Узбекское агенство связи и информатизации

Ташкентский университет информационных технологий

Факультет информационных технологий

Кафедра «Электронная коммерция»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторных работ по курсу

«Администрирование информационных систем и компьютерных сетей»

для направления образования бакалавиатуры

5523600 - «Электронная коммерция»

Ташкент - 2007

Составители:

Р.Х.Хамдамов - Ташкентский университет информационных технологий

Д.Н.Рахматов - Ташкентский университет информационных технологий

Методические указания по выполнению лабораторных работ по курсу «Администрирование информационных систем и компьютерных сетей» для направления образования бакалавиатуры 5523600 - «Электронная коммерция»

Методические указания по выполнению лабораторных работ по курсу «Администрирование информационных систем и компьютерных сетей» обсуждены и одобрены на заседании кафедры «Электронная коммерция» (№ 20 протокола от 20 декабря 2007 г.)

Заведующей кафедрой Р.Х.Хамдамов

Методические указания обсуждены и рекомендованы к опубликованию на заседании научно-методического совета факультета Информационных технологий Ташкентского университета информационных технологий.

(№ _____протокола от «____» _____ 2007г.)

Введение

Лабораторные работы должны быть выполнены студентами 4 курса, бакалавиатуры, которые изучают курс «Администрирование информационных систем и компьютерных сетей» и обучаются по направлению образования бакалавиатуры 5523600 - «Электронная коммерция».

Первая лабораторная работа касается освоить технологию ручной установки операционной системы Windows 2003 Server.

Вторая лабораторная работа посвящена построение локальных сетей используя сетевых программ.

В рамках третей лабораторной работы требуется проведение установки и настройки DHCP сервиса.

Четвертая лабораторная работа посвящена настройка и установка серверов для использования локальных сетей.

Пятая лабораторная работа посвящена установки почтового сервера и запустить на эксплуатацию.

Шестая лабораторная работа посвящена Remote Access и услугам Routing.

Седьмая лабораторная работа посвящена изучению дистанционного управления и настройкам ДУ.

В рамках восьмой лабораторной работы требуется проведение установки и настройки ЛВС и их программ.

Девятая лабораторная работа посвящена установки и настройки пользователей сетей.

В результате выполнения лабораторных работ студенты должны представить отчет, в котором должны быть описаны обзорный материал по исследуемой теме, необходимые нормативно-правовые документы электронной коммерции, проекты новых документов, презентация выполненной работы.

Лабораторная работа № 1

«Основные сведения об инфраструктуре сети и создание сетей на основе стандартных компонентов Windows Server 2003»
(2 часа)

Цель: Изучить инфраструктуру сети и создание сетей на основе стандартных компонентов Windows Server 2003.

Постановка задачи:
Создать сеть на основе стандартных компонентов Windows Server 2003.

Инфраструктура сети – совокупность определенных компонентов, обеспечивающих связь, управление, безопасность и другие свойства сети. Синонимом физической инфраструктуры является термин «топология» - фактическое расположение сетевых узлов и соединительных элементов сети (кабелей, маршрутизаторов, компьютеров, серверов и пр.). Также к ней относятся транспортные технологии: 802.11x, Ethernet и другие. Логическая инфраструктура – множество программных элементов, используемых для связи управления и безопасности сети. Например, система доменных имен (DNS), сетевые протоколы (UDP), сетевые службы и прочие.

В серверных продуктах Microsoft сетевыми подключениями называют логические интерфейсы между программными и аппаратными средствами (связующий элемент между «железом» и программным кодом). Все сетевые подключения, настроенные на компьютере отображаются в окне **Сетевые подключения**. Сетевые подключения поддерживают различные протоколы, службы и клиентов. Сетевые протоколы – это языки взаимодействия компьютеров в сети (стандартизированные методы передачи информации от одного узла к другому). В сетях Windows для соединения компьютеров используются только те протоколы, которые установлены на локальном компьютере. По умолчанию устанавливается только протокол TCP/IP, все остальные протоколы нужно устанавливать вручную. Сетевые службы – это подпрограммы, предоставляющие определенные функции узлам или протоколам в сети. Сетевые клиенты – это подпрограммы, позволяющие компьютеру подключаться к уже организованным сетям. Список доступных для установки сетевых служб, протоколов и клиентов можно увидеть в свойствах сетевого подключения.

Адресация – это система назначения и использования компьютерами сетевых адресов, позволяющая объединять их друг с другом. Тип адресации зависит от используемого протокола и внутренних правил организации. Адреса можно настраивать вручную, распределять в сети с помощью DHCP – сервера или операционная система назначит их автоматически.

Контрольные вопросы:

1. Локальная сеть.
2. Глобальная сеть.
3. Основные стандартные компоненты Windows Server 2003.
4. Настройка TCP/IP.
5. Сетевые операционные системы.

Контрольная задача:

Вы работаете системным администратором домена Contoso.com. Сеть Contoso содержит 7 серверов приложений. Каждый сервер приложений поддерживает приложение

базы данных, которое называется Contosoapp. Требования для использования этого приложения таковы, что добавлять нового пользователя нужно на сервер, который имеет наибольшее свободное дисковое пространство. Вы должны убедиться в исполнении указанных требований при добавлении нового пользователя. **Что Вам делать?**

Рекомендация: при выполнении лабораторной работы использовать данные по создание сетей на основе стандартных компонентов Windows Server 2003.

Используемая литература:

1. **«Управление и поддержка Microsoft Windows Server 2003»**. Дэн Холме, Орин Томас, М., Русская Редакция, 2004 г.
2. **«Внедрение, управление и поддержка сетевой инфрастуктуры Microsoft Windows Server 2003».** Дж. С. Макин, Йен Маклин, М., Русская Редакция, 2004 г.

Рекомендуемые Интернет ресурсы:

1. www.opennet.ru
2. www.microsoft.com
3. www.intuit.ru

Лабораторная работа № 2

«Обзор семейства систем Windows Server 2003»

(2 часа)

Цель: Ознакомление с Windows Server 2003 .

Постановка задачи:

Настройка и установка операционной системы Windows Server 2003.

