

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ**

С.М. Платунова

**Администрирование вычислительных сетей
на базе MS Windows Server® 2008**

Учебное пособие



Санкт-Петербург

2012

Платунова С.М. Администрирование вычислительных сетей на базе MS Winsows Server® 2008. Учебное пособие по дисциплине «Администрирование вычислительных сетей». – СПб: НИУ ИТМО, 2012. – 41 с.

В учебном пособии содержатся основные сведения об администрировании вычислительных сетей на базе MS Winsows®, такие как: требования к аппаратным средствам, процесс инсталляции, управление учетными записями пользователей и групп, настройка программной среды пользователя, управление безопасностью, доступом к файлам и каталогам, архивирование и восстановление системы.

Пособие адресовано специалистам с высшим и средним профессиональным образованием, имеющим опыт работы в области IT технологий, обучающихся по направлению 230100 Информатика и вычислительная техника.

Рекомендовано к печати Ученым советом факультета Академии ЛИМТУ, протокол № 6 от 23.12.2011



В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

© Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, 2012

© С.М. Платунова, 2012

СОДЕРЖАНИЕ

Введение	4
Тема 1. Установка Windows Server® 2008	5
1.1 Установка новой операционной системы Windows Server® 2008.....	5
1.2 Установка с обновлением.....	8
Тема 2. Установка контроллера домена и подключение к нему рабочих станций.....	9
2.1 Установка роли контроллера домена	9
2.2 Подключение к домену рабочих станций	11
Тема 3. Управление учетными записями пользователей и групп	12
3.1 Учетные записи пользователей.....	12
3.2 Создание пользователей при помощи оснастки «Active Directory – пользователи и компьютеры»	13
3.3 Создание пользователей на основании шаблонов	15
3.4 Учетные записи групп пользователей.....	17
3.5 Создание групп при помощи оснастки «Active Directory – пользователи и компьютеры»	21
Тема 4. Понятие и управление групповыми политиками.....	22
4.1 Управление политиками сайта, домена, подразделения	23
4.2 Создание объекта групповой политики	24
4.3 Редактирование объекта групповой политики.....	25
4.4 Поиск и удаление объектов групповой политики.....	25
Тема 5. Предоставление общего доступа к файлам сервера	27
5.1 Создание общего ресурса с помощью Проводника.....	29
5.2 Создание общего ресурса с помощью консоли «Управление компьютером».....	31
5.3 Создание общего ресурса с помощью консоли «Управление общими ресурсами и хранилищами»	32
Тема 6. Резервное копирование и восстановление данных.....	34
6.1 Создание резервной копии	35
6.2 Восстановление сервера из резервной копии.....	37
Вопросы для самоподготовки.....	37
Литература.....	38

Введение

Таблица 1. Требования к аппаратуре, предъявляемые ОС

	Минимальные	Рекомендуемые
Процессор	1 ГГц (x86) или 1.4 ГГц (x64)	2 ГГц и выше
ОЗУ	512 МБ ОЗУ (возможно ограничение производительности и некоторых возможностей)	2 ГБ ОЗУ и выше Максимально (для 32-бит): 4 ГБ ОЗУ (Standard) или 64 ГБ ОЗУ (Enterprise и Datacenter) Максимально (для 64-бит): 32 ГБ ОЗУ (Standard) или 2 Тб ОЗУ (Enterprise, Datacenter и в Itanium-Based системах)
Видеокарта и монитор	Super VGA (800 x 600)	Super VGA (800 x 600) и более высокое разрешение
Свободное место на жёстком диске	10 ГБ	40 ГБ и выше Сервер с более чем 16 ГБ ОЗУ требует больше места для swap и dump файлов.
Другие приводы	DVD-ROM	DVD-ROM
Прочие устройства	клавиатура и мышь	

Большинство изданий Microsoft Windows Server[®] 2008 доступны в версиях x64 (64-bit) и x86 (32-bit). Windows Server 2008 для Itanium поддерживает IA-64 процессоры. Версия IA-64 оптимизирована под высокую нагрузку, например — в серверах баз данных, и не имеет дополнительной оптимизации для использования в роли файлового или медиа-сервера. Windows Server[®] 2008 доступна в следующих редакциях:

- Windows Server 2008 Standard Edition (x86 и x64)
- Windows Server 2008 Enterprise Edition (x86 и x64)

- Windows Server 2008 Datacenter Edition (x86 и x64)
- Windows Web Server 2008 (x86 и x64)
- Windows Storage Server 2008 (x86 и x64)
- Windows Server 2008 для систем, основанных на Itanium

Server Core доступен в Web, Standard, Enterprise и Datacenter изданиях. Он не доступен в Itanium edition. Windows Server 2008 Standard Edition доступен для студентов бесплатно по программе DreamSpark. Требования, предъявляемые операционной системой Windows Server 2008 к аппаратуре указаны в таблице 1.

Тема 1. Установка Windows Server® 2008

ОС Windows Server 2008 можно установить как новую систему или как обновление имеющейся. В первом случае программа установки полностью заменит имеющуюся ОС на Windows Server 2008, а все имевшиеся пользователи и параметры приложений будут потеряны. Если выбрано обновление, программа установки выполняет установку Windows Server 2008, а затем переносит в неё параметры пользователей, документы и приложения из прежней системы.

Перед началом установки Windows Server 2008 следует убедиться, что компьютер удовлетворяет минимальным требованиям устанавливаемой версии. Майкрософт указывает как минимальные, так и рекомендуемые характеристики компьютера. Если компьютер не удовлетворяет минимальным требованиям, установить Windows Server 2008 будет не возможно. Если характеристики компьютера ниже рекомендуемых, возможны проблемы с производительностью.

Для установки базовых компонентов операционной системы требуется не менее 8 Гб дискового пространства. Рекомендуется иметь не менее 40 Гб доступного дискового пространства для установки ядра сервера и не менее 80 Гб для полной установки. Дисковое пространство требуется для файлов подкачки и дампов памяти, а так же для установки компонентов, ролей и служб ролей. Для достижения оптимальной производительности рекомендуется иметь не менее 10% свободного пространства на всех дисках сервера.

1.1 Установка новой операционной системы Windows Server® 2008

Для установки новой операционной системы необходимо включить компьютер, вставить установочный DVD-диск Windows Server® 2008,

выставить в BIOS загрузку с CD/DVD привода и нажать любую клавишу, когда на экране появляется приглашение. После загрузки программа установки убеждается в наличии как минимум 512 Мбайт памяти и предлагается выбрать язык, формат времени и представления денежных единиц, клавиатуру или метод ввода, который предполагается задействовать в установке.

Затем появляется окно, предлагающее варианты дальнейших действий — Установка или Восстановление системы.

При выборе опции «Установить» запускается процедура установки setup.exe. Пока выполняется setup.exe, всегда можно воспользоваться комбинацией Shift+F10, чтобы открыть окно для ввода команды в том случае, если необходимо выполнить другие функции, например, запустить сценарий добавления служебного раздела или осуществить диагностику проблем в ходе установки; пока окно для ввода команды открыто, программа установки не будет перезапускать сервер.

Вариант восстановления компьютера Repair your computer открывает доступ к среде восстановления Windows® и некоторым автоматизированным возможностям восстановления.

Средства восстановления очень эффективны, поэтому рекомендуется на всякий случай всегда иметь под рукой DVD Server 2008.

Можно в любой момент создать диск аварийного восстановления в среде Server® 2008 после установки функции Windows Backup Server; создание диска аварийного восстановления — одна из возможностей функции резервного копирования.

Нажать «Установить» и программа установки открывает окно с предложением ввести ключ продукта из 25 символов, привязанный к конкретной версии Server 2008. Можно ввести ключ продукта, либо оставить поле пустым, после чего нажать Next для запуска диалогового окна подтверждения.

Окно ввода ключа есть не во всех дистрибутивах Windows Server 2008, поэтому следующий рисунок приведен от другой версии операционной системы Windows Server 2008.

На данном этапе можно не вводить ключ продукта, чтобы испытать операционную систему в течение 30 дней или вставить ключ продукта из файла после установки операционной системы.

Когда будет производиться активация Windows Server® 2008, что следует сделать не позднее, чем через 30 дней после установки, нужно

убедиться, что версия, которую установили, соответствует версии, на которую имеется лицензия. Если это не так, то есть два варианта действий.

