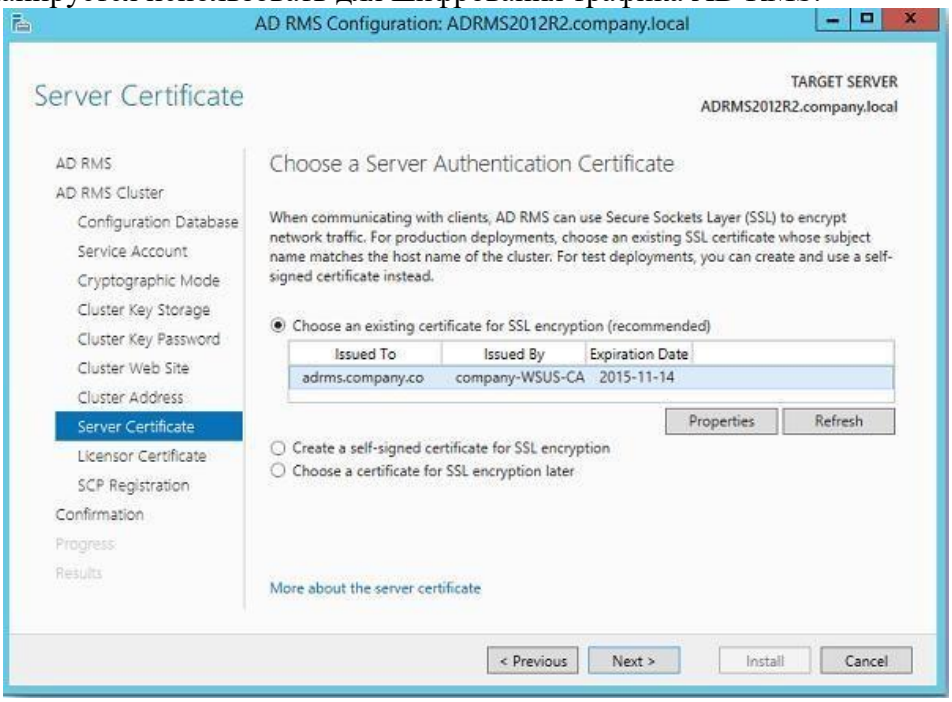
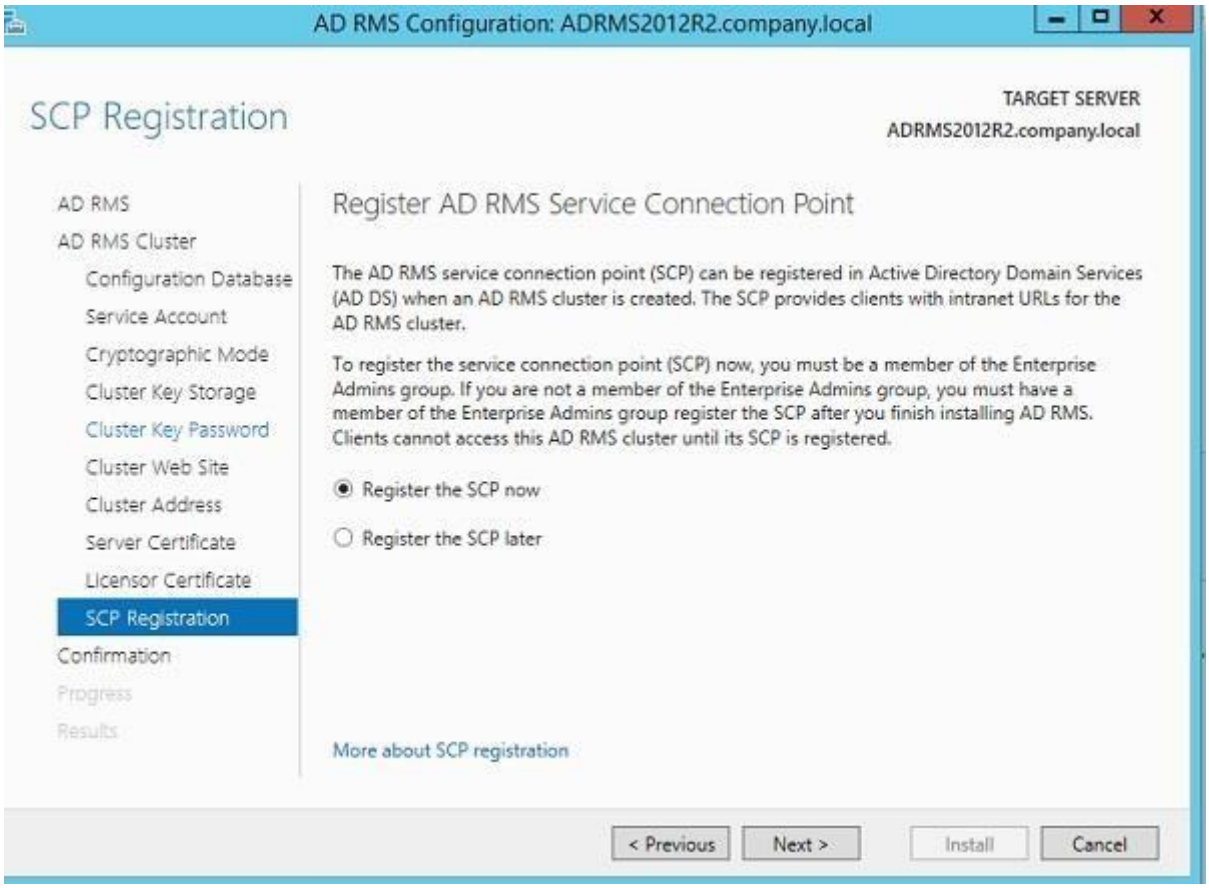


Рис. 55

1.12 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.



Совет: Чтобы удостовериться, что точка обнаружения AD RMS — SCP (Service Connection Point) зарегистрировалась в Active Directory, нужно открыть консоль dssite.msc. Затем перейдти в раздел Services -> RightManagementServices, в правой панели открыть свойства SCP. Убедитесь что значение атрибута distinguishedName имеет такой вид: CN=SCP,CN=RightsManagementServices,CN=Services,CN=Configuration,DC=company,DC=co

На этом процесс установки роли AD RMS закончен. Завершите текущий сеанс (logoff), и перезалогиньтесь на сервер.

1.13 Запустите консоль ADRMS.

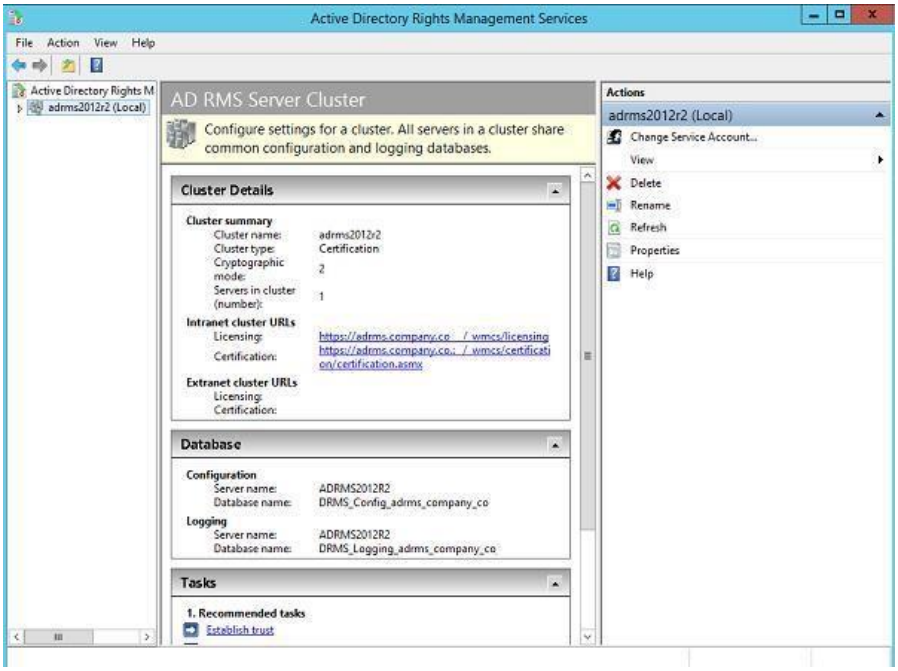


Рис. 56

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.

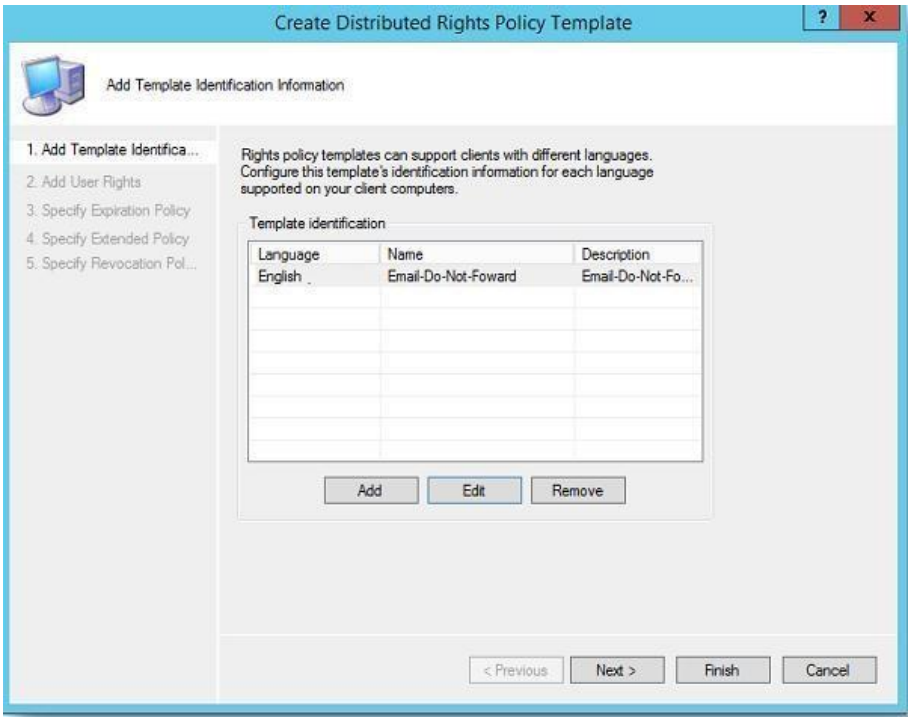


Рис. 57

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

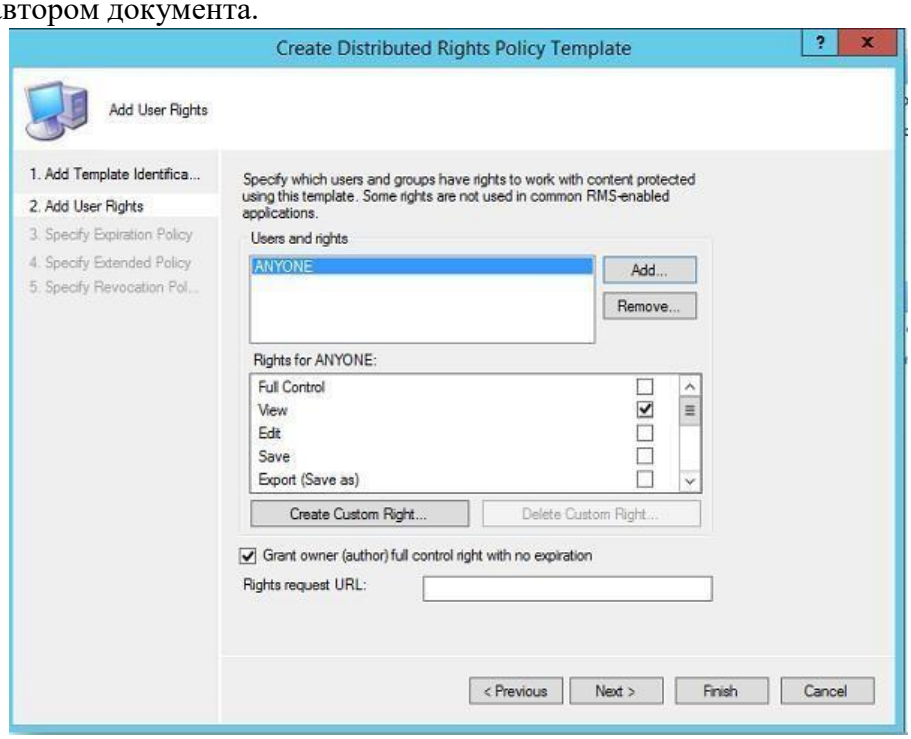


Рис. 58

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

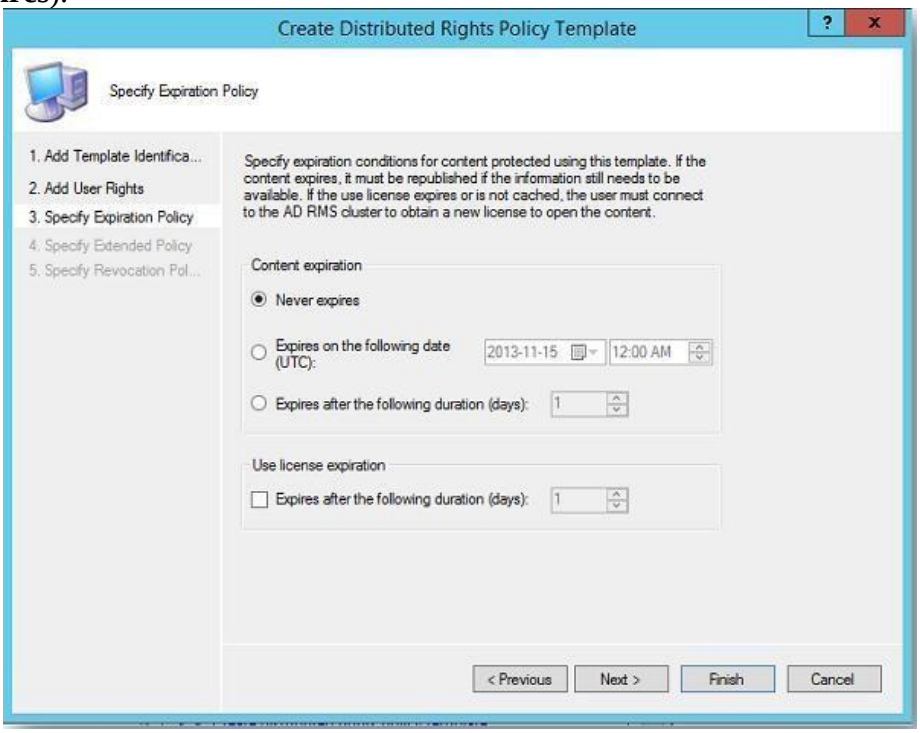


Рис. 59

1.16 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**).

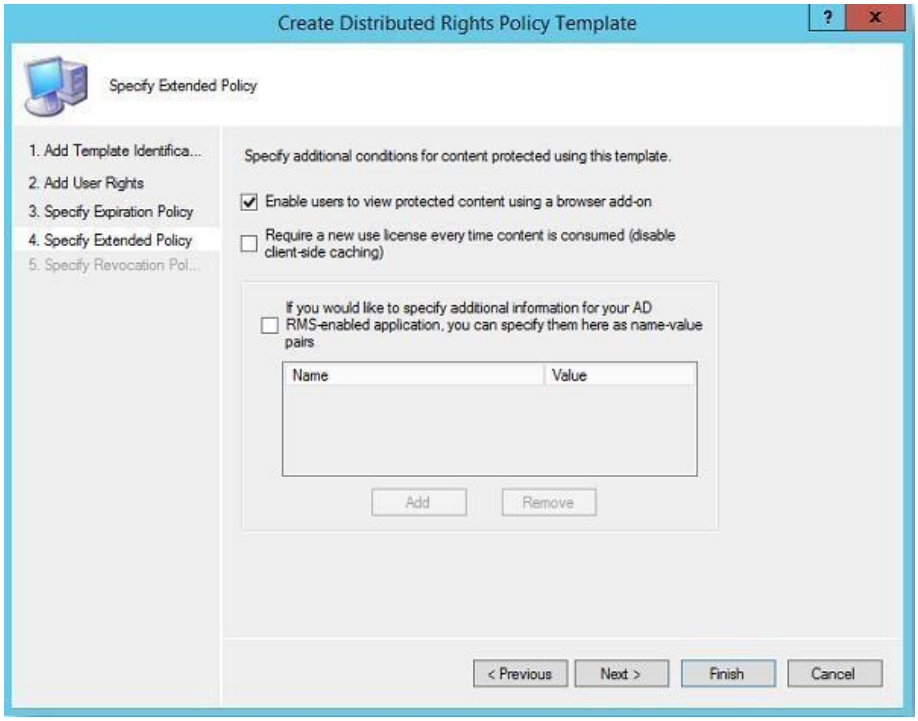
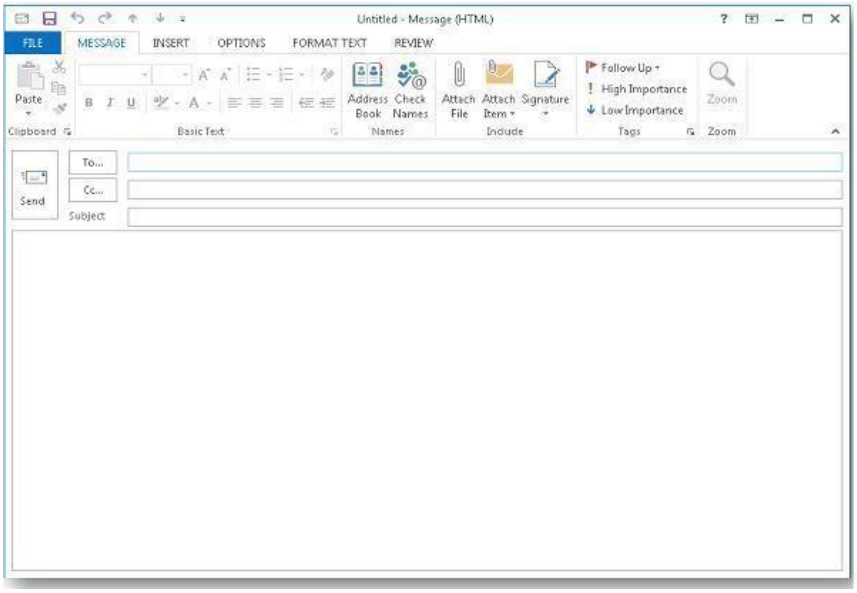
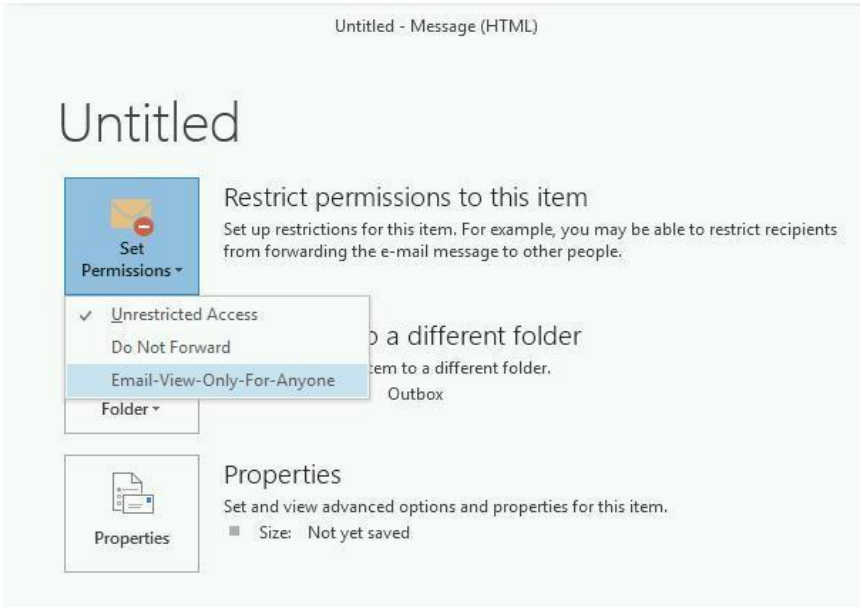


Рис. 60

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.

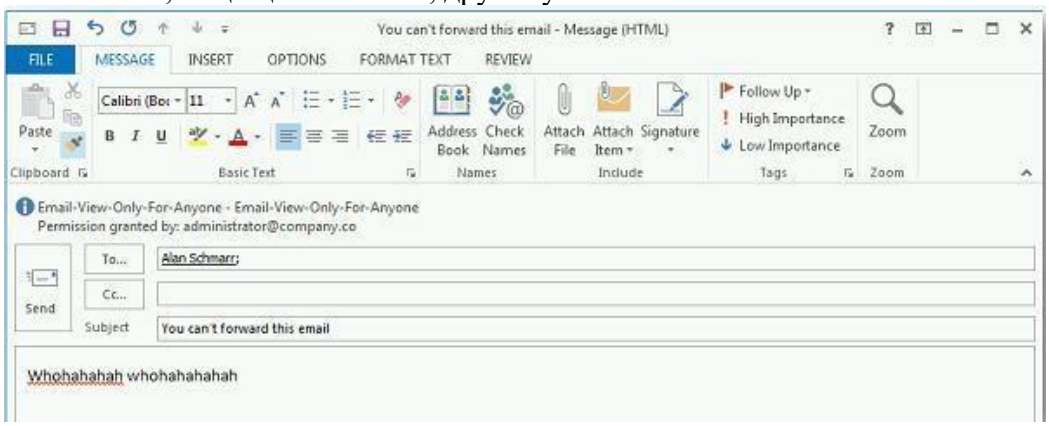


Рис. 61

1.17 Посмотрим, как выглядит защищенное письмо в ящике получателя.

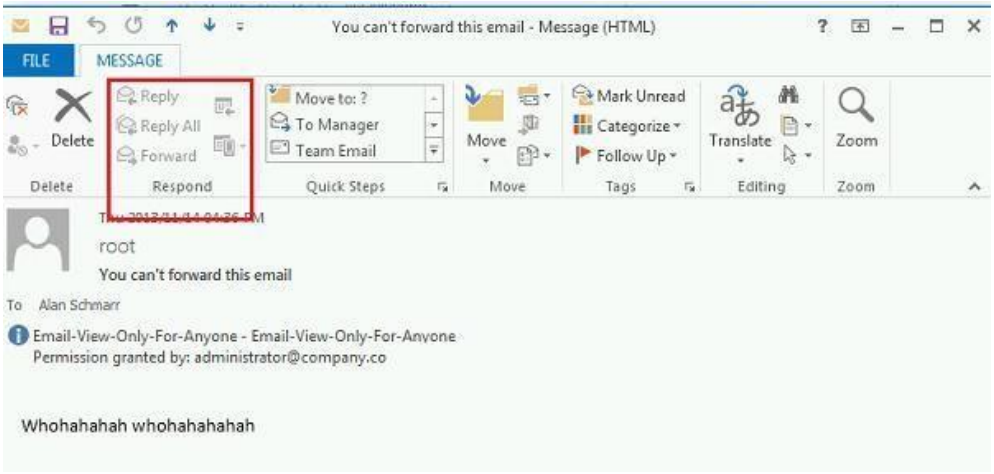


Рис. 62

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.

2.4. Практическая работа № 4 «Подключение сетевых периферийных устройств через Групповую политику»

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

1.1 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
```

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

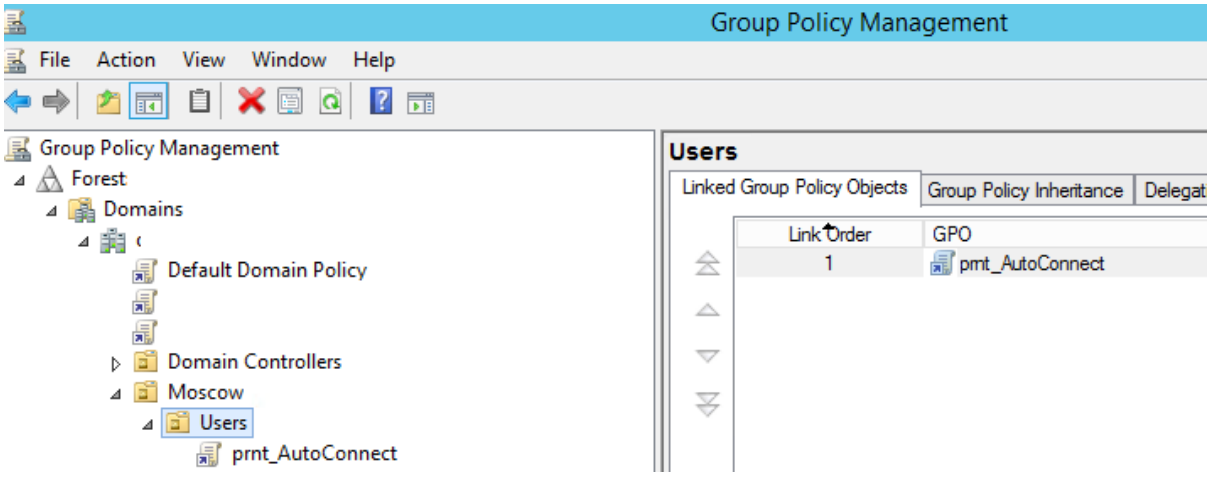


Рис. 63

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.

1.3 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**.

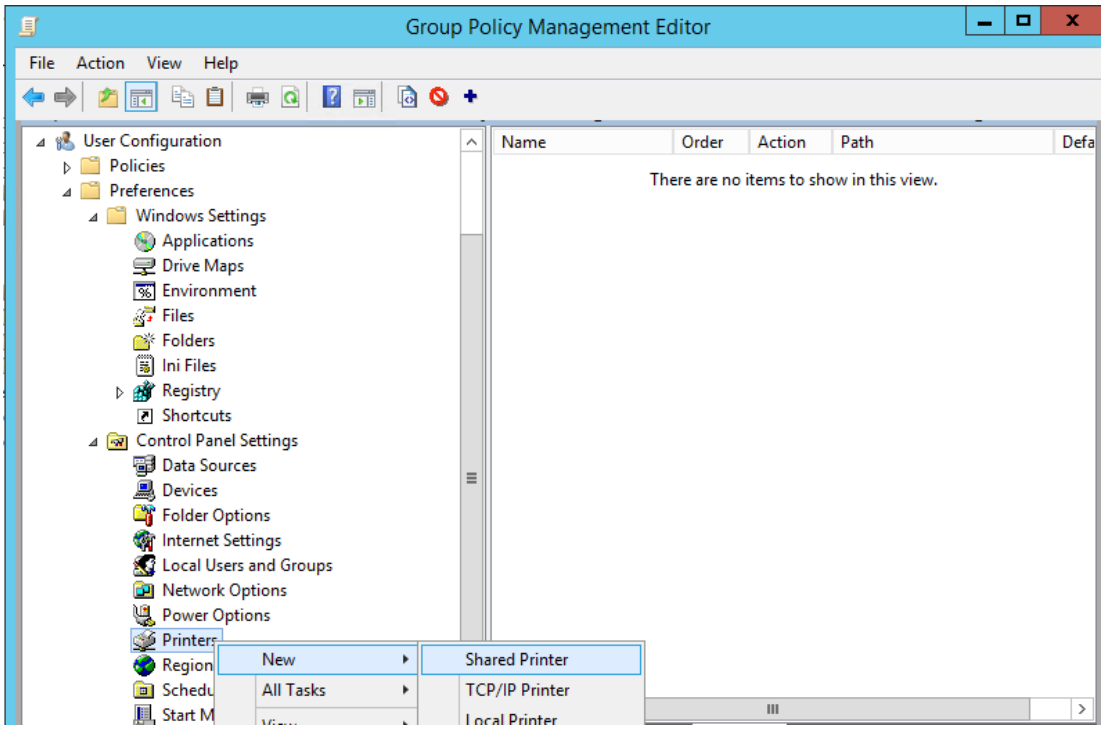


Рис. 64

1.4 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;

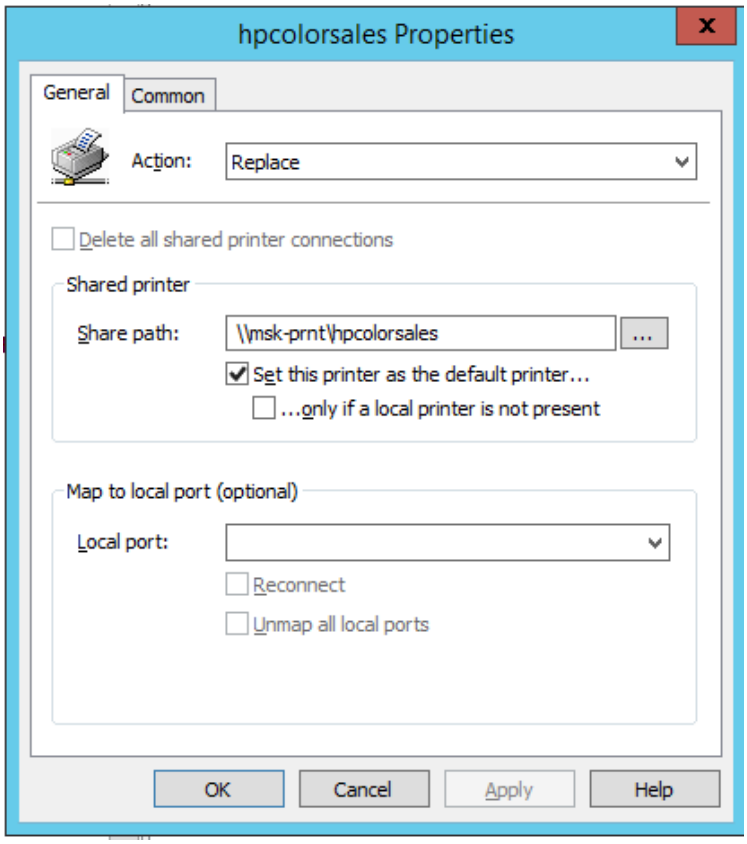


Рис. 65

1.5 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**;

1.6 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;

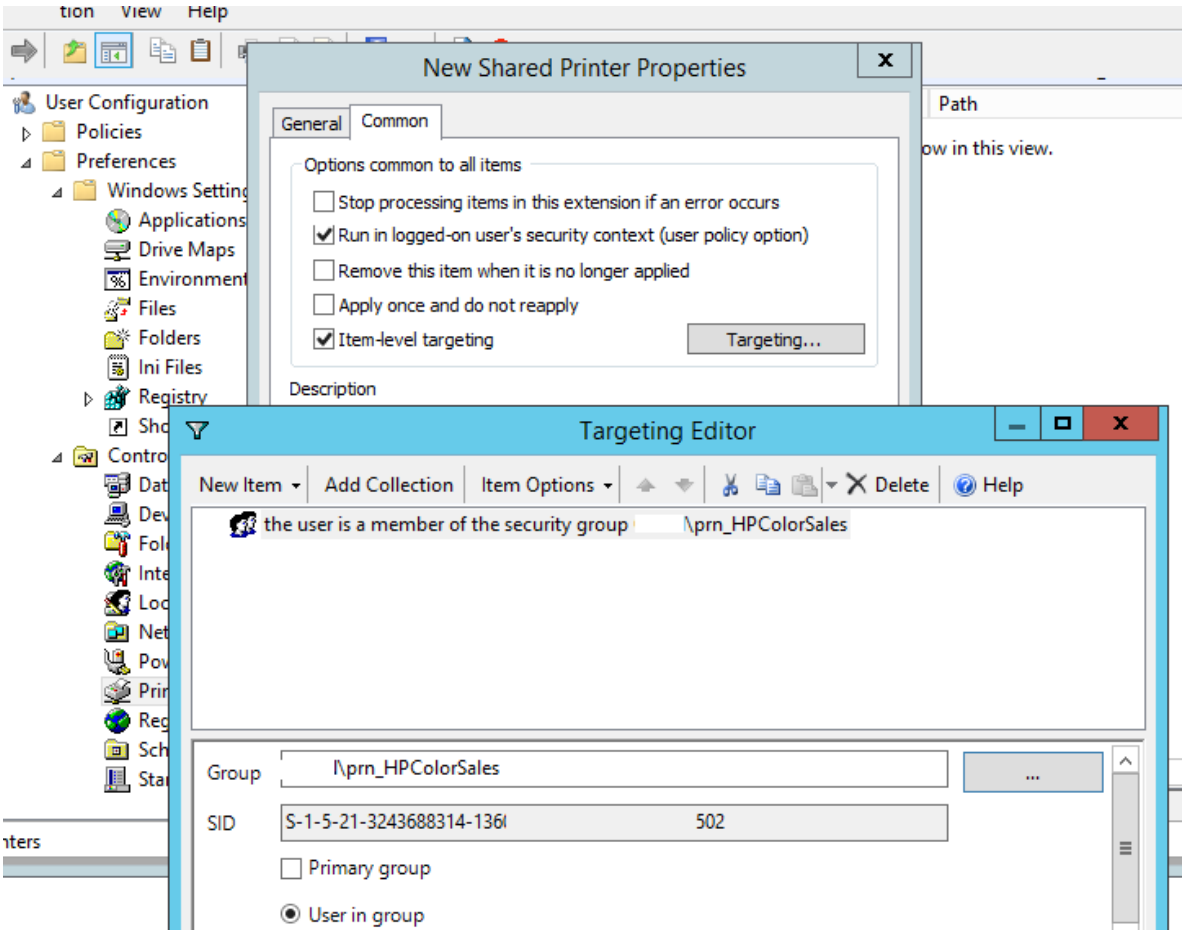


Рис. 66

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.

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

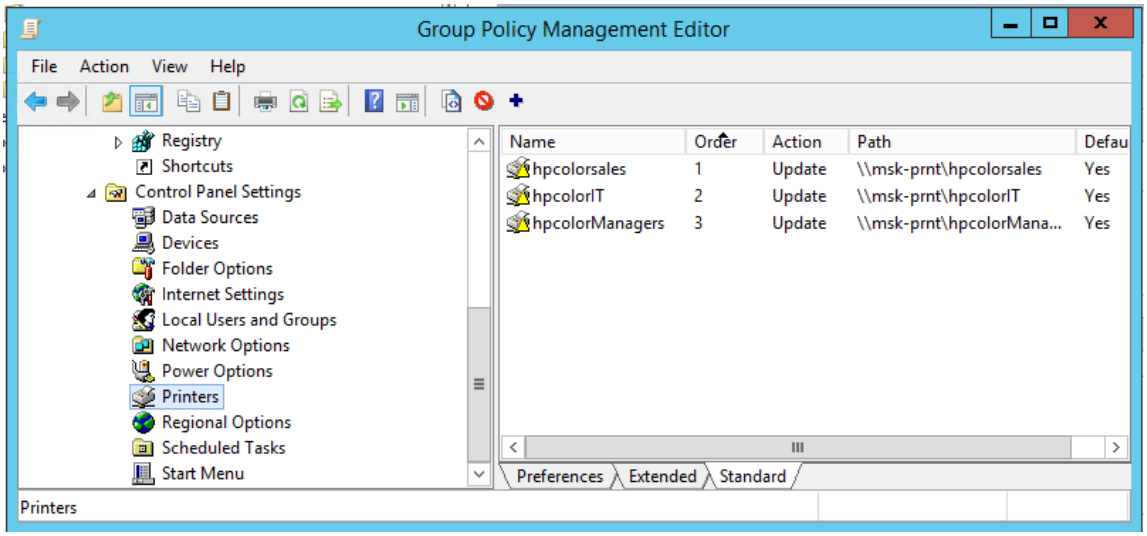


Рис. 67

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

2.1 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.

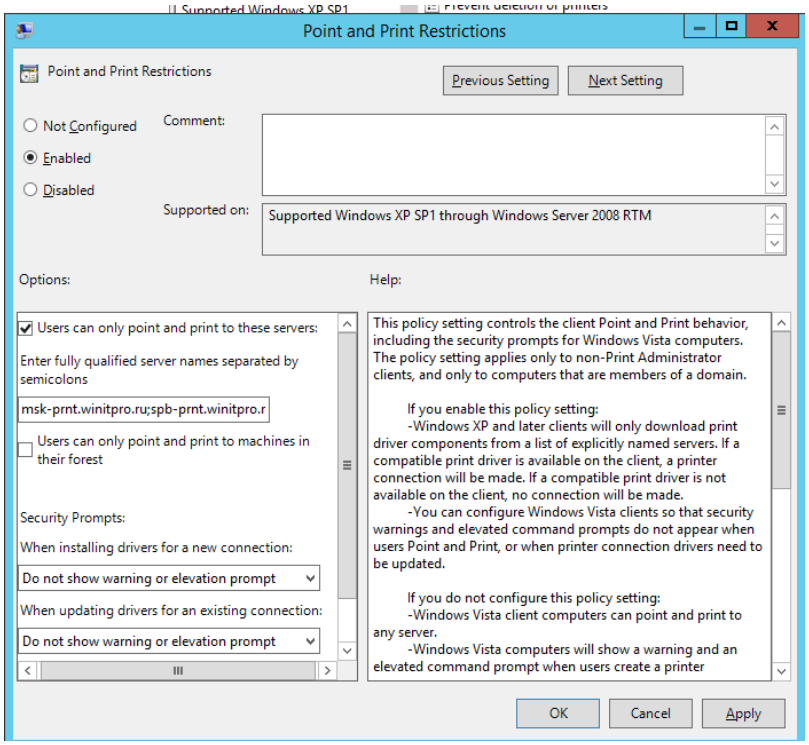


Рис. 68

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.

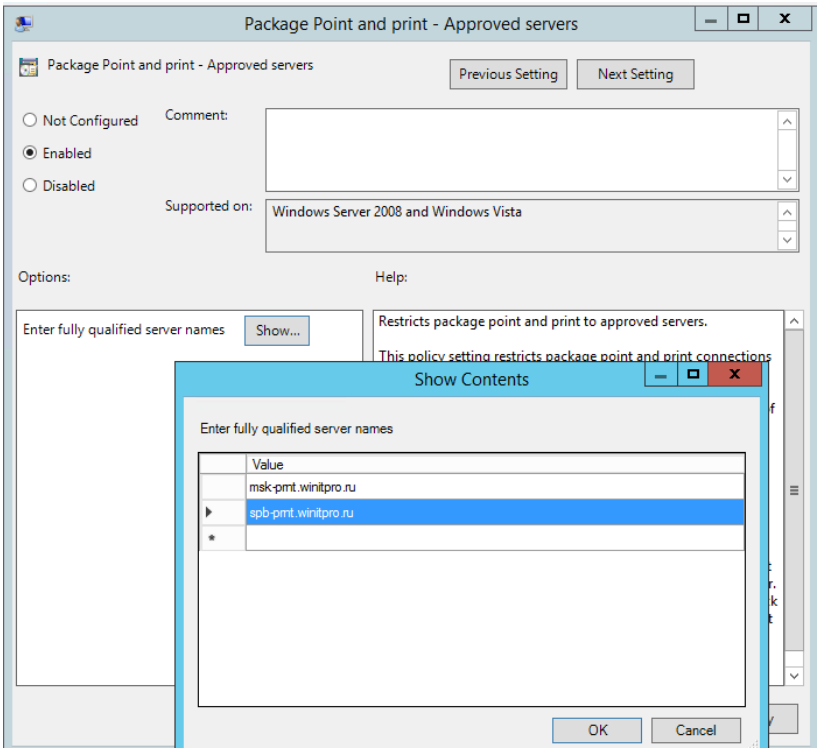


Рис. 69

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 «Установка и настройка сервера времени и сервера лицензирования»

Задание:

1. Настройка синхронизации времени по NTP с помощью групповых политик

Служба времени Windows, несмотря на кажущуюся простоту, является одной из основ, необходимых для нормального функционирования домена Active Directory. В правильно настроенной среде AD служба времени работает следующим образом: компьютеры пользователей получают точное время от ближайшего контроллера домена, на котором они зарегистрировались. Все контроллеры домена в свою очередь получают точное время от DC с FSMO ролью «**Эмулятор PDC**», а контролер PDC синхронизирует свое время с неким внешним источником времени. В качестве внешнего источника времени может выступать один или несколько NTP серверов, например time.windows.com или NTP сервер вашего Интернет-провайдера. Также нужно отметить, что по умолчанию клиенты в домене синхронизируют время с помощью службы времени Windows (Windows Time), а не с помощью протокола NTP.

Если вы столкнулись с ситуацией, когда время на клиентах и контроллерах домена различается, возможно, в вашем домене есть проблемы с синхронизацией времени и эта статья будет вам полезна.

В первую очередь выберите подходящий NTP сервер, который вы могли бы использовать. Список общедоступных NTP серверов доступен на сайте http://ntp.org. В нашем примере мы будем использовать NTP сервера из пула ru.pool.ntp.org:

- 0.ru.pool.ntp.org
- 1.ru.pool.ntp.org
- 2.ru.pool.ntp.org
- 3.ru.pool.ntp.org

Настройка синхронизации времени в домене с помощью групповых политик состоит из двух шагов:

1) Создание GPO для контроллера домена с ролью PDC

2) Создание GPO для клиентов (опционально)

2. Настройка политики синхронизации NTP на контролере домена PDC

2.1 Этот шаг предполагает настройку контроллера домена с ролью эмулятора PDC на синхронизацию времени с внешним NTP сервером. Т.к. теоретически роль эмулятора PDC может перемещаться между контроллерами домена, нам нужно сделать политику, которая применялась бы только к текущему владельцу роли PDC. Для этого в консоли управления **Group Policy Management Console** (GPMC.msc), создадим новый WMI фильтр групповых политик. Для этого в разделе **WMI Filters** создадим фильтр и именем **PDC Emulator** и WMI запросом: `Select * from Win32_ComputerSystem where DomainRole = 5`

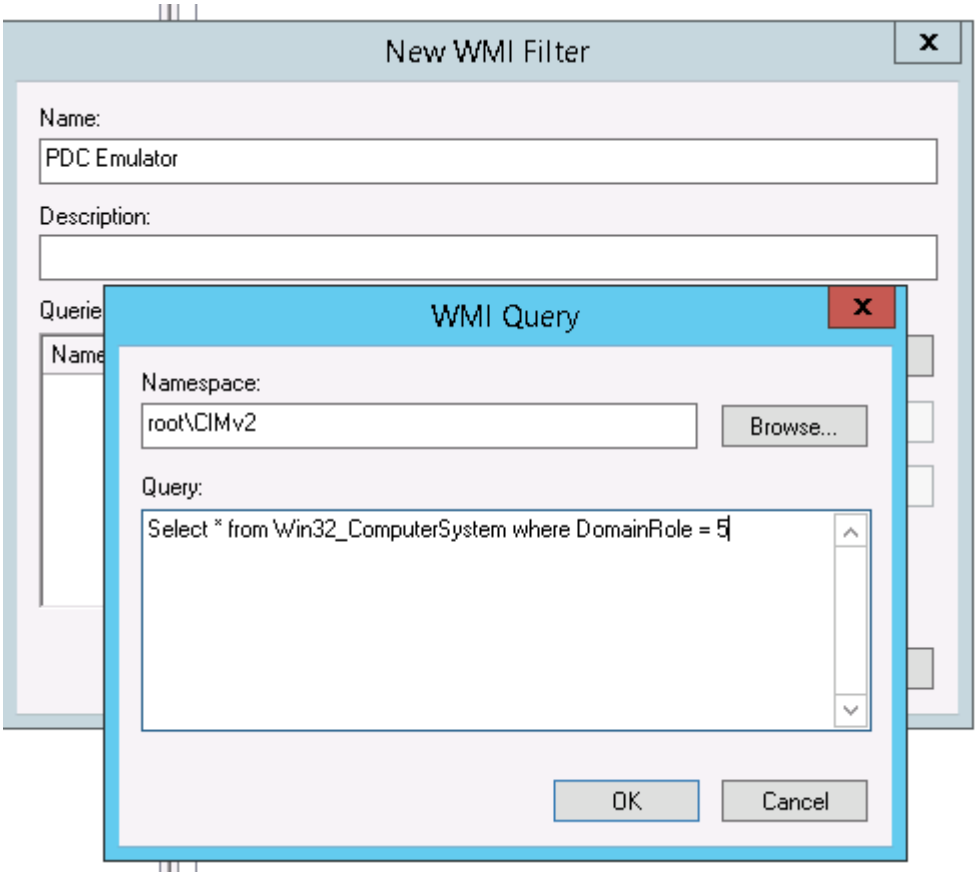


Рис. 70

2.2 Затем создайте новую GPO и назначьте ее на контейнер Domain Controllers.

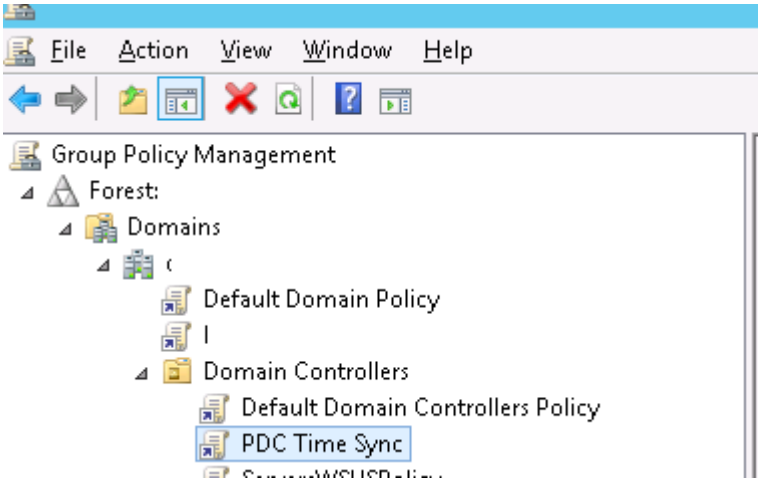


Рис. 71

2.3 Перейдите в режим редактирования политики и разверните следующий раздел политик: **Computer Configuration->Administrative Templates->System->Windows Time Service->Time Providers**

Нас интересуют три политики:

- **Configure Windows NTP Client**: Enabled (настройки политики описаны ниже)
- **Enable Windows NTP Client**: Enabled
- **Enable Windows NTP Server**: Enabled

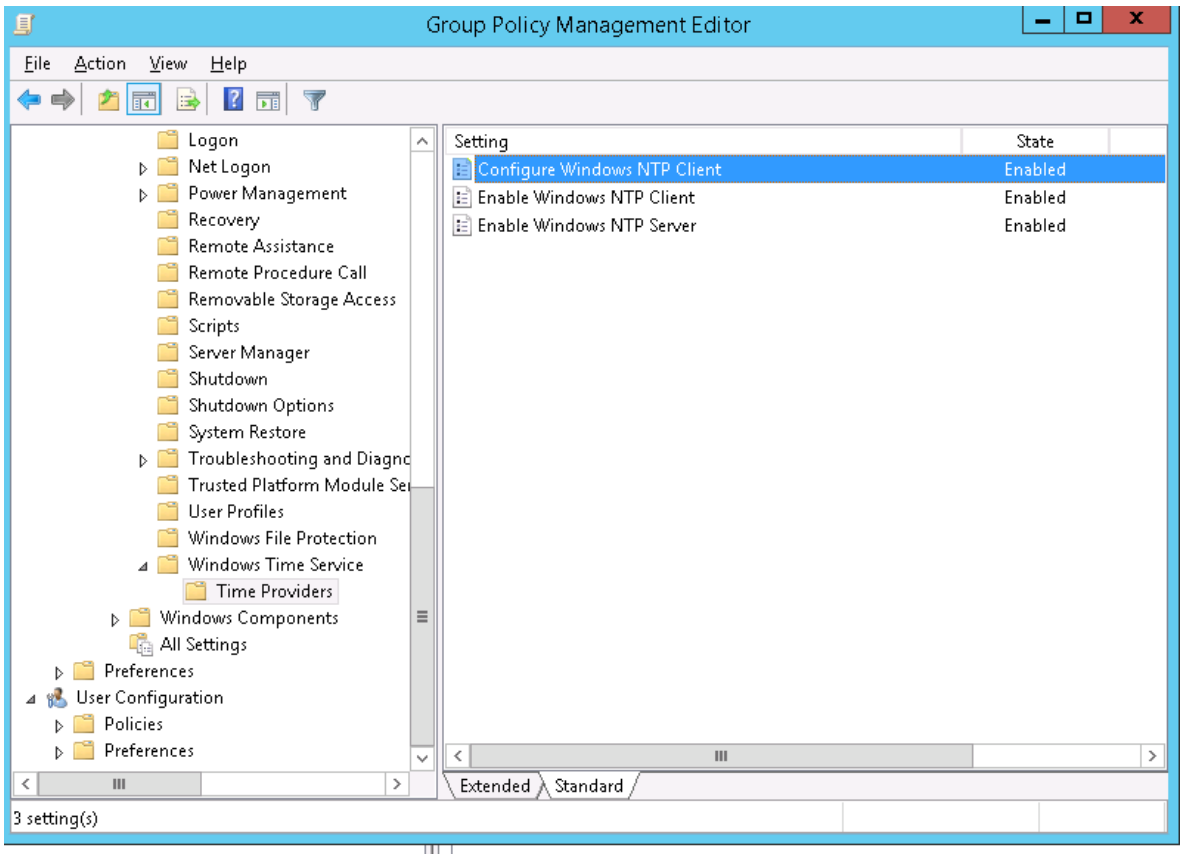


Рис. 72

2.4 В настройках политики *Configure Windows NTP Client* укажите следующие параметры:

- **NtpServer**: 0.ru.pool.ntp.org,0x1 1.ru.pool.ntp.org,0x1 2.ru.pool.ntp.org,0x1 3.ru.pool.ntp.org,0x1
- **Type**: NTP
- **CrossSiteSyncFlags**: 2
- **ResolvePeerBackoffMinutes**: 15
- **Resolve Peer BAckoffMaxTimes**: 7
- **SpecilalPoolInterval**: 3600
- **EventLogFlags**: 0

Совет. Не забудьте настроить межсетевой экран таким образом, чтобы сервер PDC мог получить доступ к внешним NTP серверам по протоколу NTP (UDP порт 123).

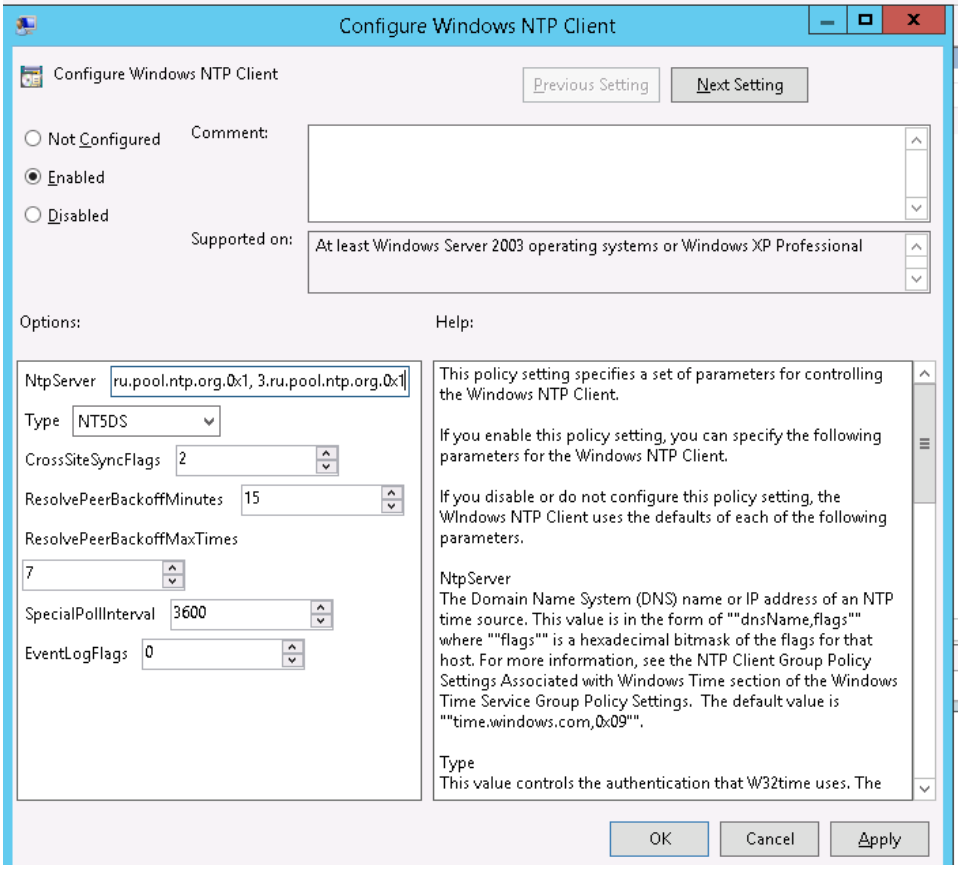


Рис. 73

Примечание. Обратите внимание на синтаксис в поле **NtpServer.** Формат указания нескольких NTP серверов такой:**ntsrv1.org,0x1 ntpsrv2.org,0x1** (разделитель пробел). На скриншоте указаны ошибочные данные!

Примените созданный ранее фильтр **PDC Emulator** к данной политике.

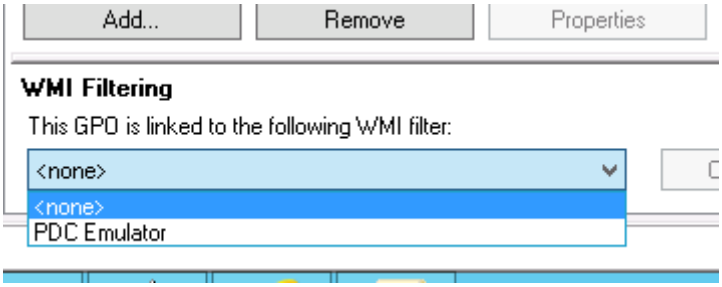


Рис. 74

Совет. Найти имя сервера с ролью PDC можно с помощью команды: netdom query fsmo

2.5 Осталось обновить политики на контроллере PDC:

```
gpupdate /force
```

Вручную запустите синхронизацию времени:

```
w32tm /resync
```

Проверьте текущие настройки NTP:

```
w32tm /query /status
```

Совет. В том случае, если время не синхронизировалось, перезапустите службу времени Windows и сбросьте текущие настройки:

```
net stop w32time
w32tm.exe /unregister
w32tm.exe /register
net start w32time
```

3. Настройка синхронизации времени на клиентах домена

В среде Active Directory по умолчанию клиенты домена синхронизируют свое время с контролерами домена (опция **Nt5DS** – синхронизировать время согласно иерархии домена). Как правило, эта схема работает и не требует перенастройки. Однако при наличии проблем с синхронизацией времени на клиентах домена, можно попробовать принудительно назначить сервер времени для клиентов с помощью GPO.

3.1 Для этого создайте новую GPO и назначьте ее на контейнеры (OU) с компьютерами. В редакторе GPO перейдите в раздел **Computer Configuration -> Administrative Templates -> System -> Windows Time Service -> Time Providers** и включите политику **Configure Windows NTP Client**.

В качестве сервера NTP укажите имя или ip адрес PDC, например msk-dc1.winitpro.ru,0x9, а в качестве типа синхронизации — NT5DS

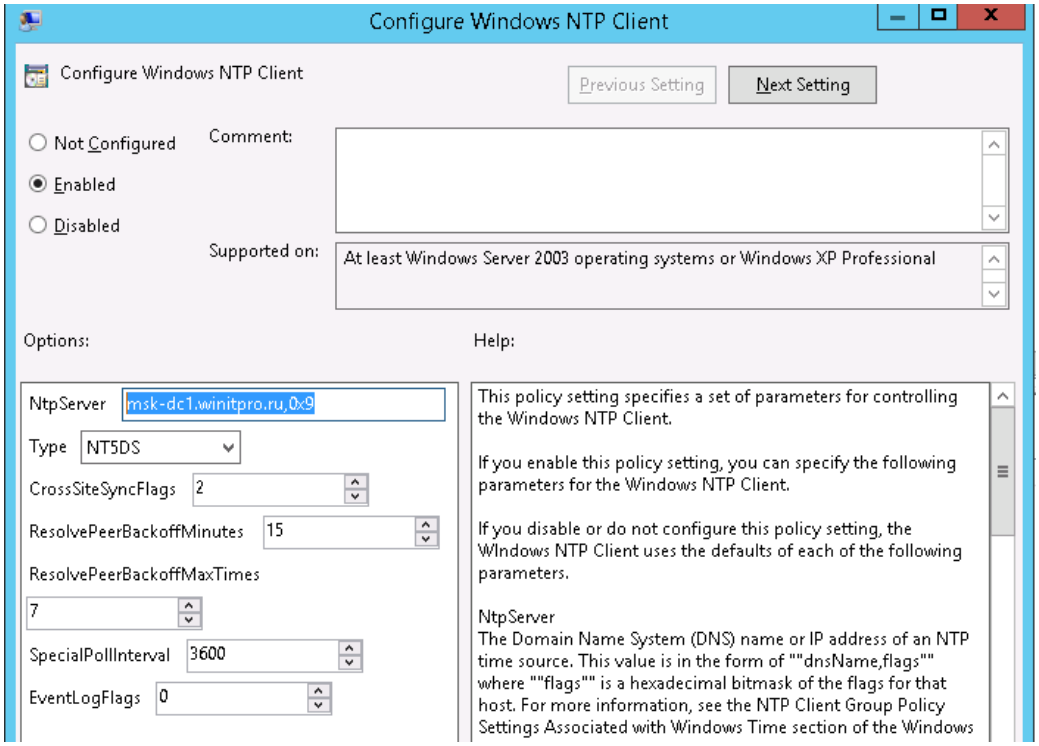


Рис. 75

3.2 Обновите настройки групповых политик на клиентах и проверьте, что клиенты успешно синхронизировали свое время с PDC.

Совет. Указанная схема применима только к небольшим доменам. Для больших распределенных доменов с большим количеством DC и сайтов придется создать отдельную политику для каждого сайта, чтобы клиенты синхронизировали свое время с DC в сайте.

4. Установка KMS сервера на базе Windows Server 2012 R2

Собственный KMS сервер позволяет значительно упростить процесс активации продуктов Microsoft в корпоративной сети, и в отличии от обычной процедуры активации, не требует предоставления каждому компьютеру доступа в интернет к серверам активации Майкрософт. Инфраструктура KMS достаточно простая, надежная и легко расширяется (один KMS сервер может обслуживать тысячи клиентов).

В этой статье мы опишем процесс установки в локальной корпоративной сети KMS сервера на базе Windows Server 2012 R2 и его активацию.

Основные аспекты функционирования технологии KMS активации продуктов Microsoft довольно подробно описаны в статье FAQ по KMS активации продуктов Microsoft.

4.1 Установка и настройка роли Volume Activation Services

Для работы службы KMS нужно установить и настроить отдельную роль сервера — **Volume Activation Services**. Сделать это можно с помощью консоли Server Manage или PowerShell:

```
Install-WindowsFeature -Name VolumeActivation  -IncludeAllSubFeature
```

При установке через графический интерфейс консоли Server Manager, запустите мастер установки ролей (Add Roles and Features Wizard), и на этапе выбора ролей сервера (Server Roles) выберите пункт **Volume Activation Services**.

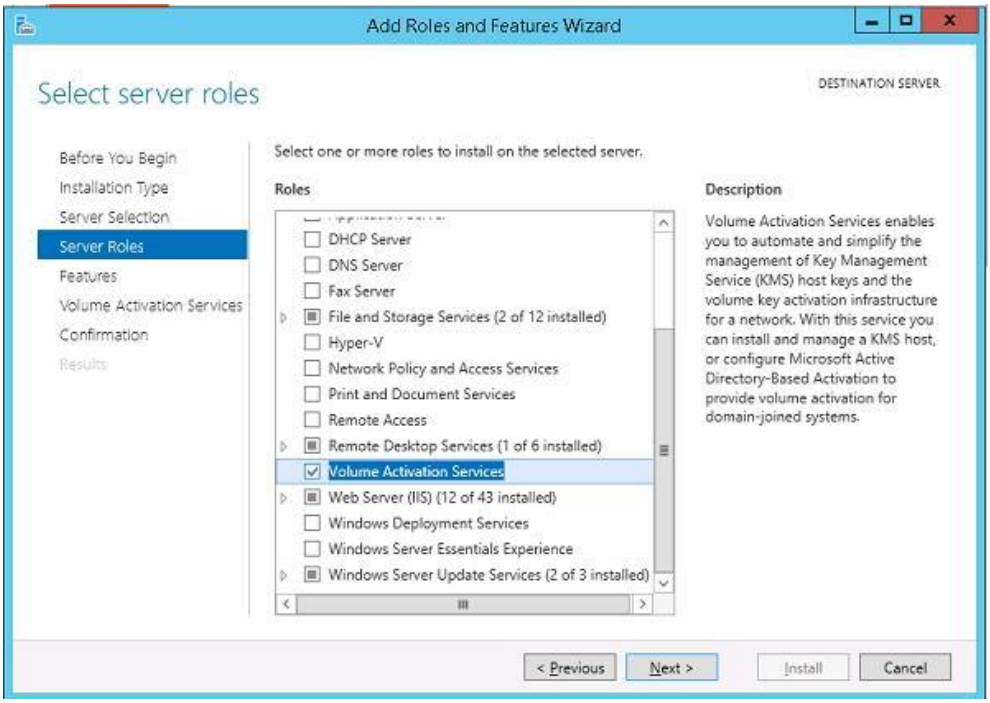


Рис. 76

После окончания установки запустите консоль Volume Activation Tools. Запустится мастер установки службы активации. Укажите, что будет устанавливаться сервер Key Management Service (KMS).

Примечание. Если все ОС Windows, которые будут активироваться на KMS сервере, состоят в одном домене Active Directory и используемые в сети версии ОС не ниже Windows 8 / Windows Server 2012 — можно воспользоваться специальным расширением технологии KMS – Active Directory Based Activation, активацией через AD.

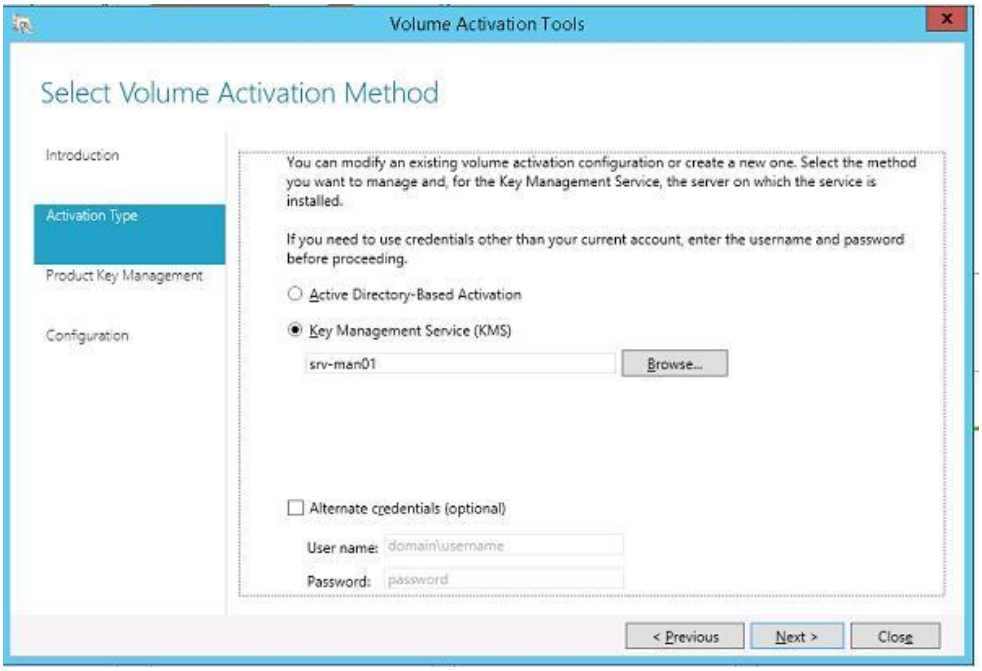


Рис. 77

Примечание. Учетная запись, из-под которой выполняется настройка KMS сервера, должна обладать правами Enterprise Admin.

Далее на сайте Microsoft (https://www.microsoft.com/Licensing/servicecenter/home.aspx) в личном разделе необходимо получить свой корпоративный KMS ключ (KMS host key, это ключ активации KMS сервера). Найти его можно в разделе **Downloads and Keys -> Windows Server -> Windows Server 2012 R2**.

Рис. 78

Найдите ключ с типом KMS (не MAK) и скопируйте его в буфер обмена.

Вставьте скопированный KMS ключ в соответствующее поле мастера установки KMS сервера (Install your KMS host key).

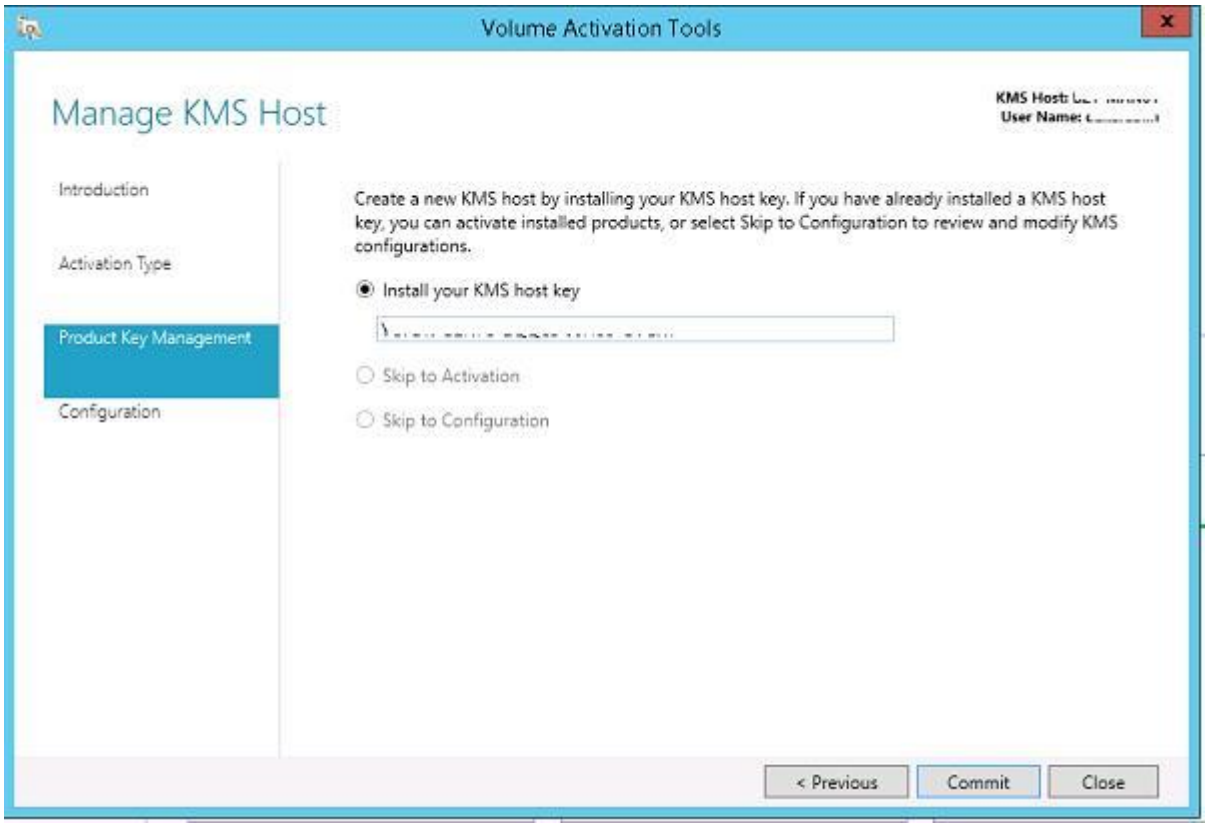


Рис. 79

Если система примет ключ, сразу же будет предложено его активировать. На основании введенного ключа система определит продукт, к которому он относится, и предложит два варианта активации (по телефону или Интернету). Во втором случае придется предоставить серверу временный доступ в Интернет (только на период активации).

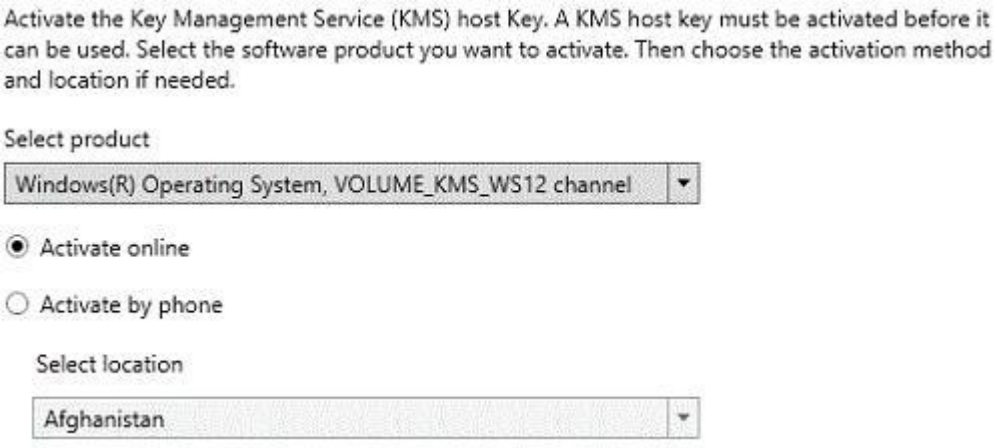


Рис. 80

После активации ключа, нужно настроить параметры службы управления ключами: интервал активации и реактивации (по умолчанию клиенты продляют активацию каждые 7 дней), порт (по умолчанию служба KMS использует TCP порт 1688), исключения для Windows Firewall. Чтобы автоматически создать запись в DNS, необходимую для автоматического поиска сервера KMS в домене (SRV запись _vlmcs._tcp), включите опцию **DNS Records – Publish**.

Если KMS сервер должен обслуживать клиентов из разных доменов, можно опубликовать DNS записи в других DNS зонах. Укажите данные зоны в списке **Publish to Custom DNS zones.**

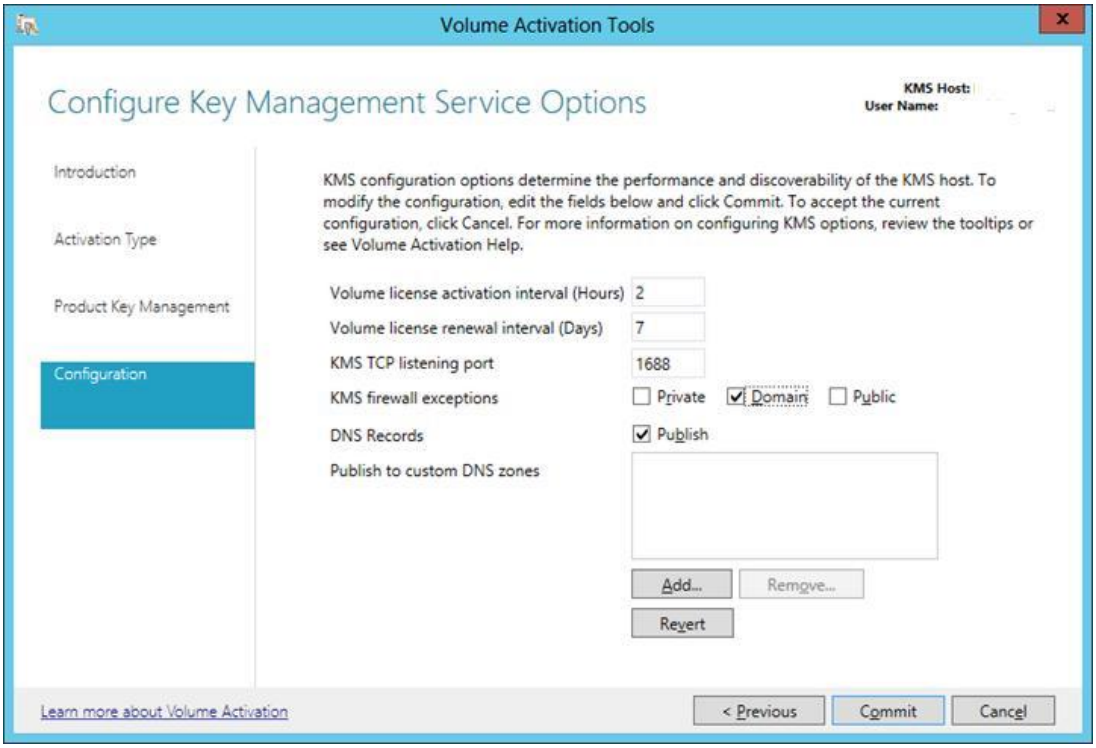


Рис. 81

Примечание. Если у вас включен Windows Firewall, убедитесь, что активно правило, разрешающее входящие подключения на порт 1688. Если правила нет, включите правило брандмауэра из PoSh:

```
Get-NetFirewallRule -DisplayName *key*

Enable-NetFirewallRule -Name SPPSVC-In-TCP
```

```
PS C:\Windows\system32> Get-NetFirewallRule -DisplayName *Key*


Name                  : SPPSVC-In-TCP
DisplayName           : Key Management Service (TCP-In)
Description           : Inbound rule for the Key Management Service t
                        ine counting and license compliance. [TCP 168
DisplayGroup          : Key Management Service
                        llAPI.dll,-28002
Enabled               : False
Profile               : Any
Platform              : {}
Direction             : Inbound
Action                : Allow
EdgeTraversalPolicy   : Block
LooseSourceMapping    : False
LocalOnlyMapping      : False
Owner                 :
PrimaryStatus         : OK
Status                : The rule was parsed successfully from the sto
EnforcementStatus     : NotApplicable
PolicyStoreSource     : PersistentStore
PolicyStoreSourceType : Local



PS C:\Windows\system32> Enable-NetFirewallRule -Name SPPSVC-In-TCP
```

Рис. 82

На это процесс настройки сервера окончен. Проверьте, что в DNS создалась специальная запись, указывающая на ваш kms сервер

```
nslookup -type=srv _vlmcs._tcp.*ваш_домен*
```

Далее получим информацию о текущем состоянии KMS сервера:

```
slmgr.vbs /dlv
```

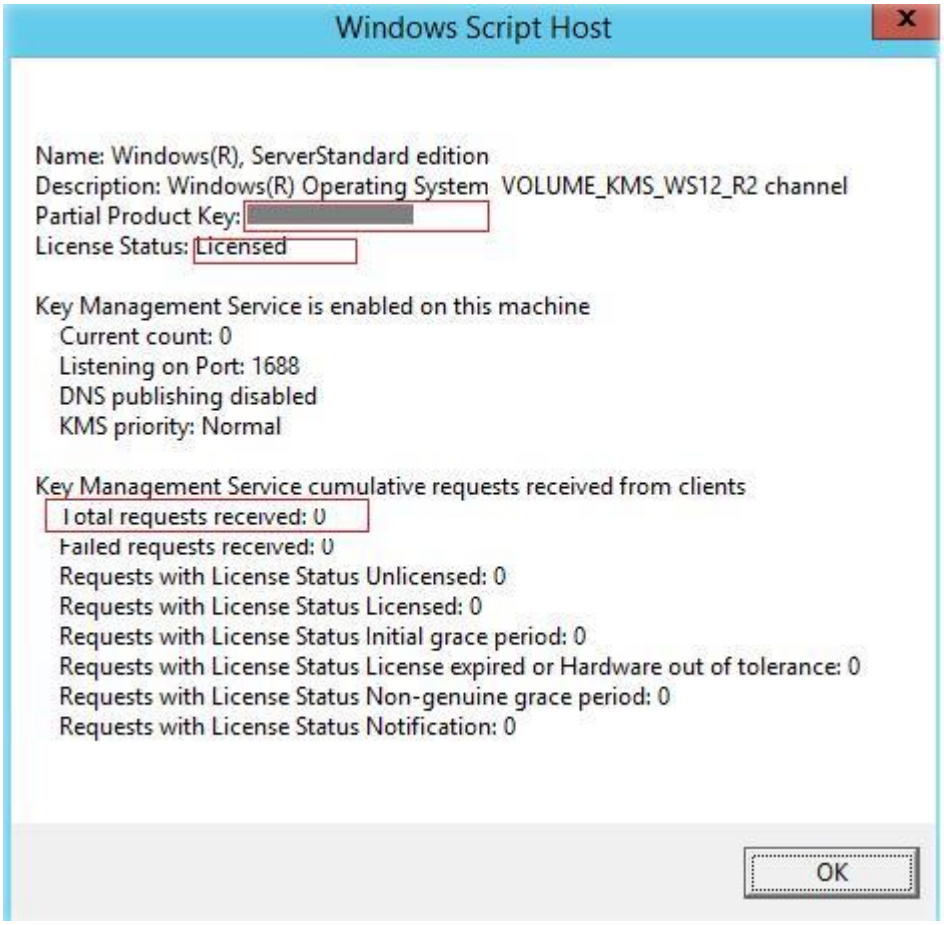


Рис. 83

Нас интересуют следующие поля:

- Partial Product Key – отображены последние 5 символов KMS ключа
- License status – статус активации лицензии (должно быть Licensed)
- Total requests received — количество запросов на активацию от клиентов(пока 0)

Внимание. Напомним, что у KMS сервера есть т.н. порог активации. Это означает, что активированный KMS сервер начинает активировать клиентов, только тогда, когда количество обратившихся к нему за последние 30 дней клиентов превысит предопределенные пороги (activation count):

- Порог активации для клиентских ОС Vista / Windows 7 / Win 8 / Win 10 – 25 клиентов
- Для серверных ОС: Windows Server 2008/ 2008 R2 / 2012 / 2012 R2 / 2016– 5 клиентов

Теперь KMS сервер может активировать клиентов. Что нужно выполнить на стороне клиента для успешной активации на KMS сервере:

1. Задайте на клиенте публичный KMS (GVLK) ключ от соответствующей редакции Windows (ссылка ниже): slmgr /ipk xxxxx- xxxxx - xxxxx - xxxxx – xxxxx

2. Если KMS сервер не опубликован в DNS, укажите его адрес вручную: slmgr /skms kmssrvwinitpro.ru:1688

3. Активируйте ОС командой: slmgr /ato

Активированный KMS сервер ключом для WS 2012 R2 (VOLUME_KMS_WS12_R2 channel) поддерживает активацию всех ОС Windows вплоть до Windows 8.1 / Windows Server 2012 R2 (для поддержки активации Windows 10 и WS 2016 нужно установить специальное обновление и активировать KMS сервер новым ключом).

В том случае, если попытаться установить новый KMS ключ для Windows 10 на KMS сервер под управлением Windows Server 2012 R2 с помощью VAMT без установки указанного обновления, появиться ошибка:

Unable to verify product key. The specified product key is invalid, or is unsupported by this version of VAMT. An update to support additional products may be available online.

Рис. 84

Сделайте скриншоты (фотографии) процесса настройки сервера времени и лицензирования и вставьте в отчёт.

2.6. Практическая работа № 6 «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**.

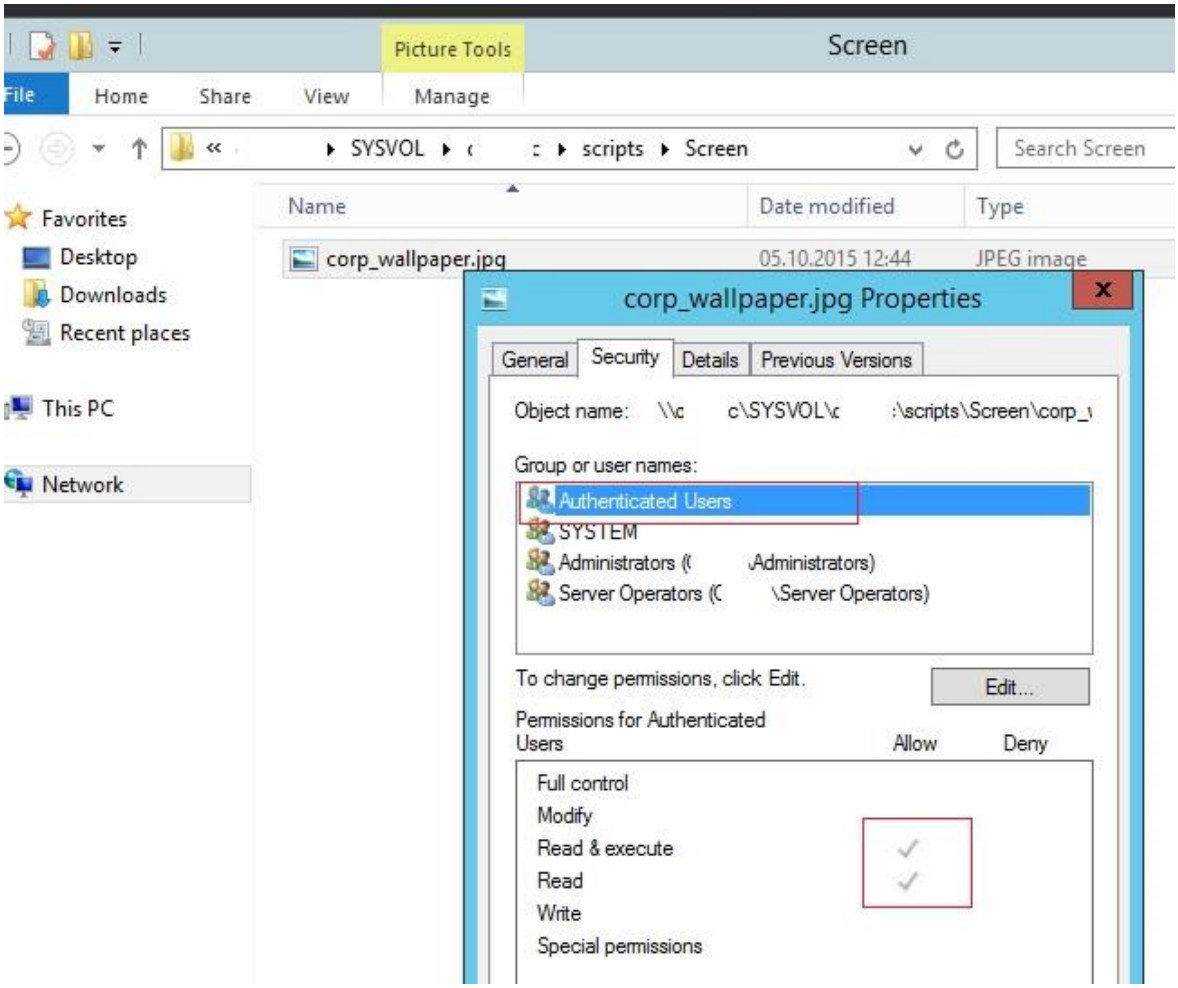


Рис. 85

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).

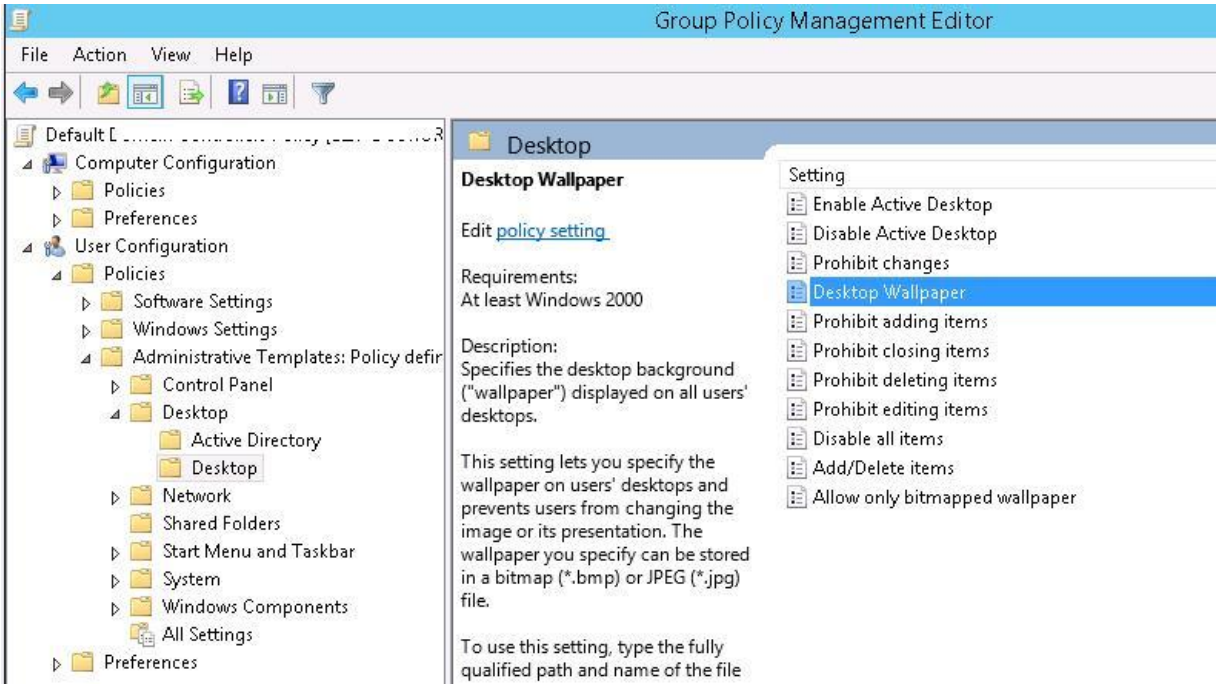


Рис. 86

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

Рис. 87

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.

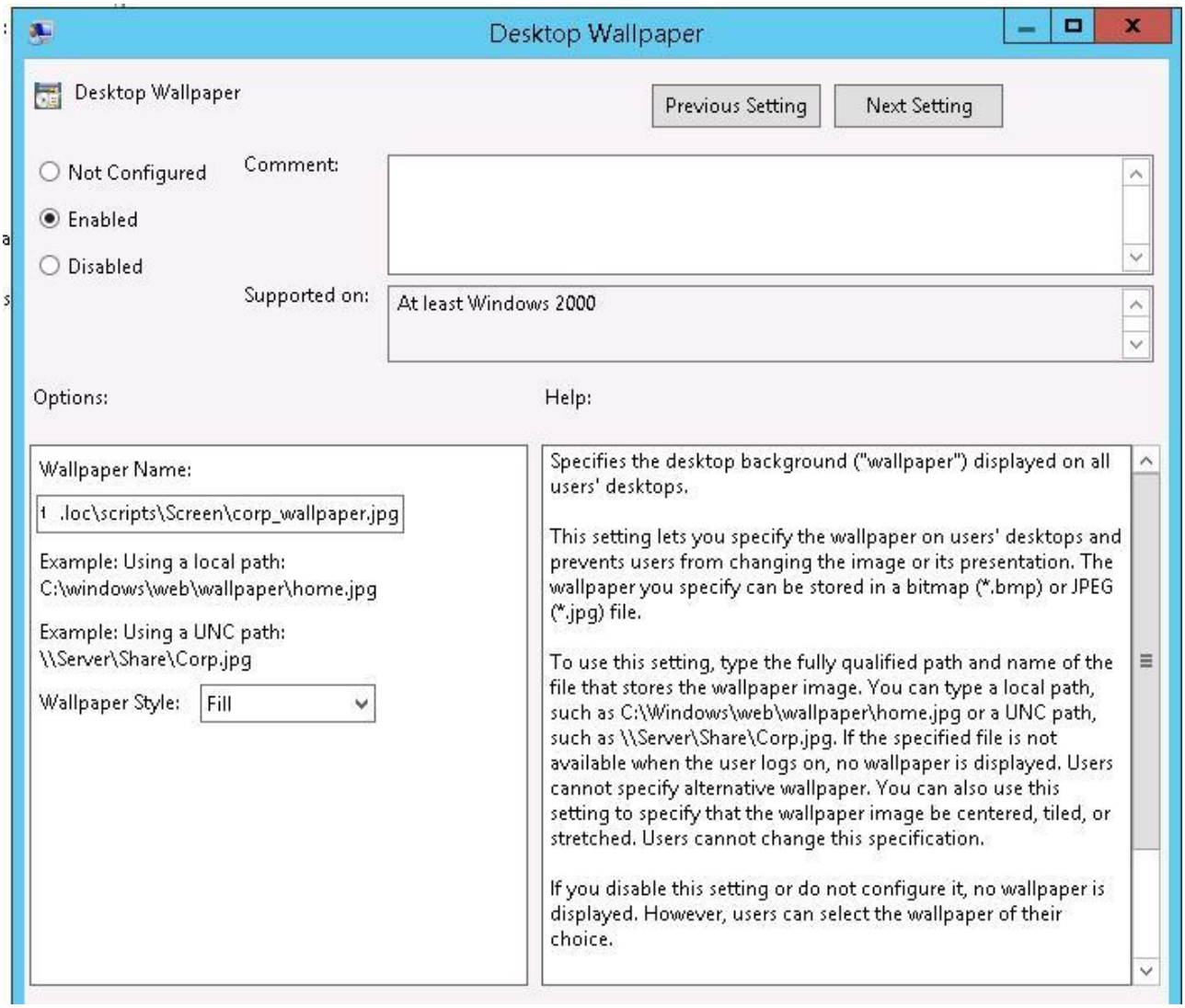


Рис. 88

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**.

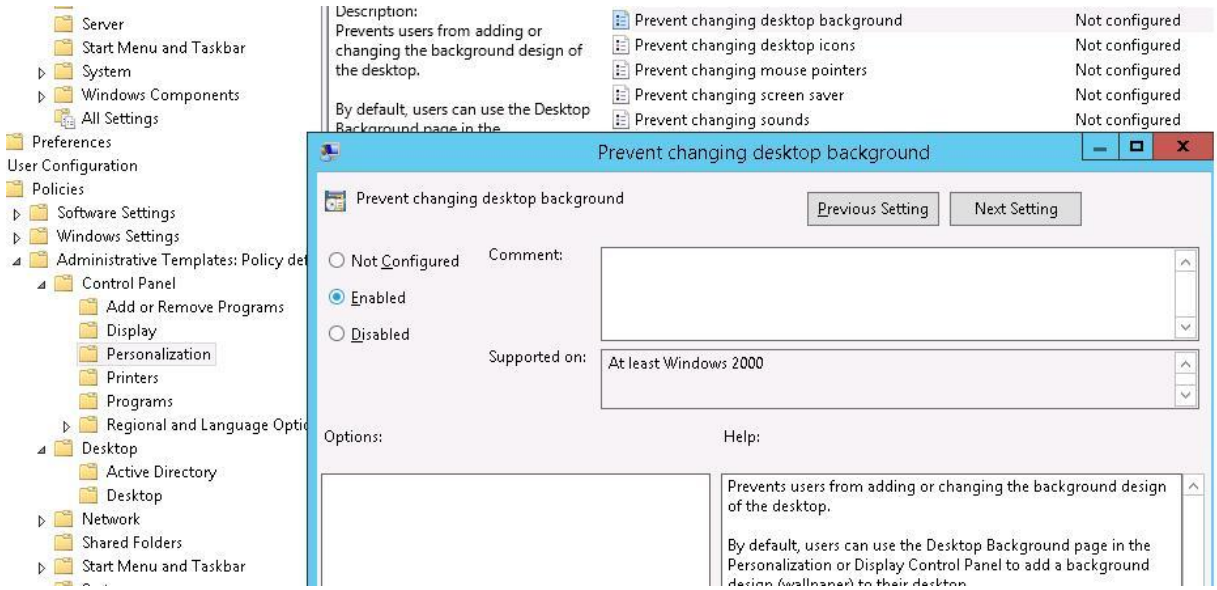


Рис. 89

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 реестра **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.

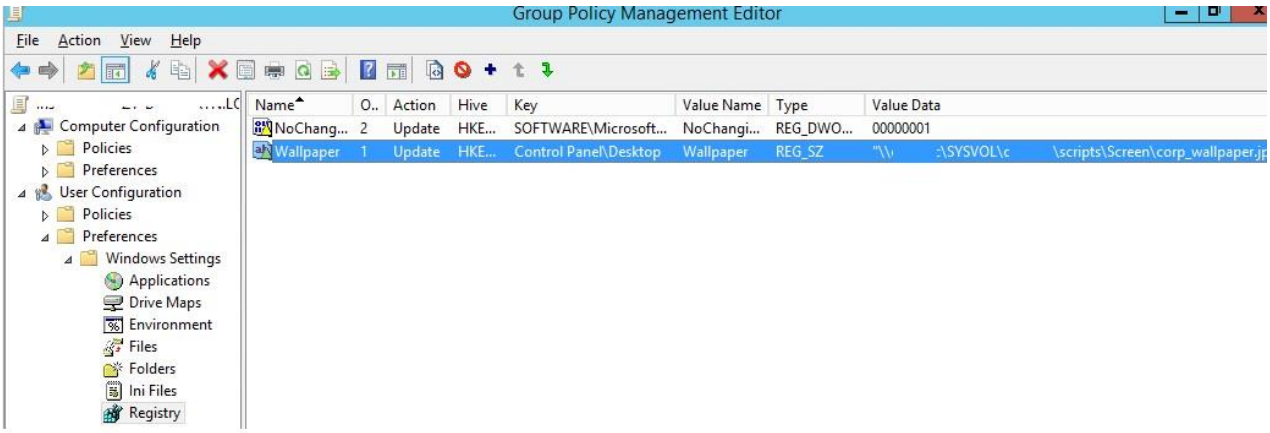


Рис. 90

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.

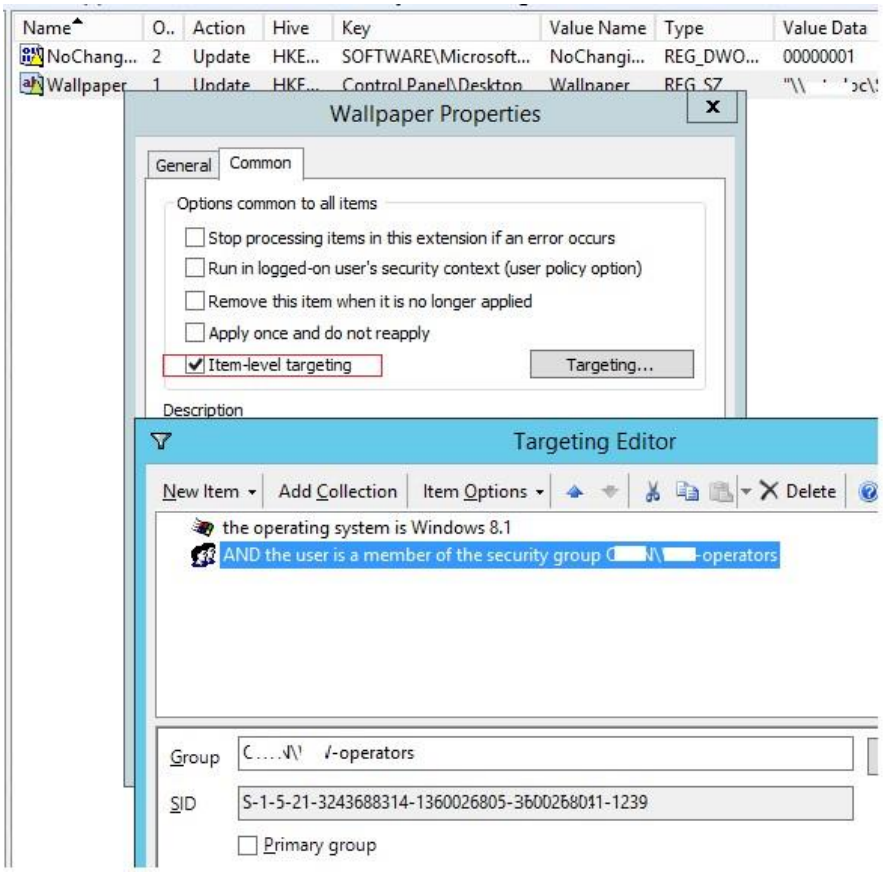


Рис. 91

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\*.*
```

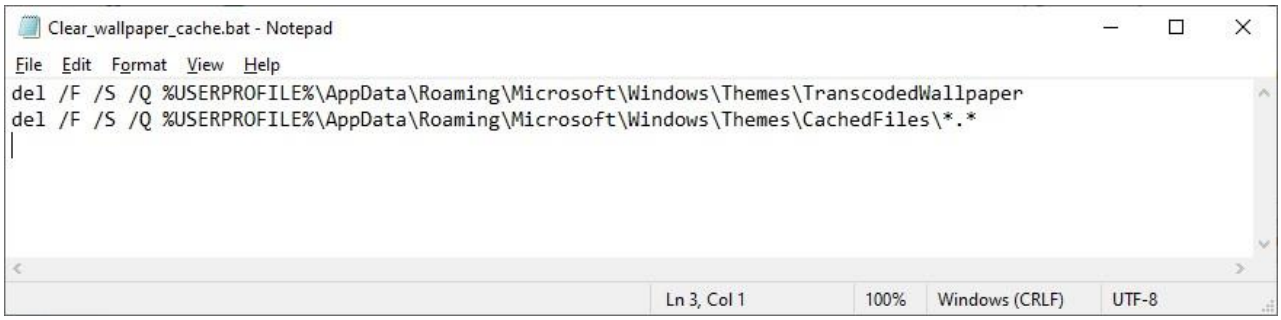


Рис. 92

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.