Система Windows Server 2003 выпускается в 32-х и 64-х разрядном вариантах в 4-х различных редакциях:

- Windows Server 2003 Web Edition (используется для развертывания Web-узлов, поддерживает неограниченное число анонимных соединений, также поддерживает 10 входящих соединений SMB, не может выполнять других серверных ролей);
- Windows Server 2003 Standard Edition (идеален на небольших предприятиях, может быть сервером баз данных, почтовым сервером, на его базе можно создавать кластеры, поддерживает любые серверные роли);
- Windows Server 2003 Enterprise Edition (платформа для крупных предприятий, поддерживает до 8 процессов 32-х Гбайт оперативной памяти, кластеры из 8 узлов, поддерживает все серверные роли и обладает полным административным инструментарием);
- Windows Server 2003 Datacenter Edition (прилагается к ультра производительным серверам, 64 процессора и 512 Гбайт оперативной памяти, обладает практически не ограниченной масштабируемостью). В данном курсе рассматривается ОС Windows Server 2003 Enterprise Edition.

Данная операционная система может быть установлена с CD и не поддерживает установку с дискет. В целом, установка этой ОС не отличается от установок других продуктов Microsoft, за исключением того, что после завершения установки, можно

настроить роли сервера с помощью специального мастера Управление данным сервером. С помощью этой утилиты можно настроить следующие роли:

1. файловый сервер (обеспечивает доступ к общим ресурсам и управляет дисковыми квотами);
2. сервер печати (обеспечивает централизованное управление печатающими устройствами и их драйверами);
3. почтовый сервер (устанавливает протоколы входящих и исходящих сообщений);
4. сервер терминалов (позволяет удаленным клиентам обращаться к дисковому пространству внутренней сети особым образом, имитируя ситуацию нахождения ресурсов внутренней сети на дисках удаленного клиента);
5. DNS-сервер (использоваться для разрешения имен в доменах AD);
6. DHCP-сервер (используется для динамического назначения IP-адресов клиентских компьютерам);
7. WINS-сервер (поддерживает базу данных имен компьютеров, разрешаемых по протоколу NetBIOS);
8. контроллер домена AD (предоставляет службу каталогов клиентам сети, создает новый контроллер домена);
9. сервер удаленного доступа или VPN (обеспечивает подключение удаленных клиентов к внутренней сети с помощью маршрутизации);
10. сервер приложений IIS (предоставляет службы для развертывания Web-сервера);
11. сервер потоков мультимедиа (позволяет серверу передавать потоки мультимедиа по запросу или в реальном времени).

Windows Server 2003 поддерживает два варианта службы каталогов: рабочую группу и домен. Домен наиболее предпочтителен, т.к. имеет общий для всех членов каталог ресурсов – Active Directory (AD). Компьютеры же в рабочей группе имеют собственные базы также. AD – не просто база данных, это совокупность средств безопасности, протоколов, общих ресурсов, сценариев, групповых политик, учетных данных пользователей и пр. Каждый контроллер домена хранит копию (реплику) AD. Изменение AD на одном из контроллеров домена влечет их дальнейшее реплицирование на все остальные контроллеры. AD не существует без домена, а домен не существует без AD.

Контрольные вопросы:

1. Как работает AD?
2. Файловая система?
3. Основные стандартные компоненты Windows Server 2003.
4. Сервер потоков мультимедиа?
5. Сервер приложений IIS.

Контрольная задача:

Вы - администратор домена Contoso.com. Все серверы работают под управлением WS2003, часть клиентов – Windows 2000 Professional, а остальные – под Windows XP. Все учетные записи пользователей в отделе продаж находятся в организационном подразделении (OU) Sales. Для хранения перемещаемых профилей пользователей Вы создали общую папку Profiles на рядовом сервере TK1. Вы настроили разрешение **Разрешить - Полный доступ** для группы Все на папку Profiles. Вы должны создать перемещаемые профили для учетных записей пользователей из Sales OU. **Что Вы должны сделать?**

Рекомендация: при выполнении лабораторной работы использовать данные по семействам Windows Server 2003 систем.

Используемая литература:

1. **«Управление и поддержка Microsoft Windows Server 2003»**. Дэн Холме, Орин Томас, М., Русская Редакция, 2004 г.
2. **«Внедрение, управление и поддержка сетевой инфрастуктуры Microsoft Windows Server 2003».** Дж. С. Макин, Йен Маклин, М., Русская Редакция, 2004 г.

Рекомендуемые Интернет ресурсы:

1. www.opennet.ru
2. www.microsoft.com
3. www.intuit.ru

Лабораторная работа № 3

«Конфигурирование DHCP-серверов и клиентов»

(2 часа)

Цель: Изучение конфигурирование DHCP-серверов и клиентов.

Постановка задачи:
Установка и настройка DHCP-серверов и клиентов.

DHSP-сервер является необходимым атрибутом сколько-нибудь больших сетей, т.к. использование данного протокола упрощает администрирование сети и позволяет избежать ошибок адресации. Добавление роли DHSP производится точно также как и DNS-сервера. Серверу, на который устанавливается DHCP, необходимо присвоить статический IP-адрес. В случае если в домене используется AD, DHCP-сервер до начала работы должен быть авторизован. Авторизация осуществляется из консоли DHCP-сервера. Неавторизованные DHCP-серверы называются ложными. В случае если в домене появляется авторизованный DHCP, ложный сервер автоматически отключается. Как и на DNS-сервере необходима настройка зон, так и на DHCP-сервере необходима настройка областей – совокупностей IP-адресов определенного диапазона, которые DHC-сервер будет присваивать клиентам. Кроме IP-адресов в областях можно определить любые другие настройки TCP/IP для клиентов. DHCP-серверу необходимо назначить статический IP-адрес из того же диапазона, из которого он предоставляет адреса клиентов. Процесс передачи IP-адреса клиенту называется арендой. Продолжительность аренды по умолчанию 8 дней, после этого клиент обязан обновить аренду. Также аренда обновляется при перезапуске клиента, при перезапуске DHCP-сервера, а также при выполнении команды ipiconfig /renew. Области на DHCP-сервере создаются с помощью Мастера, позволяющего настроить следующие параметры:

1. имя области;
2. диапазон адресов – набор последовательных адресов, составляющих подсеть, в которую устанавливается DHCP. Однако из этого диапазона необходимо исключить уже используемые в нем статические IP-адреса (например, для самого DHCP, контроллера домена, DNS-сервера и пр.). в свойствах области указываются начальный и конечный адреса желаемого диапазона. В случае если сеть уже сконфигурирована полностью, для выделения компьютеров со статическими IP-адресами задают Диапазон исключений. Если же сеть еще не сформирована, то начальный адрес диапазона увеличивают на двадцать, тем самым резервируя двадцать первых IP-адресов для важных серверов;

3. диапазоны исключения – множество IP-адресов из диапазона области, которые никогда не должны предоставляться в аренду. Адреса области, предоставляемые в аренду, составляют так называемый пул адресов;
4. срок действия аренды адреса;
5. IP-адрес основного шлюза;
6. имя домена и список DNS-серверов;
7. список WINS-серверов.

