

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Петербургский государственный университет путей сообщения
Императора Александра I»
(ФГБОУ ВО ПГУПС)

Петрозаводский филиал ПГУПС

ОДОБРЕНО

на заседании цикловой комиссии
протокол № 11 от 23.06.2017

Председатель цикловой комиссии:

И.И. Каминский

УТВЕРЖДАЮ

Начальник УМО

А.В. Калько А.В. Калько

«23» 06 2017.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по организации и проведению лабораторных работ
и практических занятий

По МДК 02.02. Организация администрирования компьютерных систем

Специальность: 09.02.02 Компьютерные сети

Разработчик: преподаватель ПФ ПГУПС Усков Алексей Андреевич

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические указания по организации и проведению лабораторных работ и практических занятий разработаны в соответствии с рабочей программой МДК 02.02. Организация администрирования компьютерных систем для специальности 09.02.02 Компьютерные сети и предназначены для выполнения лабораторных работ и практических занятий обучающимися.

Практические занятия и лабораторные работы по МДК 02.02. Организация администрирования компьютерных систем направлены на усвоение знаний, освоение умений, и формирование элементов общих компетенций, предусмотренных рабочей программой учебной дисциплины.

В результате освоения учебной дисциплины обучающийся должен

иметь практический опыт:

- установки web-сервера;
- организации доступа к локальным и глобальным сетям;
- сбора данных для анализа использования и функционирования программно – технических средств компьютерных сетей;

уметь:

- администрировать локальные вычислительные сети;
- создавать и конфигурировать учетные записи отдельных пользователей и пользовательских групп;
- обеспечивать защиту при подключении к Интернет средствами операционной системы;

знать:

- основные направления администрирования компьютерных сетей;
- типы серверов, технологию «клиент – сервер»;
- способы установки и управления сервером;
- утилиты, функции, удаленное управление сервером;
- мониторинг и настройку производительности;
- технологию ведения отчётной документации;
- оценку стоимости программного обеспечения в зависимости от способа и места его использования

В результате освоения МДК 02.02. Организация администрирования компьютерных систем происходит поэтапное формирование элементов общих и профессиональных компетенций:

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

ПК 2.2. Администрировать сетевые ресурсы в информационных системах.

ПК 2.3. Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.

ПК 2.4. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

- ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
- ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
- ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
- ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
- ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.
- ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.
- ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполненных заданий.
- ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
- ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Распределение результатов освоения учебного материала в ходе выполнения лабораторных работ и практических заданий на практических занятиях происходит в соответствии с таблицей 1.

Таблица 1 – Распределение результатов освоения учебного материала

Элемент модуля	Контрольно-оценочные мероприятия	Результаты			Поэтапно формируемые элементы общих и профессиональных компетенций
		усвоенные знания	освоенные умения	практический опыт	
Раздел 1. Разработка методов, средств и технологий применения и	Практические занятия №1-20, тестирование	-использование кластеров; -взаимодействие различных операционных систем; -классификацию программного обеспечения сетевых	-устанавливать информационную систему; -рассчитывать стоимость лицензионного программного	-настройки сервера и рабочих станций для безопасной передачи	ПК 2.1-2.4 ОК 1-9

<p>управления сетевыми ресурсами в информационных системах.</p>		<p>технологий и область его применения; -лицензирование программного обеспечения;</p>	<p>обеспечения сетевой инфраструктуры; - устанавливать и конфигурировать антивирусное программное обеспечение, программное обеспечение баз данных, программное обеспечение мониторинга;</p>	<p>информации; -установки web-сервера; -расчёта стоимости лицензионного программного обеспечения сетевой инфраструктуры;</p>	
<p>МДК 02.01. «Программное обеспечение компьютерных сетей»</p>					
<p>Раздел 2. Администрирование локальных вычислительных сетей, сбор и анализ данных о функционировании программно-технических средств компьютерных сетей и принятие мер по устранению возможных сбоев.</p>	<p>Практические занятия 1-3 Лабораторные работы №1-11, тестирование</p>	<p>-основные направления администрирования компьютерных сетей; -типы серверов, технологию «клиент – сервер»; -способы установки и управления сервером; -утилиты, функции, удаленное управление сервером; -мониторинг и настройку производительности; -технологию ведения отчётной документации; - оценку стоимости программного обеспечения в зависимости от способа и места его использования</p>	<p>администрировать локальные вычислительные сети; - создавать конфигурировать учетные записи отдельных пользователей пользовательских групп; - обеспечивать защиту при подключении Интернет средствами операционной системы;</p>	<p>-установки web-сервера; -организации доступа к локальным и глобальным сетям; -сбора данных для анализа использования и функционирования программно – технических средств компьютерных сетей;</p>	<p>ПК 2.1-2.4, ОК 1-9</p>
<p>МДК 02.02. «Организация администрирования компьютерных сетей»</p>					
<p>Учебная практика УП.02.01 «Администрирование сетей»</p>	<p>Практические занятия</p>	<p>-основные направления администрирования компьютерных сетей; -типы серверов, технологию «клиент – сервер»; -способы установки и управления сервером; -утилиты, функции, удаленное управление сервером; -мониторинг и настройку производительности; -технологию ведения отчётной документации; - оценку стоимости</p>	<p>администрировать локальные вычислительные сети; - создавать конфигурировать учетные записи отдельных пользователей пользовательских групп; - обеспечивать защиту при подключении Интернет средствами операционной системы;</p>	<p>-установки web-сервера; -организации доступа к локальным и глобальным сетям; -сбора данных для анализа использования и функционирования программно – технических</p>	<p>ПК 2.1-2.4</p>

		программного обеспечения в зависимости от способа и места его использования		средств компьютерных сетей;	
Раздел 3. Администрирование адресного пространства и организация межсетевого взаимодействия в сетях различного масштаба.	Практические занятия 1-15, тестирование,	-технологии безопасности, протоколы авторизации, конфиденциальность и безопасность при работе в web;	- принимать меры по устранению возможных сбоев	-организации доступа к локальным и глобальным сетям;	ПК 2.1-2.4 ОК 1-9
МДК 02.03 «Межсетевое взаимодействие в крупных и глобальных сетях»					
Учебная практика УП.02.02 «Межсетевое взаимодействие в крупных сетях»	Практические занятия	-технологии безопасности, протоколы авторизации, конфиденциальность и безопасность при работе в web;	- принимать меры по устранению возможных сбоев	-организации доступа к локальным и глобальным сетям;	ПК 2.1-2.4
Производственная практика (по профилю специальности) итоговая по модулю	Практические занятия	-технологии безопасности, протоколы авторизации, конфиденциальность и безопасность при работе в web;	- принимать меры по устранению возможных сбоев	сопровождения и контроля использования почтового сервера, SQL сервера;	ПК 2.1-2.4 ОК 1-9

Перечень практических занятий и лабораторных работ

Практические занятия

1. Расчет адресного пространства локальной телекоммуникационной сети состоящей из одного сегмента. 2ч
2. Расчет адресного пространства локальной телекоммуникационной сети состоящей из двух сегментов. 4ч
3. Расчет адресного пространства локальной телекоммуникационной сети состоящей переменного количества сегментов. 4ч

Лабораторные работы

1. Установка серверной операционной системы Windows Server 2008 R2 2ч

2. Изучение консолей управления, оснасток. Создание консолей MMC. Создание панели задач 2ч
3. Мониторинг процессов, служб и событий 2ч
4. Установка Active Directory, контроллера домена 2ч
5. Создание учетных записей 4ч
6. Создание и настройка групповых политик 4ч
7. Управление файловыми системами и дисками 4ч
8. Общий доступ
9. Управление службой DNS
10. Управление службой DHCP
11. Изучение журналов и оповещений Windows, настройка службы аудита в Windows 4ч

Порядок выполнения

1. Приведите примеры адресов конечных узлов классов А, В, С. Используя стандартные маски, рассчитайте адреса соответствующих сетей.
2. Переведите адреса 10.169.77.19, 172.18.190.59 и 192.168.55.112 в двоичную систему.
3. Рассчитайте максимальное количество хостов в подсетях 10.169.77.16/28, 172.18.190.16/27 и 192.168.55.112/29.
4. Для выделенного диапазона адресов 172.16.10.0/24 сформируйте 10 подсетей по 8-14 компьютеров в каждой. Какова будет сетевая маска?
5. Для выделенного адреса 10.1.5.0/24 сформируйте 2 подсети по 50-60 компьютеров, 2 подсети по 25-30 компьютеров, 2 подсети по 10-12 компьютеров, 2 подсети по 5 – 6 компьютеров, остальные адреса используйте для адресации соединений "точка-точка".
6. Каким агрегированным адресом может быть представлена группа из четырех подсетей: 172.16.16.0/24, 172.16.17.0/24, 172.16.18.0/24, 172.16.19.0/24?
7. Оформить типовой отчет.

Контрольные вопросы

1. Кто назначает логические адреса интерфейсам и конечным узлам сети?
2. Сколько двоичных разрядов содержат логические адреса узлов в IP-сетях версии IPv4?
3. Что определяют старшие и младшие разряды сетевого адреса?
4. Какие классы уникальных адресов используются в сетях?
5. Какие размеры имеют стандартные маски адресов классов А, В, С?
6. Какое максимальное число узлов могут задавать адреса класса С?

7. Какой адрес используется для самотестирования?
8. Какие параметры задаются в таблицах маршрутизации?
9. Для чего нужны сетевые маски?
10. Как называется общая часть адреса нескольких устройств?
11. Для чего необходимы маски переменной длины?
12. Что позволит радикально решить проблему дефицита IP-адресов?
13. Сколько двоичных разрядов содержат логические адреса узлов в IP-сетях версии IPv6?
14. Как представлены адреса версии IPv6?
15. Для чего используются частные адреса в локальных сетях?
16. Каковы диапазоны частных адресов?
17. Можно ли использовать частные адреса в сети Интернет?
18. Что переводит частные адреса в общественные?

Лабораторная работа № 1

Тема: Установка серверной операционной системы Windows Server 2008 R2

Цель выполнения работы: формирование профессиональных умений по установке серверной операционной системы

Порядок выполнения

1. Подключиться к удаленному рабочему столу, сервера **virtual**.
2. Открыть программу **VirtualBox**.
3. Создать новую виртуальную машину Windows Server 2008 R2 x64.
Выделить оперативной памяти **1024 Мб**, жесткого диска **25 Гб**.
4. Подключить образ DVD-диска с дистрибутивом операционной системы.
5. Установить операционную систему, выбрать редакцию **Standart (полная установка)**. Зафиксировать в отчете все шаги установки.
6. Настроить сеть в программе **VirtualBox**. Настроить сетевое подключение в операционной системе. Необходимо выбрать единое адресное пространство и распределить адреса между одногруппниками, так чтобы все виртуальные машины находились в одной сети, и не было одинаковых адресов.
7. Проверить достижимость серверов одногруппников.
8. Оформить типовой отчет.

Контрольные вопросы

1. Какие редакции ОС Windows Server 2008 вы знаете?
2. Какие режимы инсталляции WS 2k8 R2 вы знаете?
3. Какими способами можно сконфигурировать разделы жесткого диска для установки ОС?
4. Какие разделы диска создаются при установке ОС?
5. Какая файловая система нужна Windows Server 2008 R2?
6. Назовите основной инструмент для управления сервером Windows Server 2008 R2.

Лабораторная работа № 2

Тема: Изучение консолей управления, оснасток. Создание консолей ММС.

Создание панели задач

Цель выполнения работы: формирование профессиональных умений по использованию консолей управления и оснасток; по созданию консолей ММС; по созданию панели задач

Порядок выполнения

1. Подключиться к удаленному рабочему столу, сервера **virtual**. Открыть программу **VirtualBox**. Открыть виртуальную машину с установленной операционной системой Windows Server 2008 R2.
2. Открыть оснастку Службы. Для трех служб выписать все основные параметры.
3. Создать новую консоль mms.
4. Добавить в консоль следующие оснастки: брандмауэр; общие папки; просмотр событий; системный монитор; службы.
5. Создать панель задач.
6. Добавить в панель задач следующие задачи:

Команды меню:

- Общие папки/ сеансы – отключить все сеансы
- Общие папки/ открытые файлы – отключить все открытые файлы
- Общие папки/ общие ресурсы – новый общий ресурс
- Просмотр событий – очистить журнал «безопасность»

Команды ОС:

- Название задачи «Проверка интернета» - выполнить пинг до узла ya.ru, пинг бесконечный (подсказка: ping.exe находится в C:\Windows\System32).
- Название задачи «Проверка DNS сервера» - создать пакетный файл .bat, который разрешает имя ya.ru в ip адрес и после этого окно командной строки не закрывается (команда nslookup – разрешает имена, команда pause – про ожидание ввода пользователя до закрытия окна).

7. Изменить режим консоли на пользовательский, полный доступ.
8. Сохранить консоль Console<ВашаФамилия> (например ConsoleIvanov, ConsolePetrov).
9. Оформить типовой отчет.

Контрольные вопросы

1. Что такое ММС, назначение ММС?
2. Из каких частей состоит рабочее окно консоли ММС?
3. Что такое оснастка, назначение оснасток?
4. Типы оснасток?
5. Способы запуска оснасток?
6. Назначение режимов консоли (авторский, пользовательские)?
7. Способы управления службами?
8. Тип запуска службы?

Лабораторная работа № 3

Тема: Мониторинг процессов, служб и событий

Цель выполнения работы: формирование профессиональных умений по использованию средств мониторинга процессов, служб и событий

Постановка задачи или ситуации

В этой работе основное внимание уделяется встроенным средствам мониторинга, ведения журналов, отладки и проверки надежности. Данные средства облегчают организациям выявление и устранение проблем возникающих в сетевых средах.

Работа состоит из 4 частей.

Первая часть посвящена диспетчеру задач.

Вторая часть посвящена средству «Просмотр событий» для мониторинга и устранения системных проблем.

Третья часть посвящена системному монитору.

Четвертая часть посвящена группам сборщиков.

Порядок выполнения

Работу выполнить в операционной системе Windows Server 2008 R2. Для этого подключиться к удаленному рабочему столу, сервера **virtual**. Открыть программу **VirtualBox**. Открыть виртуальную машину с установленной операционной системой Windows Server 2008 R2.

После выполнения всех частей работы оформить типовой отчет.

Часть 1. Использование диспетчера задач для ведения журналов и отладки

1. Открыть диспетчер задач разными способами.
2. Открыть вкладку **Приложения**. Остановить какое-нибудь приложение (Снять задачу. Если останавливать нечего, запустить Блокнот и остановить его). Запустите новую программу – командную строку.
3. Открыть вкладку **Процессы**. Упорядочить процессы в порядке использования: ресурсов процессора; памяти. Добавить следующие характеристики процессов: идентификатор процесса (PID); время ЦП.
4. Открыть вкладку **Службы**. Выполнить переход к соответствующему процессу, который реализует выполнение службы.
5. Открыть вкладку **Быстродействие**. Отобразить график использования процессорного времени в режиме ядра: меню View – пункт Show Kernel Times (Вывод времени ядра).
6. Открыть вкладку **Сеть**. Добавьте столбцы: Bytes Sent (Отправлено байт); Received (Получено байт) и Total Bytes (Всего байт).
7. Открыть вкладку **Пользователи**. Для пользователя выписать следующие столбцы: Пользователь, код, состояние, имя клиента, сеанс

Часть 2. Использование программы просмотра событий для ведения журналов и отладки

1. Открыть журнал “Система” для трех событий определить: источник события; уровень события; дату и время; код события.
2. Открыть настраиваемое представление “События управления”. Описать, какие события выводит это представление.
3. Создать **настраиваемое представление**: Последние 7 дней; уровень: предупреждения и ошибки; журналы: приложения, безопасность, установка. Задать имя: “Ошибки и предупреждения в журналах Приложения, Безопасность, Установка”.
4. Создать **фильтр** для журнала «Система»: последние 30 дней; ошибки и предупреждения. Зафиксировать результат в отчет. Очистить фильтр.
5. Настроить **параметры** журнала “Безопасность”: максимальный размер - 320 000 Кб; при достижении максимального размера: не переписывать события.
6. Выполнить **архивирование** журнала Система в формате .evtx. Файл назвать: system_log.
7. **Открыть сохраненный** журнал. Ввести имя сохраненного журнала: Журнал система архив 1.
8. Очистить журнал Система.
9. Просмотреть журнал на удаленном сервере одногруппника. Команда Connect to Another Computer (Подключиться к другому компьютеру). Для просмотра журналов событий на удаленном компьютере необходимы полномочия администратора или члена группы администраторов.