2.7. Практическая работа № 7 «Установка, настройка и устранение неполадок роли Сервер Сетевой политики»

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**).

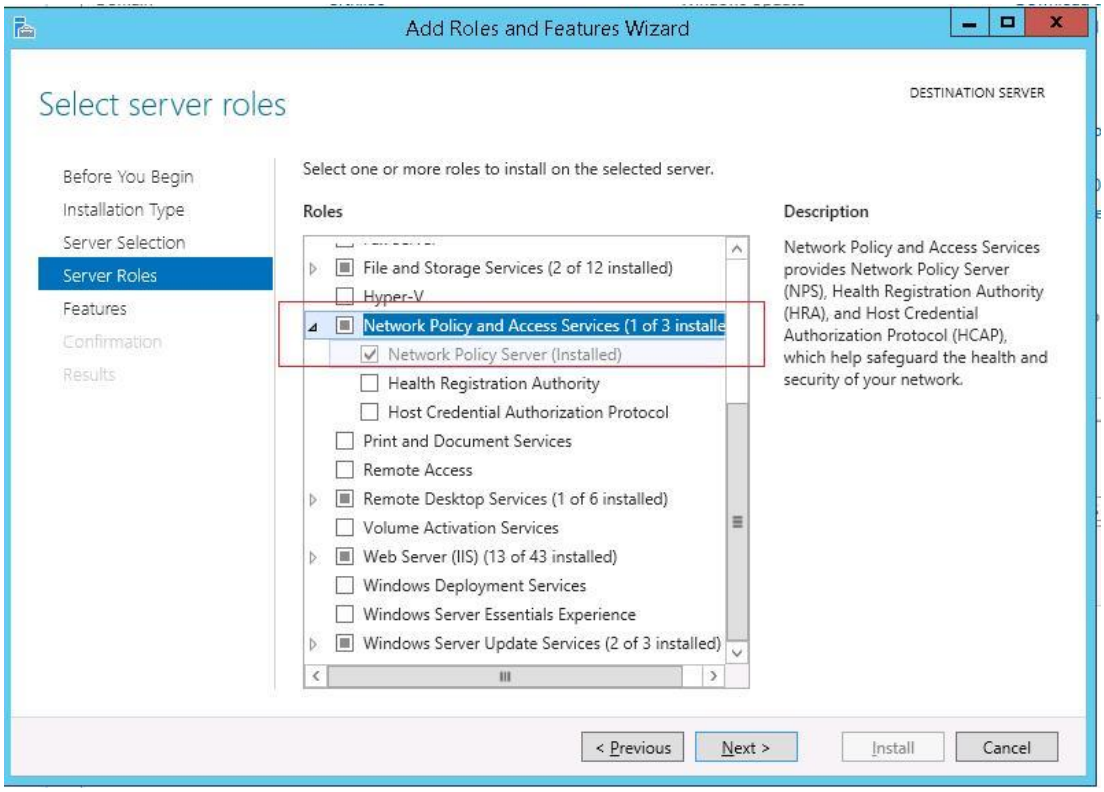


Рис. 93

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

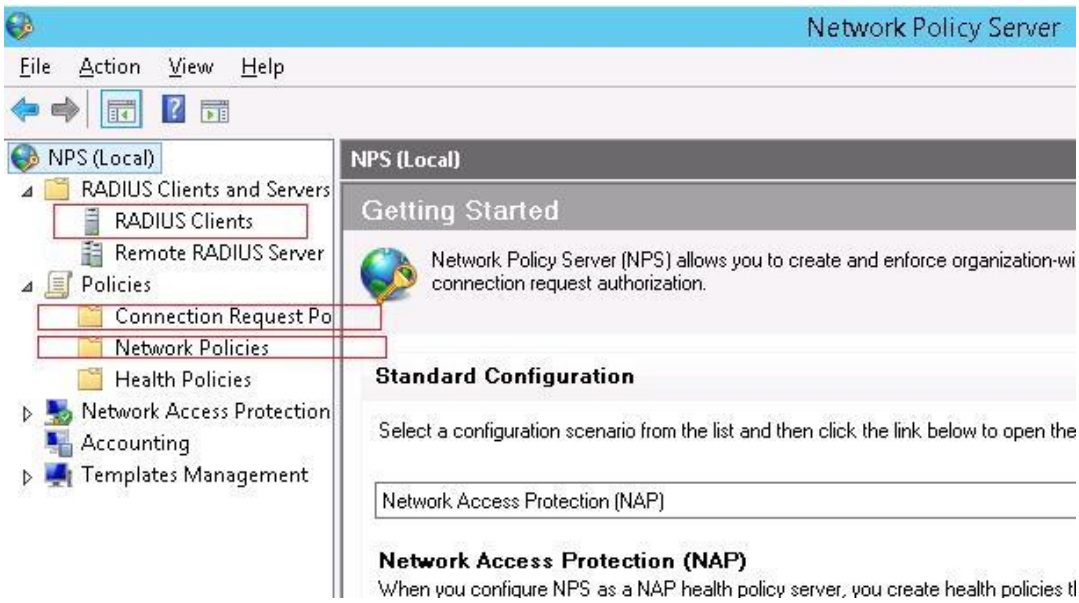


Рис. 94

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).

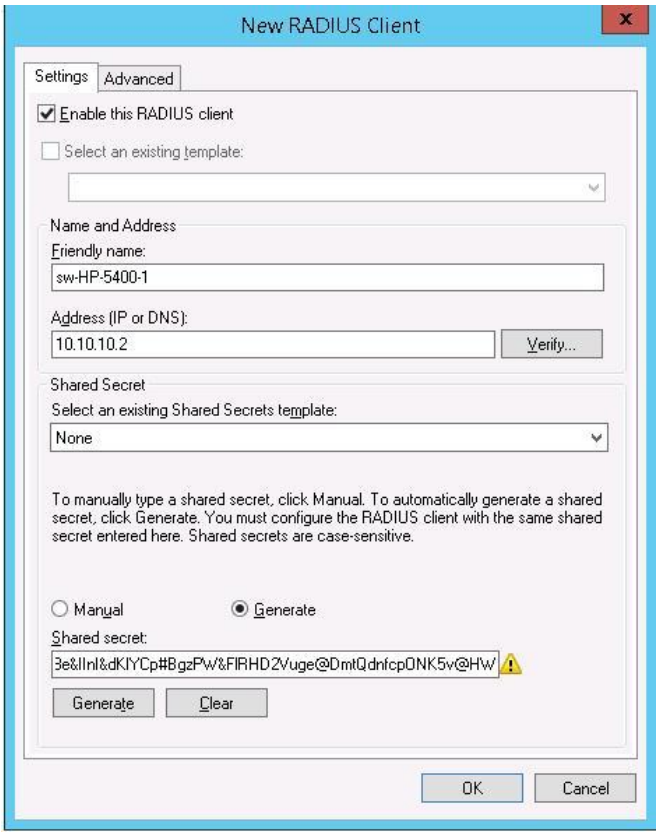


Рис. 95

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**.

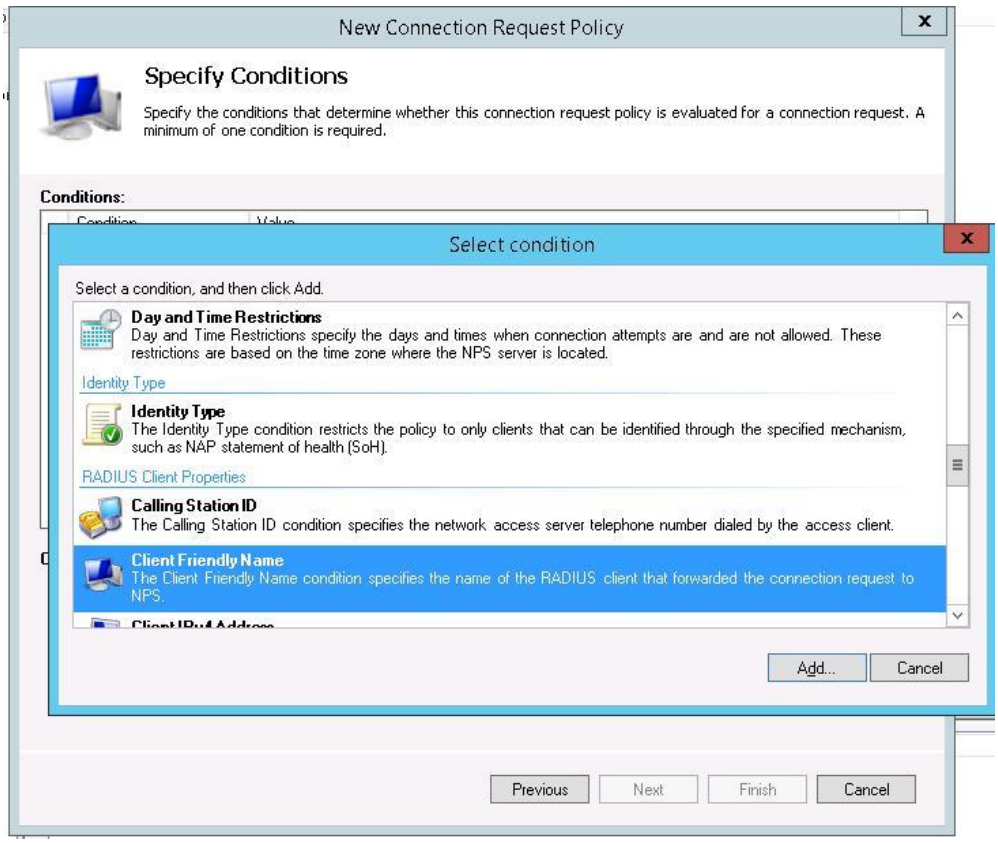


Рис. 96

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.

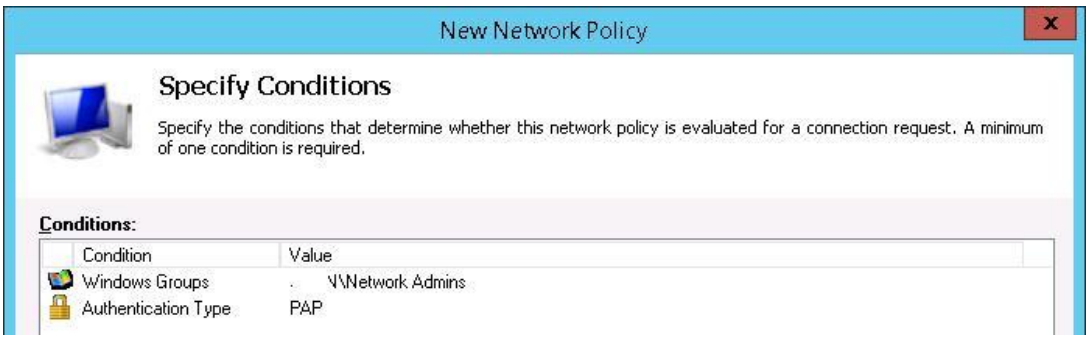


Рис. 97

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**.

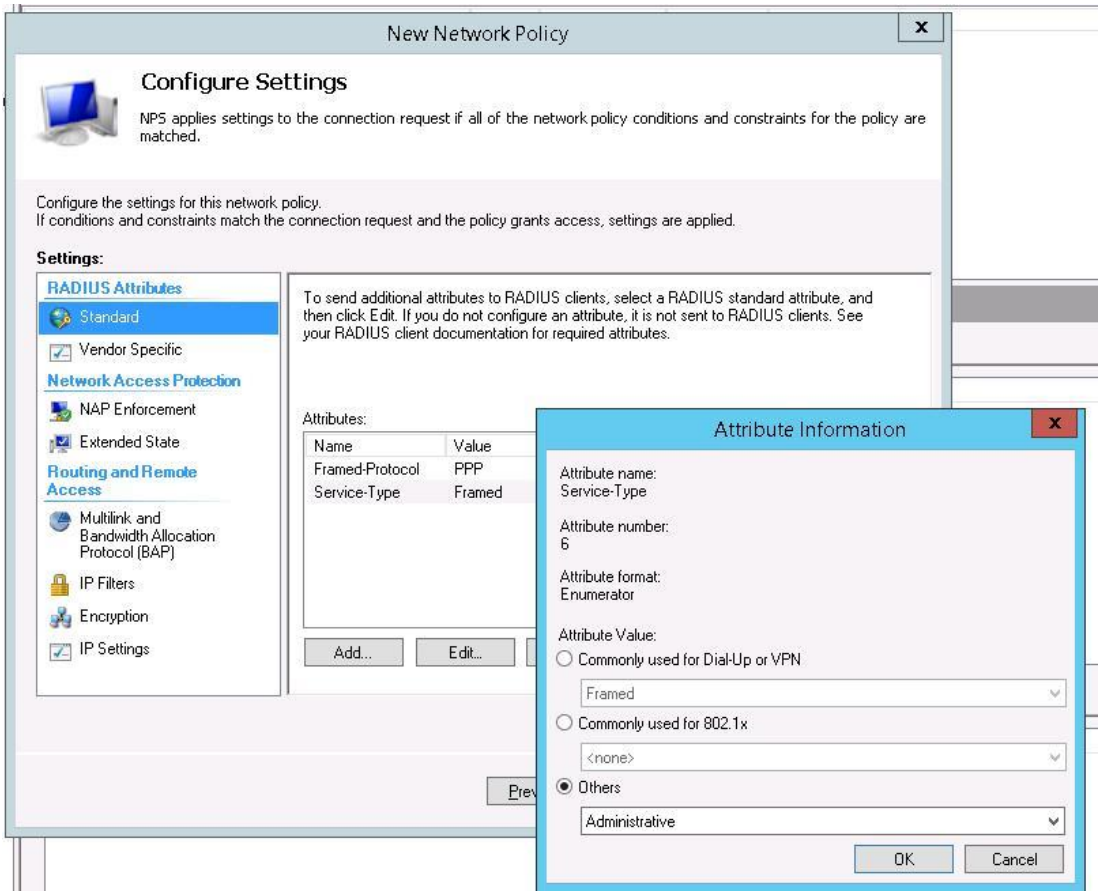


Рис. 98

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

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

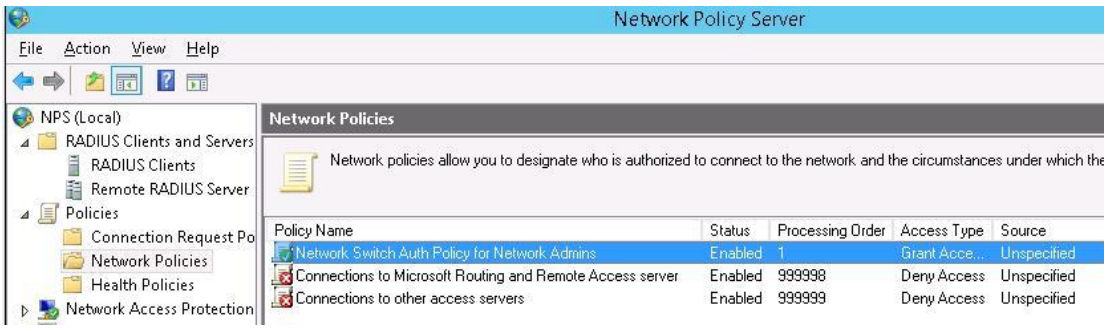


Рис. 99

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. 100

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.

Практическая работа № 8 «Применение 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.

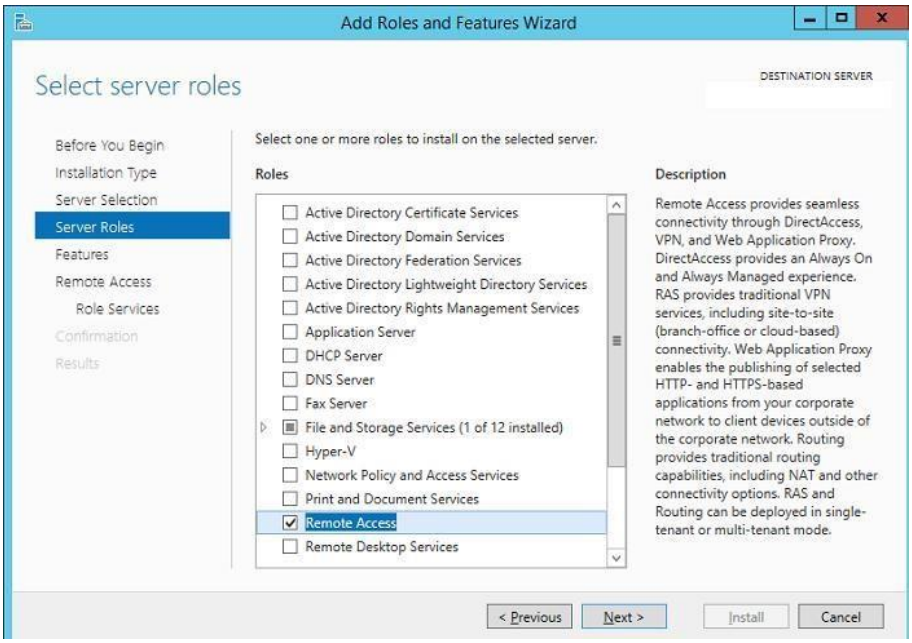


Рис. 101

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

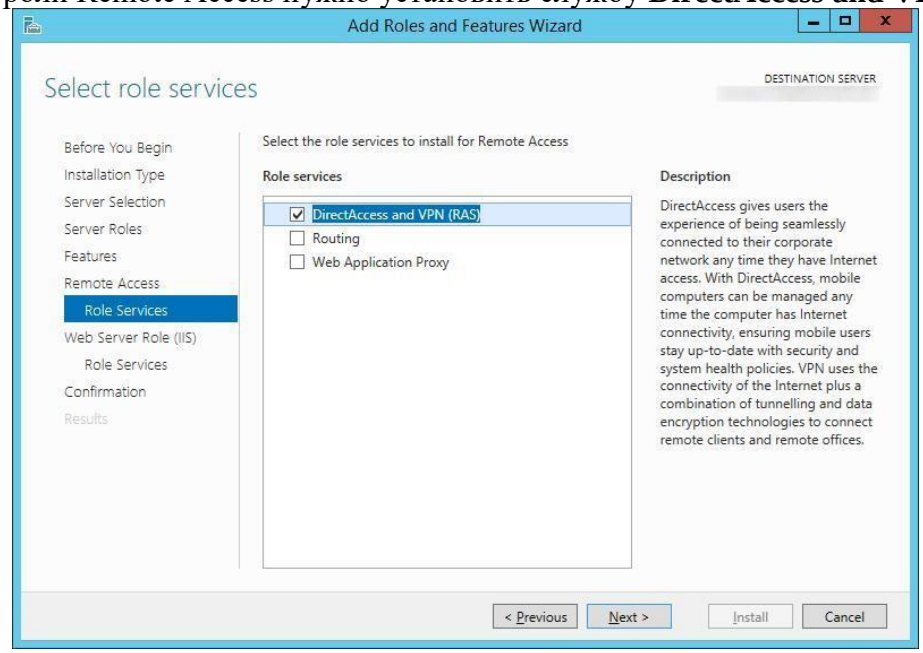


Рис. 102

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**.

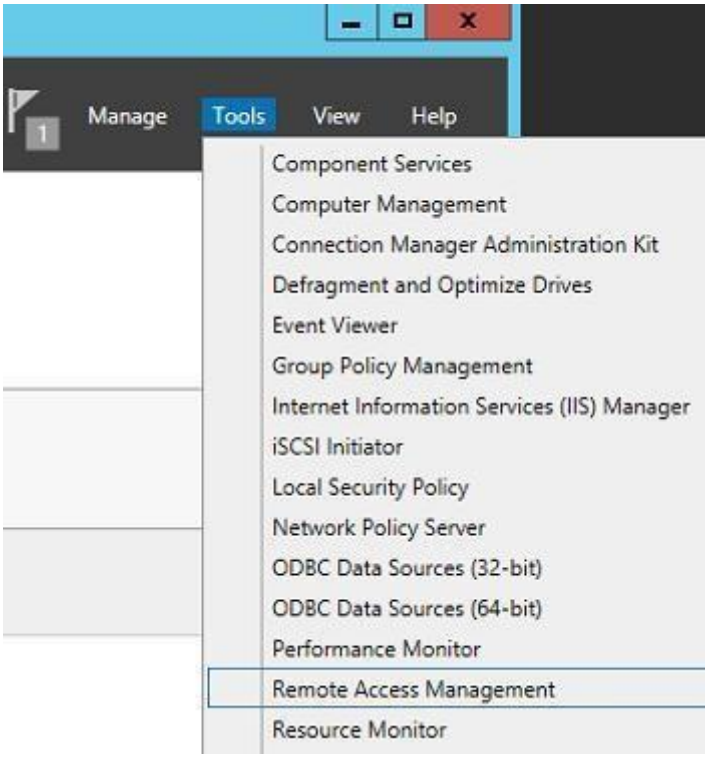


Рис. 103

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

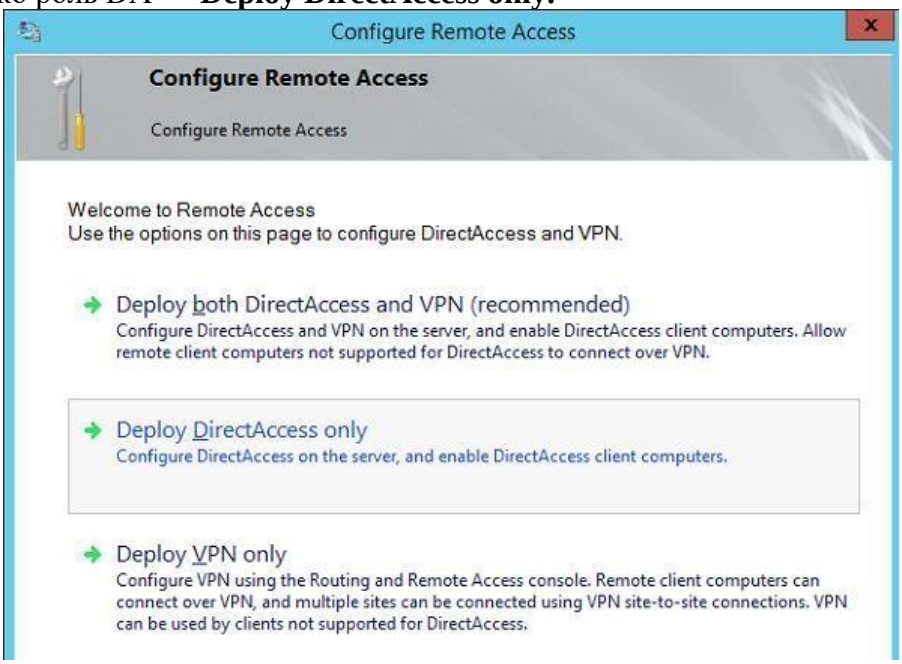


Рис. 104

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

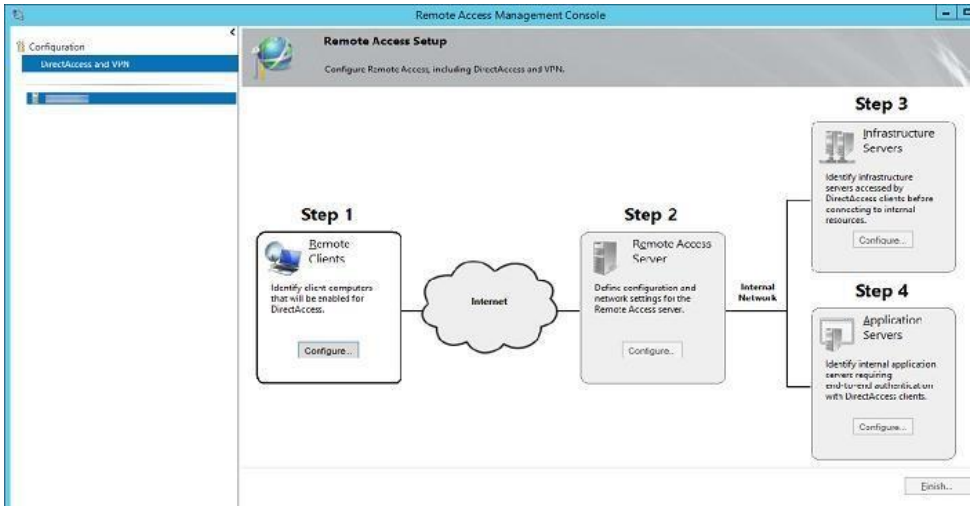


Рис. 105

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**.

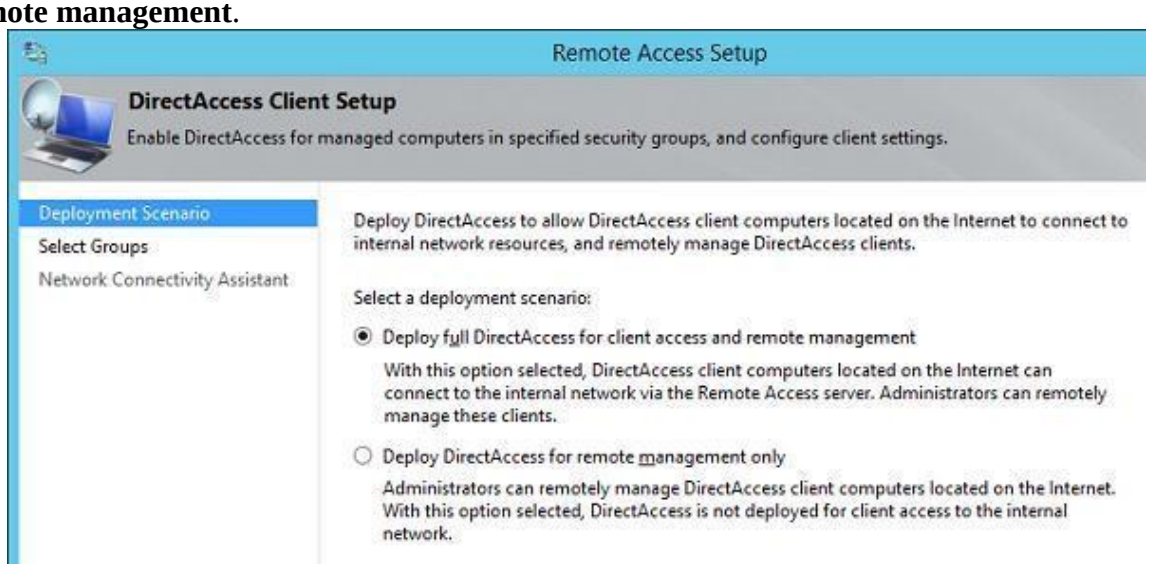


Рис. 106

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).

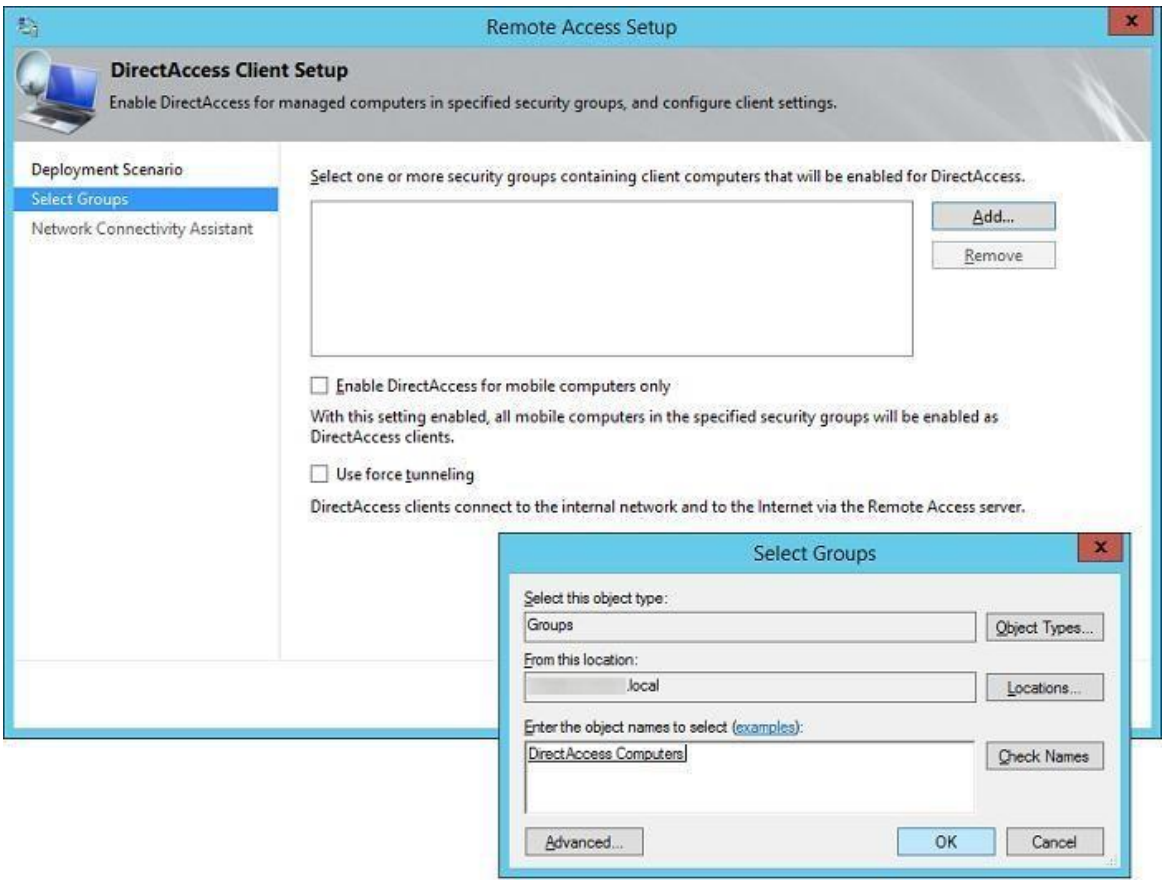


Рис. 107

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 DNSсервера компании (адреса DNS серверов могут получаться по DHCP).

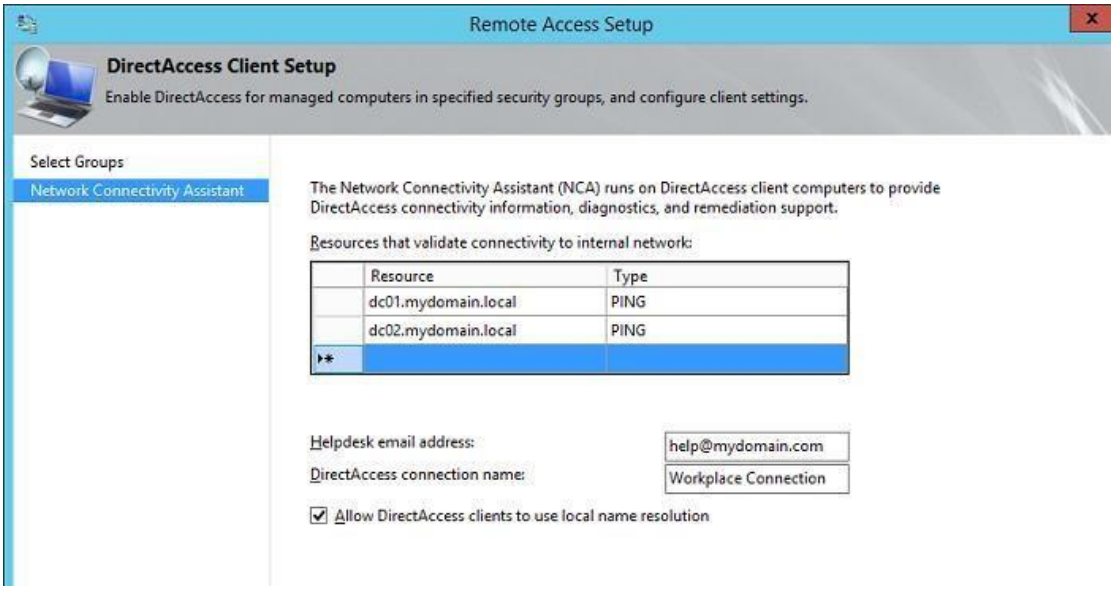


Рис. 108

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.

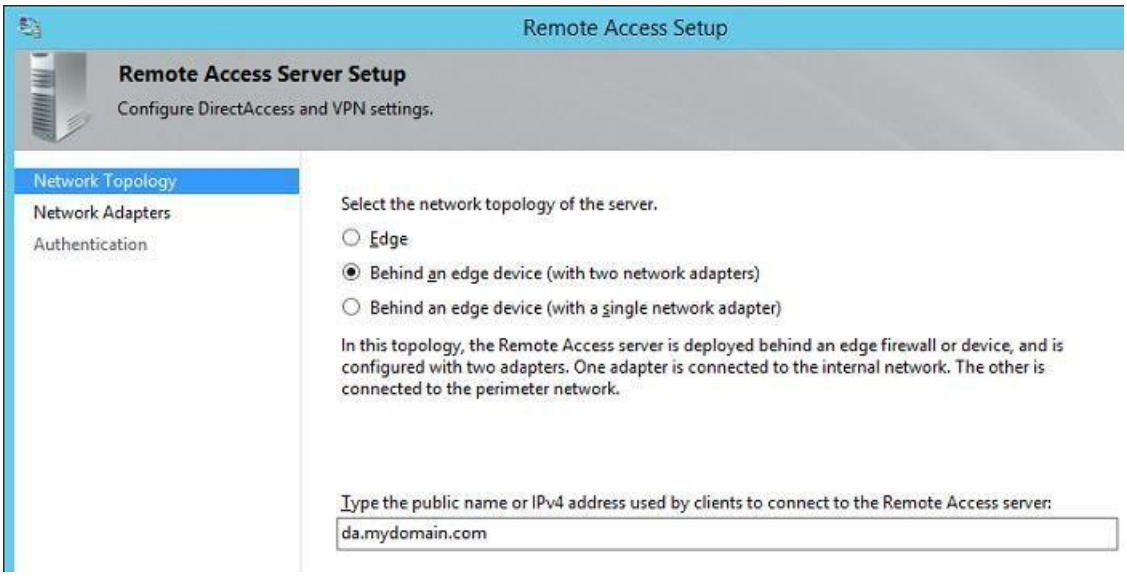


Рис. 109

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

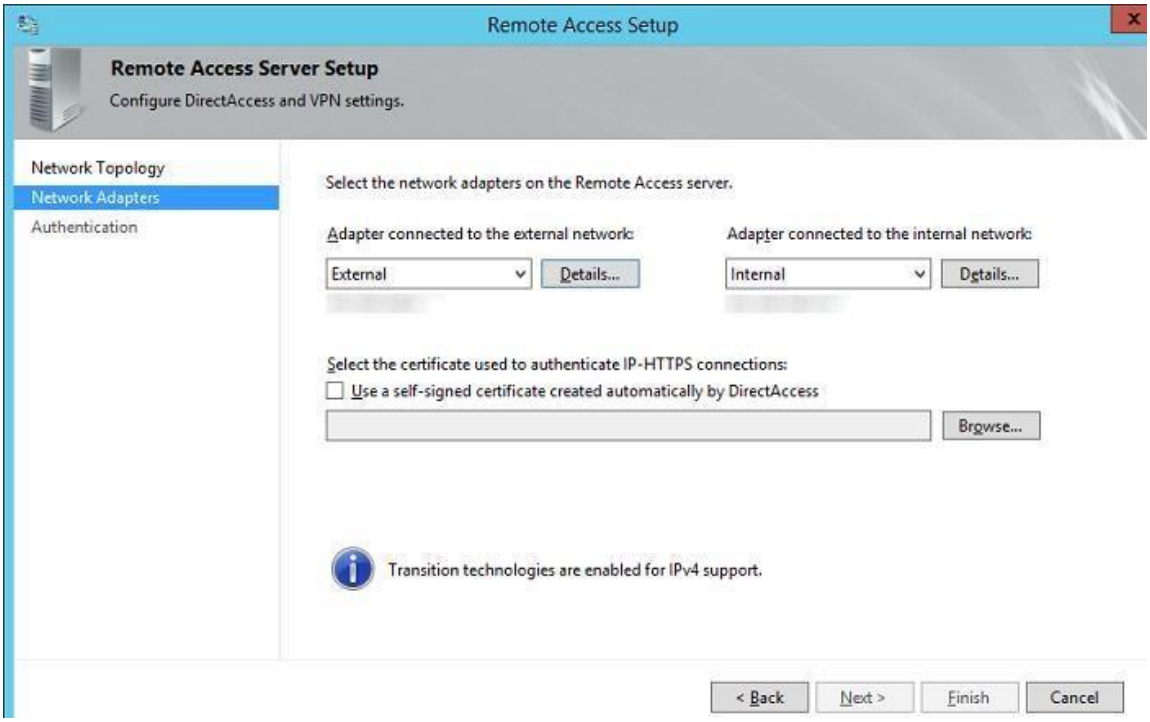


Рис. 110

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**)

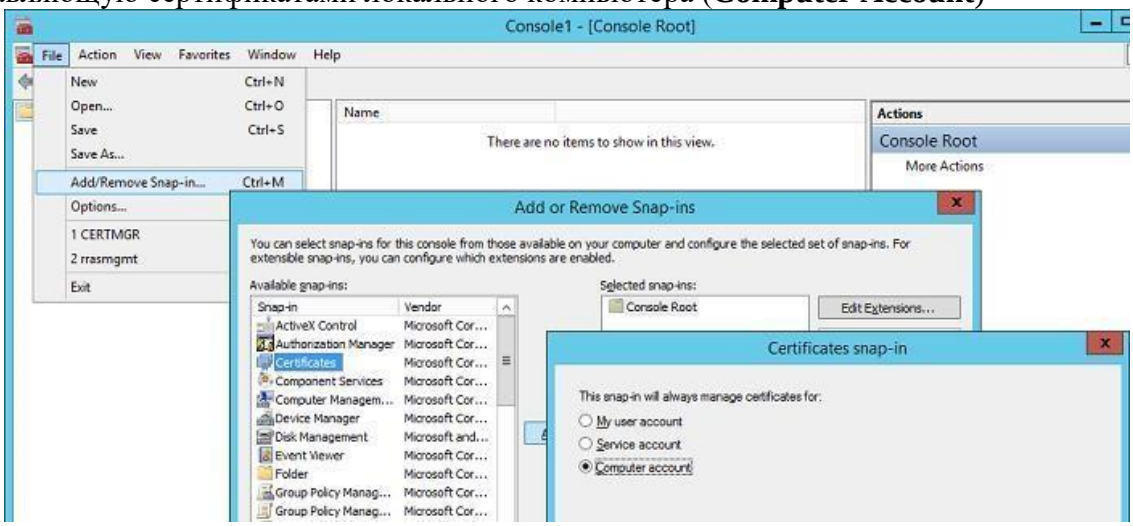


Рис. 111

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**.

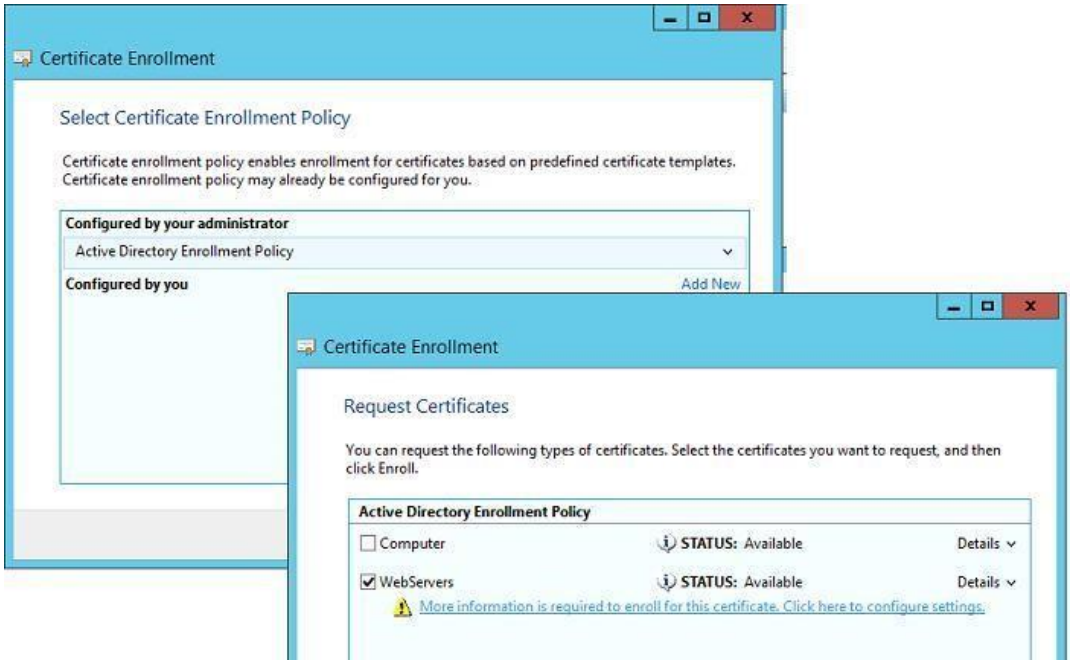


Рис. 112

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**).

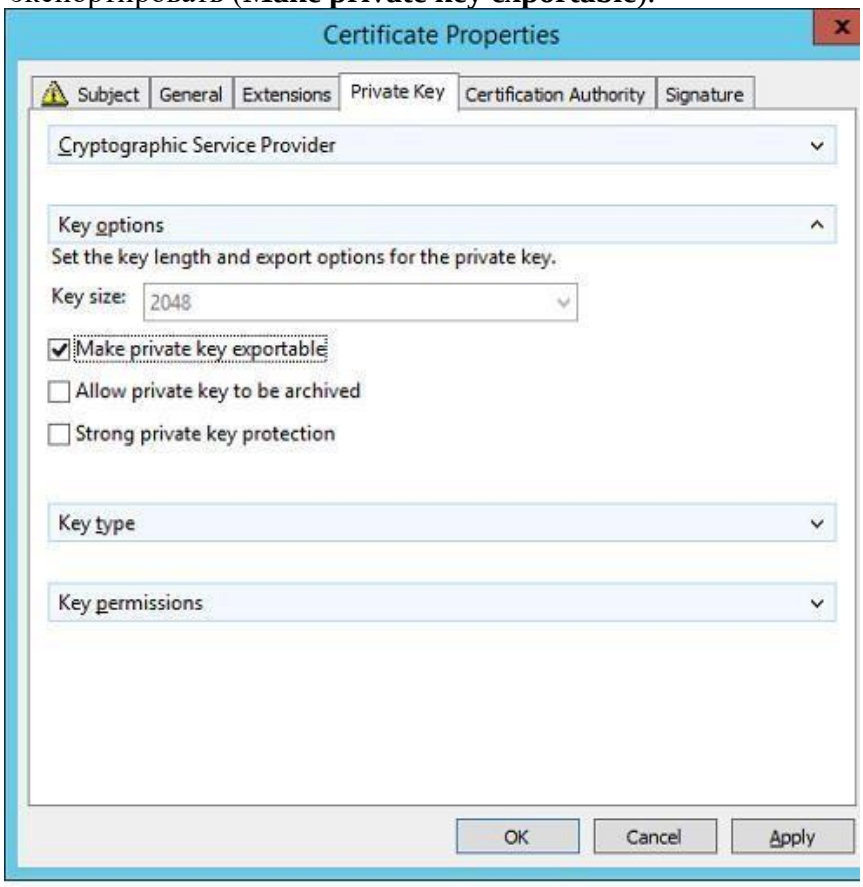


Рис. 113

Сохраним изменения и запросим новый сертификат у CA.

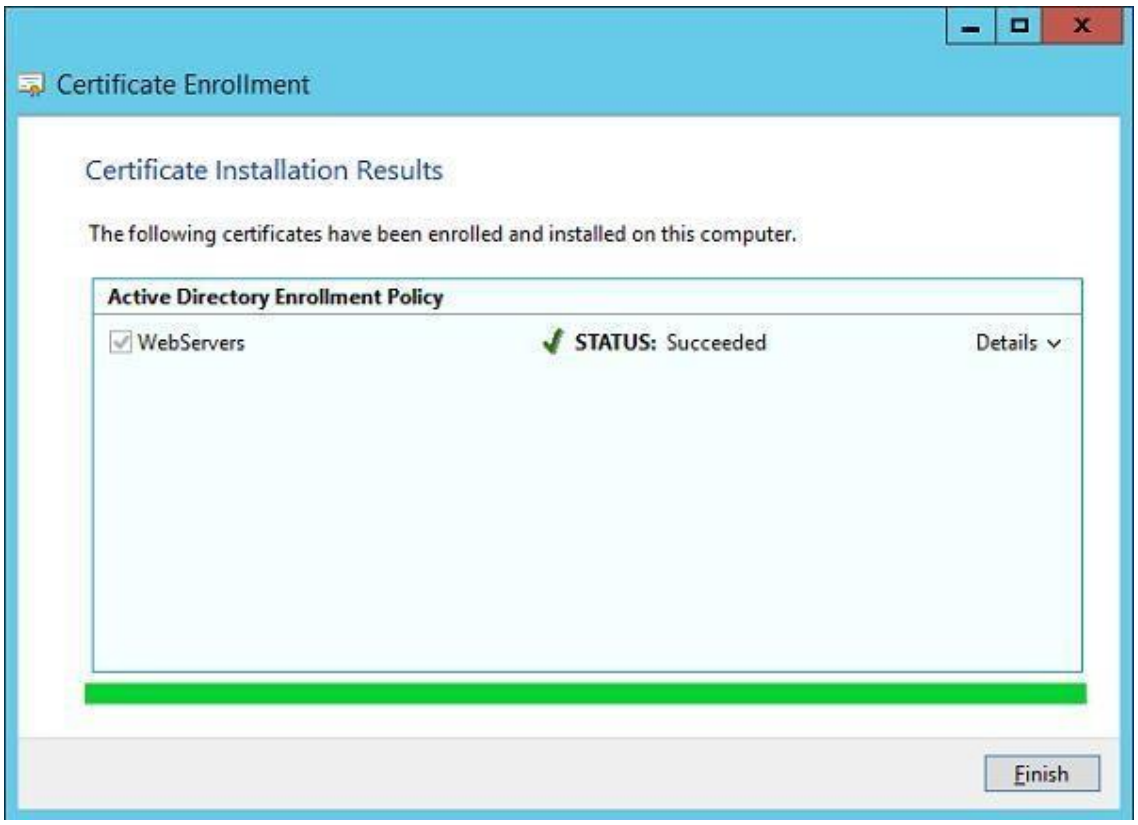


Рис. 114

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

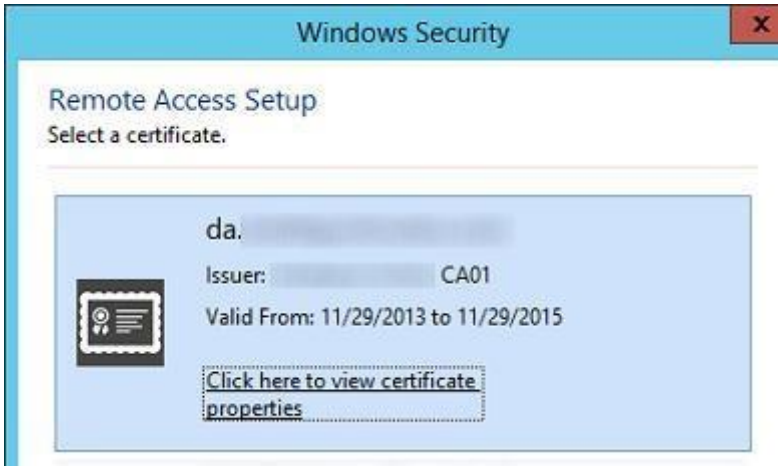


Рис. 115

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.

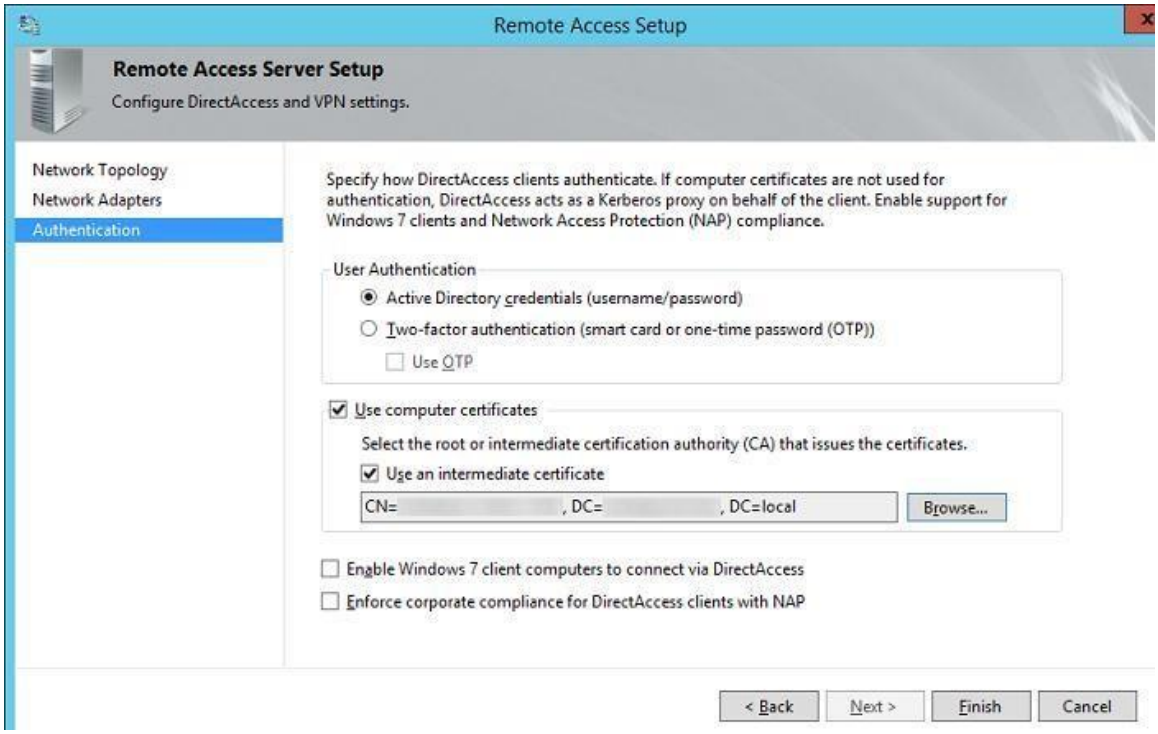


Рис. 116

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.

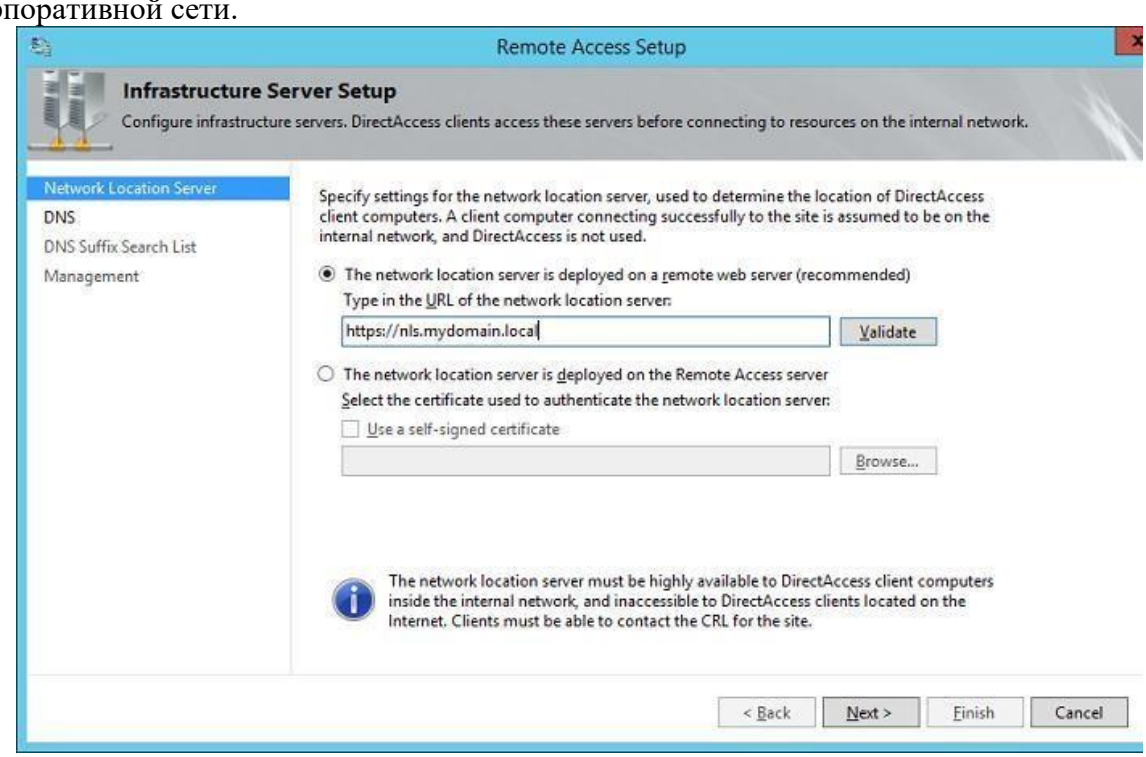


Рис. 117

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).**

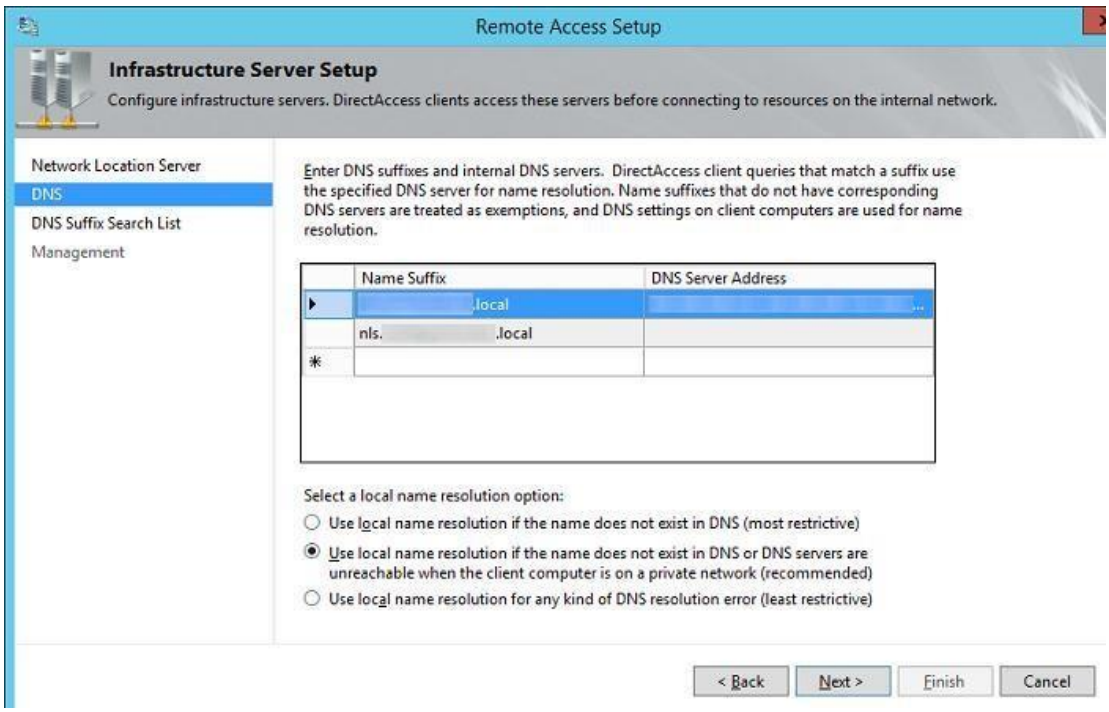


Рис. 118

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

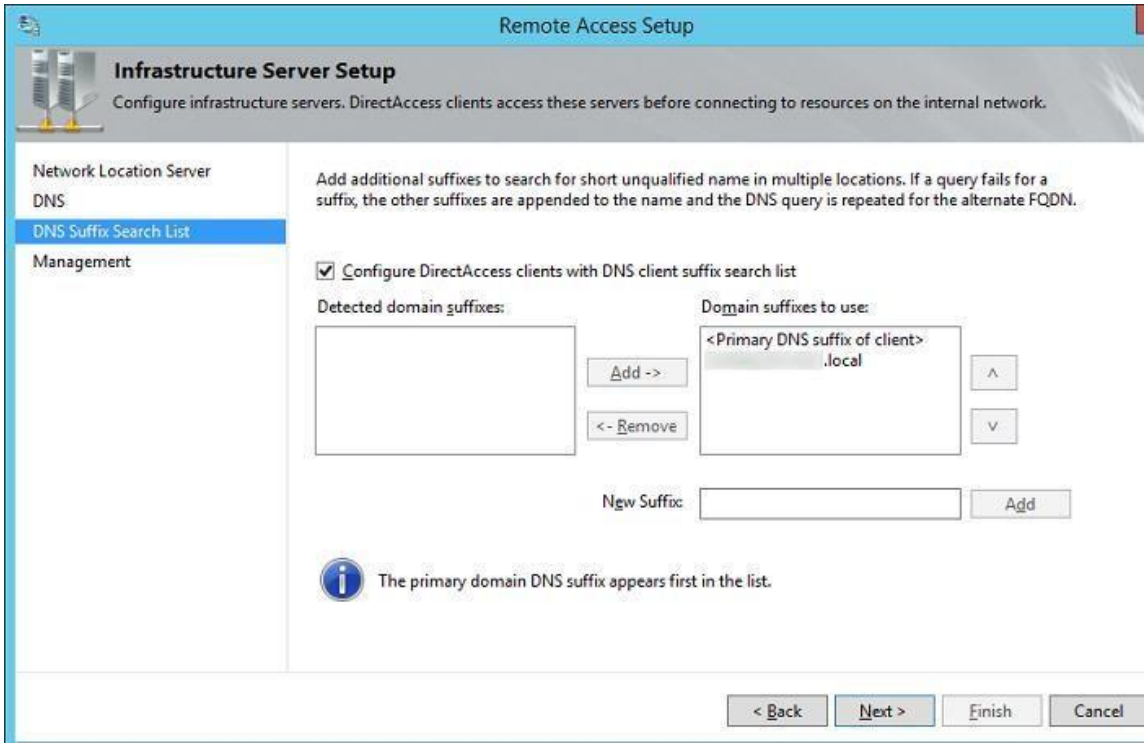


Рис. 119

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.**

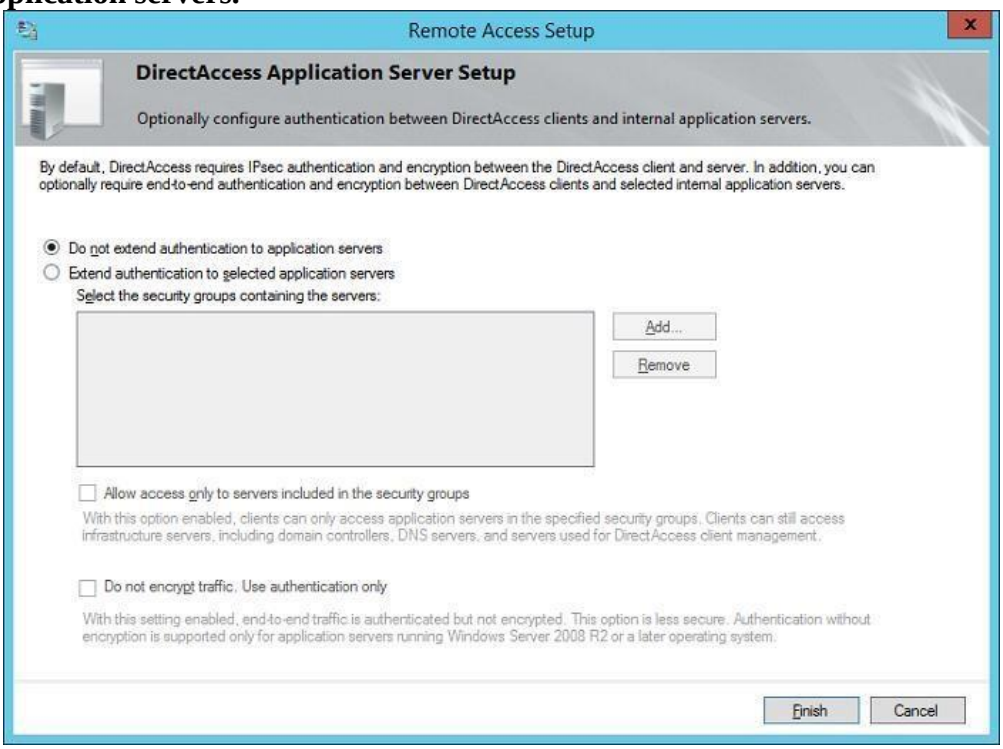


Рис. 120

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

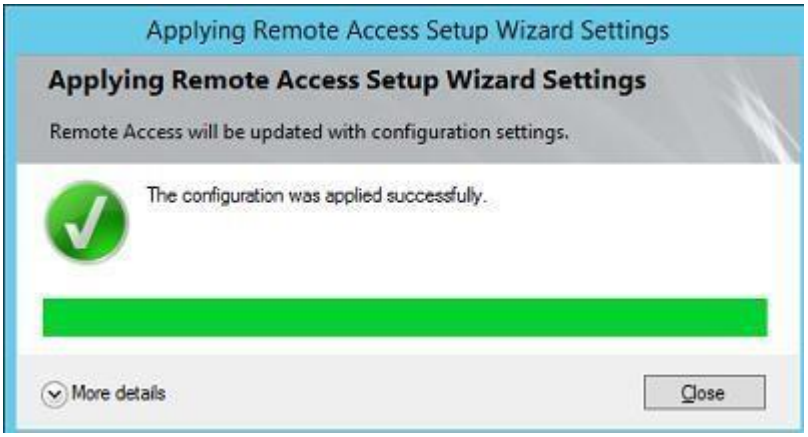


Рис. 121

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

2.9. Практическая работа № 9 «Развертывание расширенной инфраструктуры DirectAccess»

Задание:

1. Установка сертификата IP-HTTPS из внутреннего ЦС

1.1 На сервере DirectAccess: на **начальном** экране введите **mmc.exe**и нажмите клавишу ВВОД.

1.2 В консоли MMC в меню **Файл** выберите **Добавить или удалить оснастку**.

1.3 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**.

1.4 В дереве консоли оснастки "Сертификаты" откройте раздел **Сертификаты (локальный компьютер)\Личные\Сертификаты**.

1.5 Щелкните правой кнопкой **Сертификаты**, наведите указатель на элемент **Все задачи**, а затем щелкните **Запрос нового сертификата**.

1.6 Щелкните дважды **Далее**.

1.7 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**.

1.8 В диалоговом окне **Свойства сертификата** на вкладке **Субъект** в области **Имя субъекта** в поле **Тип** выберите **Общее имя**.

1.9 В поле **Значение** укажите IPv4-адрес внешнего сетевого адаптера сервера DirectAccess или полное доменное имя URL-адреса IPHTTPS, а затем нажмите кнопку **Добавить**.

1.10 В области **Альтернативное имя** в поле **Тип** выберите **DNS**.

1.11 В поле **Значение** укажите IPv4-адрес внешнего сетевого адаптера сервера DirectAccess или полное доменное имя URL-адреса IPHTTPS, а затем нажмите кнопку **Добавить**.

1.12 На вкладке **Общие** в поле **Понятное имя** можно ввести имя, которое упростит идентификацию сертификатов.

1.13 На вкладке **Расширения** щелкните стрелку рядом с элементом **Расширенное использование ключа** и убедитесь, что элемент **Проверка подлинности сервера** есть в списке **Выбранные параметры**.

1.14 Нажмите кнопку **ОК**, щелкните **Зарегистрировать** и нажмите кнопку **Готово**.

1.15 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 пакеты 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 **OK**, 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.

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.

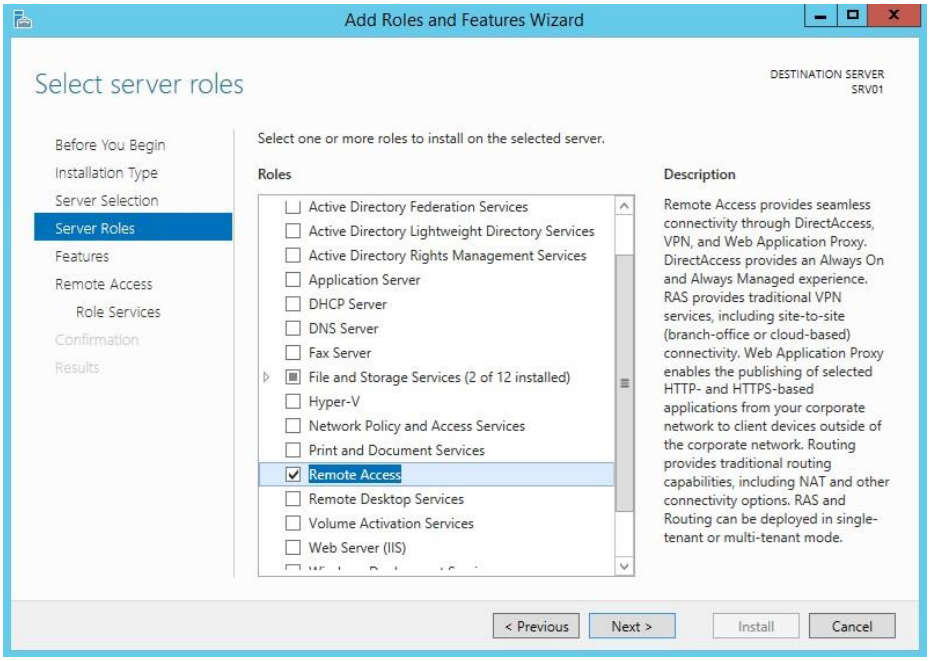


Рис. 122

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

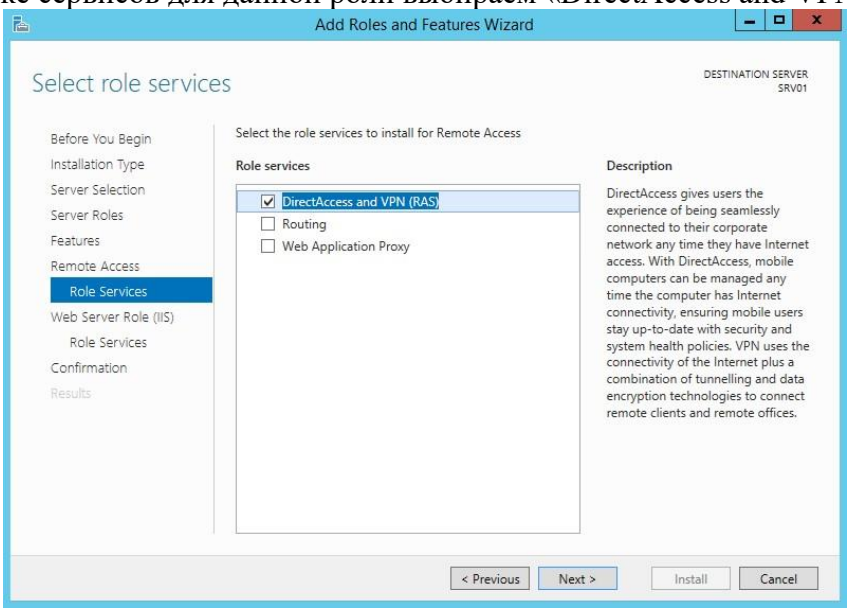


Рис. 123

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.

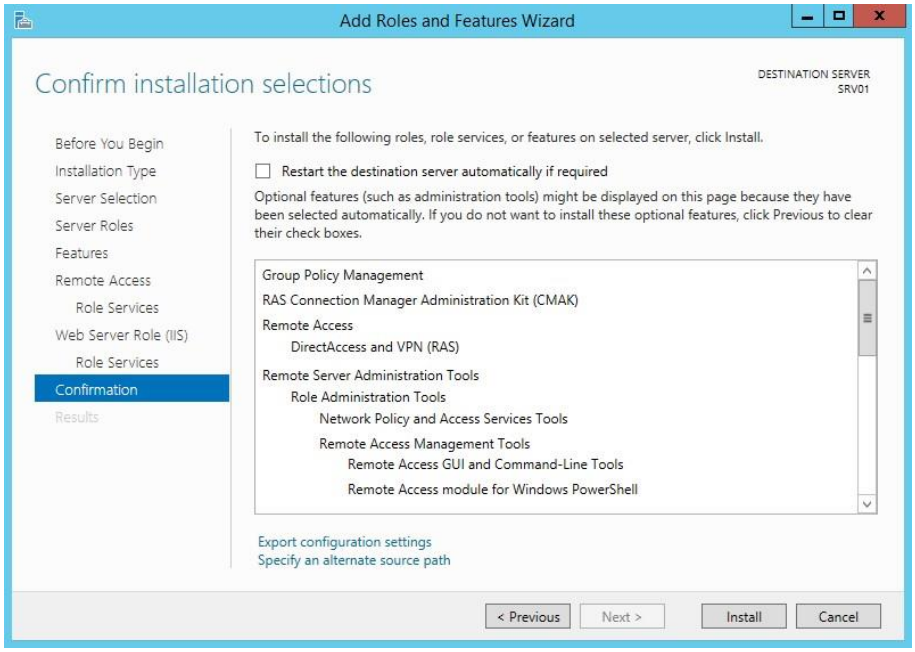


Рис. 124

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 In-cludeManagementTools

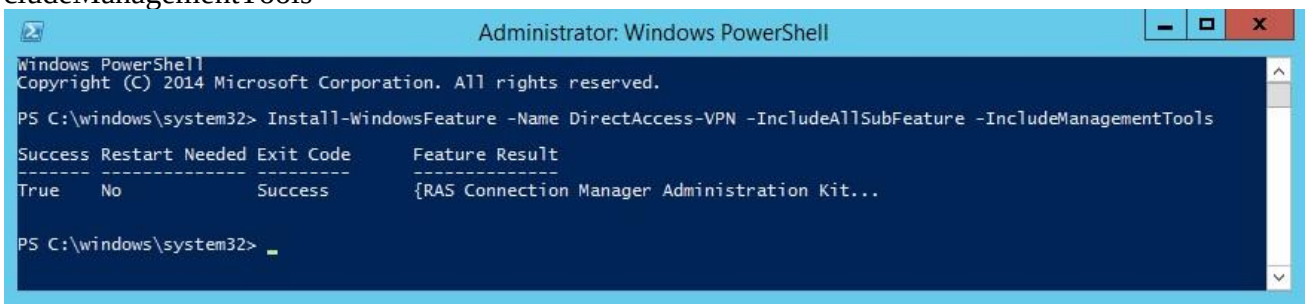


Рис. 125

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

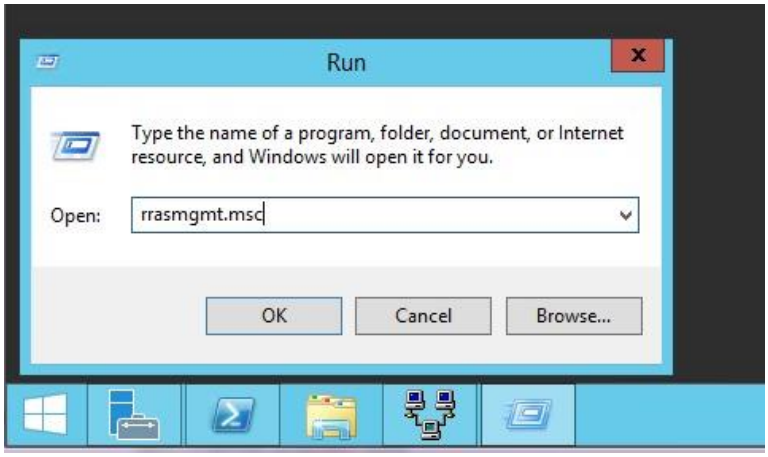


Рис. 126

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

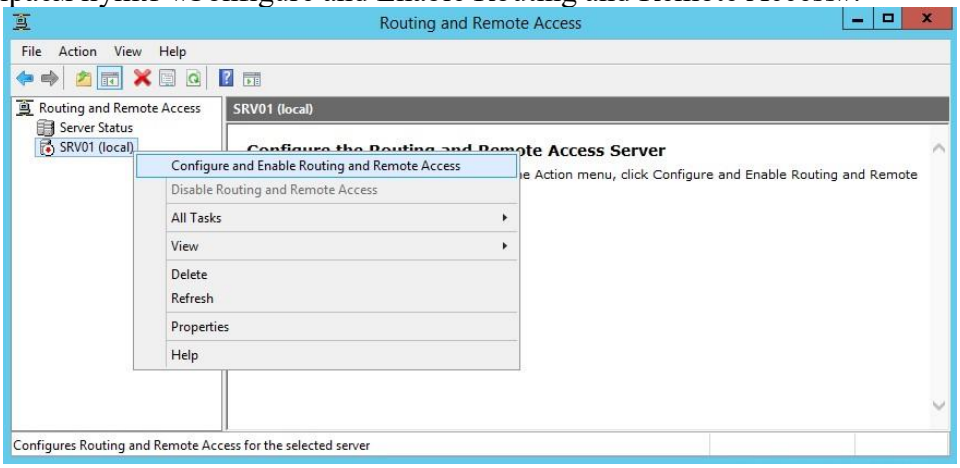


Рис. 127

В окне мастера настройки выбираем пункт «Custom configuration».

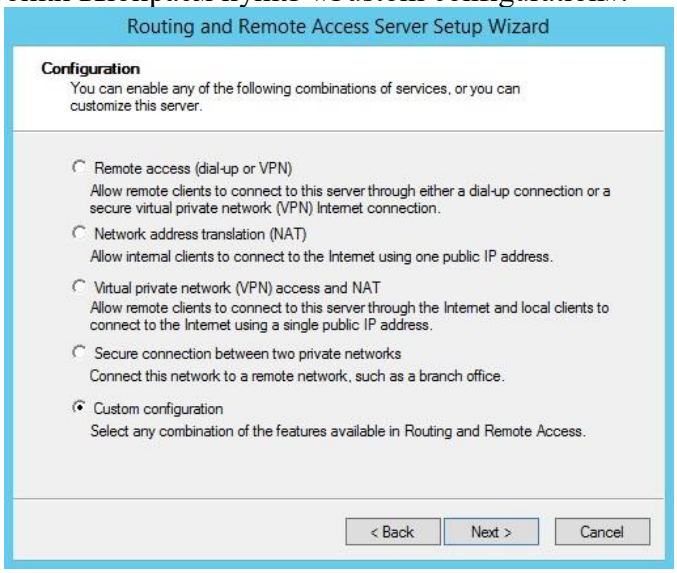


Рис. 128

И отмечаем сервис «VPN access».

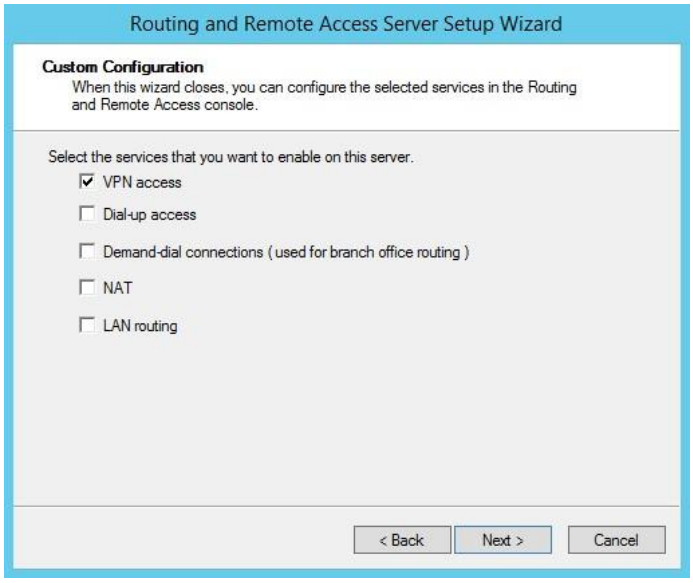


Рис. 129

В завершение настройки стартуем сервис удаленного доступа.

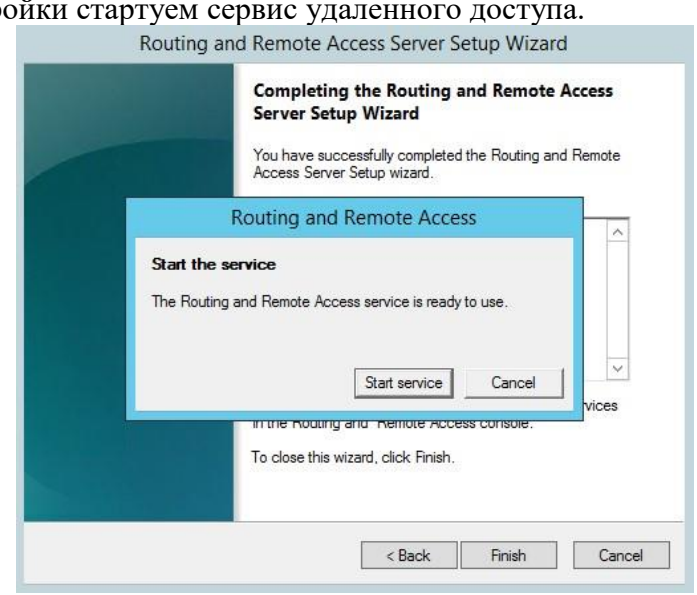


Рис. 130

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

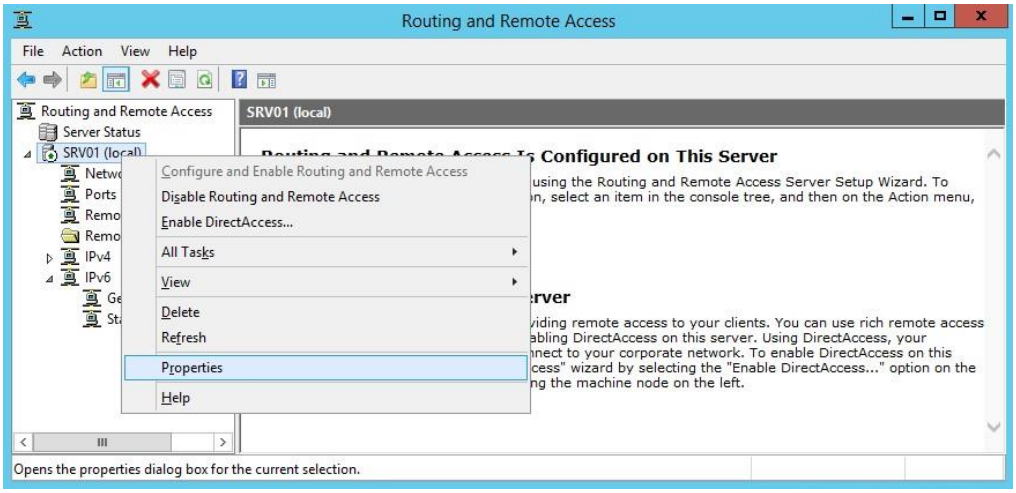


Рис. 131

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.

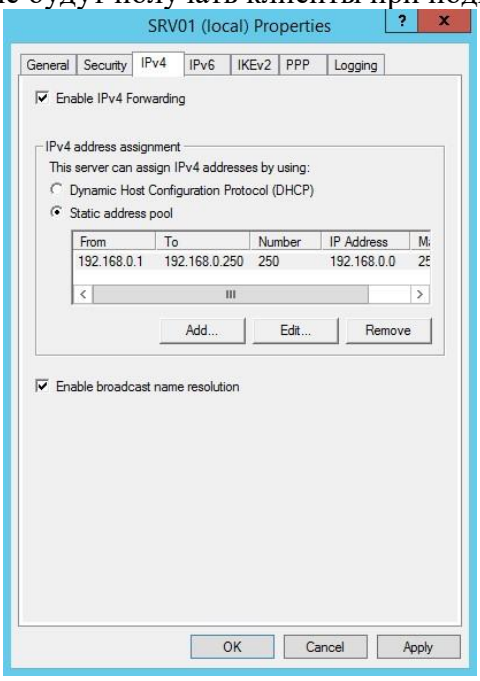


Рис. 132

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

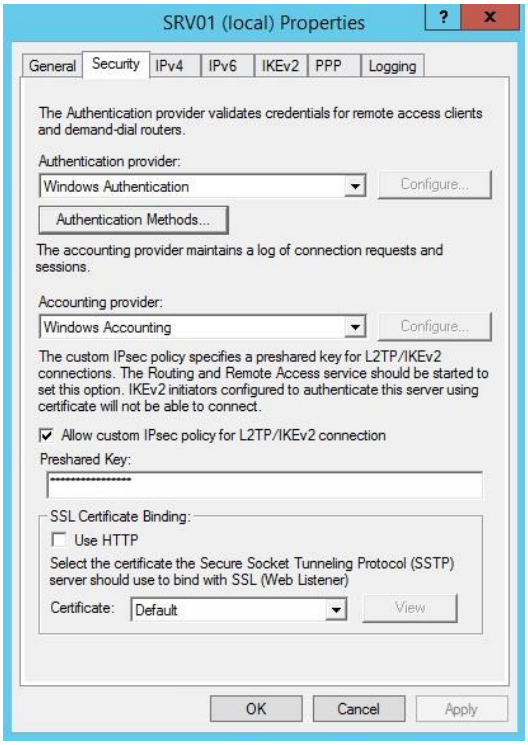


Рис. 133

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

2.11. Практическая работа № 11 «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 допол-

нительные 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.**

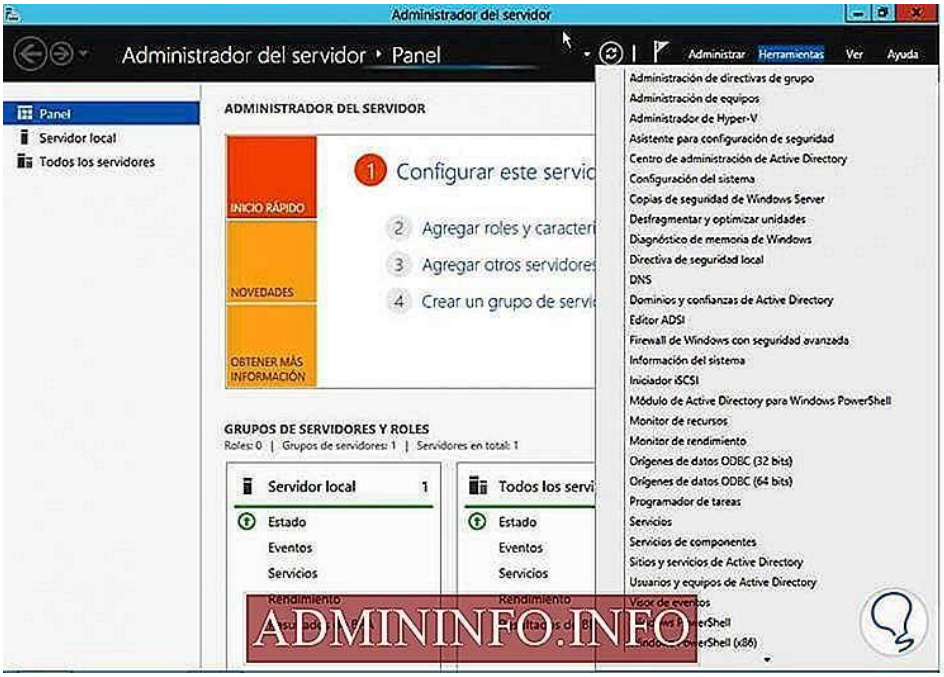


Рис. 134

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

Рис. 135

Шаг 2

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

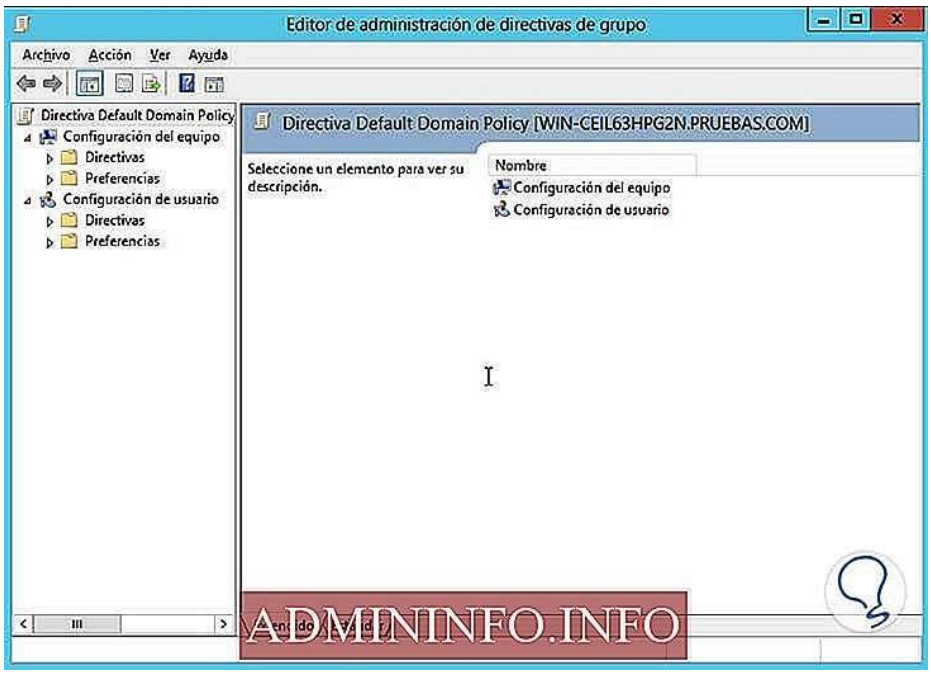


Рис. 136

Мы развернем следующий маршрут:

- Конфигурация оборудования
- Директивы
- Настройки Windows
- Настройки безопасности
- Местные директивы
- Директива об аудите

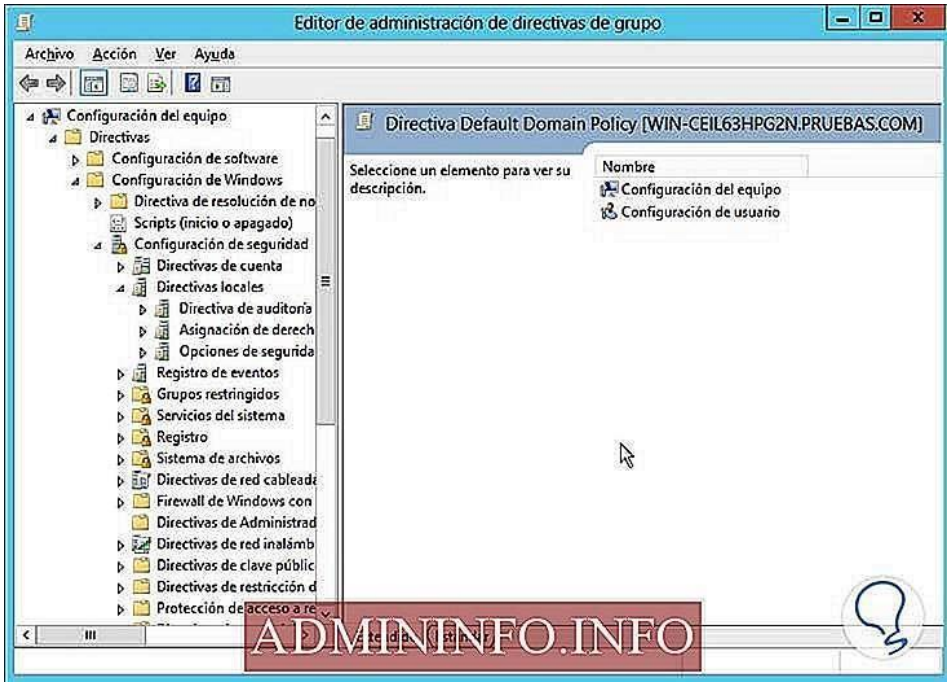


Рис. 137

Шаг 3
Мы увидим окно с различными **параметрами для аудита**:

Рис. 138

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

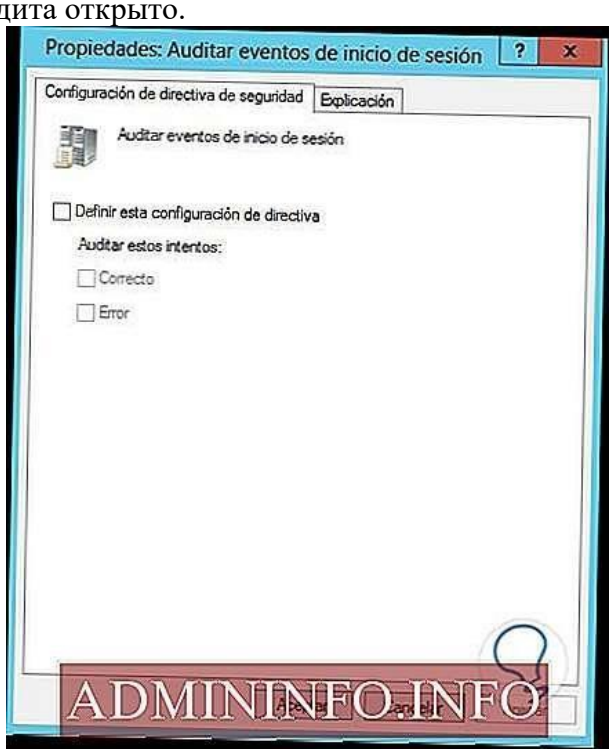


Рис. 139

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.