Контрольные вопросы:

1. Как работает DHCP?
2. Адресация.
3. Основные стандартные компоненты Windows Server 2003.
4. WINS-серверы?
5. Динамические и статические IP адреса.

Контрольная задача:

Вы администратор домена Contoso.com. Все сервера управляются WS2003, а клиенты – Windows XP. Пользователи, которые неправильно ввели пароль больше, чем 2 раза в день, должны быть заблокированы. **Вы должны настроить политику доменных учетных записей на выполнение этого правила.**

Рекомендация: при выполнении лабораторной работы использовать данные по DHCP-серверы.

Используемая литература:

1. **«Управление и поддержка Microsoft Windows Server 2003»**. Дэн Холме, Орин Томас, М., Русская Редакция, 2004 г.
2. **«Внедрение, управление и поддержка сетевой инфрастуктуры Microsoft Windows Server 2003».** Дж. С. Макин, Йен Маклин, М., Русская Редакция, 2004 г.

Рекомендуемые Интернет ресурсы:

1. www.opennet.ru
2. www.microsoft.com
3. www.intuit.ru

Лабораторная работа № 4

«Конфигурирование серверов и сети»
(2 часа)

Цель: Установка и настройка серверов для локальной сети.

Постановка задачи: Установить и настроить DHCP – серверов для локальной сети.

Часто в крупных сетях диапазоны IP-адресов, предназначенные для аренды, в разных логических подсетях объединяют в единый объект администрирования – суперобласть. Суперобсласти используются в двух случаях:

1. если число клиентских компьютеров в подсети превышает емкость изначального адресного пространства;
2. если в одном физическом сегменте сети сконфигурированы два или более DHCP-серверов, предоставляющих клиентам IP-адреса из разных диапазонов. В этом случае создание суперобласти на всех серверах имитирует ситуацию балансировки нагрузки с использованием нескольких DHCP-серверов.

При необходимости изменения адресации в подсетях недостаточно просто изменить диапазон в используемой области, необходимо сначала создать новую область, обновить клиенты, выполнив на них последовательно команды ipiconfig/release и ipiconfig/renew. После этого старую область можно деактивировать и удалить.

Для восстановления DHCP-сервера после сбоя или для его переноса на другой сервер необходимо архивировать базу данных DHCP. DHCP-сервер может архивироваться автоматически и вручную. Автоматические копии используются для восстановления поврежденных баз данных DHCP, а для восстановления вручную пригодны копии только заархивированные вручную. Существуют данные, которые не сохраняются ни при каком способе архивирования. Например, реквизиты динамического обновления в DNS. При переносе DHCP-сервера с одного сервера на другой нужно заархивировать базу данных DHCP, а затем восстановить на новом месте. Эту операцию можно выполнить из консоли DHCP. Для исправления ошибок в базе данных DHCP и ее одновременного сжатия для экономии пространства используется утилита Jetpack. Нужно пользоваться ею если размер базы DHCP превышает 30 Мбайт и при появлении сообщений об ошибках базы данных DHCP.

Часто в сетях возникает потребность предоставлять клиентским компьютерам конфигурацию в зависимости от выполняемых ими функций. Для этого в DHCP реализованы так называемые классы параметров:

- классы поставщиков – для назначения параметров клиентам, для которых определен конкретный тип поставщика;
- классы пользователей – для назначения параметров клиентам, которым необходимы одинаковые параметры настройки DHCP.

Для создания класса компьютеров необходимо сначала определить его на DHCP-сервере, назначив ему идентификатор и набор параметров. Затем на нужных клиентских компьютерах выполнить команду ipiconfig /setclassad.

DHCP-сервер автоматически обновляет записи ресурсов PTR на DNS-серверах для DHCP-клиентов. Однако можно настроить DHCP-сервер и на обновление записей ресурсов A. Эта функция настраивается на вкладке DNS свойств DHCP-сервера. DHCP-сервер может обновлять записи ресурсов в DNS по запросу DHCP-клиента или без такового при каждом событии, связанном с адресом. Также можно настроить DHCP-сервер на удаление записей ресурсов A и PDR при истечении срока аренды. В случае если система DNS интегрирована в AD, DHCP-сервера рекомендуется добавлять в группу безопасности DNSUpdateProxy для предотвращения проблем с владельцем записи ресурса. Такое решение ухудшает безопасность сети, т.к. любые имена DNS, зарегистрированные DHCP-сервером являются небезопасными. Если DHCP-сервер член группы DNSUpdateProxy устанавливается на контроллере домена, то в этом случае все записи ресурсов A, SRV и CNAME, зарегистрированные в DNS этим DHCP-сервером, являются небезопасными. Поэтому совмещать роли контроллера домена и DHCP-сервера крайне не рекомендуется.

Контрольные вопросы:

1. Локальная сеть.
2. Глобальная сеть.
3. Основные стандартные компоненты Windows Server 2003.
4. Настройка TCP/IP.

5. Сетевые операционные системы.

Контрольная задача:

Вы - сетевой администратор домена Contoso.com. Вы администрируете файловый сервер под управлением WS2003. Тома на сервере сконфигурированы по технологии RAID-5. Один диск из этого тома сломался. Вы заменили испорченный диск. Вы запустили оснастку **Управление дисками** и получили следующий результат:

Disk	Status	Type
Disk1	Online	Dynamic
Disk2	Online	Dynamic
Disk3	Not initiated	Unknown
Missing	Offline	Dynamic

Вы должны восстановить отказоустойчивость. **Какие действия Вы предпримите?**

Рекомендация.