Часть 3. Мониторинг производительности и надежности

1. Открыть «Системный монитор» (Производительность).
2. Изучить экран общих сведений – «Сводные сведения о системе». Выписать в отчет: для памяти - % использования памяти, объем доступной памяти; для процессора - % загруженности процессора; для физического диска - процент времени бездействия.
3. Открыть «Системный монитор». Добавить следующие счетчики: Сетевой интерфейс – текущая пропускная способность; Физический диск - % активности диска; Процессор - % загруженности процессора; Память - % использования выделенной памяти. Изучить различные типы диаграмм: строка, линейчатая гистограмма, отчет. На основе этих счетчиков создать группу сборщиков данных с именем «Основные подсистемы».
4. Удалить все счетчики, добавленные ранее.
5. Добавить счетчики для осуществления мониторинга следующих подсистем сервера: использование памяти и кэширование; загруженность процессора; дисковый ввод-вывод; пропускная способность сети и возможность подключения. Наборы счетчиков представлены ниже. Сохранить каждый набор счетчиков как группу сборщиков с соответствующим именем (название области мониторинга).

а) Мониторинг и настройка использования памяти

область: использование физической и виртуальной памяти

счетчики:

Память\Доступно байт (Memory\ Available Kbytes)

Память\Байт выделенной виртуальной памяти (Memory\Committed Bytes)

Как анализировать:

Первый счетчик соответствует объему физической памяти, доступной для процессов, работающих на сервере. Второй счетчик равен объему выделенной виртуальной памяти. Если на сервере мало доступной памяти, возможно, придется нарастить ее объем. Как правило, желательно, чтобы объем свободной памяти был не менее 5% от общей физической памяти сервера. Если велико отношение выделенной памяти к общей физической памяти системы, вам также следует добавить память. В общем случае объем выделенной памяти не должен превышать 75% от общей физической памяти.

область: Ошибки страниц

счетчики:

Память\Ошибок страницы/сек (Memory\ Page Faults/sec)

Память\Ввод страниц/сек (Memory\ Pages Input/sec)

Память\Чтений страниц/сек (Memory\ Page Reads/sec)

Как анализировать:

Ошибка страницы возникает, когда процесс запрашивает страницу в памяти, а система не может найти ее в запрошенном месте. Если запрошенная страница находится где-то в другом месте памяти, ошибка называется программной. Если запрошенная страница должна быть загружена с диска, то ошибка называется аппаратной. Большинство процессоров способны обрабатывать значительное число программных ошибок. Аппаратные ошибки могут привести к значительным задержкам. Счетчик Память\Ошибок страницы/сек (Page Faults/sec) указывает общий темп обработки процессором всех типов ошибки страниц. В счетчике Память\Ввод страниц/сек (Pages Input/sec) записывается общее число страниц, считанных с диска для разрешения аппаратных ошибок. Счетчик Память\Чтений страниц/сек (Page Reads/sec) представляет общее число операций чтения с диска, необходимых для разрешения аппаратных ошибок. Значение счетчика Память\Ввод страниц/сек (Pages Input/sec) будет больше или равно значению счетчика Память\Чтений страниц/сек (Page Reads/sec) и позволяет оценить темп возникновения аппаратных ошибок. Высокий темп аппаратных ошибок означает, что вам следует увеличить объем памяти или уменьшить размер кеша сервера.

область: Файл подкачки

счетчики: Память\Байт в выгружаемом страничном пуле (Memory\ Pool Paged Bytes)

Память\Байт в невыгружаемом страничном пуле (Memory\Pool Nonpaged Bytes)

Как анализировать

Эти счетчики отслеживают число байтов в выгружаемом и невыгружаемом пуле. Выгружаемый пул — область системной памяти для объектов, которые могут быть записаны на диск в случае, если они не используются. Невыгружаемый пул — область системной памяти для объектов, которые нельзя записывать на диск. Если размер выгружаемого пула велик относительно общего объема физической памяти системы, вероятно, следует добавить в систему памяти. Если размер невыгружаемого пула велик относительно общего объема виртуальной памяти, вероятно, вам следует увеличить размер виртуальной памяти.

b) Мониторинг и настройка использования процессора

область: Очередь потоков

счетчики:

Система\Длина очереди процессора (System\Processor Queue Length)

Как анализировать:

Этот счетчик показывает число потоков, ожидающих выполнения. Потоки выстраиваются в очередь в области, общей для всех процессоров системы. Если значение этого счетчика на протяжении длительного времени равно 2 и более, вам требуется обновить или добавить процессоры.

область: Использование процессора

счетчики:

Процессор\% загрузки процессора (Processor\% Processor Time)

Как анализировать:

Этот счетчик показывает долю времени, которое данный процессор затрачивает на выполнение активных потоков. Этот счетчик нужно контролировать отдельно для каждого процессора, установленного на сервере. Если его значения высоки при умеренной загруженности системы ввода-вывода и сетевого интерфейса, вам требуется обновить или добавить процессоры.

с) Мониторинг и настройка операций ввода-вывода

область: Общая производительность диска

счетчики:

Физический диск\% активности диска (PhysicalDisk\% Disk Time)

Процессор % загруженности процессора (Processor\% Processor Time)

Сетевой интерфейс\Всего байт/сек (Network Interface Connection\Bytes Total/sec)

Как анализировать:

Если значение счетчика % активности диска (% Disk Time) велико при умеренной загруженности процессора и сетевого подключения, жесткий диск может стать причиной снижения производительности. Отслеживайте значение этого счетчика для всех жестких дисков сервера.

область: Дисковый ввод-вывод

счетчики:

Физический диск\Обращений записи на диск/сек (PhysicalDisk\Disk Writes/sec)

Физический диск\Обращений чтения с диска/сек (PhysicalDisk\Disk Reads/sec)

Физический диск\Средняя длина очереди записи на диск (PhysicalDisk\Avg.Disk Write Queue Length)

Физический диск\Средняя длина очереди чтения диска (PhysicalDisk\Avg.Disk Read Queue Length)

Физический диск\Текущая длина очереди диска (PhysicalDisk\Current Disk Queue Length)

Как анализировать:

Число операций записи и чтения в секунду демонстрирует интенсивность дискового ввода-вывода. Длина очередей чтения и записи подскажет, сколько запросов на чтение или запись ожидают обработки. В общем случае, желательно, чтобы ожидающих запросов было поменьше. Помните, что задержки запросов пропорциональны длине очереди за вычетом числа дисков в массиве RAID

d) Мониторинг и настройка сетевого подключения

Область: Пропускная способность сети и возможность подключения

Счетчики:

Сетевой интерфейс\Получено байт/сек (Network\Bytes Received/sec)

Сетевой интерфейс\Отправлено байт/сек (Network\Bytes Sent/sec)

Сетевой интерфейс\Всего байт/сек (Network\Bytes Total/sec)

Сетевой интерфейс\Текущая пропускная способность (Network\ Current Bandwidth)

Как анализировать:

Если при средней нагрузке общее число байтов в секунду превышает 50% пропускной способности, сервер, возможно, не справится с пиковыми нагрузками. Рассмотрите

возможность выполнения операций, требующих большой пропускной способности, например, сетевого резервного копирования, на отдельной сетевой плате. Помните, что значения этих счетчиков следует сравнивать в сочетании со счетчиками Физический диск\% активности диска (PhysicalDisk\% Disk Time) и Процессор\% загрузки процессора (Processor\% Processor Time). Если нагрузка на диск и процессор невелика, а показания сетевых счетчиков значительны, ваша проблема, вероятно, связана с пропускной способностью. Оптимизируйте настройки сетевой платы или установите дополнительную сетевую плату. Помните о планировании — важно понимать, что не всегда бывает достаточно просто вставить плату в разъем и подключить ее к сети.

Часть 4. Группы сборщиков данных

1. Создать группу сборщиков из шаблона – Основной. Назвать «Из шаблона Основной». Запустить сборщик. Дать поработать 10 минут. Остановить. Проанализировать отчет.
2. Создать группу сборщиков из шаблона System Performance (производительность системы). Назвать «Из шаблона производительность». Запустить сборщик. Дать поработать 10 минут. Остановить. Проанализировать отчет.
3. Создать группу сборщиков из шаблона System Diagnostics (диагностика системы). Назвать «Из шаблона диагностика». Запустить сборщик. Дать поработать 10 минут. Остановить. Проанализировать отчет.
4. Для группы сборщиков с именем «Основные подсистемы» задать расписание: сегодняшний день, через 10 минут, остановка спустя 5 минут работы. Дождаться запуска группы сборщиков. После того как группа сборщиков отработает, проанализировать отчет.
5. Запустить все группы сборщиков для основных подсистем сервера созданные ранее. Дать группам сборщиков поработать 15 минут. Остановить все группы сборщиков данных. Проанализировать отчеты согласно рекомендациям по анализу. Выводы представить в отчете.

Контрольные вопросы

1. Какие типы журналов существуют?
2. События какого типа регистрируются в журнале “Система”?
3. События какого типа регистрируются в журнале “Безопасность”?
4. Какие уровни событий существуют?
5. Что собой представляют и для чего используются настраиваемые представления?
6. Что собой представляют и для чего используются группы сборщиков?
7. Какие счетчики необходимо добавить в системный монитор, чтобы отследить основные показатели работы сервера, основные подсистемы?

Лабораторная работа № 4

Тема: Установка Active Directory, контроллера домена

Цель выполнения работы: формирование профессиональных умений по установке служб каталога, и повышению сервера до контроллера домена

Постановка задачи или ситуации

В этой работе Вам необходимо установить Доменные службы Active Directory (Active Directory Domain Services) и повысить сервер до контроллера домена с помощью утилиты dcpromo.

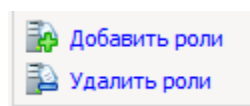
Порядок выполнения

Работу выполнить в операционной системе Windows Server 2008 R2. Для этого подключиться к удаленному рабочему столу, сервера **virtual**. Открыть программу **VirtualBox**. Открыть виртуальную машину с установленной операционной системой Windows Server 2008 R2.

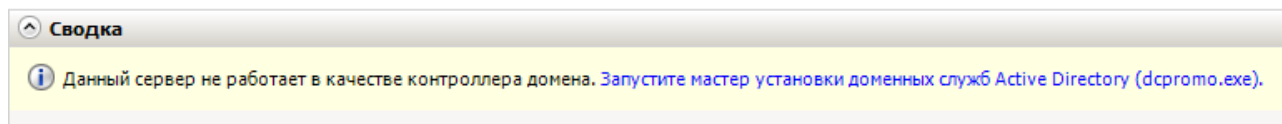
После выполнения всех частей работы оформить типовой отчет.

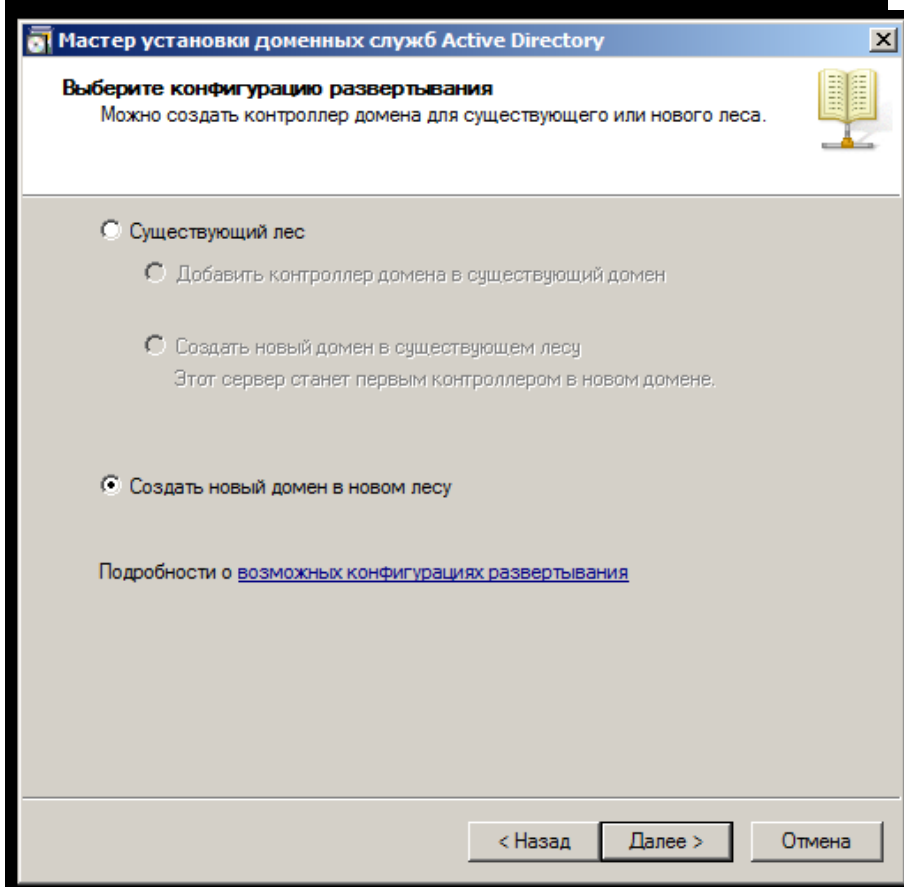
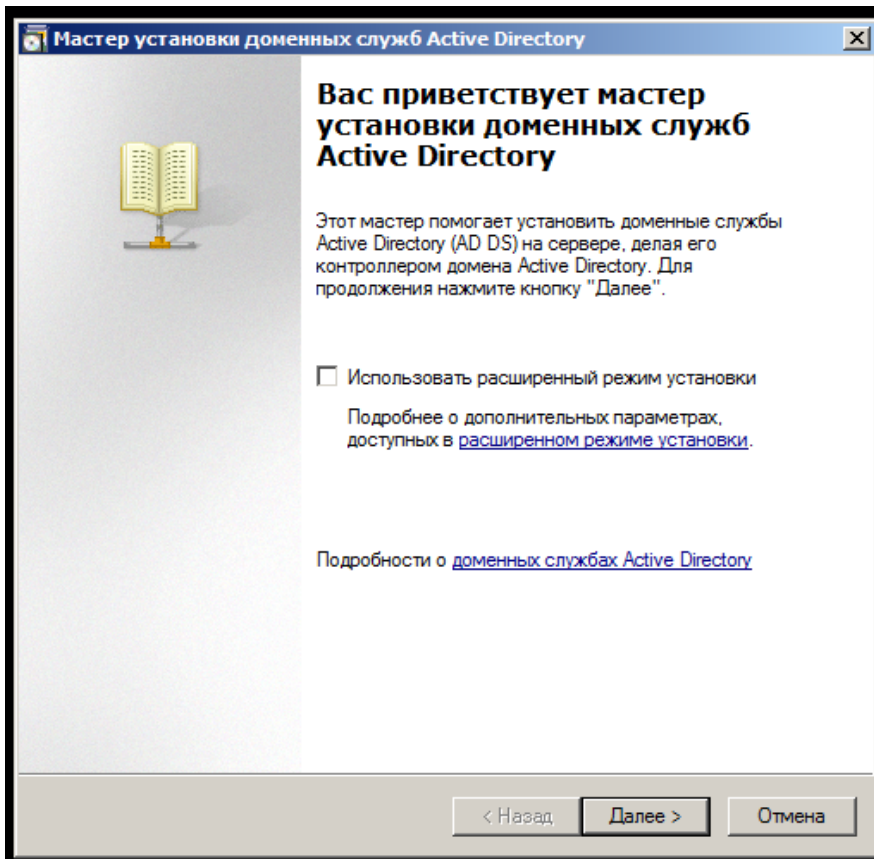
6. Установить доменные службы Active Directory
7. Повысить сервер до контроллера домена
8. *При необходимости, интегрировать зону DNS в Active Directory.