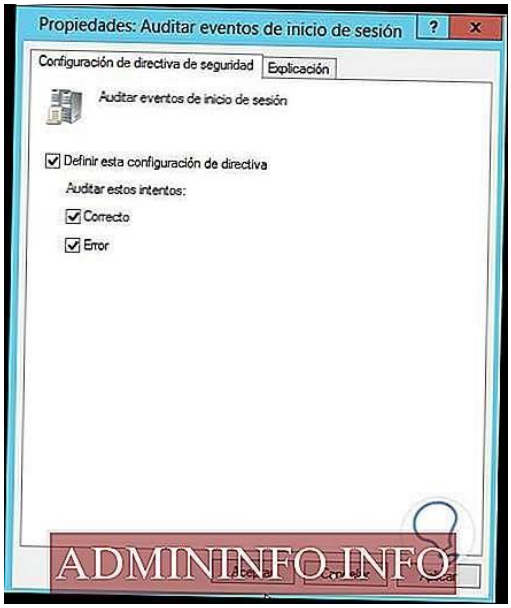


Рис. 140

Мы увидим изменения, отраженные в нашем аудите:

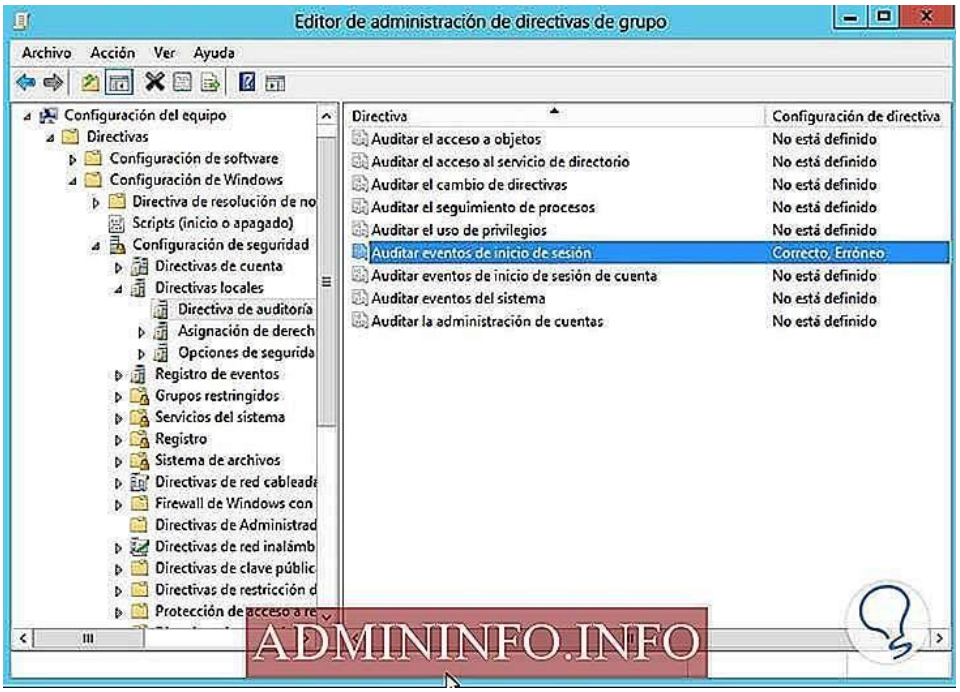


Рис. 141

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».**

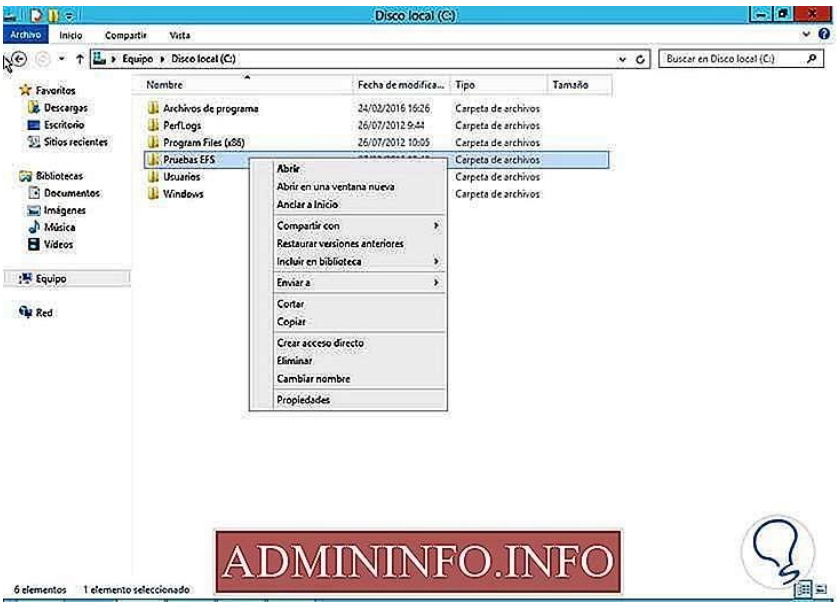


Рис. 142

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

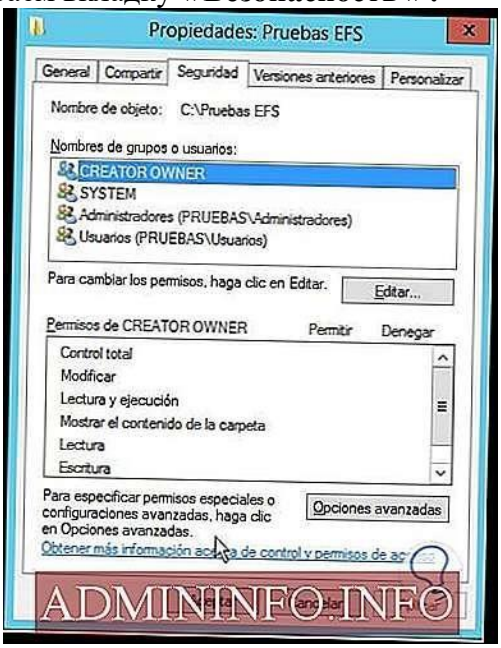


Рис. 143

Шаг 2

Мы нажимаем на Дополнительные параметры, и появится следующее окно:

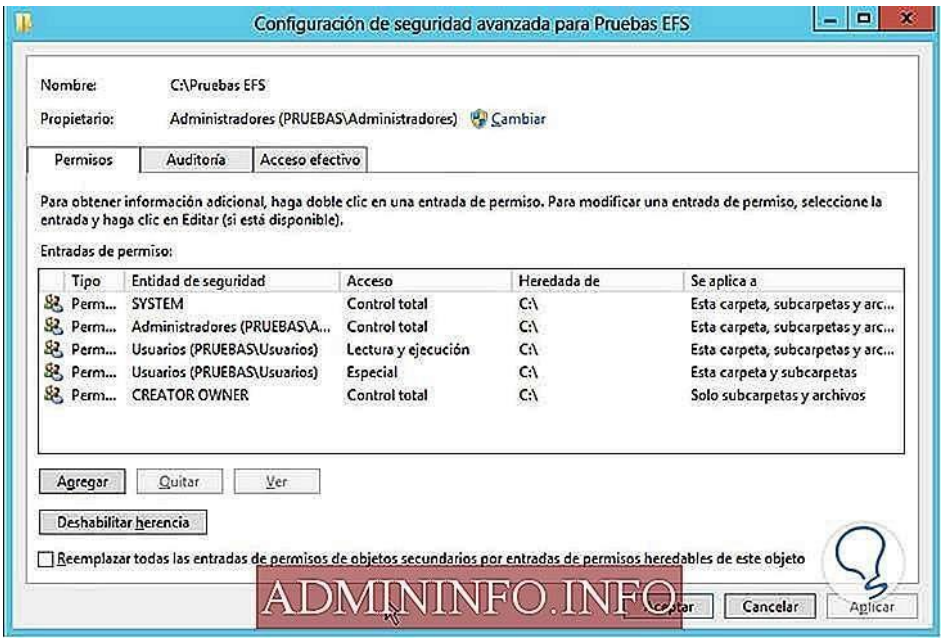


Рис. 144

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

Рис. 145

Шаг 3

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

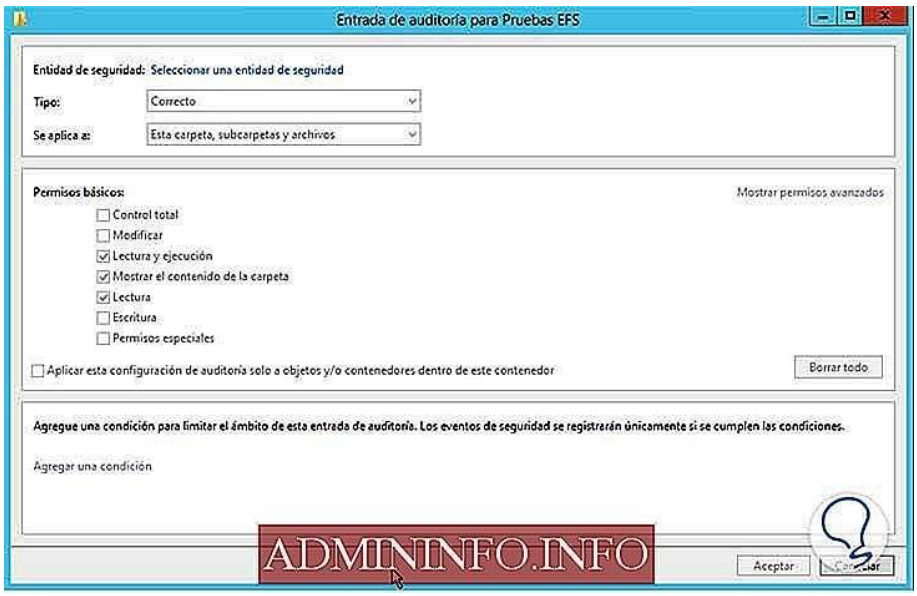


Рис. 146

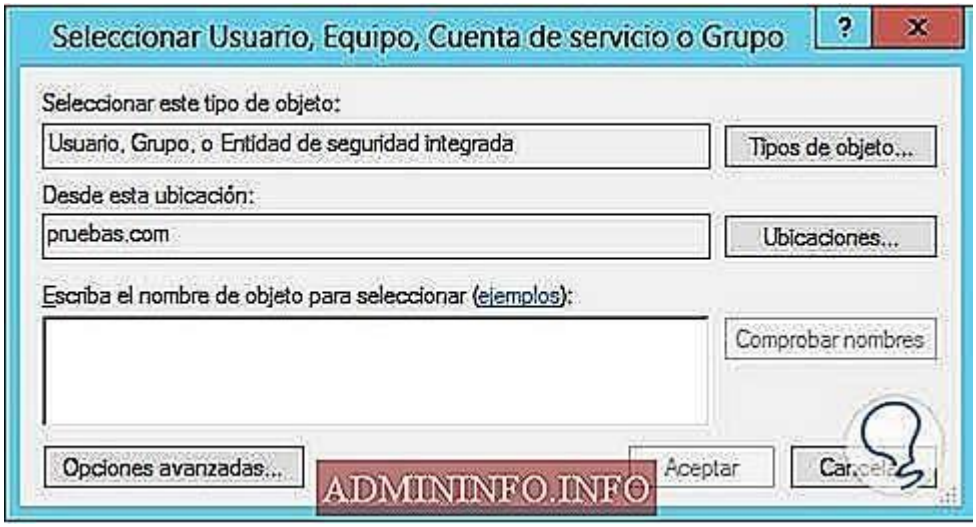


Рис. 147

Мы выбираем **объект для применения аудита** :

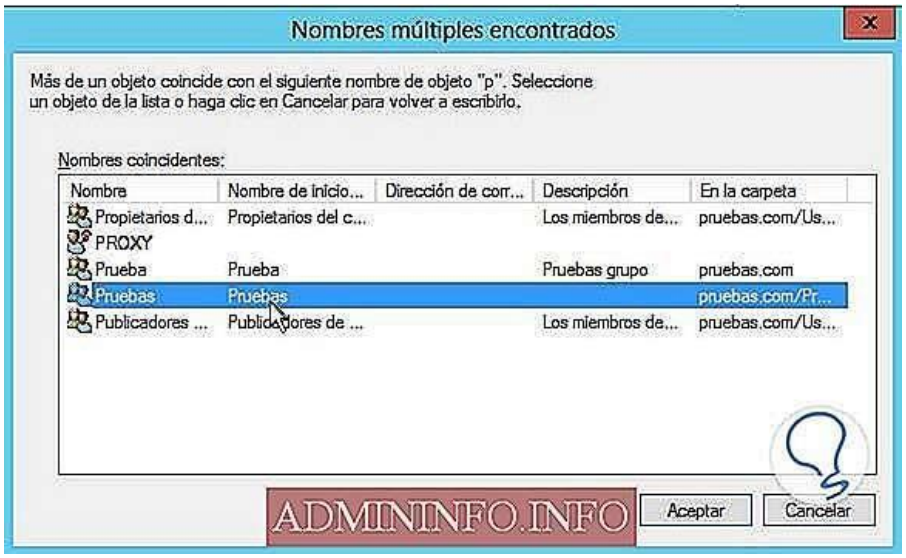


Рис. 148

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

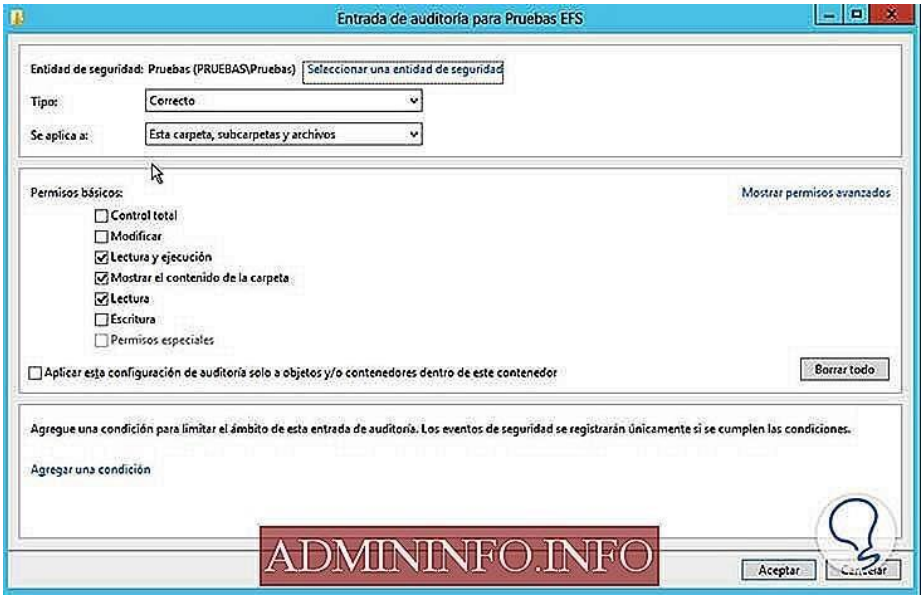


Рис. 149

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

2.12. Практическая работа № 12 «Использование службы развертывания Windows для развертывания Windows Server 2012»

Задание:

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

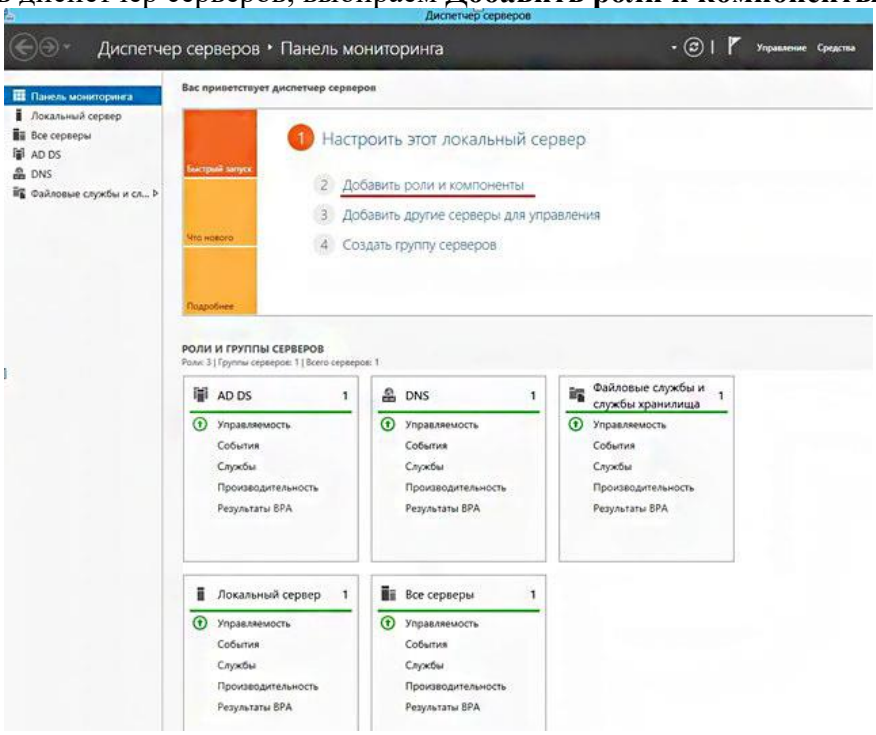


Рис. 150

Далее

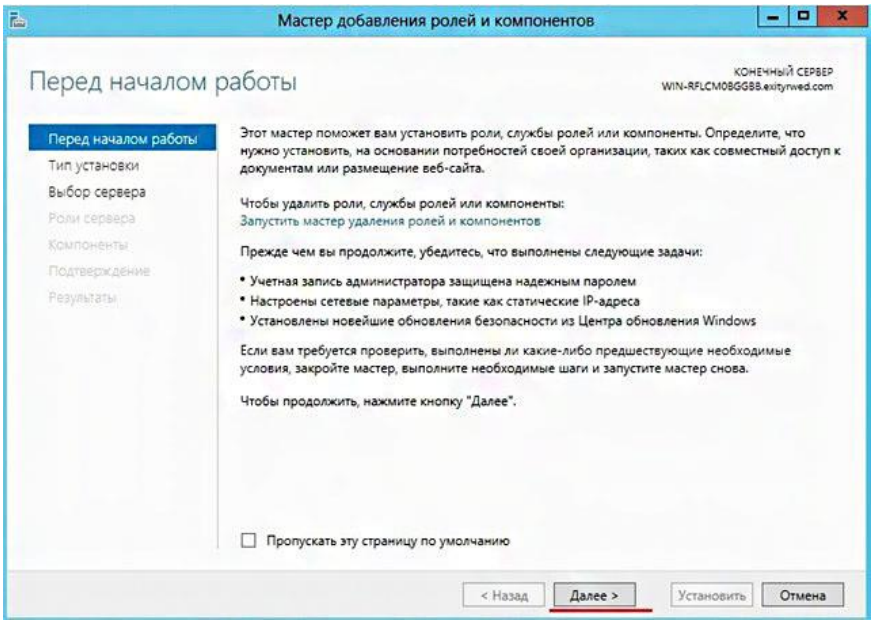


Рис. 151

Выбираем **Установка ролей или компонентов**

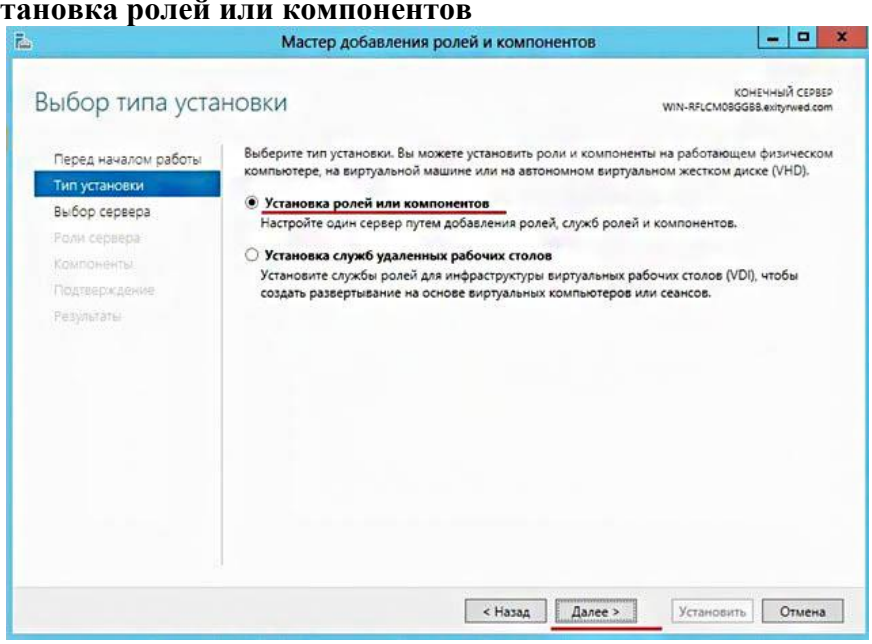


Рис. 152

Выбираем **целевой сервер**, далее

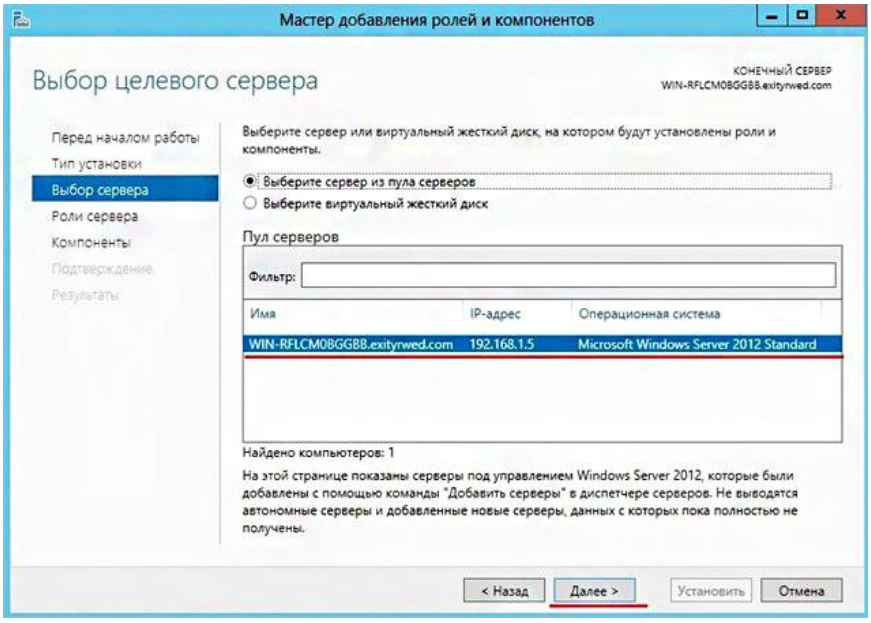


Рис. 153

Выбираем **службы развертывания Windows**, добавить компоненты

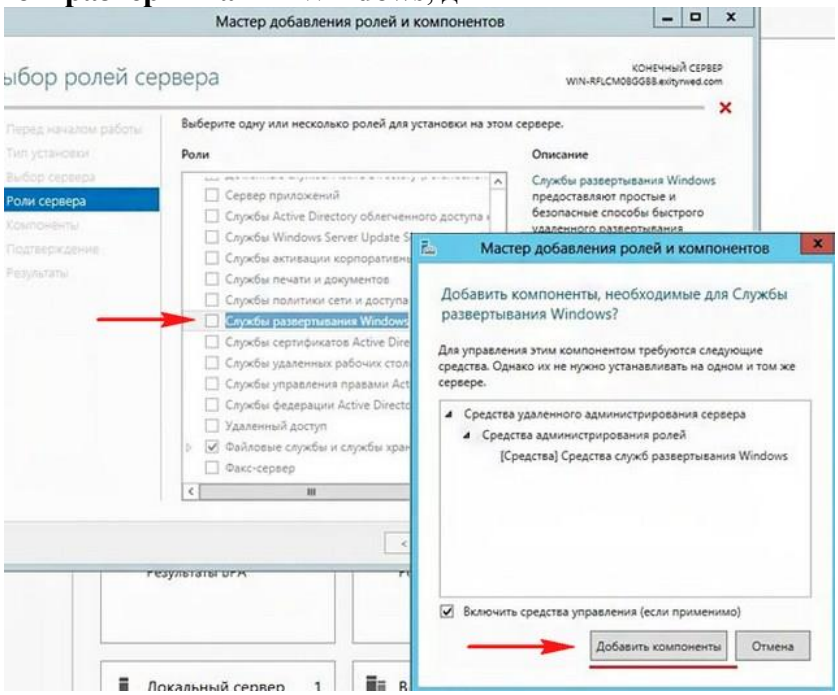


Рис. 154

Далее

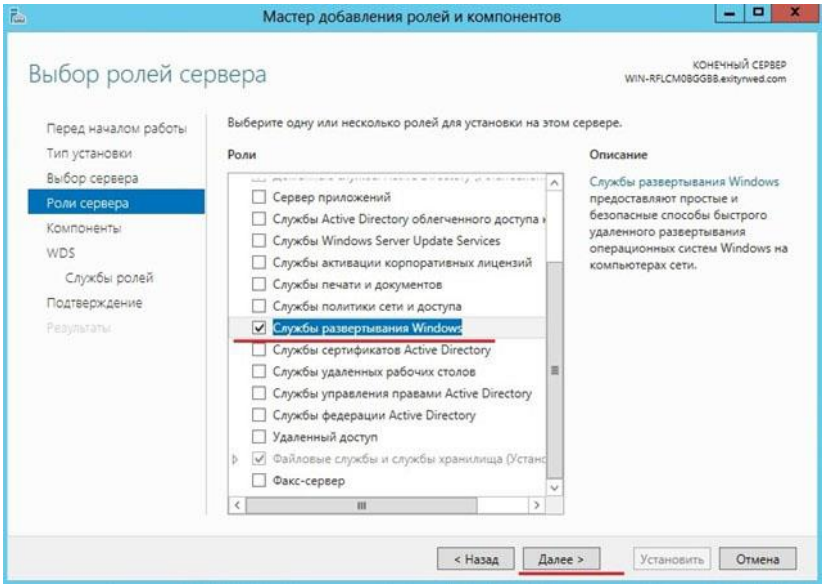


Рис. 155

Из компонентов ничего не нужно выбирать, далее

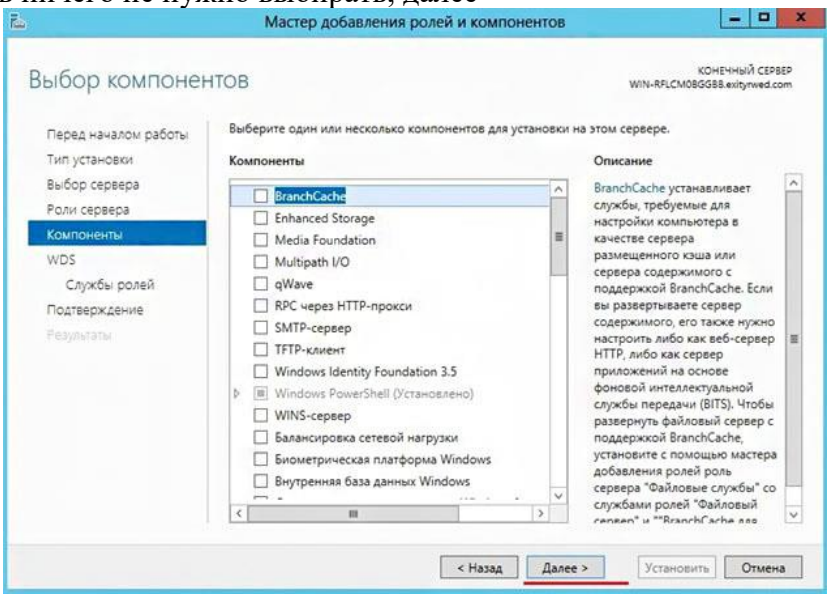


Рис. 156

Далее

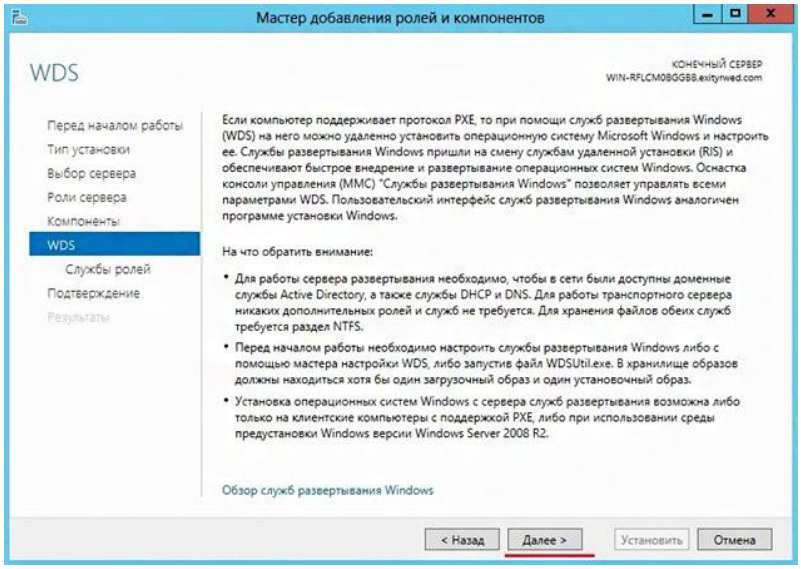


Рис. 157

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

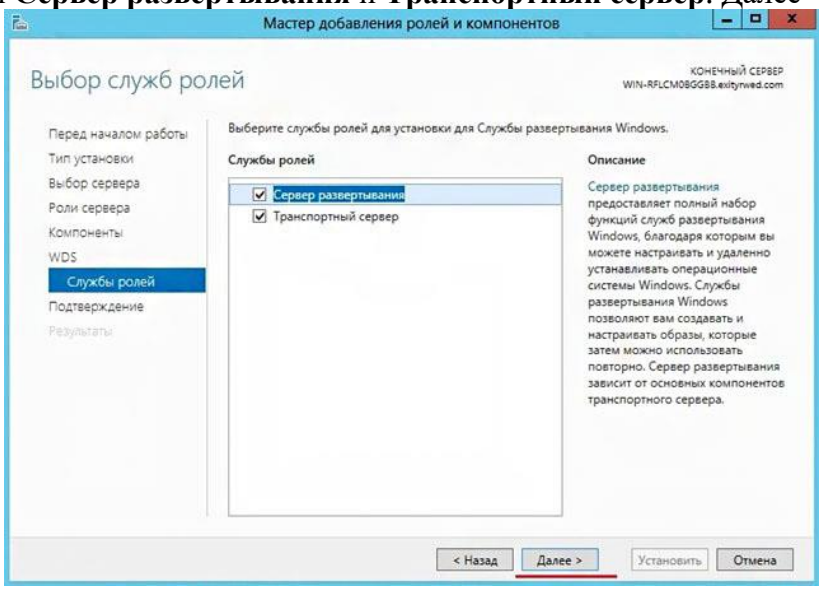


Рис. 158

Установить

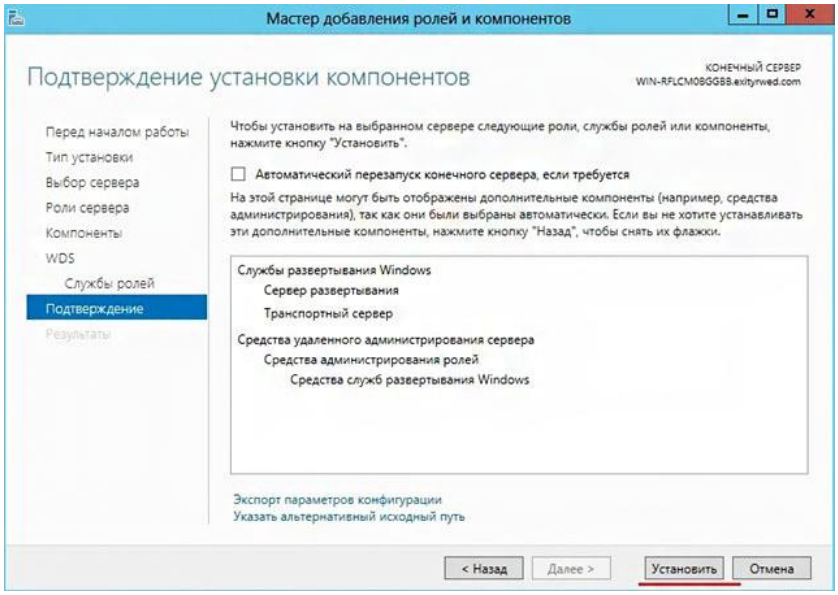


Рис. 159

Идет установка

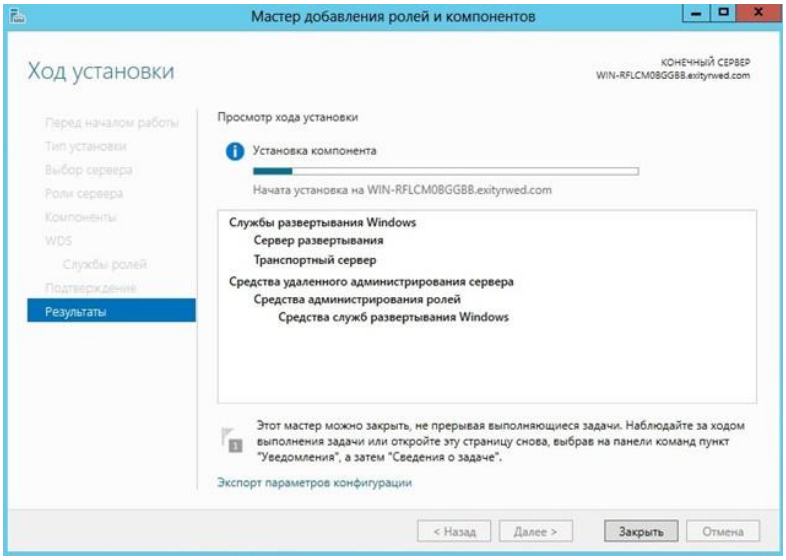


Рис. 160

Установка завершена

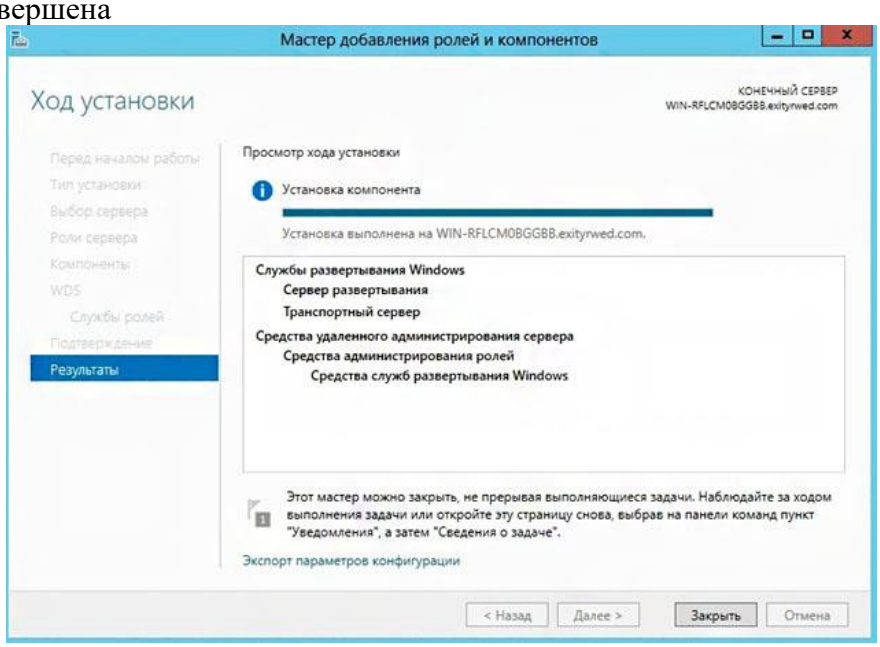


Рис. 161

Появился наш WDS

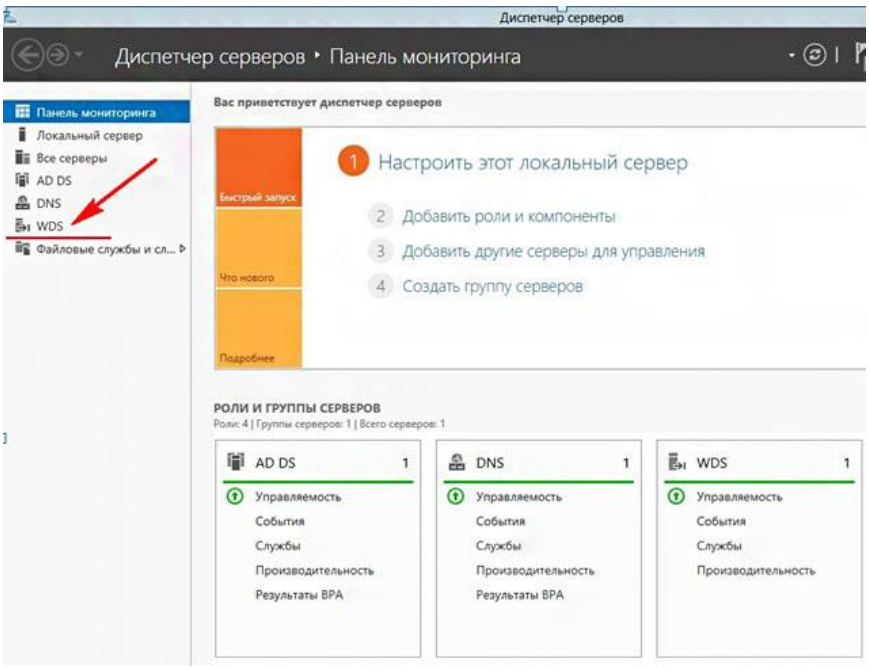


Рис. 162

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**

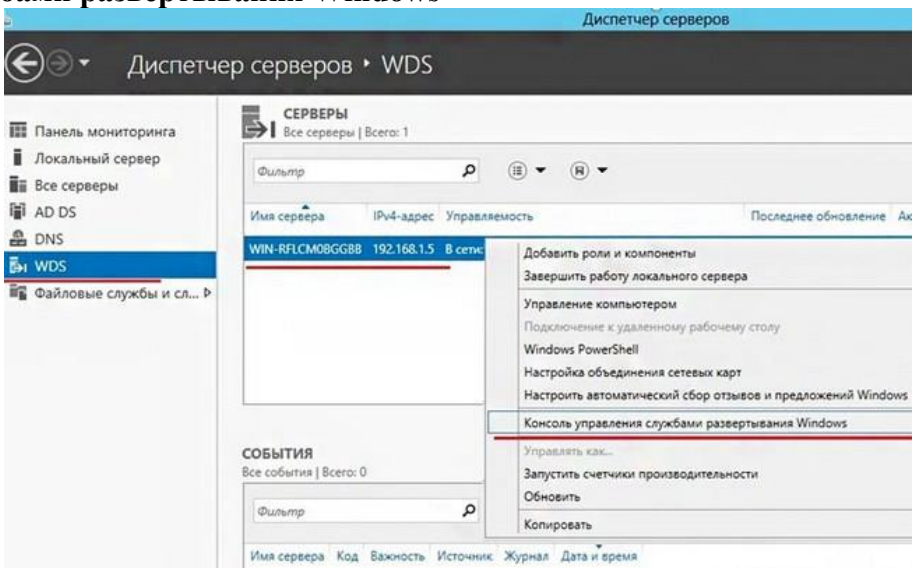


Рис. 163

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.

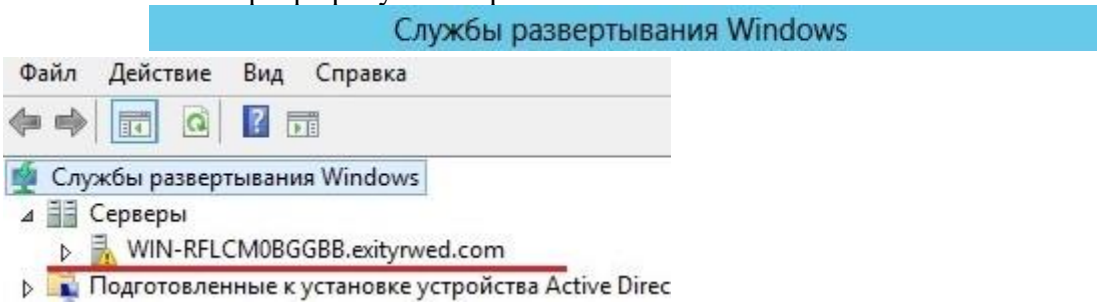


Рис. 164

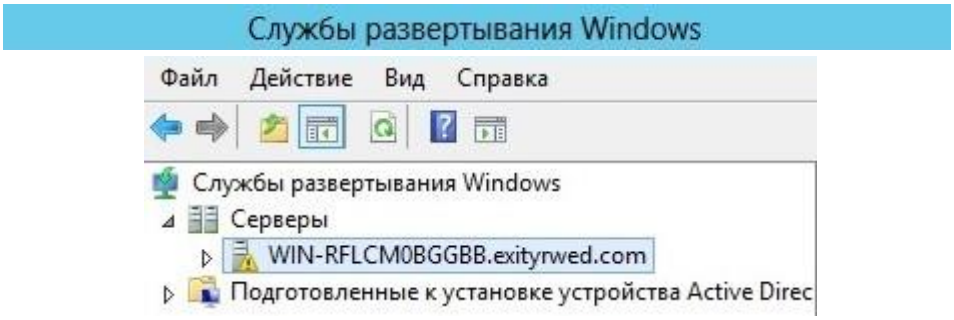
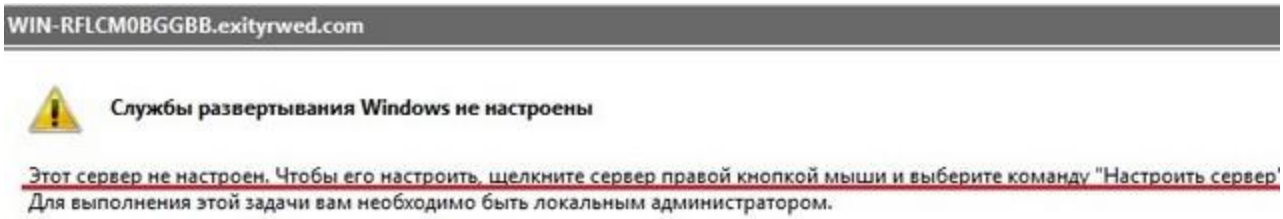
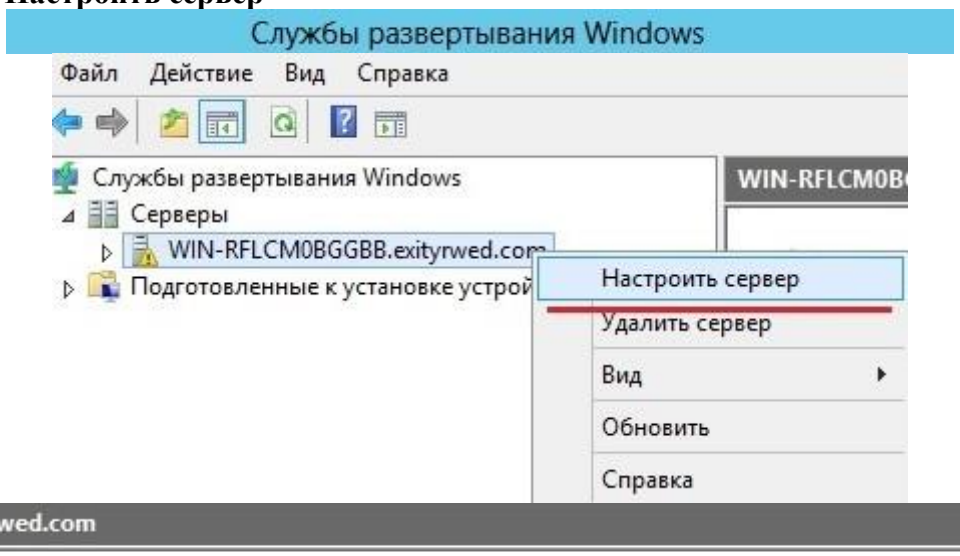


Рис. 165



Выбираем **Настроить сервер**



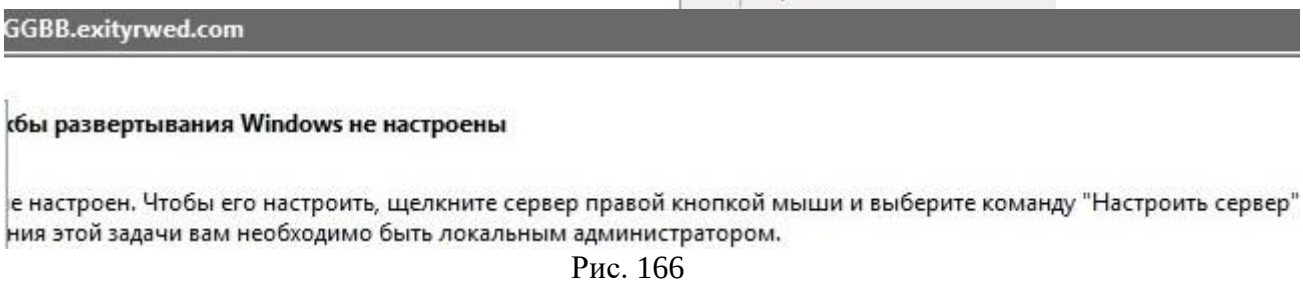


Рис. 166

Далее

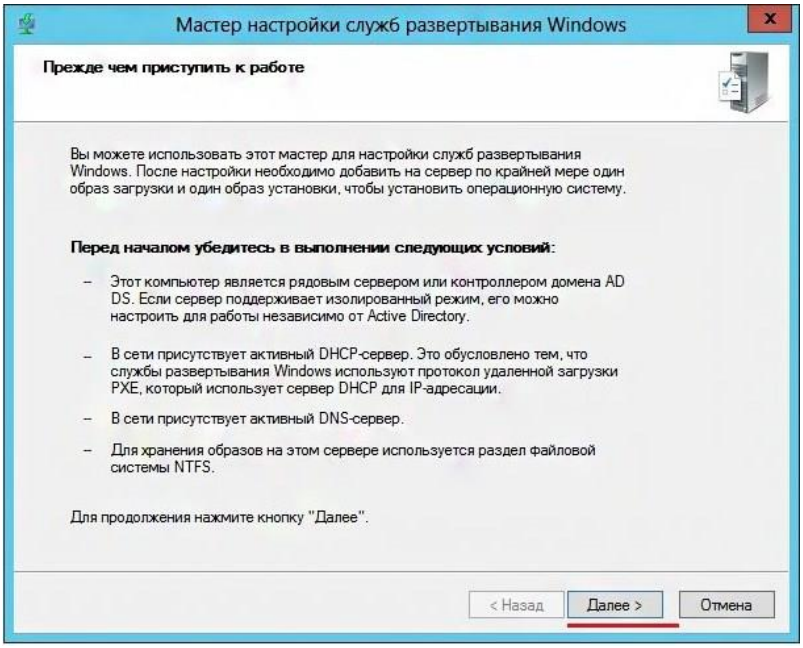


Рис. 167

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

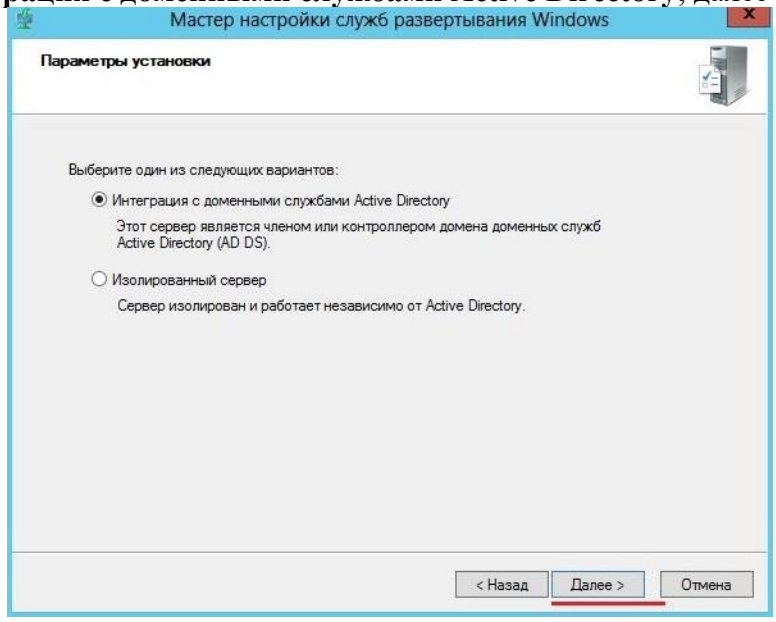


Рис. 168

Выбираем раздел для хранения загрузочных и установочных образов

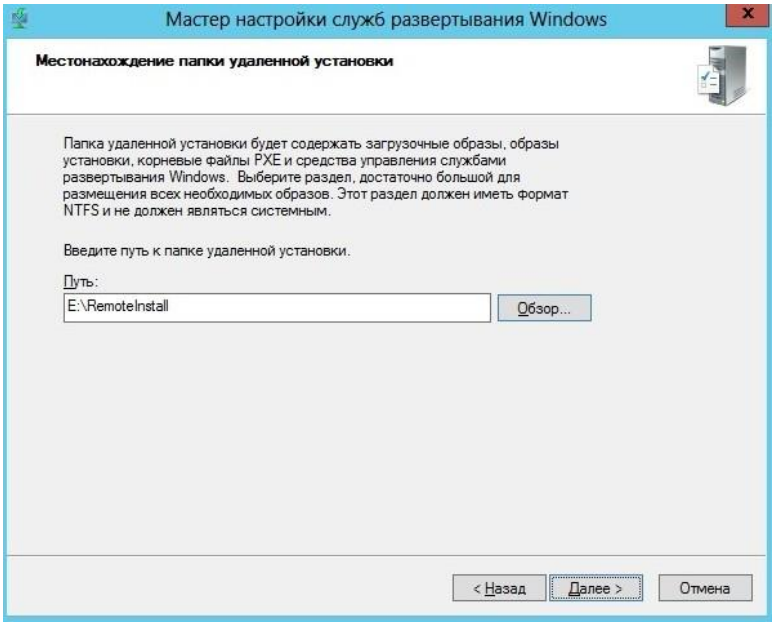


Рис. 169

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

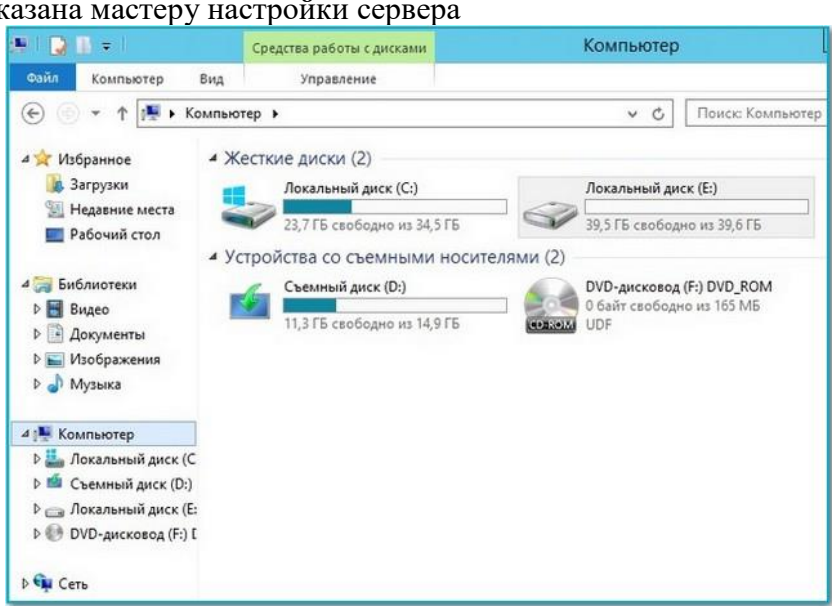


Рис. 170

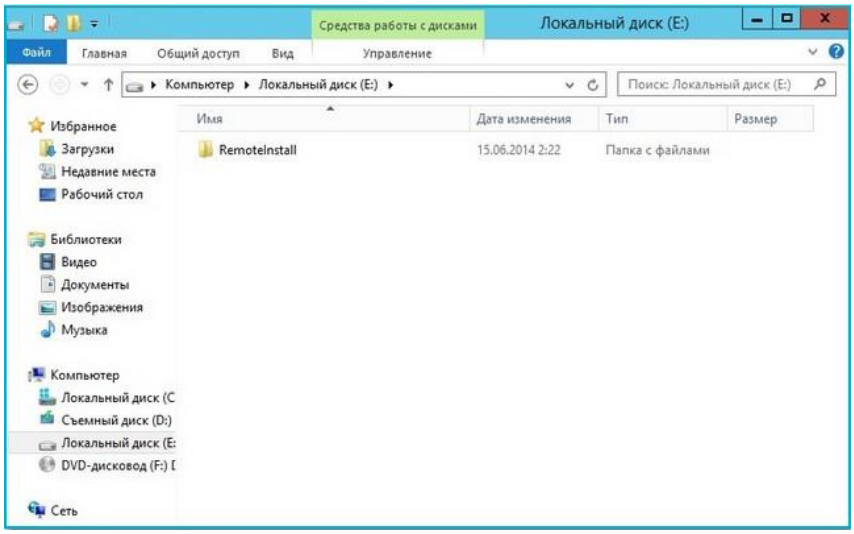


Рис. 171

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

Далее

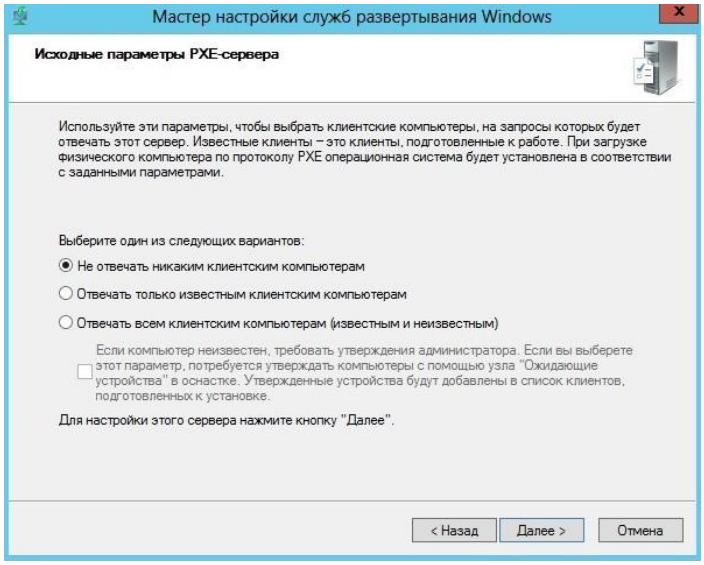


Рис. 172

Запуск служб развертывания Windows

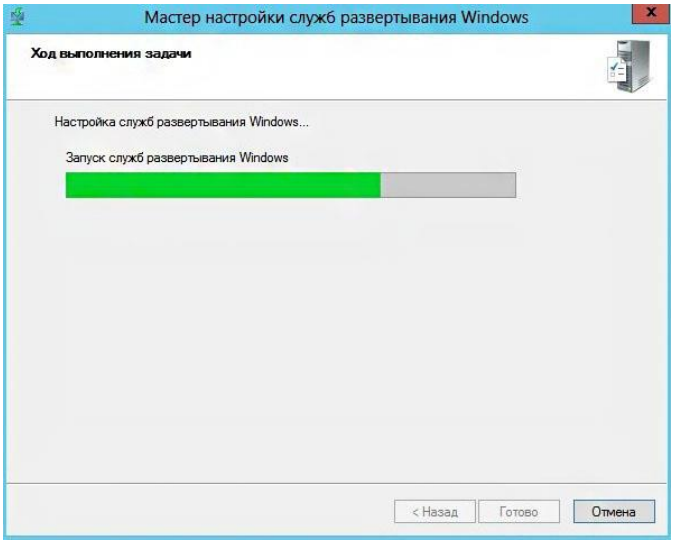


Рис. 173

Службы развертывания успешно настроены. Готово

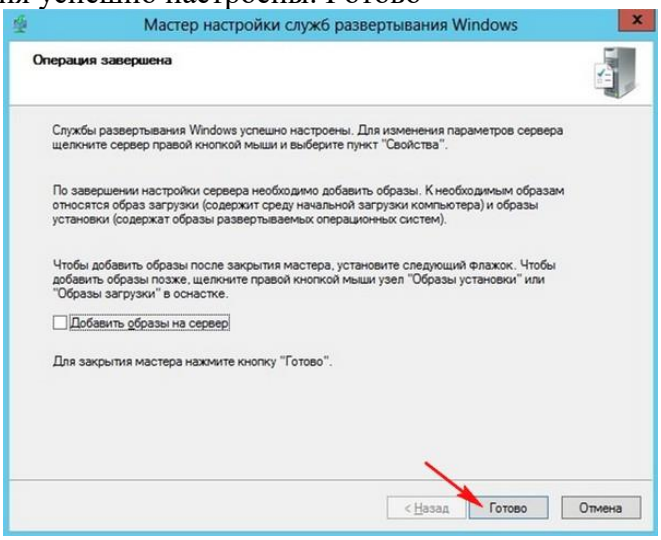


Рис. 174

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

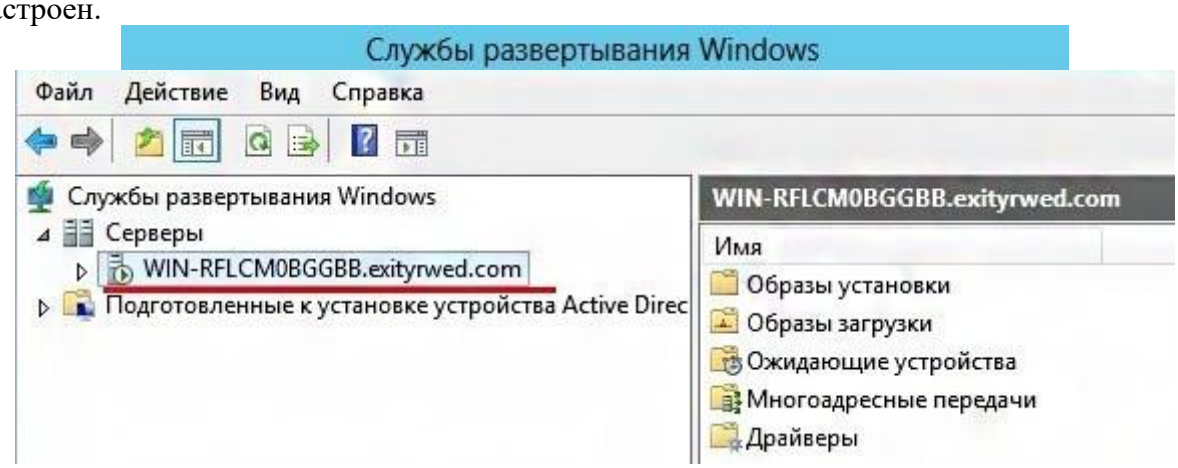


Рис. 175

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

2.13. Практическая работа № 13 «Внедрение управления обновлениями. Мониторинг Windows Server 2012»

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).

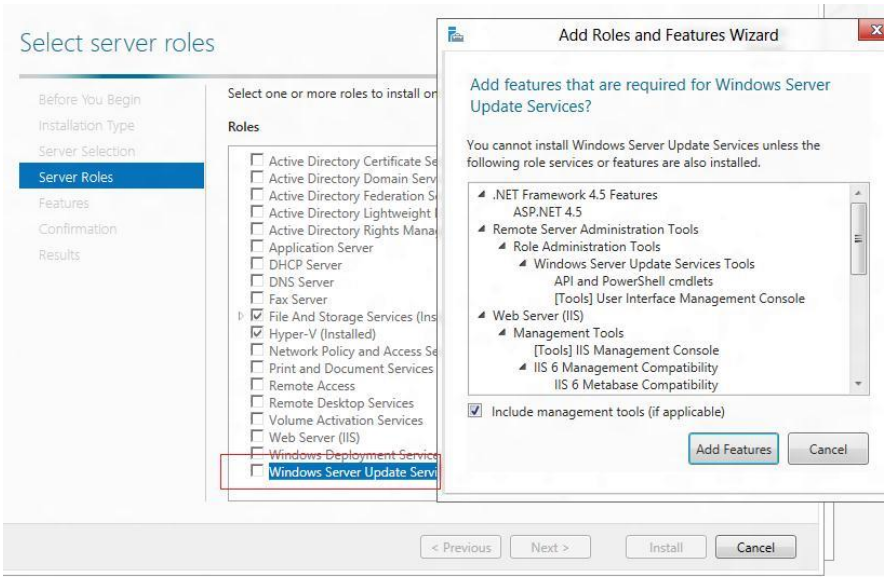


Рис. 176

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**.

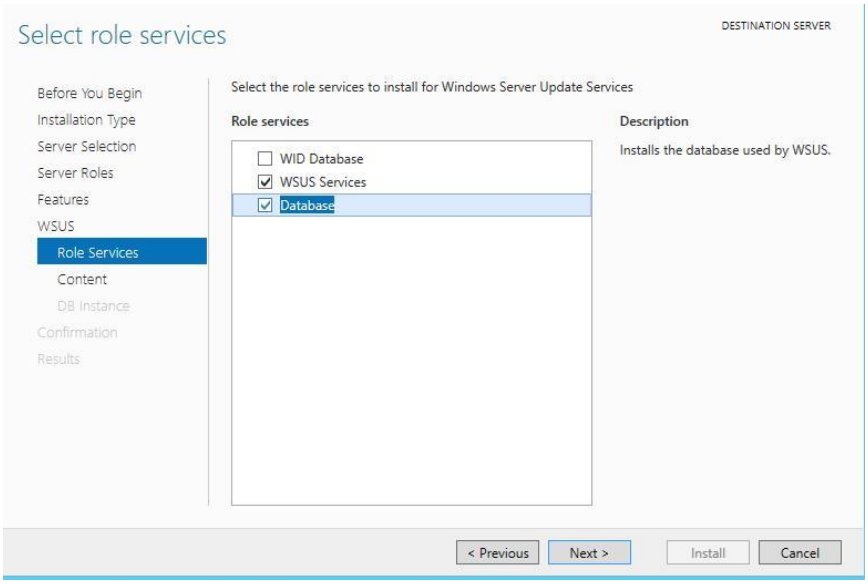


Рис. 177

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.

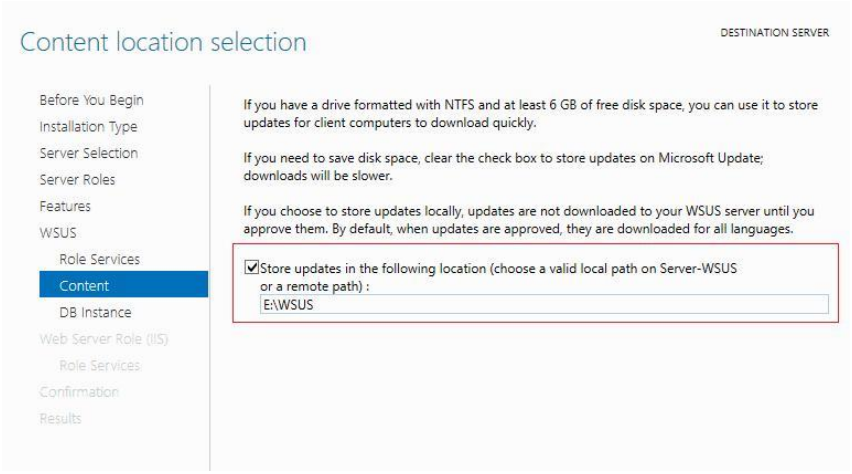


Рис. 178

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

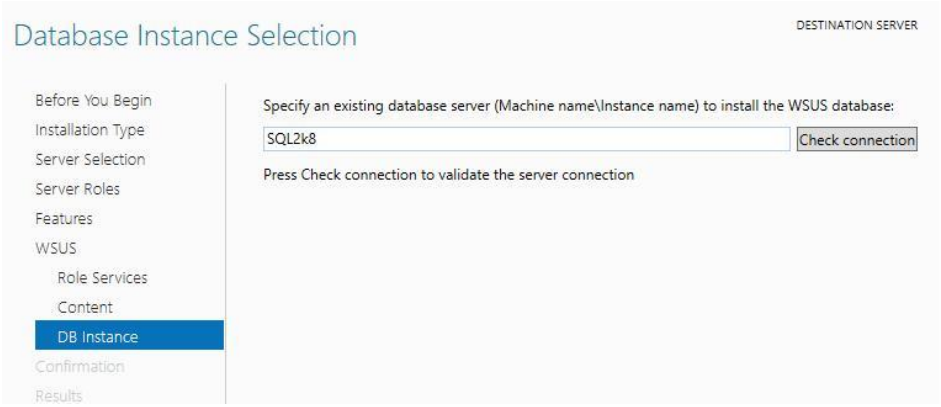


Рис. 179

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

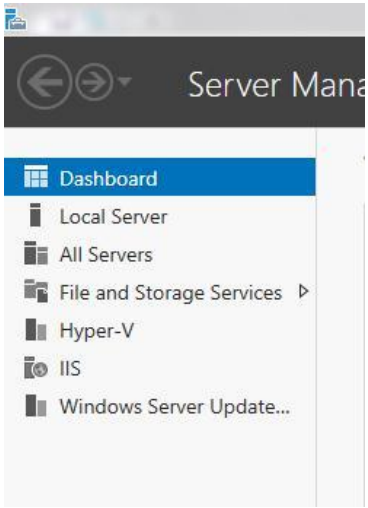


Рис. 180

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).

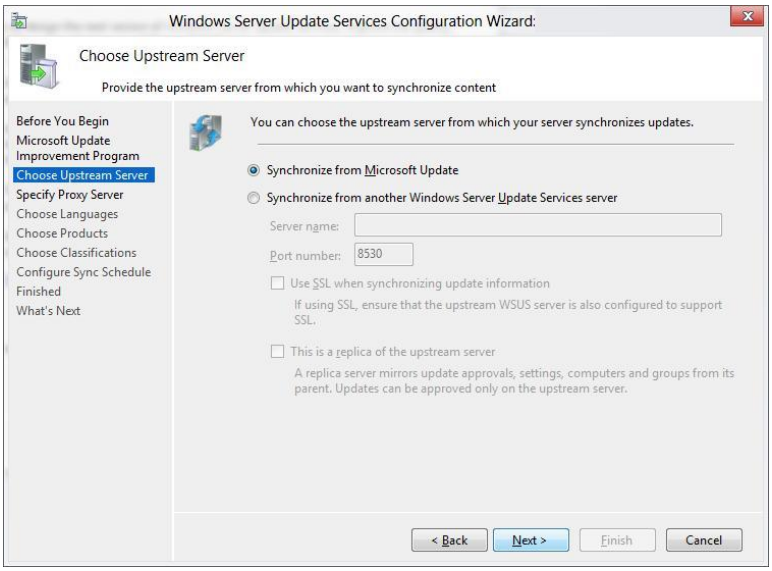


Рис. 181

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.

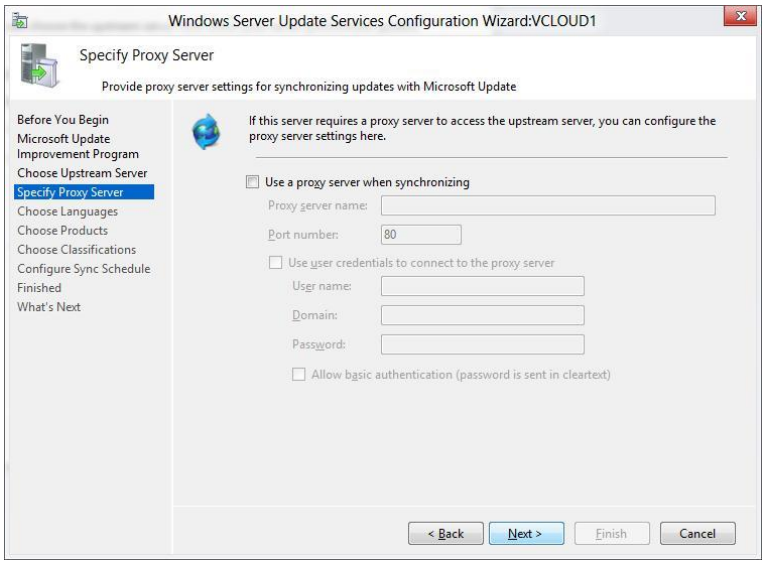


Рис. 182

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

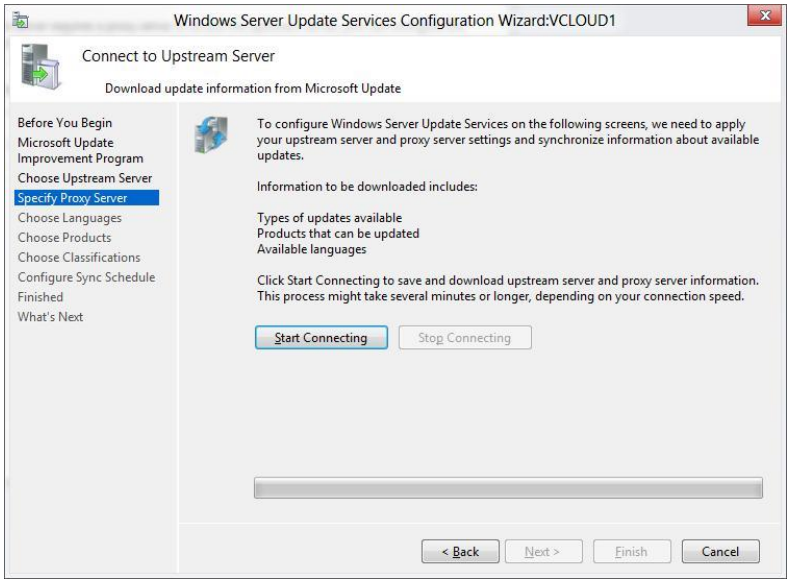


Рис. 183

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).

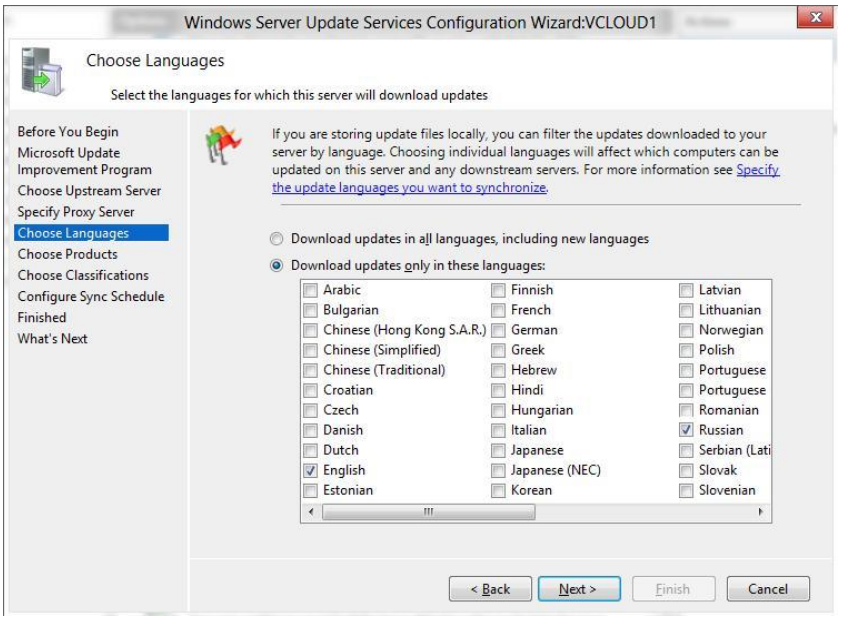


Рис. 184

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.

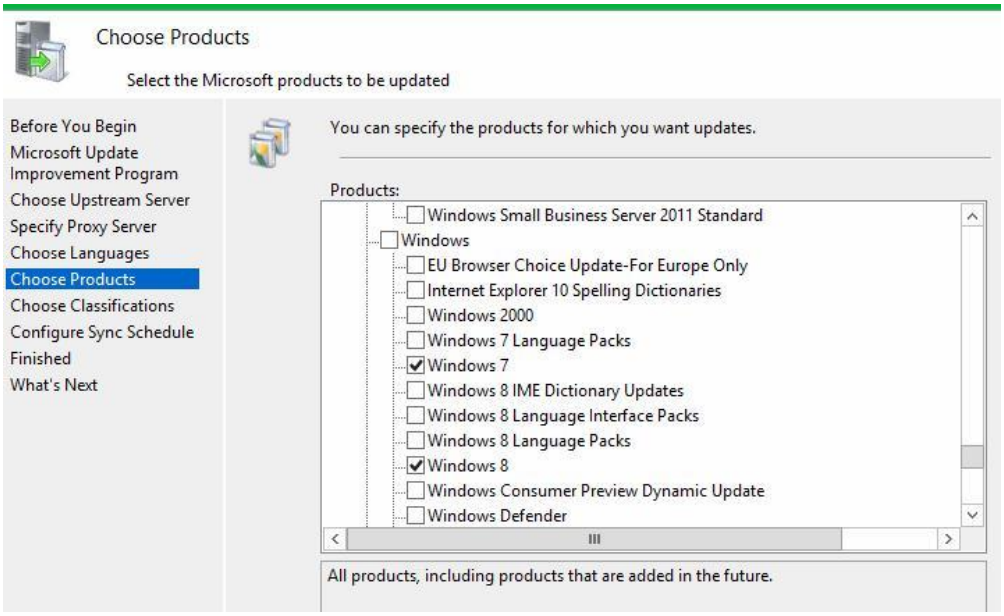


Рис. 185

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.

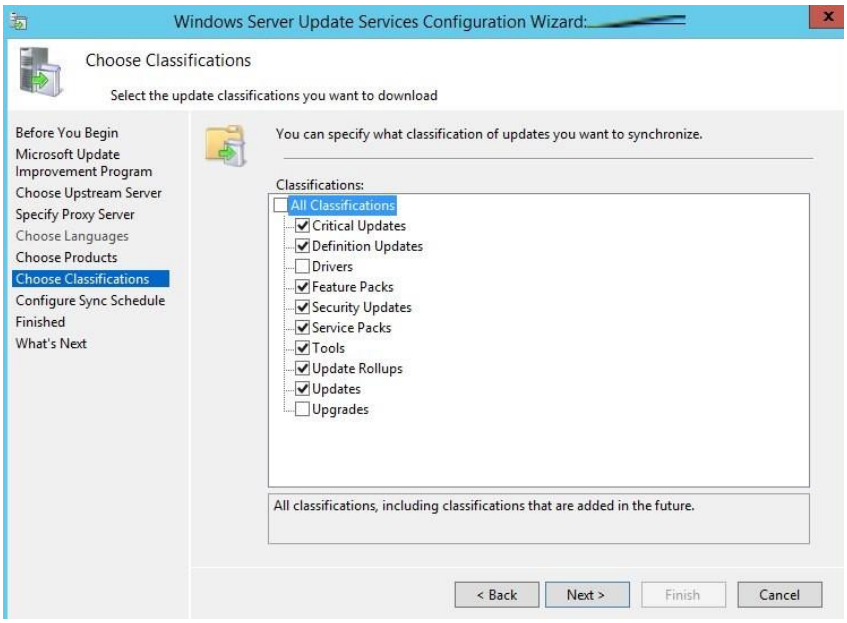


Рис. 186

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.

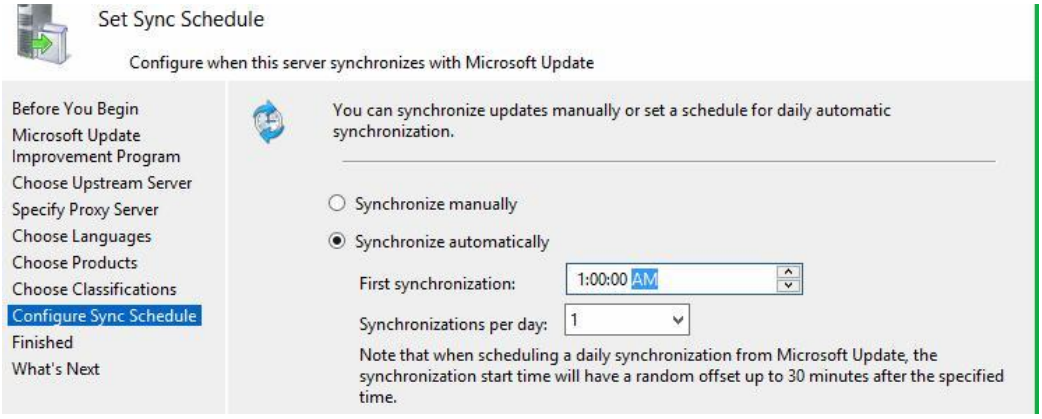


Рис. 187

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.

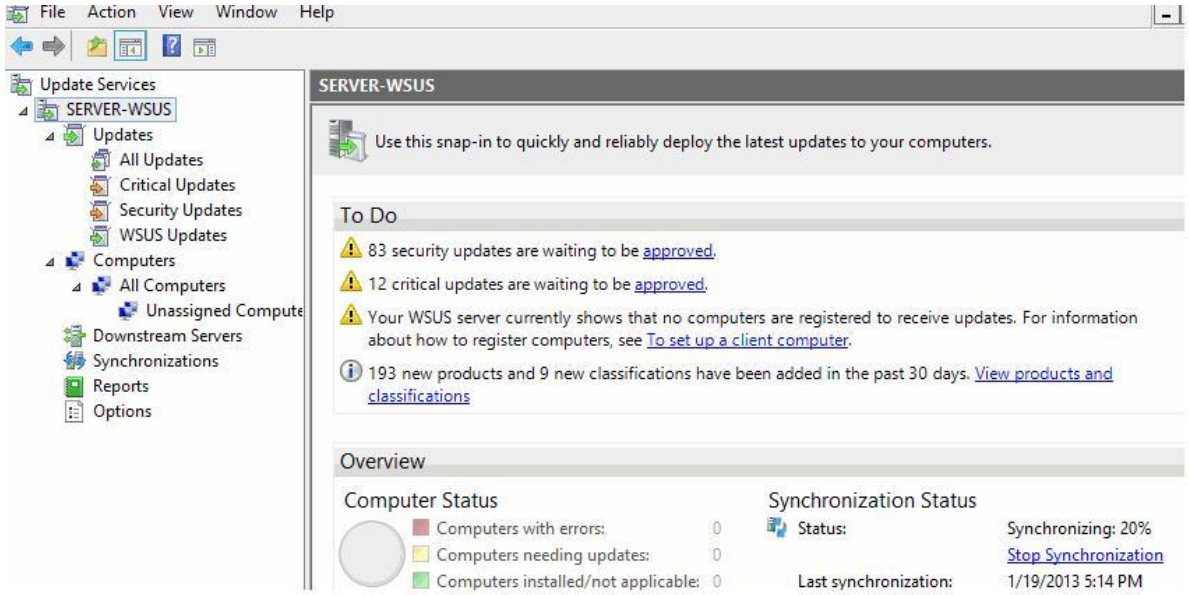


Рис. 188

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).

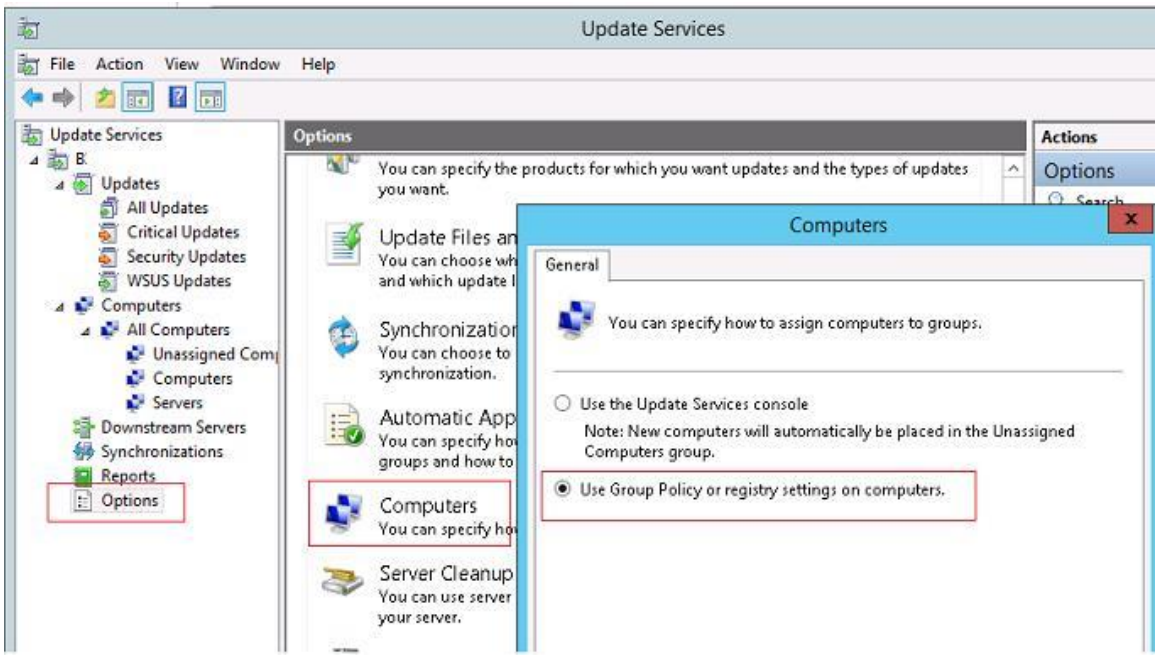


Рис. 189

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).

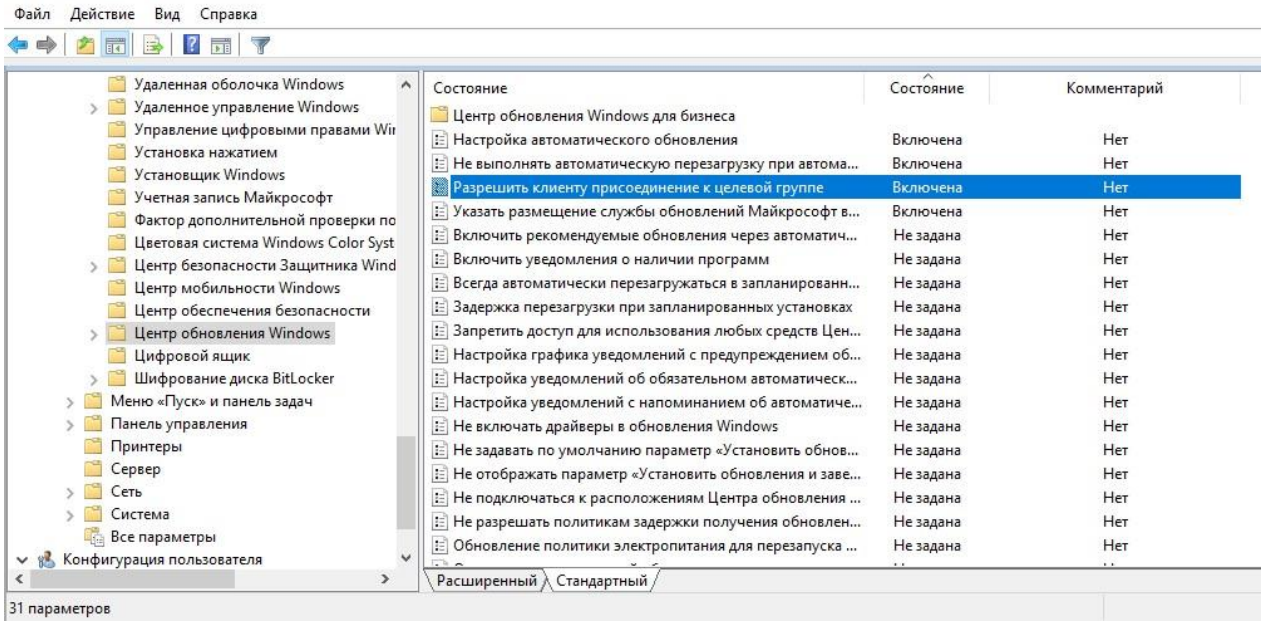


Рис. 190

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 локальный 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.

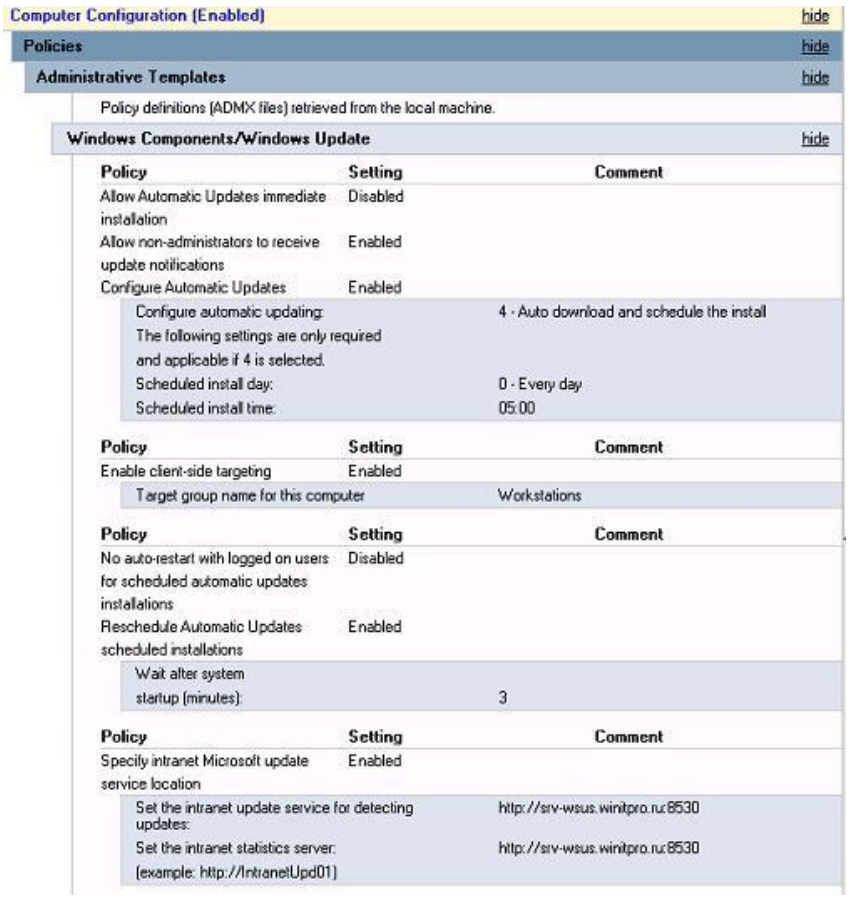


Рис. 191

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**).

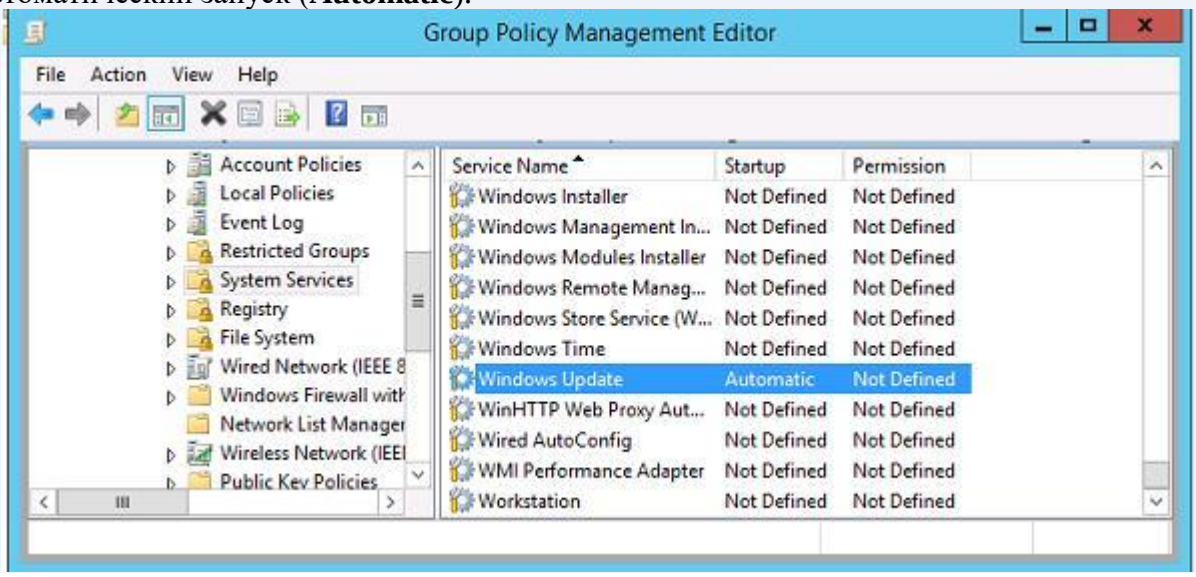


Рис. 192

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.