при выполнении лабораторной работы использовать данные по установке и настройке локальных сетей с помощью DHCP-серверов.

Используемая литература:

1. **«Управление и поддержка Microsoft Windows Server 2003»**. Дэн Холме, Орин Томас, М., Русская Редакция, 2004 г.
2. **«Внедрение, управление и поддержка сетевой инфрастуктуры Microsoft Windows Server 2003».** Дж. С. Макин, Йен Маклин, М., Русская Редакция, 2004 г.

Рекомендуемые Интернет ресурсы:

1. www.opennet.ru
2. www.microsoft.com
3. www.intuit.ru

Лабораторная работа № 5

«Обслуживание операционной системы»
(2 часа)

Цель: Проведение анализа и обслуживание операционной системы.

Постановка задачи: Проведение анализа и обслуживание операционной системы Windows 2003.

С точки зрения безопасности очень важно вовремя устанавливать обновления и исправления для операционной системы. Последние 10 лет корпорация Windows поддерживает глобальный источник обновлений систему серверов Windows Update, позволяющую через Интернет устанавливать критические обновления на компьютере пользователя. Последние усовершенствования этого – Службы обновления ПО (SUS), содержащие следующие компоненты:

- службы, запущенные на сервер IIS (синхронизирует внутренний сервер с Интернет серверами Windows Update);
- Web-узел управления SUS (интерфейс управления автоматическими обновлениями);
- служба Автоматическое обновление (загрузка и распространение обновлений в сети);

- параметры групповой политики.

Службы SUS не устанавливаются автоматически и не входят в комплект поставки Windows Server 2003, но их можно бесплатно загрузить по адресу http://go.microsoft.com/fwlink/?LinkID=6930. Для функционирования SUS необходимы службы IIS. После установки SUS может управлять только локальный администратор. Для вызова интерфейса управления SUS-сервером в поле Адрес браузера необходимо ввести http://<имя_сервера_SUS>/SUSAdmin . На Web-узле SUS можно настраивать параметры, синхронизировать и утверждать содержимое. Для корректной работы SUS-сервера необходимо указать его полноеDNS-имя, параметры proxy-сервера (если он используется в сети), место хранения файлов обновлений и источник синхронизации (SUS-сервер может синхронизироваться либо с Интернет серверами Windows Update непосредственно, либо с другими SUS-серверами во внутренней сети. Синхронизацию можно осуществлять вручную или по расписанию (если компьютер выключен в момент, когда должна произойти установка обновлений, она будет перенесена на следующий период. Если в такие периоды компьютер выключен постоянно, установка никогда не выполнится).

Для распространения обновлений на клиентские компьютеры одной успешной синхронизации не достаточно. По сети распространяются только те обновления, которые были явно одобрены администратором на Web-странице управления SUS. Начиная с Windows 2000 SP3, Клиент службы Автоматическое обновление входит в состав системы. Для более ранних версий Windows Клиент можно скачать с того же адреса, что и SUS-сервер.

В случае если на клиентском компьютере включено автоматическое обновление, можно настроить компьютер на синхронизацию компьютера с внутренним SUS-сервером компании. Автоматическое обновление поддерживает два режима загрузки: Автоматический и С уведомлением. В первом случае обновления загружаются независимо от пользователя, а во втором случае обновления не загружаются до тех пор, пока администратор компьютера не загрузит их лично. После загрузки обновлений их необходимо установить. Режимы установки совпадают по названию и смыслу с режимами загрузки с той лишь разницей, что после установки обновлений возможно потребуется перезагрузка компьютера. Если выбран режим установки с уведомлением, то пользователь сможет отложить перезагрузку. В автоматическом режиме перезагрузку компьютера сможет отложить только администратор, а обычному пользователю дается 5 минут до перезагрузки, чтобы успеть сохранить сделанную работу.

Также настраивать службу Автоматическое обновление можно с помощью групповой политики. Для этого в редакторе групповой политики необходимо раскрыть узел Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Windows Update. Для базовой настройки можно применять шаблон, находящийся в файле по адресу %WinDir%\Inf\waua.inf .

По умолчанию клиенты службы Автоматическое обновление опрашивают назначенный SUS-сервер на предмет новых обновлений каждые 22 часа минус случайные смещения.

Для наблюдения за работой SUS служит страница Monitor Server на Web-узле управления SUS. Там содержатся журналы синхронизации, журналы информации об утвержденных пакетах обновлений и журналы взаимодействия клиента и сервера SUS. Системное событие SUS регистрируется в журнале Система из консоли Просмотр событий.

Для устранения неполадок SUS иногда необходимо: перезапустить службу синхронизации (если не удается получить доступ к настройкам SUS-сервера), перезапустить кэш памяти (в случае если очень долго нет новых обновлений), перезапуск служб IIS (если не удается подключиться к SUS-серверу). Также нужно убедиться, что на клиентских компьютерах в разделе реестра HKLM\Software\Policies\Microsoft\Windows\WindowsUpdate есть следующие параметры:

WUServer (URL SUS-сервера), WUStatusServer (URL сервера статистики) и UseWUServer со значением dword=00000001.

Архивировать SUS-сервер необходимо в следующем порядке: заархивировать папку с содержимым SUS, Web-узел управления SUS и метабазу IIS. Метабазу необходимо архивировать сначала с помощью средств управления IIS, потом с помощью утилиты Ntbackup необходимо заархивировать Web-узел по умолчанию, Web-узел управления SUS, виртуальный каталог AutoUpdate. Восстанавливать сервер SUS необходимо в обратном порядке.

Пакеты обновлений (Service Pack) можно устанавливать на компьютер прямо с Web-узла Microsoft или с CD. На множество компьютеров сети пакеты обновлений распространяются средствами групповой политики. При этом иногда возникает проблема: пакет обновления не устанавливается на клиентский компьютер при старте системы. Это возникает из-за того, что вход в систему осуществляется раньше, чем загружаются средствами поддержки сети. Чтобы избежать такой ситуации в локальных политиках безопасности компьютера необходимо активировать параметр Всегда ожидать инициализации сети при загрузке и входе в систему.