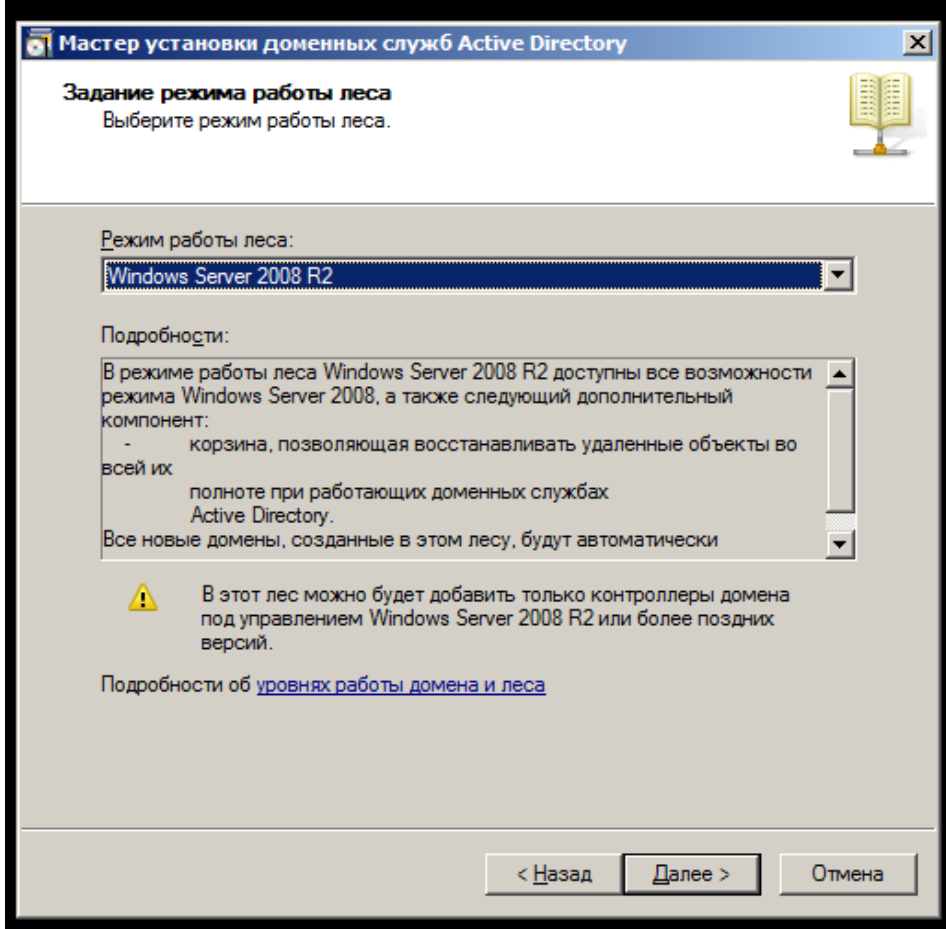
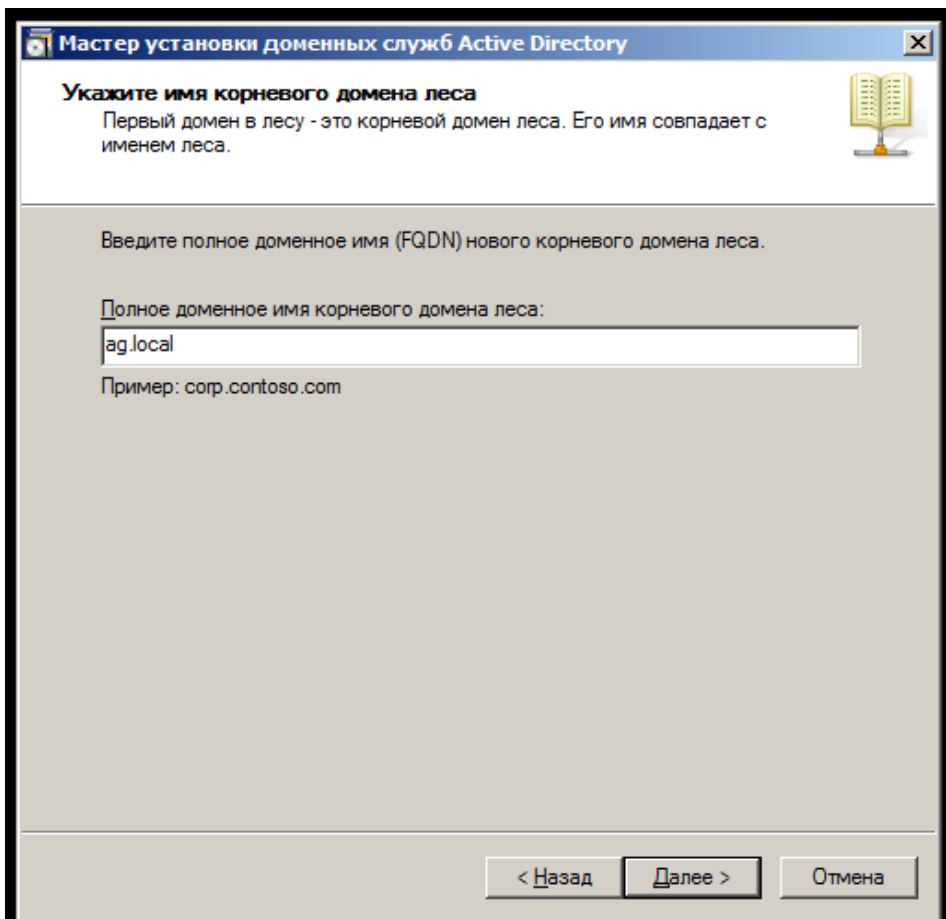
Ниже представлены скриншоты, демонстрирующие процесс установки доменных служб Active Directory и повышения сервера до контроллера домена.

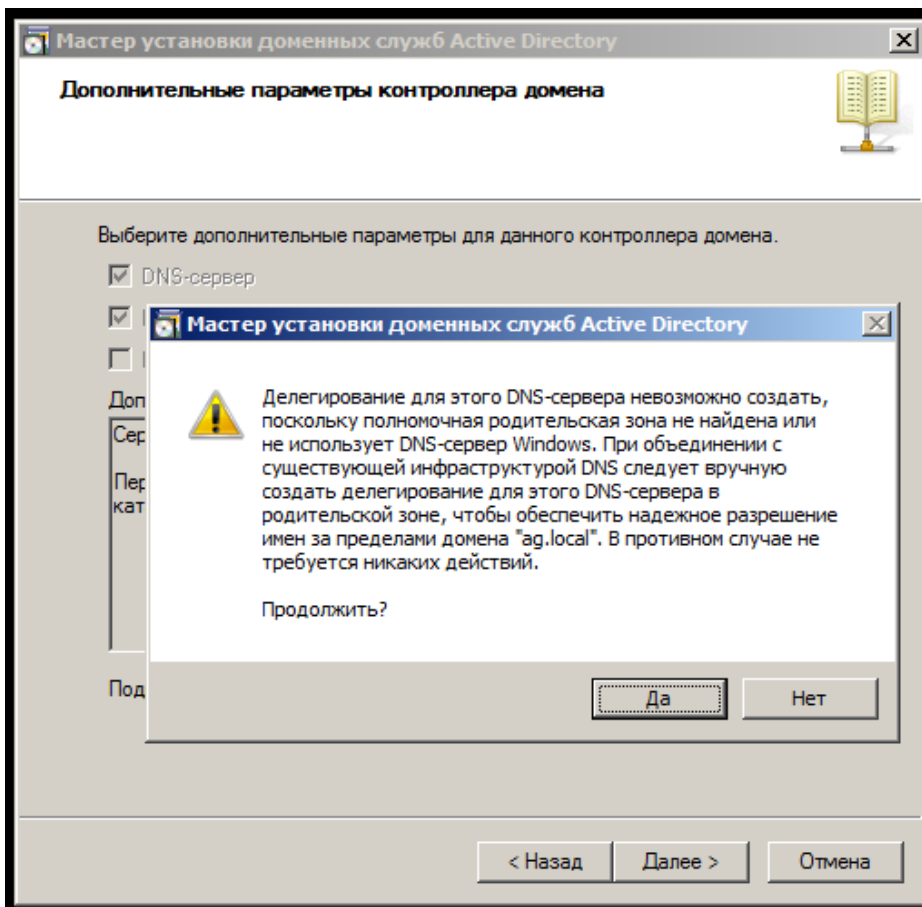
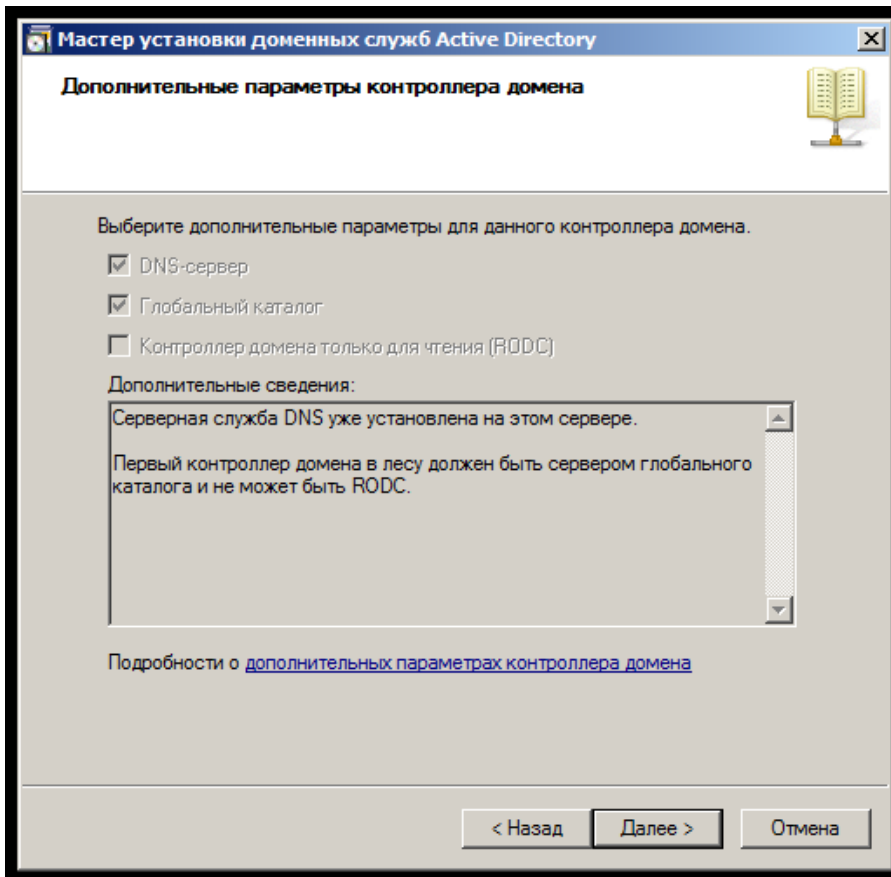


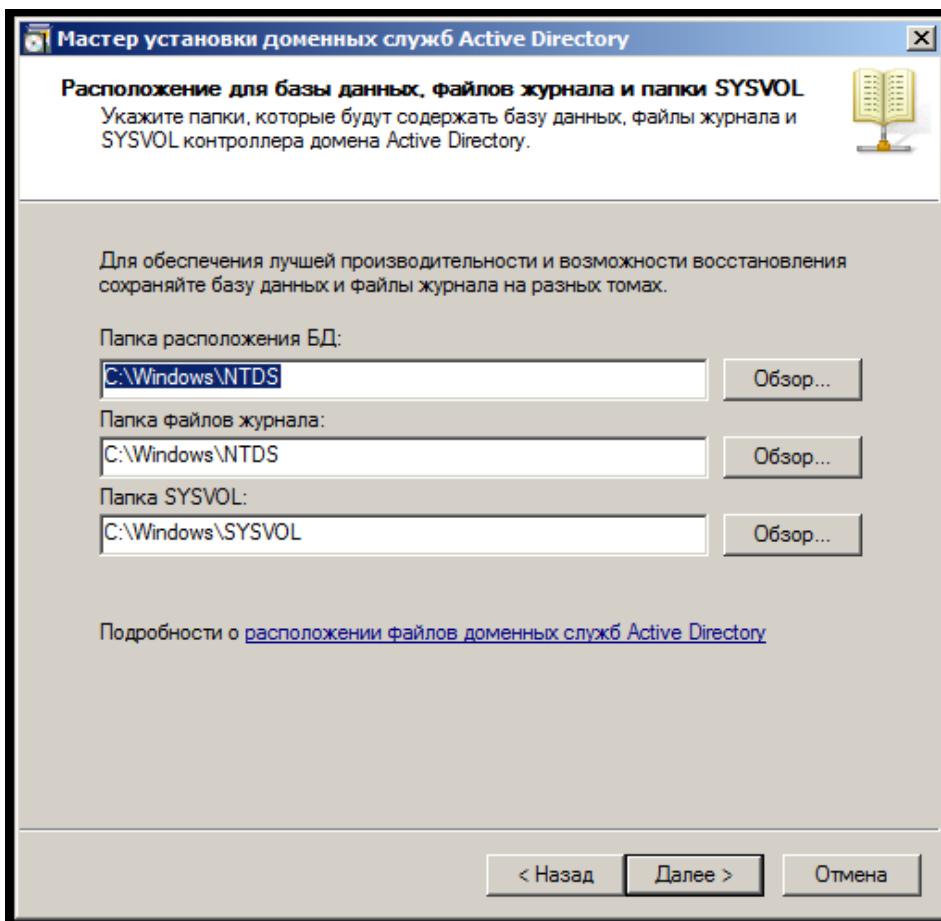
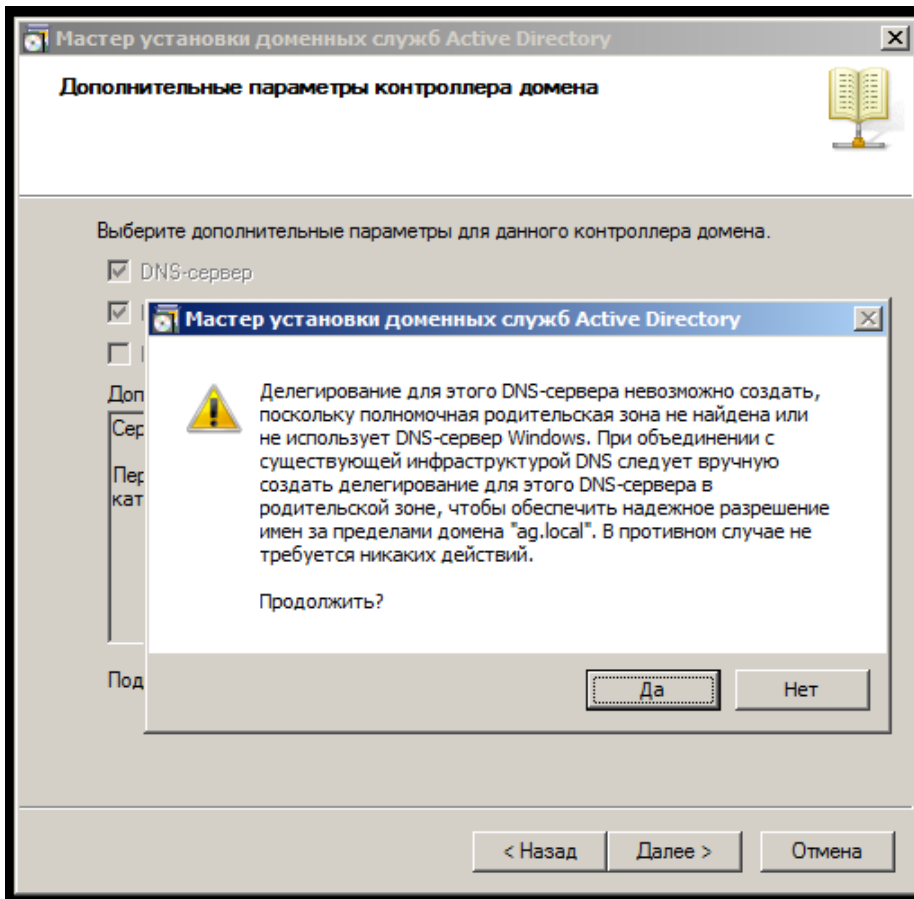
- Веб-сервер (IIS)
- Доменные службы Active Directory
- Сервер приложений
- Службы Active Directory облегченн
- Службы Windows Server Update Ser

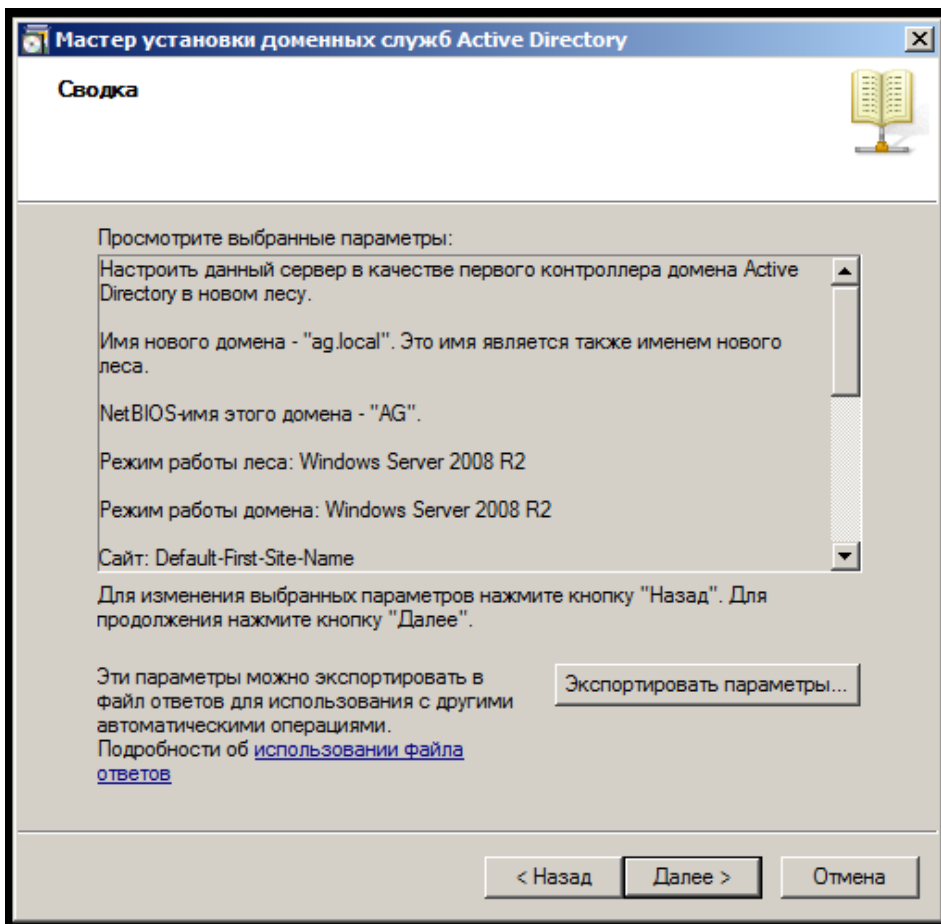
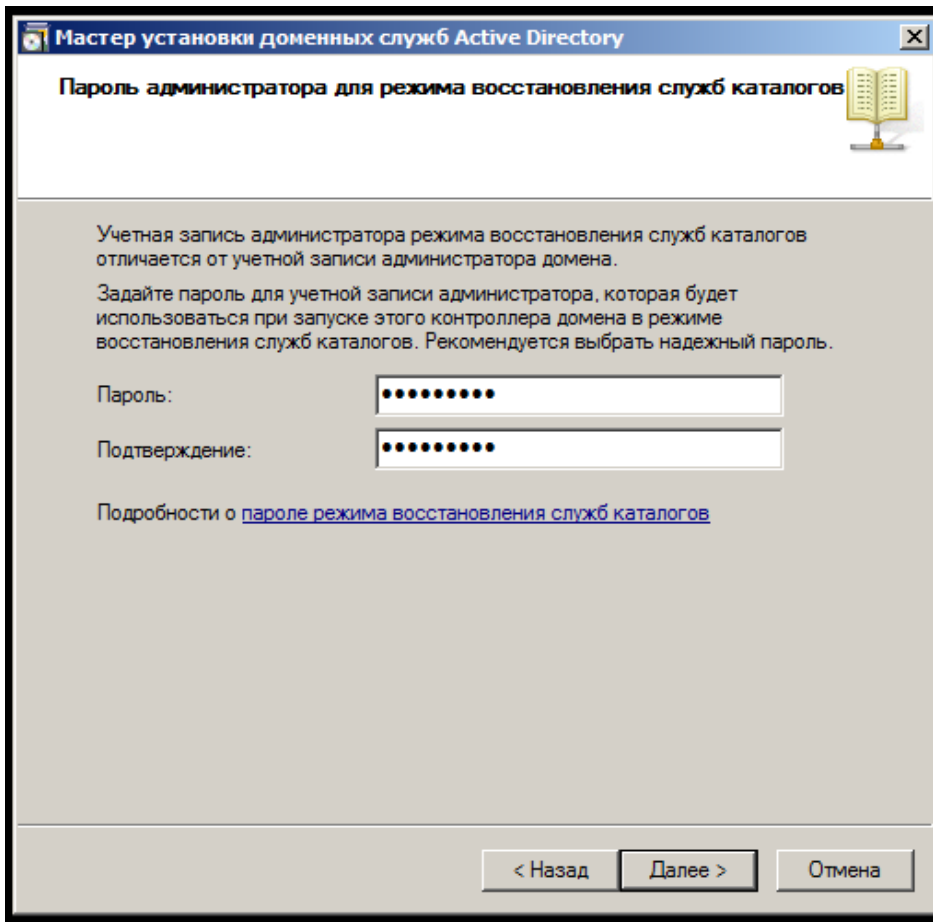


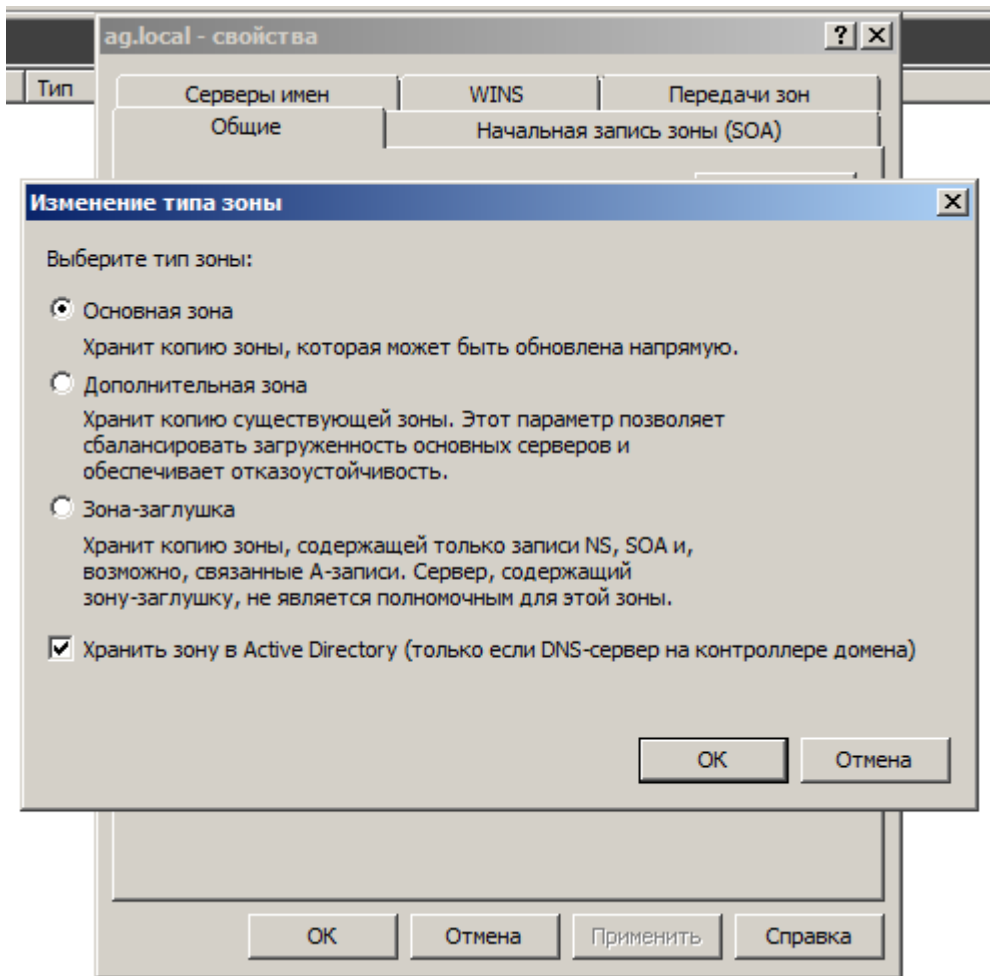






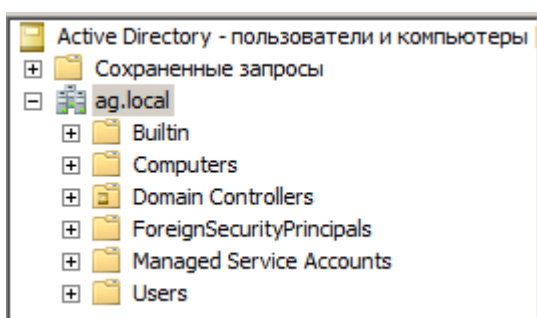






Зоны прямого просмотра зон: 1

Название	Тип	Состояние
ag.local	Интегрированная в Active Directory основная	Выполняется



Контрольные вопросы

8. Как взаимосвязаны Active Directory и DNS?
9. Как установить Active Directory?
10. Как проверить правильность установки Active Directory?
11. Что такое RODC (Read-Only Domain Controller)? Зачем он может использоваться?
12. Что такое логическая структура Active Directory? Что в нее входит?
13. Что такое физическая структура Active Directory? Что в нее входит?
14. Что такое домен в AD?
15. Что такое лес, дерево в AD?
16. Что такое подразделение в AD?
17. Что такое сайт, подсеть в AD?
18. Назовите средства управления Active Directory?

Лабораторная работа № 5

Тема: Создание учетных записей

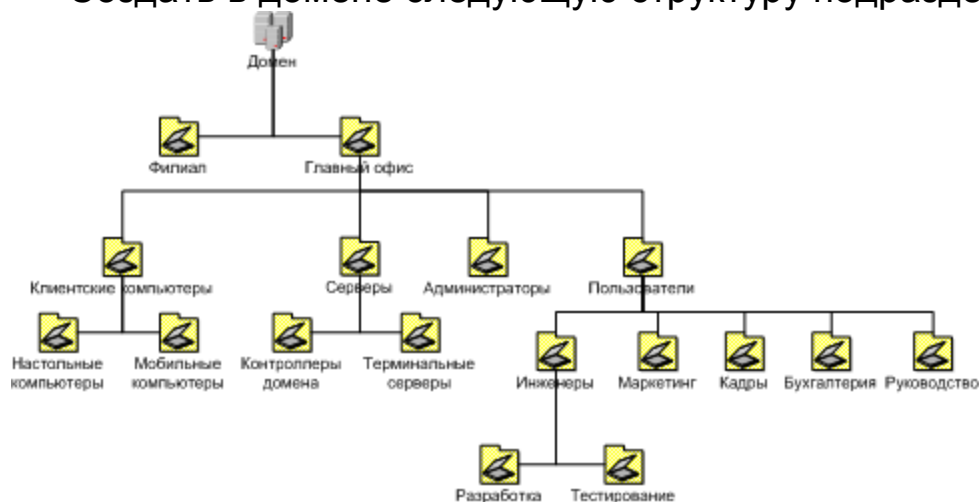
Цель выполнения работы: формирование профессиональных умений по: планированию учетных записей пользователей и групп; созданию учетных записей пользователей и групп; созданию подразделений; управлению учетными записями пользователей и групп.

Порядок выполнения

Подключиться к удаленному рабочему столу, сервера **virtual**. Открыть программу **VirtualBox**. Открыть виртуальную машину с установленной операционной системой Windows Server 2008 R2.

Часть 1. Создание структуры подразделений.

-Создать в домене следующую структуру подразделений:



Часть 2. Планирование новых учетных записей.

- Спланировать 15 учетных записей.
- Заполнить таблицу - «Шаблон планирования учетных записей».
- Определить соглашение об именах. Затем по нему определить учетное имя каждого пользователя и записать его в колонку «Учетная запись».
- Разработать требования к паролю каждого из пользователей и перечислить их в колонке «Требования к паролю».
- В колонке «Местонахождение домашнего каталога» указать один из двух вариантов: локальный компьютер или сервер.

- В колонке «Время работы» записать допустимые часы регистрации для каждого пользователя (например, 24/7, если пользователю разрешено регистрироваться круглые сутки 7 дней в неделю).
- В колонке «Допустимые рабочие места» указать «Да», если работа пользователя с разных машин будет ограничена и «Нет» — в противном случае.

Заполняя шаблон, помните о некоторых тонкостях:

- У двоих сотрудников могут совпадать имена.
- Сотрудникам из ОУ «Инженеры» нужно разрешить менять свои пароли.
- Каждому сотруднику нужен домашний каталог. Все каталоги следует архивировать каждую ночь.
- Сотрудники, работающие в дневную смену, должны иметь доступ в сеть круглосуточно 7 дней в неделю.

Шаблон планирования учетных записей

Полное имя	Учетная запись	Описание	Требование к паролю	Местонахождение домашнего каталога	Время работы	Допустимые места работы
Синеоков Сергей Прохорович		Директор				
Плеханова Алина Вячеславовна		Руководитель отдела разработки ПО				
Белова Валентина Константиновна		Руководитель отдела кадров				
Набокина Ксения Юлиевна		Менеджер по продажам				
Панфёров Павел Эдуардович		Старший Android Developer				
Фамусов Иван Фролович		Android Developer				
Иньков Константин Казимирович		Старший iPhone Developer				
Дуболазов Евгений Капитонович		iPhone Developer				
Харламов Виктор Тимурович		iPhone Developer				
Набокина Валентина Владленовна		Тестировщик				

Онипченко Майя Серафимовна		Тестировщик				
Куваева Валентина Фомевна		Главный бухгалтер				
Третьяков Сергей Андроникович		Бухгалтер				
Яценко Тарас Самсонович		Менеджер проектов				
Круминь Владислава Игнatieвна		Специалист отдела кадров				

Часть 3. Создание и настройка учетных записей пользователей.

Создать подразделения.

- Создать домашний каталог для пользователей (C:\users).
- Создать учетную запись Template Profile - модель профиля.
- Настроить шаблон профиля. Настроить путь к профилю (Profile path). Настроить домашнюю папку (Home folder).
- Создать 15 пользователей согласно таблице “Шаблон планирования учетных записей”. Пользователей разместить в соответствующих подразделениях.
- Зайти в клиентскую ОС (например **Windows XP**) под учетными записями - Директора, Тестировщика, Android Developer’a.

В подразделении «Настольные компьютеры» создать учетные записи компьютеров: PC1, PC2, PC3, PC4, PC5, PC6.

В подразделении «Мобильные компьютеры» создать учетные записи компьютеров: notebook1, notebook2, notebook3, notebook4, notebook4, notebook5.

В подразделении «Серверы» создать учетные записи компьютеров: FILE-SERVER, APP-SERVER, PRINT-SERVER.

В подразделении “Разработка” создать группу “iPhone разработчики”.
Добавить в группу трех iPhone разработчиков.

В подразделении “Разработка” создать группу “Andorid разработчики”.
Добавить в группу “Andorid разработчики” соответствующих Android-разработчиков.

В подразделении «Тестирование» создать группу «Тестировщики», включить в нее всех тестируемых.

В подразделении «Кадры» создать группу «Отдел кадров», включить в нее всех «кадровиков».

В подразделении «Руководство» создать группу «Руководители» включить в нее директора и всех руководителей.

Вложенные группы.

Создать группу “Инженеры” в подразделении “Инженеры”. Добавить в группу “Инженеры” группы “iPhone разработчики”, “Android разработчики”, “Тестировщики”.

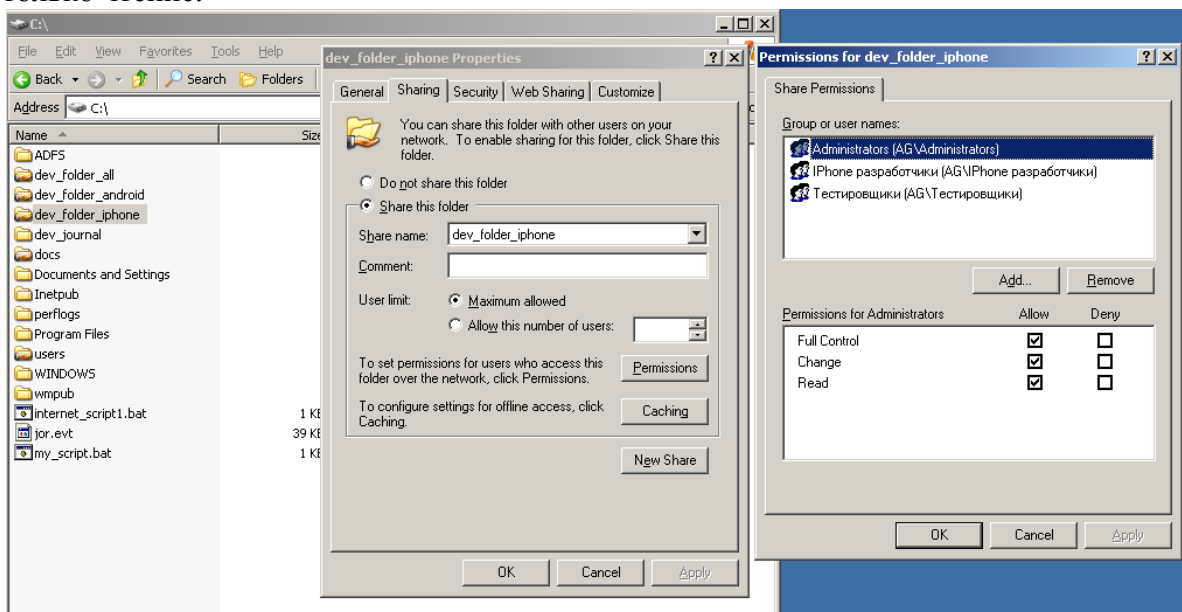
Экспортировать учетные записи. Использовать утилиту CSVDE. (csvde -f имя-файла)

Часть 4. Настройка доступа к сетевым ресурсам на основе групп безопасности.

1. Создать на диске C:\ сервера, три общедоступные папки (видимые по сети): dev_folder_iphone, dev_folder_android, dev_folder_all.

2. Для dev_folder_iphone:

Сделайте папку общедоступной, и настройте права доступа по сети сл. образом: для iPhone разработчиков и Администраторов - полный доступ, для Тестировщиков - только чтение.

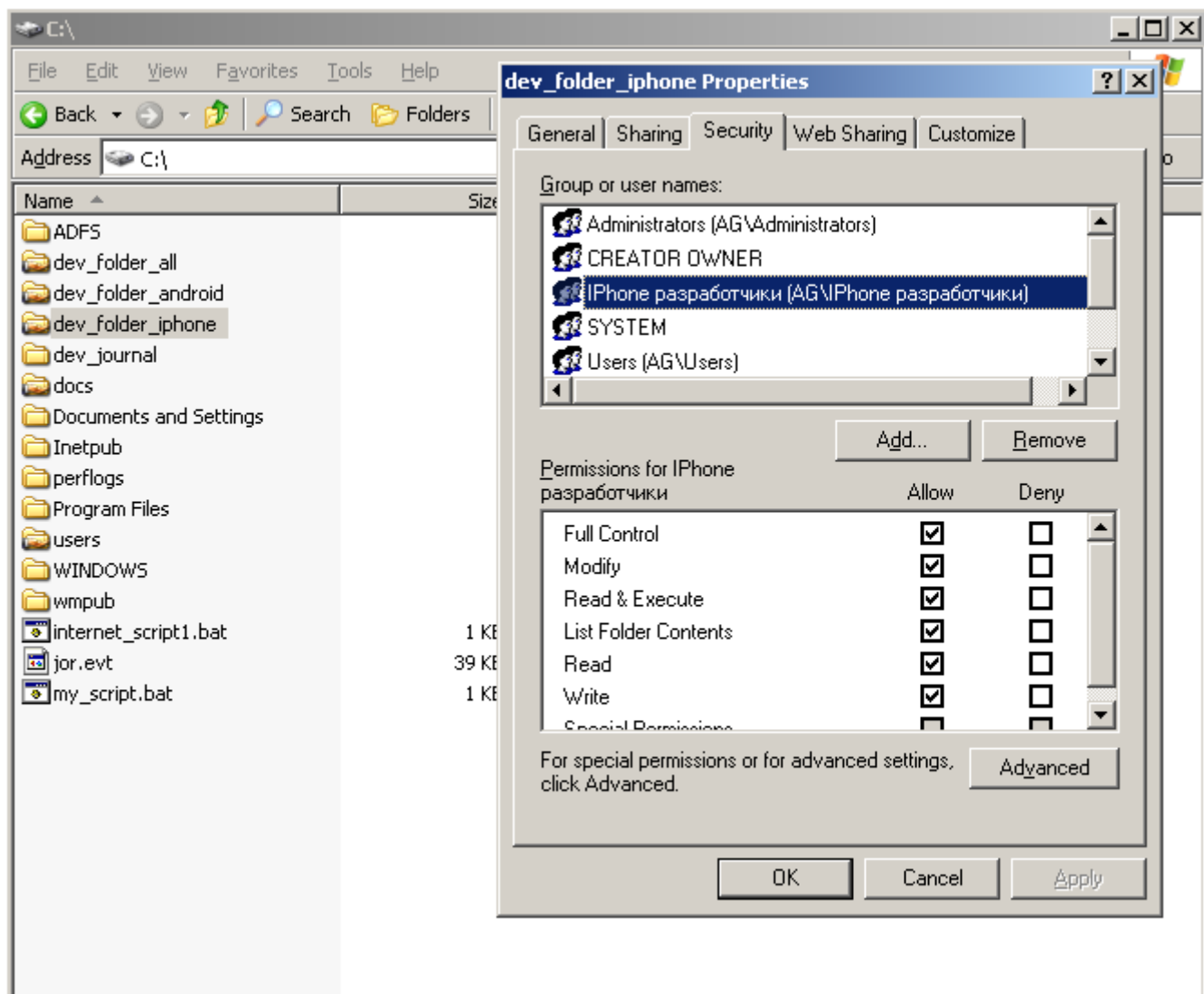


На вкладке Security настройте права доступа:

группе “iPhone разработчики” - предоставить полный доступ

группе “Тестировщики” - предоставить доступ: Чтения, Чтения и выполнения,

Просмотра содержимого папки.



- Для dev_folder_android, настройте права доступа аналогичным образом. Сначала права доступа по сети (Share permission) - только вместо “iPhone разработчиков”, разрешите доступ “Android разработчикам”.

Затем настройте Security Permission сл. образом:

группе “Android разработчики” - предоставить полный доступ.
группе “Тестировщики” предоставить доступ: Чтения, Чтения и выполнения, просмотра содержимого папки.

- Для dev_folder_all: настроить Share Permission для Администраторов и Инженеров в полный доступ.

Настроить Security Permission, сл. образом:

группе “Инженеры” предоставить полный доступ.

- Проверить правильность настройки прав доступа (проверять надо в проводнике выполнив переход к сетевому ресурсу \\имя_сервера) сл. образом:

Выполнить вход под учетной записью “iPhone разработчика”, проверить доступ к каждой из трех папок. Оценить результаты.

Выполнить вход под учетной записью “Тестировщика”, попробовать создать файл в каждой из трех папок. Оценить результаты.

Выполнить вход под учетной записью “Менеджера по продажам”. Попробовать открыть каждую из трех папок. Оценить результат.

Часть 5. Делегирование административных полномочий

1. Откройте остнастку Active Directory - Пользователи и компьютеры.
2. Создайте нового пользователя - второго администратора в подразделении "Администраторы".
3. Предоставьте административные права на ОУ: кадры, маркетинг, бухгалтерия - второму администратору.

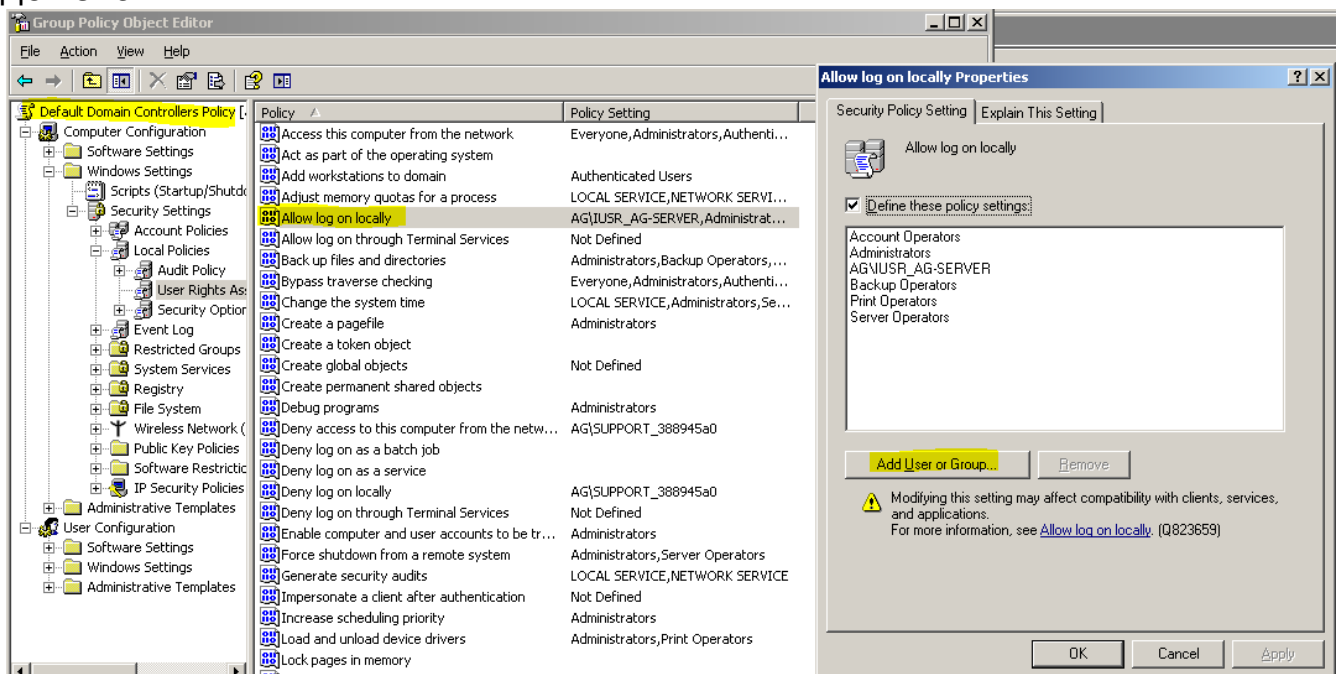
Для этого:

- Щелкнуть пр. кнопкой мыши на подразделении
- Выбрать "Делегирование управления"
- Кнопка "Далее" - Кнопка "Добавить" -
- Выбрать пользователя
- Кнопка "Далее" - Выбрать "Делегировать следующие обычные задачи"- Поставить галочки у всех пунктов списка
- Кнопка "Далее" - Кнопка "Готово"

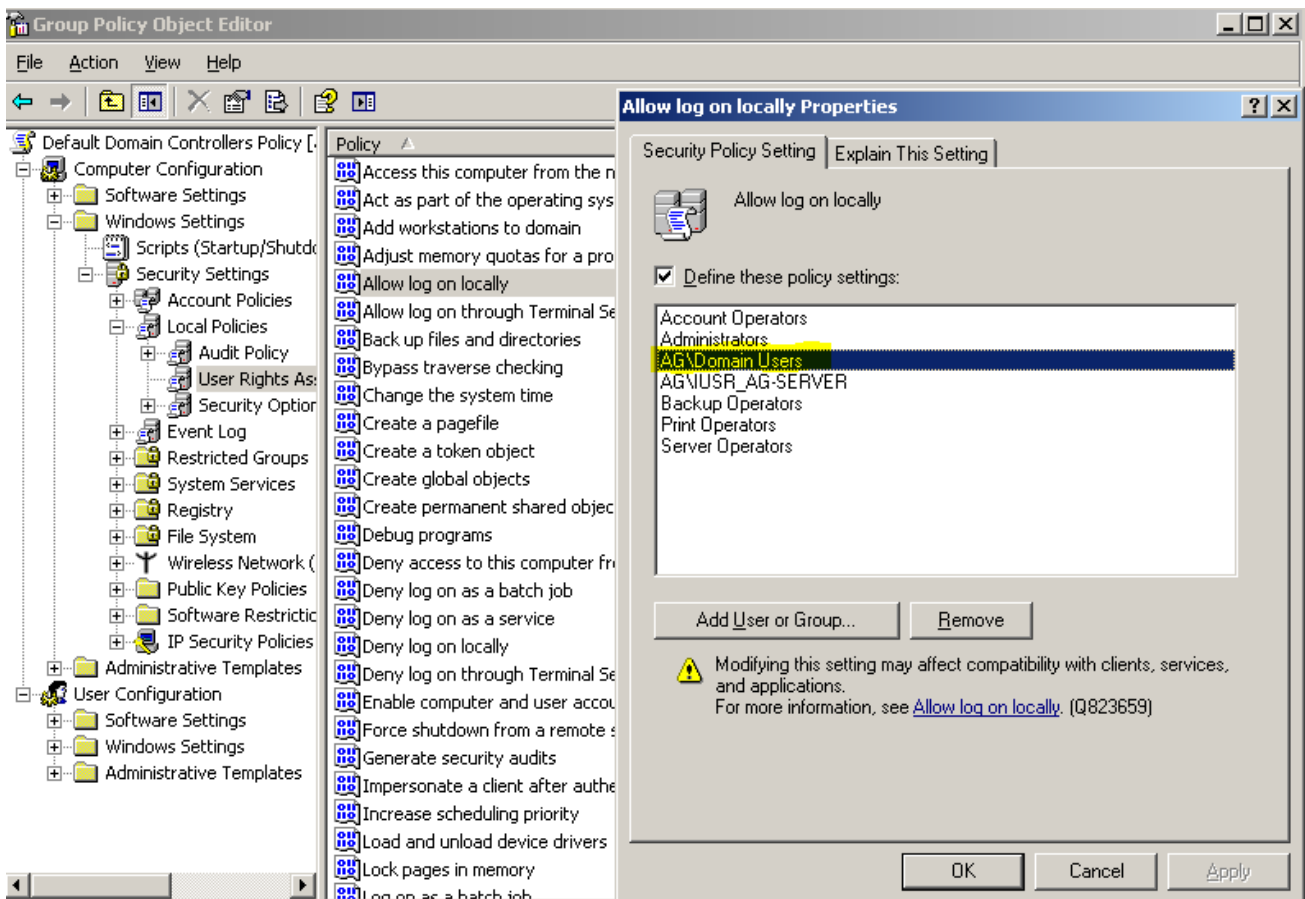
4. Войдите в систему как второй администратор.

Для этого предварительно нужно настроить групповую политику контроллера домена (Default Domain Controllers Policy). Нужно разрешить все пользователям домена (Domain Users) - локально входить на контроллер домена. Для этого: откройте Default Domain Controllers Policy в остнастке Group Policy Object Editor.

найдите политику Allow log on locally и добавьте в нее пользователей домена.



После добавления, должна появиться соответствующая строка.



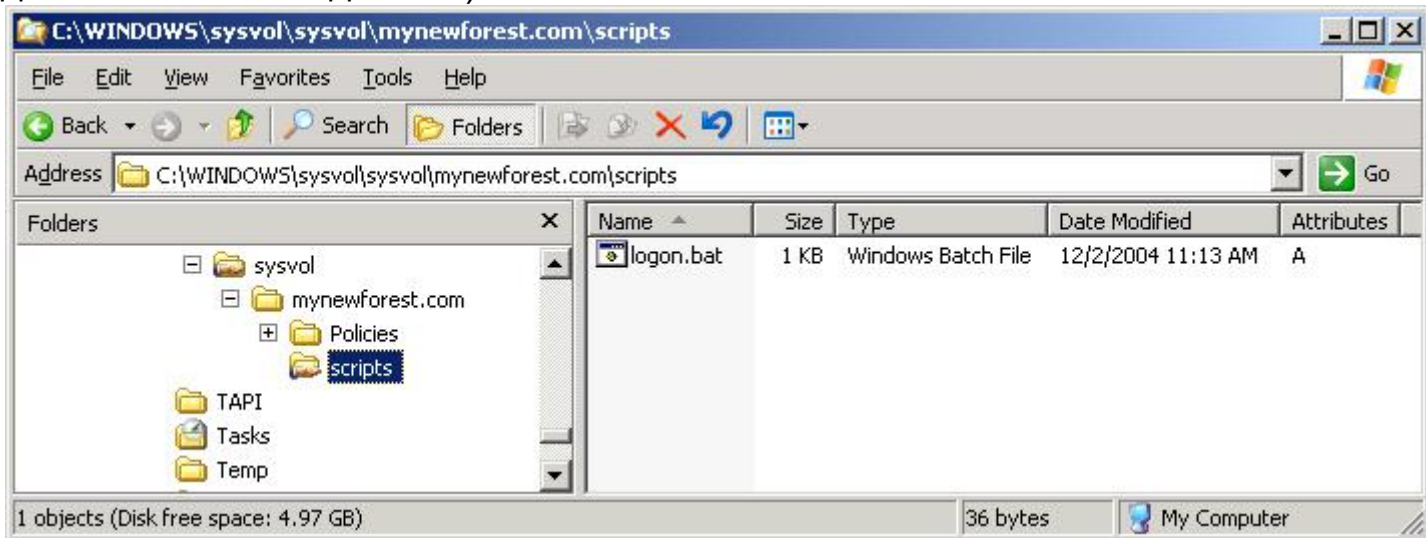
5. Откройте остнастку Active Directory - Users and Computers (Выполнить - dsa.msc).
6. Попробуйте изменять свойства пользователей в подразделениях кадры, маркетинг, бухгалтерия. Попробуйте добавить туда новых пользователей.
7. Попробуйте изменять, добавлять пользователей в подразделениях - разработка, тестирование, руководство.
8. Выйти из учетной записи второго администратора.

Часть 6. Сценарии входа для пользователей

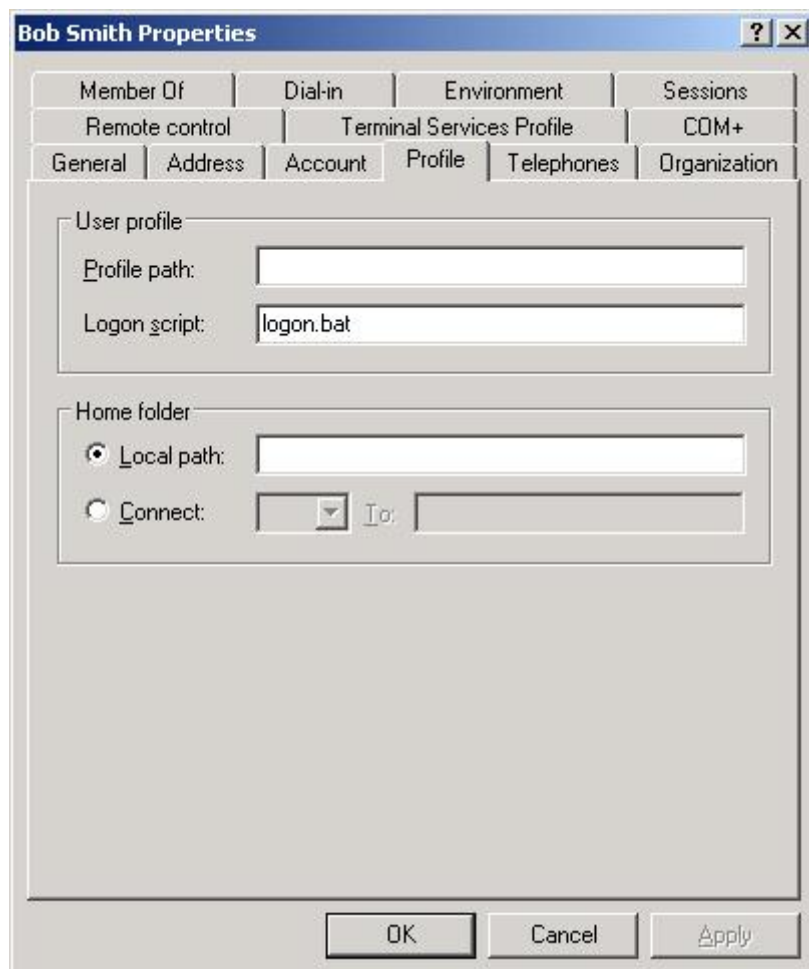
1. Создать сценарий (скрипт) для “менеджера по продажам”, который добавляет сетевой диск (созданный в предыдущей части), для совместного использования.
2. Создать файл с именем logon.bat. Файл с batch сценарием должен выглядеть так:


```
@echo off
net use x: \\VasyaServer\Share /user:VASYADOMAIN\VASYA 12345
```
3. Поместите файл сценария в NETLOGON контроллере домена, %systemroot%\sysvol\sysvol\\scripts как показано на рисунке (После того, как сценарий помещен в

NETLOGON, он автоматически будет размещен на всех контроллерах домена в вашем домене):



4. Назначьте сценарий для учетной записи “менеджера по продажам” (Если вы храните ваш сценарий не в NETLOGON, то вам необходимо набрать полный UNC путь к сценарию в поле Logon Script)



5. Проверить работу сценария - выполнив вход под учетной записью “менеджера по продажам”.

10. Оформить типовой отчет.

Контрольные вопросы

1. Учетные записи пользователей. Локальные. Доменные.
2. Учетные записи групп. Типы групп. Область действия.
3. Встроенные учетные записи пользователей
4. Возможности учетной записи
5. Административные группы
6. Неявные группы и идентификаторы
7. Инструменты для создания учетных записей пользователей и групп (AD пользователи и компьютеры, Локальные пользователи и группы)
8. Правила именования учетных записей (Отображаемое имя, Имя для входа).
9. Схемы именования.

Лабораторная работа № 6

Тема: Создание и настройка групповых политик

Цель выполнения работы: формирование профессиональных умений по: созданию, настройке и управлению групповыми политиками

Порядок выполнения

Подключиться к удаленному рабочему столу, сервера virtual. Открыть программу VirtualBox. Открыть виртуальную машину с установленной операционной системой Windows Server 2008 R2.

Время выполнения: 4 часа (2 занятия).

Ход работы:

Часть 1. Изучение остнастки Group Policy Editor.

1. Открыть Управление групповой политикой
2. Открыть групповую политику домена по умолчанию для редактирования в остнастке Group Policy Editor.
3. Изучить доступные для редактирования политики.

Часть 2. Создание групповых политик.

1. Создать групповую политику MarketingGroupPolicy для подразделения “Маркетинг”, и настроить ее следующим образом:
 - запретить использование командной строки.
 - запретить доступ к диспетчеру задач
 - сделать недоступными средства редактирования реестра;
 - запретить изменять настройки сетевых подключений.
 - запретить доступ к мастеру новых подключений;
 - " Конфигурация пользователя " / " Административные шаблоны " / " Компоненты Windows " / " Проводник" / " Удалить меню " Файл " из проводника Windows "
 - " Конфигурация пользователя " / " Административные шаблоны " / " Компоненты Windows " / " Проводник" / " Удалить кнопку " Поиск " из проводника Windows "
 - " Конфигурация пользователя " / " Административные шаблоны " / " Панель задач и меню " Пуск "" / "Удалить меню " Найти " из главного меню "
 - " Конфигурация пользователя " / " Административные шаблоны " / " Панель задач и меню " Пуск "" / "Удалить команду " Выполнить " из меню " Пуск ""
 - " Конфигурация пользователя " / " Административные шаблоны " / " Рабочий стол " / " Удалить значок "Мои документы " с рабочего стола "
 - " Конфигурация пользователя " / " Административные шаблоны " / " Рабочий стол " / " Удалить значок "Мой компьютер " с рабочего стола "
 - " Конфигурация пользователя " / " Административные шаблоны " / " Рабочий стол " / " Не показывать значок Internet Explorer "

2. Проверить политику MarketingGroupPolicy выполнив вход под учетной записью “Менеджера по продажам”. Проверить сл. образом:
 - Выполнить -> regedit
 - Выполнить -> cmd
 - Попробовать изменить настройки сетевого подключения
 - Попробовать создать новое сетевое подключение
 - Проанализировать изменения интерфейса

Часть 3. Работа с Group Policy Management Console (Управление групповой политикой)

1. Открыть консоль.
2. Изучить управление политиками с помощью данной консоли:
 1. установите указатель мыши на различных объектах AD (домен, Организационные подразделения), просмотрите списки объектов ГП, привязанных к выбранным объектам AD;
 2. раскройте контейнер Group Policy Objects (объекты групповой политики), просмотрите полный список ГП в вашем домене;
 3. в этом же списке откройте какой-либо объект ГП для редактирования (щелкнуть правой кнопкой мыши на объекте ГП, выбрать Edit);
 4. создайте резервную копию (задача «архивировать») объекта ГП на жестком диске.
 5. Смоделируйте групповую политику для любого пользователя из подразделения маркетинг на компьютере PC1.
 6. Создайте результирующую политику для любого пользователя из подразделения маркетинг на компьютере PC2.

Часть 4. Создание и настройка групповой политики. Ограничение запускаемых программ.

1. Открыть оснастку Управление групповой политикой
2. Для подразделения “Бухгалтерия” создать новую групповую политику - Clerks Group Policy.
3. Включить, и настроить политики (user configuration) - ограничивающие запуск следующих программ (использовать правило пути): Paint , Windows Media Player , косынка, червы, солитер, пасьянс “паук”.
4. Зайти под учетной записью Бухгалтера и проверить действие политики (желательно выполнить вход в Windows XP).

Часть 5. Установка программ средствами групповых политик с использованием msi файлов

1. Скачать msi-файл установки Adobe Reader’a.
2. Поместить файл в общедоступную папку на сервере.
3. Для Clerks Group Policy настроить политику - User Configuration - Software Settings - Software installation. Добавить пакет Adobe Reader. Выбрать Deployment method - Assigned; в окне “Свойства” во вкладке Deployment установить флаг - Install this application at logon.
4. Выполнить вход под учетной записью “Бухгалтера”. Проверить установилась ли программа Adobe Reader.

Часть 6. Установка программ средствами групповых политик с использованием zip файлов

1. Скачать exe-файл установки vlc player’a.
2. Поместить файл в общедоступную папку на сервере.
3. Создать zip-файл для установки программы vlc player (установку выполнить с созданием иконки на рабочем столе, с созданием группы в меню Пуск).
4. Для Clerks Group Policy настроить политику для установки программы vlc player.

5. Выполнить вход под учетной записью “Бухгалтера”, зайти в “Установка и удаление программ” - “Установка программ” и установить vlc player.

Часть 7. Сценарии входа

1. Открыть папку %systemroot%\sysvol\sysvol\<domain_DNS_name>\scripts
2. Создать сценарий входа который добавляет сетевой диск (сетевую папку), для совместного использования. Файл с batch сценарием должен выглядеть так:
@echo off
net use x: \\server\name_of_folder /user:YOURDOMAIN\USERNAME 12345pwd
3. Для Clerks Group Policy настроить соответствующую политику (User Configuration - Windows Settings - Scripts (Logon/Logoff)- Logon).
4. Проверить работу групповой политики - выполнив вход под учетной записью “Бухгалтера”.

Оформить типовой отчет.

Контрольные вопросы

10. Назовите определение групповой политики?
11. Назовите назначение групповой политики?
12. Расскажите про GPO, линки?
13. Расскажите про порядок наследования?
14. Расскажите про порядок применения ГП?
15. Расскажите про разделы ГП?
16. Назовите средства редактирования ГП?
17. Расскажите про обновление групповых политик. Как оно происходит, когда?
18. Назовите задачи по управлению ГП?
19. Назовите способы устранения проблем связанных с ГП?
20. Расскажите про управление сценариями средствами ГП?
21. Расскажите про развертывание программ средствами ГП?

Тема: Управление файловыми системами и дисками

Цель выполнения работы: формирование профессиональных умений по использованию консолей управления файловыми системами и дисками

Порядок выполнения

Подключиться к удаленному рабочему столу, сервера **virtual**. Открыть программу **VirtualBox**. Открыть виртуальную машину с установленной операционной системой Windows Server 2008 R2.

Управление дисками

В ходе выполнения лабораторной работы нам понадобится добавить диски к виртуальной машине. Добавить два жестких диска по 2 Гб.

Запустить оснастку ServerManager и в ней открыть узел Storage-> Disk Management.

Преобразовать новые диски в тип Dynamic.

Для первого диска создать новый том D:

Теперь предположим, что вам понадобилось увеличить объем логического диска. Для этого задействуйте второй физический диск. В контекстном меню для тома D: - пункт Extend Volume. С помощью мастера добавьте все пространство второго диска к тому D:. Обратите внимание, что тип тома изменится с «Простого» на «Составной».

Квоты и сетевые папки

Предположим, нам нужно разместить на сервере файлы пользователей нашего домена. И для этого будем использовать диск D:. Зачастую при администрировании файлового сервера возникает необходимость отслеживать, сколько дискового пространства используется каждым из пользователей и, при необходимости, ограничивать это значение. Сделать это позволяет механизм дисковых квот.

В проводнике откройте окно свойств диска D: (Start->Computer щелчок правой клавишей на диске D:, пункт Properties в контекстном меню). Перейдите на вкладку Quota и отметьте флажок Enable quota management, установите какую-нибудь небольшую квоту (например, 1 Мб) и пороговое значение для предупреждения администратора (оно должно быть не больше размера квоты, а чаще берется чуть меньше). Просмотреть текущее использование дисковых квот можно, нажав на кнопку Quota Entries.

Для дальнейшего выполнения лабораторной работы проверьте, чтобы на сервере была установлена роль File Services. Если роли нет, добавьте ее.

Теперь создадим на диске E: папку и предоставим ее в общий доступ. Для этого откроем свойства папки и перейдем на вкладку Sharing.

Для более точной настройки общего доступа вместо кнопки Sharing нажмите Advanced Sharing. Отметьте переключатель Share this folder и введите имя общей папки (по умолчанию, подставляется такое же, как имя папки на диске). Если понадобится создать

папку, которая не будет отображаться в «Сетевом окружении», то в конце ее имени ставится знак \$. Но в нашем случае этого не требуется.

Теперь нажмите кнопку Permissions, чтобы отредактировать разрешения для пользователей. Вы увидите, что группа Everyone имеет разрешение на чтение (Read). Добавим в список (кнопка Add) доменного пользователя Администратор и дадим ему полный доступ к файлам папки (разрешение Full Control).

Тут надо отметить, что на файловой системе NTFS также устанавливаются разрешения на работу с файлами и папками (их можно просмотреть в свойствах файла или папки на вкладке Security). При доступе к папке локально, работают только разрешения NTFS.

При доступе к папке через сеть срабатывают и разрешения NTFS, и разрешения на общий доступ (итоговое разрешение – наименьшее из двух).

Оформить типовой отчет.

Контрольные вопросы

1. Расскажите, какими возможностями обладает оснастка Управление дисками?
2. Назовите типы дисков?
3. Что вы знаете про состояние дисков?
4. Назовите типы разделов динамических дисков?

Лабораторная работа № 8

Тема: Общий доступ

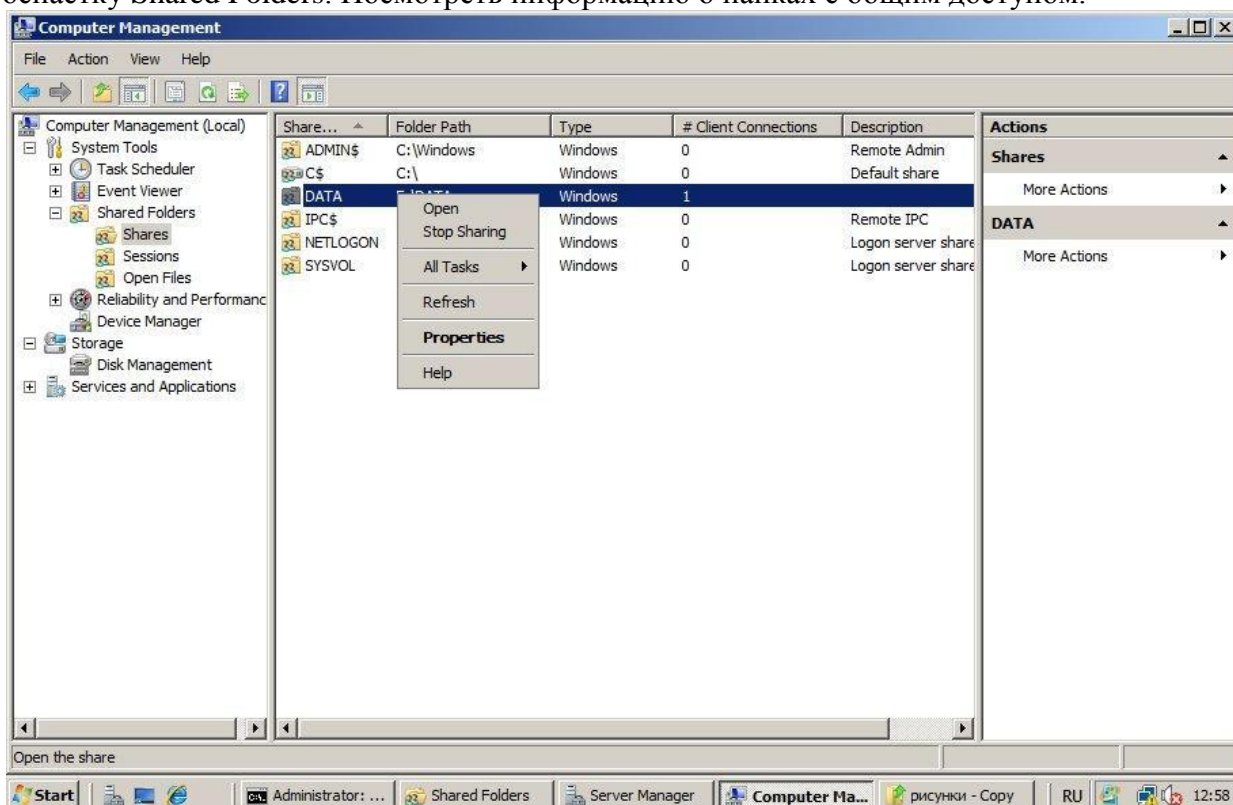
Цель выполнения работы: формирование профессиональных умений по управлению общими папками

Порядок выполнения

Подключиться к удаленному рабочему столу, сервера **virtual**. Открыть программу **VirtualBox**. Открыть виртуальную машину с установленной операционной системой Windows Server 2008 R2.

Управление общими папками

Первая задача – получение информации обо всех папках на компьютере, предоставляемых в общий доступ. Ее можно решить с помощью оснастки Shared Folders, входящей в состав оснастки Computer Management (Start->Administrative Tools-> Computer Management). Открыть оснастку Shared Folders. Посмотреть информацию о папках с общим доступом.



Из командной строки получить информацию о папках в общем доступе позволяет команда net share. Запустить команду, проанализировать ее вывод.

Посмотреть подробную информацию по конкретной папке net share имя_папки

Посмотреть список общих папок, на удаленном компьютере: net view \\server_name

Подключить две любые сетевые папки с сервера соседа\сервера колледжа. Двумя способами:

- с помощью команды net use
- с помощью диалогового окна

Диспетчер ресурсов файлового сервера (File Server Resource Manager)

Теперь познакомимся с дополнительными средствами администрирования файлового сервера. С помощью File Server Resource Manager можно, например, устанавливать квоты на отдельные папки или ограничить перечень типов файлов, которые пользователь может хранить на сетевом диске. Это средство добавляется как отдельная служба роли File Services.

Запустить Server Manager, открыть узел Роли -> File Services -> проверить установлена ли служба File Server Resource Manager. Если не установлена, добавить ее.

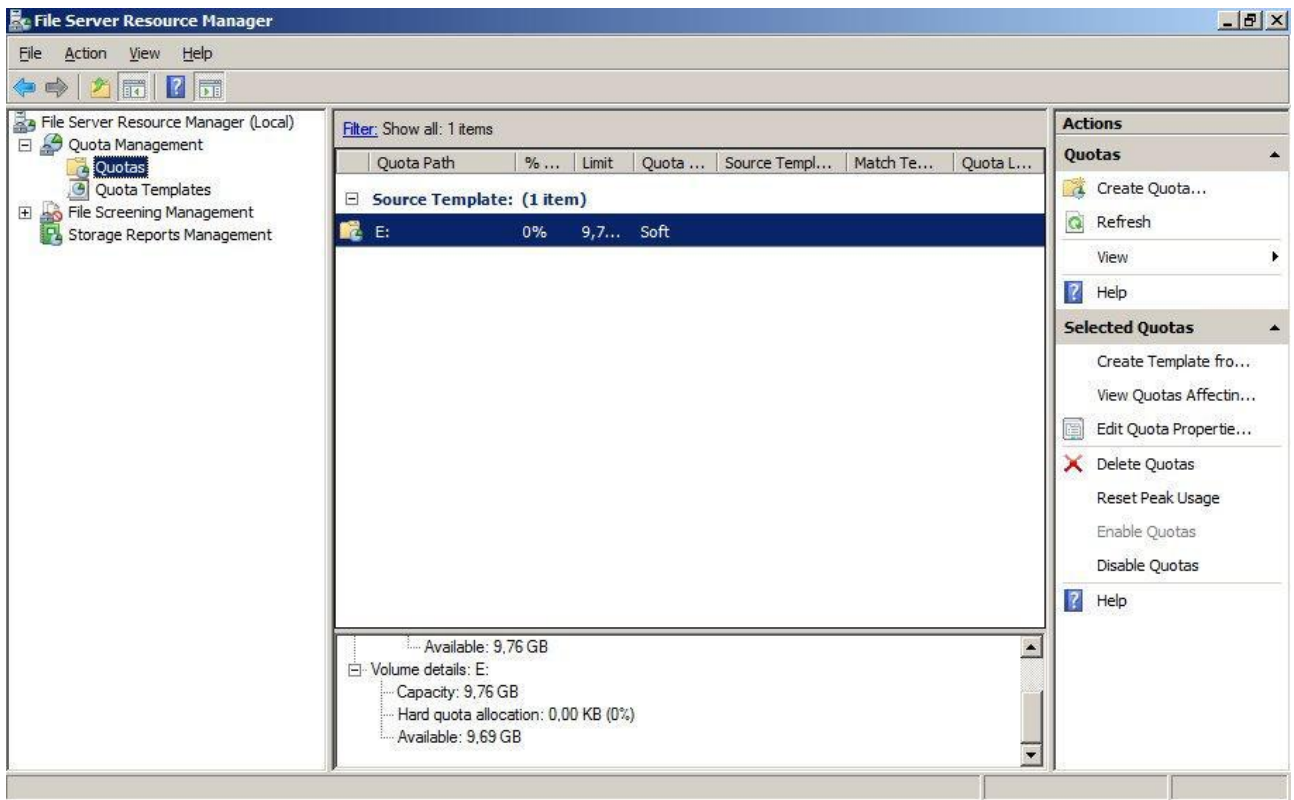
При добавлении службы появится запрос, состояние каких дисков будет отслеживать данная служба. Нам будет интересовать диск, выделяемый для хранения файлов пользователей сети. Также выводится список формируемых отчетов, который можно откорректировать, нажав кнопку Options. Следующее окно мастера установки File Server Resource Manager позволяет указать путь к папке, где будут храниться генерируемые отчеты. При необходимости, можно сконфигурировать автоматическую отправку отчетов администратору по электронной почте.

После установки в разделе Administrative Tools появится оснастка File Server Resource Manager. В оснастке есть три узла – Quota Management (позволяет устанавливать квоты на папки или диски), File Screening Management (позволяет определить, какие файлы нельзя записывать в папки) и Storage Reports Management (для работы с отчетами).

Начнем с создания квоты на папку. Чтобы результаты выполнения предыдущей практической работы не оказывали влияния, проверьте, чтобы в свойствах выбранного для экспериментов диска были отключены квоты на диск.

Создать квоту не используя шаблон. Установить на папку предоставляемую в общий доступ. Квота жесткая на 10 МВ.

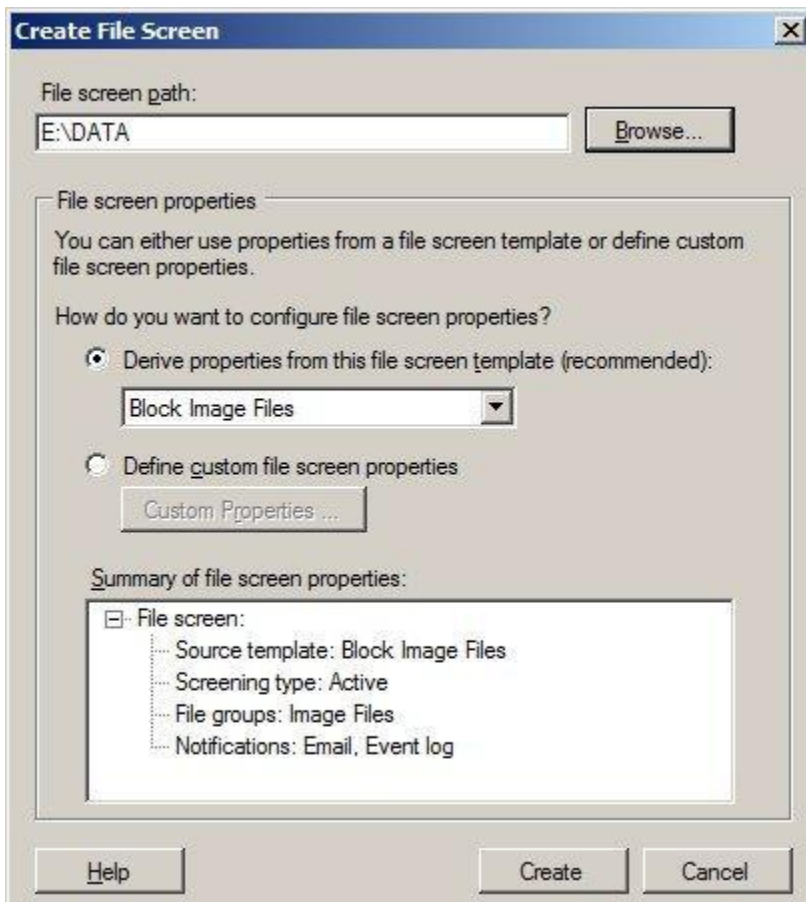
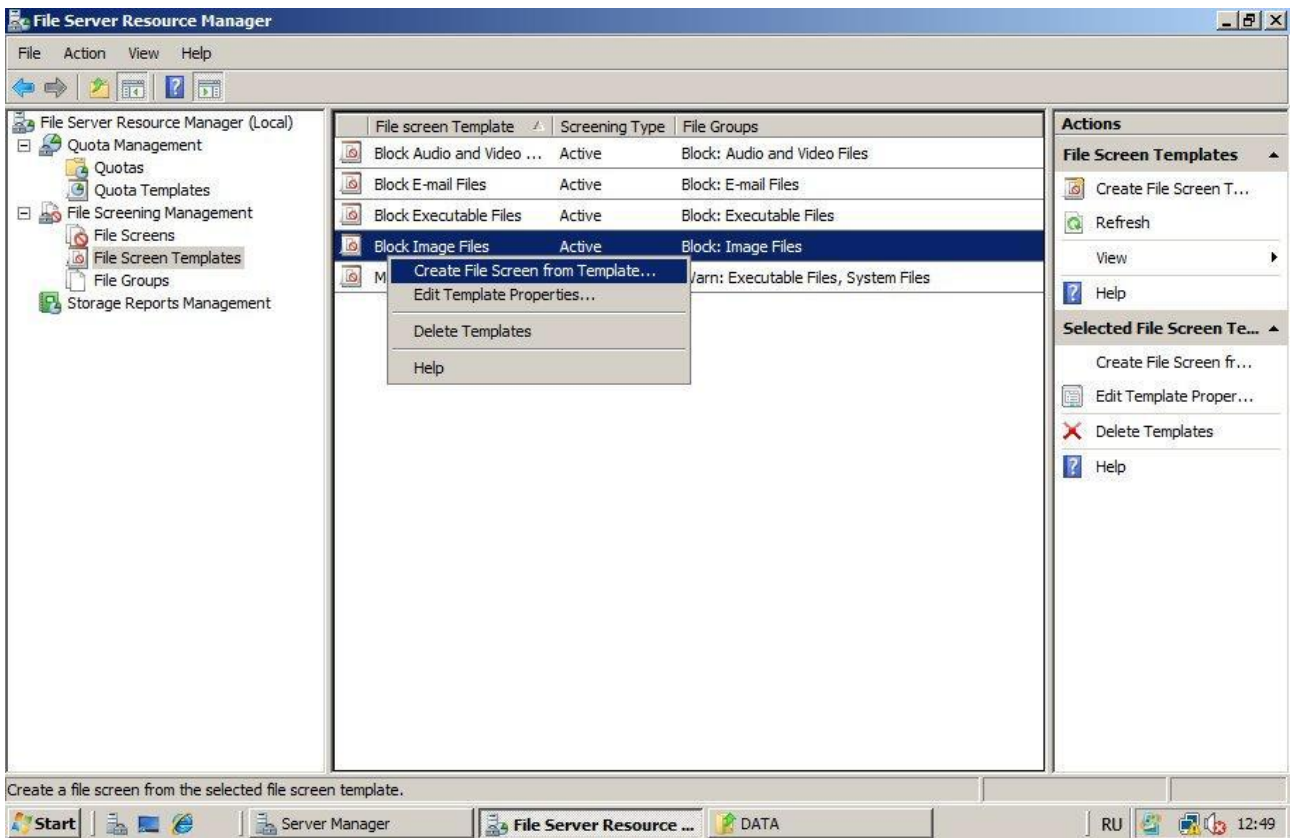
Разница между квотой на диск из предыдущей работы и квотами на общий ресурс: В первом случае, квота устанавливается для каждого пользователя индивидуально, во втором – для папки, не зависимо от того, какие пользователи туда записывают файлы.



Теперь нас будет интересовать узел File Screening Management. Здесь можно создать ограничение по типу записываемых на диск (в папку) файлов. Например, если файловый ресурс предназначен только для хранения документов, можно запретить запись туда мультимедийных и исполняемых файлов.

Посмотрите список предустановленных шаблонов. Воспользуемся шаблоном Block Image Files, чтобы запретить запись в нашу папку файлов изображений. На его основе создадим новое ограничение.

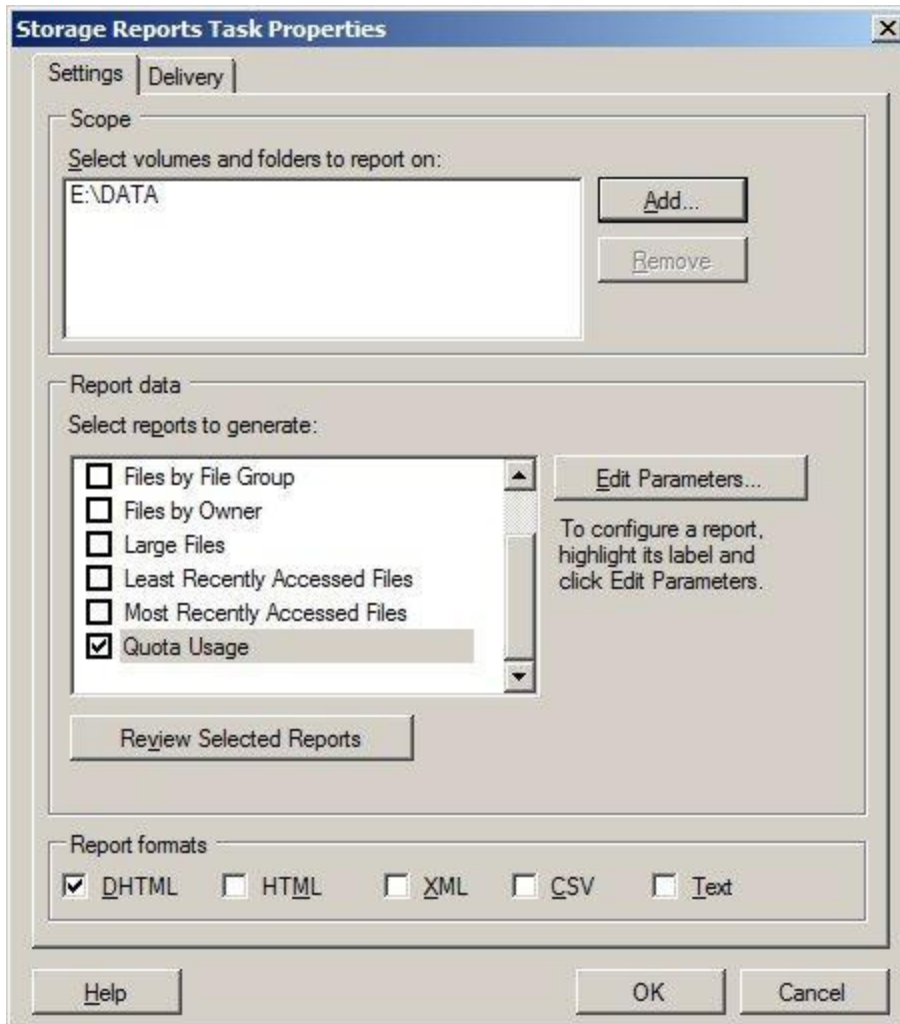
Попробуйте сначала с сервера, потом с рабочей станции записать картинку в папку. Убедитесь, что ограничение работает.



И закончим знакомство с оснасткой File Server Resource Manager созданием отчета.

Запишем в нашу папку какие-нибудь файлы. В оснастке перейдите на узел Storage Reports Management, щелкните на нем правой клавишей и выберите в контекстном меню Generate Reports Now...

В открывшемся окне выберите папку, для которой будет создаваться отчет, и типы отчетов. В следующем окне подтвердите, что нужно сгенерировать отчет и отобразить «прямо сейчас», и после создания отчет будет открыт в браузере.



1. **Управление общими ресурсами и хранилищами**
2. Установить службы NFS (роль файловый сервер)
3. Открыть оснастку Управление общими ресурсами и хранилищами.
4. Создать общий ресурс: расположение "C:\Data"; разрешение NTFS не изменять; протокол общего доступа: NFS; проверка подлинности - оставить значения без изменений; разрешения NTFS - оставить без изменений
5. Оформить типовой отчет.

Контрольные вопросы

1. Назовите две модели совместного использования файлов?
2. Как можно создавать общие папки (назовите 3 способа) ?
3. Как можно управлять разрешениями общего ресурса?
4. Как применяются разрешения общего ресурса и разрешения NTFS?
5. Где можно управлять сеансами и общими ресурсами, открытыми ресурсами?
6. Что нужно дополнительно установить на сервере чтобы настраивать общий доступ по NFS?
7. Как можно подключать сетевые диски (назовите два способа) ?

Лабораторная работа №9.

Тема: Управление службой DNS

Порядок выполнения

1. Открыть программу VirtualBox. Запустить виртуальную машину с установленной операционной системой Windows Server 2008 R2.
2. Настроить сеть. - VirtualBox – сетевой мост; неразборчивый режим – разрешить все. - Windows Server 2008 R2 – назначить статический IP адрес из диапазона адресов сети колледжа. Проверить доступность шлюза и DNS-сервера колледжа.
3. Открыть Диспетчер Сервера.
4. Добавить роль DNS сервер, установить роль с помощью Мастера добавления ролей.
5. Открыть оснастку Службы. Найти службу DNS-сервер. Выписать в отчет следующие поля: описание; состояние; тип запуска; вход от имени. Открыть Свойства вкладку Восстановление и выписать действие компьютера, выполняемое при сбое службы.
6. Открыть Брандмауэр. Найти правила для входящих подключений касающиеся работы службы DNS-сервер. Найти правила для исходящих подключений касающиеся работы службы DNS-сервер. Выписать все правила. Для каждого правила открыть диалоговое окно Свойства и выписать имя правила, описание правила, тип протокола, номер протокола, локальный порт, удаленный порт.
7. Открыть консоль управления DNS-сервером. Открыть диалоговое окно Свойства DNS-сервера. Перейти на вкладку Сервер Пересылки. Добавить сюда известный вам DNS-сервер (сервер учебного заведения).
8. Создать новую зону прямого просмотра. Тип зоны: основная зона, имя зоны: ваша-фамилия.local, создать новый файл, запретить динамические обновления.
9. Запустить утилиту nslookup. Разрешить имя имя-вашего-компьютера.имя-вашего-домена.local (имя должно выглядеть следующим образом: 524-ваша- фамилия.ваша-фамилия.local). Сделать так, чтобы DNS-сервер, разрешал имя вашего сервера в IP-адрес.
10. Добавить в зону прямого просмотра записи (A) про: file-server, app-server, print-server. IP адреса выбрать самостоятельно, так чтобы сервера находились в одной подсети с DNS-сервером.
11. Запустить nslookup. Проверить, что DNS-сервер умеет разрешать доменные имена: file-server.ваша-фамилия.local, app-server.ваша-фамилия.local, print-server.ваша-фамилия.local.
12. Разрешить IP-адреса, соответствующие DNS-серверу, file-server, app-server, print-server в доменные имена. В отчете написать вывод о полученных результатах.

13. Создать зону обратного просмотра. Тип зоны: основная зона; зона обратного просмотра IPv4.
14. Добавить в обратную зону, записи про: DNS-сервер, file-server, app-server, print-server.
15. Запустить nslookup. Проверить, что DNS-сервер разрешает IP-адреса: DNS-сервера, file-server, app-server, print-server.
16. Создать псевдонимы (CNAME), apps для app-server, files для file-server, print для print-server.
17. Запустить nslookup. Разрешить имена apps.ваша-фамилия.local, files.ваша-фамилия.local, print.ваша-фамилия.local.
18. В существующей зоне прямого просмотра создать новый домен hr.ваша-фамилия.local. Внутри этого домена, создать запись типа (A) для компьютера pc1, IP-адрес выбрать самостоятельно.
19. Запустить nslookup. Убедиться, что DNS-сервер разрешает имя pc1.hr.ваша-фамилия.local.
20. Приостановить DNS-сервер. Открыть nslookup, разрешить имена: apps.ваша-фамилия.local, files.ваша-фамилия.local, print.ваша-фамилия.local. В отчете сделать вывод, о результатах работы утилиты nslookup.
21. Запустить DNS-сервер.

Вопросы

1. Что такое сетевые службы?
2. Как расшифровывается DNS?
3. Какие функции выполняет DNS-клиент?
4. Какие функции выполняет DNS-сервер?
5. Для чего используется утилита nslookup?
6. Можно ли организовать работу службы DNS автономно (без связи с сетью Интернет)?
7. Для чего нужна зона прямого просмотра?

Лабораторная работа №10.

Тема: Управление службой DHCP

Порядок выполнения

1. Открыть Диспетчер сервера.
2. Добавить роль DHCP-сервер. Настройки при установке задать следующие: Выбор привязки сетевого подключения выбрать настроенный статически IP-адрес; Указать параметры IPv4 DNS-сервера – указать родительский домен (ваша-фамилия.local), проверить адрес основного сервера; Задать параметры IPv4 WINS-сервера – WINS не требуется для приложений в этой сети; создать новую область с именем ваша-фамилияScore; для новой области задать начальный и конечный IP-адрес, задать основной шлюз; Настроить режим DHCPv6 без отслеживания состояния – Отключить режим без отслеживания состояния DHCPv6 для этого сервера.
3. Открыть оснастку Службы. Найти службу DHCP-сервер. Выписать в отчет следующие поля: описание; состояние; тип запуска; вход от имени. Открыть Свойства вкладки Восстановление и выписать действие компьютера, выполняемое при сбое службы.
4. Открыть Брандмауэр. Найти правила для входящих подключений касающиеся работы службы DHCP-сервер. Найти правила для исходящих подключений касающиеся работы службы DHCP -сервер. Выписать все правила. Для каждого правила открыть диалоговое окно Свойства и выписать имя правила, описание правила, тип протокола, номер протокола, локальный порт, удаленный порт
5. Открыть консоль управления DHCP-сервером. Изучить содержимое консоли.

Вопросы

1. Что такое сетевые службы?
2. Для чего нужна обратная зона DNS?
3. Как работает рекурсивная схема разрешения имен?
4. Как работает не рекурсивная схема разрешения имен?
5. Как расшифровывается DHCP?
6. Режимы работы DHCP сервера?
7. Что такое DHCP-агент, зачем он применяется?
8. Алгоритм работы DHCP?
9. Что такое области адресов (scope)?
10. Что такое «исключения» в DHCP?

Лабораторная работа № 11

Тема: Изучение журналов и оповещений Windows, настройка службы аудита в Windows

Цель выполнения работы: ознакомление с журналами и оповещениями в операционной системе Windows,. Изучение видов и назначений журналов. Изучение типов событий. Изучение служб аудита. Изучение средств для просмотра событий.

Порядок выполнения

Часть 1. Журналы и оповещения в Windows

Раздел про журналы и события

1. Открыть оснастку **Службы**. Найти службу Журнал событий Windows (Windows Event Log). Выписать в отчет следующие поля: описание, состояние, тип запуска, вход от имени.
2. Найти службу Журналы и оповещения производительности. Выписать в отчет следующие поля: описание, состояние, тип запуска, вход от имени.
3. Открыть оснастку Просмотр событий. Изучить, что отображается в окне Сводка административных событий. Изучить, что отображается в окне Сводка журнала.
4. Просмотреть все ошибки и предупреждения – для этого развернуть узел **Настраиваемые представления** и выделить **События управления**. В отчет для первых пяти событий, записать: уровень, источник, код события.
5. Создать настраиваемое представление. Отобразить все ошибки и предупреждения за последние 30 дней, для всех журналов, всех источников, всех кодов событий, всех пользователей и всех компьютеров.
6. Сохранить все события в настраиваемом представлении в новый журнал.
7. Удалите настраиваемое представление.
8. Открыть сохраненный журнал.
9. Настроить максимальный размер журнала **Установка** – 2048 КБ. Настроить **поведение при достижении максимального размера** – Архивировать журнал при заполнении; не перезаписывать события.
10. Очистить журнал **Установка**, не сохраняя содержимое.
11. Заархивировать содержимое журнала **Система**. Выбрать формат .evtx.

Раздел про оповещения

12. Открыть оснастку **Системный монитор**.
13. Прочитать содержимое окна Знакомство с монитором производительности

14. Изучить содержимое окна Сводные сведения о системе
15. Открыть Системный монитор. Добавить счетчики для памяти и для процессора. Сохранить как группу сборщиков данных.
16. Создать оповещение счетчиков производительности для счетчика: Процессор/ % загруженности процессора. Оповещение при: выше, порог: 90. Развернуть получившийся узел новой группы сборщиков данных. Открыть свойства оповещения. Настроить **интервал выборки**: 30 сек. Настроить **действие оповещения**: Сделать запись в журнале событий приложений и **запустить группу сборщиков данных**: выбрать группу созданную ранее для памяти и процессора.

Часть 2. Аудит в Windows

1. Настроить политику аудита: Конфигурация компьютера – Конфигурация Windows - Параметры безопасности - Локальные политики - Политика аудита.
2. Включить Аудит входа в систему, Аудит доступа к объектам.
3. Создать папку C:/Files. Настроить аудит для папки. Создавать и удалять файлы и папки в C:/Files
4. Найти в оснастке Просмотр событий – события входа/выхода пользователя в систему; события создания/удаления файлов и папок (например: Выполнение попытки получения доступа к объекту, где операция доступа: DELETE). Зафиксировать события в отчете.

Контрольные вопросы

1. Какие уровни событий бывают?
2. В какой журнал пишутся события аудита?
3. В какой консоли можно смотреть журналы событий?