Можно приобрести ключ продукта для версии, установленной на компьютере, что может оказаться слишком дорого, если, например, установлен выпуск Enterprise Edition, а ключ продукта привязан к Standard Edition, либо переустановить версию, соответствующую ключу продукта, что может привести к утрате данных, информации и программ, помещенных в систему после последней установки операционной системы. В приведенном примере нажать «No» в диалоговом окне подтверждения. Откроется новое окно с вопросом, какую редакцию Windows Server® 2008 предстоит устанавливать? Поскольку ключ продукта не введен, в окне отображаются все версии Server® 2008, заключенные в файле образа, а также флажок, подтверждающий, что выбран именно тот выпуск Windows®, который был приобретен (I have selected the edition of that I purchased).

Если ключ продукта был введен ранее, будет предложено два варианта установки на выбор — Полная установка (Full Installation) или Установка ядра сервера (Server Core Installation) — для редакции операционной системы, определяемой по ключу продукта.

Server Core — «облегченный» вариант установки сервера с минимальным объемом занимаемой памяти, обеспечивающий ограниченную среду управления сервером.

Server Core предлагает лишь основные компоненты Server® 2008 — без оболочки «Проводника Windows», но с интерфейсом командной строки — и поддержкой основных ролей сервера, а именно, сервер файлов, сервер DHCP, сервер печати и сервер DNS.

Server Core не является платформой для разработки или обслуживания приложений, в том числе и не включает среду .NET Framework.

Вариант Server Core выбирается при минимальной визуальной функциональности Windows®, при этом отпадает необходимость применения многих обновлений к системам Server Core — следовательно, эти системы легче обслуживать.

Кроме того, системы Server Core используют меньше ресурсов (например, дискового пространства), а благодаря отсутствию графического интерфейса они меньше подвержены риску.

После выбора варианта установки Server® 2008 и нажатия «Далее» открывается лицензионное соглашение. Следует внимательно прочитать его, затем отметить флажок «Я принимаю условия лицензии» и нажать «Далее».

Открывается окно с просьбой указать тип установки — Обновление (Upgrade) или Полная установка (Custom).

Поскольку выполняется новая установка с носителя, вариант «Обновление» недоступен для выбора (затенен), так что остается выбрать «Полная установка».

Если программа установки запускается из среды Windows Server 2003, оба варианта недоступны для выбора.

Открывается окно с вопросом: «В какой раздел установить Windows?». В окне отображаются логические разделы и свободное место.

Здесь можно добавлять и удалять разделы, отформатировать ранее использовавшийся жесткий диск перед установкой Server 2008, а также загрузить при необходимости дополнительные драйверы.

Следует выбрать раздел для установки, затем нажать Далее. Если раздел не отформатирован, программа установки быстро отформатирует его в формате NTFS и продолжит работу.

Далее начнется непосредственно установка файлов на диск и в течение установки компьютер перезагрузится два раза.

Первое, что можно увидеть по завершении установки — окно с сообщением о необходимости изменения пароля пользователя перед первой регистрацией в системе. При установке Server® 2008 учетная запись администратора создается с пустым паролем, поэтому первое действие — задание нового пароля администратора. После задания пароля администратора происходит регистрация пользователя в системе как администратора.

1.2 Установка с обновлением

Возможность обновления ОС при установке Windows Server® 2008 несколько отличается от предыдущих версий. Обновление состоит в том, что программа установки все равно выполняет чистую установку ОС, а затем переносит в неё параметры пользователя, документы и приложения из предыдущей версии Windows.

В процессе переноса программа установки перемещает папки и файлы предыдущей системы в папку Windows.old, в результате чего старая система перестает запускаться. Перенос параметров выполняется потому,

что в Windows Server® 2008 информация о пользователях и приложениях хранится не так, как в предыдущих версиях.

Чтобы установить Windows Server® 2008 с обновлением, нужно производить установку непосредственно из запущенной ОС, с учётной записью и правами администратора. При установке в диалоговом окне выбора типа установки задается установка с обновлением.

Тема 2. Установка контроллера домена и подключение к нему рабочих станций

В сетях Microsoft Windows Server контроллером домена называется центральный компьютер локальной сети (сервер), на котором работают службы каталогов, и располагается хранилище данных каталогов. Контроллер домена хранит параметры учётных записей пользователей, параметры безопасности (применимо к томам с файловой системой NTFS), параметры групповой и локальной политик.

Устанавливая Windows Server® 2008 на новый компьютер, его настраивают как рядовой сервер, контроллер домена или изолированный сервер. Изолированные серверы не являются частью домена. Рядовые серверы являются частью домена, но не сохраняют информацию каталога. Контроллеры доменов отличаются от рядовых серверов тем, что хранят информацию каталога и предоставляют всему домену службы каталогов и проверки подлинности.

2.1 Установка роли контроллера домена

Открыть «Диспетчер сервера» (Server Manager) и узел Роли (Roles) в левой панели консоли. Затем нажать Добавить роли (Add Roles) в правой панели.

Далее предлагается выбор ролей для установки. Необходимо выбрать и установить роль контроллера домена (DC).

Выбрать Active Directory Domain Services, отмечая соответствующую опцию. Мастер отобразит ряд функций, которые будут установлены наряду с ролью Active Directory Server Role. Нажать кнопку Добавить нужные функции (Add Required Features), чтобы установить эти функции во время установки роли Active Directory Server.

Дополнительные компоненты для установки AD нужны не на всех версиях ОС Windows Server® 2008.

После выбора роли Active Directory Domain Service, отображается информация об этой роли сервера.

- Желательно устанавливать как минимум два доменных контроллера в сети для повышения отказоустойчивости. Установка одного контроллера в сети является предпосылкой сбоя.
- После установки роли необходимо запустить `dcpromo`. При запуске утилиты `dcpromo` установится роль сервера DNS, поддерживающего службы Active Directory.
- Во время установки роли Active Directory Domain Services также устанавливаются службы DFS пространства имен, DFS репликации и репликации файлов, все эти службы используются службами Active Directory Domain Services, поэтому устанавливаются автоматически.

Перейти в меню Пуск и ввести ***dcpromo*** в текстовом поле «Выполнить», который находится в списке, Выбрать «`dcpromo`».

Запустится мастер установки доменных служб Active Directory. Здесь можно выбрать расширенные опции установки или пропустить их и нажать «Далее».

На странице Выбор конфигурации установки (Choose a Deployment Configuration) выбрать опцию «Создание нового домена в новом лесу (Create a new domain in a new forest)».

На странице имя корневого домена в лесу (Name the Forest Root Domain) ввести название домена, в формате DNS, в текстовое поле FQDN корневого домена в лесу. Если использовать имя, которое уже используется в интернете (имя, которое уже было зарегистрировано), то могут возникнуть проблемы раздвоения имен. Нажать «Далее».

На странице «Определение функционального уровня леса (Set Forest Functional Level)» выбрать опцию Windows Server® 2008, чтобы воспользоваться всеми возможностями, включенными в Windows Server® 2008. Нажать «Далее».

На странице «Дополнительные параметры» контроллера домена (Additional Domain Controller Options) имеется единственный выбор: DNS сервер. Служба DNS преобразует имена компьютеров в IP-адреса. При её использовании полное имя хоста преобразуется в IP-адрес, который позволяет компьютерам находить друг друга. Опция глобального каталога выбрана, так как это единственный DC в этом домене, поэтому он должен быть сервером глобального каталога.

Опция контроллера домена с разрешением только чтения (Read-only domain controller - RODC) не отмечена, поскольку необходимо иметь другой не-RODC в сети, чтобы включить эту опцию. Выбрать опцию DNS сервер и нажать «Далее».

Нажать Да, чтобы продолжить. Оставить папки для Database, Log Files и SYSVOL на предложенных местах по умолчанию и нажать «Далее».

На странице Directory Service Restore Mode Administrator Password ввести надежный пароль (буквы верхнего и нижнего регистра, цифры) в текстовые поля Пароль (Password) и Подтверждение (Confirm password).

Проверить информацию на странице Summary и нажать Далее.

Установка первого доменного контроллера занимает немного времени. Отметить опцию «перезагрузить по окончании» (Reboot on completion), чтобы компьютер автоматически перезагрузился после установки доменного контроллера

Компьютер автоматически перезагрузится. Установка будет завершена после входа в систему. Служба DNS была установлена во время установки Active Directory.

2.2 Подключение к домену рабочих станций

Для присоединения компьютеров рабочих станций к домену требуется чтобы:

- подсети сервера и рабочих станций были одинаковыми,
- маски подсетей одинаковы,
- адреса компьютеров были разными,
- имена компьютеров были разными,
- выключены брандмауэры на рабочих станциях и сервере (пуск → панель → управления → брандмауэр → ☉ выключить).