Для того, чтобы клиенты могли законно подключаться к серверу, необходимо приобрести лицензию клиентского доступа (CAL). Такие лицензии необходимо иметь для каждого подключения (CAL не требуется на доступ к серверу через Интернет без авторизации). Есть два типа CAL: на пользователя (пользователь может подключиться к серверу с любого устройства), на устройства (с одного и того же устройства могут работать несколько пользователей). Количество необходимых лицензий равно количеству устройств или пользователей, которые обращаются к серверам. Для управления лицензиями существует служба Лицензирование в Панели управления..

Контрольные вопросы:

1. Клиентский доступ - CAL.
2. SUS-сервер.
3. Основные стандартные компоненты Windows Server 2003.
4. Службы обновления.
5. Сетевые операционные системы.

Контрольная задача:

Вы - администратор домена Contoso.com. Все серверы работают под управлением WS2003, а все клиенты – под Windows XP Professional. Вы внедряете стратегию архивирования на главном файловом сервере. Вы должны выбрать типы архивации, позволяющие восстановить информацию за наименьшее время, при этом задачи архивации не должны мешать пользователям в рабочее время. **Что Вам сделать?**

а) Настроить полную архивацию каждое воскресенье. Настроить добавочную архивацию ежедневно с понедельника по субботу.

б) Настроить полную архивацию каждое воскресенье. Настроить разностную архивацию ежедневно с понедельника по субботу.

в) Настроить ежедневную архивацию (daily backup).

г) Настроить полную архивацию каждый день.

Рекомендация. при выполнении лабораторной работы использовать данные по обслуживание ОС Windows Server 2003.

Используемая литература:

1. **«Управление и поддержка Microsoft Windows Server 2003»**. Дэн Холме, Орин Томас, М., Русская Редакция, 2004 г.
2. **«Внедрение, управление и поддержка сетевой инфрастуктуры Microsoft Windows Server 2003».** Дж. С. Макин, Йен Маклин, М., Русская Редакция, 2004 г.

Рекомендуемые Интернет ресурсы:

1. www.opennet.ru
2. www.microsoft.com
3. www.intuit.ru

Лабораторная работа № 6

«Сервисы Remote Access и Routing»
(2 часа)

Цель: Ознакомление с сервисными службами Remote Access и Routing.

Постановка задачи:
Установить и настроить службу Remote Access и Routing.

Политики удаленного доступа определяются для конкретного компьютера, а не для службы Маршрутизация и удаленный доступ. Информация политик хранится на жестком диске компьютере и обрабатывается либо RADIUS-сервером, либо службой RRAS, поэтому даже при остановке последней политики продолжают действовать до их прямого удаления. К каждому подключению применяется ровно одна политика – первая, отвечающая заданным условиям. Если ни одной подходящей политики нет, подключение блокируется.

Можно настроить сервер на проверку номера абонента. Если проверяемого номера абонента нет в списке или если его номер определить не удалось, подключения будут разрываться. Сервер NAS может назначать клиенту один и тот де статический IP-адрес, указанный в настройках сервера в зависимости от телефонного номера или Мас-адреса сетевой платы клиента.

Устранять неполадки подключений по телефонным линиям нужно в следующем порядке: в консоли RRAS должен быть активизирован параметр Сервер удаленного доступа; в сети должен быть доступен DHCP-сервер или на сервере NAS должен быть настроен статический пул адресов с необходимым запасом; в узле Порты должно быть достаточно устройств для одновременного подключения нужного количества клиентов; должен быть сконфигурирован хотя бы один протокол аутентификации и один уровень шифрования, поддерживаемый одновременно клиентом, сервером и политикой удаленного доступа; учетной записи пользователя, выполняющего подключение должно хватать разрешений; сервер NAS должен входить в группу безопасности Серверы RAS и IAS.

На этом заканчивается первый этап настройки. Теперь необходимо настроить сервер NAS в качестве маршрутизатора, чтобы удаленные клиенты могли получать доступ к внутренним ресурсам сети. В консоли RRAS можно просматривать текущие подключения клиентов удаленного доступа. Там же можно отключать их и отправлять сообщения одному или всем удаленны клиентам. Помимо текущего управления всеми клиентами удаленного доступа можно управлять с помощью политики удаленного доступа.

В сетях Microsoft есть своя реализация RADIUS-сервера и RADIUS-прокси – Служба проверки подлинности в Интернете (IAS). Серверы удаленного доступа

пересылают запросы удаленного доступа на RADIUS-сервер по особому протоколу, потом последний соединяется с контроллером домена для выполнения аутентификации пользователей. После этого к подключению применяются политики удаленного доступа, настроенные на RADIUS-сервере. Если у подключения есть нужное разрешение, RADIUS-сервер устанавливает соединение с сервером удаленного доступа, в противном случае подключение разрывается. RADIUS-сервер удобен в случаях одновременного использования разнородных подключений удаленного доступа (VPN, беспроводные и телефонные подключения). Целесообразно устанавливать RADIUS-сервер на сервере удаленного доступа (хотя можно выделить для этого и отдельный компьютер). Службу IAS можно использовать и в качестве RADIUS-прокси. Для этого нужно настроить сервера удаленного доступа на пересылку учетных данных пользователей на IAS-сервер, который проведет централизованную аутентификацию.

Чтобы сконфигурировать IAS как RADIUS-сервер, необходимо настроить службу Маршрутизации и удаленный доступ и службу IAS. Службу RRAS необходимо настроить на проверку подлинности по протоколу RADIUS, а также выбрать RADIUS-учет, настроить IP-адрес RADIUS-сервера, секрет (пароль для клиента сервера RADIUS) и прочие параметры.

При настройке IAS-сервера необходимо зарегистрировать его в AD, присоединив предварительно сервер к группе RAS и IAS. В дальнейшем необходимо определить список IP-адресов RADIUS-клиентов, пересылающих запросы аутентификации RADIUS-серверу.

VPN (виртуальная частная сеть) – это логическая сеть, проходящая через Интернет. В ней пакеты от компьютера-отправителя шифруются, затем инкапсулируются в открытые пакеты, передаются в особый тоннель через Интернет удаленному VPN-серверу, который дешифрует полезную информацию и пересылает пакет адресату.

