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 R2

Учебное пособие

Санкт-Петербург

2013

Платунова С. М. Администрирование вычислительных сетей на базе MS Winsows Server® 2008 R2. Учебное пособие по дисциплине «Администрирование вычислительных сетей». – СПб: НИУ ИТМО, 2013. – 127 с.

В учебном пособии содержатся основные сведения об администрировании вычислительных сетей на базе MS Winsows® 2008 R2, 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, политики безопасности, службы сетевой файловой системы, виртуализация.

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 № 7 от 12.12.2012

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»

ОГЛАВЛЕНИЕ

Обзор редакций ОС Windows Server® 2008 R2

Операционная система Windows Server® 2008 R2 расширяет базовые возможности операционной системы Windows Server® и предоставляет новые мощные средства, помогая организациям всех размеров повышать управляемость, доступность и гибкость в соответствии с изменяющимися требованиями бизнеса. Новые веб-средства, технологии виртуализации, средства управления и расширенные возможности масштабирования экономят время, снижают затраты и предоставляют надежную платформу для создания ИТ-инфраструктуры организации. Windows Server® 2008 R2 содержит новые и усовершенствованные средства и возможности в следующих пяти категориях[1].

1. Платформа веб-приложений

В сервер Windows Server® 2008 R2 включены множество усовершенствований, превращающих его в самую надежную платформу веб-приложений на основе Windows Server среди всех версий Windows. Он содержит обновленную роль веб-сервера и службы IIS 7.5 и обеспечивает расширенную поддержку .NET в режиме Server Core.

2. Виртуализация

Виртуализация играет важнейшую роль в работе современных центров обработки данных. Обеспечиваемое виртуализацией повышение эффективности работы позволяет организациям значительно снизить трудоемкость эксплуатации и энергопотребление. Windows Server® 2008 R2 поддерживает следующие типы виртуализации: виртуализацию клиентских и серверных систем с помощью Hyper-V и виртуализацию представлений с помощью служб удаленных рабочих столов.

3. Масштабируемость и надежность

Windows Server® 2008 R2 поддерживает недостижимые ранее объемы рабочих нагрузок, динамическую масштабируемость, доступность и надежность на всех уровнях, а также ряд других новых и обновленных возможностей, включая использование современных архитектур процессоров, повышение уровня компонентного представления операционной системы и повышение производительности и масштабируемости приложений и служб.

4. Управление

Постоянное управление серверами в центрах обработки данных — одна из тех задач, которые отнимают у ИТ-специалистов наибольшее время. Применяемая в организации стратегия управления должна поддерживать управление физическими и виртуальными средами. Чтобы помочь в решении этой задачи, в состав Windows Server 2008 R2 включены новые средства, уменьшающие тру-

доемкость управления серверами Windows Server® 2008 R2 и выполнения повседневных задач по администрированию серверов.

5. Совместная работа с Windows 7

Операционная система Windows Server® 2008 R2 поддерживает ряд функций, рассчитанных на работу с клиентскими компьютерами под управлением Windows 7.

Все редакции Windows Server® 2008 R2 поддерживают основные возможности, необходимые для решения задач, которые возникают в работе ИТ-систем и организаций любого размера. Основные особенности различных редакций Windows Server 2008 R2, которые поставляются совместно с серверами DEPO Storm.

Windows MultiPoint Server 2010 – продукт семейства Windows, при помощи которого несколько человек могут одновременно работать на одном компьютере. MultiPoint Server является идеальным решением для образовательных учреждений, поскольку предоставляет большему числу преподавателей и учащихся доступ к компьютерным технологиям, а также:

- сокращает начальные вложения в оборудование и текущие эксплуатационные расходы;
- сокращает потребление электроэнергии;
- упрощает управление ИТ-инфраструктурой.

Сравнительные характеристики различных редакций ОС Windows Server® 2008 R2 приведены в таблице.

Windows Server® 2008 R2 Foundation предназначена для небольших организаций, где рассматривается приобретение первого сервера или уже используется клиентская операционная система (например, Windows XP) для обеспечения базовой инфраструктуры. Это недорогая, удобная в развертывании и надежная платформа, на которой можно запускать распространенные бизнес-приложения и обеспечивать общий доступ к информации и ресурсам. Windows Server® 2008 R2 Foundation основан на Windows Server® 2008 R2 и сможет обеспечить все ключевые элементы ИТ в бизнесе: совместная работа с файлами и принтерами, удаленный доступ, безопасность ИТ среды.

Однако Windows Server® 2008 R2 Foundation имеет ограничения по количеству клиентских подключений и не поддерживает функции виртуализации.

Таблица 1 - Сравнительные характеристики различных редакций ОС Windows Server® 2008 R2

Технические характеристики	**MultiPoint Server (OEM)**	**Windows Server 2008 R2 Foundation**	**Windows Small Business Server 2008**	**Windows Server 2008 R2 Standard**	**Windows Server 2008 R2 Enterprise**

Количество CPU	1	1	4	4	8
Объем ОЗУ	8 Гб	8 Гб	32 Гб	32 Гб	2 ТБ
Количество подключений для удаленного управления (Remote Desktop)	Нет	2	2	2	2
Количество клиентских лицензий в комплекте	0	15	5	5	25
Кол-во CAL (Max)	10	Не требуются Ограничено подключением до 15 пользователей	75	Без ограничений	Без ограничений
Кол-во терминальных лицензий (Max)	Нет	15	75	Без ограничений	Без ограничений
Сетевые подключения (RRAS)	Нет	50	75	250	Без ограничений
Сетевые подключения (IAS)	Нет	10	50	50	Без ограничений
Количество одновременных подключений через Шлюз Терминальных Служб	Нет	50	75	250	Без ограничений
Поддержка виртуализации	Нет	Нет	Нет	Лицензия на 1 физическую машину + лицензия на 1 вир-	Лицензия на 1 физическую машину + лицензия на 4 виртуальных

туальную машину	машины. При использовании 4 виртуальных машин - на физической машине роль только Hyper-V.

Windows Server® 2008 R2 Foundation обладает следующими функциональными возможностями:

- поддержка 1 многоядерного процессора (количество ядер в процессоре неограниченно);
- поддержка 8 ГБ ОЗУ для 64-разрядных систем (4 ГБ для 32-разрядных систем);
- до 50 подключений службы сетевого доступа (RRAS);
- до 10 подключений сервера политики сети;
- до 50 подключений сервера терминалов;
- до 15 пользователей (учетных записей в Active Directory).

Windows Small Business Server® 2008 – полностью интегрированное ИТ-решение, включающее в себя все, что нужно малым и средним компаниям. Оно позволяет улучшить защиту данных и повысить эффективность работы компании, значительно снизив при этом расходы на развертывание и поддержку.

Электронная почта, подключение к Интернету, внутренние веб-узлы, удаленный доступ к файлам и почте, поддержка мобильных устройств, совместное использование файлов и принтеров, резервное копирование и восстановление – неполный список возможностей Windows Small Business Server 2008.

Windows Small Business Server® 2008 поставляется в двух вариантах: Standard и Premium.

Версия Standard содержит средства для подключения локальной сети предприятия к Интернету. В состав продукта входит надежный межсетевой экран, сервер сообщений Microsoft Exchange со встроенной системой web-почты Microsoft Outlook Web Access, динамический web-сайт Remote Web Workplace, позволяющий сотрудникам получать быстрый и безопасный доступ к данным через Интернет.

Версия Premium содержит необходимые средства для подключения локальной сети предприятия к Интернету. В состав продукта входит мощный и надежный межсетевой экран, сервер сообщений Microsoft Exchange со встроенной системой web-почты Microsoft Outlook Web Access, динамический web-сайт Remote Web Workplace, позволяющий сотрудникам получать быстрый и безопасный доступ к данным через Интернет.

Windows Server® 2008 R2 Standard – это система имеет встроенный веб-сервер и возможности виртуализации. Она поможет повысить надежность и гибкость серверной инфраструктуры при снижении расходов и экономии времени. Мощные инструменты обеспечивают более удобное управление серверами, упрощают настройку и управление. Надёжные средства безопасности этой операционной системы защищают сети и данные, что даёт возможность построить прочный фундамент для ИТ-среды.

Windows Server 2008 Standard обладает следующими функциональными возможностями:

- поддержка до 4-х многоядерных процессоров (количество ядер в процессоре неограниченно);
- поддержка 32 ГБ ОЗУ для 64-разрядных систем;
- до 250 подключений службы сетевого доступа (RRAS);
- до 50 подключений сервера политики сети;
- до 250 подключений сервера терминалов;
- практически неограниченное кол-во пользователей (учетных записей в Active Directory);
- поддержка виртуализации на базе технологии Hyper-V и один бесплатный виртуальный экземпляр.

Windows Server® 2008 R2 Enterprise — ОС Windows Server® 2008 R2 Enterprise обеспечивает бесперебойное функционирование, безопасность на основе новейших технологий и высокую масштабируемость, которая необходима для поддержки расширения критически важных приложений. Кроме того, она позволяет недорого и эффективно виртуализировать оборудование.

Windows Server® 2008 Enterprise обладает следующими функциональными возможностями:

- поддержка до 8-ми многоядерных CPU для обработки пиковых нагрузок;
- 2 ТБ ОЗУ для эксплуатации ресурсоемких приложений;
- поддержка неограниченного количества VPN-подключений;
- проверка подлинности и авторизация для неограниченного количества подключений службы сетевого доступа и сервера политики сети;
- практически неограниченное количество подключений шлюза удаленных служб;
- поддержка виртуализации на базе технологии Hyper-V (лицензия на 1 физическую машину + лицензия на 4 виртуальных машины).

Кроме того, в Windows Server® 2008 R2 Enterprise имеется функция горячего добавления памяти, которая позволяет без перезагрузки устанавливать на сервере дополнительные блоки памяти и сразу делать их доступными для операционной системы и приложений в рамках обычного пула памяти.

Windows Server® 2008 R2 Enterprise — оптимальная операционная система для серверов с приложениями для управления работой сети, обмена сообще-

ниями, инвентаризации, обслуживания заказчиков и приложениями баз данных. Она поддерживает все функциональные возможности Windows Server 2008 R2 Standard, а также имеет ряд преимуществ. Благодаря таким возможностям, как отказоустойчивые кластеры, Server Core, отказоустойчивая синхронизация памяти и распределенной файловой репликации (DFS-R), ОС Windows Server 2008 R2 Enterprise обеспечивает высокий уровень доступности для критически важных приложений, например баз данных, систем обмена сообщениями, файловых служб и служб печати.

Windows Server 2008 R2 Enterprise является платформой для виртуализации в масштабах всей компании с помощью гибкой и высокопроизводительной технологии Hyper-V™. Лицензия Windows Server® 2008 R2 Enterprise включает право на использование до четырех дополнительных виртуальных экземпляров Windows Server на одном сервере с лицензией Windows Server® 2008 R2 Enterprise.

Тема 1. Требования к оборудованию ОС Windows Server® 2008 R2

Перед установкой Windows Server® 2008 R2 как в лабораторной, так и в производственной среде необходимо удостовериться, что выбранное оборудование отвечает минимальным требованиям к системе. В большинстве ситуаций соответствия оборудования официальным минимальным требованиям далеко не достаточно. При проектировании и выборе технических характеристик системы для нового серверного решения даже предлагаемых Microsoft оптимальных требований к системе может оказаться не достаточно. Поэтому рекомендуется оценивать характеристики сервера для выбранной серверной роли с учетом нагрузки во время развертывания и возможности ее увеличения в будущем. Для работы с Windows Server 2008 R2 компьютер должен удовлетворять следующим требованиям*:

Компонент	Требование
Процессор	1,4 ГГц (процессор с архитектурой x64)
Память	Минимальный объем: 512 МБ Максимальный объем: Foundation — 8 ГБ, Standard — 32 ГБ, Enterprise — 2 ТБ
Требования к свободному пространству на диске	Минимальный объем: 32 ГБ Foundation — 10 ГБ или более. На компьютерах, оснащенных более чем 16 ГБ ОЗУ, потребуется больше места на диске для файлов подкачки, спящего режима и дампа памяти
Монитор	Монитор с разрешением Super VGA (800x600) или более высоким
Прочее	Дисковод для DVD-дисков, клавиатура и мышь (Microsoft) или совместимое указывающее устройство, доступ в Интернет

В Windows Server® 2008 R2 поддерживается использование процессоров только с 64-разрядной архитектурой. Серверы, работающие под управлением процессоров с 32-разрядной архитектурой не поддерживаются.

Преимущества обновления существующего сервера

Такой вариант обновления подразумевает замену текущих файлов Windows и сохранение всех существующих пользователей, параметров, групп, прав и полномочий в нетронутом состоянии. В случае его применения не требуется ни устанавливать какие-либо приложения заново, ни восстанавливать какие-либо данные. Однако перед его применением нужно проверить все приложения на предмет совместимости. То, что эти приложения работали в предыдущих версиях Windows, отнюдь не означает, что они будут работать и под управлением Windows Server® 2008 R2.

Перед выполнением любой процедуры по обслуживанию сервера, в том числе установки Windows Server® 2008 R2, должна быть подготовлена полная резервная копия всех приложений и данных, которые требуется сохранить. При создании резервной копии данных предыдущей операционной системы Windows следует также получить и резервную копию данных состояния системы (System State), потому что эти данные потребуются при восстановлении.

Обновлять до версии Windows Server® 2008 R2 допускается только операционные системы уровня сервера. В их число не входят операционные системы Windows XP, Windows Vista и даже Windows 7, функционирующие в редакции Workstation или Home. Это значит, что для обновления существующего сервера на нем обязательно должна быть установлена ОС Windows Server 2008 либо Windows Server 2003. Обновление с Windows NT 4.0 и Windows 2000 Server не поддерживается.

Преимущества выполнения установки ОС с нуля

При наличии рабочей среды Windows приходится выбирать между вариантом выполнения установки с нуля и вариантом обновления существующего сервера до версии Windows Server® 2008 R2. С каждым из этих вариантов связаны свои преимущества.

Главное преимущество такого варианта в том, что он позволяет получить заведомо работоспособный сервер и избавиться от проблем, которые, возможно, существовали на предыдущем сервере, например, из-за повреждения программного обеспечения, неправильной настройки параметров конфигурации или некорректной установки приложений. Однако следует иметь в виду, что он также приводит и к потере всех имеющихся в предыдущей системе настроек и по завершении инсталляции новой операционной системы требует установки всех необходимых приложений, которые существовали на предыдущем сервере. Перед его применением обязательно документируется вся касающуюся конфигурации информация, готовятся все приложения, которые планируется устанавливать заново, и делается резервная копия всех важных данных.

При установке с нуля систему можно устанавливать как на новом жестком диске (или в новом разделе), так и в другом каталоге на том же диске, на кото-

ром находится предыдущая система. Обычно все новые системы устанавливаются на новых или только что отформатированных жестких дисках, поскольку в таком случае все старое программное обеспечение удаляется и установка получается максимально чистой.

Задание сетевых параметров сервера

Во время процесса установки Windows Server® 2008 R2 мастеру установки понадобится предоставить информацию о том, как должен быть сконфигурирован сервер. Мастер на основе этой информации необходимым образом настроит параметры сервера.

Несмотря на то, что для нормальной работы сервера обязательно нужны такие сведения, как имя сервера и IP-адрес, они вводятся вручную после окончания процесса установки, если только не используется вариант автоматизированной установки с файлом ответов (answer file).

- Выбор имени компьютера

Каждый компьютер в сети должен иметь уникальное имя в пределах этой сети. Во многих компаниях для серверов и рабочих станций применяется стандартизованная схема именования. Хотя в имени компьютера допускается указывать до 63 символов, на рабочих станциях и серверах, функционирующих под управлением версий, предшествующих Windows 2000, распознаются только первые 15 символов.

- Имя рабочей группы или домена

По окончании процесса установки сервера необходимо указать имя рабочей группы или домена, к которому будет присоединен этот сервер. Допускается вводить как имя существующего домена или рабочей группы, так и совершенно новое имя и тем самым создать новую рабочую группу. Домен представляет собой совокупность компьютеров и вспомогательного оборудования, которые совместно используют одну и ту же базу данных безопасности.

- Сетевой протокол и IP-адрес сервера

При установке Windows Server® 2008 R2 должен быть обязательно установлен и сконфигурирован сетевой протокол, который позволит данной системе взаимодействовать с другими машинами в сети. После установки протокола TCP/IP необходимо сконфигурировать IP-адрес для сервера.

Тема 2. Серверные функции Windows Server® 2008 R2

В небольших организациях в целях экономии разные серверные функции могут объединяться и устанавливаться на одну или несколько систем. Однако в крупных организациях серверные службы предпочтительнее распределять по множеству серверов для улучшения производительности, распределения обязанностей по администрированию, возможности резервирования серверов, реа-

лизации стратегии восстановления после аварий, обеспечения безопасности или обслуживания пользователей, работающих в удаленных офисах организации [1].

Ниже перечислены некоторые основные встроенные функции сервера приложений в Windows Server® 2008 R2:

- Контроллер домена (Domain Controller). Как и в предыдущих версиях операционной системы Windows, контроллер домена позволяет пользователям посредством аутентификации подключаться к домену для получения доступа к сетевым ресурсам.
- Сервер глобального каталога (Global Catalog Server). Сервер глобального каталога - это контроллер домена, на котором также хранится набор объектов AD DS из других доменов в лесе. Когда какой-то внутренний или внешний пользователь с соответствующими правами доступа хочет просмотреть список имеющихся в лесе пользователей Active Directory, сервер глобального каталога предоставляет ему такой список.
- Сервер DNS (DNS Server). Система доменных имен (Domain Name System — DNS) создает список имеющихся в сети серверов и систем и их IP-адресов, так что сервер DNS, соответственно, предоставляет информацию о подключенных к сети устройствах.
- Сервер DHCP (DHCP Server). Протокол DHCP (Dynamic Host Configuration Protocol -протокол динамического конфигурирования хостов) назначает подключаемым к сети устройствам сетевые адреса в стандарте IPv4 и/или IPv6. В Windows Server 2008 R2 предлагается служебная функция, которая позволяет упрощать назначение DHCP-адресов сетевым устройствам.
- Кластерный сервер (Cluster Server). Когда отказоустойчивость играет важную роль в организации, кластеризация позволяет обеспечить в случае аварии переключение с одной системы на другую. В Windows Server 2008 R2 имеется возможность связывать системы вместе так, чтобы в случае выхода из строя одной системы ее обязанности переходили к другой.
- Сервер сетевых политик (Network Policy Server — NPS). Сервер NPS представляет собой предлагаемую Microsoft реализацию сервера и прокси-сервера RADIUS (Remote Authentication Dial-in User Service — служба удаленной аутентификации пользователей по коммутируемым линиям). Он умеет выполнять с помощью централизованного подключения аутентификацию, авторизацию и учет для многих типов сетевого доступа, беспроводных соединений и соединений виртуальной частной сети (VPN) включительно, а также маршрутизировать сообщения об аутентификации и ведении учета других серверов RADIUS и выступать в роли сервера оценки работоспособности для точек доступа в сеть (Network Access Points - NAP).
- Сервер удаленных рабочих столов (Remote Desktop Server — RDS). Вместо полнофункциональных настольных или переносных компьютеров в

организациях для пользователей могут быть установлены недорогие терминальные устройства, позволяющие получать доступ к сетевым ресурсам. С помощью Remote Desktop Services можно заставить единственный сервер предоставлять сетевой доступ в систему десяткам рядовых пользователей.

- Сервер удаленного доступа (Remote Access Server - RAS). Если удаленный пользователь должен получать доступ к сетевым службам, службы удаленного доступа Windows Server® 2008 R2 позволяют удаленным системам устанавливать безопасное удаленное соединение.
- Веб-сервер (Web Server). Поскольку все больше и больше технологий поддерживает веб-возможности и обслуживается на веб-серверах, в Windows Server 2008 R2 предлагается технология, позволяющая обслуживать подобные приложения так, чтобы к ним можно было получать доступ с помощью браузера.
- Сервер медиасредств (Media Server). Из-за расширения спектра обмениваемой информации от текстовых документов и электронных таблиц до сложных медиадан-ных, таких как аудио- и видеофайлы, в Windows Server 2008 R2 предлагается источник для обслуживания и публикации видео- и аудиосодержимого.
- Сервер виртуализации (Visualization Server). В Windows Server® 2008 R2 предлагаются основные возможности для виртуализации серверов, которые позволяют организациям сокращать количество физических серверов до нескольких серверных систем и, следовательно, снижать общую стоимость ГГ-операций.
- Сервер распределенной файловой системы (Distributed File System (DFS) Server). Для организаций, в которых файлы данных постоянно хранятся на разбросанных повсюду файловых серверах, в Windows Server® 2008 R2 предлагается сервер распределенных файловых систем, позволяющий объединять распределенные файлы в одно общее пространство имен.

Эти и другие функции позволяют организациям предоставлять эффективные сетевые службы, превращая технологии Windows Server® 2008 R2 в решения, которые способны удовлетворять их производственные потребности.

Определение типа и роли сервера

Сервер можно делать сервером служб доменов Active Directory (Active Directory Domain Services — AD DS), рядовым сервером (member server), автономным сервером или сервером, функционирующим в режиме Server Core. Для определения, какая из этих ролей больше всего подходит серверу, потребуется спланировать задачи, которые он должен выполнять.

Контроллеры доменов и рядовые серверы применяются в новых или существующих доменах. Автономные серверы к какому-либо конкретному домену не присоединяются. Серверы, функционирующие в режиме Server Core, впервые появились вместе с выходом линейки операционных систем Windows Server® 2008 и подразумевают использование минимального набора компонен-

тов. На таких серверах традиционные средства с графическим пользовательским интерфейсом не доступны.

Поддерживаются следующие роли: доменные службы Active Directory® (Active Directory Domain Services), службы Active Directory облегченного доступа к каталогам (Active Directory Lightweight Directory Services — AD LDS), DHCP-сервер (DHCP Server), DNS-сервера (DNS Server), файловые службы (File Services), сервер печати (Print Server), службы потокового мультимедиа (Streaming Media Services) и веб-сервер (Web Server IIS).

Чтобы просмотреть список всех доступных для назначения ролей, ввести в командной строке сервера Server Core команду *oclist*. В Windows Server® 2008 R2 появилась новая команда *sconfig*, которая существенно упрощает настройку систем, устанавливаемых с использованием режима Server Core.

Функциональный статус серверов

Как и в прежних версиях Windows, функциональный статус серверов можно повышать и понижать в соответствии с имеющимися потребностями. Например, статус автономных серверов можно повысить до уровня серверов-членов домена, присоединив их к домену: В свою очередь, статус серверов-членов домена можно повысить до уровня контроллеров домена с помощью утилиты *dcpromo*. Удаление роли Active Directory Domain Services (Доменные службы Active Directory) приводит к понижению до уровня серверов-членов. Кроме того, в Windows Server® 2008 R2 такие роли, как Web Server (IIS) (Веб-сервер IIS) DHCP (DHCP-сервер) и DNS (DNS-сервер), теперь можно добавлять и удалять через программу Server Manager (Диспетчер сервера).

Тема 3. Установка Windows Server® 2008 R2 и базовая настройка.

Загрузить пробную версию Windows Server® 2008 R2 можно с сайта www.microsoft.com.

1) Скопированный образ записать на DVD и загрузиться с DVD диска.

2) Нажать Next и Install now

3) Установить Windows Server® 2008 R2 Enterprise (Full Installation), после чего нажать next

4) Принять лицензионное соглашение.

5) Выбрать метод установки: Custom (advanced) для новой установки Windows Server® 2008 R2.

6) Выбрать на какой жесткий диск будет устанавливаться система.

7) Далее происходит копирование файлов системы на жесткий диск.

8) Создать пароль для Администратора, нажать OK

9) Ввести пароль; если пароль не сложный, будет появляться соответствующее сообщение

10) Ввести сложный пароль (например, 5tudenT) и увидеть сообщение, что пароль достаточно сложный.

11) Далее происходит подготовка рабочего стола

12) После старта запустится окно начальной конфигурации

A) Настроить время на сервере: нажать Set time zone и настроить время в зависимости от региона.

B) Назначить статический IP адрес серверу, нажать Configure networking, выбрать сетевой адаптер и нажать Properties, выбрать IPv4 и нажать Properties

C) Изменить имя сервера, нажать Provide computer name and domain, после Change... нажать OK и перезагрузить сервер

D) После перезагрузки снова откроется окно базовой конфигурации, в котором настроить автоматическое обновление и обновить сервер. В разделе Update This Server нажать Enable automatic updating and feedback, после чего Enable Windows Automatic updating and feedback. Это нужно для того, что бы по мере выхода обновлений системы безопасности, система устанавливала их автоматически.

E) Установить последние обновления для сервера Windows, нажать Download and install updates и Install updates; скорость загрузки обновлений зависит от скорости интернет подключения. По окончании установки обновлений нужно перезагрузить сервер.

F) Включить на сервере возможность удаленного подключения по RDP (Удаленному рабочему столу) что бы удаленно подключатся к серверу через встроенный в Windows клиент (пуск → Все программы → Стандартные → Подключение к удаленному рабочему столу). Login: Administrator Password: пароль, который введен при установке.

Откроется уведомление, что порт для RDP автоматически открыт для Windows Vista и Windows 7. Если нужно подключатся к серверу с системы Windows XP или с Linux выбрать Allow connection from cumputers running any version Remote Desctop (less secure)

Тема 4. Технологии Active Directory Domain Services

Организации, в которых пока нет среды Active Directory, должны начинать с решения этого вопроса, поскольку технология Active Directory Domain Services (Доменные службы Active Directory) играет в Windows Server 2008 R2 ключевую роль в процессе аутентификации пользователей и приложений. Что касается организаций, в которых уже имеется полностью работоспособная среда Active Directory, функционирующая под управлением Windows Server 2003/2008, то они могут просто обновить ее до Active Directory Domain Services 2008 R2. Это вовсе не обязательно предпринимать на самом первом этапе цикла обновления до Windows Server 2008 R2: это допускается делать позже, когда возникнет необходимость в функциональности AD DS 2008 R2. Дело в том, что многие из функциональных средств Windows Server® 2008 R2 типа 2008 R2 DFS, SharePoint Services, Hyper-V и т.д. могут быть запущены в среде более старой версии Active Directory (чаще всего — в собственном режиме Active Directory 2003).

Поскольку Active Directory® представляет каталог, который в Windows Server® 2008 R2 встроен в средства безопасности на основе политик безопасности удаленного доступа и безопасности на основе сертификатов, то внедрение AD DS 2008 R2 должно быть проведено на одном из начальных этапов процес-

са миграции в организациях, где планируется развертывание новых технологий Active Directory® 2008 R2, таких как Active Directory Recycle Bin (Корзина Active Directory), Offline Domain Join (Автономное присоединение к домену), Managed Service Accounts (Управляемые учетные записи служб) и применение командлетов PowerShell внутри объекта групповой политики (Group Policy Object).

Windows Server® 2008 R2 расширяет возможности Active Directory® за счет предоставления более удобных средств управления, а также обеспечивает более эффективную репликацию каталогов по всему предприятию и более высокую степень масштабируемости и резервирования, что улучшает выполнение операций с каталогами. Windows Server® 2008 R2, по сути, привносит в систему более высокую надежность, увеличенную производительность и дополнительные средства управления, превращая ее в эффективный инструмент для работы с каталогами предприятия, а также для отслеживания и управления ресурсами.

Установка Active Directory на Windows Server® 2008 R2

Active Directory - LDAP-совместимая реализация службы каталогов корпорации Microsoft для операционных систем семейства Windows NT.

Active Directory позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, развёртывать программное обеспечение на множестве компьютеров через групповые политики или посредством System Center Configuration Manager (ранее Microsoft Systems Management Server), устанавливать обновления операционной системы, прикладного и серверного программного обеспечения на всех компьютерах в сети, используя Службу обновления Windows Server.

Active Directory хранит данные и настройки среды в централизованной базе данных. Сети Active Directory могут быть различного размера: от нескольких сотен до нескольких миллионов объектов.

При установке имеются особенности:

- Нужно установить как минимум два domain controller (DC) в своей сети для повышения отказоустойчивости. Установка одного DC в сети является предпосылкой отказа.
- Требуется работающая служба DNS. При запуске утилиты *dcpromo*, устанавливают и 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.

1. Найти в **Диспетчере сервера** (Server Manager) узел **Роли** (Roles) в левой панели консоли. Затем нажать **Добавить роли** (Add Roles) в правой панели.
2. Открывается страница **Before You Begin**. Прочитать информацию на этой странице и нажать **Далее**.

3. 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.
4. После выбора роли **Active Directory DC Server**, показана информация об этой роли сервера.
5. Нажать Установить для установки файлов, необходимых для запуска *dcpromo*.
6. Установка завершена. Нажать Закрыть.
7. В меню Пуск и в текстовом поле Выполнить ввести *dcpromo*. Нажать *dcpromo*.
8. Запустится мастер Welcome to the Active Directory Domain Service Installation Wizard. Нажать Далее.
9. На странице Совместимость операционной системы (Operating System Compatibility) мастер предупреждает о том, что NT и non-Microsoft SMB клиенты будут испытывать проблемы с некоторыми криптографическими алгоритмами, используемыми в Windows Server 2008 R2. Нажать Далее.
10. В следующем окне Выбор конфигурации установки (Choose a Deployment Configuration) выбрать опцию Создание нового домена в новом лесу (Create a new domain in a new forest).
11. В окне Имя корневого домена в лесу (Name the Forest Root Domain) ввести название домена в текстовое поле FQDN корневого домена в лесу. Нажать Далее.
12. В окне Определение функционального уровня леса (Set Forest Functional Level) выбрать опцию Windows Server 2008 R2 (опция Windows Server 2003 используется, если в домене имеются серверы Windows Server 2003). Выбрать опцию Windows Server 2008 R2, чтобы воспользоваться всеми новыми удивительными возможностями, включенными в Windows Server 2008 R2. Нажать Далее.
13. В окне Дополнительные опции контроллера домена (Additional Domain Controller Options) есть единственный выбор: DNS сервер. Опция глобального каталога выбрана и не является опцией по выбору, так как пока что 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.
14. Появится диалоговое окно, говорящее о том, что невозможно создать делегирование для этого сервера DNS, поскольку полномочная родительская зона не может быть найдена или не использует Windows DNS сервер. Причина в том, что это первый DC в сети. нажать Да.
15. Оставить умолчания и нажать Далее.

16. В окне Directory Service Restore Mode Administrator Password ввести надежный пароль в текстовые поля Пароль (Password) и Подтверждение (Confirm password).
17. Проверить информацию на странице Summary и нажать Далее.
18. Отметить опцию Перезагрузить по окончании (Reboot on completion), чтобы машина автоматически перезагрузилась после установки DC.

Рис. 1. Отметка опции Перезагрузить по окончании

Тема 5. Управление учетными записями

Учётная запись - запись, содержащая сведения, которые пользователь сообщает о себе некоторой компьютерной системе. Как синонимы в обиходе могут использоваться учётка, акка́унт и экка́унт, от англ. Account — учётная запись, личный счёт[2].

Содержание учётной записи

Учётная запись, как правило, содержит сведения, необходимые для идентификации пользователя при подключении к системе, информацию для авторизации и учёта. Это имя пользователя (логин) и пароль. Пароль или его аналог, как правило, хранится в зашифрованном или хэшированном виде для обеспечения его безопасности. Для аутентификации могут использоваться аппаратные средства (вырабатывающие одноразовые ключи, считывающие биометрические характеристики и т. п.), а также одноразовые пароли.

Учётная запись может содержать также дополнительные анкетные данные о пользователе - имя, фамилию, отчество, псевдоним, дату рождения, адрес e-mail, домашний адрес, рабочий адрес, нетмейловый адрес, номер домашнего телефона, номер рабочего телефона, номер сотового телефона, адрес домашней страницы и/или блога в Паутине или интранете, о культурных предпочтениях и так далее. Учётная запись может также содержать одну или несколько фотографий пользователя.

Учётная запись пользователя также может учитывать различные статистические характеристики поведения пользователя в системе: давность последнего входа в систему, продолжительность последнего пребывания в системе, адрес использованного при подключении компьютера, интенсивность использования системы, суммарное и (или) удельное количество определённых операций, произведённых в системе, и так далее.

Создание нового пользователя

Запустить диспетчер сервера («Пуск» → «Администрирование» → «Диспетчер сервера»). Раскрыть вкладку «Конфигурация», затем «Локальные пользователи и группы» и выбрать оснастку «Пользователи». В таблице справа видны уже существующие пользователи. Кликнуть в свободном месте таблицы правой кнопкой мыши и выбрать «Новый пользователь».

Создание нового пользователя

Откроется окно ввода данных пользователя. В поле «*Пользователь*» необходимо указать имя, которым пользователь будет входить (логиниться на) в сервер, поля «*Полное имя*» и «*Описание*» могут быть любыми. Далее ввести 2 раза пароль. По умолчанию пароль должен отвечать требованиям сложности.

Если оставить флажок «*Требовать смены пароля при следующем входе в систему*», то, соответственно, при первом входе пользователя система попросит его ввести новый пароль. Здесь можно запретить пользователю менять свой пароль. И если не ставить флажок «*Срок действия пароля не ограничен*» то через количество дней, указанных в политике безопасности паролей, система потребует у пользователя ввести новый пароль. После того как все настройки определены (их можно поменять в любое время) нажать «*Создать*»

В списке должен появиться только что созданный пользователь. Кликнув по нему правой кнопкой мыши, видно, что из контекстного меню можно изменить пароль пользователя, удалить, переименовать пользователя, а также отредактировать его свойства.

Редактирование свойств пользователя

Ниже рассмотрены некоторые из свойств пользователя:

- Вкладка «*Общие*» - здесь можно изменить начальные данные пользователя. О них было сказано выше.
- «*Членство в группах*» - здесь можно определить в какие группы будет входить пользователь. Например, если предполагается, что пользователь будет работать через удаленный рабочий стол, то его нужно добавить в группу «*Пользователи удаленного рабочего стола*». Для этого нажимаем кнопку «*Добавить*», затем «*Дополнительно*», в окне выбора группы жмем «*Поиск*», выбрать нужную группу из списка и кликнуть «*ОК*» 3 раза.

- На вкладке «*Профиль*» можно изменить путь хранения профиля (По умолчанию это C:\Users\), указать сценарий входа, а так же задать сетевой диск, который будет подключаться при входе пользователя.
- «Среда пользователя» - здесь можно задать программу, которая будет запускаться при входе пользователя на удаленный рабочий стол. В этом случае пользователю будут недоступен рабочий стол, панель задач, а также другие программы сервера. При закрытии этой программы также будет выгружаться и учетная запись. Т.е. пользователь сможет работать только с этой программой и ни с чем больше. Также на этой вкладке можно разрешить/запретить подключение устройств при работе через удаленный рабочий стол.
- Вкладка «сеансы» отвечает за установку параметров тайм-аута и повторного подключения к удаленному рабочему столу. Очень часто на практике я сталкивался с ситуацией, когда пользователь не отключался от удаленного рабочего стола, просто закрывая терминал «крестиком». Учетная запись в этом случае продолжает «висеть» на сервере. Помогает в данной ситуации выставление тайм-аута отключения сеанса.
- Вкладка «*Профиль служб терминалов*» аналогична вкладке «*Профиль*» , с той лишь разницей, что относится к профилю пользователя, загружаемому при входе на сервер через удаленный рабочий стол. Также здесь можно запретить данное подключение.
- На вкладке «*Удаленное управление*» можно включить/отключить удаленное управление учетной записью пользователя при работе через удаленный рабочий стол. Обычно здесь я снимаю галочку «*Запрашивать разрешение пользователя*» т. к. если пользователь отключился от сеанса службы терминалов, то управлять этой учеткой уже не получится.

Создание доменной учетной записи пользователя

1. Чтобы открыть оснастку "Active Directory - пользователи и компьютеры", нажать кнопку **Пуск**, щелкнуть **Панель управления**, дважды щелкнуть **Администрирование**, а затем дважды щелкнуть **Active Directory - пользователи и компьютеры**.
2. В дереве консоли щелкнуть правой кнопкой мыши папку, в которую нужно добавить учетную запись пользователя.
3. Выделить пункт **Создать** и щелкнуть **Пользователь**.
4. В поле **Имя** ввести имя пользователя.
5. В поле **Инициалы** ввести инициалы пользователя.
6. В поле **Фамилия** ввести фамилию пользователя.
7. Изменить **Полное имя**, чтобы добавить инициалы или поменять имя и фамилию местами.
8. В поле **Имя пользователя** ввести имя пользователя для входа, щелкнуть суффикс основного имени пользователя (UPN) в раскрывающемся списке, а затем нажать кнопку **Далее**.

9. Если пользователь будет использовать другое имя для входа на компьютеры, работающие под управлением операционных систем Microsoft® Windows® 95, Windows 98 или Windows NT®, можно сменить имя пользователя для входа, отображающееся в пункте **Имя входа пользователя (пред-Windows 2000)**.
10. В поле **Пароль** и поле **Подтверждение** ввести пароль пользователя, а затем выбрать подходящие параметры пароля.
11. Для выполнения этой процедуры необходимо быть членом группы "Операторы учета", "Администраторы домена" или "Администраторы предприятия" в AD DS либо получить соответствующие полномочия путем делегирования. По соображениям безопасности для выполнения этой процедуры рекомендуется использовать команду **Запуск от имени**.
12. Новая учетная запись пользователя с таким же именем, как и у ранее удаленной учетной записи пользователя, не приобретает автоматически разрешения и членства ранее удаленной учетной записи, потому что идентификатор безопасности (SID) каждой учетной записи уникален. Если требуется воспроизвести удаленную учетную запись пользователя, необходимо вручную заново создать все разрешения и членства.
13. При создании учетной записи пользователя атрибут **полное имя** создается в формате **ИмяФамилия** по умолчанию. Атрибут **полное имя** также управляет форматом выводимого имени, которое отображается в глобальном списке адресов. Формат выводимого имени можно изменить с помощью средства "Редактирование ADSI". Если изменить формат выводимого имени, формат полного имени тоже изменится.
14. Задачу этой процедуры можно также выполнить, используя модуль Active Directory для Windows PowerShell™. Чтобы открыть Модуль Active Directory, нажать кнопку **Пуск**, щелкнуть **Администрирование**, а затем щелкнуть Модуль Active Directory для Windows PowerShell.
15. Чтобы открыть модуль Active Directory для Windows PowerShell, открыть **Диспетчер серверов**, щелкнуть **Сервис**, а затем **Модуль Active Directory для Windows PowerShell**.

Создание учетной записи пользователя с помощью командной строки

1. Чтобы открыть командную строку, нажать кнопку **Пуск**, щелкнуть **Выполнить**, ввести **cmd**, а затем нажать кнопку **ОК**.
2. Ввести следующую команду и нажать клавишу ВВОД ↵.

```
dsadd user <UserDN> [-samid<SAMName>] -pwd {<Password>|*}
```

Параметр	Описание
<UserDN>	Задает различающееся имя добавляемого объекта-пользователя.
-samid	Устанавливает значение <SAMName>.

<SAMName>	Задает имя диспетчера учетных записей безопасности (SAM) как уникальное имя учетной записи SAM для данного пользователя (например, Linda). Если имя SAM не указано, **dsadd** попытается создать имя учетной записи SAM, используя до 20 первых символов обычного имени (CN) *UserDN*.
-pwd	Устанавливает значение пароля.
<Password>	Задает пароль для использования в учетной записи пользователя. Если для этого параметра установлено значение *****, выводится запрос на ввод пароля.

Для просмотра полного синтаксиса данной команды, а также сведений о вводе в командную строку информации учетной записи пользователя ввести следующую команду, а затем нажать клавишу ВВОД↵.

```
dsadd user /?
```

- Для выполнения этой процедуры необходимо быть членом группы "Операторы учета", "Администраторы домена" или "Администраторы предприятия" в доменных службах Active Directory либо получить соответствующие полномочия путем делегирования. По соображениям безопасности для выполнения этой процедуры рекомендуется использовать команду **Запуск от имени**.
- Новая учетная запись пользователя с таким же именем, как и у ранее удаленной учетной записи пользователя, не приобретает автоматически разрешения и членства ранее удаленной учетной записи, потому что идентификатор безопасности (SID) каждой учетной записи уникален. Если требуется воспроизвести удаленную учетную запись пользователя, необходимо вручную заново создать все разрешения и членства.
- Задачу этой процедуры можно также выполнить, используя Модуль Active Directory для Windows PowerShell. Чтобы открыть Модуль Active Directory, нажать кнопку **Пуск**, щелкнуть **Администрирование**, а затем щелкнуть **Модуль Active Directory для Windows PowerShell**.
- Чтобы открыть модуль Active Directory для Windows PowerShell, открыть **Диспетчер серверов**, щелкнуть **Сервис**, а затем щелкнуть **Модуль Active Directory для Windows PowerShell**.

Создание перемещаемых профилей

При создании перемещаемых профилей нужно настроить сетевое размещение, где будут располагаться данные профили, а затем сконфигурировать каждую учетную запись пользователя для сопоставления с созданным ранее сетевым размещением. Эти действия описаны далее:

1. На файловом или специально выделенном профильном сервере создать папку, которая будет использоваться для хранения перемещаемых поль-

зовательских профилей. Данная папка будет считаться папкой верхнего уровня для всех индивидуальных профилей пользователей;

2. Перейти в свойства в свойства текущей папки. В отобразившемся диалоговом окне **«Свойства: %имя_папки%»** перейти на вкладку **«Доступ»** и предоставить для группы **«Прошедшие проверку»** полный доступ. Это действие следует выполнить для того, чтобы пользователи, прошедшие проверку могли получать доступ к текущему ресурсу, а также создавать свои профили. Помимо этого, назначить дополнительные разрешение NTFS для группы **«Пользователи»**. Папка, которая используется для хранения настраиваемого профиля, должна называться DefaultUser.v2, для которой назначить полный доступ группе **«Все»**;
3. Открыть оснастку **«Active Directory – пользователи и компьютеры»**, выбрать пользователя, для которого нужно настроить перемещаемый профиль, нажать на нем правой кнопкой мыши и выбрать команду **«Свойства»**;
4. В отобразившемся диалоговом окне перейти на вкладку **«Профиль»** и в соответствующем текстовом поле ввести путь к общей папке, где содержится профиль текущего пользователя. Можно использовать переменную среды %UserName% в качестве заполнителя имени входа в систему, которое используется в пути профиля. После того как пользователь в первый раз войдет в домен, на сервере автоматически будет создана папка профиля в формате имени пользователя или, если пользователь выполнил вход из операционной системы Windows Vista или более поздней версии операционной системы, то будет создана папка имя_пользователя.v2 с соответствующими разрешениями.

Обязательный пользовательский профиль создается по аналогии, только после настройки рабочего стола (достаточно чтобы пользователь, например, начальник отдела, выполнил все настройки для текущего профиля), файл данного профиля следует переименовать с NTUSER.DAT в NTUSER.MAN.

Также каждый обязательный пользовательский профиль следует хранить в специально выделенной папке верхнего уровня.

То есть, нужно создать следующую иерархию папок: корневая папка верхнего уровня, например, Profiles, в которой будет расположена папка mandatory_user_profiles, внутри которой уже будут расположены папки с обязательными профилями пользователей.

Для этой папки нужно предоставить разрешения только на уровне «Чтения», что не позволит вносить пользователям изменения в свой обязательный пользовательский профиль, который расположен на сервере.

После этого, на вкладке «Профиль» пользователя, в соответствующем текстовом поле, задать имя с суффиксом .man (.man.v2 для пользователей, которые выполняют вход под операционными системами Windows Vista и выше) в конце для папки пользователя, которая станет обязательным пользовательским профилем.

Управление перемещаемыми пользовательскими профилями средствами групповой политики

В доменах Active Directory для снижения стоимости управления компьютерными системами принято целесообразно использовать групповые политики. Групповые политики позволяют управлять большинством задач, которые могут стать перед вами при развертывании перемещаемых пользовательских профилей.

Для этого корпорация Microsoft предоставляет 23 параметра групповой политики, расположенных в узлах Политики\Административные шаблоны\Система\Профили пользователей разделов конфигурации компьютера и конфигурации пользователя. Ниже рассмотрены эти параметры:

Добавлять группу безопасности «Администраторы» к перемещаемым профилям пользователя.

Данный параметр групповой политики используется для добавления группы безопасности «Администраторы» в общий ресурс с перемещаемым профилей пользователя, а также для назначения полного доступа.

После того как настроен перемещаемый пользовательский профиль, он будет создан при следующем входе пользователя в систему в указанном алиминистратором расположении. Если параметр отключен или не задан, то только пользователь получит полный доступ к своему профилю, а у группы администраторов не будет доступа к файлам, а если данный параметр включен, то группа администраторов также будет иметь все права доступа к папке профиля пользователя. Если включить данный параметр после создания профиля, он не будет влиять на созданный ранее профиль. Стоит отметить, что данный параметр нужно настраивать не на профильном сервере, а на компьютере пользователя, так как разрешения общего файлового доступа назначается к перемещаемому профилю во время его создания.

Удалять при перезагрузке системы профили пользователей по истечении указанного числа дней.

Текущий параметр позволяет администратору при перезагрузке системы автоматически удалять профили пользователей, которые не были использованы в течение указанных в этой политике дней, при этом днем считается 24 часа с момента получения доступа к данному профилю. В том случае, если параметр активирован, то при перезагрузке системы неиспользованные в указанном количестве дней профили автоматически удаляются службой пользовательских профилей. Если же параметр не настроен или отключен, то автоматического удаления не произойдет. Для пользователей, находящихся в частых и длительных командировках применение данного профиля следует планировать в частном порядке.

Не проверять собственность пользователя перемещаемых папок профиля.

Этот параметр отключает безопасную настройку по умолчанию для пользовательской папки перемещаемых пользовательских профилей, определяет действия с существующей папкой при обновлении компьютеров, поддерживает и повышает уровень безопасности пользовательского профиля. Начиная с операционной системы Windows XP SP1, папка перемещаемого профиля недоступна для копирования в том случае, если она уже существует и разрешения на нее не верны.

При включенном параметре, операционная система Windows не проверяет разрешения на существующую папку. При отключенном или не заданном параметре в существующей папке перемещаемого пользовательского профиля, копирование файлов отсутствует, а в журнале событий выводится сообщение об ошибке. В случае отсутствия кэшированного профиля, используется временный профиль пользователя.

Удалять кэшированные копии перемещаемых профилей.

Используя данный параметр, можно определить возможность сохранения копий пользовательского перемещаемого профиля на жестком диске при выходе из системы. Совместно со связанными с ним параметрами данной папки, этот параметр определяет стратегию управления пользовательскими профилями, которые расположены на удаленных серверах и определяют действия системы при длительном времени загрузки профиля.

Как было сказано ранее, при выходе пользователя из системы производится сохранение перемещаемого профиля пользователя на локальный жесткий диск для исключения ситуации недоступного профильного сервера. При включенном параметре, все локальные копии удаляются, при этом оставляя перемещаемый профиль только на профильном или файловом сервере. В случае медленного подключения этот параметр должен быть отключен, так как он требует наличие локальной копии перемещаемого профиля.

Не выполнять принудительной выгрузки реестра пользователя при его выходе из системы.

Данный параметр групповой политики используется в случае проблем совместимости приложений. Операционная система производит выгрузку системного реестра пользователя при выходе из системы, невзирая на открытые дескрипторы к пользовательским разделам реестра. Так как применение данного параметра может препятствовать получению обновлений перемещаемых профилей, данный параметр рекомендуется использовать только в крайних случаях.

В том случае, если этот параметр включен, принудительная выгрузка реестра при выходе из системы не производится, но системный реестр будет перезагружаться после закрытия дескрипторов к пользовательским разделам сис-

темного реестра. Отключенный или не настроенный параметр будет выгружать реестр всегда, даже при открытых дескрипторах.

Не определять медленные сетевые подключения.

Как известно, медленное подключение характеризуется измерением скорости подключения пользовательского компьютера к удаленному серверу, содержащему перемещаемый профиль пользователя. При определении системой медленного подключения, параметры папки перемещаемого профиля определяют характер реакции системы на медленное подключение. При включенном параметре система не определяет медленное подключение и ни одно из сетевых подключений не будет таковым считаться, соответственно, всегда заграждаются перемещаемые профили.

Система игнорирует параметры, задающие реакцию на медленные подключения. При отключенном или не настроенном параметре, система измеряет скорость подключения к удаленному серверу, хранящему пользовательский профиль. При медленном подключении система задействует другие параметры, установленные в папке перемещаемого профиля для дальнейших действий, загружая локальную копию пользовательского профиля по умолчанию.

Выдавать запрос пользователю при обнаружении медленного сетевого подключения.

Текущий параметр групповой политики поможет в том случае, если пользователи требуют загрузки перемещаемого профиля даже при наличии медленного сетевого подключения к профильному серверу. В операционных системах Windows XP и более ранних, при обнаружении медленного подключения отображается диалоговое окно для выбора параметра загрузки удаленной копии перемещаемого профиля. В операционных системах Windows Vista и более поздних, при входе в систему отображается только флажок, определяющий необходимость загрузки пользовательского профиля.

При активированном параметре данной политики, пользователи сами определяют необходимость загрузки перемещаемого профиля при медленном подключении к серверу. При отключенном или не заданном параметре, используется локальная копия профиля пользователя. При включенном параметре «Дождаться загрузки перемещаемого пользовательского профиля», удаленная копия профиля будет загружена автоматически или же система будет полностью игнорировать предварительный выбор пользователя. Для настройки времени, выделенного на ответ в операционных системах ниже Windows Vista, используется параметр «Таймаут диалоговых окон». При включенном параметре «Не определять медленное подключение», данный параметр игнорируется. При включенном параметре «Удалять кэшируемые копии перемещаемых профилей», локальная копия профиля отсутствует, соответственно локальная копия профиля не загружается при медленном подключении.

Оставить установочные данные установщика Windows и групповой политики.

Использование данного параметра позволяет определить, оставляет ли операционная система установочные данные установщика Windows и групповой политики при удалении перемещаемого профиля пользователя. По умолчанию удаляются все относящиеся к нему сведения, в том числе и связанные с установщиком, поэтому при следующем входе в систему возникает необходимость установки всех приложений публикуемых с помощью политики, что, соответственно, увеличивает время входа в систему.

При включении данного параметра, установочные данные установщика Windows и групповой политики не удаляются с компьютера, что повышает производительность при следующем входе в систему пользователей с удаленным профилем. При отключенной или не настроенной политике, перемещаемый профиль пользователя удаляется целиком, включая данные установщика Windows и групповой политики. При включённой политике локальный администратор должен удалить данные установщика Windows и групповой политики из реестра и файловой системы пользователя.

Разрешить использование только локальных профилей.

При помощи данного параметра групповой политики, можно запретить пользователям с перемещаемым профилем получать его на отдельно взятом компьютере. По умолчанию, при первом входе пользователя в систему, его перемещаемый профиль загружается на локальный компьютер. При последующем входе, перемещаемый профиль объединяется с локальным профилем пользователя. При завершении работы и выходе из системы, локальная копия профиля с произведенными в процессе сеанса изменениями, объединяется с серверной копией профиля. Используя данный параметр, можно запретить пользователям получать свой перемещаемый профиль на отдельно взятом компьютере.

При включенном параметре, при первом входе в систему, пользователь получает новый локальный профиль, в котором и будут сохранены все изменения системы. Этот же локальный профиль будет использоваться при всех последующих входах в систему, не синхронизируя с сервером. Если данный параметр отключен или не задан, то по умолчанию используется перемещаемый профиль пользователя.

Установить путь к перемещаемым профилям для всех пользователей, входящих в систему на данном компьютере.

Данный параметр определяет необходимость использования указанного сетевого пути для всех пользователей, отдельно взятого компьютера. Для использования данного параметра вводится путь к общему сетевому ресурсу в следующем формате: \\имя_компьютера\имя_общего_ресура. Для предоставле-

ния индивидуальной папки профиля для каждого пользователя на отдельно взятом компьютере, добавьте пути %Username%, иначе все пользователи будут использовать одну и ту же папку профиля, при этом необходимо убедиться в наличие соответствующих настроек безопасности.

При включенном параметре все пользователи используют указанный путь к перемещаемым профилям. При отключенном или не настроенном параметре, пользователи используют локальный или стандартный перемещаемый пользовательский профиль.

Таймаут диалоговых окон.

Используя текущий параметр групповой политики, можно определить, как долго операционная система должна ожидать ответа пользователя, прежде чем выполнить действие, которое установлено по умолчанию. Последнее используется в том случае, если пользователь не ответил на сообщение о возникновении событий обнаружения медленного подключения, недоступности профильного сервера или повествующего о том, что локальный пользовательский профиль новее, чем серверный профиль. Целесообразно использовать данный параметр для предопределения системного значения, которое равно 30 секундам. Значение можно указать в интервале от 0 до 600 секунд.

Не регистрировать в системе пользователей с временными профилями.

Текущий параметр групповой политики позволяет автоматически отключать пользователей от системы при невозможности загрузки их профилей. Данная политика также распространяется в том случае, когда профиль содержит ошибки препятствующие загрузке, при этом, не позволяя операционной системе регистрировать пользователя с временным профилем.

При включении данного параметра, операционная система не будет регистрировать пользователя с временным профилем пользователя. Если же параметр отключен или не задан, при невозможности загрузки пользовательских профилей, операционная система будет регистрировать в системе временные профили.

Максимальное число повторов выгрузки и обновления профиля пользователя.

При помощи этого параметра групповой политики можно определить количество повторных попыток обновления файла NTUSER.DAT при выходе пользователя или ошибки обновления. Когда пользователь выходит из системы, операционная система выгружает пользовательскую часть реестра и обновляет ее. Система прекращает эти попытки тогда, когда указанное количество попыток оказывается исчерпывающим.

По умолчанию система повторяет попытки 60 раз. Если включить данный параметр, то можно изменить количество повторных попыток выполнения загрузки и обновления пользовательских параметров реестра. В том случае, если

установлено значение равное нулю, то операционная система будет выполнять выгрузку и обновление параметров реестра только один раз. Если на компьютере расположено много профилей, то желательно увеличить количество повторных попыток.

Запретить передачу на сервер изменений в перемещаемом профиле.

Используя данный параметр, можно предотвратить внесение изменений, сделанных в перемещаемом профиле на конкретном компьютере, в копию компьютера на сервере.

При выполнении пользователем входа в систему, его перемещаемый профиль копируется на локальный компьютер, причем перемещаемый профиль объединяется с локальным в том случае, если ранее уже выполнялся вход. Если включить данный параметр, то при входе пользователь получит свой перемещаемый профиль, но все изменения сделанные пользователем в своем профиле, не будут внесены в его перемещаемый профиль при выходе из системы.

Дождаться загрузки перемещаемого профиля.

Данный параметр групповой политики указывает на то, что операционная система должна дождаться загрузки удаленной копии перемещаемого профиля пользователя, даже в том случае, когда он подключен через медленное подключение. Включив данный параметр, позволено всегда загружать перемещаемый пользовательский профиль с сервера. Стоит обратить внимание на то, что если включен параметр «Не определять медленные подключения», то данный параметр групповой политики игнорируется. Также, при включенном параметре «Удалять кэшированные копии перемещаемых профилей», в случае медленного подключения, нет локальной копии перемещаемого профиля, которую можно было бы загрузить. Если же данный параметр групповой политики отключен или не настроен, то при обнаружении медленного подключения система загружает локальную копию перемещаемого профиля пользователя

Таймаут медленных сетевых подключений для профилей пользователей.

Текущий параметр позволяет указать, какое подключение для загрузки перемещаемых профилей пользователей будет считаться медленным. Операционная система считает подключение медленным в том случае, если сервер, на котором располагается перемещаемый профиль пользователя, отвечает медленнее, чем указано в данном параметре. Для компьютеров, подключенных к IP-сетям, операционная система вычисляет скорость, с которой удаленный сервер должен возвращать данные в ответ на ping-сообщение.

Для задания порогового значения для этой проверки в текстовом поле «Скорость подключения» ввести десятичное число от 0 до 4294967200, представляющее минимальную приемлемую скорость передачи в килобитах в секунду. Значение, установленное по умолчанию равняется 500 кбит/с.

Помимо этого, если для компьютеров не в IP-сетях файловая система сервера не отвечает в течение максимальной приемлемой задержки в миллисекундах, которая указывается в текстовом поле «Время», сервер также считается медленным. В данное текстовое поле можно ввести значение от 0 до 20000. В том случае, если включен параметр групповой политики «Не определять медленные подключения», то данный параметр игнорируется.

Фоновая передача файла реестра перемещаемого профиля пользователя при входе пользователя в систему.

Данный параметр появился только в операционных системах Windows 7 и Windows Server 2008 R2. При помощи этого параметра можно задать расписание фоновой передачи файла реестра перемещаемого профиля пользователя. Передача осуществляется только в том случае, если пользователь вошел в систему. Стоит обратить внимание на то, что данный параметр не препятствует передаче файла реестра перемещаемого профиля пользователя при выходе пользователя из системы. Основное отличие данного параметра от всех остальных заключается в том, что для использования этого параметра сначала необходимо выбрать используемый метод планирования расписания. Существует два метода расписания:

- **Запуск с заданным интервалом**. Выбрав данный план расписания, файл реестра профиля пользователя будет передаваться с указанным интервалом после входа пользователя в систему. В текстовом поле **«Интервал»** можно указать интервал от 1 до 720 часов. Например, если указать интервал 4 часа, то файл реестра будет передаваться в фоновом режиме каждые четыре часа, даже если пользователь не выходит из системы. При следующем входе пользователя в систему таймер начнет работать заново;
- **Запуск в указанное время**. При выборе данного плана куст реестра будет передаваться лишь один раз ежедневно в одно и то же время.

Установить максимальное время ожидания для сети, если пользователь имеет перемещаемый профиль или удаленный основной каталог.

По умолчанию, при перемещении профиля или удаления основной папки с профилем во время недоступности сетевого подключения, после выполнения пользователем входа в систему, операционная система Windows ожидает возобновления работы сети в течение 30 секунд. Используя этот параметр, можно задать время ожидания возобновления работы сети. В том случае, если по истечении максимального времени ожидания сеть останется недоступной, то вход пользователя в систему будет продолжен без сети. Как только сеть станет доступной до истечения максимального времени ожидания, то вход пользователя непременно продолжится.

Подключить домашнюю папку к корню общего ресурса.

Текущий параметр определяет параметры переменных сред %HOMESHARE% и %HOMEPATH%, которые определяет домашнюю папку пользовательского профиля, а также содержит полный путь к домашней папке. В этом случае пользователи могут получать доступ к домашней папке и любым ее подпапкам через букву диска домашней папки, но в то же время не могут просматривать или получать доступ к ее родительским папкам. При отключении данного параметра, домашние папки сопоставляются с папкой пользователя, а не с общим ресурсом более высокого уровня. Данный параметр нельзя использовать на операционных системах, которые были созданы после операционной системы Windows XP.

Синхронизировать основные папки только в момент входа или выхода системы.

При помощи данного параметра групповой политики можно указать сетевые папки, которые будут синхронизироваться, используя политики автономных файлов при входе и выходе из системы. Этот параметр целесообразно использовать для разрешения проблем с приложениями, работающими некорректно с автономными файлами, когда пользователь находится в интерактивном режиме. Если данный параметр включен, то сетевые пути, которые указаны в параметре будут синхронизироваться при помощи политики автономных файлов. Если отключен или не задан, то пути, которые указаны в текущем параметре, будут вести себя аналогично другим кэшированным данным, обрабатываемым политикой автономных файлов, и останутся в интерактивном режиме при нахождении пользователя в системе, если сетевые пути доступны.

Исключить папки из перемещаемого профиля.

Этот параметр групповой политики позволяет исключить папки, которые должны включаться в перемещаемый профиль пользователя, что позволяет не сохранять определенные папки на профильном сервере. Как известно, в перемещаемых профилях обязательно исключаются папки «Appdata\Local», «Appdata\LocalLow», а также папки, содержащие временные файлы и историю браузера Internet Explorer. Если включить данный параметр, то можно исключить любые папки, которые расположены в пользовательском профиле. При отключении данного параметра перемещаться будут, соответственно, только папки по умолчанию.

Ограничить размер профиля.

Данный параметр позволяет задать максимальный размер пользовательского профиля и определяет действие операционной системы в том случае, когда профиль достигает максимального значения. При помощи этого параметра можно установить максимальный размер профиля, определить, включается ли в

размер профиля файлы реестра, указать, будут ли конечные пользователи получать уведомления при превышении максимального размера профиля, указывать специальное сообщение, уведомляющее пользователя о превышении размера профиля, а также определить, как часто это сообщение должно отображаться. Если отключить или не задать параметры для данного параметра, то операционная система не будет ограничивать размер пользовательского профиля.

Тема 6. Разрешения файловой системы

Для управления доступом пользователей к папкам и файлам используется детализированная и сложная система разрешений. Механизм управления доступом к объектам Windows - один из самых детализированных среди известных операционных систем. Для файлов и папок существует не менее 14 разрешений NTFS, которые могут быть включены или блокированы, и проверены. Эти разрешения можно назначать файлам или папкам и пользователям или группам. Также, можно назначать порядок наследования разрешений для файлов или папок и пользователей или групп.

Основы доступа к объектам

Пользователь никогда не входит в непосредственное "соприкосновение" с каким-либо объектом Windows. Весь доступ к объектам осуществляется через программы (например, Windows Explorer, Microsoft Office) или процессы. Программа, которая обращается к ресурсам от лица пользователя, выполняет процедуру, которая называется имперсонализацией (impersonation). Программа, которая обращается к удаленному ресурсу, выполняет процедуру, которая называется делегированием (delegation).

После регистрации пользователя его системный идентификатор (System Identifier - SID) и идентификаторы SID группы обрабатываются процессом lsass.exe, который генерирует маркер безопасного доступа пользователя. В маркер безопасного доступа вводится и другая информация, в том числе о назначенных пользователю правах (разрешениях), ID сеанса пользователя (уникален для каждого сеанса), маске разрешений с детальным описанием типа запрошенного доступа. Права, назначенные пользователю, можно увидеть с помощью команды

WHOAMI /all

Если программа обращается от лица пользователя к защищенному ресурсу, то монитор защиты (security reference monitor) Windows запрашивает у программы маркер безопасного доступа пользователя. Затем монитор защиты анализирует маркер, чтобы определить эффективные разрешения пользователя, и разрешает или запрещает выполнение запрошенной пользователем операции. Эффективные разрешения более подробно описаны ниже.

Файловые разрешения NTFS

Файловые разрешения NTFS определяют пользователей, которые могут просматривать или обновлять файлы. Например, с помощью файловых разре-

шений NTFS можно разрешить отделам кадров доступ к файлам персонала и запретить доступ к этим файлам для остальных пользователей [1].

Файловые разрешения NTFS для пользователей и системных папок, назначаемые по умолчанию, соответствуют стандартным требованиям.

Для различных типов файлов назначаются отдельные разрешения.

- Пользовательские файлы. Пользователи получают полный доступ к своим файлам. Администраторы также получают полный доступ. Другие пользователи без административных привилегий не могут читать или записывать данные в эти файлы.
- Системные файлы. Пользователи могут читать папку %SystemRoot% и ее подпапки, но не могут записывать данные в них. Администраторы могут добавлять и обновлять файлы. Таким образом, лишь администраторы могут устанавливать обновления и приложения.
- Программные файлы. Аналогично разрешениям для системных файлов, разрешения для папки %ProgramFiles% позволяют пользователям запускать приложения, а администраторам они позволяют устанавливать программы. Пользователи в этом случае получают право чтения, а администраторы - полный доступ. Кроме того, все новые папки, создаваемые в корне диска, предоставят администраторам полный доступ, а пользователям — право чтения.
- Разрешения, назначаемые файлам и папкам по умолчанию, соответствуют требованиям настольных сред. Однако файловые серверы требуют назначать разрешения группам пользователей, чтобы обеспечить возможность совместной работы. Например, можно создать папку, которую смогут читать и обновлять все пользователи отдела маркетинга, с запретом доступа для всех пользователей вне этой группы.

Если в Windows используется файловая система NTFS (а не FAT), то все файлы, папки, разделы реестра и многие другие объекты имеют разрешения NTFS. Разрешения NTFS применяются как при локальном, так и при дистанционном доступе к объекту. Для просмотра и изменения разрешений NTFS файла или папки достаточно щелкнуть правой кнопкой мыши на объекте, выбрать пункт Properties и перейти к вкладке Security.

В Таблице 1 показаны 7 суммарных разрешений NTFS. Суммарные разрешения представляют собой различные комбинации 14 более детализированных разрешений, показанных в Таблице 2. Просмотреть детализированные разрешения можно, открыв диалоговое окно Advanced Security Settings для объекта щелчком на кнопке Advanced во вкладке Security, а затем щелкнуть на кнопке Edit во вкладке Permissions. Знакомиться с детализированными разрешениями объекта (особенно требующего повышенной безопасности) - полезная привычка, хотя для этого требуется больше усилий. Суммарные разрешения не всегда точно отражают состояние детализированных разрешений.

Аналогично разрешению Full Control Share, разрешение Full Control NTFS предоставляет владельцам большие возможности. Пользователи, не являющиеся администраторами, часто имеют разрешение Full Control в своем домашнем каталоге и других файлах и папках. Как уже отмечалось, обладатель прав тако-

го уровня может изменять разрешения файла и назначить себя владельцем. Вместо того чтобы предоставлять пользователям разрешение Full Control, можно дать им лишь право Modify. Если пользователь - владелец файла, то при необходимости можно вручную запретить ему изменять разрешения.

Технически, разрешения NTFS известны как избирательные списки управления доступом (discretionary ACL - DACL). Разрешения аудита известны как системные ACL (SACL). Большинство защищенных объектов NTFS располагают разрешениями обоих видов.

Влияние доверительных отношений Windows

По умолчанию все домены и леса Windows 2000 и более поздних версий имеют двусторонние доверительные отношения со всеми другими доменами леса. Если домен доверяет другому домену, то все пользователи в доверенном домене имеют те же разрешения безопасности в доверяющем домене, что и группа Everyone и группа Authenticated Users доверяющего домена. В любом домене многие разрешения этим группам назначаются по умолчанию, и доверительные отношения неявно обеспечивают широкие права, которые не были бы предоставлены в ином случае. Следует помнить, что если доверительные отношения не носят выборочного характера, то любые разрешения, предоставляемые группам Everyone и Authenticated Users, назначаются и всем другим пользователям в лесу.

Проверка разрешений из командной строки

Администраторы часто используют такие инструменты командной строки, как subinacl.exe, xacls.exe и cacls.exe для проверки разрешений NTFS. Subinacl входит в набор ресурсов Windows Server 2003 Resource Kit Tools, и программу можно загрузить отдельно из адреса http://www.microsoft.com/downloads/details.aspx?familyid=e8ba3e56-d8fe-4a91-93cf-ed6985e3927b&displaylang=en.

С помощью Subinacl можно просматривать и изменять разрешения NTFS для файлов, папок, объектов, разделов реестра и служб. Самая важная возможность Subinacl - скопировать разрешения пользователя, группы или объекта и применить их к другому пользователю, группе или объекту в том же или другом домене. Например, при перемещении пользователя из одного домена в другой в Windows создается новая учетная запись user; все ранее существовавшие SID или разрешения, связанные с первоначальным пользователем, отменяются. Скопировав разрешения в новую учетную запись user с помощью Subinacl, можно сделать их идентичными.

Xcacls функционирует аналогично Subinacl и входит в состав комплекта ресурсов Windows 2000 Server Resource Kit. Программу можно также загрузить по адресу http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/xcacls-o.asp.

Программа Cacls описана в опубликованной компанией Microsoft статье "Undocumented CACLS: Group Permissions Capabilities" (http://support.microsoft.com/?kbid=162786). Это более старый инструмент, который появился в составе Windows со времени Windows NT. Cacls не столь полезна, как Subinacl или Xacls, но утилита всегда имеется в системе Windows. С

помощью Cacls можно просматривать и изменять файлы и разрешения по пользователям и группам, но не создавать детализированные разрешения NTFS. В настоящее время возможности Cacls ограничены работой с разрешениями No Access, Read, Change и Full Control, которые соответствуют разрешениям NTFS, но не разрешением Share. Кроме того, разрешение Read программы Cacls соответствует разрешению Read & Execute системы NTFS.

Наследование

По умолчанию все файлы, папки и разделы реестра наследуют разрешения от родительского контейнера. Наследование можно активизировать или отключить для индивидуальных файлов, папок или разделов реестра и для отдельных пользователей или групп. Администратор может назначить разрешение (для отдельных пользователей), которые наследуются или нет.

Если файл или папка наследует большинство своих разрешений, но имеет также и набор явно заданных разрешений, то последние имеют приоритет перед унаследованными правами. Например, можно предоставить пользователю разрешение Full Control-Deny в корневом каталоге конкретного тома, и задать наследование этих разрешений всеми файлами и папками диска. Затем можно назначить любому файлу или папке на диске право доступа, которое отменяет унаследованный режим Full Control-Deny.

Эффективные разрешения

Монитор защиты Windows определяет эффективные разрешения пользователей (реальные разрешения, которыми они располагают на практике) с учетом нескольких факторов. Как отмечалось выше, монитор защиты сначала собирает информацию об индивидуальной учетной записи пользователя и всех группах, к которым он принадлежит, и обобщает все разрешения, назначенные всем пользовательским и групповым SID. Если разрешения Deny и Allow существуют на одном уровне, то, как правило, приоритет имеет Deny. Если приоритет получает Full Control-Deny, то пользователь, как правило, не имеет доступа к объекту.

По умолчанию при учете разрешений NTFS и Share (пользователь подключается к ресурсу через сеть) монитор защиты должен собрать все разрешения Share и NTFS. В результате эффективные разрешения пользователя представляют собой набор разрешений, предоставленных как разрешениями Share, так и NTFS.

Например, в конечном итоге у пользователя могут оказаться Share-разрешения Read и Change, и NTFS-разрешения Read и Modify. Эффективные разрешения - самый ограниченный набор разрешений. В данном случае разрешения почти идентичны. Эффективными разрешениями будут Read и Change/Modify. Многие администраторы ошибочно полагают, что эффективные разрешения - только Read, из-за плохих, чрезмерно упрощенных примеров или устаревшей документации.

В диалоговом окне Advanced Security Settings в Windows XP и более новых версиях появилась вкладка Effective Permissions. К сожалению, на вкладке Effective Permissions отражаются только разрешения NTFS. Не учитывается влияние разрешений Share, групп на базе действий, членства в которых пользо-

ватель не имеет, и других факторов, таких как файловая система с шифрованием (Encrypting File System - EFS). Если EFS активизирована для файла или папки, то пользователь с соответствующими разрешениями NTFS и Share может лишиться возможности доступа к объекту, если не имеет права доступа EFS к папке или файлу.

Рекомендации по работе с файлами и папками:

- Осмотрительно предоставлять разрешения Full Control обычным пользователям. Полезно назначить им вместо этого разрешение Modify. В большинстве случаев такой подход обеспечивает пользователям все необходимые разрешения, не позволяя изменять права или присваивать себе владение.
- Аккуратно работать с группой Everyone; лучше использовать группу Authenticated Users (или Users), или специальную группу с ограниченными правами. Важные упущения группы Authenticated Users - отсутствие Guest и неаутентифицированного пользователя.
- Нередко сетевых администраторов просят ввести гостевые учетные записи для сторонних пользователей (например, консультантов, подрядчиков, внештатных программистов). Но права обычного пользователя часто избыточны для гостя. Следует сформировать и использовать группу, права которой по умолчанию сильно урезаны (например, разрешение Full Control-Deny для корневых каталогов), а затем явно разрешить доступ только к файлам и папкам, необходимым данной гостевой учетной записи. Явно назначаемые разрешения предпочтительны, поскольку предоставляют гостевым пользователям именно те разрешения, которые необходимы для их работы, но не больше.
- Следует проявлять осторожность, налагая запреты на группы Everyone и Users, так как администраторы входят и в эти группы.
- В случае доверительных отношений с другими доменами полезно применять одностороннее и селективное доверие, чтобы ограничить права пользователей доверенного домена.
- Необходимо периодически осуществлять аудит разрешений NTFS и Share, чтобы убедиться в том, что они максимально ограничены.

Таблица 2 - Сводка разрешений NTFS

Разрешение	Действие
Read	Обеспечивает просмотр, копирование, печать и переименование файлов, папок и объектов. Не позволяет запускать выполняемые программы, кроме файлов сценариев. Позволяет считывать разрешения объектов, атрибуты объектов и расширенные атрибуты (например, бит Archive, EFS). Позволяет составить список файлов и под-

	папок папки
Write	Разрешения чтения, плюс создание и перезапись файлов и папок
List Folder Content (Folders Only)	Позволяет просматривать имена файлов и подпапок внутри папки
Read & Execute	Чтение разрешений и запуск программных файлов
Modify	Предоставляет все разрешения, кроме возможности присвоить владение и назначать разрешения. Позволяет читать, удалять, изменять и перезаписывать файлы и папки
Full Control	Обеспечивает полное управление папками и файлами, в том числе позволяет назначать разрешения
Special Permissions	Позволяет составлять комбинации из 14 более детальных разрешений, которые не входят ни в одно из остальных 6 суммарных разрешений. К этой группе относится разрешение Synchronize

Таблица 3 - Детальные разрешения NTFS

Разрешение	Действие
Traverse Folder / Execute File	Traverse Folder позволяет перемещаться по папкам для доступа к другим файлам и папкам, даже если субъект безопасности не имеет разрешений в транзитной папке. Применяется только к папкам. Traverse Folder вступает в силу, только если субъект безопасности не имеет разрешения Bypass traverse checking user (предоставляется группе Everyone по умолчанию). Execute File позволяет запускать программные файлы. Назначение разрешения Traverse Folder для папки не устанавливает автоматически разрешения Execute File для всех файлов в папке
List Folder / Read Data	Обеспечивает просмотр имен файлов и подпапок в папке. List Folder воздействует толь-

	ко на содержимое папки -- оно не влияет на то, будет ли внесена в список папка, для которой назначается разрешение. Read Data позволяет просматривать, копировать и печатать файлы
Read Attributes	Субъект безопасности видит атрибуты объекта (например, Read-only, System, Hidden)
Read Extended Attributes	Субъект безопасности видит расширенные атрибуты объекта (например, EFS, Compression)
Create Files / Write Data	Create Files позволяет создавать файлы внутри папки (применяется только к папкам). Write Data позволяет вносить изменения в файл и перезаписывать существующий контент (применяется только к файлам)
Create Folders / Append Data	Create Folders позволяет создавать папки внутри папки (применяется только к папкам). Append Data позволяет вносить изменения в конец файла, но не изменять, удалять или перезаписывать существующие данные (применяется только к файлам)
Write Attributes	Определяет, может ли субъект безопасности записывать или изменять стандартные атрибуты (например, Read-only, System, Hidden) файлов и папок. Не влияет на содержимое файлов и папок, только на их атрибуты.
Write Extended Attributes	Определяет, может ли субъект безопасности записывать или изменять расширенные атрибуты (например, EFS, Compression) файлов и папок. Не влияет на содержимое файлов и папок, только на их атрибуты
Delete Subfolders and Files	Позволяет удалять подпапки и файлы, даже если разрешение Delete не предоставлено подпапке или файлу
Delete	Позволяет удалять папку или файл. При отсутствии разрешения Delete для файла или папки ее можно удалить, если имеется разрешение Delete Subfolders and Files в роди-

	тельской папке
Read Permissions	Позволяет читать разрешения (например, Full Control, Read, Write) файла или папки. Не позволяет прочитать сам файл
Change Permissions	Позволяет изменять разрешения (например, Full Control, Read, Write) файла или папки. Не позволяет изменять сам файл
Take Ownership	Определяет, кто может быть владельцем файла или папки. Владельцы всегда могут иметь Full Control, и их разрешения в файле или папке не могут быть постоянно отменены, если при этом не отменяется и право владения
Synchronize	Администраторы редко используют это разрешение. Применяется для синхронизации в многопотоковых, многопроцессных программах и определяет взаимодействие между несколькими потоками, которые обращаются к одному ресурсу

Улучшение производительности NTFS

Файловая система NTFS – огромная базы данных, которая отслеживает все файлы на жестком диске. Когда файл создается, редактируется, а затем сохраняется, NTFS создает запись о времени создания или модификации файла, эту информация впоследствии видна в свойствах файла. NTFS также создает и отслеживает и другие временные метки при доступе к файлу. Например, метки последнего доступа, последнего открытия, сохранения и изменения файла. Каждое действие NTFS по обновлению свойств файла сопровождается операциями чтения/записи диска. В том случае, если информация в таких метках не интересна, можно не без причины решить, что эти дополнительные операции чтения/записи несколько расточительны.

Если используются некие инструменты поиска в файлах, которые часто получают доступ к множеству файлов на чтение, модифицируя атрибут со временем последнего доступа, в таком случае нагрузка на дисковую подсистему сильно возрастает и общая производительность ухудшается. Можно отключить использование меток при доступе к фалам при помощи команды *FSUtil*.

Использование команды FSUTIL

Нажать Пуск > Выполнить, и ввести cmd

В открывшейся командной строке ввести следующую команду:

FSUTIL behavior set disablelastaccess 1

Если требуется вернуть атрибут со временем последнего доступа, то повторить команду и заменить 1 на 0.

Сохранение разрешений NTFS при копировании или перемещении файлов

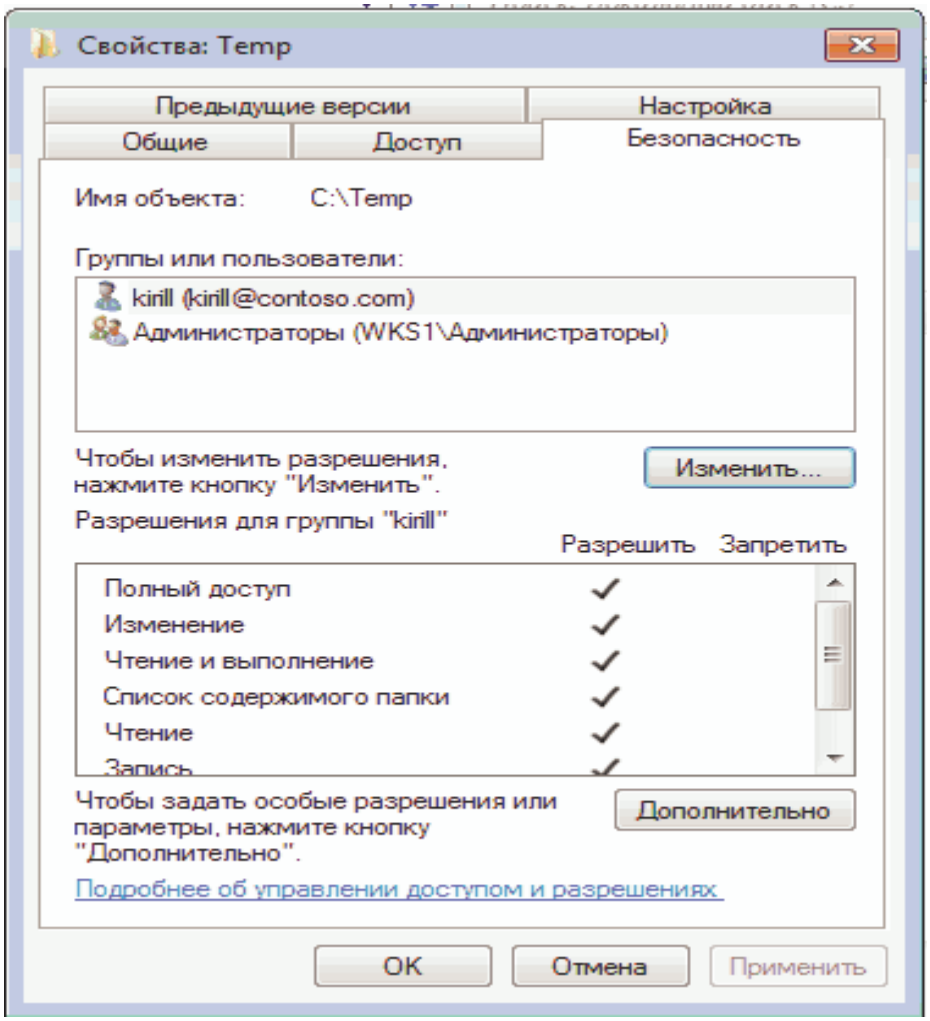

Рис. 2. Разрешения на папку

В файловой системе NTFS каждый объект (файл или папка) имеет свой список контроля доступа (Access Control List, ACL), в котором содержится информация о том, кто (или что) имеет доступ к объекту и какие операции разрешено (или запрещено) этому субъекту проводить над объектом. А что происходит с ACL при копировании или перемещении объекта?

Например, создать пользователем папку *Temp* в корне диска C. Открыть свойства папки и посмотреть ее разрешения (рис.2). В списке доступа есть только группа локальных администраторов и пользователь kirill .

С помощью Проводника скопировать папку Temp на другой компьютер *SRV1*, также в корень диска *C*.

Если посмотреть разрешения скопированной папки, то видно, что они полностью изменились.

Для того чтобы понять, откуда взялись новые разрешения, пройти в дополнительные параметры безопасности папки (кнопка Advanced). Все разрешения папки Temp унаследованы от диска *C* компьютера *SRV1*.

По умолчанию разрешения NTFS сохраняются только при копировании\перемещении в пределах **одного логического диска**, или тома. Если же объект перемещается на другой диск того же (или другого) компьютера, то все разрешения заменяются наследуемыми от родительского объекта, которым в примере является диск *C* компьютера *SRV1*.

В примере скопирована всего лишь одна папка с несколькими файлами, поэтому при необходимости восстановить утерянные разрешения несложно. А если подобное случиться при переносе серьезного файлового ресурса с высоким уровнем вложенности и сложной структурой разрешений NTFS, заданных вручную?

К сожалению, проводник Windows не умеет копировать разрешения файловой системы, для этого используются альтернативные средства.

Утилита Icacls

Эта утилита специально предназначена для работы с ACL. В числе прочего она может сохранить список доступа указанного объекта в файл, а затем применить этот список к указанному объекту.

Открыть командную консоль и сохранить ACL исходного каталога Temp со всем его содержимым (подкаталоги и файлы) в файл tempACL командой:

Icacls C:\Temp* /save tempACL /t

По умолчанию утилита сохраняет файл в профиле пользователя — C:\Users\Имя_пользователя. Это обычный текстовый файл, который при желании можно открыть в Блокноте.

Перенести созданный файл tempACL на SRV1 и восстановить из него ACL каталога Temp командой:

Icacls C:\temp /restore C:\tempACL

Затем еще раз посмотреть разрешения скопированной папки Temp и увидеть, что и исходные разрешения восстановлены.

Утилита Xcopy

Xcopy является продвинутым вариантом команды Copy и в отличие от нее умеет работать с сетевыми путями, а также копировать сведения о владельце и данные ACL объекта.

В примере для того, чтобы скопировать каталог Temp на SRV1 с сохранением списков доступа пользуются командой:

Xcopy C:\Temp \\SRV1\C$\Temp /E /O

Total Commander

Можно воспользоваться файловым менеджером стороннего производителя, например Total Commander.

В нем при копировании\переносе есть возможность скопировать разрешения NTFS, просто отметив флажок ☑ «Copy NTFS permissions».

И в завершение один важный момент, который надо учитывать при перемещении файловых ресурсов - разрешения NTFS можно свободно переносить только в пределах одного домена или леса доменов.

Если, например, скопировать папку со списком доступа на компьютер, не входящий в домен, то получим интересную ситуацию: ACL перенесен, но в локальной базе учетных записей нет такого пользователя.

В этом случае при просмотре разрешений в списке доступа будет показан ошибочный идентификатор пользователя.

Разрешения Share

Каждый защищенный объект Windows - в том числе файлы, папки, общие ресурсы, принтеры и разделы реестра - поддерживает разрешения безопасности.

Любую папку Windows можно сделать общедоступной, чтобы разрешить дистанционный доступ.

Разрешения Share можно назначать любым объектам folder и printer в Windows, но разрешения применяются, только если обращение к объекту происходит через сетевой ресурс.

К разрешениям Folder Share относятся Full Control, Change и Read.

Субъекты безопасности, которым присвоено право полного доступа (Full Control) к объекту, могут производить с объектом почти любые операции.

Они могут удалить, переименовать, копировать, переместить и изменить объект.

Пользователь с правом *Full Control* может изменить разрешения Share объекта и стать владельцем объекта (если он уже не является владельцем и не имеет разрешения Take Ownership).

Таким образом, любой пользователь с разрешением Full Control может отменить разрешения других лиц, в том числе администратора (хотя администратор может всегда вернуть себе владение и разрешения).

Возможность изменять разрешения - обязательное требование любой операционной системы с избирательным управлением доступом (discretionary access control - DAC), такой как Windows.

В большинстве случаев, основное разрешение доступа к ресурсу, необходимое обычным пользователям - *Change*.

С помощью разрешения Change пользователь может добавлять, удалять, изменять и переименовывать любые ресурсы в соответствующей папке.

Разрешение *Read* обеспечивает просмотр, копирование, переименование и печать объекта.

Пользователь с разрешением Read может копировать объект в другое место, в котором имеет право Full Control.

Создание разделяемого ресурса на Windows Server® 2008 R2 с квотами

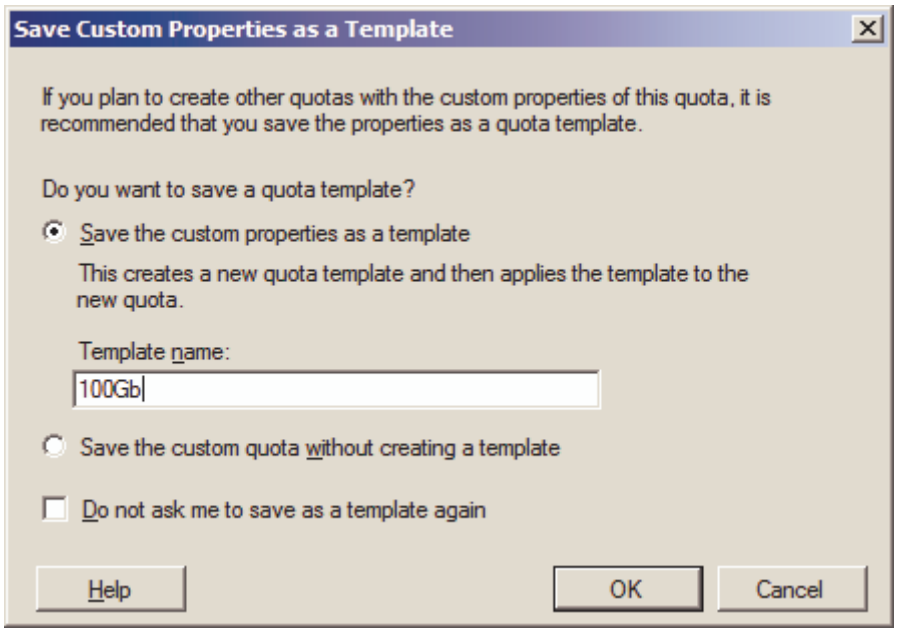

Рис. 3. Создание квоты

Рассмотрена установка файлового сервера и настройки каталога общего доступа с возможностью установки квот. Квота - это ограничение на использование чего-либо, в данном случае - дискового пространства. Установка включает шаги:

1. Создать на диске каталог, который будет раделяться.

2. Добавить роль файлового каталога:

    a. Открыть оснастку Server Manager

    b. где в меню выбрать Roles, а в поле ролей нажать Add roles

    c. в появившемся Мастере добавления ролей отметить галочкой File Services

    d. в окне выбора ролей сервиса – выбрать «File Server Resource Manager», данная роль предназначена для создания и распределения квот

    e. пропустить окно мониторинга использования дискового пространства

    f. запустить установку:

3. Создание квоты дискового пространства:

a. Запустить оснастку «File Server Resource Manager» через Start > Administrative Tools.

b. В меню «Actions» выбрать «Create Quota», где в строке адреса нужно прописать путь к папке, к которой назначается квота.

c. Выбрать «Custom properties», где в поле «Space limit» вписать нужное значение дискового пространства (в примере – 100Gb)

d. В разделе «Notification tresholds» нажать «Add» для определения дополнительных параметров «Журнал событий» (Создание события)

e. Во вкладке «Reports» выбрать параметры создания отчёта

f. Сохранить все настройки порога

g. Сохранить текущую квоту как шаблон

4. Создание общего доступа:

a. Запустить оснастку «Share and Storage Management», где в меню «Actions» выбрать «Provision Share»

b. В запустившемся мастере выбрать путь к папке общего доступа

c. Пропустить определение разрешений безопасности NTFS.

d. Определить имя общего ресурса, отображаемое в сети

e. Определить разрешения общего доступа для ресурса (по умолчанию – «Все – для чтения»)

f. Определение политики квот – выбрать созданную политику

g. Определение политики фильтра содержимого – выбрать нужный фильтр файлов (Блокировать медиа-файлы)

h. Пропустить шаг публикации DFS-имени

i. Закончить создание клавишей «Create»

Теперь имеется разделяемая папка с фильтром содержимого и квотой переполнения.

Некоторые особенности общего доступа Windows Server® 2008 R2

Для администраторов Windows, которым часто приходится работать с хранением и общим доступом в своих инфраструктурах Windows, инструмент

управления хранением и общим доступом **Windows Server 2008 Share and Storage Management** является обязательным инструментом, который нужно использовать ежедневно. Каково назаначение инструмента и как его использовать?

Существует гораздо больше задач, которые можно выполнить помимо создания ресурса.

Ниже приведены 6 основных задач, которые можно выполнить с помощью этого инструмента:

1. Создать хранилища (Provision storage) - это отличная функция для серверов с большим количеством хранилищ, на которых часто изменяют, добавляют и удаляют хранилища сервера. Хранилище, которое создается, может представлять собой либо LUN, либо локальный том. Однако следует учитывать, что невозможно создать хранилище, если нет специально выделенного места под это хранилище.
2. Увеличить том
3. Форматировать том
4. Изменить свойства тома, включая доступ к таким инструментам, как дефрагментация и проверка ошибок
5. Запретить общий доступ к ресурсу
6. И даже управлять общим доступом и хранилищами на других компьютерах

Диагностика Share and Storage Management

Этот инструмент может помочь в диагностировании управления общим доступом и хранилищами, позволяя работать с сеансами и открытыми файлами.

Инструмент можно использовать для просмотра того, кто к какому ресурсу подключен, и какие файлы они открывали.

При необходимости можно Запретить общий доступ **(Stop Sharing)** к определенному ресурсу.

Следует обратить внимание на то, что отсутствует возможность «Удалить ресурс» **(‘Delete a Share’)**, она просто называется Stop Sharing.

Инструмент Share and Storage Management может также помочь решить общие проблемы.

В руководстве **Microsoft TechNet Share and Storage Management** приведен список 8 распространенных проблем, связанных с общим доступом и хранением, которые можно решить с помощью данного инструмента.

Существует также проблема, когда имелась разделяемая папка с общим доступом, и без причины при входе в неё по сети требуется логин и пароль, хотя на другом ПК нет защиты при входе.

Причина в безопасности **Windows**, чтобы избежать такой ситуации, нужно знать IP-адрес компьютера, к которому подключаются: если в IP-параметрах установлено Получть IP-адрес автоматически, значит нужно присвоить IP-адрес вручную и заменить в свойствах папки (Диска), имя компьютера на IP-адрес.

Тема 7. Локальная политика безопасности. Часть 1.

Конфигурирование политик безопасности

Политика безопасности – это набор параметров, которые регулируют безопасность компьютера и управляются с помощью локального объекта GPO [2]. Настраивать данные политики можно при помощи оснастки **«Редактор локальной групповой политики»** или оснастки **«Локальная политика безопасности»**. Оснастка **«Локальная политика безопасности»** используется для изменения политики учетных записей и локальной политики на локальном компьютере, а политики учетных записей, привязанных к домену Active Directory можно настраивать при помощи оснастки **«Редактор управления групповыми политиками»**. Перейти к локальным политикам безопасности, можно следующими способами:

1. Нажать кнопку **«Пуск»** для открытия меню, в поле поиска ввести *Локальная политика безопасности* и открыть приложение в найденных результатах;
2. В диалоговом окне **«Выполнить»**, в поле **«Открыть»** ввести *secpol.msc* и нажать кнопку **«ОК»**;
3. Открыть **«Консоль управления ММС»**. Для этого нажать кнопку **«Пуск»**, в поле поиска ввести *mmc*, а затем нажать кнопку **«Enter»**. Откроется пустая консоль ММС. В меню **«Консоль»** выбрать команду **«Добавить или удалить оснастку»** или воспользоваться комбинацией клавиш **Ctrl+M**. В диалоге **«Добавление и удаление оснасток»** выбрать оснастку **«Редактор локальной групповой политики»** и нажать кнопку **«Добавить»**. В появившемся диалоге **«Выбор объекта групповой политики»** нажать кнопку **«Обзор»** для выбора компьютера или нажать на кнопку **«Готово»** (по умолчанию установлен объект **«Локальный компьютер»**). В диалоге **«Добавление или удаление оснасток»** нажать кнопку **«ОК»**. В оснастке **«Редактор локальной групповой политики»** перейти в узел **«Конфигурация компьютера»**, а затем открыть узел **«Параметры безопасности»**.

В том случае, если компьютер подсоединен к домену Active Directory, политика безопасности определяется политикой домена или политикой подразделения, членом которого является компьютер.

Применение политик безопасности для локального компьютера и для объекта групповой политики рабочей станции, подсоединенной к домену

При помощи следующих примеров видна разница между применением политики безопасности для локального компьютера и для объекта групповой политики рабочего компьютера, присоединенного к домену Windows Server 2008 R2.

Применение политики безопасности для локального компьютера

Для успешного выполнения текущего примера, учетная запись, под которой выполняются данные действия, должна входить в группу «Администраторы» на локальном компьютере.

Если компьютер подключен к домену, то эти действия могут выполнять только пользователи, которые являются членами группы **«Администраторы домена»** или групп, с разрешенными правами на редактирование политик.

В примере ниже переименуем гостевую учетную запись. Для этого выполнить следующие действия:

1. Открыть оснастку **«Локальные политики безопасности»** или перейти в узел **«Параметры безопасности»** оснастки **«Редактор локальной групповой политики»**;
2. Перейти в узел **«Локальные политики»**, а затем **«Параметры безопасности»**;
3. Открыть параметр **«Учетные записи: Переименование учетной записи гостя»** дважды щелкнув на нем или нажав на клавишу **Enter**;
4. В текстовом поле ввести *Гостевая запись* и нажать кнопку **«ОК»**;
5. Перезагрузить компьютер.

После перезагрузки компьютера, для того чтобы проверить, применилась ли политика безопасности к компьютеру, нужно открыть в панели управления компонент **«Учетные записи пользователей»** и перейти по ссылке **«Управление другой учетной записью»**.

В открывшемся окне показаны все учетные записи, созданные на локальном компьютере, в том числе переименованная учетная запись гостя:

Применение политики безопасности для объекта групповой политики рабочего компьютера, присоединенного к домену Windows Server® 2008 R2

В следующем примере запретим пользователю Test_ADUser изменять пароль для учетной записи на своем компьютере.

Для выполнения следующих действий надо входить в группу **«Администраторы домена»**. Выполнить следующие действия:

1. Открыть **«Консоль управления MMC»**. Для этого нажать на кнопку **«Пуск»**, в поле поиска ввести *mmc*, а затем нажать кнопку **«Enter»**;
2. В меню **«Консоль»** выбрать команду **«Добавить или удалить оснастку»** или нажать комбинацию клавиш **Ctrl+M**;
3. В диалоге **«Добавление и удаление оснасток»** выбрать оснастку **«Редактор локальной групповой политики»** и нажать кнопку **«Добавить»**;
4. В появившемся диалоге **«Выбор объекта групповой политики»** нажать кнопку **«Обзор»** для выбора компьютера и выбрать нужный компьютер, как показано на рис. 4:

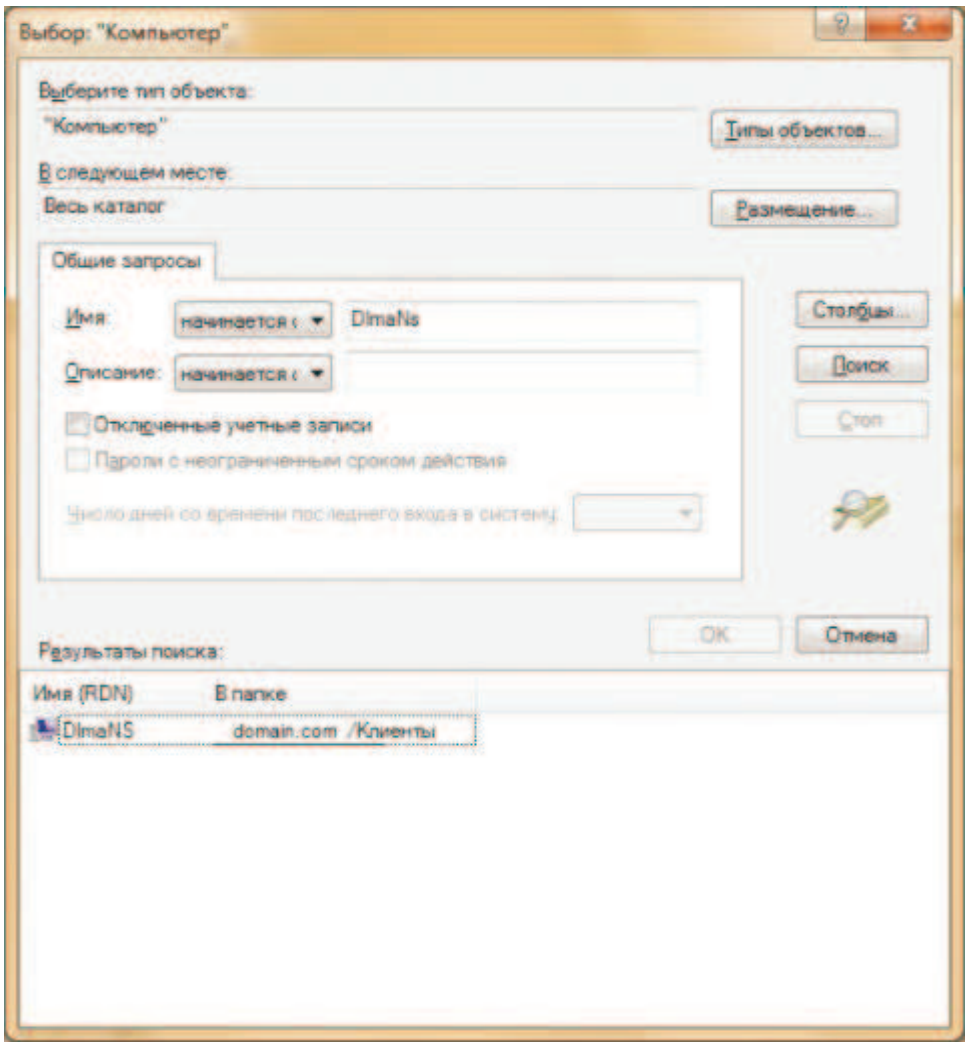

Рис. 4 Выбор компьютера

5. В диалоге **«Выбор объекта групповой политики»** убедиться, что выбран нужный компьютер и нажать кнопку **«Готово»**;
6. В диалоге **«Добавление или удаление оснасток»** нажать кнопку **«ОК»**;
7. В оснастке **«Редактор локальной групповой политики»** перейти в узел **«Конфигурация компьютера»**, а затем открыть узел **Параметры безопасности\Локальный компьютер\Параметры безопасности**;
8. Открыть параметр **«Контроллер домена: Запретить изменение пароля учетных записей компьютера»** дважды щелкнув на нем или нажав на клавишу **Enter**;
9. В диалоге настроек параметра политики безопасности выбрать опцию **«Включить»** и нажать кнопку **«ОК»**;
10. Перезагрузить компьютер.

После перезагрузки компьютера, для того чтобы проверить, применилась ли политика безопасности, перейти на компьютер, с которым проводились изменения и открыть консоль управления MMC.

В ней добавить оснастку **«Локальные пользователи и группы»** и попробовать изменить пароль для своей доменной учетной записи.

Применение политики безопасности для объекта групповой политики с контроллера домена Windows Server 2008 R2

При помощи следующего примера, изменим число новых уникальных паролей, которые должны быть назначены учетной записи пользователя до повторного использования старого пароля. Эта политика позволяет улучшать безопасность, гарантируя, что старые пароли не будут повторно использоваться в течении нескольких раз. Войти на контроллер домена или использовать средства администрирования удаленного сервера. Выполнить следующие действия:

1. Открыть консоль **«Управление групповой политикой»** - в диалоговом окне **«Выполнить»**, в поле **«Открыть»** ввести *gpmc.msc* и нажать **«ОК»**;
2. В контейнере **«Объекты групповой политики»** щелкнуть правой кнопкой мыши и из контекстного меню выбрать команду **«Создать»**;
3. В поле **«Имя»** ввести название объекта GPO, например **«Объект политики, предназначенный для тестирования»** и нажать **«ОК»**;
4. Щелкнуть правой кнопкой мыши на созданном объекте и из контекстного меню выбрать команду **«Изменить»**;
5. В окне **«Редактор управления групповыми политиками»** развернуть узел **Конфигурация компьютера\Политики\Конфигурация Windows\Параметры безопасности\Политики учетных записей\Политика паролей**;
6. Открыть параметр **«Вести журнал паролей»** дважды щелкнув на нем или нажав на клавишу **Enter**;
7. В диалоге настройки параметра политики установить флажок на опции **«Определить следующий параметр политики»**, в тестовом поле ввести 5 и нажать **«ОК»**;
8. Закрыть оснастку **«Редактор управления групповыми политиками»**.
9. В консоли **«Управление групповой политикой»** нажать правой кнопкой мыши на группе безопасности, для которой будут применяться изменения, и из контекстного меню выбрать команду **«Связать существующий объект групповой политики…»**. В диалоге **«Выбор объекта групповой политики»** выбрать созданный объект.
10. В фильтрах безопасности объекта политики выбрать пользователя или группу, на которых будет распространяться указанные настройки.
11. Обновить параметры политики на клиентском компьютере при помощи команды **gpupdate**.

Тема 8. Локальная политика безопасности. Часть 2: Политики учетных записей

Применение «Политики учетных записей» распространено в предприятиях с доменной средой. Для обеспечения безопасности компьютеров, применение политик этой группы на компьютерах, не входящих в доменную среду (например, использование политик на домашнем компьютере) поможет существенно повысить безопасности компьютера [2].

Для того чтобы найти политики, предназначенные для управления учётными записями, в редакторе управления групповыми политиками надо открыть узел **Конфигурация компьютера\Параметры безопасности\Политики учетных записей**. В этом узле имеются следующие политики.

Политика паролей

При помощи этого узла можно изменять настройки паролей учетных записей пользователей, которые состоят как в домене, так и в рабочих группах. В организациях можно применять одинаковые политики паролей для всех пользователей, входящих в домен или только для отдельных групп при помощи оснастки «Консоль управления групповыми политиками». В узле «Политика паролей» можно использовать до шести политик безопасности, при помощи которых можно указать наиболее важные параметры безопасности, применяемые для управления паролями учетных записей. Настоятельно рекомендуется не игнорировать данные политики. Если правильно настроить все шесть политик безопасности, расположенных в этом узле, безопасность паролей пользователей организации значительно повысится. Применив все политики, пользователям действительно придется создавать безопасные пароли, в отличие от тех, которые они считают «сложными». Доступны следующие политики безопасности:

Вести журнал паролей. Насколько не был бы ваш пароль безопасным, злоумышленник рано или поздно сможет его подобрать. Поэтому необходимо периодически изменять пароли учетных записей. При помощи этой политики вы можете указать количество новых паролей, которые назначаются для учетных записей до повторного использования старого пароля. После того как эта политика будет настроена, контроллер домена будет проверять кэш предыдущих хэш-кодов пользователей, чтобы в качестве нового пароля пользователи не могли использовать старый. Число паролей может варьироваться от 0 до 24. Т.е., если указано в качестве параметра число 24, то пользователь сможет использовать старый пароль с 25-ого раза.

Максимальные срок действия пароля. Эта политика указывает период времени, в течение которого пользователь может использовать свой пароль до последующего изменения. По окончанию установленного срока пользователь обязан изменить свой пароль, так как без изменения пароля войти в систему ему не удастся. Доступные значения могут быть установлены в промежутке от 0 до 999 дней. Если установлено значения равное 0, срок действия пароля неограничен. В связи с мерами безопасности желательно отказаться от такого выбора. Если значения максимального срока действия пароля варьируется от 1 до 999 дней, значение минимального срока должно быть меньше максимального. Лучше всего использовать значения от 30 до 45 дней.

Минимальная длина пароля. При помощи этой политики вы можете указать минимальное количество знаков, которое должно содержаться в пароле. Если активировать этот параметр, то при вводе нового пароля количество знаков будет сравниваться с тем, которое установлено в этой политике. Если количество знаков будет меньше указанного, то придется изменить пароль в соответствии с политикой безопасности. Можно указать значение политики от 1 до

14 знаков. Оптимальным значением для количества знаков для пароля пользователей является 8, а для серверов от 10 до 12.

Минимальные срок действия пароля. Многие пользователи не захотят утруждать себя запоминанием нового сложного пароля и могут попробовать сразу при вводе изменить такое количество новых паролей, чтобы использовать свой хорошо известный первоначальный пароль. Для предотвращения подобных действий была разработана текущая политика безопасности. Вы можете указать минимальное количество дней, в течение которого пользователь должен использовать свой новый пароль. Доступные значения этой политики устанавливаются в промежутке от 0 до 998 дней. Установив значение равное 0 дней, пользователь сможет изменить пароль сразу после создания нового. Необходимо обратить внимание на то, что минимальный срок действия нового пароля не должен превышать значение максимального срока действия.

Пароль должен отвечать требованиям сложности. Это одна из самых важных политик паролей, которая отвечает за то, должен ли пароль соответствовать требованиям сложности при создании или изменении пароля. В связи с этими требованиями, пароли должны:

- содержать буквы верхнего и нижнего регистра одновременно;
- содержать цифры от 0 до 9;
- содержать символы, которые отличаются от букв и цифр (например, !, @, #, $, *);
- Не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков.

В том случае, если пользователь создал или изменил пароль, который соответствует требованиям, то пароль пропускается через математический алгоритм, преобразовывающий его в хэш-код (также называемый односторонней функцией), о котором шла речь в политике **«Вести журнал паролей»**.

Хранить пароли, используя обратимое шифрование. Для того чтобы пароли невозможно было перехватить при помощи приложений, Active Directory хранит только хэш-код. Но если необходима поддержка приложений, использующих протоколы, требующие знание пароля пользователя для проверки подлинности, можно использовать текущую политику. Обратимое шифрование по умолчанию отключено, так как, используя эту политику, уровень безопасности паролей и всего домена в частности, значительно понижается. Использование этой функции аналогично хранению пароля в открытом виде.

По умолчанию все пароли в Windows должны отвечать политике безопасности. Чтобы изменить политику паролей надо зайти в «*Пуск*» — «*Администрирование*» — «*Локальная политика безопасности*». В открывшейся оснастке раскрыть ветку «*Политика учетных записей*» и «*Политику паролей*». Здесь можно изменять несколько параметров, в частности отключить политику «*Пароль должен отвечать требованиям сложности*».

Если переключатели, чтобы убрать политику, не активны, то войти в домене в администрирование → управление групповой политикой Default Domain

Policy, закладка параметры политики → конфигурация windows → параметры безопасности правый клик по «политика учетных записей/политика паролей» и изменить. Далее открыть Конфигурация компьютера → политики → конфигурация windows → параметры безопасности → политики учетных записей и поменять политику паролей. Там же можно запретить и разрешить изменение политики паролей в «локальной политике безопасности», тогда и появятся неактивные флажки.

Политика блокировки учетной записи

Даже после создания сложного пароля и правильной настройки политик безопасности, учетные записи ваших пользователей все еще могут быть подвергнуты атакам недоброжелателей. Например, если установлен минимальный срок действия пароля в 20 дней, у хакера достаточно времени для подбора пароля к учетной записи. Узнать имя учетной записи не является проблемой для хакеров, так как, зачастую имена учетных записей пользователей совпадает с именем адреса почтового ящика. А если будет известно имя, то для подбора пароля понадобится какие-то две-три недели.

Групповые политики безопасности Windows могут противостоять таким действиям, используя набор политик узла **«Политика блокировки учетной записи»**. При помощи данного набора политик, есть возможность ограничения количества некорректных попыток входа пользователя в систему. Для пользователей это может быть проблемой, так как не у всех получится ввести пароль за указанное количество попыток, но зато безопасность учетных записей перейдет на «новый уровень». Для этого узла доступны только три политики, которые рассматриваются ниже.

Время до сброса счетчиков блокировки. Active Directory и групповые политики позволяют автоматически разблокировать учетную запись, количество попыток входа в которую превышает установленное пороговое значение. При помощи этой политики устанавливается количество минут, которые должны пройти после неудачной попытки для автоматической разблокировки. Можно установить значение от одной минуты до 99999. Это значение должно быть меньше значения политики **«Продолжительность блокировки учетной записи»**.

Пороговое значение блокировки. Используя эту политику, можно указать количество некорректных попыток входа, после чего учетная запись будет заблокирована. Окончание периода блокировки учетной записи задается политикой **«Продолжительность блокировки учетной записи»** или администратор может разблокировать учетную запись вручную. Количество неудачных попыток входа может варьироваться от 0 до 999. Рекомендуется устанавливать допустимое количество от трех до семи попыток.

Продолжительность блокировки учетной записи. При помощи этого параметра можно указать время, в течение которого учетная запись будет заблокирована до ее автоматической разблокировки. Можно установить значение от 0 до 99999 минут. В том случае, если значение этой политики будет равно 0,

учетная запись будет заблокирована до тех пор, пока администратор не разблокирует ее вручную.

Политика Kerberos

В доменах Active Directory для проверки подлинности учетных записей пользователей и компьютеров домена используется протокол Kerberos. Сразу после аутентификации пользователя или компьютера, этот протокол проверяет подлинность указанных реквизитов, а затем выдает особый пакет данных, который называется **«Билет предоставления билета (TGT – Ticket Granting Ticket)»**. Перед подключением пользователя к серверу для запроса документа на контроллер домена пересылается запрос вместе с билетом TGT, который идентифицирует пользователя, прошедшего проверку подлинности Kerberos. После этого контроллер домена передает пользователю еще один пакет данных, называемый билетом доступа к службе. Пользователь предоставляет билет на доступ службе на сервере, который принимает его как подтверждение прохождения проверки подлинности.

Данный узел можно обнаружить только на контроллерах домена. Доступны следующие пять политик безопасности:

Максимальная погрешность синхронизации часов компьютера. Для предотвращения «атак повторной передачи пакетов» существует текущая политика безопасности, которая определяет максимальную разность времени, допускающую Kerberos между временем клиента и временем на контроллере домена для обеспечения проверки подлинности. В случае установки данной политики, на обоих часах должны быть установлены одинаковые дата и время. Подлинной считается та отметка времени, которая используется на обоих компьютерах, если разница между часами клиентского компьютера и контроллера домена меньше максимальной разницы времени, определенной этой политикой.

Максимальный срок жизни билета пользователя. При помощи данной политики можно указать максимальный интервал времени, в течение которого может быть использован билет представления билета (TGT). По истечении срока действия билета TGT необходимо возобновить существующий билет или запросить новый.

Максимальный срок жизни билета службы. Используя эту политику безопасности, сервер будет выдавать сообщение об ошибке в том случае, если клиент, запрашивающий подключение к серверу, предъявляет просроченный билет сеанса. Можно определить максимальное количество минут, в течение которого полученный билет сеанса разрешается использовать для доступа к конкретной службе. Билеты сеансов применяются только для проверки подлинности на новых подключениях к серверам. После того как подключение пройдет проверку подлинности, срок действия билета теряет смысл.

Максимальный срок жизни для возобновления билета пользователя. С помощью данной политики можно установить количество дней, в течение которых может быть восстановлен билет предоставления билета.

Принудительные ограничения входа пользователей. Эта политика позволяет определить, должен ли центр распределения ключей Kerberos прове-

рять каждый запрос билета сеанса на соответствие политике прав, действующей для учетных записей пользователей.

Локальные политики - Назначение прав пользователя

Эта политика определяет, какие пользователи и группы обладают правами на вход в систему и выполнение различных задач. Всего можно настроить 39 прав. Ниже рассмотрены некоторые права, наиболее важные для обеспечения безопасности ПК:

1. Доступ к компьютеру из сети
2. Локальный вход в систему
3. Разрешение входа в систему через службы терминалов
4. Архивирование файлов и каталогов
5. Изменение системного времени
6. Отказ в доступе к компьютеру из сети
7. Запрещение локального входа
8. Запрещение входа в систему через службы терминалов
9. Принудительное удаленное завершение работы
10. Создание журналов безопасности
11. Восстановление файлов и каталогов
12. Завершение работы системы
13. Смена владельца файлов или иных объектов

1. Доступ к компьютеру из сети

Это право пользователя определяет, каким пользователям и группам разрешается подключаться к компьютеру через сеть (т.е. «не пройдет» такой номер, как \\<имя ПК>\C$, удаленно подключиться к компьютеру через оснастку «Управление компьютером» и т.п.). Право не влияет на службы терминалов. Т.е. если лишить, допустим, администратора, права доступа к компьютеру из сети, то он все равно сможет подключиться с использованием терминального клиента (mstsc.exe). Конечно, если такое подключение разрешено.

По умолчанию имеют разрешение

На рабочих станциях и серверах: Администраторы, Операторы архива, Опытные пользователи, Пользователи, Все

На контроллерах домена: Администраторы, Прошедшие проверку, Все

Рекомендуется или вовсе лишить всех пользователей и группы этого права, либо подходить к предоставлению права доступа к компьютеру из сети с особой осторожностью. В любом случае рекомендуется удалить группу «Все». Однако следует заметить, что лишение этого права для некоторых пользователей и групп может привести к некоторым ошибкам в работе сетевых приложений.

2. Локальный вход в систему

Это право определяет пользователей, имеющих возможность интерактивно входить в систему. Данное право необходимо для входа пользователя в систему после одновременного нажатия клавиш CTRL+ALT+DEL на клавиатуре ком-

пьютера. Кроме того, это право на вход в систему может понадобиться некоторым службам или административным приложениям, во время работы которых происходит вход пользователей в систему. Если эта политика определена для пользователя или группы, группа «Администраторы» также должна получить это право. Иначе просто невозможно будет войти в систему в качестве администратора.

По умолчанию имеют право:

На рабочих станциях и серверах: «Администраторы», «Операторы архива», «Опытные пользователи», «Пользователи» и «Гость».

На контроллерах домена: «Операторы учета», «Администраторы», «Операторы архива», «Операторы печати» и «Операторы сервера».

Очень хорошо оставить это право только тем пользователям и группам, которые реально работают на компьютере. Различные группы типа «Гость», «Операторы архива» - лучше удалить.

3. Разрешение входа в систему через службы терминалов

Эта настройка безопасности определяет, каким пользователям и группам разрешается входить в систему в качестве клиента служб терминалов.

По умолчанию имеют право:

На рабочих станциях и серверах: «Администраторы», «Пользователи удаленного рабочего стола».

На контроллерах домена: «Администраторы».

Если не пользуетесь службой терминалов – то лучше лишить данного права всех пользователей и группы.

4. Архивирование файлов и каталогов

Это право пользователя определяет, какие пользователи могут архивировать содержимое системы, невзирая на имеющиеся разрешения для файлов, каталогов, реестра и других объектов.

Эта привилегия эквивалентна предоставлению указанным пользователям и группам следующих разрешений на доступ ко всем файлам и папкам системы:

- Обзор папок / Выполнение файлов
- Содержание папки / Чтение данных
- Чтение атрибутов
- Чтение дополнительных атрибутов
- Чтение разрешений. Предоставление этого права пользователю может быть связано с риском для безопасности. Назначать это право надо только надежным пользователям, чтобы исключить возможность хищения или копирования данных для их распространения.

По умолчанию имеют право: «Администраторы» и «Операторы архива».

Если у злоумышленника и нет разрешений на работы с некими файлами, но есть право архивирования файлов и каталогов, он может заархивировать интересующую его информацию, перенести на другой ПК и далее сделать с ней все, что ему надо.

5. Изменение системного времени

Это право пользователя определяет, какие пользователи и группы могут изменять время и дату на встроенных часах компьютера. Пользователи, обла-

дающие данным правом, могут изменять представление журналов безопасности. При изменении системного времени события будут заноситься в журнал с указанием измененного, а не реального времени.

Данное право пользователя определено в объекте групповой политики стандартного контроллера домена, а также в локальной политике безопасности рабочих станций и серверов.

По умолчанию имеют право:

На рабочих станциях и серверах: Администраторы, Опытные пользователи

На контроллерах домена: Администраторы, Операторы сервера.

6. Отказ в доступе к компьютеру из сети

Эта настройка безопасности определяет, каким пользователям запрещается доступ к данному компьютеру через сеть. Эта политика отменяет политику Доступ к компьютеру из сети, если учетная запись пользователя контролируется обеими политиками.

По умолчанию: Не определена.

Как видно из описания, данная политика имеет более высокий приоритет, чем политика «Доступ компьютера из сети», так что манипулировать ей нужно с особой осторожностью.

7. Запрещение локального входа

Эта настройка безопасности определяет, каким пользователям запрещается вход в систему на данном компьютере. Эта политика отменяет политику Локальный вход в систему, если учетная запись пользователя контролируется обеими политиками.

Применение этой политики безопасности к группе «Все» сделает невозможным локальный вход в систему.

По умолчанию Отсутствуют.

8. Запрещение входа в систему через службы терминалов

Этот параметр безопасности определяет, каким пользователям и группам запрещается входить в систему в качестве клиента служб терминалов.

По умолчанию: не установлено.

9. Принудительное удаленное завершение работы

Этот параметр безопасности определяет, каким пользователям разрешено завершать работу компьютера из удаленного узла сети. Неверное использование этого права пользователя может привести к атаке на службу.

Данное право пользователя определено в объекте групповой политики стандартного контроллера домена, а также в локальной политике безопасности рабочих станций и серверов.

По умолчанию имеют право на рабочих станциях и серверах: «Администраторы».

На контроллерах домена: «Администраторы», «Операторы сервера».

10. Создание журналов безопасности

Этот параметр безопасности определяет, какие учетные записи могут быть использованы процессом для добавления записей в журнал безопасности. Журнал безопасности используется для отслеживания попыток несанкционированного доступа в систему. Неправильное использование этого права может при-

вести к созданию множества событий аудита, что позволит скрыть следы атаки или вызвать отказ в обслуживании, если включен параметр Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности политики безопасности..

По умолчанию: «Локальная система».

11. Восстановление файлов и каталогов

Этот параметр безопасности определяет, какие пользователи могут восстанавливать архивированные файлы и каталоги, невзирая на имеющиеся у них разрешения для этих файлов и каталогов, а также назначать любого действительного участника безопасности владельцем объекта.

Эта привилегия эквивалентна предоставлению указанным пользователям и группам следующих разрешений на доступ ко всем файлам и папкам системы.

• Обзор папок / Выполнение файлов

• Запись

• Предоставление этого права пользователя может быть связано с риском для безопасности. Назначают это право только надежным пользователям, так как оно позволяет изменять параметры реестра, скрывать данные и получать право владения системными объектами.

По умолчанию имеют право на Рабочих станциях и серверах: «Администраторы», «Операторы архива».

Предоставление этого права пользователям влечет примерно такие же риски, что и предоставление права «Архивирование файлов и каталогов».

12. Завершение работы системы

Этот параметр безопасности определяет, какие пользователи могут, войдя на локальный компьютер, завершить работу операционной системы с помощью команды Завершение работы. Неверное использование этого права пользователя может привести к атаке на службу.

По умолчанию имеют право на Рабочих станциях: «Администраторы», «Операторы архива», «Опытные пользователи», «Пользователи».

13. Смена владельца файлов или иных объектов

Этот параметр безопасности определяет, какие пользователи могут становиться владельцем любого объекта системы, контролируемого средствами безопасности, в том числе объектов Active Directory, файлов и папок, принтеров, разделов реестра, процессов и потоков.

Предоставление этого права пользователя может быть связано с риском для безопасности. Предоставлять данное право необходимо только надежным пользователям, так как владельцы объектов получают полный контроль над ними.

По умолчанию имеют право администраторы.

Риски безопасности связаны с тем, что в случае наличия у пользователя данного права, он может получить доступ к файлам и папкам даже в том случае, когда доступ к данным ему запрещен. В таком случае пользователь просто становиться владельцем и автоматически получает полные права на нужные файлы и папки.

Тема 9. Локальная политика безопасности. Часть 3: Политика аудита

Политика аудита настраивает в системе определенного пользователя и группы аудит активности. Для того чтобы отконфигурировать политики аудита, в редакторе управления групповыми политиками нужно открыть узел **Конфигурация компьютера/Конфигурация Windows/Параметры безопасности/Локальные политики/Политика аудита**. Необходимо помнить, что по умолчанию параметр политики аудита, для рабочих станций установлен в **«Не определено»**. В общей сложности, можно настраивать девять политик аудита.

Так же, как и с остальными политиками безопасности, для настройки аудита нужно определить параметр политики. После двойного нажатия левой кнопкой мыши на любом из параметров, установить флажок на опции **«Определить следующие параметры политики»** и указать параметры ведения аудита успеха, отказа или обоих типов событий.

После настройки политики аудита события будут заноситься в журнал безопасности. Просмотреть эти события можно в журнале безопасности.

Аудит входа в систему. Текущая политика определяет, будет ли операционная система пользователя, для компьютера которого применяется данная политика аудита, выполнять аудит каждой попытки входа пользователя в систему или выхода из нее. Например, при удачном входе пользователя на компьютер генерируется событие входа учетной записи. События выхода из системы создаются каждый раз, когда завершается сеанс вошедшей в систему учетной записи пользователя. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.

Аудит доступа к объектам. Данная политика безопасности выполняет аудит попыток доступа пользователей к объектам, которые не имеют отношения к Active Directory. К таким объектам можно отнести файлы, папки, принтеры, разделы системного реестра, которые задаются собственными списками в системном списке управления доступом (SACL). Аудит создается только для объектов, для которых указаны списки управления доступом, при условии, что запрашиваемый тип доступа и учетная запись, выполняющая запрос, соответствуют параметрам в данных списках.

Аудит доступа к службе каталогов. При помощи этой политики безопасности можно определить, будет ли выполняться аудит событий, указанных в системном списке контроля доступа (SACL), который можно редактировать в диалоговом окне **«Дополнительные параметры безопасности»** свойств объекта Active Directory. Аудит создается только для объектов, для которых указан системный список управления доступом, при условии, что запрашиваемый тип доступа и учетная запись, выполняющая запрос, соответствуют параметрам в данном списке. Данная политика в какой-то степени похожа на политику **«Аудит доступа к объектам»**. Аудит успехов означает создание записи аудита при каждом успешном доступе пользователя к объекту Active Directory, для которого определена таблица SACL. Аудит отказов означает создание записи аудита

при каждой неудачной попытке доступа пользователя к объекту Active Directory, для которого определена таблица SACL.

Аудит изменения политики. Эта политика аудита указывает, будет ли операционная система выполнять аудит каждой попытки изменения политики назначения прав пользователям, аудита, учетной записи или доверия. Аудит успехов означает создание записи аудита при каждом успешном изменении политик назначения прав пользователей, политик аудита или политик доверительных отношений. Аудит отказов означает создание записи аудита при каждой неудачной попытке изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

Аудит изменения привилегий. Используя эту политику безопасности, можно определить, будет ли выполняться аудит использования привилегий и прав пользователей. Аудит успехов означает создание записи аудита для каждого успешного применения права пользователя. Аудит отказов означает создание записи аудита для каждого неудачного применения права пользователя.

Аудит отслеживания процессов. Текущая политика аудита определяет, будет ли операционная система выполнять аудит событий, связанных с процессами, такими как создание и завершение процессов, а также активация программ и непрямой доступ к объектам. Аудит успехов означает создание записи аудита для каждого успешного события, связанного с отслеживаемым процессом. Аудит отказов означает создание записи аудита для каждого неудачного события, связанного с отслеживаемым процессом.

Аудит системных событий. Данная политика безопасности имеет особую ценность, так как именно при помощи этой политики можно узнать, перегружался ли у пользователя компьютер, превысил ли размер журнала безопасности пороговое значение предупреждений, была ли потеря отслеженных событий из-за сбоя системы аудита и даже вносились ли изменения, которые могли повлиять на безопасность системы или журнала безопасности вплоть до изменения системного времени. Аудит успехов означает создание записи аудита для каждого успешного системного события. Аудит отказов означает создание записи аудита для каждого неудачного завершения системного события.

Аудит событий входа в систему. При помощи этой политики аудита можно указать, будет ли операционная система выполнять аудит каждый раз при проверке данным компьютером учетных данных. При использовании этой политики создается событие для локального и удаленного входа пользователя в систему. Члены домена и компьютеры, не входящие в домен, являются доверенными для своих локальных учетных записей. Когда пользователь пытается подключиться к общей папке на сервере, в журнал безопасности записывается событие удаленного входа, причем события выхода из системы не записываются. Аудит успехов означает создание записи аудита для каждой успешной попытки входа в систему. Аудит отказов означает создание записи аудита для каждой неудачной попытки входа в систему.

Аудит управления учетными записями. Эта последняя политика тоже считается очень важной, так как именно при помощи нее можно определить, необходимо ли выполнять аудит каждого события управления учетными запи-

сями на компьютере. В журнал безопасности будут записываться такие действия как создание, перемещение и отключение учетных записей, а также изменение паролей и групп. Аудит успехов означает создание записи аудита для каждого успешного события управления учетными записями. Аудит отказов означает создание записи аудита для каждого неудачного события управления учетными записями. Необходимо спланировать, что именно необходимо для аудита. Например, чтобы удостовериться в том, что к одной из учетных записей постоянно пытаются получить несанкционированный доступ методом подбора пароля, можно указать аудит неудачных попыток входа.

Пример использования политики аудита

Например, имеется домен testdomain.com, в котором имеется пользователь с учетной записью User1.Vista. в данном примере применим для этого пользователя политику «Аудит событий входа в систему» и увидим, какие события записываются в журнал безопасности при попытке несанкционированного доступа в систему. Для воспроизведения подобной ситуации выполнить следующие действия:

1. На контроллере домена создать пользовательскую учетную запись и поместить ее в группу безопасности «Vista», которая расположена в подразделении **«Группы»**;
2. Открыть консоль **«Управление групповой политикой»**, где выбрать контейнер **«Объекты групповой политики»** и нажать на этом контейнере правой кнопкой мыши для отображения контекстного меню;
3. В контекстном меню выбрать команду **«Создать»** и в отобразившемся диалоговом окне **«Новый объект групповой политики»** ввести **«Политика аудита»**, после чего нажать кнопку **«ОК»**;
4. Выбрать данный объект групповой политики и из контекстного меню выбрать команду **«Изменить»**;
5. В появившемся окне **«Редактор управления групповыми политиками»** развернуть узел **Конфигурация компьютера/Политика/Конфигурация Windows/Параметры безопасности/Локальные политики/Политика аудита** и открыть параметр политики **«Аудит событий входа в систему»**;
6. Установить флажки возле опций **«Определить следующие параметры политики»** и **«отказ»**, как показано на рис.5 и нажать **«ОК»**;
7. Закрыть редактор управления групповыми политиками;
8. Связать объект **«Политики аудита»** с подразделением **«Группы»**. Для этого щелкнуть правой кнопкой мыши на подразделение **«Группы»** и из контекстного меню выбрать команду **«Связать существующий объект групповой политики»**;
9. В диалоговом окне **«Выбор объекта групповой политики»** выбрать объект **«Политика аудита»** и нажать **«ОК»**;

10. Развернуть подразделение **«Группы»** и в области **«Фильтры безопасности»** удалить фильтр **«Прошедшие проверку»**. После этого нажать кнопку **«Добавить»** и выбрать группу **«Vista»**, которая создана ранее;
11. Перейти на клиентскую машину и обновить групповые политики при помощи команды *gpupdate*;
12. Заблокировать компьютер и попробовать войти в систему, используя заведомо неправильный пароль;
13. На контроллере домена открыть оснастку **«Просмотр событий»** и перейти в журнал **«Безопасность»**;
14. сгенерируется сообщение аудита отказа (сгенерировался EventID 4771).

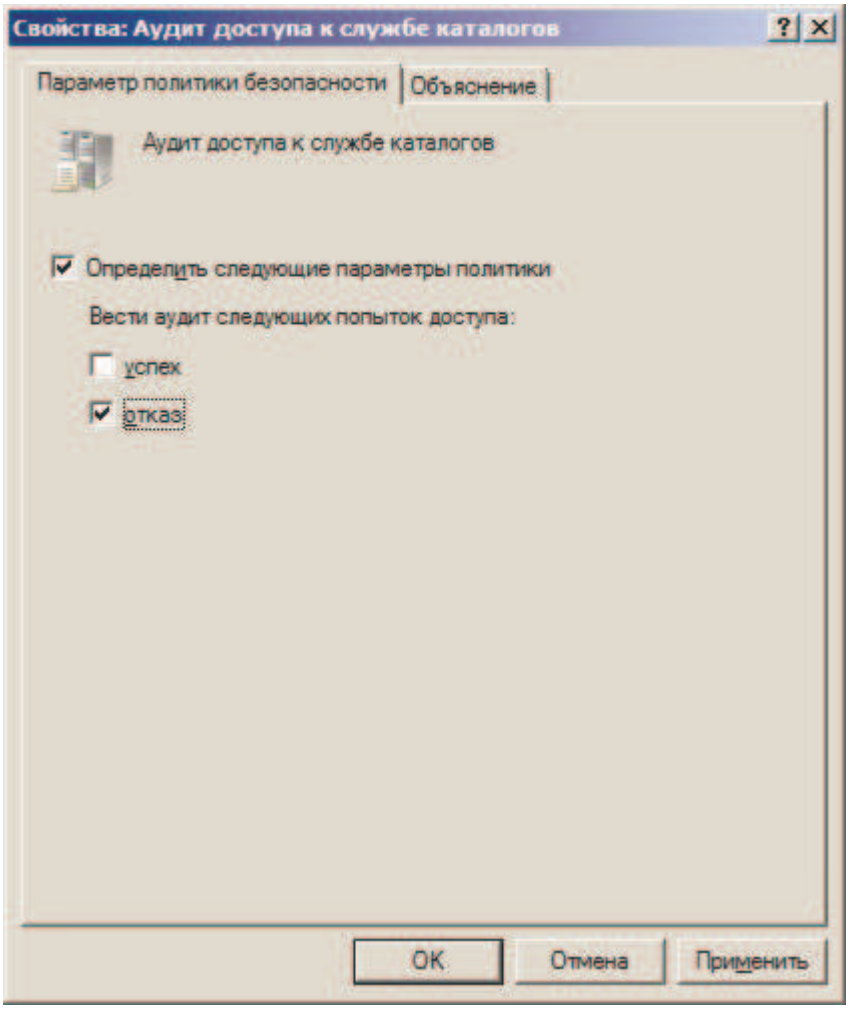

Рис. 5. Свойства политики аудита «Аудит доступа к службе каталогов»

Тема 10. Политики проводной сети

В серверных операционных системах [2] компании Microsoft, начиная с Windows Server 2008, появился компонент политик проводной сети (IEEE 802.3), который обеспечивает автоматическую конфигурацию для развертывания услуг проводного доступа с проверкой подлинности IEEE 802.1X для сетевых клиентов Ethernet 802.3. Для реализации параметров безопасности проводных сетей средствами групповых политик, в операционных системах используется служба проводной автонастройки (Wired AutoConfig - DOT3SVC). Теку-

щая служба отвечает за проверку подлинности IEEE 802.1X при подключении к сетям Ethernet при помощи совместимых коммутаторов 802.1X, а также управляет профилем, используемого с целью настройки сетевого клиента для доступа с проверкой подлинности. Стоит отметить, что если будут использоваться данные политики, то желательно запретить пользователям домена изменять режим запуска данной службы.

Настройка политики проводной сети

Задать настройки политики проводных сетей можно из оснастки «Редактор управления групповыми политиками». Для того чтобы настроить данные параметры, выполнить следующие действия:

1. Открыть оснастку **«Редактор управления групповыми политиками»** и в дереве консоли выбрать узел **«Политики проводной сети (IEEE 802.3)»**, нажать на нем правой кнопкой мыши и из контекстного меню выбрать команду **«Создание новой политики проводных сетей для Windows Vista и более поздних версий»**.
2. В открывшемся диалоговом окне **«Новая политика для проводных сетей Properties»**, на вкладке **«Общие»**, можно задать применение службы автонастройки проводных сетей для настройки адаптеров локальных сетей для подключения к проводной сети. Помимо параметров политики, которые распространяются на операционные системы Windows Vista и более поздние, существуют некоторые опции, которые будут применяться только к операционным системам Windows 7 и Windows Server 2008 R2. На этой вкладке можно выполнять следующие действия:
    - **Имя политики**. В этом текстовом поле можно задавать наименование для политики проводной сети. Имя политики можно увидеть в области сведений узла **«Политики проводной сети (IEEE 802.3)»** оснастки **«Редактор управления групповыми политиками»**;
    - **Описание**. Данное текстовое поле предназначено для заполнения подробного описания назначения политики проводной сети;
    - **Использовать службу автонастройки проводных сетей Windows для клиентов**. Данная опция выполняет реальную настройку и подключает клиентов к проводной сети 802.3. Если отключить эту опцию, то операционная система Windows не будет контролировать проводное сетевое подключение, и параметры политики действовать не будут;
    - **Запретить использование общих учетных данных пользователя для проверки подлинности сети**. Этот параметр определяет, следует ли пользователю запрещать хранить общие учетные данные пользователя для проверки подлинности сети. Локально можно изменять данный параметр при помощи команды **netsh lan set allowexplicitcreds**;
    - **Включить период блокировки**. Эта настройка определяет, следует ли запрещать компьютеру автоматически подключаться к провод-

ной сети на протяжении указанного количества минут. По умолчанию указано 20 минут. Настраивается период блокировки в диапазоне от 1 до 60 минут.

3. На вкладке **«Безопасность»** предоставлены параметры конфигурации метода проверки подлинности и режима проводного подключения. Можно настраивать следующие параметры безопасности:
    - **Включать проверку подлинности IEEE 802.1X для доступа к сети**. Эта опция используется непосредственно для включения или отключения проверки подлинности 802.1X сетевого доступа. По умолчанию данная опция включена;
    - **Выберите метод проверки подлинности сети**. При помощи данного раскрывающегося списка можно указать один из методов проверки подлинности сетевых клиентов, который будет применен для политики проводной сети. Доступны для выбора следующие два параметра:
        - **Microsoft: Защищенные EAP (PEAP)**. Для этого метода проверки подлинности, окно **«Свойства»** содержит параметры конфигурации используемого метода проверки подлинности;
        - **Microsoft: смарт-карты или другой сертификат**. Для этого метода проверки подлинности, в окне **«Свойства»** предоставлены параметры конфигурации, с помощью которых можно указать смарт-карту или сертификат для подключения, а также список доверенных корневых центров сертификации.

По умолчанию выбран метод **Microsoft: защищенные EAP (PEAP)**;

- **Режим проверки подлинности**. Данный раскрывающийся список применяется для выполнения сетевой проверки подлинности. Для выбора доступны следующие четыре параметра:
    - **Проверка подлинности пользователя или компьютера**. В том случае, если будет выбран этот параметр, учетные данные безопасности будут использоваться на основе текущего состояния компьютера. Даже если в систему не входил ни один пользователь, проверка подлинности будет выполняться по учетным данным компьютера. При входе пользователя будут использоваться учетные данные вошедшего в систему пользователя. Компания Microsoft рекомендует в большинстве случаев использовать именно этот параметр режима проверки подлинности.
    - **Только для компьютера**. В этом случае проверка подлинности выполняется только для учетных данных компьютера;
    - **Проверка подлинности пользователя**. При выборе данного параметра включается принудительная проверка подлинности пользователя только при подключении к новому устройству

802.1X. Во всех остальных случаях проверка подлинности выполняется только для компьютера;

- **Проверка подлинности гостя**. Данный параметр разрешает подключаться к сети на основе гостевой учетной записи.

- **Максимальное число ошибок проверки подлинности**. Этот параметр позволяет указать максимальное число ошибок при проверке подлинности. Значение по умолчанию: 1;
- **Кэшировать данные пользователя для последующих подключений к этой сети**. При включении данного параметра, пользовательские учетные данные будут сохраняться в системном реестре, при выходе пользователя из системы и при последующем входе учетные данные запрашиваться не будут.

Свойства режимов проверки подлинности

Для обоих методов проверки подлинности есть дополнительные настройки, которые вызываются нажатием кнопки «Свойства». Ниже рассмотрены все возможные настройки для методов проверки подлинности.

Настройки метода проверки подлинности «Microsoft: Защищенные EAP (PEAP)»

EAP (Extensible Authentication Protocol, Расширяемый Протокол Аутентификации) – это расширяемая инфраструктура аутентификации, которая определяет формат посылки. Для настройки данного метода проверки подлинности доступны следующие параметры:

- **Проверять сертификат сервера**. Данная опция позволяет задавать проверку сертификата сервера, который предоставляется на клиентские компьютеры на наличие валидной не просроченной подписи, а также наличие доверенного корневого центра сертификации, который выдал сертификат данному серверу. Этот флажок лучше оставлять включенным, так как при отсутствии проверки на подлинность серверов, уровень безопасности пользователей значительно понижается;
- **Подключаться к серверам**. Данная настройка позволяет указать имена серверов службы RADIUS, которые обеспечивают авторизацию и сетевую проверку подлинности. При указании имени сервера можно использовать как полный синтаксис регулярного выражения, так и использовать символ *;
- **Доверенные корневые центры сертификации**. В данном списке отображены все доверенные корневые центры сертификации, которые установлены в хранилищах сертификата пользователя и компьютера. Здесь можно указать те ЦС, которые будут использовать соискатели при проверке. Если не выбран ни один доверенный корневой центр сертификации, то клиент будет проверять, был ли сертификат компьютера для сервера RADIUS выдан установленным доверенным корневым центром сертификации.

- **Не запрашивать пользователя авторизовать новые серверы или доверенные центры сертификации**. Установив флажок для этой опции, при наличии неправильно настроенного сертификата сервера или присутствующего в списке для пользователя не будет отображаться диалоговое окно с предложением авторизации такого сертификата. По умолчанию эта опция отключена;
- **Выбор способа проверки подлинности**. В этом раскрывающемся меню можно открыть диалоговое окно настроек для одного из следующих методом проверки:
    - **Защищенный пароль (EAP-MSCHAP v2)**. Это настройки типа EAP, которые используются в PEAP-MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol - протокол, разработанный корпорацией Microsoft для выполнения процедур проверки подлинности удалённых рабочих станций Windows, который поддерживает функциональные возможности, привычные пользователям локальных сетей, и интегрирует алгоритмы шифрования и хеширования, действующие в сетях Windows) для проверки подлинности по паролю. По сути, из всех настроек присутствует только одна опция, которая позволяет использовать текущие имя и пароль входа в Windows в качестве учетных данных сетевой проверки подлинности. Данная опция отключена только в VPN соединениях.
    - **Свойства смарт-карты или другого сертификата – настройки EAP-TLS**. Данные настройки будут рассмотрены в следующем подразделе.
- **Включить быстрое переподключение**. Данная опция позволяет пользователям с беспроводными компьютерами быстро перемещаться между точками доступа без повторной проверки подлинности в новой сети. Такое переключение может работать только для точек доступа, которые настроены как клиенты службы RADIUS. По умолчанию эта опция включена;
- **Включить защиту доступа к сети**. При выборе этой опции, перед разрешением подключения к сети соискателей EAP, для определения проверки требований работоспособности, будут выполняться соответствующие проверки;
- **Отключаться, если сервер не поддерживает привязку с шифрованием через механизм TLV**. Эта опция отвечает за прерывание подключающимися клиентами процесса проверки подлинности в том случае, если RADIUS-сервер не предоставляет криптографическое значение привязки TLV, которая повышает безопасность TLS-туннеля в PEAP, объединяя способы внутренней и внешней проверки подлинности, чтобы злоумышленники не могли выполнять атаки типа вмешательства третьей стороны;
- **Включить удостоверение конфиденциальности**. Данный параметр отвечает за то, чтобы клиенты не могли отправлять свое удостоверение перед тем, как клиент проверил подлинность сервера RADIUS, и при необ-

ходимости обеспечивать место для ввода значения анонимного удостоверения.

Настройки метода проверки подлинности «Смарт-карты или другой сертификат – настройки EAP-TLS»

Для настройки данного метода проверки подлинности существуют следующие параметры:

- **При подключении использовать мою смарт-карту**. Если установить переключатель на данную позицию, то клиенты, выполняющие запросы проверки подлинности, будут представлять сертификат смарт-карты для сетевой проверки подлинности;
- **При подключении использовать сертификат на этом компьютере**. При выборе этой опции, при проверке подключения клиентов будет использоваться сертификат, расположенный в хранилище текущего пользователя или локального компьютера;
- **Использовать выбор простого сертификата**. Эта опция позволяет операционной системе Windows отфильтровывать сертификаты, которые не соответствуют требованиям проверки подлинности;
- **Проверять сертификат сервера**. Данная опция позволяет задавать проверку сертификата сервера, который предоставляется на клиентские компьютеры на наличие валидной не просроченной подписи, а также наличие доверенного корневого центра сертификации, который выдал сертификат данному серверу
- **Подключаться к серверам**. Эта опция идентична одноименной опции, о которой рассказывалось в предыдущем разделе;
- **Доверенные корневые центры сертификации**. Также как и в диалоговом окне свойств защищенного EAP, в этом списке можно найти все доверенные корневые центры сертификации, которые установлены в хранилищах сертификата пользователя и компьютера;
- **Не запрашивать пользователя авторизовать новые серверы или доверенные Центры Сертификации**. Установив флажок для этой опции, при наличии неправильно настроенного сертификата сервера или присутствующего в списке для пользователя, не будет отображаться диалоговое окно с предложением авторизации такого сертификата. По умолчанию эта опция отключена;
- **Использовать для подключения другое имя пользователя**. Этот параметр определяет, нужно ли использовать для проверки подлинности имя пользователя, отличное от имени пользователя в сертификате. При включенной опции использования другого имени пользователя необходимо выбрать как минимум один сертификат из списка доверенных корневых центров сертификации.

Если нет уверенности в выбираемом сертификате, то, нажав кнопку «Просмотреть сертификат» можно просмотреть все подробные сведения о выбранном сертификате.

Дополнительные параметры безопасности политики проводных сетей

На вкладке «Безопасность» диалогового окна настроек политики проводной сети присутствуют дополнительные параметры безопасности, предназначенные для изменения поведения сетевых клиентов, подающих запросы на доступ с проверкой подлинности 802.1X. Дополнительные параметры политик проводных сетей можно разделить на две группы – настройки IEEE 802.1X и настройки единого входа. Рассмотрим каждую из этих групп:

В группе настроек IEEE 802.1X можно указать характеристики запросов проводных сетей с проверкой подлинности 802.1X. Для изменения доступны следующие параметры:

- **Применить дополнительные параметры 802.1X**. Эта опция позволяет активировать следующие четыре настройки;
- **Макс. EAPOL-сообщений**. EAPOL – это протокол EAP, который используется до того, как компьютер успевает аутентифицироваться, и только после успешного «логина» весь остальной трафик сможет проходить через тот порт коммутатора, к которому подключен данный компьютер. Этот параметр отвечает за максимальное количество отправляемых сообщений EAPOL-Start;
- **Период задержки (сек)**. Этот параметр отвечает за задержку в секундах перед выполнением следующего запроса проверки подлинности 802.1X после получения уведомления об отказе при проверке подлинности;
- **Start Period (период начала)**. Этот параметр отвечает за время ожидания перед повторной отправкой последовательных сообщений EAPOL-Start;
- **Период проверки (сек)**. Этот параметр определяет число секунд между повторной передачей последовательных начальных сообщений EAPOL после инициации сквозной проверки доступа 802.1X;
- **Сообщение EAPOL-Start**. При помощи данного параметра можно указать следующие характеристики передачи начальных сообщений EAPOL:
    - **Не передавать**. При выборе данного параметра, EAPOL сообщения не будут передаваться;
    - **Передано**. При выборе этого параметра, клиенту нужно будет вручную отправлять начальные сообщения EAPOL;
    - **Передача по протоколу IEEE 802.1X**. при выборе данного параметра (он определен по умолчанию) сообщения EAPOL будут отправляться в автоматическом режиме, ожидая запуска проверки подлинности 802.1X.

При использовании единого входа, проверка подлинности должна выполняться на основании конфигурации безопасности сети в процессе входа пользо-

вателя в операционную систему. Для полной настройки профилей единого входа в систему доступны следующие параметры:

- **Включить единую регистрацию для сети**. При включении данной опции активируются настройки единого входа в систему;
- **Включить непосредственно перед входом пользователя**. Если установить переключатель на эту опцию, то проверка подлинности 802.1X будет выполняться перед завершением входа пользователя в систему;
- **Включить сразу после входа пользователя**. Если установить переключатель на эту опцию, то проверка подлинности 802.1X будет выполняться после завершения входа пользователя в систему;
- **Макс. задержка подключения**. Этот параметр задает максимальное время, за которое должна быть завершена проверка подлинности и, соответственно, как долго будет ждать пользователь перед появлением окна пользовательского входа в систему;
- **Разрешить отображение дополнительных диалоговых окон при едином входе**. Этот параметр отвечает за отображение диалогового окна входа пользователя в систему;
- **Эта сеть использует разные виртуальные локальные сети для проверки подлинности по учетным данными компьютеров и пользователей**. При указании этой настройки, при запуске, все компьютеры будут помещаться в одну виртуальную сеть, а после успешного входа пользователя в систему, в зависимости от разрешений, будут переводиться в различные виртуальные сети. Эту опцию имеет смысл активировать только в том случае, если на предприятии используются несколько виртуальных локальных сетей VLAN.

Тема 11. Локальная политика безопасности. Политики беспроводной сети (IEEE 802.11)

Так как почти во всех производственных [2] сетях расположены мобильные клиенты, помимо всех локальных политик безопасности, которые рассматривались выше, в групповой политике Windows Server 2008/2008 R2 обеспечены параметры конфигурации клиентов для безопасного подключения к беспроводным точкам доступа IEEE 802.11.

Стандарт IEEE 802.1X определяет доступ с проверкой подлинности для беспроводных подключений (IEEE 802.11). Такие параметры предназначены для определения разрешений не прошедшим проверку подлинности и неавторизированным пользователям и компьютерам подключаться к беспроводной сети.

Можно настраивать политики беспроводной сети для клиентов Windows XP, Windows Server 2003, Windows Vista, Windows 7, а также Windows Server 2008/2008 R2. Используя данную политику безопасности, можно настраивать несколько профилей для подключения к одной беспроводной сети, используя обычный идентификатор беспроводной сети, при этом в каждом профиле могут быть заданы уникальные свойства безопасности.

Создание политики беспроводной сети для операционных систем не ниже Windows Vista

С помощью политик беспроводной сети (IEEE 802.11) Windows Vista, можно задать улучшенные параметры настройки беспроводной сети, безопасности и управления, которые доступны только для компьютеров с Windows Vista, Windows 7 и Windows Server 2008/2008 R2, использующих беспроводное подключение. Для того чтобы создать политику беспроводных сетей для операционных систем не ниже Windows Vista, выполнить следующие действия:

1. Открыть оснастку **«Редактор управления групповыми политиками»** и в дереве консоли выбрать узел **«Политики беспроводной сети (IEEE 802.11)»**, в контекстном меню выбрать команду **«Создание новой политики беспроводных сетей для Windows Vista и более поздних версий»**;
2. В открывшемся диалоговом окне **«Новая политика для беспроводных сетей»**, можно определить параметры, предназначенные для управления профилями беспроводных интерфейсов и определения списка предпочтительных беспроводных сетей, который задает порядок подключения клиентов, входящих в состав домена. Параметры, которые можно найти на вкладке **«Общие»**, используются для создания профилей беспроводных подключений, управления этими профилями, а также для определения списка предпочитаемых беспроводных сетей для клиентов, которые являются членами домена. На этой вкладке можно выполнять следующие действия:
    - **Имя политики**. В этом текстовом поле можно задавать наименование для политики проводной сети. Имя политики можно увидеть в области сведений узла **«Политики беспроводной сети (IEEE 802.3)»** оснастки **«Редактор управления групповыми политиками»**;
    - **Описание**. Текущее текстовое поле предназначено для заполнения подробного описания назначения политики проводной сети, которое также будет доступно в области сведений указанного выше узла;
    - **Использовать службу автонастройки WLAN Windows для клиентов**. Эта опция выполняет реальную настройку и указывает, что для настройки подключения беспроводной сети клиентов под управлением Windows Vista и Windows 7используется служба автонастройки WLAN;
    - **Подключаться к доступным сетям в порядке перечисления профилей**. В данном списке отображается предпочтительный порядок беспроводных сетей, в котором следует подключаться к сети. Можно добавить профиль беспроводной сети, нажав кнопку **«Добавить»**. Нажав эту кнопку, можно выбрать один из двух указанных параметров: **«Инфраструктура»**, которая задает сеть, использующую одну или несколько точек доступа, а также **«Прямое подключение»**, которое задает сеть «компьютер-компьютер». Стоит

учесть, что приоритет профилей инфраструктуры всегда выше приоритета прямого подключения. Для того чтобы изменить существующий профиль, нажать кнопку **«Изменить»**, а для его удаления, соответственно, кнопку **«Удалить»**. Изменять приоритеты можно, используя кнопку со стрелками, направленными вверх и вниз, которые находятся справа от самого списка. Помимо этого, можно импортировать сохраненные ранее профили подключений из xml-файла или экспортировать существующие профили в xml-файл.

3. При выборе добавляемого типа профиля откроется диалоговое окно **«Свойства Новый профиль»**, предназначенное для создания профилей беспроводных сетей (т.е. набора параметров конфигурации беспроводной сети, сохраняемых в виде XML-файлов), к которым могут подключаться клиенты беспроводных сетей, входящих в состав домена. В этом диалоговом окне можно указывать настройки профилей, расположенных на двух вкладках.
    - На вкладке **«Подключение»** можно назначать имя профиля и указывать идентификатор SSID. Профиль представляет собой набор параметров конфигурации для беспроводной сети, сохраненный в виде XML-файла. Профили инфраструктуры имеют больший приоритет, нежели профили прямых соединений. Вкладка **«Подключение»** диалогового окна **«Новый профиль»** профиля инфраструктуры и прямого соединения очень похожи за исключением трех последних опций и возможности добавления нескольких идентификаторов SSID для профилей инфраструктуры. На этой вкладке доступны следующие параметры:
        - **Имя профиля**. В текущем текстовом поле можно указать имя профиля, отображаемое в списке диалогового окна политики беспроводных сетей;
        - **Сетевые имена SSID**. Здесь можно задать один (для профиля прямых соединений) или несколько (только для профилей инфраструктуры) идентификаторов SSID. SSID (Service Set Identifier) – это 32-битная строка, используемая в качестве сетевого имени (стоит запомнить, что идентификатор SSID не является MAC-адресом). Чтобы связать рабочую станцию с точкой доступа, обе системы должны иметь один и тот же SSID. Указанное значение SSID должно полностью соответствовать тому идентификатору, который указан в точке беспроводного доступа;
        - **Подключаться автоматически, если сеть в радиусе действия**. Эта опция позволяет автоматически подключаться к беспроводной сети в том случае, если компьютер расположен в диапазоне вещания любой точки беспроводного доступа с указанным SSID. Эта опция доступа только для профилей инфраструктуры;

- **Подключаться к более подходящей сети, если она есть**. В том случае, если на вкладке **«Общие»** диалогового окна подключения к беспроводным сетям находятся несколько профилей, данная опция позволяет подключаться к самой подходящей сети из списка. Эта опция также доступна только для профилей инфраструктуры;
- **Подключаться, даже если сеть не ведет вещание**. Если активировать данную опцию, то будет выполняться активный поиск точек беспроводного доступа с указанными SSID в том случае, если в настройке точек беспроводного доступа запрещена рассылка сигналов;

o Вкладка **«Безопасность»** предназначена для настройки параметров безопасности в политиках беспроводной сети, которые используются для задания параметров проверки подлинности, используемых клиентами беспроводной сети. В отличие от вкладки подключения, настройки на вкладке **«Безопасность»** для профилей инфраструктуры и прямого соединения существенно отличаются. Рассмотрим настройки вкладки **«Безопасность»** профиля инфраструктуры:

- Параметры безопасности инфраструктуры можно разделить на две части: метод безопасности для сети и метод проверки подлинности. В группе методов безопасности для сети можно указать способ сетевой проверки подлинности при установке связи беспроводной сети с точкой беспроводного доступа и метод шифрования системы безопасности. По умолчанию выбран наиболее безопасный метод проверки подлинности – **«WPA2-предприятие»**. Помимо метода проверки подлинности по умолчанию, можно выбрать такие методы, как **«Открыть»**, **«Совместная»**, **«WPA-предприятие»**, **«WPA-личное»**, **«WPA2-предприятие»**, **«WPA2-личное»**, а также **«Открыть с 802.1X»**. Стоит обратить внимание на то, что настройки метода проверки подлинности сети можно задавать только в случае, если в раскрывающемся списке **«Проверка подлинности»** выбраны такие методы, как **«WPA-предприятие»**, **«WPA2-предприятие»** или **«Открыть с 802.1X»**. Также только при выборе метода **«WPA2-предприятие»** доступны настройки быстрого перемещения, которые будут рассмотрены ниже. Также как и настройки метода подлинности проверки и быстрого перемещения, метод шифрования зависит от выбранного метода проверки подлинности. Можно выбрать метод шифрования **«AES»** или **«TKIP»** в том случае, если в раскрывающемся списке **«Проверка подлинности»** были выбраны **«WPA-предприятие»**, **«WPA-личное»**, **«WPA2-предприятие»** или **«WPA2-личное»**. Если будет выбрано **«Открыть»**, **«Совместная»**

или **«Открыть с 802.1X»**, то можно выбрать метод шифрования **«WEP»** или **«Отключен»**.

В раскрывающемся списке **«Выберите метод проверки подлинности сети»** можно указать один из методов проверки подлинности сетевых клиентов, который будет применен для политики беспроводной сети. Доступны для выбора следующие два параметра:

- **Microsoft: Защищенные EAP (PEAP)**. Для этого метода проверки подлинности, окно **«Свойства»** содержит параметры конфигурации используемого метода проверки подлинности;
- **Microsoft: смарт-карты или другой сертификат**. Для этого метода проверки подлинности, в окне **«Свойства»** предоставлены параметры конфигурации, с помощью которых можно указать смарт-карту или сертификат для подключения, а также список доверенных корневых центров сертификации;

По умолчанию выбран метод **Microsoft: защищенные EAP (PEAP)**;

Опция **«Режим проверки подлинности»** применяется для выполнения сетевой проверки подлинности. Для выбора доступны следующие четыре параметра;

- **Проверка подлинности пользователя или компьютера**. В том случае, если будет выбран этот параметр, учетные данные безопасности будут использоваться на основе текущего состояния компьютера. Даже если в систему не входил ни один пользователь, проверка подлинности будет выполняться по учетным данным компьютера. При входе пользователя будут использоваться учетные данные вошедшего в систему пользователя. Компания Microsoft рекомендует в большинстве случаев использовать именно этот параметр режима проверки подлинности;
- **Только для компьютера**. В этом случае проверка подлинности выполняется только для учетных данных компьютера;
- **Проверка подлинности пользователя**. При выборе данного параметра включается принудительная проверка подлинности пользователя только при подключении к новому устройству 802.1X. Во всех остальных случа-

ях проверка подлинности выполняется только для компьютера;

- **Проверка подлинности гостя**. Данный параметр разрешает подключаться к сети на основе гостевой учетной записи.

Помимо вышеперечисленных настроек, опция **«Максимальное число ошибок проверки подлинности»** позволяет указать максимальное число ошибок при проверке подлинности (Значение по умолчанию: 1). А опция **«Кэшировать данные пользователя для последующих подключений к этой сети»** позволяет сохранять пользовательские учетные данные в системном реестре при выходе пользователя из системы, причем при последующем входе учетные данные запрашиваться не будут.

- Параметры безопасности прямого соединения имеют более скромные настройки. Здесь можно указать только три метода проверки подлинности – **«Открыть»**, **«Совместная»** и **«WPA2-личное»**, а также указать для них соответствующий метод шифрования.

4. После того как заданы необходимые настройки подключения и безопасности, нажать кнопку **«ОК»** для перехода в диалоговое окно свойств политики беспроводной сети. На вкладке **«Сетевые размещения»** можно использовать параметры, которые предназначены для определения дополнительных беспроводных сетей, а также для разрешения или запрета подключений беспроводных клиентов, входящих в состав домена. Помимо этого, на данной вкладке также можно заблокировать отображение дополнительных беспроводных сетей для беспроводных клиентов, входящих в состав домена. Например, параметр **«Запретить подключения к сетям с прямым соединением»** указывает на то, что клиенты не смогут создавать или подключаться к какой-либо сети типа «компьютер-компьютер», а параметр **«Запретить подключения к сетям с инфраструктурой»** запрещает подключаться к инфраструктурным сетям. На этой вкладке можно найти параметры политики, которые могут применяться только к операционным системам Windows 7 и Windows Server® 2008 R2. К этим параметрам относятся параметры **«Запретить размещенную сеть»**, который запрещает размещение беспроводных сетей на компьютерах с операционной системой Windows 7, **«Запретить общие учетные данные пользователя для сетевой проверки подлинности»**, при помощи которого можно запретить сохранение своих учетных данных, которые компьютер может использовать для подключения к сети. Также доступен параметр **«Включить период блокировки»**, запрещающий компьютеру под управлением Windows 7 автоматические попытки подключения к сети в течение указанного количества времени.

5. В том случае, если планируется создавать идентичные профили в другом объекте групповой политики, то надо экспортировать получившиеся профили и, при необходимости, добавить в список столько профилей, сколько нужно, после чего нажать **«ОК»**.

Свойства методов проверки подлинности

Как для метода проверки подлинности «Microsoft: Защищенные EAP (PEAP)», так и для «Microsoft: Смарт-карта или иной сертификат» доступны дополнительные параметры, вызываемые нажатием кнопки «Свойства». В диалоговом окне свойств выбранного метода проверки подлинности можно задать множество параметров, которые существенно переведут уровень безопасности проверки подлинности на новый уровень.

Дополнительные параметры безопасности

Дополнительные параметры безопасности профиля беспроводной сети могут быть применены только для профилей инфраструктуры и влияют на изменение поведения сетевых клиентов, подающих запросы на доступ с проверкой подлинности 802.1X. в отличие от дополнительных параметров проводной сети, дополнительные параметры беспроводной сети делятся на три группы: IEEE 802.1X, настройки единой регистрации, а также (в том случае, если был выбран метод проверки подлинности «WPA2-предприятие») настройки быстрого перемещения. Так как настройки IEEE 802.1X и единой регистрации идентичны с дополнительными настройками проводной сети, ниже рассмотрены только настройки быстрого перемещения.

Быстрым перемещением называется возможность WPA2, которая представляет собой предварительную проверку подлинности и кеширование парных основных ключей (PMK), позволяющие клиентам быстро переключаться между различными точками беспроводного доступа. Для настройки быстрого перемещения доступны следующие параметры:

- **Включить кэширование парных основных ключей (PMK)**. Данный параметр задает кэширование парных основных ключей для быстрого перемещения WPA2;
- **Срок жизни PMK (мин.)**. Этот параметр определяет длительность хранения PMK в кэше. Значение по умолчанию – 720 минут;
- **Число записей в кэше PMK**. При помощи текущего параметра можно определить максимальное количество записей PMK, которое будет храниться в кэше. Значение по умолчанию: 128;
- **Сеть использует предварительную проверку подлинности**. Данную настройку целесообразно использовать только в том случае, если в настройках беспроводной точки доступа указана возможность предварительной проверки подлинности в рассылаемых сообщениях Probe Response и Beacon. Эта настройка позволяет клиентам выполнять проверку подлинности 802.1X с других точек доступа в пределах данного диапазона. При активированной данной на-

стройке сведения сохраняются в кэше PMK. Если данная опция активна, то значение по умолчанию для следующих двух настроек будет равняться трем;

- **Максимальное число попыток предварительной проверки подлинности**. Текущий параметр определяет максимальное допустимое количество попыток предварительной проверки подлинности других беспроводных точек доступа в сети, которые расположены в диапазоне ее действия;
- **Выполнять шифрование в сертифицированном режиме FIPS 140-2**. Данный параметр определяет, что беспроводные передачи соответствуют режиму 140-2 стандарта FIPS для криптования, который используется для сертификации криптографических модулей.

Создание политики беспроводной сети для систем Windows XP

В том случае, если в корпоративной сети не все компьютеры обновлены до операционных систем Windows Vista или Windows 7, можно создать политику беспроводной сети для операционных систем Windows XP. Параметры беспроводных сетей для Windows XP включают в себя глобальные параметры беспроводных подключений, список предпочтительных сетей, параметры WEP, а также параметры 802.1X. В диалоговом окне политики беспроводных сетей XP доступны параметры на следующих вкладках:

- На вкладке **«Общие»** можно указать такие параметры, как:
  - **«Имя политики XP»**, где можно указать имя профиля, отображаемое в списке диалогового окна политики беспроводных сетей;
  - **«Описание»**, текстовое поле предназначено для заполнения подробного описания назначения политики проводной сети, которое также будет доступно в области сведений указанного выше узла;
  - **«Сети для доступа»**, представляет собой типы беспроводных сетей, к которым разрешается создавать подключение клиентам Windows XP. Можно выбрать **«Любая доступная сеть (с точкой доступа)»**, **«Сеть по точке доступа только»**, **«Сеть «компьютер-компьютер» только (произв.)»**;
  - **Использовать службу автонастройки WLAN Windows для клиентов**. Служба автонастройки WLAN перечисляет адаптеры беспроводной сети и управляет беспроводными подключениями и профилями беспроводной связи, содержащими параметры для настройки подключения клиента к беспроводной сети. Включенная служба беспроводной настройки ис-

пользуется для настройки и подключения к беспроводным сетям;

- **Автоматически подключаться к любой сети**. Если активировать данную опцию, то клиенты беспроводных сетей смогут подключаться к сетям, которые не указаны как предпочтительные.

- На вкладке **«Предпочитаемые сети»** можно добавлять беспроводные сети. Данная вкладка напоминает группу **«Подключаться к доступным сетям в порядке перечисления профилей»** диалогового окна политики беспроводной сети Windows Vista и более поздних версий. Здесь также можно добавить профиль инфраструктуры и прямого соглашения, однако, их настройки будут не настолько мощными, как в профилях, которые были рассмотрены. Помимо добавления, также можно изменять или удалять существующие профили. Для политики беспроводной сети XP нет возможности импорта и экспорта настроек в xml файл.

Настройка профиля политики беспроводной сети XP

При добавлении профиля инфраструктуры или прямого соединения открывается диалоговое окно **«Свойства: Новая предпочитаемая настройка»**, в которой можно указать сетевое имя SSID, описание для создаваемого профиля, выполнять активный поиск точек беспроводного доступа с указанными SSID в том случае, если в настройке точек беспроводного доступа запрещена рассылка сигналов.

Можно настраивать метод проверки подлинности (методы проверки подлинности в профилях беспроводной сети XP могут быть **«Открыть»**, **«Совместная»**, **«WPA»**, **«WPA2»**, а также **«Открыть с 802.1X»**, где **«WPA2»** и **«WPA»** соответствуют параметрам **«WPA2-предприятие»** и **«WPA-предприятие»** в политиках беспроводной сети (IEEE 802.11) Windows Vista), а также метод шифрования, в зависимости от выбранного метода проверки подлинности. При выборе параметра WPA2 становятся доступны дополнительные параметры для быстрого перемещения, параметры которых идентичны тем, которые были описаны ранее.

Все параметры, расположенные на вкладке IEEE 802.1X доступны только в том случае, если добавляется профиль инфраструктуры. На этой вкладке флажок **«Управлять сетевым доступом с помощью IEEE 802.1X»**, который предназначен для включения проверки подлинности IEEE 802.1X для данной беспроводной сети, установлен по умолчанию и заблокирован от редактирования. Так же, как и в политиках проводной и беспроводной сети Windows Vista, при помощи соответствующих раскрывающихся меню можно выбрать метод и режим проверки подлинности. Стоит отметить группу **«EAPOL-сообщение»**, в которой можно указать, следует ли передавать пакеты сообщения EAPOL (Extensible Authentication Protocol over LAN), и, если следует, инструкции по их передаче. В данном диалоговом окне, группа IEEE 802.1X идентична одно-

именной группе, расположенной в дополнительных параметрах безопасности политики проводной и беспроводной сети Windows Vista.

Помимо этого, если парк компьютеров уже переведен на операционные системы Windows Vista или Windows 7, но в объекте групповой политики создана только политика беспроводной сети XP, можно обновить данную политику до последней версии. Для этого, в области сведений, выбрать данную политику, нажать на ней правой кнопкой мыши и из контекстного меню выбрать команду **«Миграция политики XP в политику Vista»**, причем после обновления можно удалить текущую политику в автоматическом режиме.

Тема 12. Серверная роль DHCP

DHCP (Dynamic Host Configuration Protocol - протокол динамической настройки узла) — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP, и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP [3], [4].

DHCP является расширением протокола BOOTP, использовавшегося ранее для обеспечения бездисковых рабочих станций IP-адресами при их загрузке. DHCP сохраняет обратную совместимость с BOOTP.

Протокол DHCP предоставляет три способа распределения IP-адресов:

- *Ручное распределение.* При этом способе сетевой администратор сопоставляет аппаратному адресу (для Ethernet сетей это MAC-адрес) каждого клиентского компьютера определённый IP-адрес. Фактически, данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять при необходимости.
- *Автоматическое распределение.* При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона.
- *Динамическое распределение.* Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок. Это называется *арендой адреса*. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым). Кроме того, клиент сам может отказаться от полученного адреса.

Некоторые реализации службы DHCP способны автоматически обновлять записи DNS, соответствующие клиентским компьютерам, при выделении им

новых адресов. Это производится при помощи протокола обновления DNS, описанного в RFC 2136.

Опции DHCP

Помимо IP-адреса, DHCP также может сообщать клиенту дополнительные параметры, необходимые для нормальной работы в сети. Эти параметры называются опциями DHCP. Список стандартных опций можно найти в RFC 2132.

Некоторыми из наиболее часто используемых опций являются:

- IP-адрес маршрутизатора по умолчанию;
- маска подсети;
- адреса серверов DNS;
- имя домена DNS.

Некоторые поставщики программного обеспечения могут определять собственные, дополнительные опции DHCP.

Протокол DHCP является клиент-серверным, то есть в его работе участвуют клиент DHCP и сервер DHCP. Передача данных производится при помощи протокола UDP, при этом сервер принимает сообщения от клиентов на порт 67 и отправляет сообщения клиентам на порт 68.

Установка и настройка DHCP-сервера на Windows Server 2008 R2

DHCP-сервер не работает в рабочей группе, он работает только в составе домена.

1. Установка DHCP

- Добавить роль, запустив Мастер добавления ролей
- Выбрать роль сервера
- Выбрать сетевой интерфейс, на котором будет работать DHCP-сервер
- Установить дополнительные параметры, выдаваемые вместе с IP-адресом
- Пропустить параметры WINS, его не используют, поскольку он используется для ОС Windows 2000 и старше
- Пропустить создание областей, их можно установить позже
- Пропустить настройки IPv6
- Подтвердить параметры IPv6
- Указать учётные данные, с помощью которых DHCP-сервер будет авторизирован в Active Directory
- Подтвердить введенные параметры
- Завершить установку. После всех манипуляций, приступить к настройке. Запустить оснастку DHCP и создать область
- Именовать область. Определить диапазон адресов
- Определить диапазоны исключений (те адреса, которые не будут выдаваться, в основном - для использования серверами)
- Определить срок аренды (по умолчанию 8 дней)
- Провести настройку DHCP-сервера

- Определить адрес маршрутизатора
- Указать DNS-суффиксы и адреса DNS-серверов
- Пропустить установки WINS серверов
- Активировать область. Просмотреть пул
- Просмотреть параметры области

Если потребуется, в любой момент можно добавить дополнительные параметры, которые будут выдаться сервером, например, NTP, SMTP, POP3 и ещё

83 ролей и служб, и градация по типу операционной системы

Резервирование. Например, необходимо, чтобы один из компьютеров никогда не менял свой IP-адрес, но и вручную его настраивать незачем. Для этого используется резервирование, которому потребуется MAC-адрес клиента. Создание резервирование заключается в указании адреса IP и MAC (рис.6).

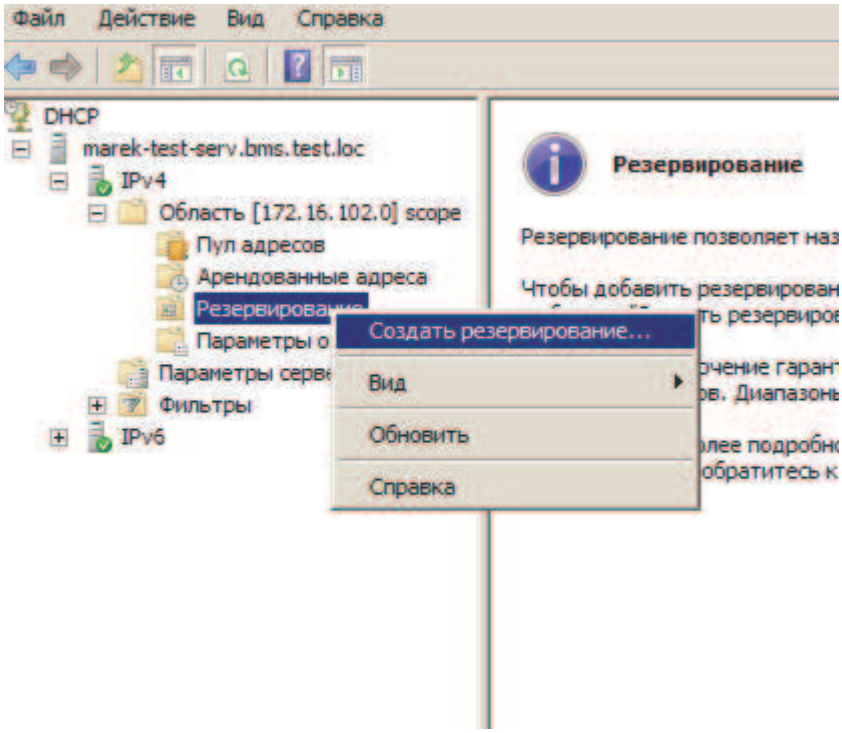

Рис.6. Настройка резервирования адресов

Тема 13. Резервное копирование и восстановление доменного каталога

Установка утилиты Windows Server Backup в Windows Server 2008 R2

По умолчанию компонент Windows Server Backup не добавлен [4]. Добавление данного компонента осуществляется с помощью Мастера добавления компонентов (Add Features Wizard).

Поставить флажки около элементов Windows Server Backup. Нажать Next.

- В появившемся окне. Нажать Install. Начнется процесс установки.

- После установки появится окно. Необходимо нажать Close. Установка завершена.

Создание резервной копии данных по расписанию

Для создания резервных копий по расписанию необходимо выполнить следующее:

Запустить утилиту Backup (Start (Пуск)/Programs(Программы)/Accessories (Стандартные)/System Tools (Системные утилиты)/Windows Server Backup (Резервное копирование)).

- Можно задать расписание, по которому будет осуществляться резервное копирование данных. В меню Action необходимо выбрать Backup Schedule, появится информационное окно, затем необходимо нажать Next. Здесь необходимо выбрать какие данные требуется сохранять, все или выборочные.

Затем требуется задать время, в которое будет происходить сохранение требуемых данных. Далее необходимо выбрать, куда будут сохраняться данные. Так же выбрать и задать другие настройки резервного копирования.

Разовое создание резервной копии данных

Для немедленного создания резервной копии необходимо выполнить следующее:

Запустить утилиту Backup (Start (Пуск)/Programs(Программы)/Accessories (Стандартные)/System Tools (Системные утилиты)/Windows Server Backup (Резервное копирование)). В меню Action необходимо выбрать Backup Once.

Далее необходимо выбрать требуемые параметры резервного копирования и нажать Next. После нажатия кнопки Backup начнется процесс резервного копирования.

Восстановление данных из BackUp.

Восстановление данных из созданной резервной копии.

Для восстановления данных из резервной копии необходимо:

1. Оповестить руководство о произошедших неполадках.
2. На работающем сервере или после его загрузки запустить утилиту Windows Server Backup (рис.7): (Start (Пуск)/All Programs(Программы)/Accessories (Стандартные)/System Tools (Системные утилиты)/ Windows Server Backup (Резервное копирование)). Запуститься мастер резервного копирования/восстановления Windows Server Backup;
3. В меню Action необходимо выбрать «Recover», откроется окно, выбрать параметр Restore files and settings. Нажать «Next».

4. Необходимо из предложенных вариантов выбрать те, которые требуются и затем нажать «Next». Перед началом процесса восстановления появится окно. В нем необходимо нажать «Recover»
5. После того как процесс восстановления завершится, появится окно, Нажать «Close», процесс восстановления данных из резервной копии завершен.

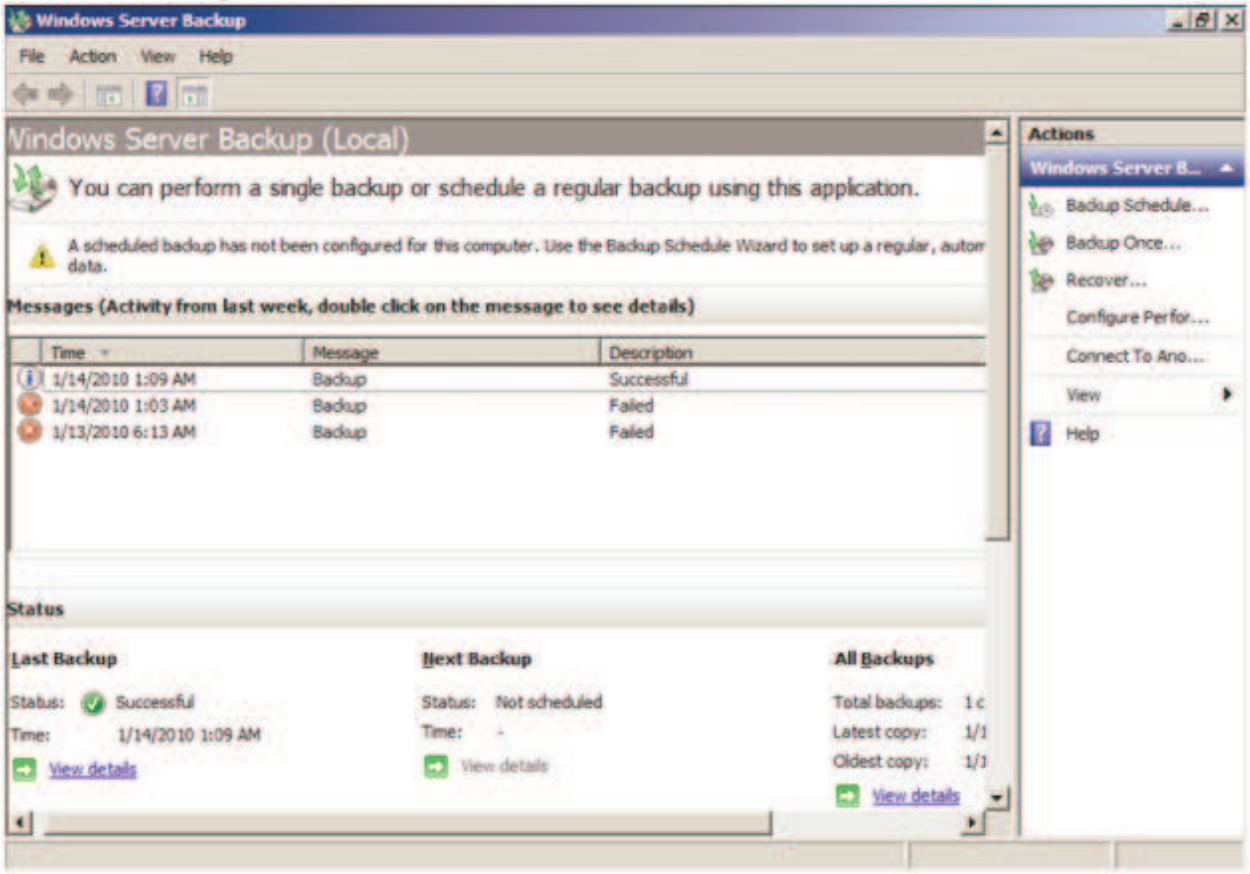

Рис. 7. Окно Windows Server Backup

Тема 14. Службы для NFS в системе Windows Server® 2008 R2

Службы для сетевой файловой системы (NFS) обеспечивают общий доступ к файлам для предприятий, использующих смешанную среду Windows и UNIX. Службы для NFS позволяют пользователям передавать файлы между компьютерами с ОС Windows Server® 2008 R2 и компьютерами с UNIX при помощи протокола NFS [3].

Возможности служб для NFS

В Windows Server® 2008 R2 реализованы следующие усовершенствования служб для NFS:

- **Поддержка сетевых групп**. Службы для NFS поддерживают сетевые группы, используемые для создания именованных групп узлов в сети. Сетевые группы упрощают управление входом пользователей и групп и их доступом к удаленным компьютерам, а также облегчают работу со списками управления доступом NFS.

- **Поддержка RPCSEC_GSS**. Службы для NFS обеспечивают встроенную поддержку средство безопасности RPC RPCSEC_GSS, с помощью которого приложения используют компоненты безопасности в интерфейсе GSS-API. Благодаря GSS-API приложения могут содержать службы проверки подлинности и целостности. RPCSEC_GSS позволяет службам для NFS использовать проверку подлинности Kerberos и предоставляет службы безопасности, не зависящие от применяемых технологий.

Службы для NFS не поддерживают службу обеспечения конфиденциальности RPCSEC_GSS.

Для включения методов проверки подлинности протокола Kerberos для общей папки на страницу «Проверка подлинности NFS» мастера подготовки общих папок и в диалоговое окно **Свойства** для общих папок на вкладке Проверка подлинности NFS добавлены следующие параметры:

  - **Проверка подлинности Kerberos v5 (Krb5)** использует протокол Kerberos v5 для проверки подлинности пользователей перед предоставлением доступа к системе общих файлов.
  - **Проверка подлинности и целостности Kerberos v5 (Krb5i)** использует проверку подлинности Kerberos v5 с проверкой целостности (контрольные суммы), что позволяет убедиться в подлинности данных.

Эти параметры можно использовать совместно и предоставлять клиентам возможность выбора любого протокола Kerberos v5 при подключении файловой системы NFS.

- **Использование инструментария управления Windows для управления сервером в NFS**. WMI позволяет ИТ-специалистам выполнять удаленное управление NFS, обеспечивая взаимодействие приложений управления предприятием через веб-интерфейс (WBEM) и поставщиков WMI на локальных компьютерах для управления объектами WMI. WMI дает возможность использования языков написания сценариев (например, VBScript или Windows PowerShell) для локального и удаленного управления компьютерами и серверами с ОС Microsoft Windows.

- **Доступ несопоставленных пользователей UNIX**. Для общих папок NFS доступен параметр **Несопоставленный пользователь UNIX**. Серверы Windows можно использовать для хранения данных NFS без создания сопоставления учетных записей UNIX с Windows. Для сопоставленных учетных записей пользователей применяются стандартные идентификаторы безопасности Windows (SID), а несопоставленные пользователи используют настраиваемые идентификаторы безопасности NFS.

Сценарии использования служб для NFS

Службы для NFS позволяют поддерживать смешанные среды с операционными системами Windows и UNIX.

Службы для NFS также позволяют обновлять компьютеры компании без прекращения поддержки старой технологии в процессе перехода.

Приведенные ниже сценарии иллюстрируют преимущества, получаемые предприятием от развертывания служб для NFS.

- **Предоставление UNIX-клиентам возможности доступа к ресурсам на компьютерах с ОС Windows Server 2008 R2.** В компании также могут быть UNIX-клиенты, работающие с ресурсами на файловых серверах UNIX (например, с файлами). Для использования новых возможностей Windows Server® 2008 R2, таких как теневые копии общих папок, можно переместить ресурсы с серверов UNIX на компьютеры с ОС Windows Server® 2008 R2. Затем можно настроить службы для NFS, чтобы позволить UNIX-клиентам с программным обеспечением NFS получать доступ к этим компьютерам. Все UNIX-клиенты смогут получать доступ к ресурсам с помощью протокола NFS без дополнительной настройки.

- **Предоставление компьютерам с ОС Windows Server 2008 R2 доступа к ресурсам на файловых серверах UNIX.** В компании может использоваться смешанная среда Windows и UNIX, в которой файлы и другие ресурсы хранятся на файловых серверах UNIX. Службы для NFS можно использовать для обеспечения доступа компьютеров с ОС Windows Server® 2008 R2 к этим ресурсам, если файловые серверы используют программное обеспечение NFS.

- **Использование 64-разрядного оборудования.** Компоненты служб для NFS могут работать на 64-разрядных выпусках Windows Server® 2008 R2.

Компоненты служб для NFS

Службы для NFS содержат следующие компоненты:

- **Сервер для NFS.** Обычно компьютер с UNIX не может получить доступ к файлам на компьютере с Windows. Компьютер с ОС Windows Server® 2008 R2 и сервером для NFS может выступать в роли файлового сервера как для компьютеров с ОС Windows, так и для компьютеров с ОС UNIX.

- **Клиент для NFS.** Обычно компьютер с ОС Windows не может получить доступа к файлам на компьютере с ОС UNIX. Однако компьютер с ОС Windows Server® 2008 R2 и клиентом для NFS может обращаться к файлам, хранящимся на NFS-сервере с ОС UNIX.

Средства администрирования служб для NFS

Службы для NFS предоставляют оснастку консоли управления Microsoft (MMC) для администрирования, а также несколько программ командной строки.

Оснастка «Службы для NFS»

Оснастка «Службы для NFS» позволяет администрировать все установленные компоненты служб для NFS. После открытия оснастки все компоненты, установленные на локальном компьютере, будут доступны для администрирования.

Для выполнения этой процедуры пользователь должен быть членом группы «Администраторы» на локальном компьютере либо ему должны быть делегированы соответствующие права. Если компьютер присоединен к домену, эту процедуру могут выполнять члены группы «Администраторы домена». Из соображений безопасности службы для NFS рекомендуется запустить от имени администратора.

Чтобы получить справочные сведения об элементе этой оснастки, правой кнопкой мыши щелкнуть элемент, а затем в контекстном меню выбрать пункт «Справка».

Открытие служб для файловой системы NFS

- Нажать кнопку **Пуск**, выбрать элемент **Администрирование** и щелкнуть элемент **Службы для файловой системы (NFS)**.

Программы командной строки служб для NFS

Службы для NFS предоставляют указанные ниже программы администрирования, работающие из командной строки Windows. Чтобы запустить программу, требуется ввести ее имя в командной строке. Для получения сведений о параметрах, доступных для программы, ввести имя программы, а после него — параметр **/?**.

- **mount.** Подключение общих сетевых ресурсов NFS.
- **nfsadmin.** Управление сервером для NFS и клиентом для NFS.
- **nfsshare.** Контроль общих файловых ресурсов NFS.
- **nfsstat.** Отображение или сброс количества обращений к серверу для NFS.
- **showmount.** Отображение подключенных файловых систем, экспортированных сервером для NFS.
- **umount.** Удаление подключенных дисков NFS.

Тестовый сценарий

В этом тестовом сценарии службы для NFS необходимо развернуть в тестовой среде, чтобы оценить, как эта технология будет работать после ее развертывания в рабочей среде.

Приведенные указания помогут выполнить перечисленные ниже операции.

- Создание общего ресурса NFS на компьютере с ОС Windows Server® 2008 R2 и сервером для NFS, который можно подключить и использовать на компьютере с UNIX.
- Создание общего ресурса NFS на файловом сервере с UNIX, который можно подключить и использовать на компьютере с ОС Windows Server® 2008 R2 и клиентом для NFS.

Предварительные условия

Предполагается, что пользователь обладает указанными ниже знаниями и навыками.

- Знаком со средами операционных систем Windows и UNIX, а также с безопасностью файлов.
- Знает, как установить и использовать ОС Windows Server® 2008 R2.
- Понимает принцип взаимодействия клиента и сервера в сетевой среде.

Этапы развертывания и тестирования служб для NFS

Далее описана настройка базовой тестовой среды для служб для NFS. В нем описана установка и настройка компонентов служб для NFS и тестирование развертывания.

Обзор системных требований служб для NFS

Службы для NFS можно установить на компьютер под управлением любого выпуска ОС Windows Server 2008 R2.

Два основных компонента служб для NFS (сервер для NFS и клиент для NFS) можно установить на один компьютер или на отдельные компьютеры.

Перед установкой служб для NFS необходимо удалить все ранее установленные компоненты NFS.

Перед удалением компонентов NFS рекомендуется создать резервную копию данных на компьютере или записать конфигурацию, чтобы конфигурацию служб для NFS в дальнейшем можно было восстановить.

Службы для NFS можно использовать с компьютерами под управлением ОС UNIX, на которых запущен клиент или сервер NFS, если они соответствуют одной из следующих спецификаций протоколов:

- Спецификация протокола NFS версии 2 согласно документу RFC 1094 (страница может быть на английском языке) (http://go.microsoft.com/fwlink/?LinkId=150364).

- Спецификация протокола NFS версии 3 согласно документу RFC 1813 (страница может быть на английском языке) (http://go.microsoft.com/fwlink/?LinkId=150365).

По умолчанию сервер для NFS поддерживает клиентские компьютеры с UNIX, использующие NFS версии 2 или 3.

Однако это можно изменить, настроив сервер для NFS таким образом, чтобы доступ разрешался только клиентам с NFS версии 2 (указания см. в разделе «Настройка сервера для NFS» в справке по службам для NFS).

Клиент для NFS поддерживает обе версии и не настраивается.

Настройка среды для служб для NFS

Следующим шагом является настройка среды служб для NFS посредством развертывания компьютеров и создания учетных записей пользователей для тестирования.

Развертывание компьютеров

Необходимо развернуть указанные ниже компьютеры и подключить их к локальной сети.

- Один или более компьютеров с ОС Windows Server® 2008 R2, на которых устанавливаются две основные службы для компонентов NFS: сервер для NFS и клиент для NFS. Эти компоненты можно установить на один компьютер или на разные компьютеры. Инструкции по установке всех компонентов служб для NFS приводятся далее.

- Один или несколько компьютеров с ОС UNIX, на которых запущен клиент или сервер NFS. На компьютере с NFS-сервером размещается общий ресурс NFS UNIX, к которому получает доступ компьютер с ОС Windows Server® 2008 R2 и клиентом для NFS. Сервер для NFS и клиент для NFS можно установить на один компьютер или на разные компьютеры.

- Контроллер домена Windows Server® 2008 R2, работающий в режиме Windows Server® 2008 R2. Контроллер домена предоставляет сведения о проверке подлинности пользователя для среды Windows. Можно также использовать локальные учетные записи пользователей.

- NIS-сервер для предоставления сведений о проверке подлинности пользователя для среды UNIX. Можно также использовать файлы паролей и групп, хранящиеся на компьютере со службой сопоставления имен пользователей. Служба сопоставления имен пользователей может быть запущена на компьютере с Windows Server 2003 R3.

Создание тестовых учетных записей пользователей

В рамках теста можно создать несколько тестовых пользователей.

Для каждого пользователя можно создать только одну учетную запись безопасности Windows и одну учетную запись безопасности UNIX.

Двум учетным записям присваиваются разные имена.

Позже эти учетные записи можно использовать для тестирования функции расширенного сопоставления имен пользователей служб для NFS.

Расширенное сопоставление имен пользователей позволяет сопоставить учетные данные определенного пользователя в Windows и UNIX даже в том случае, если используются разные имена пользователя.

Альтернативой расширенному сопоставлению является простое сопоставление.

Простое сопоставление можно использовать в том случае, когда имена пользователей в ОС Windows и ОС UNIX совпадают для каждого пользователя.

Учетные записи пользователей ОС Windows можно создать на контроллере домена Windows Server 2008 R2.

Можно также создать локальные учетные записи пользователей на каждом компьютере с Windows в системе.

Указания по настройке учетных записей пользователей см. в документации к Windows Server 2008 R2.

Учетные записи пользователей UNIX можно создать как на NIS-сервере, так и в файлах UNIX /etc/passwd и /etc/group.

Указания по созданию учетных записей пользователей NIS см. в документации к NIS-серверу.

Инструкции по созданию файлов /etc/passwd и /etc/group см. в документации по операционной системе UNIX.

В таблице 4 приведены некоторые примеры тестовых пользователей и соответствующих учетных записей пользователей и групп, которые можно использовать в данном тестировании.

Таблица 4 - Примеры тестовых пользователей

Вымышленный пользователь	**Имя пользователя Windows**	**Имя пользователя UNIX**	**Имя группы Windows**	**Имя группы UNIX**
Анна Иванова	WindowsDomain\AnnaI	AIvanova@NISDomain	WinGroup	UNIXGrp
Роман Петров	WindowsDomain\RomanP	RomanP@NISDomain	WinGroup	UNIXGrp
Леонид Алексеев	WindowsDomain\LeonidA	LAlekseev@NISDomain	WinGroup	UNIXGrp

Установка служб для NFS

Компоненты служб для NFS необходимо установить на компьютер с ОС Windows Server® 2008 R2. В приведенных указаниях предполагается, что все компоненты устанавливаются на один компьютер.

Для выполнения этой процедуры пользователь должен быть членом группы «Администраторы» на локальном компьютере либо ему должны быть делегированы соответствующие права. Если компьютер присоединен к домену, эту процедуру могут выполнять члены группы «Администраторы домена». Из соображений безопасности службы для NFS рекомендуется запустить от имени администратора.

Перед установкой служб для NFS необходимо удалить все ранее установленные компоненты NFS. Перед удалением компонентов NFS рекомендуется создать резервную копию данных на компьютере или записать конфигурацию, чтобы конфигурацию служб для NFS в дальнейшем можно было восстановить.

Установка служб для компонентов NFS

1. Нажать кнопку **Пуск**, выбрать элемент **Администрирование**, а затем - элемент **Диспетчер сервера**.
2. В левой области щелкнуть элемент **Управление ролями**.
3. Щелкнуть пункт **Добавить роли**. Откроется мастер добавления ролей.
4. Нажать кнопку **Далее**. Откроется страница «Выбор ролей сервера»
5. Установить флажок **Файловый сервер** и нажать кнопку **Далее**.
6. Откроется экран файлового сервера. Для просмотра параметров служб роли нажать кнопку **Далее**.
7. Установить флажок **Службы для NFS** и нажать кнопку **Далее**.
8. Подтвердить выбранные параметры и нажать кнопку **Установить**.
9. По завершении установки будут выведены ее результаты. Нажать кнопку **Закрыть**.

При выборе компонентов «Сопоставление имен пользователей», «Сервер для NFS» или «Клиент для NFS» мастер компонентов Windows также выберет необходимый набор вспомогательных компонентов.

Настройка проверки подлинности NFS

В этом тесте должен использоваться контроллер домена Windows Server® 2008 R2, работающий в режиме Windows Server® 2008 R2. В целях безопасности рекомендуется установить Windows Server® 2008 R2 и все последние обновления системы безопасности.

Создание общей папки NFS

Следующим этапом является создание общей папки NFS при помощи общего доступа к NFS на компьютере со службами для NFS. Позже эту общую папку можно подключить на клиенте UNIX и создать на нем тестовый файл.

Для выполнения этой процедуры пользователь должен быть членом группы «Администраторы» на локальном компьютере либо ему должны быть делегированы соответствующие права.

Создание тестовой папки с помощью совместного доступа NFS

1. На компьютере с сервером для NFS создать папку, используемую в качестве общей папки NFS.
2. Правой кнопкой мыши щелкнуть созданную папку, а затем в контекстном меню выбрать команду **Общий доступ NFS**.
3. Установить флажок **Открыть общий доступ к этой папке**.
4. Если необходим анонимный доступ, установить флажок **Разрешить анонимный доступ**.
5. Щелкнуть **Разрешения**, нажать кнопку **Добавить** и выполнить одно из следующих действий:
    - В списке **Имена** выбрать клиентов и группы, которые нужно добавить, а затем нажать кнопку **Добавить**.
    - В текстовом поле **Добавить имена** ввести имена клиентов и групп, которые необходимо добавить, разделяя имена в списке точками с запятой.
6. В списке **Тип доступа** выбрать тип доступа, который необходим для выбранных клиентов и групп.
7. Выбрать параметр **Разрешить доступ пользователю root**, если пользователь *root* не должен иметь доступ в качестве анонимного пользователя. По умолчанию идентификатор пользователя *root* приводится к идентификатору анонимного пользователя.
8. В списке **Кодировка** выбрать тип кодировки имен каталогов и файлов, используемой для выбранных клиентов и групп.
9. Дважды нажать кнопку **ОК**, а затем нажать кнопку **Применить**.

Чтобы просмотреть список участников группы, выбрать группу в списке «Имена» и нажать кнопку «Участники».

Задание разрешений по умолчанию для новых файлов и папок

Существует возможность задания разрешений по умолчанию, которые будут применены компьютером с клиентом для NFS к общему ресурсу NFS. Можно назначить разрешения «Чтение», «Запись» и «Выполнение» для владельца, группы и других пользователей.

- **Владелец**. Пользователь, создавший файл. По умолчанию для пользователя установлены разрешения на чтение, запись и выполнение.
- **Группа**. Основная группа пользователя, создавшего файл. По умолчанию для группы установлены разрешения на чтение и выполнение.

- **Другие.** Другие пользователи системы (эквивалентно группе «Все» в Windows). По умолчанию для группы «Другие» установлены разрешения на чтение и выполнение.

Для выполнения этой процедуры пользователь должен быть членом группы «Администраторы» на локальном компьютере либо ему должны быть делегированы соответствующие права.

Задание разрешений для файлов по умолчанию

1. На компьютере с клиентом для NFS открыть службы для NFS. Чтобы открыть службы для NFS, нажать кнопку **Пуск**, выбрать пункт **Администрирование**, затем щелкнуть элемент **Службы для NFS**.
2. В дереве консоли правой кнопкой мыши щелкнуть элемент **Клиент для NFS**, а затем в контекстном меню выбрать пункт **Свойства**.
3. На вкладке **Разрешения для файлов** выбрать разрешения для файлов, которые будут по умолчанию применяться ко всем новым файлам и папкам, созданным этим компьютером, а затем нажать кнопку **ОК**.

Включение общего доступа к файлам и принтерам для программ администрирования

На компьютере с оснасткой «Службы для NFS» и средствами командной строки «Службы для NFS» необходимо включить общий доступ к файлам и принтерам в брандмауэре Windows

Открытие общего доступа к файлам и принтерам

1. На компьютере со службами для NFS нажать кнопку **Пуск**, выбрать команду **Выполнить**, ввести **firewall.cpl**, а затем нажать кнопку **ОК**.
2. Перейти на вкладку **Исключения**, выбрать пункт **Общий доступ к файлам и принтерам** и нажать кнопку **ОК**.
3. Повторить эти действия на каждом компьютере со службами для NFS.

Тестирование развертывания

После выполнения настройки можно выполнить проверку развернутой системы, чтобы убедиться в ее работоспособности. Далее предлагается несколько простых тестов.

Тест 1. На компьютере с клиентом для NFS назначить букву диска общему ресурсу NFS на UNIX.

Тест успешен, если удается назначить букву диска и просмотреть тестовый файл на общем ресурсе NFS с компьютера с клиентом для NFS.

Назначение буквы диска общему ресурсу NFS на UNIX

1. На сервере UNIX с программным обеспечением NFS создать общий ресурс NFS. Создать тестовый файл на общем ресурсе.
2. Войти в систему на компьютере с Windows Server® 2008 R2и клиентом для NFS с одной из учетных записей Windows, созданных для этого теста.
3. Откройте проводник и в меню **Сервис** выбрать команду **Подключить сетевой диск**.
4. Ввести имя сервера и общего ресурса в стандарте UNIX (сервер://имя_общего_ресурса) или UNC-путь к общему ресурсу NFS на файловом сервере UNIX.
5. Нажать кнопку **ОК**.

Тест 2. На компьютере с клиентом для NFS создать тестовый файл и проверить его разрешения.

Тест выполнен успешно, если удается создать новый документ, а его тип собственности и разрешения совпадают с разрешениями, которые были указаны для файлов по умолчанию.

Создание тестового файла и проверка его разрешений

1. Войти в систему на компьютере с клиентом для NFS с использованием одной из учетных записей Windows, созданных для этого теста.
2. Открыть общий ресурс NFS, который использовался в первом тесте.
3. Щелкнуть список правой кнопкой мыши, выбрать пункт **Создать**, затем выбрать команду **Текстовый документ**.
4. Ввести имя файла. Не использовать пробелы.
5. Щелкнуть файл правой кнопкой мыши, выбратьь пункт **Свойства**, а затем щелкнуть команду **Атрибуты NFS**.
6. Убедиться, что атрибуты NFS совпадают с указанными ранее атрибутами по умолчанию (см. раздел «Задание разрешений по умолчанию для новых файлов и папок»). Также убедиться в правильности идентификаторов пользователя и группы.

Тест 3. На клиентском компьютере с UNIX подключить общий ресурс NFS Windows.

Тест выполнен успешно, если удается подключить общий ресурс NFS.

Подключение общего ресурса NFS Windows

- В командной оболочке клиента UNIX с программным обеспечением клиента NFS ввести следующую команду:

  mount *имя_узла* **:/** *имя_ресурса точка_подключения*

Переменная	Описание
имя_узла	Имя компьютера с сервером для NFS, на котором ранее создан общий ресурс NFS (см. раздел «Создание общей папки NFS»).
имя_ресурса	Имя общего ресурса NFS.
точка_подключения	Точка в файловой системе, куда команда подключит общий ресурс NFS, например /home/username/testshare.

Тест 4. На клиенте UNIX создать тестовый файл и убедиться в том, что разрешения в Windows и UNIX совпадают.

Тест выполнен успешно, если удается создать текстовый файл, разрешения для которого совпадают в Windows и UNIX

Создание тестового файла и проверка соответствия разрешений файла

1. На клиентском компьютере UNIX, использовавшемся в третьем тесте, создать текстовый файл с помощью простого текстового редактора. Сохранить файл на общий ресурс NFS, смонтированный при выполнении третьего теста.
2. На компьютере с сервером для NFS и общим ресурсом NFS открыть Проводник Windows и перейти на общий ресурс NFS.
3. Правой кнопкой мыши щелкнуть имя файла и выбать в контекстном меню элемент **Свойства**, а затем — элемент **Безопасность**.
4. Сравнить разрешения файла, указанные в ОС Windows, с разрешениями файла, указанными в том же клиенте UNIX, который использовался в третьем тесте.

Тема 15. Виртуализация

Виртуализация - это изоляция вычислительных процессов и ресурсов друг от друга [4].

Типы виртуализации

Виртуализация — это общий термин, охватывающий абстракцию ресурсов для многих аспектов вычислений. Типы виртуализации приводятся ниже.

Программная виртуализация

Динамическая трансляция

При динамической (бинарной) трансляции проблемные команды гостевой ОС перехватываются гипервизором. После того как эти команды заменяются безопасными, происходит возврат управления гостевой ОС.

Паравиртуализация

Паравиртуализация - техника виртуализации, при которой гостевые операционные системы подготавливаются для исполнения в виртуализированной среде, для чего их ядро незначительно модифицируется. Гостевая операционная система взаимодействует с программой гипервизора, который предоставляет ей гостевой API, вместо использования напрямую таких ресурсов, как таблица страниц памяти.

Метод паравиртуализации позволяет добиться более высокой производительности, чем метод динамической трансляции.

Метод паравиртуализации применим лишь в том случае, если гостевые ОС имеют открытые исходные коды, которые можно модифицировать согласно лицензии, или же гипервизор и гостевая ОС разработаны одним производителем с учетом возможности паравиртуализации гостевой ОС (при условии того, что под гипервизором может быть запущен гипервизор более низкого уровня, то и паравиртуализации самого гипервизора).

Встроенная виртуализация

Преимущества:

1. Совместное использование ресурсов обеими ОС (каталоги, принтеры и т.д.).
2. Удобство интерфейса для окон приложений из разных систем (перекрывающиеся окна приложений, одинаковая минимизация окон, как в хост-системе)
3. При тонкой настройке на аппаратную платформу производительность мало отличается от оригинальной нативной ОС. Быстрое переключение между системами (менее 1 сек.)
4. Простая процедура обновления гостевой ОС.
5. Двухсторонняя виртуализация (приложения одной системы запускаются в другой и наоборот)

Аппаратная виртуализация

Аппаратная виртуализация - виртуализация с поддержкой специальной процессорной архитектуры. В отличие от программной виртуализации, с помощью данной техники возможно использование изолированных гостевых систем, управляемых гипервизором напрямую. Гостевая система не зависит от архитектуры хостовой платформы и реализации платформы виртуализации. Например, с помощью технологий аппаратной виртуализации возможен запуск 64-битных гостевых систем на 32-битных хостовых системах.

Аппаратная виртуализация обеспечивает производительность, сравнимую с производительностью невиртуализованной машины, что дает виртуализации возможность практического использования и влечет её широкое распространение. Наиболее распространены технологии виртуализации Intel-VT и AMD-V.

1. В Intel VT (Intel Virtualization Technology) реализована виртуализация режима реальной адресации (режим совместимости с 8086). Соответствующая аппаратная виртуализация ввода-вывода - VT-d. Часто обозначается аббревиатурой VMX (Virtual Machine eXtension). Кодовое название - Vanderpool.
2. AMD-V часто обозначается аббревиатурой SVM (Secure Virtual Machines). Кодовое название - Pacifica. Соответствующая технология виртуализации ввода-вывода - IOMMU. Поддержка AMD-V появилась в Xen 3.3.

Преимущества Аппаратной виртуализации:

- Упрощение разработки программных платформ виртуализации за счет предоставления аппаратных интерфейсов управления и поддержки виртуальных гостевых систем. Это уменьшает трудоемкость и время на разработку систем виртуализации.
- Возможность увеличения быстродействия платформ виртуализации. Управление виртуальными гостевыми системами осуществляет напрямую небольшой промежуточный слой программного обеспечения, гипервизор, что дает увеличение быстродействия.
- Улучшается защищённость, появляется возможность переключения между несколькими запущенными независимыми платформами виртуализации на аппаратном уровне. Каждая из виртуальных машин может работать независимо, в своем пространстве аппаратных ресурсов, полностью изолированно друг от друга. Это позволяет устранить потери быстродействия на поддержание хостовой платформы и увеличить защищенность.
- Гостевая система становится не привязанной к архитектуре хостовой платформы и к реализации платформы виртуализации. Технология аппаратной виртуализации делает возможным запуск 64-битных гостевых систем на 32-битных хостовых системах (с 32-битными средами виртуализации на хостах).

Виртуализация на уровне операционной системы

Виртуализация на уровне операционной системы — метод виртуализации, при котором ядро операционной системы поддерживает несколько изолированных экземпляров пространства пользователя, вместо одного.

Экземпляры (часто называемые контейнерами или зонами) с точки зрения пользователя полностью идентичны реальному серверу.

Ядро обеспечивает полную изолированность контейнеров, поэтому программы из разных контейнеров не могут воздействовать друг на друга.

Виртуализация на уровне операционной системы виртуализирует физический сервер на уровне ОС, позволяя запускать изолированные и безопасные виртуальные серверы на одном физическом сервере. Эта технология не позволяет запускать ОС с ядрами, отличными от типа ядра базовой ОС.

При виртуализации на уровне операционной системы не существует отдельного слоя гипервизора. Вместо этого сама хостовая операционная система отвечает за разделение аппаратных ресурсов между несколькими виртуальными серверами и поддержку их независимости друг от друга.

Области применения виртуализации

Виртуальные машины

Виртуальная машина — это окружение, которое представляется для «гостевой» операционной системы, как аппаратное.

Однако это программное окружение, которое эмулируется программным обеспечением хостовой системы.

Эта эмуляция должна быть достаточно надёжной, чтобы драйверы гостевой системы могли стабильно работать.

При использовании паравиртуализации, виртуальная машина не эмулирует аппаратное обеспечение, а предлагает использовать специальное API.

Виртуальная машина (ВМ, от англ. *virtual machine*) -

1. программная и/или аппаратная система, эмулирующая аппаратное обеспечение некоторой платформы (target — целевая, или гостевая платформа) и исполняющая программы для target-платформы на host-платформе (host — хост-платформа, платформа-хозяин)
2. виртуализирующая некоторую платформу и создающая на ней среды, изолирующие друг от друга программы и даже операционные системы (см.: песочница);
3. спецификация некоторой вычислительной среды (например: «виртуальная машина языка программирования Си»).

Виртуальная машина исполняет некоторый машинно-независимый код (например, байт-код, шитый код, p-код) или машинный код реального процессора. Помимо процессора, ВМ может эмулировать работу, как отдельных компонентов аппаратного обеспечения, так и целого реального компьютера (включая BIOS, оперативную память, жёсткий диск и другие периферийные устройства).

В последнем случае в ВМ, как и на реальный компьютер, можно устанавливать операционные системы (например, Windows можно запускать в виртуальной машине под Linux или наоборот).

На одном компьютере может функционировать несколько виртуальных машин (это может использоваться для имитации нескольких серверов на одном реальном сервере с целью оптимизации использования ресурсов сервера).

Виртуальные машины могут использоваться для:

1. защиты информации и ограничения возможностей программ;

2. исследования производительности ПО или новой компьютерной архитектуры;
3. эмуляции различных архитектур;
4. оптимизации использования ресурсов мейнфреймов и прочих мощных компьютеров (например: IBM eServer);
5. вредоносного кода для управления инфицированной системой: вирус PMBS, обнаруженный в 1993 году, а также руткит SubVirt, созданный в 2006 году в Microsoft Research, создавали виртуальную систему, которой ограничивался пользователь и все защитные программы.
6. моделирования информационных систем с клиент-серверной архитектурой на одной ЭВМ (эмуляция компьютерной сети с помощью нескольких виртуальных машин).
7. упрощения управления кластерами — виртуальные машины могут просто мигрировать с одной физической машины на другую во время работы.
8. тестовые лаборатории и обучение: Тестированию в виртуальных машинах удобно подвергать приложения, влияющие на настройки операционных систем, например инсталляционные приложения. За счёт простоты в развёртывании виртуальных машин, они часто используются для обучения новым продуктам и технологиям.
9. распространение предустановленного ПО: многие разработчики программных продуктов создают готовые образы виртуальных машин с предустановленными продуктами и предоставляют их на бесплатной или коммерческой основе. Такие услуги предоставляют VMWare VMTN или Parallels PTN

Таблица 5 - Некоторые известные виртуальные машины

Среды языков программирования	Операционные системы и гипервизоры	Автономные эмуляторы компьютеров
• ActionScript Virtual Machine • Common Language Runtime • Форт • Java Virtual Machine • UCSD p-System	• Система виртуальных машин • ICore Virtual Accounts • Kernel-based Virtual Machine • Hyper-V • User-mode Linux • VM/CMS • VMware ESX • Xen	• bochs • DOSBox • Virtual PC • Parallels Workstation • QEMU • VirtualBox • VMware Fusion • VMware Workstation

Виртуализация серверов

Виртуализация сервера – это:

1. размещение нескольких логических серверов в рамках одного физического (консолидация)
2. объединение нескольких физических серверов в один логический для решения определенной задачи. Пример: Oracle Real Application Cluster, grid-технология, кластеры высокой производительности.

Виртуализация сервера упрощает восстановление вышедших из строя систем на любом доступном компьютере, вне зависимости от его конкретной конфигурации.

Виртуализация рабочих станций

Виртуализация ресурсов

- **Разделение ресурсов (partitioning)**. Виртуализация ресурсов может быть представлена как разделение одного физического сервера на несколько частей, каждая из которых видна для владельца в качестве отдельного сервера. Не является технологией виртуальных машин, осуществляется на уровне ядра ОС. В системах с гипервизором второго типа обе ОС (гостевая и гипервизора) отнимают физические ресурсы, и требует отдельного лицензирования. Виртуальные серверы, работающие на уровне ядра ОС, почти не теряют в быстродействии, что дает возможность запускать на одном физическом сервере сотни виртуальных, не требующих дополнительных лицензий. Разделяемое дисковое пространство или пропускной канал сети на некоторое количество меньших составляющих, легче используемых ресурсов того же типа.
- **Агрегация, распределение или добавление множества ресурсов в большие ресурсы или объединение ресурсов**. Например, симметричные мультипроцессорные системы объединяют множество процессоров; RAID и дисковые менеджеры объединяют множество дисков в один большой логический диск; RAID и сетевое оборудование использует множество каналов, объединённых так, чтобы они представлялись, как единый широкополосный канал. На мета-уровне компьютерные кластеры делают все вышеперечисленное. Иногда сюда же относят сетевые файловые системы, абстрагированные от хранилищ данных на которых они построены, например, Vmware VMFS, Solaris/OpenSolaris ZFS, NetApp WAFL.

Виртуализация приложений

Виртуализация приложений - процесс использования приложения преобразованного из требующего установки в ОС в не требующий (требуется только запустить). Для виртуализации приложений программное обеспечение виртуализатора определяет при установке виртуализуемого приложения, какие тре-

буются компоненты ОС и их эмулирует, таким образом, создаётся необходимая специализированная среда для конкретно этого виртуализируемого приложения и, тем самым, обеспечивается изолированность работы этого приложения.

Для создания виртуального приложения виртуализируемое помещается в контейнер, оформленный, как правило, в виде папки. При запуске виртуального приложения запускается виртуализируемое приложение и контейнер, являющийся для него рабочей средой.

Рабочая среда запускается и предоставляет локальные ранее созданные ресурсы, которое включает в себя ключи реестра, файлы и другие компоненты, необходимые для запуска и работы приложения. Такая виртуальная среда работает как прослойка между приложением и операционной системой, что позволяет избежать конфликтов между приложениями. Виртуализацию приложений обеспечивают, например, программы Citrix XenApp, SoftGrid и VMWare ThinApp

Достоинства:

- изолированность исполнения приложений: отсутствие несовместимостей и конфликтов;
- каждый раз в первозданном виде: не загромождается реестр, нет конфигурационных файлов — необходимо для сервера;
- меньшие ресурсозатраты по сравнению с эмуляцией всей ОС.

Гипервизор

Гипервизор (или Монитор виртуальных машин) - в компьютерах программа или аппаратная схема, обеспечивающая или позволяющая одновременное, параллельное выполнение нескольких или даже многих операционных систем на одном и том же хост-компьютере [2]. Гипервизор также обеспечивает изоляцию операционных систем друг от друга, защиту и безопасность, разделение ресурсов между различными запущенными ОС и управление ресурсами.

Гипервизор также может (но не обязан) предоставлять работающим под его управлением на одном хост-компьютере ОС средства связи и взаимодействия между собой (например, через обмен файлами или сетевые соединения) так, как если бы эти ОС выполнялись на разных физических компьютерах.

Гипервизор сам по себе в некотором роде является минимальной операционной системой (микроядром или наноядром). Он предоставляет запущенным под его управлением операционным системам сервис виртуальной машины, виртуализируя или эмулируя реальное (физическое) аппаратное обеспечение конкретной машины, и управляет этими виртуальными машинами, выделением и освобождением ресурсов для них. Гипервизор позволяет независимое «включение», перезагрузку, «выключение» любой из виртуальных машин с той или иной ОС. При этом операционная система, работающая в виртуальной машине под управлением гипервизора, может, но не обязана «знать», что она выполняется в виртуальной машине, а не на реальном аппаратном обеспечении.

Типы гипервизора

Автономный гипервизор (Тип 1)

Имеет свои встроенные драйверы устройств, модели драйверов и планировщик и поэтому не зависит от базовой ОС. Так как автономный гипервизор работает непосредственно на оборудовании, то он более производителен. Пример: VMware ESX

На основе базовой ОС (Тип 2, V)

Это компонент, работающий в одном кольце с ядром основной ОС (кольцо 0). Гостевой код может выполняться прямо на физическом процессоре, но доступ к устройствам ввода-вывода компьютера из гостевой ОС осуществляется через второй компонент, обычный процесс основной ОС - монитор уровня пользователя. Примеры: Microsoft Virtual PC, VMware Workstation, QEMU, Parallels, VirtualBox.

Гибридный (Тип 1+)

Гибридный гипервизор состоит из двух частей: из тонкого гипервизора, контролирующего процессор и память, а также работающей под его управлением специальной сервисной ОС в кольце пониженного уровня. Посредством сервисной ОС гостевые ОС получают доступ к физическому оборудованию. Примеры: Microsoft Virtual Server, Sun Logical Domains, Xen, Citrix XenServer, Microsoft Hyper-V.

Тема 16. Hyper-V

Microsoft Hyper-V (кодовое имя Viridian) — система виртуализации для x64-систем на основе гипервизора [4]. Бета-версия Hyper-V была включена в x64-версии Windows Server 2008. Ранее была известна как виртуализация Windows Server (Windows Server Virtualization)

Версии и варианты

Hyper-V существует в двух вариантах:

1. отдельный продукт Microsoft Hyper-V Server 2008 (Hyper-V Server 2008 R2 для второй версии)
2. как роль в Windows Server 2008 и Windows Server 2008 R2.

Отдельная версия Hyper-V Server является бесплатной. Является базовым («Server Core») вариантом Windows Server 2008, то есть включает в себя полную функциональность Hyper-V; прочие роли Windows 2008 Server отключены, также лимитированы службы Windows. Бесплатная 64-битная Core-версия Hyper-V ограничена интерфейсом командной строки (CLI PowerShell), где конфигурация текущей ОС, физического аппаратного и программного оборудования выполняется при помощи команд оболочки. Новое меню интерфейса управления позволяет выполнить простую первичную конфигурацию, а некоторые свободно распространяемые скрипты расширяют данную концепцию.

Администрирование и конфигурирование виртуального сервера (или гостевых ОС) осуществляется при помощи ПО, установленного на ПК под управлением Windows Vista, Windows 7 или Windows 2008 Server с установленным дополнением для администрирования Hyper-V из MMC. Другим вариантом администрирования/конфигурирования сервера Windows 2008 Core является использование удаленной Windows или Windows Server при перенаправлении (некоторой) консоли управления (MMC), указывающей на Core Server. Это значительно упрощает настройку, сводя её к нескольким кликам мыши.

Архитектура

Hyper-V поддерживает разграничение согласно понятию раздел. Раздел - логическая единица разграничения, поддерживаемая гипервизором, в котором работают операционные системы. Каждый экземпляр гипервизора должен иметь один родительский раздел, с запущенной Windows Server 2008. Стек виртуализации запускается на родительском разделе и обладает прямым доступом к аппаратным устройствам. Затем родительский раздел порождает дочерние разделы, на которых и располагаются гостевые ОС. Дочерний раздел также может породить собственные дочерние разделы. Родительский раздел создает дочерние при помощи API гипервызова, представленного в Hyper-V.

Виртуализированные разделы не имеют ни доступа к физическому процессору, ни возможности управлять его реальными прерываниями. Вместо этого, у них есть виртуальное представление процессора и гостевой виртуальный адрес, зависящий от конфигурации гипервизора, вовсе необязательно при этом занимающий все виртуальное адресное пространство. Гипервизор может определять подмножество процессоров для каждого раздела. Гипервизор управляет прерываниями процессора и перенаправляет их в соответствующий раздел, используя логический контроллер искусственных прерываний (Synthetic Interrupt Controller или сокр. SynIC).

Hyper-V может аппаратно ускорять трансляцию адресов между различными гостевыми виртуальными адресными пространствами при помощи IOMMU (I/O Memory Management Unit - Устройство управления вводом-выводом памяти), которое работает независимо от аппаратного управления памятью, используемого процессором.

Дочерние разделы не имеют непосредственного доступа к аппаратным ресурсам, но зато получают виртуальное представление ресурсов, называемое виртуальными устройствами. Любая попытка обращения к виртуальным устройствам перенаправляется через VMBus к устройствам родительского раздела, которые и обработают данный запрос. **VMBus -** это логический канал, осуществляющий взаимодействие между разделами.

Ответ возвращается также через VMBus. Если устройства родительского раздела также являются виртуальными устройствами, то запрос будет передаваться дальше пока не достигнет такого родительского раздела, где он получит доступ к физическим устройствам. Родительские разделы запускают провайдер сервиса виртуализации (Virtualization Service Provider или сокр. VSP), который

соединяется с VMBus и обрабатывает запросы доступа к устройствам от дочерних разделов. Виртуальные устройства дочернего раздела работают с клиентом сервиса виртуализации (Virtualization Service Client или сокр. VSC), который перенаправляет запрос через VMBus к VSP родительского раздела. Этот процесс прозрачен для гостевой ОС.

Виртуальные устройства также поддерживают технологию Windows Server Virtualization, называемую прогрессивный ввод/вывод (англ. Enlightened I/O), для накопителей, сетевых и графических подсистем в том числе. Enlightened I/O - специализированая виртуализационая реализация высокоуровневых протоколов как, например, SCSI, для возможности работать с VMBus напрямую, что позволяет параллельно обрабатывать любые уровни эмуляции устройства. Это делает взаимодействие более эффективным, но взамен требует от гостевой ОС поддержки Enlightened I/O.

Системные требования / Спецификации

1. x64-совместимый процессор, поддерживающий запуск x64-версии Windows Server 2008 Standard, Windows Server 2008 Enterprise или Windows Server 2008 Datacenter.
2. Аппаратная поддержка виртуализации. Эта особенность процессоров, дающая возможность аппаратной виртуализации; касается технологий Intel VT и AMD Virtualization (AMD-V, ранее известная как Pacifica).
3. NX-бит-совместимый процессор и активированая аппаратная поддержка Data Execution Prevention (DEP).
4. Память объёмом минимум 2 Гб (каждая виртуальная ОС требует собственного объёма памяти, поэтому реально нужно больше).
5. Windows 2008 Standard (64-bit) Hyper-V Core требует примерно 3 Гб дискового пространства в установленном виде.
6. Windows 2008 Standard (64-bit) Hyper-V с GUI требует примерно 8 Гб дискового пространства в установленном виде.
7. Windows 2008 Standard (64-bit) Hyper-V с GUI или в виде Core версии поддерживает до 31 Гб памяти для работы VM, плюс 1 Гб для родительской ОС Hyper-V.
8. Windows 2008 Standard (64-bit) Hyper-V с GUI или в виде Core поддерживает до 8 процессоров с 1, 2 или 4 ядрами.
9. Windows 2008 Standard (64-bit) Hyper-V с GUI или в виде Core поддерживает до 384 гостевых ОС.
10. Windows 2008 Standard (64-bit) Hyper-V с GUI или в виде Core поддерживает 32-битные (x86) и 64-битные (x86_64) гостевые виртуальные машины.

Отдельный Hyper-V Server не требует установленного Windows Server 2008, а требование к минимуму памяти составляет 1Гб и дискового пространства 2Гб.

Поддержка гостевых ОС

Список поддерживаемых/протестированных операционных систем включает

- Windows Server 2008 x86/x64 SP1/SP2 и R2
- Windows HPC Server 2008
- Windows Server 2003 x86/x64 SP2 R2
- Windows 2000 Server SP4 и Advanced Server SP4
- Windows 7 (кроме Home editions)
- Windows Vista SP1/SP2 (кроме Home editions)
- Windows XP Professional SP2/SP3/x64
- SUSE Linux Enterprise Server (SLES) 10 SP3 и 11
- Red Hat Enterprise Linux (RHEL) 5.2 - 5.6 (x86 Edition или x86_64 Edition)
- Red Hat Enterprise Linux (RHEL) 6.0, 6.1 (x86 Edition или x86_64 Edition)
- CentOS 5.2 - 5.6, 6.0
- FreeBSD 8.2-8.3
- Ubuntu 12.04

Ограничения

Имеются ограничения на доступ к USB-накопителям в гостевых ВМ, в поддержке старых приложений для MS-DOS, игр, Unreal mode. Hyper-V поддерживает живую миграцию (начиная с Windows Server 2008 R2) гостевых ВМ, где живая миграция понимается как поддержка сетевых соединений и отсутствие прерываний выполнения служб во время переноса ВМ.

Hyper-V Security или безопасность Hyper-V

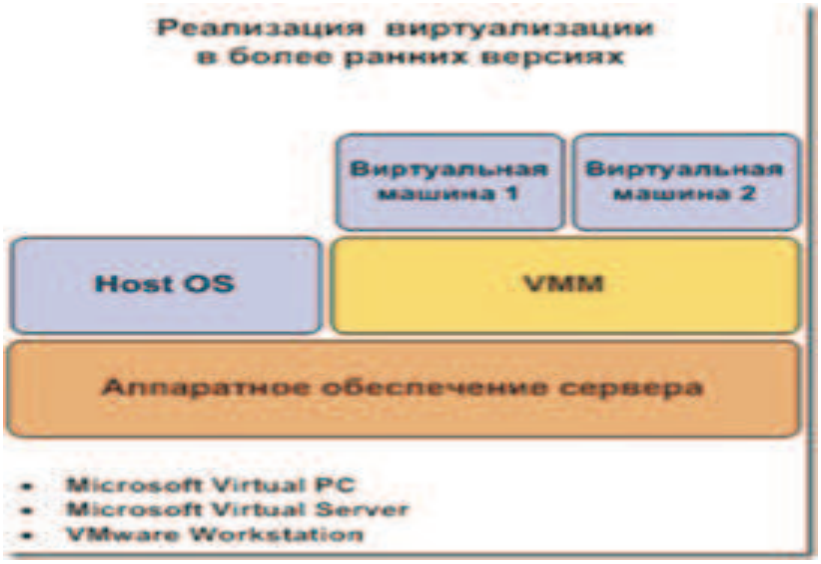

Рис. 8. Архитектура систем виртуализации более ранних версий.

Существует несколько типов систем виртуализации - предыдущие версии систем виртуализации и системы виртуализации на базе гипервизора[4].

В качестве примера предыдущих версий систем можно привести:

- Microsoft Virtual PC
- Microsoft Virtual Server
- VMware Workstation
- VMware Player

Архитектура предыдущих систем виртуализации (рис.8.) предполагает, что монитор виртуальных машин (МВМ) устанавливается прямо поверх операционной системы и работает в среде хостовой операционной системы (ОС).

Монитор виртуальных машин является приложением или службой операционной системы. Если посмотреть более детально, то процесс установки мониторов виртуальных машин предыдущих версий выглядит следующим образом:

В обычной операционной системе Windows Server 2003 или Windows XP выполняется установка программного обеспечения, будь то Virtual Server или WMware Workstation. При этом в операционную систему устанавливаются и настраиваются некоторые службы, которые запускаются после загрузки основной операционной системы. Данные службы выполняются в пользовательском окружении процессора – так называемом пользовательском режиме. Этот режим является самым низкоприоритетным. Все виртуальные машины, которые запускаются данными службами, работают в этом же режиме. Основным недостатком работы такого типа виртуальных машин являются возникающие сложности с операциями ввода-вывода при обращении к устройствам ввода-вывода: сетевому адаптеру, жесткому диску, клавиатуре, мыши, видеоподсистеме и т.д.

Виртуальная машина ничего не знает о системе виртуализации. С точки зрения виртуальной машины, она работает на некоем аппаратном обеспечении, которое в свою очередь эмулируется приложением и службами систем виртуализации (за исключением Windows Vista, Windows 7, Windows Server 2008/R2).

Чтобы обработать запрос виртуальной машины (например, на отправку одного сетевого пакета) операционной системе хоста необходимо сделать следующее.

Виртуальная машина отправляет запрос на отправку пакета данных по сети (происходит это в пользовательском режиме), запрос направляется виртуальным устройствам, эмулируемым для этой виртуальной машины, далее монитор виртуальных машин перехватывает данный запрос и выполняет его обработку, ставит его в очередь, после чего монитор виртуальных машин снова обращается к виртуальной машине, чтобы проверить наличие других запросов, для формирования буфера перед отправкой данных драйверу устройства.

Таким образом, обработка операций ввода вывода с виртуальных машин занимает немалое время.

Для ускорения операций в разных системах виртуализации реализованы некоторые инструменты, так называемые «Компоненты интеграции». Для Virtual Server это VM editions, в VMware Workstation это VMware Tools. Инст-

рументы интеграции позволяют устранить некоторые прослойки между виртуальным оборудованием и уровнем абстрагирования физического сервера.

И все равно процесс работы выполняется значительно медленнее, чем при работе с физическим сервером. Существуют также и другие недостатки в работе мониторов виртуальных машин предыдущих версий.

Виртуализация на базе гипервизора (рис.9.) основана на том, что между оборудованием и виртуальными машинами появляется прослойка, перехватывающая обращения операционных систем к процессору, памяти и другим устройствам. При этом доступ к периферийным устройствам в разных реализациях гипервизоров может быть организован по-разному.

Архитектура гипервизора предполагает, что монитор виртуальных машин (МВМ) устанавливается прямо поверх аппаратного обеспечения, в отличие от случая, где МВМ работает в среде хостовой операционной системы (ОС).

Такой подход к построению МВМ позволяет достичь более высокой производительности, также исключает накладные расходы, связанные с работой хостовой ОС.

Благодаря использованию в Hyper-V синтетических драйверов, которые не требуют дополнительной эмуляции виртуальных устройств, обмены данными при операциях ввода/вывода происходят гораздо быстрее по сравнению с традиционными решениями.

Максимальный эффект достигается при использовании в гостевых виртуальных машинах операционных систем Windows Server® 2008 и Windows Vista™ с установленными в них драйверами синтетических устройств.

В такой конфигурации находят, в частности применение синтетические драйверы для сетевых адаптеров и адаптеров памяти, тесно взаимодействующие с Windows-API.

Рис. 9. Архитектура систем виртуализации на базе гипервизора.

Это позволяет Hyper-V осуществлять быстрое преобразование I/O-запросов от гостевых систем в запросы к физическому оборудованию на родительском разделе.

Используя соответствующие компоненты интеграции, синтетические драйверы могут применяться также в отличных от Windows операционных системах (таких, как, например, операционные системы Linux с XEN).

В разных решениях виртуализации применяются разные подходы к реализации архитектуры построения гипервизоров - монолитный и микроядерный. В частности, в VMware ESX реализован принцип монолитного гипервизора. Microsoft Hyper-V реализована архитектура микроядерного гипервизора.

Монолитный подход в реализации гипервизора

Монолитный подход в реализации гипервизора (рис.10) подразумевает, что все драйверы устройств помещены в гипервизор. Вроде бы это дает некое преимущество с точки зрения безопасности драйверов. Нет возможности доработать драйверы, соответственно, никакой сторонний код не попадает в гипервизор. В монолитной (monolithic) модели гипервизор для доступа к оборудованию использует собственные драйверы.

Гостевые ОС работают на виртуальных машинах поверх гипервизора. Когда гостевой системе нужен доступ к оборудованию, она должна пройти через гипервизор и его модель драйверов. Обычно одна из гостевых ОС играет роль администратора или консоли, в которой запускаются компоненты для предоставления ресурсов, управления и мониторинга всех гостевых ОС, работающих на сервере.

Рис. 10. Архитектура монолитного гипервизора.

Модель монолитного гипервизора (рис.10) обеспечивает прекрасную производительность, но «хромает» с точки зрения защищенности и устойчивости. Это связано с тем, что она обладает более широким фронтом нападения и под-

вергает систему большему потенциальному риску, поскольку разрешает работу драйверов (а иногда даже программ сторонних производителей) в очень чувствительной области.

Вредоносная программа способна жить в гипервизоре под видом драйвера устройства. Если такое случиться, под контролем такой программы окажутся все гостевые ОС системы, что, конечно, не радует. Хуже того, этот «жучок» будет совершенно невозможно обнаружить средствами гостевых ОС: гипервизор ими по определению не видим!

Еще одна проблема – устойчивость: если в обновленную версию драйвера затесалась ошибка, в результате сбои начнутся во всей системе, во всех ее виртуальных машинах.

Иными словами, в этой модели критическое значение приобретает устойчивость драйверов, а они зачастую создаются сторонними производителями, что может стать причиной проблем. При этом оборудование серверов постоянно эволюционирует, и потому драйверы обновляются довольно часто, что увеличивает риск различных неприятностей. Можно считать монолитную модель моделью «толстого гипервизора» – из-за количества драйверов, поддержка которых ему требуется.

Также можно отметить проблему обновления драйверов – например, сетевой адаптер некорректно обрабатывает запросы. В обычной ситуации проблема решается обновлением драйвера на более новую версию. В случае с монолитным гипервизором обновить драйвер нельзя и придется ждать выхода новой версии гипервизора, в которую будет интегрирован новый драйвер для устройства.

Такая реализация гипервизора накладывает существенные проблемы с точки зрения неподдерживаемого оборудования. Например, собрались использовать оборудование «Сервер» достаточно мощный и надежный, но при этом в гипервизоре не оказалось нужного драйвера для RAID-контроллера или сетевого адаптера. Это сделает невозможным использование соответствующего оборудования, а, значит, и сервера. Тоже справедливо и для вновь подключаемых устройств - если в гипервизоре нет драйвера для устройства, его использовать нельзя.

Если даже в новой версии гипервизора будет нужный драйвер, потребуется остановить все виртуальные машины на узле или перенести виртуальные машины (в случае, если это кластер) на другой узел, после чего произвести обновление гипервизора. Сами обновления, с точки зрения безопасности, тоже не самое безопасное мероприятие.

Микроядерный подход в реализации гипервизора

В микроядерной модели гипервизора (microkernelized) (рис.11) можно говорить о «тонком гипервизоре», в этом случае в нем совсем нет драйверов. Вместо этого драйверы работают в каждом индивидуальном разделе, чтобы любая гостевая ОС имела возможность получить через гипервизор доступ к оборудованию. При такой расстановке сил каждая виртуальная машина занима-

ет совершенно обособленный раздел, что положительно сказывается на защищенности и надежности.

В микроядерной модели гипервизора (в виртуализации Windows Server 2008 R2 используется именно она) один раздел является родительским (parent), остальные – дочерними (child). Раздел – это наименьшая изолированная единица, поддерживаемая гипервизором.

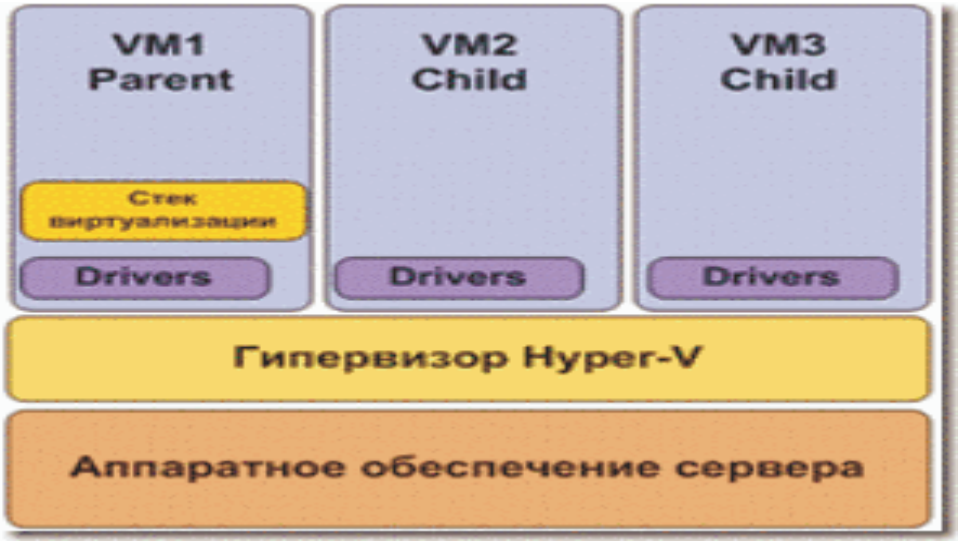

Рис. 11. Микроядерный подход в реализации гипервизора.

Каждому разделу назначают конкретные аппаратные ресурсы - долю процессорного времени, объем памяти, устройства и пр. Родительский раздел создает дочерние разделы и управляет ими, а также содержит стек виртуализации (virtualization stack), используемый для управления дочерними разделами. Родительский раздел, вообще говоря, является также корневым (root), поскольку он создается первым и владеет всеми ресурсами, не принадлежащими гипервизору. Обладание всеми аппаратными ресурсами означает среди прочего, что именно корневой (то есть, родительский) раздел управляет питанием, подключением самонастраивающихся устройств, ведает вопросами аппаратных сбоев и даже управляет загрузкой гипервизора.

В родительском разделе содержится стек виртуализации - набор программных компонентов, расположенных поверх гипервизора и совместно с ним обеспечивающих работу виртуальных машин. Стек виртуализации обменивается данными с гипервизором и выполняет все функции по виртуализации, не поддерживаемые непосредственно гипервизором. Большая часть этих функций связана с созданием дочерних разделов и управлением ими и необходимыми им ресурсами (ЦП, память, устройства).

Стек виртуализации также обеспечивает доступ к интерфейсу управления, который в случае Windows Server 2008 R2 является поставщиком WMI.

Преимущество микроядерного подхода, примененного в Windows Server 2008 R2, по сравнению с монолитным подходом состоит в том, что драйверы, которые должны располагаться между родительским разделом и физическим сервером, не требуют внесения никаких изменений в модель драйверов. Иными

словами, в системе можно просто применять существующие драйверы. В Microsoft этот подход избрали, поскольку необходимость разработки новых драйверов сильно затормозила бы развитие системы.

Что же касается гостевых ОС, они будут работать с эмуляторами или синтетическими устройствами.

С другой стороны, нужно признать, что микроядерная модель может несколько проигрывать монолитной модели в производительности.

Однако для большинства компаний вполне приемлема будет потеря пары процентов в производительности ради повышения устойчивости.

Размер гипервизора Hyper-V менее 1,5 Мб, он может поместиться на одну 3.5-дюймовую дискету.

Выводы

Основная задача гипервизора – это планирование ресурсов, гипервизор отвечает за то, кто, когда получает доступ к таким ресурсам как процессор и память, каким образом разделяется доступ между операционной памятью физической ОС и виртуальной. Доступ к физическим устройствам контролируется основной операционной системой.

Эта ОС отвечает за доступ к устройствам ввода/вывода. Драйверы всех устройств устанавливаются поверх Windows Server 2008 R2. Большим преимуществом такого подхода является возможность обновлять драйверы устройств. При этом нет необходимости выполнять переустановку гипервизора. Не нужно вносить никакие исправления в гипервизор, нет прямой зависимости от вендора в части драйверов и обновлений. С точки зрения безопасности такой процесс является оптимальным.

С точки зрения безопасности, чем меньше объем самого гипервизора, тем безопаснее; меньше вероятность потенциальных ошибок в коде. Сам гипервизор работает с уровнем привелегий Ring 0 – это ниже чем приоритет работы ядра ОС – включение драйверов в гипервизор увеличивает его объем и потенциальную возможность уязвимости такого гипервизора.

Если посмотреть динамику выхода обновлений для гипервизора с монолитной реализацией, можно увидеть, что обновления, появляются довольно часто. А это означает, что в большинстве случаев требуется проводить и обновление гипервизора для исправления тех или иных дыр в безопасности.

Вместе с исправлениями публикуется и информация о том, какого рода уязвимость корректируется путем установки данного обновления. Эта информация легко доступна в Интернете и может быть использована злоумышленниками для реализации всевозможного рода эксплойтов.

Тем самым увеличивается потенциальная возможность уязвимости данных систем. Естественно необходимо следить и вовремя устанавливать всевозможные обновления для гипервизора.

Безопасность гипервизора

Далее рассмотрено, как реализуется безопасность на уровне самого гипервизора и в целом на начальном уровне.

Защита памяти: привязка физической памяти к виртуальной машине

Каждая виртуальная машина использует только свою физическую область памяти. Виртуальные машины не могут совместно использовать одни и те же области памяти.

Гипервизор в любой момент времени может перераспределять права на чтение области памяти, изменять их или лишать прав доступа вовсе. Это сделано для использования технологии динамического распределения памяти.

Защита системы ввода-вывода

Основная ОС имеет возможность настройки правил доступа к устройствам ввода/вывода для виртуальных машин. Это позволит ограничивать доступ к тем или иным устройствам ввода/вывода посредством применения политик.

Реализация механизма защиты доступа к гипервызовам

Гипервизор не дает использовать привилегированные инструкции процессора.

Тесная интеграция с Authorization Manager

Система позволяет настроить ролевое управление виртуальными машинами.

Разграничение прав на группы виртуальных машин

Позволено устанавливать явно заданные права на виртуальные машины, запуск, остановку, создание, подключение образов.

Защита общих ресурсов

Доступ ко всем ресурсам Hyper-V предоставляется только на чтение. Например, нельзя подключить образ к нескольким виртуальным машинам и произвести изменения с любой из них.

SID виртуальной машины

С появлением механизма виртуализации Hyper-V в составе Windows Server 2008 встал вопрос об изоляции файлов и памяти одной виртуальной машины от других. Очевидно, что все виртуальные машины работают в контексте службы Hyper-V Virtual Machine Management в рамках процесса Virtual Machine Worker Process (vmwp.exe). Так как же давать раздельные права объектам, работающим внутри одной службы?

Для этого введено понятие SID виртуальной машины. Если взглянуть на ACL файлов ВМ, то виден SID вида NT VIRTUAL, который используется для

изоляции процесса работы одной виртуальной машины от другой. Полностью изолируется возможность доступа к файлам, дискам, памяти одной виртуальной машины к другой.

Рис. 12. SID виртуальной машины.

Установка роли Hyper-V в ОС Windows Server 2008 в варианте установки Server Core

Требуется использовать оборудование, протестированное для работы с Hyper-V. Ознакомиться со списком оборудования можно на сайте Microsoft в разделе Windows Server catalog.

Требования к оборудованию для развертывания роли Hyper-V

Процессор с 64-разрядной архитектурой. Сервер Hyper-V доступен в 64-разрядных версиях Windows Server 2008 R2, а именно в 64-разрядных версиях Windows Server 2008/R2 Standard, Windows Server 2008/R2 Enterprise и Windows Server 2008/R2 Datacenter. Роль Hyper-V недоступна для 32-разрядных версий (версий x86) Windows Server 2008/R2. Также эта роль недоступна для серверов на базе процессоров Itanium. Однако средства управления Hyper-V доступны для 32-разрядных версий ОС.

Аппаратная поддержка виртуализации. Эта возможность доступна в процессорах с поддержкой виртуализации, а именно в процессорах, построенных с использованием технологии виртуализации Intel (Intel VT) или технологии виртуализации AMD (AMD-V).

Аппаратно реализуемое предотвращение выполнения данных (Data Execution Prevention, DEP) должно присутствовать и быть задействовано. В частности, необходимо выставить разряд Intel XD (разряд отключения исполнения) или разряд AMD NX (разряд запрета исполнения).

При установке:

- Для роли Hyper-V использовать сервер, установленный в режиме Server Core;
- Перед установкой роли Hyper-V установить все необходимые обновления на сервер, используя соответствующие команды, после установки обновлений перезагрузить сервер;
- Перед установкой роли Hyper-V убедиться, что на оборудовании активированы соответствующие опции для поддержки виртуализации;

- После установки роли Hyper-V проверить системные журналы на предмет ошибок;
- После установки роли Hyper-V проверить наличие обновлений для Hyper-V и установить их.

Для управления средой Hyper-V использовать последние версии инструментов управления для Windows Vista/Windows 7 или Windows 2008 Server, которые позволяют в полной мере управлять сервером Hyper-V через графический интерфейс.

Конфигурация сетевых интерфейсов

Правильная конфигурация сетевых интерфейсов значительно повышает общий уровень безопасности узлов Hyper-V. Microsoft рекомендует использовать как минимум два сетевых адаптера на узле Hyper-V. Для операционной системы сервера виртуализации используется выделенный сетевой адаптер. По умолчанию для управляющей операционной системы виртуальная сеть не настраивается. Для управления сервером, где выполняется Hyper-V, используется выделенный сетевой адаптер, его надо подключить к доверенной подсети и изолировать от всех остальных подсетей.

Не использовать этот сетевой адаптер для работы виртуальных машин. Для работы сети виртуальных машин использовать один или несколько различных выделенных сетевых адаптеров. Это позволяет применять разные уровни политик безопасности сети и конфигурации виртуальных машин.

Например, можно настроить сеть таким образом, что доступ к сети для виртуальных машин будет отличаться от доступа к сети для управляющей операционной системы, включая использование виртуальных локальных сетей, IP-безопасность (IPSec), защиту доступа к сети (NAP).

Перед настройкой виртуальной сети необходимо определить структуру и тип виртуальной сети, которую планируется использовать. Следует иметь в виду, что Hyper-V не поддерживает беспроводные сети.

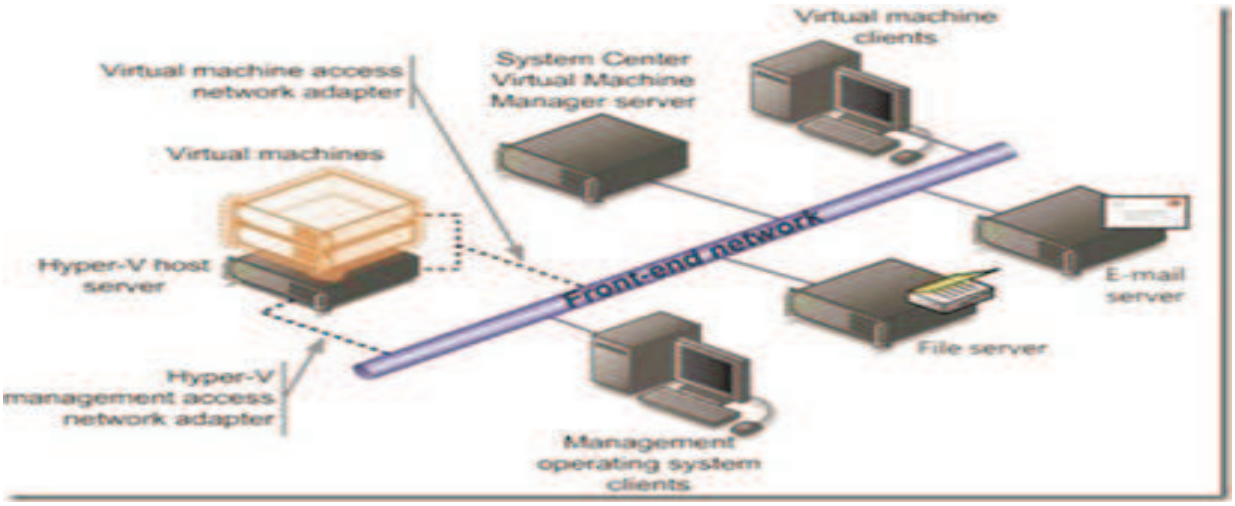

Рис. 13. Сетевые подключения.

Вторая рекомендация: после настройки роли Hyper-V правильно конфигурировать виртуальные коммутаторы. Можно подключать виртуальные сетевые адаптеры к нужным подсетям посредством виртуальных сетевых коммутаторов.

Типы виртуальных сетей

Виртуальные сети можно создать на компьютере под управлением Hyper-V. Это позволит определить различные топологии сети для виртуальных машин и сервера виртуализации. Используя диспетчер виртуальной сети (доступный из диспетчера Hyper-V), можно настраивать три различных типа виртуальных сетей.

Внешние (External) виртуальные сети. Этот тип сетей используется, если нужно, чтобы виртуальные машины могли взаимодействовать с внешними серверами и управляющей операционной системой (иногда называемой родительским разделом). Этот тип также позволяет виртуальным машинам на одном физическом сервере взаимодействовать друг с другом.

Внутренние (Internal) виртуальные сети. Этот тип сетей используется, если нужно разрешить взаимодействие между виртуальными машинами на одном физическом сервере и взаимодействие виртуальных машин с управляющей операционной системой. Внутренняя виртуальная сеть не привязана к физическому сетевому адаптеру. Она обычно используется для построения тестовой среды, в которой необходимо подключение к виртуальным машинам из управляющей операционной системы.

Частные (Private) виртуальные сети. Этот тип сетей используется, если нужно разрешить взаимодействие только между виртуальными машинами на одном физическом сервере. Частной виртуальной сети не требуется виртуальный сетевой адаптер в управляющей операционной системе. Частные виртуальные сети обычно используются, если нужно изолировать виртуальные машины от сетевого трафика в управляющей операционной системе и во внешних сетях.

Пример конфигурации для среды многоуровневых Web-приложений

Например, инфраструктура, которая включает в себя:

- базу данных;
- сервер приложений;
- web-сервер.

В приведенном примере сервер с установленной ролью Hyper-V имеет два физических сетевых интерфейса (рис.14).

Первый сетевой интерфейс подключается к сети управления и полностью изолирован от других сетей. Он используется для управления узлом Hyper-V с рабочего места администратора. Второй сетевой адаптер подключен к общедоступной сети (сеть отмечена на рисунке «Front-end network»).

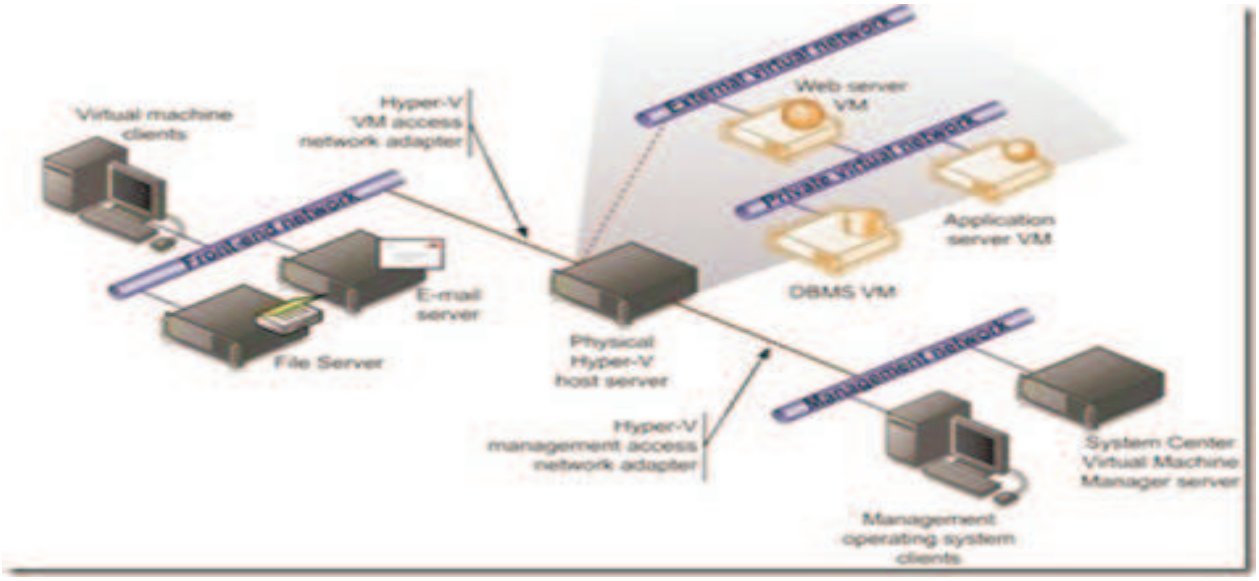

Рис. 14. Пример конфигурации для среды многоуровневых web-приложений.

К этой же сети подключены серверы и клиенты. Виртуальная машина с веб-сервером подключена к общедоступной сети через внешнюю виртуальную сеть External. Дополнительно в данной конфигурации существует частная виртуальная сеть Private (отмечена на рисунке, как «Private Virtual Network»), посредством которой web-сервер подключен к виртуальной машине с установленной базой данных и виртуальной машиной с установленным сервером приложений.

Такая конфигурация позволяет изолировать весь трафик между web-сервером и другими виртуальными машинами от внешней сети, а также обеспечивает выделенный изолированный сетевой интерфейс для управления узлом Hyper-V.

Такое разделение сетей обеспечивает защиту виртуальной сети от внешних атак, однако это решение не допускает прослушивание трафика средствами NIDS (инструменты обнаружения вторжений, если они используются), подключенных к внешней сети. Для контроля трафика в виртуальном сегменте потребуется развернуть дополнительные инструменты обнаружения вторжений в нем, если таковые потребуются.

Конфигурация местоположения файлов виртуальных машин

Файлы, содержащие информацию о конфигурации виртуальных машин, по умолчанию располагаются в папке:

%programdata%\Microsoft\Windows\Hyper-V

Файлы конфигурации не занимают много места; теоретически местоположение по умолчанию может быть приемлемым для любых сценариев работы узлов Hyper-V.

Однако если решено переместить эти файлы на другой ресурс, важно, чтобы у системной учетной записи и группы администраторов имелись полные права на этот ресурс. Остальным учетным записям доступ должен быть строго ограничен в соответствии с политикой безопасности.

Также следует помнить, что виртуальные диски могут быть, как фиксированного размера (Fixed), так и динамически расширяться (Dynamic). Microsoft рекомендует использовать фиксированные размеры дисков виртуальных машин для большей производительности и исключения ситуации, когда место на физических носителях может неожиданно закончиться.

По умолчанию все файлы VHD храниться в папке **%users %\Public\Documents\Hyper-V\.** Можно изменить местоположение на то, которое необходимо.

Таблица 6 - Разрешения папки (хранилище VHD).

Имена	**Разрешения**	**Применимо**
Administrators	Full Control	К текущей папке, подпапкам и файлам
System		
Creator Owner	Full Control	Только к подпапкам и файлам
Interactive	Create files/write data	К текущей папке, подпапкам и файлам
Service		
Batch	Create folders/append data	
	Delete	
	Delete subfolders and files	
	Read attributes	
	Read extended attributes	
	Read permissions	
	Write attributes	
	Write extended attributes	

Для упрощения работы и делегирования полномочий рекомендуется создать удобную структуру папок (например, типичная структура могла бы быть следующей):

- W:\Virtualization Resources\Virtual Machines
- W:\Virtualization Resources\Virtual Hard Disks
- W:\Virtualization Resources\Virtual Floppy Disks
- W:\Virtualization Resources\ISO files

Разрешения, которые необходимо установить на хранилище VHD-файлов в случае, если его переместили предложены в таблице 3.

В стандартной конфигурации для упрощения администрирования рекомендуется хранить все файлы образов VFD и ISO на том же самом логическом диске, что и файлы VHD.

Не надо запускать приложения в управляющей операционной системе – все приложения должны выполняться в виртуальных машинах. Если все же необходимо использовать программы на управляющей операционной системе, необходимо запустить в ней антивирусное программное обеспечение и добавить в исключения антивирусной программы следующие ресурсы:

- Каталог файлов конфигурации виртуальных машин.
- Каталог файлов виртуальных жестких дисков виртуальных машин.
- Каталог файлов моментальных снимков.

Дополнительно рекомендуется ознакомиться с документом Windows Server 2008 Security Guide. В данный документ входит ряд рекомендаций по установке значений безопасности для достижения оптимального уровня безопасности. Microsoft рекомендует применять базовые настройки безопасности, описанные в документе Windows Server 2008 Security Guide и Windows Server 2008 Security Compliance Management Toolkit для серверов Windows Server 2008, выполняющих роль Hyper-V.

Управление хост-сервером и администрирование виртуальных машин

Не надо предоставлять администраторам виртуальных машин разрешения в управляющей операционной системе. Согласно принципу предоставления наименьших привилегий, администраторам виртуальных машин (иногда называемым администраторами отделов или делегированными администраторами) необходимо предоставлять минимально необходимые разрешения. Управление требуемыми разрешениями на всех объектах, связанных с виртуальной машиной, может быть сложным и при неверном использовании может привести к проблемам безопасности.

Безопасность хост-сервера с установленной ролью Hyper-V

Когда на одном или нескольких серверах Hyper-V развертываются несколько десятков виртуальных машин, появляется необходимость правильно разграничить права доступа между пользователями. Настроить необходимые разрешения на создание, управление, удаление и конфигурацию виртуальных машин.

Рекомендуется использовать управление доступом на основе ролей, которое дает возможность задавать управление доступом в терминах организационной структуры компании, то есть путем создания нового объекта, называемого ролью. Пользователям назначаются роли для выполнения своих должностных

обязанностей. Hyper-V использует политики диспетчера авторизации для управления доступом на основе ролей.

Для стандартной небольшой инфраструктуры рекомендуется разделять полномочия администраторов по следующему типу:

Администраторы Hyper-V – административные учетные записи, у которых есть полный административный доступ ко всем ресурсам Hyper-V, включая конфигурации виртуальных машин. Администраторы Hyper-V осуществляют глобальные настройки конфигурации, которые затрагивают, как саму операционную систему управления, так и все виртуальные машины на узлах Hyper-V.

Администраторы виртуальных машин – это административные учетные записи, обладающие административным доступом к виртуальным машинам, для которых сопоставлены те или иные виртуальные машины и области. Архитектура Hyper-V позволяет создать схему, при которой администраторы виртуальных машин не могут управлять основной операционной системой.

Рекомендуется использовать учетную запись с правом администратора Hyper-V только в тех случаях, когда это необходимо.

Следует помнить, что по умолчанию администраторы виртуальных машин не могут выполнять локальный вход на хост Hyper-V и изменять какие-либо настройки ОС.

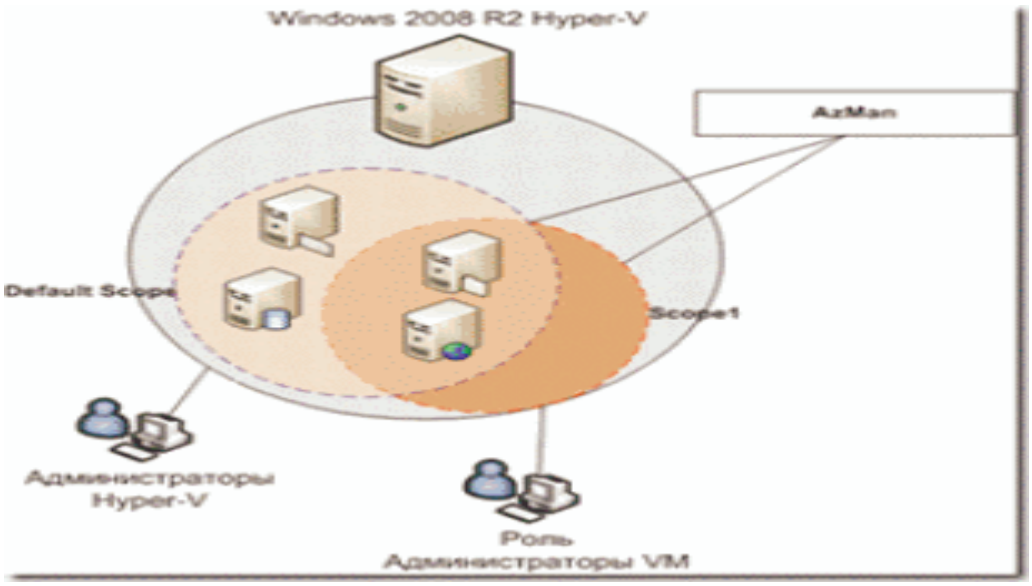

Рис. 15. Делегирование управления VM.

Обычно такая конфигурация является приемлемой, однако может возникнуть ситуация, когда потребуется более тонко разграничить права доступа к управлению виртуальными машинами. Для этого рассмотрены инструменты делегирования виртуальных машин (рис.15). Интерфейс консоли управления Hyper-V позволяет полностью управлять виртуальными машинами на хосте Hyper-V. По умолчанию все учетные записи, включенные в группу локальных администраторов, могут управлять виртуальными машинами на этом узле. Консоль управления Hyper-V обеспечивает минимальный функционал для работы с

виртуальными машинами, и не позволяет в полной мере разграничивать права доступа, что может вызвать определенные трудности при администрировании.

Чтобы избежать их, существует ряд инструментов позволяющих в полной мере разграничивать права доступа между пользователями и администраторами. Примерами таких инструментов является Authorization Manager и System Center Virtual Machine Manager.

Использование Authorization Manager для делегирования управления VM

Для разграничения прав на операции с виртуальными машинами можно использовать приложение Authorization Manager, которое входит в состав ОС Windows 2008 Server.

Authorization Manager – это инструмент, позволяющий разграничивать права доступа на основе ролей, основанных на предоставлении необходимого функционала для каждой роли.

Authorization Manager позволяет размещать информацию в файле,в Active Directory или в базе данных. Поддерживает как 64-разрядные, так и 32-разрядные системы. По умолчанию Authorization Manager хранит свои данные в текстовом файле формата *xml* на локальном сервере.

Рассмотрим, какие компоненты существуют в Authorization Manager:

- Operation – Операция
- Task – Задача
- Role – Роль
- Scope – Область

Operation (Операция). Минимальное действие, которое можно совершить над объектом является операцией. Например, создание, включение, остановка виртуальной машины, изменение конфигурации.

Task (Задача). Операции группируются в задачи. Таким образом, получается группа операций, которые можно делегировать пользователю. В Authorization Manager уже есть сформированные задачи практически на все основные действия с виртуальными машинами; дополнительно существует возможность формировать свои задачи, если это необходимо.

Роль (Role). Определяет круг задач для учетной записи. Например, учетная запись может иметь право выполнять все операции и задачи, связанные с конфигурацией виртуальной сети. При необходимости такую роль можно создать и делегировать пользователю.

Область (Scope). Параметр, который позволяет указать какими виртуальными машинами может управлять определенная роль пользователя. По умолчанию при создании виртуальных машин они помещаются в область по умолчанию Default Scope. Если требуется предоставить административный доступ к определенным виртуальным машинам, то потребуется создать область, в которую необходимо поместить эти виртуальные машины, после чего применить настройки к данной области. Это можно реализовать специальным сценарием.

Пользователь, которому делегирована некая область управления, будет видеть только свои виртуальные машины, и не будет видеть, и иметь доступа к другим.

Если в организации более трех узлов Hyper-V, рекомендуется опубликовать хранилище Authorization Manager в Active Directory.

Использование System Center Virtual Machine Manager 2008 R2

В крупной инфраструктуре для управления виртуальными машинами и делегирования прав на виртуальные машины и хост-системы рекомендуется использовать System Center Virtual Machine Manager.

Ключевое достоинство System Center Virtual Machine Manager – тесная интеграция с другими решениями Microsoft для управления инфраструктурой Windows-серверов семейства System Center. System Center Virtual Machine Manager позволяет создать гибкую виртуальную инфраструктуру на основе платформы Hyper-V и упростить развертывание виртуальных систем из центральной библиотеки шаблонов. Основные возможности System Center Virtual Machine Manager включают в себя:

- использование базы данных Operations Manager 2007, в которой собраны данные о производительности физических серверов, и определение наиболее подходящих для виртуализации серверов;
- встроенные средства миграции (ранее для этих целей использовался Virtual Server Migration Toolkit), использующие службы теневого копирования тома для преобразования физических серверов в виртуальные, без их остановки. Кроме того, System Center Virtual Machine Manager позволяет преобразовать виртуальные машины VMware в формат Hyper-V;
- возможность автоматически перемещать виртуальные серверы на физических компьютерах, используя данные об их рабочих нагрузках;
- централизацию управления ресурсами, управление гипервизорами Hyper-V, Virtual Server, VMware ESX и др. Пакет позволяет увеличить доступность виртуальных машин с точки зрения их переноса в случае проблем с оборудованием и в случае большой нагрузки на оборудование. Он позволяет управлять ресурсами хост-сервера и ресурсами виртуальных машин;
- возможность создавать группы физических серверов Hyper-V и делегировать управление ими;
- создание библиотек, которые могут быть использованы для хранения виртуальных машин, образов и шаблонов;
- предоставление портала самообслуживания, который представляет собой web-приложение для самостоятельного развертывания виртуальных машин пользователями. Администратор определяет политики самообслуживания, которые включают в себя правила создания, развертывания и использования виртуальных систем. Взаимодействие портала с управляющим сервером производится по модели сервисно-ориентированных систем WCF (Windows Communication Foundation);

- создание пользовательских ролей, делегирование разрешений для групп хост-серверов, виртуальных машин и серверов библиотек.

Серверы Hyper-V могут быть объединены в группы, организованные по некоторым логическим категориям (например, «Тестовые машины», «Веб-порталы» и т.п.). Удобно организовать группы хостов в соответствии со структурой Active Directory. Естественно, System Center Virtual Machine Manager полностью поддерживает службу каталога Active Directory.

Использование групп хостов позволяет упростить управление виртуальными серверами и облегчить их мониторинг. Кроме того, группы хостов используются для назначения им определенных политик и свойств. Компания Microsoft рекомендует привязывать каждую группу хостов к одной библиотеке шаблонов, которую используют серверы этой группы.

Установка роли Hyper-V средствами графического интерфейса

Роль Hyper-V средствами графического интерфейса устанавливается при помощи «**Диспетчера сервера**». Для того чтобы установить эту роль на Windows Server 2008/2008 R2, выполнить следующие действия:

1. Открыть консоль **«Диспетчер сервера»**. Если после загрузки операционной системы окно диспетчера сервера не открылось, в меню **«Пуск»** открыть подменю **«Администрирование»**, а затем выбрать команду **«Диспетчер сервера»**; В окне консоли **«Диспетчер сервера»** нажать кнопку **«Добавить роли»** в разделе **«Сводка по ролям»**. Также можно в дереве консоли нажать правой кнопкой мыши на узле **«Роли»** и из контекстного меню выбирать команду **«Добавить роли»**;
2. Откроется диалоговое окно **«Мастер добавления ролей»**. На первой странице мастера можно узнать краткую информацию о назначении данного мастера. Если не хотите впредь видеть этот шаг, установите флажок на опции **«Пропустить эту страницу по умолчанию»**. Ознакомьтесь с информацией, приведенной на этом шаге, после чего нажмите кнопку **«Далее»**;
3. На странице **«Выбор ролей сервера»** предоставляется выбор ролей, которые будут установлены на сервере. Одновременно можно выбрать несколько ролей. В данном случае установить флажок на опции **«Hyper-V»**, ознакомиться с информацией, указанной в области **«Описание»** и нажать кнопку **«Далее»**.
4. На странице **«Hyper-V»** можно ознакомиться с технологией Hyper-V, перейдя по ссылкам в разделе **«Дополнительные сведения»**. Нажать кнопку **«Далее».**
5. На странице **«Создание виртуальных сетей»** выбрать необходимые сетевые интерфейсы из списка **«Сетевые платы»**, чтобы создать виртуальную сеть для взаимодействия виртуальных машин между собой и с ком-

пьютерами. После того как сетевые адаптеры будут выбраны, нажать на кнопку **«Далее»**;

6. На странице **«Подтверждение выбранных элементов для установки»** просмотреть сводную информацию и нажать кнопку **«Установить»**;
7. На странице **«Ход выполнения установки»** мастер добавления ролей предоставляет возможность следить за процессом установки выбранных ролей.
8. Для завершения установки роли Hyper-V, мастер добавления ролей проинформирует о том, что необходимо перезагрузить компьютер. Закрыть диалог **«Мастер добавления ролей»**, используя кнопку **«Закрыть»**.После того как вы нажмете на кнопку **«Закрыть»**, мастер предложит перезагрузить сервер самостоятельно. Нажав на кнопку **«Да»**, сервер будет автоматически перезагружен для завершения установки роли. Если же нужно до перезагрузки выполнить еще какие-то действия, нажать кнопку **«Нет»**, но тогда нужно будет перезагрузить сервер вручную.
9. Во время перезагрузки сервера роль Hyper-V устанавливается подобно обычным системным обновлениям. Для полного завершения установки, войти в систему с той же учетной записью, при помощи которой устанавливали данную роль. Последний раз откроется мастер добавления ролей со страницей **«Результаты установки»**, где можно увидеть, нормально ли прошла установка роли. Нажать кнопку **«Закрыть»**.

Установка роли Hyper-V средствами командной строки

В операционных системах Windows Server 2008/2008 R2 роль Hyper-V можно устанавливать как для полных версий, так и для систем, установленных в режиме ядра, или в режиме минимальной конфигурации. Установка системы в режиме ядра занимает около трех гигабайт на жестком диске и потребляет менее чем 256 Мбайт оперативной памяти, а также обеспечивает только ограниченное количество серверных ролей и возможностей их администрирования, понижая области уязвимости.

Из общего количества существующих ролей, в редакции системы в режиме ядра, доступны только следующие девять: «Доменные службы Active Directory», «Службы Active Directory облегченного доступа к каталогам», «DHCP-сервер», «DNS-сервер», «Файловые службы», «Сервер печати», «Сервер потокового мультимедиа», «Веб-сервер (IIS)», а также «Hyper-V».

Средство управления конфигурацией сервера в командной строке, аналогичное диспетчеру сервера – ***ServerManagerCmd***. При помощи данной утилиты можно не только добавлять и удалять роли и компоненты серверных операционных систем Windows, но и просматривать конфигурацию и состояние установленных на сервере ролей и компонентов.

Для установки роли Hyper-V операционной системы в режиме ядра или полной установки при помощи утилиты командной строки ***ServerManagerCmd*** выполнить следующие действия:

1. Войти в систему под учетной записью администратора и открыть командную строку (в случае с системой в режиме ядра достаточно только войти в систему);
2. В командной строке ввести:
   ServerManagerCmd –install Hyper-V –resultPath c:result.xml
   где:

   -install – параметр, при помощи которого можно указать роль, службу роли или компонент, которые необходимо установить;

   -resultPath – параметр, при помощи которого можно сохранить результат выполнения команды в xml файл.

3. После завершения установки нужно перезагрузить сервер. Для этого выполнить команду: ***shutdown –r –t 0***.

Вопросы для самоподготовки

1. Каковы задачи администрирования сети?
2. Какие требования предъявляются к оборудованию при установке ОС MS Windows Server® 2008 R2?
3. Описать процесс установки ОС MS Windows Server® 2008 R2.
4. В чем состоит базовая настройка сервера?
5. Каковы серверные функции ОС MS Windows Server® 2008 R2?
6. Каково назначение службы Active Directory® MS Windows Server® 2008 R2?
7. Описать установку службы Active Directory®.
8. Учетные записи пользователей и их назначение.
9. Учетные записи групп и их назначение.
10. В чем состоит настройка программной среды для определенного пользователя.
11. Профили пользователей и их назначение.
12. Что такое общий доступ к файлам и каталогам?
13. Назвать разрешения для общего доступа к файлам и каталогам.
14. Назвать стандартные разрешения NTFS для файлов и каталогов.
15. Каковы политики безопасности?
16. Назвать политики учетных записей.
17. Что такое политика аудита?
18. Каково назначение политик проводной сети?
19. Каково назначение политик беспроводной сети?
20. Назначение и процесс резервного копирования и восстановления системы.
21. Серверная роль DHCP-сервера и ее назначение.
22. Описать Службы для сетевой файловой системы: возможности и компоненты..

23. Описать типы виртуализации.
24. Гипервизор и его назначение.
25. В чем состоит безопасность гипервизора?
26. Описать установки роли Hyper-V®.

Литература

1. Windows Server 2008 R2, Полное руководство. Авторы: Рэнд Моримото, Майкл Ноэл, Омар Драуби, Росс Мистри, Крис Амарис, Редактор: Гай Ярдени, Издательство: Вильямс, ISBN 978-5-8459-1653-2, 978-0-672-33092-6; 2011 г. 1456 стр.
2. http://www.oszone.net/
3. technet.microsoft.com›ru-ru/library/.aspx
4. http://ru.wikipedia.org/wiki .

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 R2

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