Доменному контроллеру должен быть назначен статический IP адрес. Чтобы установить его вручную, требуется зайти в панель управления, центр управления сетями и общим доступом и управление сетевыми подключениями, свойства подключения и в свойствах протокола версии 4 установить IP адрес, например 192.168.0.1, маска подсети 255.255.255.0

Для подключения рабочей станции под управлением ОС Windows® XP изменить IP адрес, например, : 192.168.0.2, маска подсети 255.255.255.0.

Для добавления системы в домен требуется войти в «Свойства компьютера» правой кнопкой мыши или можно нажать клавишу с эмблемой Windows (« Win ») и Паузу (« Pause / Break ») одновременно.

Перейти на вкладку «Имя компьютера» и щелкнуть «Изменить». Здесь необходимо задать имя компьютера и имя домена.

Появится диалоговое окно с просьбой ввести имя пользователя, обладающего полномочиями для присоединения рабочей станции к домену и пароль. О создании в домене учетной записи для данного подключения необходимо позаботиться заранее. Так же вход возможен с помощью учётной записи администратора доменного контроллера.

Если присоединение прошло удачно, то появится сообщение «Добро пожаловать в домен». После чего потребуется перезагрузить рабочую станцию.

В операционной системе «Виста» действия аналогичны. Задать IP-адрес 192.168.0.12. (Панель управления → центр управления сетями и общим доступом → управление сетевыми подключениями). Изменить IP адрес в свойствах протокола версии 4. путь аналогичен ОС Windows® XP.

При этом возможна проблема: «Не удастся разрешить DNS-имя контроллера домена в присоединяемом домене...» Чтобы ее решить, необходимо сделать две действия. Во-первых, ввести предпочитаемый DNS-сервер (адрес 192.168.0.1). В окне изменения имени компьютера выбрать «Дополнительно» и снять флажок «Сменить Основной DNS-суффикс» при смене членства в домене.

Тема 3. Управление учетными записями пользователей и групп

3.1 Учетные записи пользователей

Одним из основополагающих компонентов идентификации являются учетные записи пользователей. По сути, учетные записи пользователей представляют собой физические объекты, в основном людей, которые являются сотрудниками той или иной организации, но бывают исключения, когда учетные записи пользователей создаются для некоторых приложений в качестве служб. Учетные записи пользователей играют важнейшую роль в администрировании предприятий. К таким ролям можно отнести:

- Удостоверение личности пользователей, так как созданная учетная запись позволяет входить на компьютеры и в домены именно с теми данными, подлинность которых проверяет домен;

- Разрешения доступа к ресурсам домена, которые назначаются пользователю для предоставления доступа к доменным ресурсам на основании явных разрешений.

Учетные записи пользователей в Windows Server 2008 существуют двух типов: доменные и локальные.

Доменные учетные записи служат для вхождения в домен. Пройдя процедуру единого входа, доменная учётная запись получает доступ к ресурсам всего домена.

Локальным учётным записям предоставляется доступ к ресурсам локального компьютера, а для доступа к сетевому ресурсу они должны быть авторизованы.

Имя учетной записи состоит из двух частей: домен или рабочая группа и текстовое обозначение учетной записи. При создании учетной записи с ней связывается идентификатор безопасности SID (Security Identifier).

3.2 Создание пользователей при помощи оснастки «Active Directory – пользователи и компьютеры»

Оснастка «Active Directory – пользователи и компьютеры», добавляется в папку «Администрирование» сразу после установки роли «Доменные службы Active Directory» и повышения сервера до контролера домена. Этот метод является наиболее удобным, так как для создания учётных записей используется графический пользовательский интерфейс, а мастер создания учетных записей пользователя прост в использовании. К недостатку данного метода можно отнести, что при создании учетной записи пользователя нельзя сразу задать большинство атрибутов, и приходится добавлять необходимые атрибуты путем редактирования учетной записи.

Для того чтобы создать пользовательскую учетную запись, выполнить следующие действия:

1. Открыть оснастку «Active Directory – пользователи и компьютеры». Для этого нужно открыть панель управления, в ней открыть раздел «Система и безопасность», затем «Администрирование» и в появившемся окне открыть оснастку «Active Directory – пользователи и компьютеры». Также можно воспользоваться комбинацией клавиш +R для открытия диалога «Выполнить» и в диалоговом окне «Выполнить», в поле «Открыть» ввести dsa.msc, а затем нажать на кнопку «ОК»;

2. В дереве оснастки, развернуть узел домена и перейти к подразделению, в котором будет создаваться пользовательская учетная запись. Для создания пользовательских учетных записей рекомендуется создавать дополнительные подразделения, после чего добавлять учетные записи пользователей в подразделения, отличающиеся от стандартного подразделения Users. Щелкнуть на этом подразделении правой кнопкой мыши и из контекстного меню выбрать команду «Создать», а затем «Пользователь».
3. В появившемся диалоговом окне «Новый объект - Пользователь» ввести следующую информацию:
 - В поле «Имя» имя пользователя;
 - В поле «Инициалы» ввести инициалы (чаще всего инициалы не используются);
 - В поле «Фамилия» ввести фамилию создаваемого пользователя;
 - Поле «Полное имя» используется для создания таких атрибутов создаваемого объекта, как основное имя (Common Name) CN и отображения свойств имени. Это поле должно быть уникальным во всем домене, и заполняется автоматически, а изменять его стоит лишь в случае необходимости;
 - Поле «Имя входа пользователя» является обязательным и предназначено для имени входа пользователя в домен. Здесь нам нужно ввести имя пользователя и из раскрывающегося списка выбрать суффикс UPN, который будет расположен после символа @;
 - Поле «Имя входа пользователя (Пред-Windows 2000)» предназначено для имени входа для систем предшествующих операционной системе Windows 2000. В последние годы в организациях все реже встречаются обладатели таких систем, но поле обязательно, так как некоторое программное обеспечение для идентификации пользователей использует именно этот атрибут;

После того как все требуемые поля заполнены, нажать кнопку Далее.

4. На следующей странице мастера создания пользовательской учетной записи ввести начальный пароль пользователя в поле «Пароль» и подтвердить его в поле «Подтверждение». Помимо этого, можно

выбрать атрибут, указывающий на то, что при первом входе пользователя в систему пользователь должен самостоятельно изменить пароль для своей учетной записи. Лучше всего использовать эту опцию в связке с локальными политиками безопасности «Политика паролей», что позволит создавать надежные пароли для пользователей. Также, установив флажок на опции «Запретить смену пароля пользователем» предоставляется пользователю нужный пароль и запрещается его изменять. При выборе опции «Срок действия пароля не ограничен» у пароля учетной записи пользователя срок действия пароля никогда не истечет и не будет необходимости в его периодическом изменении. Если установить флажок «Отключить учетную запись», то данная учетная запись будет не предназначена для дальнейшей работы и пользователь с такой учетной записью не сможет выполнить вход до ее включения. После выбора всех атрибутов, нажать кнопку «Далее». На последней странице мастера представлена сводная информация о введенных параметрах. Если информация внесена корректно, нажать на кнопку «Готово» для создания пользовательской учетной записи и завершения работы мастера.

3.3 Создание пользователей на основании шаблонов

Обычно в организациях существует несколько подразделений или отделов, в которые входят пользователи. В подразделениях пользователи обладают схожими свойствами (например, название отдела, должности, номер кабинета и пр.). Для наиболее эффективного управления учетными записями пользователей из одного подразделения, например, используя групповые политики, целесообразно их создавать внутри домена в специальных подразделениях (иначе говоря, контейнерах) на основании шаблонов.

Шаблоном учетной записи называется учетная запись, впервые появившаяся еще во времена операционных систем Windows[®] NT, в которой заранее заполнены общие для всех создаваемых пользователей атрибуты. Для того чтобы создать шаблон учетной записи пользователя, выполнить следующие действия:

1. Открыть оснастку «Active Directory – пользователи и компьютеры» и создать стандартную учетную запись пользователя. При создании стандартной учетной записи желательно чтобы в списке пользователей в подразделении имя данной записи выделялось из

общего списка, и всегда было расположено на видном месте. Например, чтобы учетная запись всегда находилась первой, задать для создаваемого шаблона имя с нижними подчеркиваниями, например, Маркетинг. Также, на странице ввода пароля устанавливаем флажок «Отключить учетную запись». Так как эта запись будет использоваться только в качестве шаблона, она должна быть отключена;

2. В области сведений оснастки выбрать созданную учетную запись (значок объекта данной учетной записи будет содержать стрелку, направленную вниз, что означает, что данная учетная запись отключена), нажать на ней правой кнопкой мыши и из контекстного меню выбрать команду «Свойства»;
3. Для того чтобы некоторые атрибуты скопировались в свойствах учетных записей пользователей, которые в последствии будут создаваться на основании шаблона, нужно заполнить необходимые поля в свойствах шаблона учетной записи.