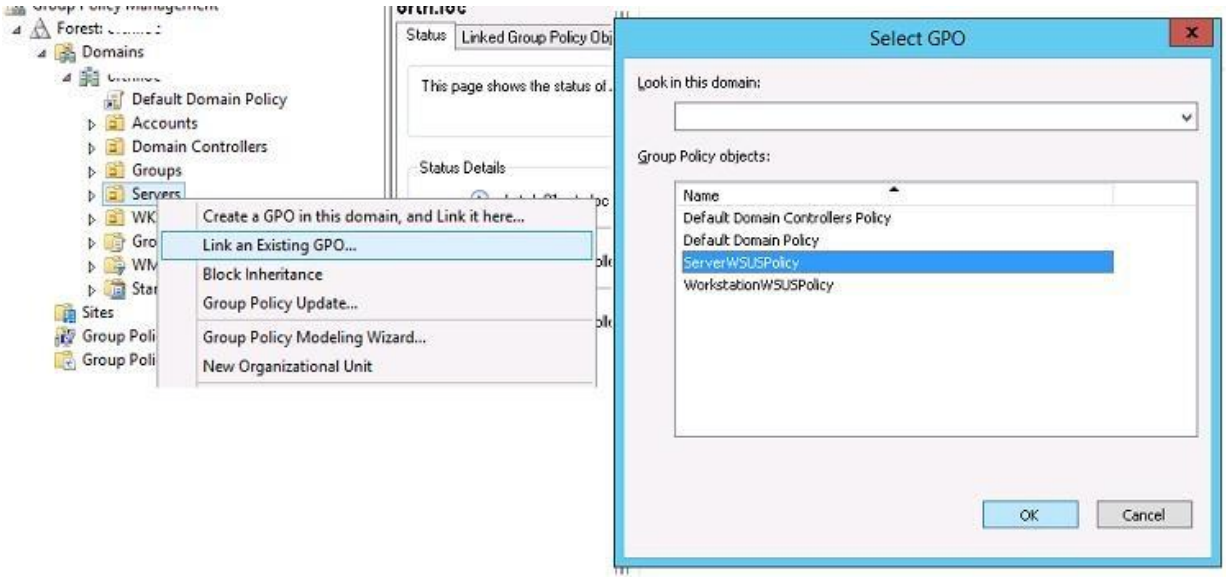


Рис. 193

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

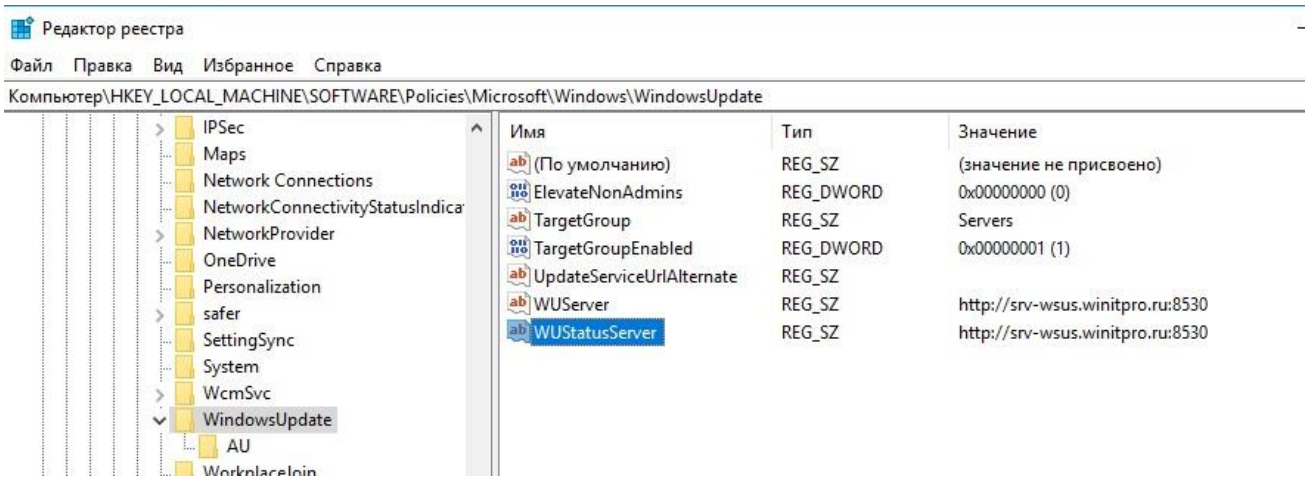


Рис. 194

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.

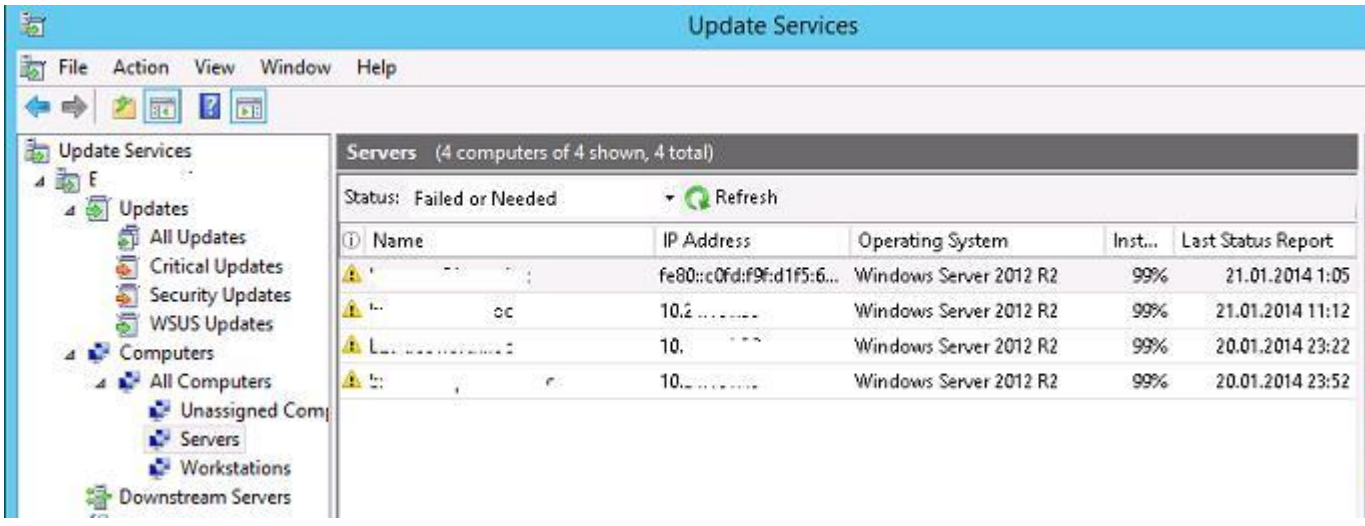


Рис. 195

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.

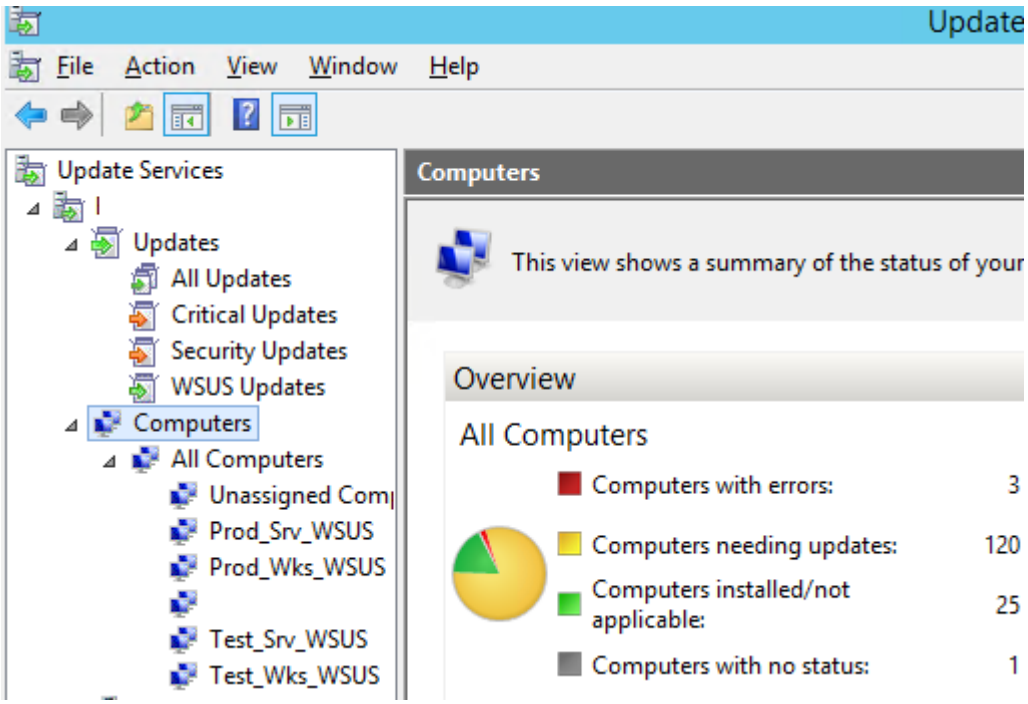


Рис. 196

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

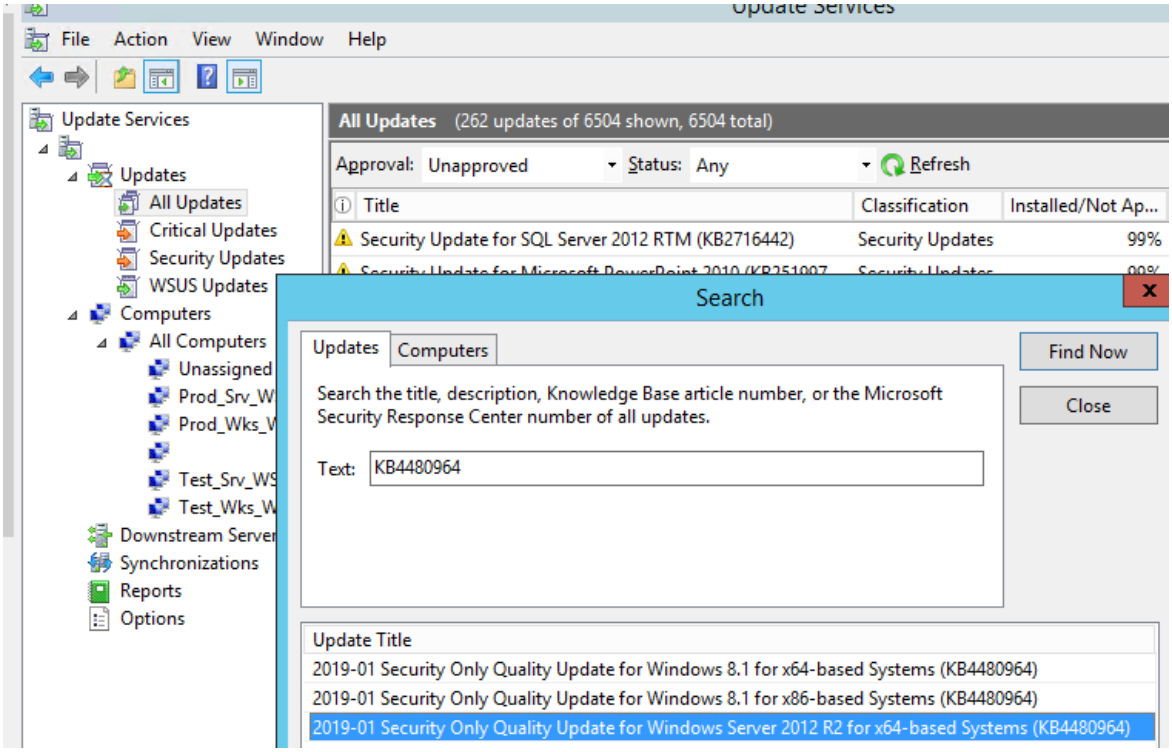


Рис. 197

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

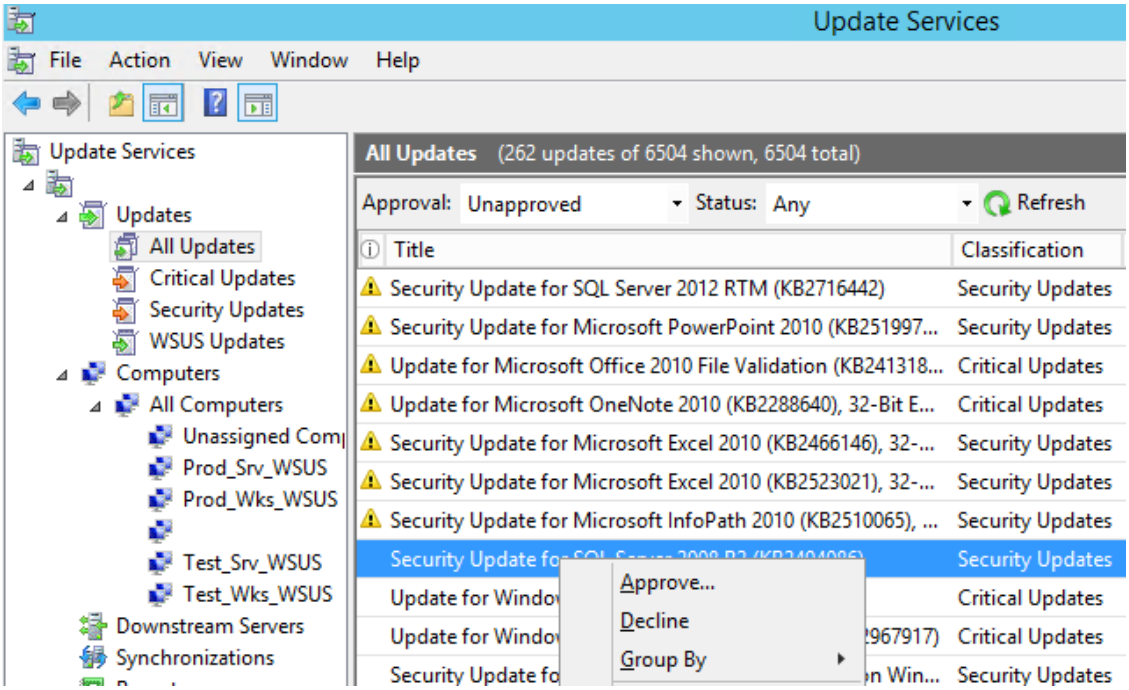


Рис. 198

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.

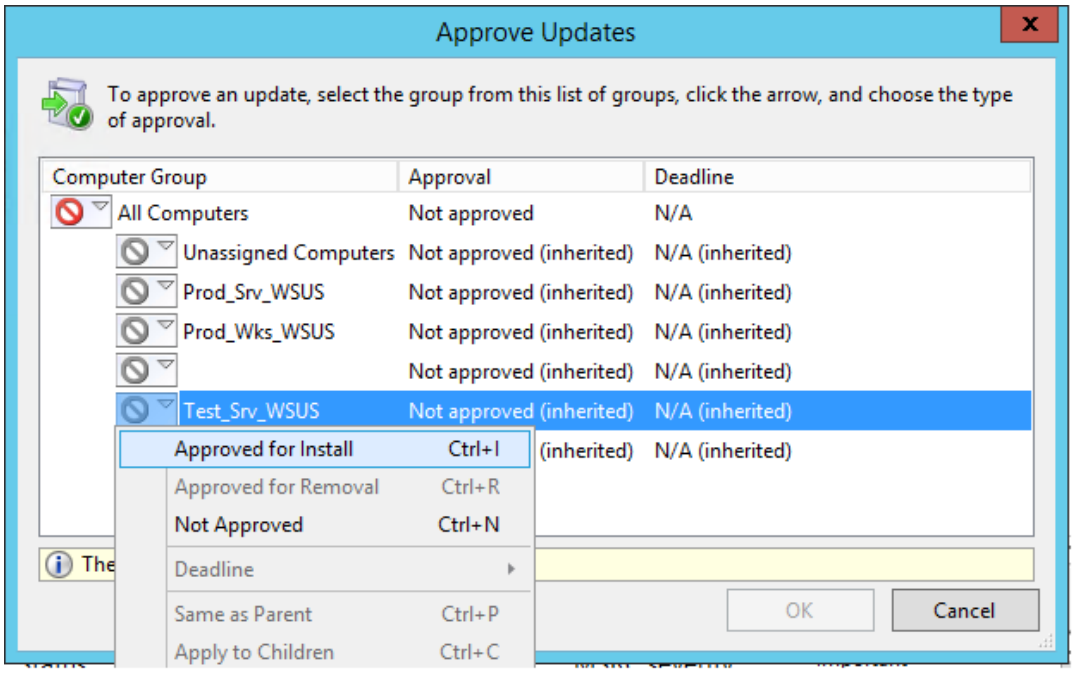


Рис. 199

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

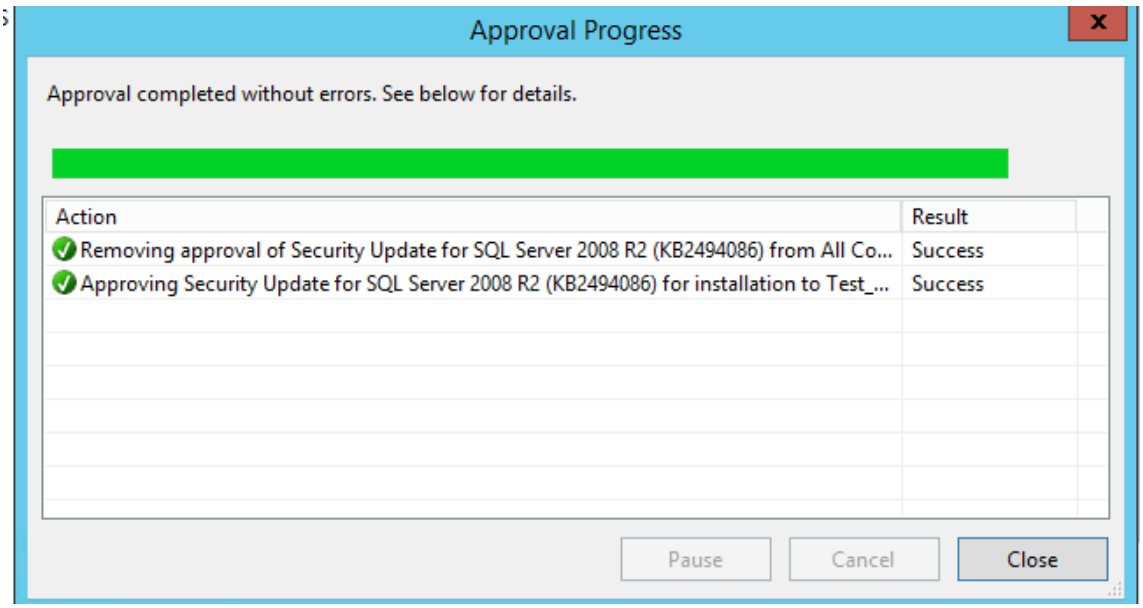


Рис. 200

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**.

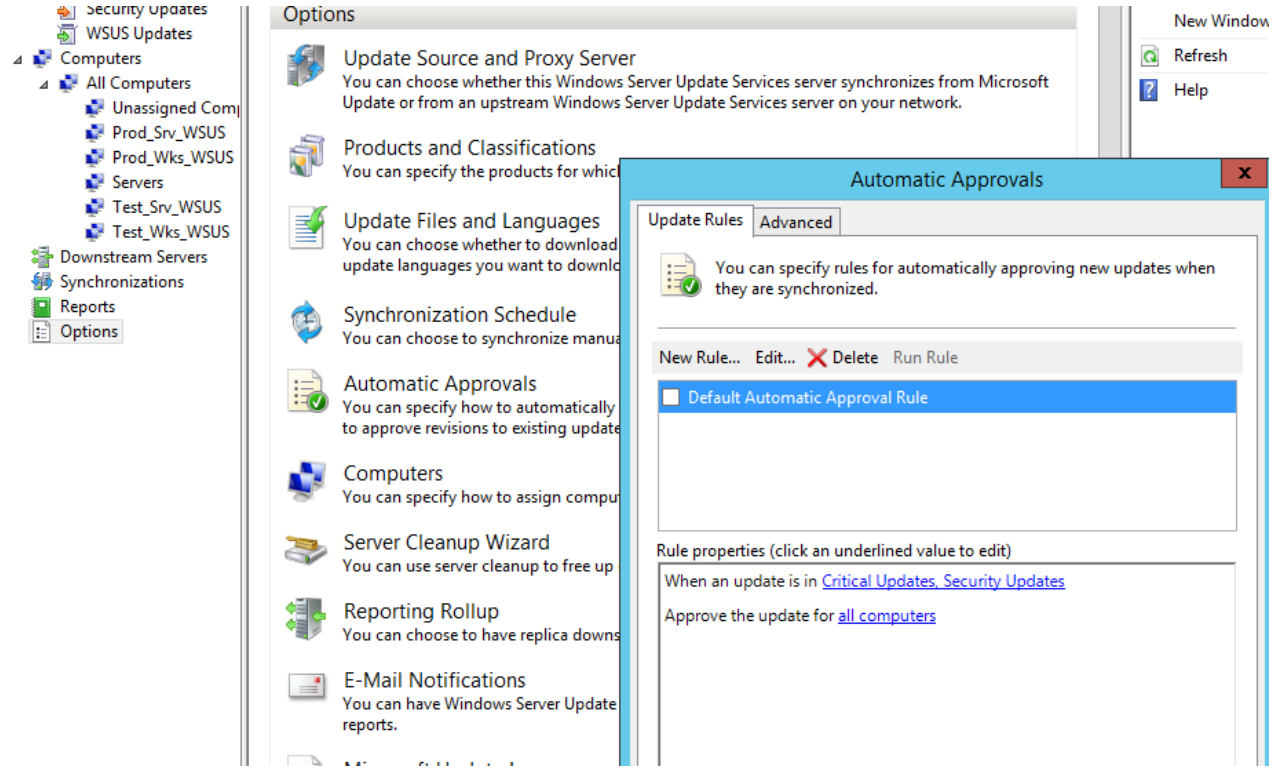


Рис. 201

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

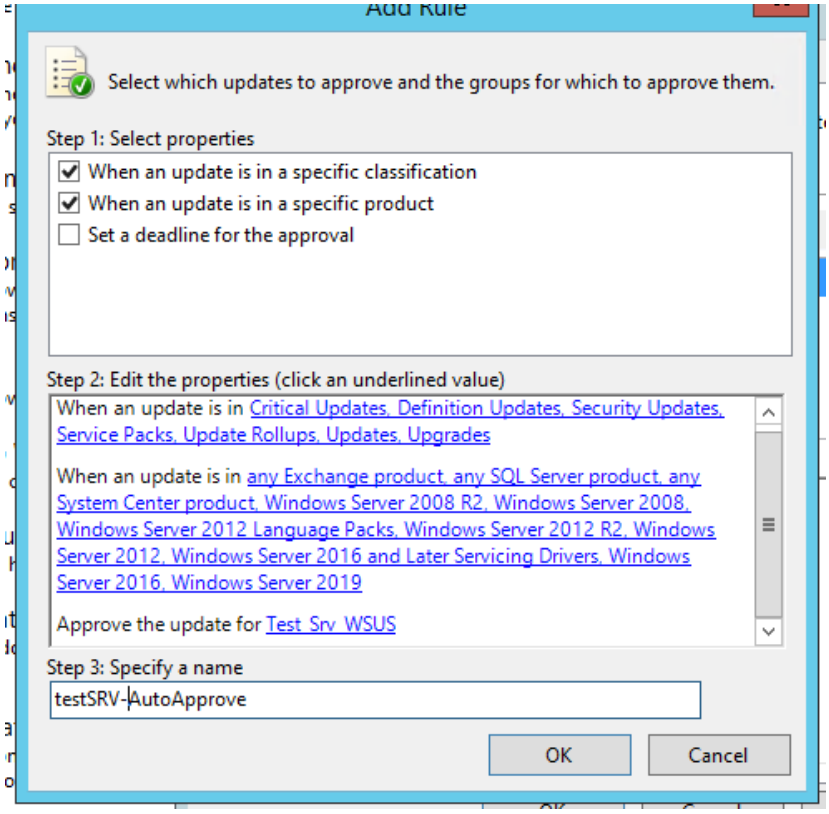


Рис. 202

Щелкая на каждую синюю ссылку, откроется соответствующее окно свойств.

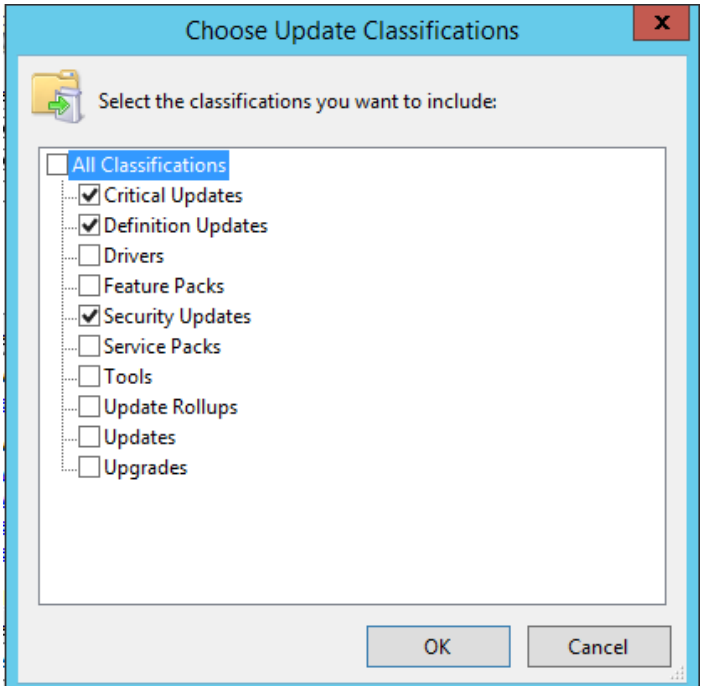


Рис. 203

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.

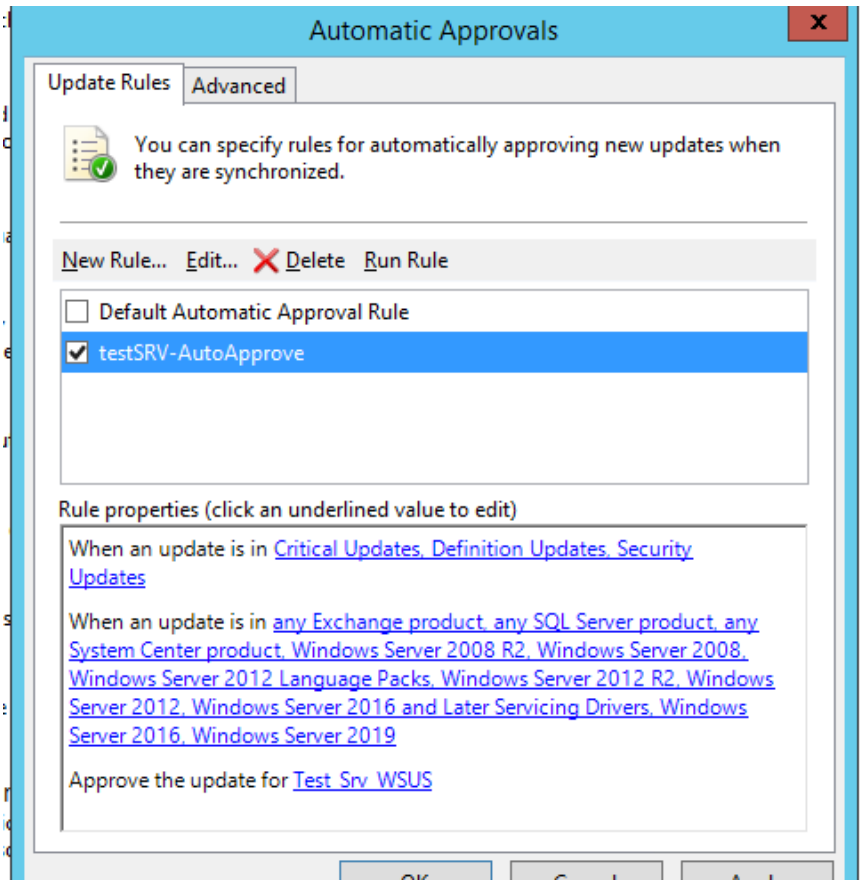


Рис. 204

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.

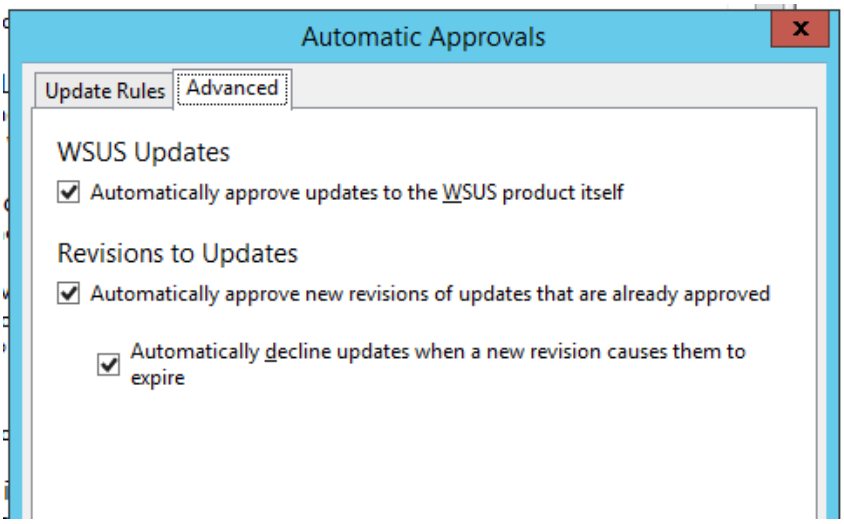


Рис. 205

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

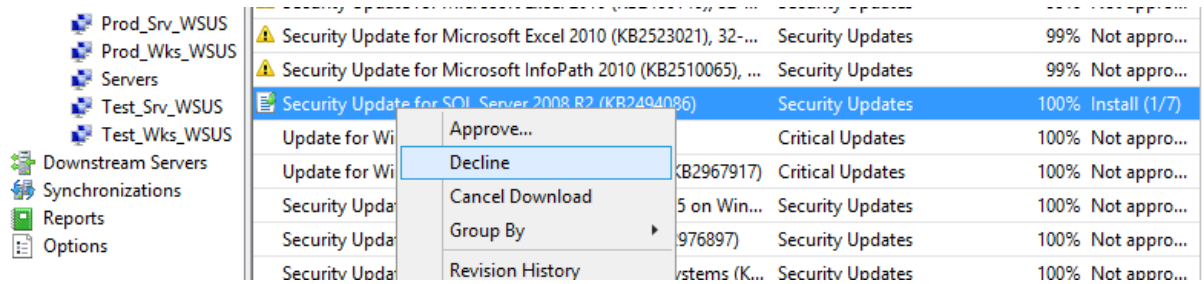


Рис. 206

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

Практическое занятие №14. Настройка файлового сервера

Задание: создать файловый сервер.

Для выполнения задания необходимо добавить службы: Файлового сервера и Диспетчера ресурсов. Далее запустить оснастку «Диспетчер ресурсов файлового сервера» (File Server

Resource Manager) через Пуск > Администрирование (Start — > Administrative Tools). В меню «Действие» (Actions) выбрать «Создать квоту»(Create Quota), в строке адреса указываем путь к каталогу, к которому нужно назначить квоту. Выбрать «Задать настраиваемые свойства квоты» и нажимаем «Настраиваемы свойства» (Custom properties), в поле «Порог» (Space limit) указываем нужное нам значение дискового пространства. После чего сохранить настройки.

Запустить оснастку «Управление общими ресурсами»(Share and Storage Management) как обычно через Пуск > Администрирование (Start — > Administrative Tools), где в меню«Действие»(Actions) выбрать «Подготовить общий ресурс»(Provision Share). В первом окне «Мастера подготовки общих папок» указать путь к папке общего доступа. Далее необходимо указать нужные варианты доступа, квоту и применяемые политики.

Сохранить все параметры и проверить работоспособность.

Практическое занятие № 15. Настройка DHCP

Задание: Установить и настроить DHCP.

Для установки и настройки DHCP необходимо выполнить следующие действия:

1. Нажмите ПУСК и выберете Панель управления;
2. Откройте Установка и удаление программ в панели управления;
3. Нажмите кнопку Установка компонентов Windows в панели установка и удаление программ;
4. В списке Компоненты Windows выберите Сетевые службы и нажмите кнопку Состав;
5. В открывшемся окне Сетевые службы установите флажок напротив элемента DHCP и нажмите кнопку OK;
6. После копирования файлов и установки службы DHCP система попросит вас перезагрузится.

Для настройки DHCP необходимо выполнить:

1. Нажмите ПУСК и выберете Панель управления;
2. В Панели управления выберите Администрирование;
3. В Администрирование выберите DHCP;
4. В дереве консоли щелкните правой кнопкой мыши сервер DHCP, для которого необходимо создать новую область DHCP, и выберите пункт Создать область;
5. В Мастере создания новой области нажмите кнопку Далее, а затем введите имя и описание области. Имя может выбираться произвольным образом. Нажмите кнопку Далее;
6. Введите диапазон адресов, входящих в область. Поскольку эти адреса будут присваиваться клиентам, они должны быть действительными внутри данной сети и не

использоваться в данный момент. При необходимости можно ввести и использовать новую маску подсети. Нажмите кнопку Далее;

7. Введите IP –адреса которые были статически присвоены некоторым компьютерам в сети, и которые следует исключить из указанного диапазона заданного ранее. Нажмите кнопку Далее;
8. Введите срок действия аренды IP-адреса из данной области (дней, часов и минут). Нажмите кнопку Далее и выберите пункт Да, настроить эти параметры сейчас, если вам нужно продолжить работу мастера и настроить основные параметры DHCP. Нажмите кнопку Далее;
9. Введите IP-адрес основного шлюза, который должен использоваться клиентами при получении адреса из данной области. Нажмите Добавить для включения адреса шлюза по умолчанию в список и щелкните кнопку Далее;
10. Если в сети уже имеется сервер DNS, введите доменное имя вашей организации в поле Родительский домен. Введите имя сервера DNS и нажмите кнопку Сопоставить, чтобы проверить способность сервера DHCP установить связь с сервером DNS и определить его адрес. Нажмите кнопку Добавить, чтобы включить этот сервер в список серверов DNS, назначенных клиентам DHCP. Нажмите кнопку Далее и выполните те же действия еще раз, если в сети имеется сервер WINS (Windows Internet Naming Service), указав его имя и IP-адрес. Нажмите кнопку Далее;
11. Щелкните Да, я хочу активировать эту область сейчас, чтобы активировать область и разрешить выделение адресов из нее клиентам, и нажмите кнопку Далее;
12. Нажмите кнопку Готово;
13. В дереве консоли выделите имя сервера и выберите из меню Действия команду Авторизовать.

Вставьте скриншоты выполнения каждого действия. А также проверьте работоспособность DHCP на сервере, подтвердив скриншотами.

Практическое занятие № 16. Настройка центра сертификации

Задание: Установить и настроить центр сертификации, выпустить сертификат.

Этапы установки и настройки Служб сертификации:

1 этап: Установка Служб сертификации. Через добавление служб установите службу сертификации, далее установите центр сертификации со стандартным шифрованием и шаблонными параметрами.

2 этап: Добавление шаблонов сертификатов в Центр Сертификации. Создайте стандартный шаблон сертификата.

3 этап: Выписка сертификатов пользователю Administrator и обычным пользователям с помощью mmc-консоли.

Вставьте скриншоты выполнения каждого действия. Подтвердите выполнение скриншотов созданного сертификата для пользователя Administrator.

Практическое занятие № 17. Настройка групповых политик

Задание: Настроить групповые политики.

1. В узле «Конфигурация пользователя» разверните «Административные шаблоны». Выберите шаблон «Система». Выберите папку «Профили пользователей». На правой панели два раза щёлкните элемент «Ограничить размер профиля». Выберите значение «Включён» и нажмите кнопку «Применить».
2. В узле «Конфигурация пользователя» разверните «Административные шаблоны». Выберите шаблон «Система». Выберите папку «Варианты действий после нажатия Ctrl+Alt+De»l. На правой панели два раза щёлкните элемент «Удалить диспетчер задач». Выберите значение Включён и нажмите кнопку «Применить». Вызовите любым удобным для вас способом «Диспетчер задач».

Самостоятельно выполните:

1. Запрет добавление значка ярлыка проигрывателя на рабочий стол пользователя.
2. Убрать все значки с Рабочего стола.
3. Запрещение изменения фонового рисунка Рабочего стола
4. Ограничение размера профиля конкретного пользователя.
5. Удаление кнопки Завершение работы из меню Пуск.
6. Установка обновления системы безопасности и других важных обновлений. Обновления должны происходить только каждый вторник в 12.00.
7. Запрет пользователям подключать и отключать подключения по локальной сети.

Добавьте скриншоты выполненных заданий.

Практическое занятие № 18. Добавление рабочих станций в домен

Задание: Добавить рабочие станции в домен.

1. Создайте 2 виртуальные машины с Windows 10.
2. Введите виртуальные машины в домен Windows Server 2019. Первую виртуальную машину добавьте с использованием графического интерфейса. 2 виртуальную машину добавьте через консоль Windows 10.
3. Проверьте факт занесения виртуальных машин в домен.

Добавьте скриншоты выполненных заданий.

Практическое занятие № 19. Установка сервера Debian.

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

1. **Установка Debian.**

Выберите "Graphical install" курсорными клавишами и нажмите "Enter" для запуска установщика.

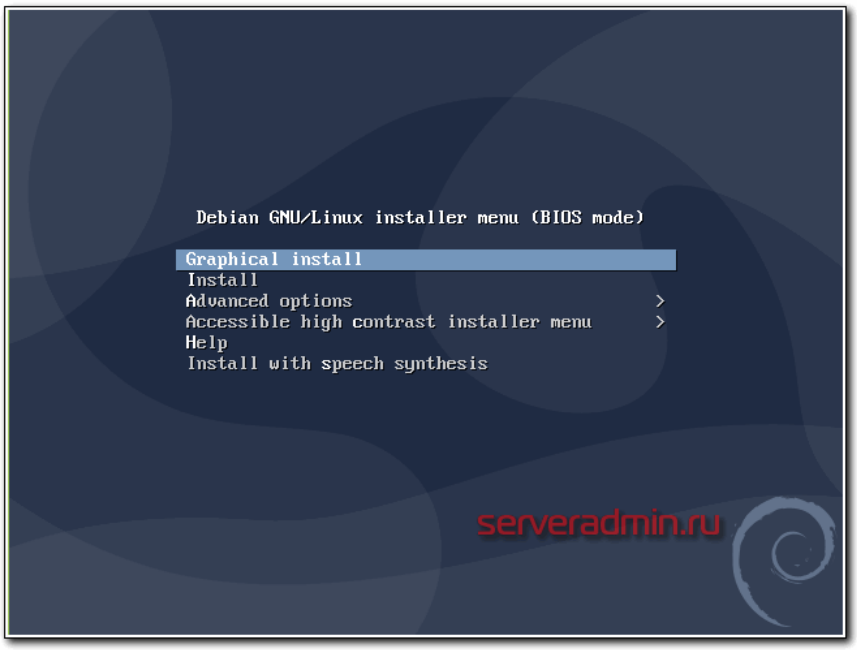


Рис. 207

Язык мастера установки и раскладка клавиатуры
Из предлагаемого списка выберите язык, который будет использоваться установщиком Debian для отображения инструкций. Для перехода к следующему шагу мастера установки ОС щелкните по кнопке «Continue».

Рис. 208

Определите местоположение, которое станет использоваться мастером установки операционной системы для определения часового пояса. Нажмите «Продолжить» и в дальнейшем щелкайте по этой кнопке для перехода к следующему шагу установки системы.

Рис. 209

Выберите клавиатурную раскладку.

Рис. 210

Из перечня выберите клавиатурную комбинацию или клавишу, с помощью которой вы станете переключаться между раскладками клавиатуры. Удобными считаются:

1. Правая клавиша «Alt».
2. Сочетание «Alt и Shift».

При выборе «Alt и Shift», сочетание не сможет использоваться в программах для других задач.

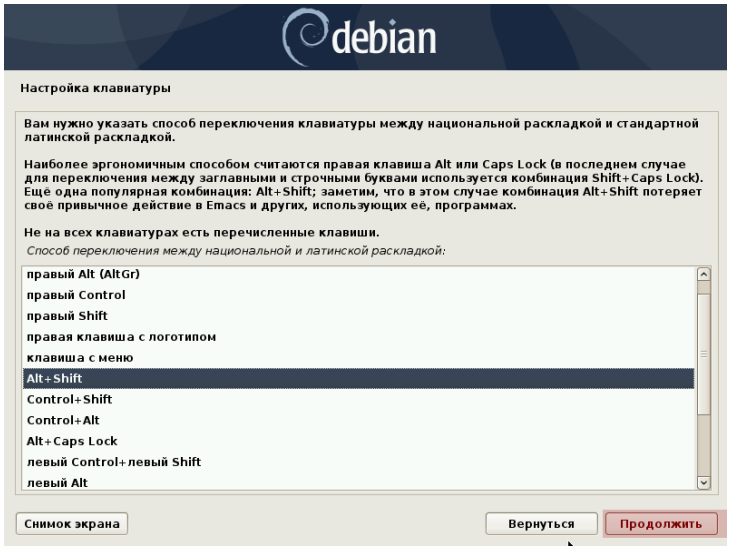


Рис. 211

Параметры установки

Стартует загрузка дополнительных компонентов. Дождитесь ее завершения.

Рис. 212

Чтобы ПК мог быть идентифицирован в сети, укажите имя пользователя, состоящее из одного слова, введенного буквами латинского алфавита. В домашних условиях — любое удобное вам. На работе — определяется администратором сети.

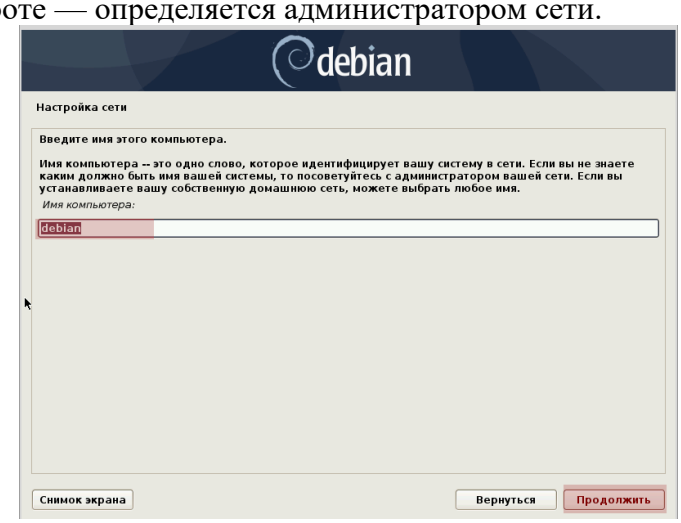


Рис. 213

Введите имя домена — часть интернет-адреса после имени пользователя. Необходимо, чтобы оно было одинаковым для всех домашних устройств. При настройке домашней сети — произвольное.

Рис. 214

Создайте пароль root:

1. Предназначен для задач администрирования системы.
2. Может включать в себя знаки препинания, цифры и латинские буквы.
3. Необходимо периодически менять.
4. Поле нельзя оставить пустым.

Повторите его в дополнительном поле.

Рис. 215

Дайте имя пользовательской учетной записи:

1. Используется вместо учетной записи root для действий, не связанных с администрированием.
2. Указывается в поле «От кого» отправляемых писем.
3. Используется всеми программами, которым необходимо реальное имя пользователя ПК.

Рис. 216

Укажите имя пользователя, под которым будете известны системе.

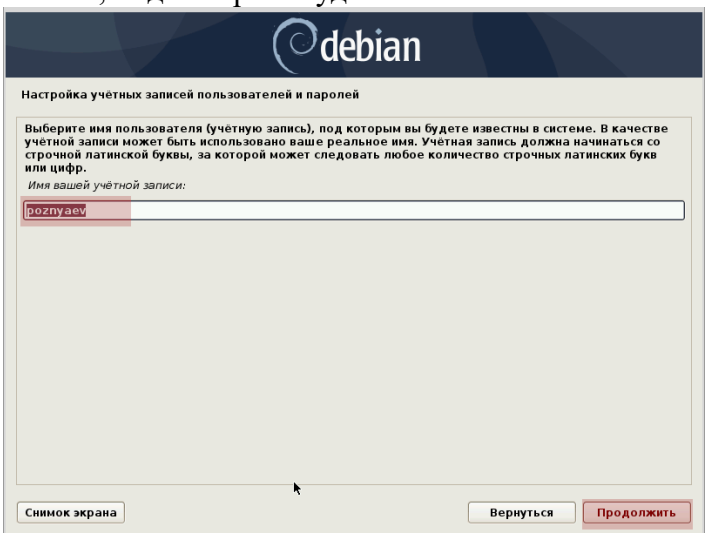


Рис. 217

Придумайте пароль. Может состоять из латинских букв, знаков препинания и цифр. Подтвердите его повторным вводом в дополнительное поле.

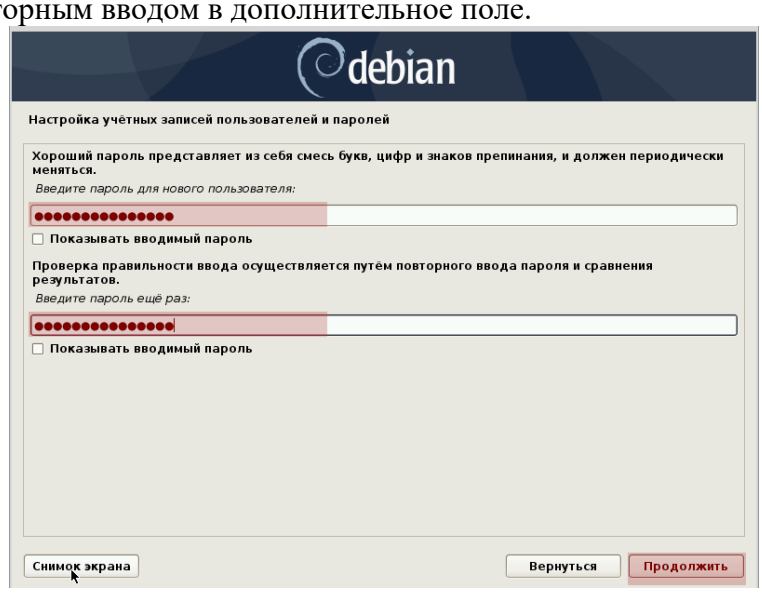


Рис. 218

Выберите часовой пояс из списка.

Рис. 219

Выберите пункт «Авто — использовать весь диск» для разметки диска, на который будет установлена ОС Debian. Все данные будут удалены с накопителя. Убедитесь, что важные файлы сохранены на дополнительных носителях.

Опытным пользователям предлагаются другие варианты разметки диска. Используйте их, если знаете, какого результата хотите достичь.

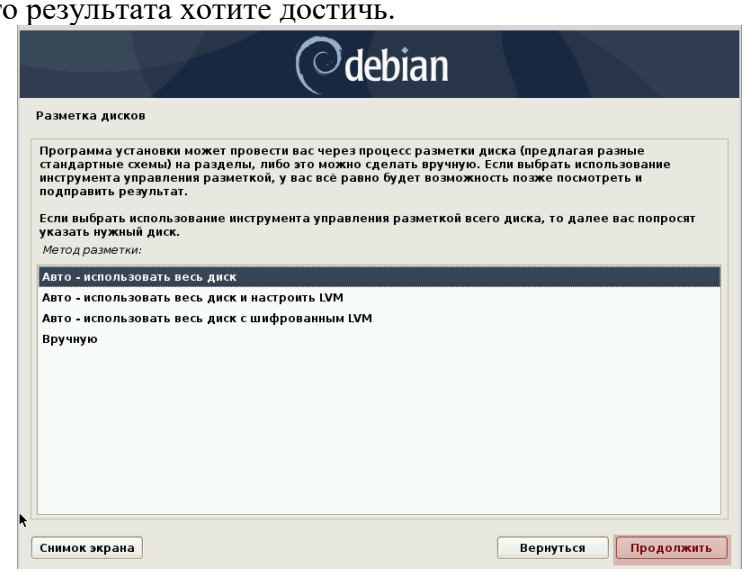


Рис. 220

Подтвердите внесение изменений.

Рис. 221

Подтвердите, что все файлы будут размещаться в одном разделе.
Предусмотрены два других подхода с созданием отдельных разделов для каталогов:

3. /home
4. /home, /var и /tmp

Рис. 222

Если вы не планируете делать другие настройки, оставьте предлагаемый по умолчанию пункт «Закончить разметку и записать изменения на диск».

Рис. 223

На экране отобразится перечень изменений, которые будут записаны на диски. Вы можете выбрать:

1. «Нет» и вернуться к ручной разметке.
2. «Да» и продолжить установку системы.

Рассматриваем второй вариант.

Рис. 224

Установка ОС, интерфейса и ПО

Дождитесь завершения установки базовой системы.

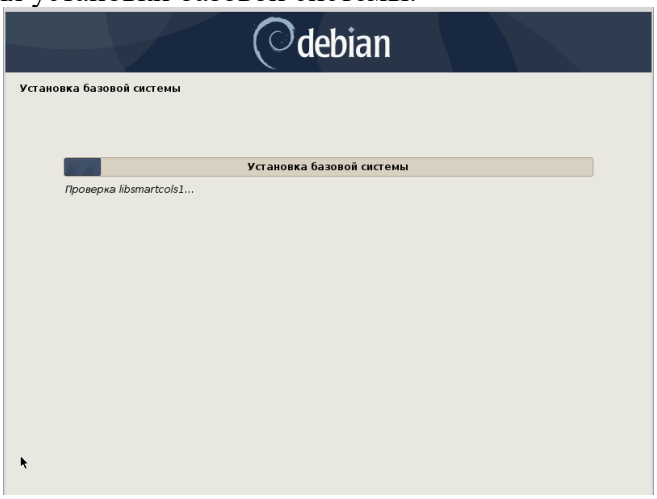


Рис. 225

Согласитесь на использование зеркала архива. Позволит настроить графическое окружение рабочего стола и устанавливать дополнительное ПО.

Помните:

1. Необходимо соединение с интернетом.
2. Используется трафик согласно тарифам вашего провайдера (оператора связи).

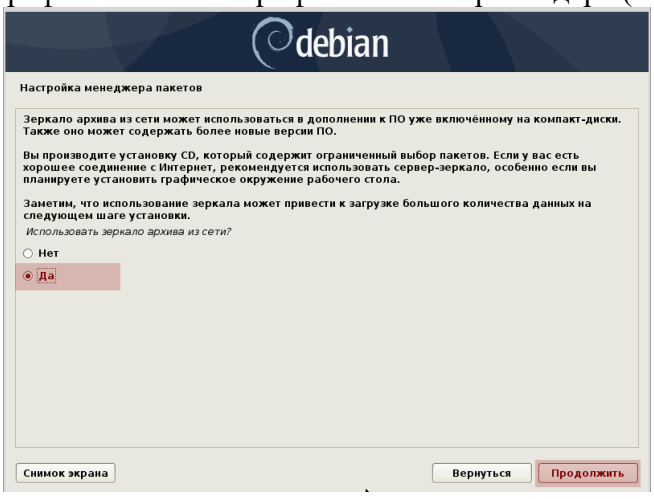


Рис. 226

Из списка выберите зеркало архива Debian в ближайшей к вам сети.

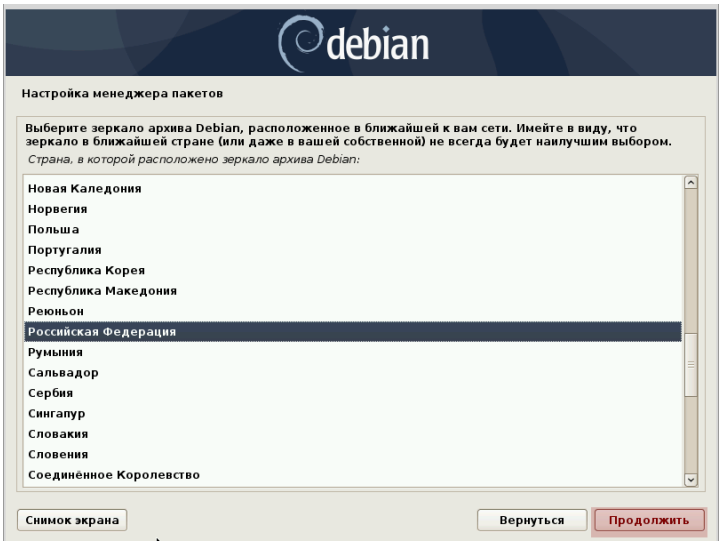


Рис. 227

«deb.debian.org» — оптимальный выбор в случаях, когда нет точного знания о том, с каким зеркалом связь лучше.

Рис. 228

Укажите HTTP-прокси, если необходимо. Если такой необходимости нет, оставьте поле пустым и перейдите к следующему шагу.

Рис. 229

Дождитесь завершения автоматической настройки менеджера пакетов…

Рис. 230

…а также выбора и установки ПО.

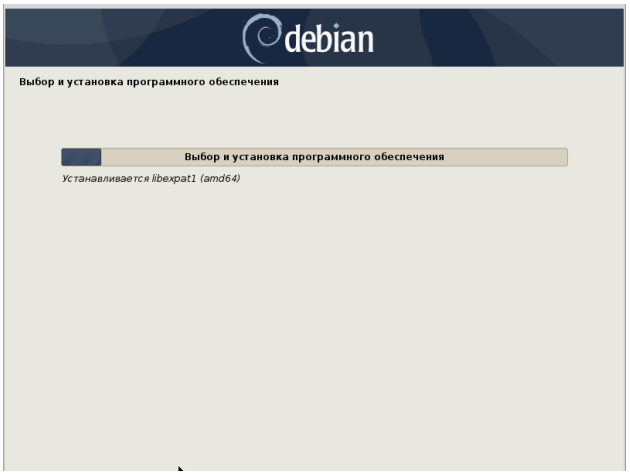


Рис. 231

Определите, позволите ли вы системе отправлять разработчикам данные о наиболее часто используемых пакетах. На основании этой информации определяется, какие пакеты добавляются на первый CD дистрибутива. Принимайте решение, внимательно ознакомившись с информацией, выведенной на экран в этом шаге установки.

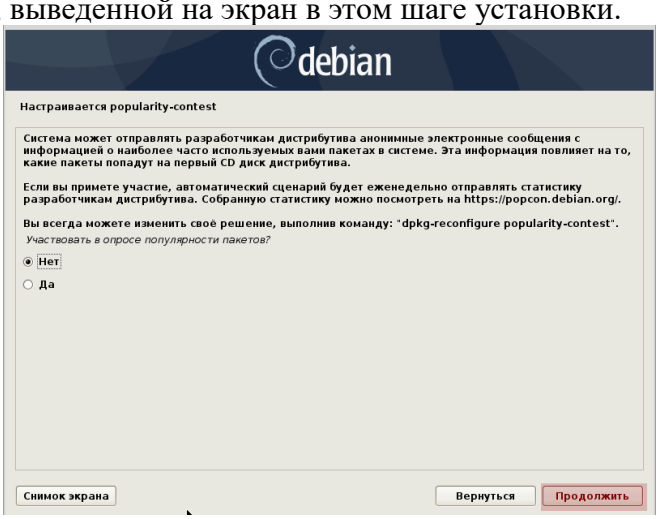


Рис. 232

Поставьте «птички» возле ПО, которое будет установлено в дополнение к базовой системе. Оставляем «птички» напротив SSH-сервер и Стандартные системные утилиты.

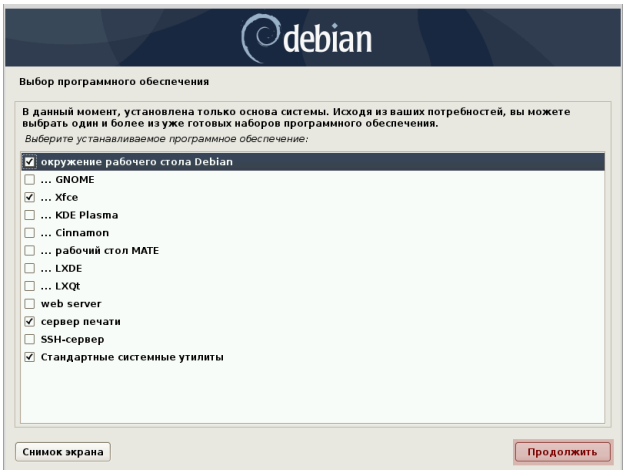


Рис. 233

Автоматическая стадия: выбор и установка программного обеспечения. Никаких действий производить не нужно. Дождитесь завершения.

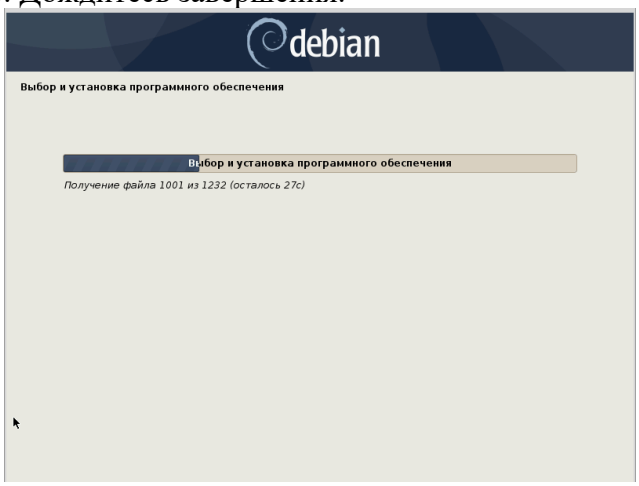


Рис. 234

Согласитесь на установку системного загрузчика GRUB. Рассматриваю этот вариант, предполагая, что Debian будет единственной ОС компьютера. Если на ПК установлена другая система, ее не получится использовать до тех пор, пока GRUB не будет настроен для ее загрузки.

Рис. 235

Подтвердите установку системного загрузчика на жесткий диск ПК.

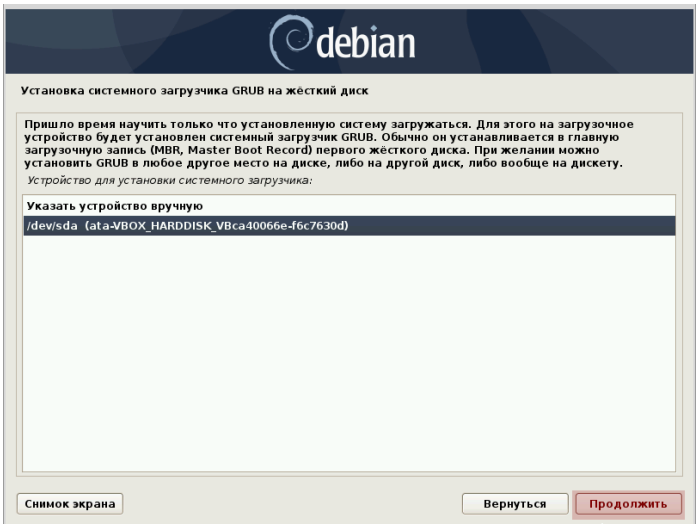


Рис. 236

Автоматическая установка загрузчика на жесткий диск.

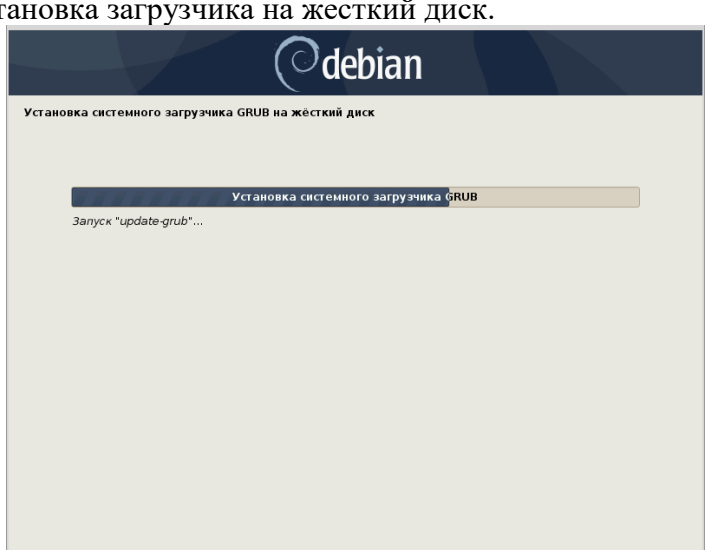


Рис. 237

Перезагружаем сервер. Установка завершена, он полностью готов к работе.

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

2.15. Практическая работа № 15 «Установка и настройка веб-сервера на базе Nginx + PHP-FPM в Debian

Задание:

1. Установка Nginx

Несмотря на то, что Nginx присутствует в репозиториях основных дистрибутивов, рекомендую использовать версию от разработчиков, это позволит более оперативно получать новые версии и новые возможности. Существует две ветки Nginx, основная и стабильная, первая имеет нечетную, вторая четную нумерацию. Разработка происходит следующим образом, все изменения основной ветки, скажем 1.7 фиксируются и переходят в стабильную 1.8, которая перестает разрабатываться и получает только обновления безопасности, основная ветка после этого получает номер 1.9 и в нее вносятся все изменения.

Сами разработчики рекомендуют использовать основную ветку, если только нет каких-то особых требований по совместимости. По своему опыту можем сказать, что основная ветка достаточно стабильна и может быть использована на рабочих серверах.

Для подключения репозиториев Nginx создадим в папке **/etc/apt/sources.list.d** файл **nginx.list**:

```
touch /etc/apt/sources.list.d/nginx.list
```

Потом добавим в него строки. Для Debian:

```
deb http://nginx.org/packages/mainline/debian/ codename nginx
deb-src http://nginx.org/packages/mainline/debian/ codename nginx
```

где **codename** - кодовое имя дистрибутива, например, **jessie** для Debian 8. Если вам не нужны исходные тексты, то репозитории **deb-src** можно не подключать (т.е. не добавлять эти строки).

Затем скачаем и установим PGP-ключ, необходимый для проверки подлинности:

```
cd
wget http://nginx.org/keys/nginx_signing.key
apt-key add nginx_signing.key
```

После чего можно обновить список пакетов и установить nginx:

```
apt-get update
apt-get install nginx
```

Теперь, если набрать в браузере адрес нашего сервера, вы увидите стандартную заглушку Nginx.

Рис. 238

Также проверить состояние веб-сервера можно командой:

```
service nginx status
```

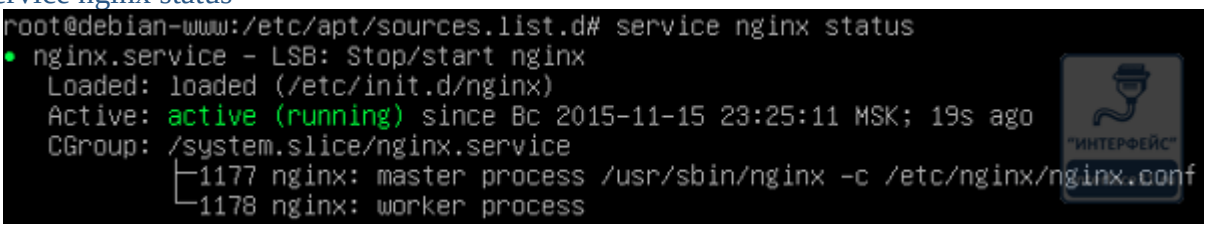


Рис. 239

Теперь перейдем к настройке. Для этого перейдем в папку **/etc/nginx** и откроем файл **nginx.conf**, мы будем перечислять настройки в порядке их нахождения в файле, если данной опции нет - ее следует добавить.

Прежде всего изменим пользователя, от имени которого работает nginx, в Debian/Ubuntu веб-сервер работает от пользователя **www-data** и чтобы избежать в будущем возможных коллизий с правами доступа приведем строку к виду:

```
user  www-data;
```

Затем укажем количество рабочих процессов, рекомендуется выбирать их количество по числу доступных процессорных ядер, в нашем случае 2:

```
worker_processes  2;
```
Приведем секцию **events** к виду:
```
events {
 worker_connections 1024;
 use epoll;
}
```
Первая опция задает количество соединений на рабочий процесс, вторая задает метод обработки соединений, явно укажем наиболее эффективный для Linux.
Теперь перейдем в секцию http и после строки
```
access_log  /var/log/nginx/access.log  main;
```
зададим следующие опции:
```
client_header_timeout 30;
client_body_timeout 30;
reset_timedout_connection on;
```
Они задают таймаут (в секундах) на чтение клиентом тела и заголовка запроса, последняя опция разрешает сброс соединений по таймауту.
```
client_max_body_size 32m;
client_body_buffer_size 128k;
```
Эти параметры ограничивают максимальный размер тела запроса клиента и задают буфер для чтения заголовка запроса. Максимальный размер тела запроса ограничивает размер файла, который может быть загружен веб-сервером.
```
sendfile on;
tcp_nopush on;
```
Также разрешим передачу файлов и оптимизируем этот процесс.
Изменим параметр:
```
keepalive_timeout  30;
```
Он задает таймаут постоянных (keep-alive) соединений, которые позволяют повысить производительность протокола HTTP/1.1, но незакрытое соединений впустую использует ресурсы сервера и поэтому такие соединения следует принудительно завершать.
Ниже зададим параметры **gzip-сжатия**:
```
gzip on;
gzip_disable "msie6";
gzip_proxied any;
gzip_min_length 1024;
gzip_comp_level 4;
gzip_types text/plain text/css application/json application/javascript application/x-javascript
text/xml application/xml application/xml+rss text/javascript application/atom+xml applica-
tion/rdf+xml;
```
Первая опция включает gzip-сжатие, затем отключаем его для младших версий IE (6 и ниже), если такие вдруг зайдут на наш сервер, разрешим сжимать проксированные запросы, это нужно для сжатия динамического содержимого, затем укажем минимальный размер сжимаемого ответа, чтобы не тратить ресурсы сервера на сжатие коротких ответов. Ниже задается уровень сжатия и типы сжимаемых данных.
В самом конце, после
```
include /etc/nginx/conf.d/*.conf;
```
добавим
```
include /etc/nginx/sites-enabled/*;
```
Это позволит подключать конфигурации виртуальных хостов из папки sites-enabled.
Сохраним и проверим конфиг командой:
```
nginx -t
```
После чего можно перезапустить nginx:

```
service nginx restart
```
Теперь можно перейти к настройке виртуальных хостов, создадим две папки:
```
mkdir /etc/nginx/sites-available
mkdir /etc/nginx/sites-enabled
```
В первой будут хранится настройки сайтов, а во второй мы будем создавать символьные ссылки для того, чтобы подключить настройки сайта к конфигурационному файлу nginx.
Перед тем как описывать виртуальные хосты, создадим структуру папок для их хранения:
```
mkdir /var/www
mkdir /var/www/example.org
```
Затем создадим конфигурационный файл для нашего первого сайта:
```
touch /etc/nginx/sites-available/example.org.conf
```
Какого-либо стандарта по названию файлов у nginx нет, поэтому можете придерживаться своей системы, главное, чтобы вам было понятно, какой файл за какой сайт отвечает. Теперь откроем его и внесем следующий текст:
```
server {
  listen 80;

  server_name example.org;
  charset utf-8;

  root /var/www/example.org;
  index index.html index.htm index.php;

  access_log /var/log/nginx/example.org_access.log;
  error_log /var/log/nginx/example.org_error.log;
}

server {

  listen 80;

  server_name www.example.org;
  rewrite ^(.*) http://example.org$1 permanent;
}
```
Его синтаксис достаточно прост и понятен, первая секция **server** задает основные параметры сайта, его имя, кодировку, расположение корневой директории и файлов логов. Вторая секция нужна для перенаправления сайта **с www** на **без www**.
Если вы хотите сделать данный виртуальный хост сайтом по умолчанию, т.е. тем на который будут переадресовываться все запросы, для которых nginx не нашел подходящего виртуального хоста или без имени сервера вообще, например, по IP-адресу, то добавьте к директиве **listen** опцию **default**, начиная с версии 0.8.1 можно использовать опцию **default_server**:
```
 listen 80 default;
```
Директива **index** указывает индексные файлы, которые будет искать в данном расположении веб-сервер в порядке их перечисления, так если в директории имеются одновременно **index.html** и **index.php** - использоваться всегда будет первый. Указанная конструкция универсальна, но на практике лучше указать один тип индексного файла, тот что реально используется.
Сохраняем конфигурацию и подключаем ее к nginx:
```
ln -s /etc/nginx/sites-available/example.org.conf  /etc/nginx/sites-enabled/
```
Проверяем конфигурацию и заставим nginx ее перечитать:

```
nginx -t
service nginx reload
```

Теперь поместим в корневую директорию сайта файл **index.html** со следующим содержимым:

```
<body><h1>OK!</h1></body>
```

Теперь набираем в браузере имя нашего сайта и убеждаемся, что все работает.

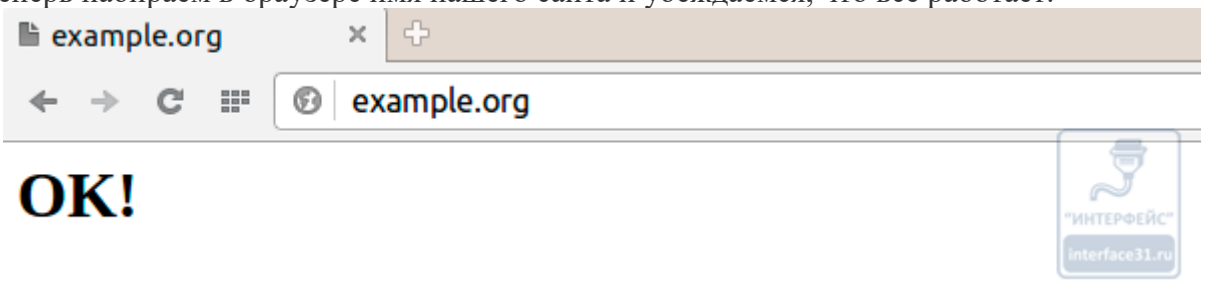


Рис. 240

2. Устанавливаем PHP-FPM

Для работы с современными веб-приложениями вам потребуется поддержка популярного скриптового языка PHP, Nginx поддерживает работу через FastCGI, но не имеет собственного менеджера процессов, поэтому мы будем использовать для этой цели PHP-FPM.

Важно! В современных дистрибутивах используется более новая версия PHP 7, чтобы работать с новой версией языка вместо **php5** в приведенных ниже командах следует указывать **php7.x** или просто **php** например, вместо **php5-imagick** нужно набрать **php7.0-imagick** или **php-imagick.**

Установим его:

```
apt-get install php5-fpm
```

Все необходимые пакеты и интерпретатор PHP будут установлены по зависимостям. Также имеет смысл сразу установить некоторые модули PHP, например, для работы с графикой:

```
apt-get install php5-gd php5-imagick
```

Настройки PHP-FPM по умолчанию достаточно оптимальны и никаких вмешательств в них не требуется, однако следует подправить некоторые опции PHP, для этого откроем **/etc/php5/fpm/php.ini** и найдем там следующие опции:

```
post_max_size = 8M
```

этот параметр задает максимальный размер данных загружаемых методом POST, влияет, например, на размер загружаемых средствами PHP файлов. По умолчанию 8 МБ, можем изменить по собственным потребностям.

Если вы будете использовать PHP-приложения (CMS) работающие в кодировке отличной от UTF-8, то приведите к следующему виду опцию:

```
default_charset = ""
```

Затем раскоменнтируйте и установите опцию:

```
cgi.fix_pathinfo=0
```

Это закроет возможную уязвимость в PHP.

Еще ниже надо найти и увеличить размер максимально загружаемого файла:

```
upload_max_filesize = 8M
```

Данное значение должно быть больше или равно значению **post_max_size**, иначе вы будете ограничены в загрузке файлов меньшим из указанных в этих опциях размером.

Сохраним изменения и перезапустим PHP-FPM:

```
service php5-fpm restart
```

Теперь следует научить Nginx работать с PHP-FPM, для этого в файл конфигурации виртуального хоста нужно добавить настройки, которые будут перенаправлять (проксировать) все запросы к динамическому содержимому на FastCGI-шлюз.

Если сайтов несколько, то аналогичные настройки потребуется добавить каждому виртуальному хосту, поэтому, чтобы не делать лишних действий, имеет смысл вынести данные настройки в шаблон и подключать к виртуальному хосту уже его. Такой подход имеет еще один плюс, если вам потребуется изменить настройки, то делать это придется только в одном месте.

Создадим директорию для хранения шаблонов:

```
mkdir /etc/nginx/templates
```

После чего создадим в ней шаблон для работы с PHP-FPM:

```
touch /etc/nginx/templates/php-fpm.conf
```

Откроем его и добавим следующий текст:

```
location ~ \.php$ {
  try_files $uri =404;
  fastcgi_pass unix:/var/run/php5-fpm.sock;
  fastcgi_index index.php;
  include fastcgi_params;
  fastcgi_param  SCRIPT_FILENAME  $document_root$fastcgi_script_name;
}
```

Указанный нами блок **location** будет обрабатывать все запросы к php-файлам, первая директива в нем проверяет наличие запрошенного файла, в противном случае отдавая ошибку 404. Вторая устанавливает параметры соединения с FastCGI-шлюзом, в нашем случае с PHP-FPM, соединение устанавливается через UNIX-сокет, как наиболее производительный способ соединения. Затем указывается индексный файл и подгружаются настройки Nginx для FastCGI.

Важно! Обратите внимание, что PHP 7 имеет иной путь к UNIX-сокету, поэтому следует указывать **/var/run/php/php7.0-fpm.sock**

В принципе этого уже достаточно, чтобы работать с динамическим содержимым, но не будем спешить и добавим в файл еще несколько блоков.

```
location ~ /\.ht {
  deny all;
}
```

Несмотря на то, что Nginx не использует htaccess-файлы, они, вместе с файлами htpasswd могут находиться в директории сайта, особенно если до этого он работал на Apache и будет правильно запретить доступ к ним в целях безопасности.

Также следует настроить кэширование статического содержимого:

```
location ~*
\.(gif|jpeg|jpg|txt|png|tif|tiff|ico|jng|bmp|doc|pdf|rtf|xls|ppt|rar|rpm|swf|zip|bin|exe|dll|deb|cur)$ {
  expires 168h;
}
```

Данная конструкция включает кэширование на стороне браузера, сообщая тому, что "срок годности" указанных файлов - 168 часов (1 неделя) и при последующих обращениях на ваш сайт данные файлы следует брать из локального кэша. Мы привели примерный список, вы можете самостоятельно добавить в него нужные расширения файлов.

Также зададим кэширование для скриптов и стилей:

```
location ~* \.(css|js)$ {
  expires 180m;
}
```

Для них установим срок кэширования в 3 часа, что позволит соблюсти баланс между скоростью применения возможных изменений в этих файлах и уменьшением количества запросов к вашему сайту.

Теперь откроем файл конфигурации виртуального хоста и в конце первой секции **server** добавим строку подключения шаблона:

```
include /etc/nginx/templates/php-fpm.conf;
```

Сохраним все настройки, проверим конфигурацию и перезапустим Nginx.

```
nginx -t
service nginx reload
```

Чтобы проверить работу PHP создадим в корневой директории сайта файл **test.php** со следующим содержимым:

```
<?php
phpinfo();
?>
```

Теперь, если обратиться к данному файлу через браузер вы должны увидеть стандартную страницу с информацией о PHP.

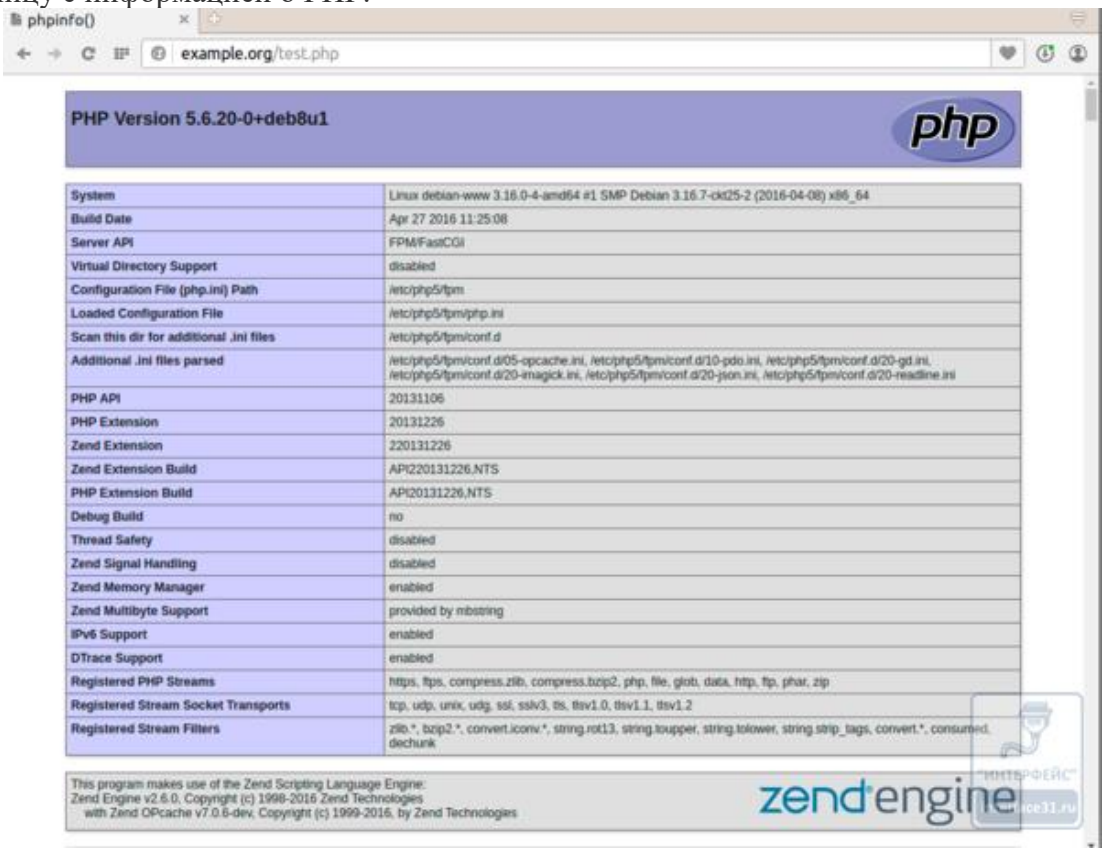


Рис. 241

3. Установка MySQL и phpMyAdmin

СУБД MySQL широко используется для хранения информации в современных веб-приложениях. Это один из самых важных компонентов веб-сервера, так как в базе данных обычно хранится вся информация сайта, кроме статического содержимого (изображений, файлов и т.п.).

Для установки MySQL выполните:

```
apt-get install mysql-server php5-mysql
```

Важно! В свежих выпусках Debian (и его производных) вместо пакета **mysql-server** следует установить **mariadb-server**, который полностью совместим с MySQL.

Данная команда установит MySQL сервер и модуль PHP для работы с ним. В процессе установки вас попросят ввести пароль суперпользователя СУБД (root), не путать с суперпользователем системы.

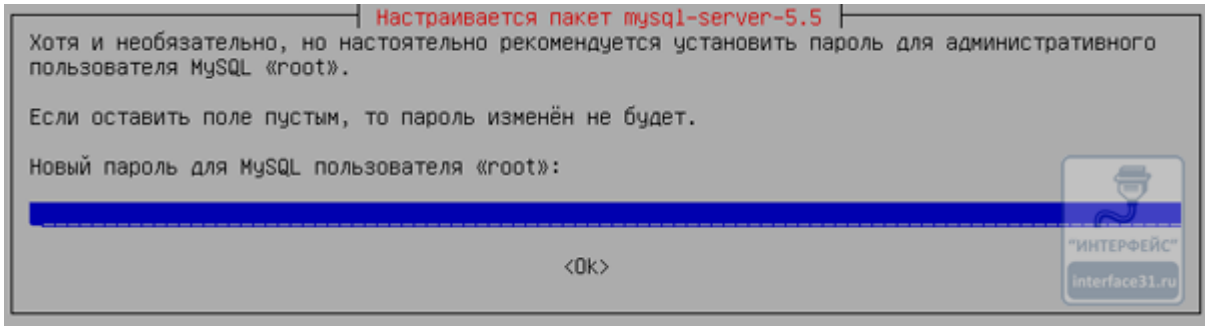


Рис. 242

Для повседневной работы с MySQL удобно использовать веб-приложение администрирования phpMyAdmin, установим его:

```
apt-get install phpmyadmin
```

Установщик phpMyAdmin не умеет конфигурировать Nginx для работы с ним, поэтому ничего не выбираем на данном этапе, а все настройки выполним позже вручную.

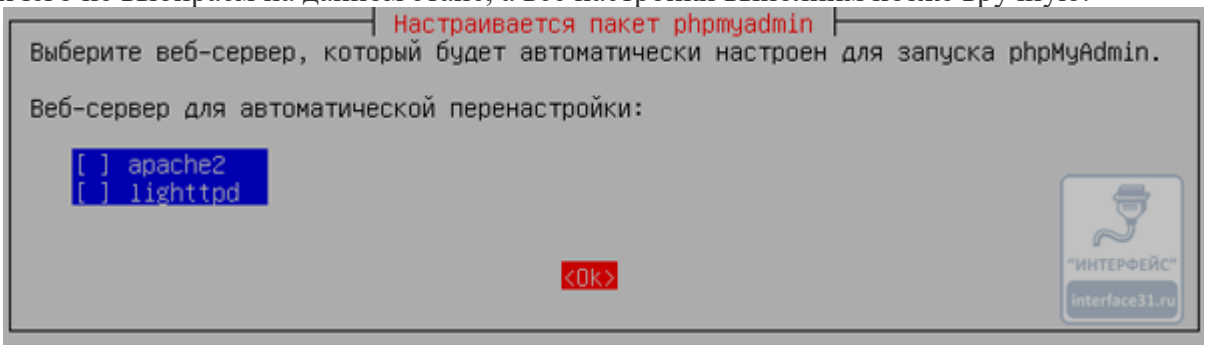


Рис. 243

Для этого создадим еще один файл шаблона:

```
touch /etc/nginx/templates/phpmyadmin.conf
```

и внесем в него следующий текст:

```
location /phpmyadmin {
  root /usr/share/;
  index index.php;

  location ~ ^/phpmyadmin/(.+\.php)$ {
    try_files $uri =404;
    root /usr/share/;
    fastcgi_pass unix:/var/run/php5-fpm.sock;
    fastcgi_index index.php;
    include fastcgi_params;
    fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
  }

  location ~* ^/phpmyadmin/(.+\.(jpg|jpeg|gif|css|png|js|ico|html|xml|txt))$ {
    root /usr/share/;
    expires 1M;
  }
}

location /phpMyAdmin {
  rewrite ^/* /phpmyadmin last;
 }
```

На первый взгляд синтаксис может показаться довольно сложным, но если разобрать правила по частям, то мы увидим, что ничего сложного нет. Все это мы уже обсуждали выше.

Самый последний **location** осуществляет перенаправление на phpMyAdmin с адресов вида **имя_домена/phpmyadmin**.

Для подключения phpMyAdmin к сайту в описание виртуального хоста добавьте включение еще одного шаблона:

```
include /etc/nginx/templates/phpmyadmin.conf;
```

Проверьте конфигурацию и перезапустите Nginx, после чего наберите в браузере имя вашего сайта, добавив после него **/phpmyadmin**, если все сделано правильно, то вы попадете в админ-панель приложения.

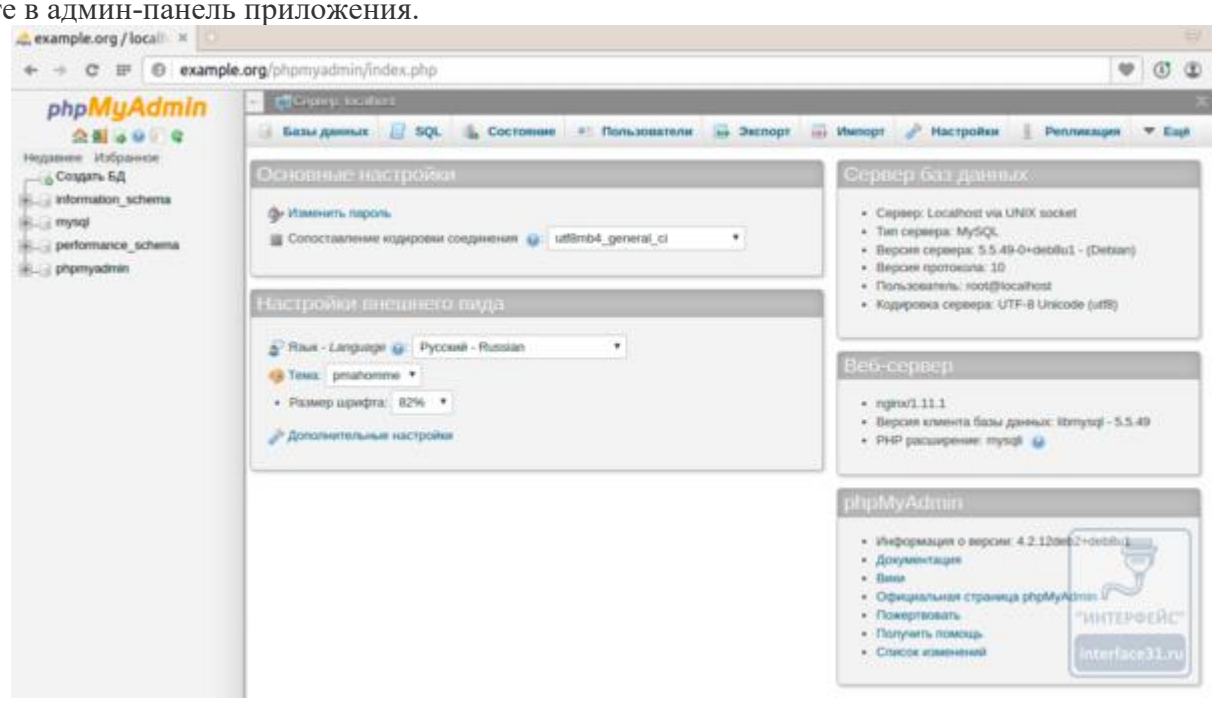


Рис. 244

Для ее устранения выполните:

```
ln -s /etc/php5/mods-available/mcrypt.ini /etc/php5/fpm/conf.d/
service php5-fpm restart
```

На этом настройку нашего сервера можно считать законченной. При переносе или размещении на нем новых сайтов не забывайте правильно устанавливать права и владельца. Стандартный набор прав: 644 для файлов и 755 для папок, его можно быстро установить командой:

```
chmod -R u=rw,g=r,o=r,a+X /var/www/example.org
```

Но учтите, что некоторые CMS требуют нестандартных прав на некоторые папки и файлы, поэтому уточните этот вопрос в документации.

Также не забывайте устанавливать правильного владельца, им должен быть пользователь, от имени которого работает веб-сервер, в нашем случае **www-data**, владелец устанавливается командой:

```
chown -R www-data:www-data /var/www/example.org
```

Обычно данных мер достаточно, но встречаются CMS которые требуют дополнительной настройки для работы с Nginx, в этом случае следует обратиться к документации или на форум поддержки движка. Поэтому мы еще раз повторимся, что данное решение требует определенного опыта и квалификации и не рекомендуется начинающим, а также тем, кто не хочет возиться с настройками, а хочет быстро получить работающий сайт.

Сделайте скриншоты (фотографии) процесса установки и настройки веб-сервера на базе Nginx + PHP-FPM и вставьте в отчёт.

Практическая работа № 16 «Настройка сервера DNS в ОС Debian

Задание:

Одной из реализацией в Linux DNS серверов является BIND. Текущая реализация это BIND9. Все настроечные файлы находятся в каталоге /etc/bind/. Основной файл конфигурации - named.conf. Установим и настроим сервер DNS BIND9 на основе операционной системы Debian.

1. Для начала откроем терминал. Все действия по установке и настройке DNS сервера производятся с правами root или с помощью sudo.

Прописываем необходимые репозитории для обновления системы, а также установки нужных пакетов:

```
# nano /etc/apt/sources.list

# security updates
deb http://security.debian.org/ jessie/updates main contrib non-free
deb-src http://security.debian.org/ jessie/updates main contrib non-free
# binary and source packages
deb http://ftp.ru.debian.org/debian/ jessie main contrib non-free
deb-src http://ftp.ru.debian.org/debian/ jessie main contrib non-free
# jessie-updates
deb http://ftp.ru.debian.org/debian/ jessie-updates main contrib non-free
deb-src http://ftp.ru.debian.org/debian/ jessie-updates main contrib non-free
```

Для **Debian 9** вместо **jessie** указываем **stretch**.

Сохраняем файл, далее выполняем следующие команды:

```
# apt-get update
# apt-get upgrade
```

Первая команда обновит информацию о пакетах, вторая команда приведет к обновлению нашей системы до актуального состояния.

