

Изучаемая тема: Обеспечение функционирования сети.

Лабораторная работа № 1 «Создание ролей. Создание контроллера домена (DC)»

Цель работы: получить навыки создания контроллера домена серверной ОС Windows 2008

В процессе занятия решаются следующие задачи:

1. приобретение навыков настройки контроллера домена,
2. формирование умения создавать роли в Windows Server 2008

Краткие теоретические и справочно-информационные материалы по теме занятия.
Серверные роли

Серверные роли описывают первичную функцию сервера. Администраторы могут выделить для каждой роли по отдельному серверу или же совместить несколько ролей на одном сервере. Каждая роль может включать один или более сервисов, называемых под-элементами роли. В Windows Server 2008 существуют следующие серверные роли, которые могут быть установлены и управляются через Server Manager.

Active Directory Certificate Services - Active Directory Certificate Services (AD CS) обеспечивает настраиваемый сервис для создания и управления сертификатами публичных ключей, используемых в системах безопасности ПО. Организации могут использовать Active Directory Certificate Services для повышения безопасности, используя привязку к пользователю, устройству или сервису к соответствующему частному ключу. В Active Directory Certificate Services также включены возможности, которые позволяют управлять выдачей сертификатов и их обновлением, в разнообразном масштабируемом окружении.

Приложения поддерживаемые Active Directory Certificate Services включают в себя: Secure/Multipurpose Internet Mail Extensions (S/MIME), безопасные беспроводные сети, Виртуальные Частные Сети (VPN), протокол IPsec, Шифрованную Файловую Систему (EFS), смарт карты, протоколы Secure Socket Layer/Transport Layer Security (SSL/TLS), и цифровые подписи.

Active Directory Domain Services - Active Directory Domain Services хранит информацию о пользователях, компьютерах, и других устройствах сети. AD DS помогает администраторам безопасно управлять этой информацией и распределением ресурсов и совместной работой между пользователями. AD DS также необходима для установки приложений использующих Active Directory (например Microsoft Exchange Server) и для применения других технологий Windows Server, таких как Групповые политики.

Active Directory Federation Services - Active Directory Federation Services (AD FS) обеспечивает функционирование технологии Web single-sign-on (SSO), которая позволяет аутентифицироваться пользователям к Web приложениям используя единый один экаунт. AD FS это законченное решения для безопасного объединения, идентификации пользователей между организациями партнерами.

Active Directory Lightweight Directory Services – организации которые используют приложения, которые требуют наличия каталога для хранения информации, могут использовать Active Directory Lightweight Directory Services (AD LDS), в качестве хранилища. AD LDS запускается как отдельный сервис, не являющийся частью операционной системы, что позволяет использовать несколько копий сервиса на одном сервере. Каждая из копий сервиса может быть сконфигурирована независимо от других копий, и использоваться разными приложениями.

Active Directory Rights Management Services (AD RMS) - AD RMS технология защиты информации, которая работает с приложениями поддерживающими эту функцию (Например Outlook 2007), и помогает защитить информацию от несанкционированного использования. Владелец информации может указать, как именно получатель может использовать информацию, например, открывать, модифицировать, печатать, пересылать,

или производить другие действия с информацией. Организации могут создавать темплейты прав, такие как «Конфиденциально – Только чтение», которые могут применяться к необходимым объектам защиты (например почтовые сообщения, финансовые отчеты и т.д.)

Application Server - Application Server комплексное решение для хостинга и управления высокопроизводительными распределенными бизнес приложениями. Включая такие сервисы как .NET Framework, поддержка Web сервера, очереди сообщений, COM+, Windows Communication Foundation, и поддержку отказоустойчивых кластеров, ускоряя производительность, на всем протяжении жизненного цикла приложения, начиная от проектирования и разработки, до внедрения, и промышленной эксплуатации.

Dynamic Host Configuration Protocol (DHCP) Server – DHCP позволяет назначать или выдавать IP адреса компьютерам и другим устройствам, которые могут функционировать, как DHCP клиенты. Развернутые DHCP серверы в сети, автоматически сообщают компьютерам и другим устройствам использующим стек протоколов TCP/IP, правильный IP адрес и другие параметры (Опции DHCP), которые позволяют устройствам соединиться с другими ресурсами, такими как DNS серверы, WINS серверы, маршрутизаторы и др.

DNS Server - Domain Name System (DNS) предоставляет стандартный метод ассоциации названий устройств, с IP адресами. Это позволяет пользователям обращаться к ресурсам, используя легко запоминающиеся имена ресурсов, а не IP адреса. Windows DNS сервер можно интегрировать с DHCP сервером, для автоматического обновления информации на DNS сервере.