VPN основан на принципах удаленного доступа к сети, поэтому в настройках VPN-сервера нужно включить поддержку локальной сети и маршрутизацию вызовов по требованию.

VPNбывает трех видов:

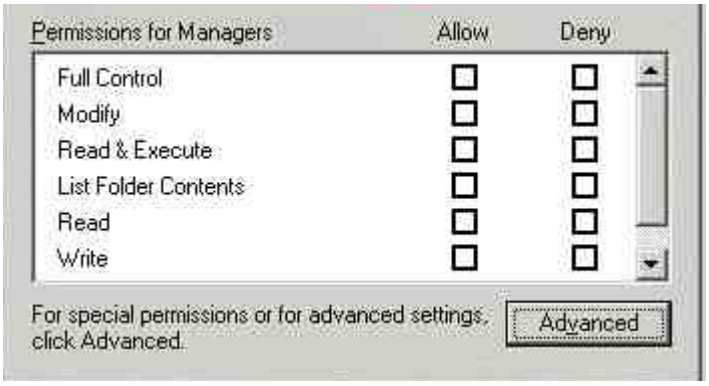
1. удаленный доступ через VPN (удаленный клиент через Интернет подключается к сети своей компании при этом отличие от удаленного доступа в чистом виде в том, что компьютер клиента «находится в одной подсети» с сетью организации);
2. экстрасеть (это подключение друг к другу двух корпоративных сетей через VPN-серверы со службой RRAS. На каждом сервере интерфейсы с вызовом по требованию инициируют и отвечают на запросы создания VPN-подключений. При подключении выполняется аутентификация интерфейсов, а не отдельных пользователей. В экстрасетях статические маршруты часто заменяют на протоколы RIP);
3. смешанный вариант с брандмауэром (при совмещении удаленного доступа и экстрасети можно разделить сеть предприятия на внутреннюю сеть, внешнюю сеть и сеть периметра – демилитаризованную зону, которую можно отделить от других сетей брандмауэрами. Как правило, брандмауэры пропускают трафик из внутренней сети и блокируют из внешней. Значит на них необходимо настроить фильтры пакетов на пропуск данных для - VPN сервера).

Контрольные вопросы:

1. RADIUS-сервер.
2. Подключение по VPN.
3. Сервер NAS.
4. Remote Desktop – принцп работы.
5. Использование протокола SSH.

Контрольная задача:

Вы - администратор домена Contoso.com. Все серверы работают под управлением WS2003, а все клиенты – под Windows XP Professional. Учетные записи всех менеджеров находятся в глобальной группе Managers. Манаджер Роджер создал папку ManagerData на компьютере Contoso1. Другие менеджеры должны только просматривать содержимое папки и читать файлы. Никаких других прав у них быть не должно. Вы добавили группу Managers в ACL папки ManagerData. **Настройте необходимые разрешения.**



Рекомендация: при выполнении лабораторной работы использовать данные по Remote Access и Routing.

Используемая литература:

1. **«Управление и поддержка Microsoft Windows Server 2003»**. Дэн Холме, Орин Томас, М., Русская Редакция, 2004 г.
2. **«Внедрение, управление и поддержка сетевой инфрастуктуры Microsoft Windows Server 2003».** Дж. С. Макин, Йен Маклин, М., Русская Редакция, 2004 г.

Рекомендуемые Интернет ресурсы:

1. www.opennet.ru
2. www.microsoft.com
3. www.intuit.ru

Лабораторная работа № 7

«Настройка и управление удаленным доступом»
(2 часа)

Цель: Настройка и управление удаленным доступом.

Постановка задачи:

Установить и настроить программы для управление удаленным доступом.

Учетной записи пользователя необходимо предоставить одно из трех разрешений для функционирования удаленного доступа:

1. управление на основе политики удаленного доступа (выполняется по умолчанию. Также по умолчанию политики удаленного доступа блокируют все подобные подключения. При выборе такого разрешения необходимо дополнительно настраивать политику удаленного доступа);
2. разрешить доступ (удаленный доступ разрешается несмотря на ограничение политики удаленного доступа. Этот параметр приоритетнее явного отказа);

3. запретить доступ (удаленный доступ для данного пользователя будет невозможен).

Для подключения к удаленной сети используется либо телефонная линия, либо VPN-подключение. Конфигурирование их практически одинаковое. Рассмотрим удаленный доступ по телефонной линии с использованием протокола PPP к компьютеру со службой Маршрутизация и удаленный доступ. Для корректной работы подключения необходимо настроить и клиент и сервер удаленного доступа (NAS). Сначала надо настроить подключение к NAS с помощью Мастера новых подключений, а потом продолжить настройку с помощью Мастера настройки NAS. Удаленным клиентам, подключающимся к NAS по протоколу PPP, IP-адрес присваивается автоматически. NAS получает его либо из DHCP, либо из статического пула адресов, заданного в настройках NAS.

При наличии в сети DHCP NAS получает от него адреса комплектами по 10 штук. Если DHCP-сервер недоступен и статический пул адресов не настроен, удаленный доступ к сети невозможен. После получения клиентом адреса NAS проводит аутентификацию клиента либо средствами Windows, либо средствами RADIUS-сервера. Аутентификация возможна по 6 разным протоколам, среди которых: CHAP (пароль шифруется по алгоритму MD5), MS-CHAP (для клиентов Windows 9x с односторонней аутентификацией). MS-CHAP V2 (для клиентов Windows 2000 XP Server 2003. Используются 2 криптографических ключа для взаимной аутентификации), EAP-TLS (аутентификация на основе сертификатов, применяется в сочетании со смарт-картами, самый защищенный метод), EAP-MD5 CHAP (обеспечивает совместимость клиентов с Mac OS), SPAP (протокол со слабым шифрованием, применяется для взаимодействия с серверами shava), PAP (пароли не шифруются и передаются по сети открытым текстом). Также возможно подключиться к NAS без аутентификации. Если в сети нет клиентов, работающих на платформе Windows 9x, предпочтительно использовать протоколы MS-CHAP V2 или EAP-TLS, при чем последний протокол можно использовать только в тех случаях, когда в сети существуют сервера сертификатов и развернута система открытых ключей. Если в сети клиенты под управлением Win 9x рекомендуется использовать протокол MS-CHAP. Использование протоколов должно быть настроено как на стороне сервера, так и на стороне клиентов. И на клиенте на сервере должны быть настроены одинаковые протоколы. В случае если для аутентификации поддерживается несколько протоколов, компьютеры пытаются соединиться по самому защищенному из них.

Контрольные вопросы:

1. Протокол MS-CHAP.
2. Использование глобальную сеть для удаленного доступа.
3. Dial-up настройка и установка.
4. Настройка TCP/IP.
5. Сетевые операционные системы.

Контрольная задача:

Вы - администратор домена Contoso.com. Все серверы работают под управлением WS2003, а все клиенты – под Windows XP Professional. В компании главный офис и пять филиалов. Сервера есть в каждом филиале. Служба тех. Поддержки находится в главном офисе. Пользователи филиалов не имеет прав локального входа на сервера филиалов. Сервера филиалов собирают информацию аудита. Вы должны просматривать эту информацию на серверах филиалов, находясь в главном офисе + Вы должны сохранять ее на локальных дисках серверов филиалов. **Какие два действия Вам предпринять (Каждый ответ – часть решения. Выберите два)**

а) в оснастке Анализ и настройка безопасности сохранить нужный .inf файл на локальном жестком диске.

б) установить с каждым сервером филиала сеанс Удаленного помощника.

в) в консоли Управление компьютером открыть Просмотр событий, сохранить нужный .evt файл на локальном жестком диске.

г) выполнить с необходимыми параметрами secedit.exe

д) установить сеанс удаленного рабочего стола с каждым сервером филиалов.

Рекомендация: при выполнении лабораторной работы использовать данные по настройки и управлением удаленным доступом.

Используемая литература:

1. **«Управление и поддержка Microsoft Windows Server 2003»**. Дэн Холме, Орин Томас, М., Русская Редакция, 2004 г.
2. **«Внедрение, управление и поддержка сетевой инфрастуктуры Microsoft Windows Server 2003».** Дж. С. Макин, Йен Маклин, М., Русская Редакция, 2004 г.

Рекомендуемые Интернет ресурсы:

1. www.opennet.ru
2. www.microsoft.com
3. www.intuit.ru

Лабораторная работа № 8

«Специальные сетевые программы для безопасности сети»
(2 часа)

Цель: Ознокомление и изучение по обеспечению безопасности сети.

Постановка задачи:
Установить и настроить программы для обеспечения безопасности сети.

Основными протоколами безопасности в сетях Windows Server 2003 являются Kerberos, NTLM и IPSec. Управлять ими можно непосредственно с помощью команд или политик безопасности, а также с помощью шаблонов. В операционной системе для управления шаблонами служит оснастка Шаблоны безопасности, содержащая большое количество предустановленных шаблонов, но при желании можно добавлять свои шаблоны. Шаблоны по умолчанию хранятся в папке Windows\security\templates (дополнительная копия хранится в папке Windows\inf. Имеющиеся шаблоны можно редактировать. Описание имеющихся шаблонов безопасности по именам файлов можно найти в справочной системе Windows. Наличие шаблона не обеспечивает безопасности компьютера. Шаблон необходимо применить, для этого используют оснастку Анализ и настройка безопасности или утилиту командной строки Secedit. Использование графической утилиты предпочтительнее, т.к. с ее помощью можно не только применять шаблоны, но и сравнивать текущие настройки безопасности компьютера с шаблонами (различия будут помечены красным крестиком). Удаление шаблона не влечет отмену установленных им параметров. Для отмены параметров удаленных шаблонов необходимо сначала применить базовый шаблон (выбранный шаблон, возвращающий все параметры в первоначальное состояние), а уже потом применять новые шаблоны. При реализации политики безопасности никогда не стоит пренебрегать Правилом наименьших привилегий, для реализации которого необходимо:

- строгая политика паролей;
- предоставление пользователям только тех прав, которые им действительно нужны (которые попросило выделить руководство);
- максимально использовать параметры безопасности доступа и ограничения выполняемых операций;
- использовать файловую систему NTFS для настройки доступа к объектам;
- использовать Группы с ограниченным членством;
- отключить все ненужные службы и ограничить круг лиц, имеющих доступ к ним;
- разработать строгую политику аудита;
- разработать базовые шаблоны безопасности в зависимости от ролей серверов и применить их.

Также необходимо применять брандмауэры, прокси-серверы и анализаторы трафика. Безусловно, политики безопасности должны придерживаться все пользователи сети, а инициатива ее применения должна исходить от руководства компании.

Политики IPSec представляют собой набор фильтров, описывающих определенные действия сетевого протокола. Множество фильтров образуют списки фильтров, которые в свою очередь являются частями правил. Фильтру можно присвоить 3 действия: Разрешить, Блокировать, Согласовать безопасность. Каждому правилу соответствует одно действия фильтра, но политика может состоять из нескольких правил. Причем правило, охватывающее либо меньшее количество трафика, либо меньше сетевой сегмент, либо меньшее время приоритетнее большего.

Редактировать политику можно с помощью команды Netsh, в групповой политике или в оснастке Управление политикой безопасности IP. Для наблюдения за IPSec используется оснастка Монитор IP-безопасности. Там содержится набор различных счетчиков, различные статистические данные о механизме работы политики.

Для записи сетевого трафика можно использовать либо Сетевой монитор, либо утилиту Netcap из набора Средств поддержки Windows. При этом сетевой монитор устанавливать не обязательно, а драйвер сетевого монитора устанавливается автоматически при ее первом запуске. Единственное ограничение использования этой утилиты в том, что она не предоставляет графической оболочки для последующего просмотра записанных данных. Но для этого подойдет любой текстовый редактор или сам Сетевой монитор.

Контрольные вопросы:

1. Строгая политика паролей.
2. Как использовать файловую систему NTFS для настройки доступа к объектам.
3. Разработать строгую политику аудита.
4. Как использовать группы с ограниченным членством?
5. Сетевые операционные системы.

Контрольная задача:

Вы администратор домена Contoso.com. В данный момент Вы администрируете компьютер Contoso3 под управлением WS2003. Этот компьютер функционирует как сервер приложений, также на нем запущены службы IIS. Вы обнаружили, что один из размещенных на сервере сайтов поврежден. Вы должны восстановить IIS-настройки сайта с минимальным уровнем административного вмешательства. **Что Вы должны сделать?**

а) Восстановить настройки IIS выполнив команду **iisweb.vbs /create**.
б) Открыть **Диспетчер служб IIS** и восстановить перыдущую версию сайта.
в) Восстановить настройки IIS выполнив команду **iisweb.vbs /restore**.
г) Восстановить настройки IIS выполнив команду **iisweb.vbs /backup**.

Рекомендация: при выполнении лабораторной работы использовать данные по безопасности сети.

Используемая литература:

1. **«Управление и поддержка Microsoft Windows Server 2003»**. Дэн Холме, Орин Томас, М., Русская Редакция, 2004 г.
2. **«Внедрение, управление и поддержка сетевой инфрастуктуры Microsoft Windows Server 2003».** Дж. С. Макин, Йен Маклин, М., Русская Редакция, 2004 г.

Рекомендуемые Интернет ресурсы:

1. www.opennet.ru
2. www.microsoft.com
3. www.intuit.ru

Лабораторная работа № 9

«Управление учетными записями пользователей»
(2 часа)

Цель: Освоить создать для групп пользователей и управлять правами пользователей.

Постановка задачи:
Создать, обновить пользователей и групп.

Объект пользователя в AD состоит из имени пользователя, пароля, идентификатор безопасности (SID), профиль пользователя. Создавать объекты пользователей можно в консоли Active Directory – пользователи и компьютеры или в командной строке с помощью команды dsedd user. При создании объекта пользователя через консоль необходимо заполнить ряд обязательных палей:

- Полное имя (на его основе генерируются обычное имя (cn), различающееся имя (dn), собственно имя и отображаемое имя (displayname);
- имя входа пользователя (представляет собой имя_пользователя@имя домена);
- имя входа пользователя (пред-Windows 2000), используется для входа в домен с клиентов под управлением ранних версий Windows;
- пароль (пароль должен отвечает требованиям сложности, установленным групповой политикой).

Также можно задать некоторые свойства пользователей: требовать смену пароля при следующем входе в систему, Запретить смену пароля пользователем, снять ограничение срока действия пароля или отключить учетную запись. В ряде случаев, настройки свойств объекта пользователя могут противоречить настройкам политики безопасности, действующей в системе. Настройки объекта пользователя приоритетнее настроек политики безопасности.

После создания объекта пользователя можно настроить его остальные свойства, среди которых путь к профилю пользователя, членство в группах, личные данные пользователя и прочее.

Также можно настроить список компьютеров, с которых пользователь может входить в сеть, время входа пользователя в систему, использование смарт-карт и срок действия самой учетной записи. Из консоли Active Directory – пользователи и

компьютеры можно управлять несколькими объектами пользователей одновременно. Для этого их достаточно выделить в рабочей области оснастки. Перемещать несколько объектов пользователей, копировать и удалять их можно без ограничений. Но далеко не все свойства учетных записей доступны для совместного редактирования (одновременно можно изменять путь к профилю пользователя, сценарий входа в систему, домашнюю папку, должность, практически все свойства адреса, срок действия учетных записей и некоторые другие свойства). Все операции с объектами пользователей, доступные в графической консоли, можно осуществлять из командной строки. Для создания объектов пользователей можно использовать так называемые шаблоны – заранее созданные объекты пользователей, копируемые при необходимости создания конкретных объектов. При копировании шаблона копируются не все свойства, настроенные в шаблоне. Свойства копируются в следующем порядке: на вкладках Общие, телефоны, входящие звонки, среда, сеансы, удаленное управление, профиль служб терминалов, COM+ - свойства не копируются; на вкладке Адрес копируются все свойства кроме Улица; на вкладке Учетная запись копируются все свойства кроме Имя входа; на вкладке Организация копируются все свойства кроме Должность; свойства на вкладках Профиль и Член групп копируются полностью.

Контрольные вопросы:

1. Что такое учетные записи?
2. Как создать пользователя?
3. Как создать груп.
4. Как изменить пароль пользователя в Windows XP?
5. Как ограничить права пользователя Windows XP?

Контрольная задача:

Вы администратор домена Contoso.com. Все сервера управляются WS2003, а все клиенты – Windows XP Professional. Вы создали общую папку AppShare. Эта папка расположена на томе с NTFS на сервере Contoso3. Вы установили разрешения NTFS на эту папку как показано в таблице.

Пользователи	**NTFS-разрешения**	**Разрешения общего доступа**
Anna	Чтение	Чтение
Group3	Чтение	Изменение
Group4	Чтение\Запись	Полный доступ
Все	Чтение и выполнение	Чтение

Том является только членом группы Все, но он должен также иметь возможность удалять файлы из папки AppShare. **Что Вы должны сделать?**

а) Назначить группе **Все** разрешение общего доступа **Разрешить – Полный доступ**.

б) сделать Тома членом группы Group4. Назначить группе Group4 NTFS-разрешение **Разрешить - Чтение и выполнение**.

в) Сделать Тома членом группы Group3. Назначить группе Group3 NTFS-разрешение **Разрешить - Изменение**.

г) Назначить группе **Все** NTFS-разрешение **Разрешить – Полный доступ**.

д) Назначить учетной записи Тома NTFS-разрешение **Разрешить – Полный доступ**

Рекомендация: при выполнении лабораторной работы использовать данные по управление учетными записями пользователей.

Используемая литература:

1. **«Управление и поддержка Microsoft Windows Server 2003»**. Дэн Холме, Орин Томас, М., Русская Редакция, 2004 г.
2. **«Внедрение, управление и поддержка сетевой инфрастуктуры Microsoft Windows Server 2003».** Дж. С. Макин, Йен Маклин, М., Русская Редакция, 2004 г.

Рекомендуемые Интернет ресурсы:

1. www.opennet.ru
2. www.microsoft.com
3. www.intuit.ru

СОДЕРЖАНИЕ