Устанавливаем пакет **bind9** (dns сервер):

```
# apt-get install bind9
```

Директория, в которой находятся настроечные файлы dns сервера - **/etc/bind/**. Основным настроечным файлом является **named.conf.options**. Настраиваем файл **named.conf.options** (находится в каталоге **/etc/bind**):

```
# cd /etc/bind
# nano named.conf.options
```

Прописываем в файле **named.conf.options**:

```
acl mynetwork { 192.168.91.0/24 ; 127.0.0.1; };
options {
    directory "/var/cache/bind";
    forwarders {
        8.8.8.8;
};
listen-on {
```

```
        192.168.91.10;
        192.168.91.20;
};
dnssec-validation auto;
auth-nxdomain no;    # conform to RFC1035
listen-on-v6 { none; };
allow-query { mynetwork; };
```

Где:
allow-query { mynetwork; }; - список тех, кто имеет право запрашивать информацию, если хотите, чтобы принимать запросы ото всех, вместо **mynetwork** ставим **any**.
acl - ограничивает адреса, которые могут запрашивать зоны с сервера DNS.
forwarders { 8.8.8.8; }; - прописываем DNS сервера, у которого можно получить информацию, если информация о доменах неизвестна нашему серверу.
listen on { 192.168.91.10; 192.168.91.20; }; - прописываем DNS сервера, которые будут использованы для отображения IP адресов в имена и наоборот.
listen-on-v6 { none; }; - если IP 6 версии не используем.
auth-nxdomain no; - параметр для совместимости с RFC1035.
Проверяем:

```
# named-checkconf
```

Далее редактируем файл named.conf.local:

```
# nano /etc/bind/named.conf.local
```

В файле прописываем зону прямого и обратного просмотра для домена. Зона прямого просмотра - тип зоны, в котором в ответ на имя получают IP адрес. Соответственно ответственность зоны обратного просмотра состоит в том, чтобы получить по IP адресу имя компьютера:

```
zone "sigro.ru" {
        type master;
        file "/etc/bind/db.sigro.ru";
};

zone "91.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/91.168.192.in-addr.arpa.zone";
};
```

91.168.192.in-addr.arpa - обратная зона просмотра, берётся из IP адреса DNS сервера (в данном случае 192.168.91.10);
db.sigro.ru - прямая зона просмотра, домен в данном случае называется sigro.ru.
После каждого изменения конфигурационного файла желательно провести проверку синтаксиса файла, затем переходить к настройке других файлов. Делается это командой:

```
# named-checkconf
```

Далее начинаем прописывать зону прямого просмотра. Чтобы произвести настройку быстрее и по шаблону, копируем фал db.local и изменяем уже вновь созданный файл

настройки зоны прямого просмотра (имена для файлов зоны прямого и обратного просмотра можно придумать любые, но принято, чтобы они были читабельны):

```
# cp db.local db.sigro.ru
# nano db.sigro.ru
;
; BIND data file for local loopback interface
;
$TTL 604800
$ORIGIN sigro.ru.

@       IN      SOA       nic1              admin (
                        2017060100                ; Serial
                         604800                   ; Refresh
                          86400                   ; Retry
                         2419200                  ; Expire
                           604800 )               ; Negative Cache TTL
;
@       IN      NS       nic1.sigro.ru.
@       IN      A        192.168.91.10
; @     IN      AAAA   ::1
nic1    IN      A        192.168.91.10
nic2    IN      A        192.168.91.20
cl1     IN      A         192.168.91.101
```

; - после данного знака возможно делать комментарий
$TTL 604800 - time to live (время кэширования из вашей зоны)
$ORIGIN sigro.ru. - при использовании $ORIGIN к именам будет автоматически дописываться в данном случае sigro.ru. (не забываем в конце точку). Например, при считывании зоны прямого просмотра, вместо nic1 автоматически будет подставлено nic1.sigro.ru.
@ IN SOA nic1 admin - запись SOA (начало ответственности)
nic1 - имя первичного dns сервера
admin - почтовый адрес пользователя, отвечающего за эту зону
2017060100 - серийный номер зоны (десятизначное число)
604800 - период обновления
86400 - повтор каждые 86400 с
2419200 - время хранения информации
604800 - время хранения в кэше удаленных серверов негативных ответов
Прописываем зону обратного просмотра. Для этого создаём файл зоны обратного просмотра и производим изменения в вновь созданном файле:

```
# cp db.sigro.ru 91.168.192.in-addr.arpa.zone
# nano 91.168.192.in-addr.arpa.zone
;
; BIND data file for local loopback interface
;
$TTL 604800
$ORIGIN 91.168.192.in-addr.arpa.

@       IN      SOA     nic1.sigro.ru.            admin.sigro.ru. (
                        2017060100                ; Serial
```

```
                        604800          ; Refresh
                         86400          ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
            NS      nic1.sigro.ru.
10          PTR     nic1.sigro.ru.
20          PTR     nic2.sigro.ru.
101         PTR     cl1.sigro.ru.
```

Делаем так, чтобы сервер DNS работал с новой конфигурацией:

```
# /etc/init.d/bind9 reload
```

Производим проверки:

```
# named-checkconf
# named-checkconf -z
# named-checkzone 91.168.192.in-addr.arpa 91.168.192.in-addr.arpa.zone
# host 192.168.91.10
# nslookup sigro.ru
# nslookup 192.168.91.10
```

named-checkconf - проверка правильности синтаксиса конфигурационных файлов, рекомендуется делать после каждого изменения в конфигурационном файле.
named-checkconf -z - пытается произвести действия, такие же как **bind** при загрузке зон.
nslookup sigro.ru - должен быть показан адрес проверяемого сервера (т.е. в данном случае **Address: 192.168.91.10**).
nslookup 192.168.91.10 - должен быть показано имя проверяемого сервера (т.е. в данном случае **name = nic1.sigro.ru**).
Если ошибок нет, то сервер DNS сконфигурирован правильно

Сделайте скриншоты (фотографии) процесса настройки сервера времени и лицензирования и вставьте в отчёт.

2.17. Практическая работа № 17 «Настройка сервера DHCP в ОС Debian»

Задание:

Рассмотрим, как установить и настроить DHCP-сервер.

1. Установка сервера ISC DHCP

Установим пакет.

```
sudo apt install isc-dhcp-server
```

На всякий случай сделаем резервную копию конфигурационного файла

```
cp /etc/dhcp/dhcpd.conf{,.backup}
```

```
cat /dev/null > /etc/dhcp/dhcpd.conf
```

2. Настройка DHCP

Задаем настройки сети, диапазон выдаваемых адресов, маску сети и выдаваемый DNS

```
nano /etc/dhcp/dhcpd.conf
subnet 192.168.38.0 netmask 255.255.255.0 {
 range 192.168.38.100 192.168.38.254;
 option subnet-mask 255.255.255.0;
 option broadcast-address 192.168.38.255;
 option domain-name-servers 8.8.8.8, 8.8.4.4;
 option domain-name "workgroup";
 option routers 192.168.38.1;
 default-lease-time 7200;
 max-lease-time 480000;
 }
```

Все строки параметров в файле конфигурации dhcp заканчиваются точкой с запятой (;). Некоторые параметры могут иметь не одно значение, например, domain-name-servers, у которого два IP-адреса, разделенные запятой. Строки, начинающиеся с '#', являются комментариями и не обрабатываются сервером dhcp.

Некоторые общие параметры сервера DHCP:

subnet— Параметр объявляет подсеть (в нашем случае 192.168.38.0 с маской 255.255.255.0)

range – Диапазон выдаваемых адресов (от 192.168.38.100 до 192.168.38.254).

option subnet-mask – Маска сети. (255.255.255.0)

option broadcast-address – Широковещательный адрес. (192.168.38.255)

domain-name-servers – Адреса серверов DNS. (8.8.8.8, 8.8.4.4)

option domain-name – Доменное имя.(workgroup)

option routers – Определяет IP-адрес вашего шлюза или точки выхода в сеть. (192.168.38.1)

После того как вы отредактировали основной файл конфигурации и объявили диапазоны IP, откройте файл **/etc/default/isc-dhcp-server** и замените параметр ***INTERFACESv4*** на имя сетевого интерфейса, который смотрит внутрь сети. Чтобы узнать его имя воспользуйтесь командами ipconfig или **ip.**

```
INTERFACESv4 = "enp1s8"
```

```
 GNU nano 2.5.3        Файл: /etc/default/isc-dhcp-server

# Defaults for isc-dhcp-server initscript
# sourced by /etc/init.d/isc-dhcp-server
# installed at /etc/default/isc-dhcp-server by the maintainer scripts

#
# This is a POSIX shell fragment
#

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPD_CONF=/etc/dhcp/dhcpd.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPD_PID=/var/run/dhcpd.pid

# Additional options to start dhcpd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACES="enp1s8"
```

Рис. 245

Наконец, после внесения всех изменений перезапустите сервер dhcp, чтобы применить новую конфигурацию и проверить статус службы, выполнив следующие команды:

```
systemctl restart isc-dhcp-server
systemctl status isc-dhcp-server
```

```
● isc-dhcp-server.service - ISC DHCP IPv4 server
   Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: enabled)
   Active: active (running) since Чт 2017-09-07 09:55:31 MSK; 1 weeks 5 days ago
     Docs: man:dhcpd(8)
 Main PID: 1067 (dhcpd)
    Tasks: 1
   Memory: 8.2M
      CPU: 90ms
   CGroup: /system.slice/isc-dhcp-server.service
           └─1067 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -cf /etc/dhcp/dhcpd.conf enp1s8

сен 18 10:05:26 router-zvezd dhcpd[1067]: DHCPACK on 192.168.38.224 to c0:3f:d5:6c:aa:97 via enp1s8
сен 18 15:29:34 router-zvezd dhcpd[1067]: reuse_lease: lease age 105514 (secs) under 25% threshold, reply with unaltered, existin
сен 18 15:29:34 router-zvezd dhcpd[1067]: DHCPREQUEST for 192.168.38.224 from c0:3f:d5:6c:aa:97 via enp1s8
сен 18 15:29:34 router-zvezd dhcpd[1067]: DHCPACK on 192.168.38.224 to c0:3f:d5:6c:aa:97 via enp1s8
сен 18 17:46:08 router-zvezd dhcpd[1067]: reuse_lease: lease age 113708 (secs) under 25% threshold, reply with unaltered, existin
сен 18 17:46:08 router-zvezd dhcpd[1067]: DHCPREQUEST for 192.168.38.224 from c0:3f:d5:6c:aa:97 via enp1s8
сен 18 17:46:08 router-zvezd dhcpd[1067]: DHCPACK on 192.168.38.224 to c0:3f:d5:6c:aa:97 via enp1s8
сен 19 10:02:54 router-zvezd dhcpd[1067]: Wrote 5 leases to leases file.
сен 19 10:02:54 router-zvezd dhcpd[1067]: DHCPREQUEST for 192.168.38.224 from c0:3f:d5:6c:aa:97 via enp1s8
сен 19 10:02:54 router-zvezd dhcpd[1067]: DHCPACK on 192.168.38.224 to c0:3f:d5:6c:aa:97 (D-002459) via enp1s8
~
~
~
```

Рис. 246

3. Настройка DHCP-сервера с резервированием IP-адреса.

Часто возникает необходимость зарезервировать за устройством (сервером, принтером и т.д.) постоянный IP-адрес. В этом случае вам нужно знать его MAC- адрес.

```
nano /etc/dhcp/dhcpd.conf
```

Пример резервирования IP-адреса 192.168.38.5 за компьютером SERVER:

```
subnet 192.168.38.0 netmask 255.255.255.0 {
range 192.168.38.100….
.....
host SERVER {
```

```
  hardware ethernet 08:60:6e:d6:5e:ff;
  fixed-address 192.168.38.5;}
}
```

После того, как вы внесли изменения в конфигурационный файл, перезапустите сервер DHCP следующей командой:

```
systemctl restart isc-dhcp-server
```

Вы успешно установили и настроили DHCP-сервер.
Сделайте скриншоты (фотографии) процесса настройки сервера DHCP и вставьте в отчёт.

2.18. Практическая работа № 18 «Настройка файловых серверов в ОС Debian»

Задание:

1. Подготовка системы

Необходимо использовать виртуальную машину с двумя жесткими дисками, один для системы, второй для данных, точку монтирования диска для данных мы указали как **/samba**.

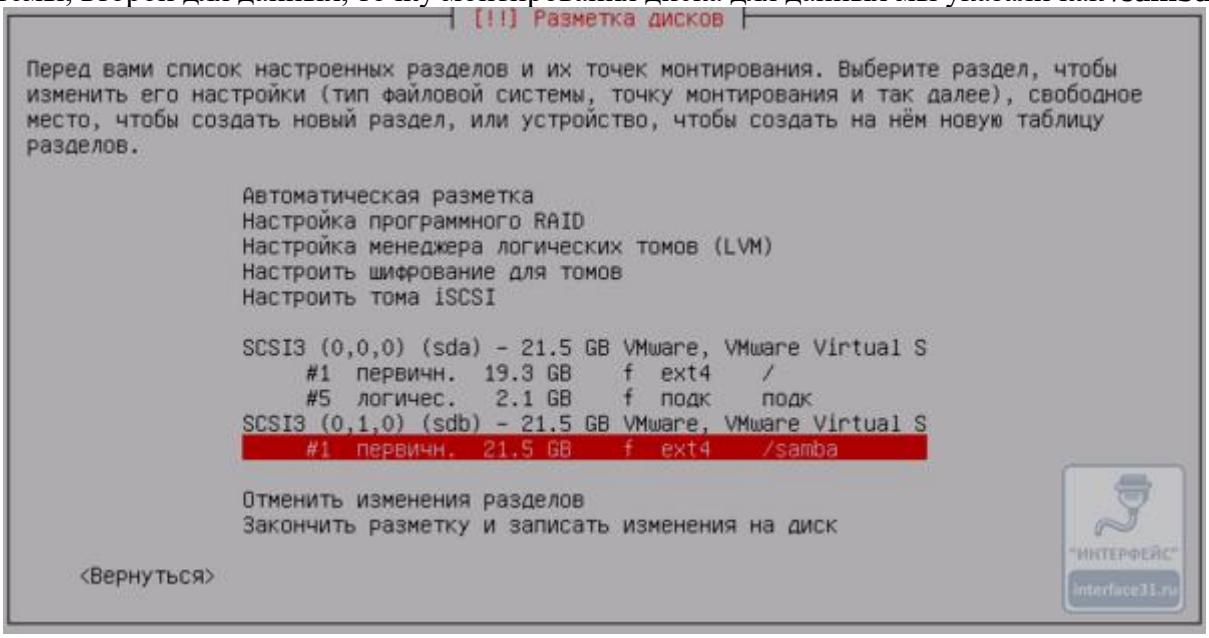


Рис. 247

Также обратите внимание на имя компьютера, Samba 4 будет использовать его в качестве NetBIOS имени.

После установки ОС следует изменить настройку лимита на количество одновременно открытых файлов, в Linux это 1024, а в Windows 16384. Для этого откройте файл **/etc/security/limits.conf** и добавьте в конце две строки:

```
*       -   nofile 16384
root    -   nofile 16384
```

После чего сервер следует перезагрузить.

2. Установка и базовая настройка Samba 4

Установка Samba предельно проста:

```
apt install samba
```

После чего откроем файл **/etc/samba/smb.conf** и выполним общие настройки. Большинство указанных опций в файле уже есть, многие из них даже не потребуется менять, но их назначение будет полезно знать, поэтому мы прокомментируем наиболее важные из них.

За общие настройки сервера отвечает секция **[global]**, которая, кстати, прекрасно прокомментирована. Обратите внимание на два вида комментариев опций, если для этого используется символ **#** - то указанное значение применяется по умолчанию, а символ **;** обозначает предлагаемый вариант настройки.

Начнем, опции перечисляются в порядке их следования в файле:

```
workgroup = WORKGROUP
```

Обозначает рабочую группу Windows, по умолчанию WORKGROUP.

```
;  interfaces = 127.0.0.0/8 eth0
```

Предлагаемая опция, которые определяет интерфейсы или подсети, с которыми будет работать Samba. Допускается смешанная запись, как в примере выше, либо можно указать только интерфейсы:

```
interfaces = lo ens33
```

Или только подсети:

```
interfaces = 127.0.0.0/8 192.168.38.0/24
```

Но само по себе указание интерфейсов не ограничивает Samba, для того чтобы ограничения начали действовать нужно включить следующую опцию:

```
bind interfaces only = yes
```

Следующая опция указывает расположение логов:

```
 log file = /var/log/samba/log.%m
```

По умолчанию лог выключен, для того чтобы его включить добавьте в файл опцию:

```
log level = 1
```

Если вам нужен более подробный лог - установите более высокий уровень, минимальное значение - 1, максимальное - 5.

Также закомментируйте опцию:

```
# syslog = 0
```

В настоящий момент она является не рекомендованной (deprecated).

```
server role = standalone server
```

Обозначает простой файловый сервер, не требующий подключения к домену.

```
map to guest = bad user
```

Определяет способ определения гостевого доступа, при указанном значении гостем будет считаться любой пользователь, который отсутствует в базе Samba. Также могут использоваться значения **never** - не использовать гостевой доступ и **bad password** - в этом случае гостем будет считаться в том числе, и существующий пользователь если он неправильно введет пароль. Данное значение использовать не рекомендуется, так как при ошибке в пароле пользователь все равно получит доступ, но с гостевыми правами.

На этом общая настройка сервера закончена. Проверим конфигурацию на ошибки:

```
testparm
```

И перезапустим сервер

```
service smbd restart
```

Настройка общего ресурса с гостевым доступом

Начнем с самого простого варианта - создадим общий ресурс, доступ к которому может иметь любой пользователь. Для этого добавим в конец файла **/etc/samba/smb.conf** следующие строки.

```
[public]
comment = Shared for all
path = /samba/public
read only = no
guest ok = yes
```

В квадратных скобках задаем имя ресурса, все что ниже скобок - секция этого ресурса. В ней мы указали следующие опции:

- **comment** - описание ресурса, необязательный параметр;
- **path** - путь к директории;
- **read only** - режим только чтения, указываем **no**;
- **guest ok** - разрешен ли гостевой доступ, указываем **yes**;

Теперь создадим саму директорию:

```
mkdir /samba/public
```

и установим на нее необходимые права, для гостевого ресурса это 777:

```
chmod 777 /samba/public
```

Перезапускаем Samba и пробуем получить доступ с любого Windows-клиента.

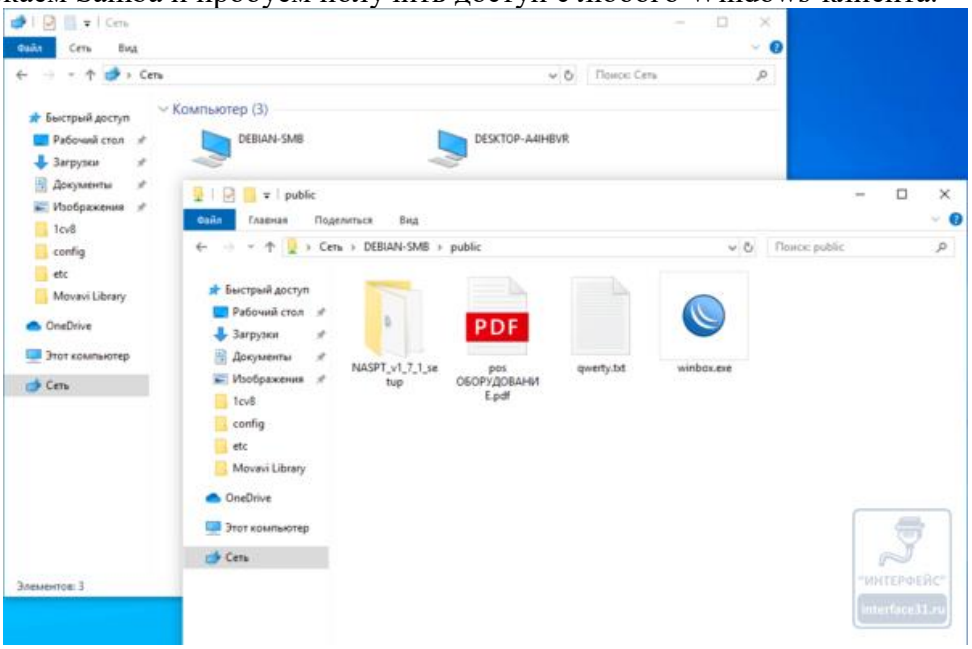


Рис. 248

Если все сделано правильно, то сервер появится в сетевом окружении, и вы без проблем получите доступ к созданной нами общей папке.

3. Настройка общего ресурса с парольным доступом

Гостевой доступ — это просто и удобно, но не всегда приемлемо. Существуют ситуации, когда доступ к общему ресурсу должны иметь только определенные пользователи. В нашем примере создадим два таких ресурса: для бухгалтерии и для IT-отдела.

Снова откроем конфигурационный файл и добавим в него две секции:

```
[buch]
path = /samba/buch
read only = no
guest ok = no
[adm]
path = /samba/adm
read only = no
guest ok = no
```

Они предельно просты и отличаются запретом гостевого доступа - **guest ok = no**. Для того, чтобы разделить доступ к ресурсам будем использовать группы пользователей, создадим две новые группы для наших подразделений:

```
groupadd smbbuch
groupadd smbadm
```

Теперь создадим каталоги:

```
mkdir /samba/buch
```

```
mkdir /samba/adm
```
и изменим группу владельца:
```
chgrp smbbuch /samba/buch
chgrp smbadm /samba/adm
```
Затем установим права:
```
chmod 2770  /samba/buch
chmod 2770 /samba/adm
```
Значение 2770 обозначает что мы предоставляем полные права владельцу и группе, для остальных доступ запрещен. А первая двойка устанавливает SGID для каталога, что обеспечивает присвоение группы каталога каждому создаваемому в нем файлу.

В некоторых случаях определенный интерес представляет выставление дял каталога **sticky bit**, который означает, что удалить или переименовать файл может только его владелец, но работать с ним, в том числе изменять, может любой пользователь, имеющий права записи в каталог. Для этого вместо набора прав **2770** используйте права **3770**.

На этом настройки закончены, не забываем перезапустить Samba. Но в наших группах пока нет пользователей, давайте добавим их туда.

Начнем с уже существующих пользователей, в нашем случае это пользователь andrey, который является главным администратором и должен иметь доступ к обоим ресурсам. Поэтому добавим его в обе группы:
```
usermod -aG smbbuch andrey
usermod -aG smbadm andrey
```
Затем добавим его в базу Samba:
```
smbpasswd -a andrey
```
При этом потребуется установить пароль для доступа к Samba-ресурсам, он должен совпадать с основным паролем пользователя. После чего включим эту учетную запись:
```
smbpasswd -e andrey
```
Проверяем, после ввода пароля мы должны получить доступ к созданным нам ресурсам. Также обратите внимание, после аутентификации в списке общих ресурсов появилась папка с именем пользователя, подключенная только на чтение.

Рис. 249

С настройками по умолчанию Samba предоставляет каждому существующему пользователю доступ только на чтение к его домашнему каталогу. На наш взгляд это довольно удобно и безопасно. Если вас не устраивает такое поведение - удалите из конфигурационного файла секцию **[homes]**.

Теперь о других пользователях. Скажем у нас есть бухгалтер Иванова и админ Петров, каждый из которых должен иметь доступ к своему ресурсу. В тоже время иметь доступ к самому Samba-серверу им необязательно, поэтому создадим новых пользователей следующей командой:
```
useradd -M -s /sbin/nologin ivanova
useradd -M -s /sbin/nologin petrov
```
Ключ **-M** заводит пользователя без создания домашнего каталога, а **-s /sbin/nologin** исключает возможность входа такого пользователя в систему.

Поместим каждого в свою группу:
```
usermod -aG smbbuch ivanova
```

```
usermod -aG smbadm petrov
```
Затем добавим их в базу Samba, при этом потребуется установить им пароли:
```
smbpasswd -a ivanova
smbpasswd -a petrov
```
И включим эти учетные записи
```
smbpasswd -e ivanova
smbpasswd -e petrov
```
Если все сделано правильно, то пользователь будет иметь доступ к своим ресурсам и не иметь к чужим.

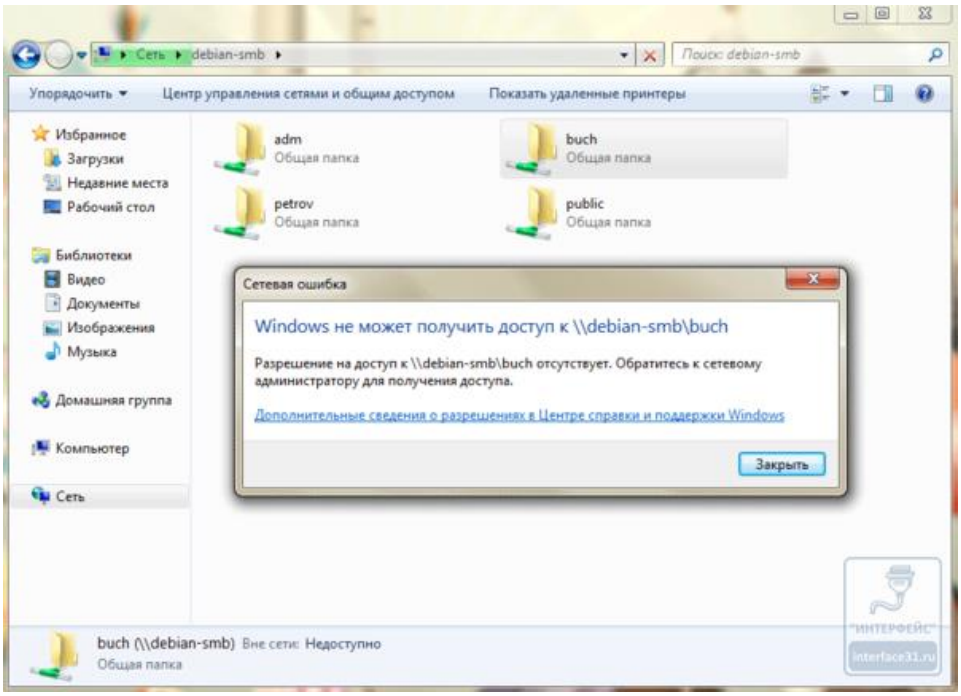


Рис. 250

Также обратите внимание, что несмотря на то, что общий ресурс с именем пользователя создан, доступ он к нему получить не сможет, так как физически его домашняя директория не существует.

4. Настройка корзины для общего ресурса

Полезность корзины на файловом сервере, пожалуй, не будет отрицать никто. Человеку свойственно ошибаться и будет очень обидно, если ценой ошибки окажется несколько часов работы, но, к счастью Samba позволяет помещать удаленные файлы в корзину.

Для активации корзины добавьте в секцию к общему ресурсу следующие строки:
```
vfs objects = recycle
recycle:repository = .recycle
recycle:versions = yes
recycle:keeptree = yes
```
Первая опция добавит в общий ресурс новый объект - корзину, вторая укажет ее расположение - скрытая папка в корне. Две следующих включают сохранение структуры папок при удалении и сохранение нескольких версий файла с одним и тем же именем. Это нужно в тех случаях, когда разные пользователи удалят разные файлы с одним и тем же именем.

Перезапустим Samba и попробуем что-нибудь удалить.

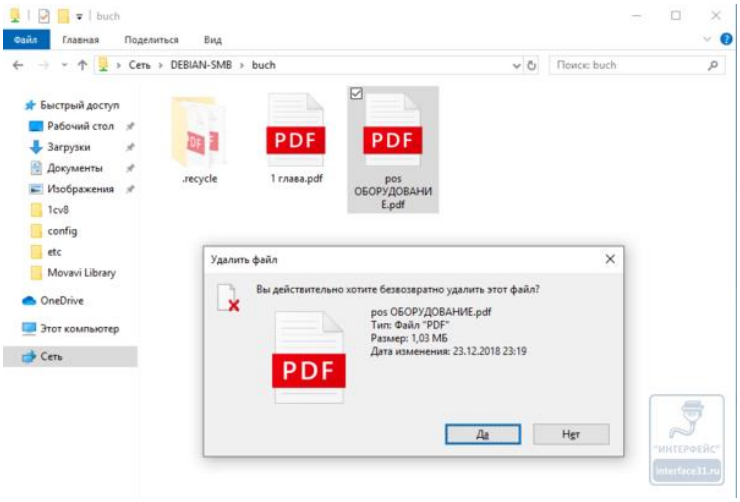


Рис. 251

Несмотря на грозное предупреждение Проводника удаляемые файлы перемещаются в корзину, откуда мы их можем восстановить.

Как видим, работать с Samba не просто, а очень просто.

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

2.19. Практическая работа № 19 «Настройка контейнеров Docker»

Задание:

1. Установка Docker

Для установки обновим индекс пакетов и установим необходимые зависимости:
root@dedicated:~# sudo apt update
root@dedicated:~# sudo apt install apt-transport-https ca-certificates curl gnupg2 software-properties-common

Подключим репозиторий Docker, предварительно добавив GPG-ключ, и обновим индексы:
root@dedicated:~# curl -fsSL https://download.docker.com/linux/debian/gpg | sudo apt-key add -
root@dedicated:~# sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/debian $(lsb_release -cs) stable"
root@dedicated:~# sudo apt update

По умолчанию, вы сейчас подключены в репозиторий Debian, для дальнейшей установки необходимо переключиться в репозиторий Docker с помощью команды:
root@dedicated:~#apt-cache policy docker-ce

В терминале вы должны увидеть следующее:

После чего можно приступить к установке Docker:
root@dedicated:~# sudo apt install docker-ce

По окончании установки, добавьте его в автозагрузку и проверьте статус:
root@dedicated:~#sudo systemctl enable docker
root@dedicated:~# sudo systemctl status docker

В окне терминала мы должны увидеть следующее:

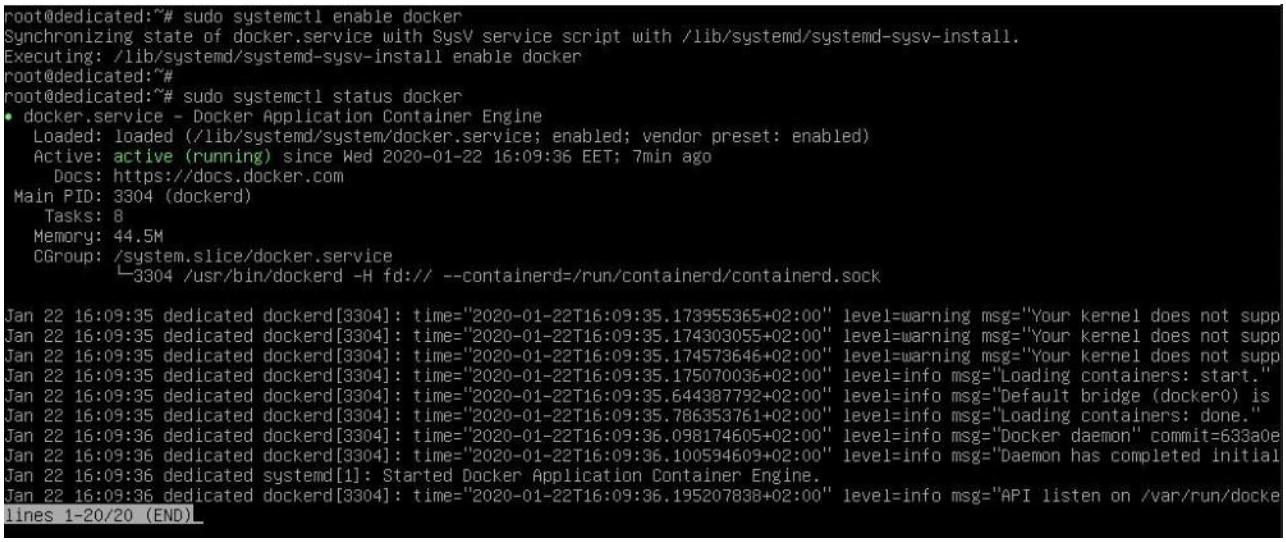


Рис. 252

На этом установка Docker завершена, и мы можем приступить к созданию и управлению контейнерами.

2.Команда Docker

Управление контейнерами осуществляется с помощью команды «docker», она имеет следующую структуру:
root@dedicated:~# docker [OPTIONS] COMMAND

Чтобы посмотреть полный список команд введите:
root@dedicated:~# docker

Мы увидим полный список команд в рассматриваемой версии Docker 19.03.5. Для примера, возьмем первую команду по списку («attach») и посмотрим более полную информацию о ней, доступные опции и аргументы:
root@dedicated:~# docker attach --help

Обратите внимание, без 'sudo', команды docker выполняются исключительно под пользователем root. Если в системе присутствуют другие учетные записи, которые работают с docker, не забываем про приставку 'sudo' к командам. Если Вы хотите работать с docker под другим пользователям, не используя постоянно 'sudo', необходимо создать группу docker, если она отсутствует, и добавить в неё нужного пользователя.
root@dedicated:~# sudo groupadd docker
root@dedicated:~# sudo gpasswd -a ${USER} docker
root@dedicated:~# sudo service docker restart
где *${USER}* - имя вашего пользователя. Так же добавьте пользователя в sudoers.

3.Образы контейнеров и управление контейнерами

По умолчанию, все доступные образы контейнеров хранятся в публичном docker-репозитории DockerHub. DockerHub представляет собой публичный реестр с доступными контейнерами, в нем размещены всевозможные образы, от отдельных компонентов до операционных систем. Запуск контейнера выполняется с помощью команды «run».

Чтобы ещё раз сделать акцент на мультиплатформенности, скачаем и запустим в нашем docker (который установлен на операционную систему Debian) контейнер с операционной системой CentOS:
root@dedicated:~# docker pull centos
root@dedicated:~# docker run -i -t centos

Команду 'run' мы запустили с аргументами, залогинившись непосредственно в shell-окружение контейнера f9b7becca15c. Находясь внутри контейнера, выполним три коман-

ды: узнаем версию нашей CentOS, отобразим список директорий внутри контейнера и запустим команду top, которая отобразит все запущенные процессы внутри контейнера:
[root@f9b7becca15c /]# cat /etc/system-release
[root@f9b7becca15c /]# ls -la
[root@f9b7becca15c /]# top

Внутри контейнера вы можете работать как в обычной терминальной среде. Командой «yum install mc» установим популярный файловый менеджер. Обратите на это внимание, к этому вопросу мы скоро вернемся.

В данном примере, командой pull мы загрузили последнюю, latest версию CentOS. Мы можем загружать с dockerhub любые другие версии, все что нам для этого нужно, это знать название репозитория и названия образа. Команда будет выглядеть так:
root@dedicated:~# docker pull [ОПЦИИ] [ПУТЬ/]ИМЯ_ОБРАЗА[:ТЕГ]
root@dedicated:~# docker pull centos:centos7.4.1708

Посмотреть список загруженных образов:
root@dedicated:~# docker images

Посмотреть запущенные контейнеры:

root@dedicated:~# docker container ls

Загрузим ещё несколько контейнеров. Они нам понадобятся для наглядности, в заключительной главе этой статьи.
root@dedicated:~# docker pull ubuntu
root@dedicated:~# docker pull ubuntu

Посмотреть список загруженных контейнеров, и список всех контейнеров (без опции '-a' команда отобразит список всех активных контейнеров) :
root@dedicated:~# docker ps -a

Вы, наверное, обратили внимание, что командой 'run', мы с образа CentOS сделали один контейнер, а в списке всех доступных их значится два. На этом моменте нужно понять особенность контейнеризации. Первоначальный образ контейнера CentOS (CONTAINER ID: f9b7becca15c) был пуст. Мы ранее установили в него файловый менеджер 'mc'. Но фактически, мы установили 'mc' не в этот контейнер, мы как бы наложили на него слой, создав на основе CentOS (CONTAINER ID: f9b7becca15c) дополнительный контейнер CentOS+mc (CONTAINER ID: 1d09ac8b4e79). У нас получилось два управляемых, автономных контейнера с разными container id.

Запустить контейнер можно по его container id:
root@dedicated:~# docker start 1d09ac8b4e79

Попасть внутрь контейнера можно с помощью команды 'exec':
root@dedicated:~# docker exec -it 1d09ac8b4e79 bash

Остановить или удалить контейнер можно так же по его container id, или по имени, которое видно на скриншоте выше. Команды для примера, контейнеры удалять пока не будем, они нам ещё будут нужны.
root@dedicated:~# docker stop 1d09ac8b4e79
или root@dedicated:~# docker stop keen_carson
root@dedicated:~# docker rm 1d09ac8b4e79
или root@dedicated:~# docker rm keen_carson

4.Dockerfile

В предыдущем разделе мы работали с уже готовыми образами Docker, которые мы загружали с DockerHub. В этом разделе рассмотрим процесс создания собственного сценария

по созданию образа. Этот сценарий пишется в текстовом формате и называется Dockerfile, в нем вы описываете набор инструкций по созданию образа.

Создадим простейший файл Dockerfile:
root@dedicated:~# mkdir /opt/freehost-imag
root@dedicated:~# cd /opt/freehost-image
root@dedicated:/opt/freehost-image# nano Dockerfile

содержимое Dockerfile:
FROM debian:latest
MAINTAINER Dmitry Shestak <shestak@freehost.com.ua>
RUN apt-get update
RUN apt-get install -y nginx mc curl atop
EXPOSE 80

Сохраните файл, и находясь в каталоге с ним, запустите создание образа:
docker build . -t freehost-image

В консоли Вы увидите подробный вывод того, что происходит внутри контейнера. А происходит следующее: поле FROM указывает исходный образ операционной системы, на основе которого будет сформирован наш собственный образ. Поле MAINTAINER указывает автора образа. Поле RUN запускает оболочку командной строки, внутри которой система сначала обновит индекс пакетов, а затем установит перечисленное программное обеспечение.

Теперь посмотрим список доступных образов:
root@dedicated:~# docker images

В списке мы видим наш образ, который мы создали: freehost-image (id 21f738109e09). Выполним в него вход и запустим что-нибудь из программного обеспечения, которое мы перечислили в сценарии.
root@dedicated:~# docker run -it freehost-imag
root@5199cfa793af:/# atop
Сложность Dockerfile ограничена лишь вашими целями, мы рассмотрели самый простой пример. Со всеми доступными переменными и инструкциями, которые можно использовать при создании образа, вы можете ознакомиться в разделе официальной документации.

5. Установка Wordpress в Docker с помощью Docker-compose

Docker-compose это инструмент, который используют для запуска нескольких контейнеров. Он является своего рода сценарием, позволяющий описать взаимодействие нескольких контейнеров для работы одного сложного приложения. Например, если нам нужен только nginx, запустить его можно командой 'docker run nginx'. Если нам потребуется более сложное приложение, включающее в себя nginx+php+mysql, нам потребуется Docker-compose.
В этом примере мы создадим собственный docker-compose для сайта на популярном движке WordPress и запустим его.
Для начала установим приложение Docker-compose:
root@dedicated:~# curl -s https://api.github.com/repos/docker/compose/releases/latest |
grep browser_download_url | grep docker-compose-Linux-x86_64 | cut -d '"' -f 4 | wget -qi -
root@dedicated:~# chmod +x docker-compose-Linux-x86_64
root@dedicated:~# sudo mv docker-compose-Linux-x86_64 /usr/local/bin/docker-compose
root@dedicated:~# docker-compose version
docker-compose version 1.25.2, build 698e2846
docker-py version: 4.1.0
CPython version: 3.7.5
OpenSSL version: OpenSSL 1.1.0l 10 Sep 2019

Создадим наш файл сценария
root@dedicated:~# mkdir /opt/wordpress && cd /opt/wordpress
root@dedicated:/opt/wordpress# mcedit docker-compose.yml

...и добавим в него содержимое:

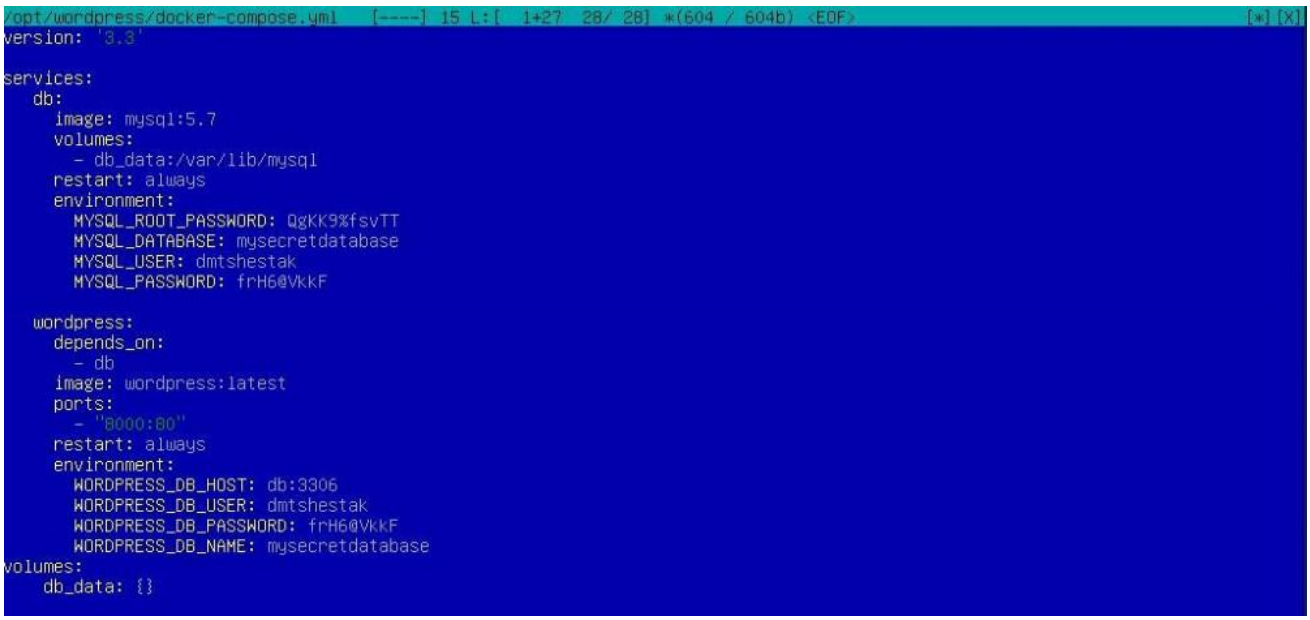


Рис. 253

Внимание! Файл в формате *.yml, который чувствителен к синтаксису. Отступы должны иметь чётное количество пробелов. Если это условие не будет соблюдено, он будет неработоспособен.

После чего, находясь в каталоге с docker-compose.yml выполните команду:
root@dedicated:~# docker-compose up -d
В консоли вы должны увидеть следующее:
Creating network "wordpress_default" with the default driver
Creating volume "wordpress_db_data" with default driver
Pulling db (mysql:5.7)...
5.7: Pulling from library/mysql
804555ee0376: Pull complete
c53bab458734: Pull complete
…….
…….

d054b015f084: Pull complete
Digest:
sha256:73e8d8adf491c7a358ff94c74c8ebe35cb5f8857e249eb8ce6062b8576a01465
Status: Downloaded newer image for wordpress:latest
Creating wordpress_db_1 ... done
Creating wordpress_wordpress_1 ... done

В сценарии нами били описаны сервисы которые нужно установить (mysql и wordpress), мы указали пароли и пробросили порт, по которому мы можем получить доступ. Если вы все сделали верно, то для того чтобы увидеть окно с первоначальной настройкой Wordpress, достаточно в оке браузера ввести: https://ваш_ip_адрес:8000

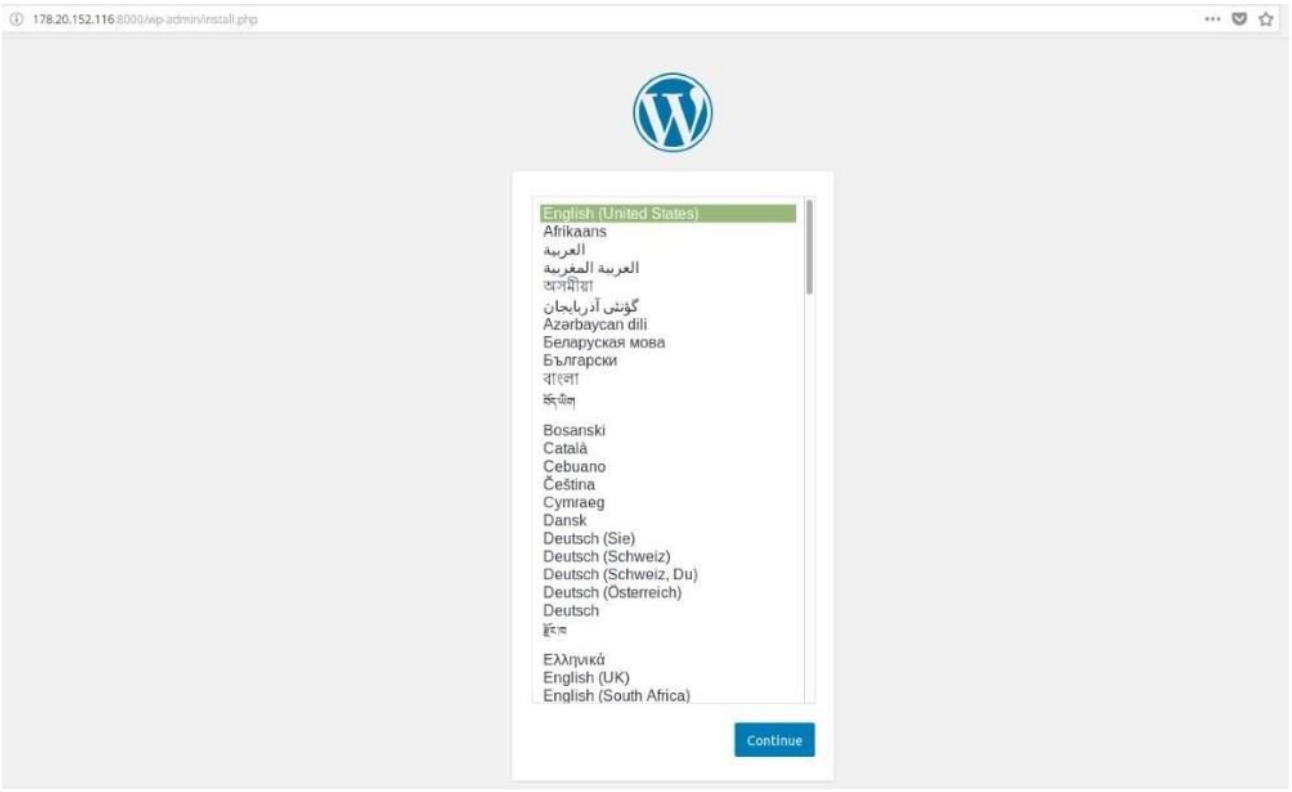


Рис. 254

Уже известной нам командой посмотрим список запущенных контейнеров:

6. Установка и управление Portainer

В предыдущих разделах мы научились загружать, создавать собственные контейнеры, а также комбинировать контейнеры в сложные приложения с помощью docker-compose. Эта глава посвящена удобному приложению для управления Docker хостами и контейнерами, имеющее на вооружении множество возможностей. Вот некоторые из них:

- Web-панель. Управление осуществляется в окне браузера с помощью web-интерфейса.
- Управление сервисами. Portainer позволяет в графической оболочке указать реестр, с которого будет загружен контейнер, название образа, даст возможность пробросить необходимые порты, настроить сеть, указать рабочие директории, подключить диски.
- Управление контейнерами и сбор статистики. Вы сможете анализировать логи каждого отдельного контейнера, собирать статистику по используемым ресурсам, работать в контейнере подключившись к нему через bash в интерактивном окне.
- Кластеризация. Portainer поддерживает кластеризацию Docker Swarm.

Установить его не сложно, так как Portainer сам представлен в виде контейнера.
Первым делом создадим каталог, где будут размещены данные:
root@dedicated:~# mkdir /root/portainer/data

Запустим контейнер следующей командой:
root@dedicated:~# docker run --name portainer --restart always -d -p 9000:9000 -v /root/portainer/data:/data -v /var/run/docker.sock:/var/run/docker.sock portainer/portainer
Так же мы можем установить Portainer через уже знакомый нам Docker-compose. Содержание файла будет следующее:

```
portainer:
    image: portainer/portainer
    container_name: portainer
    hostname: portainer
```

restart: always
command: --no-auth --no-analytics
volumes:
- /var/run/docker.sock:/var/run/docker.sock
ports:
- "9000:9000"

По окончании установки, web-интерфейс Portainer будет доступен по ссылке: https://ваш_ip_адрес:9000

Первым делом вы увидите окно регистрации, с предложением ввести пароль администратора. Введите сложный пароль и подтвердите его.

Перед вами появится с окно с выбором окружения, Local или Remote. Так как Docker у нас установлен локально, выбираем Local и подключаемся нажатием Connect. После чего вы увидите рабочее окружение Portainer.

На первый взгляд UI Portainer может показаться перегруженным и запутанным, но это только на первый взгляд. Меню и функционал интуитивно понятен. Предлагаем вам самостоятельно пройтись по всевозможным меню и вкладкам.

На следующем скриншоте, в разделе Containers мы можем увидеть все контейнеры, которые мы создали ранее в этой статье:

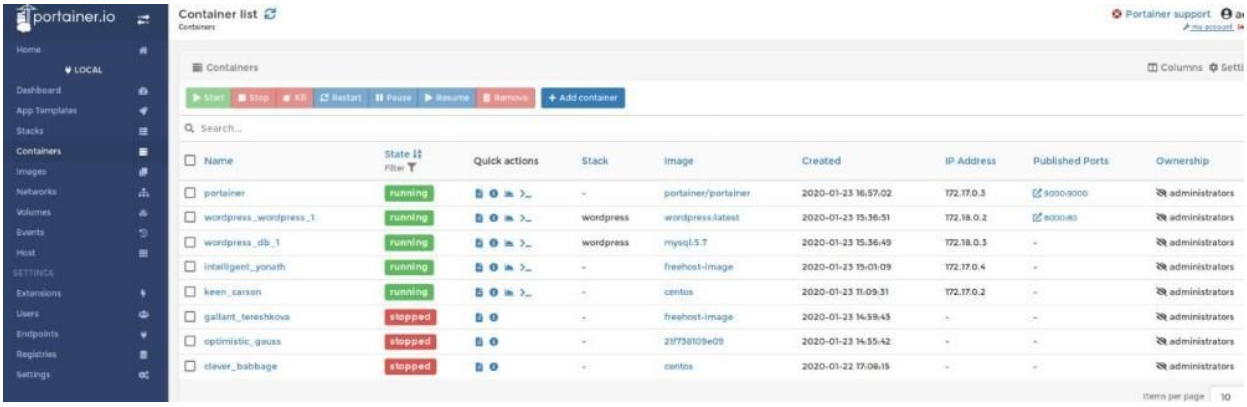


Рис. 255

Portainer достаточно хорошо документирован. Мы не видим смысла перегружать статью графическим контентом и скриншотами, все это доступно и подробно описано в официальном руководстве, с которым рекомендуем ознакомиться для решения более сложных задач.

Сделайте скриншоты (фотографии) процесса настройки контейнеров Dockeri вставьте в отчёт.

2.20. Практическая работа № 20 «Установка сервера CentOS»

Задание:

1. Установка CentOS 8 с помощью ISO-образа

В рекомендуемых требования указано, что для установки CentOS 8 необходимо минимум 10 Гб места на диске и 512 Мб RAM на одно ядро процессора.
Первым шагом, вам будет предложено выбрать дальнейшие действия. Так как вы выполняете установку, нам интересен первый пункт меню:

```
Install CentOS Linux 8.0.1905
```

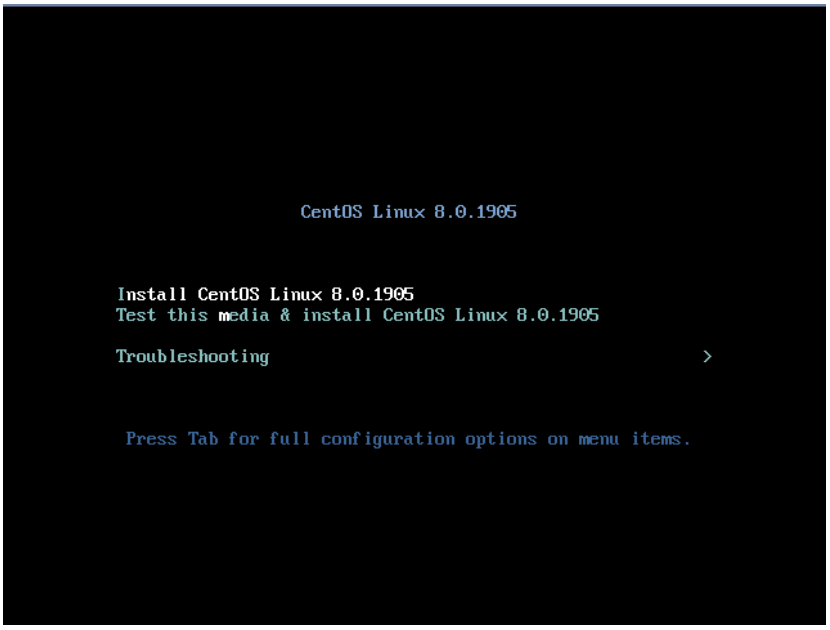


Рис. 256

Выбрав его, у вас запустится процесс установки:

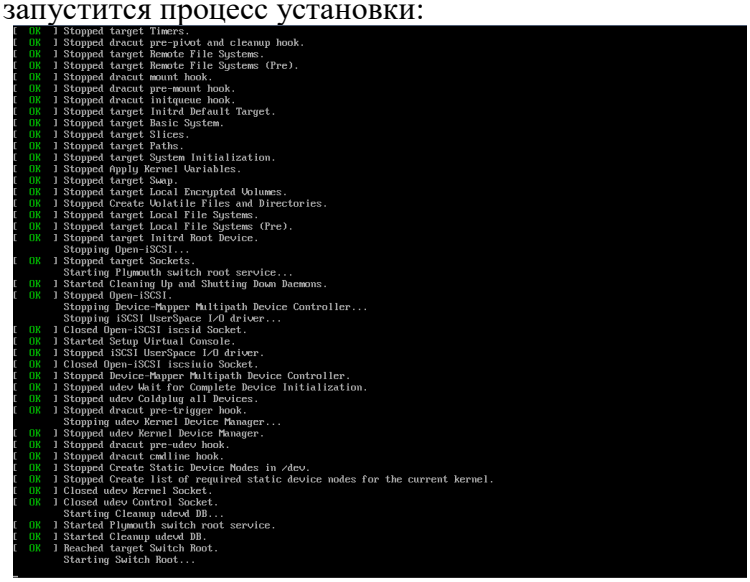


Рис. 257

В процессе пока все необходимое ПО загружается, можно просто наблюдать за процессом, от вас не требуется никаких действий.

И когда черный экран сменится на интерактивный с логотипом **CentOS**, пора брать в руки мышь и клавиатуру.

В приветствии, система попросит вас выбрать язык.

Нажмите кнопку **“Continue”**. В следующем меню нужно выбрать основные настройки для установки CentOS.

Для запуска установки, обязательно настроить только один пункт **“Installation Destination”**, там вы указываете разбивку диска, но давайте сразу настроим сеть и дату со временем.

В зависимости от вашего часового пояса, вы устанавливаете свои параметры, для нас это Москва.

Чтобы настроить сеть, переходим в пункт **“Network & Host Name”**

В поле **“Host Name”** указываем имя сервера и для конфигурации сетевых интерфейсов нажимаем **“Configure”**

В главной вкладке, нужно отметить галочкой **“Automatically connect to this network when it is available”**, это нужно для того, чтобы сетевой интерфейс поднимался автоматически.

Перейдите во вкладку **“IPv4 Settings”** (либо **IPv6** если вы используете данный протокол) настройте **IP**-адрес, маску подсети и шлюз.
Для ввода конкретного **IP (192.168.1.N, где N – номер вашего пользователя)**, нужно выбрать метод **“Manual”** и нажать кнопку **“Add”**, после чего у вас появится возможность ввести нужные данные. Сохранив все, мы вернемся к начальному окну настроек сети.
Как можно увидеть на скриншоте, **IP** адрес добавился и сетевой интерфейс уже поднят (состояние Connected).
Следующим шагом мы перейдем к разбивке диска:

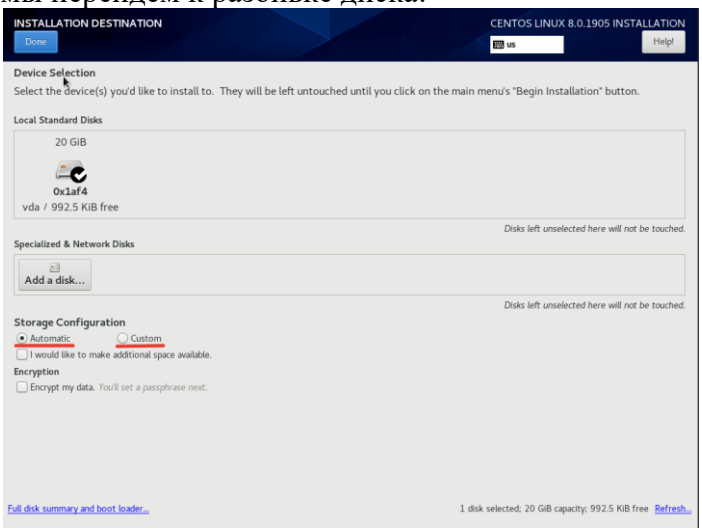


Рис. 258

Для примера установки воспользуемся автоматической разбивкой от разработчиков **CentOS**. Если вы хотите разбить диск по-своему, нужно выбрать пункт **“Custom”.**
Если контроллер вашего сервера не поддерживает аппаратный RAID, в этом пункте меню вы можете собрать программный RAID из дисков сервера на базе mdadm.
Список пакетов для установки выбирается в пункте Software Selection. Если вы планируете использовать CentOS 8 в качестве сервера, достаточно выбрать Minimal Install, а из добавлений Standard и Guest Agents (если вы ставите гостевую ОС в виртуальной машине).
После вышеописанных действий, можно запускать установку кнопкой **“Begin Installation”**
В процессе уже самой распаковки и установки необходимых компонентов, вам потребуется указать пароль для **root**-пользователя и можно создать дополнительного пользователя, но это не обязательный пункт.
Нажмите на кнопку **“Root Password”**, введите и повторите пароль и нажмите **“Done”**, чтобы вернуться к установке:

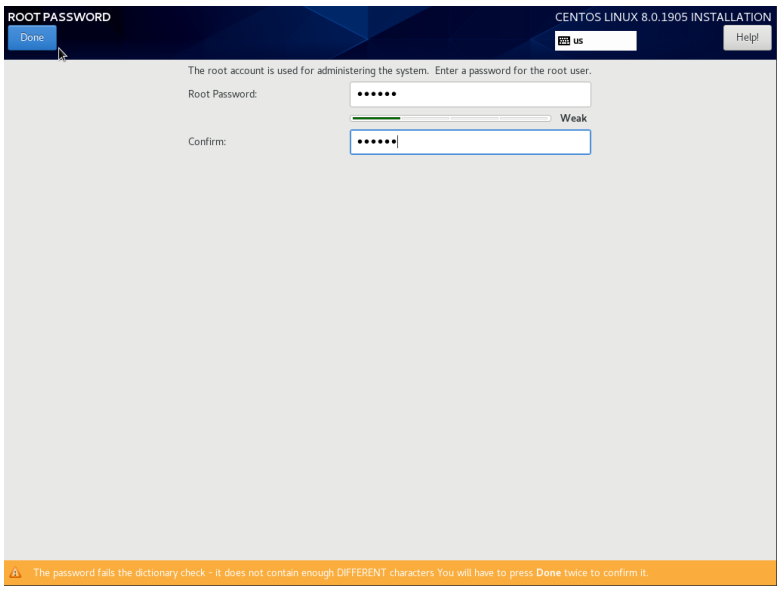


Рис. 259

Изначально предлагаю установить простой пароль, чтобы в случае проблем с сетью, вы могли легко его вспомнить и исправить проблемы. После того, как система будет установлена, пароль рекомендуется изменить на более сложный.

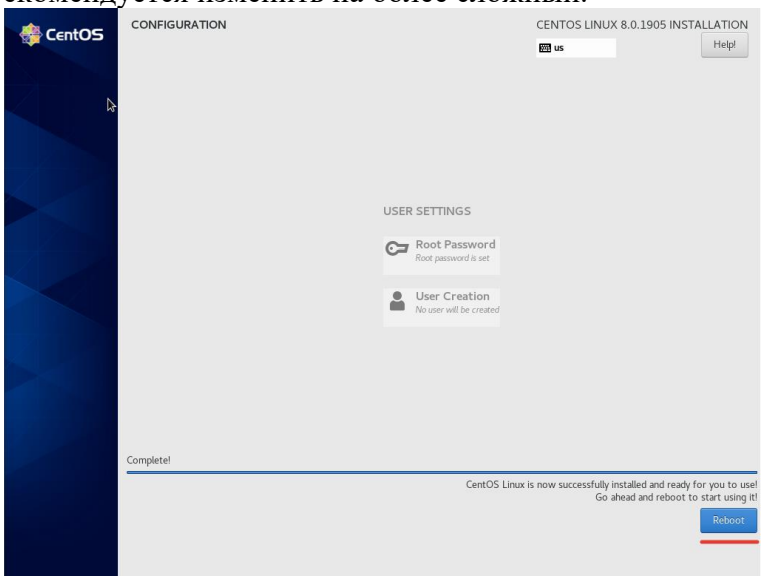


Рис. 260

На этом установка **CentOS 8** завершена.

2.Базовая настройка CentOS 8 после установки

Базовая настройка **CentOS 8** практически не отличается от настройки CentOS, я делаю базовые настройки одинаковые на всех серверах.

1. CentOS 8: Установка обновлений и инструментов администратора

В **CentOS 8** на замену **yum**, пришел **dnf**.

Dnf – это следующее поколение приложения **YUM**, менеджер пакетов для дистрибутивов Linux на основе **RPM**-пакетов. Ранее **dnf** использовался в дистрибутивах **Fedora**, а теперь и в **CentOS 8**.

Первое действие, которое необходимо выполнить на вновь установленном сервере, это обновление системы:

```
dnf update -y
```

Если образ свежий, то скорее всего у вас не будет пакетов для обновлений:

```
[root@centos var]# dnf update

Last metadata expiration check: 0:21:47 ago on Wed 09 Oct 2020 02:36:45 PM +06.
```

```
Dependencies resolved.
Nothing to do.
Complete!
```

Если у вас обнаружатся обновления, обязательно их установите.
Следующим шагом, подключим репозиторий **EPEL** и установим необходимые утилиты для удобного администарирования сервера:

```
dnf install epel-release –y
dnf install mc wget screen nano net-tools bind-utils curl lsof vim -y
```

Для комфортного администрирования хватает этого набора утилит, вы можете установить свои привычные утилиты.
Автоматическое обновление системы не включаем, так как всегда требуется устанавливать необходимые обновления вручную. Если вы хотите настроить автоматическое обновление, установите пакет **dnf-automatic**:

```
dnf install -y dnf-automatic
```

Чтобы проверить активные задания на обновления системы введите:

```
systemctl list-timers *dnf-*
```

2. Отключение SELinux

На начальном этапе необходимо отключить **SELinux** (для применения изменения нужно перезагрузить сервер):

```
nano /etc/sysconfig/selinux
reboot
```

Отключение **SELinux** налету, можно выполнить командой:

```
setenforce 0
```

3. Настройка сети в CentOS 8

Так как сеть мы настроили на этапе установки системы, настройка ее в данный момент не требуется. Необходимо добавить, что в **CentOS 8**, сеть управляется только через **Network Manager и утилиту** nmcl. **Network-scripts** по умолчанию не поддерживаются.
Проверка статуса сети:

```
[root@server ~]# systemctl status NetworkManager
```

```
● NetworkManager.service - Network Manager
Loaded: loaded (/usr/lib/systemd/system/NetworkManager.service; enabled; vendor preset: enabled)
Active: active (running) since Mon 2019-10-07 08:23:11 MSK; 3h 37min ago
Docs: man:NetworkManager(8)
Main PID: 870 (NetworkManager)
Tasks: 3 (limit: 5060)
Memory: 4.7M
CGroup: /system.slice/NetworkManager.service
└─870 /usr/sbin/NetworkManager --no-daemon
```

4. Установка и смена hostname

Если вы не задали корректный **hostname** сервера при установке или просто хотите изменить, это можно выполнить несколькими способами. Измените его в файле **/etc/hostname** или поменяйте с помощью команды:

```
hostnamectl set-hostname нужный_хостнейм
```

5. Настройка firewalld в CentOS 8

Добавим в доверенные зоны на **firewalld**, нужные для начальной работы сервисы (SSH и HTTP/HTTPS):

```
firewall-cmd –-add-service=ssh
firewall-cmd --permanent –-add-service=http
firewall-cmd --permanent –-add-service=https
```

6. Настройка времени и часового пояса (time-zone)

Чтобы посмотреть текущее время и time-zone, нужно ввести команду **date**:

```
[root@centos var]# date
Wed Oct 9 13:03:00 MSK 2020
```

Мы указали **time-zone** при установке самой системы, поэтому у нас время по Москве. Чтобы поменять **time-zone**, нужно воспользоваться соответствующей командой:

```
timedatectl set-timezone Europe/Moscow
```

Где вместо **Europe/Moscow** вы можете указать свой вариант, например:

```
[root@server network-scripts]# date
Mon Oct 7 12:46:09 MSK 2019
[root@server network-scripts]# timedatectl set-timezone Asia/Almaty
[root@server network-scripts]# date
Mon Oct 7 15:46:22 +06 2019
```

Для синхронизации времени используется **chronyd**, мы включим его и добавим в автозагрузку через systemctl:

```
dnf install chrony
systemctl enable chronyd
systemctl start chronyd
 [root@server network-scripts]# systemctl status chronyd
● chronyd.service - NTP client/server
Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; vendor preset: enabled)
Active: active (running) since Mon 2019-10-07 16:13:48 +06; 9s ago
Docs: man:chronyd(8)
man:chrony.conf(5)
Main PID: 31700 (chronyd)
Tasks: 1 (limit: 5060)
Memory: 1.1M
CGroup: /system.slice/chronyd.service
└─31700 /usr/sbin/chronyd
```

7. Настройка истории команда в bash_history

Для удобного просмотра истории, предлагаю добавить пару строк в **.bashrc**, чтобы в последствии можно было легко ориентироваться в отчетах.

При настройке по умолчанию, вывод **history** выглядит следующим образом:

```
[root@centos ~]# history
1 dnf repolist
2 dnf install epel-release
```

То есть мы видим, что выполнялось на сервере, но не видим время и точную дату, для нас это критично, так как доступ к серверам могут иметь несколько специалистов. Поэтому приведем **history** к приятному виду:

```
export HISTSIZE=10000
export HISTTIMEFORMAT="%h/%d/%y - %H:%M:%S "
```

Теперь при проверке **history,** мы видим точное время выполнения той или иной команды:

```
[root@centos ~]# history
1 Oct/07/19 - 16:16:29 dnf repolist
2 Oct/07/19 - 16:16:29 dnf install epel-release
```

8. Cockpit: Веб-интерфейс управления сервером в CentOS 8

В CentOS 8 предустановлен веб-интерфейс управления сервером cockpit. Он также управляется через systemctl. Вы можете запустить его и добавить в автозгрузку:

```
# systemctl enable cockpit.socket
# systemctl start cockpit.socket
```

По–умолчанию веб сервер Cockpit слушает на порту 9090. Добавьте этот порт в разрешенные:

```
# firewall-cmd --get-active-zones
# firewall-cmd --add-port=9090/tcp --zone=MY_ACTIVE_ZONE
# firewall-cmd --reload
```

Для доступа к веб-интерфейсу Cockpit, откройте в браузере URL адрес https://your-CentOS8-IP:9090 и авторизуйтесь.

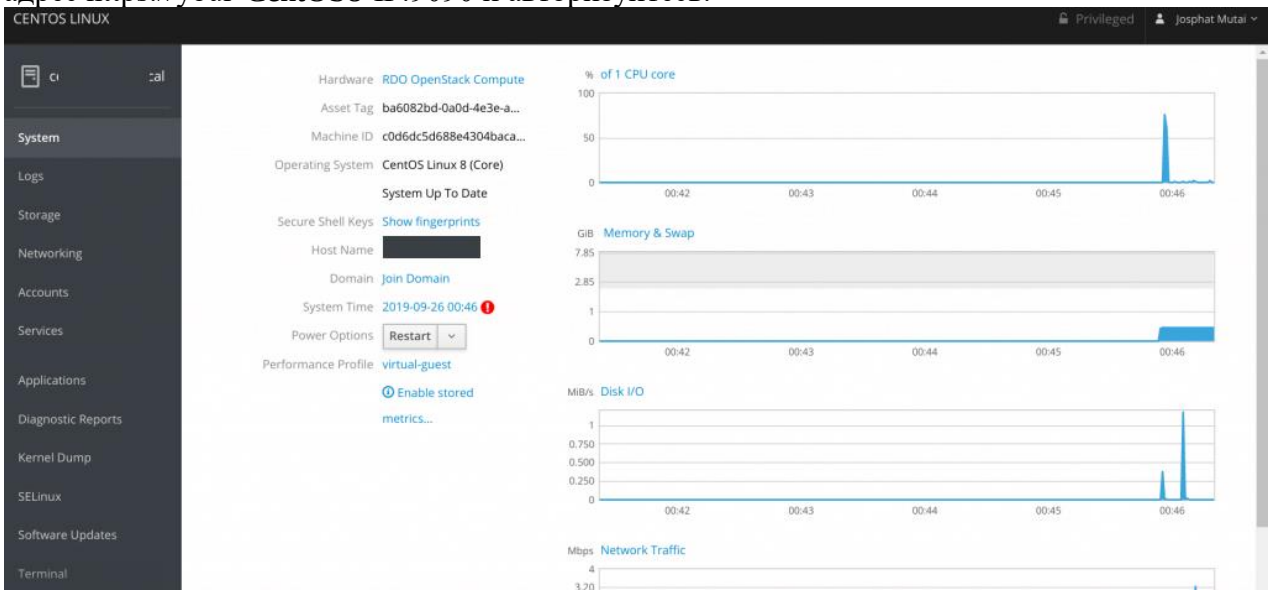


Рис. 261

С помощью веб-интерфейса Cockpit вы можете смотреть загрузку своего сервера, управлять сетями и хранилищами, контейнерами, смотреть логи.

На этом типовая настройка CentOS сервера закончена.

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

2.21. Практическая работа № 21 «Настройка web-сервера в CentOS»

Задание:

1. Установка пакетов

1.1 Обновляем CentOS:

```
dnf update
```

1.2 Устанавливаем дополнительные пакеты для загрузки и распаковки:

```
dnf install unzip
```

1.3 Настройка безопасности

Открываем необходимые порты в брандмауэре:

```
firewall-cmd --permanent --add-port={80,443,8080}/tcp
firewall-cmd --permanent --add-port={20,21,60000-65535}/tcp
firewall-cmd --permanent --add-port={25,465,587}/tcp
```

```
firewall-cmd --reload
```

** 80, 443 и 8080 порты для веб-сервера; 20, 21 порты нужны для работы FTP;* 60000-65535 *также необходимы для работы FTP (динамические порты для пассивного режима); 25, 465 и 587 порты нужны для работы почтового сервера по SMTP; последняя команда перезапускает firewalld, чтобы применить новые правила.*

2. Установка NGINX

2.1 Устанавливаем NGINX:

```
dnf install nginx
```

2.2 Внесем небольшую корректировку в файл nginx.conf:

```
nano /etc/nginx/nginx.conf
```

2.3 В секцию http добавим строку:

```
http {
    ...
    server_names_hash_bucket_size 64;
    ....
}
```

** на практике, может встретиться ошибка* ***could not build server_names_hash, you should increase server_names_hash_bucket_size: 32****. Она возникает при большом количестве виртуальных серверов или если один из них будет иметь длинное название. Данная строка в конфиге исправит ситуацию.*

2.4 Разрешаем автозапуск сервиса и запустим его:

```
systemctl enable nginx
systemctl start nginx
```

2.5 Проверим, что веб-сервер работает. Для этого открываем браузер на другом компьютере, который находится в одной сети и вводим в адресной строке IP-адрес сервера. В итоге мы должны увидеть заголовок «Welcome to nginx!»:

Рис. 262

** обратите внимание, что данное приветствие может иметь и другой вид.*

3. Установка PHP и PHP-FPM

3.1 Устанавливаем PHP и php-fpm следующей командой:

```
dnf install php php-fpm
```

** В CentOS 8 будет установлена версия php 7.2 и выше*

3.2 Запускаем php-fpm и разрешаем его автозапуск:

```
systemctl enable php-fpm --now
```

4. Настройка связки NGINX + PHP

4.1 Открываем файл для настройки виртуального домена по умолчанию:

```
nano /etc/nginx/nginx.conf
```

В секции **location** редактируем параметр **index** на следующее значение:

```
   location / {
      index  index.php index.html index.htm;
   }
```

** добавляем **index.php** в начало списка. Если параметра **index** нет, создаем его.*

4.2 Внутри секции **server** добавим следующее:

```
   location ~ \.php$ {
      set $root_path /usr/share/nginx/html;
      fastcgi_pass unix:/run/php-fpm/www.sock;
      fastcgi_index index.php;
      fastcgi_param SCRIPT_FILENAME $root_path$fastcgi_script_name;
      include fastcgi_params;
      fastcgi_param DOCUMENT_ROOT $root_path;
   }
```

** где **/usr/share/nginx/html** — корневой путь хранения скриптов; **unix:/run/php-fpm/www.sock** — файл для взаимодействия с php-fpm.*

4.3 Открываем настройки php-fpm:

```
nano /etc/php-fpm.d/www.conf
```

4.4 Проверяем, что параметр listen настроен так:

```
listen = /run/php-fpm/www.sock
```

... иначе, меняем значение. После перезагружаем php-fpm:

```
systemctl restart php-fpm
```

** в данном примере мы указываем, что php-fpm будет использовать сокетный файл **/run/php-fpm/www.sock** для взаимодействия. Этот файл мы указали выше в настройке NGINX.*

4.5 Проверяем правильность настроек nginx:

```
nginx -t
```

И перезагружаем его:

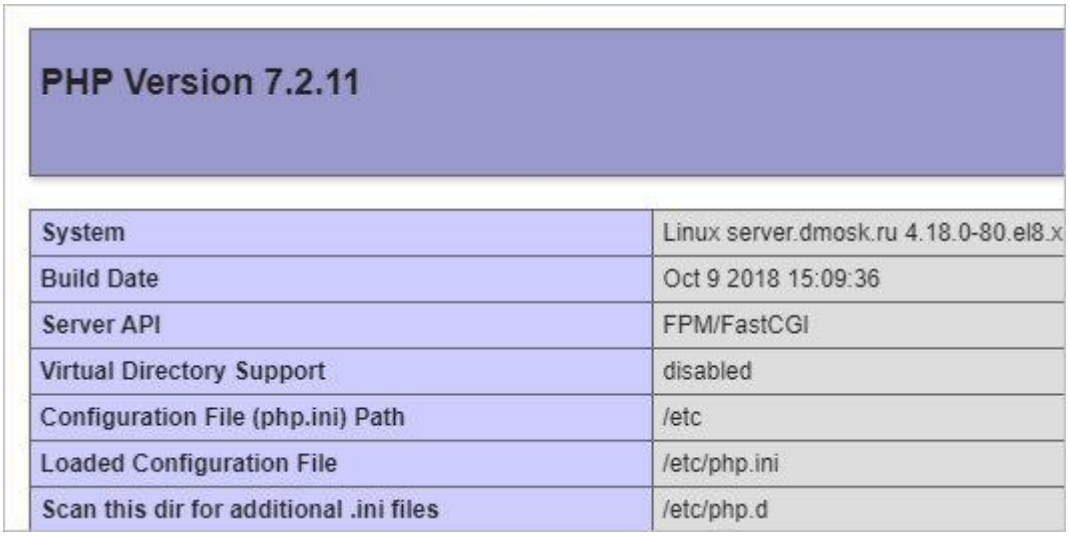
```
systemctl restart nginx
```

4.6 Создаем index.php в каталоге сайта по умолчанию со следующим содержимым:

```
nano /usr/share/nginx/html/index.php
```

```
<?php phpinfo(); ?>
```

Открываем в браузере IP-адрес нашего сервера. Теперь мы должны увидеть сводную информацию по PHP и его настройкам, например:



PHP Version 7.2.11

System	Linux server.dmosk.ru 4.18.0-80.el8.x
Build Date	Oct 9 2018 15:09:36
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d

Рис. 263

5. Установка MariaDB или MySQL

5.1. Устанавливаем MariaDB следующей командой:

```
dnf install mariadb mariadb-server
```

** для установки mysql выполняем команду **dnf install mysql***

5.2. Разрешаем автозапуск и запускаем СУБД:

```
systemctl enable mariadb --now
```

** для работы с mysql меняем **mariadb** на **mysql**.*

5.3. Сразу создаем пароль для учетной записи root:

```
mysqladmin -u root password
```

6. PHP + MariaDB (MySQL)

6.1. Для возможности подключаться к базе данных скриптами PHP необходимо установить следующие модули:

```
dnf install php-mysqli
```

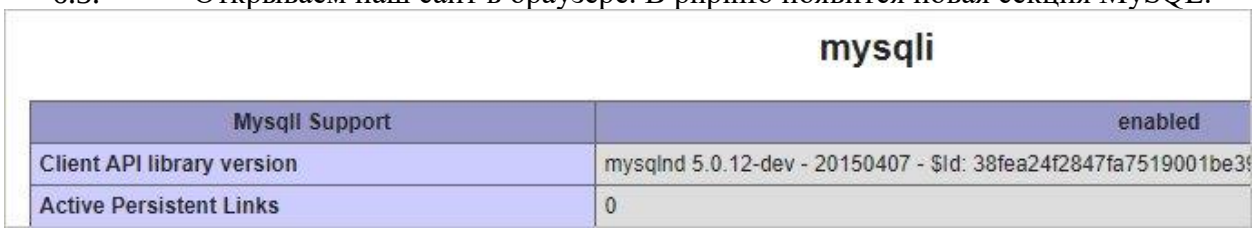
6.2. Если мы установили php5, также ставим php-mysql:

```
dnf install php-mysql
```

После перезагружаем php-fpm:

```
systemctl restart php-fpm
```

6.3. Открываем наш сайт в браузере. В phpinfo появится новая секция MySQL:



mysqli

Mysqli Support	enabled
Client API library version	mysqlnd 5.0.12-dev - 20150407 - $Id: 38fea24f2847fa7519001be3
Active Persistent Links	0

Рис. 264

** нас не должно смущать, что установили мы mariadb, а заголовок mysql. Если посмотреть в таблицу, можно увидеть ячейку **Client API version**, в которой указано, что используется именно mariadb.*

7. Установка phpMyAdmin

Переходим на сайт разработчика phpMyAdmin и копируем ссылку на нужную нам версию, например, последнюю:

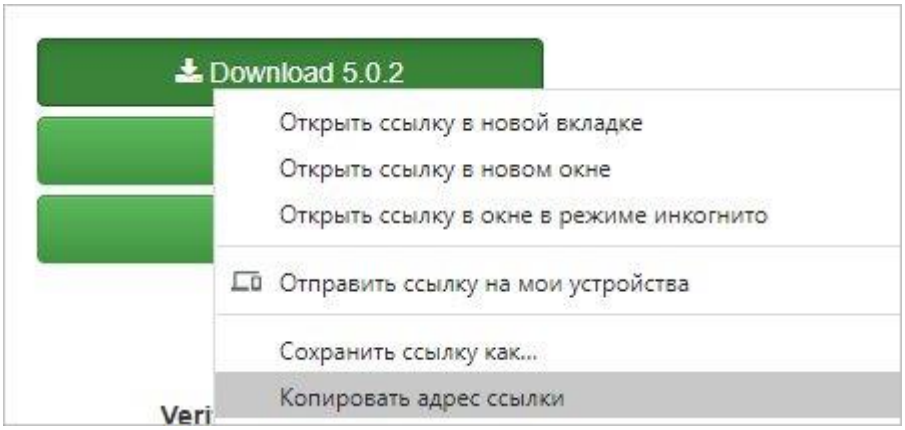


Рис. 265

Воспользовавшись скопированной ссылкой, скачиваем архив с установочными файлами:

```
wget https://files.phpmyadmin.net/phpMyAdmin/5.0.2/phpMyAdmin-5.0.2-all-languages.zip
```

Распаковываем скачанный архив:

```
unzip phpMyAdmin-*-all-languages.zip
```

Создаем каталог для phpmyadmin:

```
mkdir /usr/share/phpMyAdmin
```

... и переносим в него содержимое распакованного архива:

```
mv phpMyAdmin-*-all-languages/* /usr/share/phpMyAdmin/
```

Задаем владельца для каталога:

```
chown -R apache:apache /usr/share/phpMyAdmin
```

** как правило, сервис, которых обрабатываем php-запросы работает от пользователя **apache**.*

Устанавливаем модули php, необходимые для корректной работы phpMyAdmin:

```
dnf install php-json php-mbstring  php-mysqli
```

Внесем небольшую настройку в конфигурацию phpMyAdmin.

Сгенерируем случайную последовательность символов:

```
head /dev/urandom | tr -dc A-Za-z0-9 | head -c 32 ; echo ''
```

Откроем на редактирование или создадим файл:

```
nano /usr/share/phpMyAdmin/config.inc.php
```

Внесем в него строку:

```
<?php
...
$cfg['blowfish_secret'] = 'jd7n6yIcHOl55ikE7l5HAdNaWwunSHvR';

?>
```

** где jd7n6yIcHOl55ikE7l5HAdNaWwunSHvR — последовательность, которую нам выдала команда head **/dev/urandom ...**; Также обратите внимание на* **<?php ?>** — если мы создали новый файл, необходимо указать данные теги, так как они открывают код PHP. В противном случае, настройка не применится.

Теперь создадим для phpmyadmin отдельный виртуальный домен в NGINX:

```
nano /etc/nginx/conf.d/phpMyAdmin.conf
```

И добавим в него следующее содержимое:

```
server {
	listen	80;
	server_name  phpmyadmin.wbsh.local;
	set $root_path /usr/share/phpMyAdmin;

	location / {
		root $root_path;
		index index.php;
	}

	location ~ \.php$ {
		fastcgi_pass unix:/run/php-fpm/www.sock;
		fastcgi_index index.php;
		fastcgi_param SCRIPT_FILENAME $root_path$fastcgi_script_name;
		include fastcgi_params;
		fastcgi_param DOCUMENT_ROOT $root_path;
		fastcgi_read_timeout 300;
	}
}
```

** где **phpmyadmin.wbsh.local** — адрес для виртуального домена, именно этот адрес должен быть введен в адресную строку браузера, чтобы открылся нужный сайт. Поэтому если нет возможности зарегистрировать домен и имя узла в DNS, можно воспользоваться локальным файлом hosts. **/usr/share/phpMyAdmin** — это каталог, в который по умолчанию устанавливается phpMyAdmin.*

После перезапускаем NGINX:

```
systemctl reload nginx
```

Также нужно перезапустить php-fpm, так как в процессе установки были добавлены модули для PHP:

```
systemctl restart php-fpm
```

И открываем в браузере наш домен, в данном примере, http://phpmyadmin.wbsh.local. Откроется форма для авторизации — вводим логин root и пароль, который мы указали после установки и запуска mariadb.

8. Установка Memcached

Первым этапом мы установим и настроим сервис memcached.

Вторым — модуль php-memcached.

8.1. Сервис memcached

Выполняем установку пакетов:

```
dnf install memcached libmemcached
```

Создаем или открываем на редактирование конфигурационный файл для запуска сервиса:

```
nano /etc/sysconfig/memcached
```

Приводим его к виду:

```
PORT="11211"
USER="memcached"
MAXCONN="1024"
CACHESIZE="512"
OPTIONS="-l 127.0.0.1 -U 0"
```

** где **PORT** указываем на каком порту будет слушать сервис кэширования; **USER** — пользователь, под которым должен запускаться сервис; **MAXCONN** — максимальное число одновременных подключений; **CACHESIZE** — размер под кэш в мегабайтах; **OPTIONS** — параметры запуска (в данном примере наш сервис будет принимать запросы только с адреса локальной петли).*

После разрешаем автозапуск и запускаем сервис кэширования:

```
systemctl enable memcached --now
```

8.2. Модуль для php

Переходим на страницу загрузки memcached сайта pecl.php.net и копируем ссылку на стабильную версию memcached:

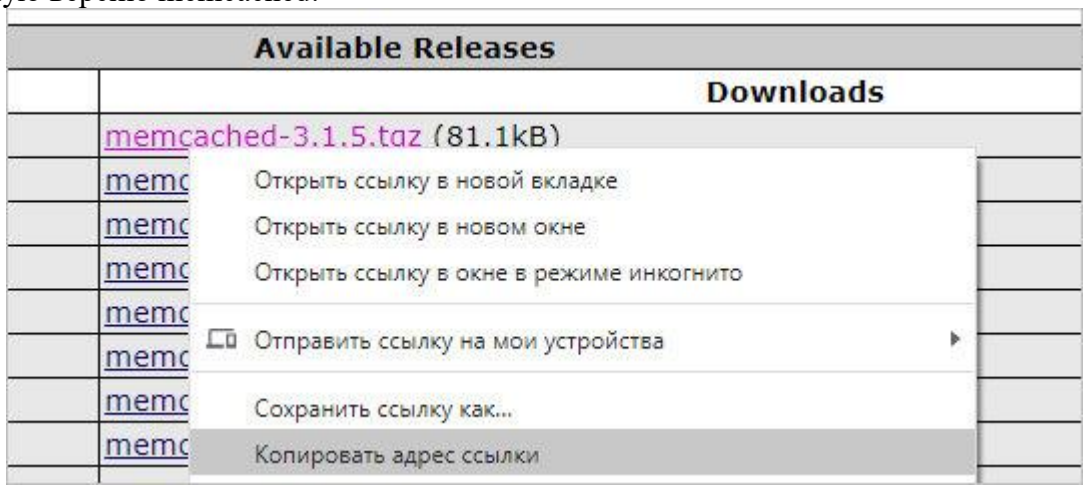


Рис. 266

Обратите внимание, что у каждой версии пакета есть свои требования к версии PHP. Внимательно изучаем, подойдет ли версия php-memcached для нашего сервера.

Скачиваем архив, ссылку на который мы скопировали:

```
wget http://pecl.php.net/get/memcached-3.1.5.tgz
```

Устанавливаем пакеты, необходимые для сборки php-pecl-memcached:

```
dnf install php-devel zlib-devel make
dnf --enablerepo=PowerTools install libmemcached-devel
```

Распаковываем скачанный архив:

```
tar -xvzf memcached-*.tgz
```

Переходим в распакованный каталог:

```
cd memcached-*/
```

Запускаем компиляцию php-расширения:

```
phpize
```

Конфигурируем исходник:

```
./configure
```

Собираем расширение:

```
make
```

Копируем созданный модуль в каталог php-модулей:

```
cp modules/memcached.so /usr/lib64/php/modules/
```

Создаем конфигурационной файл для подключения расширения:

```
nano /etc/php.d/20-memcached.ini
```

```
extension=memcached.so
```

После установки модуля перезапускаем php-fpm:

```
systemctl restart php-fpm
```

Чтобы проверить, что модуль memcached работаем, открываем наш сайт в браузере — в phpinfo должна появиться новая секция:

memcached

memcached support	enabled
Version	3.1.5
libmemcached version	1.0.18
SASL support	yes

... или вводим команду:

```
php -m | grep memcached
```

Мы должны получить:

```
memcached
```

8.3. Установка и настройка FTP-сервера

В качестве FTP-сервера будем использовать ProFTPd, так как он позволяет авторизовываться под uid системных учетных записей.

ProFTPd можно устанавливать командой:

```
dnf install proftpd
```

Загружаем скрипт ftpasswd:

```
wget http://www.castaglia.org/proftpd/contrib/ftpasswd -P /etc/proftpd
```

Разрешаем запуск на выполнение скрипта:

```
chmod +x /etc/proftpd/ftpasswd
```

Создаем виртуального пользователя:

```
/etc/proftpd/ftpasswd --passwd --file=/etc/proftpd/ftpd.passwd --name=ftpwww --uid=48 --gid=48 --home=/var/www --shell=/sbin/nologin
```

** где*

- ***/etc/proftpd/ftpd.passwd*** *— путь до файла, в котором хранятся пользователи;*
- ***ftpwww*** *— имя пользователя (логин);*
- ***uid*** *и* ***gid*** *— идентификаторы пользователя и группы системной учетной записи (apache);*
- ***/var/www*** *— домашний каталог пользователя;*
- ***/sbin/nologin*** *— оболочка, запрещающая локальный вход пользователя в систему.*

Изменим права для созданного файла с паролями:

```
chmod 440 /etc/proftpd/ftpd.passwd
```

** в противном случае, при запуске proftpd мы получим ошибку «...fatal: AuthUserFile: unable to use /etc/proftpd.d/ftpd.passwd: Operation not permitted...»*

Открываем на редактирование конфигурационный файл proftpd:

```
nano /etc/proftpd.conf
```

И редактируем следующее (комментируем):

```
#AuthOrder ...
```

Создадим конфигурационный файл со своими настройками:

```
nano /etc/proftpd/conf.d/custom.conf
```

И добавим следующее:

```
UseIPv6 off
IdentLookups off
PassivePorts 60000 65535

RequireValidShell off
AuthUserFile /etc/proftpd/ftpd.passwd
AuthPAM off
LoadModule mod_auth_file.c
AuthOrder mod_auth_file.c
```

** где **60000 - 65535** — диапазон динамических портов для пассивного режима.*

Разрешаем автозапуск FTP-серверу и запускаем его:

```
systemctl enable proftpd --now
```

Пробуем подключиться к серверу, использую любые FTP-клиенты, например, FileZilla, Total Commander или тот же браузер.

Это базовая и самая простая настройка ProFTPd, но если необходимо настроить TLS или хранить виртуальных пользователей в базе MySQL, читайте подробнее инструкцию по настройке ProFTPd на CentOS.

8.4. Apache (httpd)

Несмотря на то, что мы установили и настроили PHP-FPM, Apache нам понадобится, как минимум, по двум причинам. Во-первых, многие сайты используют файл .htaccess, который читает Apache. Во-вторых, последний включает большое число модулей, которые может использовать портал.

И так, устанавливаем httpd:

```
dnf install httpd
```

Заходим в настройки:

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

И редактируем следующее:

```
Listen 8080
```

** наш веб-сервер будет слушать на порту **8080**, так как на 80 уже работает NGINX.*

```
<IfModule dir_module>
    DirectoryIndex index.php index.html
</IfModule>
```

** если не указан конкретный скрипт, сначала веб-сервер пытается найти и запустить **index.php**, затем **index.html***

Добавляем:

```
<Directory /var/www/*/www>
   AllowOverride All
   Options Indexes ExecCGI FollowSymLinks
   Require all granted
</Directory>
```

** где **Directory** — разрешенные каталоги для запуска из apache; **Options** — разрешенные опции; **Require** — с каких IP-адресов можно открывать сайты, определенные в данном каталоге. Итого, мы разрешаем все каталоги в **/var/www**, но только если следующий каталог будет **www**; разрешаем опции **Indexes** (возвращает список файлов, если нет индексного файла, например, index.php), **ExecCGI** (разрешены сценарии CGI), **FollowSymLinks** (включены символические ссылки в этом каталоге); доступ для данных каталогов разрешен со всех адресов (**all granted**).*

Проверяем синтаксис конфигурационного файла httpd:

```
apachectl configtest
```

И если получаем ответ:

```
Syntax OK
```

... разрешаем автозапуск и запускаем службу:

```
systemctl enable httpd
systemctl start httpd
```

Создаем php-файл со следующим содержимым:

```
nano /var/www/html/index.php
```

```
<?php phpinfo(); ?>
```

Открываем браузер и вводим в адресную строку IP-адрес нашего сервера и добавляем :8080 (http://<IP-адрес нашего сервера>:8080). Откроется привычная нам страница с информацией о PHP. В разделе «PHP Variables» мы должны увидеть Apache для опции $_SERVER['SERVER_SOFTWARE']:

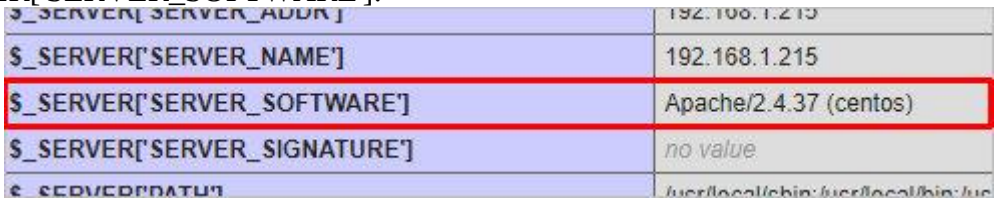


Рис. 267

8.5. NGINX + Apache

Ранее нами была настроена связка nginx + php-fpm. Теперь проверяем совместную работу первого с apache.