Fax Server - Fax Server позволяет получать и отправлять факсимильные сообщения, управлять ресурсами факсов, такими как настройки, задания, факсами.

File Services - File Services предоставляют технологии для управления хранилищами, файловой репликацией, распределенной файловой системой, быстрый поиск файлов и ускоренный доступ клиентов к файлам.

Network Policy and Access Services - Network Policy and Access Services предоставляет различные методы для доступа к локальным и удаленным сетевым ресурсам, и позволяет сетевым администраторам централизованно управлять сетевым доступом и клиентскими политиками. Совместно с сервисом Network Access Services, вы можете развернуть серверы VPN, серверы dial-up, маршрутизаторы, и защищенные беспроводные сети (802.11). Также вы можете развернуть RADIUS серверы, прокси, использовать Connection Manager Administration Kit для создания профилей удаленного доступа, которые позволят клиентским компьютерам соединиться с вашей сетью.

Print Services - Print Services позволяют управлять принт серверами и принтерами. Принт серверы снижают управляющую нагрузку на администраторов, за счет централизованного управления принтерами.

Terminal Services - Terminal Services предоставляют возможность пользователям использовать программное обеспечение, установленное на терминальном сервере, или же получить удаленный доступ к своему рабочему столу с любого компьютера. Пользователи могут соединиться с терминальными серверами, для запуска приложений и для использования сетевых ресурсов (сетевые диски, печать и т.д.).

Universal Description, Discovery, and Integration Services - Universal Description, Discovery, and Integration (UDDI) Services предоставляют возможности для распределения информации с использованием Web сервисов внутри сети (Интранет), между бизнес партнерами (Экстранет), или же в Интернет. UDDI Services может помочь увеличить производительность разработчиков и IT профессионалов с более надежными и управляемыми приложениями. С UDDI Services вы можете сократить возможное дублирование работы коллегами и снизить накладные расходы.

Web Server (IIS) - Web Server (IIS) предоставляет информацию в Интернет, Интранет, Экстранет. Это объединенная Web платформа на базе IIS 7.0, ASP.NET, Windows Communication Foundation, и Windows SharePoint Services. В IIS 7.0 увеличена безопасность, упрощена диагностика и администрирование.

Windows Deployment Services – Вы можете использовать Windows Deployment Services для инсталляции и конфигурирования операционных систем семейства Microsoft Windows, с использованием образов Pre-boot Execution Environment (PXE) boot ROMs. Администрирование упрощается с использованием MMC оснастки WdsMgmt, который управляет всеми аспектами Windows Deployment Services. Windows Deployment Services также позволяет пользователям получить опыт в развертывании Windows.

Windows SharePoint Services - Windows SharePoint Services позволяет организациям увеличить производительность, путем создания Web сайтов для совместной работы над документами, задачами и событиями, распространения контактов и другой информации. Окружение, спроектированное для гибкого развертывания, администрирования, и разработки приложений.

Server Core Installation

В Windows Server 2008, администраторы могут инсталлировать минимально необходимое окружение для работы определенных ролей. Также это повышает безопасность сервера (уменьшая поверхность атаки), снижает затраты на управление, и требования к ресурсам. Для установки в режиме Server Core Installation на жестком диске достаточно 2Гб свободного места! Уверен, в ближайшем будущем, во многих компаниях будут стоять двухпроцессорные серверы (4х или 8ми ядерные), с ПО Virtual Server, на которых будет крутиться два-четыре Windows Server 2008 в режиме Server Core Installation, каждый, со своей ролью.

В режиме Server Core Installation можно инсталлировать роли:

- Active Directory Domain Services
- Active Directory Lightweight Directory Services (AD LDS)
- DHCP Server
- DNS Server
- File Services
- Print Server
- Streaming Media Services

Опциональные возможности Server Core Installation:

- Backup
- BitLocker Drive Encryption
- Failover Clustering
- Multipath IO
- Network Load Balancing
- Removable Storage
- Simple Network Management Protocol (SNMP)
- Subsystem for UNIX-based applications
- Telnet client
- Windows Internet Name Service (WINS)

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

Роли и компоненты

Сейчас у нас имеется установленная операционная система Windows Server 2008, но для того, чтобы использовать ее для выполнения некоторой серверной функции надо установить роль (role). Роль включает одну или несколько служб (role services), необходимых для выполнения определенной функции. Например, File Services (файловые службы) или Web-server (IIS). Когда роль объединяет несколько служб, то могут устанавливаться или все сразу, или отдельные службы. Дополнительная функциональность может быть получена путем установки программных модулей

называемых компонентами (feature). Пример компоненты – это SMTP Server. Роли компоненты могут быть как независимыми, так и взаимосвязанными.

Добавить или удалить роли и компоненты можно с помощью оснастки Server Manager (Start -> Administrative tools -> Server Manager). Окно оснастки представлено на рис.11.

Если выделить узел Roles, то увидим список установленных ролей. Добавлять или удалять роли можно, перейдя по ссылкам Add Roles или Remove Roles соответственно. Добавьте роль File Services (не устанавливая дополнительных служб, таких как DFS т.д.). Теперь наш сервер сможет выполнять роль файлового сервера. Работе файловыми ресурсами будет посвящена отдельная лабораторная работа. Сейчас же стоит отметить только, то что в данном случае никакого дополнительного конфигурирования после установки роли не потребовалось.



Рисунок 11- Окно администрирования оснастки Server Manager

Одна из задач текущей практической работы – сделать наш сервер контроллером домена Windows. Для этого понадобится установить роль Active Directory Domain Services и выполнить настройку параметров домена.

Домен Windows логически объединяет несколько компьютеров для того, чтобы можно было их централизованно администрировать. Примером административной задачи может быть создание такой учетной записи, чтобы пользователь мог входить под ней на любой компьютер своего подразделения организации. В этом случае, чтобы такую запись завести только один раз (а не на каждом компьютере), нужно вести единую базу данных с информацией о пользователях и компьютерах. Подобная база называется каталогом, а разработанная Microsoft служба каталога – Active Directory. Серверы, на которых работает служба и которые, в частности, выполняют проверку пользователей с доменными учетными записями, называются контроллерами домена.

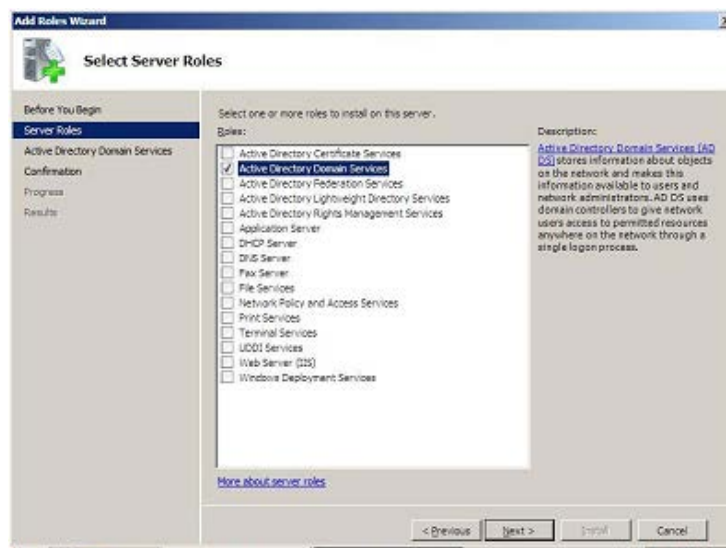


Рисунок 12- Добавление роли Active Directory Domain Services

Из оснастки Server Manager добавляем роль Active Directory Domain Services (рис.12).

Когда роль добавлена, потребуется произвести начальное конфигурирование нового контроллера. Делается это запуском утилиты dcpromo из основного меню (Start->Run...-> dcpromo) или по ссылке, которая появится в окне Server Manager после установки роли.

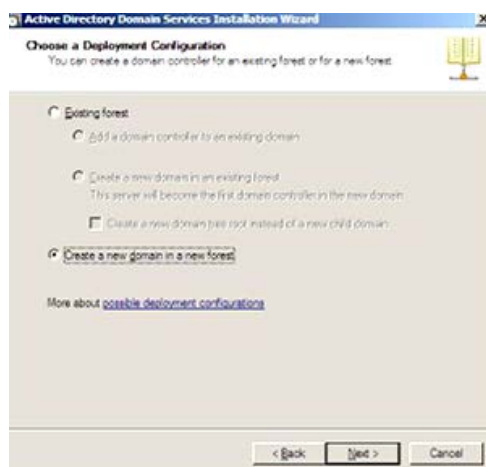


Рисунок 13- Создание нового домена в новом лесе

Для понимания дальнейшего надо ввести несколько понятий. Как мы уже разобрались, информация об объектах сети хранится в каталоге. Для этого сначала создаются определения объектов, которые помещаются в служебную структуру, называемую схема каталога. Если хотим создать объект нового типа, нужно сначала поместить в схему его определение. Совокупность доменов, использующих единую схему каталога и общую конфигурацию, называют лесом доменов (forest).

В окне мастера, представленном на рисунке 13, мы указываем, что создаем новый лес, т.е. мы конфигурируем первый контроллер первого (корневого) домена в нашей организации. В следующем окне мастера (рис.13) запрашивается имя домена. Обычно имена соотносятся с доменными именами Интернет (например, flk.spbstu.ru), но для наших лабораторных будем использовать имя SAIU_Test.

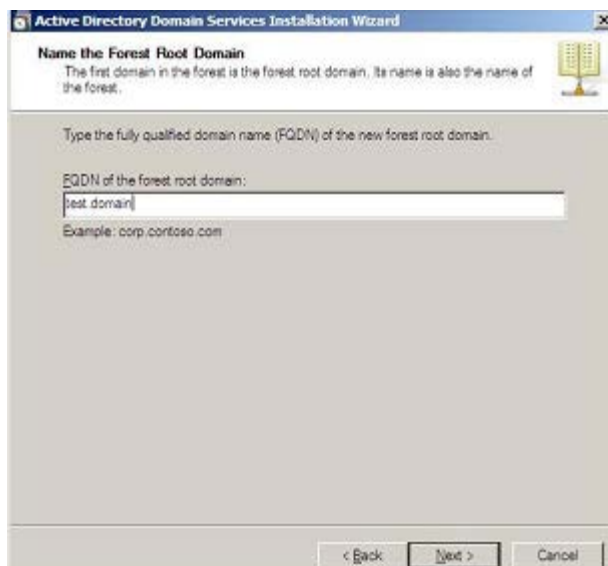


Рисунок 14- ввод имени домена

Далее, так как в нашей виртуальной сети пока нет DNS сервера, мастер предложит установить DNS сервер (рис.14). Служба DNS используется для разрешения доменных имен компьютеров в ip-адреса (например, имени www.ftk.spbstu.ru сопоставляется адрес 195.19.212.13). В домене Windows клиентские компьютеры с помощью DNS получают информацию о контроллерах домена поэтому хотя бы один DNS сервер необходим.

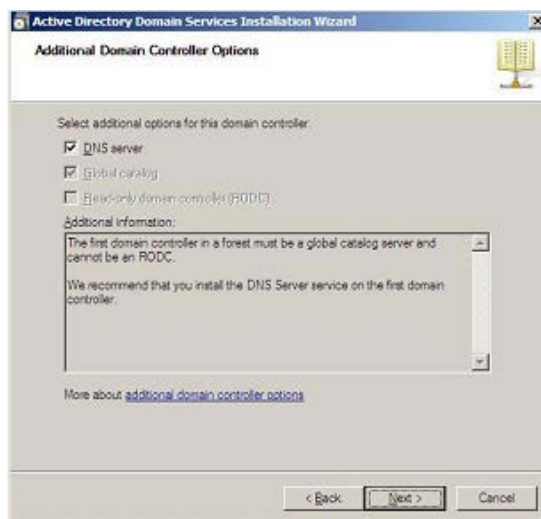


Рисунок 15- Установка DNS сервера

Следующее окно позволяет выбрать функциональный уровень домена. Если выбрать уровень Windows Server 2008, то мы получим поддержку всех новых функций, но в роли контроллеров домена смогут выступать только компьютеры с Windows Server 2008 (и, наверное, более новых ОС после их появления). Наоборот, выбор уровня Windows 2000 позволит использовать контроллеры с более старыми версиями серверных ОС (Windows 2000 Server, Windows Server 2003), но не даст использовать некоторые возможности, имеющиеся только в Windows Server 2008. Выберем уровень Windows Server 2008.

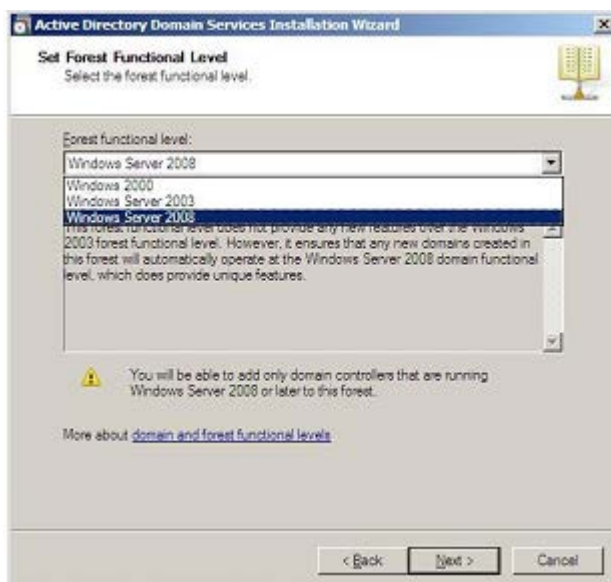


Рисунок 16- Выбор функционального уровня домена

Следующее окно мастера позволяет выбрать расположение базы каталога, файлов журнала и служебного каталога SYSVOL (в нем, в частности, хранятся политики и скрипты, запускающиеся при входе пользователя в домен). Можно согласиться с настройками по умолчанию.

В конце надо будет задать пароль для доменной учетной записи Administrator (пусть это снова будет Serv08Saiu) и перезагрузить нашу виртуальную машину.

После перезагрузки зайдите под учетной записью Administrator. **Последнее задание** – создание нового пользователя. Для этого надо запустить административную оснастку Active Directory Users and Computers (Start-> Administrative Tools-> Active Directory Users and Computers) или можно получить к ней доступ из окна Server Manager, как показано на рис.17.

Раскройте узел, соответствующий нашему домену, перейдите на контейнер Users и вы увидите список созданных автоматически стандартных групп и учетных записей.

В контекстном меню выберите создание нового пользователя (New->User) пусть имя учетной записи будет Labos, пароль Lab0s123 (имя и фамилию пользователя придумайте сами). Укажите, что пользователю не надо менять пароль при первом входе.

Когда учетная запись создана, попробуйте войти под ней на сервер. Должно появиться сообщение, что действующая политика не позволяет это сделать. Дело в том, что настройки по умолчанию не позволяют обычным пользователям локально входить на контроллер домена.

Созданная учетная запись нам понадобится на следующей лабораторной работе, когда мы добавим в домен рабочую станцию.

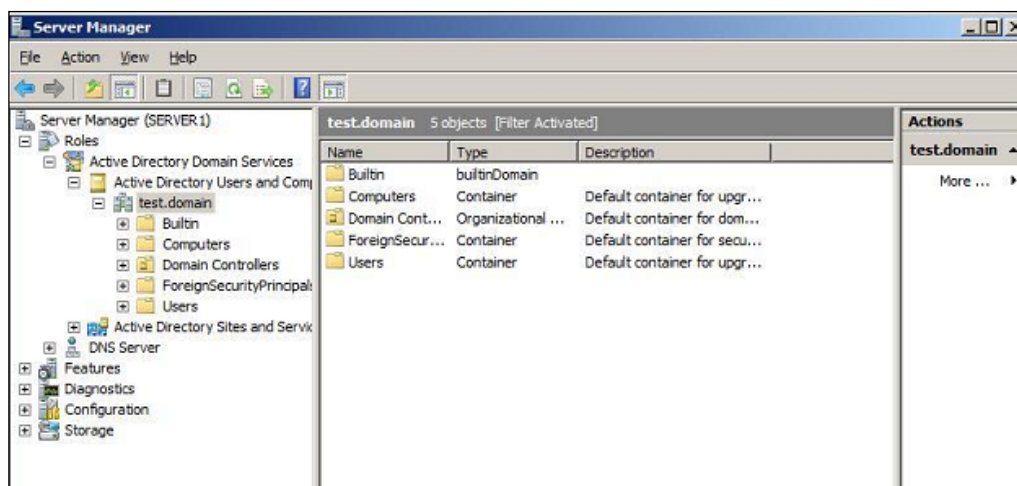


Рисунок 17- Управление доменными учетными записями

Время выполнения работы 90 мин;

Контрольные вопросы

1. Что такое служба каталогов?
2. Служба каталогов Active Directory- это...
3. Основное назначение и функции Active Directory
4. Что такое контроллер домена?
5. **Какие службы необходимы для нормальной работы Active Directory Domain Services?**
6. Порядок настройки DHCP и DNS

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки:

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания, выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

Список использованной литературы

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2013. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия] / Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2008. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия] /А. В. Кузин. - 3-е изд., перераб. и доп. - М.: ФОРУМ: ИНФРА-М, 2011.- 192 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия] /В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2010.
5. Microsoft Windows Server 2003. Справочник администратора[электронная версия] /Пер. с англ. — М.: Русская Редакция, 2004. - 640 с.

6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 [электронная версия] / Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2003: Справочник администратора [электронная версия] / Ч. Рассел, Ш. Кроуфорд, Дж. Джеренд., пер. с англ. – 2-е изд., -М.: Русская Редакция, 2007.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия] / С. В. Бормотов — СПб.: Питер, 2006. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2008 [электронная версия] / Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2008 R2. Полное руководство. Пер. с англ. [электронная версия] / Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд.-М.: ООО «И.Д. Вильямс», 2011.-1456 с.: ил.- Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство [электронная версия] / Т. Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2009. – 944 с., ил.