Чаще всего при редактировании свойств учетных записей используются вкладки:

- Общие. Данная вкладка предназначена для заполнения индивидуальных пользовательских атрибутов. К этим атрибутам относятся имя пользователя и его фамилия, краткое описание для учетной записи, контактный телефон пользователя, номер комнаты, его электронный ящик, а также веб-сайт. Ввиду того, что данная информация является индивидуальной для каждого отдельного пользователя, данные заполненные на этой вкладке не копируются;
- Адрес. На текущей вкладке можно заполнить почтовый ящик, город, область, почтовый индекс и страну, где проживают пользователи, которые будут созданы на основании данного шаблона. Так как у каждого пользователя названия улиц обычно не совпадают, данные из этого поля не подлежат копированию;
- Учетная запись. В этой вкладке можно указать точно время входа пользователя, компьютеры, на которые смогут заходить пользователи, такие параметры учетных записей как хранение паролей, типы шифрования и пр., а также срок действия учетной записи;

- Профиль. Текущая вкладка позволяет указать путь к профилю, сценарий входа, локальный путь к домашней папке, а также сетевые диски, на которых будет размещена домашняя папка учетной записи;
- Организация. На этой вкладке можно указать должность сотрудников, отдел, в котором они работают, название организации, а также имя руководителя отдела;
- Члены групп. Здесь указывается основная группа и членство в группах. Это основные вкладки, которые заполняются при создании шаблонов учетной записи. Помимо вышеуказанных вкладок, можно заполнять данные на остальных вкладках.
- На следующем шаге создается учетная запись пользователя, основанная на текущем шаблоне. Для этого нажать правой кнопкой мыши на шаблоне учетной записи и из контекстного меню выбрать команду «Копировать»;
- В диалоговом окне «Копировать объект - Пользователь» ввести имя, фамилию, а также имя входа пользователя. На следующей странице ввести пароль и подтверждение, снять флажок с опции «Отключить учетную запись». Завершить работу мастера;

После создания учетной записи перейти в свойства созданной учетной записи и просмотреть добавленные свойства в шаблон. Отконфигурованные атрибуты будут скопированы в новую учетную запись.

3.4 Учетные записи групп пользователей

Несмотря на то, что доступ к сетевым ресурсам основан на учетных записях отдельных пользователей, компьютеров или служб, со временем состав учетных записей может меняться. В средних и крупных компаниях управление существующими пользователями требует большой административной нагрузки.

Стоит учесть, что пользователи, выполняющие в компании конкретную роль, могут меняться, но сама роль должна оставаться без каких-либо изменений.

Если назначать доступ к сетевым ресурсами индивидуально для каждого отдельного пользователя, то списки контроля доступа ACL вскоре станут неуправляемыми и при изменении отдела пользователем нужно будет учесть все возможные разрешения доступа.

Так как этот процесс может легко выйти из-под контроля, задачи, связанные с управлением должны быть привязаны к объектам групп.

Чаще всего группы используются для идентификации ролей пользователей и компьютеров, фильтрации групповой политики, назначения уникальных политик паролей, прав, разрешений доступа, приложений электронной почты и многое другое.

Группы представляют собой объекты с уникальными SID, которые могут содержать в атрибуте member такие пункты, как пользователи, компьютеры, группы и контакты.

Так как структура доменных служб предназначена для поддержки сложных и крупных распределенных сред, Active Directory включает в себя два типа групп домена с тремя областями действия в каждой из них, а также локальную группу безопасности.

Типы групп:

В доменных службах Active Directory Windows Server® 2008 существуют два типа групп: безопасности и распространения.

При создании новой группы в диалоговом окне «Новый объект - группа» оснастки «Active Directory – пользователи и компьютеры» можно выбрать одну из этих двух групп.

Группы безопасности относятся к объектам с SID-идентификаторами. В связи с этим данный тип группы считается самым распространенным и группы такого типа можно использовать для управления безопасностью и назначения разрешений доступа к сетевым ресурсам в списках ACL.

Группу безопасности стоит использовать в том случае, если они будут использоваться для управления безопасностью.

В свою очередь, группа распространения изначально используется приложениями электронной почты. Этот тип группы не является субъектом безопасности и не содержит SID-идентификатор.

Так как группу распространения нельзя использовать для назначения доступа к ресурсам, она чаще всего используется при установке Microsoft Exchange Server в том случае, когда пользователей необходимо объединить в группу с целью отправки электронной почты сразу всей группе.

Ввиду того, что именно группы безопасности можно использовать как с целью назначения доступа к ресурсам, так и с целью распространения электронной почты, многие организации используют только этот тип группы.

В домене с функциональным уровнем не ниже Windows® 2000 можно преобразовывать группы безопасности в группы распространения и наоборот.

Область действия групп:

Область действия группы определяет часть сети, в которой применяется группа внутри домена.

Помимо того, что группы могут содержать пользователей и компьютеры, они могут быть членами других групп, ссылаться на списки ACL, фильтры объектов и групповых политик и пр.

Граница области действия группы может определяться заданием режима работы домена.

К основным характеристикам области действия групп можно отнести членство (определение принципалов безопасности, которые может содержать группа), репликация (определение области репликации группы), а также доступность (определение местонахождения группы, возможности включения этой группы в членство другой, добавление группы в список ACL).

Существует четыре области действия групп: локальные доменные группы (domain local), встроенные локальные группы (built-in-local), глобальные (global) и универсальные (universal) группы. Рассмотрим подробнее каждую из них:

- Локальные доменные группы. Используются, в основном, для предоставления доступа к ресурсам внутри одного домена. В локальные доменные группы можно включать членов любого домена в лесу, а также членов доверенных доменов в других лесах. Как правило, членами локальных доменных групп являются глобальные и универсальные группы.
- Встроенные группы домена. Группы с особой областью действия, обладающие локальными разрешениями в домене. Для простоты их часто объединяют с локальными доменными группами. Отличие встроенных групп состоит в том, что их нельзя создавать и удалять. Все сказанное о локальных доменных группах применимо и к встроенным локальным группам, если не оговорено иное.
- Глобальные группы. В основном, используются для определения наборов пользователей или компьютеров в пределах одного домена, выполняющих сходную роль, функцию или работу.

Членами глобальной группы могут быть только учетные записи или группы домена, в котором она определена.

- Универсальные группы. В основном, используются для определения наборов пользователей или компьютеров, которым требуется широкий спектр разрешений в домене или лесе. Членами универсальных групп могут быть учетные записи, глобальные группы и другие универсальные группы из любого домена дерева или леса. Универсальные группы безопасности доступны только при работе Active Directory в основном режиме Windows 2000 или в режиме Windows Server® 2008. Универсальные группы распространения доступны в любом режиме работы домена. Универсальные группы полезны в больших предприятиях с несколькими доменами. Не следует часто менять членов универсальных групп, т.к. при каждом изменении членов универсальной группы следует реплицировать изменения во все глобальные каталоги доменного дерева или леса. Для сокращения объема изменений, рекомендуется добавлять в универсальную группу другие группы, а не пользователей.

После создания группы, ее область действия можно изменить на вкладке «Общие» диалогового окна свойств группы, одним из следующих доступных способов:

- Глобальную группу в универсальную в том случае, если изменяемая группа не является членом другой глобальной группы;
- Локальную группу в домене в универсальную в том случае, если эта группа не содержит другую локальную группу в домене в качестве члена;
- Универсальную группу в глобальную в том случае, если эта группа не содержит в качестве члена другую универсальную группу;
- Универсальную группу в локальную группу в домене.

Глобальную группу просто так невозможно модифицировать в локальную группу в домене.

Несмотря на это, можно сначала глобальную группу преобразовать в универсальную, а затем уже получившуюся универсальную группу в локальную группу в домене.

3.5 Создание групп при помощи оснастки «Active Directory – пользователи и компьютеры»

Как и учетные записи пользователей, создавать группы проще, используя функционал оснастки «Active Directory – пользователи и компьютеры».

Эта оснастка обладает графическим интерфейсом, который позволяет корректно создать группу любого типа и с любой областью действия.

Для того чтобы создать группу при помощи данной оснастки, нужно выполнить следующие действия:

1. Открыть оснастку «Active Directory – пользователи и компьютеры». Для этого нужно открыть панель управления, в ней открыть раздел «Система и безопасность», затем «Администрирование» и в появившемся окне открыть оснастку «Active Directory – пользователи и компьютеры». Также можно воспользоваться комбинацией клавиш +R для открытия диалога «Выполнить» и в диалоговом окне «Выполнить», в поле «Открыть» ввести `dsa.msc`, а затем нажать на кнопку «ОК»;
2. В дереве оснастки, развернуть узел домена и перейти к подразделению, в котором будет создаваться пользовательская учетная запись. Для создания пользовательских учетных записей рекомендуется создавать дополнительные подразделения, после чего добавлять учетные записи пользователей в подразделения, отличающиеся от стандартного подразделения Users. Щелкнуть это подразделение правой кнопкой мыши и из контекстного меню выбрать команду «Создать», а затем «Группа».
3. В отобразившемся диалоговом окне «Новый объект - Группа», в поле «Имя группы» ввести смысловое название группы, которое будет отображаться в области сведений оснастки. Желательно, чтобы имена в обоих полях были идентичными. В группе «Тип группы» выбрать тип группы, а в группе «Область действия группы», соответственно, область действия группы. По умолчанию переключатели установлены так, что будет создана глобальная группа безопасности. После того как вся информация будет задана, нажать кнопку «ОК».

Тема 4. Понятие и управление групповыми политиками

Групповые политики упрощают администрирование, позволяя централизованно управлять полномочиям, разрешениями и возможностями пользователей и компьютеров. При помощи групповых политик можно:

- Управлять доступом к компонентам Windows[®], системным и сетевым ресурсам, утилитам панели управления, рабочему столу и меню Пуск.
- Создавать централизованно управляемые каталоги для специальных папок. Например, папок документов пользователя.
- Создавать сценарии пользователя и компьютера для запуска в определенные моменты.
- Настраивать политики учетных записей, паролей, аудита, назначения прав пользователей и безопасности.

Групповую политику можно считать набором правил управления пользователями и компьютерами. Групповые политики применяются к группам доменов, к отдельным доменам, к подмножествам компьютеров домена и к отдельным компьютерам. Политика, применяемая к конкретному компьютеру, называется локальной групповой политикой (local group policy) и хранится только на соответствующем компьютере. Другие групповые политики хранятся как объекты хранилища данных Active Directory и называются нелокальными.

Параметры групповой политики хранятся в объекте групповой политики (Group Policy Object, GPO) – контейнере для применяемых политик и их параметров. К одному и тому же сайту, домену или подразделению можно применить несколько GPO. К GPO применимо наследование, т.е. от родительского контейнера к дочернему контейнеру. Порядок наследования таков: сайт – домен – подразделение. То есть, параметры групповой политики сайта передаются доменам этого сайта и далее подразделениям этих доменов.

Порядок применения групповых политик:

1. Локальные групповые политики.
2. Групповые политики сайта.
3. Групповые политики домена.
4. Групповые политики подразделения.
5. Групповые политики дочернего подразделения.

Если параметры различных политик конфликтуют друг с другом, приоритет отдается параметрам, примененным позже.

По умолчанию групповые политики обновляются в 4 случаях:

1. При выходе пользователя из системы.
2. При перезапуске компьютера.
3. По истечении интервала обновления.
4. По команде командной строки `gpupdate`.

4.1 Управление политиками сайта, домена, подразделения

В каждом домене Active Directory по умолчанию имеется два объекта групповых политик:

1. Политика контроллера домена по умолчанию
2. Политика домена по умолчанию

Политика контроллера домена по умолчанию применима ко всем контроллерам домена и применяется для управления их параметрами безопасности.

Политика домена по умолчанию политика применяется для домена Active Directory в целом.

Политика домена по умолчанию применяется только для управления стандартными параметрами политик учетных записей: политик паролей, политик блокировки учетных записей.

Перекрыть политику домена по умолчанию, можно создав новый GPO с другими значениями и связав его с контроллером домена более высокого приоритета.

В политику контроллера домена по умолчанию включены права пользователей и параметры использования контроллера домена.

Перекрыть эти политики можно, создав новый GPO с другими значениями и связав его с более высокоприоритетным контроллером домена.

Управление групповыми политиками производится через управление групповой политикой, которая находится в меню администрирование. Редактор групповых политик имеет две части окна – слева дерево папок, справа область сведений.

Любая GPO состоит из двух узлов:

1. Конфигурация компьютера
2. Конфигурация пользователя

Каждый из этих узлов содержит три подузла:

1. Конфигурация программ. Содержит политики программного обеспечения и установки программного обеспечения.
2. Конфигурация Windows. Содержит политики перенаправления папок, сценарии и параметры безопасности.
3. Административные шаблоны. Содержит компоненты Windows, меню пуск, контроль управления, рабочий стол, сеть, система.

Политики в шаблонах находятся в одном из трех состояний: не задан, включен, отключен.

Создав GPO, его необходимо связать с контейнером AD.

Полномочия по управлению групповыми политиками имеют все администраторы.

Наследование политик может быть изменено следующими способами:

1. Изменением порядка и приоритета связей.
2. Перекрытием наследования, если не задано принудительное выполнение.
3. Блокировкой наследования.
4. Заданием принудительного наследования, отменяющее перекрытие и блокировку.

Администратор домена может применить блокировку, чтобы запретить наследование политик уровня сайта.

Администратор сайта может задать принудительное наследование, чтобы администратор домена не блокировал его политики.

4.2 Создание объекта групповой политики

Один или несколько параметров групповой политики, который применяется к одному или нескольким пользователям или компьютерам, обеспечивая конкретную конфигурацию, называется объектом групповой политики.

Для того чтобы создать новый объект групповой политики, выполнить следующие действия:

1. В оснастке «Управление групповой политикой» развернуть узел лес, домен, название домена и выбрать контейнер «Объекты групповой политики». Именно в этом контейнере будут храниться все объекты групповой политики, которые будут созданы;
2. Щелкнуть правой кнопкой мыши на данном контейнере и из контекстного меню выбрать команду «Создать»:

3. В диалоговом окне «Новый объект групповой политики» ввести название объекта в поле «Имя», например, «Корпоративные требования» и нажать кнопку «ОК».

4.3 Редактирование объекта групповой политики

После создания объекта групповой политики, для того чтобы настроить определенную конфигурацию данного объекта, нужно указать параметры групповой политики при помощи оснастки «Редактор управления групповыми политиками».

Например, необходимо отключить Windows Media Center, средство звукозаписи, а также ссылку «Игры» в меню «Пуск». Для этого выполнить следующие действия:

1. Выделить созданный ранее объект групповой политики, нажать на нем правой кнопкой мыши и из контекстного меню выбрать команду «Изменить»;
2. Развернуть узел Конфигурация пользователя/ Политики/ Административные шаблоны/ Компоненты Windows/ Windows Media Center;
3. Открыть свойства параметра политики «Не запускать Windows Media Center» и установить переключатель на опцию «Включить». В поле комментарий ввести комментарий, например, «В связи с корпоративными требованиями не разрешается данным пользователям использовать текущее приложение» и нажать кнопку «ОК».
4. Повторить аналогичные действия для параметров политик «Запретить выполнение программы «Звукозапись»» и «Удалить ссылку «Игры» из меню «Пуск»» из узла Конфигурация пользователя/Политики/Административные шаблоны/Меню «Пуск» и панель задач.
5. Закрыть редактор управления групповыми политиками.

4.4 Поиск и удаление объектов групповой политики

При развертывании групповых политик в организации могут быть созданы десятки, а то и сотни объектов групповых политик. Если в организации есть только один домен, то обнаружить необходимый объект групповых политик много времени не займет. Но как быть, если в лесу организации развернуто несколько доменов? Для этого имеется функционал поиска объектов групповых политик. Для того чтобы найти

существующий объект групповой политики, выполнить следующие действия:

1. В дереве консоли оснастки «Управление групповой политикой» щелкнуть правой кнопкой мыши на лесе (или если известно, в каком домене нужно провести поиск объекта, то можно вызвать контекстное меню для конкретного домена) и из контекстного меню выбрать команду «Найти»;
2. В диалоговом окне «Поиск объектов групповой политики» в раскрывающемся списке «Искать объекты групповой политики в домене» можно выбрать домен, для которого будет производиться поиск или оставить значение, используемое по умолчанию;
3. В раскрывающемся списке «Элемент поиска», выбрать тип объекта, для которого будет выполняться поиск. В этом случае нужно выбрать элемент «Имя объекта групповой политики»;
4. Раскрывающийся список «Условие» позволяет выбрать условие для поиска. Доступные варианты «Содержит», «Не содержит» и «совпадает». При выборе условия «совпадает» нужно ввести точное название политики. В противном случае поиск закончится ошибкой;
5. В поле «Значение» ввести значение, которое будет использовано для фильтрации поиска. Если результаты предыдущего поиска были сохранены, то значение можно будет выбрать из раскрывающегося списка;
6. Нажать кнопку «Добавить» для выбора условия поиска;
7. По нажатию кнопки «Найти» будут выведены все результаты, согласно условиям поиска.
8. Для того чтобы сразу перейти к оснастке «Редактор управления групповыми политиками» нажать кнопку «Изменить», для сохранения текущих результатов поиска нажать кнопку «Сохранить результаты» (результаты будут сохранены в указанной папке с расширением *.csv). По нажатию кнопку «Очистить», результаты поиска будут очищены без сохранения, а для закрытия данного диалога нажать кнопку «Закрыть» или «Esc».

При работе с объектами групповых политик когда-нибудь понадобится удалить существующий объект GPO. Для этого необходимо выбрать объект групповой политики и выполнить одно из следующих действий:

- Нажать клавишу «Delete» и в диалоговом окне «Управление групповой политикой» нажимаем на кнопку «Да»;

- Нажать на кнопку «Удалить» (в виде красного креста) на панели инструментов, а затем в диалоговом окне «Управление групповой политикой» нажать кнопку «Да»;
- Нажать правой кнопкой мыши на объекте групповой политики и из контекстного меню выбрать команду «Удалить». Затем в диалоговом окне «Управление групповой политикой» нажать кнопку «Да»

Тема 5. Предоставление общего доступа к файлам сервера

Способ, которым осуществляется совместное использование файлов, определяется параметрами общего доступа. В Windows Server® 2008 существуют две модели совместного использования файлов:

- Обычный общий доступ. Позволяет удаленным пользователям обращаться к файлам, папкам и дискам по сети. Предоставляя общий доступ к папке или диску, мы делаем все содержащиеся в них файлы и подпапки доступными для определенного круга пользователей. Регулировать доступ к совместно используемым файлам позволяют разрешения общего ресурса и разрешения NTFS. Общий доступ можно организовать также на съемных носителях отформатированных в FAT и на любых дисках в формате NTFS. К съемным дискам в FAT применяется единственный набор полномочий – это разрешение общего ресурса. К дискам NTFS применяются два набора полномочий: разрешение NTFS и разрешения общего ресурса.
- Общий доступ к файлам из папки «Общие» (Public). Позволяет всем локальным, а при необходимости, и удаленным пользователям обращаться ко всем файлам, расположенным в папке «Общие». Для определения списка пользователей и групп, которые имеют доступ к файлам этой папки, а так же уровень доступа, используются разрешения доступа для папки Общие.

Обычный общий доступ не подразумевает автоматического доступа ко всем хранящимся на компьютере данным. Управление локальным доступом к файлам и папкам осуществляется с помощью параметров безопасности на локальном диске. При использовании папки «Общие», скопированные или перемещенные в папку файлы доступны каждому, кто вошел в систему локально. К папке «Общие» можно также открыть сетевой доступ. Это приведет к тому, что папка «Общие» и ее содержимое

будут открыты каждому, кто может получить сетевой доступ к компьютеру.

Для управления конфигурацией совместного доступа на компьютере выполнить::

1. Открыть Центр управления сетями и общим доступом (Network And Sharing Center), щелкнув Пуск и Сеть, а затем на панели инструментов консоли Сеть щелкнуть команду Центр управления сетями и общим доступом.
2. Элемент Общий доступ к файлам (File Sharing) управляет сетевым доступом к общим ресурсам. Чтобы настроить обычный общий доступ, щелкнуть кнопку со стрелкой соответствующую элементу Общий доступ к файлам. Выполнить можно одно из следующих действий:
 - Включить общий доступ к файлам (Turn On File Sharing)
 - Отключить общий доступ к файлам (Turn Off File Sharing)
3. Чтобы настроить общий доступ к папке Общие (Public), щелкнуть кнопку со стрелкой, соответствующую элементу Общий доступ к общим папкам (Public Folder Sharing). Выполнить можно одно из следующих действий:
 - Включить общий доступ, чтобы сетевые пользователи могли открывать файлы.
 - Включить общий доступ, чтобы сетевые пользователи могли открывать, изменять и создавать файлы.
 - Отключить общий доступ.
4. Элемент Использование общих принтеров (Printer Sharing) управляет доступом к принтерам компьютера. Для настройки общего доступа к принтерам щелкнуть соответствующую кнопку со стрелкой. Выполнить можно одно из следующих действий:
 - Включить общий доступ к принтерам (Turn On Printer Sharing)
 - Выключить общий доступ к принтерам (Turn Off Printer Sharing)
5. Пароль позволяет ограничить доступ в пределах рабочей группы, так что доступ к общим ресурсам будет только у пользователей, имеющих учетную запись и пароль на этом компьютере. Чтобы настроить общий доступ, защищенный паролем, щелкнуть кнопку со стрелкой, соответствующую элементу Общий доступ с парольной

защитой (Password Protected Sharing). Выполнить можно одно из следующих действий:

- Включить общий доступ с парольной защитой (Select Turn On Password Sharing)
- Отключить общий доступ с парольной защитой (Select Turn Off Password Protected Sharing)

Система Windows Server[®] 2008 позволяет открывать общий доступ к папкам несколькими способами:

1. При помощи Проводника Windows[®] (Windows Explorer)
2. При помощи консоли Управление компьютером (Computer Management)
3. При помощи консоли Управление общими ресурсами и хранилищами (Share And Storage Management).

5.1 Создание общего ресурса с помощью Проводника

Для того чтобы дать доступ к любой папке, расположенной на компьютере и указать пользователей с различными правами, которые будут иметь к ней доступ выполнить следующее:

1. Создать папку, для которой будет предоставлен общий доступ, например, папку «папка1» на диске С;
2. Открыть проводник Windows[®], выделить ее, нажать на ней правой кнопкой мыши и из контекстного меню выбрать команду «Свойства»;
3. В диалоговом окне «Свойства: папка1» перейти на вкладку «Доступ»;
4. Нажать кнопку «Общий доступ» для предоставления разрешений пользователя и группам.

В диалоговом окне «Общий доступ к файлам» по умолчанию владелец папки имеет к ней полный доступ и называется «Владелец». Можно добавить любого существующего пользователя, который был создан на компьютере. Существующих пользователей можно найти в оснастке «Локальные пользователи и группы». Для примера, на компьютере был создан пользователь «user».

Для предоставления пользователю доступа, в раскрывающемся списке диалогового окна «Общий доступ к файлам» ввести имя пользователя или выбрать его из списка и нажать на кнопку «Добавить». Любому добавленному пользователю можно присвоить права «Читатель», «Соавтор» или «Совладелец».

- Пользователь с уровнем прав «Читатель» – может просматривать файлы данного ресурса.
- Пользователь с уровнем прав «Соавтор» – может просматривать файлы и добавлять новые; редактировать и удалять добавленные им файлы
- Пользователь с уровнем прав «Совладелец» – может читать, редактировать, добавлять и удалять любые файлы в общей папке

Выбрав разрешения для пользователей, нажать кнопку «Общий доступ».

5. В диалоговом окне «Папка открыта для общего доступа», нажать кнопку «Готово»
6. Для предоставления дополнительных настроек для общедоступной папки, в диалоговом окне «Доступ» свойств папки, нажать кнопку «Дополнительный доступ».

В диалоговом окне «Дополнительный доступ» можно изменять следующие настройки:

- Изменять отображаемое имя общей папки. Для этого нажимаем на кнопку «Добавить». В диалоговом окне «Новый общий ресурс» ввести имя и, по желанию, описание ресурса и нажать кнопку «ОК». Для того чтобы у подключенных пользователей отображалось только указанное имя общего ресурса – из списка выбрать оригинальное название папки и нажать кнопку «Удалить»;
 - Ограничивать количество одновременных подключений к общему ресурсу. Например, если в нашей локальной сети только пять компьютеров, мы можем изменить количество пользователей, которые могут одновременно использовать ресурс;
 - Настраивать разрешения для папки и настройки автономного режима.
7. Установить флажок напротив пункта «Открыть общий доступ к этой папке».
 8. Обычный общий доступ и дополнительный общий доступ связаны, и если в первом, для какого-либо пользователя, выставлены права превышающие «Чтение», то в дополнительном общем доступе необходимо добавить требуемого пользователя и назначить ему

аналогичные разрешения, т.к. по умолчанию в дополнительном доступе присутствуют только разрешения на чтение для всех.

По окончании настроек общего доступа для папки нажать кнопку «Закрывать». Общий ресурс создан.

5.2 Создание общего ресурса с помощью консоли «Управление компьютером»

Чтобы создать общий ресурс при помощи консоли Управление компьютером необходимо выполнить следующие действия:

1. В дереве консоли последовательно развернуть узлы: Служебные программы, Общие папки, а затем выбрать элемент Общие ресурсы (Shares). На экране отобразятся текущие общие ресурсы системы.
2. Щелкнуть правой кнопкой элемент Общие ресурсы и выбрать команду Новый общий ресурс (New Share). Откроется мастер создания общей папки. Щелкнуть Далее.
3. В поле «Путь к папке» ввести локальный путь папки, к которой требуется открыть общий доступ. Путь должен быть полным. Если не известен полный путь, щелкнуть кнопку Обзор, чтобы найти папку в диалоговом окне Обзор папок. Щелкнуть ОК и Далее.
4. В поле Общий ресурс ввести имя общего ресурса. Это имя папки, по которому к ней будут подключаться пользователи. В каждой системе имена общих ресурсов должны быть уникальными.
5. При необходимости ввести описание общего ресурса в поле Описание. Позже, во время просмотра общих ресурсов на компьютере, описание отображается в консоли Управление компьютером.
6. По умолчанию в автономном режиме доступны только указанные пользователем файлы и программы. Если нужно запретить автономное использование файлов или, напротив, разрешить автономное использование файлов и программ, щелкнуть кнопку «Изменить» и задать нужные параметры в диалоговом окне Настройка автономного режима (Offline Settings).
7. Щелкнуть «Далее» и задать базовые разрешения для общего ресурса:
 - У всех пользователей доступ только для чтения (All Users Have Read-Only Access). Предоставляет пользователям доступ для просмотра файлов и чтения.
 - Администраторы имеют полный доступ, остальные – доступ только для чтения (Administrators Have Full Access; Other Users

Have Read-Only Access). Предоставляет администраторам полный контроль над общим ресурсом. Они могут создавать, изменять и удалять файлы и папки.

- Администраторы имеют полный доступ, остальные не имеют доступа (Administrators Have Full Access; Other Users Have No Access). Предоставляет администраторам полный контроль над общим ресурсом и запрещает доступ к нему другим пользователям.
- Настройка разрешений доступа (Customize Permissions). В большинстве случаев это оптимальный вариант настройки, позволяющий индивидуально управлять доступом отдельных пользователей и групп.

8. Щелкнуть кнопку Готово. На экране появится страница с отчетом: Ресурс успешно создан общим. Ещё раз щелкнуть «Готово».

5.3 Создание общего ресурса с помощью консоли «Управление общими ресурсами и хранилищами»

Одной из лучших функций инструмента Управление общими ресурсами и хранилищами является инициализация мастера настройки общих папок (Provision a Shared Folder Wizard).

Мастер упрощает работу администраторам, задавая вопросы, на которые нужно ответить, после чего мастер выполняет все необходимые шаги.

Например, мастер помогает выбрать папку или том, к которому мы хотим предоставить общий доступ, задать протокол, предоставляющий доступ, определить NTFS разрешения для ресурса, настроить общие разрешения, опубликовать его в DFS, задать NFS разрешения (если применимо) и применить квоты хранения (если установлен диспетчер управления файловым сервером).

Для создания общего ресурса нужно сделать следующее:

1. Открыть пункт Администрирование, консоль Управление общими ресурсами и хранилищами. Для предоставления общего доступа к ресурсу нужно нажать «Действие», затем «Подготовить общий ресурс».
2. После появления мастера указать путь создания нового ресурса.
3. Появляется диалоговое окно с возможностью выбора NTFS разрешений. Выбрать пункт Да, изменить разрешения NTFS, и добавить тех пользователей и группы, которым хотим предоставить

- общий доступ, а так же установить им нужные права доступа к ресурсу (чтение, изменение или полный доступ).
4. Далее появится диалоговое окно выбора протокола общего доступа. SMB является единственной опцией, если не установлена служба для NFS. Служба NFS представляет собой решение совместного использования файлов на предприятиях со смешанной средой операционных систем Windows и UNIX, которая позволяет перемещать файлы между ОС Windows Server 2008 и UNIX при помощи протокола NFS. Нажать «Далее».
 5. Определить SMB параметры, такие как лимит пользователей, перечисление доступа и параметры автономного режима. Нажать «Далее».
 6. Далее мастер попросит задать SMB разрешения этого нового ресурса. Здесь будет предоставлено несколько быстрых опций для облегчения работы:
 - Все пользователи и группы имеют доступ только на чтение
 - Администраторы имеют полный доступ; все остальные пользователи и группы имеют доступ только на чтение.
 - Администраторы имеют полный доступ; все остальные пользователи и группы имеют доступ на чтение и на запись.
 - Пользователи и группы имеют особые разрешения для общего ресурса. Здесь можно вручную добавить конкретных пользователей и группы, и назначить им нужные разрешения SMB.
 7. Если используется DFS, то нужно будет настроить DFS пространство имен для нового ресурса. Пространства имен DFS предоставляют возможность объединения общих папок, находящихся на разных серверах, в одно или несколько логически структурированных пространств имен. Каждое пространство имен представляется пользователям как одна общая папка с серией вложенных папок. Однако базовая структура пространства имен может состоять из многочисленных общих папок, которые находятся на разных серверах и в нескольких узлах. Эта структура повышает доступность и обеспечивает автоматическое подключение пользователей к общим папкам на одном и том же сайте доменных служб Active Directory, когда он доступен, вместо маршрутизации пользователей по подключениям глобальной сети.

8. Появляется окно, оповещающее о том, что ресурс успешно создан. Нажать «Закреть».

Во вкладке Общие ресурсы появилась только что созданная общая папка. Из этой вкладки можно просматривать общие ресурсы, удалять общий доступ, а так же редактировать ресурсы.

Тема 6. Резервное копирование и восстановление данных

Для защиты данных предприятия нужно уметь настраивать расписание архивации и восстановления.

Архивация – это средство защиты данных от случайной потери, повреждения БД, аппаратных сбоев и даже стихийных бедствий. В задачу администратора входит создание и безопасное хранение резервных копий. Система архивации данных Windows Server (Windows Server Backup) – это один из компонентов операционной системы Windows Server® 2008, позволяющий выполнять основные задачи, связанные с резервным копированием и восстановлением данных на том сервере, на котором этот компонент установлен. Данная система резервного копирования пришла на смену той, что использовалась в предыдущих версиях ОС Microsoft® Windows®.

Система резервного копирования – это один из дополнительных компонентов операционной системы Windows Server 2008, позволяющий выполнять надежное резервное копирование и восстановление операционной системы, а также файлов и папок, расположенных на сервере.

В состав системы резервного копирования входит соответствующая оснастка консоли MMC, а также средства командной строки.

Существует много способов архивации файлов. Какой способ выбрать, зависит от типа копируемых данных, от того, насколько удобным должен быть процесс восстановления и т.д.

В свойствах файла или папки в Проводнике Windows®, можно увидеть атрибут Архивный. Он часто используется, чтобы определить, следует ли выполнять архивацию файла или папки. Если этот атрибут задан, файл или папка нуждаются в архивации.

Существуют следующие основные типы архивации:

- Нормальная, или полная архивация. Архивация всех выбранных файлов выполняется независимо от значения атрибута Архивный. После создания резервной копии файла атрибут Архивный снимается. В случае последующего изменения файла, этот

атрибут восстанавливается, указывая на необходимость архивации файла.

- Архивация копированием. Архивация всех выбранных файлов выполняется независимо от значения атрибута Архивный. В отличие от нормальной архивации атрибут Архивный после архивации не изменяется. Это позволяет впоследствии выполнять другие типы архивации.
- Разностная архивация. Создаются резервные копии файлов, изменившихся с момента последней нормальной архивации. Наличие атрибута Архивный указывает, что файл был изменен. Архивация выполняется только для файлов с этим атрибутом, на сам атрибут после архивации не сбрасывается. Это позволяет впоследствии выполнять другие типы архивации.
- Добавочная архивация. Создаются резервные копии файлов, изменившихся с момента последней нормальной или добавочной архивации. Наличие атрибута Архивный указывает, что файл был изменен. Архивация выполняется только для файлов с этим атрибутом. После создания резервной копии файла атрибут Архивный сбрасывается. Он восстанавливается после изменения файла, указывая на необходимость его архивации.
- Ежедневная архивация. Предназначена для архивации файлов на основании даты изменения. Если файл был изменен в день проведения архивации, будет создана его резервная копия. Значение атрибута «Архивный» не меняется.

6.1 Создание резервной копии

Для работы необходимо установить службу архивации и восстановления Windows, для этого выполняются следующие действия:

1. В консоли Диспетчер сервера выбираем узел Компоненты и щелкаем команду Добавить компоненты. Откроется Мастер добавления компонентов.
2. На странице Выбор компонентов установить флажок Возможности системы архивации данных Windows. При этом будут выбраны компоненты Система архивации данных Windows Server (Windows Server Backup) и Программы командной строки (Command-Line Tools). Нажать «Далее».
3. Нажать «Установить». По завершении установки щелкнуть «Заккрыть». После этого в меню Администрирование появится

команда Система архивации данных Windows Server.

После установки системы архивации необходимо настроить расписание задачи, которая будет делать архивную копию Раздела 1 (в нем находится Windows Server 2008 и Active Directory).

1. Установить расписание так, чтобы архив делался раз в неделю, например в воскресенье. Для этого запускается оснастка "Системы архивации данных Windows Server" и запускается расписание архивации. Если нужно создать один архив, то выбрать пункт «однократная архивация». После этого пропустить приветствие и нажать «Далее». Выбрать, как осуществлять резервное копирование (Весь сервер или настраиваемый). Поскольку в архив должен попадать только Раздел 1, выбрать «Настраиваемый». Открывается список разделов сервера, в котором должны снять флажки на всех разделах, кроме того, который содержит систему.
2. Выбрав, что будет архивироваться, перейти к настройке расписания.
3. Из окна тонко настроить расписание задачи нельзя, поэтому требуется оставить расписание по умолчанию. В дальнейшем расписание можно изменить.
4. Далее необходимо выбрать место хранения архива. Выбрать доступный раздел.
5. После чего запускается процесс форматирования, по окончании которого раздел пропадет из зоны видимости, т.к. его буква диска будет удалена.
6. Архивный раздел можно найти через оснастку «Управление дисками».
7. После окончания процесса необходимо несколько раз нажать «Далее».
8. Оставить все параметры «По умолчанию».
9. Настройка резервного копирования завершена. Остается подправить расписание запуска задачи.
10. Для этого открыть «Планировщик Заданий» в Панели управления, найти задачу, установить нужное время архивации.
11. Выбрать свойства задачи, где изменить расписание. Например, необходимо сделать запуск задачи каждое воскресенье.
12. После настройки, каждое воскресенье в 21:00 на отдельный раздел жесткого диска будет создаваться резервная копия «Раздела 1» содержащего системные файлы и базу Active Directory.

Рекомендуется периодически переносить архивы для хранения за пределы сервера и серверной, чтобы не остаться в случае пожара или других крупных неприятностей без сервера и архива одновременно.

Резервное копирование может проводить пользователь, состоящий в группе Administrators (Администраторы) или Backup Operators (Операторы архива). При этом, у членов группы Backup Operators при запуске оснастки Windows Server Backup будет дополнительно запрашиваться пароль (в окне User Account Control), т.к. эти операции относятся к рискованным.

6.2 Восстановление сервера из резервной копии

Запустить восстановление сервера можно несколькими путями, самый простой: загрузиться с установочного диска Windows Server® 2008. На этапе приглашения к установке, необходимо выбрать «Восстановление системы». После чего будет запущена среда «Windows RE».

Далее, мастер находит установленные операционные системы на жестких дисках и спрашивает, какую из них требуется восстанавливать. На этом этапе также можно подгрузить драйверы для жестких дисков, если в этом есть необходимость.

Остается запустить "Восстановление архива Windows Complete PC Restore". После запуска мастер архивации предложит самую свежую копию архива. Если не планируется использовать последний архив, то требуется выбрать «Восстановить другой архив».

Далее следует окна, которые оставляются неизменными. По завершению мастера запускается процесс восстановления, продолжительность которого зависит от быстродействия оборудования и размера раздела.

После окончания восстановления компьютер перезагрузится. И следующий запуск сервера уже произойдет в восстановленном состоянии.

Поскольку восстановление системы происходит путем перезаписи раздела, рекомендуется отделить раздел с пользовательскими файлами и приложениями. При раздельном хранении системы и пользовательских файлов, можно спокойно восстанавливать сервер, не опасаясь вернуть важные документы в состояние недельной давности.

Вопросы для самоподготовки

1. Каковы задачи администрирования сети?

2. Какие требования предъявляются к аппаратуре при инсталляции ОС?
3. Описать процесс инсталляции ОС.
4. В чем состоит первичная настройка сервера?
5. Каково назначение службы Active Directory MS Windows Server® 2008?
6. Описать установку службы Active Directory.
7. Учетные записи пользователей и их назначение.
8. Учетные записи групп и их назначение.
9. Настройка программной среды для определенного пользователя.
10. Профили пользователей и их назначение.
11. Что такое административные общие ресурсы?
12. В чем состоит наследование и владение ресурсами?
13. Что такое групповые политики, и каково их назначение?
14. Что такое общий доступ к файлам и каталогам?
15. Назвать разрешения для общего доступа к файлам и каталогам.
16. Назвать стандартные разрешения NTFS для файлов.
17. Назвать стандартные разрешения NTFS для каталогов.
18. Назначение и процесс архивирования системы.
19. Назначение и процесс восстановления системы.

Литература

- Уильям Р. Станек. Windows Server® 2008. Справочник администратора / Пер. с англ. – М.: Издательство «Русская редакция»; СПб.: БХВ-Петербург, 2009.-688 стр. : ил.
- Митч Таллоч. Знакомство с Windows Server® 2008, Пер. с англ. – М.: Издательство «Русская редакция»; СПб. : «БХВ-Петербург», 2008. – 400 стр. : ил.
- Макин Дж. К., Десаи Анил. Развертывание и настройка Windows Server® 2008. Учебный курс Microsoft / Пер. с англ. – М.: Издательство «Русская редакция», 2008. – 640 стр.: ил.
- Internet-ресурсы:
 - www.microsoft.com/ru/ru/
 - www.technet.microsoft.com/ru-ru
 - www.citforum.ru
 - www.intuit.ru
 - www.wikipedia.org



В 2009 году Университет стал победителем многоэтапного конкурса, в результате которого определены 12 ведущих университетов России, которым присвоена категория «Национальный исследовательский университет». Министерством образования и науки Российской Федерации была утверждена программа его развития на 2009–2018 годы. В 2011 году Университет получил наименование «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»

КАФЕДРА АППАРАТНО-ПРОГРАММНЫХ КОМПЛЕКСОВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Кафедра Аппаратно-программных комплексов вычислительной техники осуществляет переподготовку и повышение квалификации специалистов с широким спектром образовательных программ по следующим направлениям:

- **Системный инженер** - специалист по эксплуатации аппаратно-программных комплексов вычислительной техники
- **Системный администратор** - специалист по эксплуатации компьютерных сетей и сопровождению программ 1С:Предприятие
- **Обслуживание, диагностика и ремонт персональных компьютеров**
- **Администрирование вычислительных сетей**
- **Конфигурирование, администрирование и программирование в среде 1С:**

На кафедре ведется подготовка магистров по направлению 230100

«Информатика и вычислительная техника»:

магистерская программа – «**Системное администрирование аппаратно-программных комплексов и сетей**» **230100.68.13.**

Кафедра является выпускающей по направлению 230100 «Информатика и вычислительная техника» на факультете ВиЗО.

Светлана Михайловна Платунова

Администрирование вычислительных сетей
на базе MS Windows Server® 2008

Учебное пособие по курсу
«Администрирование вычислительных сетей»

В авторской редакции

Редакционно-издательский отдел Санкт-Петербургского национального
исследовательского университета информационных технологий, механики
и оптики

Зав. РИО

Н.Ф. Гусарова

Лицензия ИД № 00408 от 05.11.99

Подписано к печати

Заказ №

Тираж 100 экз.

Отпечатано на ризографе

Редакционно-издательский отдел
Санкт-Петербургского национального
исследовательского университета
информационных технологий, механики
и оптики
197101, Санкт-Петербург, Кронверкский пр., 49