Открываем конфигурационный файл nginx:

```
nano /etc/nginx/nginx.conf
```

Находим наш настроенный location для php-fpm:

```
...
   location ~ \.php$ {
```

```
        set $root_path /usr/share/nginx/html;
        fastcgi_pass unix:/run/php-fpm/www.sock;
        fastcgi_index index.php;
        fastcgi_param SCRIPT_FILENAME $root_path$fastcgi_script_name;
        include fastcgi_params;
        fastcgi_param DOCUMENT_ROOT $root_path;
    }
...
```

и меняем на:

```
...
    location ~ \.php$ {
        proxy_pass http://127.0.0.1:8080;
        proxy_redirect     off;
        proxy_set_header   Host             $host;
        proxy_set_header   X-Forwarded-Proto $scheme;
        proxy_set_header   X-Real-IP        $remote_addr;
        proxy_set_header   X-Forwarded-For  $proxy_add_x_forwarded_for;
    }
...
```

Проверяем, есть ли файл:

```
nano /etc/nginx/default.d/php.conf
```

... и если есть, комментируем его содержимое:

```
#index index.php index.html index.htm;
#
#location ~ \.(php|phar)(/.*)?$ {
#    fastcgi_split_path_info ^(.+\.(?:php|phar))(/.*)$;
#
#    fastcgi_intercept_errors on;
#    fastcgi_index  index.php;
#    include        fastcgi_params;
#    fastcgi_param  SCRIPT_FILENAME  $document_root$fastcgi_script_name;
#    fastcgi_param  PATH_INFO $fastcgi_path_info;
#    fastcgi_pass   php-fpm;
#}
```

** в данном примере мы отключили обработку всех php-файлов с помощью php-fpm, так как это у нас должен делать apache.*

Проверяем и перезапускаем nginx:

```
nginx -t
systemctl restart nginx
```

Пробуем снова открыть в браузере адрес http://<IP-адрес нашего сервера> (уже без 8080) — должна открыться та же страница, что при проверке Apache (с добавлением 8080):

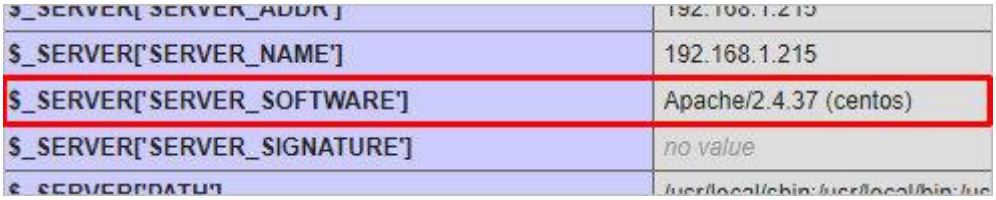


Рис. 268

8.6. Apache Real IP

Так как все запросы на httpd приходят от NGINX, они воспринимаются как от IP-адреса 127.0.0.1. На практике, это может привести к проблемам, так как некоторым сайтам необходимы реальные адреса посетителей.

Для решения проблемы будем использовать модуль mod_rpaf. Устанавливаем набор разработчика для apache:

```
dnf install httpd-devel gcc unzip redhat-rpm-config
```

Переходим в каталог /usr/local/src:

```
cd /usr/local/src
```

Скачиваем модуль:

```
wget https://github.com/gnif/mod_rpaf/archive/stable.zip
```

Распаковываем его:

```
unzip stable.zip
```

Переходим в распакованный каталог:

```
cd mod_rpaf-stable/
```

Собираем модуль и устанавливаем его:

```
make
make install
```

** при возникновении ошибки **./apxs.sh: line 15: -c: command not found**, необходимо поставить **which** командой **dnf install which**.*

Создаем конфигурационный файл со следующим содержимым:

```
nano /etc/httpd/conf.d/mod_rpaf.conf
```

```
LoadModule            rpaf_module modules/mod_rpaf.so
RPAF_Enable           On
RPAF_ProxyIPs         127.0.0.1
RPAF_SetHostName      On
RPAF_SetHTTPS         On
RPAF_SetPort          On
RPAF_ForbidIfNotProxy Off
```

Перезапускаем httpd:

```
systemctl restart httpd
```

Для проверки открываем нашу страницу с phpinfo и находим $_SERVER['REMOTE_ADDR'] — его значение должно быть равно адресу компьютера, с которого мы открыли страницу:

$_SERVER['REQUEST_SCHEME']	http
$_SERVER['DOCUMENT_ROOT']	/var/www/html
$_SERVER['REMOTE_ADDR']	192.168.0.23
$_SERVER['SERVER_PORT']	80
$_SERVER['SERVER_ADDR']	127.0.0.1

Рис. 269

8.7. Postfix

Устанавливаем postfix командой:

```
dnf install postfix
```

Теперь нам необходимо сделать несколько простых настроек:

```
nano /etc/postfix/main.cf
```

Редактируем:

```
...
myorigin = $mydomain
...
inet_protocols = ipv4
...
```

Добавляем:

```
smtp_generic_maps = hash:/etc/postfix/generic_map
```

** **myorigin** — имя домена, которое будет подставляться всем отправляемым сообщениям без явного указания оного; **inet_protocols** — задает версию IP, с которой будет работать Postfix (если на нашем сервере используется ipv6, значение параметра стоит оставить **all**); **smtp_generic_maps** указывает на карту с общими правилами пересылки.*

Открываем карту пересылки:

```
nano /etc/postfix/generic_map
```

И добавляем:

```
@wbsh.local    no-reply@wbsh.local
```

** данной настройкой мы будем подставлять всем отправляемым письмам без поля FROM адрес **no-reply@wbsh.local**.*

Создаем карту:

```
postmap /etc/postfix/generic_map
```

Для применения настроек перезагружаем почтовый сервер:

```
systemctl restart postfix
```

9. Тюнинг веб-сервера

9.1. PHP

Открываем на редактирование следующий файл:

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

И правим следующее:

```
upload_max_filesize = 512M
...
post_max_size = 512M
...
```

```
short_open_tag = On
...
date.timezone = "Europe/Moscow"
```

Перезапускаем php-fpm и httpd:

```
systemctl restart php-fpm
systemctl restart httpd
```

9.2. NGINX

Открываем на редактирование следующий файл:

```
nano /etc/nginx/nginx.conf
```

И внутри секции http добавляем:

```
client_max_body_size 512M;
```

После перезапускаем nginx:

```
systemctl restart nginx
```

9.3. Создание первого сайта

Задаем переменную, значение которой будет домен сайта:

```
TMP_SITE=site1
```

** где **site1** — имя домена. Нам будет намного удобнее копировать и вставлять команды с переменной (не придется править после копипасты).*

Создаем новый файл виртуального домена NGINX:

```
nano /etc/nginx/conf.d/$TMP_SITE.conf
```

** обязательно на конце должен быть **.conf**, так как только такие файлы веб-сервер подгружает в конфигурацию.*

И добавляем следующее содержимое.

Для HTTP:

```
server {
   listen       80;
   server_name  site1.local www.site1.local;
   set $root_path /var/www/site1/www;

   access_log /var/www/site1/log/nginx/access_log;
   error_log /var/www/site1/log/nginx/error_log;

   gzip  on;
   gzip_disable "msie6";
   gzip_min_length 1000;
   gzip_vary on;
   gzip_proxied    expired no-cache no-store private auth;
   gzip_types      text/plain text/css application/json application/x-javascript text/xml application/xml application/xml+rss text/javascript application/javascript;

   root   $root_path;
```

```
   location / {
      proxy_pass http://127.0.0.1:8080/;
      proxy_redirect     off;
      proxy_set_header   Host             $host;
      proxy_set_header   X-Forwarded-Proto $scheme;
      proxy_set_header   X-Real-IP        $remote_addr;
      proxy_set_header   X-Forwarded-For  $proxy_add_x_forwarded_for;
   }

   location ~*
^.+\.(jpg|jpeg|gif|png|css|zip|tgz|gz|rar|bz2|doc|docx|xls|xlsx|exe|pdf|ppt|tar|wav|bmp|rtf|js)$ {
         expires modified +1w;
   }
}
```

** где **site1.local** — домен, для которого создается виртуальный домен; **/var/www/site1** — каталог, в котором будет размещаться сайт.*

*** все запросы будут переводиться на локальный сервер, порт 8080, на котором работает apache, кроме обращений к статическим файла (jpg, png, css и так далее).*

**** обратите внимание на выделения полужирным — здесь нужно подставить свои данные.*

Для HTTPS:

```
server {
   listen 80;
   server_name site1.local www.site1.local;
   return 301 https://$host$request_uri;
}

server {
   listen       443 ssl;
   ssl on;
   ssl_certificate /etc/nginx/ssl/cert.pem;
   ssl_certificate_key /etc/nginx/ssl/cert.key;

   server_name  site1.local www.site1.local;
   set $root_path /var/www/site1/www;

   access_log /var/www/site1/log/nginx/access_log;
   error_log /var/www/site1/log/nginx/error_log;

   gzip  on;
   gzip_disable "msie6";
   gzip_min_length 1000;
```

```
    gzip_vary on;
    gzip_proxied    expired no-cache no-store private auth;
    gzip_types      text/plain text/css application/json application/x-javascript text/xml applica-
tion/xml application/xml+rss text/javascript application/javascript;

    root   $root_path;

    location / {
        proxy_pass http://127.0.0.1:8080/;
        proxy_redirect     off;
        proxy_set_header   Host             $host;
        proxy_set_header   X-Forwarded-Proto $scheme;
        proxy_set_header   X-Real-IP        $remote_addr;
        proxy_set_header   X-Forwarded-For  $proxy_add_x_forwarded_for;
    }

    location ~*
^.+\.(jpg|jpeg|gif|png|css|zip|tgz|gz|rar|bz2|doc|docx|xls|xlsx|exe|pdf|ppt|tar|wav|bmp|rtf|js)$ {
            expires modified +1w;
    }
}
```

** в первой секции server мы перенаправляем все запросы по незащищенному **http** на **https**.*

*** **ssl_certificate** и **ssl_certificate_key** — пути к публичному и приватному ключам соответственно.*

Теперь настроим виртуальный домен в Apache:

```
nano /etc/httpd/conf.d/$TMP_SITE.conf
```

```
<VirtualHost *:8080>
    Define root_domain site1.local
    Define root_path /var/www/site1

    ServerName ${root_domain}
    ServerAlias www.${root_domain}
    DocumentRoot ${root_path}/www

    ErrorLog     ${root_path}/log/apache/error_log
    TransferLog  ${root_path}/log/apache/access_log
</VirtualHost>
```

Создаем каталоги для сайта:

```
mkdir -p /var/www/$TMP_SITE/{www,tmp}
mkdir -p /var/www/$TMP_SITE/log/{nginx,apache}
```

Создаем индексный файл со следующим содержимым:

```
nano /var/www/$TMP_SITE/www/index.php
```

```
<?php echo "<h1>Hello from site1</h1>"; ?>
```

Задаем права на папки:

```
chown -R apache:apache /var/www/$TMP_SITE
chmod -R 775 /var/www/$TMP_SITE
```

Проверяем корректность настроек конфигурационных файлов:

```
nginx -t
apachectl configtest
```

Перезапускаем веб-сервер:

```
systemctl reload nginx
systemctl reload httpd
```

Открываем сайт в браузере.

При необходимости, создаем базу данных.

```
mysql -uroot -p
> CREATE DATABASE site1 DEFAULT CHARACTER SET utf8 DEFAULT COLLATE utf8_general_ci;
> GRANT ALL PRIVILEGES ON site1.* TO dbuser@localhost IDENTIFIED BY 'password' WITH GRANT OPTION;
```

** данными sql-командами мы создаем базу данных **site1** и предоставляем к ней доступ для учетной записи **dbuser** с паролем **password**. При желании сделать соединение более безопасным, можно убрать* **WITH GRANT OPTION**.

Сделайте скриншоты (фотографии) процесса настройки web-сервера и вставьте в отчёт.

2.22. Практическая работа № 22 «Настройка сервера DNS в CentOS»

Задание:

1. Инсталляция необходимых пакетов

Перед началом рассмотрения следующих инструкций хотим отметить, что на нашем сайте уже имеется общее руководство по конфигурации стандартного DNS в Linux. Мы рекомендуем задействовать именно тот материал, если следует выставить настройки для обычного посещения интернет-сайтов. Далее же мы покажем, как инсталлируется основной локальный DNS-сервер с клиентской частью.

В качестве средства создания локального DNS-сервера рекомендуем задействовать **bind9**. Настройка последующих конфигурационных файлов тоже будет базироваться на общих принципах поведения этого компонента. По умолчанию **bind9** отсутствует в операционной системе, поэтому начнем с ее добавления.

1.1 Введем команду sudo dnf install bind bind-utils -y и нажать на **Enter** для ее активации.

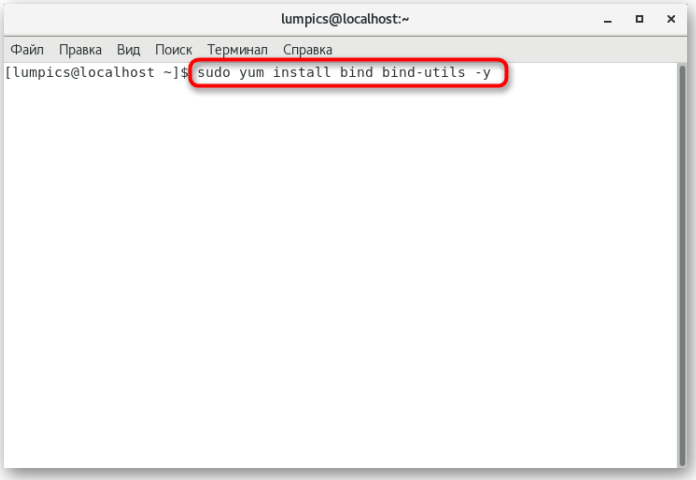


Рис. 270

1.2 Данное действие выполняется от имени суперпользователя (**sudo**), поэтому придется подтвердить учетную запись, введя пароль в появившуюся строку.

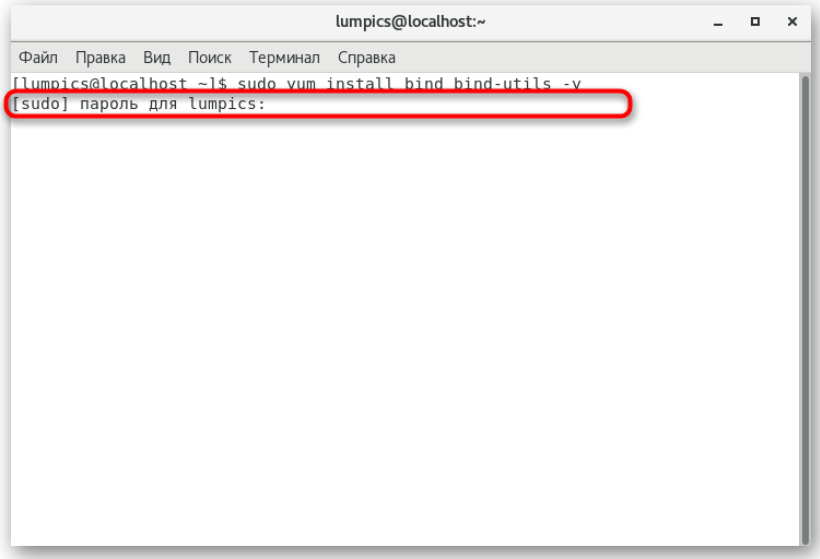


Рис. 271

1.3 Ожидайте завершения скачивания и установки пакетов.

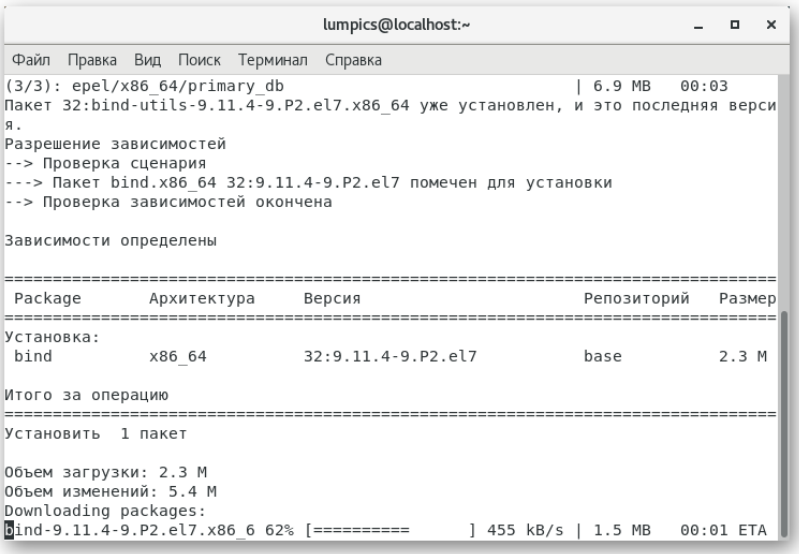


Рис. 272

По окончании данного процесса вы будете уведомлены о том, что все пакеты успешно добавлены в систему. После этого переходите к следующему шагу.

2. Глобальная настройка DNS-сервера

2.1 Для редактирования конфигурационных объектов можно использовать любой текстовый редактор. Предлагаем инсталлировать удобный **nano**, введя в консоли sudo dnf install nano.

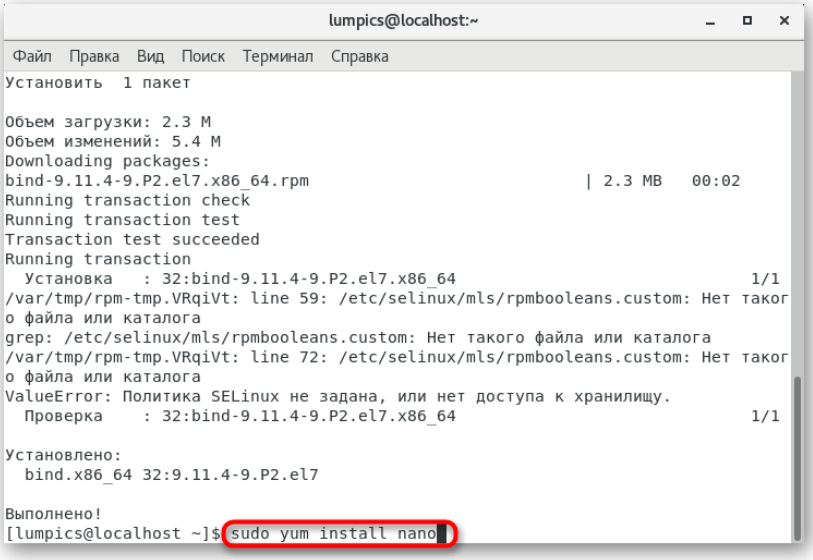


Рис. 273

2.2 Все необходимые пакеты будут загружены, а если они уже присутствуют в дистрибутиве, вы получите уведомление **«Выполнять нечего»**.

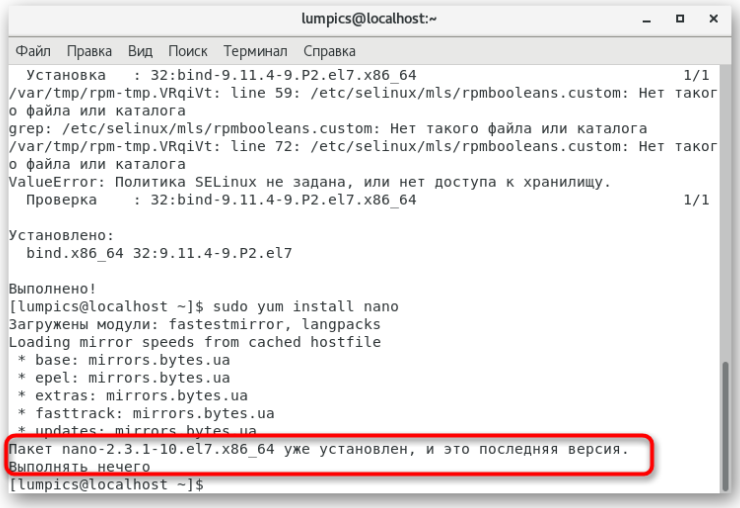


Рис. 274

2.3 Приступим к редактированию самого файла. Откройте его через sudo nano /etc/named.conf. При необходимости замените желаемый текстовый редактор, тогда строка получится примерно такой: sudo vi /etc/named.conf.

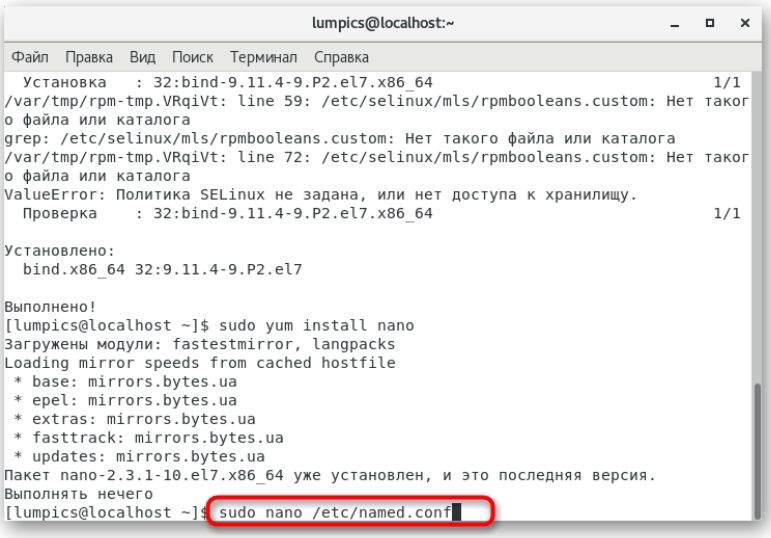


Рис. 275

2.4 Ниже мы приведем содержимое, которое нужно вставить в открывшийся файл или сверить его с уже существующим, добавив недостающие строки.

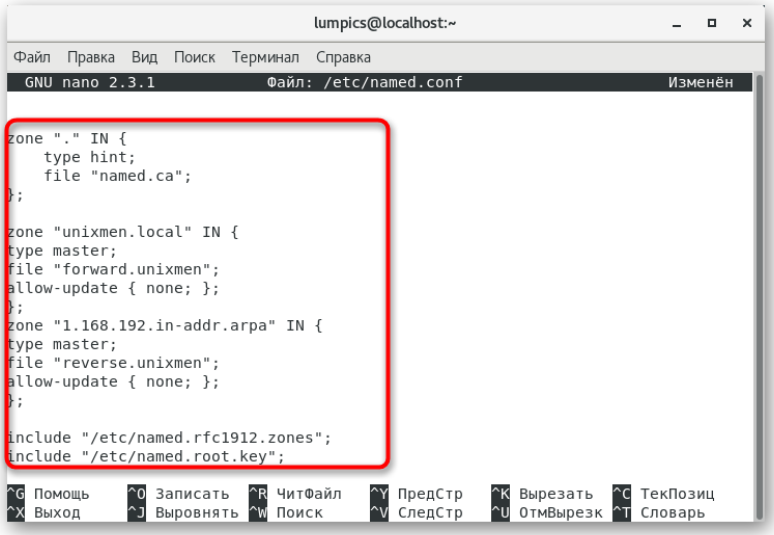


Рис. 276

2.5 После этого нажмите на **Ctrl + O**, чтобы записать изменения.

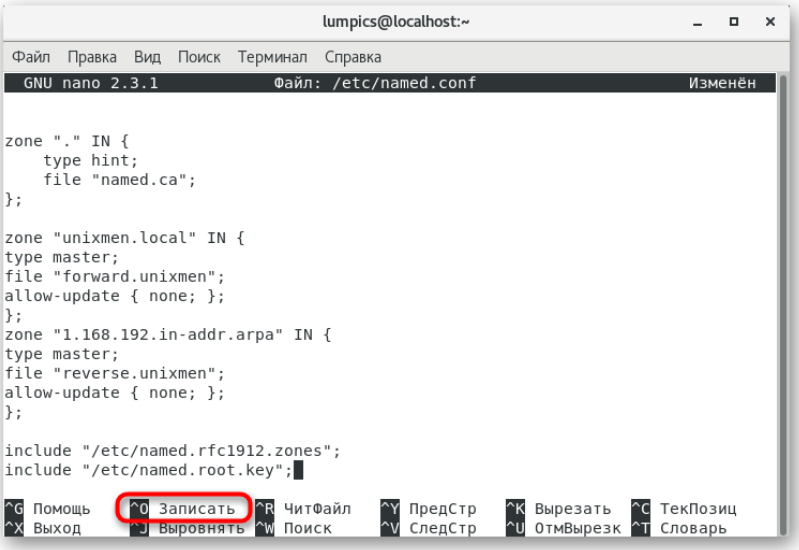


Рис. 277

2.6 Менять название файла не нужно, достаточно просто нажать на **Enter**.

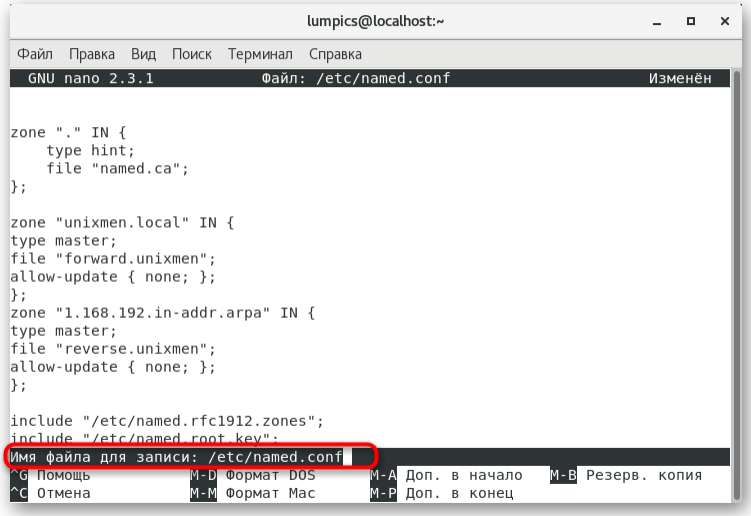


Рис. 278

2.7 Покиньте текстовый редактор через **Ctrl + X**.

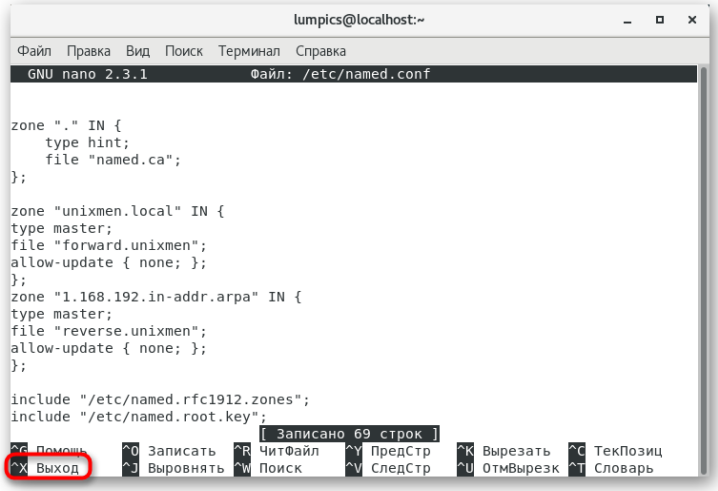


Рис. 279

Как уже было сказано ранее, в конфигурационный файл потребуется вставить определенные строки, задающие общие правила поведения DNS-сервера.

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
options {
listen-on port 53 { 127.0.0.1; 192.168.1.101;}; ### Master DNS IP ###
# listen-on-v6 port 53 { ::1; };
directory "/var/named";
dump-file "/var/named/data/cache_dump.db";
statistics-file "/var/named/data/named_stats.txt";
memstatistics-file "/var/named/data/named_mem_stats.txt";
allow-query { localhost; 192.168.1.0/24;}; ### IP Range ###
allow-transfer{ localhost; 192.168.1.102; }; ### Slave DNS IP ###
```

```
/*
- If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
- If you are building a RECURSIVE (caching) DNS server, you need to enable
recursion.
- If your recursive DNS server has a public IP address, you MUST enable access
control to limit queries to your legitimate users. Failing to do so will
cause your server to become part of large scale DNS amplification
attacks. Implementing BCP38 within your network would greatly
reduce such attack surface
*/
recursion yes;
dnssec-enable yes;
dnssec-validation yes;
dnssec-lookaside auto;
/* Path to ISC DLV key */
bindkeys-file "/etc/named.iscdlv.key";
managed-keys-directory "/var/named/dynamic";
pid-file "/run/named/named.pid";
session-keyfile "/run/named/session.key";
};
logging {
channel default_debug {
file "data/named.run";
severity dynamic;
};
};
zone "." IN {
type hint;
file "named.ca";
};
zone "unixmen.local" IN {
type master;
file "forward.unixmen";
allow-update { none; };
};
zone "1.168.192.in-addr.arpa" IN {
type master;
file "reverse.unixmen";
allow-update { none; };
};
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

** где **192.168.1.101** — IP-адрес нашего NS-сервера, на котором он будет принимать запросы; **allow-query** из соображений безопасности можно ограничить доступ для конкретной сети, например, вместо **any** написать **192.168.1.0/24**.*

Убедитесь, что все выставлено в точности так, как показано выше, а уже потом переходите к следующему шагу.

3. Создание прямой и обратной зоны

Для получения информации об источнике DNS-сервер использует прямые и обратные зоны. Прямая позволяет получать IP-адрес по имени хоста, а обратная через IP выдает до-

менное имя. Корректная работа каждой зоны должна быть обеспечена специальными правилами, созданием которых мы и предлагаем заняться далее.

3.1 Для прямой зоны создадим отдельный файл через тот же текстовый редактор. Тогда строка будет выглядеть так: sudo nano /var/named/forward.unixmen.

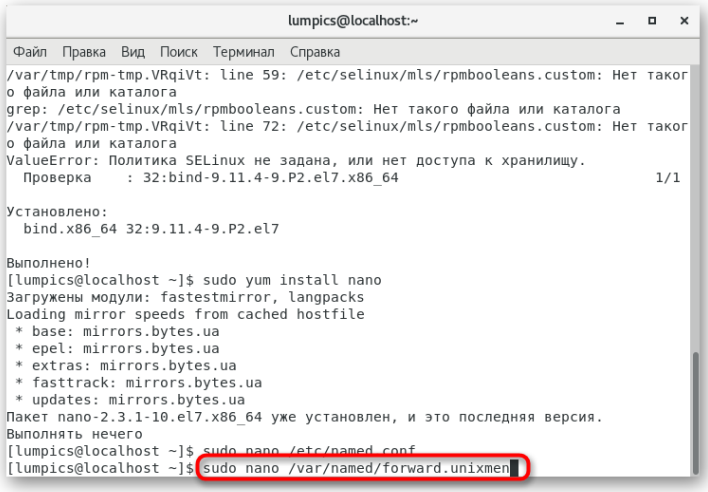


Рис. 280

3.2 Вы будете уведомлены о том, что это пустой объект. Вставьте туда указанное ниже содержимое:

```
$TTL 86400
@ IN SOA masterdns.unixmen.local. root.unixmen.local. (
2011071001 ;Serial
3600 ;Refresh
1800 ;Retry
604800 ;Expire
86400 ;Minimum TTL
)
@ IN NS masterdns.unixmen.local.
@ IN NS secondarydns.unixmen.local.
@ IN A 192.168.1.101
@ IN A 192.168.1.102
@ IN A 192.168.1.103
masterdns IN A 192.168.1.101
secondarydns IN A 192.168.1.102
client IN A 192.168.1.103
```

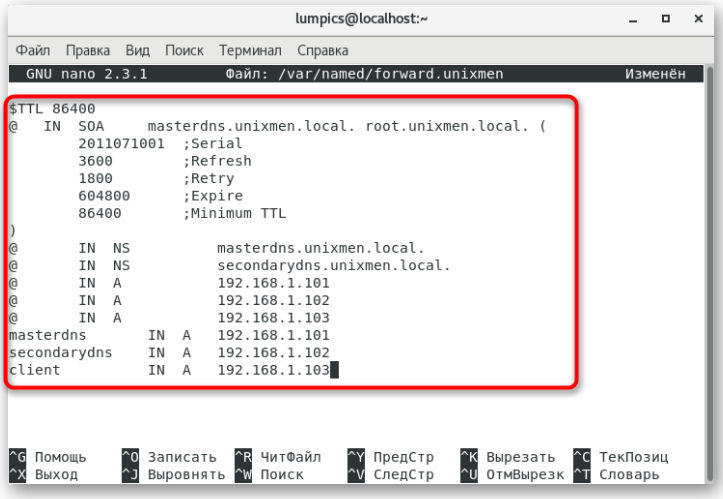


Рис. 281

3.3 Сохраните изменения и закройте текстовый редактор.

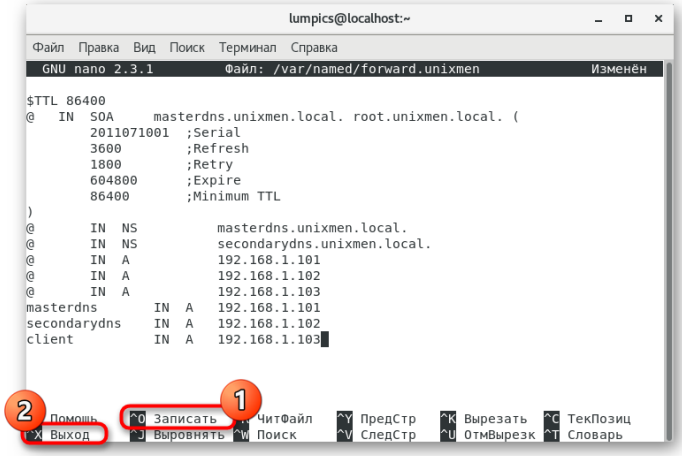


Рис. 282

3.4 Теперь перейдем к обратной зоне. Для нее требуется файл /var/named/reverse.unixmen.

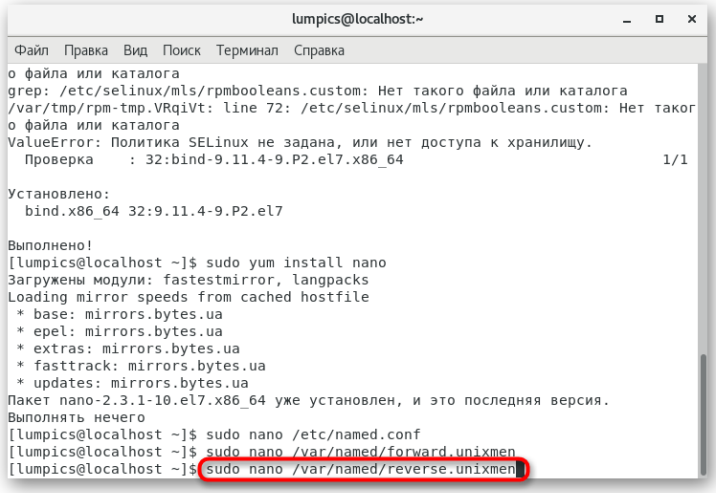


Рис. 283

3.5 Это тоже будет новый пустой файл. Вставьте туда:

$TTL 86400

@ IN SOA masterdns.unixmen.local. root.unixmen.local. (

2011071001 ;Serial
3600 ;Refresh
1800 ;Retry
604800 ;Expire
86400 ;Minimum TTL
)
@ IN NS masterdns.unixmen.local.
@ IN NS secondarydns.unixmen.local.
@ IN PTR unixmen.local.
masterdns IN A 192.168.1.101
secondarydns IN A 192.168.1.102
client IN A 192.168.1.103
101 IN PTR masterdns.unixmen.local.
102 IN PTR secondarydns.unixmen.local.
103 IN PTR client.unixmen.local.

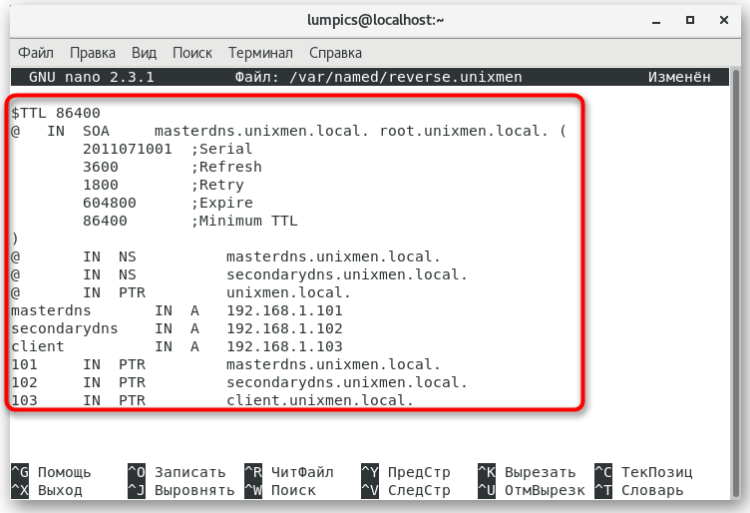


Рис. 284

3.6 При сохранении не изменяйте название объекта, а просто нажмите на клавишу **Enter**.

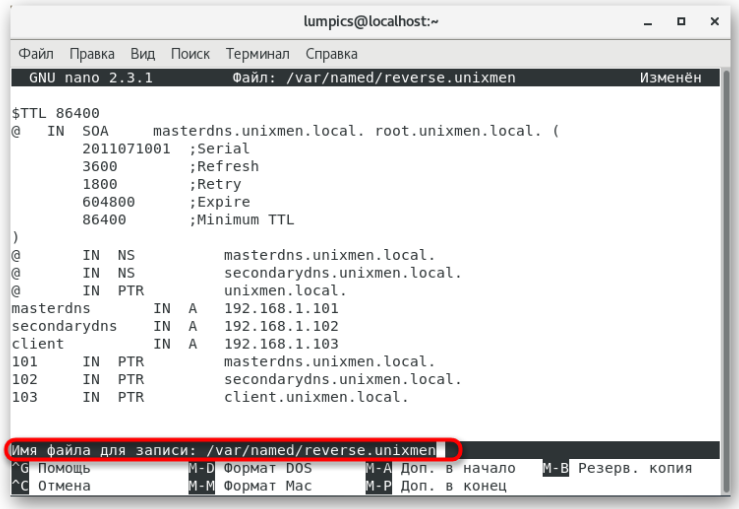


Рис. 285

Теперь указанные файлы будут использованы для прямой и обратной зоны. При необходимости следует редактировать именно их, чтобы изменить какие-то параметры. Об этом вы тоже можете прочесть в официальной документации.

4. Запуск DNS-сервера

После выполнения всех предыдущих указаний можно уже запустить DNS-сервер, чтобы в будущем легко проверить его работоспособность и продолжить настройку важных параметров. Осуществляется поставленная задача следующим образом:

4.1 В консоли введите sudo systemctl enable named, чтобы добавить DNS-сервер в автозагрузку для автоматического запуска при старте операционной системы.

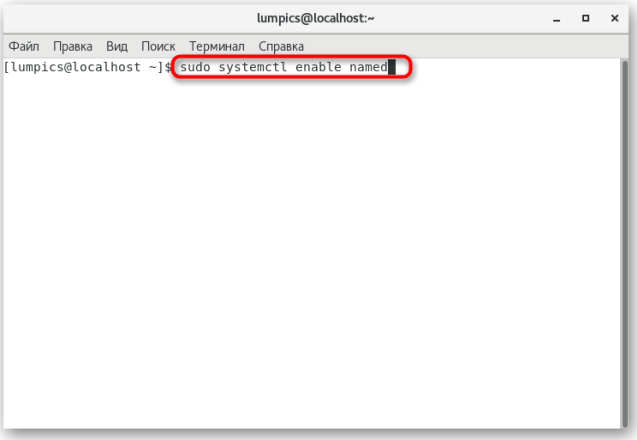


Рис. 286

4.2 Подтвердите это действие, введя пароль суперпользователя.

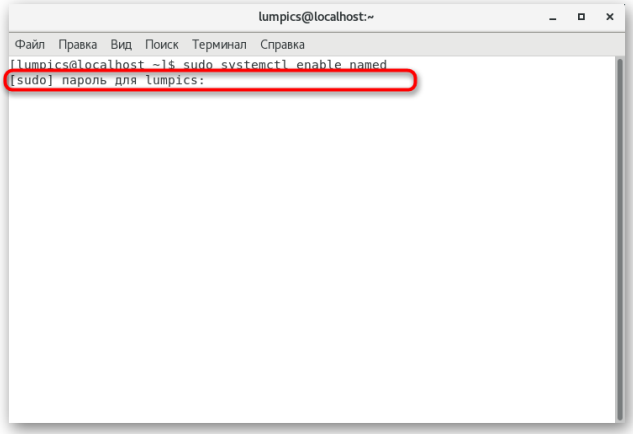


Рис. 287

4.3 Вы будете уведомлены о создании символической ссылки, а значит, действие выполнено успешно.

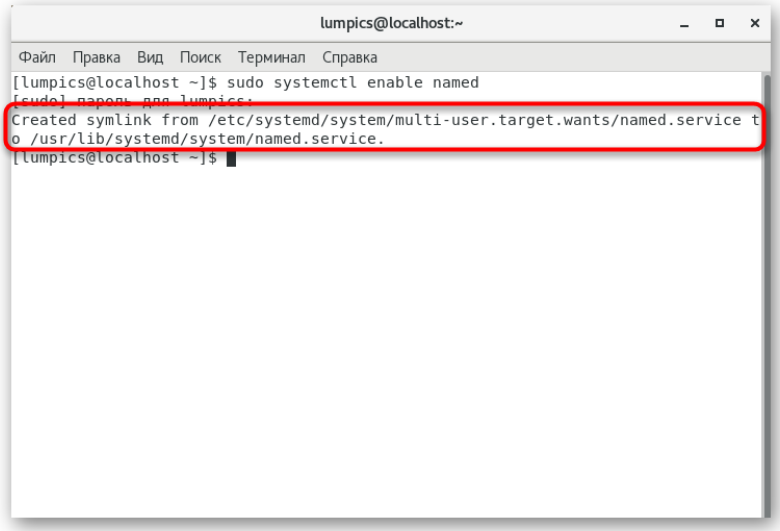


Рис. 288

4.4 Запустите утилиту через systemctl start named. Остановить ее можно так же, только заменив опцию **start** на stop.

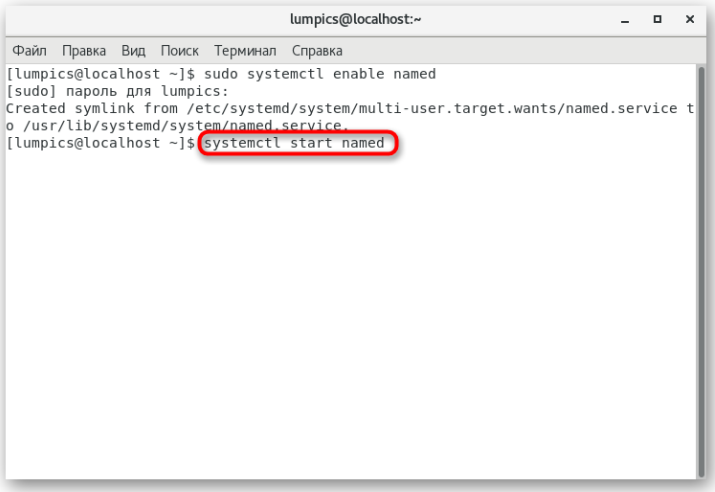


Рис. 289

4.5 При отображении всплывающего окна с подтверждением подлинности введите пароль от root.

5. Изменение параметров межсетевого экрана

Для корректного функционирования DNS-сервера потребуется открыть порт 53, что осуществляется через стандартный межсетевой экран FirewallD. В **«Терминале»** потребуется ввести всего три простых команды:

5.1. Первая имеет вид firewall-cmd --permanent --add-port=53/tcp и отвечает за открытие порта TCP-протокола. Вставьте ее в консоль и нажмите на **Enter**.

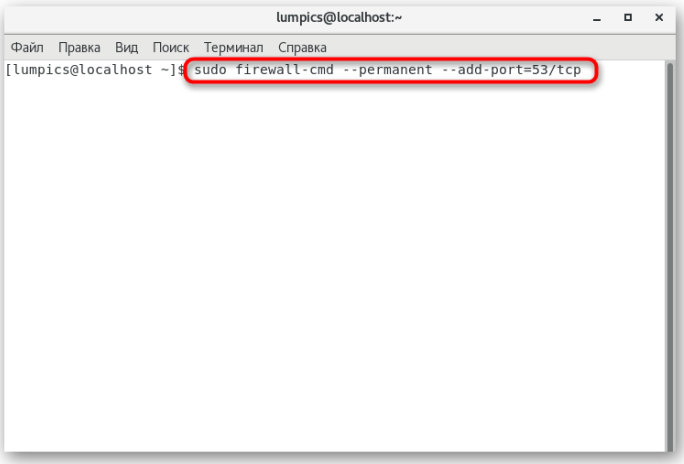


Рис. 290

5.2. Вы должны получить уведомление **«Success»**, что свидетельствует об успешном применении правила. После этого вставьте строку firewall-cmd --permanent --add-port=53/udp для открытия порта протокола UDP.

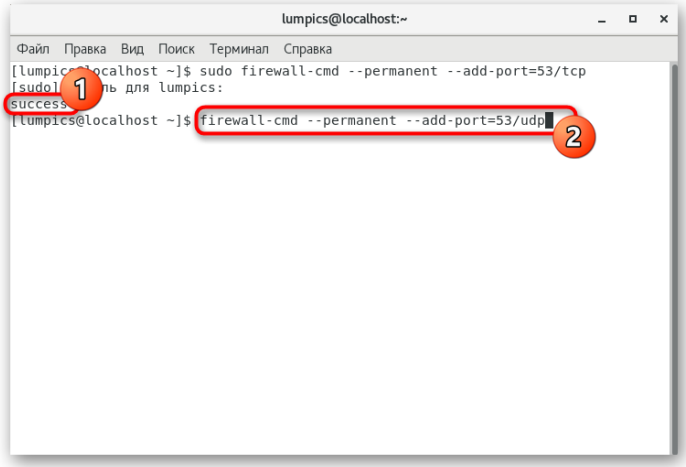


Рис. 291

5.3. Все изменения будут применены только после перезагрузки межсетевого экрана, что производится через команду firewall-cmd --reload.

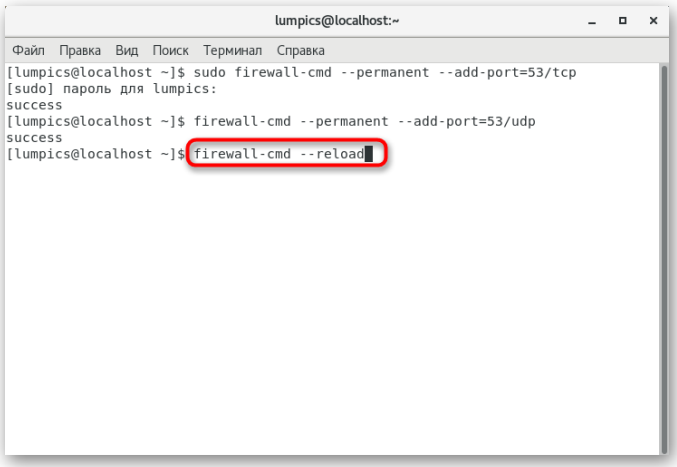


Рис. 292

Больше никаких изменений с брандмауэром производить не придется. Держите его постоянно во включенном состоянии, чтобы не возникло проблем с получением доступа.

6. Настройка прав доступа

Сейчас потребуется выставить основные разрешения и права доступа, чтобы немного обезопасить функционирование DNS-сервера и оградить обычных пользователей от возможности изменять параметры.

Все последующие команды должны быть активированными от имени суперпользователя. Чтобы постоянно не вводить пароль, советую включить перманентный рут-доступ для текущей терминальной сессии. Для этого в консоли введите su.

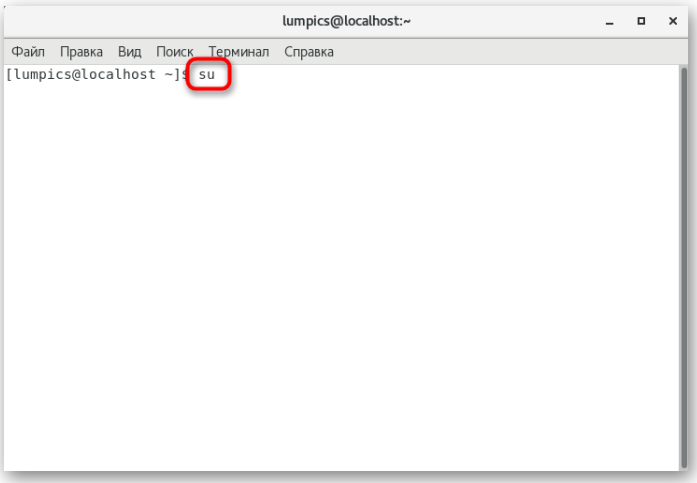


Рис. 293

6.1. Укажите пароль доступа.

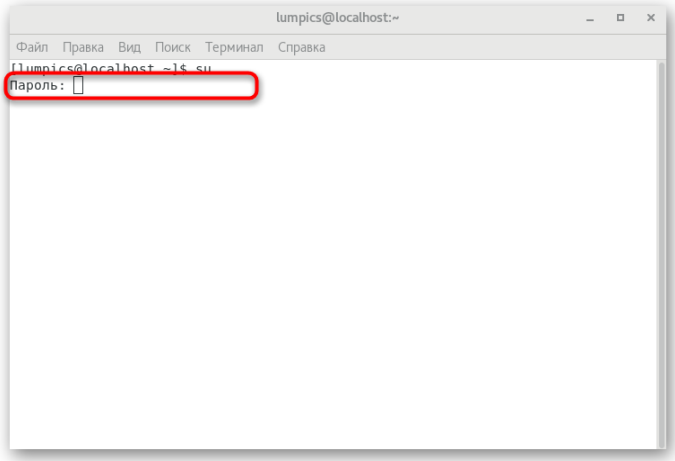


Рис. 294

6.2. После этого поочередно впишите указанные ниже команды, чтобы создать оптимальную настройку доступа:

```
chgrp named -R /var/named
chown -v root:named /etc/named.conf
restorecon -rv /var/named
restorecon /etc/named.conf
```

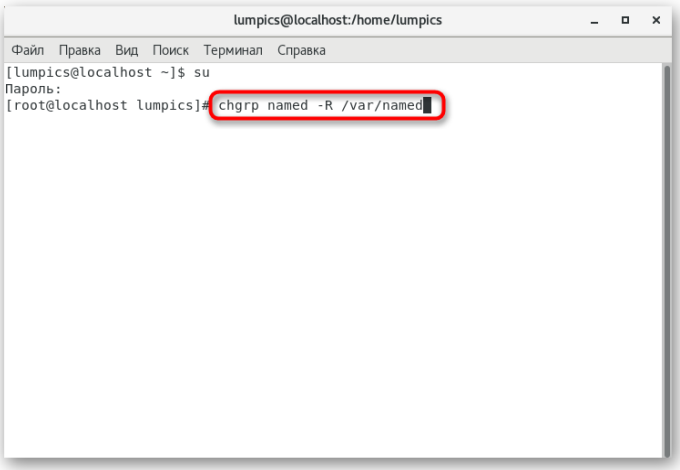


Рис. 295

На этом общая конфигурация главного DNS-сервера закончена. Осталось только отредактировать несколько конфигурационных файлов и произвести тестирование на ошибки. Со всем этим мы и предлагаем разобраться в следующем шаге.

7. Тестирование на ошибки и завершение настройки

Рекомендуем начать с проверок на ошибки, чтобы в будущем не пришлось менять и оставшиеся конфигурационные файлы. Именно поэтому мы и рассмотрим все это в пределах одного шага, а также приведем образцы правильного вывода команд для тестирования.

7.1. Введите в **«Терминале»** named-checkconf /etc/named.conf. Это позволит проверить глобальные параметры. Если в результате никакого вывода не последовало, значит, все настроено корректно. В противном случае изучите сообщение и, отталкиваясь от него, решите проблему.

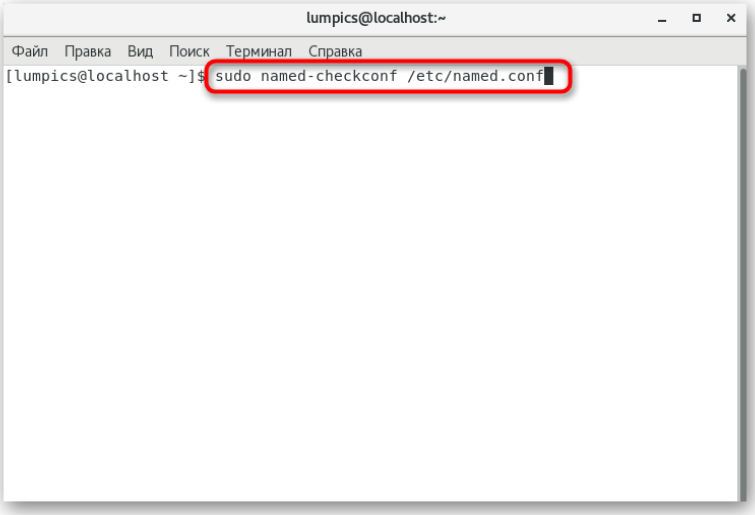


Рис. 296

7.2. Далее требуется проверить прямую зону, вставив строку named-checkzone unixmen.local /var/named/forward.unixmen.

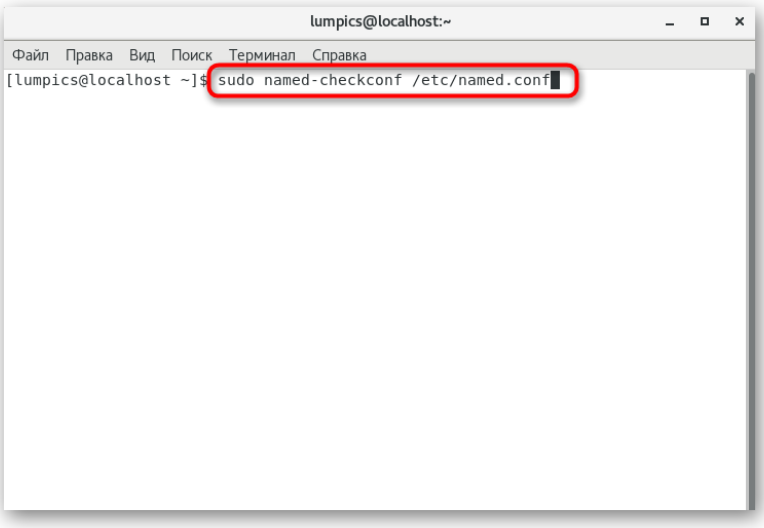


Рис. 297

7.3. Образец вывода выглядит следующим образом: zone unixmen.local/IN: loaded serial 2011071001 OK.

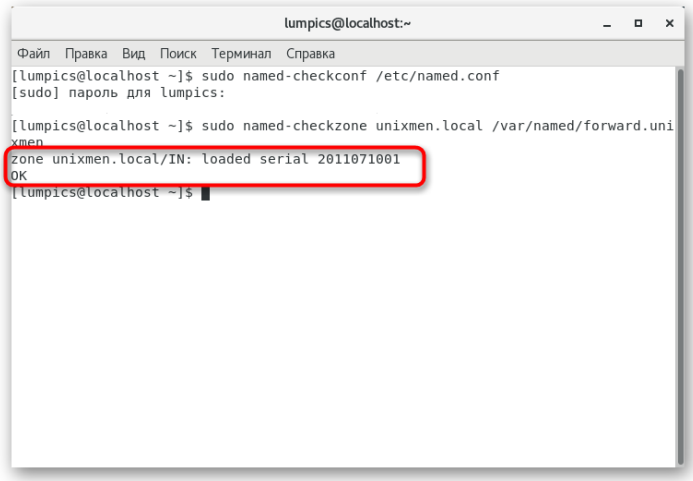


Рис. 298

7.4. Примерно то же самое осуществляем и с обратной зоной через named-checkzone unixmen.local /var/named/reverse.unixmen.

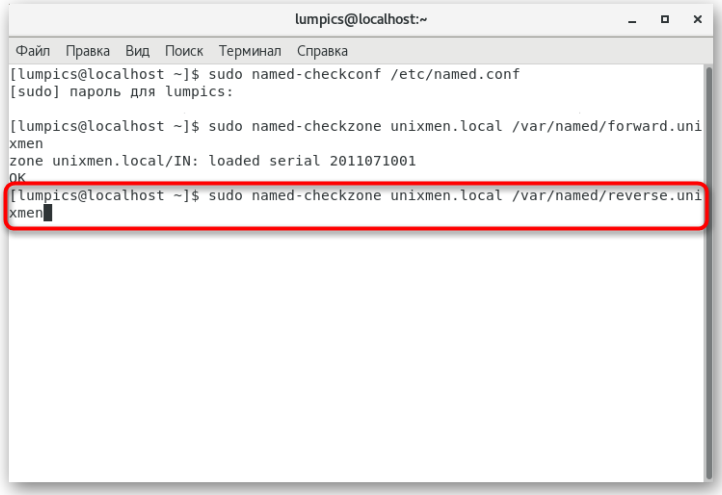


Рис. 299

7.5. Правильный вывод должен быть таким: zone unixmen.local/IN: loaded serial 2011071001 OK.

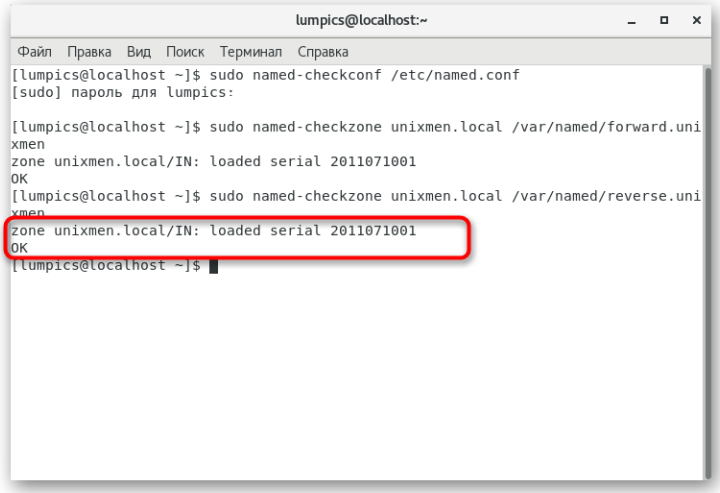


Рис. 300

7.6. Теперь перейдем к настройкам основного сетевого интерфейса. В него потребуется добавить данные текущего DNS-сервера. Для этого откройте файл /etc/sysconfig/network-scripts/ifcfg-enp0s3.

* enp0s3 – сетевой интерфейс в примере, у вас может отличаться.

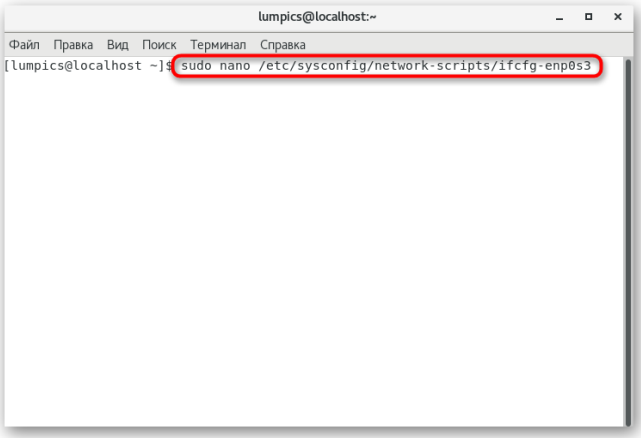


Рис. 301

7.7. Проверьте, чтобы содержимое было такое, как показано ниже. При необходимости вставьте параметры DNS.

```
TYPE="Ethernet"
BOOTPROTO="none"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
NAME="enp0s3"
UUID="5d0428b3-6af2-4f6b-9fe3-4250cd839efa"
ONBOOT="yes"
HWADDR="08:00:27:19:68:73"
IPADDR0="192.168.1.101"
PREFIX0="24"
```

```
GATEWAY0="192.168.1.1"
DNS="192.168.1.101"
IPV6_PEERDNS="yes"
IPV6_PEERROUTES="yes"
```

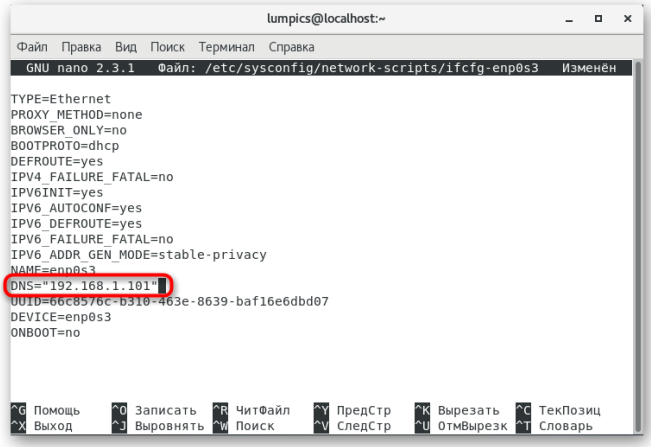


Рис. 302

7.8. После сохранения изменений переходите к файлу /etc/resolv.conf.

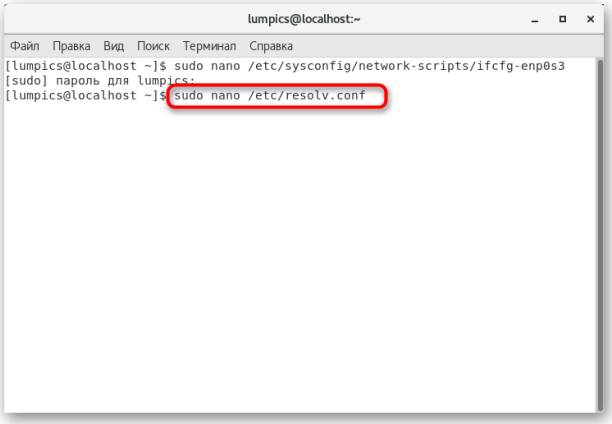


Рис. 303

7.9. Здесь нужно добавить всего одну строку: nameserver 192.168.1.101.

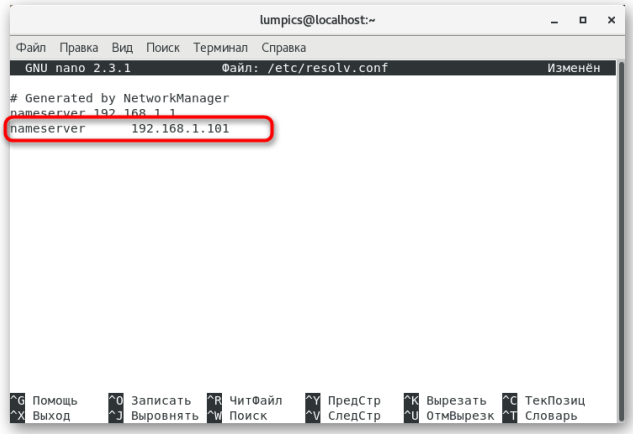


Рис. 304

7.10. По завершении остается только перезагрузить сеть или компьютер, чтобы обновить конфигурацию. Служба сети перезапускается через команду systemctl restart network.

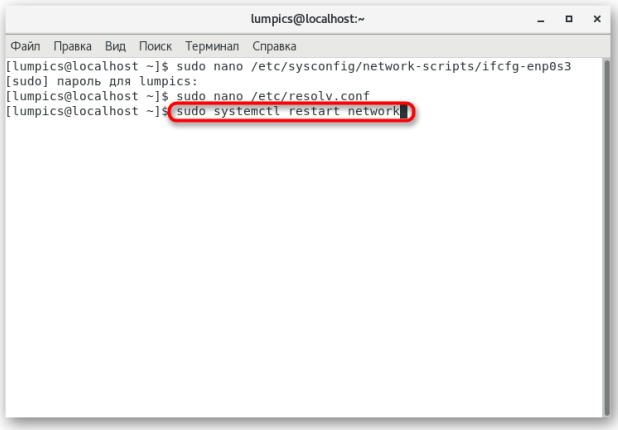


Рис. 305

8. Проверка установленного DNS-сервера

В завершении конфигурации остается только проверить работу имеющегося DNS-сервера после его добавления в глобальную службу сети. Эта операция так же выполняется при помощи специальных команд. Первая из них имеет вид dig masterdns.unixmen.local.

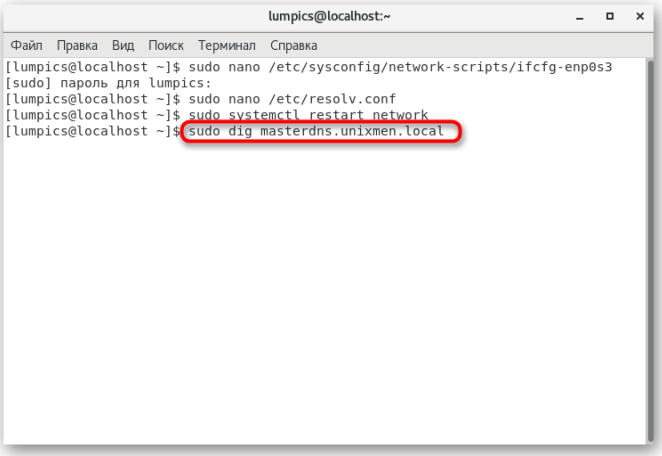


Рис. 306

В результате на экране должен появиться вывод, имеющий схожее представление с указанным ниже содержимым.

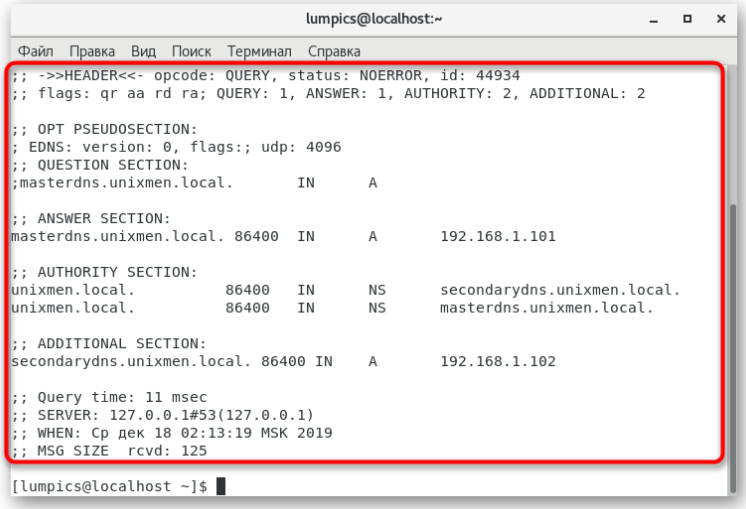


Рис. 307

```
; <> DiG 9.9.4-RedHat-9.9.4-14.el7 <> masterdns.unixmen.local
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25179
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;masterdns.unixmen.local. IN A
;; ANSWER SECTION:
masterdns.unixmen.local. 86400 IN A 192.168.1.101
;; AUTHORITY SECTION:
unixmen.local. 86400 IN NS secondarydns.unixmen.local.
unixmen.local. 86400 IN NS masterdns.unixmen.local.
;; ADDITIONAL SECTION:
secondarydns.unixmen.local. 86400 IN A 192.168.1.102
;; Query time: 0 msec
;; SERVER: 192.168.1.101#53(192.168.1.101)
;; WHEN: Wed Aug 20 16:20:46 IST 2014
;; MSG SIZE rcvd: 125
```

Дополнительная команда позволит узнать о состоянии локальной работы DNS-сервера. Для этого в консоль вставьте nslookup unixmen.local и нажмите на **Enter**.

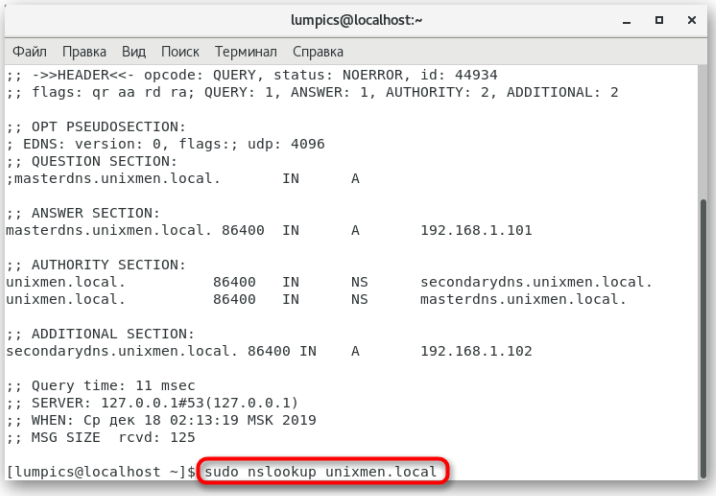


Рис. 308

В результате должно отобразиться три разных представления адресов IP и доменных имен.

```
Server: 192.168.1.101
Address: 192.168.1.101#53
Name: unixmen.local
Address: 192.168.1.103
Name: unixmen.local
Address: 192.168.1.101
Name: unixmen.local
Address: 192.168.1.102
```

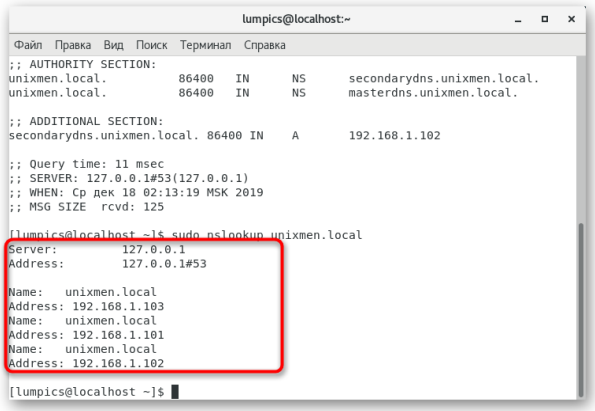


Рис. 309

Если вывод соответствует тому, который указан выше, значит, конфигурация завершена успешно и можно переходить к работе с клиентской частью DNS-сервера.

9. Настройка клиентской части DNS-сервера

Мы не будем разделять эту процедуру на отдельные шаги, поскольку она выполняется путем редактирования всего одного конфигурационного файла. В него необходимо добавить информацию обо всех клиентах, которые будут подключены к серверу, а пример такой настройки выглядит так:

9.1. Откройте файл /etc/resolv.conf через любой удобный текстовый редактор.

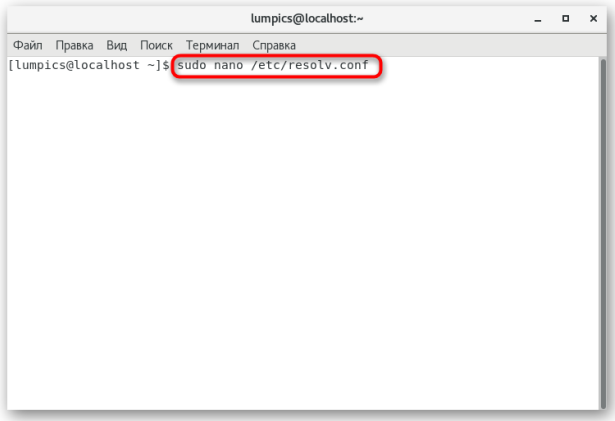


Рис. 310

9.2. Добавьте туда строки search unixmen.local nameserver 192.168.1.101 и nameserver 192.168.1.102, заменив необходимое на клиентские адреса.

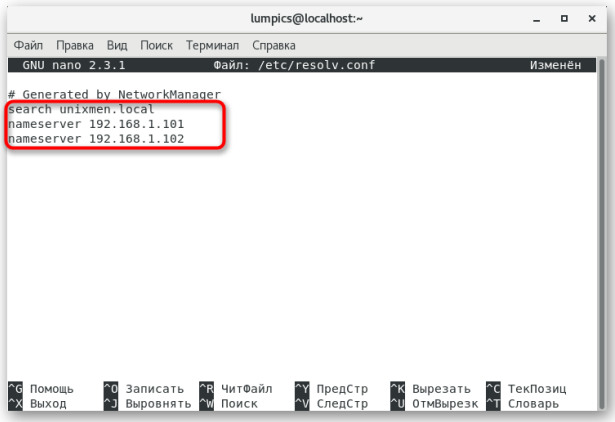


Рис. 311

9.3. При сохранении не изменяйте имя файла, а просто нажмите на клавишу **Enter**.

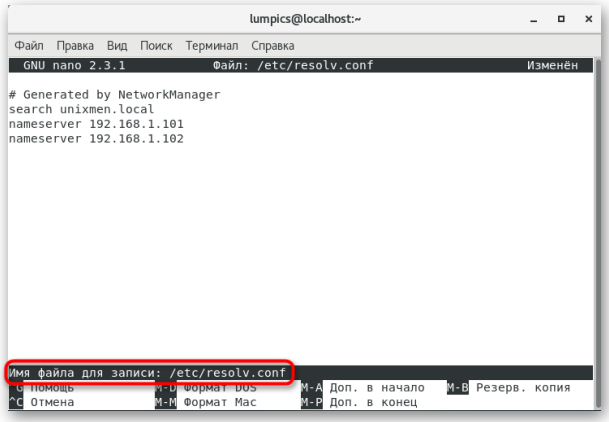


Рис. 312

9.4. После выхода из текстового редактора в обязательном порядке перезагрузите глобальную сеть через команду systemctl restart network.

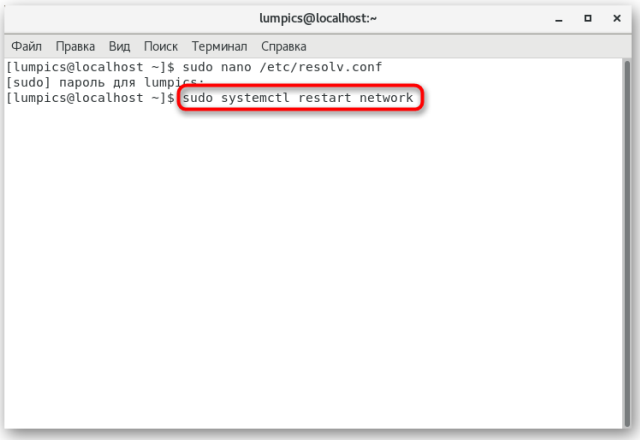


Рис. 313

10. Тестирование DNS-сервера

Последний этап нашего сегодняшнего материала — завершающее тестирование DNS-сервера. Ниже вы видите несколько команд, позволяющий справиться с поставленной задачей. Используйте одну из них, активировав через **«Терминал»**. Если в выводе не наблюдается никаких ошибок, следовательно, весь процесс выполнен верно.

dig masterdns.unixmen.local
dig secondarydns.unixmen.local
dig client.unixmen.local
nslookup unixmen.local

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

2.23. Практическая работа № 23 «Настройка сервера DHCP в CentOS»

Задание:

1. Устанавливаем DHCP:

```
dnf install dhcp-server
```

Теперь откроем на редактирование конфигурационный файл:

```
nano /etc/dhcp/dhcpd.conf
```

И внесем в него, примерно, следующее:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.200 192.168.0.250;
  option domain-name-servers 192.168.1.101, 192.168.1.102;
  option domain-name "wbsh.local";
  option routers 192.168.1.1;
  option broadcast-address 192.168.1.255;
  default-lease-time 600;
  max-lease-time 7200;
}
```

** где*

- ***subnet*** *обозначает сеть, в области которой будет работать данная группа настроек;*
- ***range*** *— диапазон, из которого будут браться IP-адреса;*
- ***option domain-name-servers*** *— через запятую перечисленные DNS-сервера;*
- ***option domain-name*** *— суффикс доменного имени;*
- ***option routers*** *— шлюз по умолчанию;*
- ***option broadcast-address*** *— адрес сети для широковещательных запросов;*
- ***default-lease-time***, ***max-lease-time*** *— время и максимальное время в секундах, на которое клиент получит адрес, по его истечению будет выполнено продление срока.*

*** все примеры настроек можно увидеть в файле* ***/usr/share/doc/dhcp*/dhcpd.conf.example*** *(вместо * будет версия установленного dhcp).*

Проверить корректность конфигурационного файла можно командой:

```
dhcpd -t -cf /etc/dhcp/dhcpd.conf
```

Разрешаем автозапуск сервиса:

```
systemctl enable dhcpd
```

и запускаем его:

```
systemctl start dhcpd
```

Добавляем правило в firewalld:

```
firewall-cmd --permanent --add-service=dhcp
firewall-cmd --reload
```

2. Определяем интерфейс для работы

Если в системе присутствует несколько сетевых адаптеров, а сервер DHCP должен работать только для определенных, открываем на редактирование следующий файл:

```
nano /etc/sysconfig/dhcpd
```

И добавляем в него следующее:

```
DHCPDARGS=ens32
```

** в данном примере сервер будет работать только для интерфейса* ***ens32****.*

Перезапускаем сервис:

```
systemctl restart dhcp
```

3. Резервирование IP

Резервирование создается по MAC-адресу сетевого адаптера.

Пример настройки dhcpd.conf:

```
nano /etc/dhcp/dhcpd.conf
```

```
host host1 {
   hardware ethernet 28:10:7B:27:C2:A0; fixed-address 192.168.1.201;
}
host host2 {
   hardware ethernet 28:10:7B:27:C2:A1; fixed-address 192.168.1.202;
}
```

** где **host1** — имя узла, для когорого резервируем адрес (не обязательно должен совпадать с реальным); **28:10:7B:27:C2:A0** — mac-адрес; **192.168.1.201** — IP, который будет назначать узлу. Аналогичо, для второго узла.*

4. Подключение конфигурационных файлов

Для удобства, некоторые блоки с настройками можно вынести в отдельные файлы и подключить их в основном конфигурационном файле:

```
nano /etc/dhcp/dhcpd.conf
```

```
include "/etc/dhcp/conf.d/subnets.conf";
```

Список арендованных адресов

Для просмотра списка адресов, которые были выданы DHCP-сервером вводим команду:

```
cat /var/lib/dhcpd/dhcpd.leases
```

5. Настройка логов

По умолчанию, сервер dhcp ведет лог в файле /var/log/messages, что не очень удобно, так как это общий лог-файл, в котором может находиться много записей.

Для того, чтобы сервер сохранял записи в отдельный файл, открываем на редактирование rsyslog.conf:

```
nano /etc/rsyslog.conf
```

И добавляем следующее:

```
local6.*/var/log/dhcp.log
```

Далее открываем конфигурационный файл dhcp:

```
nano /etc/dhcp/dhcpd.conf
```

И добавляем:

```
log-facility local6;
```

Перезапускаем сервисы:

```
systemctl restart dhcpd
systemctl restart rsyslog
```

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

2.24. Практическая работа № 24 «Установка и настройка OpenVPN»

Задание:

1. Подготовка операционной системы

Мы внесем небольшие правки в настройки. Настроим время для правильного формирования клиентских сертификатов, отключим систему безопасности SELinux, откроем нужные порты брандмауэра.

1.1 Настройка времени

Установим правильную временную зону:

```
\cp /usr/share/zoneinfo/Europe/Moscow /etc/localtime
```

** в данном примере мы укажем московское время.*

Устанавливаем утилиту для синхронизации времени:

```
dnf install chrony
```

Разрешаем автозапуск службы chronyd и запускаем ее:

```
systemctl enable chronyd
systemctl start chronyd
```

Проверить корректность времени можно командой:

```
date
```

1.2 Настройка SELinux

В нашей инструкции мы просто отключим SELinux. Если необходимо его настроить и оставить включенным, используем инструкцию Настройка SELinux в CentOS 7 (для CentOS 8 она также подходит).

И так, отключаем Selinux командой:

```
setenforce 0
```

Чтобы Selinux не включился после перезагрузки, открываем на редактирование файл:

```
nano /etc/selinux/config
```

... и редактируем опцию *SELINUX*:

```
...
SELINUX=disabled
...
```

1.3 Настройка брандмауэра

Создаем правило для firewalld:

```
firewall-cmd --permanent --add-port=443/udp
```

** в данной инструкции мы настроим работу OpenVPN на порту **443** по **UDP**. Если в вашем случае необходим другие порт и протокол, меняем значения на соответствующие.*

Применяем настройку:

```
firewall-cmd --reload
```

1.4 Установка и создание сертификатов

Использование сертификатов является обязательным условием при использовании VPN. Поэтому сразу после установки мы создадим все необходимые ключи.

2. Установка OpenVPN

Устанавливаем репозиторий epel:

```
dnf install epel-release
```

Устанавливаем необходимые пакеты следующей командой:

```
dnf install openvpn easy-rsa
```

2.1 Создание сертификатов

Переходим в каталог easy-rsa:

```
cd /usr/share/easy-rsa/3
```

** в зависимости от версии easy-rsa, последний каталог может быть другим. Увидеть точное название каталога можно командой **ls /usr/share/easy-rsa/**.*

Чтобы упростить и ускорить процесс создания ключей, создаем следующий файл:

```
nano vars
```

```
export KEY_COUNTRY="RU"
export KEY_PROVINCE="Sankt-Petersburg"
export KEY_CITY="Sankt-Petersburg"
export KEY_ORG="DMOSK COMPANY"
export KEY_EMAIL="master@dmosk.ru"
export KEY_CN="DMOSK"
export KEY_OU="DMOSK"
export KEY_NAME="name-openvpn-server.dmosk.ru"
export KEY_ALTNAMES="name-openvpn-server"
```

** где **KEY_CN** и **KEY_OU**: рабочие подразделения (например, можно указать название отдела); **KEY_NAME**: адрес, по которому будет выполняться подключение (можно указать полное наименование сервера); **KEY_ALTNAMES** — альтернативный адрес.*

** так как мы генерируем самоподписный сертификат, значения данных полей никак не повлияют на работу OpenVPN, однако, для удобства, лучше подставить реальные данные.*

Справка: когда клиенты подключаются к OpenVPN, они используют асимметричное шифрование (также известное как открытый/закрытый ключ) для выполнения TLS-рукопожатия. Однако при передаче шифрованного VPN-трафика сервер и клиенты используют симметричное шифрование, которое также известно как шифрование общедоступного ключа.

Симметричное шифрование требует гораздо меньшего количества вычислений по сравнению с асимметричным: используемые числа гораздо меньше, и современные процессоры имеют инструкции для выполнения оптимизированного симметричного шифрования. Для переключения с асимметричного на симметричное шифрование сервер OpenVPN и клиент будут использовать алгоритм Диффи — Хеллмана на эллиптических кривых для согласования общего секретного ключа в максимально короткие сроки.

Запускаем созданный файл на исполнение:

```
. ./vars
```

2.2 Генерация ключей

Инициализируем PKI:

```
./easyrsa init-pki
```

Мы должны увидеть:

```
init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /usr/share/easy-rsa/3/pki
```

... а в текущем каталоге появится папка pki.

Генерируем корневой сертификат (CA):

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

... после ввода **Enter** обязательно задаем пароль дважды. На запрос ввести **Common Name** можно просто нажать ввод или написать свое имя:

```
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:
```

Создаем ключ Диффи-Хеллмана:

```
./easyrsa gen-dh
```

Для создания сертификата сервера необходимо сначала создать файл запроса:

```
./easyrsa gen-req vpn-server nopass
```

** на запрос ввода **Common Name** просто вводим **Enter**, чтобы использовать настройку из файла vars; **nopass** можно упустить, если хотим повысить безопасность с помощью пароля на сертификат.*

... и на его основе — сам сертификат:

```
./easyrsa sign-req server vpn-server
```

После ввода команды подтверждаем правильность данных, введя **yes:**

```
Confirm request details: yes
```

... и вводим пароль, который указывали при создании корневого сертификата.

Для создания ta ключа используем команду:

```
openvpn --genkey --secret pki/ta.key
```

Сертификаты сервера готовы и находятся в каталоге **pki.**

Создаем каталог в /etc/openvpn, в котором будем хранить сертификаты:

```
mkdir -p /etc/openvpn/server/keys
```

Переходим в каталог pki:

```
cd pki
```

Копируем в него необходимые сертификаты:

```
cp ca.crt issued/vpn-server.crt private/vpn-server.key dh.pem ta.key /etc/openvpn/server/keys/
```

3. Настройка и запуск сервера

Создаем конфигурационный файл для сервера openvpn:

```
nano /etc/openvpn/server/server.conf
```

И вставляем в него следующее:

```
local 192.168.0.15
port 443
proto udp
dev tun
ca keys/ca.crt
cert keys/vpn-server.crt
key keys/vpn-server.key
dh keys/dh.pem
tls-auth keys/ta.key 0
server 172.16.10.0 255.255.255.0
ifconfig-pool-persist ipp.txt
keepalive 10 120
max-clients 32
persist-key
persist-tun
status /var/log/openvpn/openvpn-status.log
log-append /var/log/openvpn/openvpn.log
verb 0
mute 20
```

```
daemon
mode server
tls-server
comp-lzo no
```

** где из всех параметров, обязательно, внести изменения нужно в следующие — **local**: IP-адрес, на котором будет обрабатывать запросы OpenVPN; **port**: сетевой порт (443 позволит избежать проблем при использовании Интернета в общественных местах, но может быть уже занят в вашей системе — посмотреть список используемых портов можно командой **ss -tunlp**. Если порт занят, используйте любой из свободных, например 1194).*

Создаем каталог для логов сервера:

```
mkdir /var/log/openvpn
```

Разрешаем автоматический старт сервиса vpn:

```
systemctl enable openvpn-server@server
```

И запускаем его:

```
systemctl start openvpn-server@server
```

4. Настройка OpenVPN-клиента

Для настройки клиента необходимо на сервере сгенерировать сертификаты, а на клиентском компьютере установить программу openvpn и настроить ее.

5. Создание сертификатов

На сервере генерируем сертификаты для клиента. Для этого снова переходим в каталог easy-rsa:

```
cd /usr/share/easy-rsa/3
```

Запускаем еще раз vars:

```
. ./vars
```

Создаем клиентский сертификат:

```
./easyrsa gen-req client1 nopass
./easyrsa sign-req client client1
```

Мы должны увидеть запрос на подтверждение намерения выпустить сертификат — вводим **yes**:

```
Confirm request details: yes
```

** в данном примере будет создан сертификат для **client1**.*

На сервере скопируем ключи во временную директорию, выполнив последовательно 3 команды:

```
mkdir /tmp/keys
cp pki/issued/client1.crt pki/private/client1.key pki/dh.pem pki/ca.crt pki/ta.key /tmp/keys
chmod -R a+r /tmp/keys
```

** сертификаты скопированы в каталог **/tmp** для удобства переноса их на клиентский компьютер.*

Сертификаты готовы для скачивания.

6. На клиенте

В качестве примера, выполним подключение к нашему серверу с компьютера Windows. Пошагово, выполняем следующие действия:

Заходим на официальную страницу загрузки openvpn и скачиваем клиента для Windows:

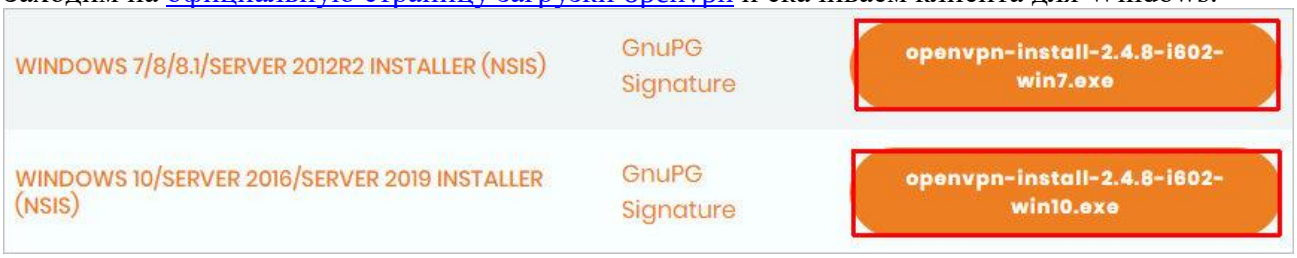


Рис. 314

Запускаем скачанный файл и устанавливаем программу, нажимая «Далее».

Переходим в папку *C:\Program Files\OpenVPN\config*.

Копируем в нее файлы ca.crt, client1.crt, client1.key, dh.pem, ta.key из каталога /tmp/keys на сервере, например, при помощи программы WinSCP.

После переноса файлов, не забываем удалить ключи из временного каталога на сервере:

```
rm -R /tmp/keys
```

Возвращаемся к компьютеру с Windows, открываем блокнот от имени администратора и вставляем следующие строки:

```
client
resolv-retry infinite
nobind
remote 192.168.0.15 443
proto udp
dev tun
comp-lzo no
ca ca.crt
cert client1.crt
key client1.key
dh dh.pem
tls-client
tls-auth ta.key 1
float
keepalive 10 120
persist-key
persist-tun
verb 0
```

** где **192.168.0.15 443** — IP-адрес OpenVPN-сервера и порт, на котором он принимает запросы.*

Сохраняем файл с именем **config.ovpn** в папке *C:\Program Files\OpenVPN\config*.

Запускаем с рабочего стола программу «OpenVPN GUI» от имени администратора.

Нажимаем правой кнопкой по появившемуся в трее значку и выбираем «Подключиться»:

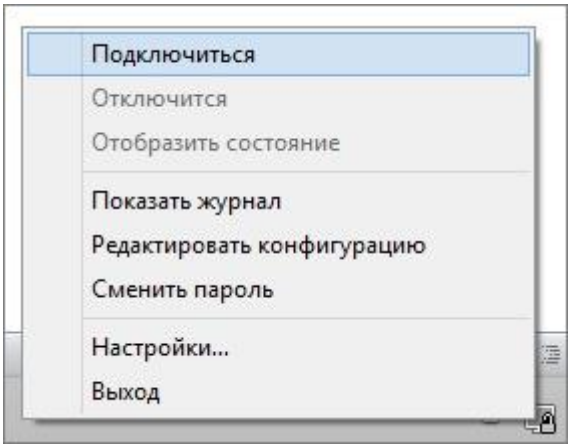


Рис. 315

Произойдет подключение и значок поменяет цвет с серого/желтого на зеленый.

Для автозапуска клиента, открываем службы Windows, находим и настраиваем службу OpenVPNService для автозапуска:

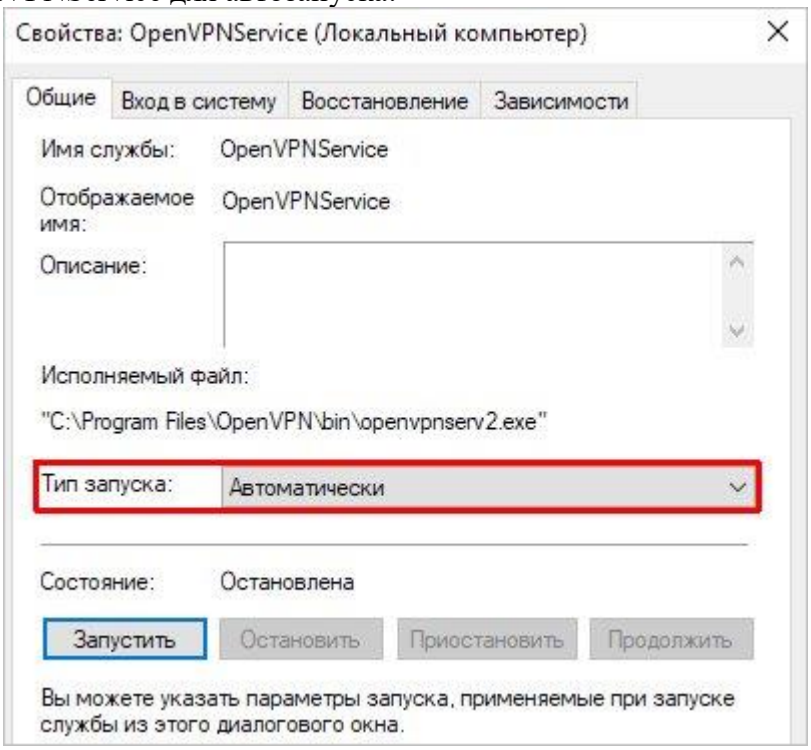


Рис. 316

7. Аутентификация пользователей

Мы можем настроить проверку пользователя по логину и паролю. Это даст дополнительный уровень защиты, а также позволит использовать один и тот же сертификат для всех подключений.

8. Настройка сервера

Открываем конфигурационный файл openvpn:

```
nano /etc/openvpn/server/server.conf
```

И добавляем следующие строчки:

```
username-as-common-name
plugin /usr/lib64/openvpn/plugins/openvpn-plugin-auth-pam.so login
```

** где **username-as-common-name** указывает на то, что openvpn должен использовать логины, как основные идентификаторы клиента; **plugin** указывает на путь к самому плаги-*

ну и для чего он используется.

** как путь, так и название файла **openvpn-plugin-auth-pam.so** могут отличаться. Это зависит от версии Linux и OpenVPN. Чтобы найти путь до нужного файла, можно воспользоваться командой **find / -name "openvpn-*auth-pam*" -print**.*

Перезапускаем сервер:

```
systemctl restart openvpn-server@server
```

При необходимости, создаем учетную запись для авторизации:

```
useradd vpn1 -s /sbin/nologin
```

И задаем ей пароль:

```
passwd vpn1
```

9. Настройка на клиенте

В конфигурационный файл клиента добавляем:

```
auth-user-pass
```

Теперь при подключении программа будет запрашивать логин и пароль.

Вход без ввода пароля (сохранение пароля)

Если необходимо настроить авторизацию, но автоматизировать вход клиента, открываем конфигурационный файл последнего и строку для авторизации меняем на:

```
auth-user-pass auth.txt
```

** где **auth.txt** — файл, в котором мы будем хранить логин и пароль.*

Создаем текстовый файл auth.txt в той же папке, где находится файл конфигурации со следующим содержимым:

```
username
password
```

** где **username** — логин пользователя, а **password** — пароль.*

Переподключаем клиента.

Описанный метод аутентификации является базовым и требует наличие обычной системной учетной записи. Если необходима более сложная авторизация на базе LDAP, можно воспользоваться инструкцией настройка OpenVPN сервера с аутентификацией через LDAP (написана на базе Linux Ubuntu).

10. Отзыв сертификата

В случае, когда необходимо прекратить действие определенного сертификата, можно его отозвать (revoke). Чтобы настроить отзыв сертификата в OpenVPN, нужно указать файл для проверки отозванных сертификатов, затем отозвать сам сертификат.

11. Настройка OpenVPN

Открываем конфигурационный файл:

```
nano /etc/openvpn/server/server.conf
```

Добавляем строку:

```
...
crl-verify keys/crl.pem
```

** в данном примере, сервер будет проверять список отозванных сертификатов в файле **keys/crl.pem**.*

12. Отзыв сертификата

В нашем примере мы создали сертификат client1 — сделаем его отзыв. Переходим в каталог:

```
cd /usr/share/easy-rsa/3
```

Отзываем сертификат командой:

```
./easyrsa revoke client1
```

** здесь мы отзываем сертификат для клиента **client1**.*

Подтверждаем наши намерения:

```
  Continue with revocation: yes
```

... и вводим пароль для центра сертификации.

После этого создаем/обновляем файл crl.pem:

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

** необходимо будет ввести пароль центра сертификации.*

Копируем файл crl.pem в каталог openvpn:

```
cp pki/crl.pem /etc/openvpn/server/keys/
```

После перезагружаем сервис openvpn:

```
systemctl restart openvpn-server@server
```

13. Доступ клиентам друг к другу

Ранее мы настроили более безопасный сценарий подключения — туннели, которые не позволяют подключенным клиентам видеть друг друга. Но если мы хотим сделать так, чтобы все подключенные к VPN устройства видели друг друга по сети, нам нужно изменить некоторые настройки на сервере и клиенте.

14. Настройка сервера

Открываем файл настроек:

```
nano /etc/openvpn/server/server.conf
```

Добавляем строку:

```
client-to-client
```

** данная настройка как раз и говорит, что клиенты могут видеть друг друга через нашу сеть VPN.*

Теперь находим настройку:

```
dev tun
```

... и меняем ее на:

```
dev tap
```

** туннели создают небольшие подсети на 4 адреса для каждого подключения, таким образом, изолируя клиентов друг от друга. Нам же нужно сделать так, чтобы клиенты были в одной сети VPN. Поэтому мы меняем тип интерфейса на **tap**.*

Перезапускаем нашу службу сервиса:

```
systemctl restart openvpn-server@server
```

15. Настройка клиента

На клиенте нам нужно изменить только тип сетевого интерфейса на tap:

```
dev tap
```

После можно подключаться к серверу.

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

2.25. Практическая работа № 25 «Применение протокола IP-sec и SSH.»

Задание:

1. Подготовка сервера

Для установки ПО потребуется репозиторий EPEL:

```
dnf install epel-release
```

Настраиваем брандмауэр:

```
firewall-cmd --permanent --add-port=1701/{tcp,udp}
firewall-cmd --permanent --add-service=ipsec
firewall-cmd --reload
```

Отключаем SELinux:

```
setenforce 0
sed -i 's/^SELINUX=.*/SELINUX=disabled/g' /etc/selinux/config
```

2. Настройка VPN-сервера

Для настройки нашего сервера мы настроим следующие компоненты: IPSEC (strongswan), L2TP (xl2tpd), PPP.

3. IPSEC

Для управления IPSec используется пакет strongswan — установим его командой:

```
dnf install strongswan
```

Открываем конфигурационный файл для настройки ipsec:

```
nano /etc/strongswan/ipsec.conf
```

Для **config setup** добавим:

```
config setup
   nat_traversal=yes
   virtual_private=%v4:10.0.0.0/8,%v4:192.168.0.0/16,%v4:172.16.0.0/12
   oe=off
   protostack=netkey
```

* *где:*

- ***nat_traversal*** *— обход NAT.*
- ***virtual_private*** *— определяет приватные сети. В данном примере просто перечислены сети, зарезервированные под локальные — мы можем указать и другие.*
- ***oe*** *— <не смог найти описание данного параметра>.*
- ***protostack*** *— определяет стек протоколов, который будет использоваться для подключения.*

... а также вставляем ниже:

```
conn L2TP-PSK-NAT
   rightsubnet=vhost:%priv
   also=L2TP-PSK-noNAT
```

```
conn L2TP-PSK-noNAT
   authby=secret
   pfs=no
   auto=add
   keyingtries=3
   rekey=no
   ikelifetime=8h
   keylife=1h
   type=transport
   left=%any
   leftprotoport=udp/1701
   right=%any
   rightprotoport=udp/%any
   ike=aes128-sha1-modp1536,aes128-sha1-modp1024,aes128-md5-modp1536,aes128-md5-
modp1024,3des-sha1-modp1536,3des-sha1-modp1024,3des-md5-modp1536,3des-md5-
modp1024
   esp=aes128-sha1-modp1536,aes128-sha1-modp1024,aes128-md5-modp1536,aes128-md5-
modp1024,3des-sha1-modp1536,3des-sha1-modp1024,3des-md5-modp1536,3des-md5-
modp1024
```

** где:*

- ***authby*** *— способы аутентификации двух узлов. Возможны варианты secret (по паролю) или rsasig (цифровые подписи RSA).*
- ***pfs*** *— расшифровывается как Perfect Forward Secrecy. Позволяет активировать совершенную секретность в канале ключей соединения.*
- ***auto*** *— операция, которая должна запуститься автоматически при старте IPsec.*
- ***keyingtries*** *— число попыток, чтобы «договориться» о соединении или его замене.*
- ***rekey*** *— перепроверить соединение, когда оно истекает.*
- ***ikelifetime*** *— время соединения до повторного согласования ISAKMP или IKE SA.*
- ***keylife*** *— как долго должен длиться конкретный экземпляр соединения.*
- ***type*** *— тип соединения. Возможны варианты tunnel (хост-хост, хост-подсеть или подсеть-подсеть); transport (хост-хост); passthrough (без обработки IPsec).*
- ***left*** *— IP-адрес левого участника (сервера). %any означает, что адрес может быть любой.*
- ***leftprotoport*** *— определяет протокол и порт, на котором будет работать левая сторона (сервер). В данном примере указан UDP и порт 1701.*
- ***right*** *— IP-адрес правого участника (клиента). %any означает, что адрес может быть любой.*
- ***rightprotoport*** *— определяет протокол и порт, на котором будет работать правая сторона (клиент). В данном примере указан UDP и любой порт.*

Создаем секретный ключ — для этого открываем на редактирование файл:

```
nano /etc/strongswan/ipsec.secrets
```

... и добавляем:

```
%any %any : PSK "my_key_password"
```

** в данном примере мы устанавливаем общий пароль **my_key_password** для соединений с любого IP.*

Разрешаем автозапуск strongswan и перезапускаем службу:

```
systemctl enable strongswan
systemctl restart strongswan
```

4. L2TP

Устанавливаем сервер L2TP:

```
dnf install xl2tpd
```

Открываем файл настройки сервера:

```
nano /etc/xl2tpd/xl2tpd.conf
```

Для раздела **[global]** добавляем:

```
[global]
port = 1701
access control = no
ipsec saref = yes
force userspace = yes
auth file = /etc/ppp/chap-secrets
```

где:

- ***port** — порт UDP, на котором работает VPN. По умолчанию, 1701.*
- ***access control** — принимать или нет запросы только от клиентов с определенными IP, перечисленными в настройках клиентов.*
- ***ipsec saref** — указывает использовать или нет ipsec Security Association, позволяющий отслеживать несколько клиентов с одинаковыми IP-адресами.*
- ***force userspace** — повышает производительность за счет декапсуляции пакетов L2TP.*
- ***auth file** — путь к файлу аутентификации.*

Раздел **[lns default]** можно полностью удалить или закомментировать (символом «;») и заменить на:

```
[lns default]
ip range = 176.16.10.10-176.16.10.200
local ip = 176.16.10.1
require authentication = yes
name = l2tp
pass peer = yes
ppp debug = no
pppoptfile = /etc/ppp/options.xl2tpd
length bit = yes
refuse pap = yes
```

где:

- ***ip range** — диапазон адресов, которые назначаются подключенным клиентам.*
- ***local ip** — IP-адрес сервера в сети VPN.*

- ***name*** *— имя сервера для процесса согласования.*
- ***pppoptfile*** *— путь к файлу с настройкой pppd.*
- ***flow bit*** *— позволяет добавлять в пакеты порядковые номера.*
- ***exclusive*** *— если поставить в yes, сервер разрешит только одно соединение с клиентом.*
- ***hidden bit*** *— скрывать или нет AVP.*
- ***length bit*** *— использовать ли бит длины, указывающий полезную нагрузку.*
- ***require authentication*** *— требовать ли аутентификацию.*
- ***require chap*** *— требовать ли аутентификацию PPP по протоколу CHAP.*
- ***refuse pap*** *— отказывать ли авторизацию пирам, использующим PAP.*

Разрешаем автозапуск vpn-сервера и перезапускаем его:

```
systemctl enable xl2tpd
systemctl restart xl2tpd
```

5. PPP

Открываем на редактирование конфигурационный файл:

```
nano /etc/ppp/options.xl2tpd
```

Можно закомментировать все, что там есть и вставить:

```
ipcp-accept-local
ipcp-accept-remote
auth
idle 1800
mtu 1200
mru 1200
nodefaultroute
lock
proxyarp
connect-delay 5000
name l2tpd
login
ms-dns 77.88.8.8
ms-dns 8.8.8.8
require-mschap-v2
```

Создаем пользователя. Для этого открываем файл:

```
nano /etc/ppp/chap-secrets
```

И добавляем:

```
user1 * password1 172.16.10.10
user2 * password2 *
user3 l2tpserver password2 *
```

** формат записи — <логин> <имя сервиса> <пароль> <IP клиента (не обязательно)>. Первая учетная запись может подключаться к любому VPN и только с IP* ***172.16.10.10****, вторая — к любому VPN с любого IP, третья — к серверу* ***l2tpserver****, но с любого IP.*

Перезапускаем xl2tpd:

```
systemctl restart xl2tpd
```

6. Настройка клиента

Рассмотрим процесс настройки клиента на базе Windows. Для андроида и устройств Apple параметры заполняются аналогично.

Графический интерфейс

В параметрах сети и Интернет в разделе **VPN** создаем новое соединение:

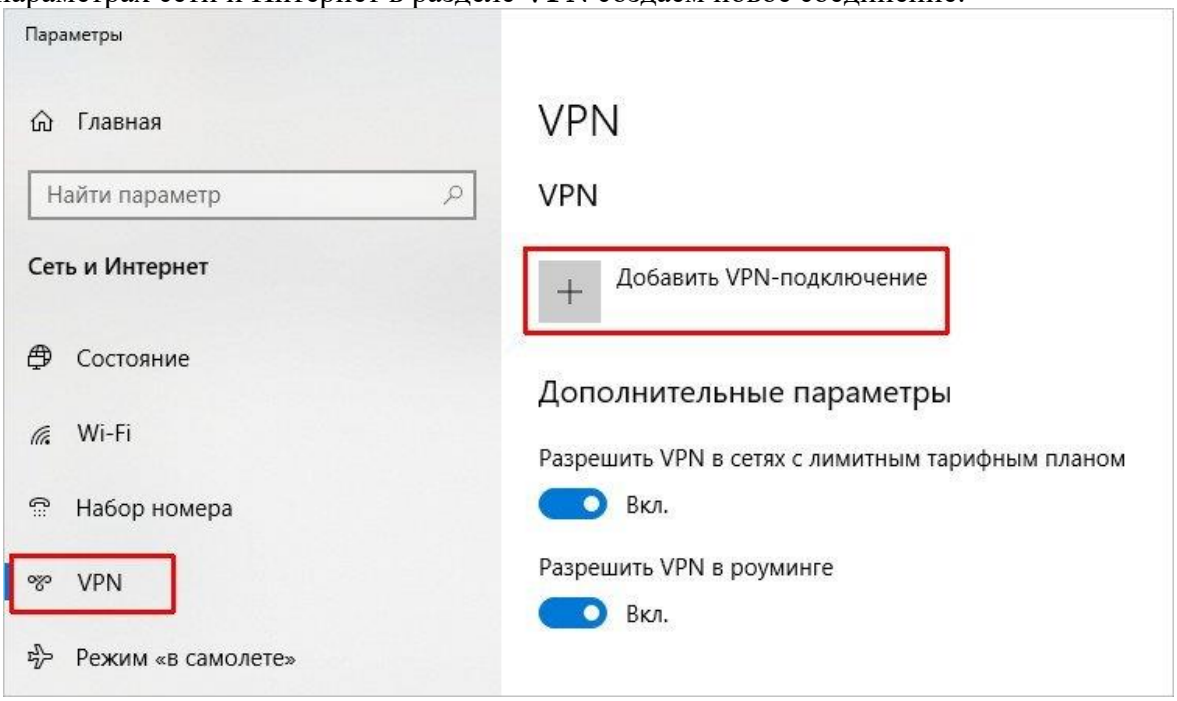


Рис. 317

Задаем настройки:

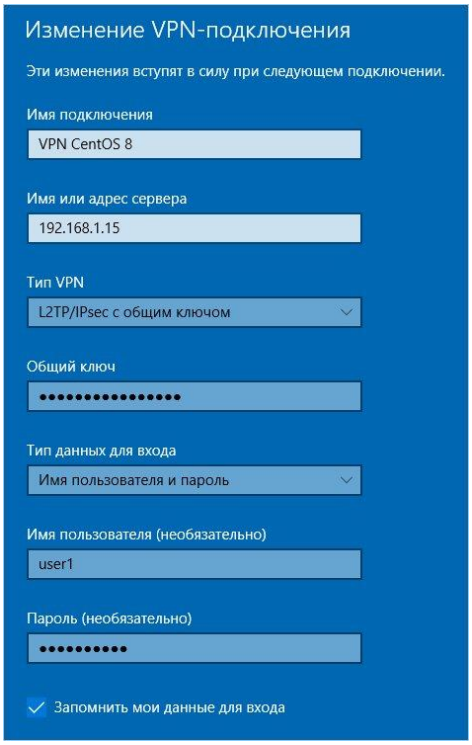


Рис. 318

** где:*

- ***Имя подключения*** *— произвольное имя для подключения.*
- ***Имя или адрес сервера*** *— адрес сервера VPN, к которому мы будем подключаться. В данном примере используем внутреннюю сеть, но в продуктивной среде адрес должен быть внешним.*
- ***Тип VPN*** *— для нашего случая, выбираем L2TP/IPsec с предварительным ключом.*
- ***Общий ключ*** *— ключ, который мы задали в файле /etc/ipsec.secrets.*
- ***Тип данных для входа*** *— выбираем пользователь и пароль.*
- ***Имя пользователя и пароль*** *— логин и пароль, которые мы задали в файле /etc/ppp/chap-secrets.*

Командная строка

Соединение VPN в Windows можно создать с помощью Powershell:

```
Add-VpnConnection -Name "VPN CentOS 8" -ServerAddress "192.168.1.15" -TunnelType "L2tp" -EncryptionLevel "Required" -AuthenticationMethod MsChapv2 -SplitTunneling -DnsSuffix "wbsh.local" -L2tpPsk "my_key_password" -Force -RememberCredential -PassThru
```

** где:*

- ***Name*** *— произвольное имя для подключения.*
- ***ServerAddress*** *— адрес сервера VPN, к которому мы будем подключаться. В данном примере используем внутреннюю сеть, но в продуктивной среде адрес должен быть внешним.*
- ***TunnelType*** *— тип туннеля. В нашем случае это L2TP.*
- ***EncryptionLevel*** *— указание на требование использования шифрованного канала.*
- ***AuthenticationMethod*** *— метод аутентификации. В нашем случае ms-chap-2.*
- ***DnsSuffix*** *— суффикс DNS. Будет автоматически подставляться к коротким именам узлов.*
- ***L2tpPsk*** *— предварительный ключ, который мы задали в файле /etc/ipsec.secrets.*

7. Доступ к локальной сети и сети Интернет

При подключении к нашему серверу VPN у клиента не будет возможности выходить в Интернет и подключаться к ресурсам сети, что делает соединение бессмысленным. Поэтому первым этапом после настройки сервера должна быть настройка маршрутизации сети. Для этого необходимо включить возможность работы в качестве шлюза и настроить правила в брандмауэре.

8. Настройка ядра

Нам нужно разрешить опцию net.ipv4.ip_forward в настройках ядра — для этого откроем файл:

```
nano /etc/sysctl.d/99-sysctl.conf
```

И добавляем в него следующую строку:

```
net.ipv4.ip_forward=1
```

После применяем настройку:

```
sysctl -p /etc/sysctl.d/99-sysctl.conf
```

В случае с единым сетевым интерфейсом больше ничего делать не потребуется — CentOS начнет работать как Интернет-шлюз.

В случае с несколькими сетевыми адаптерами, настраиваем сетевой экран.

9. Настройка брандмауэра

Настройка выполняется для двух сетевых интерфейсов на примере **ens32** (внутренний) и **ens34** (внешний):

```
firewall-cmd --permanent --zone=public --add-masquerade
firewall-cmd --direct --permanent --add-rule ipv4 filter FORWARD 0 -i ens32 -o ens34 -j ACCEPT
firewall-cmd --reload
```

10. Аутентификация через Active Directory

Проверка подлинности через активный каталог от Microsoft в xl2tp выполняется с помощью winbind и samba.

11. Подготовка сервера

Для корректной работы сервера с Active Directory необходимо задать ему имя (hostname), которое будет доступно в DNS. Также на сервере должно быть задано точное время. Необходимо убедиться, что сервер доступен по своему доменному имени. Если серверу так и не было задано вменяемого имени, вводим команду:

```
hostnamectl set-hostname vpn.wbsh.local
```

** где **vpn** — имя сервера; **wbsh.local** — домен.*

После добавляем в DNS наш сервер VPN. Ждем минут 15 (если у нас используется доменная инфраструктура с несколькими сайтами, иначе ждать не нужно).

Задаем временную зону:

```
\cp /usr/share/zoneinfo/Europe/Moscow /etc/localtime
```

** в данном примере мы задаем зону по московскому времени.*

Устанавливаем утилиту для синхронизации времени, разрешаем запуск демона и стартуем его.

```
dnf install chrony
systemctl enable chronyd
systemctl restart chronyd
```

12. Присоединяем сервер к домену

Устанавливаем необходимые компоненты:

```
dnf install samba-client samba-winbind samba-winbind-clients krb5-workstation
```

Открываем конфигурационный файл samba:

```
nano /etc/samba/smb.conf
```

В разделе [global] редактируем следующие опции:

```
workgroup = WBSH
security = ads
```

** где **WBSH** — NETBIOS имя домена; **ads** — указывает, что для samba будет использоваться модель безопасности LDAP Active Directory.*

Также в [global] добавим следующие строки:

```
kerberos method = secrets and keytab
realm = WBSH.LOCAL
winbind enum groups = Yes
winbind enum users = Yes
idmap config * : rangesize = 1000000
```

```
idmap config * : range = 1000000-19999999
idmap config * : backend = autorid
```

** где:*

- ***kerberos method*** *— метод проверки kerberos. В данном примере сначала используется secretts.tdb, а затем системная таблица ключей.*
- ***realm*** *— сервер Active Directory. В нашем примере прописан домен, так как по нему можно обратиться к любому из серверов AD.*
- ***winbind enum groups*** *— задает пределы перечисления групп через setgrent(), getgrent() и endgrent().*
- ***winbind enum users*** *— задает пределы перечисления пользователей через setpwent(), getpwent()и endpwent().*
- ***idmap config * : rangesize*** *— определяет количество доступных uids и gids в каждом доменном диапазоне.*
- ***idmap config * : range*** *— определяет доступные совпадающие диапазоны uid и gid, для которых серверная часть является авторитетной.*
- ***idmap config * : backend*** *— задает idmap плагин для использования в качестве SID/uid/gid подсистемы*

Вводим сервер в домен:

```
net ads join -U Administrator@wbsh.local
```

** где* ***Administrator*** *— учетная запись пользователя AD с правами на ввод компьютеров в домен;* ***wbsh.local*** *— наш домен.*

Мы должны увидеть, примерно, следующее:

```
Using short domain name -- WBSH
Joined 'SAMBA' to dns domain 'wbsh.local'
```

Разрешаем автозапуск winbind и стартуем его:

```
systemctl enable winbind --now
```

Выбираем профиль для аутентификации:

```
authselect select winbind --force
```

Проверяем, что наш сервер может получить список пользователей Active Directory:

```
wbinfo -u
```

... и групп:

```
wbinfo -g
```

Если мы увидели список пользователей и групп, то присоединение сервера к домену завершено.

После проверяем, что аутентификация в AD через модуль ntlm_auth работает корректно:

```
ntlm_auth --request-nt-key --domain=WBSH.LOCAL --username=Administrator
```

** где* ***WBSH.LOCAL*** *— наш домен;* ***Administrator*** *— пользователь, под которым будем логиниться для проверки работы модуля.*

13. Настройка PPP для аутентификации через AD

Открываем конфигурационный файл options.xl2tpd:

```
vi /etc/ppp/options.xl2tpd
```

Добавляем в самый низ:

```
...
plugin winbind.so
ntlm_auth-helper '/usr/bin/ntlm_auth --helper-protocol=ntlm-server-1 --require-membership-of="WBSH\\VPN Users"'
```

** где **VPN Users** — группа в AD, пользователи который будут иметь возможность использовать VPN.*

Перезапускаем xl2tpd:

```
systemctl restart xl2tpd
```

14. Проверка

В Active Directory добавляем группу VPN Users (если еще нет). Группа должна быть локальная в домене. В группу добавим пользователей, которым хотим дать доступ для VPN-подключения.

В настройках подключения к серверу меняем пользователя и пароль на доменные.

15. Диагностика проблем

Описанная выше настройка не предполагает наличие лога. Для этого открываем конфигурационный файл для ppp:

```
nano /etc/ppp/options.xl2tpd
```

Добавим:

```
...
logfile /var/log/xl2tpd/xl2tpd.log
debug
```

Создадим каталог для лога:

```
mkdir /var/log/xl2tpd
```

Перезапускаем сервис xl2tpd:

```
systemctl restart xl2tpd
```

Пробуем подключиться к серверу — в случае наличия проблем, наблюдаем за логом:

```
tail -f /var/log/xl2tpd/xl2tpd.log
```

16. Настройка доступа по ssh в centos

SSH-сервер (OpenSSH) позволяет производить удалённое управление операционной системой, а также копирование файлов между компьютерами по шифрованному каналу связи. SSH расшифровывается как Secure Shell. OpenSSH обеспечивает надежную авторизацию и безопасную передачу данных по открытым каналам связи.

Установка SSH-сервера

Для установки SSH-сервера в CentOS необходимо установить пакет openssh-server:

```
# sudo dnf install openssh-server
```

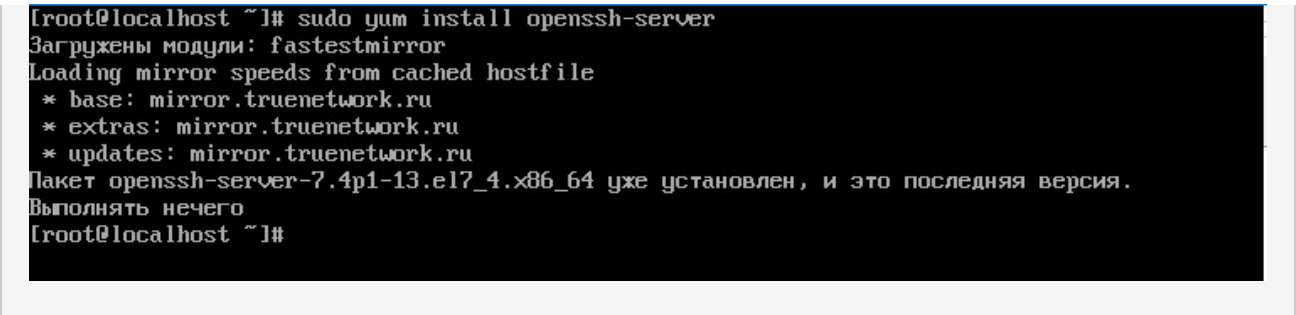


Рис. 319

Добавляем OpenSSH в автозагрузку:

sudo chkconfig sshd on

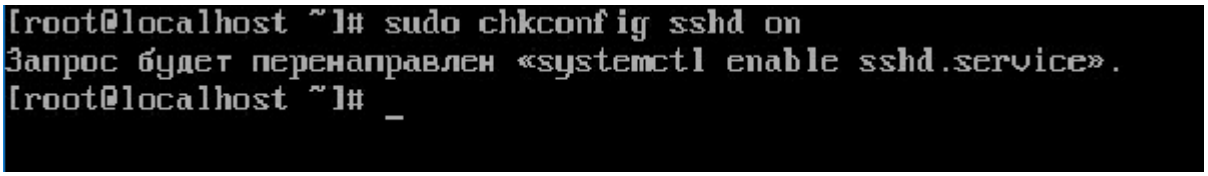


Рис. 320

Для дальнейшей работы нам необходимо запустить сервер OpenSSH.

Запуск OpenSSH:

service sshd start

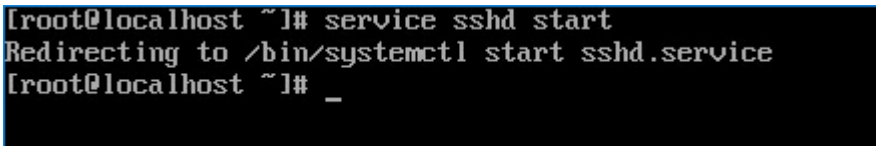


Рис. 321

Настройки SSH-сервера
Настройки SSH-сервера хранятся в файле `/etc/ssh/sshd_config`.

Для приведенного выше примера он может быть следующим:

Рис. 322

Наиболее важные опции с точки зрения безопасности:

- `Port 22` – Порт по умолчанию.
- `Protocol 2,1` – Какая реализация протокола SSH будет использоваться. Рекомендую оставить только 2.
- `ListenAddress` – По умолчанию SSH сервер прослушивает все доступные интерфейсы, что абсолютно не нужно в большинстве ситуаций. Необходимо прописать сетевой интерфейс, с которого будет осуществляться управление сервером.
- `PermitRootLogin yes` – По умолчанию разрешает входить по SSH суперпользователю root. Необходимо указать no.
- `AllowUsers adminsys` – Данный параметр разрешает входить по SSH только перечисленным пользователям.
- `AllowGroups wheel` – Группа пользователей которой можно входить по SSH, опцию можно не использовать если указана опция `AllowUsers`.

- `DenyUsers baduser` – Данная опция запрещает вход по SSH перечисленным пользователям.
- `DenyGroups badgroup` – Данная опция запрещает вход по SSH перечисленным группам пользователей.
- `MaxAuthTries 3` – Сколько раз переспрашивать пароль при неверном вводе. В данном случае SSH-сервер после 3 неверных попыток разорвет соединение с клиентом.
- `LoginGraceTime 60` – Через сколько секунд разрывать соединение при отсутствии аутентификации со стороны клиента.
- `PermitEmptyPasswords no` – Разрешать использовать пустые пароли. По вполне понятным причинам значение этого параметра no.
- `PrintLastLog yes` – при входе пользователя в систему по SSH ему будет показано когда и откуда последний раз был произведен вход под данным пользователем.
- `LogLevel INFO` – В качестве параметра этой опции необходимо указать уровень журналирования. Возможные значения QUIET, FATAL, ERROR, INFO, VERBOSE, DEBUG1, DEBUG2, DEBUG3. Чем выше уровень журналирования, тем больше информации появится в файле регистрации событий.
- `SyslogFacility AUTHPRIV` – Куда будут попадать логи. Возможные значения: DAEMON, USER, AUTH, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7.

Вход на сервер через PUTTY PORTABLE

Для начала нам нужно узнать IP-адрес сервера:

ifconfig

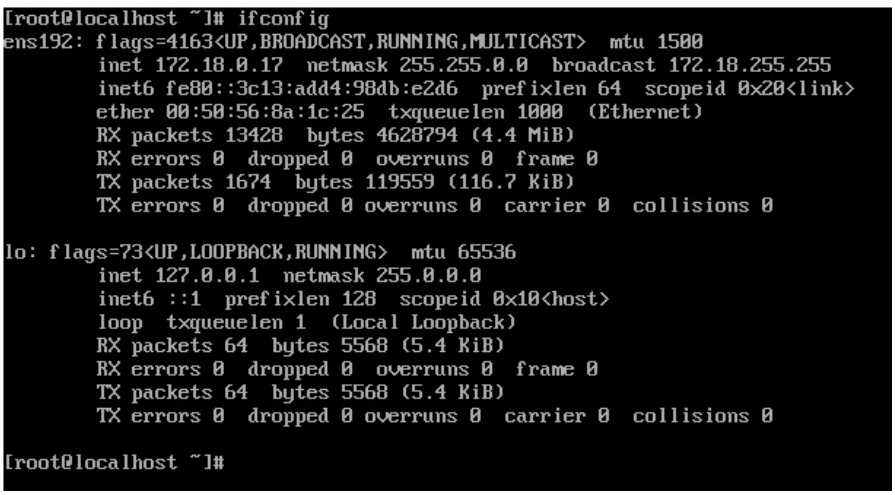


Рис. 323

После чего вводим IP-адрес в PUTTY указав 22 порт (стоит по умолчанию).

Указываем SSH соединение и заходим на сервер.

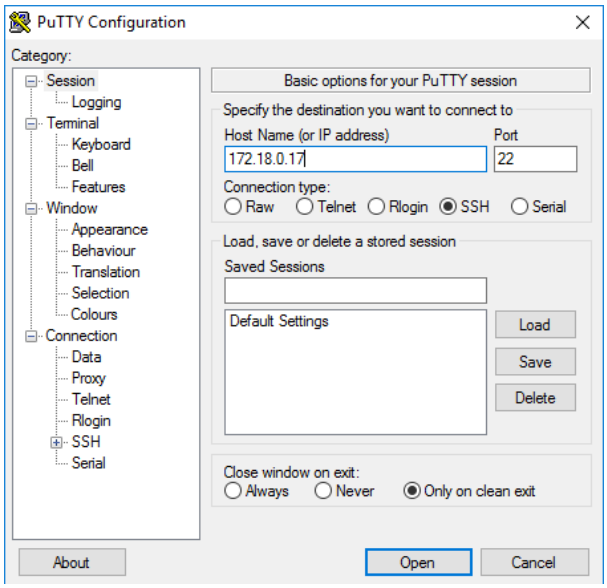


Рис. 324

При входе на сервер он попросит вас зайти под своей учетной записью.

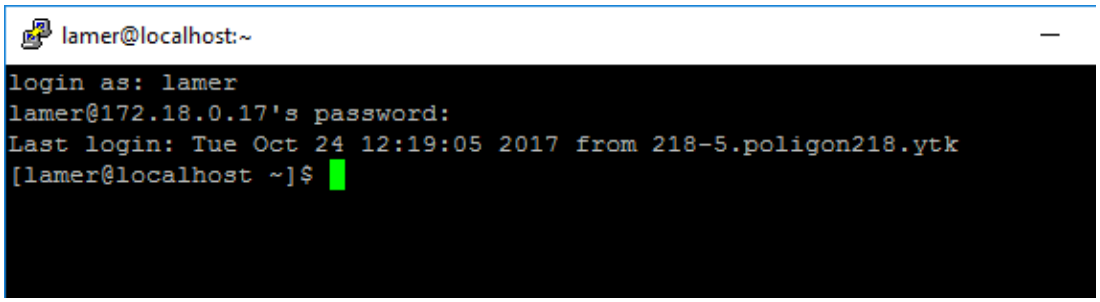


Рис. 325

Сделайте скриншоты (фотографии) процесса настройки протокола IP-sec и SSH и вставьте в отчёт.

2.26. Практическая работа № 26 «Настройка регистрации действий»

Задание:

В данной практической работе мы рассмотрим основы работы с rsyslog. В примерах мы будем использовать следующие узлы:

Сервер:192.168.241.140

Клиент: 172.31.21.58

1. Установка и настройка сервера Rsyslog

В большинстве дистрибутивов Linux пакет rsyslog предустановлен. Если у вас его нет, установите его при помощи менеджера пакетов:

Для RHEL/CentOS:

```
$ dnf install rsyslog
```

После установки rsyslog нужно запустить службу, активировать автоматический запуск при загрузке и проверить состояние при помощи команды systemctl.

```
$ sudo systemctl start rsyslog
$ sudo systemctl enable rsyslog
```

```
$ sudo systemctl status rsyslog
```

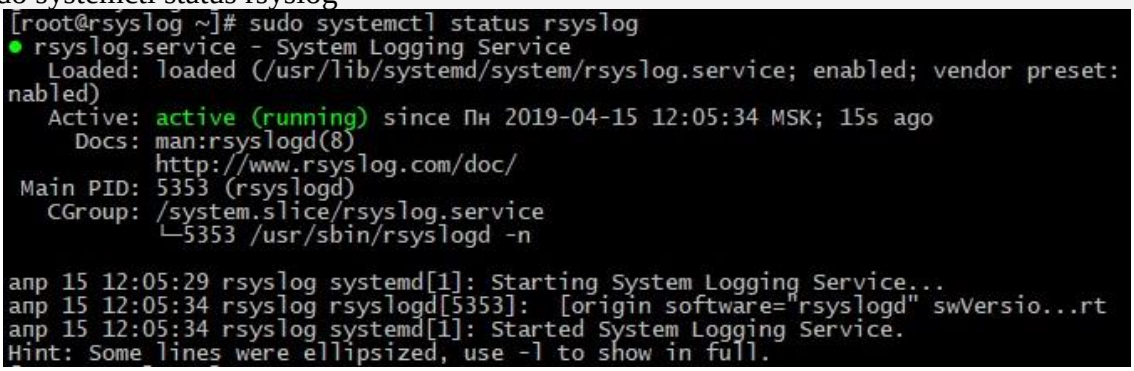


Рис. 326

Главный файл конфигурации rsyslog — `/etc/rsyslog.conf`. Он загружает модули, определяет глобальные директивы, содержит правила по обработке сообщений логов, а также включает пути ко всем файлам конфигурации в директории `/etc/rsyslog.d/` для различных приложений и служб.

```
$ sudo nano /etc/rsyslog.conf
```

По умолчанию rsyslog использует модули imjournal и imusock для импорта структурированных записей логов из журнала systemd и для приема через сокетов Unix сообщений системных логов от приложений, запущенных в локальной системе, соответственно.

Чтобы настроить rsyslog как сетевой централизованный сервер ведения логов, нужно установить протоколы (UDP, TCP или оба), которые будут использоваться для приема удаленных сообщений системных логов, а также прослушиваемые порты.

Если вы хотите использовать UDP-соединение, более быстрое, но ненадежное, найдите в файле конфигурации следующие строки, раскомментируйте их и замените 514 на порт, который вы хотите прослушивать. Этот порт должен соответствовать порту, на который клиенты будут отправлять сообщения, мы рассмотрим это ниже при настройке клиента rsyslog:

```
$ModLoad imudp
$UDPServerRun 514
```

Для использования TCP-соединения (медленнее, но надежнее) найдите и раскомментируйте следующие строки:

```
$ModLoad imtcp
$InputTCPServerRun 514
```

В нашем случае мы будем использовать оба протокола.

Далее вам потребуется определить набор правил для обработки удаленных логов в следующем формате:

```
источник.уровень_важности место_записи_лога
```

источник: тип процесса или приложения, от которого исходит сообщение, значение может быть auth, cron, daemon, kernel, local0..local7. Использование звездочки (*) означает все источники.

уровень_важности: тип сообщения логов: emerg-0, alert-1, crit-2, err-3, warn-4, notice-5, info-6, debug-7. Использование звездочки означает все уровни важности, если ничего не указывать, предполагается отсутствие уровня важности.

- 0, emerg – система не работоспособна
- 1, alert – система требует немедленного вмешательства
- 2, crit – состояние системы критическое
- 3, err – сообщение об ошибке
- 4, warning – предупреждение о возможной проблеме
- 5, notice – нормальное, но важное событие
- 6, info – информационное сообщение
- 7 , debug – отладочное сообщение

- место_записи_лога: локальный файл или удаленный сервер rsyslog (определенный в формате IP-адрес:порт).

Для сбора логов удаленных узлов мы будем использовать следующий набор правил с шаблоном RemoteLogs. Обратите внимание, что эти правила должны предшествовать правилам обработки локальных сообщений.

```
$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"
*.* ?RemoteLogs
& ~
```

Рассмотрим набор правил более подробно. Первое правило в нем следующее: **«$template RemoteLogs,”/var/log/%HOSTNAME%/%PROGRAMNAME%.log”»**.

Директива *$template* дает демону rsyslog команду собирать полученные сообщения из источников и записывать их в отдельные логи в директории `/var/logs` в соответствии с именем узла (машины клиента) и источником (программой/приложением), от которых были получены сообщения, что определено соответствующим шаблоном.

Вторая строка **«*.* ?RemoteLogs»** означает запись сообщений всех уровней важности от всех источников в соответствии с шаблоном *RemoteLogs*.

Последняя строка **«& ~»** задает rsyslog прекратить обработку сообщений после их записи в файл. Если не указать «& ~», сообщения будут записаны в локальные файлы. Настройка сервера для нашего примера завершена. Теперь нужно сохранить и закрыть файл конфигурации, а также перезапустить демон rsyslog, чтобы изменения вступили в силу:

```
$ sudo systemctl restart rsyslog
```

Далее требуется проверить сетевые сокеты rsyslog. Воспользуйтесь netstat

```
$ netstat -nap | grep "rsyslog"
```

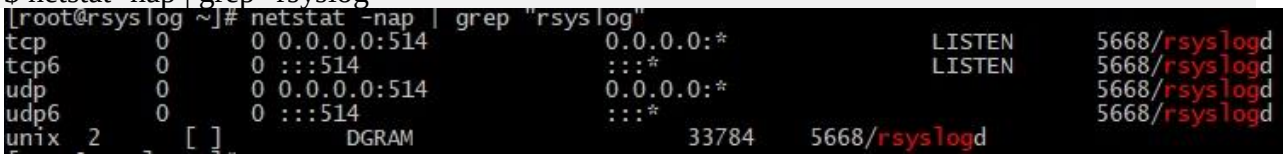


Рис. 327

Если у вас включена служба SELinux, нужно выполнить следующие команды, чтобы разрешить трафик rsyslog:

```
$ sudo semanage -a -t syslogd_port_t -p udp 514
$ sudo semanage -a -t syslogd_port_t -p tcp 514
```

При включенном брандмауэре нужно открыть TCP и UDP порты 514, чтобы разрешить подключение к серверу rsyslog по обоим протоколам:

Для CentOS (брандмауэр firewalld):

```
$ sudo firewall-cmd --permanent --add-port=514/udp
$ sudo firewall-cmd --permanent --add-port=514/tcp
$ sudo firewall-cmd --reload
```

Для Ubuntu (брандмауэр ufw):

```
$ sudo ufw allow 514/udp
$ sudo ufw allow 514/tcp
$ sudo ufw reload
```

2. Настройка клиента Rsyslog для отправки логов на сервер

Проверьте, запущена ли служба rsyslog на клиентской машине, при помощи следующей команды:

```
$ sudo systemctl status rsyslog
```

Если она не установлена, установите и запустите службу точно так же, как для сервера: После запуска службы откройте файл конфигурации:

```
$ sudo nano /etc/rsyslog.conf
```

Чтобы демон rsyslog работал как клиент и отправлял все локальные логи на удаленный сервер rsyslog, добавьте следующее правило перенаправления в конце файла, как показано на скриншоте ниже. Номер порта должен соответствовать номеру порта, прописанному в конфигурации сервера:

```
*. * @@192.168.100.10:514
```

Приведенное правило будет отправлять сообщения всех уровней важности от всех источников. Для отправки сообщений от конкретного источника, например, auth, воспользуйтесь следующим правилом:

```
auth. * @@192.168.100.10:514
```

Сохраните и закройте файл, а также перезагрузите службу rsyslog чтобы изменения вступили в силу.

```
$ sudo systemctl restart rsyslog
```

3. Мониторинг логов на сервере

Последний этап – проверить, действительно ли rsyslog получает сообщения от клиента и сохраняет их в директории `/var/log` и формате имя_узла/имя_программы.log. Выполните команду ls, чтобы получить список файлов директории логов и проверьте, есть ли там директории под названием ip-172.31.21.58 (или с соответствующим именем узла вашего клиента).

```
$ ls -l /var/log/
```

Если директория существует, проверьте файлы логов в ней следующей командой:

```
$ sudo ls -l /var/log/ip-172-31-21-58/
```

Сделайте скриншоты (фотографии) процесса настройки регистрации действийи вставьте в отчёт.

2.27. Практическая работа № 27 «Установка и настройка OpenLDAP»

Задание:

1. Установка Open LDAP на CentOS

Установите openldap, openldap-серверы, openldap-клиенты и миграционные *инструменты* из *YUM* .

```
[root@localhost]# yum -y install openldap openldap-servers openldap-clients
migration tools
 Loaded plugins: fastestmirror, langpacks
 updates
 | 3.4 kB  00:00:00
 updates/7/x86_64/primary_db
 | 2.2 MB  00:00:05
 Determining fastest mirrors
 (1/2): extras/7/x86_64/primary_db
 | 121 kB  00:00:01
 (2/2): base/7/x86_64/primary_db
 | 5.6 MB  00:00:16
 Package openldap-2.4.40-13.el7.x86_64 already installed and latest version
 Resolving Dependencies
 --> Running transaction check
 ---> Package openldap-clients.x86_64 0:2.4.40-13.el7 will be installed
 ---> Package openldap-servers.x86_64 0:2.4.40-13.el7 will be installed
 --> Finished Dependency Resolution
 base/7/x86_64/group_gz
 | 155 kB  00:00:00

 Dependencies Resolved
```

```
================================================================================
================================================================================
Package                              Arch
Version                            Repository                          Size
================================================================================
================================================================================
Installing:
openldap-clients                     x86_64
2.4.40-13.el7                      base                                188 k
openldap-servers                     x86_64
2.4.40-13.el7                      base                                2.1 M

Transaction Summary
================================================================================
================================================================================
Install  2 Packages

Total download size: 2.3 M
Installed size: 5.3 M
Downloading packages:

Installed:
openldap-clients.x86_64 0:2.4.40-13.el7
openldap-servers.x86_64 0:2.4.40-13.el7
Complete!
[root@localhost]#
```

Теперь давайте запустим и *включим* сервис *slapd* —

```
[root@centos]# systemctl start slapd
[root@centos]# systemctl enable  slapd
```

Теперь давайте убедимся, что у нас есть структура *openldap* в */ etc / openldap* .

```
root@localhost]# ls /etc/openldap/
certs  check_password.conf  ldap.conf  schema  slapd.d
[root@localhost]#
```

Затем убедитесь, что наш сервис slapd запущен.

```
root@centos]# netstat -antup | grep slapd
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN
1641/slapd
tcp6       0      0 :::389                  :::*                    LISTEN
1641/slapd

[root@centos]#
```

Далее, давайте настроим нашу установку *Open LDAP* .
Убедитесь, что наш системный пользователь *ldap* создан.

```
[root@localhost]# id ldap
uid=55(ldap) gid=55(ldap) groups=55(ldap)
[root@localhost]#
```

Создайте наши учетные данные LDAP.

```
[root@localhost]# slappasswd
New password:
Re-enter new password:
{SSHA}20RSyjVv6S6r43DFPeJgASDLlLoSU8g.a10
```

```
[root@localhost]#
```

Нам нужно сохранить вывод из slappasswd.

2. Настройка Open LDAP

Шаг 1 — Настройте LDAP для домена и добавьте администратора.

Во-первых, мы хотим настроить нашу среду openLDAP. Ниже приведен шаблон для использования с командой *ldapmodify* .

```
dn: olcDatabase={2}hdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=vmnet,dc=local
dn: olcDatabase = {2}hdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=ldapadm,dc=vmnet,dc=local
dn: olcDatabase = {2}hdb,cn=config
changetype: modify
replace: olcRootPW
olcRootPW: <output from slap
```

Внесите изменения в /etc/openldap/slapd.d/cn=config/olcDatabase = {1} monitor.ldif с помощью команды ldapmodify.

```
[root@localhost]# ldapmodify -Y EXTERNAL -H ldapi:/// -f /home/rdc/Documents/db.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber = 0+uidNumber = 0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase = {2}hdb,cn=config"
modifying entry "olcDatabase = {2}hdb,cn=config"
modifying entry "olcDatabase = {2}hdb,cn=config"

[root@localhost cn=config]#
```

Давайте проверим измененную конфигурацию LDAP.

```
root@linux1 ~]# vi /etc/openldap/slapd.d/cn=config/olcDatabase={2}hdb.ldif

[root@centos]# cat /etc/openldap/slapd.d/cn\=config/olcDatabase\=\{2\}hdb.ldif
 # AUTO-GENERATED FILE - DO NOT EDIT!! Use ldapmodify.
 # CRC32 a163f14c
dn: olcDatabase = {2}hdb
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {2}hdb
olcDbDirectory: /var/lib/ldap
olcDbIndex: objectClass eq,pres
olcDbIndex: ou,cn,mail,surname,givenname eq,pres,sub
structuralObjectClass: olcHdbConfig
entryUUID: 1bd9aa2a-8516-1036-934b-f7eac1189139
creatorsName: cn=config
createTimestamp: 20170212022422Z
olcSuffix: dc=vmnet,dc=local
olcRootDN: cn=ldapadm,dc=vmnet,dc=local
olcRootPW:: e1NTSEF1bUVyb1VzZTRjc2dkYVdGaDY0T0k =
entryCSN: 20170215204423.726622Z#000000#000#000000
modifiersName: gidNumber = 0+uidNumber = 0,cn=peercred,cn=external,cn=auth
modifyTimestamp: 20170215204423Z

[root@centos]#
```

Как вы можете видеть, наши модификации LDAP предприятия были успешными.
Далее мы хотим создать самозаверяющий ssl-сертификат для OpenLDAP. Это защитит связь между корпоративным сервером и клиентами.
Шаг 2 — Создайте самоподписанный сертификат для OpenLDAP.
Мы будем использовать *openssl* для создания ssl-сертификата с собственной подписью. Перейдите к следующей главе « **Создание сертификата SSL LDAP с помощью openssl»,** чтобы получить инструкции по обеспечению безопасности связи с OpenLDAP. Затем, когда SSL-сертификаты будут настроены, мы завершим нашу корпоративную конфигурацию OpenLDAP.
Шаг 3 — Настройте OpenLDAP для использования безопасной связи с сертификатом.
Создайте файл *certs.ldif* в *vim* со следующей информацией —

```
dn: cn=config
changetype: modify
replace: olcTLSCertificateFile
olcTLSCertificateFile: /etc/openldap/certs/yourGeneratedCertFile.pem

dn: cn=config
changetype: modify
replace: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/openldap/certs/youGeneratedKeyFile.pem
```

Затем снова используйте команду *ldapmodify* для объединения изменений в конфигурацию OpenLDAP.

```
[root@centos rdc]# ldapmodify -Y EXTERNAL  -H ldapi:/// -f certs.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber = 0+uidNumber = 0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=config"

[root@centos]#
```

Наконец, давайте проверим нашу конфигурацию OpenLADP.

```
[root@centos]# slaptest -u
config file testing succeeded
[root@centos]#
```

Шаг 4 — Настройте базу данных slapd.

```
cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG &&
chown ldap:ldap /var/lib/ldap/*
```

Обновляет схему OpenLDAP.
Добавьте косинус и nis схемы LDAP.

```
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif
```

Наконец, создайте схему предприятия и добавьте ее в текущую конфигурацию OpenLDAP.
Следующее для домена под названием vmnet. *локальный* с администратором LDAP под названием *ldapadm* .

```
dn: dc=vmnet,dc=local
dc: vmnet
objectClass: top
objectClass: domain
```

```
dn: cn=ldapadm ,dc=vmnet,dc=local
objectClass: organizationalRole
cn: ldapadm
description: LDAP Manager

dn: ou = People,dc=vmnet,dc=local
objectClass: organizationalUnit
ou: People

dn: ou = Group,dc=vmnet,dc=local
objectClass: organizationalUnit
ou: Group
```

Наконец, импортируйте это в текущую схему OpenLDAP.

```
[root@centos]# ldapadd -x -W -D "cn=ldapadm,dc=vmnet,dc=local" -f ./base.ldif
 Enter LDAP Password:
adding new entry "dc=vmnet,dc=local"

adding new entry "cn=ldapadm ,dc=vmnet,dc=local"

adding new entry "ou=People,dc=vmnet,dc=local"

adding new entry "ou=Group,dc=vmnet,dc=local"

[root@centos]#
```

Шаг 5 — Настройка пользователей OpenLDAP Enterprise.
Откройте *vim* или ваш любимый текстовый редактор и скопируйте следующий формат. Это настройка для пользователя с именем «entacct» в домене LDAP «vmnet.local».

```
dn: uid=entacct,ou=People,dc=vmnet,dc=local
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: entacct
uid: entacct
uidNumber: 9999
gidNumber: 100
homeDirectory: /home/enyacct
loginShell: /bin/bash
gecos: Enterprise User Account 001
userPassword: {crypt}x
shadowLastChange: 17058
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
```

Теперь импортируйте вышеуказанные файлы, как сохраненные, в схему OpenLdap.

```
 [root @ centos] # ldapadd -x -W -D "cn = ldapadm, dc = vmnet, dc = local" -f en-
tuser.ldif
  Введите пароль LDAP:
 добавление новой записи "uid = entacct, ou = People, dc = vmnet, dc = local"

 [Корень @ CentOS] #
```

Прежде чем пользователи смогут получить доступ к LDAP Enterprise, нам нужно назначить пароль следующим образом:

```
ldappasswd -s password123 -W -D "cn=ldapadm,dc=entacct,dc=local" -x "uid=entacct
```

```
,ou=People,dc=vmnet,dc=local"
```

-s указывает пароль для пользователя
-x — имя пользователя, к которому применяется обновленный пароль
-D — это * отличительное имя для аутентификации по схеме LDAP.
Наконец, прежде чем войти в учетную запись Enterprise, давайте проверим нашу запись *OpenLDAP* .

```
[root@centos rdc]# ldapsearch -x cn=entacct -b dc=vmnet,dc=local
 # extended LDIF
 #
 # LDAPv3
 # base <dc=vmnet,dc=local> with scope subtree
 # filter: cn=entacct
 # requesting: ALL
 #
 # entacct, People, vmnet.local
dn: uid=entacct,ou=People,dc=vmnet,dc=local
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: entacct
uid: entacct
uidNumber: 9999
gidNumber: 100
homeDirectory: /home/enyacct
loginShell: /bin/bash
gecos: Enterprise User Account 001
userPassword:: e2NyeXB0fXg=
shadowLastChange: 17058
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
```

Преобразование таких вещей, как */ etc / passwd* и */ etc / groups* в аутентификацию OpenLDAP, требует использования инструментов миграции. Они включены в пакет migtools. Затем устанавливается в */ usr / share /igrationtools* .

```
[root@centos openldap-servers]# ls -l /usr/share/migrationtools/
total 128
-rwxr-xr-x. 1 root root  2652 Jun  9  2014 migrate_aliases.pl
-rwxr-xr-x. 1 root root  2950 Jun  9  2014 migrate_all_netinfo_offline.sh
-rwxr-xr-x. 1 root root  2946 Jun  9  2014 migrate_all_netinfo_online.sh
-rwxr-xr-x. 1 root root  3011 Jun  9  2014 migrate_all_nis_offline.sh
-rwxr-xr-x. 1 root root  3006 Jun  9  2014 migrate_all_nis_online.sh
-rwxr-xr-x. 1 root root  3164 Jun  9  2014 migrate_all_nisplus_offline.sh
-rwxr-xr-x. 1 root root  3146 Jun  9  2014 migrate_all_nisplus_online.sh
-rwxr-xr-x. 1 root root  5267 Jun  9  2014 migrate_all_offline.sh
-rwxr-xr-x. 1 root root  7468 Jun  9  2014 migrate_all_online.sh
-rwxr-xr-x. 1 root root  3278 Jun  9  2014 migrate_automount.pl
-rwxr-xr-x. 1 root root  2608 Jun  9  2014 migrate_base.pl
```

Шаг 6 — Наконец, нам нужно разрешить доступ к сервису slapd, чтобы он мог обслуживать запросы.

```
firewall-cmd --permanent --add-service=ldap
firewall-cmd --reload
```

3. Настройте клиентский доступ LDAP

Настройка клиентского доступа LDAP требует наличия следующих пакетов на клиенте: клиенты openldap, open-ldap и nss_ldap.
Настройка аутентификации LDAP для клиентских систем немного проще.
Шаг 1 — Установите зависимые пакеты —

```
# yum install -y openldap-clients nss-pam-ldapd
```

Шаг 2 — Настройте аутентификацию LDAP с помощью *authconfig* .

```
authconfig --enableldap --enableldapauth --ldapserver=10.25.0.1 --
ldapbasedn="dc=vmnet,dc=local" --enablemkhomedir --update
```

Шаг 3 — Перезапустите службу nslcd.

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

2.28. Практическая работа № 28 «Установка и настройка IPtables»

Задание:

1. Отключение firewalld

Первым делом отключим firewalld, который присутствует в centos 7 по-умолчанию сразу после установки:

```
# systemctl stop firewalld
```

Теперь удалим его из автозагрузки, чтобы он не включился снова после рестарта:

```
# systemctl disable firewalld
```

После этого на сервере настройки сетевого экрана становятся полностью открытыми. Посмотреть правила iptables можно командой:

```
# iptables -L -v -n
```

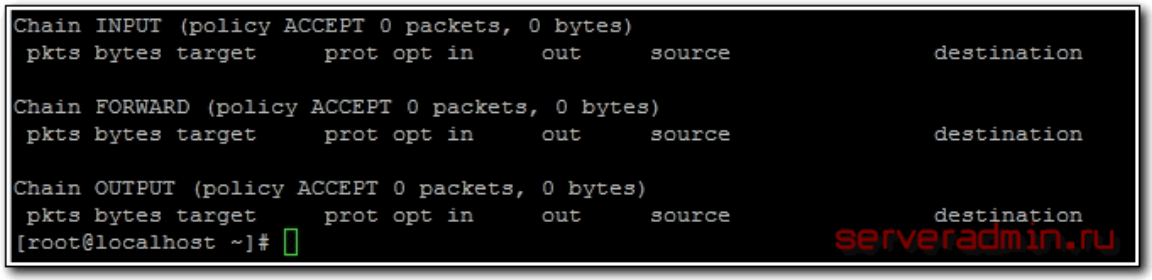


Рис. 328

Дальше пойдет информация исключительно по конфигурированию только iptables. Темы firewalld я больше касаться не буду.

2. Установка iptables

На самом деле фаервол у нас на сервере уже стоит и работает, просто нет никаких правил, все открыто. Установить нам нужно будет дополнительные утилиты управления, без которых конфигурировать iptables невозможно. Например, нельзя будет перезапустить фаервол:

```
# systemctl restart iptables.service
```

```
Failed to issue method call: Unit iptables.service failed to load: No such file or directory.
```

Или добавить в автозапуск не получится:

```
# systemctl enable iptables.service
Failed to issue method call: No such file or directory
```

Чтобы подобных ошибок не было, установим необходимый пакет с утилитами:

```
# yum -y install iptables-services
```

Теперь можно добавить iptables в автозагрузку и запустить:

```
# systemctl enable iptables.service
# systemctl start iptables.service
```

3. Настройка фаервола

Для управления правилами фаервола я использую скрипт. Создадим его:

```
# mcedit /etc/iptables.sh
```

Далее будем наполнять его необходимыми правилами. Я буду разбирать все значимые части скрипта, а **полностью его приведу в виде текстового файла в конце статьи**. Правила сделаны в виде картинок, чтобы запретить копирование и вставку. Это может привести к ошибкам в работе правил, с чем я сам столкнулся во время подготовки статьи.

Мы рассмотрим ситуацию, когда сервер является шлюзом в интернет для локальной сети. Первым делом зададим все переменные, которые будем использовать в скрипте. Это не обязательно делать, но рекомендуется, потому что удобно переносить настройки с сервера на сервер. Достаточно будет просто переназначить переменные.

```
#!/bin/bash
export IPT="iptables"
# Внешний интерфейс
export WAN=eth0
export WAN_IP=85.31.203.127
# Локальная сеть
export LAN1=eth1
export LAN1_IP_RANGE=10.1.3.0/24
```

Перед применением новых правил, очищаем все цепочки:

```
$IPT -F
$IPT -F -t nat
$IPT -F -t mangle
$IPT -X
$IPT -t nat -X
$IPT -t mangle -X
```

Блокируем весь трафик, который не соответствует ни одному из правил:

```
$IPT -P INPUT DROP
$IPT -P OUTPUT DROP
$IPT -P FORWARD DROP
```

Разрешаем весь трафик локалхоста и локалки:

```
$IPT -A INPUT -i lo -j ACCEPT
$IPT -A INPUT -i $LAN1 -j ACCEPT
$IPT -A OUTPUT -o lo -j ACCEPT
$IPT -A OUTPUT -o $LAN1 -j ACCEPT
```

Разрешаем делать ping:

```
$IPT -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
$IPT -A INPUT -p icmp --icmp-type destination-unreachable -j ACCEPT
$IPT -A INPUT -p icmp --icmp-type time-exceeded -j ACCEPT
$IPT -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

Если вам это не нужно, то не добавляйте разрешающие правила для icmp.
Открываем доступ в инет самому серверу:

```
$IPT -A OUTPUT -o $WAN -j ACCEPT
```

Если вы хотите открыть все входящие соединения сервера, то добавляйте дальше правило:

```
$IPT -A INPUT -i $WAN -j ACCEPT
```

Делать это не рекомендуется, привожу просто для примера, если у вас появится такая необходимость.
Дальше разрешим все установленные соединения и дочерние от них. Так как они уже установлены, значит прошли через цепочки правил, фильтровать их еще раз нет смысла:

```
$IPT -A INPUT -p all -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT -A OUTPUT -p all -m state --state ESTABLISHED,RELATED -j ACCEPT
$IPT -A FORWARD -p all -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Теперь добавим защиту от наиболее распространенных сетевых атак. Сначала отбросим все пакеты, которые не имеют никакого статуса:

```
$IPT -A INPUT -m state --state INVALID -j DROP
$IPT -A FORWARD -m state --state INVALID -j DROP
```

Блокируем нулевые пакеты:

```
$IPT -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
```

Закрываемся от syn-flood атак:

```
$IPT -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
$IPT -A OUTPUT -p tcp ! --syn -m state --state NEW -j DROP
```

Следом за этими правилами рекомендуется поставить правила на запрет доступа с определенных IP, если у вас имеется такая необходимость. Например, вам надоел адрес 84.122.21.197 брутом ssh. Блокируем его:

```
$IPT -A INPUT -s 84.122.21.197 -j REJECT
```

Если вы не ставите ограничений на доступ из локальной сети, то разрешаем всем выход в интернет:

```
$IPT -A FORWARD -i $LAN1 -o $WAN -j ACCEPT
```

Следом запрещаем доступ из инета в локальную сеть:

```
$IPT -A FORWARD -i $WAN -o $LAN1 -j REJECT
```

Чтобы наша локальная сеть пользовалась интернетом, включаем nat:

```
$IPT -t nat -A POSTROUTING -o $WAN -s $LAN1_IP_RANGE -j MASQUERADE
```

Чтобы не потерять доступ к серверу, после применения правил, разрешаем подключения по ssh:

```
$IPT -A INPUT -i $WAN -p tcp --dport 22 -j ACCEPT
```

И в конце записываем правила, чтобы они применились после перезагрузки:

```
/sbin/iptables-save  > /etc/sysconfig/iptables
```

Мы составили простейший конфиг, который блокирует все входящие соединения, кроме ssh и разрешает доступ из локальной сети в интернет. Попутно защитились от некоторых сетевых атак.
Сохраняем скрипт, делаем исполняемым и запускаем:

```
# chmod 0740 /etc/iptables.sh
# /etc/iptables.sh
```

Выполним просмотр правил и проверим, все ли правила на месте:

```
# iptables -L -v -n
```

Обращаю ваше внимание - применять правила нужно лишь в том случае, если у вас имеется доступ к консоли сервера. При ошибке в настройках вы можете потерять доступ. Убедитесь, что в нештатной ситуации вы сможете отключить фаервол и скорректировать настройки.

4. Открытие портов

Теперь немного расширим нашу конфигурацию и откроем в iptables порты для некоторых сервисов. Допустим, у нас работает веб-сервер и необходимо открыть к нему доступ из интернета. Добавляем правила для веб-трафика:

```
#$IPT -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
#$IPT -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
```

Было добавлено разрешение на входящие соединения по 80-му и 443-му портам, которые использует web сервер в своей работе.
Если у вас установлен почтовый сервер, то нужно разрешить на него входящие соединения по всем используемым портам:

```
$IPT -A INPUT -p tcp -m tcp --dport 25 -j ACCEPT
$IPT -A INPUT -p tcp -m tcp --dport 465 -j ACCEPT
$IPT -A INPUT -p tcp -m tcp --dport 110 -j ACCEPT
$IPT -A INPUT -p tcp -m tcp --dport 995 -j ACCEPT
$IPT -A INPUT -p tcp -m tcp --dport 143 -j ACCEPT
$IPT -A INPUT -p tcp -m tcp --dport 993 -j ACCEPT
```

Для корректной работы DNS сервера, нужно открыть UDP порт 53

```
$IPT -A INPUT -i $WAN -p udp --dport 53 -j ACCEPT
```

И так далее. По аналогии можете открыть доступ для всех необходимых сервисов.

5. Проброс (forward) порта

Рассмотрим ситуацию, когда необходимо выполнить проброс портов с внешнего интерфейса на какой-то компьютер в локальной сети. Допустим, вам необходимо получить rdp доступ к компьютеру 10.1.3.50 из интернета. Делаем проброс TCP порта 3389:

```
$IPT -t nat -A PREROUTING -p tcp --dport 3389 -i ${WAN} -j DNAT --to 10.1.3.50
```

Если вы не хотите светить снаружи известным портом, то можно сделать перенаправление с нестандартного порта на порт rdp конечного компьютера:

```
$IPT -t nat -A PREROUTING -p tcp --dport 23543 -i ${WAN} -j DNAT --to 10.1.3.50:3389
```

Если вы пробрасываете порт снаружи внутрь локальной сети, то обязательно закомментируйте правило, которое блокирует доступ из внешней сети во внутреннюю. В моем примере это правило:

```
$IPT -A FORWARD -i $WAN -o $LAN1 -j REJECT
```

Либо перед этим правилом создайте разрешающее правило для доступа снаружи к внутреннему сервису, например вот так:

```
$IPT -A FORWARD -i $WAN -d 10.1.3.50 -p tcp -m tcp --dport 3389 -j ACCEPT
```

6. Включение логов

Во время настройки полезно включить логи, чтобы мониторить заблокированные пакеты и выяснять, почему отсутствует доступ к необходимым сервисам, которые мы вроде бы уже открыли. Я отправляю все заблокированные пакеты в отдельные цепочки (block_in, block_out, block_fw), соответствующие направлению трафика и маркирую в логах каждое направление. Так удобнее делать разбор полетов. Добавляем следующие правила в самый конец скрипта, перед сохранением настроек:

```
$IPT -N block_in
$IPT -N block_out
$IPT -N block_fw

$IPT -A INPUT -j block_in
$IPT -A OUTPUT -j block_out
$IPT -A FORWARD -j block_fw

$IPT -A block_in -j LOG --log-level info --log-prefix "--IN--BLOCK"
$IPT -A block_in -j DROP
$IPT -A block_out -j LOG --log-level info --log-prefix "--OUT--BLOCK"
$IPT -A block_out -j DROP
$IPT -A block_fw -j LOG --log-level info --log-prefix "--FW--BLOCK"
$IPT -A block_fw -j DROP
```

Все заблокированные пакеты вы сможете отследить в файле /var/log/messages.

После того, как закончите настройку, закомментируйте эти строки, отключив логирование. Обязательно стоит это сделать, так как логи очень быстро разрастаются. Практического смысла в хранении подобной информации лично я не вижу.

Как отключить iptables

Если вы вдруг решите, что firewall вам больше не нужен, то отключить его можно следующим образом:

```
# systemctl stop iptables.service
```

Эта команда останавливает фаервол. А следующая удаляет из автозагрузки:

```
# systemctl disable iptables.service
```

Отключив сетевой экран, мы разрешили все соединения.

Сделайте скриншоты (фотографии) процесса настройки IPTABLESи вставьте в отчёт.

Практическое занятие № 34. Установка и базовая настройка Kali Linux

Задание: Установите Kali Linux на виртуальную машину в VirtualBox. Подробно опишите процесс установки и параллельной настройки базовых функций Kali Linux.

Отчет должен содержать:

1. Процесс создания виртуальной машины с указанием выбранных параметров (ОЗУ, места хранения)
2. Процесс добавления выбранного образа Kali Linux.
3. Процесс установки Kali Linux. (в пункте добавление grub обязательно выбрать «да»).
4. Настройку сетевых параметров Kali Linux.
5. Итоговый скриншот, показывающий установку и работоспособности виртуальной машины.

   Ответ:

Практическое занятие № 35. Администрирование Kali Linux

Задание: установить настройки виртуальной машины с Kali Linux.

1. Создайте дополнительных пользователей – одного администратора, двух пользователей.
2. Установите сложные пароли всем пользователям.
3. Настройте SSH для удалённого доступа.
4. Настройте управление сервисами.
5. Запретите лишние порты.
6. Установите политики безопасности.
7. Установите брандмауэр netfilter.

Сделайте скриншоты (фотографии) процесса выполнения заданий и их результата

Практическое занятие №36. Установка и настройка утилит в Kali Linux

Задание: Установите Kali Linux на виртуальную машину в VirtualBox. Подробно опишите процесс установки и параллельной настройки базовых функций Kali Linux.

1. Установите распаковщик и установщик пакетов gdebi для дальнейшей работы.
2. Установите htop и nethogs для мониторинга ресурсов системы и сети.
3. Установите java, Phyton для облегчения дальнейшей работы.
4. Установите Atom editor для удобного редактирования кода.
5. Установите дополнительный набор инструментов для анализа уязвимостей Git.
6. Установите архиваторы Kali Linux
7. Установите дополнительный браузер

Сделайте скриншоты (фотографии) процесса выполнения заданий и их результата

Практическое занятие № 37. Поиск уязвимостей информационных систем

Задание:

Kali включает в себя очень способный OpenVAS, который является бесплатным и с открытым исходным кодом.

Это просто потому, что сканеры уязвимостей часто имеют слабую репутацию, прежде всего потому, что их роль и цель неправильно поняты.

Сканеры Vulnerabilty сканируют уязвимости – но они не являются волшебными машинами эксплойта и должны быть одним из многих источников информации, используемых в оценке безопасности.

Слепой запуск сканера уязвимостей на цель почти наверняка закончится разочарованием и горем, с десятками (или даже сотнями) результатов низкого уровня или неинформативных результатов.

1. Системные Требования

Основная жалоба, которую получают о OpenVAS (или любом другом сканере уязвимостей), можно резюмировать как «она слишком медленная и сбойная и не работает, и это плохо, и очень плохо».

Почти во всех случаях медленность и / или сбои связаны с недостаточными системными ресурсами.

OpenVAS имеет десятки тысяч сигнатур, и если вы не дадите вашей системе достаточного количества ресурсов, особенно оперативной памяти, вы окажетесь в мире страданий.

Для некоторых коммерческих сканеров уязвимостей требуется как минимум 8 ГБ ОЗУ и рекомендуется еще больше.

OpenVAS не требует около такого объема памяти, но чем больше вы можете предоставить ему, тем более плавно система сканирования будет работать.

Для этого урока наша виртуальная машина Kali имеет 3 процессора и 3 ГБ оперативной памяти, что обычно достаточно для сканирования небольшого количества хостов одновременно.

2. Начальная установка OpenVAS в Кали

У OpenVAS много движущихся частей, и настройка вручную может быть проблемой.
К счастью, Kali содержит простую в использовании утилиту под названием «openvas-setup», которая занимается настройкой OpenVAS, загрузкой сигнатур и созданием пароля для пользователя admin.
Эта первоначальная настройка может занять довольно много времени, даже при быстром подключении к Интернету, можно просто сидеть сложа руки.
В конце настройки будет отображаться автоматически созданный пароль для пользователя admin.
Обязательно сохраните этот пароль где-нибудь в безопасности.

```
root@kali:~# openvas-setup
ERROR: Directory for keys (/var/lib/openvas/private/CA) not found!
ERROR: Directory for certificates (/var/lib/openvas/CA) not found!
ERROR: CA key not found in /var/lib/openvas/private/CA/cakey.pem
ERROR: CA certificate not found in /var/lib/openvas/CA/cacert.pem
ERROR: CA certificate failed verification, see /tmp/tmp.7G2IQWtqwj/openvas-manage-certs.log for details. Aborting.ERROR: Your OpenVAS certificate infrastructure did NOT pass validation.
See messages above for details.
Generated private key in /tmp/tmp.PerU5lG2tl/cakey.pem.
Generated self signed certificate in /tmp/tmp.PerU5lG2tl/cacert.pem.
...
/usr/sbin/openvasmd
User created with password 'xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx'.
```

3. Работа с ошибками установки

Иногда скрипт «openvas-setup» будет отображать ошибки в конце загрузки NVT, аналогичные приведенным ниже.

```
(openvassd:2272): lib kb_redis-CRITICAL **: get_redis_ctx: redis connection error: No such file or directory
(openvassd:2272): lib kb_redis-CRITICAL **: redis_new: cannot access redis at '/var/run/redis/redis.sock'
(openvassd:2272): lib kb_redis-CRITICAL **: get_redis_ctx: redis connection error: No such file or directory
openvassd: no process found
```

Если вам посчастливилось столкнуться с этой проблемой, вы можете запустить «openvas-check-setup», чтобы узнать, какой компонент вызывает проблемы.
В этом конкретном случае мы получаем следующее из скрипта:

```
...
ERROR: The number of NVTs in the OpenVAS Manager database is too low.
FIX: Make sure OpenVAS Scanner is running with an up-to-date NVT collection and run 'openvasmd --rebuild'.
...
```

Скрипт «openvas-check-setup» обнаруживает проблему и даже предоставляет команду для запуска (надеюсь) решения этой проблемы.
После восстановления коллекции NVT рекомендуется пройти все проверки.

```
root@kali:~# openvasmd --rebuild
root@kali:~# openvas-check-setup
```

```
openvas-check-setup 2.3.7
Test completeness and readiness of OpenVAS-9
...
It seems like your OpenVAS-9 installation is OK.
...
```

4. Управление пользователями OpenVAS

Если вам нужно (или хотите) создать дополнительных пользователей OpenVAS, запустите ‘openvasmd’ с параметром -create-user, который добавит нового пользователя и отобразит случайно сгенерированный пароль.

```
root@kali:~# openvasmd --create-user=dookie
User created with password 'yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyy'.
root@kali:~# openvasmd --get-users
admin
dookie
```

К счастью, изменение паролей пользователей OpenVAS легко осуществляется с помощью опции «openvasmd» и «new-password».

```
root@kali:~# openvasmd --user=dookie --new-password=s3cr3t
root@kali:~# openvasmd --user=admin --new-password=sup3rs3cr3t
```

5. Запуск и остановка OpenVAS

Сетевые службы по умолчанию отключены в Kali Linux, поэтому, если вы не настроили OpenVAS для запуска при загрузке, вы можете запустить необходимые службы, запустив «openvas-start».

```
root@kali:~# openvas-start
Starting OpenVas ServicesПосле того, как у вас есть список хо-
стов, вы можете импортировать их в разделе «Цели» в меню «Конфи-
гурация».
```

Когда службы завершают инициализацию, вы должны найти TCP-порты 9390 и 9392, которые прослушивают ваш loopback-интерфейс.

```
root@kali:~# ss -ant
State Recv-Q Send-Q Local Address:Port Peer Address:Port
LISTEN 0 128 127.0.0.1:9390 *:*
LISTEN 0 128 127.0.0.1:9392 *:*
```

Из-за нагрузки на системные ресурсы вы, вероятно, захотите остановить OpenVAS, когда вы закончите использовать его, особенно если вы не используете специальную систему для сканирования уязвимостей.

OpenVAS можно остановить, запустив «openvas-stop».

```
root@kali:~# openvas-stop
Stopping OpenVas Services
```

6. Использование Greenbone Security Assistant

Greenbone Security Assistant – это веб-интерфейс OpenVAS, доступный на вашем локальном компьютере (после запуска OpenVAS) на **https://localhost: 9392.**

После принятия самозаверенного сертификата вам будет представлена страница входа в систему и после аутентификации вы увидите основную панель.

Рис. 329

7. Настройка учетных данных

Сканеры уязвимостей обеспечивают наиболее полные результаты, когда вы можете предоставить механизму сканирования учетные данные для использования на сканируемых системах.

OpenVAS будет использовать эти учетные данные для входа в сканированную систему и выполнения подробного перечисления установленного программного обеспечения, патчей и т. д.

Вы можете добавить учетные данные через запись «Credentials» в меню «Configuration».

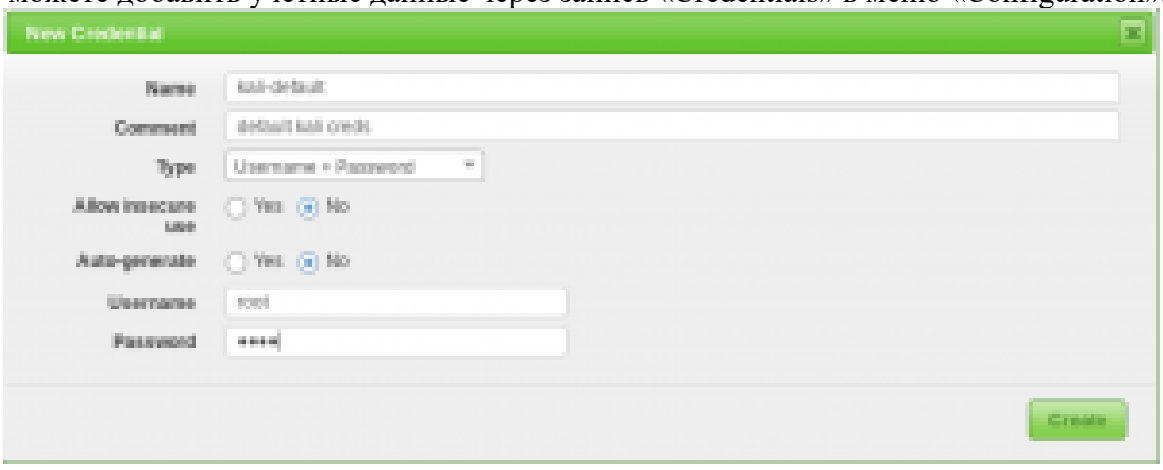


Рис. 330

8. Конфигурация цели

OpenVAS, как и большинство сканеров уязвимостей, может сканировать удаленные системы, но это сканер уязвимостей, а не сканер портов.

Вместо того, чтобы полагаться на сканер уязвимостей для идентификации хостов, вы значительно упростите свою жизнь с помощью специализированного сетевого сканера, такого как Nmap или Masscan, и импортируйте список целей в OpenVAS.

```
root@kali:~# nmap -sn -oA nmap-subnet-86 192.168.86.0/24
root@kali:~# grep Up nmap-subnet-86.gnmap | cut -d " " -f 2 >
live-hosts.txt
```

После того, как у вас есть список хостов, вы можете импортировать их в разделе «target» в меню «Configuration».

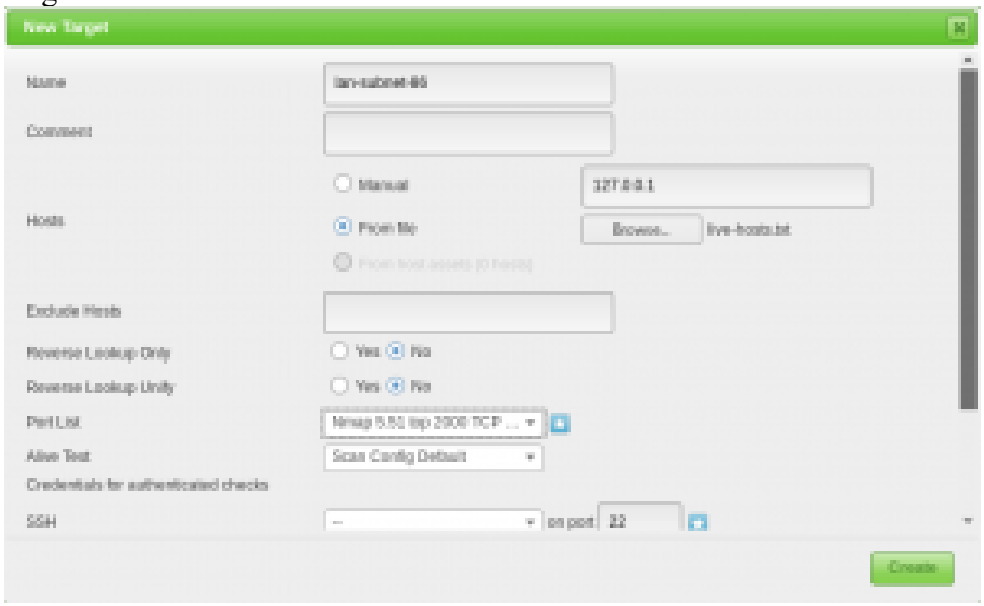


Рис. 331

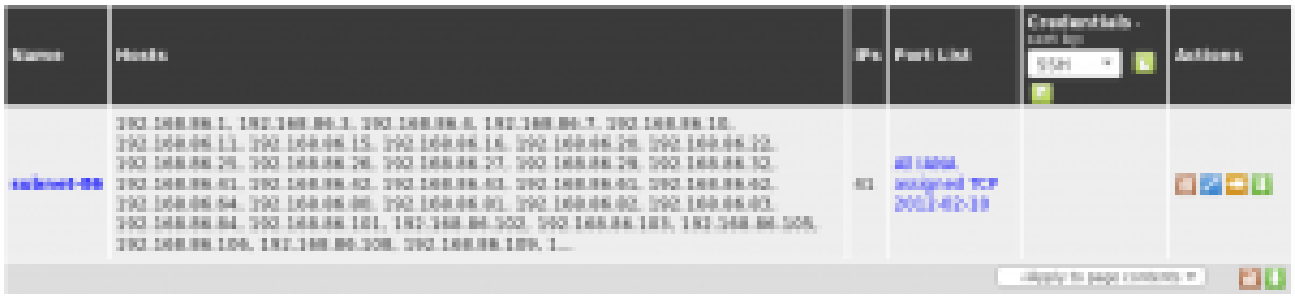


Рис. 332

9. Конфигурация сканирования

Перед запуском сканирования уязвимостей вы должны точно настроить Scan Config/,
Это можно сделать в разделе “Scan Configs” в меню “Config”.
Вы можете клонировать любую конфигурацию сканирования по умолчанию и редактировать ее параметры, отключая любые службы или проверки, которые вам не нужны.
Если вы используете Nmap для проведения предварительного анализа ваших целевых объектов, вы можете сэкономить время сканирования уязвимости.

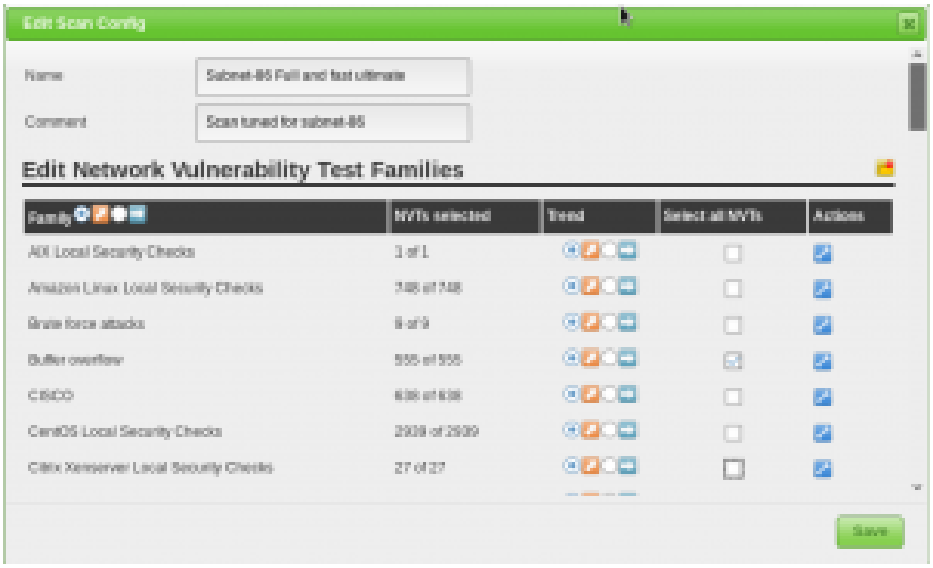


Рис. 333

10. Конфигурация задачи

Ваши учетные данные, цели и конфигурации сканирования настроены таким образом, что теперь вы готовы собрать все вместе и запустить сканирование уязвимостей.

В OpenVAS сканирование уязвимостей проводится как «tasks».

Когда вы настраиваете новую задачу, вы можете дополнительно оптимизировать сканирование путем увеличения или уменьшения одновременных действий, которые происходят.

С нашей системой с 2 ГБ оперативной памяти мы скорректировали наши настройки задач, как показано ниже.

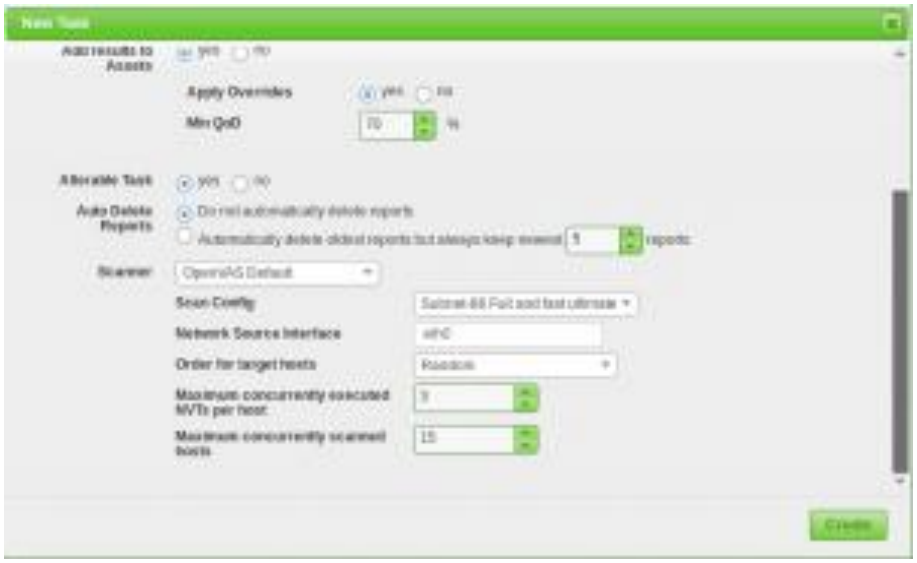


Рис. 334

Благодаря нашим более точно настроенным параметрам сканирования и целевому выбору результаты нашего сканирования намного полезнее.

Рис. 335

11. Автоматизация OpenVAS

Одной из менее известных функций OpenVAS является интерфейс командной строки, с которым вы взаимодействуете с помощью команды «omp».

Его использование не совсем интуитивно, но мы не единственные поклонники OpenVAS, и мы столкнулись с несколькими базовыми скриптами, которые вы можете использовать и расширить сканирование для автоматизации OpenVAS.

Первый – openvas-automate.sh от mgeeky, полуинтерактивный скрипт Bash, который предлагает вам тип сканирования и заботится обо всем остальном.

Конфигурации сканирования жестко закодированы в сценарии, поэтому, если вы хотите использовать свои настроенные конфиги, их можно добавить в разделе «targets».

```
root@kali:~# apt -y install pcregrep
root@kali:~# ./openvas-automate.sh 192.168.86.61:: OpenVAS auto-
mation script.
mgeeky, 0.1[>] Please select scan type:
1. Discovery
2. Full and fast
3. Full and fast ultimate
4. Full and very deep
5. Full and very deep ultimate
6. Host Discovery
7. System Discovery
9. Exit

--------------------------------
Please select an option: 5

[+] Tasked: 'Full and very deep ultimate' scan against
'192.168.86.61'
[>] Reusing target...
[+] Target's id: 6ccbb036-4afa-46d8-b0c0-acbd262532e5
[>] Creating a task...
[+] Task created successfully, id: '8e77181c-07ac-4d2c-ad30-
9ae7a281d0f8'
[>] Starting the task...
[+] Task started. Report id: 6bf0ec08-9c60-4eb5-a0ad-
33577a646c9b
[.] Awaiting for it to finish. This will take a long while...
```

```
8e77181c-07ac-4d2c-ad30-9ae7a281d0f8 Running 1% 192.168.86.61
```

Мы также наткнулись на сообщение в блоге по code16, которое представляет и объясняет их скрипт Python для взаимодействия с OpenVAS.

Подобно скрипту Bash выше, вам нужно будет внести некоторые изменения в скрипт, если вы хотите настроить тип сканирования.

```
root@kali:~# ./code16.py 192.168.86.27
-------------------------------------------------------------------
--------------
code16
-------------------------------------------------------------------
--------------
small wrapper for OpenVAS 6[+] Found target ID: 19f3bf20-441c-
49b9-823d-11ef3b3d18c2
[+] Preparing options for the scan...
[+] Task ID = 28c527f8-b01c-4217-b878-0b536c6e6416
[+] Running scan for 192.168.86.27
[+]   Scan   started...   To   get   current   status,   see   be-
low:zZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZz
zZzzZzzZzzZzzZzz
...
zZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzzZzz
ZzzZzzZzzZzz
[+] Scan looks to be done. Good.
[+] Target scanned. Finished taskID : 28c527f8-b01c-4217-b878-
0b536c6e6416
[+] Cool! We can generate some reports now ... :)
[+] Looking for report ID...
[+] Found report ID : 5ddcb4ed-4f96-4cee-b7f3-b7dad6e16cc6
[+] For taskID : 28c527f8-b01c-4217-b878-0b536c6e6416
[+] Preparing report in PDF for 192.168.86.27
[+] Report should be done in : Report_for_192.168.86.27.pdf
[+] Thanks. Cheers!
```

Сделайте скриншоты (фотографии) процесса поиска уязвимостей информационных систем и вставьте в отчёт.

Практическое занятие № 38. Применение антивирусной защиты

Задание: протестировать антивирусное средство.

1. Установите на виртуальную машину с Windows 10 антивирусное средство Kaspersky.
2. Изучить настройки антивирусной программы (отразить в отчете).
3. Провести тестирование системной памяти, объектов автозапуска, жестких дисков (отчет в отчет по лабораторной работе, получить подробный отчет).
4. Необходимо скачать тестовый файл eicar и распаковать его (https://support.kaspersky.ru/common/diagnostics/7399).
5. Проверить диски компьютера на наличие вирусов (получить подробный отчет), должен быть обнаружен скачанный вирус.
6. Повторить пункт 4, далее требуется скачать и запустить программу DrWebCureit (https://free.drweb.ru/download+cureit+free/) и выполнить проверку компьютера на наличие вирусов. Если на дисках будут обнаружены вирусы, выполнить лечение зараженных файлов.

7. Посетить web-страницу https://www.broadcom.com/support/security-center/a-zонлайн-экспедиции вирусов на сайте компания Symantec. На этой странице можно просмотреть, чем заражен тот или иной файл и как удалить этот вирус. Выбрать любой вирус и описать его.

Сделайте скриншоты процесса выполнения заданий. Опишите все выполненные действия и получившиеся результаты.

Практическое занятие № 39. Настройка безопасности веб-браузеров

Задание: установить дополнительные параметры для повышения безопасности веб-браузеров.

В браузерах Yandex и Google Chrome выполните следующие действия:

1. Установите автоматическое обновление.
2. Запретите сохранять пароли внутри браузера.
3. Отключите синхронизацию устройств.
4. Запретите сайтам отслеживание местоположения
5. Запретите сайтам отслеживание действий
6. Установите настройки конфиденциальности

Сделайте скриншоты процесса выполнения заданий. Опишите все выполненные действия и получившиеся результаты. Объясните, как эти действия помогают повысить безопасность.

Практическое занятие № 40. Оценка рисков информационной безопасности с использованием классификации веб-угроз

Задание:

Провести «светофорную» оценку риска каждой веб-угрозы для смоделированной организации используя полученные результаты из практической работы №29. Заполнить таблицу. (Воспользоваться таблицей выше)

Название угрозы	Возможность угрозы	Последствия	Уровень риска

В настоящий момент существует множество методик оценки опасности уязвимости, но наиболее распространены следующие подходы:

- классическая «светофорная» оценка, выделяющая уязвимости «высокой», «средней» и «низкой» степени риска;
- пятиуровневая модель, принятая в стандарте PSI DSS и определяющая уровни «критичный», «неотложный», «высокий», «средний» и «низкий» (Urgent, Critical, High, Medium, Low)
- метод Common Vulnerability Scoring System (CVSS) , оценивающий степень риска как число от 0 до 10.

Классы атак

1. Аутентификация (Authentication)

Раздел, посвященный аутентификации, описывает атаки направленные на используемые Web-приложением методы проверки идентификатора пользователя, службы или приложения. Аутентификация использует как минимум один из трех механизмов (факторов): "что-то, что мы имеем", "что-то, что мы знаем" или "что-то, что мы есть". В этом разделе описываются атаки, направленные на обход или эксплуатацию уязвимостей в механизмах реализации аутентификации Web-серверов.

1. Подбор (Brute Force)

автоматизированный процесс проб и ошибок, использующийся для того, чтобы угадать имя пользователя, пароль, номер кредитной карточки, ключ шифрования и т.д.

2. Недостаточная аутентификация (Insufficient Authentication)

эта уязвимость возникает, когда Web-сервер позволяет атакующему получать доступ к важной информации или функциям сервера без должной аутентификации

3. Небезопасное восстановление паролей (Weak Password Recovery Validation)

эта уязвимость возникает, когда Web-сервер позволяет атакующему несанкционированно получать, модифицировать или восстанавливать пароли других пользователей

2. Авторизация (Authorization)

Данный раздел посвящен атакам, направленным на методы, которые используются Web-сервером для определения того, имеет ли пользователь, служба или приложение необходимые для совершения действия разрешения. Многие Web-сайты разрешают только определенным пользователям получать доступ к некоторому содержимому или функциям приложения. Доступ другим пользователям должен быть ограничен. Используя различные техники, злоумышленник может повысить свои привилегии и получить доступ к защищенным ресурсам.

1. Предсказуемое значение идентификатора сессии (Credential/Session Prediction)

предсказуемое значение идентификатора сессии позволяет перехватывать сессии других пользователей

2. Недостаточная авторизация (Insufficient Authorization)

недостаточная авторизация возникает, когда Web-сервер позволяет атакующему получать доступ к важной информации или функциям, доступ к которым должен быть ограничен

3. Отсутствие таймаута сессии (Insufficient Session Expiration)

в случае если для идентификатора сессии или учетных данных не предусмотрен таймаут или его значение слишком велико, злоумышленник может воспользоваться старыми данными для авторизации

4. Фиксация сессии (Session Fixation)

используя данный класс атак, злоумышленник присваивает идентификатору сессии пользователя заданное значение

3. Атаки на клиентов (Client-side Attacks)

Этот раздел описывает атаки на пользователей Web-сервера. Во время посещения сайта, между пользователем и севером устанавливаются доверительные отношения, как в технологическом, так и в психологическом аспектах. Пользователь ожидает, что сайт предоставит ему легитимное содержимое. Кроме того, пользователь не ожидает атак со стороны сайта. Эксплуатируя это доверие, злоумышленник может использовать различные методы для проведения атак на клиентов сервера.

1. Подмена содержимого (Content Spoofing)

используя эту технику, злоумышленник заставляет пользователя поверить, что страницы сгенерированны Web-сервером, а не переданы из внешнего источника

2. Межсайтовое выполнение сценариев (Cross-site Scripting, XSS)

наличие уязвимости Cross-site Scripting позволяет атакующему передать серверу исполняемый код, который будет перенаправлен браузеру пользователя

3. Расщепление HTTP-запроса (HTTP Response Splitting)

при использовании данной уязвимости злоумышленник посылает серверу специальным образом сформированный запрос, ответ на который интерпретируется целью атаки как два разных ответа

4. Выполнение кода (Command Execution)

Эта секция описывает атаки, направленные на выполнение кода на Web-сервере. Все серверы используют данные, преданные пользователем при обработке запросов. Часто эти данные используются при составлении команд, применяемых для генерации динамического содержимого. Если при разработке не учитываются требования безопасности, злоумышленник получает возможность модифицировать исполняемые команды.

1. Переполнение буфера (Buffer Overflow)

эксплуатация переполнения буфера позволяет злоумышленнику изменить путь исполнения программы путем перезаписи данных в памяти системы

2. Атака на функции форматирования строк (Format String Attack)

при использовании этих атак путь исполнения программы модифицируется методои перезаписи областей памяти с помощью функций форматирования символьных переменных

3. Внедрение операторов LDAP (LDAP Injection)

атаки этого типа направлены на Web-серверы, создающие запросы к службе LDAP на основе данных, вводимых пользователем

4. Выполнение команд ОС (OS Commanding)

атаки этого класса направлены на выполнение команд операционной системы на Web-сервере путем манипуляции входными данными

5. Внедрение операторов SQL (SQL Injection)

эти атаки направлены на Web-серверы, создающие SQL запросы к серверам СУБД на основе данных, вводимых пользователем

6. Внедрение серверных сценариев (SSI Injection)

атаки данного класса позволяют злоумышленнику передать исполняемый код, который в дальнейшем будет выполнен на Web-сервере

7. Внедрение операторов XPath (XPath Injection)

эти атаки направлены на Web-серверы, создающие запросы на языке XPath на основе данных, вводимых пользователем

5. Разглашение информации (Information Disclosure)

Атаки данного класса направлены на получение дополнительной информации о Web-приложении. Используя эти уязвимости, злоумышленник может определить используемые дистрибутивы ПО, номера версий клиента и сервера и установленные обновления. В других случаях, в утекающей информации может содержаться расположение временных файлов или резервных копий. Во многих случаях эти данные не требуются для работы пользователя. Большинство серверов предоставляют доступ к чрезмерному объему данных, однако необходимо минимизировать объем служебной информации. Чем большими знаниями о приложении будет располагать злоумышленник, тем легче ему будет скомпрометировать систему.

1. Индексирование директорий (Directory Indexing)

атаки данного класса позволяют атакующему получить информацию о наличии файлов в Web каталоге, которые недоступны при обычной навигации по Web сайту

2. Идентификация приложений (Web Server/Application Fingerprinting)

определение версий приложений используется злоумышленником для получения информации об используемых сервером и клиентом операционных системах, Web-северах и браузерах

3. Утечка информации (Information Leakage)

эти уязвимости возникают в ситуациях, когда сервер публикует важную информацию, например, комментарии разработчиков или сообщения об ошибках, которая может быть использована для компрометации системы

4. Обратный путь в директориях (Path Traversal)

данная техника атак направлена на получение доступа к файлам, директориям и командам, находящимся вне основной директории Web-сервера.

5. Предсказуемое расположение ресурсов (Predictable Resource Location)

позволяет злоумышленнику получить доступ к скрытым данным или функциональным возможностя

6. Логические атаки (Logical Attacks)

Атаки данного класса направлены на эксплуатацию функций приложения или логики его функционирования. Логика приложения представляет собой ожидаемый процесс функционирования программы при выполнении определенных действий. В качестве примеров можно привести восстановление пролей, регистрацию учетных записей, , аукционные торги, транзакции в системах электронной коммерции. Приложение может требовать от пользователя корректного выполнения нескольких последовательных действий для выполнения определенной задачи. Злоумышленник может обойти или использовать эти механизмы в своих целях.

1. Злоупотребление функциональными возможностями (Abuse of Functionality)

данные атаки направлены на использование функций Web-приложения с целью обхода механизмов разграничение доступа

2. Отказ в обслуживании (Denial of Service)

данный класс атак направлен на нарушение доступности Web-сервера

3. Недостаточное противодействие автоматизации (Insufficient Anti-automation). Эти уязвимости возникают в случае, если сервер позволяет автоматически выполнять операции, которые должны проводиться вручную

4. Недостаточная проверка процесса (Insufficient Process Validation). Уязвимости этого класса возникают, когда сервер недостаточно проверяет последовательность выполнения операций приложения.

Практическое занятие № 41. Сканирование системы с помощью IP-сканера

Задание: провести сканирование сети IP-сканером Windows

1. Запустите улучшенный IP сканнер (Windows 10).

2. Главное окно программы.

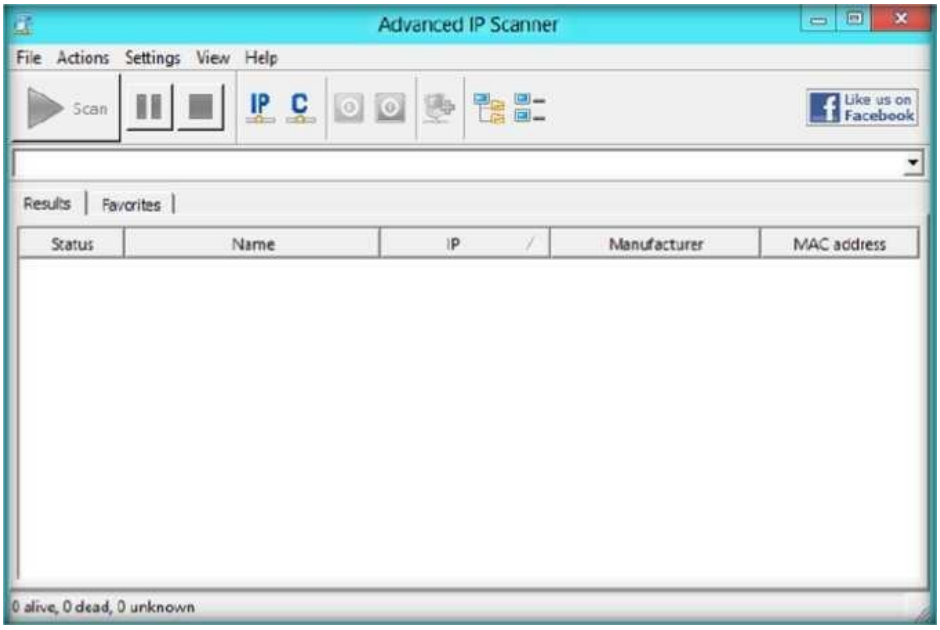


Рисунок 1.3.: Главное окно программы

3. Теперь запустите виртуальную машину Server 2019.

4. Теперь вернитесь в атакующую машину Windows и введите IP адрес в поле.

5. Начните сканирование.

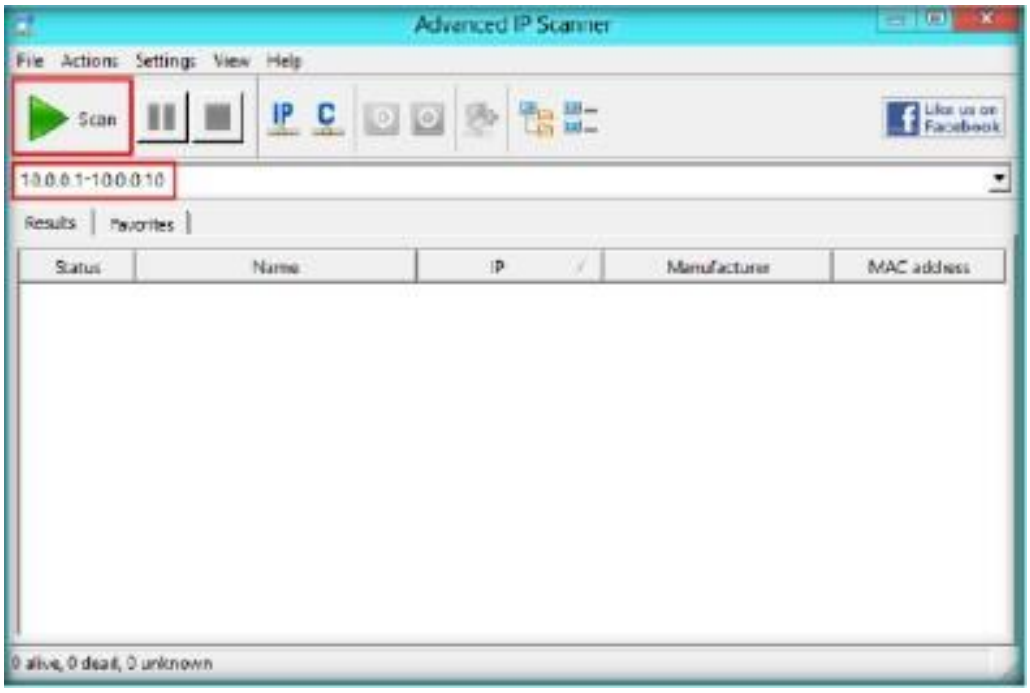


Рисунок 1.5: Сканирование

6. Усовершенствованный сканер IP сканирует все IP-адреса в диапазоне и выводит на экран результаты сканирования после завершения.

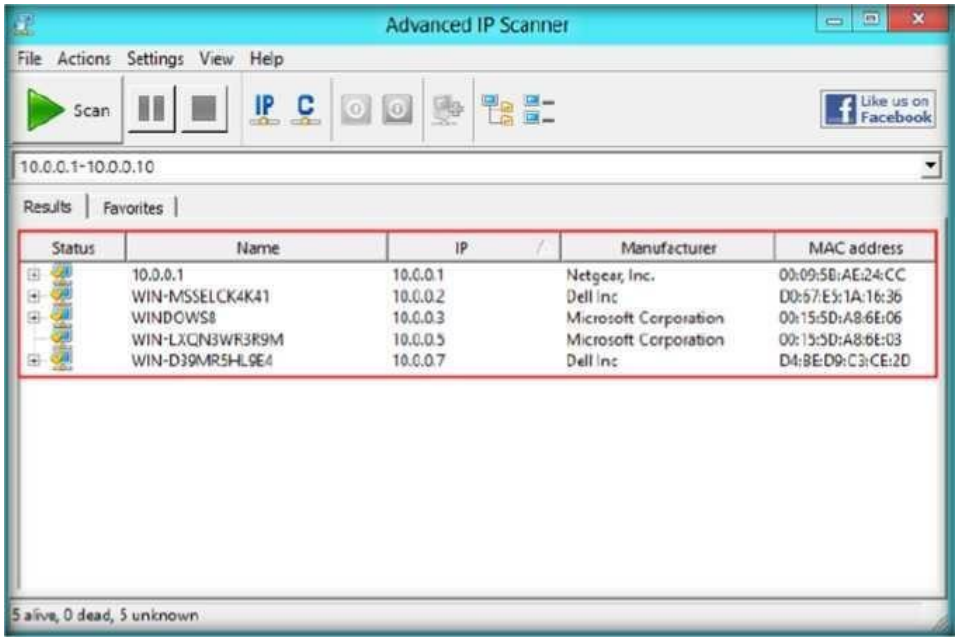


Рисунок 1.6: Результат сканирования

7. Сканер обнаружил IP адрес жертвы и ее состояние, как живое.
8. Правой мышкой на IP вызовите меню.

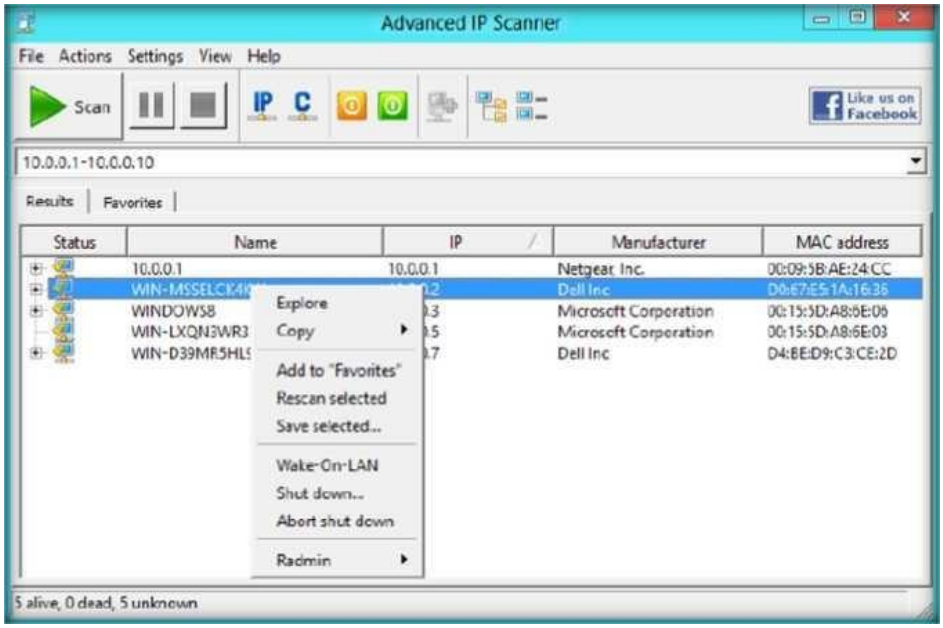


Рисунок 1.7: Меню

9. В результате сканер выводит на экран свойства обнаруженного компьютера, такие как IP-адрес. Имя, MAC и информация о NetBIOS.
10. Вы можете завершить работу, перезагрузить или аварийное выключить машину жертвы.

Рисунок 1.8: Дополнительные свойства

11. Полученная информация о машине жертвы.

Анализ практической работы

Запишите все полученные IP адреса, открытые порты, запущенные приложения и протоколы.

Средства	Собранная информация
Advanced IP Scanner	Информация: – IP адрес; – Имя системы; – MAC адрес; – Информация NetBIOS; – производитель; – статус системы.

Вопросы

1. Исследуйте и оцените IP-адреса и диапазон IP-адресов.

Практическое занятие № 42. Сканирование системы с помощью CFI LanGuard

Задание: просканировать систему Windows Server 2019

Следуя шагам мастера установки установите GFI LANguard network scanner на хост машину.

1. Нажмите Пуск.
2. Запустите GFI LANguard.

Рисунок 5.2 Windows Server 2019 – приложения

3. Главное окно GFI LanGuard 2012.

Рисунок 5.3: The GFI LANguard

4. Нажмите запустить сканирование GFI LANguard.

Рисунок 5.4: The GFI LANguard

5. Откроется новое окно сканирования.
   - В Scan Target, выберите localhost.
   - В Profile option, выберите Full Scan.
   - В Credentials option, выберите currently logged on user.
6. Нажмите Scan.

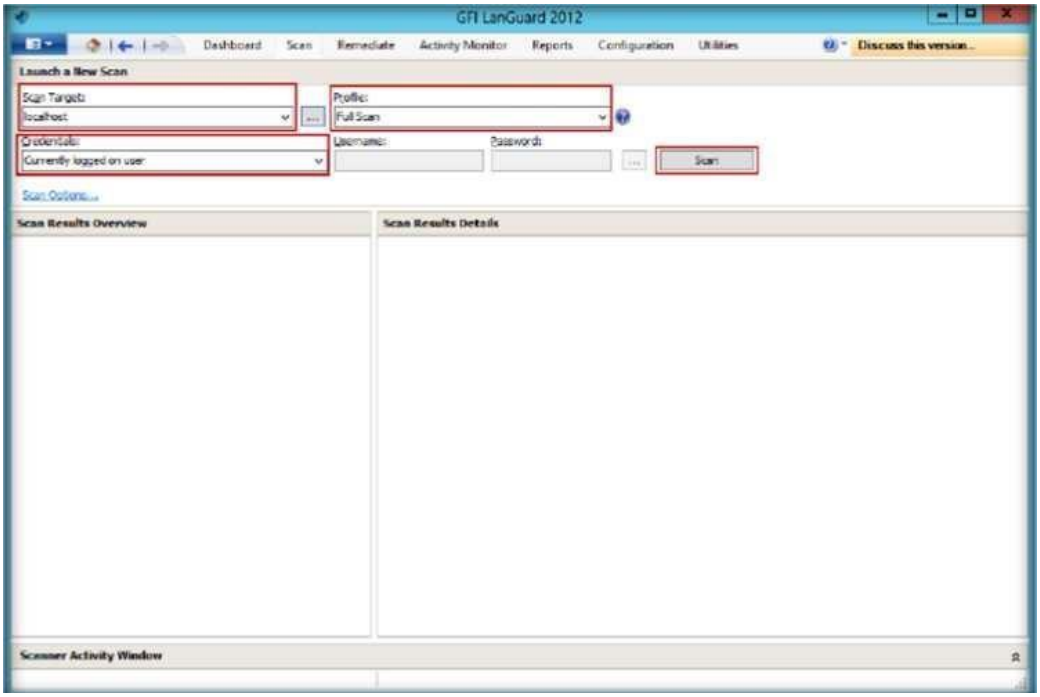


Рисунок 5.5: Настройки

7. Сканирование запустилось и оно займёт какое то время, которое указанно ниже.

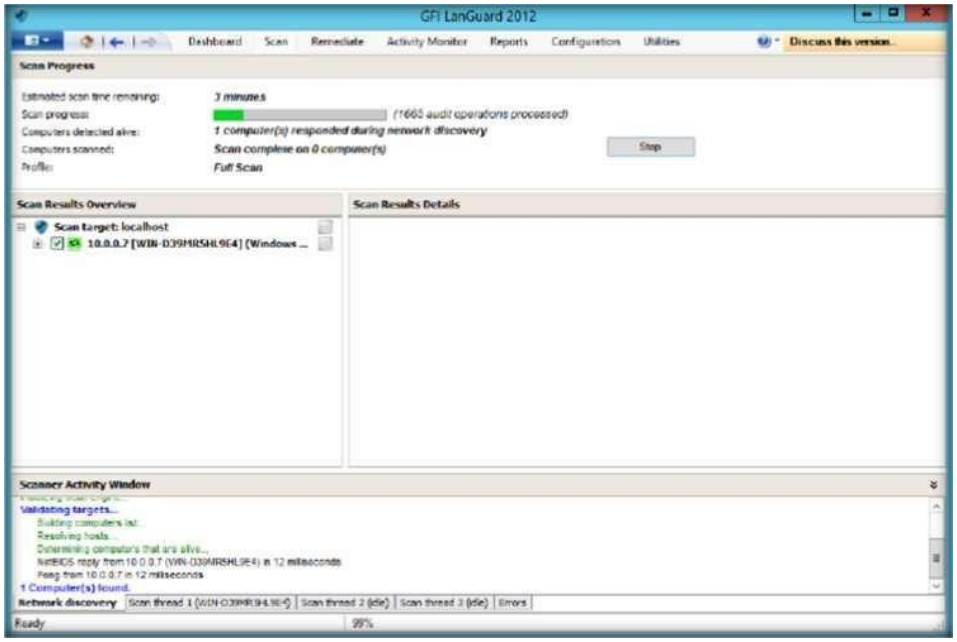


Рисунок 5.6: The GFI LanGuard

8. После завершения сканирование, вы увидите результат.

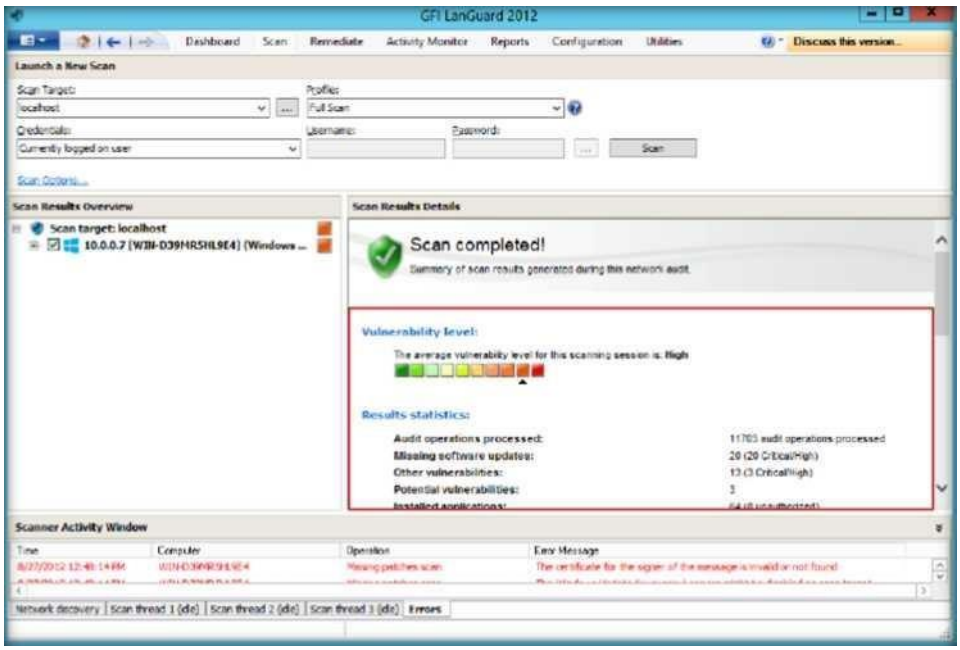


Рисунок 5.7: The GFI LanGuard

9. Чтобы просмотреть результат сканирования щелкните по IP адресу.
10. Нажмите Vulnerability Assessment, это покажет оценку уязвимостей и аудит По и сети

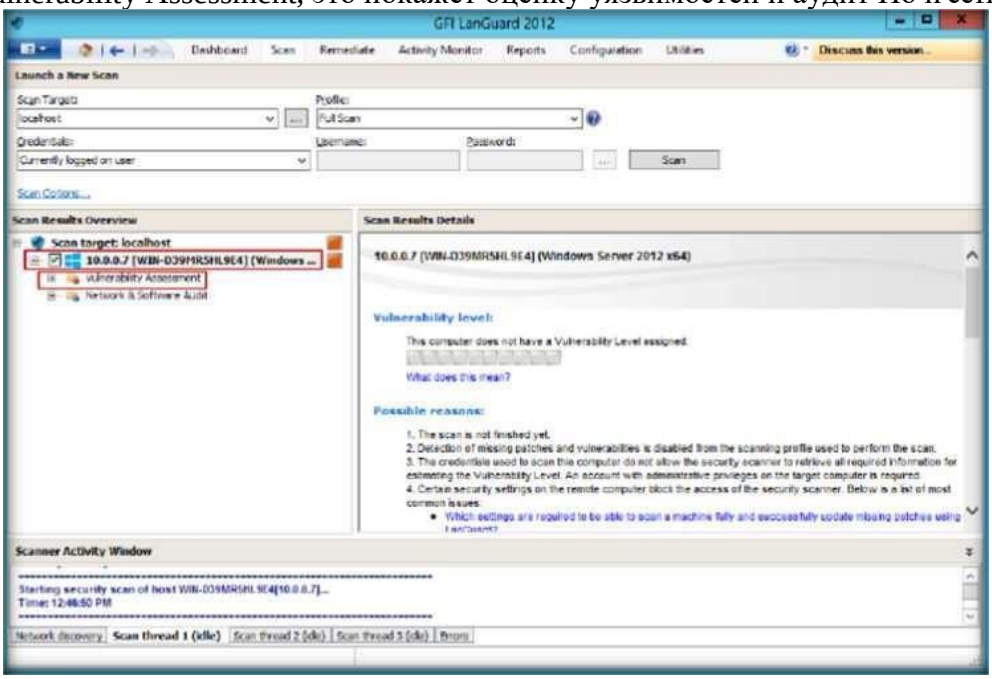


Рисунок 5.8: Vulnerability Assessment

11. Это покажет все индикаторы Vulnerability Assessment по категориям.

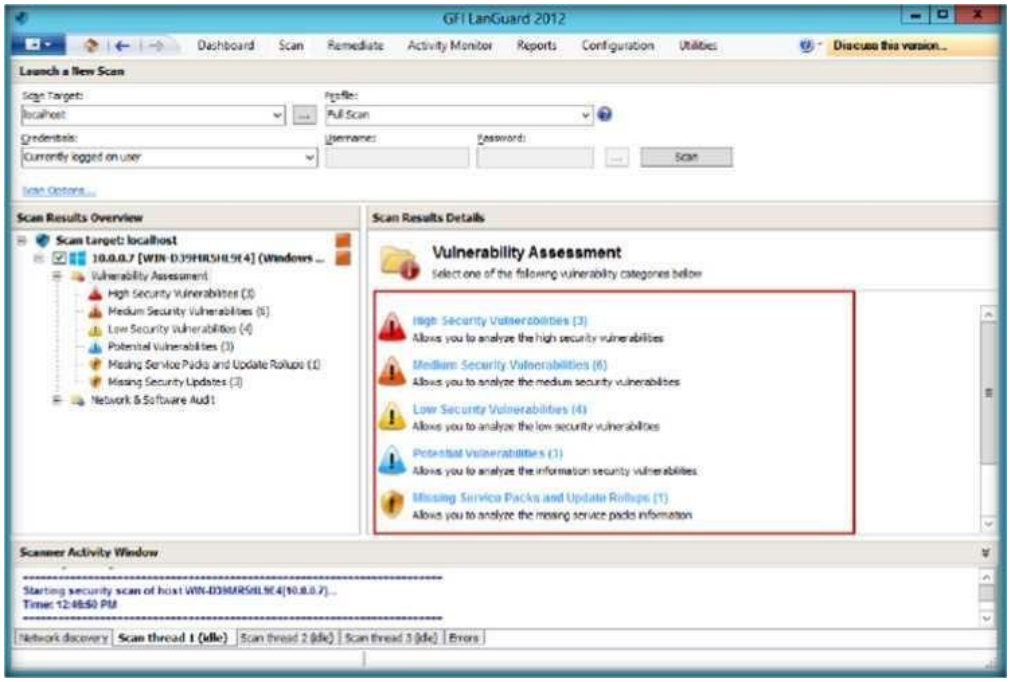


Рисунок 5.9: Категории Vulnerability Assessment

12. Нажмите Network & Software Audit и потом System Patching Status, который покажет все системные исправления.

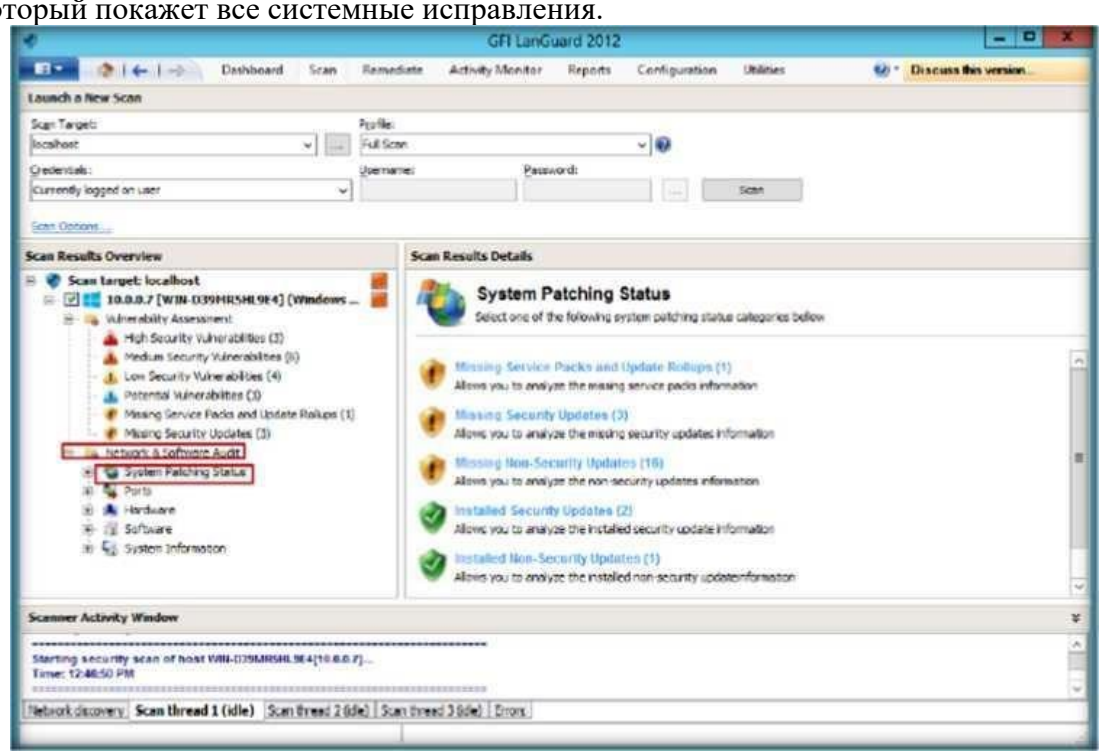


Рисунок 5.10: Состояние обновлений

13. Нажмите Ports, затем Open TCP Ports.

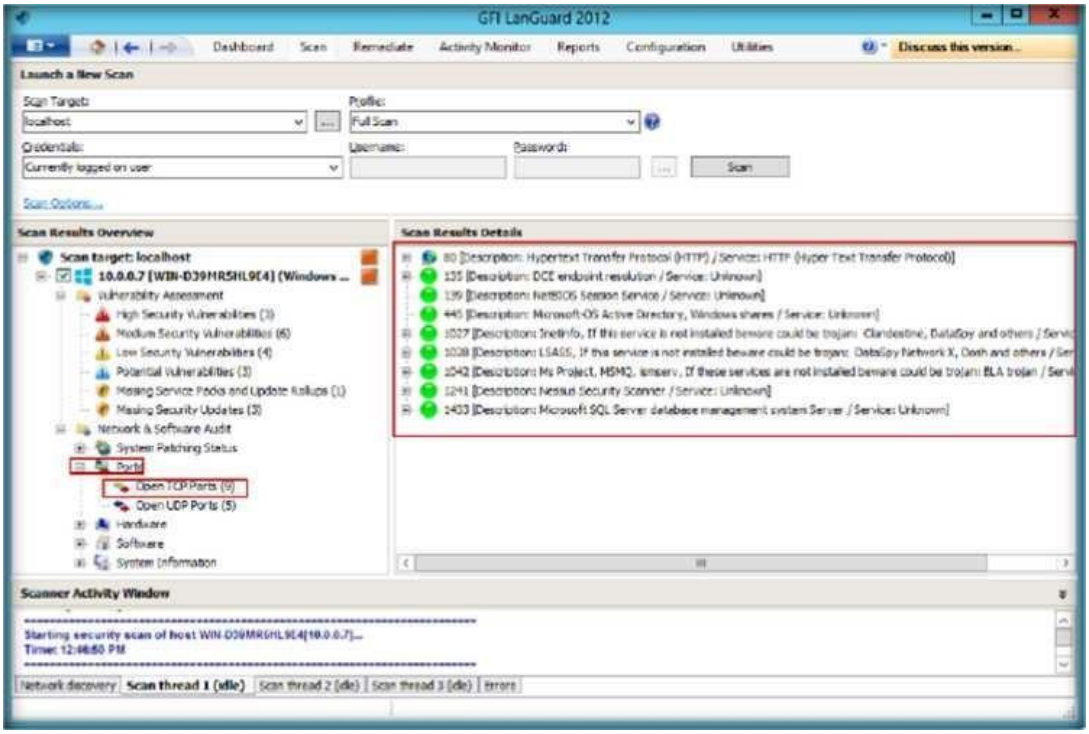


Рисунок 5.11: TCP/UDP Порты

14. Нажмите System Information, которая покажет всю системную информацию.
15. Нажмите Password Policy.

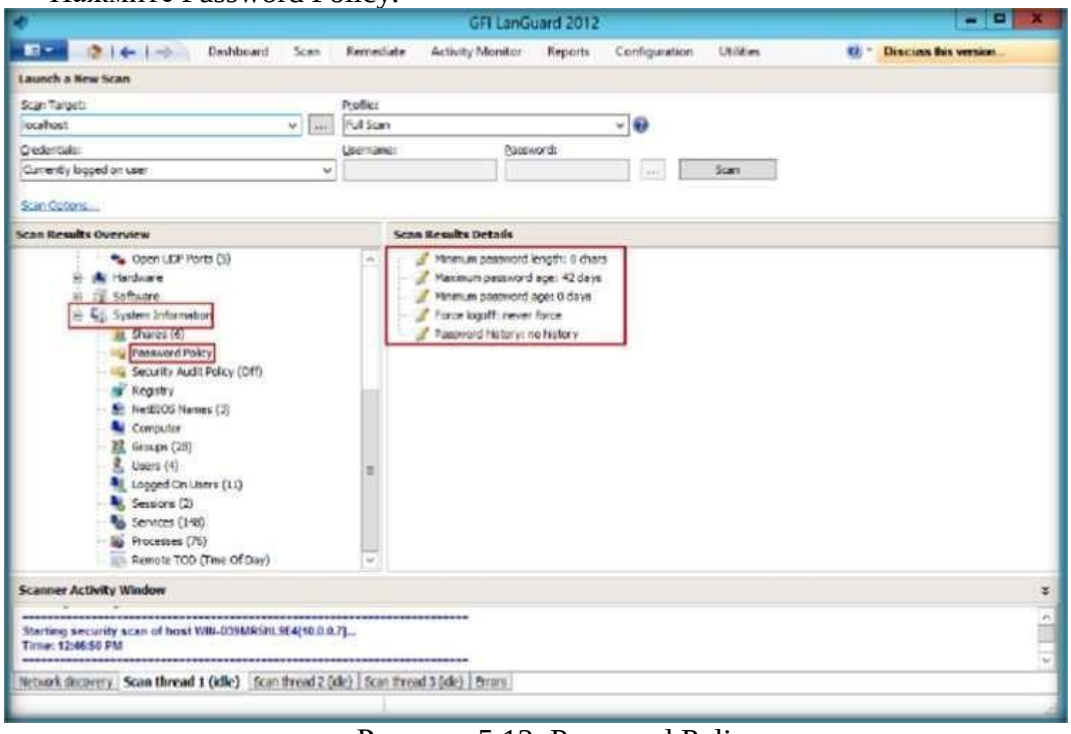


Рисунок 5.12: Password Policy

16. Нажмите Groups, которая покажет все группы в системе.

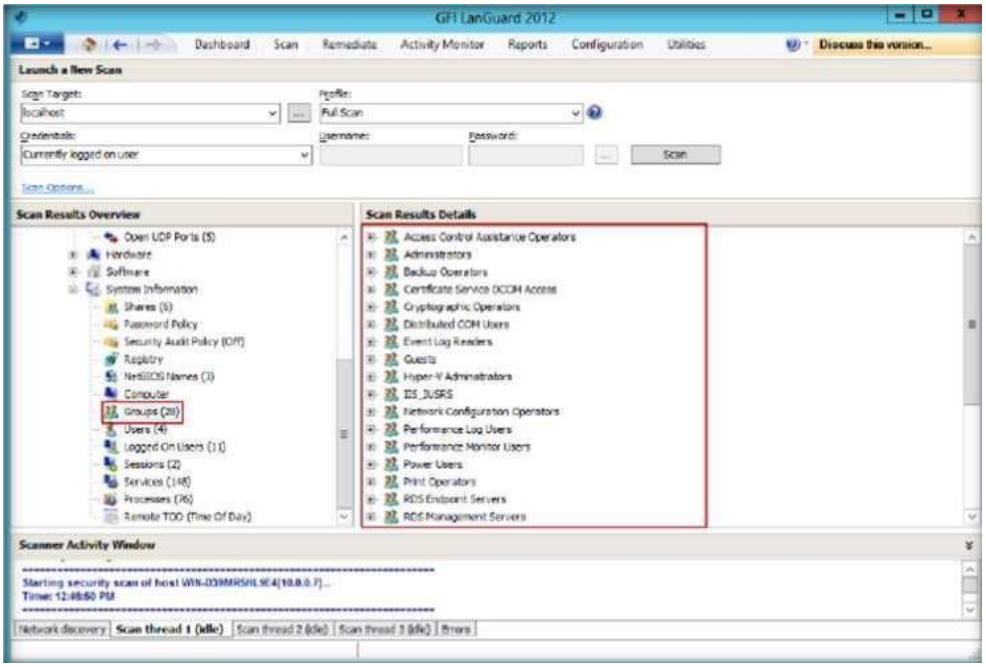


Рисунок 5.13: Информация о группах Groups

17. Нажмите Dashboard tab, которая покажет всю информацию сети.

Рисунок 5.14: Отчет состояния сети

Запишите все результаты, угрозы и уязвимости обнаруженные во время сканирования проведенного в практической.

Средства	**Собранная информация**
The GFI LANguard	Уровень уязвимостей
	Оценка уязвимостей
	Состояние системного исправления
	Детали сканирования открытых портов TCP

	Детали результатов сканирования для политики паролей
	Вся сеть: – Уровень уязвимостей – Датчики безопасности – Уязвимые компьютеры – Состояние агента – Тенденция уязвимостей в течении времени – Распределение уязвимостей

Вопросы

1. Проанализируйте как GFI LANguard защищает против червей.
2. При каких обстоятельствах GFI LANguard вывод диалог во время патча.
3. Вы можете изменить сообщение, выведенное на экран, когда GFI LANguard выполняет административные задачи? Если да, то как?

Практическое занятие № 43. Поиск открытых портов

Задание: просканировать открытые порты и найти цифровые отпечатки.

1. Запустите amap www.certifiedhacker.com 80.

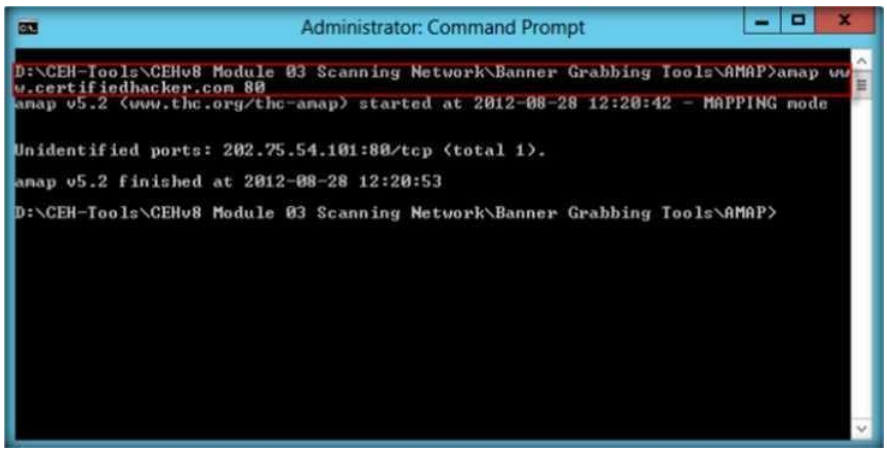


Рисунок 3.1: Amap www.ceitifiedhacker.com с Port 80

2. Видно, что определённые прикладные протоколы работают для введенного имени хоста и 80 порта.
3. Используйте IP адрес для проверки приложений на порту.
4. В командной строке введите IP своего локального Windows Server 2008 amap

10.0.0.4 75-81 и нажмите enter.

5. Попытайтесь просканировать различные веб-сайты используя различные ди

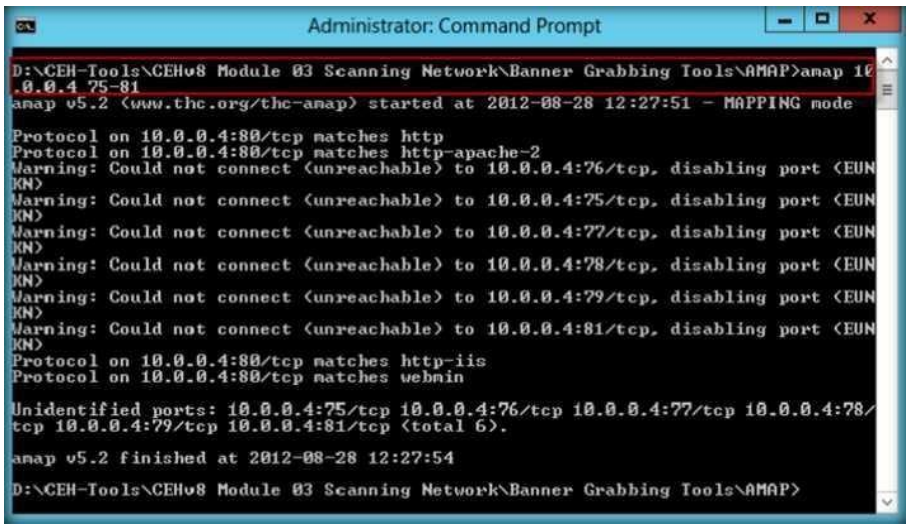


Рисунок 3.2: Amap с IP в диапозоне 75-81

Анализ практической работы

Запишите все IP адреса, открытые порты и их приложения и протоколы открытые в практической.

Практическое занятие № 44. Сканирование сети с помощью NetScan

Задание: необходимо:
1) Обнаружить IPv4/IPv6 адрес, имя хоста, имя узла, email и URLs.
2) Определить локальный порт.

Установите NetScan Tool Pro в Window Server 2012.

1. Нажмите Пуск.

Рисунок 7.1: Windows Server 2012 – Рабочий стол

2. Нажмите NetScan Tool Pro.

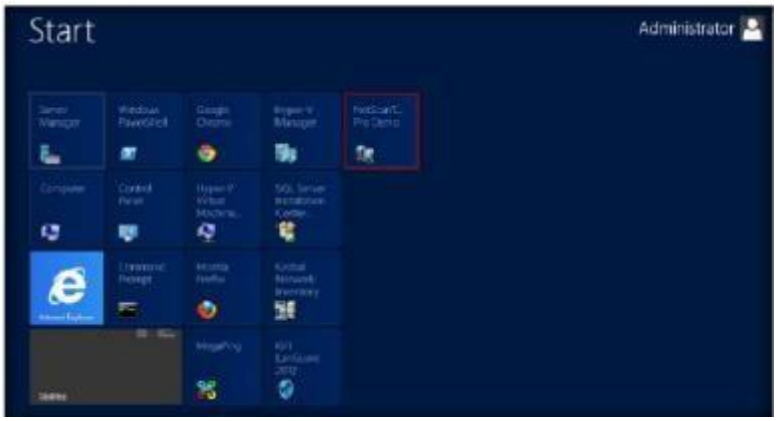


Рисунок 7.2 Windows Server 2012 – Приложения

3. Если вы используете демо-версию NetScan Tools Pro, тогда нажмите начать Demo.
4. Откройте или создайте окно New Result Database-NetScanTools Pro, введите имя новой БД
5. Расположение каталога по умолчанию, нажмите продолжить.

Рисунок 7.3: NetScan Tools Pro

6. Главное окно The NetScan Tools Pro представлено на рисунке.

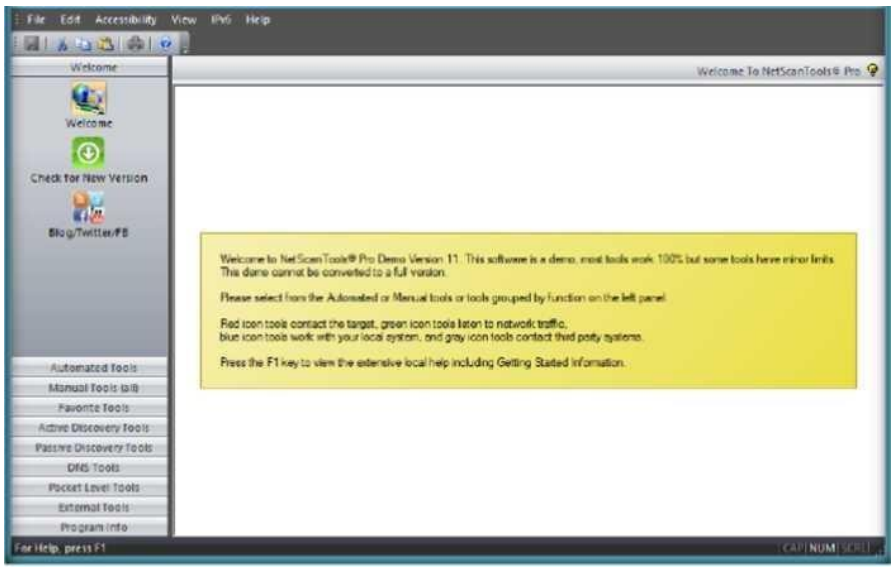


Рисунок 7.4: NetScan Tools Pro

7. Выберите Manual Tools (all) слева и нажмите ARP Ping.
8. Нажмите OK.

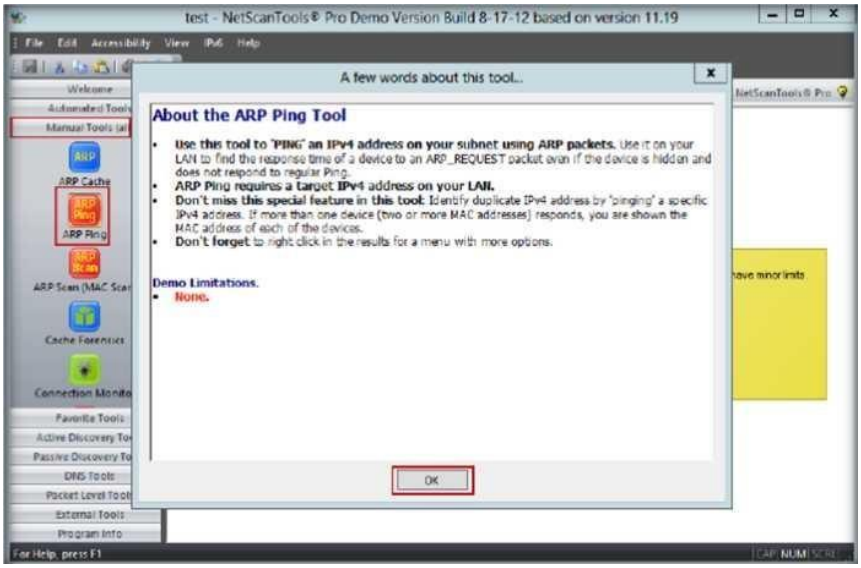


Рисунок 7.5: Опции

9. Выберите Send Broadcast ARP, затем переключатель Unicast ARP, введите IP адрес IPv4 Address, и нажмите Send Arp.

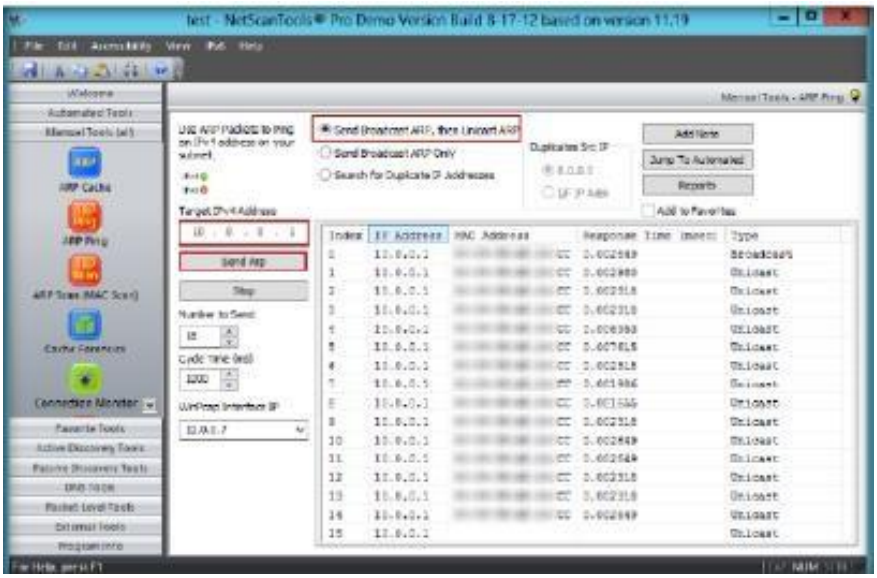


Рисунок 7.6: Результат ARP Ping

10. Нажмите ARP Scan (MAC Scan) слева. Откроется окно с информацией. Нажмите OK.

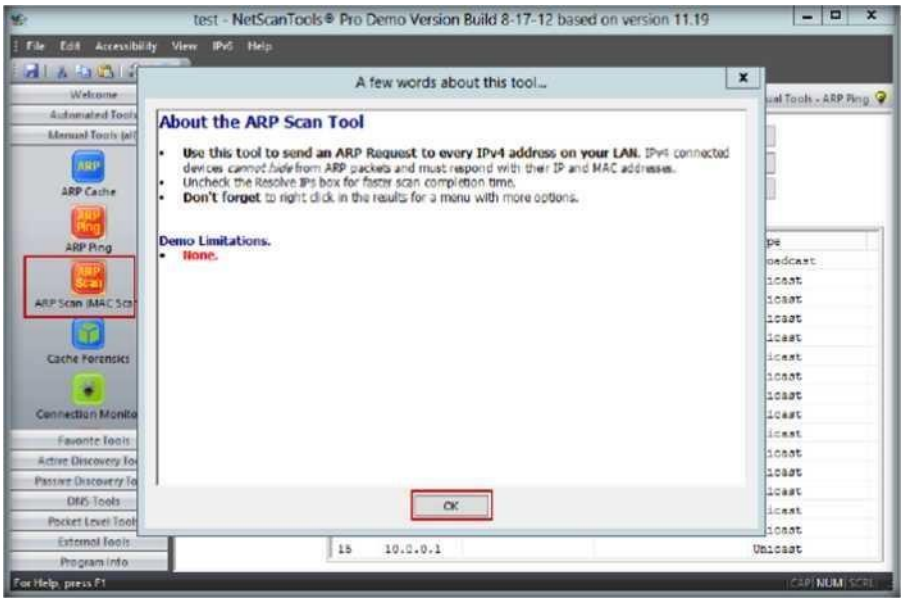


Рисунок 7.7: ARP Scan (MAC Scan)

11. Введите диапазон IPv4адреса.
12. Нажмите Do Arp Scan.

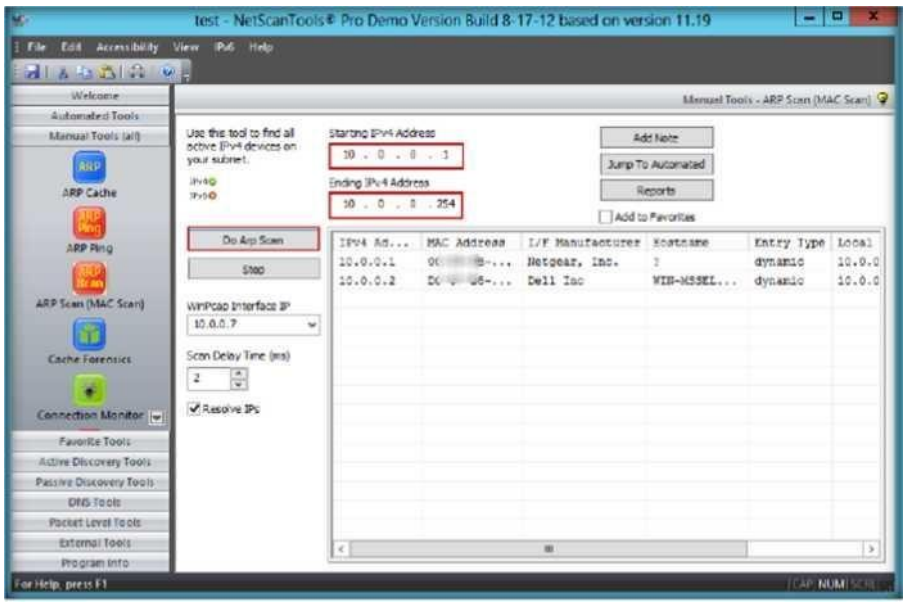


Рисунок 7.8 Результат ARP Scan (MAC Scan)

13. Нажмите DHCP Server Discovery слева, откроется окно с информацией о DHCP Server Discovery Tool. Нажмите OK.

Рисунок 7.9: DHCP Server Discovery Tool

14. Выберете все опции Discover и нажмите Discover DHCP Servers.

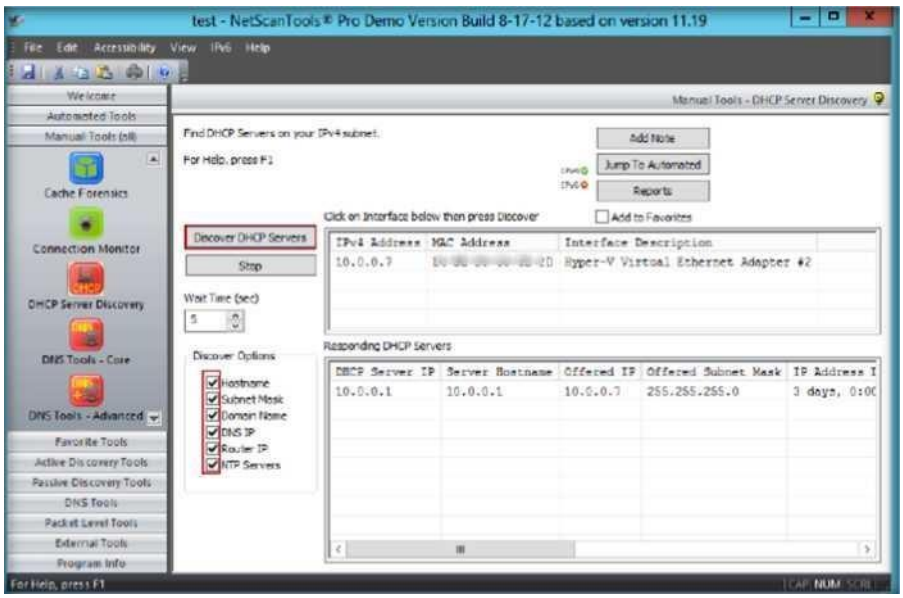


Рисунок 7.10: Результат DHCP Server Discovery

15. Нажмите Ping сканер. Появится окно с информацией о Ping Scanner tool. Нажмите OK.

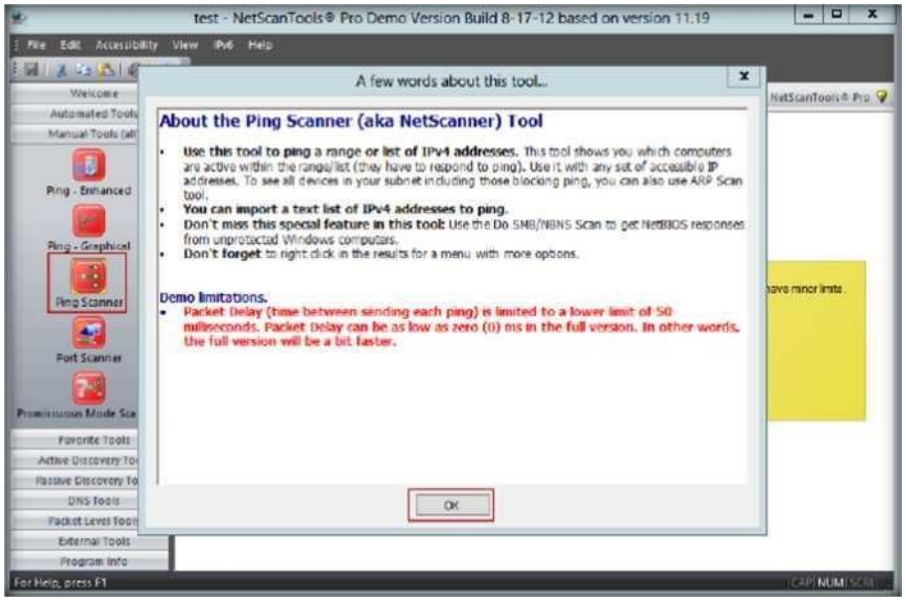


Рисунок 7.11: Ping scanner

16. Выберете переключатель Use Default System DNS, и введите диапазон IP в полях Start IP и End IP.
17. Нажмите Start.

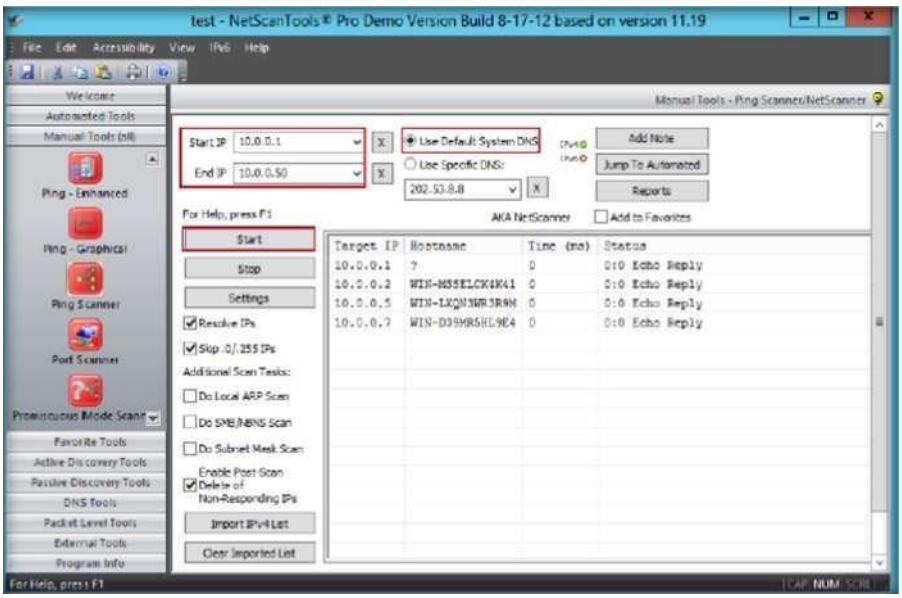


Рисунок 7.12: Результат

18. Нажмите Port scanner. Появится окно с информацией о port scanner tool. Нажмите OK.

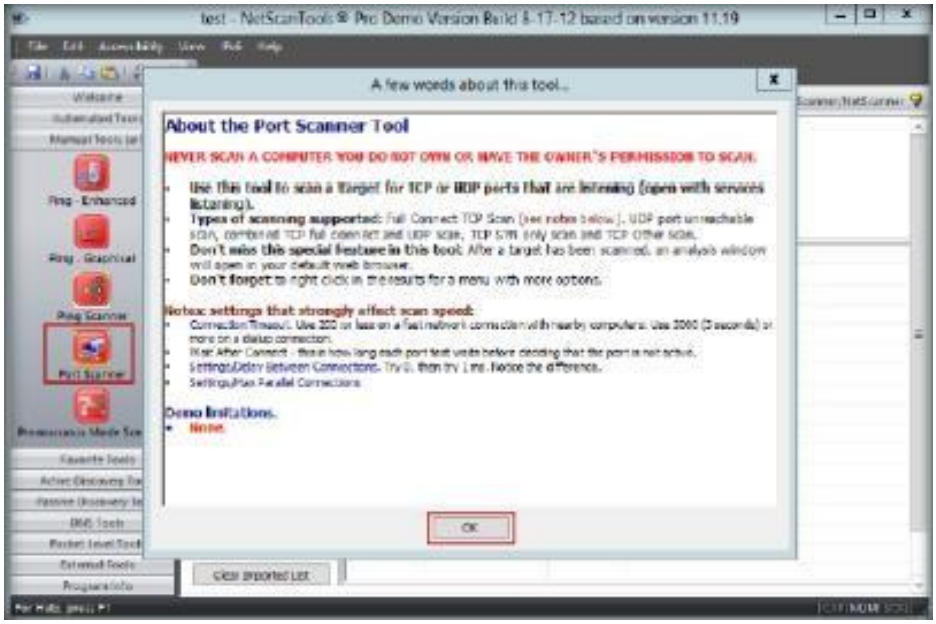


Рисунок 7.13: Port scanner

19. Введите IP адрес и выберете переключатель TCP Ports only.
20. Нажмите Scan Range of Ports.

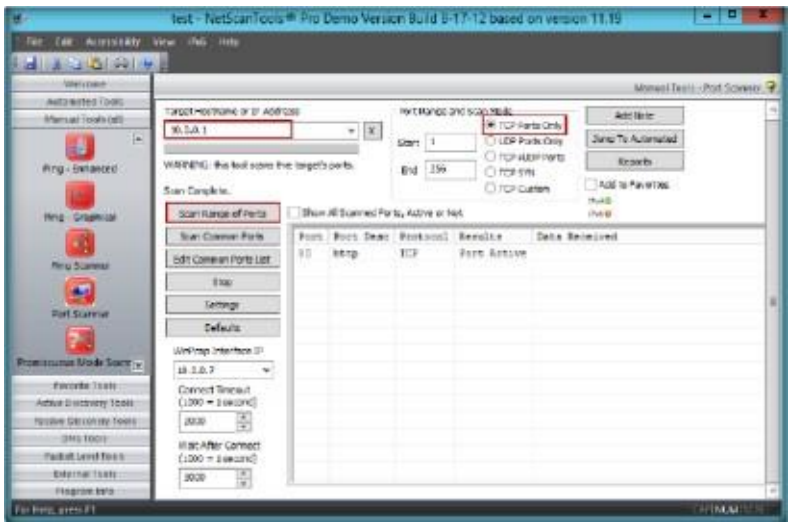


Рисунок 7.14: Результат Port scanner

Запишите все IP адреса, порты, службы и протоколы, которые вы обнаружили. Опишите их.

Практическое занятие № 45. «Сканирование сети с помощью Nessus Tool

Задание: провести сканирование сети с помощью Nessus Tool

Nessus помогает студентам изучать, понимать, и определять уязвимости и слабые места системы и сети, чтобы знать, как можно использовать систему. Сетевые уязвимости могут быть и топологией сети, и уязвимостями ОС, открытыми портами и рабочими службами, приложением и ошибками конфигурации службы.

Выполнение:

1. Установите Nessus Tool
2. Просканируйте локальную сеть с помощью
3. Загрузите отчет
4. Проанализируйте полученный отчет

Изучите полученную информацию, опишите, какие уязвимости удалось обнаружить. Как можно защитить сеть от полученных уязвимотей? Дополните отчет скриншотами.

Практическое занятие № 46. Сканирование сети с помощью Colasoft Packet Builder

Задание: провести сканирование сети с помощью Colasoft Packet Builder

Colasoft Packet Builder создает и включает пользовательские сетевые пакеты. Этот инструмент может использоваться, чтобы проверить сетевую защиту

от атак и злоумышленников. Функции редактора декодирования Colasoft Packet Builder разрешают пользователям отредактировать значения полей протокола.

Пользователи также в состоянии отредактировать информацию о декодировании в двух редакторах: Decode Editor и HEX-редактор. Пользователи могут выбрать любой из обеспеченных шаблонов: Пакет Ethernet, Пакет IP, Пакет ARP или Пакет TCP.

Выполнение:

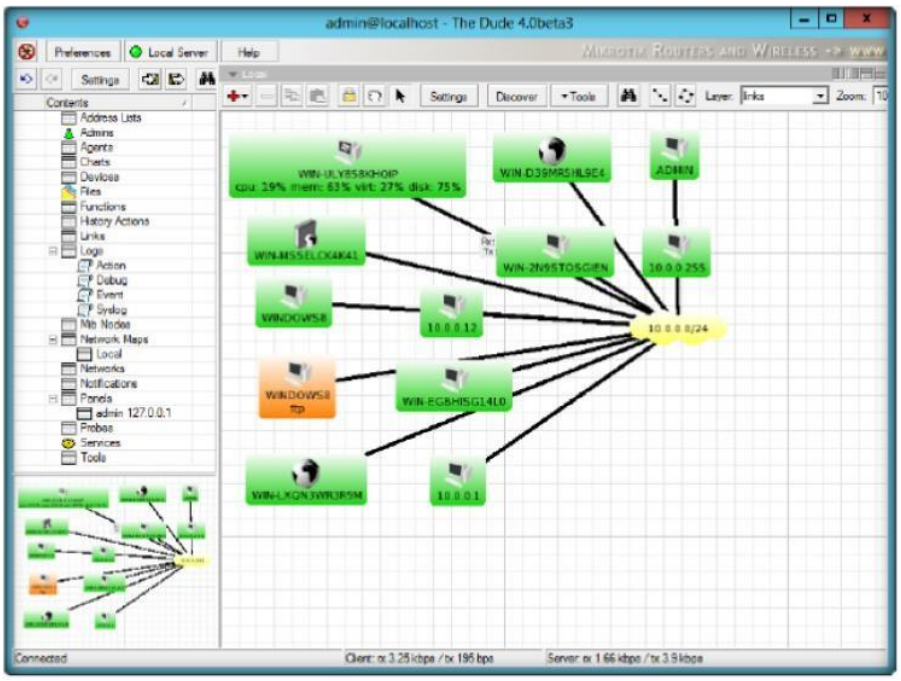
1. Откройте приложение
2. Запустите дополнительные пользовательские пакеты.
3. Зафиксируйте их, указав время работы приложения.
4. Сохраните полученные результаты.
5. Проанализируйте, как Colasoft Packet Builder влияет на сетевой трафик при анализе сети.

Добавьте скриншоты всех выполненных действий, опишите полученные результаты.

Практическое занятие № 47. Сканирование устройства в сети с помощью Dude.

Задание: провести сканирование устройств в сети.

Проведите обзор сетевого окружения своего рабочего места.



Проанализируйте полученные результаты. Какие выводы по безопасности можно сделать?

Напишите отчет, указав подробные действия проведенного сканирования. Добавьте скриншоты.

Практическое занятие № 48. Отображение сети с помощью Friendly Pinger

Задание: получить необходимую информацию о сети.

Средства	Необходимая информация
FriendlyPinger	IP адреса: 10.0.0.1 -10.0.0.20
	Найденные IP адреса: – 10.0.0.2 – 10.0.0.3 – 10.0.0.5 – 10.0.0.7
	Детали по 10.0.0.7: – Computer name – Operating system – IP Address – MAC address – File system – Size of disk – Hardware information – Software information

В отчет добавить скриншоты с полученной информацией. Проанализировать ее. Сделать выводы.

Практическое занятие № 49. Анализ уязвимостей серверов

Цель занятия: Изучить способы применения и возможности общедоступных программных средств тестирования информационной безопасности (сканеров безопасности).

Задания:

1. Исследовать наличие открытых портов сервера 217.71.139.66 и определить тип операционной системы сервера. Определить наличие уязвимостей, слабых паролей.
2. Исследовать наличие открытых портов сервера 217.71.139.95 и определить тип операционной системы сервера. Определить наличие уязвимостей, слабых паролей.
3. Исследовать наличие открытых портов сервера 217.71.138.1 и определить тип операционной системы сервера. Определить наличие уязвимостей, слабых паролей.

Порядок работы:

1. Используя утилиту ping, убедиться в доступности заданного сервера.

2. Используя последовательно программы nmap и nessus, просканировать указанный сервер.
3. Определить наличие уязвимостей, слабых паролей. Перечислить их.
4. Определить ОС сервера.

Практическое занятие № 50. Поиск и устранение неисправностей сети с помощью MegaPing

Задание: провести поиск неисправностей в сети.

Команда ping отправляет пакеты эхо-запроса Internet Control Message Protocol (Протокола межсетевых управляющих сообщений) (ICMP) в целевой узел и ожидает ответа ICMP. Во время этого процесса запрос-ответ, ping измеряет время от передачи до приема, известного как круговая задержка, и записывает любые потери пакетов.

Проведите:

1. Сканирование IP
2. Сканирование NetBIOS
3. Traceroute
4. Сканирование портов

Проанализируйте полученную информацию.

Ответ:

Практическое занятие № 51. Настройка межсетевого экрана

Цель занятия: Изучить правила построения фильтров TCP/IP пакетов (программного межсетевого экрана) в ОС LINUX.

Задание: разрешить или запретить указанные порты и сервисы.

Разрешить	Входящие	Исходящие
	http(80)	http(80)
	domain	domain
	ftp,ftp-data	ftp,ftp-data
Запретить	icmp с 192.168.1.2	udp 334
	tcp с портов 20,21 192.168.1.2	tcp 365

Практическое занятие № 52. Настройка параметров безопасности Windows.

Задание: настроить параметры безопасности Windows 10:

1. Установить ограничения пользователям;
2. Запретить использование USB-носителей;
3. Установить требования к паролям(длину, количество символов и знаков, срок действия);
4. Установить запреты автозапуска установленных приложений;
5. Установить запрет на установку приложений;
6. Запретить изменение реестра;
7. Отключить доступ к реестру;
8. Настроить выключение компьютеров в указанное время (после 19:00);
9. Установить блокировку компьютера при простое (более 30 минут);
10. Отключить принудительный перезапуск;
11. Отключить автоматическое обновление драйверов и ПО.

Ответ:

Практическое занятие № 53. Составление рекомендаций по повышению уровня защищенности информационной инфраструктуры

Задание: составьте список рекомендаций по повышению уровня защищенности информационной инфраструктуры.

Список должен содержать:

1. Рекомендации по парольной защите
2. Рекомендации по использованию ПО для защиты
3. Рекомендации по поиску и анализу уязвимостей
4. Рекомендации по работе с пользователями.

Ответ:

Практическое занятие № 54. Выявление предпосылок и обстоятельств, приведших к возникновению компьютерного инцидента.

Задание. Выполнить работу для инцидентов, повлекших:
1) Отказ в обслуживании;
2) Сбор информации;
3) Несанкционированный доступ.

Таблица 1.1–Примеры угроз информационной безопасности

№	1	2	3	4
	Направление обеспечения безопасности	**Техногенные**		**Природные**
		Преднамеренные	**Случайные**	
1.	Контроль физического доступа	Бомбардировка	Сон вахтерши	Торнадо

2.	Сохранность оборудования	Вандализм	Запыление	Шаровые молнии
3.	Управление коммуникациями	Прослушивание сети	Флуктуация в сети	Магнитные бури
4.	Защита информационных хранилищ	Взлом парольной защиты	Сбой крипто средств	Грибки
5.	Управление непрерывной деятельностью	Последствия DOS атаки	Последствия тестов на проникновения	Карстовые процессы
6.	Соответствие законодательству	Компьютерное пиратство	Тиражирование персональных данных	Природные пожары

Таблица 1.2–Кодировка заданий по вариантам

№ варианта	**Адреса ячеек табл.3.1**
1.	(1,3) (2,4)(3,1)(4,6)
2.	(1,2)(2,2)(3,6)(4,5)
3.	(1,4)(2,3)(3,4)(4,1)
4.	(1,1)(2,1)(3,5)(4,2)
5.	(1,5)(2,6)(3,2)(4,3)
6.	(1,6)(2,5)(3,3)(4,4)

Выявить предпосылки и обстоятельства, приведшие к возникновению инцидентов.

Предпосылки и обстоятельства, приведшие к событию:

Вариант №1

Управление коммуникациями (отказ в обслуживании, несанкционированный доступ, сбор информации):

наличие уязвимости непосредственной сетевой среды, которые можно использовать (сбор информации);

неудачно и (или) неправильно сконфигурированная сетевая среда организации;

отсутствие средств защиты информации (межсетевых экранов или их неверная конфигурация);

использование «простых паролей» (123, 12345, qwerty и т.д.);

Взлом парольной защиты (отказ в обслуживании, несанкционированный доступ, сбор информации - смотря для чего был совершён взлом):

- использование «простых паролей» (123, 12345, qwerty и т.д.);

- отсутствие парольной политики (регламента, где оговорены частота смены паролей, длина и сложность пароля, место хранения и т.д.);
- отсутствие системы мониторинга по обнаружению инцидентов информационной безопасности (при подборе пароля - большое количество ошибочных вводов пароля было бы зафиксировано);
- «неудачное» увольнение с предыдущим администратором информационной безопасности, не сменили пароли после увольнения;
- продажа паролей сотрудниками;
- «человеческий» фактор (пароли, хранящиеся под клавиатурой, на мониторе и т.д.;
- заражение системы вредоносным ПО (случайное, преднамеренное);
- реализация уязвимостей ПО.

Сон вахтерши (может быть использован для несанкционированного физического доступа, а как следствие для сбора (хищения или копирования) информации или для отказе в обслуживании (хищение, физическая поломка техники):

- неправильный подбор персонала (в случае, если информация представляет интерес для конкурентов или иностранных разведок необходимо пользоваться услугами проверенных лицензированных охранных агентств);
- отсутствие правил охраны объекта (документ, в котором прописано как, когда и что необходимо проверять, обходы, пропускной режим на объекте), отсутствие административных мер (если инцидент произошёл не в первый раз);
- отсутствие дополнительных мер защиты во вне рабочее время;
- умышленное усыпление вахтёрши;
- вахтёрша = «инсайдер» (специально нанятый человек для проведения или осуществления вредоносных действий).

Природные пожары (отказ в обслуживании в случае физического повреждения техники и коммуникаций, несанкционированный доступ в случае эвакуации персонала и ненадёжной защиты техники (кража и т.д.), сбор информации в случае предумышленной провокации природных пожаров с последующим хищением накопителей информации)

- размещение объекта в условиях повышенной пожарной опасности (в случае ежегодных пожаров);
- не принятие мер по снижению рисков возгорания в результате природных пожаров;
- отсутствие современной системы пожаротушения;
- отсутствия регламента действий при возникновении пожара;
- отсутствие регламента эвакуации или защиты техники во время природных катаклизмов;

Практическое занятие № 55. Обнаружение события информационной безопасности. Оценка события информационной безопасности

Задание

Заполнить форму отчета о событии информационной безопасности. Оценить является ли событие информационной безопасности инцидентом информационной безопасности составить отчет.

Выполнить лабораторную работу для событий, повлекших:

4) Отказ в обслуживании;
5) Сбор информации;
6) Несанкционированный доступ.

Таблица 1.1–Примеры угроз информационной безопасности

№	1	2	3	4
	Направление обеспечения безопасности	**Техногенные**		**Природные**
		Преднамеренные	**Случайные**	
1.	Контроль физического доступа	Бомбардировка	Сон вахтерши	Торнадо
2.	Сохранность оборудования	Вандализм	Запыление	Шаровые молнии
3.	Управление коммуникациями	Прослушивание сети	Флуктуация в сети	Магнитные бури
4.	Защита информационных хранилищ	Взлом парольной защиты	Сбой крипто средств	Грибки
5.	Управление непрерывной деятельностью	Последствия DOS атаки	Последствия тестов на проникновения	Карстовые процессы
6.	Соответствие законодательству	Компьютерное пиратство	Тиражирование персональных данных	Природные пожары

Таблица 1.2–Кодировка заданий по вариантам

№ варианта	**Адреса ячеек табл.3.1**
1.	(1,3) (2,4)(3,1)(4,6)

2.	(1,2)(2,2)(3,6)(4,5)
3.	(1,4)(2,3)(3,4)(4,1)
4.	(1,1)(2,1)(3,5)(4,2)
5.	(1,5)(2,6)(3,2)(4,3)
6.	(1,6)(2,5)(3,3)(4,4)

Рекомендации по заполнению

Назначением данной формы (формы отчета о событиях и инцидентах ИБ) является обеспечение информацией о событии ИБ, а затем, если оно определено как инцидент ИБ, то и об инциденте ИБ, для определенных лиц.

Если подозревается, что событие ИБ развивается или уже свершилось, особенно событие, которое может привести к существенным потерям или ущербу собственности или репутации организации, то необходимо немедленно заполнить и передать форму отчета о событии ИБ в соответствии с процедурами, описанными в системе менеджмента инцидентов ИБ организации.

Представленная информация будет использована для инициирования соответствующего процесса оценки, которая определит, должно ли это событие категорироваться как инцидент ИБ и (в случае положительного ответа), какие корректирующие меры, необходимые для предотвращения или ограничения потерь или ущерба, следует предпринять. Поскольку процесс оценки по своему характеру является краткосрочным, то в данный момент необязательно заполнять все поля формы отчета.

Если сотрудник является членом группы обеспечения эксплуатации, анализирующим полностью/частично заполненные формы отчета, то он должен принять решение, надо ли отнести данное событие к категории инцидента ИБ. При положительном решении сотрудник должен внести в форму отчета об инциденте ИБ как можно больше информации и передать формы отчетов о событии и инциденте ИБ в ГРИИБ. Независимо оттого, будет ли событие ИБ отнесено к категории инцидента ИБ, база данных событий/инцидентов ИБ должна быть обновлена.

Если сотрудник является сотрудником ГРИИБ, анализирующим формы отчетов о событиях и инцидентах ИБ, переданные членом группы обеспечения эксплуатации, то форма отчета об инциденте ИБ должна обновляться по ходу расследования и, соответственно, должна обновляться база данных событий/инцидентов ИБ.

При заполнении форм следует соблюдать следующие рекомендации:

- по возможности формы отчета должны заполняться и передаваться в электронном виде. В случае если существуют проблемы или считается, что существуют проблемы с принятыми по умолчанию механизмами электронного оповещения (например, электронная почта), включая случаи, когда система может подвергаться атаке и формы отчета могут быть прочитаны несанкционированными лицами, должны использоваться альтернативные средства связи. Альтернативными средствами связи могут быть телефон или текстовые сообщения, а также использование курьеров;

- следует представить информацию, основанную на фактах, в которой сотрудник уверен, не следует что-либо придумывать для того, чтобы заполнить все формы. Если сотрудник считает уместным включить иную информацию, которую не может подтвердить, следует указать, что это неподтвержденная информация, и причину убежденности в ее недостоверности;

- следует подробно указать, как можно связаться с сотрудником. Немедленно или спустя некоторое время может возникнуть необходимость контакта с ним для получения дальнейшей информации, касающейся Вашего отчета.

Если позднее сотрудник обнаружит, что какая-либо представленная им информация неточна, неполна или ошибочна, то следует внести поправки в отчет и представить его повторно.

[1)] Если возможно, то формы отчетов должны быть, например, на безопасной web-странице с привязкой к электрон-
ной базе данных событий инцидентовИБ. В настоящее время основанная на бумажной технологии система я вляется слишком медленно действующей и далеко не самой эффективной вэксплуатации.

Отчет о событии информационной безопасности

Дата события

Номер события [1)]: Соответствующиеидентификационныеномера событий и(или) инцидентов(если требуется):

Информация о сообщающем лице

Фамилия	_____	Адрес	_____
Организация	_____		_____
Телефон	_____	Электронная почта	_____

Описание события ИБ

Описание события:

Что произошло

Как произошло

Почему произошло

Пораженные компоненты

Негативное воздействие на бизнес

Любые идентифицированные уязвимости

Подробности о событии ИБ

Дата и время наступления события

Дата и время обнаружения события

Дата и время сообщения о событии

Закончилось ли событие? (отметить в квадрате) Да ☐ Нет ☐

Если «да», то уточнить длительность события в днях/часах/минутах

[1)] Номера событий назначаются руководителем ГРИИБ организации.

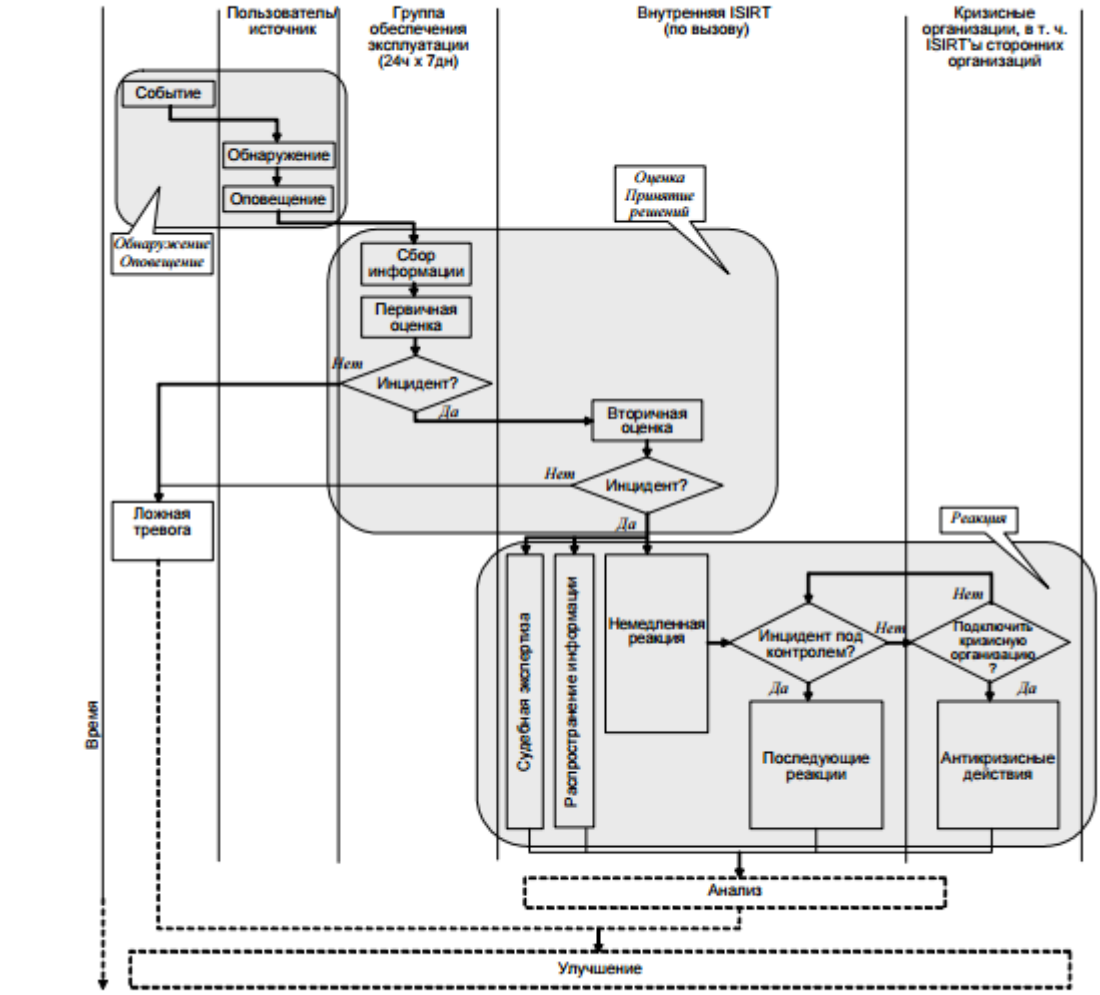


Рисунок 1 Блок – схема последовательности операций обработки событий и инцидентов ИБ (процесс «Использование»

Отчет о событии информационной безопасности

Дата события 31.08.2016 г.

Номер события[1]: 100

Соответствующие идентификационные номера событий и (или) инцидентов (если требуется):

Информация о сообщающем лице

Фамилия	Иванов И.Г.	Адрес	г. Магнитогорск
Организация	ООО «123»		
Телефон	75-16-58	Электронная почта	658@123.ru

Описание события ИБ

Описание события:

Что произошло уничтожение части техники

Как произошло возгорание в результате природного пожара

Почему произошло отсутствие автоматической системы пожаротушения, техника не была эвакуирована

Пораженные компоненты файловый сервер, коммуникации

Негативное воздействие на бизнес отказ в обслуживании клиентов на 2 дня

Любые идентифицированные уязвимости отсутствие системы автоматического пожаротушения, правил эвакуации

Подробности о событии ИБ

Дата и время наступления события 30.08.2016 22:30

Дата и время обнаружения события 30.08.2016 22:45

Дата и время сообщения о событии 30.08.2016 22:45

Закончилось ли событие? (отметить в квадрате)	Да	■	Нет	□
Если «да», то уточнить длительность события в днях/часах/минутах	1 час 16 минут			

[1)] Номера событий назначаются руководителем ГРИИБ организации.

Событие является инцидентом информационной безопасности в связи с тем, что имеет место временное отказа в обслуживании (2 дня). Возможна утеря части данных (в зависимости от частоты бекапов).

Отчет о событии информационной безопасности

Дата события 21.09.2016 г.

Номер события[1)]: 101

Соответствующие идентификационные номера событий и (или) инцидентов (если требуется):

Информация о сообщающем лице

Фамилия	Васильев С.И.	Адрес	г. Магнитогорск
Организация	ООО «123»		
Телефон	75-16-89	Электронная почта	689@123.ru

Описание события ИБ

Описание события:

Что произошло взлом парольной защиты

Как произошло системой мониторинга выявлены подключения с нетипичных IP адресов

Почему произошло некорректная конфигурация системы защиты информации

Пораженные компоненты компрометация системы безопасности, логинов и паролей организации

Негативное воздействие на бизнес несанкционированный доступ к внутренней информа-

ции организации, компрометация системы безопасности.

Любые идентифицированные уязвимости система безопасности

Подробности о событии ИБ

Дата и время наступления события 21.09.2016 04:30

Дата и время обнаружения события 21.09.2016 07:01

Дата и время сообщения о событии 21.09.2016 07:15

Закончилось ли событие? (отметить в квадрате)	Да	■	Нет	□
Если «да», то уточнить длительность события в днях/часах/минутах	2 часа 31 минута			

[1)] Номера событий назначаются руководителем ГРИИБ организации.

Событие является инцидентом информационной безопасности в связи с тем, что имеет место несанкционированный доступ к внутренней информации организации. Произошла компрометация логинов/паролей пользователей и системы безопасности в целом. Необходимо провести расследование инцидента, найти причину возникновения данного инцидента и как можно быстрее её устранить.

Отчет о событии информационной безопасности

Дата события 10.10.2016 г.

Номер события[1)]: 102

Соответствующие идентификационные номера событий и (или) инцидентов (если требуется):

Информация о сообщающем лице

Фамилия	Мерзов И.Л.	Адрес	г. Магнитогорск
Организация	ООО «123»		
Телефон	75-15-35	Электронная почта	535@123.ru

Описание события ИБ

Описание события:

Что произошло сон вахтёрши

Как произошло во время ночного дежурства вахтёрша спала, возможно несанкционированное проникновение на объект

Почему произошло неправильный подбор персонала

Пораженные компоненты угроза несанкционированного проникновение на объект и сбора информации

Негативное воздействие на бизнес компрометация системы безопасности (физический доступ на объект), возможен сбор и хищение информации, несанкционированный доступ на объект

Любые идентифицированные уязвимости пропускной режим на объект

Подробности о событии ИБ

Дата и время наступления события 10.10.2016 02:45

Дата и время обнаружения события 10.10.2016 06:00

Дата и время сообщения о событии 10.10.2016 06:05

Закончилось ли событие? (отметить в квадрате)	Да	■	Нет	□
Если «да», то уточнить длительность события в днях/часах/минутах	3 часа 15 минут			

[1)] Номера событий назначаются руководителем ГРИИБ организации.

Событие нуждается в дополнительно расследовании (просмотр камер наблюдения, проверка доступа к информационным ресурсам и т.д.), в случае если не было несанкционированного доступа на объект, сбора или хищения информации то событием является ложным. В противном случае событие будет являться инцидентом информационной безопасности.

Отчет о событии информационной безопасности

Дата события 28.10.2016 г.

Номер события[1)]: 104

Соответствующие идентификационные номера событий и (или) инцидентов (если требуется):

Информация о сообщающем лице

Фамилия	Мухина Е.И.	Адрес	г. Магнитогорск
Организация	ООО «123»		
Телефон	75-11-12	Электронная почта	112@123.ru

Описание события ИБ

Описание события:

Что произошло сбой в работе коммуникаций

Как произошло после применения новой конфигурации сети всем пользователям стали доступны все ресурсы

Почему произошло некорректная конфигурация сети

Пораженные компоненты все информационные ресурсы организации

Негативное воздействие на бизнес компрометация системы безопасности, возможен сбор и хищение информации, несанкционированный доступ к информации, лиц недопущенных к ней (инсайдеры и просто любопытные).

Любые идентифицированные уязвимости

Подробности о событии ИБ

Дата и время наступления события 01.11.2016 16:32

Дата и время обнаружения события 10.10.2016 16:44

Дата и время сообщения о событии 10.10.2016 16:44

Закончилось ли событие? (отметить в квадрате)	Да ■	Нет □
Если «да», то уточнить длительность события в днях/часах/минутах	0 часов 12 минут	

[1)] Номера событий назначаются руководителем ГРИИБ организации.

Событие является инцидентом информационной безопасности в связи с тем, что имелась возможность несанкционированного доступа к информации, возможны попытки сбора информации (копирование баз и т.д.)

Практическое занятие № 56. Исследование открытой информации в поисковых системах

Цель занятия: Научиться искать информацию по ключевым параметрам.

Задание:

У нас появилось новое дело, со слов заказчика он пытался заказать на одном сайте взлом почты и его кинули на все деньги, ему нужно помочь, но к сожалению все что у него осталось это клочок бумаги с частью сайта "jje5vh25v7gsuxja". Первая задача это найти сайт и предоставить его название заказчику для проверки.

We had a new request, according to the customer, he tried to order hacking services on the same site and he was thrown for all the money, he needs help, but unfortunately all he had left was a scrap of paper with part of the site "jje5vh25v7gsuxja". The first task is to find the site and give its name to the customer for verification.

Необходимо найти адрес кошелька мошенника, его имя и фамилию.

Ответ:

Практическое занятие № 57. Поиск информации в социальных сетях

Цель занятия: Научиться искать информацию в социальных сетях.

Задание: найти ответы на вопросы.

Поступил заказ на сбор всех данных на Марка, единственное, что нам дали это его номер телефона(+38 095 596 80 81), попробуй для начала узнать его имя.

An order was received to collect all the data on Mark, the only thing we were given was his phone number (+38 095-596-80-81), try to get to know his first name.

1. Узнайте его имя.
2. Узнайте его псевдоним
3. Узнайте, где и кем он работает
4. Узнайте его почту
5. Узнайте, где он живет

Ответьте на вопросы, подкрепив скриншоты с найденной информацией

Практическое занятие № 58. Поиск информации с помощью утилит

Цель занятия: Научиться пользоваться утилитами для поиска информации в открытых источниках.

Задание: имея ссылку на социальную сеть, необходимо найти ответы на вопросы:

1. Узнайте его имя.
2. Узнайте его псевдоним
3. Узнайте, где и кем он работает
4. Узнайте его почту
5. Узнайте, где он живет
6. Откуда он родом
7. Кто его близкий родственник?
8. Чем он увлекается
9. Где недавно отдыхал

Ссылка: **https://vk.com/0n1zz**

Требование: использовать не менее 3 платформ и 2 приложи для поиска по открытым источникам.

Ответ: