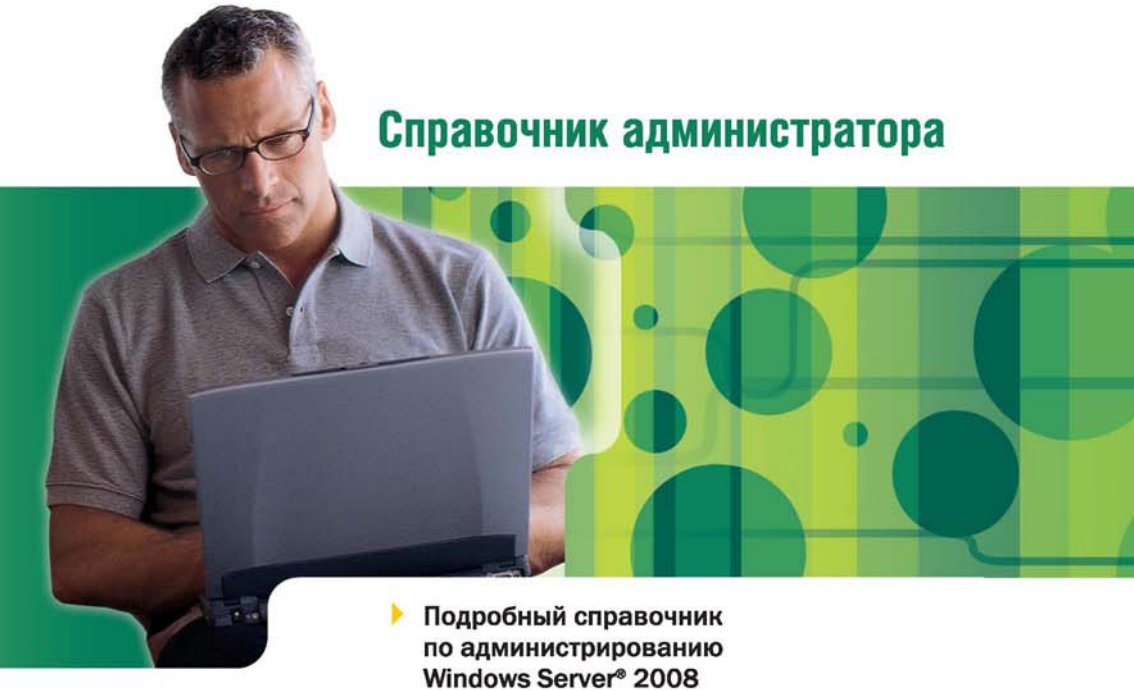
Уильям Р. Станек

Windows Server® 2008

Справочник администратора



- Подробный справочник по администрированию Windows Server® 2008
- Таблицы, пошаговые инструкции, списки параметров

IT Professional

РУССКАЯ РЕДАКЦИЯ Microsoft bhv®

William R. Stanek

Windows Server® 2008

Administrator's Pocket Consultant

Microsoft® Press

Уильям Р. Станек

Windows Server® 2008

Справочник администратора

РУССКАЯ РЕДАКЦИЯ

bhv®

2008

УДК 681.3.06
ББК 32.973.26–018.2
С76

Станек Уильям Р.

С76 Windows Server 2008. Справочник администратора / Пер. с англ. — М. : Издательство «Русская редакция» ; СПб. : БХВ-Петербург, 2008. — 688 стр. : ил.

ISBN 978-5-7502-0370-3 («Русская редакция»)
ISBN 978-5-9775-0009-8 («БХВ-Петербург»)

Данная книга — краткий исчерпывающий справочник по администрированию новейшей серверной операционной системы Windows Server 2008. В ней содержится описание архитектуры системы, сведения по ее установке и развертыванию, а также информация о различных ролях и компонентах сервера. Подробно рассказывается об управлении сервером Windows Server 2008, о мониторинге процессов и событий, об использовании групповой политики. Ряд глав посвящен различным аспектам работы с Active Directory — ее администрированию, работе с учетными записями пользователей, групп и компьютеров. Приводятся сведения о настройке и администрировании различных серверов: файлового сервера, сервера печати, DHCP-сервера и DNS-сервера. Особое внимание уделено вопросам производительности системы, безопасности данных, а также их архивации и восстановлению.

Книга состоит из 20 глав, хорошо иллюстрирована и предназначена для администраторов и ИТ-специалистов общего профиля.

УДК 681.3.06
ББК 32.973.26–018.2

РУССКАЯ РЕДАКЦИЯ bhv®

Уильям Р. Станек

Windows Server 2008.
Справочник администратора

Совместный проект издательства «Русская Редакция» и издательства «БХВ-Петербург»

Оглавление

Благодарности

Писать эту книгу было интересно, но нелегко. Когда я приступал к работе над ней, моей первой целью было определить, чем отличаются Windows Server 2003 и Windows Server 2008 и какие новые возможности администрирования появились в Windows Server 2008. Для этого мне пришлось провести серьезную исследовательскую работу и изрядно углубиться во внутреннее устройство ОС. К счастью, я уже написал несколько книг о Windows Vista и ее новых функциях, так что отправная точка для исследования у меня имелась, но не более того.

Едва познакомившись с Windows Server 2008, вы сразу же увидите, что эта операционная система отличается от предыдущих версий Windows Server. Однако полностью оценить эти отличия при первом знакомстве вам не удастся — поскольку наиболее важные отличия скрыты в глубине ОС. Изменился не только интерфейс. Переработана сама архитектура, и именно поэтому мое исследование оказалось столь непростым.

Справочники серии Pocket Consultants (Справочник администратора) должны быть компактными и понятными. Книги такого сорта призваны помочь вам в оперативном решении проблем там, где эти проблемы вас настигли. Мне пришлось немало поработать, чтобы не выйти за рамки описания ключевых аспектов администрирования Windows Server 2008. Результат вы держите в руках. Надеюсь вы согласитесь, что это один из лучших справочников по Windows Server 2008.

Мне приятно, что в эту книгу попали приемы и методики, которые я на протяжении многих лет применял для решения различных проблем, — теперь они помогут и вам. Но человек — не остров, и эта книга не была бы написана без помощи многих замечательных людей. Во многих своих книгах, изданных в Microsoft Press, я уже писал, что команда Microsoft Press — вне всякой конкуренции. На протяжении всей работы над книгой Карен Салл (Karen Szall) и Дениз Банкайтис (Denise Bankaitis) помогали мне не выйти из графика и снабжали меня всем, необходимым для написания книги. Они руководили процессом редактирования, как профессионалы высочайшего уровня. Я благодарен Мартину Дель-Ре (Martin DelRe) за то, что он верил в мою работу и все это время присматривал за мной.

К несчастью для автора (но к счастью для читателя), процесс публикации книги не ограничивается ее написанием. Затем наступает этап редактирования. Не могу не признать, что в Microsoft Press к редактированию подходят с такой тщательностью, которой я не видел нигде, а я опубликовал множество книг во многих издательствах. Хочу особо упомянуть технического обозревателя Рэндалла Гэлоуэя (Randall Galloway), менеджера проекта Кертиса Филипса (Curtis Philips), редактора Бека Маккей (Becka McKay) и корректора Андреа Фокс (Andrea Fox).

Введение

Знакомьтесь — *Справочник администратора Windows Server 2008*. Я начал профессионально писать о компьютерах в 1994 году и написал с тех пор больше 65 книг. На протяжении этих лет мне приходилось писать о различных серверных технологиях и продуктах, но Windows Server, бесспорно относится к числу моих фаворитов. Windows Server 2008 буквально во всем отличается от предыдущих версий Windows Server. Начнем с того, что многие ключевые компоненты Windows Server основаны на той же программной базе, что и Windows Vista. Это означает, что к Windows Server 2008 применимы почти все ваши познания о Windows Vista. Это хорошо, но есть и плохие новости: практически все остальное в Windows Server 2008 так или иначе изменилось.

Поскольку я написал уже немало книг о Windows Server, у меня выработался особый взгляд на предмет — тот взгляд, что появляется только после многолетней работы с какой-либо технологией. Задолго до появления продукта с именем Windows Server 2008 я работал с его бета-версией, а еще до этого я работал с альфа-версией продукта, о существовании которого за пределами Майкрософт мало кто знал. Иными словами, я следил за развитием Windows Server 2008 с самого-самого начала и до тех пор, когда система превратилась в законченный продукт, доступный сегодня.

Вы, вероятно, заметили, что информации о Windows Server 2008 более чем достаточно — как в Интернете, так в других печатных книгах. К вашим услугам учебники, справочники, дискуссионные группы — все для того, чтобы облегчить вам работу с Windows Server 2008. Однако, у этой книги есть одно важное преимущество — вся информация, необходимая для изучения Windows Server 2008, собрана под одной обложкой и изложена понятно и упорядоченно. В этой книге есть все сведения необходимые для настройки Windows Server 2008 и обслуживания серверов Windows Server 2008.

В этой книге я рассказал о том, как работают компоненты системы, почему они работают именно так, а не иначе, как настроить их согласно вашим потребностям. Я также привожу конкретные примеры использования компонентов, как с их помощью разрешать возникающие проблемы. Кроме того, в книге вы найдете советы, рекомендации, примеры оптимизации Windows Server 2008. И это не просто учебник по настройке Windows Server 2008. Вы узнаете, как извлечь из системы максимум пользы и как заставить компоненты и функции Windows Server 2008 работать «на полную катушку».

В отличие от большинства других книг на ту же тему, это издание не ориентировано на читателей с определенным уровнем подготовки. Конечно, это не облегченный текст для начинающих. Но большая часть содержания книги будет полезна как администраторам-новичкам, так и опытным профессионалам.

Кому адресована книга

Справочник администратора Windows Server 2008 в равной степени относится ко всем версиям Windows Server 2008 — Standard, Enterprise, Web и Datacenter. Основная аудитория книги такова:

- администраторы систем Windows;
- опытные пользователи, частично выполняющие обязанности администраторов;
- администраторы, переходящие на Windows Server с предыдущих версий;
- администраторы, переходящие на Windows Server с других платформ.

Чтобы поместить в книгу как можно больше информации, я предполагаю, что у вас имеются навыки по работе в сети и общее знакомство с Windows Server. Поэтому в книге нет глав с описанием архитектуры и преимуществ Windows Server, запуска и завершения работы системы. Я предпочел отвести больше места настройке сервера Windows, групповым политикам, безопасности, аудиту, архивации данных, восстановлению системы и пр.

Я также предполагаю, что вы хорошо знакомы с командами и пользовательским интерфейсом Windows. Если вам требуется знакомство с основами Windows, вы можете почерпнуть его из других ресурсов (в том числе, в других книгах Microsoft Press).

Структура книги

Москва не сразу строилась, и книгу эту вы одолеете не в одночасье. Я не предлагаю вам проглотить ее за день, неделю или даже за месяц. В идеале вы будете читать эту книгу по мере надобности, понемногу каждый день и ровно столько, сколько нужно для знакомства с очередным компонентом Windows Server 2008. Книга разделена на 20 глав, расположенных в логическом порядке — от раннего планирования и развертывания до настройки и обслуживания.

Книга снабжена подробным оглавлением и предметным указателем, которые помогут вам найти нужную информацию. В текст включены многие компоненты, типичные для справочника: пошаговые инструкции, списки, таблицы и перекрестные ссылки.

Как и другие книги серии, *Справочник администратора Windows Server 2008* призван стать простым и полным руководством по управлению серверами Windows. Надеюсь, он станет вашей настольной книгой. В книге описано все необходимое для выполнения основных административных функций

на сервере Windows. Поскольку главной целью при написании книги были компактность и полнота, вам не придется продираться через сотни страниц лишней информации, чтобы найти интересующие вас сведения. Вы найдете именно ту информацию, которая необходима для оперативного решения возникшей проблемы.

Говоря коротко, я надеюсь, что эта книга станет для вас единым ресурсом, к которому вы будете обращаться с любыми вопросами об администрировании Windows Server. Поэтому книга посвящена повседневным административным процедурам, типичным задачам, конкретным примерам и чаще всего используемым параметрам. Я стремился сделать книгу краткой, простой, но вместе с тем максимально информативной.

Соглашения, принятые в книге

Чтобы текстом было проще пользоваться, я включил в него некоторые специфические элементы оформления. Примеры кодов и команд даны моноширинным шрифтом. Строки и команды, которые вы должны вводить с клавиатуры, отмечены **полужирным** шрифтом. Новые термины выделяются *курсивом*.

Примечание Размещение параметров групповых политик в Windows Server 2008 претерпело значительные изменения. В узлах **Конфигурация компьютера (Computer Configuration)** и **Конфигурация пользователя (User Configuration)** появились два новых узла: **Политики (Policies)** и **Настройка (Preferences)**. В первом собраны общие политики, во втором — общие параметры. Обращаясь к узлам редактора групповых политик, я буду пропускать имена этих узлов, то есть, вместо Конфигурация пользователя\Политики\Административные шаблоны: Определения политик\Компоненты Windows (User Configuration\Policies\Administrative Templates: Policy Definitions\Windows Components) я буду по-прежнему писать Конфигурация пользователя\Административные шаблоны\Компоненты Windows (User Configuration\Administrative Templates\Windows Components).

В книге использованы следующие виды примечаний:

Примечание	Дополнительные сведения по конкретной теме, которые необходимо особо подчеркнуть
Безопасность	Указание на аспекты, связанные с безопасностью
Совет	Полезная рекомендация или дополнительные сведения
Внимание!	Предупреждение о возможной проблеме
Ближе к реальности	Примеры реального приложения обсуждаемых вопросов и методик

Я искренне надеюсь, что в *Справочнике администратора Windows Server 2008* вы оперативно и эффективно найдете все необходимое для выполнения основных административных функций на серверах Windows. Жду ваших комментариев по адресу *williamstanek@aol.com*. Спасибо.

Другие ресурсы

Не существует волшебной палочки, по мановению которой вы в миг узнали бы все, что вам нужно знать о Windows Server 2008. Хотя в некоторых книгах утверждается, что они являют собой всеохватывающий источник информации, нельзя объять необъятное в одной книге. Я надеюсь, что вы будете пользоваться этой книгой именно так, как ею надлежит пользоваться. Помните: девиз этой книги — информативность и легкость. В ней приведены все сведения, необходимые для выполнения основных административных задач на серверах Windows, но она ни в коей мере не является исчерпывающей.

Ключом к успеху в изучении этой книги, другой книги или любого ресурса Windows будет ваше трудолюбие. Познакомившись с новой темой, не пожалейте времени и постарайтесь на практике закрепить то, что вы узнали. При необходимости ищите более подробную информацию.

Всем своим читателям я рекомендую регулярно заходить на веб-сайт Майкрософт, посвященный Windows Server (*http://www.microsoft.com/windowsserver/*), и на сайт службы поддержки Майкрософт (*http://support.microsoft.com*) , чтобы быть в курсе последних изменений. Загляните также на мой веб-сайт (*http://www.williamstanek.com/windows*). Там вы найдете информацию о Windows Server 2008, обновления к книге и свежую информацию о Windows Server 2008.

Поддержка

Мы приложили значительные усилия, чтобы сделать содержание этой книги максимально точным. Список поправок (если таковой имеется) вы найдете по адресу: *http:/www.microsoft.com/mspress/support*.

Если у вас возникнут вопросы или комментарии по поводу этой книги, обращайтесь в Microsoft Press по следующим адресам:

Обычная почта:
Microsoft Press
Attn: *Windows Server 2008 Administrator's Pocket Consultant* Editor
One Microsoft Way
Redmond, WA 98052-6399

Электронная почта:
mspinput@microsoft.com

Имейте в виду, что эти адреса *не предназначены* для поддержки программных продуктов. За информацией о поддержке обращайтесь на веб-узел Майкрософт по адресу *http://www.microsoft.com/support*.

Часть I

Основы администрирования Windows Server 2008

Глава 1

Обзор администрирования Windows Server 2008

Windows Server 2008 — мощная, гибкая, полнофункциональная серверная операционная система (ОС), в основе которой лежат усовершенствования, впервые появившиеся в Windows Server 2003 SP1 и Windows Server 2003 Release 2. ОС Windows Server 2008 имеет несколько общих компонентов с Windows Vista, поскольку обе ОС созданы в рамках одного проекта. Эти компоненты связаны общей программной основой и охватывают многие аспекты действия ОС, включая управление, обеспечение безопасности, работу с сетью и хранение информации. Таким образом, при работе с Windows Server 2008 найдет себе применение значительная часть ваших познаний о Windows Vista.

В этой главе описаны основы работы с Windows Server 2008, а также показано, насколько изменения в архитектуре повлияли на приемы работы с системой и управление ею. В этой и других главах вам также будут предложены детальные описания изменений в системе безопасности, включая физическую защиту, защиту информации и безопасность работы в сети. Хотя эта книга, в основном, посвящена администрированию Windows Server 2008, рекомендации и методики, обсуждаемые в тексте, будут полезны специалистам, которые осуществляют поддержку системы, разрабатывают для нее приложения или просто с ней работают.

Windows Server 2008 и Windows Vista

Операционная система Windows Server 2008, как и Windows Vista, обладает принципиально новой архитектурой со следующими основными особенностями:

- **Модули, обеспечивающие независимость от языка, и образы дисков, обеспечивающие аппаратную независимость** Каждый компонент системы представляет собой независимый модуль, который легко добавить или удалить. Эта функциональность составляет основу новой архитектуры Windows Server 2008. ОС распространяется на носителях в виде об-

разов WIM (Windows Imaging Format), в которых применяется сжатие и хранение в одном экземпляре, что позволяет значительно сократить размер файлов.

- **Предустановочная и предзагрузочная среда** В качестве предустановочной среды на смену MS-DOS пришла среда Windows PE 2.0 (Windows Preinstallation Environment 2.0), обеспечивающая установку, развертывание, восстановление или устранение неисправностей ОС. Предзагрузочная среда Windows Pre-Boot Environment обеспечивает работу диспетчера загрузки, который позволяет выбрать для запуска ОС подходящее загрузочное приложение. В загрузочной среде на системах с несколькими ОС доступ к версиям Windows, предшествующим Windows Vista, открывает элемент для устаревших ОС.
- **Управление учетными записями и повышение полномочий** Управление учетными записями (User Account Control, UAC) повышает безопасность компьютера, обеспечивая подлинное разделение записей обычных пользователей и администраторов. Благодаря UAC все приложения в ходе работы используют либо полномочия обычного пользователя, либо полномочия администратора. Каждый раз, когда запускается приложение, требующее администраторских прав, вы (по умолчанию) получаете от системы безопасности запрос на повышение полномочий. Способ работы сообщений системы безопасности зависит от настроек групповых политик. Если вы вошли в систему, используя встроенную учетную запись администратора, запросов службы безопасности на повышение полномочий вы, скорее всего, не увидите.

Компоненты Windows Vista и Windows 2008 Server с общей программной базой также обладают одинаковыми управляющими интерфейсами. По сути, почти каждая утилита панели управления Windows 2008 Server совпадает или почти совпадает с аналогичной утилитой в Windows Vista. Конечно, есть и исключения. Поскольку в Windows 2008 Server не используются индексы производительности, у серверов под управлением этой ОС нет оценки Windows Experience Index. Поскольку в Windows Server 2008 не используется спящий режим и другие подобные состояния, серверы под ее управлением не обладают функциями сна, гибернации или пробуждения. Обычно на серверах Windows не нужны функции управления питанием, поэтому в Windows 2008 Server есть лишь ограниченный набор параметров электропитания. Кроме того, в Windows 2008 Server нет усовершенствований Windows Aero (Aero Glass, Flip, 3D Flip и т.д.), боковой панели Windows, мини-приложений Windows и прочих улучшений, касающихся внешнего вида. Это связано с необходимостью обеспечить оптимальную производительность системы.

Поскольку у компонентов Windows Vista и Windows Server 2008 много общего, я не буду тратить время на описание изменений в интерфейсе по сравнению с предыдущими версиями системы, обсуждение UAC и пр. Исчерпывающую информацию по этим вопросам вы найдете в книге *Microsoft Windows Vista. Справочник администратора (Русская Редакция, БХВ-*

Петербург, 2008), которую я всячески рекомендую использовать параллельно с этой книгой. Помимо общих задач администрирования в упомянутой книге рассматриваются настройка ОС и рабочей среды Windows, конфигурация оборудования и сетевых устройств, управление правами доступа пользователей и глобальными параметрами, настройка ноутбуков, работа в сети с мобильными устройствами, использование удаленного управления и удаленной помощи, решение системных проблем и многое другое. В этой книге мы сосредоточимся на администрировании службы каталогов, данных и сети.

Знакомство с Windows Server 2008

В семейство операционных систем Windows Server 2008 входят версии Standard Edition, Enterprise Edition и Datacenter Edition. У каждой версии есть свое особое предназначение:

- **Windows Server 2008 Standard Edition** Эта версия должна непосредственно заменить Windows Server 2003. Она предоставляет службы и ресурсы для других систем сети, обладает богатым набором компонентов и параметров конфигурации. Версия Standard Edition поддерживает двунаправленную и четырехнаправленную симметричную многопроцессорную обработку (symmetric multiprocessing, SMP), до 4 Гб памяти для 32-разрядных систем и до 32 Гб памяти для 64-разрядных систем.
- **Windows Server 2008 Enterprise Edition** Этот вариант обладает более широкими возможностями, чем Standard Edition, обеспечивает большую масштабируемость и доступность, а также поддерживает дополнительные службы, например, кластеризацию и службы федерации Active Directory. Кроме того, поддерживаются 64-разрядные системы, оперативная память с горячей заменой и неоднородный доступ к памяти (non-uniform memory access, NUMA). На серверах Enterprise Edition можно устанавливать до 32 Гб RAM при использовании архитектуры *x*86 и до 2 Тб памяти на 64-разрядных восьмипроцессорных системах.
- **Windows Server 2008 Datacenter Edition** Самая мощная система семейства. В ней расширены возможности кластеризации, добавлена поддержка до 64 Гб памяти на системах *x*86 и до 2 Тб памяти на 64-разрядных системах. Для ее работы требуется не менее 8 процессоров; возможна поддержка до 64 процессоров.
- **Windows Web Server 2008** Этот вариант предназначен для предоставления веб-служб при развертывании веб-сайтов и веб-приложений, поэтому в нем поддерживаются только соответствующие компоненты. Точнее, в эту версию включены Microsoft .NET Framework, Microsoft Internet Information Services (IIS), ASP.NET, сервер приложений и компоненты для балансировки нагрузки на сеть. Многие другие компоненты, включая Active Directory, в этой версии отсутствуют. Вам придется установить ядро сервера, чтобы получить хотя бы частичный доступ к стандартной

функциональности. Windows Web Server 2008 поддерживает до 2 Гб оперативной памяти и 2 процессора.

Примечание В различных версиях ОС поддерживаются одни и те же основные компоненты и инструменты администрирования. Это означает, что описанные в книге методики вы можете применять независимо от того, какой вариант Windows Server 2008 вы используете. Учтите, что на Web Server нельзя установить Active Directory, поэтому вам не удастся сделать сервер с Windows Web Server 2008 контроллером домена (хотя он может входить в домен Active Directory).

Совет Системы с 64-разрядной архитектурой основательно изменились со времени их внедрения в ОС Windows. Я буду называть 32-разрядными системы, созданные для архитектуры *x*86, и 64-разрядными — системы, созданные для архитектуры *x*64. Поддержка 64-разрядных процессоров Itanium (IA-64) в ОС Windows более не является стандартом. Для компьютеров на базе Itanium в Майкрософт разработана специальная версия Windows Server 2008, которая предназначена для предоставления особых серверных функций. Некоторые роли серверов и компоненты могут не поддерживаться IA-64 системами.

Устанавливая ОС Windows Server 2008, вы настраиваете систему сообразно ее роли в сети, учитывая следующие соображения:

- серверы обычно являются частью рабочей группы или домена;
- рабочие группы — это неорганизованные объединения компьютеров, в которых каждый компьютер управляется отдельно;
- домены — это группы компьютеров, управляемых коллективно при помощи контроллеров домена, то есть, систем на базе Windows Server 2008, управляющих доступом к сети, базе данных каталогов и общим ресурсам.

Примечание В этой книге под Windows Server 2008 или семейством Windows Server 2008 понимаются четыре продукта: Windows Server 2008 Standard Edition, Windows Server 2008 Enterprise Edition, Windows Server 2008 Datacenter Edition и Windows Web Server 2008. В этих вариантах ОС поддерживаются одни и те же ключевые компоненты и инструменты администрирования.

Во всех версиях Windows Server 2008 меню **Пуск (Start)** доступно в двух вариантах:

- **Классическое меню** Это меню использовалось в предыдущих версиях Windows. Щелчок кнопки **Пуск (Start)** открывает диалоговое окно с общими меню и командами.

Чтобы получить доступ к меню **Администрирование (Administrative Tools)** при использовании классического представления, нужно щелкнуть кнопку **Пуск (Start)**, указать мышью на меню **Программы (Programs)**, а затем щелкнуть меню **Администрирование (Administrative Tools)**. Чтобы открыть панель управления, щелкните кнопку **Пуск (Start)**, укажите мышью на команду **Настройки (Settings)** и щелкните **Панель управления (Control Panel)**.

- **Простое меню** Оно упрощает доступ к основным программам и позволяет напрямую выполнять некоторые типичные действия. Можно, например, щелкнуть **Пуск (Start)** и **Компьютер (Computer)**, чтобы получить доступ к жестким дискам и съемным накопителям сервера.

Чтобы получить доступ к меню **Администрирование (Administrative Tools)** при использовании простого представления, щелкните **Пуск (Start)** и **Администрирование (Administrative Tools)**. Чтобы открыть панель управления, щелкните **Пуск (Start)** и **Панель управления (Control Panel)**.

Сетевые инструменты и протоколы

Подобно Windows Vista, Windows Server 2008 содержит новый набор сетевых инструментов, включающий обозреватель сети, Центр управления сетями и общим доступом (Network and Sharing Center), Карту сети (Network Map) и диагностику сети. На рис. 1-1 показан Центр управления сетями и общим доступом (Network and Sharing Center).

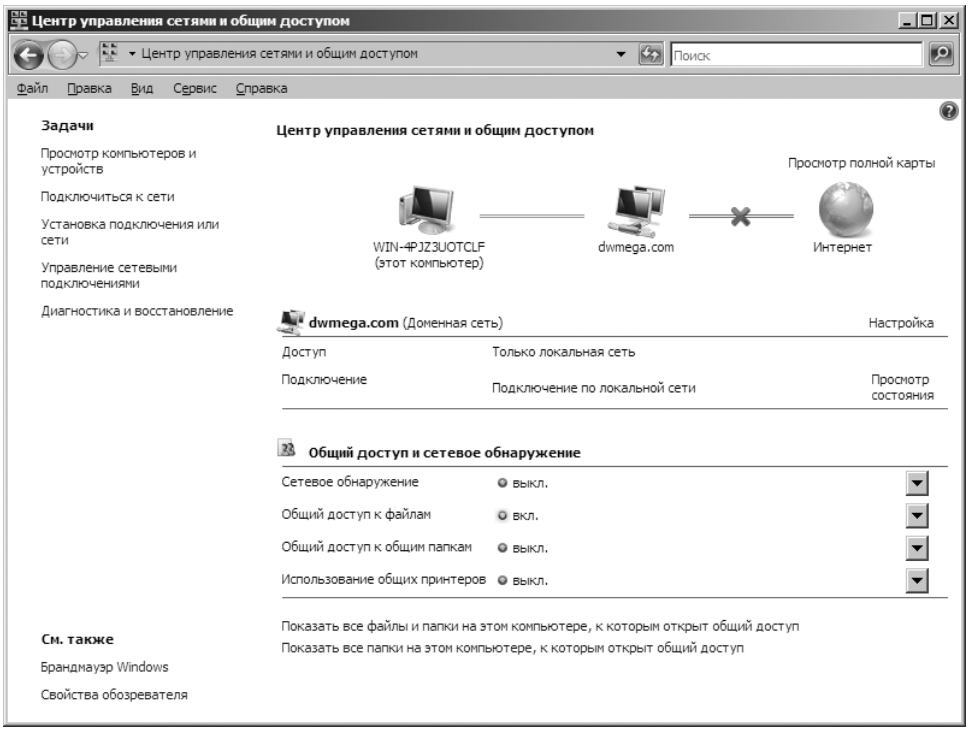


Рис. 1-1. Центр управления сетями и общим доступом (Network and Sharing Center) служит для настройки параметров общего доступа, обнаружения и работы в сети

Введение в сетевые параметры

Основные параметры сети в центре управления сетями и общим доступом настраиваются в разделе **Общий доступ и сетевое обнаружение (Sharing and Discovery)**. Если обнаружение включено и сервер подключен к сети, он может «видеть» другие компьютеры и устройства сети, а они, в свою очередь, «видят» его. Разрешение (или запрет) общего доступа означает, что разрешены (или запрещены) различные варианты общего доступа — общий

доступ к файлам, папкам, принтерам, общий доступ, защищенный паролем. Подробнее — в главе 15.

В Windows Vista и Windows Server 2008 сети разделяются на следующие типы:

- **Сеть домена** Компьютеры подключены к корпоративному домену, членами которого они являются. По умолчанию в сети домена разрешено обнаружение, что позволяет компьютерам сети видеть в ней другие компьютеры и устройства.
- **Частная сеть** Компьютеры настроены как члены рабочей группы и не подключены напрямую к открытой части Интернета. По умолчанию в частной сети обнаружение также разрешено.
- **Общественная сеть** Это сеть в общественном месте, например, в кафе или аэропорту. По умолчанию обнаружение в общественной сети запрещено, что не позволяет компьютерам обнаруживать друг друга или сетевые устройства.

Поскольку в компьютере настройки для каждой категории сетей хранятся отдельно, вы вольны использовать для них различные разрешения. Когда вы подключаетесь к сети впервые, на экран выводится диалоговое окно, в котором вы указываете тип сети: частная или открытая. Если вы выберете частную сеть и компьютер определит, что производится подключение к домену, членом которого он является, сеть будет отнесена к доменной категории.

Работа с сетевыми протоколами

Чтобы сервер мог выходить в сеть, вы должны установить протокол TCP/IP и сетевой адаптер. В качестве протокола глобальной сети (WAN) в Windows Server 2008 по умолчанию используется TCP/IP. Обычно сеть настраивается во время установки ОС. Вы также вольны настроить сеть TCP/IP при помощи окна свойств подключения по локальной сети.

Протоколы TCP и IP позволяют компьютерам обмениваться данными через различные сети и Интернет, используя сетевые адаптеры. В Windows Server 2008, как и в Windows Vista, используется двойная IP-архитектура с поддержкой IPv4 и IPv6 с общими транспортным и кадровым уровнями. В IPv4 — основе большинства современных сетей — используются 32-разрядные адреса. В IPv6 — сетевом протоколе следующего поколения — используются 128-разрядные адреса.

32-разрядные адреса IPv4 обычно записываются в виде четырех десятичных чисел, разделенных точками, например, 127.0.0.1 или 192.168.10.52. Эти числа называют октетами, поскольку каждое из них представляет 8 битов 32-разрядного числа. Стандартный одноадресный IPv4-адрес разделяется на идентификатор сети и идентификатор хоста, причем разделение адреса на идентификаторы в каждой сети может быть своим. IPv4-адрес хоста и аппаратный (MAC) адрес адаптера никак не связаны между собой.

128-разрядные IPv6-адреса делятся на восемь 16-разрядных блоков, разделяемых двоеточиями. Каждый блок записывается в шестнадцатеричном формате, например, FEC0:0:0:02BC:FF:BECB:FE4F:961D. В стандартном одноадресном IPv6-адресе первые 64 бита представляют собой идентификатор сети, вторые 64 бита — сетевой интерфейс. Многие блоки IPv6-адресов заполнены нулями, и для них предусмотрена специальная нотация: непрерывный набор нулей можно заменить двумя двоеточиями («::»). В приведенном выше примере можно «сжать» два нулевых блока — FEC0::02BC:FF:BECB:FE4F:961D. Таким же образом можно сократить и большее количество нулевых блоков. Например, адрес FFE8:0:0:0:0:0:0:1 записывается как FFE8::1.

Если во время установки операционной системы обнаружено сетевое оборудование, по умолчанию включаются как IPv4, так и IPv6, т. е. устанавливать отдельный компонент для поддержки IPv6 не нужно. Модернизированная IP-архитектура Windows Vista и Windows Server 2008 называется стеком TCP/IP нового поколения (Next Generation TCP/IP stack). В ней усовершенствованы многие аспекты использования IPv4 и IPv6.

Контроллеры доменов, рядовые серверы и доменные службы

Устанавливая Windows Server 2008 на новый компьютер, вы настраиваете его как рядовой сервер, контроллер домена или изолированный сервер. Разница между этими типами крайне важна. Рядовые серверы являются частью домена, но не сохраняют информацию каталога. Контроллеры доменов отличаются от рядовых серверов тем, что хранят информацию каталога и предоставляют всему домену службы каталогов и проверки подлинности. Изолированные серверы не являются частью домена. Поскольку на изолированных серверах используются собственные базы данных пользователей, они авторизуют запросы на регистрацию независимо.

Работа с Active Directory

В Windows Server 2008, как и в Windows 2000 или Windows Server 2003, контроллеры домена не разделяются на основные и резервные. В этой ОС используется модель репликации с несколькими хозяевами: любой контроллер домена способен обрабатывать изменения в каталоге, а затем автоматически реплицировать эти изменения на другие контроллеры. Эта модель отличается от использованной в Windows NT модели репликации с одним хозяином, в которой основная копия каталога хранится на главном контроллере домена, а на резервных контроллерах хранятся, соответственно, резервные копии каталога. Кроме того, в Windows NT распространялась только база данных SAM (Security Account Manger), тогда как в Windows 2000 и последующих версиях Windows Server распространяется весь каталог, называемый *хранилищем данных* (data store). Внутри хранилища данных находятся объекты,

представляющие пользователей, группы и учетные записи, а также общие ресурсы, например, серверы, файлы и принтеры.

Домены, использующие Active Directory, мы так и будем называть — домены Active Directory, чтобы отличать их от доменов Windows NT. Хотя домены Active Directory будут нормально работать и под управлением одного контроллера, никогда не помешает иметь в домене несколько контроллеров. Если один из контроллеров выйдет из строя, проверку подлинности и другие критически важные задачи возьмут на себя другие контроллеры.

Службы Active Directory в Windows Server 2008 претерпели несколько фундаментальных изменений. В связи с перестройкой их функциональности появилось несколько новых семейств связанных служб:

- **Службы сертификации Active Directory (Active Directory Certificate Services, AD CS)** Обеспечивают выпуск и отзыв цифровых сертификатов для пользователей, клиентских компьютеров и серверов. За проверку подлинности пользователей и компьютеров и выпуск сертификатов, подтверждающих эту подлинность, в AD CS отвечают центры сертификации. В доменах имеются корневые центры сертификации предприятия, лежащие в основе иерархии сертификатов для доменов и являющиеся наиболее доверенными серверами сертификации, а также подчиненные центры сертификации — члены конкретной иерархии сертификатов. В рабочих группах есть собственные корневые центры сертификации, лежащие в основе иерархий, не входящих в предприятие, и изолированные подчиненные центры сертификации.
- **Доменные службы Active Directory (Active Directory Domain Services, AD DS)** Предоставляют важнейшие службы каталогов, необходимые для организации работы домена, включая хранение информации об объектах сети и предоставление пользователям доступа к ней. Для управления доступом к сетевым ресурсам применяются контроллеры домена. Как только пользователь зарегистрировался в домене, его учетные данные, сохраненные в каталоге, могут использоваться для доступа к ресурсам сети. Поскольку службы AD DS лежат в основе Active Directory и необходимы для всех приложений и технологий, опирающихся на каталоги, я обычно буду говорить просто об Active Directory, а не об AD DS или доменных службах Active Directory.
- **Службы федерации Active Directory (Active Directory Federation Services, AD FS)** Распространяют функции проверки подлинности и управления компонентами на веб. В AD FS используются веб-агенты (для предоставления пользователям доступа к внутренним веб-приложениям) и прокси (для управления клиентским доступом). Благодаря AD FS пользователи могут использовать свои цифровые учетные данные для проверки подлинности через веб и получить доступ к внутренним веб-приложениям с помощью браузера, например, Internet Explorer.

- **Службы Active Directory облегченного доступа к каталогам (Active Directory Lightweight Directory Services, AD LDS)** Обеспечивают хранилищем данных приложения, которые основаны на использовании каталога, но не нуждаются в AD DS и не будут развертываться на контроллерах домена. AD LDS не запускается как служба ОС и может использоваться как в домене, так и в рабочей группе. Каждое приложение, запускаемое на сервере, может иметь собственное хранилище данных, организованное посредством AD LDS.
- **Службы управления правами Active Directory (Active Directory Rights Management Services, AD RMS)** Обеспечивают безопасность корпоративной информации за пределами предприятия. Позволяют защитить от несанкционированного доступа электронную почту, документы, веб-страницы интрасети и многое другое. В AD RMS служба сертификации используется для создания сертификатов прав учетных записей, при помощи которых идентифицируются доверенные пользователи, доверенные группы и службы. Служба лицензирования предоставляет авторизованным пользователям, группам и службам доступ к защищенной информации. Служба протоколирования применяется для мониторинга и обслуживания службы управления правами. Когда отношения доверия установлены, пользователи с сертификатами прав учетной записи могут назначать разрешения для данных. Эти разрешения управляют доступом пользователей к информации и действиями, которые они могут предпринимать в отношении этой информации. Пользователи, у которых есть сертификаты прав учетной записи, также могут использовать защищенное содержимое, к которому им предоставлен доступ. Шифрование гарантирует управление доступом к защищенной информации как внутри предприятия, так и вне его.

Контроллеры домена с доступом только для чтения

В Window Server 2008 поддерживаются контроллеры домена, доступные только для чтения и допускающие перезапуск AD DS. Контроллер домена с доступом только для чтения (read-only domain controller, RODC) — это дополнительный контроллер домена, содержащий копию хранилища данных Active Directory, доступную только для чтения. RODC-контроллер идеально подходит для филиалов компании, где нельзя гарантировать физическую защищенность компьютеров. За исключением паролей в RODC хранятся те же объекты и атрибуты, что и на обычных контроллерах домена. Эти объекты и атрибуты копируются в RODC при помощи однонаправленной репликации с обычного контроллера домена, играющего роль партнера репликации.

Поскольку на RODC по умолчанию не хранятся пароли и учетные данные пользователей (кроме собственной учетной записи компьютера и записи Kerberos Target), RODC извлекает учетные данные пользователей и компьютеров с обычного контроллера домена, работающего под управлением

Windows Server 2008. При необходимости RODC кеширует учетные данные, пока они не изменятся, если это разрешено политикой репликации паролей. Поскольку на RODC хранится только часть учетных данных, сокращается объем подвергающейся риску критической информации.

Совет Полномочия локального администратора RODC могут делегироваться любому пользователю домена без предоставления ему каких-либо дополнительных прав в этом домене. RODC не может выполнять функции глобального каталога или хозяина операций. Хотя RODC способен извлекать информацию с контроллеров домена под управлением Windows Server 2003, с контроллеров домена Windows Server 2008 он получает лишь обновления раздела домена.

Перезапускаемые доменные службы Active Directory

В консоли **Службы (Services)** на контроллерах доменов доступна служба AD DS, которую можно останавливать и запускать, как любую локальную службу. Остановив AD DS, вы можете выполнять задачи по обслуживанию, которые в другом случае потребовали бы перезагрузки сервера, например, дефрагментацию базы данных Active Directory, установку обновлений ОС или принудительное восстановление. Пока AD DS остановлена на одном сервере, проверкой подлинности и входом в систему управляют другие контроллеры домена. Кешированные учетные данные, смарт-карты и биометрические методы работают как обычно. Даже если ни один контроллер домена не доступен и ни один из указанных выше методов не работает, вы можете зарегистрироваться на сервере с учетной записью и паролем для восстановления службы каталогов.

Перезапуск доменных служб Active Directory поддерживают все контроллеры домена под управлением Windows Server 2008, даже RODC. Поскольку доменные службы Active Directory являются перезапускаемыми, контроллеры домена под управлением Windows Server 2008 могут находится в трех состояниях:

- **Служба Active Directory запущена** Active Directory работает, и контроллер домена находится в том же состоянии, что и контроллеры под управлением Windows 2000 Server или Windows Server 2003. Это позволяет контроллеру домена проверять подлинность и управлять входом в сеть.
- **Служба Active Directory остановлена** Active Directory остановлена. Контроллер домена не может проверять подлинность и управлять входом в домен. Этот режим представляет собой сочетание режимов работы рядового сервера и контроллера домена в режиме восстановления службы каталогов. Как и рядовой сервер, этот сервер присоединен к домену. Пользователи могут интерактивно регистрироваться на нем с помощью кешированных учетных данных, смарт-карт или биометрических датчиков. Пользователи также могут входить в сеть, используя для регистрации другой контроллер. Как и в режиме восстановления службы каталогов, база данных Active Directory (Ntds.dit) на локальном контроллере

домена не подключена к сети. Это означает, что вы можете выполнять автономные операции с AD DS, например, дефрагментировать базы данных и устанавливать обновления системы безопасности, без перезагрузки контроллера домена.

- **Режим восстановления службы каталогов** Контроллер домена находится в том же состоянии восстановления, что и контроллер домена под управлением Windows Server 2003. Этот режим позволяет выполнять принудительное или непринудительное восстановление базы данных Active Directory.

Останавливая AD DS, вы должны помнить, что останавливаются и зависимые службы, например, служба репликации файлов (FRS), центр распределения ключей Kerberos (KDC) и межсайтовый обмен сообщениями. Далее, в режиме восстановления службы каталогов контроллер домена можно перезапустить, а в режиме остановки Active Directory — нельзя. Чтобы остановить Active Directory, вы должны обычным способом запустить контроллер домена и лишь затем остановить AD DS.

Службы разрешения имен

В Windows разрешение имен применяется для облегчения обмена данными между компьютерами сети. Система разрешения имен связывает имена компьютеров с их IP-адресами, используемыми в сетевых коммуникациях. Вместо длинной строки чисел пользователь может получить доступ к компьютеру сети с помощью понятного имени.

В Windows Vista и Windows Server 2008 поддерживаются три системы разрешения имен: DNS, WINS и LLMNR. Далее эти службы описываются подробно.

DNS

Служба DNS преобразует имена компьютеров в IP-адреса. При ее использовании полное имя хоста, например, computer84.cpandl.com, преобразуется в IP-адрес, который позволяет компьютерам находить друг друга. DNS работает через стек TCP/IP и может интегрироваться с WINS, DHCP и доменными службами Active Directory. Протокол DHCP, обсуждаемый в главе 19, используется для динамического назначения IP-адресов и параметров TCP/IP.

В DNS группы компьютеров разделены на домены, образующие иерархическую структуру в масштабах Интернета для общественных сетей или в масштабах предприятия для частных сетей (интрасетей или экстрасетей). Различные уровни иерархии соответствуют индивидуальным компьютерам, доменам организаций и доменам первого уровня. Имя *computer84.cpandl.com* включает имя хоста *computer84*, домен организации *cpandl* и домен первого уровня *com*.

Домены первого уровня находятся в основе DNS-иерархии и, соответственно, называются корневыми доменами. Они организованы географичес-

ки, по типу организации и по своему назначению. Обычные домены, вроде *cpandl.com*, называются также родительскими доменами. Родительские домены могут разделяться на поддомены для отдельных групп или отделов организации. Поддомены обычно называются дочерними доменами. Например, полное имя компьютера отдела кадров может выглядеть как *jacob.hr.cpandl.com*. Здесь *jacob* — имя хоста, *hr* — дочерний домен и *cpandl.com* — родительский домен.

В доменах Active Directory служба DNS используется для создания собственной структуры имен и иерархии. Active Directory и DNS настолько тесно связаны, что перед установкой Active Directory необходима установка DNS. Во время установки первого контроллера домена в сети Active Directory у вас будет возможность автоматически установить DNS, если в сети еще нет DNS-сервера. Также вы сможете указать, должны ли Active Directory и DNS быть полностью интегрированы. В большинстве случаев следует утвердительно ответить на оба предложения. При полном объединении информация DNS хранится непосредственно в Active Directory. Разница между частичным и полным объединением очень важна.

- **Частичное объединение** Домен использует стандартное хранилище файлов. Информация DNS хранится в текстовых файлах с расширением .dns, по умолчанию — в папке %SystemRoot%\System32\Dns. Обновления DNS обрабатываются через полномочный DNS-сервер, который считается основным DNS-сервером конкретного домена или части домена — зоны. Клиенты, использующие динамические обновления DNS через DHCP, должны быть настроены на использование основного DNS-сервера зоны, иначе информация DNS не будет обновляться. Также динамические обновления через DHCP невозможны, если основной DNS-сервер отключен от сети.
- **Полное объединение** Домен использует хранилище, интегрированное в Active Directory. Информация DNS хранится непосредственно в Active Directory и доступна через контейнер dnsZone. Поскольку информация является частью Active Directory, к ней может получить доступ любой контроллер домена, и для динамических обновлений через DHCP можно использовать подход с несколькими хозяевами. При этом любой контроллер домена, на котором запущена служба DNS Server, может обрабатывать динамические обновления. Клиенты, использующие динамические обновления DNS через DHCP, могут обращаться к любому DNS-серверу зоны. Для управления доступом к информации DNS можно использовать службу безопасности Active Directory.

Рассмотрев подробно репликацию информации DNS в сети, вы увидите преимущества полного объединения DNS с Active Directory. При частичном объединении информация DNS хранится и реплицируется отдельно от Active Directory. Наличие двух самостоятельных структур сокращает эффективность обеих и усложняет администрирование. Поскольку в задачах

репликации изменений DNS менее эффективна, чем Active Directory, следует ожидать увеличения трафика и времени, необходимого для репликации изменений DNS.

Чтобы использовать DNS в сети, необходимо настроить DNS-клиенты и серверы. Настройка DNS на клиенте состоит в указании IP-адреса DNS-сервера, который позволяет клиенту обмениваться данными с сервером, даже если тот находится в другой подсети.

В сети DHCP вы должны настроить DHCP для работы с DNS. Чтобы сделать это, необходимо задать в параметрах DHCP-области адрес DNS-сервера и имя DNS-домена, как описано в главе 19. Если к компьютерам домена необходимо получить доступ из других доменов Active Directory, для этих компьютеров необходимо создать записи в DNS. Записи DNS разделены на зоны; зона — это просто часть домена. Настройка DNS-сервера описана в главе 20.

Когда вы устанавливаете службу DNS на RODC, он извлекает копии всех разделов каталога, используемых DNS, включая ForestDNSZones и DomainDNSZones. После этого клиенты могут обращаться к RODC за разрешением имен, как к любому другому DNS-серверу. Однако, как и в случае с Active Directory, DNS-сервер на RODC не поддерживает прямых обновлений. Это означает, что RODC не регистрирует записи ресурсов сервера имен ни для одной обслуживаемой им зоны, объединенной с Active Directory. Когда клиент пытается обновить записи DNS через RODC, сервер возвращает ссылку на DNS-сервер, которым клиент может воспользоваться для обновления.

WINS

WINS — еще одна служба, разрешающая имена компьютеров в IP-адреса. Имя компьютера, например, COMPUTER84, будет преобразовано в IP-адрес, позволяющий компьютерам сети Microsoft находить друг друга и обмениваться информацией. Служба WINS необходима для поддержки систем с версиями Windows до Windows 2000 и старых приложений, в которых применяется NetBIOS через TCP/IP, например, для утилит командной строки NET. Если в вашей сети нет систем со старыми версиями ОС или старыми приложениями, WINS вам не нужна.

WINS лучше всего работает в клиент-серверных средах: WINS-клиенты посылают запросы на разрешение имен WINS-серверам, те выполняют разрешение и отправляют ответ. Для передачи WINS-запросов и другой информации компьютеры используют протокол NetBIOS. Для разрешения имен компьютеров в IP-адреса приложения NetBIOS применяют WINS или локальный файл LMHOSTS. В сетях на базе систем, предшествующих Windows 2000, WINS является главной службой разрешения имен. В сетях Windows 2000 и более поздних разрешением имен занимается DNS, а у WINS другая функция: предоставлять системам до Windows 2000 возможность просматривать списки ресурсов сети, а системам с Windows 2000 и более поздним — обнаруживать NetBIOS-ресурсы.

Чтобы включить разрешение имен WINS, вы должны настроить клиенты и серверы WINS. Настройка клиентов состоит в указании IP-адресов серверов WINS. С помощью IP-адреса клиенты способны связаться с WINS-сервером, даже если он расположен в другой подсети. Также клиенты WINS могут связываться при помощи широковещательной рассылки, отправляя другим компьютерам сегмента локальной сети сообщения с запросом их IP-адресов. Поскольку сообщения являются широковещательными, сервер WINS не используется. Любые не-WINS-клиенты, поддерживающие этот тип рассылки сообщений, также могут использовать данный метод для разрешения имен компьютеров в IP-адреса.

Связываясь с сервером WINS, клиенты создают сеансы, состоящие из трех ключевых этапов:

- **Регистрация имени** Клиент передает серверу свое имя и IP-адрес и просит добавить их в базу данных WINS. Если указанные имя и IP-адрес не используются в сети, сервер WINS принимает запрос и регистрирует клиента в базе данных.
- **Обновление имени** Имя закрепляется за клиентом не навсегда. Он пользуется им в течение определенного времени, называемого временем аренды. Клиенту также указывается временной интервал, в течение которого аренда должны быть обновлена. В течение интервала обновления клиент должен повторно зарегистрироваться на сервере.
- **Освобождение имени** Если клиент не обновляет аренду, имя освобождается, что позволяет другой системе в сети использовать то же самое имя компьютера, тот же IP-адрес или и то, и другое. Также имена освобождаются при отключении клиента WINS.

Организовав сеанс с сервером WINS, клиент может посылать запросы службе разрешениям имен. Метод разрешения имени зависит от настроек сети. Вообще, существует четыре метода:

- **B-узел (широковещательный метод)** Для разрешения имен компьютеров в IP-адреса используются широковещательные сообщения. Компьютеры, которым требуется разрешение, посылают сообщение каждому хосту локальной сети, запрашивая IP-адрес, соответствующий имени компьютера. В больших сетях из сотен и тысяч компьютеров эти сообщения могут занимать значительную часть полосы пропускания.
- **P-узел (одноранговый метод)** Для разрешения имен компьютеров в IP-адреса используются WINS-серверы. Когда клиенту требуется разрешить имя компьютера в IP-адрес, клиент посылает запрос на сервер, а сервер посылает ему ответ.
- **M-узел (смешанный метод)** Совмещает широковещательный и одноранговый методы. Клиент WINS сначала пытается использовать для разрешения имени B-узел. Если это не удается, он использует P-узел. Поскольку B-узел применяется первым, этому методу присущи те же проблемы с загруженностью сети, что и широковещательному методу.

- **H-узел (гибридный метод)** Также совмещает широковещательный и одноранговый методы. Клиент сначала пытается использовать одноранговый метод, потом (в случае сбоя) — широковещательный. Поскольку P-узел применяется первым, в большинстве сетей гибридный метод позволяет достичь наилучшей производительности. По умолчанию в WINS используется именно он.

Если в сети имеются WINS-серверы, клиенты Windows используют для разрешения имен метод P-узла. Если WINS-серверы отсутствуют, применяется широковещательный метод. Windows-компьютеры также могут использовать для разрешения имен DNS и локальные файлы LMHOSTS и HOSTS. О работе DNS рассказывается в главе 20.

Если вы применяете DHCP для назначения IP-адресов, вы должны указать метод разрешения имен для DHCP-клиентов. Как это сделать, описано в главе 19. Предпочтительным является гибридный метод.

LLMNR

Служба LLMNR (Link-Local Multicast Name Resolution) позволяет организовать одноранговое разрешение имен в пределах одной подсети для IPv4, IPv6 или обоих видов адресов сразу без обращения к серверам, на что не способны ни DNS, ни WINS. WINS предоставляет как клиент-серверную, так и одноранговую службу разрешения имен, но не поддерживает адреса IPv6. DNS, с другой стороны, поддерживает оба типа адресов, но требует наличия серверов.

Разрешение имен LLMNR, поддерживаемое как в Windows Vista, так и в Windows Server 2008, работает для адресов IPv6 и IPv4 в тех случаях, когда другие службы разрешения имен недоступны, например, в домашних сетях, в небольших предприятиях, во временных сетях или в корпоративных сетях, где по каким-то причинам недоступны DNS-службы.

LLMNR призвана дополнить DNS, обеспечивая разрешение имен в случаях, когда обычное DNS-разрешение невозможно. Если у вас нет необходимости в NetBIOS, LLMNR может полностью заменить WINS. Полностью заменить DNS не получится, поскольку LLMNR работает только в локальной подсети. Поскольку трафик LLMNR не проходит через маршрутизаторы, вы не рискуете случайно заполнить им сеть.

Как и WINS, LLMNR позволяет преобразовать имя хоста, например, COMPUTER84, в IP-адрес. По умолчанию LLMNR включена на всех компьютерах под управлением Windows Vista и Windows Server 2008. Эти компьютеры прибегают к LLMNR, если попытки узнать имя хоста через DNS окончились неудачей. В результате, разрешение имен в Widows Vista и в Windows Server 2008 работает следующим образом:

1. Хост посылает запрос на первичный DNS-сервер. Если он не получает ответа или получает сообщение об ошибке, он по очереди посылает запросы на все вторичные DNS-серверы. Если и это не помогло, разрешение имени передается LLMNR.

2. Хост посылает многоадресный UDP-запрос, запрашивая IP-адрес для нужного имени компьютера. Этот запрос идет только по локальной подсети.
3. Каждый компьютер локальной подсети, поддерживающий LLMNR и сконфигурированный для ответа на поступающие запросы, сравнивает имя со своим хост-именем. Если они не совпадают, компьютер отбрасывает запрос. Если имена совпадают, компьютер пересылает исходному хосту одноадресное сообщение с IP-адресом.

Вы также можете использовать LLMNR для обратного разрешения. При этом компьютер посылает одноадресный запрос по конкретному IP-адресу, запрашивая имя хоста. Компьютер с включенной LLMNR, получив запрос, посылает одноадресный ответ, содержащий имя хоста.

Компьютеры с включенной LLMNR должны проверять уникальность своих имен в подсети. В большинстве случаев это происходит при запуске, восстановлении из спящего режима или при смене параметров сетевого интерфейса. Если компьютер еще не проверил уникальность своего имени, он должен указывать это в ответе на запрос.

Ближе к реальности По умолчанию LLMNR автоматически включается на компьютерах под управлением Window Vista и Windows Server 2008. Чтобы отключить LLMNR для всех сетевых интерфейсов, создайте в реестре параметр HKLM/SYSTEM/CurrentControlSet/Services/Dnscache/Parameters/EnableMulticast и присвойте ему нулевое значение. Чтобы отключить конкретный сетевой интерфейс, создайте параметр реестра HKLM/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/*GUID_адаптера*/EnableMulticast и присвойте ему нулевое значение. Здесь *GUID_адаптера* — идентификатор GUID адаптера сетевого интерфейса, для которого вы хотите отключить LLMNR. Чтобы включить LLMNR, присвойте этим параметрам значение 1. Также LLMNR можно управлять посредством групповых политик.

Другие важные инструменты

Для администрирования Windows Server 2008 применяется множество утилит. Ниже перечислены наиболее часто используемые:

- **Панель управления** Набор инструментов для управления конфигурацией системы. Панель управления обладает различными представлениями, то есть, способами организации параметров. По умолчанию используется представление по категориям, в котором инструменты панели управления разбиты на группы. В классическом представлении все инструменты отображаются единой группой.
- **Графические инструменты администрирования** Основные инструменты для управления компьютерами сети и их ресурсами. Доступ к ним открывает меню **Администрирование (Administrative Tools)**.
- **Административные мастера** Инструменты для выполнения ключевых задач администрирования. Доступ ко многим мастерам открывает диспетчер сервера — центр управления Windows Server 2008.

- **Утилиты командной строки** Большинство административных утилит можно запускать из командной строки.

Чтобы узнать, как использовать инструменты командной строки NET, введите **NET HELP** и имя команды, например, **NET HELP SEND**. Windows предоставит справку по использованию этой команды.

Windows PowerShell

Дополнительную гибкость командной строке придает Windows PowerShell — полнофункциональная командная оболочка, в которую помимо стандартных утилит командной строки включены встроенные *cmdlet*-команды и возможности программирования. По умолчанию PowerShell не устанавливается. Чтобы установить ее, выполните следующие действия:

1. Щелкните кнопку **Диспетчер сервера (Server Manager)** на панели быстрого запуска или щелкните кнопку **Пуск (Start)** и выберите команды **Администрирование (Administrative Tools)** и **Диспетчер сервера (Server Manager)**.
2. В диспетчере сервера выберите узел **Компоненты (Features)** и щелкните ссылку **Добавить компоненты (Add Features)**.
3. Пролистайте список компонентов и выберите **Windows PowerShell**.
4. Щелкните **Далее (Next)** и **Установить (Install)**.

Оболочка PowerShell из комплекта поставки может быть не самой новой. Проверьте центр загрузки на сайте Майкрософт на предмет наличия более новой версии. Установив PowerShell, вы обнаружите команду для ее запуска в меню **Пуск (Start)**. Если вы хотите вызвать PowerShell из командной строки, помните, что соответствующий исполняемый файл (powershell.exe) находится в папке %SystemRoot%\System32\WindowsPowerShell*Версия*, где *Версия* — номер установленной версии PowerShell, например, v.1.0 или v.1.1.

Запустив PowerShell, введите в командной строке имя cmdlet-команды, и она запустится, как любая команда. Команды cmdlet можно также запускать из сценариев. Названия cmdlet-команд состоят из пар «глагол-существительное». Глагол говорит о действии cmdlet-команды, а существительное указывает на объект этого действия. Например, команда get-variable возвращает имена и значения переменных среды Windows PowerShell. Обычно в именах cmdlet-команд используются следующие глаголы:

- **Get** Запрашивает специфический объект или подмножество типа объекта, например, выбранный почтовый ящик или всех пользователей почтовых ящиков.
- **Set** Модифицирует параметры объекта.
- **Enable** Включает параметр.
- **Disable** Выключает параметр.
- **New** Создает новый экземпляр объекта, например, почтового ящика.
- **Remove** Удаляет экземпляр объекта.

Чтобы просмотреть полный список cmdlet-команд, введите в командной строке PowerShell команду **help *.***. Чтобы получить справку по конкретной команде, введите **help** и имя команды, например, **help get-variable**.

У cmdlet-команд есть настраиваемые псевдонимы, которые можно использовать для запуска cmdlet-команд. Чтобы просмотреть список псевдонимов, введите в командной строке PowerShell **get-item –path alias**. С помощью следующей команды вы создадите псевдоним для любой команды:

```
new-item -path alias:Псевдоним -value:ПолныйПутьКоманды
```

Здесь *Псевдоним* — имя создаваемого псевдонима, а *ПолныйПутьКоманды* — полный путь к команде. Например:

```
new-item -path alias:sm -value:c:\windows\system32\compmgmtlauncher.exe
```

В этом примере создается псевдоним sm для запуска диспетчера сервера. Чтобы использовать этот псевдоним при работе с PowerShell, просто введите в командной строке **sm** и нажмите Enter.

Глава 2

Развертывание Windows Server 2008

Прежде чем развертывать Windows Server 2008, следует тщательно спланировать архитектуру сервера. В процессе планирования тщательно изучите конфигурацию ПО, которое предполагается использовать, и соответственно измените конфигурацию оборудования, причем индивидуально для каждого сервера. Для обеспечения дополнительной гибкости при развертывании серверов используйте один из двух типов установки:

- **Полная установка сервера** Полная установка версий Windows Server 2008 Standard, Enterprise и Datacenter обеспечивает доступ ко всей функциональности ОС. При настройке сервера можно использовать любую комбинацию ролей, служб ролей и компонентов. Для управления сервером к вашим услугам полнофункциональный пользовательский интерфейс. Это вариант установки является наиболее динамичным и рекомендуется в тех случаях, когда роль сервера со временем может изменяться.
- **Установка ядра сервера** Минимальная установка версий Windows Server 2008 Standard, Enterprise и Datacenter предоставляет ограниченный набор ролей, а для управления сервером предлагается пользовательский интерфейс с минимумом возможностей. Этот вариант идеально подходит в тех случаях, когда сервер предназначен для выполнения определенной роли или комбинации ролей. Дополнительные компоненты не устанавливаются, что снижает нагрузку, вызванную излишними службами, и высвобождает больше ресурсов для выделенной роли или ролей.

Тип установки выбирается во время установки операционной системы. После этого изменить его уже нельзя. Поэтому перед развертыванием серверов следует тщательно продумать, какой тип установки выбрать. В типичной сети найдутся как серверы, выделенные для определенной роли или сочетания ролей, так и серверы, роль которых меняется со временем, в результате чего, как правило, в ход идут оба варианта установки.

Роли, службы ролей и компоненты Windows Server 2008

Архитектура Windows Server 2008 отличается от предшествующих ОС. Готовя сервер к развертыванию, вы устанавливаете и настраиваете следующие модули:

- **Роль сервера** Связанный набор программ, позволяющий серверу выполнять определенную функцию по обслуживанию пользователей и других компьютеров. Сервер может быть выделен для одной роли, например, Active Directory Domain Services, а может выполнять и несколько ролей.
- **Служба роли** Программа, обеспечивающая функциональность роли сервера. С каждой ролью сервера связана одна или несколько служб. Некоторые роли сервера, например, DNS и DHCP, выполняют строго определенную функцию, которая устанавливается при установке роли. Другие роли, например, Network Policy, Access Services и Active Directory Certificate Services, имеют несколько служб ролей, которые можно устанавливать по выбору.
- **Компонент** Программный модуль, обеспечивающий дополнительную функциональность ОС. Компоненты, например, BitLocker Drive Encryption и Windows PowerShell, устанавливаются и удаляются отдельно от ролей и служб ролей. На компьютере в зависимости от конфигурации может быть установлено несколько компонентов, а может не быть и ни одного.

Для настройки ролей, служб ролей и компонентов используются консоль MMC **Диспетчер сервера (Server Manager)** и утилита командной строки **ServerManagerCmd.exe**.

Некоторые роли, службы ролей и компоненты зависят от других ролей, служб ролей и компонентов. При их установке диспетчер сервера предлагает установить все недостающие модели. Аналогично, если попытаться удалить компонент, необходимый для установленной роли, службы роли или компонента, диспетчер сервера предупредит, что этот компонент удалить нельзя, если не удалить также роль, службу роли или компонент, которые от него зависят.

Добавление или удаление ролей, служб ролей и компонентов может изменить требования к аппаратному обеспечению, поэтому вам следует тщательно продумывать любые изменения конфигурации, определяя, как они повлияют на общую производительность сервера. Обычно возникает искушение объединить родственные роли, но это увеличивает нагрузку на сервер, и вы должны соответствующим образом изменить аппаратную часть сервера. В табл. 2-1 приведен обзор основных ролей и связанных с ними служб, которые можно развертывать на сервере Windows Server 2008.

Табл. 2-1. Основные роли Windows Server 2008 и связанные с ними службы

Роль	Описание
DHCP-сервер (DHCP Server)	Предоставляет возможность централизованного управления IP-адресами. DHCP-серверы выдают динамические IP-адреса и назначают основные параметры TCP/IP другим компьютерам в сети. Не включает дополнительных служб ролей
DNS-сервер (DNS Server)	DNS — система разрешения имен, сопоставляющая имена компьютеров с их IP-адресами. Серверы DNS являются неотъемлемой частью системы разрешения имен в доменах Active Directory. Не включает дополнительных служб ролей
Windows SharePoint Services	Позволяет организовать работу в команде, объединяя пользователей и данные. Сервер SharePoint является, по сути, веб-сервером с полностью установленными службами IIS. Функциональность, необходимую для совместной работы, предоставляют управляемые приложения
Веб-сервер (IIS) (Web Server (IIS))	Используется для размещения веб-сайтов и веб-приложений. Веб-сайты, размещенные на веб-сервере, могут включать как статическое, так и динамическое содержимое. Веб-приложения, размещенные на веб-сервере, могут создаваться с использованием ASP.NET и .NET Framework 3.0. При развертывании веб-сервера можно управлять конфигурацией сервера при помощи модулей IIS 7 и административных модулей (подробнее — в книге *«Information Server 7.0 Administrator's Pocket Consultant»*)
Доменные службы Active Directory (Active Directory Domain Services, AD DS)	Предоставляет функции хранения информации о пользователях, группах, компьютерах и других объектах сети, а также делает эту информацию доступной пользователям и компьютерам. Контроллеры домена AD предоставляют сетевым пользователям и компьютерам доступ к разрешенным ресурсам сети
Сервер приложений (Application Server)	Позволяет размещать на сервере распределенные приложения, написанные с использованием ASP.NET, Enterprise Services и .NET Framework 3.0. Включает более десятка ролей служб, подробно описанных в книге *«Information Server 7.0 Administrator's Pocket Consultant»* (Microsoft Press, 2007)
Службы Active Directory облегченного доступа к каталогам (Active Directory Lightweight Directory Services, AD LDS)	Предоставляет хранилище данных для приложений с поддержкой каталога, которым не требуются службы каталогов AD DS и развертывание на контроллерах домена. Не включает дополнительных служб ролей

Табл. 2-1. (*продолжение*)

Роль	Описание
Службы UDDI (Universal Description Discovery Integration Services, UDDI)	Предоставляет возможность общего доступа к информации о веб-службах, как в одной сети, так и между сетями. Включает следующие службы ролей: База данных служб UDDI (UDDI Services Database) и Веб-приложение служб UDDI (UDDI Services Web Application)
Службы печати (Print Services)	Предоставляет основные службы для управления сетевыми принтерами и драйверами печати. Включает следующие службы ролей: Сервер печати (Print Server), Служба LPD (LPD Service) и Печать через Интернет (Internet Printing)
Службы политики сети и доступа (Network Policy and Access Services, NPAS)	Предоставляет основные службы для управления маршрутизацией и удаленным доступом. Включает следующие службы ролей: Сервер политики сети (Network Policy Server, NPS), Службы маршрутизации и удаленного доступа (Routing and Remote Access Services, RRAS), Служба удаленного доступа (Remote Access Service), Маршрутизация (Routing), Центр регистрации работоспособности (Health Registration Authority) и Протокол авторизации учетных данных узла (Host Credential Authorization Protocol, HCAP)
Службы развертывания Windows (Windows Deployment Services, WDS)	Предоставляет службы для развертывания в сети компьютеров под управлением Windows. Включает следующие службы ролей: Сервер развертывания (Deployment Server) и Транспортный сервер (Transport Server)
Службы сертификации Active Directory (Active Directory Certificate Services, AD CS)	Предоставляет функции выдачи и отзыва цифровых сертификатов пользователей, клиентских компьютеров и серверов. Включает следующие службы роли: Центр сертификации (Certification Authority), Служба подачи заявок в центр сертификации через Интернет (Certification Authority Web Enrollment), Сетевой ответчик (Online Certificate Status Protocol) и Служба подачи заявок на сетевые устройства (Microsoft Simple Certificate Enrollment Protocol, MSCEP)
Службы терминалов (Terminal Services)	Предоставляет службы, позволяющие пользователям запускать Windows-приложения, установленные на удаленном сервере. Когда пользователь запускает приложение на сервере терминалов, запуск и обработка данных происходят на сервере, а по сети передаются только данные приложения. Включает следующие службы ролей: Сервер терминалов (Terminal Server), Лицензирование служб терминалов (TS Licensing), Посредник сеансов служб терминалов (TS Session Broker), Шлюз служб терминалов (TS Gateway) и Веб-доступ к службам терминалов (TS Web Access)
Службы управления правами Active Directory (Active Directory Rights Management Services, AD RMS)	Предоставляет управляемый доступ к защищенным сообщениям электронной почты, документам, веб-страницам интрасети и файлам иных типов. Включает следующие службы ролей: Сервер управления правами Active Directory (Active Directory Rights Management Server) и Поддержка федерации удостоверений (Identity Federation Support)

Табл. 2-1. (*окончание*)

Роль	Описание
Службы федерации Active Directory (Active Directory Federation Services, AD FS)	Дополняет функции проверки подлинности и управления доступом AD DS, распространяя их на Интернет. Включает следующие службы ролей и подслужбы: Служба федерации (Federation Service), Прокси-агент службы федерации (Federation Service Proxy), Веб-агенты (AD FS Web Agents), Агент, поддерживающий утверждения (Claims-aware Agent) и Агент Windows на основе маркеров (Windows Token-based Agent)
Файловые службы (File Services)	Предоставляет базовые службы для управления файлами, а также обеспечивает их доступность и репликацию в сети. Некоторым ролям сервера необходима файловая служба определенного типа. Включает следующие службы ролей и подслужбы: Файловый сервер (File Server), Распределенная файловая система DFS (Distributed File System), Пространства имен DFS (DFS Namespace), Репликация DFS (DFS Replication), Диспетчер ресурсов файлового сервера (File Server Resource Manager), Службы для NFS (Services for Network File System), Служба поиска Windows (Windows Search Service), Файловые службы Windows Server 2003 (Windows Server 2003 File Services), Служба репликации файлов (File Replication Service, FRS) и Служба индексирования (Indexing Service)
Факс-сервер (Fax Server)	Обеспечивает централизованное управление отправкой и получением факсов в сети. Сервер факсов может действовать как шлюз для отправки и получения факсов и позволяет управлять ресурсами факса, например, задачами и отчетами, а также устройствами для отправки факсов, подключенными к серверу и другим компьютерам сети. Не включает дополнительных служб ролей

В табл. 2-2 приведен обзор основных компонентов, которые можно развертывать на сервере Windows Server 2008. В отличие от предыдущих версий Windows, некоторые важные компоненты сервера автоматически не устанавливаются. Например, чтобы использовать встроенные возможности резервного копирования и восстановления, необходимо установить компонент **Возможности системы архивации Windows Server (Windows Server Backup)**.

Табл. 2-2. Основные компоненты Windows Server 2008

Компонент	Описание
Возможности .NET Framework 3.0 (.NET Framework 3.0)	Предоставляет API-интерфейс .NET Framework 3.0 для разработки приложений. Включает подкомпоненты: .NET Framework 3.0, Средства просмотра XPS (XPS Viewer) и Активация WCF (Windows Communication Foundation Activation Components)
Шифрование диска BitLocker (BitLocker Drive Encryption)	Обеспечивает защиту данных при помощи аппаратного шифрования всего тома, предотвращая изменение данных вне операционной системы. На компьютерах с установленным модулем TPM (Trusted Platform Module) можно использовать компонент Шифрование диска BitLocker (BitLocker Drive Encryption) в режимах Startup Key и TPM-only. В обоих режимах выполняется предварительная проверка целостности
Серверные расширения BITS [Background Intelligent Transfer Service (BITS) Server Extensions)	Обеспечивает интеллектуальную фоновую передачу данных. После установки этого компонента сервер может действовать как BITS-сервер, на который клиенты могут выгружать файлы. Для загрузки данных клиентами посредством BITS этот компонент не нужен
Пакет администрирования диспетчера подключений (Connection Manager Administration Kit (CMAK))	Обеспечивает функциональность для генерации профилей диспетчера подключений
Возможности рабочего стола (Desktop Experience)	Обеспечивает на сервере дополнительную функциональность рабочего стола Windows Vista. К компонентам Windows Vista относятся Windows Media Player, темы рабочего стола и Windows Photo Gallery. Они позволяют использовать сервер подобно обычной рабочей станции, но снижают его общую производительность
Средство отказоустойчивости кластеров (Failover Clustering)	Обеспечивает функциональность кластеризации, позволяющую нескольким серверам совместно обеспечивать высокий уровень доступности служб и приложений. В кластере могут работать службы многих типов, включая файловые службы и службы печати. Идеальное применение кластеризации — серверы баз данных и серверы сообщений
Управление групповой политикой (Group Policy Management)	Устанавливает консоль GPMC (Group Policy Management Console) для централизованного управления групповой политикой
Клиент печати через Интернет (Internet Printing Client)	Предоставляет функциональность, позволяющую клиентам использовать протокол HTTP для подключения к принтерам на серверах веб-печати

Табл. 2-2. (*продолжение*)

Компонент	Описание
Монитор LPR-портов (Line Printer Remote (LPR) Port Monitor)	Устанавливает монитор порта LPR, позволяющий печатать на устройствах, подключенных к компьютерам под управлением UNIX
Очередь сообщений (Message Queuing)	Предоставляет управляющие и серверные функции для обработки очередей сообщений. К нему прилагается группа связанных подкомпонентов.
Многопутевой ввод-вывод (Multipath I/O (MPIO))	Предоставляет функциональность, необходимую для использования множественных путей к устройствам хранения
Балансировка сетевой нагрузки (Network Load Balancing, NLB)	Обеспечивает отказоустойчивость и балансировку нагрузки для приложений и служб на основе протокола IP, распределяя входящие запросы к приложениям между несколькими участвующими серверами. Веб-серверы — идеальные объекты для балансировки нагрузки
Протокол PRNL (Peer Name Resolution Protocol, PNRP)	Обеспечивает функциональность LLMNR (Link-Local Multicast Name Resolution) для служб одноранговогo разрешения имен. После установки этого компонента приложения, работающие на сервере, могут регистрировать и разрешать имена при помощи LLMNR
Удаленный помощник (Remote Assistance)	Позволяет удаленному пользователю подключаться к серверу для предоставления или получения услуг удаленного помощника
Средство удаленного администрирования сервера (Remote Server Administration Tools, RSAT)	Устанавливает средства управления ролями и компонентами для удаленного администрирования Windows Server 2008. Можно устанавливать отдельные инструменты, подкатегории или целиком категории
Диспетчер съемных носителей (Removable Storage Manager, RSM)	Устанавливает утилиту Диспетчер съемных носителей (Removable Storage Manager) для управления съемными носителями
RPC через HTTP-прокси (Remote Procedure Call (RPC) over HTTP Proxy)	Устанавливает прокси для ретрансляции серверу RPC-сообщений по протоколу HTTP от клиентских приложений. RPC over HTTP — альтернатива предоставления клиентам доступа к серверу через VPN-соединение
Простые службы TCP/IP (Simple TCP/IP Services)	Устанавливает дополнительные службы TCP/IP, в том числе, Character Generator, Daytime, Discard, Echo и Quote of the Day
Сервер SMTP (Simple Mail Transfer Protocol (SMTP) Server)	SMTP — это сетевой протокол для управления передачей и маршрутизацией сообщений электронной почты. После установки этого компонента сервер может действовать как базовый SMTP-сервер. Для получения полномасштабного решения необходима установка сервера сообщений, например,Microsoft Exchange Server 2007

Табл. 2-2. (*окончание*)

Компонент	Описание
Диспетчер хранилища для сетей SAN (Storage Manager for SANs)	Устанавливает консоль **Диспетчер хранилища для сетей SAN (Storage Manager for SANs)** для централизованного управления устройствами, входящими в сеть хранения данных (Storage Area Network, SAN). При помощи этой консоли можно просматривать подсистемы хранения, создавать и управлять логическими номерами устройств (Logical Unit Number, LUN) и управлять целевыми устройствами iSCSI. Устройства SAN должны поддерживать службы Visual Disk Services (VDS)
Подсистема для UNIX-приложений (Subsystem for UNIX-based Applications, SUA)	Предоставляет функциональность для запуска UNIX-программ. С веб-сайта Майкрософт можно загрузить дополнительные средства управления
Внутренняя база данных Windows (Windows Internal Database)	Устанавливает SQL Server 2005 Embedded Edition. Это позволяет серверу использовать реляционные базы данных при работе с ролями и компонентами Windows, которым необходима внутренняя база данных, например, AD RMS, службы UDDI, службы обновления WSUS (Windows Server Update Services,), службы Windows SharePoint и Диспетчер системных ресурсов (System Resource Manager)
Windows PowerShell	Устанавливает оболочку Windows PowerShell — расширенную среду командной строки для управления системами Windows
Служба активации процессов Windows (Windows Process Activation Service)	Обеспечивает поддержку распределенных веб-приложений, использующих протокол HTTP и другие протоколы
Windows Recovery Environment	Среда восстановления сервера, используемая при отсутствии доступа к вариантам восстановления, предоставленным производителем сервера
Возможности системы архивации Windows Server (Windows Server Backup)	Позволяет архивировать и восстанавливать состояние операционной системы и любую другую информацию, хранящуюся на сервере
Диспетчер системных ресурсов (Windows System Resource Manager, WSRM)	Позволяет управлять использованием ресурсов для каждого процессора в отдельности
WINS-сервер (WINS Server)	WINS — служба разрешения имен, сопоставляющая имена компьютеров и IP-адреса. Установка этого компонента позволяет компьютеру функционировать в качестве WINS-сервера
Служба беспроводной локальной сети (Wireless Networking)	Позволяет серверу использовать беспроводные подключения и профили

Полная установка и установка ядра Windows Server 2008

При полной установке сервера вы получаете полнофункциональную рабочую версию Windows Server 2008, которую можно развертывать с любой допустимой комбинацией ролей, служб ролей и компонентов. Установка ядра сервера — это минимальная конфигурация Windows Server 2008, поддерживающая ограниченный набор ролей и их сочетаний. Поддерживаются, в частности, роли AD DS, DNS-сервера, DHCP-сервера, файловых служб и служб печати. В текущей реализации ядро сервера не может быть платформой для запуска серверных приложений.

Оба типа установки опираются на одинаковые правила лицензирования и могут управляться при помощи любых доступных и допустимых способов удаленного администрирования. Однако полная установка и установка ядра сервера сильно отличаются в отношении локального администрирования с консоли. В полном варианте доступен полнофункциональный пользовательский интерфейс с обширным набором инструментов для локального управления сервером. В установке ядра доступен лишь интерфейс с минимальным набором компонентов, включая следующие:

- начальный экран **Вход в Windows (Windows Logon)** для входа и выхода из системы;
- текстовый редактор **Блокнот (Notepad)** для редактирования конфигурационных файлов;
- **Редактор реестра (Regedit)**;
- **Диспетчер задач (Task Manager)** для управления задачами и запуска новых задач;
- командная строка.

При запуске системы с установкой ядра сервера, как и в полном варианте, для входа можно использовать экран **Вход в Windows (Windows Logon)**. В домене применяются стандартные ограничения входа на серверы. Войти в систему может любой пользователь, имеющий соответствующие права и разрешения на вход. Чтобы разрешить пользователям локальный вход на серверы, не являющиеся контроллерами домена, а также в рабочих группах используйте команду NET USER для добавления локальных пользователей или команду NET LOCALGROUP для включения пользователей в локальные группы.

После входа в систему Windows Core Server вам доступна ограниченная рабочая среда с административной командной строкой. Если пользователь случайно закрыл командную строку, ее можно запустить повторно, выполнив следующие действия:

1. Нажмите Ctrl+Shift+Esc, чтобы открыть **Диспетчер задач (Task Manager)**.
2. Перейдите на вкладку **Приложения (Applications)** и щелкните кнопку **Новая задача (New Task)**.

3. В диалоговом окне **Создать новую задачу (Create New Task)** в поле **Открыть (Open)** введите **cmd** и щелкните **OK**.

Так же можно открывать дополнительные окна командной строки или ввести место команды **cmd** команды **notepad.exe** или **regedit.exe**, чтобы открыть Блокнот (Notepad) или редактор реестра. Эти программы можно запускать и непосредственно из командной строки. Чтобы открыть панель управления, введите **control.cpl**.

Чтобы открыть экран **Вход в Windows (Windows Logon)** после входа в систему, нажмите сочетание клавиш Ctrl+Alt+Delete. Возможности этого экрана те же, что и в полной установке: можно заблокировать компьютер, сменить пользователя, выйти из системы, поменять пароль или запустить диспетчер задач. В командной строке доступны все стандартные команды и утилиты для управления сервером. Однако помните, что они будут работать только в том случае, если на сервере установлены необходимые для их работы службы и компоненты.

Установка Windows Core Server поддерживает ограниченный набор ролей и служб ролей, но в ней можно устанавливать большинство имеющихся компонентов. Основным исключением являются компоненты, зависящие от .NET Framework. Поскольку .NET Framework в текущей реализации не поддерживается, вам недоступны такие компоненты, как оболочка PowerShell. Это ограничение, возможно, будет устранено в будущих пакетах обновлений или исправлениях. Для удаленного управления Windows Core Server можно использовать службы терминалов. В табл. 2-3 перечислены некоторые распространенные задачи, которые можно выполнять, войдя в систему локально.

Табл. 2-3. Команды и утилиты для управления Windows Core Server

Команда	Описание
Control desk.cpl	Просмотр и изменение параметров экрана
Control intl.cpl	Просмотр и изменение региональных и языковых параметров, включая раскладку клавиатуры и форматы
Control sysdm.cpl	Просмотр и изменение свойств системы
Control timedate.cpl	Просмотр и изменение даты, времени и часового пояса
Cscript slmgr.vbs –ato	Активация операционной системы
DiskRaid.exe	Настройка программного массива RAID
ipconfig /all	Получение информации о параметрах IP
NetDom RenameComputer	Изменение имени сервера и членства в домене
OCList.exe	Получение списка ролей, служб ролей и компонентов
OCSetup.exe	Добавление или удаление ролей, служб ролей и компонентов
PNPUtil.exe	Установка или обновление драйверов аппаратных устройств

Табл. 2-3. (*окончание*)

Команда	Описание
Scregedit.wsf	Настройка операционной системы. Параметр **/cli** позволяет получить список доступных разделов конфигурации
ServerWerOptin.exe	Настройка службы сообщений об ошибках Windows
SystemInfo	Получение информации о конфигурации системы
WEVUtil.exe	Просмотр и поиск информации в журналах событий
Wmic datafile where name="FullFilePath" get version	Получение информации о версии файла
Wmic nicconfig index=9 call enabledhcp	Включение динамического получения IP-адреса вместо использования статического IP-адреса
Wmic nicconfig index=9 call enable static("IPAddress"), ("SubnetMask")	Установка статического IP-адреса и маски подсети
Wmic nicconfig index=9 call setgateways("GatewayIPAddress")	Установка или изменение шлюза по умолчанию
Wmic product get name /value	Получение списка названий установленных приложений MSI
Wmic product where name="Name" call uninstall	Удаление приложения MSI
Wmic qfe list	Получения списка установленных обновлений и исправлений
Wusa.exe PatchName.msu /quiet	Применение обновления или исправления операционной системы

Установка Windows Server 2008

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

Перед началом установки Windows Server 2008 следует убедиться, что компьютер удовлетворяет минимальным требованиям устанавливаемой версии. Майкрософт указывает как минимальные, так и рекомендуемые характеристики компьютера. Если компьютер не удовлетворяет минималь-

ным требованиям, установить Windows Server 2008 будет невозможно. Если характеристики компьютера ниже рекомендуемых, возможны проблемы с производительностью.

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

Новая установка

Новая установка Windows Server 2008 выполняется следующим образом:

1. Запустите программу установки. Включите компьютер, вставьте установочный DVD-диск Windows Server 2008 и нажмите любую клавишу, когда на экране появится приглашение. Чтобы выполнить новую установку поверх существующей, запустите компьютер и войдите в систему с административными полномочиями. Когда будет вставлен установочный DVD-диск Windows Server 2008, программа установки запустится автоматически. Если этого не произошло, откройте диск в Проводнике и запустите программу **Setup.exe**.

Примечание Если во время загрузки приглашение на установку с DVD-диска не появилось, измените параметры BIOS компьютера

2. Выберите язык, время, формат валюты и раскладку клавиатуры. Во время установки доступна только одна раскладка. Если язык клавиатуры и язык устанавливаемой версии Windows Server 2008 различаются, при вводе с клавиатуры могут появляться не те символы, которых вы ожидаете. Чтобы избежать проблем, внимательно выбирайте язык клавиатуры. Когда будете готовы продолжать установку, щелкните кнопку **Далее (Next)**.
3. Щелкните **Установить (Install Now)**, чтобы начать установку. Если установка запущена из существующей ОС, подключенной к локальной сети или к Интернету, можно задать поиск обновлений во время установки. Щелкните команду **Выполнить подключение к Интернету для получения последних обновлений программы установки (Go Online to Get the Latest Updates for Installation)** или **Не загружать последние обновления программы установки (Do Not Get Latest Updates for Installation)**.
4. В корпоративных вариантах лицензирования Windows Server 2008 при установке операционной системы указывать ключ продукта не требуется. Если устанавливается не корпоративная версия, введите ключ продукта и щелкните **Далее (Next)**. По умолчанию установлен флажок **Автоматически активировать Windows при подключении к Интернету (Activate**

Windows When I'm Online), чтобы при подключении к Интернету появилось предложение активировать ОС.

Примечание После установки Windows Server 2008 необходимо выполнить активацию. Если этого не сделать в течение отведенного времени, появится сообщение о том, что разрешенный период работы без активации истек, или о том, что установлена нелицензированная версия Windows Server 2008. После этого система будет работать в режиме с ограниченной функциональностью. Чтобы вернуться в полнофункциональный режим, необходимо выполнить активацию.

5. На странице **Выберите операционную систему, которую следует установить (Select The Operating System You Want To Install)** выберите полную установку или установку ядра сервера и щелкните **Далее (Next)**.
6. В Windows Server 2008 лицензионное соглашение отличается от предыдущих версий Windows. Прочитав соглашение, установите **Я принимаю условия лицензии (I Accept the License Terms)** и щелкните **Далее (Next)**.
7. На странице **Выберите тип установки (Which Type Of Installation Do You Want)** выберите тип установки. Если нужно выполнить чистую установку, чтобы полностью заменить существующую ОС или установите Windows Server 2008 на компьютер без ОС, выберите в качестве типа установки **Полная установка (Дополнительные параметры) (Custom (Advanced))**. Если программа установки запущена с установочного DVD-диска, а не из Windows, вариант с обновлением будет недоступен. Если вам требуется обновить систему, а не устанавливать ее заново, перезагрузите компьютер, загрузите имеющуюся ОС и запустите программу установки из этой ОС.
8. На странице **Выберите раздел для установки Windows (Where Do You Want To Install Windows)** выберите диск или раздел, на который хотите установить ОС. Для установки потребуется от трех до восьми Гб дискового пространства. Существует две версии страницы **Выберите раздел для установки Windows (Where Do You Want To Install Windows)**, так что учитывайте следующее:
   - Если на компьютере установлен один жесткий диск с одним разделом, охватывающим весь диск, или с одной областью нераспределенного пространства, по умолчанию выбирается раздел, занимающий весь диск. Щелкните **Далее (Next)**, чтобы принять такой вариант и продолжить установку. Если диск еще не размечен, перед установкой необходимо создать раздел (подробнее об этом далее).
   - Если на компьютере установлено несколько дисков или один диск с несколькими разделами, необходимо выбрать или создать раздел, в который будет установлена операционная система.
   - Если диск не был инициализирован или BIOS компьютера не поддерживает запуск ОС с выбранного диска, необходимо выполнить инициализацию, создав на диске один или несколько разделов. Нельзя выбрать или отформатировать раздел с файловой системой FAT или

FAT32 и другими несовместимыми параметрами. Чтобы обойти эту проблему, преобразуйте раздел в NTFS. На этой странице можно открыть командную строку, чтобы выполнить необходимые действия (см. раздел «Выполнение дополнительных административных команд во время установки» этой главы).

9. Если в выбранном разделе уже установлена Windows, программа установки сообщит, что имеющиеся параметры пользователей и приложений будут перемещены в папку **Windows.old**, откуда их можно будет скопировать в новую систему. Щелкните **OK**.
10. Щелкните **Далее (Next)**, чтобы начать установку ОС. Программа установки скопирует полный образ диска Windows Server 2008 в указанный раздел, а затем развернет его. В зависимости от конфигурации компьютера и обнаруженных устройств будут установлены различные компоненты. Несколько раз произойдет автоматическая перезагрузка. Когда установка закончится, загрузится ОС, и на экране появится консоль **Задачи начальной настройки (Initial Configuration Tasks)** для начальной настройки сервера, например, для задания пароля администратора и имени сервера.

Установка с обновлением

Возможность обновления ОС при установке Windows Server 2008 несколько отличается от того, к чему все привыкли. Обновление, по сути, состоит в том, что программа установки все равно выполняет чистую установку ОС, а затем переносит в нее параметры пользователя, документы и приложения из предыдущей версии Windows.

В процессе переноса программа установки перемещает папки и файлы предыдущей системы в папку **Windows.old**, в результате чего старая система перестает запускаться. Перенос параметров выполняется потому, что в Windows Server 2008 информация о пользователях и приложениях хранится не так, как в предыдущих версиях.

Установка с обновлением выполняется следующим образом:

1. Запустите компьютер и войдите в систему под учетной записью с административными полномочиями. Вставьте установочный DVD-диск Windows Server 2008. Программа установки должна запуститься автоматически. Если этого не произошло, откройте диск в Проводнике и запустите программу **Setup.exe**.
2. Поскольку обновляется существующая ОС, вам не будет предложено выбрать язык, время, формат валюты и раскладку клавиатуры. Во время установки доступна только одна раскладка. Если язык клавиатуры и язык версии Windows Server 2008 различаются, при вводе текста могут появляться не те символы, которые нужны.
3. На следующей странице щелкните **Установить (Install Now)**. Затем укажите, нужно ли искать обновления во время установки.

4. В корпоративных вариантах лицензирования Windows Server 2008 при установке операционной системы указывать ключ продукта не требуется. Если устанавливается не корпоративная версия, введите ключ продукта и щелкните **Далее (Next)**. По умолчанию установлен флажок **Автоматически активировать Windows при подключении к Интернету (Activate Windows When I'm Online)**, чтобы при подключении к Интернету появилось предложение активировать операционную систему.
5. На странице **Выберите операционную систему, которую следует установить (Select The Operating System You Want To Install)** выберите полную установку или установку ядра сервера и щелкните **Далее (Next)**.
6. В Windows Server 2008 лицензионное соглашение отличается от предыдущих версий Windows. Прочитав соглашение, установите **Я принимаю условия лицензии (I Accept The License Terms)** и щелкните **Далее (Next)**.
7. На странице **Выберите тип установки (Which Type Of Installation Do You Want)** задайте установку с обновлением.
8. Начнется процесс установки. Поскольку выполняется обновление, вам не будет предложено выбрать место для установки. Программа установки скопирует на системный диск полный образ диска Windows Server 2008. Затем, в зависимости от конфигурации компьютера и обнаруженных устройств, будут установлены различные компоненты. В процессе этого несколько раз произойдет автоматическая перезагрузка. Когда установка закончится, загрузится операционная система, и на экране появится консоль **Задачи начальной настройки (Initial Configuration Tasks)** для начальной настройки сервера, например, для задания пароля администратора и имени сервера.

Выполнение дополнительных административных команд во время установки

Случается, что администратор забывает выполнить какую-то задачу перед запуском программы установки. В этом случае вам не нужно перезапускать операционную систему. Чтобы выполнить необходимые действия, откройте командную строку из программы установки или воспользуйтесь дополнительными параметрами дисков.

Использование командной строки во время установки

Обращаясь к командной строке из программы установки, вы фактически обращаетесь к среде MINWINPC, которая используется для установки ОС. В процессе установки открыть командную строку можно со страницы **Выберите раздел для установки Windows (Where Do You Want To Install Windows)**, нажав Shift+F10. Как показано в табл. 2-4, среда MINWINPC предоставляет доступ ко многим средствам командной строки, доступным в стандартном варианте Windows Server 2008.

Табл. 2-4. Утилиты командной строки, доступные в среде MINWINPC

Команда	Назначение
ARP	Отображение и изменение таблиц сопоставления IP-адресов и физических адресов для протокола ARP
ASSOC	Отображение и изменение программ, связанных с расширениями файлов
ATTRIB	Отображение и изменение атрибутов файлов
CALL	Вызов сценария или метки сценария как процедуры
CD/CHDIR	Отображение и изменение текущей папки
CHKDSK	Проверка диска на наличие ошибок и отображение отчета
CHKNTFS	Отображение состояния томов. Включает или исключает тома из автоматической системной проверки, выполняемой при запуске компьютера
CHOICE	Создание списка, из которого пользователи могут выбирать варианты при работе с пакетными сценариями
CLS	Очистка окна консоли
CMD	Запуск нового экземпляра окна командной строки
COLOR	Изменение цветов окна командной строки
CONVERT	Преобразование тома FAT в NTFS
COPY	Копирование или слияние файлов
DATE	Отображение и изменение системной даты
DEL	Удаление файлов
DIR	Отображение списка файлов и подпапок в папке
DISKPART	Управление дисками, разделами и томами при помощи собственной командной строки и внутренних команд DISKPART
DOSKEY	Редактирование командной строки, повторный вызов команд Windows и создание макросов
ECHO	Отображение сообщений, включение и выключение вывода на экран
ENDLOCAL	Завершает локализацию изменений переменных среды в пакетном файле
ERASE	Удаление файлов
EXIT	Выход из командного интерпретатора
EXPAND	Распаковка файлов
FIND	Поиск текстовой строки в файлах
FOR	Выполнение команды для каждого файла из указанного набора
FORMAT	Форматирование дисков

Табл. 2-4. (*продолжение*)

Команда	Назначение
FTYPE	Отображение или изменение зарегистрированных типов файлов
GOTO	Перевод интерпретатора команд Windows к строке сценария, имеющей указанную метку
HOSTNAME	Вывод на экран имени компьютера
IF	Обработка условия в пакетных программах
IPCONFIG	Отображение параметров TCP/IP
LABEL	Создание, изменение или удаление метки тома
MD/MKDIR	Создание папки или подпапки
MORE	Постраничное отображение выходных данных
MOUNTVOL	Управление точками подключения томов
MOVE	Перемещение файлов из одной папки в другую на том же диске
NBTSTAT	Отображение состояния NetBIOS
NET ACCOUNTS	Управление учетными записями пользователей и политиками паролей
NET COMPUTER	Добавление или удаление компьютеров домена
NET CONFIG SERVER	Отображение и изменение конфигурации службы сервера
NET CONFIG WORKSTATION	Отображение и изменение конфигурации службы рабочей станции
NET CONTINUE	Запуск приостановленной службы
NET FILE	Отображение открытых файлов сервера и управление ими
NET GROUP	Отображение глобальных групп и управление ими
NET LOCAL GROUP	Отображение учетных записей локальных групп и управление ими
NET NAME	Отображение и изменение получателей сообщений, отправляемых службой сообщений
NET PAUSE	Приостановка работы службы
NET PRINT	Отображение заданий и очередей печати и управление ими
NET SEND	Отправка сообщения через службу сообщений
NET SESSION	Вывод списка сеансов и с возможностью их завершения
NET SHARE	Отображение общих принтеров и папок и управление ими
NET START	Вывод списка сетевых служб и их запуск
NET STATISTICS	Отображение статистики рабочей станции и сервера

Табл. 2-4. (*продолжение*)

Команда	Назначение
NET TIME	Отображение и синхронизация сетевого времени
NET USE	Отображение удаленных подключений и управление ими
NET USER	Отображение локальных учетных записей и управление ими
NET VIEW	Отображение списка сетевых ресурсов или компьютеров
NETSH	Вызывает отдельную командную строку, позволяющую управлять конфигурацией различных сетевых служб на локальном и удаленных компьютерах
NETSTAT	Отображение состояния сетевых подключений
PATH	Отображение и изменение пути поиска исполняемых файлов в текущем окне командной строки
PATHPING	Отслеживание маршрутов и отображение информации о потере пакетов
PAUSE	Приостановка выполнения сценария до ввода данных с клавиатуры
PING	Проверка сетевого подключения
POPD	Переход в папку, сохраненную командой PUSHD
PRINT	Вывод текстового файла
PROMPT	Изменение формата приглашения командной строки Windows
PUSHD	Сохранение текущей папки и переход в новую
RD/RMDIR	Удаление папки
RECOVER	Восстановление информации с поврежденного диска
REG ADD	Добавление в реестр нового подраздела или параметра
REG COMPARE	Сравнение подразделов и параметров реестра
REG COPY	Копирование элемента реестра в указанный раздел на локальной или удаленной системе
REG DELETE	Удаление подраздела или параметра реестра
REG QUERY	Вывод списка параметров раздела и имен подразделов (если они имеются)
REG RESTORE	Запись сохраненных подразделов и параметров обратно в реестр
REG SAVE	Сохранение копий указанных подразделов, параметров и значений в файл
REGSVR32	Регистрация и отмена регистрации DLL
REM	Комментарий в сценарии
REN	Переименование файла

Табл. 2-4. (*окончание*)

Команда	Назначение
SET	Отображение и изменение переменных среды Windows. Также используется для вычислений в командной строке
SETLOCAL	Начало локализации изменений среды в пакетном файле
SFC	Просмотр и проверка защищенных системных файлов
SHIFT	Сдвиг позиции заменяемых параметров в сценарии
START	Запуск нового окна командной строки для выполнения заданной команды или программы
SUBST	Добавление новой буквы диска для указанного пути
TIME	Отображение или изменение системного времени
TITLE	Изменение заголовка окна командной строки
TRACERT	Отображение маршрута между компьютерами
TYPE	Отображение текстового файла
VER	Отображение версии Windows
VERIFY	Включение и выключение режима проверки правильности записи файлов на диск
VOL	Отображение метки и серийного номера тома

Принудительное удаление раздела диска во время установки

Во время установки вам иногда не удается выбрать тот жесткий диск, который вы хотите использовать. Это происходит, например, из-за того что раздел диска содержит недопустимое значение смещения байтов. Для решения этой проблемы придется удалить разделы диска (все данные на них будут уничтожены), а затем создать необходимый раздел, используя дополнительные параметры программы установки. Нераспознаваемые разделы диска удаляются на странице **Выберите раздел для установки Windows (Where Do You Want To Install Windows)**. Выполните следующие действия:

1. Нажмите Shift+F10, чтобы открыть командную строку.
2. В командной строке введите **diskpart**.
3. Чтобы просмотреть список дисков, введите команду **list disk**.
4. Выберите нужный диск командой **select disk НомерДиска**, где *НомерДиска* — номер диска, с которым вы будете работать.
5. Чтобы удалить разделы на выбранном диске, введите команду **clean**.
6. Когда удаление завершится, введите команду **exit**, чтобы выйти из утилиты **DiskPart**.
7. Введите команду **exit**, чтобы выйти из командной строки.
8. В диалоговом окне **Установка Windows (Install Windows)** щелкните кнопку **Назад (Back)**, чтобы вернуться в предыдущее окно.

9. На странице **Выберите тип установки (Which Type Of Installation Do You Want)** щелкните **Полная установка (Дополнительные параметры) (Custom (Advanced))**, чтобы начать установку.
10. На странице **Выберите раздел для установки Windows (Where Do You Want To Install Windows)** выберите диск, который только что очистили. Щелкните ссылку **Настройка диска (Disk Options)**, чтобы получить доступ к командам удаления, форматирования, создания и расширения разделов.
11. Выберите **Создать (New)**. В поле **Размер (Size)** введите размер раздела в мегабайтах и щелкните **Применить (Apply)**.

Загрузка драйверов дисков во время установки

Страница **Выберите раздел для установки Windows (Where Do You Want To Install Windows)** предоставляет возможность загрузить драйверы устройств для жестких дисков или их контроллеров. Эта полезно, когда диск, на который нужно установить ОС, недоступен из-за отсутствия драйвера.

Чтобы загрузить драйвер устройства и сделать диск доступным для установки, выполните следующие действия:

1. На странице **Выберите раздел для установки Windows (Where Do You Want To Install Windows)** щелкните **Загрузка драйвера (Load Drivers)**.
2. Дождавшись приглашения, вставьте установочный диск и щелкните **OK**. Программа установки выполнит поиск драйверов устройств.
   - Если найдено несколько драйверов, выберите нужный и щелкните **Далее (Next)**.
   - Если драйвер не найден, щелкните кнопку **Обзор (Browse)**, чтобы открыть диалоговое окно **Обзор папок (Browse For Folder)**, выберите драйвер вручную и щелкните **OK**. Затем щелкните **Далее (Next)**.

Можно также щелкнуть кнопку **Повторить (Rescan)**, чтобы повторно выполнить поиск драйверов. Если установить драйвер устройства не удалось, щелкните кнопку **Назад (Back)** в левом верхнем углу диалогового окна **Установка Windows (Install Windows)**, чтобы вернуться на предыдущую страницу.

Создание, форматирование, удаление и расширение разделов диска во время установки

Щелкнув кнопку **Настройка диска (Drive Options)** на странице **Выберите раздел для установки Windows (Where Do You Want to Install Windows)**, вы получите доступ к дополнительным параметрам:

- **Создать (New)** Создание раздела. Созданный раздел необходимо отформатировать.
- **Форматировать (Format)** Форматирование раздела, чтобы его можно было использовать для установки операционной системы.

- **Удалить (Delete)** Удаление раздела.
- **Расширить (Extend)** Расширение раздела с целью увеличения его размера.

Ниже описано, как использовать каждый из этих параметров.

Создание разделов во время установки

Создавая раздел, вы указываете его размер. Поскольку создать новый раздел можно только в нераспределенном пространстве, вам, возможно, придется удалить существующие разделы, чтобы создать новый раздел нужного размера. После создания раздела его можно сразу же отформатировать, чтобы создать на нем файловую систему, но для установки ОС это необязательно. Если вы зададите установку ОС на неформатированный раздел, программа установки сама отформатирует его.

Чтобы создать раздел, выполните следующие действия:

1. На странице **Выберите раздел для установки Windows (Where Do You Want To Install Windows)** щелкните **Настройка диска (Drive Options)**, чтобы получить доступ к дополнительным функциям по работе с дисками.
2. Укажите диск, на котором хотите создать раздел, и щелкните **Создать (New)**.
3. В поле **Размер (Size)** укажите размер раздела в мегабайтах, а затем щелкните **Применить (Apply)**, чтобы создать на выбранном диске новый раздел.

Форматирование разделов во время установки

При форматировании в разделе создается файловая система. Когда форматирование завершено, раздел можно использовать для хранения файлов и установки операционной системы. Помните, что при форматировании раздела уничтожаются хранящиеся в нем данные. Существующие разделы (не те, что были только что созданы) нужно форматировать только в случае, если требуется удалить все их содержимое и выполнить установку в пустой раздел.

Чтобы отформатировать раздел, выполните следующие действия:

1. На странице **Выберите раздел для установки Windows (Where Do You Want To Install Windows)** щелкните **Настройка диска (Drive Options)**, чтобы получить доступ к дополнительным функциям по работе с дисками.
2. Выберите раздел, который хотите форматировать.
3. Щелкните **Форматировать (Format)**. Появится окно, в котором нужно подтвердить форматирование. Щелкните **OK**, и программа установки отформатирует раздел.

Удаление разделов во время установки

Раздел, который больше не нужен, можно удалить. Место, которое занимал удаленный раздел, станет неразмеченным. Удаление раздела уничтожает все хранящиеся в нем данные. Обычно удалять разделы требуется только в случае, когда они имеют неверный формат или когда нужно объединить области свободного пространства на диске.

Чтобы удалить раздел, выполните следующее:

1. На странице **Выберите раздел для установки Windows (Where Do You Want To Install Windows)** щелкните **Настройка диска (Drive Options)**, чтобы получить доступ к дополнительным функциям по работе с дисками.
2. Выберите раздел, который хотите удалить.
3. Щелкните **Удалить (Delete)**. Появится окно, в котором нужно подтвердить удаление. Щелкните **OK**, и программа установки удалит раздел.

Расширение разделов диска во время установки

Для установки Windows Server 2008 требуется минимум 8 Гб дискового пространства. Если раздел слишком мал, его нельзя использовать для установки. Чтобы решить эту проблему, расширьте раздел за счет неразмеченного пространства на текущем диске. Существующие разделы можно расширять только в случае, если они отформатированы с использованием файловой системы NTFS 5.2 и выше. Новые разделы, созданные программой установки, также можно расширять, при условии что на диске есть нераспределенное пространство.

Чтобы расширить раздел, выполните следующие действия:

1. На странице **Выберите раздел для установки Windows (Where Do You Want To Install Windows)** щелкните **Настройка диска (Drive Options)**, чтобы получить доступ к дополнительным функциям по работе с дисками.
2. Выберите раздел, который хотите расширить.
3. Щелкните **Расширить (Extend)**. В поле **Размер (Size)** укажите размер раздела в мегабайтах и щелкните **Применить (Apply)**, чтобы расширить выбранный раздел.
4. Появится окно, в котором нужно подтвердить расширение. Щелкните **OK**, и программа установки расширит раздел.

Управление ролями, службами ролей и компонентами

Основной инструмент для управления ролями, службами ролей и компонентами — консоль **Диспетчер сервера (Server Manager)**. С ее помощью можно добавлять или удалять роли, службы ролей и компоненты, а также просматривать информацию о конфигурации и состоянии этих компонентов.

Ближе к реальности Утилита командной строки **ServerManagerCmd.exe** позволяет решать те же задачи, что и **Диспетчер сервера (Server Manager)**. Из командной строки с повышенными полномочиями можно получить подробные сведения о текущем состоянии сервера, относящиеся к ролям, службам ролей и компонентам, выполнив команду **servermanagercmd –query**. При этом будут перечислены все установленные роли, службы ролей и компоненты, а в квадратных скобках будут указаны имена, используемые для управления ими. Указав такое имя следом за параметром **–install** или **–remove**, вы установите или удалите соответствующую роль, службу ролей или компонент. Например, чтобы установить службу балансировки нагрузки на сеть, выполните команду **servermanagercmd –install nlb**. Добавьте параметр **–allSubFeatures**, чтобы установить все подчиненные службы ролей и компоненты.

Просмотр настроенных ролей и служб ролей

Чтобы диспетчер сервера отобразил список установленных ролей, щелкните узел **Роли (Roles)** в левой панели. В основном представлении узла **Роли (Roles)** отображается раздел **Сводка по ролям (Roles Summary)**, в котором указано количество установленных ролей и перечислены их имена (рис. 2-1). Если с ролью сервера связаны события-ошибки, диспетчер сервера отобразит слева от имени роли значок предупреждения.

В панели **Роли (Roles)** имя роли представляет собой ссылку, которую можно щелкнуть, чтобы получить об этой роли следующую информацию:

- Состояние связанных системных служб. Диспетчер сервера указывает количество служб, которые запущены или остановлены, например, **Системные службы: Выполняется 6, Остановлено 2 (System Services: 6 Running, 2 Stopped)**;
- События, сгенерированные связанными службами и компонентами за последние 24 часа, включая количество ошибок. Например, **2 ошибки, 8 предупреждений, 14 информационных за последние 24 часа (2 error(s), 8 warning(s), 14 informational in the last 24 hours)**;
- Количество и состояние установленных служб роли.

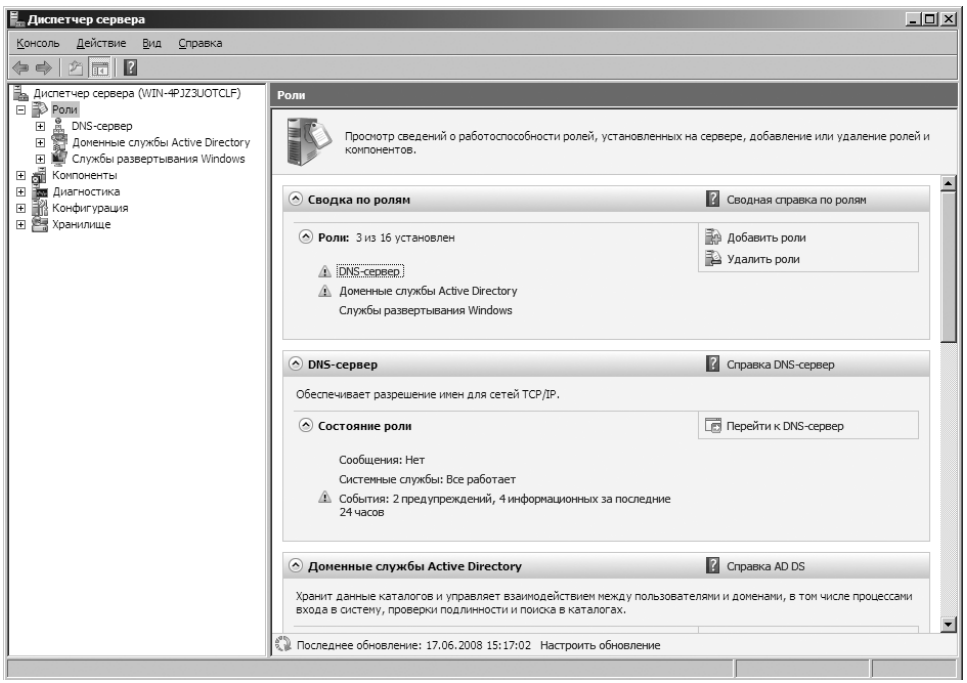


Рис. 2-1. Просмотр информации о состоянии установленных ролей

Совет По умолчанию диспетчер сервера обновляет информацию ежечасно, но обновление можно произвести и вручную, выбрав в меню **Действие (Action)** команду **Обновить (Refresh)**. Если хотите установить другой интервал обновления по умолчанию, щелкните ссылку **Настроить обновление (Configure Refresh)** в нижней части основной панели, задайте новый интервал обновления и щелкните **OK**.

Если в окне диспетчера сервера щелкнуть название роли в сводной информации, будут отображены более подробные сведения о событиях и службах соответствующей роли. Будут показаны все события за последние 24 часа. Если выбрать событие и щелкнуть **Свойства (View Event Properties)**, можно получить подробную информацию о событии. Кроме того, диспетчер сервера предоставляет сведения о системных службах, используемых ролью, и их состоянии. Чтобы управлять службой, щелкните ее имя и выполните команду **Остановить (Stop)**, **Пуск (Start)** или **Начать сначала (Restart)**. Во многих случаях, когда служба функционирует некорректно, проблему можно решить, воспользовавшись командой **Начать сначала (Restart)**. Подробнее о работе с событиями и системными службами рассказывается в главе 4.

Добавление и удаление ролей

Выделите узел **Роли (Roles)** в окне диспетчера сервера, чтобы отобразить на панели сведений информацию о ролях, которые установлены на сервере. В разделе **Сводка по ролям (Roles Summary)** имеются команды для добавления и удаления ролей.

Чтобы добавить роль сервера, выполните следующие действия:

1. Запустите диспетчер сервера, воспользовавшись значком на панели быстрого запуска, или выбрав команду **Пуск | Администрирование | Диспетчер сервера (Start | Administrative Tools | Server Manager)**.
2. В левой части окна диспетчера сервера выберите узел **Роли (Roles)**, после чего щелкните **Добавить роли (Add Roles)**. Запустится мастер добавления ролей. Если первой открылась страница **Перед началом работы (Before You Begin)**, прочитайте вводный текст и щелкните **Далее (Next)**. Чтобы в следующий раз эта страница не открывалась, установите флажок **Пропустить эту страницу по умолчанию (Skip This Page By Default)**.
3. На странице **Выбор ролей сервера (Select Server Roles)** выберите роль или роли, которые хотите установить. Если для установки роли требуются дополнительные компоненты, откроется диалоговое окно с их списком. Щелкните кнопку **Добавить требуемые компоненты (Add Required Features)**, чтобы закрыть это диалоговое окно и добавить требуемые компоненты. Два раза щелкните **Далее (Next)**.

Примечание Некоторые роли нельзя добавлять одновременно с другими ролями, поэтому их придется устанавливать отдельно. Также есть роли, которые нельзя сочетать с другими ролями. В этом случае на экране появится соответствующее предупреждение. При добавлении роли **Доменные службы Active Directory (Active Directory Domain Services)** компьютер не становится автоматически контроллером домена. Чтобы настроить сервер в качестве контроллера домена, необходимо запустить утилиту **DCPROMO.exe** (см. главу 7). Кроме того, если контроллер домена предполагается также использовать как DNS-сервер, Майкрософт рекомендует установить роль **Доменные службы Active Directory (Active Directory Domain Services)**, а затем при помощи утилиты DCPROMO настроить сервер в качестве DNS-сервера и контроллера домена. Сервер Windows Core Server может функционировать как контроллер домена, а также может содержать любое число ролей FSMO (Flexible Single Master Operations) для Active Directory.

4. Для каждой добавляемой роли будет открыта последовательность страниц, позволяющих настроить соответствующие службы ролей и все необходимые параметры. Выбирая или отменяя выбор служб ролей, помните о следующем:
   - Если вы выбрали службу роли, которой требуются дополнительные компоненты, появится диалоговое окно с их списком. Просмотрев список, щелкните кнопку **Добавить требуемые службы роли (Add Required Role Services)**, чтобы установить эти роли и закрыть диалоговое окно. Если вместо этого щелкнуть кнопку **Отмена (Cancel)**, программа установки отменит выбор компонента и не установит его.
   - Если вы пытаетесь удалить службу роли, которая необходима для работы другой службы роли, появится предупреждение о наличии зависимых служб, которые также придется удалить. В большинстве случаев предпочтительнее отменить удаление, чтобы сохранить зависимые службы. Если вы щелкните кнопку **Удалить службы зависимой роли (Remove Dependent Role Services)**, программа установки удалит зависимые службы, что может привести к сбою в работе сервера.
5. На странице **Подтвердите выбранные элементы (Confirm Installation Options)** щелкните ссылку **Печать, отправка по электронной почте или сохранение этих сведений (Print, E-Mail, Or Save This Information)**, чтобы создать отчет об установке и открыть его в Internet Explorer. После этого отчет можно сохранить или распечатать при помощи стандартных команд обозревателя. После просмотра и сохранения параметров установки щелкните **Установить (Install)**, чтобы начать процесс установки.
6. Когда установка выбранных компонентов завершится, откроется страница **Результаты установки (Installation Results)**. Просмотрите информацию об установке, чтобы убедиться, что все ее этапы прошли успешно. Если на каком-то этапе произошел сбой, выполните следующие действия:
   а) Открыв отчет в Internet Explorer, щелкните ссылку **Полное протоколирование (только для устранения неполадок) (Full Log**

(Troubleshooting Only)) в нижней части отчета, чтобы открыть файл журнала в Блокноте (Notepad).

б) Нажмите Ctrl+F, введите текущую дату в формате, заданном в системе (например, 2009-08-30), а затем щелкните кнопку **Найти далее (Find Next)**, чтобы найти первую запись с указанной датой.

в) Просмотрите записи диспетчера сервера о проблемах с установкой и примите соответствующие меры.

Чтобы удалить роль сервера, выполните следующие действия:

1. Запустите диспетчер сервера, воспользовавшись значком на панели быстрого запуска, или выбрав команду **Пуск | Администрирование | Диспетчер сервера (Start | Administrative Tools | Server Manager)**.
2. В левой части окна диспетчера сервера выберите узел **Роли (Roles)**, после чего щелкните **Удалить роли (Remove Roles)**. Запустится мастер удаления ролей. Если первой открылась страница **Перед началом работы (Before You Begin)**, прочитайте вводный текст и щелкните **Далее (Next)**. Чтобы в следующий раз эта страница не открывалась, установите флажок **Пропустить эту страницу по умолчанию (Skip This Page By Default)**.
3. На странице **Удаление ролей сервера (Remove Server Roles)** сбросьте флажок роли, которую хотите удалить, и щелкните **Далее (Next)**. Если от выбранной роли зависят другие роли, появится предупреждение о том, что эту роль нельзя удалить, не удалив также другие роли. Если щелкнуть кнопку **Удалить зависимую роль (Remove Dependent Role)**, программа установки удалит и зависимые роли.
4. На странице **Подтверждение выборов для удаления (Confirm Removal Selections)** просмотрите еще раз, какие службы ролей программа установки собирается удалить, и щелкните **Удалить (Remove)**.
5. Когда программа установки завершит изменение конфигурации сервера, появится страница **Результаты удаления (Removal Results)**. Просмотрите информацию об изменениях, чтобы убедиться в том, что все этапы процесса удаления прошли успешно. Если на каком-то этапе произошел сбой, выясните причину и выполните действия по решению этой проблемы, как описано выше.

Просмотр и изменение служб ролей

В диспетчере сервера можно просмотреть службы ролей для определенной роли, выбрав узел **Роли (Roles)** в левой панели и найдя раздел со сведениями о нужной роли. Там перечислены службы ролей, которые можно установить, и их состояние — **Установлено (Installed)** или **Не установлено (Not Installed)**. Для управления службами ролей используйте команды **Добавить службы ролей (Add Role Services)** и **Удалить службы ролей (Remove Role Services)** в разделе соответствующей роли. Некоторые роли не имеют отдельных служб, которыми можно управлять таким способом. В таких случаях можно только изменять роль сервера или удалять ее.

Чтобы добавить службы ролей, выполните следующие действия:

1. Запустите диспетчер сервера, воспользовавшись значком на панели быстрого запуска, или выбрав команду **Пуск | Администрирование | Диспетчер сервера (Start | Administrative Tools | Server Manager)**.
2. В левой панели диспетчера сервера выделите узел **Роли (Roles)** и найдите раздел с информацией о нужной роли. Щелкните **Добавить службы ролей (Add Role Services)**. Запустится мастер добавления служб ролей.
3. На странице **Выбор служб ролей (Select Role Services)** выберите в списке добавляемую службу роли. Установленные службы затенены, и выделить их нельзя. Закончив с выбором, щелкните **Далее (Next)** и **Установить (Install)**.

Чтобы удалить службы ролей, выполните следующие действия:

1. Запустите диспетчер сервера, воспользовавшись значком на панели быстрого запуска, или выбрав команду **Пуск | Администрирование | Диспетчер сервера (Start | Administrative Tools | Server Manager)**.
2. В левой панели диспетчера сервера выделите узел **Роли (Roles)** и найдите раздел с информацией о нужной роли. Щелкните **Удалить службы ролей (Remove Role Services)**. Запустится мастер удаления служб ролей.
3. На странице **Выбор служб ролей (Select Role Services)** программа установки выделит службы, установленные в данный момент. Чтобы удалить службу роли, сбросьте ее флажок. Если удаляется служба роли, от которой зависит другая служба роли, появится предупреждение, что удалить ее нельзя, не удалив также другую службу. Если щелкнуть кнопку **Удалить службы зависимой роли (Remove Dependent Role Service)**, будут удалены обе службы.
4. Закончив выбор удаляемых служб ролей, щелкните **Далее (Next)** и **Удалить (Remove)**.

Добавление и удаление компонентов Windows Server 2008

В предыдущих версиях Windows для добавления и удаления компонентов ОС использовался модуль **Установка компонентов Windows (Add/Remove Windows Components)** утилиты **Установка и удаление программ (Add Or Remove Programs)**. В Windows Server 2008 компоненты ОС добавляются и удаляются при помощи диспетчера сервера.

Чтобы добавить компоненты сервера, выполните следующие действия:

1. Запустите диспетчер сервера, воспользовавшись значком на панели быстрого запуска или выбрав команду **Пуск | Администрирование | Диспетчер сервера (Start | Administrative Tools | Server Manager)**.
2. В левой панели диспетчера сервера выделите узел **Компоненты (Features)** и щелкните **Добавить компоненты(Add Features),** чтобы запустить мастер добавления компонентов. Если откроется страница **Перед началом работы (Before You Begin)**, прочитайте вводный текст и щелк-

ните **Далее (Next)**. Чтобы в следующий раз эта страница не открывалась, установите флажок **Пропустить эту страницу по умолчанию (Skip This Page By Default)**.

3. На странице **Выбор компонентов (Select Features)** выберите компонент или компоненты, которые хотите установить. Если для установки компонента требуются дополнительные компоненты, появится диалоговое окно с их списком. Щелкните кнопку **Добавить требуемые компоненты (Add Required Features)**, чтобы закрыть это диалоговое окно и добавить необходимые компоненты.
4. Выбрав компоненты, которые хотите добавить, щелкните **Далее (Next)** и **Установить (Install)**.

Чтобы удалить компоненты сервера, выполните следующие действия:

1. Запустите диспетчер сервера, воспользовавшись значком на панели быстрого запуска или выбрав команду **Пуск | Администрирование | Диспетчер сервера (Start | Administrative Tools | Server Manager)**.
2. В левой панели диспетчера сервера выделите узел **Компоненты (Features)** и щелкните **Удалить компоненты (Remove Features)** чтобы запустить мастер удаления компонентов. Если откроется страница **Перед началом работы (Before You Begin)**, прочитайте вводный текст и щелкните **Далее (Next)**. Чтобы в следующий раз эта страница не открывалась, установите флажок **Пропустить эту страницу по умолчанию (Skip This Page By Default)**.
3. На странице **Выбор компонентов (Select Features)** перечислены компоненты, установленные в данный момент. Чтобы удалить компонент, сбросьте соответствующий флажок. Если попытаться удалить компонент, от которого зависит другой компонент, появится предупреждение, что этот компонент нельзя удалить, не удалив зависимый компонент. Если щелкнуть кнопку **Удалить зависимый компонент (Remove Dependent Feature)**, программа установки удалит оба компонента.
4. Выбрав компоненты, которые вы хотите удалить, щелкните **Далее (Next)** и **Удалить (Remove)**.

Глава 3

Управление сервером Windows Server 2008

Сервер — ключевое звено любой сети Microsoft Windows, и управление им — одна из основных обязанностей администратора. В комплект Windows Server 2008 включено несколько инструментов для управления сервером, в том числе, консоль **Задачи начальной настройки (Initial Configuration Tasks)** для первичного конфигурирования сервера и Диспетчер сервера (Server Manager) для решения основных задач системного администрирования. Консоль **Задачи начальной настройки (Initial Configuration Tasks)** удобна для оперативной настройки, но возможности ее ограничены. Диспетчер сервера, помимо функциональности окна **Задачи начальной настройки (Initial Configuration Tasks)**, включает также функции консоли **Управление компьютером (Computer Management)** и дополнительные возможности для управления ролями, компонентами и их параметрами . Вы будете использовать диспетчер сервера для решения широкого круга задач администрирования, в число которых входят:

- управление параметрами и конфигурацией сервера;
- управление сеансами пользователей и подключениями к серверам;
- управление использованием файлов, каталога и общих ресурсов;
- настройка административных уведомлений
- управление приложениями и сетевыми службами;
- настройка оборудования;
- просмотр и настройка дисков и сменных носителей.

Диспетчер сервера поможет вам в осуществлении общего администрирования системы, но для более детальной настройки свойств системного окружения предназначена утилита **Система (System)**. Она используется в следующих целях:

- изменение имени компьютера;
- настройка параметров производительности приложений, виртуальной памяти и реестра;
- управление системными и пользовательскими переменными среды;
- настройка параметров загрузки и восстановления системы.

Первичная настройка сервера

Консоль **Задачи начальной настройки (Initial Configuration Tasks)**, показанная на рис. 3-1, поможет быстро настроить новый сервер. Windows Server 2008 автоматически запускает эту консоль после завершения установки операционной системы. Если вы не хотите, чтобы консоль запускалась при каждом входе в систему, установите флажок **Не показывать это окно при входе в систему (Do Not Show This Window At Logon)** в ее левом нижнем углу. Если вы отменили автоматический запуск консоли или закрыли консоль и хотите снова открыть ее, щелкните кнопку **Пуск (Start)**, введите **oobe** в поле **Начать поиск (Search)** и нажмите **Enter**.

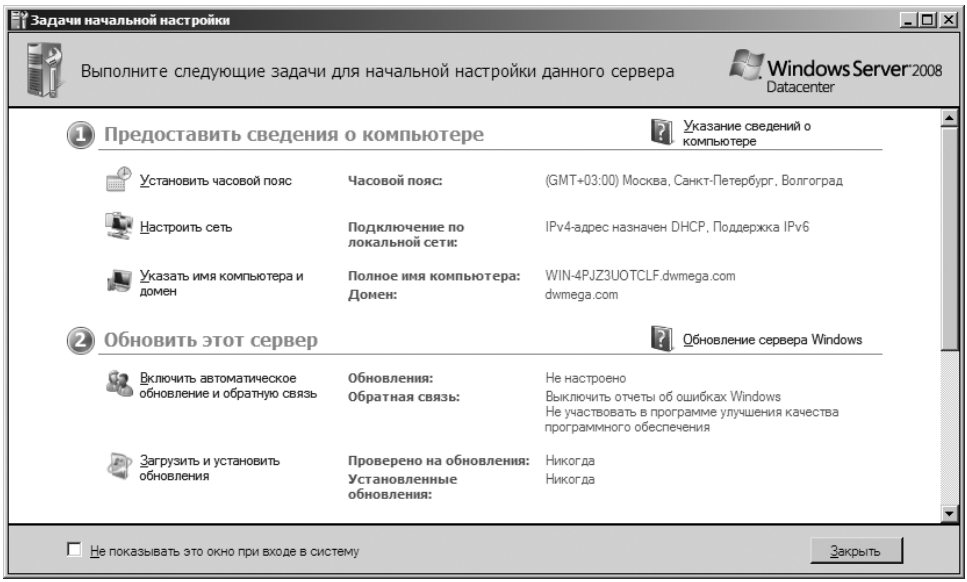


Рис. 3-1. Консоль Задачи начальной настройки (Initial Configuration Tasks) поможет быстро настроить новый сервер

Консоль **Задачи начальной настройки (Initial Configuration Tasks)** применяется для выполнения следующих настроек:

- **Установить часовой пояс (Set Time Zone)** Щелкнув эту ссылку, вы откроете диалоговое окно **Дата и время (Date And Time)**. Чтобы настроить часовой пояс сервера, щелкните кнопку **Изменить часовой пояс (Change Time Zone)**, выберите нужный пояс и дважды щелкните OK. Вы также можете открыть диалоговое окно **Дата и время (Date And Time)**, щелкнув правой кнопкой мыши часы в панели задач рабочего стола и выбрав команду **Настройка даты/времени (Adjust Date/Time)**. Хотя все серверы настроены на автоматическую синхронизацию с сервером времени в Интернете, процесс синхронизации не изменяет часовой пояс компьютера.
- **Настроить сеть (Configure Networking)** Щелкнув эту ссылку, вы откроете консоль **Сетевые подключения (Network Connections)**. Чтобы

настроить сетевое подключение, дважды щелкните его, щелкните кнопку **Свойства (Properties)** и задайте нужные параметры в открывшемся диалоговом окне. По умолчанию серверы настроены на использование динамической адресации как для IPv4, так и для IPv6. Вы также можете открыть консоль **Сетевые подключения (Network Connections)**, щелкнув ссылку **Управление сетевыми подключениями (Manage Network Connections)** в разделе **Задачи (Tasks)** окна **Центра управления сетями и общим доступом (Network And Sharing Center)**.

- **Указать имя компьютера и домен (Provide Computer Name And Domain)** С помощью этой ссылки вы откроете диалоговое окно **Свойства системы (System Properties)** на вкладке **Имя компьютера (Computer Name)**. Чтобы изменить имя компьютера и информацию о домене, щелкните кнопку **Изменить (Change)**, задайте имя компьютера и информацию о домене, затем щелкните **OK**. По умолчанию серверам назначается случайно выбранное имя, и они включаются в рабочую группу WORKGROUP. В классическом представлении панели управления вы можете открыть диалоговое окно **Свойства системы (System Properties)** на вкладке **Имя компьютера (Computer Name)**, дважды щелкнув значок **Система (System)** и затем щелкнув ссылку **Изменить параметры (Change Settings)** в разделе **Имя компьютера, имя домена и параметры рабочей группы (Computer Name, Domain, And Workgroup Settings)**.
- **Включить автоматическое обновление и обратную связь (Enable Automatic Updating And Feedback)** Используйте эту ссылку, чтобы разрешить автоматическое обновление Windows и обратную связь. По умолчанию на сервере автоматическое обновление не конфигурируются, но обратная связь разрешена. Это означает, что при помощи компонента **Отчеты об ошибках Windows (Windows Error Reporting)** в Майкрософт будут посылаться отчеты об ошибках. Эта информация посылается анонимно в рамках Программы улучшения качества программного обеспечения (Customer Experience Improvement Program). Майкрософт рекомендует включать все эти компоненты, чтобы серверы гарантированно получали обновления, а также в целях усовершенствования будущих версий ОС Windows.
- **Загрузить и установить обновления (Download And Install Updates)** Используйте эту ссылку, чтобы открыть утилиту **Центр обновления Windows (Windows Update)** панели управления, которая затем может быть использована для включения автоматического обновления (если оно выключено), либо для проверки наличия обновлений (если оно включено). По умолчанию автоматическое обновление выключено. В классическом представлении панели управления вы можете открыть **Центр обновления Windows (Windows Update)**, дважды щелкнув одноименный значок.
- **Добавить роли (Add Roles)** Используйте эту ссылку для запуска Мастера добавления ролей (Add Roles Wizard), который используется для

установки ролей на сервер. По умолчанию после установки на сервере роли не настроены. В **Диспетчере сервера (Server Manager)** команды для добавления или удаления ролей появляются при выборе узла **Роли (Roles)**.

- **Добавить компоненты (Add Features)** Используйте эту ссылку для запуска **Мастера добавления компонентов (Add Features Wizard)**. По умолчанию на сервере компоненты не устанавливаются. В **Диспетчере сервера (Server Manager)** команды для добавления или удаления при выборе узла **Компоненты (Features)**.
- **Включить удаленный рабочий стол (Enable Remote Desktop)** Используйте эту ссылку, чтобы открыть диалоговое окно **Свойства системы (System Properties)** на вкладке **Удаленное использование (Remote)**. Настройте **Удаленный рабочий стол (Remote Desktop)**, установив нужный переключатель, и щелкните **OK**. По умолчанию удаленные подключения к серверу запрещены. В классическом режиме панели представления, чтобы открыть диалоговое окно **Свойства системы (System Properties)** на вкладке **Удаленное использование (Remote)**, дважды щелкните значок **Система (System)** и выберите команду **Настройка удаленного доступа (Remote Settings)** в группе **Задачи (Tasks)**.
- **Настроить брандмауэр Windows (Configure Windows Firewall)** Используйте эту ссылку, чтобы открыть **Брандмауэр Windows (Windows Firewall)**. Чтобы настроить брандмауэр, щелкните ссылку **Изменить параметры (Change Settings)**. По умолчанию брандмауэр Windows включен. В классическом режиме панели представления, чтобы открыть окно **Брандмауэр Windows (Windows Firewall)**, дважды щелкните одноименный значок.

Примечание Здесь я лишь коротко представил эти возможности для первого знакомства с ними. Соответствующие настройки и технологии будут более подробно рассматриваться в этой главе и других главах книги.

Управление серверами

Консоль **Диспетчер сервера (Server Manager)** предназначена для выполнения основных задач системного администрирования. Вы проведете немало времени, работая с этим инструментом, и потому вам следует изучить его в подробностях. Откройте консоль **Диспетчер сервера (Server Manager)** одним из следующих способов:

- Щелкните кнопку **Пуск (Start)**, выберите команды **Администрирование (Administrative Tools)** и **Диспетчер сервера (Server Manager)**.
- Щелкните значок **Диспетчер сервера (Server Manager)** на панели быстрого запуска.

Как показано на рис. 3-2, главное окно диспетчера разделено на две панели, наподобие консоли **Управление компьютером (Computer Management)**.

Дерево консоли на левой панели используется для навигации и выбора инструментария. Узлы дерева разделены на пять основных категорий:

- **Роли (Roles)** Сведения о состоянии ролей, установленных на сервере, а также команды для управления ими. Для каждой установленной роли в дереве имеется собственный узел, выделив который вы определите состояние роли, просмотрите события, произошедшие за последние 24 часа, увидите список установленных и неустановленных служб роли, а также ссылки на ресурсы. Раскройте узел роли, чтобы получить доступ к инструментам для управления ею.
- **Компоненты (Features)** Сведения о состоянии компонентов, установленных на сервере, а также команды для управления ими. Установленные компоненты, добавляются в дерево диспетчера сервера.
- **Диагностика (Diagnostics)** Основные инструменты для управления службами и устройствами, мониторинга производительности и просмотра событий.
- **Конфигурация (Configuration)** Основные конфигурационные инструменты.
- **Хранилище (Storage)** Инструменты для управления устройствами хранения информации.

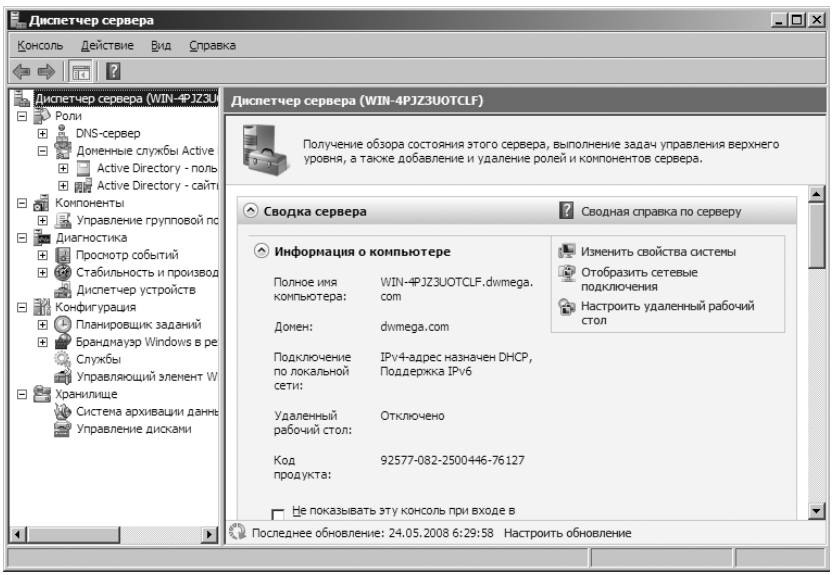


Рис. 3-2. Консоль Диспетчер сервера (Server Manager) предназначена для управления конфигурацией сервера

Правая панель — область сведений. Когда вы выбираете в левой панели узел самого верхнего уровня **Диспетчер сервера (Server Manager)**, на правой отображается обзор конфигурации сервера. В разделе **Информация о компьютере (Computer Information)** показаны имя компьютера, имя ра-

бочей группы или домена, сетевая конфигурация и код продукта. Также вы найдете здесь следующие ссылки:

- **Изменить свойства системы (Change System Properties)** Используйте эту ссылку, чтобы открыть диалоговое окно **Свойства системы (System Properties)**, в котором настраиваются основные параметры системы.
- **Отобразить сетевые подключения (View Network Connections)** Используйте эту ссылку, чтобы открыть консоль **Сетевые подключения (Network Connections)**, в которой настраиваются сетевые подключения.
- **Настроить удаленный рабочий стол (Configure Remote Desktop)** Используйте эту ссылку, чтобы открыть диалоговое окно **Свойства системы (System Properties)** на вкладке **Удаленное использование (Remote)**. Эта вкладка позволяет настроить параметры удаленного рабочего стола.

Примечание Эти и другие ссылки диспетчера сервера во многом сходны с аналогичными ссылками консоли **Задачи начальной настройки (Initial Configuration Tasks)**, поэтому здесь я описываю их довольно кратко. Соответствующие настройки и технологии будут более подробно рассматриваться в этой главе и других главах книги.

В разделе **Сведения системы безопасности (Security Information)** показаны состояние Брандмауэра Windows (Windows Firewall), конфигурация Центра обновления Windows (Windows Update), последнее время проверки и установки обновлений, а также состояние конфигурации усиленной безопасности Internet Explorer (Internet Explorer Enhanced Security Configuration). Вы найдете здесь следующие ссылки:

- **Перейти к брандмауэру Windows (Go To Windows Firewall)** Используйте эту ссылку для открытия панели **Брандмауэр Windows в режиме повышенной безопасности (Windows Firewall With Advanced Security)**, где вы зададите необходимые правила безопасности подключений, входящего и исходящего трафика.
- **Настроить обновления (Configure Updates)** Используйте эту ссылку, чтобы открыть Центр обновления Windows (Windows Update), который используется для включения автоматического обновления (если оно выключено) или проверки наличия обновлений вручную (если автоматическое обновление включено).
- **Проверить наличие новых ролей (Check For New Roles)** Используйте эту ссылку, чтобы проверить, не устанавливались ли на сервер новые роли с момента последнего обновления или перезапуска диспетчера сервера.
- **Запустить мастер настройки безопасности (Run Security Configuration Wizard)** Используйте эту ссылку, чтобы запустить Мастер настройки безопасности (Security Configuration Wizard), предназначенный для создания, редактирования, применения или отмены политик безопасности. Политики безопасности, описанные в главе 5, представляют собой один из способов настройки обширного набора параметров безопасности. Для

настройки безопасности сервера используются также шаблоны безопасности. Чтобы объединить преимущества двух этих методик, включите шаблон безопасности в файл политики безопасности.

- **Настроить конфигурацию усиленной безопасности Internet Explorer (Configure IE ESC)** Используйте эту ссылку, чтобы включить или выключить усиленную безопасность Internet Explorer (IE ESC). Щелкнув эту ссылку, вы сможете включить или выключить этот компонент для администраторов, пользователей или и тех, и других. При использовании конфигурации усиленной безопасности повышаются уровни для зон безопасности Internet Explorer, а также меняются настройки Internet Explorer по умолчанию. Благодаря IE ESC сервер менее подвержен потенциальным атакам. По умолчанию конфигурация IE ESC включена как для администраторов, так и для пользователей.

Ближе к реальности В большинстве случаев IE ESC на сервере следует включить как для пользователей, так и для администраторов. Правда, эта конфигурация сужает функциональность Internet Explorer. При этом зоны безопасности настраиваются следующим образом: зоне **Интернет (Internet)** назначается уровень **Высокий (High)**, зоне **Надежные узлы (Trusted Sites)** — уровень **Средний (Medium)**, зоне **Местная интрасеть (Local Intranet)** — **Ниже среднего** (Medium-Low), зоне **Ограниченные узлы (Restricted)** — **Высокий (High)**. Изменяются следующие параметры Internet Explorer: включено диалоговое окно **Конфигурация повышенной безопасности (Enhanced Security Configuration)**, надстройки браузера от сторонних разработчиков выключены, звуки на веб-страницах выключены, анимация на веб-страницах выключена, проверка подписи загружаемых программ включена, отзыв сертификата сервера включен, шифрованные страницы не сохраняются, временные файлы Интернета удаляются при закрытии браузера, предупреждения о переходе из безопасного режима в небезопасный включены, защита памяти включена.

В разделе **Сводка по ролям (Roles Summary)** перечислены роли, установленные на сервере. Здесь вы также найдете следующие ссылки:

- **Перейти к ролям (Go To Roles)** Открывает узел **Роли (Roles)** диспетчера сервера с подробными сведениями о каждой установленной роли.
- **Добавить роли (Add Roles)** Запускает Мастер добавления ролей (Add Roles Wizard), применяемый для установки ролей на сервере.
- **Удалить роли (Remove Roles)** Запускает Мастер удаления ролей (Remove Roles Wizard), применяемый для удаления ролей с сервера.

В разделе **Сводка компонентов (Features Summary)** представлены компоненты, установленные на сервере. Здесь вы также найдете следующие ссылки:

- **Добавить компоненты (Add Features)** Запускает Мастер добавления компонентов (Add Features Wizard), применяемый для установки компонентов на сервере.
- **Удалить компоненты (Remove Features)** Запускает Мастер удаления компонентов (Remove Features Wizard), применяемый для удаления компонентов с сервера.

В разделе **Ресурсы и поддержка (Resources And Support)** представлены текущие параметры программы улучшения качества программного обеспечения (Customer Experience Improvement Program) и отчетов об ошибках Windows (Windows Error Reporting). Помимо ссылок на соответствующие веб-сайты Майкрософт и команды для отправки отчета, вы найдете здесь следующие ссылки:

- **Участвовать в программе улучшения качества программного обеспечения (Configure CEIP)** Используйте эту ссылку для настройки параметров программы CEIP. Участие в ней позволяет Майкрософт получать информацию об использовании вашего сервера. Майкрософт собирает эти данные с целью усовершенствования будущих версий Windows. Ни в каких данных, собираемые в рамках программы CEIP, ни вы, ни ваша компания не идентифицируются. Решив поучаствовать в программе, вы также можете предоставить информацию о числе серверов и настольных компьютеров в вашей организации, а также описать сферу ее деятельности. Выключив компонент CEIP, вы упустите возможность помочь в улучшении Windows.
- **Включить отчеты об ошибках Windows (Configure Windows Error Reporting)** Используйте эту ссылку, чтобы изменить параметры отчетов об ошибках Windows (Windows Error Reporting, WER). В большинстве стоит включить отчеты об ошибках, по крайней мере, на первые два месяца после установки операционной системы. Отчеты об ошибках передаются с ваших серверов в Майкрософт, и вам предлагаются возможные решения проблемы. Чтобы просмотреть отчеты об ошибках и возможные решения, дважды щелкните значок **Отчеты о проблемах и решениях (Problem Reports And Solutions)** в классическом представлении панели управления.

Управление свойствами системы

Консоль **Система (System)** используется для просмотра информации о системе и выполнения основных действий по ее настройке. Чтобы открыть консоль **Система (System)** дважды щелкните одноименный значок в панели управления. Как показано на рис. 3-3, консоль **Система (System)** разделена на четыре основных области, в которых расположены ссылки для выполнения общих задач и обзора системы:

- **Издание Windows (Windows Edition)** Вариант и версия операционной системы. Дополнительно перечисляются установленные пакеты обновления.
- **Система (System)** Процессор, оперативная память и тип операционной системы, установленной на компьютере (32-разрядная или 64-разрядная).
- **Имя компьютера, имя домена и параметры рабочей группы (Computer Name, Domain, And Workgroup Settings)** Имя компьютера, его описа-

ние, домен и рабочая группа. Если вы хотите изменить что-либо из этого списка, щелкните ссылку **Изменить параметры (Change Settings)**, а затем щелкните кнопку **Изменить (Change)** в диалоговом окне **Свойства системы (System Properties)**.

- **Активация Windows (Windows Activation)** Показывает, произведена ли активация операционной системы, а также содержит код продукта. Если Windows Server 2008 еще не активирована, щелкните предоставленную ссылку, чтобы начать процесс активации, и следуйте указаниям. Чтобы изменить ключ продукта, щелкните ссылку **Изменить ключ продукта (Change Product Key)** и введите новый ключ.

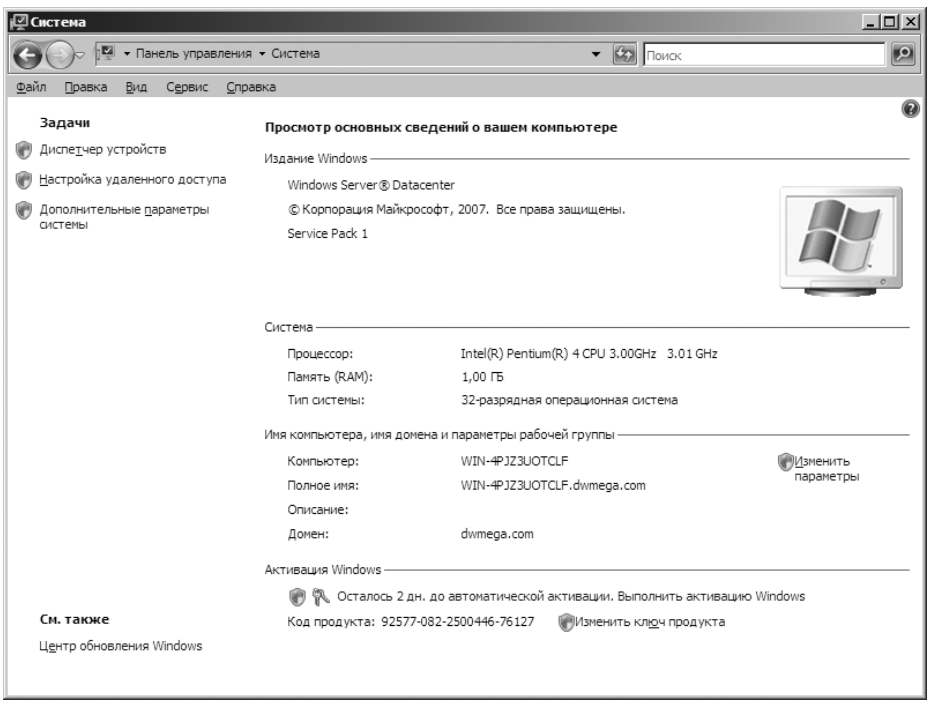


Рис. 3-3. Консоль Система (System) служит для просмотра и управления свойствами системы

Ссылки в левой панели консоли **Система (System)** предоставляют быстрый доступ к основным средствам обслуживания, включая следующие:

- **Диспетчер устройств (Device Manager)**;
- **Настройка удаленного доступа (Remote Settings)**;
- **Дополнительные параметры системы (Advanced System Settings)**.

Для версий Windows Server 2008, приобретенных по программам корпоративного лицензирования, как правило, не требуются ни активация, ни ключ продукта. Для розничных версий Windows Server 2008 необходимо и то, и другое. Если Windows Server 2008 не активирована, активируйте ее, щелкнув ссылку **Выполнить активацию Windows (Activate Windows Now)** в разделе **Активация Windows (Windows Activation)**.

В отличие от предыдущих версий Windows теперь вам разрешается изменить ключ продукта, введенный при установке, если это необходимо в соответствии с вашим планом лицензирования. Чтобы изменить ключ продукта, выполните следующие действия:

1. Дважды щелкните значок **Система (System)** в панели управления.
2. В разделе **Активация Windows (Windows Activation)** консоли **Система (System)** щелкните **Изменить ключ продукта (Change Product Key)**.
3. В окне **Активация Windows (Windows Activation)** введите ключ продукта.
4. Щелкните **Далее (Next)**. Ключ продукта пройдет проверку, после чего вам необходимо будет повторно активировать ОС.

Для управления свойствами системы применяется также диалоговое окно **Свойства системы (System Properties)**. Чтобы открыть его из консоли **Система (System)**, щелкните ссылку **Изменить параметры (Change Settings)** в разделе **Имя компьютера, имя домена и параметры рабочей группы (Computer Name, Domain, And Workgroup Settings)**. Далее рассматриваются основные области операционной системы, которые настраиваются при помощи диалогового окна **Свойства системы (System Properties)**.

Вкладка Имя компьютера (Computer Name)

Вкладка **Имя компьютера (Computer Name)** предназначена для просмотра и изменения сетевой идентификации компьютера. На ней показано полное имя системы и отражено ее членство в домене. По существу, полное имя компьютера — это его DNS-имя, которое также определяет положение компьютера в иерархии Active Directory. Если компьютер является контроллером домена или центром сертификации, изменить имя компьютера можно только после удаления соответствующей роли.

Чтобы включить компьютер в домен или группу, выполните следующие действия:

1. На вкладке **Имя компьютера (Computer Name)** диалогового окна **Свойства системы (System Properties)** щелкните кнопку **Изменить (Change)**. Откроется диалоговое окно **Изменение имени компьютера или домена (Computer Name/Domain Changes)**.
2. Чтобы включить компьютер в рабочую группу, выберите вариант **Рабочей группы (Workgroup)** и введите имя рабочей группы, в которую хотите включить компьютер.
3. Чтобы включить компьютер в домен, выберите вариант **Домена (Domain)** и введите имя домена, в который хотите включить компьютер.
4. Если вы изменили членство компьютера в домене, щелкнув **OK**, вы увидите сообщение службы безопасности Windows. Для добавления компьютера в домен или удаления компьютера из домена введите имя и пароль учетной записи с достаточными полномочиями и щелкните **OK**.

5. Получив сообщение о том, что компьютер включен в указанную рабочую группу или домен, щелкните **OK**.
6. На экране появится сообщение о необходимости перезагрузить компьютер. Щелкните **OK**.
7. Щелкните **Закрыть (Close)** и **Перезагрузить сейчас (Restart Now)**.

Чтобы изменить имя компьютера, выполните следующие действия:

1. На вкладке **Имя компьютера (Computer Name)** диалогового окна **Свойства системы (System Properties)** щелкните кнопку **Изменить (Change)**. Откроется диалоговое окно **Изменение имени компьютера или домена (Computer Name/Domain Changes)**.
2. Введите новое имя компьютера в поле **Имя компьютера (Computer Name)**.
3. На экране появится сообщение о необходимости перезагрузить компьютер. Щелкните **OK**.
4. Щелкните **Закрыть (Close)** и **Перезагрузить сейчас (Restart Now)**.

Вкладка Оборудование (Hardware)

Вкладка **Оборудование (Hardware)** диалогового окна **Свойства системы (System Properties)** предоставляет доступ к Диспетчеру устройств (Device Manager) и параметрам обновления драйверов Windows. **Диспетчер устройств (Device Manager)**, включенный в диспетчер сервера в качестве оснастки MMC, рассматривается далее в этой главе.

При подключении нового устройства Windows Server 2008 автоматически проверяет наличие драйвера, используя систему обновления Windows. Если вы не хотите, чтобы компьютер автоматически искал драйверы, щелкните кнопку **Поиск драйверов в Центре обновления Windows (Windows Update Driver Settings)** и установите нужный переключатель — **При подключении нового устройства спрашивать, надо ли выполнять поиск драйверов (Ask Me Each Time I Connect A New Device Before Checking For Drivers)** или **Не выполнять поиск драйверов при подключении новых устройств (Never Check For Drivers When I Connect A Device)**. Затем щелкните **OK**.

Примечание Вкладка **Оборудование (Hardware)** более не предоставляет доступ к настройкам подписи драйвера или профилям оборудования. Начиная с Windows Server 2008, конфигурирование параметров подписи драйвера производится с помощью групповой политики Active Directory или локальной групповой политики. Настройка профилей оборудования отменена, поскольку Windows Server 2008 использует аппаратно-независимую архитектуру. Вы по-прежнему вольны разрешать или запрещать системные службы для определенных аппаратных конфигурации в процессе устранения проблем, однако утилита **Конфигурация системы (System Configuration)** предоставляет больше возможностей для управления поведением ОС при загрузке. Она открывается командой из меню **Администрирование (Administrative Tools)**. Ее использование описано в главе 2 книги *«Microsoft Windows Vista. Справочник администратора (Русская Редакция, БХВ-Петербург, 2008)»*.

Вкладка Дополнительно (Advanced)

На вкладке **Дополнительно (Advanced)** диалогового окна **Система (System)** осуществляется управление многими ключевыми возможностями ОС Windows, включая производительность, использование виртуальной памяти, профили пользователя, переменные среды, загрузку и восстановление.

Настройка быстродействия Windows

В интерфейс Windows Server 2008 добавлено много графических усовершенствований, включающих визуальные эффекты для меню, панелей инструментов и панели задач. Чтобы настроить производительность Windows, выполните следующие действия:

1. Перейдите на вкладку **Дополнительно (Advanced)** диалогового окна **Свойства системы (System Properties)** и щелкните кнопку **Параметры (Settings)** в разделе **Быстродействие (Performance)**. Откроется диалоговое окно **Параметры быстродействия (Performance Options)**.
2. Перейдите на вкладку **Визуальные эффекты (Visual Effects)**. Вам доступны следующие варианты управления визуальными эффектами:
   - **Восстановить значения по умолчанию (Let Windows Choose What's Best For My Computer)** ОС сама выберет параметры производительности на основании конфигурации оборудования. На современных компьютерах этот вариант, скорее всего, будет идентичен варианту **Обеспечить наилучший вид (Adjust For Best Appearance)**. Ключевое различие состоит в том, что этот вариант все-таки выбирается Windows на основании доступного оборудования и его возможностей.
   - **Обеспечить наилучший вид (Adjust For Best Appearance)** Включаются все визуальные эффекты для всех графических интерфейсов. В меню и панели задач используются переходы и тени. У экранных шрифтов сглажены углы. В раскрывающихся списках используется плавная прокрутка, в папках — веб-представление и пр.
   - **Обеспечить наилучшее быстродействие (Adjust For Best Performance)** Выключаются все визуальные эффекты, интенсивно потребляющие ресурсы компьютера, например, плавные переходы и сглаженные углы для шрифтов. Базовый набор визуальных эффектов остается включенным.
   - **Особые эффекты (Custom)** Все визуальные эффекты включаются и выключаются индивидуально. Если вы отмените все варианты, Windows не будет использовать визуальные эффекты.
3. Закончив настройку визуальных эффектов, щелкните **Применить (Apply)**. Затем два раза щелкните **OK**, чтобы закрыть открытые диалоговые окна.

Настройка производительности приложений

Производительность приложения связана с параметрами кеша процессора, заданными в системе Windows Server 2008. Параметры распределения времени процессора определяют быстродействие приложений, которые выполняются интерактивно (в отличие от фоновых приложений, например, служб). Чтобы изменить производительность приложений, выполните следующие действия:

1. Перейдите на вкладку **Дополнительно (Advanced)** диалогового окна **Свойства системы (System Properties)** и щелкните кнопку **Параметры (Settings)** в разделе **Быстродействие (Performance)**. Откроется диалоговое окно **Параметры быстродействия (Performance Options)**.
2. В диалоговом окне **Параметры быстродействия (Performance Options)** перейдите на вкладку **Дополнительно (Advanced)**.
3. В разделе **Распределение времени процессора (Processor Scheduling)** вам доступны следующие варианты оптимизации:
   - **Программ (Programs)** Обеспечивает наилучшее время отклика и максимальную долю доступных ресурсов интерактивным приложениям. Как правило, этот вариант нужно использовать на рабочих станциях под управлением Windows Server 2008.
   - **Служб, работающих в фоновом режиме (Background Services)** Обеспечивает быстрое время отклика фоновым приложениям. Этот вариант надлежит использовать на серверах Windows Server 2008, то есть, на компьютерах, на которых установлены серверные роли и которые не используются как рабочие станции.
4. Щелкните **OK**.

Настройка виртуальной памяти

Виртуальная память позволяет расширить объем доступной оперативной памяти (RAM) за счет дискового пространства. Эта возможность впервые появилась в процессорах Intel 386. Запись содержимого RAM на диски называется подкачкой. Определенный объем памяти, скажем, 1024 Мб, записывается на диск в виде файла. При необходимости обращения к нему чтение осуществляется с диска, а не из физической RAM.

Исходный файл подкачки автоматически создается на диске, содержащем операционную систему. По умолчанию на других дисках файлов подкачки нет. Если они нужны, вам придется создать их вручную. Создавая файл подкачки, вы задаете начальный и максимальный размеры. Файлы подкачки записываются на том под именем PAGEFILE.SYS.

Ближе к реальности Windows Server 2008 автоматически управляет виртуальной памятью гораздо лучше, чем ее предшественницы. Обычно Windows Server 2008 выделяет виртуальную память в объеме не менее общего объема оперативной памяти, установленной на компьютере. Это гарантирует, что файлы подкачки не будут фрагментироваться (фрагментация снижает производительность системы). Управляя виртуальной памятью вручную, в большинстве случаев вы будете использовать фиксированный размер виртуальной памяти, для чего начальному и максимальному размеру файла подкачки нужно присвоить одно и то же значение. Это гарантирует, что данные подкачки будут записаны в одном непрерывном файле (если на томе достаточно свободного пространства). Для компьютеров с объемом RAM 8 Гб или менее я рекомендую задавать общий размер файла подкачки в два раза больше объема физической памяти системы. Например, на компьютере с 1024 Мб оперативной памяти присвойте параметру **Общий объем файла подкачки на всех дисках (Total Paging File Size For All Drives)** значение не менее 2048 Мб. На системах с памятью более 8 Гб следуйте рекомендациям производителя оборудования. Обычно это означает, что размер файла подкачки должен равняться объему физической памяти.

Чтобы вручную сконфигурировать виртуальную память, выполните следующие действия:

1. Перейдите на вкладку **Дополнительно (Advanced)** диалогового окна **Свойства системы (System Properties)** и щелкните кнопку **Параметры (Settings)** в разделе **Быстродействие (Performance)**. Откроется диалоговое окно **Параметры быстродействия (Performance Options)**.
2. В диалоговом окне **Параметры быстродействия (Performance Options)** перейдите на вкладку **Дополнительно (Advanced)**. Щелкните кнопку **Изменить (Change)**, чтобы открыть диалоговое окно **Виртуальная память (Virtual Memory)**, показанное на рис. 3-4. На нем представлена следующая информация:
   - **Диск [Метка тома] (Drive [Volume Label]) и Файл подкачки (Мб) (Paging File Size (MB))** Текущие параметры виртуальной памяти. Каждый том выводится с соответствующим файлом подкачки (если он присутствует). Диапазон указывает значения начального и максимального размера, заданные для файла подкачки.
   - **Размер файла подкачки для каждого диска (Paging File Size For Each Drive)** Здесь показаны сведения по выбранному диску, и задаются размеры файла подкачки на нем. В поле **Свободно (Space Available)** показано, сколько пространства доступно на диске.
   - **Общий объем файла подкачки на всех дисках (Total Paging File Size For All Drives)** Рекомендуемый для системы размер виртуальной памяти и реальный объем, выделенный в данный момент. Если вы впервые настраиваете виртуальную память, обратите внимание, что файл рекомендуемого размера уже есть на системном диске (в большинстве случаев).

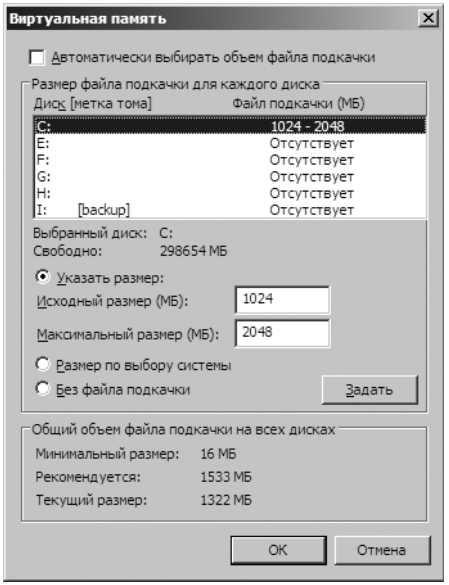


Рис. 3-4. Виртуальная память увеличивает объем оперативной памяти системы

3. По умолчанию Windows Server 2008 управляет размером файла подкачки для всех дисков. Чтобы настроить виртуальную память вручную, сбросьте флажок **Автоматически выбирать объем файла подкачки (Automatically Manage Paging File Size For All Drives)**.
4. В списке **Диск (Drive)** выберите том, с которым хотите работать.
5. Установите переключатель **Указать размер (Custom Size)** и заполните поля **Исходный размер (Initial Size)** и **Максимальный размер (Maximum Size)**.
6. Щелкните кнопку **Задать (Set)** для сохранения изменений.
7. Повторите шаги 4–6 для каждого тома, который хотите сконфигурировать.

Примечание Файл подкачки также используется в целях отладки, если в системе возникает ошибка STOP. Если файл подкачки на системном диске оказался меньше, чем нужно для записи отладочной информации, эта функция будет отключена. Если вы хотите использовать отладку, установите минимальный размер, равный объему памяти системы. Например, в системе с оперативной памятью объемом 1 Гб потребуется файл подкачки размером 1 Гб на системном диске.

8. Щелкните **OK**. Если на экране появится сообщение о перезаписи существующего файла PAGEFILE.SYS, щелкните **Да (Yes)**.
9. Если вы обновили настройки файла подкачки, который используется в данный момент, на экране появится сообщение о том, что изменения вступят в силу после перезагрузки системы. Щелкните **OK**.
10. Дважды щелкните OK, чтобы закрыть открытые диалоговые окна. Закрывая окно **Система (System)**, вы увидите сообщение с запросом, хотите ли вы перезапустить систему. Щелкните **Перезагрузить (Restart)**.

Чтобы Windows Server 2008 автоматически управляла виртуальной памятью, выполните следующие действия:

1. Перейдите на вкладку **Дополнительно (Advanced)** диалогового окна **Свойства системы (System Properties)** и щелкните кнопку **Параметры (Settings)** в разделе **Быстродействие (Performance)**. Откроется диалоговое окно **Параметры быстродействия (Performance Options)**.
2. В диалоговом окне **Параметры быстродействия (Performance Options)** перейдите на вкладку **Дополнительно (Advanced)**. Щелкните кнопку **Изменить (Change)**, чтобы открыть диалоговое окно **Виртуальная память (Virtual Memory)**.
3. Установите флажок **Автоматически выбирать объем файла подкачки (Automatically Manage Paging File Size For All Drives)**.
4. Трижды щелкните **OK**, чтобы закрыть открытые диалоговые окна.

Примечание Если вы обновили настройки файла подкачки, который используется в данный момент, на экране появится сообщение о том, что изменения вступят в силу после перезагрузки системы. Щелкните **OK**. Закрывая окно **Система (System)**, вы увидите сообщение с запросом, хотите ли вы перезапустить систему. Щелкните **Перезагрузить (Restart)**. На рабочем сервере выполняйте перезагрузку в нерабочие часы.

Предотвращение выполнения данных

Технология предотвращения выполнения данных (Data Execution Prevention, DEP) предназначена для защиты памяти. Она указывает процессору отметить все адреса памяти в приложении как неисполняемые, если они явным образом не содержат исполняемый код. Когда производится попытка выполнить код из страницы памяти, которая помечена как неисполняемая, процессор вызывает исключение и предотвращает выполнение. Это не дает вредоносному коду, например, вирусу, разместиться в большинстве областей памяти.

Примечание В 32-разрядных версиях Windows поддерживается реализация DEP, определенная в процессорах корпорации Advanced Micro Devices (AMD) в виде функции NX (no-execute page-protection). Такие процессоры поддерживают соответствующие инструкции и должны работать в режиме PAE (Physical Address Extension). Функция NX поддерживается и в 64-разрядных версиях Windows.

Использование и конфигурирование DEP Чтобы выяснить, поддерживает ли компьютер DEP, воспользуйтесь утилитой **Система (System)**:

1. Перейдите на вкладку **Дополнительно (Advanced)** диалогового окна **Свойства системы (System Properties)** и щелкните кнопку **Параметры (Settings)** в разделе **Быстродействие (Performance)**, чтобы открыть диалоговое окно **Параметры быстродействия (Performance Options)**.
2. В диалоговом окне **Параметры быстродействия (Performance Options)** перейдите на вкладку **Предотвращение выполнения данных (Data Execution Prevention)**. В нижней части вкладки указано, поддерживает ли компьютер DEP.

3. Если компьютер поддерживает DEP, настройте ее при помощи следующих вариантов:
   - **Включить DEP только для основных программ и служб Windows (Turn On DEP For Essential Windows Programs And Services Only)** Этот вариант задан по умолчанию и рекомендуется для компьютеров, которые поддерживают предотвращение выполнения данных.
   - **Включить DEP для всех программ и служб, кроме выбранных ниже (Turn On DEP For All Programs Except Those I Select)** Позволяет определить исключения. Выберите этот переключатель, затем щелкните кнопку **Добавить (Add)**, чтобы указать программы, которые должны исполняться без предотвращения выполнения данных.
4. Щелкните **OK**.

Если вы включили DEP и разрешили исключения, то можете добавлять или удалять программы в списке исключений, выполнив следующие действия:

1. Перейдите на вкладку **Дополнительно (Advanced)** диалогового окна **Свойства системы (System Properties)** и щелкните кнопку **Параметры (Settings)** в разделе **Быстродействие (Performance)**, чтобы открыть диалоговое окно **Параметры быстродействия (Performance Options)**.
2. В диалоговом окне **Параметры быстродействия (Performance Options)** перейдите на вкладку **Предотвращение выполнения данных (Data Execution Prevention)**.
3. Чтобы добавить программу-исключение, щелкните кнопку **Добавить (Add)**, найдите исполняемый файл программы и щелкните **Открыть (Open)**.
4. Чтобы временно отменить исключение для программы (это может потребоваться при выявлении проблем), сбросьте флажок рядом с ее именем.
5. Чтобы удалить программу из списка исключений, выделите название программы и щелкните **Удалить (Remove)**.
6. Щелкните **OK**, чтобы сохранить изменения.

Совместимость с DEP Чтобы быть совместимыми с DEP, приложения должны уметь явно отмечать память как выполняемую. Приложения, неспособные это делать, несовместимы с функцией процессора NX. Если при выполнении приложений вы испытываете проблемы с памятью, выясните, с какими приложениями они возникают, и настройте их как исключения, вместо того чтобы полностью отказываться от предотвращения выполнения данных. При этом вы сохраните достоинства защиты памяти и выборочно запретите ее для программ, которые некорректно работают с функцией NX.

Защита выполнения применяется как к программам пользовательского режима, так и к программам режима ядра. В пользовательском режиме попытка выполнения данных приводит к исключению STATUS_ACCESS_VIOLATION. В большинстве процессов это исключение не будет обработано, что приведет к завершению процесса. Такое поведение вполне оправдано,

поскольку большинство программ, нарушающих данное правило, являются вредоносными, например, вирусами или червями.

В отличие от приложений, выборочно включить или выключить защиту от выполнения данных для драйверов устройств режима ядра нельзя. Кроме того, на совместимых 32-разрядных системах предотвращение выполнения по умолчанию применяется к стеку памяти. На совместимых 64-разрядных системах, предотвращение выполнения по умолчанию применяется к стеку памяти, выгружаемому пулу и пулу сеансов. Попытка выполнения данных в режиме ядра для драйвера устройства приведет к исключению ATTEMPTED_EXECUTE_OF_NOEXECUTE_MEMORY.

Настройка системных и пользовательских переменных среды

В Windows переменные среды используются для хранения важных текстовых данных, например, путей, по которым расположены файлы, или имя хоста контроллера домена. Переменные среды, используемые ОС Windows — они называются системными переменными — всегда одни и те же независимо от того, кто зарегистрировался на компьютере. Переменные среды, предназначенные для пользователей и программ, называются пользовательскими переменными и различны для каждого пользователя компьютера.

Системные и пользовательские переменные среды настраиваются при помощи диалогового окна **Переменные среды (Environment Variables)**, показанного на рис. 3-5. Чтобы открыть его, откройте диалоговое окно **Свойства системы (System Properties)**, перейдите на вкладку **Дополнительно (Advanced)** и щелкните кнопку **Переменные среды (Environment Variables)**.

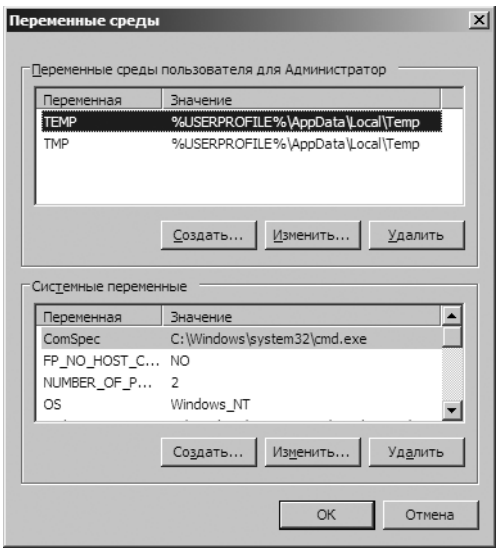


Рис. 3-5. Настройка системных и пользовательских переменных среды

Создание переменной среды Чтобы создать переменную среды, выполните следующие действия:

1. Щелкните кнопку **Создать (New)** в разделе **Переменные среды пользователя (User Variables)** или **Системные переменные (System Variables)**. Будет открыто диалоговое окно **Новая пользовательская переменная (New User Variable)** или **Новая системная переменная (New System Variable)**.
2. В поле **Имя переменной (Variable Name)** введите имя переменной. В поле **Значение переменной (Variable Value)** введите ее значение.
3. Щелкните **OK**.

Редактирование переменной окружения Чтобы изменить существующую переменную среды, выполните следующие действия:

1. Выберите переменную в списке **Переменные среды пользователя (User Variables)** или **Системные переменные (System Variables)**.
2. Щелкните кнопку **Изменить (Edit)**. Откроется диалоговое окно **Изменить пользовательскую переменную (Edit User Variable)** или **Изменить системную переменную (Edit System Variable)**.
3. Введите новое значение в поле **Значение переменной (Variable Value)** и щелкните **OK**.

Удаление переменной окружения Чтобы удалить переменную окружения, выделите ее и щелкните кнопку **Удалить (Delete)**.

Примечание Вновь созданные или измененные системные переменные среды вступают в силу после перезапуска компьютера. Вновь созданные или измененные пользовательские переменные среды вступают в силу при следующей регистрации пользователя в системе.

Настройка загрузки и восстановления системы

Настройка загрузки и восстановления системы производится в диалоговом окне **Загрузка и восстановление (Startup and Recovery)**, показанном на рис. 3-6. Чтобы открыть его, откройте диалоговое окно **Свойства системы (System Properties)**, перейдите на вкладку **Дополнительно (Advanced)** и щелкните кнопку **Параметры (Settings)** в разделе **Загрузка и восстановление (Startup and Recovery)**.

Установка параметров загрузки Параметры раздела **Загрузка операционной системы (System Startup)** диалогового окна **Загрузка и восстановление (Startup And Recovery)** управляют загрузкой системы. Чтобы задать ОС по умолчанию на компьютере с несколькими загружаемыми ОС, выберите одну из системы, перечисленных в списке **Операционная система, загружаемая по умолчанию (Default Operating System)**. Тем самым вы измените настройку диспетчера загрузки Windows (Windows Boot Manager).

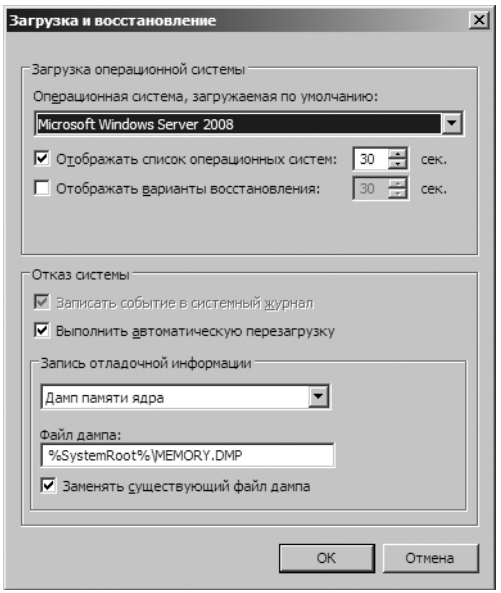


Рис. 3-6. Настройка параметров загрузки и восстановления

При загрузке компьютера с несколькими ОС Windows Server 2008 по умолчанию выводит меню загрузки на 30 секунд. Вы можете изменить это время одним из перечисленных способов:

- Чтобы немедленно загружать операционную систему по умолчанию, сбросьте флажок **Отображать список операционных систем (Time To Display List Of Operating Systems)**.
- Чтобы задать время отображения списка загружаемых ОС, установите флажок **Отображать список операционных систем (Time To Display List Of Operating Systems)** и задайте временную задержку в секундах.

В большинстве систем достаточно задержки от трех до пяти секунд. Этого достаточно, чтобы принять решение, и в то же время достаточно мало, чтобы не задерживать процесс загрузки системы.

При загрузке системы в режиме восстановления можно отобразить список параметров восстановления. Как и в случае обычной загрузки, настройка параметров восстановления осуществляется одним из двух способов. Вы можете задать немедленную загрузку компьютера, сбросив флажок **Отображать варианты восстановления (Time To Display Recovery Options When Needed)**, или указать время отображения вариантов, установив флажок **Отображать варианты восстановления (Time To Display Recovery Options When Needed)** и задав задержку в секундах.

Установка параметров восстановления Восстановлением системы вы управляете при помощи разделов **Отказ системы (System Failure)** и **Запись отладочной информации (Write Debugging Information)** диалогового окна **Загрузка и восстановление (Startup And Recovery)**. Параметры восстанов-

ления применяются для задания действий в случае возникновения системной ошибки STOP. Параметры, доступные в разделе **Отказ системы (System Failure)** перечислены ниже:

- **Записать событие в системный журнал (Write An Event To The System Log)** Ошибка записывается в системный журнал, что позволяет администратору впоследствии просмотреть ее при помощи консоли **Просмотр событий (Event Viewer)**.
- **Выполнить автоматическую перезагрузку (Automatically Restart)** Выберите этот параметр, чтобы система автоматически перезагружалась при возникновении фатальной системной ошибки.

Примечание Автоматическая перезагрузка — не всегда оптимальный выбор. Иногда желательно, чтобы система осталась в нерабочем состоянии, а не перезагрузилась, чтобы ей с гарантией было уделено должное внимание. В противном случае вы узнаете о перезагрузке системы, только просмотрев системные журналы, если, конечно, вам не посчастливилось в момент перезагрузки находиться у монитора системы.

В списке **Запись отладочной информации (Write Debugging Information)** выберите тип отладочной информации, которую хотите записать в файл дампа. Позже его можно будет использовать для диагностики системных ошибок. Варианты перечислены ниже:

- **Нет (None)** Используйте этот вариант, чтобы не записывать отладочную информацию.
- **Малый дамп памяти (Small Memory Dump)** Будет записан только дамп сегмента физической памяти, в котором произошла ошибка. Его размер — 64 Кб.
- **Дамп памяти ядра (Kernel Memory Dump)** Будет записан дамп области физической памяти, используемой ядром Windows. Размер дампа зависит от размера ядра Windows.

Выбрав запись файла дампа, вы также должны задать его расположение. По умолчанию малые дампы записываются в папку %SystemRoot%\Minidump, а остальные дампы в папку %SystemRoot%\MEMORY.DMP. Обычно стоит также установить флажок **Заменять существующий файл дампа (Overwrite Any Existing File)**, чтобы существующие файлы дампов перезаписывались при возникновении новой ошибки STOP.

Ближе к реальности Создать файл дампа можно только в том случае, если система настроена должным образом. На системном диске должен находиться файл подкачки достаточно большого размера (раньше мы говорили о том, как задать размер виртуальной памяти), а на диске, куда сохраняется файл дампа, должно быть достаточно свободного места. Например, на моем сервере установлено 4 Гб оперативной памяти, что требует файла подкачки на системном диске того же размера — 4 Гб. Определив базовый уровень использования памяти ядра, я обнаружил, что сервер использует от 678 до 892 Мб памяти ядра. Поскольку для файла дампа используется тот же диск, на нем должно быть не менее 5 Гб свободного пространства для создания дампа отладочной информации (4 Гб для файла подкачки и около 1 Гб для файла дампа).

Вкладка Удаленное использование (Remote)

На вкладке **Удаленное использование (Remote)** диалогового окна **Свойства системы (System Properties)** вы управляете параметрами **Удаленного помощника (Remote Assistance)** и подключениями **Удаленного рабочего стола (Remote Desktop)**. Эти параметры обсуждаются в начале главы 5.

Управление динамическими библиотеками

Вам как к администратору часто будут поступать запросы на установку или удаление библиотек DLL, особенно если вы работаете с группами разработки ИТ. Утилита для работы с DLL называется Regsvr32 и запускается из командной строки.

Открыв окно командной строки, вы можете установить или зарегистрировать DLL, набрав **regsvr32 имя.dll**, например:

```
regsvr32 mylibs.dll
```

Чтобы отменить установку или регистрацию DLL, введите **regsvr32 /u имя.dll**, например:

```
regsvr32 /u mylibs.dll
```

Система **Защита системных файлов (Windows File Protection)** предотвращает перезапись защищенных системных файлов. Вы сможете заменить только DLL, установленные ОС Windows Server 2008 в составе исправления, пакета обновления или обновления Windows. Система защиты системных файлов — важная часть архитектуры безопасности Windows Server 2008.

Глава 4

Мониторинг процессов, служб и событий

В обязанности администратора входит контроль за состоянием сетевых систем. Состояние системных ресурсов и нагрузка на них в процессе работы могут существенно меняться: к системе пытаются получить доступ неавторизованные пользователи, останавливаются службы, заканчивается свободное пространство на дисках, в приложениях возникают исключения, приводящие к сбоям во всей системе... Приемы, рассматриваемые в этой главе, помогут вам выявить и разрешить эти и другие системные проблемы.

Управление приложениями, процессами и производительностью

Каждый раз, когда вы запускаете приложение или вводите команду в командной строке, Microsoft Windows Server 2008 порождает один или несколько процессов для обслуживания соответствующей программы. Процессы, которые запускаются подобным образом — с помощью клавиатуры или мыши, — называются *интерактивными* (interactive). Если приложение активно и владеет фокусом ввода, клавиатурой и мышью управляет соответствующий интерактивный процесс, пока вы не переключите управление, завершив приложение или выбрав другую программу. Про процесс, владеющий фокусом ввода, говорят, что он работает *на переднем плане* (foreground).

Процессы также могут выполняться *в фоновом режиме* (background). Фоновые программы, запущенные пользователями, продолжают работать, но обычно им не предоставляется такой же приоритет, как активным процессам. Существуют также фоновые процессы, работающие независимо от пользовательского сеанса. Они обычно запускаются операционной системой. Примером такого фонового процесса является запуск операционной системой задания по расписанию.

Диспетчер задач

Основным инструментом для управления системными процессами и приложениями является **Диспетчер задач (Task Manager)**. Его можно запустить следующими способами:

- Нажмите Ctrl+Shift+Esc.
- Нажмите Ctrl+Alt+Del и щелкните **Запустить диспетчер задач (Task Manager)**.
- Щелкните кнопку **Пуск (Start)**, введите **taskmgr** в поле **Начать поиск (Search)** и нажмите Enter.
- Щелкните правой кнопкой мыши панель задач и выберите команду **Диспетчер задач (Task Manager)**.

В следующих разделах описаны способы использования диспетчера задач.

Управление приложениями

На рис. 4-1 показана вкладка **Приложения (Applications)** диспетчера задач. Здесь отображается состояние программ, работающих в данный момент. В нижней части вкладки находятся кнопки для управления приложениями:

- Чтобы остановить приложение, выделите его и щелкните кнопку **Снять задачу (End Task)**.
- Чтобы перейти к приложению и сделать его активным, выделите приложение и щелкните **Переключиться (Switch To)**.
- Чтобы запустить новую программу, щелкните кнопку **Новая задача (New Task)** и введите команду для запуска приложения. Действие этой кнопки подобно действию команды **Выполнить (Run)** из меню **Пуск (Start)**.

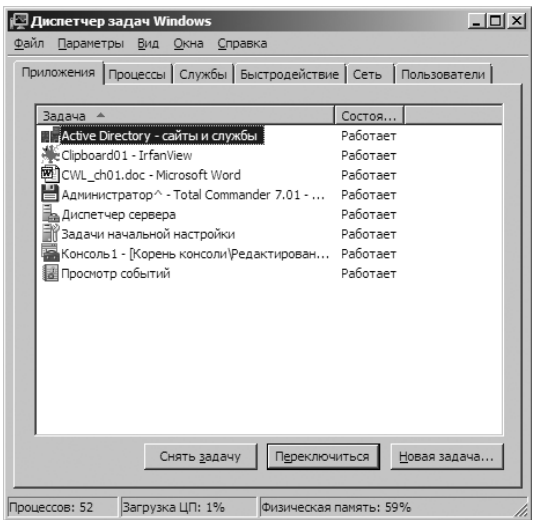


Рис. 4-1. На вкладке Приложения (Applications) диспетчера задач Windows показано состояние программ, которые работают в данный момент

Совет По содержимому столбца **Состояние (Status)** вы определите, нормально ли работает приложение. Состояние **Не отвечает (Not Responding)** означает, что приложение «зависло» и вам, скорее всего, придется остановить соответствующую задачу. Однако иногда приложения временно не отвечают на запросы ОС во время выполнения определенных задач при повышенной нагрузке. Поэтому сначала убедитесь, что приложение на самом деле зависло, и только потом принудительно завершайте его.

Контекстное меню списка приложений

Щелкнув правой кнопкой мыши список приложений в диспетчере задач, вы откроете контекстное меню, которое позволяет выполнить следующие действия:

- переключиться в приложение и сделать его активным;
- вывести приложение на передний план;
- свернуть или развернуть приложение;
- разместить окна приложений на экране мозаикой или каскадом;
- завершить приложение;
- создать файл дампа для отладки приложения;
- перейти к соответствующему процессу на вкладке **Процессы (Processes)**.

Примечание Команда **Перейти к процессу (Go To Process)** полезна, когда вы пытаетесь найти главный процесс определенного приложения. Выбрав эту команду, вы перейдете к соответствующему процессу на вкладке **Процессы (Processes)**.

Администрирование процессов

Вкладка **Процессы (Processes)** окна диспетчера задач показана на рис. 4-2. На ней отображена детальная информация обо всех процессах, выполняемых в данный момент, включая процессы операционной системы, локальные службы, процессы как интерактивного пользователя (зарегистрировавшегося с локальной консоли), так и удаленных пользователей. Чтобы скрыть процессы удаленных пользователей, сбросьте флажок **Отображать процессы всех пользователей (Show Processes From All Users)**.

Поля на вкладке **Процессы (Processes)** содержат много информации о выполняющихся процессах. При помощи этой информации вы определите, какие процессы чрезмерно загружают системные ресурсы, например, процессорное время и память. По умолчанию отображаются следующие поля:

- **Имя образа (Image Name)** Имя процесса или исполняемого файла, запустившего процесс.
- **Пользователь (User Name)** Имя пользователя или системной службы, запустившей процесс.
- **ЦП (CPU)** Доля ресурсов процессора, занятая данным процессом (в процентах).
- **Память (частный рабочий набор) (Memory (Private Working Set))** Объем памяти, используемой процессом в данный момент.
- **Описание (Description)** Описание процесса.

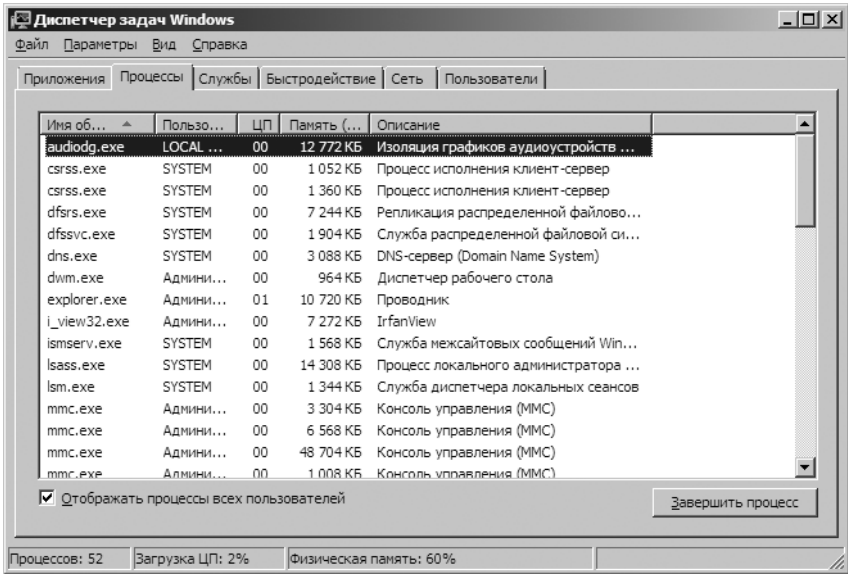


Рис. 4-2. На вкладке Процессы (Processes) собрана детальная информация о запущенных процессах

Выберите в меню **Вид (View)** команду **Выбрать столбцы (Select Columns)**, чтобы добавить столбцы на вкладку **Процессы (Processes)**. Когда в системе возникли проблемы, полезными могут оказаться следующие столбцы:

- **Базовый приоритет (Base Priority)** Базовый приоритет определяет, сколько системных ресурсов выделяется процессу. Чтобы задать приоритет процесса, щелкните процесс правой кнопкой мыши, выберите команду **Приоритет (Set Priority)** и выберите один из следующих вариантов: **Низкий (Low)**, **Ниже среднего (Below Normal)**, **Средний (Normal)**, **Выше среднего (Above Normal)**, **Высокий (High)** и **Реального времени (Real-Time)**. Большинство процессов по умолчанию имеет средний приоритет. Наивысший приоритет назначается процессам реального времени.
- **Время ЦП (CPU Time)** Общее количество циклов процессора, использованное процессом с момента запуска. Чтобы быстро выявить процессы, которые в наибольшей мере загружают процессор, выведите этот столбец и щелкните его заголовок, чтобы отсортировать записи о процессах по времени ЦП.
- **Дескрипторы (Handle Count)** Общее количество дескрипторов файлов, обрабатываемых процессом. Счетчик дескрипторов позволяет оценить, насколько процесс зависит от файловой системы. С некоторыми процессами, например, с процессами Microsoft Internet Information Services (IIS), связаны тысячи открытых дескрипторов файлов. Для обслуживания каждого дескриптора требуется системная память.

- **Число чтений (I/O Reads), Число записей (I/O Writes)** Общее число дисковых операций чтения или записи с момента запуска процесса. Оба этих параметра говорят о том, сколько дисковых операций произведено процессом. Если число чтений и записей растет непропорционально действительной нагрузке на сервер, возможно, процесс не кеширует файлы или кеширование настроено неправильно. В идеале кеширование должно снижать потребность в операциях чтения и записи.
- **Ошибки страниц (Page Faults)** Ошибка страницы происходит, когда процесс запрашивает страницу в памяти, а система не может найти ее в запрошенном месте. Если запрошенная страница находится в другой области памяти, ошибка называется *программной* (soft page fault). Если запрошенная страница отсутствует на диске, ошибка называется *аппаратной* (hard page fault). Большинство процессоров способны обработать большое число программных ошибок. Дисковые ошибки могут привести к значительным задержкам.
- **Память — выгружаемый пул (Paged Pool), Память — невыгружаемый пул (Nonpaged Pool)** *Выгружаемый пул* — область системной памяти для объектов, которые можно записать на диск, если они не используются. *Невыгружаемый пул* — область системной памяти для объектов, которые нельзя записывать на диск. Следует обратить внимание на процессы, которым требуется большой объем невыгружаемой памяти. Если на сервере недостаточно свободной памяти, эти процессы могут стать причиной большого числа ошибок страниц.
- **Память — пик рабочего набора (Peak Memory Usage)** Максимальный объем памяти, использованный процессом. Важно также следить за разницей между текущим и пиковым использованием памяти. Приложениям с большой разницей между типичным и максимальным объемом занимаемой памяти, например, Microsoft SQL Server, необходимо выделить при запуске больше памяти, чтобы они работали эффективнее.
- **Счетчик потоков (Thread Count)** Текущее количество потоков, используемых процессом. Большинство серверных приложений — многопоточные. Многопотоковость обеспечивает одновременное выполнение запросов процесса. Некоторые приложения способны динамически управлять числом потоков для повышения своей производительности. С другой стороны, чрезмерное количество потоков может привести к снижению производительности, поскольку операционной системе приходится слишком часто переключаться между контекстами потоков.

В списке выполняющихся процессов вы увидите процесс **Бездействие системы (System Idle Process)**. Задать приоритет этого процесса нельзя. В отличие от других процессов, использующих системные ресурсы, процесс **Бездействие системы (System Idle Process)** отслеживает незанятые системные ресурсы. Число 99 в столбце **ЦП (CPU)** для процесса **Бездействие системы (System Idle Process)** означает, что 99% процентов ресурсов процессора в данный момент не используется.

Просматривая процессы помните, что одно приложение может породить несколько процессов. Обычно они зависимы от главного процесса, начиная с которого формируется дерево зависимых процессов. Чтобы найти главный процесс приложения, щелкните правой кнопкой приложение на вкладке **Приложения (Applications)** и выберите команду **Перейти к процессу (Go To Process)**. Если вы хотите завершить процесс, обычно следует указывать главный процесс приложения, а не зависимые процессы. Это гарантирует полную остановку приложения.

Есть несколько способов остановить главный процесс приложения и все зависимые процессы:

- выделить приложение на вкладке **Приложения (Applications)** и щелкнуть кнопку **Снять задачу (End Task)**;
- щелкнуть правой кнопкой главный процесс приложения на вкладке **Процессы (Processes)** и выбрать команду **Завершить процесс (End Process)** или щелкнуть одноименную кнопку;
- щелкнуть правой кнопкой главный или зависимый процесс на вкладке **Процессы (Processes)** и выбрать команду **Завершить дерево процессов (End Process Tree)**.

Просмотр системных служб

На вкладке **Службы (Services)** диспетчера задач перечислены системные службы. Для каждой службы приводится имя, идентификатор процесса (PID), описание, состояние и группа. Как показано на рис. 4-3, обычно несколько служб работают с одним и тем же идентификатором процесса. Чтобы быстро отсортировать службы по идентификаторам, щелкните заголовок соответствующего столбца. Щелкнув заголовок столбца **Состояние (Status)**, вы отсортируете службы в соответствии с их состоянием: **Работает (Running)** или **Остановлено (Stopped)**.

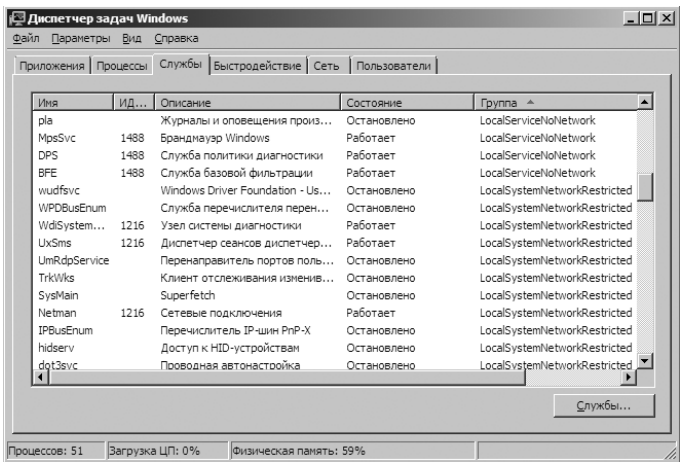


Рис. 4-3. На вкладке Службы (Services) перечислены системные службы

В столбце **Группа (Group)** содержатся дополнительные сведения об учетных записях или контекстах, в рамках которых работают службы:

- Если на учетную запись службы наложены ограничения, они указаны в этом столбце. Например, служба, работающая под учетной записью LocalService, может быть помечена как LocalServiceNoNetwork (служба не имеет доступа к сети) или как LocalSystemNetworkRestricted (служба имеет ограниченный доступ к сети).
- Для служб, запущенных svchost.exe, выводится контекст, указанный в параметре –k. Например, служба RemoteRegistry запускается командой svchost.exe –k regsvc. В столбце **Группа (Group)** для этой службы отображается regsvc.

Щелкнув правой кнопкой список служб диспетчера задач, вы откроете контекстное меню, которое позволит вам:

- запустить остановленную службу;
- остановить работающую службу;
- перейти к соответствующему процессу на вкладке **Процессы (Processes)**.

Управление быстродействием

Вкладка **Быстродействие (Performance)** диспетчера задач содержит сведения по использованию процессора и памяти в виде диаграмм и статистики (рис. 4-4). Эта информация поможет вам быстро проверить использование системных ресурсов. Для получения более детальных сведений, используйте **Монитор производительности (Performance Monitor)**, описанный далее в этой главе.

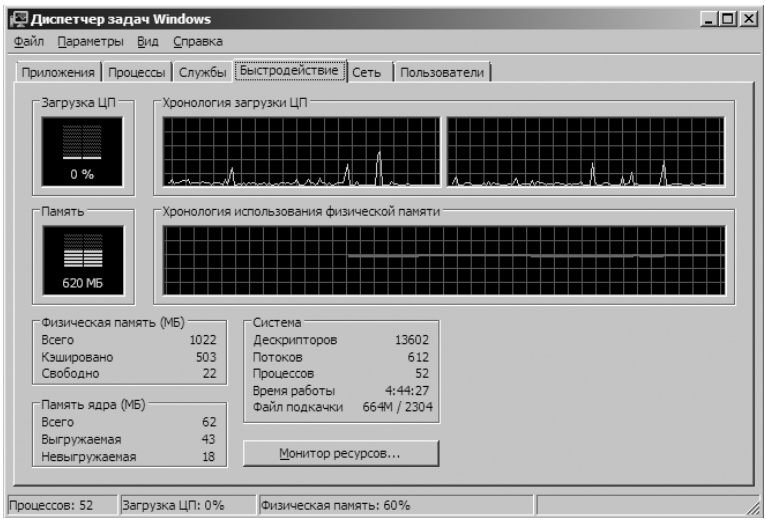


Рис. 4-4. Вкладка Быстродействие (Performance) поможет быстро оценить использование системных ресурсов

Диаграммы на вкладке Быстродействие (Performance)

Диаграммы на вкладке **Быстродействие (Performance)** содержат следующую информацию:

- **Загрузка ЦП (CPU Usage)** На сколько процентов в данный момент используются ресурсы процессора.
- **Хронология загрузки ЦП (CPU Usage History)** История использования процессора. Частоту обновления диаграммы можно изменить.
- **Память (Memory)** Объем физической памяти, используемый системой в данный момент.
- **Хронология использования физической памяти (Physical Memory Usage History)** История использования памяти.

Примечание Если в системе установлено несколько процессоров, по умолчанию отображаются хронологии для каждого процессора. На рис. 4-4 показана вкладка **Быстродействие (Performance)** с двухпроцессорного компьютера, поэтому на ней выведено две диаграммы хронологии загрузки ЦП.

Совет Чтобы посмотреть на диаграмму использования процессора крупным планом, дважды щелкните вкладку **Быстродействие (Performance)**. Повторный двойной щелчок вернет нормальный режим просмотра. Если загруженность процессора даже при средней нагрузке постоянно держится на высоком уровне, вероятно, для выявления причин стоит провести более детальный мониторинг производительности. Часто источником проблем производительности становится память, так что начните анализ с нее, прежде чем обновлять или добавлять процессоры. Подробнее — в разделе «Настройка производительности системы» этой главы.

Настройка и обновление диаграмм

Для настройки и обновления диаграмм используйте следующие команды меню **Вид (View)**:

- **Скорость обновления (Update Speed)** Позволяет изменить частоту обновления диаграмм, а также приостановить обновление. Скорость **Низкая (Low)** соответствует обновлению раз в четыре секунды, **Обычная (Normal)** — раз в две секунды, **Высокая (High)** — дважды в секунду.
- **Загрузка ЦП (CPU History)** На многопроцессорных системах позволяет указать, как следует выводить диаграммы процессоров. Можно, например, выводить отдельный график для каждого процессора (по умолчанию) или один график для всех процессоров.
- **Вывод времени ядра (Show Kernel Times)** Позволяет выводить время процессора, использованное ядром операционной системы. График для ядра чертится красной линией (в отличие от зеленых линий обычных диаграмм).

Примечание Мониторинг ресурсов, используемых ядром, полезен для выявления некоторых проблем. Например, если вы используете IIS 7 с кешированием вывода в режиме ядра, контроль за временем процессора, использованным ядром, поможет вам получить более полное представление о том, как кеширование отражается на загрузке процессора и общей производительности. По умолчанию мониторинг ресурсов, используемых ядром, выключен, поскольку приводит к дополнительным накладным расходам.

Ниже диаграмм приводятся некоторые численные данные:

- **Физическая память (МБ) (Physical Memory (MB))** Информация об оперативной памяти системы. В поле **Всего (Total)** показан общий объем физической оперативной памяти, в поле **Кэшировано (Cached)** — объем памяти, используемой для кеширования, в поле **Свободно (Free)** — объем неиспользуемой оперативной памяти. Если на сервере мало доступной физической памяти, вам стоит увеличить ее объем. Вообще, всегда нужно следить, чтобы объем свободной памяти был не менее 5% от физической памяти сервера.
- **Память ядра (МБ) (Kernel Memory (MB))** Информация о памяти, используемой ядром операционной системы. Самые важные фрагменты ядра должны располагаться в оперативной памяти и не могут размещаться в виртуальной памяти. Этот тип памяти обозначен как **Невыгружаемая (Nonpaged)**. Оставшаяся часть памяти ядра может быть выгружена в виртуальную память и потому обозначена как **Выгружаемая (Paged)**. Общий объем памяти, используемой ядром, указан в поле **Всего (Total)**.
- **Система (System)** Информация об использовании процессора. В поле **Дескрипторов (Handles)** указано число используемых дескрипторов ввода-вывода — маркеров, предоставляющих программам доступ к ресурсам. В поле **Потоков (Threads)** показано число используемых потоков. Потоки являются основной единицей исполнения в рамках процессов. В поле **Процессов (Processes)** показано число используемых процессов — экземпляров приложений или исполняемых файлов. В поле **Время работы (Up Time)** указано, сколько времени прошло с момента запуска системы. В поле **Файл подкачки (Page File)** показана используемая в данный момент виртуальная память и общий объем доступной виртуальной памяти. Если загруженность файла подкачки постоянно находится на уровне 10% от общего объема виртуальной памяти, вам, вероятно, следует добавить физической памяти или увеличить объем виртуальной памяти (или и то, и другое).

Управление производительностью сети

На вкладке **Сеть (Networking)** диспетчера задач представлен обзор сетевых адаптеров системы. С помощью приведенной здесь информации вы быстро определите процент загруженности, скорость подключения и состояние всех сетевых адаптеров, установленных на компьютере.

Если в системе установлен один сетевой адаптер, на вкладке **Сеть (Networking)** отображается график для этого адаптера (рис. 4-5). Если в системе установлено несколько сетевых адаптеров, на диаграмме показан составной индекс для всех сетевых подключений, представляющий общий сетевой трафик. По умолчанию на диаграмме показывается только общее число байтов сетевого трафика. Чтобы изменить отображаемую информацию, откройте меню **Вид (View)**, выберите **Журнал сетевого адаптера (Network Adapter History)** и задайте вариант **Отправлено байт (Bytes Sent)**, **Получено байт (Bytes Received)** или оба варианта. Отправленные байты показываются красным цветом, полученные байты — желтым, суммарный трафик — зеленым.

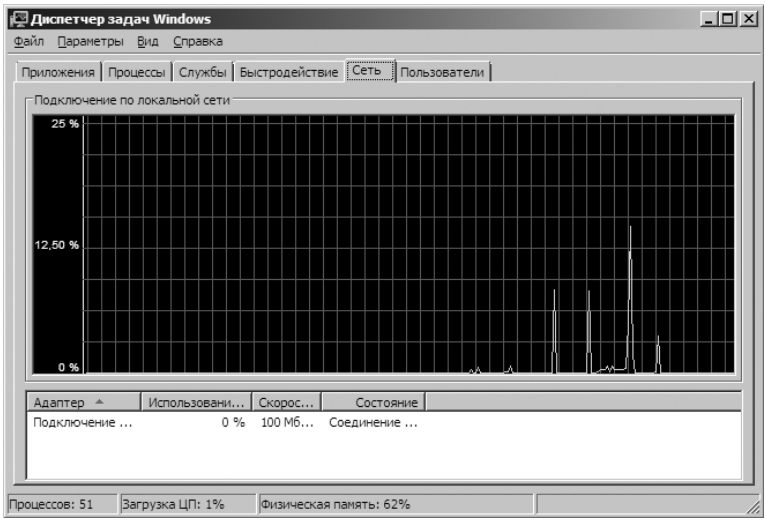


Рис. 4-5. На вкладке Сеть (Networking) представлены параметры работы сети

Поля на вкладке **Сеть (Networking)** содержат обширную информацию о входящем и исходящем сетевом трафике сервера. По этой информации вы легко определите, какой объем внешнего трафика сервер обрабатывает в данный момент времени. Следующие поля выводятся по умолчанию:

- **Адаптер (Adapter Name)** Имя сетевого адаптера в папке Сетевые подключения (Network Connections).
- **Использование сети (Network Utilization)** Процент использования сети, вычисленный по исходной скорости соединения для интерфейса. Например, адаптер с исходной скоростью 100 мегабит в секунду и текущим трафиком 10 мегабит в секунду имеет 10-процентную нагрузку.
- **Скорость линии (Link Speed)** Исходная скорость соединения для интерфейса.
- **Состояние (State)** Рабочее состояние адаптера.

Ближе к реальности Если загруженность адаптера регулярно превышает 50% от общей пропускной способности, следует осуществить более внимательный мониторинг сервера. Возможно, стоит подумать о добавлении новых сетевых адаптеров. Тщательно продумывайте любую модернизацию; зачастую требуется более подробное планирование, чем казалось сначала. Принимайте во внимание не только сервер, но и всю сеть в целом. Иногда проблемы подключения связаны с тем, что вы превысили полосу пропускания, выделенную поставщиком услуг. Иногда на получение дополнительной полосы пропускания для внешних подключений уходят месяцы.

Выбрав в меню **Вид (View)** команду **Выбрать столбцы (Select Columns)**, вы увидите список столбцов, которые можно добавить на вкладку **Сеть (Networking)**. При диагностике сетевых проблем полезные следующие столбцы:

- **Пропускная способность отправки (Bytes Sent Throughput)** Процент текущей полосы пропускания, используемый исходящим трафиком.
- **Пропускная способность получения (Bytes Received Throughput)** Процент текущей полосы пропускания, используемый входящим трафиком.
- **Общая пропускная способность (Bytes Throughput)** Процент текущей полосы пропускания, используемый общим сетевым трафиком адаптера.
- **Отправлено байт (Bytes Sent)** Общее число байтов, отправленных через соединение до данного момента.
- **Получено байт (Bytes Received)** Общее число байтов, полученных через соединение до данного момента.
- **Байт (Bytes)** Общее число байтов, прошедших через соединение до данного момента.

Управление сеансами удаленных пользователей

Удаленные пользователи могут использовать для подключения к системе службы терминалов или удаленный рабочий стол. В первом случае осуществляется удаленное терминальное подключение. Удаленный рабочий стол позволяет удаленно администрировать систему, как если бы вы находились за клавиатурой.

При установке Windows Server 2008 подключения удаленного рабочего стола автоматически разрешены. Окно **Диспетчер задач (Task Manager)** предоставляет один из способов просмотра и управления подключениями к удаленному рабочему столу. Запустите диспетчер задач и перейдите на вкладку **Пользователи (Users)**, показанную на рис. 4-6. На ней показаны интерактивные пользовательские сеансы как для локальных, так и для удаленных пользователей.

Для каждого подключения приводится имя пользователя, код сеанса, состояние, имя клиентского компьютера и тип сеанса. Пользователю, зарегистрировавшемуся в системе локально, соответствует тип сеанса **Console**. У других пользователей в качестве типа сеанса отображается тип подключения и протокол, например, **RDP-TCP** для подключений с использованием

протокола RDP и TCP в качестве транспортного протокола. Если вы щелкнете сеанс правой кнопкой мыши, то увидите следующие команды:

- **Подключить (Connect)** Подключает неактивный сеанс пользователя.
- **Отключить (Disconnect)** Отключает сеанс пользователя, завершая без сохранения данных все запущенные пользователем приложения.
- **Выход из системы (Log Off)** Отключает пользователя с использованием обычного процесса выхода. Данные приложения и информация о состоянии системы сохраняются.
- **Удаленное управление (Remote Control)** Назначает горячие клавиши для завершения сеансов удаленного управления. По умолчанию — Ctrl+*.
- **Отправить сообщение (Send Message)** Посылает консольное сообщение пользователям, зарегистрировавшимся на удаленных системах.

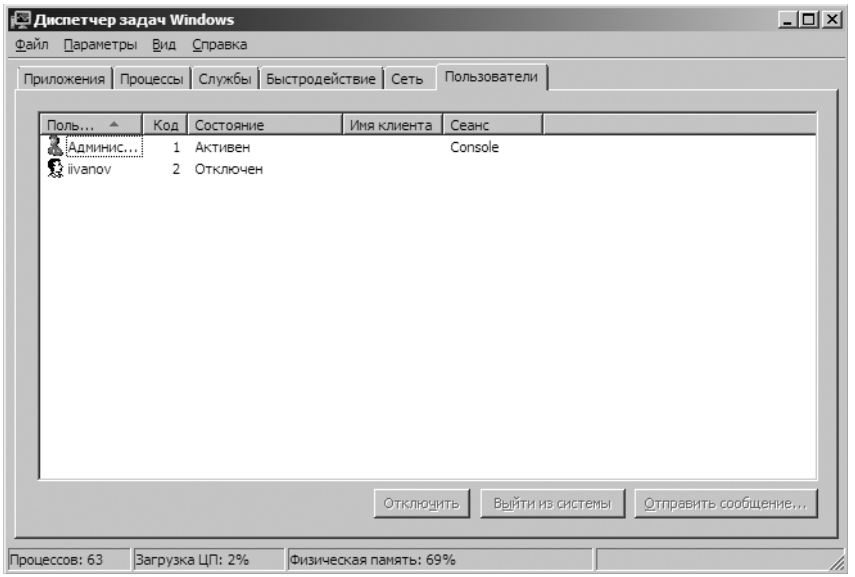


Рис. 4-6. Вкладка Пользователи (Users) позволяет просматривать пользовательские сеансы и управлять ими

Управление системными службами

Службы обеспечивают ключевую функциональность рабочих станций и серверов. Для управления системными службами вы будете использовать узел **Службы (Services)** диспетчера сервера. Чтобы запустить диспетчер сервера и получить доступ к узлу **Службы (Services)**, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и команду **Администрирование (Administrative Tools)**, затем выберите команду **Диспетчер сервера (Server Manager)**. Или щелкните кнопку **Диспетчер сервера (Server Manager)** на панели быстрого запуска.

2. В окне **Диспетчер сервера (Server Manager)** разверните узел **Конфигурация (Configuration)**.
3. Выделите узел **Службы (Services)**, чтобы просмотреть полный список служб, установленных в системе (рис. 4-7). По умолчанию список отсортирован по имени службы и включает следующие столбцы:
   - **Имя (Name)** Имя службы. Дважды щелкните запись, чтобы настроить параметры запуска. Здесь перечислены только установленные службы. Если необходимая вам служба отсутствует, установите ее, добавив соответствующую роль или компонент, как описано в главе 2.
   - **Описание (Description)** Краткое описание назначения службы.
   - **Состояние (Status)** Состояние службы — работает, приостановлена или остановлена (остановленной службе соответствует пустое поле).
   - **Тип запуска (Startup Type)** Настройка запуска службы. Автоматические службы запускаются при загрузке. Пользователи и службы могут запускать другие службы вручную. Отключенные службы нельзя запустить, пока они выключены.
   - **Вход от имени (Log On As)** Учетная запись, от имени которой работает служба. В большинстве случаев это учетная запись локальной системы.

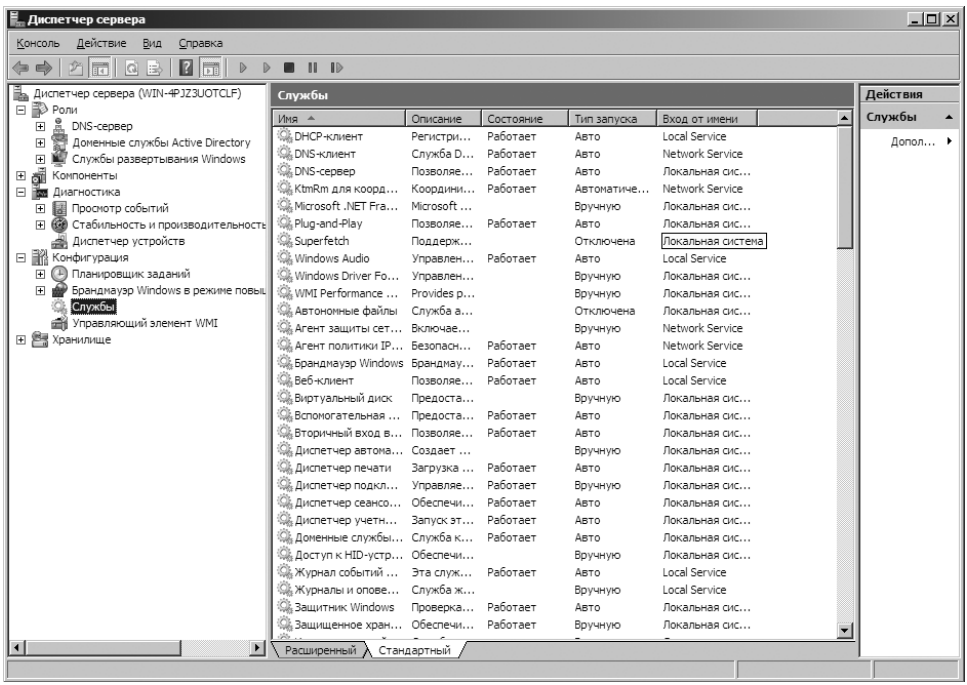


Рис. 4-7. Используйте панель Службы (Services) для управления службами на рабочих станциях и серверах

У панели **Службы (Services)** два представления: расширенное и стандартное. Чтобы изменить представление, щелкните соответствующую вкладку в нижней части панели **Службы (Services)**. В расширенном представлении отображаются быстрые ссылки для управления службами. Щелкните **Запустить (Start)**, чтобы запустить остановленную службу. Щелкните **Перезапустить (Restart)** для остановки и повторного запуска работающей службы, по существу, для ее перезагрузки. Если вы выделите службу в расширенном представлении, то увидите также ее описание.

Примечание Отключать службы могут как пользователи, так и операционная система. Обычно Windows Server 2008 отключает службы, если возникает вероятность конфликта с другой службой.

Запуск, остановка, и приостановка служб

Администратору часто приходится запускать, останавливать или приостанавливать службы Windows Server 2008. Для запуска, остановки или приостановки службы выполните следующие действия:

1. В окне **Диспетчер сервера (Server Manager)** разверните узел **Конфигурация (Configuration)**.
2. Выделите узел **Службы (Services)**.
3. Щелкните правой кнопкой мыши нужную службу и выберите команду **Запустить (Start)**, **Остановить (Stop)** или **Приостановить (Pause)**. Можно также выбрать команду **Перезапустить (Restart)**, чтобы ОС остановила службу и повторно запустила ее после небольшой паузы. Если вы приостановили службу, выберите команду **Продолжить (Resume)** для восстановления ее нормальной работы.

Примечание Если служба, настроенная на автоматический запуск, останавливается из-за ошибки, в столбце состояния выводится пустая строка. Как правило, вы также получаете оповещение во всплывающем диалоговом окне. Кроме того, ошибки служб регистрируются в журнале событий системы. В Windows Server 2008 можно настроить действие для автоматической обработки ошибки службы, например, настроить ее перезапуск. Подробнее — в разделе «Настройка восстановления службы».

Настройка запуска службы

Службы Windows Server 2008 запускаются автоматически или вручную. Также их можно выключить. Настройка запуска службы производится следующим образом:

1. В окне **Диспетчер сервера (Server Manager)** разверните узел **Конфигурация (Configuration)**.
2. Выделите узел **Службы (Services)**, щелкните правой кнопкой службу, которую хотите настроить, и выберите команду **Свойства (Properties)**.
3. На вкладке **Общие (General)** выберите в раскрывающемся списке **Тип запуска (Startup Type)** один из следующих вариантов (рис. 4-8).

- **Авто (Automatic)** Служба будет запускаться при загрузке.
- **Автоматически (отложенный запуск) (Automatic (Delayed Start))** Служба запускается автоматически, но только после того как стартуют все обычные автоматические службы.
- **Вручную (Manual)** Служба запускается вручную.
- **Отключена (Disabled)** Служба не работает.

4. Щелкните **OK**.

Ближе к реальности Если на сервере имеется несколько профилей оборудования, вы вольны разрешить или отключить службы для определенного профиля. Прежде чем отключать службы, стоит создать отдельный аппаратный профиль для тестирования сервера с отключенными службами. Это позволит вам при необходимости легко восстановить исходное состояние сервера. Другие параметры службы в профиле не сохраняются. Чтобы разрешить или отключить службу в профиле, перейдите на вкладку **Вход в систему (Log On)** диалогового окна свойств службы. Выберите в списке нужный профиль и щелкните нужную кнопку — **Разрешить (Enable)** или **Запретить (Disable)**.

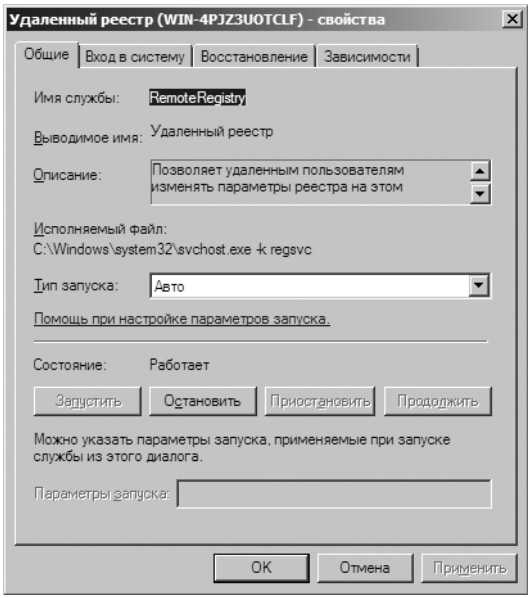


Рис. 4-8. Настройка параметров запуска службы

Настройка входа службы в систему

Вы может настроить службу Windows Server 2008 на работу от имени системной учетной записи или определенного пользователя, выполнив следующие действия:

1. В окне **Диспетчер сервера (Server Manager)** разверните узел **Конфигурация (Configuration)**.

2. Выделите узел **Службы (Services)**, щелкните правой кнопкой службу, которую хотите настроить, и выберите команду **Свойства (Properties)**.
3. Перейдите на вкладку **Вход в систему (Log On)**, показанную на рис. 4-9.
4. Установите переключатель **С системной учетной записью (Local System Account)**, чтобы служба работала от имени системной учетной записи (для большинства служб это вариант по умолчанию). Если у службы есть пользовательский интерфейс, установите флажок **Разрешить взаимодействие с рабочим столом (Allow Service To Interact With Desktop)**, чтобы разрешить пользователям управлять интерфейсом службы.
5. Установите переключатель **С учетной записью (This Account)**, если хотите, чтобы служба работала от имени определенной учетной записи. Введите имя учетной записи и пароль в соответствующих полях. При необходимости используйте для поиска учетной записи пользователя кнопку **Обзор (Browse)**.
6. Щелкните OK.

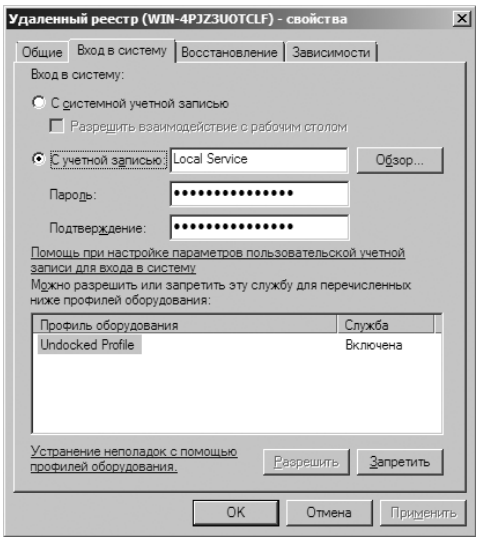


Рис. 4-9. Используйте вкладку Вход в систему (Log On) для настройки учетной записи службы

Безопасность Администратор должен контролировать все учетные записи, используемые службами, поскольку их некорректная настройка может стать источником существенных проблем для безопасности. Учетные записи служб должны работать с максимумом ограничений и с минимумом полномочий — им нужны лишь те разрешения, что необходимы для выполнения задач службы. Как правило, большинство полномочий, назначаемых обычным пользовательским записям, учетным записям служб не нужны. Например, им не требуется право локального входа. Относитесь к учетным записям служб так же, как к учетным записям администратора. Это означает безопасные пароли, тщательный мониторинг использования, продуманное назначение полномочий и т. д.

Настройка восстановления службы

Вы можете настроить службы Windows Server 2008 на выполнение определенного действия в случае аварийной остановки. Например, можно попытаться перезапустить службу или запустить определенное приложение. Чтобы настроить параметры восстановления службы, выполните следующие действия:

1. В окне **Диспетчер сервера (Server Manager)** разверните узел **Конфигурация (Configuration)**.
2. Выделите узел **Службы (Services)**, щелкните правой кнопкой службу, которую хотите настроить, и выберите команду **Свойства (Properties)**.
3. Перейдите на вкладку **Восстановление (Recovery)**, показанную на рис. 4-10.

Примечание В процессе установки Windows Server 2008 автоматически настраивает восстановление критических системных служб. В большинстве случаев для них задан автоматический перезапуск. В случае аварийной остановки некоторых особенно важных служб, например, **Модуль запуска процессов DCOM-сервера (DCOM Server Process Launcher)** и **Клиент групповой политики (Group Policy Client)**, производится перезапуск компьютера. Эти настройки изменить нельзя.

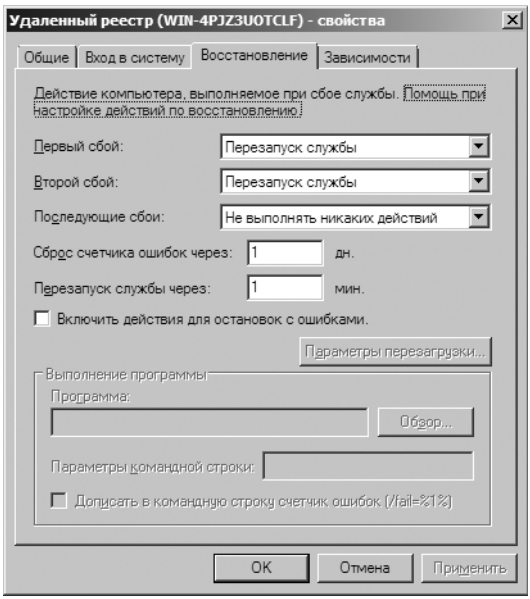


Рис. 4-10. На вкладке Восстановление (Recovery) задаются действия, которые следует предпринять при аварийной остановке службы

4. Настройте параметры для первой, второй и последующих попыток восстановления. Возможны следующие варианты:

- **Не выполнять никаких действий (Take No Action)** ОС не будет пытаться восстановить службу в случае возникновения этой ошибки, но может пытаться провести восстановление для предыдущей или последующей ошибок.
- **Перезапуск службы (Restart the Service)** Служба останавливается, а затем после короткой паузы снова запускается.
- **Запуск программы (Run a Program)** Позволяет в случае возникновения ошибки запустить программу, пакетный файл или сценарий Windows. Выбрав этот вариант, вы должны указать полный путь к программе, которую хотите запустить, и задать необходимые параметры командной строки.
- **Перезагрузка компьютера (Restart the Computer)** Завершает работу компьютера и перезагружает его. Прежде чем выбрать этот вариант, проверьте параметры запуска и восстановления компьютера. Необходимо, чтобы система быстро и автоматически выбирала настройки по умолчанию.

Ближе к реальности Восстановление критических служб предпочтительно проводить следующим образом: перезапуск службы при первой и второй ошибке и перезагрузка сервера при третьей ошибке.

5. Настройка других параметров зависит от параметров, выбранных на предыдущем шаге. Если вы выбрали запуск программы при сбое службы, вам нужно заполнить поля раздела **Выполнение программы (Run Program)**. Если вы решили перезапустить службу, необходимо задать продолжительность паузы перед перезапуском. В большинстве случаев достаточно одной-двух минут.
6. Щелкните **OK**.

Отключение неиспользуемых служб

Неиспользуемые службы являются потенциальным источником проблем. Например, во многих организациях, где мне довелось анализировать проблемы безопасности, я видел работающие службы **Служба веб-публикации (Worldwide Web Publishing Service)**, **Simple Mail Transfer Protocol (SMTP)** и **Служба FTP-публикации (File Transfer Protocol (FTP) Publishing Service)**, хотя в них не было необходимости. К сожалению, именно эти службы предоставляют возможность доступа к серверам анонимных пользователей, а также при неправильном конфигурировании открывают сервер для атаки.

Если вы обнаружили неиспользуемые службы, у вас есть несколько вариантов действия. Если служба установлена в составе роли или компонента, вы вольны удалить соответствующую роль или компонент, чтобы удалить и все относящиеся к нему службы. Можно также просто отключить службы, которые в данные момент не используются. Обычно следует начинать

с отключения служб, а не с удаления компонентов. Если после отключения службы другой администратор или пользователь сообщит, что ему не удается выполнить некое действие, вы при необходимости легко восстановите соответствующую службу.

Чтобы отключить службу, выполните следующие действия:

1. В окне **Диспетчер сервера (Server Manager)** разверните узел **Конфигурация (Configuration)**.
2. Выделите узел **Службы (Services)**, щелкните правой кнопкой службу, которую хотите настроить, и выберите команду **Свойства (Properties)**.
3. На вкладке **Общие (General)** выберите в раскрывающемся списке **Тип запуска (Startup Type)** вариант **Отключена (Disabled)**.

Отключение службы не останавливает ее, но всего лишь предотвращает ее запуск при следующей загрузке компьютера. Это означает, что угроза безопасности все еще существует. Чтобы исключить ее, щелкните кнопку **Остановить (Stop)** на вкладке **Общие (General)** диалогового окна **Свойства (Properties)** и щелкните **OK**.

Журналы событий

В журналы событий записывается хронологическая информация, которая поможет вам выявить проблемы в системе и безопасности. Отслеживанием событий на системах Windows Server 2008 управляет служба **Журнал событий Windows (Windows Event Log)**. Журналы бывают двух основных типов:

- **Журналы Windows (Windows logs)** Используются операционной системой для записи основных системных событий, связанных с приложениями, безопасностью, настройкой и системными компонентами.
- **Журналы приложений и служб (Applications and Services logs)** Используются отдельными приложениями и службами для записи событий, специфических для приложения или службы.

К журналам Windows относятся следующие журналы:

- **Безопасность (Security Log)** В него записываются события, для которых в локальных или глобальных групповых политиках безопасности задан аудит. По умолчанию располагается в файле %SystemRoot%\System32\Winevt\Logs\Security.evtx.

Примечание Для чтения журнала безопасности пользователю необходимо разрешение **Управление аудитом и журналом безопасности (Manage Auditing and the Security Log)**. По умолчанию это разрешение назначено членам группы **Администраторы (Administrators)**. Подробнее о назначении прав пользователей — в разделе «Настройка политик прав пользователей» главы 10.

- **Настройка (Setup Log)** Сюда записываются события, зарегистрированные ОС и ее компонентами в процессе установки. По умолчанию располагается в файле %SystemRoot%\System32\Winevt\Logs\Setup.evtx.

- **Пересланные события (Forwarded Events)** Если настроена пересылка событий, в этот журнал записываются события, пересланные с других серверов. По умолчанию располагается в файле %SystemRoot%\System32\Config\FordwardedEvents.evtx.
- **Приложение (Application)** В него записываются события, зарегистрированные приложениями, например, ошибка при осуществлении доступа к базе данных Microsoft SQL Server. По умолчанию он располагается в файле %SystemRoot%\System32\Winevt\Logs\Application.evtx.
- **Система (System Log)** Сюда записываются события, зарегистрированные ОС и ее компонентами, например, неудачный запуск службы при загрузке. По умолчанию располагается в файле %SystemRoot%\System32\Winevt\Logs\System.evtx.

Безопасность Администратору в большей степени интересны журналы приложений и системы, но не забывайте и про журнал безопасности. Это один из самых важных журналов, и вам необходимо внимательно просматривать его. Если в журнале безопасности сервера отсутствуют события, скорее всего, на сервере не настроен локальный аудит, или же аудит настроен на уровне домена, и потому следует просматривать журнал безопасности на контроллерах домена, а не на рядовых серверах. Помните, что для чтения журнала безопасности пользователю необходимо разрешение **Управление аудитом и журналом безопасности (Manage Auditing and the Security Log)**. По умолчанию это разрешение назначено членам группы **Администраторы (Administrators)**. Подробнее о назначении прав пользователей — в разделе «Настройка политик прав пользователей» главы 10.

К журналам приложений и служб относятся следующие журналы:

- **Репликация DFS (DFS Replication)** В этом журнале протоколируется активность служб репликации DFS. По умолчанию располагается в файле %SystemRoot%\System32\Winevt\Logs\DfsReplication.evtx.
- **Служба каталогов (Directory Service)** Сюда записываются события, зарегистрированные доменными службами Active Directory. По умолчанию располагается в файле %SystemRoot%\System32\Winevt\Logs\Directory Service.evtx.
- **Служба репликации файлов (File Replication Service)** Здесь протоколируется активность службы репликации файлов. По умолчанию располагается в файле %SystemRoot%\System32\Winevt\Logs\File Replication Service.evtx.
- **События оборудования (Hardware Events)** Если настроена регистрация событий аппаратной подсистемы, в этот журнал записываются аппаратные события, зарегистрированные ОС. По умолчанию располагается в файле %SystemRoot%\System32\Config\Hardware.evtx.
- **DNS-сервер (DNS Server)** Сюда записываются DNS-запросы, ответы и прочая активность DNS. По умолчанию располагается в файле %SystemRoot%\System32\Winevt\Logs\DNS Server.evtx.
- **Microsoft\Windows** Журналы событий, относящихся к определенным службам и компонентам Windows. Журналы организуются по типу ком-

понентов и категории событий. В операционных журналах регистрируются события, вызванные текущими операциями соответствующего компонента. В некоторых случаях вы увидите также дополнительные журналы для анализа, отладки и регистрации административных задач.

- **Windows PowerShell** В этом журнале записываются события, относящиеся к использованию **Windows PowerShell**. По умолчанию располагается в файле %SystemRoot%\System32\Winevt\Logs\Windows PowerShell.evtx.

Просмотр журналов событий и пользование ими

Чтобы получить доступ к журналам событий, выполните следующие действия:

1. Разверните узел **Диагностика (Diagnostics)** диспетчера сервера.
2. Раскройте узел **Просмотр событий (Event Viewer)**. Работать с журналами событий сервера можно несколькими способами:
   - Чтобы просмотреть все ошибки и предупреждения во всех журналах, разверните узел **Настраиваемые представления (Custom Views)** и выделите **События управления (Administrative Events)**. На главной панели вы увидите список всех событий сервера, связанных с ошибками и предупреждениями.
   - Чтобы просмотреть все ошибки и предупреждения для определенной роли сервера, разверните узел **Настраиваемые представления (Custom Views)**, выделите **Роли сервера (Server Roles)** и выберите роль для просмотра. На главной панели вы должны увидеть список всех событий выбранной роли.
   - Чтобы просмотреть события в определенном журнале, разверните узел **Журналы Windows (Windows Logs)**, узел **Журналы приложений и служб (Applications And Services Logs)** или оба узла сразу. Выделите журнал, который хотите просмотреть, например, **Приложение (Application)** или **Система (System)**.
3. По содержанию столбца **Источник (Source)** определите, какая служба или процесс записали событие.

Как показано на рис. 4-11, записи на главной панели консоли **Просмотр событий (Event Viewer)** содержат краткую информацию о том, когда, где и при каких условиях произошло событие. Чтобы получить более подробную информацию, выделите событие и просмотрите содержимое нижней части главной панели. Перед датой и временем события в списке указан его уровень или ключевые слова. Уровни событий таковы:

- **Сведения (Information)** Информационное событие, обычно относящееся к успешному выполнению действия.
- **Аудит выполнен успешно (Audit Success)** Событие, относящееся к успешному выполнению действия.

- **Сбой аудита (Audit Failure)** Событие, относящееся к неудачному выполнению действия.
- **Предупреждение (Warning)** Они часто очень полезны для предотвращения будущих проблем системы.
- **Ошибка (Error)** Например неудачная попытка запуска службы.

Примечание Предупреждения и ошибки — два основных типа событий, на которые вам следует обратить особое внимание. Если вы не уверены, что понимаете причину их возникновения, просмотрите детальное описание.

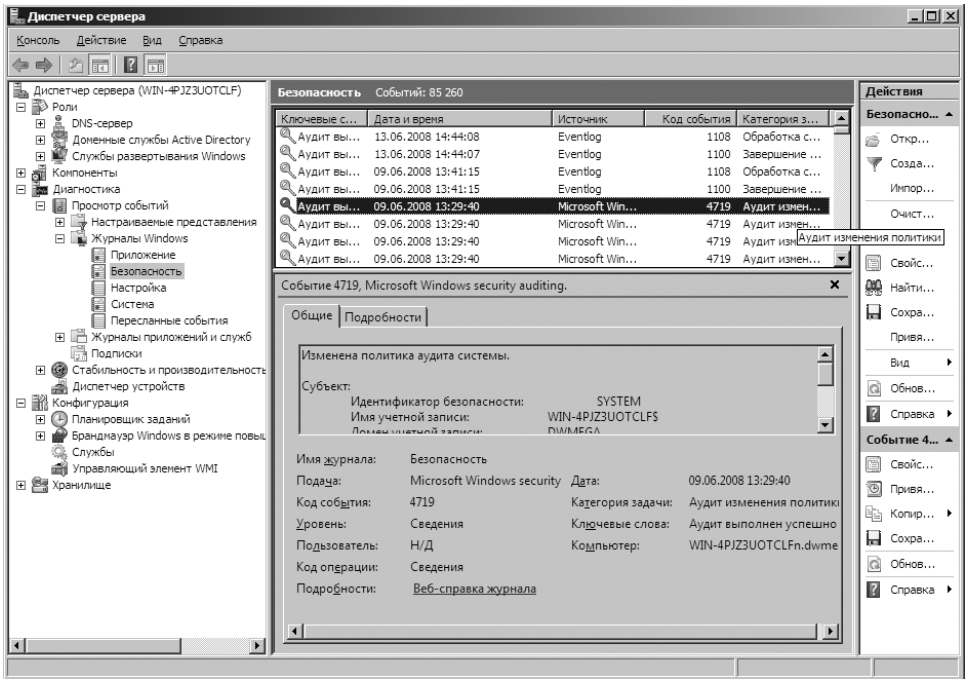


Рис. 4-11. В консоли Просмотр событий (Event Viewer) показаны события выбранного журнала или представления

Помимо уровня, даты и времени регистрации, в кратких и подробных записях о событии представлена следующая информация:

- **Источник (Source)** Приложение, служба или компонент, зарегистрировавший событие.
- **Код события (Event ID)** Как правило, числовой идентификатор, который может пригодиться при поиске по базам знаний.
- **Категория задачи (Task Category)** Категория события, которая почти всегда имеет значение **Отсутствует (None)**, но иногда используется для дополнительного описания события.
- **Пользователь (User)** Учетная запись пользователя, который был зарегистрирован, когда произошло событие.

- **Компьютер (Computer)** Имя компьютера, на котором произошло событие.
- **Подробности (Description)** В подробных записях — текстовое описание события.
- **Данные (Data)** В подробных записях — код ошибки, возвращенный событием.

Фильтрование журналов событий

В консоли **Просмотр событий (Event Viewer)** автоматически создано несколько представлений с фильтрами. Они включены в узел **Настраиваемые представления (Custom Views)**. Выделив узел **События управления (Administrative Events)**, вы получите список всех ошибок и предупреждений из всех журналов. Выделив узел **Роли сервера (Server Roles)** и выбрав представление, относящееся к определенной роли, вы получите список всех событий этой роли.

Чтобы создать собственное представление, выполните следующие действия:

1. В диспетчере сервера разверните узлы **Диагностика (Diagnostics)** и **Просмотр событий (Event Viewer)**.
2. Выделите узел **Настраиваемые представления (Custom Views)**. В области действий или в меню **Действие (Action)** выберите команду **Создать настраиваемое представление (Create Custom View)**. Откроется диалоговое окно, показанное на рис. 4-12.
3. В списке **Дата (Logged)** выберите интервал времени для просмотра событий — **Последний час (Last Hour)**, **Последние 12 часов (Last 12 Hours)**, **Последние 24 часа (Last 24 Hours)**, **Последние 7 дней (Last 7 Days)** или **Последние 30 дней (Last 30 Days)**.
4. При помощи флажков **Уровень события (Event Level)** укажите уровень событий, включаемых в представление. Установите флажок **Подробности (Verbose)**, чтобы получить дополнительные сведения.
5. Создайте пользовательское представление для определенного набора журналов или источников событий:
   - В списке **Журналы событий (Event logs)** выберите включаемые журналы событий. Можно выбрать несколько журналов, установив соответствующие флажки. Все остальные журналы событий будут исключены из представления.
   - В списке **Источники событий (Event Sources)** выберите включаемые источники событий. Можно выбрать несколько источников событий, установив соответствующие флажки. Остальные источники событий будут исключены из представления.

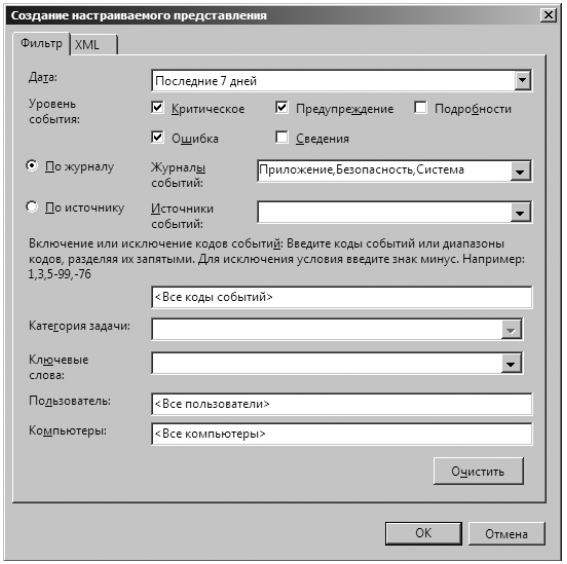


Рис. 4-12. Вы можете отфильтровать журналы так, чтобы отображались только определенные события

6. При желании в полях **Пользователь (User)** и **Компьютеры (Computer(s))** укажите включаемых пользователей и компьютеры. Если вы этого не сделаете, будут включены события всех пользователей и компьютеров.
7. Щелкните **OK**. Откроется диалоговое окно **Сохранить фильтр в настраиваемое представление (Save Filter To Custom View)**, показанное на рис. 4-13.

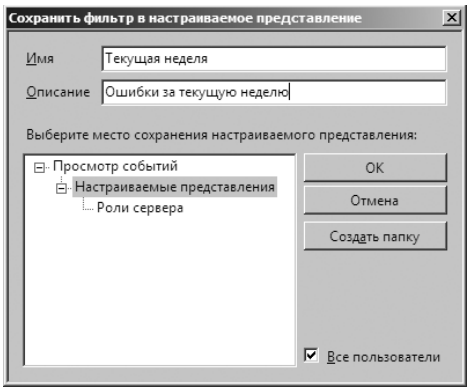


Рис. 4-13. Сохранение отфильтрованного представления

8. Введите имя и описание представления.
9. Укажите, где нужно сохранить представление. По умолчанию они сохраняются в узле **Настраиваемые представления (Custom Views)**. Вы можете создать новый узел, щелкнув **Создать папку (New Folder)**, введя имя новой папки и щелкнув **OK**.

10. Щелкните **OK**, чтобы закрыть диалоговое окно **Сохранить фильтр в настраиваемое представление (Save Filter To Custom View)**. Теперь вы должны увидеть список событий, ограниченный фильтрами. Внимательно изучите этот список и предпримите меры для устранения проблем.

Чтобы просмотреть события определенного типа, отфильтруйте журнал, выполнив следующие действия:

1. В диспетчере сервера разверните узлы **Диагностика (Diagnostics)** и **Просмотр событий (Event Viewer)**.
2. Разверните узел **Журналы Windows (Windows Logs)** или **Журналы приложений и служб (Applications And Services Logs)**. Появится список журналов событий.
3. Выберите журнал, с которым хотите работать. В области действий или в меню **Действие (Action)** выберите команду **Фильтр текущего журнала (Filter Current Log)**. Откроется диалоговое окно, подобное окну на рис. 4-12.
4. В списке **Дата (Logged)** выберите интервал времени для просмотра событий — **Последний час (Last Hour)**, **Последние 12 часов (Last 12 Hours)**, **Последние 24 часа (Last 24 Hours)**, **Последние 7 дней (Last 7 Days)** или **Последние 30 дней (Last 30 Days)**.
5. При помощи флажков **Уровень события (Event Level)** укажите уровень событий, включаемых в представление. Установите флажок **Подробности (Verbose)**, чтобы получить дополнительные сведения.
6. Выберите в списке **Источники событий (Event Sources)** источники событий, включаемые в фильтр. Если вы выберете определенные источники событий, остальные источники будут исключены.
7. При желании в полях **Пользователь (User)** и **Компьютеры (Computer(s))** укажите включаемых пользователей и компьютеры. Если вы этого не сделаете, будут включены события всех пользователей и компьютеров.
8. Щелкните **OK**. Теперь вы должны увидеть список событий, ограниченный фильтрами. Внимательно изучите этот список и предпримите меры для устранения проблем. Чтобы сбросить фильтр и увидеть все события журнала, щелкните команду **Очистить фильтр (Clear Filter)** в области действий или меню **Действие (Action)**.

Настройка параметров журнала событий

Вы можете управлять размером журналов событий, а также тем, как выполняется протоколирование. По умолчанию файлам журналов событий назначается максимальный размер. Когда журнал вырастает до этого предела, события начинают перезаписываться.

Чтобы задать параметры журнала, выполните следующие действия:

1. В диспетчере сервера разверните узлы **Диагностика (Diagnostics)** и **Просмотр событий (Event Viewer)**.

2. Разверните узел **Журналы Windows (Windows Logs)** или **Журналы приложений и службы (Applications And Services Logs)**.
3. Щелкните правой кнопкой журнал событий, параметры которого хотите изменить, и выберите в контекстном меню команду **Свойства (Properties)**. Откроется диалоговое окно, показанное на рис. 4-14.

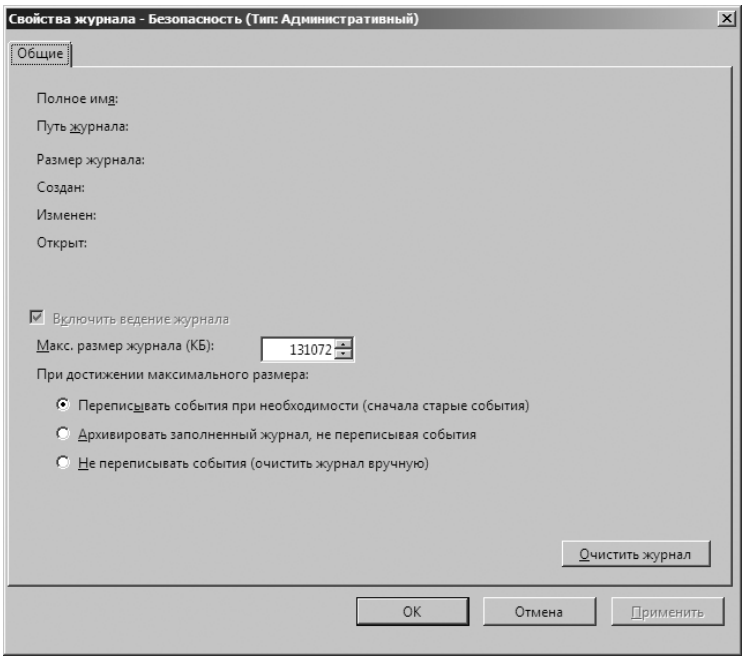


Рис. 4-14. Настройте параметры журнала в соответствии с уровнем аудита системы

4. Введите максимальный размер журнала в килобайтах в поле **Макс. размер журнала (Maximum Log Size)**. Убедитесь, что на диске ОС достаточно свободного пространства для заданного вами размера. По умолчанию файлы журналов хранятся в каталоге %SystemRoot%\System32\Winevt\Logs.
5. Задайте способ перезаписи журнала. Возможны следующие варианты:
   - **Переписывать события при необходимости (Overwrite Events As Needed (Oldest Events First))** События в журнале перезаписываются при достижении максимального размера файла. Как правило, это оптимальный вариант для системы с невысоким приоритетом.
   - **Архивировать заполненный журнал, не переписывая события (Archive The Log When Full, Do Not Overwrite Events)** При достижении максимального размера файла Windows архивирует события, сохраняя копию текущего журнала в папке по умолчанию. Затем создается новый журнал для сохранения текущих событий.
   - **Не переписывать события (очистить журнал вручную) (Do Not Overwrite Events (Clear Logs Manually))** При достижении макси-

мального размера файла система выдает сообщение об ошибке с информацией о том, что журнал событий заполнен.

6. Щелкните **OK**.

Примечание На ключевых системах, где очень важны безопасность и своевременная регистрация событий, следует использовать вариант **Архивировать заполненный журнал, не переписывая события (Archive The Log When Full, Do Not Overwrite Events)**. Этот метод гарантирует, что история событий автоматически сохраняется в архиве.

Очистка журналов событий

Если журнал событий заполнен, его необходимо очистить, выполнив следующие действия:

1. В диспетчере сервера разверните узлы **Диагностика (Diagnostics)** и **Просмотр событий (Event Viewer)**.
2. Разверните узел **Журналы Windows (Windows Logs)** или **Журналы приложений и службы (Applications And Services Logs)**.
3. Щелкните правой кнопкой мыши нужный журнал и выберите в контекстном меню команду **Очистить журнал (Clear Log)**.
4. Щелкните кнопку **Сохранить и очистить (Save And Clear)**, чтобы сохранить копию журнала перед его очисткой. Щелкните **Очистить (Clear)**, чтобы продолжить без сохранения файла журнала.

Архивирование журнала событий

На ключевых системах, например, контроллерах домена и серверах приложений, необходимо хранить журналы за несколько месяцев. Однако, как правило, неудобно обеспечивать столь длительное хранение путем увеличения максимального размера журнала. Вместо этого укажите Windows периодически архивировать журнал событий или делайте это вручную.

Форматы архива журнала

Журналы могут архивироваться в четырех форматах:

- Формат .evtx для просмотра в консоли **Просмотр событий (Event Viewer)**.
- Текст с символами табуляции в качестве разделителей (.txt) для просмотра в текстовом редакторе или для импорта в электронные таблицы и базы данных.
- Текст с запятыми в качестве разделителей (.csv) для импорта в электронные таблицы и базы данных.
- Формат XML.

При экспорте журнала в файл с разделителями-запятыми разделено каждое поле в записи о событии. Запись выглядит следующим образом:

```
Сведения,18.05.2008 09:43:24,EventLog,6005,Отсутствует,Запущена служба
журнала событий.
Предупреждение,18.05.2008 09:40:04,Microsoft-Windows-Time-Service,134,Отсут-
ствует,Ntp-клиенту не удалось задать настроенный вручную узел как источник
времени из-за ошибки разрешения имен DNS…
```

Формат записей о событии таков:

```
Уровень,Дата и время,Источник,Код события,Категория задачи,Описание
```

Создание архивов журнала

Windows автоматически создает архивы журнала, если вы выбрали режим перезаписи **Архивировать заполненный журнал, не переписывая события (Archive The Log When Full, Do Not Overwrite Events)**. Чтобы создать архив журнала вручную, выполните следующие действия:

1. В диспетчере сервера разверните узлы **Диагностика (Diagnostics)** и **Просмотр событий (Event Viewer)**.
2. Разверните узел **Журналы Windows (Windows Logs)** или **Журналы приложений и службы (Applications And Services Logs)**.
3. Щелкните правой кнопкой журнал, для которого хотите создать архив, и выберите в контекстном меню команду **Сохранить события как (Save Events As)**.
4. В диалоговом окне **Сохранить как (Save As)** выберите папку и введите имя файла журнала.
5. В списке **Тип файла (Save As Type)** по умолчанию выбрано значение **Файлы событий (*.evtx) (Event Files (*.evtx))**. Выберите подходящий формат журнала и щелкните кнопку **Сохранить (Save)**.

Примечание Если вы планируете регулярно архивировать журналы, создайте для них специальную папку, чтобы их было проще находить. Имя для файла журнала задавайте таким образом, чтобы легко было определить тип файла журнала и охваченный им период времени. Например, если вы архивируете системный журнал за январь 2009 года, назовите файл «Системный журнал январь 2009».

Совет Оптимальным форматом для архивирования является .evtx. Используйте его, если планируете просматривать старые журналы в консоли **Просмотр событий (Event Viewer)**. Если вы планируете просматривать журналы в других приложениях, возможно, вам стоит сохранять журналы в файлах с разделителями (табуляторами или запятыми). Правда, такой файл иногда приходится редактировать в текстовом редакторе, чтобы его можно было правильно интерпретировать. Журнал, сохраненный в формате .evtx, вы впоследствии всегда можете сохранить в другом формате, открыв архив в консоли **Просмотр событий (Event Viewer)** и выбрав команду **Сохранить как (Save As)**.

Просмотр архивов журнала

Сохранив архивы журнала в текстовом формате, вы можете просмотреть их в любом текстовом редакторе. Архивы в формате журнала событий следу-

ет просматривать в консоли **Просмотр событий (Event Viewer)**. Для этого нужно выполнить следующие действия:

1. В окне **Диспетчер сервера (Server Manager)** щелкните правой кнопкой мыши узел **Просмотр событий (Event Viewer)**. Выберите в контекстном меню команду **Открыть сохраненный журнал (Open Saved Log File)**.
2. В диалоговом окне **Открыть (Open)** найдите нужную папку и выберите файл журнала. В списке форматов по умолчанию выбран вариант **Файлы журнала событий (Event Logs Files)**. Это означает, что показаны будут файлы с расширениями .evtx, .evt и .etl. Каждый из этих типов можно также выбрать по отдельности.
3. Щелкните **Открыть (Open)**. Windows выведет диалоговое окно **Открыть сохраненный журнал (Open Saved Log)**.
4. Введите имя и описание сохраненного журнала.
5. Укажите, куда сохранить журнал. По умолчанию сохраненные журналы помещаются в узел **Сохраненные журналы (Saved Logs)**. Вы можете создать новый узел, щелкнув **Создать папку (New Folder)**. Введите имя новой папки и щелкните **OK**.
6. Щелкните **OK**, чтобы закрыть диалоговое окно **Открыть сохраненный журнал (Open Saved Log)**. Теперь вы должны увидеть содержимое сохраненного файла.

Совет Чтобы удалить сохраненный журнал из консоли **Просмотр событий (Event Viewer)**, щелкните команду **Удалить (Delete)** в области действий или в меню **Действие (Action)**. В запросе на подтверждение щелкните **Да (Yes)**. Сохраненный файл журнала по-прежнему останется там же, где и был.

Мониторинг производительности и работы сервера

Мониторинг сервера нельзя осуществлять бессистемно. У вас должен быть четкий план со списком целей, которых вы хотите достичь. Рассмотрим причины, которые заставляют проводить мониторинг сервера, и инструменты, которые помогут вам в этом.

Зачем нужен мониторинг сервера?

Главный повод для мониторинга — устранение проблем в работе. Допустим, у пользователей возникли сложности с подключением к серверу, и вы хотите при помощи мониторинга выявить причину.

Другая частая причина мониторинга сервера — стремление повысить его производительность. Для этого нужно оптимизировать дисковые операции, снизить нагрузку на процессор, сократить сетевой трафик сервера. К сожалению, когда речь идет об использовании ресурсов, часто приходится принимать компромиссные решения. Например, если растет число пользователей, работающих с сервером, вам вряд ли удастся сократить сетевой трафик, но у вас всегда есть возможность повысить производительность сервера,

сбалансировав сетевую нагрузку или распределив основные файлы данных по разным дискам.

Подготовка к мониторингу

Прежде чем приступить к мониторингу сервера, следует определить базовый уровень показателей его производительности, оценив работу сервера в различное время при разной нагрузке. Затем вы будете сравнивать базовый уровень с результатами последующих измерений производительности, чтобы определить эффективность работы сервера. Показатели производительности, существенно превышающие базовый уровень, указывают на области, в которых сервер необходимо оптимизировать или перенастроить.

Определив базовый уровень, сформулируйте план мониторинга. Он, как правило, включает в себя следующие этапы:

1. Выбор событий, за которыми вы будете следить.
2. Настройка фильтров для уменьшения объема собираемой информации.
3. Настройка счетчиков производительности для контроля за использованием ресурсов.
4. Протоколирование информации о событиях.
5. Анализ информации и выявление проблем.

Каждый из этих этапов подробно рассматривается далее в этом разделе. Иногда некоторые из них можно пропустить. Например, вместо протоколирования информации и последующего изучения можно осуществлять мониторинг работы сервера и анализ результатов в реальном времени.

Основные инструменты мониторинга таковы:

- **Системный монитор (Performance Monitor)** Здесь вы при помощи счетчиков следите за тем, как со временем меняется загруженность ресурсов. Используйте эту информацию для оценки производительности сервера и выявления областей, которым не помешает оптимизация.
- **Монитор стабильности системы (Reliability Monitor)** В нем изменения в системе сопоставляются с изменениями в стабильности системы, в графическом виде представляя связь между изменениями системной конфигурации и устойчивостью ее работы.
- **Журналы событий** Используйте их для выявления системных проблем, включая ОС и установленные приложения. Чаще всего вы будете работать с журналами **Система (System)**, **Безопасность (Security)** и **Приложение (Application)**, а также с журналами ролей сервера.

Консоль Надежность и производительность (Reliability And Performance)

Предпочтительный инструмент для настройки производительности — консоль **Надежность и производительность (Reliability And Performance)**. Чтобы получить доступ непосредственно к ней, щелкните кнопку **Пуск**

(Start), раскройте меню **Администрирование (Administrative Tools)** и выберите команду **Монитор надежности и производительности (Reliability And Performance Monitor)**. В окне **Диспетчер сервера (Server Manager)** эта консоль размещена в узле **Диагностика (Diagnostics)**. Разверните узел **Диагностика (Diagnostics)** и выделите узел **Стабильность и производительность (Reliability And Performance)**. Как показано на рис. 4-15, статистика использования ресурсов разделена на четыре категории:

- **ЦП (CPU Usage)** Здесь показана текущая загруженность процессора в сравнении с максимальной нагрузкой на него. Если вы развернете соответствующий элемент под графиком, щелкнув белую стрелку в его правой части, то увидите список работающих в данный момент исполняемых модулей с именами, кодами процессов, описаниями, числом используемых потоков, текущей и средней нагрузкой на процессор.
- **Диск (Disk Usage)** Количество килобайт в секунду, считываемых или записываемых на диск, а также максимальная нагрузка. Если вы развернете соответствующий элемент под графиком, щелкнув белую стрелку в его правой части, то увидите список работающих в данный момент исполняемых модулей, осуществляющих операции ввода-вывода, с именами, кодами процессов, описаниями, указанием файлов, в которые производились запись или чтение, количеством байтов, считываемых и записываемых в минуту, приоритетом ввода-вывода и временем отклика диска.
- **Сеть (Network Usage)** Текущее использование полосы пропускания сети. Если вы развернете соответствующий элемент под графиком, щелкнув белую стрелку в его правой части, то увидите список работающих в данный момент исполняемых модулей, которые передавали или передают данные по сети, с именами, кодами процессов, IP-адресами, с которым производится взаимодействие, количеством байтов, передаваемых и получаемых в минуту, а также суммарным трафиком.
- **Память (Memory Usage)** Текущее использование памяти и число отказов в секунду. Если вы развернете соответствующий элемент под графиком, щелкнув белую стрелку в его правой части, то увидите список работающих в данный момент исполняемых модулей с именами, кодами процессов, числом ошибок в минуту, объемом выделенной памяти в килобайтах, рабочим набором памяти в килобайтах, объемом разделяемой и неразделяемой памяти в килобайтах.

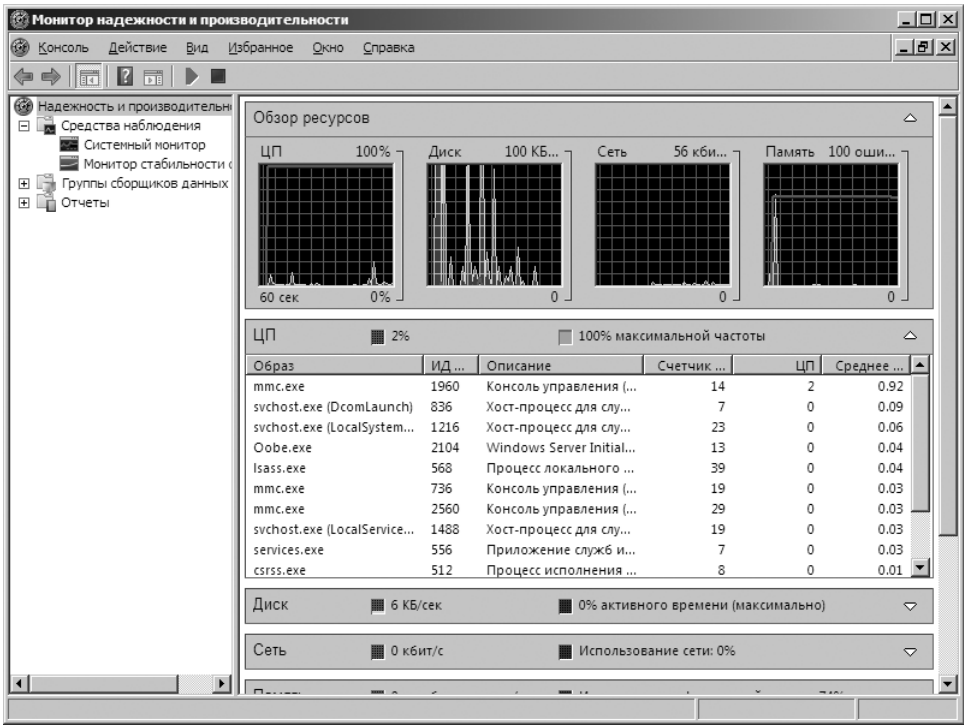


Рис. 4-15. Обзор использования ресурсов сервера

В узле **Средства наблюдения (Monitoring Tools)** консоли **Надежность и производительность (Reliability And Performance)** вы найдете два дополнительных инструмента:

- **Системный монитор (Performance Monitor)**;
- **Монитор стабильности системы (Reliability Monitor)**.

В **Системном мониторе (Performance Monitor)** графически представлена статистика для заданных *счетчиков* (counter) производительности. Доступные счетчики определяются набором установленных на сервере служб и компонентов.

Как показано на рис. 4-16, в окне **Системный монитор (Performance Monitor)** отслеживаемые счетчики представлены в виде диаграммы. Интервал обновления диаграммы по умолчанию равен 1 секунде, но его можно изменить. Работая с **Системным монитором (Performance Monitor)**, вы вскоре убедитесь, что его информацию удобно сохранить в файле для последующего воспроизведения. С помощью **Системного монитора (Performance Monitor)** можно также настроить оповещения, чтобы своевременно узнавать об определенных событиях.

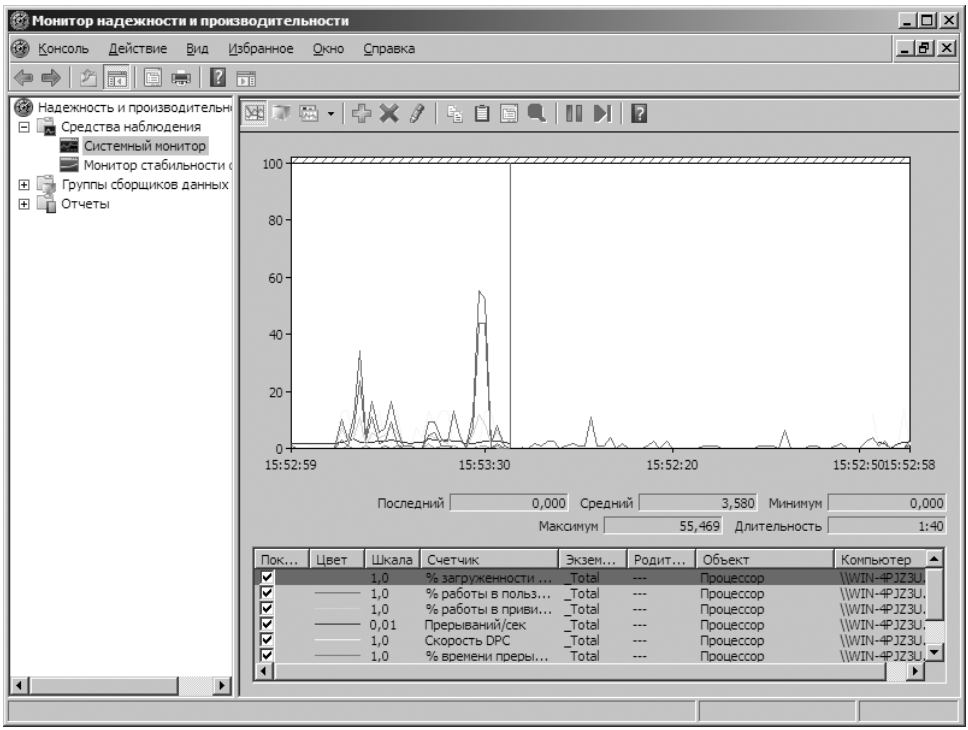


Рис. 4-16. Обзор параметров производительности сервера

Консоль **Надежность и производительность (Reliability And Performance)** также включает в себя **Монитор стабильности системы (Reliability Monitor)**, показанный на рис. 4-17. Он отслеживает изменения на сервере и сопоставляет их со стабильностью системы. С помощью этого монитора вы в графическом виде оцените связь устойчивости системы с установкой и удалением программ, ошибками приложений, аппаратными сбоями, ошибками ОС, а также изменениями в конфигурации сервера. Затем вы используете эту информацию для более тщательного анализа изменений, которые вызвали нарушение стабильности. Если вы отметили внезапное падение устойчивости, щелкните точку данных и разверните относящийся к ней набор данных, например, **Ошибки приложений (Application Failure)** или **Неполадки оборудования (Hardware Failure)**, чтобы выявить конкретное событие, которое привело к снижению стабильности.

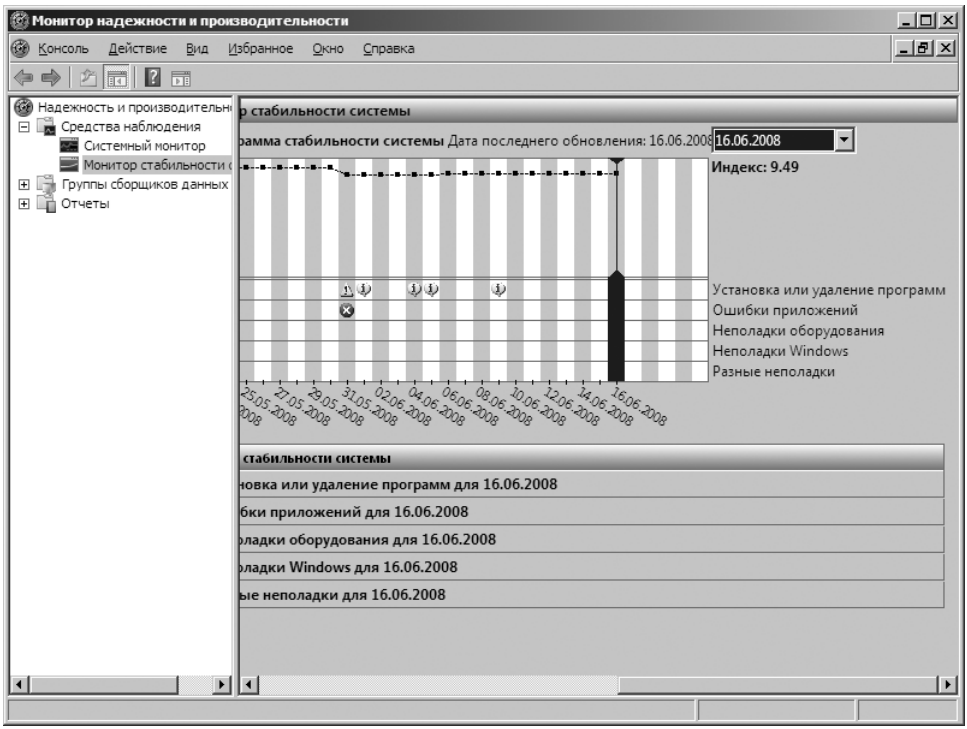


Рис. 4-17. Обзор стабильности сервера

Выбор счетчиков для мониторинга

Инструмент **Системный монитор (Performance Monitor)** отображает информацию только для выбранных вами счетчиков. Вам предлагаются тысячи счетчиков, относящихся практически к каждой установленной роли сервера. Самый простой способ получить сведения об этих счетчиках — прочитать их описания в диалоговом окне **Добавить счетчики (Add Counters)**. Запустите **Системный монитор (Performance Monitor)**, щелкните кнопку **Добавить (Add)** на панели инструментов и разверните нужный объект в списке **Имеющиеся счетчики (Available Counters)**. Затем установите флажок **Отображать описание (Show Description)** и просмотрите список счетчиков данного объекта.

Системный монитор (Performance Monitor) способен отслеживать все экземпляры всех счетчиков конкретного объекта. Например, когда вы отслеживаете счетчики для объекта **Процессор (Processor)** на многопроцессорной системе, у вас имеется выбор — контролировать экземпляры всех процессоров или определенного процессора. Если вы подозреваете, что один из процессоров работает нестабильно или испытывает другие проблемы, отслеживайте экземпляр только этого процессора.

Чтобы выбрать счетчики, выполните следующие действия:

1. В консоли **Надежность и производительность (Reliability And Performance)** разверните узел **Средства наблюдения (Monitoring Tools)** и выберите **Системный монитор (Performance Monitor)**.
2. У **Системного монитора (Performance Monitor)** есть несколько представлений. Щелкните значок **Просмотр текущей активности (View Current Activity)** на панели инструментов или нажмите Ctrl+T. Чтобы выбрать тип представления — **Строка (Line)**, **Линейчатая гистограмма (Histogram Bar)** или **Отчет(Report)**, — щелкните кнопку **Изменить тип диаграммы (Change Graph Type)** или нажмите Ctrl+G.

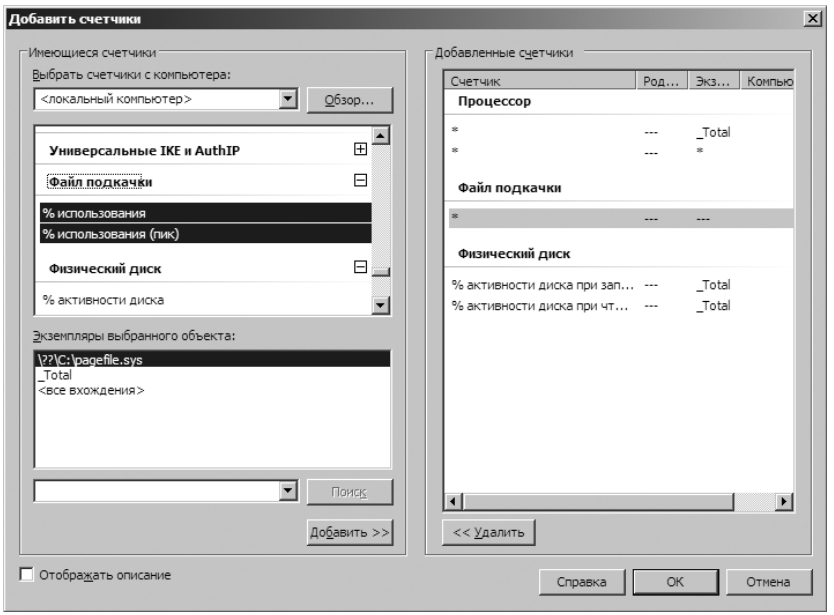


Рис. 4-18. Выбор объектов и счетчиков для мониторинга

3. Чтобы добавить счетчики, щелкните кнопку **Добавить (Add)** на панели инструментов или нажмите Ctrl+I. Откроется диалоговое окно **Добавить счетчики (Add Counters)**, показанное на рис. 4-18.
4. В поле **Выбрать счетчики с компьютера (Select Counters From Computer)** введите UNC-имя сервера, с которым хотите работать, например, **CorpServer84**, или выберите вариант **Локальный компьютер (Local Computer)**.

Примечание Чтобы выполнять удаленный мониторинг, вы должны входить в группу уровнем не ниже группы **Пользователи системного монитора (Performance Monitor Users)** домена или локального компьютера. Чтобы работать с журналами производительности на удаленных компьютерах, вы должны входить в группу **Пользователи журналов производительности (Performance Log Users)** домена или локального компьютера.

5. В списке **Имеющиеся счетчики (Available Counters)** в алфавитном порядке перечислены объекты производительности. Если вы выбираете элемент списка, выбираются все соответствующие ему счетчики. Развернув узел объекта, вы увидите список его счетчиков, и сможете выбрать из них те, что вам нужны.
6. Когда вы выбираете объект или любой из его счетчиков, под списком отображаются доступные экземпляры. Выберите вариант **Все вхождения (All Instances)**, чтобы осуществлять мониторинг всех экземпляров, или укажите один или несколько конкретных экземпляров.
7. Выбрав объект или группу счетчиков для объекта, а также экземпляры объекта, щелкните **Добавить (Add)**, чтобы добавить счетчики на диаграмму. Повторите шаги 5–7, чтобы добавить другие счетчики производительности.
8. Завершив добавление счетчиков, щелкните **ОК**.

Совет Не выводите на диаграмму слишком много счетчиков или их экземпляров одновременно. Это затрудняет восприятие информации и к тому же перегружает системные ресурсы, точнее, время процессора и память, что отразится на доступности сервера.

Журналы производительности

Новинка Windows Server 2008 — группы сборщиков данных (data collector set) и отчеты (report). Группы сборщиков данных позволяют создавать списки объектов производительности и счетчиков, которые нужно отслеживать. Создав группу сборщиков данных, вы с легкостью запустите или остановите мониторинг объектов производительности и счетчиков, включенных в группу. В некоторой степени это делает группы похожими на журналы производительности из предыдущих версий Windows. Однако группы сборщиков данных намного проще. Группу можно применять для создания нескольких журналов производительности и трассировки. Кроме того, вы можете:

- управлять доступом к собранным данным;
- создать несколько расписаний выполнения и условий остановки мониторинга;
- использовать диспетчеры данных для управления размером собранных данных и отчетов:
- создавать отчеты на основе собранных данных.

В консоли **Надежность и производительность (Reliability And Performance)** сконфигурированные в данный момент группы сборщиков данных и отчеты расположены в узлах **Группы сборщиков данных (Data Collector Sets)** и **Отчеты (Reports)**, соответственно. Как показано на рис. 4-19, группы данных и отчеты делятся на пользовательские (особые) и системные. Группы сборщиков данных, созданные пользователем, применяются для общего мониторинга и настройки производительности. Системные группы

данных создаются операционной системой для автоматизированной диагностики.

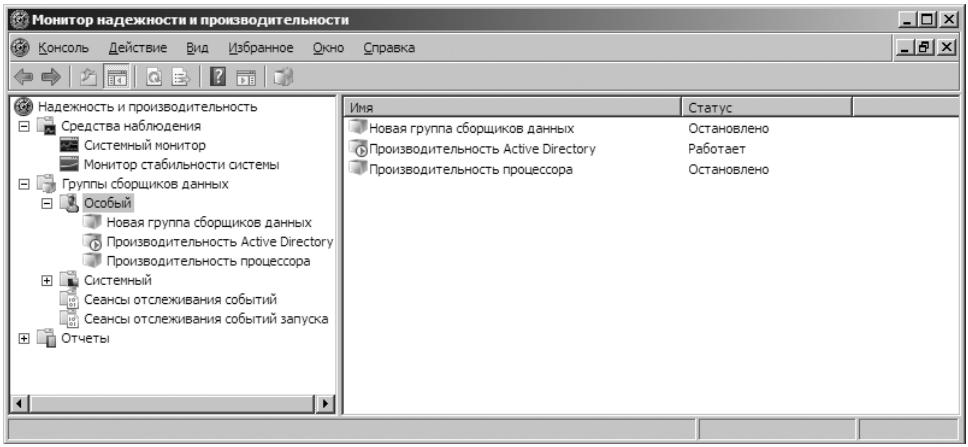


Рис. 4-19. Доступ к группам сборщиков данных и отчетам

Создание и управление группами сборщиков данных

Чтобы просмотреть настроенные в данный момент группы сборщиков данных, запустите **Монитор надежности и производительности (Reliability And Performance Monitor)**, выбрав одноименную команду в меню **Администрирование (Administrative Tools)**, и разверните узел **Группы сборщиков данных (Data Collector Sets)**. Работать со сборщиками данных можно несколькими способами.

- Чтобы просмотреть настроенные в данный момент пользовательские или системные группы сборщиков данных, выделите узлы **Особый (User Defined)** или **Системный (System)**, соответственно. Выделив группу сборщиков данных в левой панели, вы увидите в области сведений список соответствующих сборщиков данных с указанием имени и типа. Тип **Слежение (Trace)** относится к сборщикам, записывающим данные о производительности при возникновении соответствующего события. Тип **Счетчик производительности (Performance Counter)** означает, что сборщик записывает данные по выбранным счетчикам через определенные интервалы времени. Тип **Настройка (Configuration)** относится к сборщикам, которые отслеживают изменения определенных разделов реестра.
- Чтобы просмотреть работающие трассировки событий, выделите узел **Сеансы отслеживания событий (Event Trace Sessions)**. Чтобы остановить сборщик данных, выполняющий отслеживание, щелкните его правой кнопкой и выберите команду **Стоп (Stop)**.
- Чтобы просмотреть состояние трассировок, настроенных на автоматический запуск при включении компьютера, выделите узел **Сеансы отслеживания событий запуска (Startup Event Trace Sessions)**. Вы можете запустить трассировку, щелкнув правой кнопкой мыши сборщик данных

и выбрав **Запустить как сеанс отслеживания событий (Start As Event Trace Session)**. Чтобы удалить сборщик данных, щелкните его правой кнопкой мыши и выберите **Удалить (Delete)**.

- Чтобы сохранить сборщик данных как шаблон, который будет использован в качестве основы для других сборщиков, щелкните его правой кнопкой мыши и выберите **Сохранить шаблон (Save Template)**. В диалоговом окне **Сохранить как (Save As)** выберите папку, введите имя шаблона и щелкните **Сохранить (Save)**. Шаблон сборщика данных сохраняется в XML-файле, который можно копировать на другие компьютеры.
- Чтобы удалить пользовательский сборщик данных, щелкните его правой кнопкой мыши и выберите **Удалить (Delete)**. Если сборщик работает, вам следует сначала остановить сбор данных. Удаление сборщика удаляет и соответствующие отчеты.

Сбор данных счетчика производительности

Сборщики данных могут использоваться для записи данных производительности по выбранным счетчикам с определенным интервалом времени. Например, можно измерять показатели производительности процессора каждые 15 минут.

Чтобы собрать данные счетчика производительности, выполните следующие действия:

1. В **Мониторе надежности и производительности (Reliability And Performance Monitor)** разверните узел **Группы сборщиков данных (Data Collector Sets)**, щелкните правой кнопкой узел **Особый (User-Defined)**, выберите **Создать (New)** и **Группа сборщиков данных (Data Collector Set)**.
2. В мастере **Создать новую группу сборщиков данных (Create New Data Collector Set Wizard)** введите имя сборщика данных, например, **Монитор производительности системы** или **Монитор состояния процессора**.
3. Установите переключатель **Создать вручную (Create Manually)** и щелкните **Далее (Next)**.
4. На странице **Какой тип данных необходимо использовать (What Type Of Data Do You Want To Include)** по умолчанию установлен переключатель **Создать журналы данных (Create Data Logs)**. Установите флажок **Счетчик производительности (Performance Counter)** и щелкните **Далее (Next)**.
5. На странице **Какие счетчики производительности следует записывать в журнал (Which Performance Counters Would You Like To Log)** щелкните кнопку **Добавить (Add)**. Откроется диалоговое окно **Добавить счетчики (Add Counter)**, которое было описано ранее. Выберите счетчики и щелкните **OK**.
6. На той же странице задайте интервал выборки, указав единицу времени — секунды, минуты, часы, дни или недели. Интервал выборки определяет, как будут собираться новые данные. Например, если вы задали 15-минут-

ный интервал, журнал будет обновляться каждые 15 минут. Затем щелкните **Далее (Next)**.

7. На странице **Где необходимо сохранить данные (Where Would You Like The Data To Be Saved)** введите путь, который будет использоваться для хранения собранных данных, или найдите нужную папку, щелкнув кнопку **Обзор** (Browse). Затем щелкните **Далее (Next)**.

Ближе к реальности По умолчанию журналы сохраняются в папке %SystemRoot%\PerfLogs\Admin. Их файлы могут очень быстро увеличиваться в размерах. Если вы планируете собирать данные в течение продолжительного периода, убедитесь, что поместили файл журнала на диске с достаточным свободным пространством. Помните, что чем чаще вы обновляете файл журнала, тем активнее используются ресурсы диска и процессора системы.

8. На странице **Создать группу сборщиков данных (Create Data Collector Set)** в поле **Пользователь (Run As)** стоит значение **По умолчанию (Default)**. Это означает, что журнал будет работать с разрешениями и полномочиями системной учетной записи по умолчанию. Чтобы вести журнал от имени другого пользователя, щелкните **Изменить (Change)**. Введите имя пользователя и пароль для нужно учетной записи и щелкните **OK**. Имена пользователей могут вводиться в формате Домен\Имя пользователя, например, CPANDL\WilliamS для учетной записи WilliamS домена CPANDL.
9. Установите переключатель **Открыть свойства группы сборщиков данных (Open Properties For This Data Collector Set)** и щелкните **Готово (Finish)**. При этом сборщик данных будет сохранен, мастер закроется и откроется диалоговое окно **Свойства (Properties)**.
10. По умолчанию ведение журнала настроено на ручной запуск. Чтобы задать расписание ведения журнала, перейдите на вкладку **Расписание (Schedule)** и щелкните кнопку **Добавить (Add)**. Задайте параметры в разделе **Активный диапазон (Active Range)**, **Время запуска (Start Time)** и дни недели для сбора данных.
11. По умолчанию ведение журнала останавливается в соответствии с заданным вами расписанием. Используя вкладку **Условие остановки (Stop Condition),** вы можете указать, что заполнение файла журнала нужно остановить по истечению заданного времени, например, через семь дней, или при заполнении файла журнала (если вы ограничили его размер).
12. Настроив расписание и условие остановки, щелкните **OK**. Управление сборщиками данных описано ранее в разделе «Создание и управление группами сборщиков данных».

Примечание При остановке сбора данных можно запускать определенную задачу. Ее параметры настраиваются на вкладке **Задача (Task)** диалогового окна **Свойства (Properties)**.

Отслеживание данных производительности

Сборщики данных можно использовать для трассировки производительности при возникновении событий, относящихся к определенным поставщикам. Поставщик — это приложение или служба ОС, для которых определены отслеживаемые события.

Чтобы собрать данные трассировки, выполните следующие действия:

1. В **Мониторе надежности и производительности (Reliability And Performance Monitor)** разверните узел **Группы сборщиков данных (Data Collector Sets)**, щелкните правой кнопкой узел **Особый (User-Defined)** в левой панели и выберите **Создать (New)** и **Группа сборщиков данных (Data Collector Set)**.
2. В мастере **Создать новую группу сборщиков данных (Create New Data Collector Set Wizard)** введите имя сборщика данных, например, **Отслеживание входа в систему** или **Отслеживание дискового ввода-вывода**.
3. Установите флажок **Создать вручную (Create Manually)** и щелкните **Далее (Next)**.
4. На странице **Какой тип данных необходимо использовать (What Type Of Data Do You Want To Include)** установите переключатель **Создать журналы данных (Create Data Logs)** и флажок **Данные отслеживания событий (Event Trace Data)**. Затем щелкните **Далее (Next)**.
5. На странице **Какие службы трассировки событий должны быть включены (Which Event Trace Providers Would You Like To Enable)** щелкните **Добавить (Add)**. Выберите поставщика отслеживания событий, например, **Active Directory Domain Services: Core**, и щелкните **ОК**. Выберите отдельные свойства в списке **Свойства (Properties)** и щелкните **Изменить (Edit)**, чтобы отслеживать не все свойства поставщика, а только заданные вами. Повторите этот процесс для другого поставщика отслеживания событий. Затем щелкните **Далее (Next)**.
6. Выполните шаги 7–12 из предыдущего раздела.

Сбор данных конфигурации

Вы можете использовать сборщики данных для записи изменений в конфигурации реестра. Чтобы собрать данные конфигурации, выполните следующие действия:

1. В **Мониторе надежности и производительности (Reliability And Performance Monitor)** разверните узел **Группы сборщиков данных (Data Collector Sets)**, щелкните правой кнопкой узел **Особый (User-Defined)** в левой панели и выберите **Создать (New)** и **Группа сборщиков данных (Data Collector Set)**.
2. В мастере **Создать новую группу сборщиков данных (Create New Data Collector Set Wizard)** введите имя сборщика данных, например, **Реестр AD**.
3. Установите флажок **Создать вручную (Create Manually)** и щелкните **Далее (Next)**.

4. На странице **Какой тип данных необходимо использовать (What Type Of Data Do You Want To Include)** установите переключатель **Создать журналы данных (Create Data Logs)** и флажок **Сведения о конфигурации системы (System Configuration Information)**. Затем щелкните **Далее (Next)**.
5. На странице **Какие разделы реестра следует записывать (Which Registry Keys Would You Like To Record)** щелкните **Добавить (Add)**. Введите раздел реестра, за которым хотите следить. Повторите эти действия для всех нужных разделов реестра. Затем щелкните **Далее (Next)**.
6. Выполните шаги 7–12 из раздела «Сбор данных счетчика производительности».

Просмотр отчетов сборщика данных

Для выявления проблем часто приходится записывать данные по производительности в течение длительного времени, а затем просматривать их для подробного анализа. Для каждого сборщика, который был активен ранее или активен в данный момент, имеются соответствующие отчеты. Они, как и сами сборщики, разделены на две категории: пользовательские и системные.

Чтобы просмотреть отчеты сборщиков данных в **Мониторе надежности и производительности (Reliability And Performance Monitor)**, разверните узел **Отчеты (Reports)**, затем — узел отчета для сборщика данных, который вы хотите просмотреть. В узле отчета находятся отдельные отчеты для каждого сеанса протоколирования. Сеанс протоколирования начинается с запуском журнала и завершается при его остановке.

У самого последнего журнала — самый большой номер. Если сборщик данных в данный момент работает, самый новый журнал просмотреть нельзя. Остановите сбор данных, щелкнув сборщик данных правой кнопкой и выбрав команду **Стоп (Stop)**. Собранные данные по умолчанию показываются в графическом виде с начала сбора данных до его окончания.

Чтобы изменить свойства отчета, выполните следующие действия:

1. Открыв отчет, щелкните кнопку **Свойства (Properties)** на панели инструментов или нажмите Ctrl+Q. Откроется диалоговое окно **Свойства: Системный монитор (Performance Monitor Properties)**.
2. Перейдите на вкладку **Источник (Source)**.
3. Выберите источники данных для анализа. В разделе **Источник данных (Data Source)** установите переключатель **Файлы журнала (Log Files)** и щелкните **Добавить (Add)**, чтобы открыть диалоговое окно **Выбор файла журнала (Select Log File)**. Можно выбрать для анализа несколько файлов.
4. Задайте интервал времени для анализа. Щелкните кнопку **Диапазон времени (Time Range)**, затем на полосе **Весь диапазон (Total Range)** при помощи бегунков установите время начала и окончания интервала.
5. Перейдите на вкладку **Данные (Data)** и выберите счетчики для показа. Чтобы удалить счетчик из представления, выделите его и щелкните **Уда-**

лить (Remove). Щелкните **Добавить (Add)**, чтобы открыть диалоговое окно **Добавить счетчики (Add Counter)** и добавить дополнительные счетчики.

Примечание Для добавления доступны только те счетчики, которые ранее были включены в журнал. Если вы не находите счетчика, с которым хотите работать, вам следует изменить свойства сборщика данных, перезапустить журнал и через некоторое время просмотреть его снова.

6. Щелкните **OK**. При необходимости на панели инструментов монитора щелкните кнопку **Изменить тип диаграммы (Change Graph Type)**.

Настройка оповещений счетчиков производительности

Чтобы своевременно узнавать о возникновении определенных событий или достижении пороговых значений, настройте соответствующие оповещения. Можно посылать оповещения как сетевые сообщения или записывать их как события в журнал приложения. Также оповещения способны запускать приложения и журналы производительности.

Чтобы настроить оповещение, выполните следующие действия:

1. В **Мониторе надежности и производительности (Reliability And Performance Monitor)** разверните узел **Группы сборщиков данных (Data Collector Sets)**, щелкните правой кнопкой узел **Особый (User-Defined)** и выберите **Создать (New)** и **Группа сборщиков данных (Data Collector Set)**.
2. В мастере **Создать новую группу сборщиков данных (Create New Data Collector Set Wizard)** введите имя сборщика данных, например, **Оповещение для процессора** или **Оповещение для дискового ввода-вывода**.
3. Установите переключатель **Создать вручную (Create Manually)** и щелкните **Далее (Next)**.
4. На странице **Какой тип данных необходимо использовать (What Type Of Data Do You Want To)** установите переключатель **Оповещение счетчика производительности (Performance Counter Alert)** и щелкните **Далее (Next)**.
5. На странице **Какие счетчики производительности следует контролировать (Which Performance Counters Would You Like To Monitor)** щелкните кнопку **Добавить (Add)**, чтобы открыть диалоговое окно **Добавить счетчики (Add Counters)** для добавления счетчиков, которые будут запускать данное оповещение. Выбрав счетчики, щелкните **OK**.
6. Выделите первый счетчик в списке **Системные счетчики (Performance Counters)** и задайте в поле **Оповещение при (Alert When Value Is)** пороговое условие, при котором для этого счетчика будет запускаться оповещение. Оповещения могут срабатывать, когда значение счетчика выше или ниже заданного предела в зависимости от выбранного в списке варианта — **Выше (Above)** или **Ниже (Below)**. Рядом введите пороговое значение. Единица измерения зависит от выбранного счетчика (или счет-

чиков). Например, чтобы генерировать оповещение, когда загруженность процессора превышает 95%, нужно выбрать вариант **Выше (Above)** и ввести значение **95**. Повторите эти действия для настройки других выбранных счетчиков.

7. Выполните шаги 8–12 из раздела «Сбор данных счетчика производительности».

Настройка производительности системы

Теперь, когда вы знаете, как осуществлять мониторинг системы, рассмотрим, как настроить производительность ОС и аппаратного обеспечения. Я буду обсуждать следующие вопросы:

- использование памяти и кеширование;
- загруженность процессора;
- дисковый ввод-вывод;
- пропускная способность сети и возможность подключения.

Мониторинг и настройка использования памяти

Память — один из основных источников проблем с производительностью, и потому, прежде чем углубляться в другие области системы, всегда сначала устраняйте проблемы памяти. В системах используются как физическая, так и виртуальная память. Чтобы свести вероятность проблем с памятью к минимуму, настройте производительность приложения, использование памяти и пропускную способность, а затем выполните мониторинг использования памяти сервера.

Настройками производительности приложения и использования памяти определяется распределение системных ресурсов. В большинстве случаев следует отдать львиную долю ресурсов операционной системе и фоновым приложениям. Это особенно верно в случае серверов Active Directory, файловых серверов, серверов печати, сетевых и коммуникационных серверов. С другой стороны, на серверах приложений и баз данных, серверах потокового медиа, нужно отдавать большую часть ресурсов работающим на сервере программам. Как это сделать, рассказано в разделе «Настройка производительности приложения» главы 3.

Используя различные варианты мониторинга, рассмотренные в этой главе, вы определите, как система использует память, и узнаете о наличии проблем. В табл. 4-1 перечислены счетчики, которые помогут вам выявить узкие места памяти, кеширования и виртуальной памяти (файла подкачки).

Табл. 4-1. Выявление узких мест, связанных с памятью

Область	Счетчики для отслеживания	Подробности
Использование физической и виртуальной памяти	**Память\Доступно байт (Memory\ Available Kbytes)** **Память\Байт выделенной виртуальной памяти (Memory\ Committed Bytes)**	Первый счетчик соответствует объему физической памяти, доступной для процессов, работающих на сервере. Второй счетчик равен объему выделенной виртуальной памяти. Если на сервере мало доступной памяти, возможно, придется нарастить ее объем. Как правило, желательно, чтобы объем свободной памяти был не менее 5% от общей физической памяти сервера. Если велико отношение выделенной памяти к общей физической памяти системы, вам также следует добавить память. В общем случае объем выделенной памяти не должен превышать 75% от общей физической памяти
Ошибки страниц	**Память\Ошибок страницы/сек (Memory\ Page Faults/sec)** **Память\Ввод страниц/сек (Memory\ Pages Input/sec)** **Память\Чтений страниц/сек (Memory\ Page Reads/sec)**	Ошибка страницы возникает, когда процесс запрашивает страницу в памяти, а система не может найти ее в запрошенном месте. Если запрошенная страница находится где-то в другом месте памяти, ошибка называется *программной*. Если запрошенная страница должна быть загружена с диска, то ошибка называется *аппаратной*. Большинство процессоров способны обрабатывать значительное число программных ошибок. Аппаратные ошибки могут привести к значительным задержкам. Счетчик **Память\Ошибок страницы/сек (Page Faults/sec)** указывает общий темп обработки процессором всех типов ошибки страниц. В счетчике **Память\Ввод страниц/сек (Pages Input/sec)** записывается общее число страниц, считанных с диска для разрешения аппаратных ошибок. Счетчик **Память\Чтений страниц/сек (Page Reads/sec)** представляет общее число операций чтения с диска, необходимых для разрешения аппаратных ошибок. Значение счетчика **Память\Ввод страниц/сек (Pages Input/sec)** будет больше или равно значению счетчика **Память\Чтений страниц/сек (Page Reads/sec)** и позволяет оценить темп возникновения аппаратных ошибок. Высокий темп аппаратных ошибок означает, что вам следует увеличить объем памяти или уменьшить размер кеша сервера

Табл. 4-1. (*окончание*)

Область	Счетчики для отслеживания	Подробности
Файл подкачки	**Память\Байт в выгружаемом страничном пуле (Memory\ Pool Paged Bytes)** **Память\Байт в выгружаемом страничном пуле (Memory\ Pool Nonpaged Bytes)**	Эти счетчики отслеживают число байтов в выгружаемом и невыгружаемом пуле. Выгружаемый пул — область системной памяти для объектов, которые могут быть записаны на диск в случае, если они не используются. Невыгружаемый пул — область системной памяти для объектов, которые нельзя записывать на диск. Если размер выгружаемого пула велик относительно общего объема физической памяти системы, вероятно, следует добавить в систему памяти. Если размер невыгружаемого пула велик относительно общего объема виртуальной памяти, вероятно, вам следует увеличить размер виртуальной памяти

Мониторинг и настройка использования процессора

Процессор выполняет на сервере фактическую обработку информации. Если узким местом являются процессоры, добавление памяти, дисков или сетевых адаптеров не устранит проблему. Вместо этого вам, вероятно, следует поменять процессоры на другие, с большей тактовой частотой, или увеличить количество процессоров. Также можно переместить приложения, интенсивно использующие процессор, например, SQL Server, на другой сервер.

Прежде чем принять решение о замене процессоров или их добавлении, следует исключить проблемы с памятью и кешированием. Если признаки все еще указывают на проблему с процессором, проведите мониторинг счетчиков производительности, перечисленных в табл. 4-2, для каждого процессора, установленного на сервере.

Табл. 4-2. Выявление узких мест, связанных с процессорами

Область	Счетчики для отслеживания	Подробности
Очередь потоков	**Система\Длина очереди процессора (System\Processor Queue Length)**	Этот счетчик показывает число потоков, ожидающих выполнения. Потоки выстраиваются в очередь в области, общей для всех процессоров системы. Если значение этого счетчика на протяжении длительного времени равно 2 и более, вам требуется обновить или добавить процессоры

Табл. 4-2. (*окончание*)

Область	Счетчики для отслеживания	Подробности
Использование процессора	**Процессор\% загруженности процессора (Processor\% Processor Time)**	Этот счетчик показывает долю времени, которое данный процессор затрачивает на выполнение активных потоков. Этот счетчик нужно контролировать отдельно для каждого процессора, установленного на сервере. Если его значения высоки при умеренной загруженности системы ввода-вывода и сетевого интерфейса, вам требуется обновить или добавить процессоры

Мониторинг и настройка операций ввода-вывода

Благодаря современным высокоскоростным дискам пропускная способность системы ввода-вывода теперь редко становится причиной проблем с производительностью. Отметим однако, что доступ к памяти по-прежнему выполняется намного быстрее, чем к дискам. Иными словами, если на сервере производится большое количество операций чтения и записи, его общая производительность ухудшится. Чтобы сократить число операций ввода-вывода, оптимизируйте использование памяти, чтобы сервер производил выгрузку страниц памяти на диск только в случае необходимости. Мониторинг и настройка использования памяти описаны выше.

В дополнение к настройке памяти, вы можете выполнять мониторинг некоторых счетчиков для оценки активности дискового ввода/вывода. Особенно вам следует следить за счетчиками, перечисленными в табл. 4-3.

Табл. 4-3. Выявление узких мест, связанных с диском

Область	Счетчики для отслеживания	Подробности
Общая производительность диска	**Физический диск\% активности диска (PhysicalDisk\% Disk Time)** **Процессор % загруженности процессора (Processor\% Processor Time)** **Сетевой интерфейс\Всего байт/сек (Network Interface Connection\Bytes Total/sec)**	Если значение счетчика **% активности диска (% Disk Time)** велико при умеренной загруженности процессора и сетевого подключения, жесткий диск может стать причиной снижения производительности. Отслеживайте значение этого счетчика для всех жестких дисков сервера

Табл. 4-3. (*окончание*)

Область	Счетчики для отслеживания	Подробности
Дисковый ввод-вывод	**Физический диск\ Обращений записи на диск/сек (PhysicalDisk\Disk Writes/sec)** **Физический диск\ Обращений чтения с диска/сек (PhysicalDisk\Disk Reads/sec)** **Физический диск\ Средняя длина очереди записи на диск (PhysicalDisk\Avg. Disk Write Queue Length)** **Физический диск\ Средняя длина очереди чтения диска (PhysicalDisk\Avg. Disk Read Queue Length)** **Физический диск\ Текущая длина очереди диска (PhysicalDisk\ Current Disk Queue Length)**	Число операций записи и чтения в секунду демонстрирует интенсивность дискового ввода-вывода. Длина очередей чтения и записи подскажет, сколько запросов на чтение или запись ожидают обработки. В общем случае, желательно, чтобы ожидающих запросов было поменьше. Помните, что задержки запросов пропорциональны длине очереди за вычетом числа дисков в массиве RAID

Мониторинг и настройка сетевого подключения

Ни один фактор не отражается так же сильно на впечатлениях пользователя о производительности сервера, как сеть, соединяющая сервер с клиентскими компьютерами. Интервал времени между отправкой запроса и получением ответа может быть очень разным. Длительное время ожидания сведет на нет преимущества даже самого быстрого сервера на планете: столкнувшись с задержкой, пользователь скажет, что сервер работает медленно.

Вообще говоря, сетевые задержки, с которыми сталкиваются пользователи, не входят в вашу компетенцию. Они зависят от типа пользовательского соединения и от маршрута, по которому запрос доставляется на сервер. Однако в ваших силах повысить общую производительность сервера по части обработки запросов и его пропускную способность.

В ряде случаев ограничивающим фактором становится пропускная способность сетевых плат. В большинстве серверов используются сетевые платы 10/100, которые допускают множество вариантов настройки. Проверьте: возможно, плата настроена на работу со скоростью 10 Мбит/с, или на ней вместо дуплексного режима задан полудуплексный.

Чтобы определить пропускную способность и текущую активность сетевых адаптеров сервера, проверьте следующие счетчики:

- **Сетевой интерфейс\Получено байт/сек (Network\Bytes Received/sec)**
- **Сетевой интерфейс\Отправлено байт/сек (Network\Bytes Sent/sec)**
- **Сетевой интерфейс\Всего байт/сек (Network\Bytes Total/sec)**
- **Сетевой интерфейс\Текущая пропускная способность (Network\ Current Bandwidth)**

Если при средней нагрузке общее число байтов в секунду превышает 50% пропускной способности, сервер, возможно, не справится с пиковыми нагрузками. Рассмотрите возможность выполнения операций, требующих большой пропускной способности, например, сетевого резервного копирования, на отдельной сетевой плате. Помните, что значения этих счетчиков следует сравнивать в сочетании со счетчиками **Физический диск\% активности диска (PhysicalDisk\% Disk Time)** и **Процессор\% загруженности процессора (Processor\% Processor Time)**. Если нагрузка на диск и процессор невелика, а показания сетевых счетчиков значительны, ваша проблема, вероятно, связана с пропускной способностью. Оптимизируйте настройки сетевой платы или установите дополнительную сетевую плату. Помните о планировании — важно понимать, что не всегда бывает достаточно просто вставить плату в разъем и подключить ее к сети.

Глава 5

Автоматизация административных задач и политики

Ежедневно повторять одни и те же команды, суетиться вокруг политик, непрестанно растолковывать пользователям азы работы с компьютером — на это ли вы хотели потратить свою жизнь? Вот если бы можно было автоматизировать решение этих задач и посвятить свое время чему-то более важному...

В Microsoft Windows Server 2008 включено несколько ролей, служб ролей и компонентов, облегчающих обслуживание серверов. Устанавливать эти компоненты и пользоваться ими довольно просто. Если вам нужен инструмент для управления ролью или компонентом на удаленном компьютере, установите компонент Средства удаленного администрирования сервера (Remote Server Administration Tools). Если на сервере есть беспроводной адаптер, установите компонент Служба беспроводной локальной сети (Wireless Networking). Беспроводные сети работают в Windows Server 2008 так же, как в Windows Vista.

Ниже перечислены основные компоненты, облегчающие обслуживание сервера:

- **Автоматическое обновление (Automatic Updates)** Отвечает за автоматическое обновление ОС и гарантирует наличие всех самых актуальных обновлений безопасности. Если вы заменили Windows Update на Microsoft Update, то сможете получать обновления и для других продуктов. По умолчанию компонент автоматического обновления на серверах Windows Server 2008 устанавливается, но не запускается. Настройка автоматического обновления производится при помощи утилиты **Центр обновления Windows (Windows Update)** из панели управления. Чтобы ее запустить, щелкните кнопку **Пуск (Start)**, **Панель управления (Control Panel)**, **Безопасность (Security)** и **Центр обновления Windows (Windows Update)**. Чтобы узнать, как настроить автоматическое обновление при помощи групповой политики, читайте раздел «Настройка автоматических обновлений» этой главы.
- **Брандмауэр Windows (Windows Firewall)** Защищает компьютер от проникновения неавторизованных пользователей. В Windows Server 2008

включен простой Брандмауэр Windows (Windows Firewall) и более сложный Брандмауэр Windows в режиме повышенной безопасности (Windows Firewall With Advanced Security). По умолчанию на серверах брандмауэры выключены. Чтобы получить доступ к простому брандмауэру, щелкните значок **Брандмауэр Windows (Windows Firewall)** в категории **Сеть и Интернет (Network And Internet)** панели управления. Чтобы получить доступ к сложному брандмауэру, выберите команду **Брандмауэр Windows в режиме повышенной безопасности (Windows Firewall With Advanced Security)** в меню **Администрирование (Administrative Tools)**.

- **Возможности рабочего стола (Desktop Experience)** Устанавливает на сервере возможности рабочего стола Windows Vista. Они полезны, если Windows Server 2008 используется в качестве настольной операционной системы. Установив эти возможности при помощи мастера добавления компонентов рабочего стола, вы также установите следующие программы: Календарь Windows (Windows Calendar), Защитник Windows (Windows Defender), Почта Windows (Windows Mail), Проигрыватель Windows Media (Windows Media Player), Фотоальбом Windows (Windows Photo Gallery), Боковая панель Windows (Windows Sidebar) и Windows SideShow.
- **Время Windows (Windows Time)** Синхронизирует системное время с сервером времени из Интернета. Вы вольны задать конкретный сервер времени. Способ работы компонента Windows Time зависит от того, является компьютер членом домена или рабочей группы. В домене для синхронизации времени используются его контроллеры, и для управления синхронизацией применяется групповая политика. В рабочей группе синхронизация времени проводится с серверами времени из Интернета, и для управления ею применяется утилита Дата и время (Date And Time).
- **Защитник Windows (Windows Defender)** Защищает сервер от шпионских и других потенциально опасных программ. При необходимости запускайте Защитник Windows (Windows Defender) вручную или настройте его автоматический запуск по расписанию. По умолчанию Защитник Windows (Windows Defender) при установке на сервер не включается. Если Защитник Windows (Windows Defender) установлен в составе компонента Возможности рабочего стола (Desktop Experience), используйте для его запуска меню **Все программы (All Programs)**.
- **Планировщик заданий (Task Scheduler)** Позволяет настраивать расписания для однократного и многократного выполнения различных задач, в частности, задач обслуживания. В Windows Server 2008, как и в Windows Vista, расписание задач используется весьма интенсивно. Для просмотра назначенных задач применяется Диспетчер сервера (Server Manager). Чтобы посмотреть настроенные расписания, разверните узлы **Конфигурация (Configuration)**, **Планировщик заданий (Task Scheduler)** и **Библиотека планировщика заданий (Task Scheduler Library)**.

- **Удаленный помощник (Remote Assistance)** Позволяет администратору отправлять старшему администратору запрос на помощь. Старший администратор, принявший этот запрос, может просмотреть рабочий стол пользователя и для разрешения проблемы временно взять на себя управление компьютером. Если вы добавили этот компонент на сервер при помощи мастера добавления компонентов, для управления им можете пользоваться вкладкой **Удаленное использование (Remote)** диалогового окна **Свойства системы (System Properties)**. Чтобы получить доступ к ней, в категории панели управления **Система и ее обслуживание (System and Maintenance)** щелкните **Система (System)** и **Настройка удаленного доступа (Remote Settings)** в группе **Задачи (Tasks)**.
- **Удаленный рабочий стол (Remote Desktop)** Позволяет удаленно подключаться к серверу с другого компьютера. По умолчанию на серверах Windows Server 2008 Удаленный рабочий стол (Remote Desktop) устанавливается, но не включается. Для управления удаленным рабочим столом используйте вкладку **Удаленное использование (Remote)** диалогового окна **Свойства системы (System Properties)**. Чтобы получить доступ к ней, в категории панели управления **Система и ее обслуживание (System and Maintenance)** щелкните **Система (System)** и **Настройка удаленного доступа (Remote Settings)** в группе **Задачи (Tasks)**. Для установления удаленных подключений используйте утилиту **Подключение к удаленному рабочему столу (Remote Desktop Connection)**. Щелкните **Пуск (Start)**, **Все программы (All Programs)**, **Стандартные (Accessories)** и **Подключение к удаленному рабочему столу (Remote Desktop Connection)**.
- **Шифрование диска BitLocker (BitLocker Drive Encryption)** Дополнительный уровень защиты жестких дисков сервера. Позволяет сберечь диски от злоумышленников, получивших физический доступ к серверу. Шифрование BitLocker можно использовать как на серверах, оборудованных модулем TPM, так и без него. Если вы добавили этот компонент на сервер при помощи мастера добавления компонентов, для управления им можете пользоваться утилитой панели управления **Шифрование диска BitLocker (BitLocker Drive Encryption)**.

В Windows Vista и Windows Server 2008 обслуживающие компоненты конфигурируются и управляются совершенно одинаково. Они подробно описаны в книге *Microsoft Windows Vista. Справочник администратора. (Русская Редакция, БХВ-Петербург, 2008)*.

Задачи обслуживания решаются также при помощи многих других компонентов, используемых в более специфических ситуациях. Например, диспетчер системных ресурсов (System Resource Manager) применяется для управления использованием процессора и памяти, когда требуется повысить доступность сервера. Службы терминалов (Terminal Services) нужны, чтобы у пользователей была возможность запускать программы на удаленном сервере. При помощи Служб развертывания Windows (Windows Deployment

Services) вы сможете автоматически развертывать ОС Windows. Главная составная часть системы обслуживания Windows Server 2008, которой вы должны владеть в совершенстве, — это групповая политика (Group Policy).

Примечание Размещение параметров групповых политик в Windows Server 2008 претерпело значительные изменения. В узлах **Конфигурация компьютера (Computer Configuration)** и **Конфигурация пользователя (User Configuration)** появились два новых узла: **Политики (Policies)** и **Настройка (Preferences)**. В первом собраны общие политики, во втором — общие параметры. Обращаясь к узлам редактора групповых политик, я буду пропускать имена этих узлов, то есть, вместо Конфигурация пользователя\Политики\Административные шаблоны: Определения политик\Компоненты Windows (User Configuration\Policies\Administrative Templates: Policy Definitions\Windows Components) я буду по-прежнему писать Конфигурация пользователя\Административные шаблоны\Компоненты Windows (User Configuration\Administrative Templates\Windows Components).

Групповые политики

Групповые политики упрощают администрирование, позволяя централизованно управлять полномочиями, разрешениями и возможностями как пользователей, так и компьютеров. При помощи групповых политик вы сможете:

- Управлять доступом к компонентам Windows, системным и сетевым ресурсам, утилитам панели управления, рабочему столу и меню **Пуск (Start)**. Подробнее — в разделе «Настройка политик при помощи административных шаблонов».
- Создавать централизованно управляемые каталоги для специальных папок, например, папок документов пользователя. Подробнее — в разделе «Централизованное управление специальными папками».
- Создавать сценарии пользователя и компьютера для запуска в определенные моменты. Подробнее — в разделе «Управление сценариями пользователя и компьютера».
- Настраивать политики учетных записей, паролей, аудита, назначения прав пользователей и безопасности. Подробнее об этих вопросах — в части 2 этой книги.

  Далее описано, как работать с групповыми политиками.

Введение в групповые политики

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

Чтобы разобраться в групповых политиках, необходимо в общих чертах представлять структуру Active Directory. В Active Directory логические объединения доменов называются *сайтами* (sites), а подгруппы компьютеров в пределах домена — *подразделениями* (organizational units). Ваша сеть может быть разделена на сайты NewYorkMain, CaliforniaMain и WashingtonMain. Внутри сайта WashingtonMain могут иметься домены SeattleEast, SeattleWest, SeattleNorth и SeattleSouth. Наконец, в домене SeattleEast могут быть подразделения Information Services, Engineering и Sales.

Групповые политики применяются только к системам, работающим под управлением Windows 2000, Windows XP Professional, Windows Vista, Windows Server 2003 и Windows Server 2008. Политики для систем Windows NT 4.0 задаются при помощи редактора системной политики (System Policy Editor, Poledit.exe). Для Windows 95 и Windows 98 вам придется воспользоваться редактором системной политики из комплекта этих ОС, а затем скопировать файл системной политики в общий ресурс Sysvol на контроллере домена.

Параметры групповой политики хранятся в объекте групповой политики (Group Policy Object, GPO) — контейнере для применяемых вами политик и их параметров. К одному и тому же сайту, домену или подразделению можно применить несколько GPO. Поскольку групповая политика описывается при помощи объектов, к ней применимы многие объектно-ориентированные понятия. Если вы знакомы с объектно-ориентированным программированием и подозреваете, что к GPO применимы понятия родительских и дочерних объектов и наследования, знайте: вы не ошиблись.

Контейнером (container) называется объект верхнего уровня, содержащий другие объекты. Благодаря наследованию политика, примененная к родительскому контейнеру, наследуется дочерним контейнером. По сути, это означает, что параметр политики, примененный к родительскому объекту, передается в дочерний объект. Скажем, если вы применили параметр политики к домену, он наследуется подразделениями этого домена. В данном случае GPO домена является родительским объектом, а GPO подразделения — дочерним объектом.

Порядок наследования таков: сайт — домен — подразделение. То есть, параметры групповой политики сайта передаются доменам этого сайта и далее подразделениям этих доменов.

Легко догадаться, что наследование можно отменить. Для этого достаточно применить непосредственно к дочернему контейнеру параметр политики, противоречащий параметру политики родительского контейнера. Сработает именно этот явно примененный параметр, если, конечно, перекрытие политик не заблокировано. Подробнее — в разделе «Блокировка, перекрытие и отключение политик».

В каком порядке применяются групповые политики?

Если задействовано несколько групповых политик, они применяются в следующем порядке:

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

Если параметры различных политик конфликтуют друг с другом, приоритет отдается параметрам, примененным позже. Скажем, политики подразделения обладают более высоким приоритетом, чем политики домена. Разумеется, у этого правила есть исключения. Подробнее о них — в разделе «Блокировка, перекрытие и отключение политик».

Когда применяются групповые политики?

Начав работать с групповыми политиками, вы сразу же обнаружите, что они разделены на две большие категории:

- политики компьютеров;
- политики пользователей.

Политики компьютера обычно применяются при загрузке системы, политики пользователя — во время его входа в систему. Часто для устранения неполадок бывает важно знать точную последовательность событий. В целом, выглядит она так:

1. После запуска сети Windows Server 2008 применяет политики компьютера. По умолчанию они применяются по одной за раз в заранее заданном порядке. В процессе обработки политик компьютера пользовательский интерфейс не отображается.
2. Windows Server 2008 выполняет сценарии запуска. По умолчанию они выполняются по одному за раз, причем очередной сценарий запускается по завершению или истечению срока действия предыдущего. Выполнение сценариев не показывается пользователю, если это не задано явным образом.
3. Пользователь нажимает Ctrl+Alt+Del, чтобы войти в систему. Проверив подлинность пользователя, Windows Server 2008 загружает его профиль.
4. Windows Server 2008 применяет политики пользователя. По умолчанию они применяются по одной за раз в заранее заданном порядке. Процесс обработки политик пользователя отображается на экране.
5. Windows Server 2008 выполняет сценарии входа. По умолчанию сценарии входа для групповой политики выполняются одновременно. Выполнение сценариев не показывается пользователю, если это не задано явным образом. Последними в обычном окне командной строки выполняются сценарии из общего ресурса Netlogon.

6. Windows Server 2008 отображает интерфейс оболочки, заданной в групповой политике.
7. По умолчанию групповая политика обновляется только при выходе пользователя из системы или перезапуске компьютера. Вы вольны отменить это правило, задав интервал обновления групповой политики, введя в командной строке команду **gpupdate**. Подробнее — в разделе «Обновление групповой политики».

Ближе к реальности Некоторые пользовательские параметры, например, перенаправление папок, нельзя обновить, пока пользователь зарегистрирован в системе. Чтобы обновленные значения этих параметров вступили в силу, пользователь должен выйти из системы и снова зайти в нее. Введите в командной строке команду **gpupdate /logoff**, чтобы после обновления автоматически завершить сеанс пользователя. Аналогично, некоторые параметры компьютера обновляются только при перезапуске. Чтобы автоматически перезапустить компьютер после обновления, введите в командной строке **gpupdate /boot**.

Требования групповых политик и совместимость версий

Групповые политики впервые появились в Windows 2000 и применимы только к системам, работающим под управлением серверной и клиентской версий Windows 2000 или более поздних версий ОС. Легко догадаться, что с каждой новой версией Windows в групповую политику вносились какие-то изменения. Иногда эти изменения приводили к тому, что некоторые политики в новых версиях утрачивали свое значение. В результате некоторые политики работают лишь в определенных версиях Windows, например, только в Windows XP Professional или Windows Server 2003.

Однако в целом большинство политик обладает прямой совместимостью. То есть, политики, появившиеся в Windows 2000, как правило, можно использовать в Windows 2000, Windows XP Professional, Windows Server 2003, Windows Vista и Windows Server 2008. С другой стороны, политики, появившиеся, например, в Windows XP Professional, как правило, неприменимы в Windows 2000, а политики, появившиеся в Windows Vista, неприменимы в Windows 2000 или Windows XP Professional.

Как узнать, применима ли данная политика на конкретной версии Windows? Легко. На вкладке **Параметр (Settings)** окна свойств политики есть поле **Поддерживается (Supported On)**, в котором указывается совместимость политики с различными версиями ОС Windows. Выделив политику в расширенном представлении любого редактора групповой политики, вы узнаете о совместимости политики из раздела **Требования (Requirements)**.

Новые политики добавляются в систему при установке пакетов обновлений, приложений и компонентов Windows. Поэтому информация о совместимости иногда довольно сложна.

Изменения в групповых политиках

Стремясь упростить управление групповыми политиками, специалисты Майкрософт удалили средства управления из инструментария Active Directory и переместили их в консоль Управление групповой политикой (Group Policy Management, GPMC). Консоль GPMC добавляется в Windows Server 2008 при помощи мастера добавления компонентов. Она также включена в комплект Windows Vista и доступна для загрузки на веб-сайте Майкрософт. После установки GPMC на сервере команда для ее вызова помещается в меню **Администрирование (Administrative Tools)**.

Если вы хотите отредактировать GPO в GPMC, консоль открывает Редактор управления групповыми политиками (Group Policy Management Editor), который применяется для управления параметрами политик. Если бы в Майкрософт остановились на двух этих инструментах, мы получили бы замечательную и простую в использовании среду для управления политиками. К сожалению, существует еще несколько почти идентичных редакторов, в том числе:

- **Редактор GPO инициирующей программы групповой политики (Group Policy Starter GPO Editor)** Редактор для создания стартовых объектов политики и управления ими. Как следует из названия, стартовый GPO призван стать отправной точкой для разработки объектов политики в вашей организации. Создавая новый объект политики, вы можете указать на стартовый GPO в качестве его основы.
- **Редактор объектов локальной групповой политики (Local Group Policy Object Editor)** Редактор для создания объектов политики на локальном компьютере и управления ими. Как следует из названия, локальные GPO содержат параметры политик для конкретного компьютера, а не для сайта, домена или подразделения.

Если вам приходилось работать в предыдущих версиях Windows, в частности, в Windows Server 2003, то вы знакомы также с Редактором объектов групповой политики (Group Policy Object Editor, GPOE), который был в них основным инструментом редактирования объектов политики. Редакторы Group Policy Object Editor, Group Policy Management Editor, Group Policy Starter GPO Editor и Local Group Policy Object Editor практически идентичны. Разница лишь в наборе объектов политики, доступ к которым они предоставляют. По этой причине в дальнейшем я не буду их различать, используя обобщающий термин «редакторы политики», при необходимости упоминая о различиях. Иногда я будут также использовать для обозначения редакторов политики сокращение GPOE.

Параметрами политик Windows Vista и Windows Server 2008 можно управлять только с компьютеров, работающих под управлением Windows Vista и Windows Server 2008. Это связано с появлением в Windows Vista и Windows Server 2008 усовершенствованных версий GPOE и GPMC, работающих с новым форматом административных шаблонов на базе XML — ADMX.

Примечание Для работы с ADMX нельзя использовать старые версии редакторов политик. Редактировать GPO, основанные на файлах ADMX, можно только на компьютерах с Windows Vista и Windows Server 2008.

Для перехода на новый формат у Майкрософт было много причин. Главная из них — потребность в большей гибкости и расширяемости. Поскольку ADMX-файлы создаются при помощи XML, они четко структурированы, что упрощает и ускоряет их разбор при инициализации. Это повышает производительность обработки групповой политики при запуске и остановке ОС, входе и выходе пользователя из системы, а также при обновлении политики. Кроме того, четкая структура ADMX-файлов отвечает намерениям Майкрософт в области интернационализации.

Файлы ADMX делятся на файлы, не зависящие от языка, с расширением .admx и файлы для конкретных языков с расширением .adml. Независимые от языка файлы гарантируют идентичность ключевых политик GPO. Языковые файлы позволяют просматривать и редактировать политики на различных языках — один пользователь может редактировать политики на английском языке, другой — на испанском и пр. Выбор языка определяется тем, какой языковой пакет установлен на конкретном компьютере.

На компьютерах с Windows Vista и Windows Server 2008 файлы ADMX, не зависящие от языка, устанавливаются в папку %SystemRoot%\PolicyDefinitions. Для языковых ADMX-файлов предназначены папки вида %SystemRoot%\PolicyDefinitions*ЯзыкКультура*. Имена подпапок определяются стандартами ISO, например, EN-US для американского английского.

Когда вы запускаете редактор политик, он автоматически считывает ADMX-файлы из папки с определениями политик. Чтобы при редактировании GPO получить доступ к нужным ADMX-файлам, скопируйте их в соответствующую папку. Если в момент копирования редактор был запущен, перезапустите его.

В доменах ADMX-файлы можно хранить в центральном хранилище — общей доменной папке в каталоге Sysvol (%SystemRoot%\Sysvol\Domain\Policies). Если вы используете центральное хранилище, административные шаблоны уже не хранятся с каждым GPO. Вместо этого в GPO хранится только текущее состояние параметров, а файлы ADMX хранятся централизованно. В результате сокращается использование дискового пространства, а также объем данных, которые нужно реплицировать. Если вы редактируете GPO средствами Windows Vista или Windows Server 2008, ни файлы ADM, ни файлы ADMX внутри GPO не хранятся. Подробнее — в разделе «Создание централизованного хранилища».

В доменном режиме Windows Server 2008 реализован новый механизм репликации групповой политики — служба репликации DFS. Он способен реплицировать только изменения в GPO, избавляя от необходимости после внесения изменений реплицировать GPO целиком.

В отличие от Windows Server 2003, в Windows Server 2008 для изоляции обработки и уведомлений групповой политики от процесса входа Windows

используется служба клиента групповой политики. Разделение групповой политики и процесса входа Windows сокращает объем ресурсов, необходимых для фоновой обработки политики, повышает общую производительность и делает применение новых файлов групповой политики частью процесса обновления без необходимости перезапуска.

В Windows Server 2008 не применяется функциональность журналов трассировки в userenv.dll. События групповой политики записываются в системный журнал. На смену журналу Userenv пришел операционный журнал групповой политики. Разбираясь с проблемами групповой политики, читайте именно операционный журнал. В консоли Просмотр событий (Event Viewer) вы найдете его в узле **Журналы приложений и служб\Microsoft\Windows\GroupPolicy (Applications And Services Logs\Microsoft\Windows\GroupPolicy)**.

Вместо протокола ICMP (ping) в Windows Server 2008 применяется служба сетевого расположения (Network Location Awareness, NLA). Благодаря ей компьютер знает, к сети какого типа он в данный момент подключен и способен реагировать на изменения состояния системы или сетевой конфигурации. При помощи NLA клиент групповой политики определяет состояние компьютера, состояние сети и скорость сетевого соединения для выявления медленных подключений.

Управление локальными групповыми политиками

В Windows Server 2008 допускается применение нескольких локальных объектов групповой политики (Local Group Policy Object, LGPO) на одном компьютере (при условии, что он не является контроллером домена). Ранее на компьютере мог быть только один LGPO. Windows Server 2008 позволяет назначать конкретный LGPO каждому локальному пользователю или LGPO, общий для всех пользователей. Это делает применение политик более гибким и обеспечивает поддержку большего количества сценариев реализации.

Локальные объекты групповой политики

Возможность конфигурирования нескольких LGPO полезна на компьютерах, которые используются изолированно, а не в составе домена. Благодаря им вам более не придется перед выполнением административных функций явно отключать или удалять параметры, влияющие на вашу способность управлять компьютером. Вместо этого вы просто реализуете один LGPO для администраторов и еще один для остальных пользователей. В домене применять несколько LGPO, вероятно, не стоит, поскольку к большинству компьютеров и так применяется несколько GPO. Добавив к их и без того сложному сочетанию еще и несколько локальных объектов, вы рискуете окончательно запутаться.

В Windows Server 2008 есть три уровня локальных объектов групповой политики:

- **Локальная групповая политика** Это единственный LGPO, позволяющий применять как параметры пользователя, так и параметры компьютера ко всем пользователям компьютера.
- **Локальная групповая политика для администраторов и для не-администраторов** Эта групповая политика содержит только параметры пользователя. Применение этой политики зависит от того, входит ли текущая учетная запись в группу локальных администраторов.
- **Локальная групповая политика для конкретного пользователя** Эта групповая политика содержит только параметры пользователя и применяется к конкретным пользователям и группам.

Три уровня LGPO обрабатываются в следующем порядке: локальная групповая политика, локальная групповая политика для администраторов и локальная групповая политика для конкретных пользователей.

Поскольку параметры конфигурации пользователя во всех LGPO одни и те же, параметр в одном GPO может конфликтовать с параметром в другом GPO. Windows Server 2008 разрешает конфликты в параметрах, перезаписывая старое значение параметра тем значением, что было считано после него. Используется всегда самое последнее значение. При этом в расчет принимается лишь значение параметра «включен-выключен». Если параметру присвоено значение **Не задан (Not Configured)**, предыдущее значение параметра изменено не будет. Чтобы упростить администрирование в домене, отключите обработку LGPO на компьютерах с Windows Server 2008, включив параметр политики **Выключение обработки локальных объектов групповой политики (Turn Off Local Объекты групповой политики (Group Policy Objects) Processing)** в доменном GPO. В редакторе политики этот параметр расположен в узле **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика (Computer Configuration\Administrative Templates\System\Group Policy)**.

Доступ к параметрам локальной политики верхнего уровня

На всех компьютерах, работающих под управлением Windows 2000 и более поздних версий, не считая контроллеров домена, имеется редактируемый объект локальной групповой политики. Самый быстрый способ получить доступ к LGPO на локальном компьютера — ввести в командной строке

```
gpedit.msc /gpcomputer: "%ComputerName%"
```

Эта команда запускает в MMC-консоли редактор GPOE для локального компьютера. Здесь *%ComputerName%* — переменная среды с именем локального компьютера. Она ставится в кавычки, как показано в приведенном выше примере. Чтобы получить доступ к локальной политике верхнего уровня на удаленном компьютере, введите в командной строке:

```
gpedit.msc /gpcomputer: "RemoteComputer"
```

где *RemoteComputer* — хост-имя или FQDN-имя удаленного компьютера. Не забудьте о кавычках, как показано в примере:

```
gpedit.msc /gpcomputer: "corpsvr82"
```

Кроме того, управлять локальной политикой верхнего уровня на компьютере можно, выполнив следующие действия:

1. Щелкните **Пуск (Start)**, введите **mmc** в поле **Начать поиск (Search)** и нажмите Enter.
2. В окне консоли раскройте меню **Консоль (File)** и выберите команду **Добавить или удалить оснастку (Add/Remove Snap-In)**.
3. В диалоговом окне **Добавление и удаление оснастки (Add or Remove Snap-Ins)** щелкните **Редактор объектов групповой политики (Group Policy Object Editor)** и **Добавить (Add)**.
4. В диалоговом окне **Выбор объекта групповой политики (Select Group Policy Object)** по умолчанию выбран локальный компьютер. Щелкните **Готово (Finish)** и **OK**.

Как видно из рис. 5-1, теперь вы можете управлять параметрами локальной групповой политики.

Совет Одну и ту же консоль MMC можно использовать для управления несколькими объектами LGPO. В диалоговом окне **Добавление и удаление оснастки (Add or Remove Snap-Ins)** добавьте по одному экземпляру редактора объектов локальной групповой политики для каждого объекта, с которым собираетесь работать.

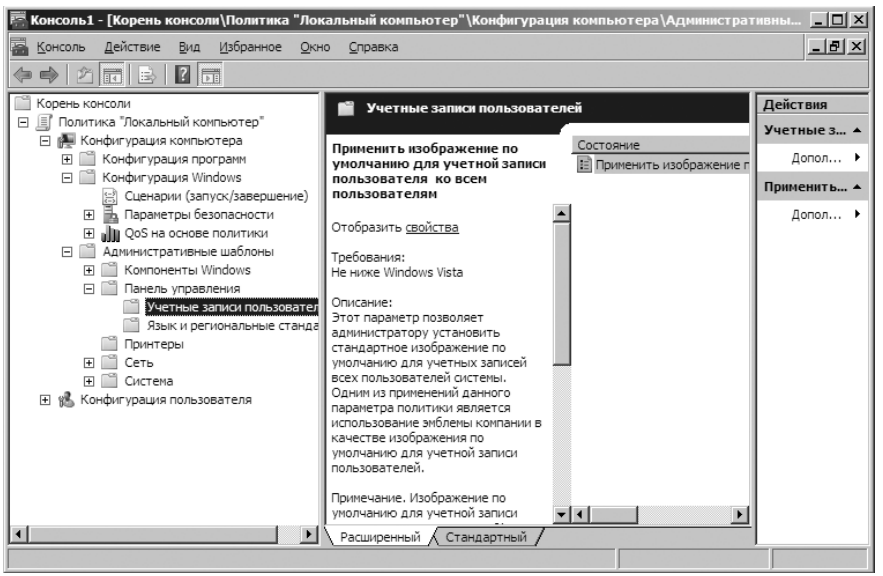


Рис. 5-1. Используйте специальный редактор для управления параметрами локальной политики

Параметры LGPO

Локальные групповые политики хранятся в папке %SystemRoot%\System32\GroupPolicy на каждом компьютере Windows Server 2008. В этой папке имеются следующие подпапки:

- **Machine** Содержит сценарии компьютера в подпапке Script и информацию о политике для раздела реестра HKEY_LOCAL_MACHINE в файле Registry.pol.
- **User** Содержит сценарии компьютера в подпапке Script и информацию о политике для раздела реестра HKEY_CURRENT_USER в файле Registry.pol.

Внимание! Не редактируйте непосредственно эти файлы и папки; используйте инструменты для управления групповыми политиками. По умолчанию эти файлы и папки скрыты. Чтобы они отображались в окне проводника Windows, выберите в меню **Сервис (Tools)** команду **Свойства папки (Folder Options)**, перейдите на вкладку **Вид (View)**, установите переключатель **Показывать скрытые файлы и папки (Show Hidden files and Folders)**, сбросьте флажок **Скрывать защищенные системные файлы (рекомендуется) (Hide Protected Operating System Files (Recommended))**, щелкните **Да (Yes)** и **OK**.

Доступ к локальным групповым политикам

По умолчанию на компьютере имеется единственный объект локальной групповой политики — Local Group Policy Object. Другие локальные объекты создаются при необходимости. Чтоб создать административный или неадминистративный объект локальной групповой политики, выполните следующие действия:

1. Щелкните **Пуск (Start)**, введите **mmc** в поле **Начать поиск (Search)** и нажмите Enter. В окне консоли раскройте меню **Консоль (File)** и выберите команду **Добавить или удалить оснастку (Add/Remove Snap-In)**.
2. В диалоговом окне **Добавление и удаление оснастки (Add or Remove Snap-Ins)** щелкните **Редактор объектов групповой политики (Group Policy Object Editor)** и **Добавить (Add)**.
3. В диалоговом окне **Выбор объекта групповой политики (Select Group Policy Object)** щелкните **Обзор (Browse)**. В диалоговом окне **Поиск объекта групповой политики (Browse For a Group Policy Object)** перейдите на вкладку **Пользователи (Users)**.
4. На то, что определенный объект локальной групповой политики уже создан, указывают элементы списка на вкладке **Пользователи (Users)**. Выполните одно из следующих действий:
   - Щелкните элемент **Администраторы (Administrators)**, чтобы создать или изменить административный объект локальной групповой политики.

- Щелкните элемент **Не администраторы (Non-Administrators)**, чтобы создать или изменить неадминистративный объект локальной групповой политики.
- Выделите локального пользователя, чтобы создать или изменить объект локальной групповой политики персонально для него.

5. Щелкните **OK**. Если выделенный объект еще не существует, он будет создан. В противном случае вы откроете для просмотра и редактирования существующий объект.

Параметры политики для администраторов, не-администраторов и пользователей хранятся в папке %SystemRoot%\System32\GroupPolicyUsers на каждом компьютере Windows Server 2008. Поскольку в этих LGPO присутствуют только параметры конфигурации пользователя, в папке %SystemRoot%\System32\GroupPolicyUsers имеется только подпапка User, в подпапке Script которой находятся сценарии пользователя, а файл Registry.pol содержит информацию о политике для раздела реестра HKEY_CURRENT_USER.

Управление политиками сайта, домена и подразделения

Развернув доменные службы Active Directory, вы можете пользоваться групповой политикой Active Directory. У каждого сайта, домена и подразделения таких политик может быть несколько. Чем выше в списке находится групповая политика, тем выше ее приоритет. Это гарантирует корректное применение политик в сайтах, доменах и подразделениях.

Введение в политики домена и политики по умолчанию

В каждом домене Active Directory по умолчанию есть два объекта групповой политики:

- **Политика контроллера домена по умолчанию (Default Domain Controllers Policy)** Стандартный GPO для подразделения Domain Controllers. Это GPO применим ко всем контроллерам домена (если они не удалены из подразделения). Применяйте его для управления параметрами безопасности контроллеров домена.
- **Политика домена по умолчанию (Default Domain Policy)** Стандартный GPO для домена Active Directory в целом. Применяйте его для настройки базового уровня параметров политик, применимых ко всем пользователям и компьютерам домена.

Как правило, политика домена по умолчанию обладает наивысшим приоритетом на уровне домена, а политика контроллера домена по умолчанию обладает наивысшим приоритетом на уровне на уровне контейнера Domain Controllers. Как с доменом, так и с контейнером Domain Controllers можно связать и другие GPO. При этом необходимо всегда помнить, что параметры GPO с высоким приоритетом перекрывают параметры GPO с низким при-

оритетом. Эти GPO не предназначены для общего управления групповой политикой.

Политика домена по умолчанию применяется только для управления стандартными параметрами политик учетных записей, в частности, политики паролей, политики блокировки учетных записей и политики Kerberos. При помощи этого GPO управляются также параметры безопасности Учетные записи: Переименование учетной записи администратора (Accounts: Rename Administrator Account), Учетные записи: Переименование учетной записи гостя (Accounts: Rename Guest Account), Сетевая безопасность: Принудительный вывод из сеанса по истечении допустимых часов работы (Network Security: Force Logoff When Logon Hours Expire) и Доступ к сети: Разрешить трансляцию анонимного SID в имя (Network Access: Allow Anonymous SID/Name Translation). Один из способов перекрытия этих параметров состоит в создании нового GPO с другими значениями для них и связывании его с контроллером домена с более высоким приоритетом.

В политику контроллера домена по умолчанию включены права пользователей и параметры безопасности, ограничивающие использование контроллера домена. Один из способов перекрытия этих параметров состоит в создании нового GPO с другими значениями для них и связывании его с контейнером Domain Controllers с более высоким приоритетом.

Для управления другими аспектами политики создайте новый GPO и свяжите его с доменом или с одним из его подразделений.

Групповые политики сайта, домена и подразделений хранятся на контроллерах домена в папке %SystemRoot%\ Sysvol\Domain\Policies. В ней вы найдете по одной подпапке для каждой политики, определенной вами на контроллере домена. Имя папки политики является идентификатором GUID этой политики. В папке политики размещены следующие подпапки:

- **Machine** Сценарии компьютера (в подпапке Script) и информация о политике для раздела реестра HKEY_LOCAL_MACHINE в файле Registry.pol.
- **User** Сценарии пользователя (в подпапке Script) и информация о политике для раздела реестра HKEY_CURRENT_USER в файле Registry.pol.

Внимание! Не редактируйте непосредственно эти файлы и папки; используйте инструменты для управления групповыми политиками.

Управление групповыми политиками

Для запуска GPMC щелкните **Пуск (Start)**, **Администрирование (Administrative Tools)** и **Управление групповой политикой (Group Policy Management)**. Как показано на рис. 5-2, корневой узел консоли называется **Управление групповой политикой (Group Policy Management)**, а ниже него располагается узел **Лес (Forest)**. Он представляет лес, к которому вы в данный момент подключены, и содержит имя корневого домена этого леса. При наличии соответствующих полномочий вы вольны создавать подключения к другим лесам, щелкнув правой кнопкой узел **Управление групповой поли-**

тикой (Group Policy Management) и выбрав команду **Добавить лес (Add Forest)**. В диалоговом окне **Добавление леса (Add Forest)** введите имя корневого домена леса и щелкните **OK**.

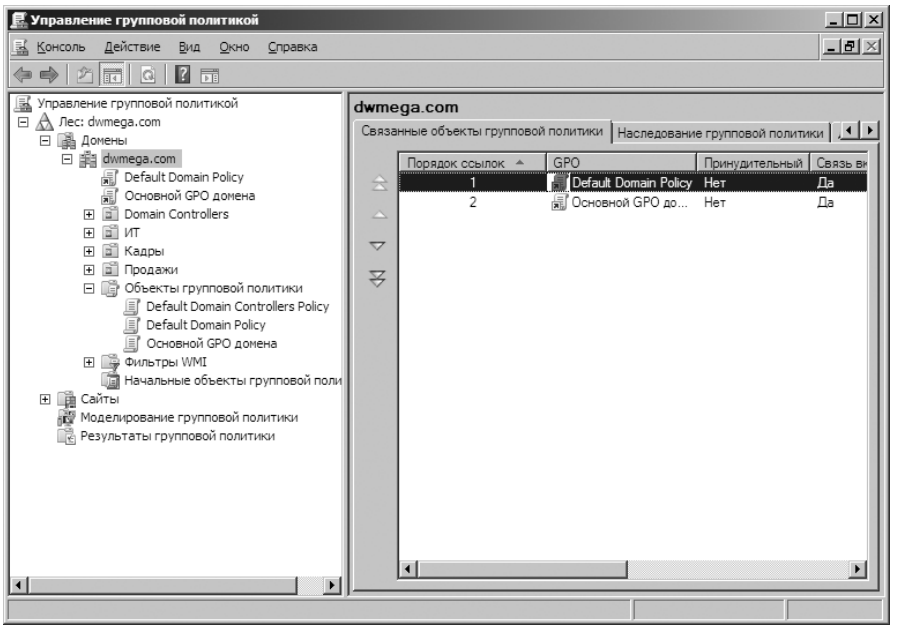


Рис. 5-2. Консоль GPMC применяется для работы с GPO сайтов, лесов и доменов

В узле **Лес (Forest)** содержатся следующие узлы:

- **Домены (Domains)** Открывает доступ к параметрам политик для доменов соответствующего леса. По умолчанию вы подключены к тому домену, в котором зарегистрировались. При наличии соответствующих полномочий вы вольны создавать подключения к другим доменам леса, щелкнув правой кнопкой узел **Домены (Domains)** и выбрав команду **Показать домены (Show Domains)**. В диалоговом окне **Отображение доменов (Show Domains)** установите флажки доменов, которые хотите отображать, и щелкните **OK**.
- **Сайты (Sites)** Открывает доступ к параметрам политик сайтов соответствующего леса. По умолчанию сайты скрыты. При наличии соответствующих полномочий вы вольны создавать подключения к сайтам. Щелкните правой кнопкой узел **Сайты (Sites)** и выберите команду **Показать сайты (Show Sites)**. В диалоговом окне **Отображение сайтов (Show Sites)** установите флажки сайтов, которые хотите отображать, и щелкните **OK**.
- **Моделирование групповой политики (Group Policy Modeling)** Открывает доступ к Мастеру моделирования групповой политики (Group Policy Modeling Wizard), который поможет вам спланировать развертывание политики и промоделировать действие назначенных параметров. Здесь же доступны сохраненные модели политик.

- **Результаты групповой политики (Group Policy Results)** Открывает доступ к Мастеру результатов групповой политики (Group Policy Results Wizard).

В каждом домене, к которому вы подключены, доступны все связанные GPO и подразделения. Элементы GPO, перечисленные в контейнерах доменов, сайтов и подразделений, являются не самими GPO, а ссылками на них. Чтобы получить доступ непосредственно к GPO, воспользуйтесь контейнером Объекты групповой политики **(Group Policy Objects)** нужного домена. Обратите внимание: на значках ссылок GPO слева внизу есть небольшие стрелки, как на значках ярлыков, а на значках самих GPO этих стрелок нет.

Когда вы запускаете GPMC, консоль подключается к Active Directory, которая работает на контроллере домена, действующем в качестве эмулятора PDC, и получает оттуда список всех GPO и подразделений домена. Для доступа к хранилищу каталога используется протокол LDAP, а для доступа к каталогу Sysvol — протокол SMB (Server Message Block). Если эмулятор PDC по каким-то причинам недоступен, например, выключен сервер, GPMC предлагает на выбор работу с параметрами политики на контроллере домена, к которому вы в данный момент подключены, или на любом другом контроллере домена. Чтобы подключиться к другому домену в процессе работы, щелкните его узел правой кнопкой и выберите команду **Сменить контроллер домена (Change Domain Controller)**. В диалоговом окне **Смена контроллера домена (Change Domain Controller)** под заголовком **Текущий контроллер домена (Current Domain Controller)** указан контроллер, к которому вы в данный момент подключены. При помощи переключателя **Изменить на (Change To)** задайте другой домен и щелкните **OK**.

Знакомство с редактором политики

Чтобы отредактировать GPO, щелкните правой кнопкой его элемент в GPMC и выберите команду **Изменить (Edit)**. Как показано на рис. 5-3, у редактора политики два основных узла:

- **Конфигурация компьютера (Computer Configuration)** Служит для настройки политик, применяемых к компьютеру независимо от того, кто на нем зарегистрирован.
- **Конфигурация пользователя (User Configuration)** Служит для настройки политик, применяемых к пользователю независимо от того, на каком компьютере он зарегистрировался.

Конкретное содержимое узлов **Конфигурация компьютера (Computer Configuration)** и **Конфигурация пользователя (User Configuration)** зависит от установленных надстроек и типа политики. Как правило, в обоих узлах имеются следующие подузлы:

- **Конфигурация программ (Software Settings)** Политики для параметров ПО и установки ПО. При установке новых программ в узел **Конфигурация программ (Software Settings)** могут добавляться новые подузлы.

- **Конфигурация Windows (Windows Settings)** Политики перенаправления папок, сценарии и параметры безопасности.
- **Административные шаблоны (Administrative Templates)** Политики для ОС, компонентов Windows и программ. Административные шаблоны настраиваются при помощи соответствующих файлов, которые можно при необходимости добавлять и удалять.

Примечание Исчерпывающее обсуждение всех возможных вариантов выходит за рамки этой книги. Далее мы сосредоточимся на перенаправлении папок и административных шаблонах. Сценарии подробно описаны в разделе «Управление сценариями пользователя и компьютера». Безопасности посвящена часть 2 этой книги.

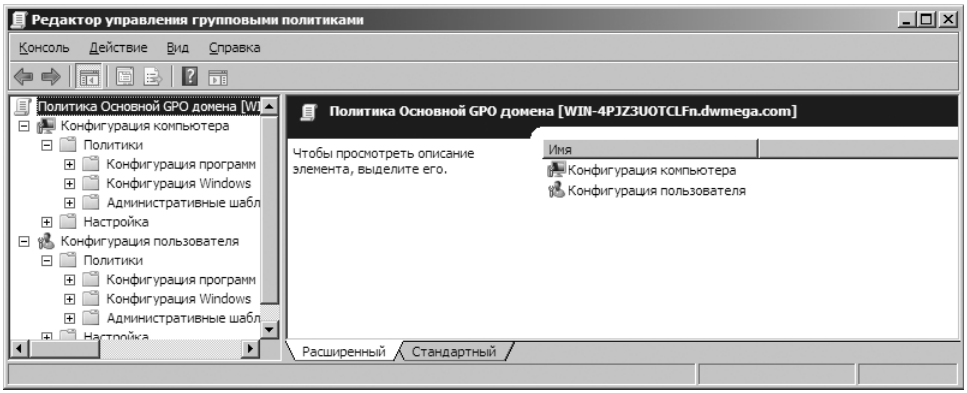


Рис. 5-3. Вид редактора политики зависит от типа политики и установленных надстроек

Настройка политик при помощи административных шаблонов

Административные шаблоны облегчают доступ к параметрам политики из реестра. В редакторе политики вы найдете набор административных шаблонов по умолчанию для компьютеров и пользователей. Административные шаблоны можно создавать и удалять. Любые изменения, вносимые в политики посредством административных шаблонов, сохраняются в реестре. Параметры конфигурации компьютера записываются в раздел HKEY_LOCAL_MACHINE, а параметры конфигурации пользователя — в раздел HKEY_CURRENT_USER.

Настроенные в данный момент шаблоны размещены в узле **Административные шаблоны (Administrative Templates)** редактора политики. Этот узел содержит политики, которые можно настраивать для локальных систем, подразделений, доменов и сайтов. В узлах **Конфигурация компьютера (Computer Configuration)** и **Конфигурация пользователя (User Configuration)** содержатся разные наборы шаблонов. Устанавливая новые компоненты Windows, вы можете вручную добавлять в редактор политики шаблоны с новыми политиками.

Узел **Административные шаблоны (Administrative Templates)** применяется для управления следующими компонентами:

- **Компоненты Windows (Windows components)** Определяет доступные параметры и конфигурацию различных компонентов Windows, включая Просмотр событий (Event Viewer), Internet Explorer, Планировщик заданий (Task Scheduler), Установщик Windows (Windows Installer) и Центр обновления Windows (Windows Updates).
- **Меню «Пуск» и панель задач (Start menu and taskbar)** Управляет доступными параметрами и конфигурацией меню **Пуск (Start)** и панели задач.
- **Общие папки (Shared folders)** Разрешает публикацию общих папок и корней DFS.
- **Панель управления (Control Panel)** Определяет доступные параметры и конфигурацию панели управления и ее утилит.
- **Принтеры (Printers)** Определяет параметры принтеров, обзор, очереди и параметры каталога.
- **Рабочий стол (Desktop)** Определяет вид рабочего стола Windows и доступные на нем параметры.
- **Сеть (Network)** Настраивает сеть и параметры сетевого клиента для автономных файлов, клиентов DNS и сетевых подключений.
- **Система (System)** Настраивает системные параметры в отношении дисковых квот, профилей пользователей, входа в систему, восстановления системы, отчетов об ошибках и т. д.

Чтобы познакомиться со всеми политиками административных шаблонов, внимательно изучите содержимое узлов **Административные шаблоны (Administrative Templates)**. Политики в шаблонах находятся в одном из трех состояний:

- **Не задан (Not Configured)** Политика не используется; никакие ее параметры в реестр не записаны.
- **Включен (Enabled)** Политика выполняется, и ее параметры сохранены в реестре.
- **Отключен (Disabled)** Политика отключена и не выполняется (если она не включена где-то еще). Этот параметр сохраняется в реестре.

Чтобы включить, отключить и настроить политику, выполните следующие действия:

1. В редакторе политик разверните узел **Административные шаблоны (Administrative Templates)** в узле **Конфигурация компьютера (Computer Configuration)** или **Конфигурация пользователя (User Configuration)**, в зависимости от типа нужной политики.
2. В левой панели выберите подпапку, которая содержит нужную политику. Содержимое папки отображается в правой панели.
3. Дважды щелкните политику или щелкните ее правой кнопкой и выберите команду **Свойства (Properties)**, чтобы открыть диалоговое окно свойств политики.

4. Перейдите на вкладку Объяснение (Explain), чтобы прочитать описание политики. Оно выводится только при условии, что описание задано в соответствующем файле шаблона.
5. Чтобы изменить состояние политики, перейдите на вкладку **Параметр (Settings)** и установите один из следующих переключателей:
   - **Не задан (Not Configured)** Политика не настроена.
   - **Включен (Enabled)** Политика включена.
   - **Отключен (Disabled)** Политика выключена.
6. При необходимости задайте на вкладке **Параметр (Settings)** дополнительные параметры и щелкните **OK**.

Примечание Как правило, в Windows Server 2008 политики компьютера обладают более высоким приоритетом. При возникновении конфликта между параметром политики компьютера и параметром политики пользователя применяться будет параметр политики компьютера.

Создание центрального хранилища

Центральное хранилище (central store) — это набор папок в каталоге Sysvol на контроллере каждого домена вашей организации. Чтобы организовать централизованное хранение файлов ADMX, создайте центральное хранилище на одном из контроллеров домена. Служба репликации затем перенесет это хранилище на все остальные контроллеры в этом домене. Поскольку репликация в масштабах предприятия занимает немало времени, как правило, создавать хранилище нужно на контроллере, исполняющем роль эмулятора PDC, поскольку GPOE и GPMC по умолчанию подключаются именно к этому контроллеру домена.

Создать центральное хранилище может любой администратор, входящий в группу администраторов домена. Для этого нужно выполнить следующие действия:

1. Зарегистрировавшись на контроллере домена, при помощи проводника Windows создайте корневую папку хранилища в папке %SystemRoot%\Domain\Policies.
2. При помощи проводника Windows Explorer создайте в папке %SystemRoot%\Domain\Policies\PolicyDefinitions подпапку для каждого языка, который будет использоваться администратором политик. Называть подпапки следует согласно стандартам ISO для пары язык-культура, например, EN-US для американского английского.
3. Запишите в хранилище файлы ADMX из комплекта Windows Vista. Зарегистрируйтесь на компьютере домена, работающем под управлением Windows Vista Business или более поздней версии со всеми пакетами обновления. Затем выполните следующие действия:
   - Скопируйте все ADMX-файлы, не зависящие от языка, из папки %SystemRoot%\PolicyDefinitions на компьютере с Windows Vista

в центральное хранилище контроллера (%SystemRoot%\Domain\Policies\PolicyDefinitions).

- Скопируйте все ADMX-файлы, зависящие от языка, из папки %SystemRoot%\PolicyDefinitions*ЯзыкКультура* в аналогичную папку центрального хранилища на контроллере домена. Например, чтобы скопировать файлы ADMX для американского английского, вам нужно скопировать файлы из папки %SystemRoot%\PolicyDefinitions\EN-US в папку %SystemRoot%\Domain\Policies\PolicyDefinitions\EN-US на контроллере домена.

4. Запишите в хранилище файлы ADMX из комплекта Windows Server 2008. Зарегистрируйтесь на компьютере домена, работающем под управлением Windows Server 2008 со всеми пакетами обновления. Затем выполните следующие действия:
   - Скопируйте все ADMX-файлы, не зависящие от языка, из папки %SystemRoot%\PolicyDefinitions на компьютере с Windows Vista в центральное хранилище контроллера (%SystemRoot%\Domain\Policies\PolicyDefinitions).
   - Скопируйте все ADMX-файлы, зависящие от языка, из папки %SystemRoot%\PolicyDefinitions*ЯзыкКультура* в аналогичную папку центрального хранилища на контроллере домена. Например, чтобы скопировать файлы ADMX для американского английского, вам нужно скопировать файлы из папки %SystemRoot%\PolicyDefinitions\EN-US в папку %SystemRoot%\Domain\Policies\PolicyDefinitions\EN-US на контроллере домена.
5. Файлы будут реплицированы на другие контроллеры домена в процессе обычной репликации Sysvol. Этот процесс может занять несколько часов, а то и больше. При необходимости повторите этот процесс, чтобы создать центральные хранилища в других доменах вашей организации.

Создание и связывание GPO

Создание объекта политики и его связывание с конкретным контейнером Active Directory — два различных действия. Только что созданный GPO не связан ни с доменом, ни с сайтом, ни с подразделением. Вы можете установить такую связь вручную или автоматически. Выбор конкретного метода определяется, главным образом, вашими личными пристрастиями и предполагаемым использованием GPO. Помните: когда вы создаете GPO и связываете его с сайтом, доменом или подразделением, он применяется к объектам пользователей и компьютеров этого сайта, домена или подразделения согласно заданным в Active Directory параметрам наследования, приоритета и другим.

Чтобы создать GPO и связать его с сайтом, доменом или подразделением, выполните следующие действия:

1. В GPMC разверните узел нужного леса, а затем разверните в нем узел **Домены (Domains)**.
2. Щелкните правой кнопкой узел **Объекты групповой политики (Group Policy Objects)** и выберите команду **Создать (New)**. В диалоговом окне **Новый объект групповой политики (New GPO)** введите понятное имя для нового GPO, например, **Secure Workstation GPO**. Если вы хотите использовать в качестве источника параметров стартовый GPO, выберите его в списке **Исходный объект групповой политики (Source Starter GPO)**. Когда вы щелкнете **OK**, в контейнер **Объекты групповой политики (Group Policy Objects)** будет добавлен новый GPO.
3. Щелкните новый GPO правой кнопкой и выберите команду **Изменить (Edit)**. Настройте в редакторе политики нужные параметры и закройте редактор.
4. В GPMC выберите сайт, домен или подразделение. На вкладке **Связанные объекты групповой политики (Linked Объекты групповой политики (Group Policy Objects))** правой панели показаны GPO, которые в данный момент связаны с выделенным контейнером (если таковые имеются).
5. Щелкните нужный сайт, домен или подразделение правой кнопкой и выберите команду **Связать существующий объект GPO (Link An Existing GPO)**. Выделите нужный GPO в диалоговом окне **Выбор объекта групповой политики (Select GPO)** и щелкните **OK**. Параметры из этого GPO будут применены при обновлении групповой политики для компьютеров и пользователей данного сайта, домена или подразделения.

Можно также указать связь для GPO одновременно с его созданием:

1. В GPMC щелкните правой кнопкой сайт, домен или подразделение, с которыми хотите связать создаваемый GPO, и выберите команду **Создать объект GPO в этом домене и связать его (Create A GPO In This Domain, And Link It Here)**.
2. В диалоговом окне **Новый объект групповой политики (New GPO)** введите понятное имя для нового GPO, например, **Secure Workstation GPO**. Если вы хотите использовать в качестве источника параметров стартовый GPO, выберите его в списке **Исходный объект групповой политики (Source Starter GPO)**. Когда вы щелкнете **OK**, новый GPO будет добавлен в контейнер **Объекты групповой политики (Group Policy Objects)** и связан с выбранным сайтом, доменом и подразделением.
3. Щелкните новый GPO правой кнопкой и выберите команду **Изменить (Edit)**. Настройте в редакторе политики нужные параметры и закройте редактор. Параметры из этого GPO будут применены при обновлении групповой политики для компьютеров и пользователей данного сайта, домена или подразделения.

Создание и использование стартовых GPO

Когда вы создаете новый GPO в GPMC, вам предоставляется возможность использовать в качестве основы стартовый GPO. Параметры стартового GPO импортируются в создаваемый GPO, закладывая основу его конфигурации. В крупных организациях следует создавать стартовые GPO нескольких категорий для различных пользователей, компьютеров и параметров безопасности.

Чтобы создать стартовый GPO, выполните следующие действия:

1. В GPMC разверните узел нужного леса, а затем разверните в нем узел **Домены (Domains)**.
2. Щелкните правой кнопкой узел **Начальные объекты групповой политики (Starter GPOs)** и выберите команду **Создать (New)**. В диалоговом окне **Новый стартовый объект GPO (New Starter GPO)** введите понятное имя для нового GPO, например, **General Management User GPO**. При необходимости введите также описание GPO и щелкните **OK**.
3. Щелкните новый GPO правой кнопкой и выберите команду **Изменить (Edit)**. Настройте в редакторе политики нужные параметры и закройте редактор.

Делегирование полномочий по управлению групповыми политиками

В Active Directory у всех администраторов имеются определенные полномочия по управлению групповыми политиками. Посредством делегирования вы можете передать другим пользователям право на выполнение следующих задач:

- создание GPO и управление ими;
- просмотр и редактирование параметров, удаление GPO, изменение параметров безопасности;
- управление связями существующих GPO и генерация результирующей политики (Resultant Set of Policy, RSoP).

В Active Directory администраторы могут создавать GPO. У любого пользователя, создавшего GPO, есть право на управлением им. Чтобы задать в GPMC, кто имеет право создавать GPO в домене, выделите узел **Объекты групповой политики (Group Policy Objects)** в этом домене и перейдите на вкладку **Делегирование (Delegation)**. Здесь перечислены группы и пользователи, которым разрешено создавать GPO в этом домене. Чтобы передать пользователю или группе право создания GPO, щелкните кнопку **Добавить (Add)**. В диалоговом окне **Выбор «Пользователь», «Компьютер» или «Группа» (Select User, Computer, Or Group)** выберите нужного пользователя или группу и щелкните **OK**.

При работе с GPMC у вас есть несколько способов определить, у кого есть право доступа к управлению групповыми политиками. Чтобы задать разре-

шения в домене, сайте или подразделении, выделите нужный домен, сайт или подразделение и перейдите на вкладку **Делегирование (Delegation)**, показанную на рис. 5-4. В списке **Разрешение (Permission)** выберите нужное разрешение. Доступны следующие варианты:

- **Связанные объекты GPO (Link GPOs)** Выводится список пользователей и групп, которым разрешается создавать и связывать GPO в выбранном сайте, домене или подразделении.
- **Анализ моделирования групповой политики (Perform Group Policy Modeling Analyses)** Выводится список пользователей и групп, которым разрешается определять результирующую политику в целях планирования.
- **Чтение результирующих данных групповой политики (Read Group Policy Results Data)** Выводится список пользователей и групп, которым разрешается в целях проверки и протоколирования определять RSoP, которая применена в данный момент.

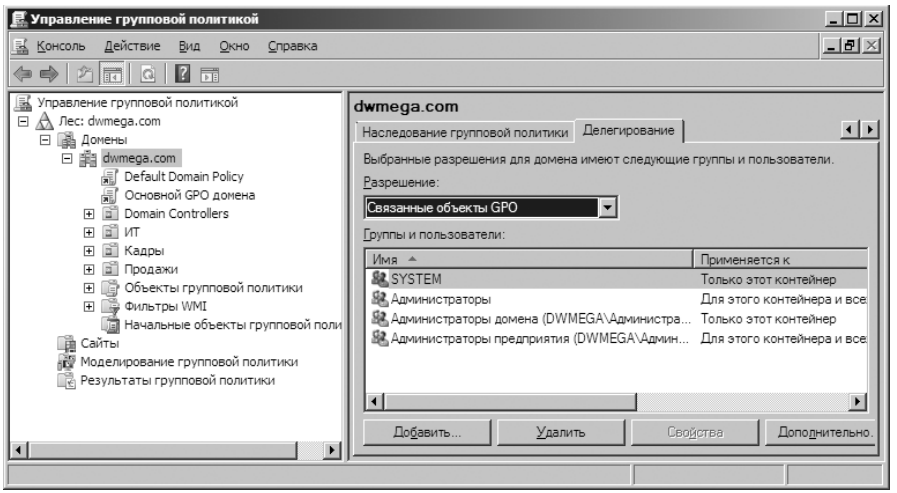


Рис. 5-4. Проверка разрешений на управление групповыми политиками

Чтобы задать разрешение для домена, сайта или подразделения, выполните следующие действия:

1. В GPMC выделите домен, сайт или подразделение и перейдите на вкладку **Делегирование (Delegation)** в правой панели.
2. Выберите в списке **Разрешение (Permission)** разрешение, которое хотите задать.
3. Щелкните **Добавить (Add)**. В диалоговом окне **Выбор «Пользователь», «Компьютер» или «Группа» (Select User, Computer, Or Group)** выберите нужного пользователя или группу и щелкните **OK**.
4. В диалоговом окне **Добавление группы или пользователя (Add Group Or User)** укажите способ применения разрешения. Чтобы применить разре-

шение к текущему контейнеру и всем дочерним контейнерам, выберите в списке вариант **Для этого контейнера и всех дочерних контейнеров (This Container And All Child Containers)**. Чтобы применить разрешение только к текущему контейнеру, выберите **Только этот контейнер (This Container Only)**. Щелкните **OK**.

Чтобы задать разрешения для отдельного GPO, выделите его в GPMC и перейдите на вкладку **Делегирование (Delegation)**. Там вы сможете задать следующие разрешения для отдельных пользователей и групп:

- **Чтение (Read)** Пользователю или группе разрешено просматривать GPO и его параметры.
- **Изменить настройки (Edit Settings)** Пользователю или группе разрешено просматривать GPO и изменять его параметры. Удалять GPO и менять параметры безопасности не разрешается.
- **Изменение параметров, удаление и изменение параметров безопасности (Edit Settings, Delete, Modify Security)** Пользователю или группе разрешено просматривать GPO и изменять его параметры, а также удалять GPO и менять параметры безопасности.

Чтобы выдать разрешение на работу с GPO, выполните следующие действия:

1. В GPMC выделите домен, сайт или подразделение и перейдите на вкладку **Делегирование (Delegation)** в правой панели.
2. Чтобы выдать разрешение на создание GPO пользователю или группе, щелкните **Добавить (Add)**. В диалоговом окне **Выбор «Пользователь», «Компьютер» или «Группа» (Select User, Computer, Or Group)** выберите нужного пользователя или группу и щелкните **OK**.
3. В диалоговом окне **Добавление группы или пользователя (Add Group Or User)** задайте нужное разрешение и щелкните **OK**.

Блокировка, перекрытие и отключение политик

Наследование гарантирует, что групповая политика подействует на все объекты компьютеров и пользователей в домене, сайте или подразделении. Большинство политик может находиться в трех состояниях: не задана, включена и отключена. По умолчанию большинство параметров политик не заданы. Включенная политика применяется ко всем связанным пользователям и компьютерам либо непосредственно, либо через наследование. Если политика выключена, она не применяется к связанным пользователям и компьютерам ни непосредственно, ни через наследование.

Есть четыре основных способа изменить работу наследования:

- изменить порядок и приоритет связей;
- перекрыть наследование (если не задано принудительное выполнение);
- заблокировать наследование (полностью отказаться от него);
- задать принудительное наследование (отменяющее перекрытие и блокировку).

Групповые политики наследуются от сайта к домену и от домена к подразделению. Учитывайте следующее:

- Если к определенному уровню привязано несколько объектов политики, порядок применения параметров политик определяется порядком связей. Сначала применяется политика с наименьшим номером связи, затем — политики с нарастающими номерами. Наивысший приоритет имеет последний примененный объект. Именно его параметры являются финальными и перекрывают аналогичные параметры всех остальных объектов политики (если не заданы блокировка или принудительное наследование).
- Если несколько объектов политики наследуются с более высокого уровня, они также применяются в порядке следования связей. Как и в предыдущем случае, сначала применяется политика с наименьшим номером связи, затем — политики с нарастающими номерами. Наивысший приоритет имеет последний примененный объект. Именно его параметры являются финальными и перекрывают аналогичные параметры всех остальных объектов политики (если не заданы блокировка или принудительное наследование).

Чтобы изменить порядок следования связей и, следовательно, порядок применения политик, выполните следующие действия:

1. В GPMC выделите контейнер нужного сайта, домена или подразделения.
2. В правой панели по умолчанию выбрана вкладка **Связанные объекты групповой политики (Linked Объекты групповой политики (Group Policy Objects))**, как показано на рис. 5-5. Щелкните нужный объект.

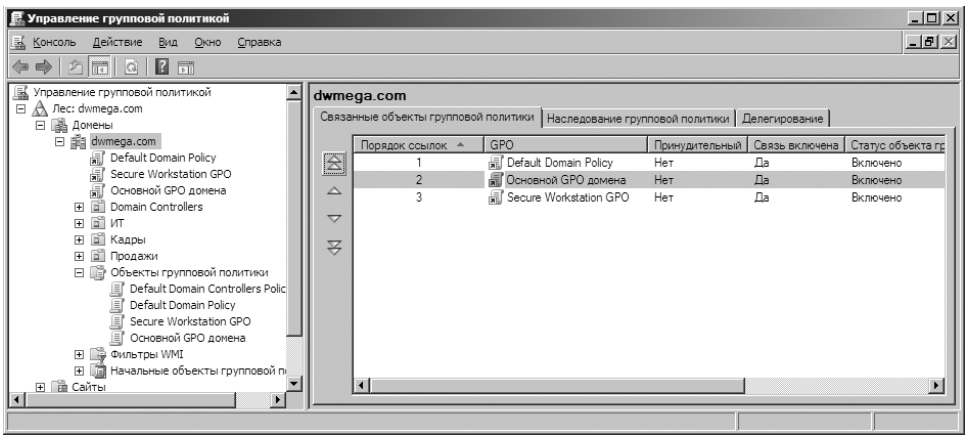


Рис. 5-5. Изменение порядка связей меняет порядок применения политик

3. При помощи кнопок **Переместить связь вверх (Move Link Up)** и **Переместить связь вниз (Move Link Down)** переместите объект на нужное место.

4. Перейдите на вкладку **Наследование групповой политики (Group Policy Inheritance)** и убедитесь, что объекты политики обрабатываются в нужном порядке.

Общий способ управления наследованием состоит в перекрытии наследуемых параметров. Если в объекте высокого уровня политика включена, вы можете перекрыть наследование, отключив политику на низком уровне. Если в объекте высокого уровня политика отключена, вы можете перекрыть наследование, включив политику на низком уровне. Этот метод приведет к желаемому результату, при условии что для политики не заданы блокировка или принудительное выполнение.

Иногда наследование нужно заблокировать, чтобы к пользователям и компьютерам определенного контейнера не применялись политики, унаследованные с более высокого уровня. При блокировке наследования применяются только настроенные параметры политик, связанных с данным уровнем, в параметры политик из контейнеров более высокого уровня блокируются (если не задано принудительное выполнение политики).

Администратор домена может применить блокировку, чтобы запретить наследование политик с уровня сайта. Соответственно, администраторы подразделений при помощи блокировки отменяют применение политик, наследуемых с уровней домена и сайта. Блокировка гарантирует «автономию» домена или подразделения, при которой все полномочия по управлению политиками оказываются в руках соответствующей администрации.

Чтобы заблокировать наследование при помощи GPMC, щелкните правой кнопкой нужный домен или подразделение и выберите команду **Блокировать наследование (Block Inheritance)**. Если она уже отмечена, ее повторный выбор отменит блокировку. Если в дереве консоли GPMC к значку контейнера добавлен синий кружок с восклицательным знаком, наследование для этого контейнера заблокировано.

Можно запретить администратору контейнера перекрывать или блокировать наследуемые параметры групповой политики, задав принудительное наследование. При этом все настроенные параметры политик с более высокого уровня наследуются и применяются независимо от того, какие параметры политик настроены на более низком уровне. Таким образом, принудительное наследование отменяет и перекрытие, и блокировку параметров политик.

При помощи принудительного наследования администраторы леса отменяют блокировку или перекрытие введенные администраторами доменов и подразделений. Администраторы домена этим же способом отменяют блокировки и перекрытия, введенные администраторами подразделений.

Чтобы ввести принудительное наследование при помощи GPMC, разверните контейнер высокого уровня, с которого нужно начать принудительное наследование, щелкните правой кнопкой ссылку на GPO и выберите команду **Принудительный (Enforced)**. Допустим, чтобы гарантировать наследование всеми подразделениями GPO уровня домена, разверните контейнер

домена, щелкните правой кнопкой GPO доменного уровня и выберите команду **Принудительный (Enforced)**. Если она уже отмечена, ее повторный выбор отменит принудительное наследование. В GPMC очень просто определить, какие политики наследуются принудительно. Выделите объект политики и перейдите на вкладку **Область (Scope)** правой панели. У принудительно наследуемой политики в столбце **Принудительный (Enforced)** стоит значение **Да (Yes)**, как показано на рис. 5-6.

Выделив объект политики, щелкните правой кнопкой соответствующий элемент в столбце **Размещение (Location)** на вкладке **Область (Scope)**, чтобы отобразить контекстное меню, позволяющее управлять связями и принудительным применением политики. Команда **Связь включена (Link Enabled)** служит для включения и выключения связей. При помощи команды **Принудительный (Enforced)** вы управляете принудительным наследованием.

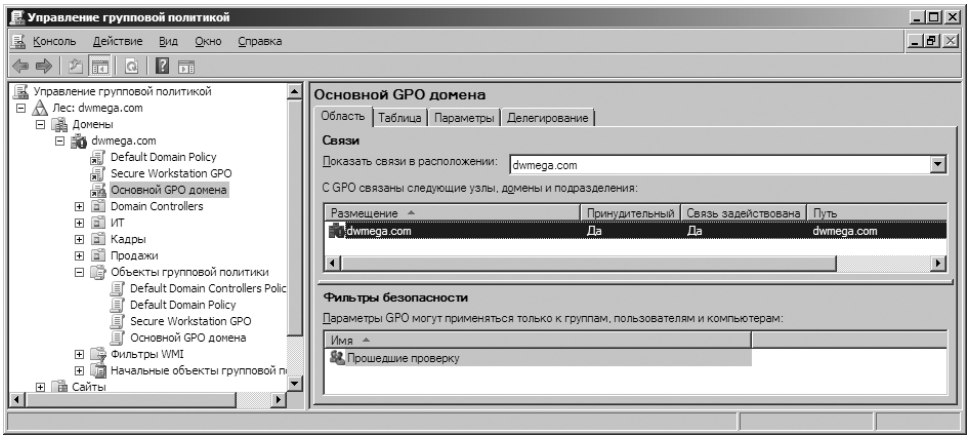


Рис. 5-6. Принудительное наследование гарантирует применение политики

Обслуживание групповых политик и устранение неисправностей

Администрирование групповых политик — обширная область деятельности, требующая продуманного управления. Подобно любой другой административной области, групповые политики нуждаются в обслуживании, гарантирующем их должную работу. Время от времени вам придется разбираться с возникающими неполадками и сбоями. Для этого вам понадобится четкое понимание процессов обновления и применения политик.

Обновление групповой политики

Изменения, вносимые в групповую политику, сохраняются немедленно, но применяются позже. Клиентские компьютеры запрашивают параметры политик в следующие моменты:

- при запуске компьютера;
- при регистрации пользователя;
- когда приложение или пользователь явно запросили обновление;
- когда истек заданный интервал обновления групповой политики.

Параметры конфигурации компьютера применяются при запуске ОС. Параметры конфигурации пользователя применяются при входе пользователя в систему. Поскольку параметры пользователя применяются позже параметров компьютера, по умолчанию приоритет конфигурации пользователя оказывается выше, чем у конфигурации компьютера. Это означает, что при возникновении конфликта между параметрами компьютера и параметрами пользователя, применены будут параметры пользователя.

После применения параметров политики их обновление производится автоматически, чтобы всегда использовалась текущая версия. Интервал обновления на контроллере домена по умолчанию равен 5 минутам, на всех остальных компьютерах — 90 минут с получасовой вариацией, чтобы не перегрузить контроллер домена массовыми одновременными клиентскими обращениями. То есть, по сути, эффективное окно обновления на обычном компьютере (не контроллере домена) составляет от 90 до 120 минут.

Обновляя групповую политику, клиентский компьютер обращается к доступному контроллеру домена из локального сайта. Если один или несколько объектов политики в домене изменились, контроллер домена предоставляет список всех объектов политики, примененных к данному компьютеру и к зарегистрированному в данный момент пользователю, независимо от того изменились ли номера версий объектов политики из этого списка. По умолчанию компьютер обрабатывает объекты политики, только если изменился номер версии хотя бы одного объекта. Если изменена хотя бы одна связанная политика, обрабатывать приходится все политики — из-за наследования и взаимозависимостей между политиками.

Важным исключением из этого правила являются параметры безопасности. По умолчанию они обновляются каждые 16 часов (960 минут) независимо от изменений в объектах политики. К интервалу обновления добавляется случайный 30-минутный сдвиг, чтобы сократить нагрузку на сеть и контроллеры домена (в результате эффективное окно обновления составляет от 960 до 990 минут). Кроме того, если клиентский компьютер обнаруживает, что скорость сетевого подключения невысока, он уведомляет об этом контроллер домена, и по сети передаются только параметры безопасности и административные шаблоны. Соответственно, по умолчанию и применяются в медленной сети только они. При помощи политики способ использования медленной сети можно изменить.

Следите за соответствием между интервалом обновления и реальной частотой внесения изменений в политики. Если политика изменяется редко, окно обновления стоит увеличить, чтобы сократить нагрузку на ресурсы.

Можно, например, задать 20-минутный интервал обновления на контроллерах домена и 180-минутный интервал на других компьютерах.

Интервал обновления задается отдельно для каждого объекта политики. Чтобы задать интервал обновления на контроллере домена, выполните следующие действия:

1. В GPMC щелкните правой кнопкой объект групповой политики, который хотите отредактировать, и выберите команду **Изменить (Edit)**. Этот GPO должен быть связан с контейнером, содержащим объекты контроллеров домена.
2. Дважды щелкните политику **Интервал обновления групповой политики для контроллеров домена (Group Policy Refresh Interval For Domain Controllers)** в узле **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика (Computer Configuration\Administrative Templates\System\Group Policy)**. Откроется диалоговое окно свойств политики, показанное на рис. 5-7.

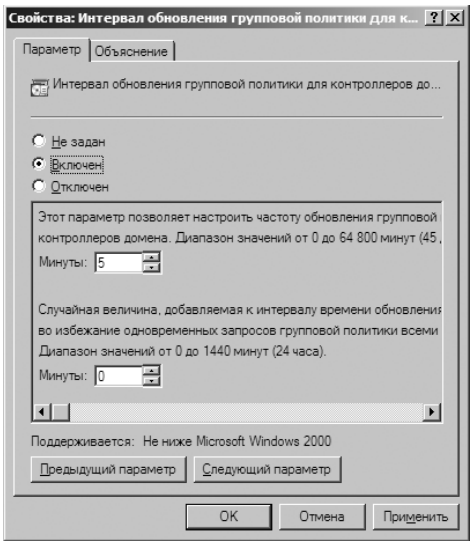


Рис. 5-7. Настройка интервала обновления групповой политики

3. Установите переключатель **Включен (Enabled)**. Задайте базовый интервал обновления в первом счетчике **Минуты (Minutes)**. Обычно его значение заключено между 5 и 59 минутами.
4. Во втором счетчике **Минуты (Minutes)** задайте минимальную и максимальную величину вариации интервала обновления. Вариация, по сути, создает окно обновления, позволяющее сократить нагрузку на сервер от одновременных клиентских обращений. Щелкните **OK**.

Примечание Чем чаще вы обновляете политику, тем надежнее гарантия того, что на компьютере всегда имеется самая актуальная информация о политиках. Чем реже вы обновляете политику, тем менее загружены ваши ресурсы, но одновременно повышается вероятность того, что на компьютере окажется устаревшая политика.

Настройка интервала обновления на других компьютерах

Чтобы задать интервал обновления на рядовых серверах и рабочих станциях, выполните следующие действия:

1. В GPMC щелкните правой кнопкой объект групповой политики, который хотите отредактировать, и выберите команду **Изменить (Edit)**. Этот GPO должен быть связан с контейнером, содержащим объекты нужных компьютеров.
2. Дважды щелкните политику **Интервал обновления групповой политики для компьютеров (Group Policy Refresh Interval For Computers)** в узле **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика (Computer Configuration\Administrative Templates\System\Group Policy)**. Откроется окно, подобное тому, что было показано ранее на рис. 5-7.
3. Установите переключатель **Включен (Enabled)**. Задайте базовый интервал обновления в первом счетчике **Минуты (Minutes)**. Обычно его значение заключено между 60 и 240 минутами.
4. Во втором счетчике **Минуты (Minutes)** задайте минимальную и максимальную величину вариации интервала обновления. Вариация, по сути, создает окно обновления, позволяющее сократить нагрузку на сервер от одновременных клиентских обращений. Щелкните **OK**.

Ближе к реальности Обновления должны происходить, с одной стороны, не слишком часто, чтобы не перегружать сервер, с другой стороны, не слишком редко, чтобы обеспечить своевременность внесения изменений. Чем чаще обновляется политика, тем больше трафик по сети. В крупных организациях обычно стоит увеличить интервал обновления по сравнению со значением по умолчанию для сокращения трафика, особенно, если политика затрагивает сотни пользователей или компьютеров. Увеличить интервал обновления можно и в небольших организациях, если пользователи жалуются на то, что их компьютеры время от времени начинают «тормозить». Подумайте: возможно в вашей организации достаточно проводить обновление раз в день или даже раз в неделю.

Администратору иногда приходится обновлять групповую политику вручную. Допустим, можно попытаться при помощи обновления политик разрешить внезапно возникшую проблему. Возможно также, что вы просто не хотите ждать автоматического обновления. Для ручного обновления групповых политик служит утилита командной строки Gpupdate.

Есть несколько способов обновления. Если вы просто введете **gpupdate** в командной строке, обновлены будут как конфигурация компьютера, так и конфигурация пользователя на локальном компьютере. Пр этом обрабатываются и применяются только обновленные параметры политик. Чтобы обновить все параметры политик, введите команду с параметром */Force*. Чтобы обновить только конфигурацию компьютера, введите в командной строке **gpupdate /target:computer**. Чтобы обновить только конфигурацию пользователя, введите **gpupdate /target:user**.

Параметры команды Gpupdate позволяют после обновления групповой политики отключить пользователя от системы или перезапустить компьютер. Это полезное свойство, поскольку некоторые групповые политики применяются только при входе пользователя в систему или при запуске компьютера. Отключение пользователя после обновления производится параметром */Logoff*, перезагрузка компьютера — параметром */Boot*.

Моделирование групповой политики для планирования

Моделирование групповой политики поможет вам протестировать различные конфигурационные сценарии, например, проверить реакцию на обнаружение медленного сетевого подключения, оценить последствия перемещения пользователей или компьютеров в другой контейнер Active Directory или убедиться в правильности изменения членства пользователей и компьютеров в группах безопасности.

Разрешение на моделирование групповой политики для планирования имеется у всех администраторов домена и предприятия, а также у пользователей, которым это разрешение делегировано. Чтобы промоделировать групповую политику и оценить последствия различных конфигурационных сценариев, выполните следующие действия:

1. В GPMC щелкните правой кнопкой узел **Моделирование групповой политики (Group Policy Modeling)**, выберите команду **Мастер моделирования групповой политики (Group Policy Modeling Wizard)** и щелкните **Далее (Next)** в первом окне мастера.
2. На странице **Выбор контроллера домена (Domain Controller Selection)** выберите в списке **Контроллеры домена в этом домене (Show Domain Controllers In This Domain)** домен, который хотите моделировать. По умолчанию вы будете моделировать политику на любом доступном контроллере. Чтобы использовать конкретный контроллер, установите переключатель **Указанный контроллер домена (This Domain Controller)** и щелкните нужный контроллер. Затем щелкните **Далее (Next)**.
3. На странице **Выбор компьютера и пользователя (User And Computer Selection)**, показанной на рис. 5-8, выберите моделирование политики на базе контейнера или для конкретных учетных записей. Выберите учетные записи одним из описанных ниже методов и щелкните **Далее (Next)**:
   - Работайте с контейнерами, чтобы моделировать изменения для контейнера в целом, например, для всего подразделения. В разделе **Сведения о пользователе (User Information)** установите переключатель **Контейнер (Container)**, щелкните кнопку **Обзор (Browse)** и выберите нужный контейнер пользователей. Проделайте те же действия в разделе **Информация о компьютере (Computer Information)**, чтобы выбрать нужный контейнер компьютеров.
   - Работайте с конкретными учетными записями, чтобы моделировать изменения для конкретного пользователя или компьютера. В разделе

Сведения о пользователе (User Information) установите переключатель **Пользователь (User)**, щелкните кнопку **Обзор (Browse)** и выберите нужную учетную запись пользователя. Проделайте те же действия в разделе **Информация о компьютере (Computer Information)**, чтобы выбрать нужную учетную запись компьютера.

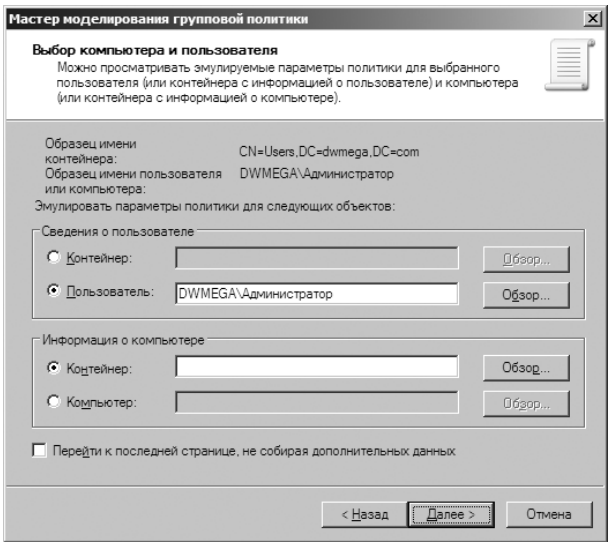


Рис. 5-8. Выбор контейнеров и учетных записей для моделирования

4. На странице **Дополнительные параметры симуляции (Advanced Simulation Options)** при необходимости задайте сайт и условие моделирования (медленное подключение, обработка замыкания на себя) и щелкните **Далее (Next)**.
5. На странице **Группы безопасности пользователя (User Security Groups)** вы можете смоделировать изменения в членстве пользователя или пользователей в группах безопасности. Например, чтобы узнать, что произойдет, если выбранный контейнер пользователей станет членом группы CorpManagers, включите эту группу в список **Группы безопасности (Security Groups)**. Затем щелкните **Далее (Next)**.
6. На странице **Группы безопасности компьютера (Computer Security Groups)** вы можете смоделировать изменения в членстве компьютера или компьютеров в группах безопасности. Например, чтобы узнать, что произойдет, если выбранный контейнер пользователей станет членом группы RemoteComputers, включите эту группу в список **Группы безопасности (Security Groups)**. Затем щелкните **Далее (Next)**.
7. С объектами групповой политики можно связать фильтры WMI. По умолчанию предполагается, что выбранные пользователи и компьютеры удовлетворяют всем требованиям фильтров WMI. При планировании это в большинстве случаев предпочтительный вариант. Два раза щелкните **Далее (Next)**, чтобы принять параметры по умолчанию.

8. Просмотрите сводку выбранных параметров и щелкните **Далее (Next)**. Когда мастер соберет всю нужную информацию, щелкните **Готово (Finish)**. Сгенерированный мастером отчет будет выделен в левой панели и отображен в правой (рис. 5-9).

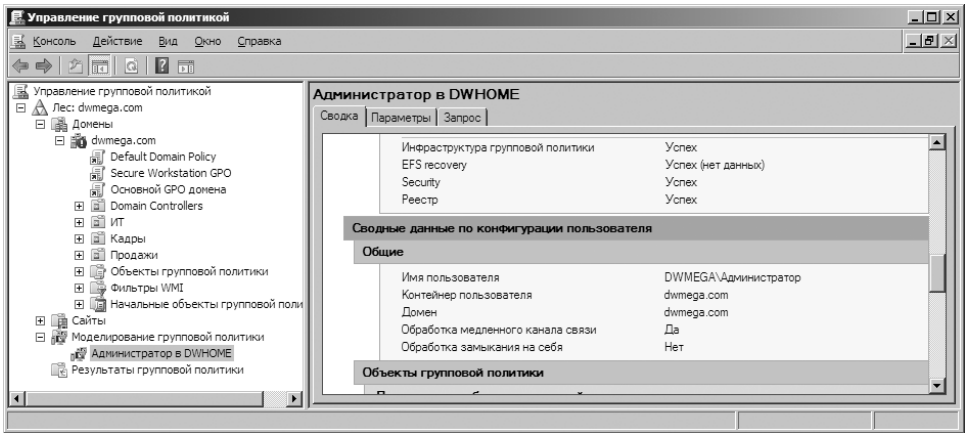


Рис. 5-9. Отчет о результатах моделирования

9. По результатам моделирования выберите параметры, которые следует применить. Информация о политиках компьютера собрана в разделе **Сводные данные по конфигурации компьютера (Computer Configuration Summary)**, информация о политиках пользователя — в разделе **Сводные данные по конфигурации пользователя (User Configuration Summary)**.

Копирование, вставка и импорт объектов политики

В GPMC встроены возможности копирования, вставки и импорта. Действие функций вставки и копирования особенно объяснять не приходится. Соответствующие команды включены в контекстное меню объектов групповой политики в GPMC. С их помощью вы можете скопировать объект политики со всеми параметрами в одном домене, потом перейти в другой домен и вставить объект туда. В качестве исходного и целевого доменов могут использоваться любые домены, к которым вы подключаетесь из GPMC и в которых у вас имеется разрешение на управление объектами политики. В исходном домене для копирования объекта политики вам понадобится разрешение на его чтение. Чтобы скопировать объект в целевой домен, соответственно, необходимо разрешение на запись. Эти разрешения имеются у администраторов, а также у тех пользователей, которым делегировано право создания объектов политики.

Копирование объектов политики из домена в домен не вызывает трудностей, если у вас есть подключение к обоим доменам и соответствующие полномочия. Если же вы администратор удаленного офиса, доступа к ис-

ходному домену у вас может и не быть. В этом случае другой администратор может создать резервную копию объекта политики, а затем переслать вам все необходимые данные. Получив их, вы импортируете резервную копию в свой домен, чтобы создать новый объект политики с теми же параметрами.

Выполнять операцию импорта разрешается любому пользователю, наделенному правом изменения параметров групповой политики. В процессе импорта все параметры выбранного объекта политики перезаписываются. Чтобы импортировать резервную копию объекта политики в своем домене, выполните следующие действия:

1. В GPMC щелкните правой кнопкой узел **Объекты групповой политики (Group Policy Objects)** и выберите команду **Создать (New)**. В диалоговом окне **Новый объект групповой политики (New GPO)** введите имя для нового GPO и щелкните **OK**. Новый GPO будет включен в контейнер **Объекты групповой политики (Group Policy Objects)**.
2. Щелкните правой кнопкой новый объект и выберите команду **Импорт параметров (Import Settings)**. Будет запущен Мастер импорта параметров (Import Settings Wizard).
3. Два раза щелкните **Далее (Next)**, чтобы миновать страницу **Архивирование GPO (Backup GPO)**. На этом этапе нет необходимости архивировать GPO, поскольку он только что создан.
4. На странице **Расположение архива (Backup Location)** щелкните **Обзор (Browse)**. Найдите папку с резервной копией объекта политики и щелкните **OK**. Затем щелкните **Далее (Next)**.
5. Если в указанной папке находится несколько архивов, их список будет приведен на странице **Исходный объект GPO (Source GPO)**. Щелкните нужный объект и кнопку **Далее (Next)**.
6. Мастер проверит объект политики на предмет наличия ссылок на участников безопасности и UNC-путей, которые необходимо переместить. Если таковые найдутся, вам будет предоставлена возможность создать новую таблицу перемещения или воспользоваться существующей.
7. Щелкните **Далее (Next)** и **Готово (Finish)**, чтобы завершить работу мастера и начать импорт. Когда импорт завершится, щелкните **OK**.

Архивирование и восстановление объектов политики

В задачу администратора входит создание резервных копий GPO. При помощи GPMC вы можете архивировать отдельные объекты политики или все объекты домена, выполнив следующие действия:

1. В GPMC разверните и выделите узел **Объекты групповой политики (Group Policy Objects)**. Чтобы архивировать все объекты политики в домене, щелкните правой кнопкой узел **Объекты групповой политики (Group Policy Objects)** и выберите команду **Архивировать все (Back Up All)**. Чтобы архивировать конкретный объект домена, щелкните правой кнопкой этот объект и выберите **Архивировать (Back Up)**.

2. В диалоговом окне **Архивация объекта групповой политики (Back Up Group Policy Object)** щелкните **Обзор (Browse)** и задайте папку для сохранения резервной копии GPO.
3. В поле **Описание (Description)** введите описание архива и щелкните кнопку **Архивировать (Backup)**.
4. Состояние процесса архивирования отражается в диалоговом окне **Архив (Backup)**. Когда создание архива завершится, щелкните **OK**. Если произойдет сбой, проверьте разрешения политики и папки, в которую вы записываете резервную копию. Вам необходимо разрешение на чтение политики и на запись в папку. По умолчанию все эти права есть у членов группы администраторов домена и предприятия.

При помощи GPMC вы можете восстановить объект политики в том состоянии, в котором он находился в момент архивирования. В консоли GPMC архивные копии каждого объекта рассматриваются отдельно, даже если вы архивировали их одной командой. Версии архивов различаются по времени создания и по описанию, поэтому для любого объекта политики вы вольны восстановить как последнюю, так и одну из предыдущих версий.

Чтобы восстановить объект политики, выполните следующие действия:

1. В GPMC щелкните правой кнопкой узел **Объекты групповой политики (Group Policy Objects)** и выберите **Управление архивацией (Manage Backups)**. Откроется одноименное диалоговое окно.
2. Щелкните кнопку **Обзор (Browse)**, найдите папку с архивами и щелкните **OK**.
3. В списке **Архивные объекты GPO (Backup Policy Objects)** перечислены все объекты из указанной папки. Чтобы отображать только последние версии архивов, установите флажок **Показывать только последнюю версию каждого объекта GPO (Show Only The Latest Version Of Each GPO)**.
4. Выделите GPO, который хотите восстановить. Чтобы убедиться в правильности выбора, щелкните кнопку **Просмотр параметров (View Settings)**. Затем щелкните **Восстановить (Restore)** и подтвердите восстановление выбранного объекта, щелкнув **OK**.
5. Ход процесса отображается в диалоговом окне **Восстановление (Restore)**. В случае сбоя проверьте разрешения объекта политики и папки, из которой вы его восстанавливаете. Чтобы восстановить GPO, вам понадобятся разрешения на редактирование его параметров, удаление и изменение параметров безопасности, а также разрешение на чтение из архивной папки. По умолчанию все эти права есть у членов группы администраторов домена и предприятия.

Определение текущих параметров и состояния обновления групповой политики

Моделирование групповой политики может применяться для построения результирующей политики. Это позволяет просматривать все объекты политики, реально примененные к компьютеру, а также выяснить, когда они в последний раз обрабатывались (обновлялись). Разрешение на моделирование групповой политики для целей протоколирование есть у всех администраторов домена и предприятия, а также у тех пользователей, которым было делегировано разрешение на чтение результатов групповой политики. Чтобы промоделировать групповую политику в GPMC, щелкните правой кнопкой узел **Результаты групповой политики Group Policy Results)** и выберите команду **Мастер результатов групповой политики (Group Policy Results Wizard)**. Затем следуйте инструкциям мастера.

Отключение неиспользуемой части групповой политики

Политику необязательно отключать целиком. Можно отключить отдельно параметры конфигурации компьютера или конфигурации пользователя, если они не нужны. Тем самым вы ускорите применение GPO и параметров безопасности.

Чтобы частично или полностью отключить политику, выполните следующие действия:

1. В GPMC выберите контейнер нужного сайта, домена или подразделения.
2. Выделите нужный объект политики и перейдите на вкладку **Таблица (Details)** в правой панели.
3. Выберите в списке **Состояние GPO (GPO Status)** один из описанных ниже вариантов и щелкните **OK**, чтобы подтвердить изменение состояния GPO:
   - **Все параметры отключены (All Settings Disabled)** Отменяет обработку объекта политики и применение всех его параметров.
   - **Параметры конфигурации компьютера отключены (Computer Configuration Settings Disabled)** Отключает обработку параметров конфигурации компьютера. Обрабатываются только параметры конфигурации пользователя.
   - **Включено (Enabled)** Разрешает обработку объекта политики и применение всех его параметров.
   - **Параметры конфигурации пользователя отключены (User Configuration Settings Disabled)** Отключает обработку параметров конфигурации пользователя. Обрабатываются только параметры конфигурации компьютера.

Изменение приоритета обработки политики

Параметры конфигурации компьютера обрабатываются при запуске компьютера и его подключении к сети. Параметры конфигурации пользователя обрабатываются при входе пользователя в сеть. При возникновении конфликта между параметрами компьютера и пользователя большим приоритетом обладают параметры компьютера. Важно также помнить, что параметры компьютера применяются из GPO компьютера, а параметры пользователя — из GPO пользователя.

Иногда возникают обстоятельства, в которых такой порядок требуется изменить. В частности, на общем компьютере или на компьютере закрытой лаборатории может потребоваться применение параметров пользователя из GPO компьютера, чтобы обеспечить соответствие правилам безопасности. Применение параметров пользователя из GPO компьютера осуществляется посредством обработки замыкания на себя (loopback processing).

Чтобы изменить параметры обработки замыкания на себя, выполните следующие действия:

1. В GPMC щелкните правой кнопкой нужный объект групповой политики и щелкните команду **Изменить (Edit)**.
2. Щелкните дважды политику **Режим обработки замыкания пользовательской групповой политики (User Group Policy Loopback Processing Mode)** из папки **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика (Computer Configuration\Administrative Templates\System\Group Policy)**. Откроется диалоговое окно свойств политики.
3. Установите переключатель **Включен (Enabled)**, выберите в списке **Режим (Mode)** один из описанных ниже вариантов и щелкните **OK**:
   - **Замена (Replace)** Это вариант означает, что обрабатываться будут только параметры пользователя из GPO компьютера, а параметры из GPO пользователя будут проигнорированы. По сути, параметры пользователя из GPO компьютера заменять параметры пользователя, которые применялись бы в обычных обстоятельствах.
   - **Слияние (Merge)** Сначала будут обрабатываться параметры пользователя из GPO компьютера, потом — из GPO пользователя, потом — опять из GPO компьютера. Такое сочетание позволяет объединить параметры пользователя из GPO обоих видов, причем в случае конфликта предпочтение будет отдано параметрам из GPO компьютера.

Настройка медленного подключения

Обнаружение медленного подключения используется клиентами групповой политики для выявление возрастающих задержек и ухудшения отклика сети. Это позволяет своевременно предпринять корректирующие меры, не дожидаясь, пока обработка групповой политики полностью парализует сеть.

Обнаружив медленное подключение, клиенты групповой политики сокращают сетевые коммуникации и запросы, уменьшая общий сетевой трафик и ограничивая объем обработки политик.

По умолчанию, обнаружив скорость соединения ниже 500 кбит/с (в быстрой сети это можно интерпретировать как значительную задержку и ухудшившийся отклик), клиентский компьютер фиксирует медленное подключение и уведомляет контроллер домена. После этого в процессе обновления контроллер домена передает клиенту только параметры безопасности и административные шаблоны из применимых объектов политики.

Для настройки обнаружения медленного подключения используется политика **Обнаружение медленных подключений для групповой политики (Group Policy Slow Link Detection)** из папки **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика (Computer Configuration\Administrative Templates\System\Group Policy)**. Если эта политика отключена или не настроена, клиенты используют для обнаружения медленного подключения значение по умолчанию — 500 кбит/с. Включив эту политику, вы вольны задать собственное значение, например, 384 кбит/с. Чтобы отключить обнаружение медленного подключения, задайте нулевое значение скорости подключения. После этого клиенты будут автоматически считать все подключения быстрыми.

По умолчанию при обнаружении медленного подключения не обрабатываются следующие разделы политики:

- **Обработка беспроводной политики (Wireless Policy Processing)**;
- **Обработка политики восстановления EFS (EFS Recovery Policy Processing)**;
- **Обработка политики дисковых квот (Disk Quota Policy Processing)**;
- **Обработка политики настройки Internet Explorer (Internet Explorer Maintenance Policy Processing)**;
- **Обработка политики перенаправления папки (Folder Redirection Policy Processing)**;
- **Обработка политики сценариев (Scripts Policy Processing)**;
- **Обработка политики установки программ (Software Installation Policy Processing)**;
- **Обработка политики IP-безопасности (IP Security Policy Processing)**.

При медленном подключении обрабатывается только раздел **Обработка политики безопасности (Security Policy Processing)**. По умолчанию политика безопасности обновляется каждые 16 часов, даже если она не изменялась. Единственный способ остановить принудительное обновление — отказаться от обработки политики безопасности во время периодических фоновых обновлений. Чтобы задать такой режим работы, установите в окне свойств политики флажок **Не применять во время периодической фоновой обработки (Do Not Apply During Periodic Background Processing)**. Поскольку политика безопасности очень важна, даже в этом случае ее об-

работка останавливается, только если в этот момент пользователь зарегистрировать и пользуется компьютером. Останавливать обновление политики безопасности нужно лишь в случае, когда этот процесс приводит к сбоям в приложениях.

Чтобы настроить обнаружение медленного подключения, выполните следующие действия:

1. В GPMC щелкните правой кнопкой нужный объект политики и выберите **Изменить (Edit)**.
2. Щелкните дважды политику **Обнаружение медленных подключений для групповой политики (Group Policy Slow Link Detection)** из папки **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика (Computer Configuration\Administrative Templates\System\Group Policy)**.
3. Установите переключатель **Включен (Enabled)**, как показано на рис. 5-10, и задайте предельную скорость подключения в поле **Скорость подключения (Connection Speed)**. Затем щелкните **OK**.

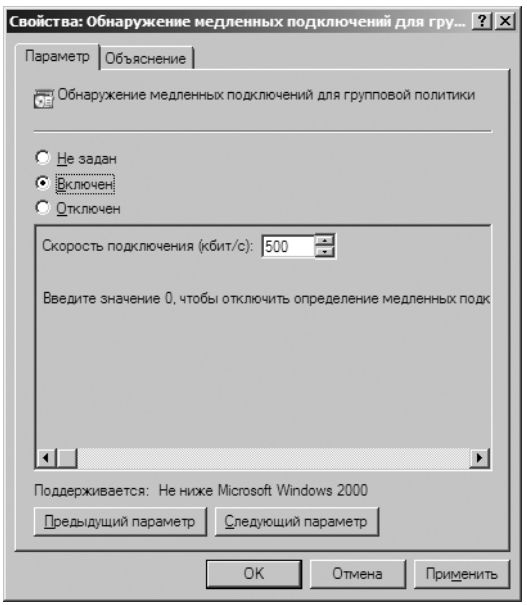


Рис. 5-10. Настройка обнаружения медленного подключения

Чтобы настроить разделы групповой политики, обрабатываемые при медленном подключении, выполните следующие действия:

1. В GPMC щелкните правой кнопкой нужный объект политики и выберите **Изменить (Edit)**.
2. Разверните папку **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика (Computer Configuration\Administrative Templates\System\Group Policy)**.

3. Щелкните дважды политику, которую хотите настроить. Установите переключатель **Включен (Enabled)**, как показано на рис. 5-11, и задайте нужные параметры. Набор доступных параметров зависит от конкретной политики. Возможны, в частности, следующие варианты:
   - **Разрешить обработку через медленное сетевое подключение (Allow Processing Across A Slow Network Connection)** Гарантирует, что параметры будут обработаны независимо от скорости подключения
   - **Не применять во время периодической фоновой обработки (Do Not Apply During Periodic Background Processing)** Политика будет обрабатываться только при запуске компьютера или регистрации пользователя.
   - **Обрабатывать, даже если объекты групповой политики не изменились (Process Even If The Group Policy Objects Have Not Changed)** При обновлении политика будет обрабатываться, даже если ее параметры не изменились.
4. Щелкните **OK**.

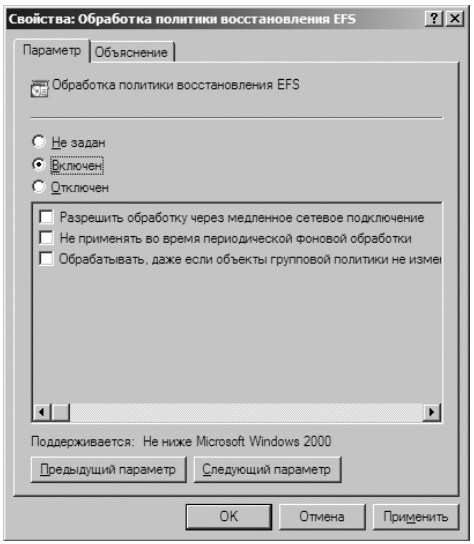


Рис. 5-11. Настройка обработки политик при медленном подключении

Разрыв связей и удаление GPO

Есть два способа остановить использование связанного GPO в GPMC:

- удалить ссылку на GPO, но не сам GPO;
- полностью удалить GPO и все ссылки на него.

Удаление ссылки приведет к тому, что на сайте, в домене или подразделении более не будут использоваться соответствующие параметры политики, но сам GPO удален не будет. Поэтому ссылки на GPO из других сайтов, доменов и подразделений сохранят работоспособность. Чтобы в GPMC уда-

лить ссылку на GPO, щелкните правой кнопкой ссылку на GPO в нужном контейнере и выберите команду **Удалить (Delete)**. Чтобы подтвердить удаление связи, щелкните **OK**. Если вы удалите все связи GPO с сайтами, доменами и подразделениями, он сохранится в контейнере **Объекты групповой политики (Group Policy Objects)**, но параметры его в вашей организации действовать уже не будут.

Полностью удаляя GPO, вы удаляете и все его связи. Он более не содержится в контейнере **Объекты групповой политики (Group Policy Objects)** и не привязан ни к каким сайтам, доменам или подразделениям. Единственный способ вернуть удаленный GPO — восстановить его из резервной копии (если она имеется). Чтобы в GPMC удалить GPO и все его связи, раскройте узел **Объекты групповой политики (Group Policy Objects)**, щелкните GPO правой кнопкой и выберите команду **Удалить (Delete)**. Чтобы подтвердить удаление GPO, щелкните **OK**.

Устранение неполадок в групповых политиках

Если групповая политика применяется не так, как вы ожидаете, первым делом проверьте результирующую политику для пользователя или компьютера (или обоих), у которых возникли проблемы. Чтобы определить, параметры из которого GPO применены, выполните следующие действия:

1. В GPMC щелкните правой кнопкой узел **Результаты групповой политики (Group Policy Results)** и выберите команду **Мастер результатов групповой политики (Group Policy Results Wizard)**. Щелкните **Далее (Next)** в первом окне мастера.
2. На странице **Выбор компьютера (Computer Selection)** установите переключатель **Этот компьютер (This Computer)**, чтобы просмотреть информацию с локального компьютера. Если вас интересует удаленный компьютер, установите переключатель **Другой компьютер (Another Computer)** и щелкните кнопку **Обзор (Browse)**. В диалоговом окне **Выбор: «Компьютер» (Select Computer)** введите имя компьютера и щелкните **Проверить имена (Check Names)**. Выбрав нужную учетную запись, щелкните **OK**.
3. На странице **Выбор пользователя (User Selection)** выберите пользователя, для которого хотите просмотреть информацию политики. Вам доступна информация для любого пользователя с выбранного компьютера. Щелкните **Далее (Next)**.
4. Проверьте заданные параметры и щелкните **Далее (Next)**. Когда мастер закончит сбор информации, щелкните **Готово (Finish)**. Отчет о работе мастера будет выделен в левой панели, а его содержимое будет размещено в правой панели.
5. Изучите отчет. Информация о политиках пользователя и компьютера приводится, соответственно, в разделах **Сводные данные по конфигурации компьютера (Computer Configuration Summary)** и **Сводные данные по конфигурации пользователя (User Configuration Summary)**.

Просматривать результирующую политику можно также при помощи утилиты командной строки Gpresult. Она выводит следующую информацию:

- специальные параметры перенаправления папок, установки программ, дисковых квот, IPSec и сценариев;
- время последнего применения групповой политики;
- контроллер домена, с которого получена политики, и членство в группах безопасности для компьютера и пользователя;
- полный список примененных GPO, а также полный список GPO, которые не были применены в результате действия фильтров.

Общий синтаксис вызова Gpresult выглядит так:

```
gpresult /s ИмяКомпьютера /user Домен\ИмяПользователя
```

где *ИмяКомпьютера* — имя компьютера, для которого требуется результирующая политика, а *Домен\ИмяПользователя* — пользователь, для которого требуется политика. Например, чтобы просмотреть результирующую политику для компьютера CorpPC85 и пользователя tedg в домене CPANDL, введите следующую команду:

```
gpresult /s corppc85 /user cpandl\tedg
```

Существует два параметра для вывода более подробной информации. Параметр */v* включает подробный вывод информации только о действующих параметрах политики. Параметр */z* включает подробный вывод информации о действующих параметрах политики, а также обо всех других GPO, в которых заданы политики. Поскольку выводная информация утилиты Gpresult может быть довольно объемистой, создайте отчет в формате HTML при помощи параметра */H* или в формате XML при помощи параметра /X. Далее приводятся примеры их использования:

```
gpresult /s corppc85 /user cpandl\tedg /h gpreport.html
gpresult /s corppc85 /user cpandl\tedg /x gpreport.xml
```

Восстановление политик по умолчанию

Политика домена по умолчанию и политика контроллера домена по умолчанию жизненно важны для работы доменных служб Active Directory. Если по какой-то причине эти политики оказались испорчены, групповая политика должным образом работать не будет. Чтобы исправить ситуацию, при помощи GPMC восстановите эти GPO из резервной копии. Если никаких резервных копий у вас нет, восстановите параметры безопасности в этих политиках при помощи утилиты DCGPOFIX. Состояние, которое она восстанавливает, зависит от того, как DCGPOFIX изменила безопасность, и от состояния безопасности контроллера домена перед запуском DCGPOFIX. Чтобы запустить DCGPOFIX, вы должны быть членом группы администраторов домена или предприятия.

При запуске DCGPOFIX по умолчанию восстанавливаются как политика домена, так и политика контроллера домена по умолчанию. Все изменения, внесенные вами в эти политики, будут утрачены. Некоторые дополнительные параметры хранятся отдельно и потому не теряются. К ним относятся параметры служб удаленной установки (Remote Installation Services, RIS), безопасности и файловой системы EFS. Остальные дополнительные параметры восстанавливаются в прежних значениях. Все внесенные в них изменения не сохраняются.

Чтобы запустить DCGPOFIX, зарегистрируйтесь на контроллере домена, в котором вы хотите восстановить политику по умолчанию. Введите **dcgpofix** в командной строке с повышенными полномочиями. DCGPOFIX проверяет номер версии схемы Active Directory, чтобы гарантировать совместимость используемой версии DCGPOFIX с конфигурацией схемы Active Directory. Если версии не совместимы, DCGPOFIX прекращает работу без восстановления групповой политики. Задав параметр */Ignoreschema*, вы разрешите использование DCGPOFIX с другими версиями Active Directory. Однако при этом возможно, что объекты политик по умолчанию не будут восстановлены в исходных состояниях. Поэтому всегда обязательно используйте версию DCGPOFIX из текущего комплекта ОС.

У вас также есть возможность восстановить только политику домена по умолчанию или только политику контроллера домена по умолчанию. В первом случае введите **dcgpofix /target:domain**, во втором — **dcgpofix /target:dc**.

Управление пользователями и компьютерами при помощи групповой политики

Есть множество способов использования групповой политики для управления пользователями и компьютерами. Далее мы рассмотрим следующие вопросы:

- перенаправление папок;
- сценарии компьютера и пользователя;
- развертывание ПО;
- подача компьютерами и пользователями заявок на сертификаты;
- параметры автоматического обновления.

Централизованное управление специальными папками

Централизованное управление специальными папками Windows Server 2008 осуществляется при помощи перенаправления папок. При этом специальные папки перенаправляются в централизованное сетевое расположение, чтобы не использовать множество расположений по умолчанию на каждом компьютере. В Windows XP Professional и более ранних версиях Windows к централизованно управляемым специальным папкам относятся Application Data, Главное меню (Start Menu), Рабочий стол (Desktop), Мои документы (My Documents) и Мои рисунки (My Pictures). В Windows Vista и более поздних

версиях Windows это папки AppData, Рабочий стол (Desktop), Главное меню (Start Menu), Документы (Documents), Изображения (Pictures), Музыка (Music), Видео (Videos), Избранное (Favorites), Контакты (Contacts), Загрузка (Downloads), Ссылки (Links), Поиски (Searches) и Сохраненные Игры (Saved Games).

Есть два варианта перенаправления: можно перенаправить специальную папку в одно и то же сетевое расположение для всех пользователей или назначить расположения на основании членства пользователей в группах безопасности. В обоих случаях обязательно проверьте, доступно ли это нужно сетевое расположение в виде общего ресурса (подробнее — в главе 15).

Перенаправление специальной папки в единое расположение

Чтобы перенаправить специальную папку в единое расположение, выполните следующие действия:

1. В GPMC щелкните правой кнопкой нужный GPO сайта, домена или подразделения и выберите команду **Изменить (Edit)**. Откроется редактор политики.
2. Разверните узлы **Конфигурация пользователя (User Configuration)**, **Конфигурация Windows (Windows Settings)** и **Перенаправление папки (Folder Redirection)**.
3. В узле **Перенаправление папки (Folder Redirection)** щелкните правой кнопкой специальную папку, которую хотите перенаправить, например, **AppData(Roaming)**, и выберите команду **Свойства (Properties)**. Откроется диалоговое окно, как на рис. 5-12.
4. На вкладке **Конечная папка (Target)** выберите в списке вариант **Перенаправлять папки всех пользователей в одно место (простая) (Basic—Redirect Everyone's Folder To The Same Location)**.

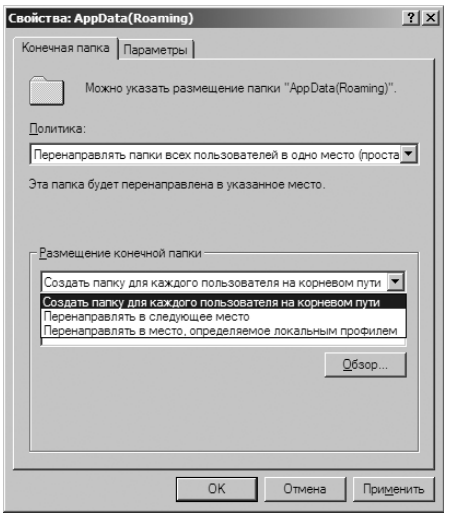


Рис. 5-12. Настройка перенаправления папки AppData(Roaming)

5. В группе **Размещение конечной папки (Target Folder Location)** доступно несколько параметров. Их конкретный набор зависит от того, с какой папкой вы работаете:
   - **Перенаправить на домашнюю папку пользователя (Redirect To The User's Home Directory)** Папка перенаправляется в подпапку домашней папки пользователя. Размещение домашней папки пользователя задается при помощи переменных среды %HomeDrive% и %HomePath%.
   - **Создать папку для каждого пользователя на корневом пути (Create A Folder For Each User Under The Root Path)** Папка для каждого пользователя создается в пути, указанном в поле **Корневой путь (Root Path)**. Имя папки совпадает с именем пользователя из переменной %UserName%. Если вы указали корневой путь \\Zeta\UserDocuments, папка для пользователя WilliamS будет расположена по адресу \\Zeta\UserDocuments\WilliamS.
   - **Перенаправлять в следующее место (Redirect To The Following Location)** Папка перенаправляется точно в размещение, указанное в поле **Корневой путь (Root Path)**. В этом случае настройка папки для каждого пользователя осуществляется при помощи переменной среды, например, \\Zeta\UserData\%UserName%\docs.
   - **Перенаправлять в место, определяемое локальным профилем (Redirect To The Local Userprofile Location)** Папка перенаправляется в подпапку профиля пользователя. Расположение профиля пользователя задается переменной среды %UserProfile%.
6. Перейдите на вкладку **Параметры (Settings)**, настройте дополнительные параметры, указанные ниже, и щелкните **OK**.
   - **Предоставить право монопольного доступа к (Grant The User Exclusive Rights To)** У пользователя будет полный доступ к данным из специальной папки.
   - **Перенести содержимое ... в новое место (Move The Contents Of ... To The New Location)** Данные из специальных папок на конкретных системах перемещаются в централизованную сетевую папку (или папки).

Перенаправление специальной папки на основании членства в группе

Чтобы перенаправить специальную папку на основании членства в группе, выполните следующие действия:

1. В GPMC щелкните правой кнопкой нужный GPO сайта, домена или подразделения и выберите команду **Изменить (Edit)**. Откроется редактор политики.
2. Разверните узлы **Конфигурация пользователя (User Configuration)**, **Конфигурация Windows (Windows Settings)** и **Перенаправление папки (Folder Redirection)**.

3. В узле **Перенаправление папки (Folder Redirection)** щелкните правой кнопкой специальную папку, которую хотите перенаправить, например, **Application Data**, и выберите команду **Свойства (Properties)**.
4. На вкладке **Конечная папка (Target)** выберите в списке вариант **Указать различные места для разных групп пользователей (Advanced–Specify Locations For Various User Groups)**. Как показано на рис. 5-13, в диалоговом окне свойство появится раздел **Членство в группе безопасности (Security Group Membership)**.

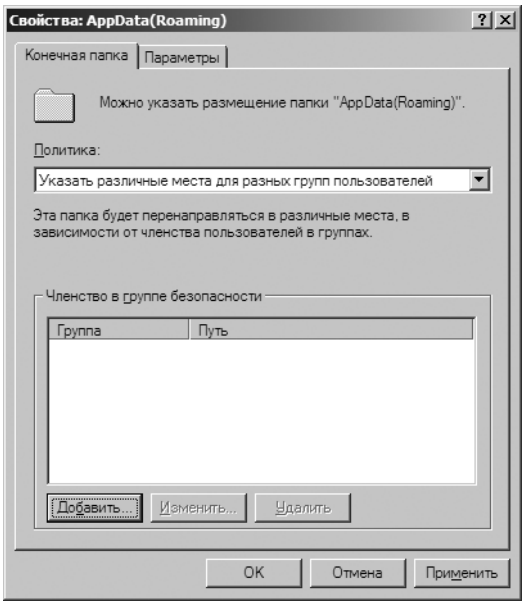


Рис. 5-13. Настройка перенаправления папок на основании членства в группе

5. Щелкните **Добавить (Add)**, чтобы открыть диалоговое окно **Выбор группы и размещения (Specify Group And Location)**. Или выберите элемент существующей группы и щелкните **Изменить (Edit)**, чтобы отредактировать его параметры.
6. В поле **Членство в группе безопасности (Security Group Membership)** введите название группы безопасности, для которой вы настраиваете перенаправление, или щелкните кнопку **Обзор (Browse)**, чтобы найти группу для добавления.
7. Как и в случае простого перенаправления, набор параметров зависит от того, с какой папкой вы сейчас работаете:
   - **Перенаправить на домашнюю папку пользователя (Redirect To The User's Home Directory)** Папка перенаправляется в подпапку домашней папки пользователя. Размещение домашней папки пользователя задается при помощи переменных среды %HomeDrive% и %HomePath%.

  - **Создать папку для каждого пользователя на корневом пути (Create A Folder For Each User Under The Root Path)** Папка для каждого пользователя создается в пути, указанном в поле **Корневой путь (Root Path)**. Имя папки совпадает с именем пользователя из переменной %UserName%. Если вы указали корневой путь \\Zeta\UserDocuments, папка для пользователя WilliamS будет расположена по адресу \\Zeta\UserDocuments\WilliamS.
  - **Перенаправлять в следующее место (Redirect To The Following Location)** Папка перенаправляется точно в размещение, указанное в поле **Корневой путь (Root Path)**. В этом случае настройка папки для каждого пользователя осуществляется при помощи переменной среды, например, \\Zeta\UserData\%UserName%\docs.
  - **Перенаправлять в место, определяемое локальным профилем (Redirect To The Local Userprofile Location)** Папка перенаправляется в подпапку профиля пользователя. Расположение профиля пользователя задается переменной среды %UserProfile%.
- Щелкните **OK**. При необходимости повторите шаги 5–7 для всех групп, которые вы хотите настроить.
- Закончив настройку групп, перейдите на вкладку **Параметры (Settings)**, задайте дополнительные параметры, перечисленные ниже, и щелкните **OK**.
  - **Предоставить право монопольного доступа к (Grant The User Exclusive Rights To)** У пользователя будет полный доступ к данным из специальной папки.
  - **Перенести содержимое ... в новое место (Move The Contents Of ... To The New Location)** Данные из специальных папок на конкретных системах перемещаются в централизованную сетевую папку (или папки).

Отказ от перенаправления

Иногда нужно отказаться от перенаправления конкретной специальной папки. Для этого выполните следующие действия:

1. В GPMC щелкните правой кнопкой нужный GPO сайта, домена или подразделения и выберите команду **Изменить (Edit)**. Откроется редактор политики.
2. Разверните узлы **Конфигурация пользователя (User Configuration)**, **Конфигурация Windows (Windows Settings)** и **Перенаправление папки (Folder Redirection)**.
3. В узле **Перенаправление папки (Folder Redirection)** щелкните правой кнопкой специальную папку, которую более не хотите перенаправлять, и выберите команду **Свойства (Properties)**.
4. Перейдите на вкладку **Параметры (Settings)** и установите нужный переключатель в разделе **Удаление политики (Policy Removal)**. Доступно два варианта:

- **После удаления политики переместить папку (Leave The Folder In The New Location When Policy Is Removed)** Папка и ее содержимое остаются в перенаправленном размещении. Текущие пользователи могут получить доступ к папке и ее содержимому по новому адресу.
- **После удаления политики перенаправить папку обратно в локальный профиль пользователя (Redirect The Folder Back To The Local Userprofile Location When Policy Is Removed)** Папка и ее содержимое возвращаются в исходное расположение. Однако и из предыдущего расположения содержимое не удаляется.

5. Перейдите на вкладку **Конечная папка (Target)**. Если вы изменили положение переключателя в разделе **Удаление политики (Policy Removal)**, перед этим щелкните **Применить (Apply)**.
6. Чтобы полностью отказаться от перенаправления, выберите в списке вариант **Не задана (Not Configured)**.
7. Чтобы отменить перенаправление для определенной группы безопасности, выберите группу в списке **Членство в группе безопасности (Security Group Membership) и** щелкните **Удалить (Remove)**. Затем щелкните **OK**.

Управление сценариями пользователя и компьютера

В Windows Server 2008 настраиваются сценарии четырех типов:

- **Автозагрузка (Computer Startup)** Выполняется во время запуска компьютера.
- **Завершение работы (Computer Shutdown)** Выполняется перед выключением компьютера.
- **Вход в систему (User Logon)** Выполняется при входе пользователя в систему.
- **Выход из системы (User Logoff)** Выполняется при выходе пользователя из системы.

Сценарии могут создаваться как командные файлы с расширением .bat или .cmd или как сценарии WSH (Windows Script Host). WSH — это компонент Windows Server 2008, который позволяет запускать сценарии, написанные на языке, подобном VBScript, без вставки в веб-страницу. Возможность многоцелевого использования сценариев в WSH обеспечивается обработчиками сценариев (scripting engine), в которых определены основы синтаксиса и структуры конкретных языков. Windows Server 2008 поставляется с обработчиками сценариев VBScript и JScript, но доступны и другие обработчики.

Назначение сценариев запуска и завершения

Сценарии запуска и завершения назначаются при помощи групповой политики. При этом сценарии автоматически выполняются при загрузке и выключении всех компьютеров, являющихся членами сайта, домена или подразделения.

Чтобы назначить сценарий запуска или завершения, выполните следующие действия:

1. Для простоты скопируйте нужные вам сценарии в папку Machine\Scripts\Startup или Machine\Scripts\Shutdown соответствующей политики. Политики хранятся в папке %SystemRoot%\Sysvol\Domain\Policies на контроллере домена.
2. В GPMC щелкните правой кнопкой GPO сайта, домена или подразделения и выберите команду **Изменить (Edit)**. Откроется редактор политики.
3. В узле **Конфигурация компьютера (Computer Configuration)** щелкните дважды узел **Конфигурация Windows (Windows Settings)**, а затем щелкните **Сценарии (Scripts)**.
4. Чтобы поработать со сценариями запуска, щелкните правой кнопкой папку **Автозагрузка (Startup)** и выберите **Свойства (Properties)**. Чтобы поработать со сценариями завершения, щелкните правой кнопкой папку **Завершение работы (Shutdown)** и выберите **Свойства (Properties)**. Откроется диалоговое окно, подобное тому, что показано на рис. 5-14.

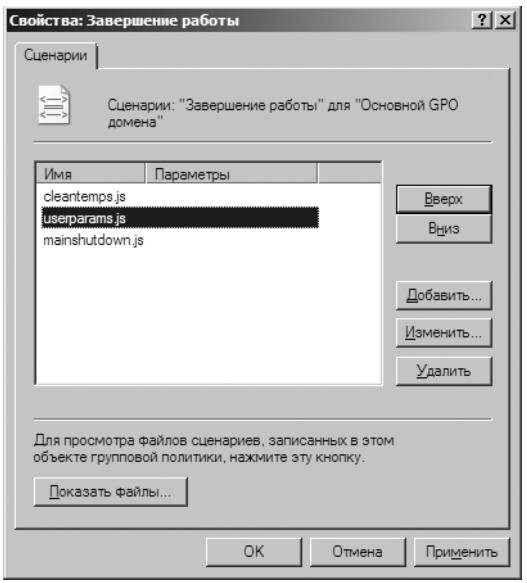


Рис. 5-14. Окно для добавления, редактирования и удаления сценариев завершения работы

5. Щелкните кнопку **Показать файлы (Show Files)**. Если вы правильно разместили сценарии внутри папки Policies, вы должны увидеть нужный сценарий.
6. Щелкните **Добавить (Add)**, чтобы открыть диалоговое окно **Добавление сценария (Add A Script)**. В поле **Имя сценария (Script Name)** введите имя файла сценария, скопированного в папку Machine\Scripts\Startup или Machine\Scripts\Shutdown соответствующей политики. В поле **Па-**

раметры сценария (Script Parameters) введите аргументы командной строки или параметры для сценария WSH. Повторите этот шаг для добавления всех нужных сценариев.

7. При запуске и выключении компьютера сценарии запускаются в том порядке, в котором они указаны в диалоговом окне свойств. При необходимости измените этот порядок с помощью кнопок **Вверх (Up)** и **Вниз (Down)**.
8. Чтобы позже отредактировать имя или параметры сценария, выберите его в списке **Сценарии… для (Script… For)** и щелкните **Изменить (Edit)**.
9. Чтобы удалить сценарий, выберите его в списке **Сценарии… для (Script… For)** и щелкните **Удалить (Remove)**.

Назначение сценариев входа и выхода

Пользовательские сценарии назначаются одним из трех способов:

- **В составе групповой политики** Сценарии автоматически выполняются при входе и выходе всех пользователей, являющихся членами сайта, домена или подразделения.
- **Индивидуально** Для этого используется консоль **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**. Собственный сценарий назначается отдельным пользователям и группам. Подробнее — в разделе «Настройка параметров среды пользователя» главы 11.
- **По расписанию** Сценарии назначаются как задачи при помощи планировщика.

Чтобы назначить сценарий входа или выхода при помощи групповой политики, выполните следующие действия:

1. Для простоты скопируйте нужные вам сценарии в папку User\Scripts\Logon или User\Scripts\Logoff соответствующей политики. Политики хранятся в папке %SystemRoot%\Sysvol\Domain\Policies на контроллере домена.
2. В GPMC щелкните правой кнопкой GPO сайта, домена или подразделения и выберите команду **Изменить (Edit)**. Откроется редактор политики.
3. В узле **Конфигурация пользователя (User Configuration)** щелкните дважды узел **Конфигурация Windows (Windows Settings)**, а затем щелкните **Сценарии (Scripts)**.
4. Чтобы поработать со сценариями входа, щелкните правой кнопкой папку **Вход в систему (Logon)** и выберите **Свойства (Properties)**. Чтобы поработать со сценариями завершения, щелкните правой кнопкой папку **Выход из системы (Logoff)** и выберите **Свойства (Properties)**. Откроется диалоговое окно, подобное тому, что показано на рис. 5-15.

Рис. 5-15. Окно для добавления, редактирования и удаления сценариев входа в систему

5. Щелкните кнопку **Показать файлы (Show Files)**. Если вы правильно разместили сценарии внутри папки Policies, вы должны увидеть нужный сценарий.
6. Щелкните **Добавить (Add)**, чтобы открыть диалоговое окно **Добавление сценария (Add A Script)**. В поле **Имя сценария (Script Name)** введите имя файла сценария, скопированного в папку User\Scripts\Logon или User\Scripts\Logoff соответствующей политики. В поле **Параметры сценария (Script Parameters)** введите аргументы командной строки или параметры для сценария WSH. Повторите этот шаг для добавления всех нужных сценариев.
7. При входе и выходе пользователя из системы сценарии запускаются в том порядке, в котором они указаны в диалоговом окне свойств. При необходимости измените этот порядок с помощью кнопок **Вверх (Up)** и **Вниз (Down)**.
8. Чтобы позже отредактировать имя или параметры сценария, выберите его в списке **Сценарии… для (Script… For)** и щелкните **Изменить (Edit)**.
9. Чтобы удалить сценарий, выберите его в списке **Сценарии… для (Script… For)** и щелкните **Удалить (Remove)**.

Развертывание программ

В групповых политиках предусмотрена для развертывания ПО — политика Установка программ (Software Installation). Она, разумеется, не призвана заменить корпоративные решения, подобные Systems Management Server (SMS), однако с ее помощью можно автоматически развертывать и обслу-

живать ПО в организациях любых размеров, при условии что на компьютерах работают корпоративные версии Windows 2000 и более поздние.

Знакомство с политикой установки программ

Групповая политика позволяет устанавливать ПО для конкретных компьютеров и конкретных пользователей. В первом случае ПО доступно всем пользователям компьютера, а его установка настраивается в узле **Конфигурация компьютера\Конфигурация программ\Установка программ (Computer Configuration\Software Settings\Software Installation)**. Во втором случае ПО доступно индивидуальным пользователям, а его установка настраивается в узле **Конфигурация пользователя\Конфигурация программ\Установка программ (User Configuration\Software Settings\Software Installation)**.

Есть три основных способа развертывания ПО:

- **Назначение компьютеру** Назначайте ПО клиентским компьютерам, чтобы оно устанавливалось при запуске компьютера. Этот метод не требует вмешательства пользователя, однако для установки требуется перезапуск компьютера. Установленное ПО доступно всем пользователям компьютера.
- **Назначение пользователю** Назначайте ПО пользователю, чтобы оно устанавливалось при его входе в систему. Этот метод не требует вмешательства пользователя, однако для установки требуется вход в систему. ПО связано только с этим пользователем.
- **Публикация для пользователя** Публикуйте ПО, чтобы пользователи устанавливали его самостоятельно при помощи утилиты Программы и компоненты (Programs And Features). Этот метод предполагает, что пользователь устанавливает ПО вручную. ПО связано только с этим пользователем.

Используя назначение пользователю или публикацию, вы можете лишь объявить о наличии ПО, с тем чтобы оно было установлено при первой попытке использования. ПО автоматически устанавливается в следующих ситуациях:

- пользователь обращается к документу, для открытия которого необходимо устанавливаемое ПО;
- пользователь открывает ярлык для ПО;
- один из компонентов ПО требуется другому приложению.

Настройку политики Установка программ (Software Installation) не стоит проводить в существующем GPO. Лучше создайте специальные GPO для настройки установки программ, а затем свяжите эти GPO с соответствующими контейнерами. При использовании этого подхода существенно облегчается повторное развертывание ПО и применение обновлений.

Создав новый GPO для развертывания ПО, вы должны затем создать точку распространения — общую папку, доступную всем компьютерам и пользователям, для которых предназначается развертываемое ПО. Для

большинства приложений это означает, что вы копируете пакет установщика и все необходимые файлы в общий ресурс и задаете разрешения, которые открывали бы доступ к этим файлам. В некоторых приложениях, например, Microsoft Office, точка распространения создается путем административной установки в общий ресурс. В Microsoft Office вы для этого должны запустить программу Setup с параметром */a* и назначить общий ресурс местом установки. Преимущество административной установки состоит в том, что ПО можно обновлять и повторно устанавливать при помощи политики Установка программ (Software Installation).

Приложения, развернутые при помощи политики Установка программ (Software Installation), обновляются путем применения обновлений, пакетов обновлений или установки более новой версии приложения. У каждого из этих способов — свои особенности.

Развертывание ПО в организации

В политике Установка программ (Software Installation) применяются пакеты установщика Windows (.msi) или файлы ZAW Down-level Application Packages (.zap). При использовании назначения ПО компьютеру или пользователю применяются пакеты .msi. При публикации ПО для пользователя могут применяться как пакеты .msi, так и файлы .zap. Во всех случаях вы должны задать для установочного пакета нужные разрешения, чтобы у всех компьютеров и пользователей, которым он предназначен, было разрешение на его чтение.

Поскольку политика Установка программ (Software Installation) применяется только при активной (не фоновой) обработке параметров политики, развертывание ПО для компьютера осуществляется при его запуске, а развертывание ПО для пользователя — при входе пользователя в систему. Для настройки установки воспользуйтесь файлами .mst, которые позволяют изменить процесс установки согласно параметрам, заданным вами для конкретных пользователей и компьютеров.

Чтобы развернуть ПО, выполните следующие действия:

1. В GPMC щелкните правой кнопкой GPO, который хотите использовать для развертывания, и выберите **Изменить (Edit)**.
2. В редакторе политики откройте узел **Конфигурация компьютера\Конфигурация программ\Установка программ (Computer Configuration\Software Settings\Software Installation)** или **Конфигурация пользователя\Конфигурация программ\Установка программ (User Configuration\Software Settings\Software Installation)** в зависимости от нужного типа развертывания.
3. Щелкните правой кнопкой папку **Установка программ (Software Installation)**. В контекстном меню выберите команды **Создать (New)** и **Пакет (Package)**.
4. В диалоговом окне **Открыть (Open)** перейдите в сетевой ресурс, где расположен пакет, выделите пакет и щелкните **Открыть (Open)**.

Примечание В списке типов файлов по умолчанию выбран вариант **Пакеты установщика программ (Windows Installer Packages)**. Выполняя публикацию, вы можете также выбрать тип файла **Пакеты ZAW Down-Level Application (ZAW Down-Level Application Packages)**.

5. В диалоговом окне **Развертывание программ (Deploy Software)**, показанном на рис. 5-16, выберите один из указанных ниже методов развертывания и щелкните **OK**:
   - **Публичный (Published)** Публикация приложения без перенастройки.
   - **Назначенный (Assigned)** Назначение приложения без перенастройки.
   - **Особый (Advanced)** Развертывание приложения с использованием дополнительных параметров.

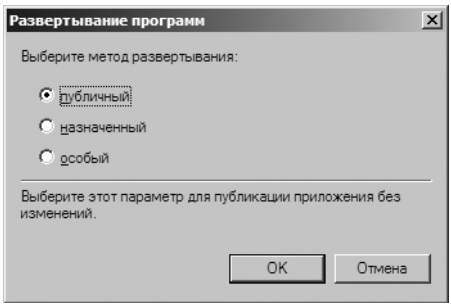


Рис. 5-16. Выбор метода развертывания

Настройка параметров развертывания ПО

Для просмотра и настройки основных параметров пакета ПО выполните следующие действия:

1. В GPMC щелкните правой кнопкой GPO, который хотите использовать для развертывания, и выберите **Изменить (Edit)**.
2. В редакторе политики откройте узел **Конфигурация компьютера\Конфигурация программ\Установка программ (Computer Configuration\Software Settings\Software Installation)** или **Конфигурация пользователя\Конфигурация программ\Установка программ (User Configuration\Software Settings\Software Installation)** в зависимости от нужного типа развертывания.
3. Щелкните дважды пакет установки ПО. В окне свойств просмотрите или измените параметры развертывания ПО.
4. На вкладке **Развертывание (Deployment)**, показанной на рис. 5-17, вы можете изменить тип развертывания и настроить следующие параметры развертывания и установки:
   - **Автоматически устанавливать приложение при обращении к файлу с соответствующим расширением (Auto-Install This Application By File Extension Activation)** Объявляет все расширения файлов, свя-

занные с приложением, для развертывания при первой попытке использования. Этот флажок по умолчанию установлен.

- **Удалять это приложение, если его использование выходит за рамка, допустимые политикой управления (Uninstall This Application When It Falls Out Of The Scope Of Management)** Удаляет приложение, если оно более не применимо к пользователю.
- **Не отображать это приложение в окне мастера установки и удаления программ панели управления (Do Not Display This Package In The Add/Remove Programs Control Panel)** Отменяет отображение приложения в окне мастера установки и удаления программ. Это лишит пользователя возможности отменить установку приложения.
- **Устанавливать это приложение при входе в систему (Install This Application At Logon)** Задает полную установку приложения — не просто объявление о наличии — при входе пользователя в систему. При развертывании публикацией этот параметр недоступен.
- **Пользовательский интерфейс при установке (Installation User Interface Options)** Управляет выполнением установки. При значении по умолчанию — **Полный (Maximum)** — пользователь видит все окна и сообщения программы установки. Выбор параметра **Простой (Basic)** означает, что пользователь в процессе установки увидит только сообщения об ошибках и о завершении работы.

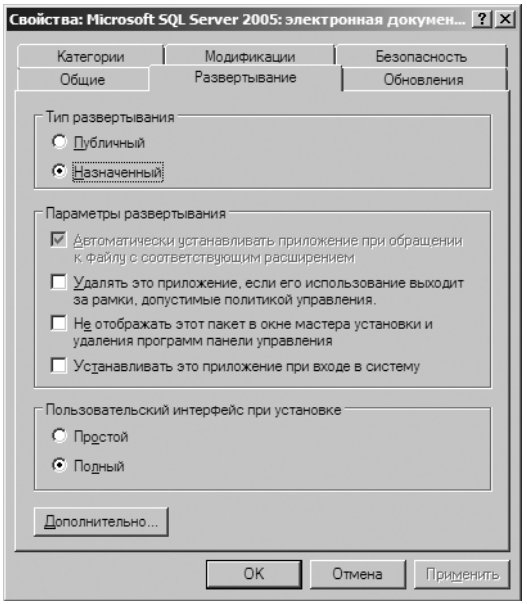


Рис. 5-17. Просмотр и редактирование параметров развертывания

5. Щелкните **OK**.

Обновление развернутого ПО

Чтобы применить обновление или пакет обновлений к приложению, развернутому при помощи пакета установщика Windows, выполните следующие действия:

1. Получив файл .msi или .msp с обновлением или пакетом обновлений, скопируйте его, а также другие установочные файлы в папку с исходным файлом .msi. При необходимости перезапишите дубликаты файлов.
2. В GPMC щелкните правой кнопкой GPO, который используется для развертывания, и выберите **Изменить (Edit)**.
3. В редакторе политики откройте узел **Конфигурация компьютера\Конфигурация программ\Установка программ (Computer Configuration\Software Settings\Software Installation)** или **Конфигурация пользователя\Конфигурация программ\Установка программ (User Configuration\Software Settings\Software Installation)** в зависимости от нужного типа развертывания.
4. Щелкните правой кнопкой нужный пакет. Выберите в контекстном меню команды **Все задачи (All Tasks)** и **Развернуть приложение заново (Redeploy Application)**.
5. Щелкните **Да (Yes)** в окне с запросом на подтверждение действия. Приложение будет повторно развернуто для всех пользователей и компьютеров, заданных для GPO, с которым вы работаете.

Чтобы применить обновление или пакет обновлений к приложению, развернутому не при помощи пакета установщика Windows, выполните следующие действия:

1. В GPMC щелкните правой кнопкой GPO, который используется для развертывания, и выберите **Изменить (Edit)**.
2. В редакторе политики откройте узел **Конфигурация компьютера\Конфигурация программ\Установка программ (Computer Configuration\Software Settings\Software Installation)** или **Конфигурация пользователя\Конфигурация программ\Установка программ (User Configuration\Software Settings\Software Installation)** в зависимости от нужного типа развертывания.
3. Щелкните пакет правой кнопкой и выберите команды **Все задачи (All Tasks)** и **Удалить (Remove)**. Щелкните **OK**, чтобы подтвердить немедленное удаление пакета, выполняемое по умолчанию.
4. Скопируйте новый .zap-файл и другие установочные файлы на сетевой ресурс и повторно разверните приложение.

Переход на следующую версию развернутого ПО

Чтобы перейти на следующую версию ранее развернутого приложения, выполните следующие действия:

1. Получив файл .msi или .msp с обновлением или пакетом обновлений, скопируйте его, а также другие установочные файлы в папку с исходным файлом .msi. Или выполните административную установку.
2. В GPMC щелкните правой кнопкой GPO, который используется для развертывания, и выберите **Изменить (Edit)**.
3. В редакторе политики откройте узел **Конфигурация компьютера\Конфигурация программ\Установка программ (Computer Configuration\Software Settings\Software Installation)** или **Конфигурация пользователя\Конфигурация программ\Установка программ (User Configuration\Software Settings\Software Installation)** в зависимости от нужного типа развертывания.
4. Щелкните правой кнопкой узел **Установка программ (Software Installation)**. Выберите в контекстном меню команды **Создать (New)** и **Пакет (Package)**. Опубликуйте или назначьте приложение, используя файл установщика для новой версии.
5. Щелкните правой кнопкой пакет новой версии и выберите **Свойства (Properties)**. Перейдите на вкладку **Обновления (Upgrades)** и щелкните кнопку **Добавить (Add)**. В диалоговом окне **Добавление обновления (Add Upgrade Package)** выполните одно из следующих действий:
   - Если как исходная, так и новая версии ПО находятся в текущем GPO, установите переключатель **Из текущего объекта групповой политики (Current Group Policy Object)** и выберите ранее развернутое приложение в списке **Обновляемое приложение (Package To Upgrade)**.
   - Если исходная и новая версии ПО находятся в разных GPO, установите переключатель **Из указанного объекта групповой политики (A Specific GPO)**, щелкните **Обзор (Browse)** и выберите GPO в диалоговом окне **Поиск объекта групповой политики (Browse For A Group Policy Object)**. Затем выберите ранее развернутое приложение в списке **Обновляемое приложение (Package To Upgrade)**.
6. Задайте способ обновления. Чтобы произвести полную переустановку приложения, выберите **Удалить приложение, затем установить его обновление (Uninstall The Existing Package, Then Install The Upgrade Package)**. Чтобы установить обновление поверх старого приложения, выберите **Обновление возможно поверх имеющегося приложения (Package Can Upgrade Over The Existing Package)**.
7. Щелкните **OK**, чтобы закрыть диалоговое окно **Добавление обновления (Add Upgrade Package)**. Чтобы сделать обновление обязательным, установите флажок **Обязательное обновление для уже установленных приложений (Required Upgrade For Existing Packages)**. Затем щелкните **OK**, чтобы закрыть окно свойств пакета.

Автоматическая подача заявки на сертификаты компьютера и пользователя

За выпуск цифровых сертификатов и управление списками отзыва сертификатов (certificate revocation list, CRL) отвечает сервер, назначенный на роль сервера сертификации (certificate authority, CA). Чтобы настроить в качестве центра сертификации сервер Windows Server 2008, установите на нем службы сертификации Active Directory. Сертификация необходима компьютерам и пользователям для проверки подлинности и шифрования.

В корпоративной конфигурации CA предприятия используются для автоматической подачи заявок (autoenrollment). Это означает, что авторизованный пользователь и компьютер может запросить сертификат, а центр сертификации способен автоматически обработать этот запрос, чтобы пользователь или компьютер мог немедленно установить сертификат.

Способ работы автоматической подачи заявок определяется групповой политикой. Когда вы устанавливаете корпоративные центры сертификации, автоматически включаются политики автоматической подачи заявок для пользователей и компьютеров. Политика автоматической подачи заявки на сертификат компьютера называется **Клиент служб сертификации: автоматическая подача заявок (Certificate Services Client–AutoEnrollment Settings)** и расположена в узле **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Политики открытого ключа (Computer Configuration\Windows Settings\Security Settings\Public Key Policies)**. Политика автоматической подачи заявки на сертификат пользователя называется так же и расположена в аналогичном подузле узла **Конфигурация пользователя (User Configuration)**.

Чтобы настроить автоматическую подачу заявок, выполните следующие действия:

1. В GPMC щелкните правой кнопкой нужный GPO и выберите **Изменить (Edit)**.
2. В редакторе политики раскройте подузел **Конфигурация Windows\Параметры безопасности\Политики открытого ключа (Windows Settings\Security Settings\Public Key Policies)** узла **Конфигурация пользователя (User Configuration)** или **Конфигурация компьютера (Computer Configuration)**.
3. Щелкните дважды **Клиент служб сертификации: автоматическая подача заявок (Certificate Services Client–AutoEnrollment Settings)**. Чтобы отключить автоматическую подачку заявок, выберите в списке **Модель конфигурации (Configuration Model)** вариант **Отключено (Disabled)**, щелкните **OK** и пропустите остальные шаги. Чтобы отключить автоматическую подачку заявок, выберите в списке **Модель конфигурации (Configuration Model)** вариант **Включено (Enabled)**.
4. Чтобы автоматически возобновлять просроченные сертификаты, обновлять ожидающие сертификаты и удалять отозванные сертификаты, установите соответствующий флажок.

5. Чтобы с гарантией запрашивать и использовать последние версии шаблонов сертификатов, установите флажок **Обновлять сертификаты, использующие шаблоны сертификатов (Update Certificates That Use Certificate Templates)**.
6. Чтобы уведомлять пользователей о скором истечении срока действия сертификата, установите флажок **Уведомлять обо окончании срока действия (Expiration Notification)** и задайте условие отправки обновления. По умолчанию, если уведомления включены, они рассылаются, когда в распоряжении пользователя осталось менее 10% времени действия сертификата.
7. Щелкните **OK**.

Управление автоматическими обновлениями

Настройку автоматического обновления можно проводить индивидуально для каждого компьютера, но гораздо эффективнее управлять им при помощи групповой политики — одновременно для всех пользователей и компьютеров, обрабатывающих данный GPO.

Настройка автоматических обновлений

Управляя автоматическим обновлением при помощи групповой политики, вы выбираете одну из следующих конфигураций:

- **Автоматическая загрузка и установка по расписанию (Auto Download And Schedule The Install)** Обновления загружаются автоматически и устанавливаются согласно заданному вами расписанию. Когда обновление загружено, ОС уведомляет пользователя о том, какие обновления будут установлены по расписанию. При этом пользователь может установить обновления немедленно или дождаться назначенного времени.
- **Автоматическая загрузка и уведомление об установке (Auto Download And Notify For Install)** ОС загружает все обновления по мере их появления, а затем сообщает пользователю о том, что обновления готовы к установке. Пользователь волен принять или отклонить обновление. Принятые обновления устанавливаются, отклоненные — нет, но они остаются в системе, чтобы их можно было установить позже.
- **Уведомления о загрузке и установке (Notify For Download And Notify For Install)** ОС уведомляет пользователя об обновлениях, прежде чем начать их загрузку. Даже согласившись с загрузкой обновления, пользователь сохраняет возможность после загрузки принять его или отказаться от установки. Принятые обновления устанавливаются, отклоненные — нет, но они остаются в системе, чтобы их можно было установить позже.
- **Локальный администратор может менять параметры (Allow Local Admin To Choose Setting)** Параметры автоматического обновления настраиваются на каждом компьютере в отдельности локальным администратором. При любом другом параметре у локальных пользователей

и администраторов нет права изменять параметры автоматического обновления.

Чтобы настроить автоматические обновления при помощи групповой политики, выполните следующие действия:

1. В GPMC щелкните правой кнопкой нужный GPO и выберите **Изменить (Edit)**.
2. В редакторе политики раскройте узел **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Центр обновления Windows (Computer Configuration\Administrative Templates\Windows Components\Windows Update)**.
3. Щелкните дважды политику **Настройка автоматического обновления (Configure Automatic Updates)**. Чтобы включить управление автоматическим обновлением при помощи групповой политики, установите переключатель **Включен (Enabled)**. Чтобы отключить его, установите переключатель **Выключен (Disabled)**, щелкните **OK** и пропустите остальные шаги.
4. Выберите нужный способ обновления в списке **Настройка автоматического обновления (Configure Automatic Update)**.
5. Если вы выбрали вариант **Автоматическая загрузка и установка по расписанию (Auto Download And Schedule The Install)**, здесь же задайте расписание. Щелкните **OK**, чтобы сохранить изменения.

Оптимизация автоматических обновлений

Как правило, большинство автоматических обновлений устанавливается при перезапуске компьютера. Некоторые обновления можно устанавливать немедленно, не прерывая работу системных служб и не требуя перезагрузки системы. Чтобы разрешить немедленную установку некоторых обновлений, выполните следующие действия:

1. В GPMC щелкните правой кнопкой нужный GPO и выберите **Изменить (Edit)**.
2. В редакторе политики раскройте узел **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Центр обновления Windows (Computer Configuration\Administrative Templates\Windows Components\Windows Update)**.
3. Щелкните дважды политику **Разрешить немедленную установку автоматических обновлений (Allow Automatic Updates Immediate Installation)**. В диалоговом окне свойств политики установите переключатель **Включен (Enabled)** и щелкните **OK**.

По умолчанию уведомления об обновлениях посылаются только пользователям с административными полномочиями. Чтобы рассылать их всем пользователям, зарегистрировавшимся на компьютере, выполните следующие действия:

1. В GPMC щелкните правой кнопкой нужный GPO и выберите **Изменить (Edit)**.
2. В редакторе политики раскройте узел **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Центр обновления Windows (Computer Configuration\Administrative Templates\Windows Components\Windows Update)**.
3. Щелкните дважды политику **Разрешать пользователям, не являющимся администраторами, получать уведомления об обновлениях (Allow Non-Administrators To Receive Update Notifications)**. В диалоговом окне свойств политики установите переключатель **Включен (Enabled)** и щелкните **OK**.

При настройке автоматических обновлений полезны также следующие политики:

- **Автоматическое обновление Windows (Windows Automatic Updates)** При каждом подключении пользователя к Интернету Windows производит поиск доступных обновлений. Чтобы отказаться от поиска, включите эту политику. Она расположена в узле **Конфигурация пользователя\Административные шаблоны\Система (User Configuration\Administrative Templates\System)**.
- **Отключить автоматическое обновление ADM-файлов (Turn Off Automatic Update Of ADM Files)** В процессе автоматического обновления может произойти изменение групповой политики. Как правило, это выражается в установке новых политики, доступ к которым открывается при очередном запуске редактора политик. Если вы не хотите, чтобы групповая политика обновлялась в процессе автоматического обновления, включите эту политику. Она расположена в узле **Конфигурация пользователя\Административные шаблоны\Система\Групповая политика (User Configuration\Administrative Templates\System\Group Policy)**. Параметры этой политики игнорируются, если вы включили политику **Всегда использовать локальные файлы ADM для редактора объектов групповой политики (Always Use Local ADM Files For The Group Policy Object Editor)**.
- **Запретить использование любых средств Центра обновления Windows (Remove Access To Use All Windows Update Features)** Закрывает доступ ко всем функциям системы обновления Windows. Если эта политика включена, все эти функции удаляются, и настроить их нельзя. В их число входят команды **Центр обновления Windows (Windows Update)** из меню **Пуск (Start)** и меню Internet Explorer **Сервис (Tools)**, а также функция обновления драйверов в Диспетчере устройств (Device Manager). Эта политика расположена в узле **Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Центр обновления Windows (User Configuration\Administrative Templates\Windows Components\Windows Update)**.

Обновление в интрасети

В сетях с сотнями и тысячами компьютеров автоматическое обновление может занимать существенную долю полосы пропускания, и, разумеется, нет никакого смысла проверять обновления и загружать их индивидуально на каждом компьютере. Помочь вам призвана политика **Указать размещение службы обновлений Майкрософт в интрасети (Specify Intranet Microsoft Update Service Location)**, которая указывает отдельным компьютерам проверять наличие обновлений на заданном внутреннем сервере.

К серверу обновлений предъявляются следующие требования: на нем должны быть запущены службы WSUS (Windows Server Update Services), он должен быть настроен как веб-сервер, работающий под управлением Microsoft Internet Information Services (IIS), и ему необходима мощность, достаточная для обработки дополнительной нагрузки, которая в больших сетях при пиковой загруженности может быть весьма значительной. Кроме того, серверу обновлений необходим доступ к внешней сети по порту 80. Проследите, чтобы ни брандмауэр, ни прокси-сервер не препятствовали работе по этому порту.

В процессе обновления отслеживается информация о конфигурации и статистике по каждому компьютеру. Эта информация необходима для нормального обновления. Она может храниться как на специальном сервере статистики (внутреннем IIS-сервере) , так и на самом сервере обновлений.

Чтобы настроить использование внутреннего сервера обновлений, выполните следующие действия:

1. Установив и настроив сервер обновлений, откройте для редактирования GPO, с которым будете работать. В редакторе политики раскройте узел **Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Центр обновления Windows (Computer Configuration\Administrative Templates\Windows Components\Windows Update)**.
2. Щелкните дважды политику **Указать размещение службы обновлений Майкрософт в интрасети (Specify Intranet Microsoft Update Service Location)**. В диалоговом окне свойств установите переключатель **Включен (Enabled)**.
3. Введите URL сервера обновлений в поле **Укажите службу обновлений в интрасети для поиска обновлений (Set The Intranet Update Service For Detecting Updates)**. В большинстве случаев URL имеет форму *http://имя_сервера*, например, *http://CorpUpdateServer01*, как показано на рис. 5-18.
4. Введите URL сервера статистики в поле **Укажите сервер статистики в интрасети (Set The Intranet Statistics Server)**. Здесь можно указать тот же самый адрес.

Примечание Если вы хотите, чтобы обновлениями и статистикой занимался один и тот же сервер, введите в оба поля один и тот же адрес. Если у вас имеется выделенный сервер статистики, введите его URL во второе поле.

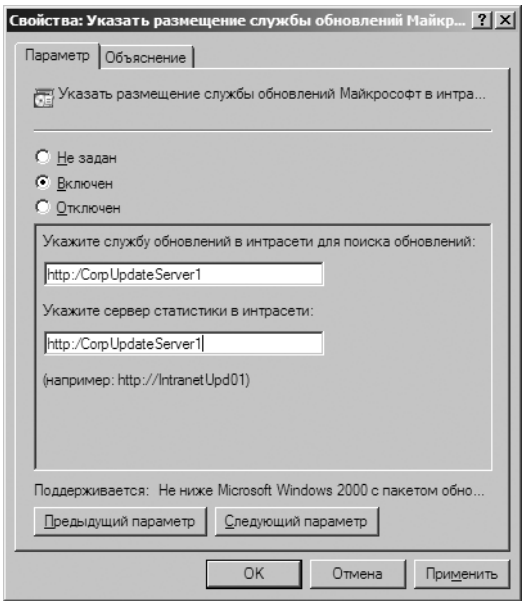


Рис. 5-18. Используйте внутренний сервер обновлений для централизации обновлений и сокращения трафика из внешней сети

5. Щелкните **OK**. После обновления соответствующего GPO системы, работающие под управлением ОС Windows 2000 Service Pack 3 или более поздней версии, Windows XP Service Pack 1 или более поздней версии, Windows Server 2003, Windows Vista и Windows Server 2008 будут в поисках обновлений связываться с внутренним сервером обновлений. Несколько первых дней или даже недель особенно внимательно следите за серверами обновлений и статистики, чтобы убедиться в их корректной работе.

Глава 6

Повышение безопасности компьютера

Решительные меры, направленные на обеспечение безопасности, — залог успешного системного администрирования. Есть два основных способа изменения параметров безопасности — шаблоны безопасности и политики безопасности. С помощью этих элементов задаются параметры системы, которыми вы иначе управляли бы при помощи групповой политики.

Шаблоны безопасности

Шаблоны безопасности (security template) позволяют централизованно управлять параметрами безопасности на рабочих станциях и серверах. Они используются для применения к отдельным компьютерам заданных наборов параметров групповой политики, связанных с безопасностью.

Эти наборы затрагивают, в основном, следующие политики:

- **Политики учетных записей** Безопасность паролей, блокировка учетных записей и Kerberos.
- **Локальные политики** Аудит, назначение прав пользователей и другие параметры безопасности.
- **Политики журнала событий** Безопасность журнала событий.
- **Политики групп с ограниченным доступом** Администрирование членства в локальных группах.
- **Политики системных служб** Безопасность и режим запуска локальных служб.
- **Политики файловой системы** Безопасность путей к файлам и папкам локальной файловой системы.
- **Политики реестра** Значения параметров реестра, связанных с безопасностью.

Примечание Шаблоны безопасности имеются во всех вариантах Windows Server 2008 и могут импортироваться в любую групповую политику. Шаблоны безопасности применимы только к разделу групповой политики **Конфигурация компьютера (Computer Configuration)** и не применимы к разделу **Конфигурация пользователя (User Configuration)**. Все изменяемые параметры находятся в узле **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности (Computer**

Configuration\Windows Settings\Security Settings). В шаблоны не включены некоторые параметры безопасности, относящиеся, например, к беспроводным сетям, параметрам открытого ключа, ограничениям программ и безопасности IP.

Приступая к работе с шаблонами безопасности, выясните, сможете ли вы воспользоваться в качестве отправной точки существующим шаблоном. Стандартные шаблоны находятся в папке %SystemRoot%\Security\Templates. Доступ к ним вы получите с помощью оснастки **Шаблоны безопасности (Security Templates)**, показанной на рис. 6-1.

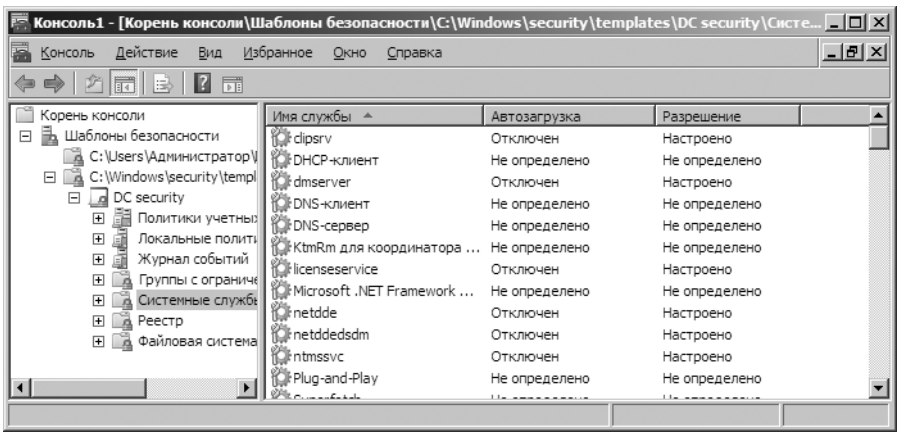


Рис. 6-1. Просмотр и создание шаблонов безопасности в оснастке **Шаблоны безопасности (Security Templates)**

Оснастка также позволяет создавать новые шаблоны. В ней доступны, в частности, следующие стандартные шаблоны:

- **dc security** Стандартные параметры безопасности для контроллеров домена.
- **setup security** Стандартные параметры безопасности для рядовых серверов.
- **securedc** Ограниченные параметры безопасности для контроллеров домена.
- **securews** Ограниченные параметры безопасности для рабочих станций.
- **hisecdc** Строжайшие параметры безопасности для контроллеров домена.
- **hisecws** Строжайшие параметры безопасности для рабочих станций.

Совет Выбрав шаблон, которым вы намереваетесь воспользоваться, просмотрите значения всех его параметров, чтобы оценить их влияние на вашу рабочую среду. Если конкретный параметр не имеет смысла, при необходимости его можно изменить или удалить.

Применить шаблоны в оснастке **Шаблоны безопасности (Security Templates)** нельзя. Для этого предназначена оснастка **Анализ и настройка безопасности (Security Configuration and Analysis)**. Она же позволяет провести сравнение параметров шаблона с параметрами, установленными в данный момент на компьютере. В результате анализа будут отмечены области, в которых текущие значения не совпадают со значениями параметров из шаблона. Это полезно, поскольку позволяет установить, например, изменились ли параметры безопасности после применения шаблона.

Использование шаблонов безопасности — многоступенчатый процесс, состоящий из следующих этапов:

1. При помощи оснастки **Шаблоны безопасности (Security Templates)** выберите шаблон и изучите его параметры.
2. При необходимости внесите изменения в шаблон.
3. При помощи оснастки **Анализ и настройка безопасности (Security Configuration and Analysis)** проанализируйте различия между параметрами безопасности выбранного шаблона и текущими параметрами компьютера.
4. Внесите в шаблон необходимые изменения.
5. При помощи оснастки **Анализ и настройка безопасности (Security Configuration And Analysis)** примените шаблон, заменив существующие параметры безопасности.

Работа с оснастками Шаблоны безопасности (Security Templates) и Анализ и настройка безопасности (Security Configuration and Analysis)

Чтобы открыть оснастки безопасности, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)**, введите **mmc** в поле **Начать поиск (Search)** и нажмите Enter.
2. В окне консоли выберите в меню **Консоль (File)** команду **Добавить или удалить оснастку (Add/Remove Snap-In)**.
3. В диалоговом окне **Добавление и удаление оснастки (Add Or Remove Snap-Ins)** выделите вариант **Шаблоны безопасности (Security Templates)** и щелкните кнопку **Добавить (Add)**.
4. Выделите вариант **Анализ и настройка безопасности (Security Configuration and Analysis)** и щелкните кнопку **Добавить (Add)**. Затем щелкните **OK**.

По умолчанию оснастка **Шаблоны безопасности (Security Templates)** извлекает шаблоны безопасности из папки %SystemDrive%\Users\%UserName%\Documents\Security\Templates. Чтобы добавить новые пути для поиска шаблонов, выполните следующие действия:

1. В оснастке **Шаблоны безопасности (Security Templates)** выберите в меню **Действие (Action)** команду **Новый путь для поиска шаблонов (New Template Search Path)**.

2. Укажите в диалоговом окне **Обзор папок (Browse For Folder)** новый путь к шаблонам, например, %SystemRoot%\Security\Templates. Щелкните **OK**.

Задав расположение папки с шаблонами, выберите нужный шаблон и переходите к его просмотру. Чтобы создать новый шаблон, выполните следующие действия:

1. В оснастке **Шаблоны безопасности (Security Templates)** щелкните правой кнопкой путь, где должен быть создан новый шаблон, и выберите в контекстном меню команду **Создать шаблон (New Template)**.
2. Введите имя и описание шаблона.
3. Щелкните **OK**, чтобы создать новый шаблон. Никакие параметры в нем не заданы, поэтому перед использованием шаблона вам придется поработать над этим.

Просмотр и изменение параметров шаблона

Управление различными видами параметров шаблона осуществляется поразному, как вы узнаете из следующих разделов.

Изменение параметров политик учетных записей, журнала событий и локальных политик

Параметры политики учетных записей отвечают за безопасность паролей, блокирование учетных данных пользователя и Kerberos. Конфигурация локальной политики обеспечивает безопасность аудита, назначение прав пользователям и другие параметры безопасности. Наконец, параметры политики журнала событий отвечают за безопасность журнала событий. Подробную информацию о параметрах политик учетных записей и локальных политик вы найдете в главе 10, а информация о журналах событий содержится в главе 4.

Чтобы изменить параметры шаблона, относящиеся к перечисленным политикам, выполните следующие действия:

1. В оснастке **Шаблоны безопасности (Security Templates)** разверните узел **Политики учетных записей (Account Policies)** или **Локальные политики (Local Policies)**. Затем выберите нужный подузел, например, **Политика паролей (Password Policy)** или **Политика блокировки учетной записи (Account Lockout Policy)**.
2. В правой панели перечислены параметры политики в алфавитном порядке. Значение в столбце **Параметр компьютера (Computer Setting)** отображает текущее значение параметра.
3. Щелкните параметр дважды, чтобы отобразить диалоговое окно его свойств, как показано на рис. 6-2. Чтобы разобраться в назначении параметра, перейдите на вкладку **Объяснение (Explain)**. Чтобы определить и применить параметр политики, установите флажок **Определить следующий параметр политики в шаблоне (Define This Policy Setting In The Template)**. Чтобы не применять данную политику, сбросьте этот флажок.

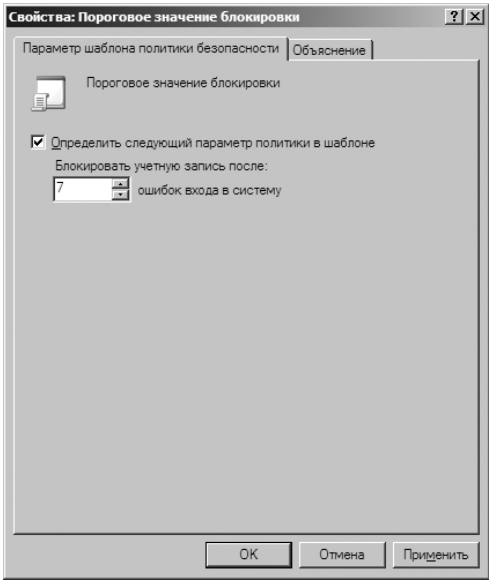


Рис. 6-2. Изменение параметров шаблона для политики блокировки учетных записей

4. Включив политику, уточните способ ее применения, настроив дополнительные параметры.
5. Щелкните **ОК**. После этого может открыться диалоговое окно **Предлагаемые изменения значений (Suggested Value Changes)** с информацией о других параметрах, значения которых будут изменены в соответствии с внесенным вами изменением. Например, при изменении параметра **Пороговое значение блокировки (Account Lockout Threshold)** Windows может также изменить параметры **Время до сброса счетчика блокировки (Reset Account Lockout Counter After)** и **Продолжительность блокировки учетной записи (Account Lockout Duration)**, как показано на рис. 6-3.

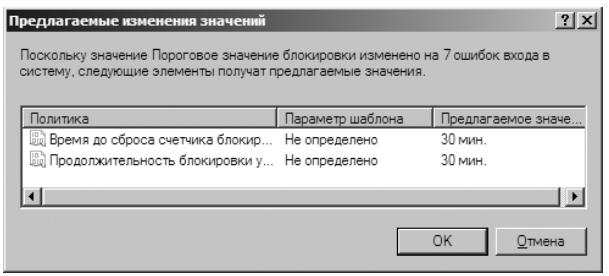


Рис. 6-3. Предлагаемые изменения параметров

Настройка групп с ограниченным доступом

Параметрами политики Группы с ограниченным доступом (Restricted Groups) определяется список членов группы, а также группы, в которые

она входит. Чтобы ограничить возможности группы, выполните следующие действия:

1. В оснастке **Шаблоны безопасности (Security Templates)** выберите узел **Группы с ограниченным доступом (Restricted Groups)**. Все настроенные в данный момент ограниченные группы будут перечислены в правой панели. Также указаны члены группы и группы, членом которых является выбранная группа.
2. Чтобы добавить группу с ограниченным доступом, щелкните правой кнопкой узел **Группы с ограниченным доступом (Restricted Groups)** в левой панели и выберите команду **Добавить группу (Add Group)**. В диалоговом окне **Добавление группы (Add Group)** щелкните кнопку **Обзор (Browse)**.
3. В диалоговом окне **Выбор: «Группы» (Select Groups)** введите имя группы, возможности которой хотите ограничить, и щелкните кнопку **Проверить имена (Check Names)**. Если найдено несколько совпадений, выберите нужную учетную запись и щелкните **ОК**. Если совпадений не найдено, исправьте введенное имя и выполните поиск еще раз.
4. Кнопка **Добавить членов группы (Add Members)** в диалоговом окне свойств группы служит для добавления в нее пользователей. Щелкните эту кнопку и укажите членов группы. Если в группе не должно быть ни одного члена, удалите из нее всех пользователей при помощи кнопки **Удалить (Remove)**. Члены ограниченной группы, не указанные в параметре политики, удаляются при применении шаблона безопасности.
5. Щелкните кнопку **Добавить группы (Add Groups)** в диалоговом окне свойств, чтобы указать группы, к которым принадлежит данная группа. При задании членства группы, к которым принадлежит данная группа, перечисляются в порядке их применения (при условии, что такие группы есть в соответствующей рабочей группе или домене). Если вы не указали членство, группы, к которым относится данная группа, после применения шаблона не изменяются.
6. Щелкните **ОК**, чтобы сохранить изменения.

Чтобы снять с группы ограничение, выполните следующие действия:

1. В оснастке **Шаблоны безопасности (Security Templates)** выберите узел **Группы с ограниченным доступом (Restricted Groups)**. Имена всех ограниченных в данный момент групп отображены в списке в правой панели. Наряду с группами, к которым принадлежит данная группа, перечислены и члены этой группы.
2. Щелкните правой кнопкой группу, с которой собираетесь снять ограничение, и выберите команду **Удалить (Delete)**. Подтвердите удаление, щелкнув **Да (Yes)**.

Запуск, остановка и настройка системных служб

Параметры политики системных служб отвечают за общую безопасность и режим запуска локальных служб. Чтобы запустить, остановить или настроить системную службу, выполните следующие действия:

1. В узле **Системные службы (System Services)** собраны все службы, установленные в данный момент на компьютере. В списке указаны имя, способ запуска и информация о разрешениях. Работая с системными службами, следует помнить о следующем:
   - Если шаблон не изменяет конфигурацию запуска службы, в столбце **Автозагрузка (Startup)** стоит значение **Не определено (Not Defined)**. Иначе способ запуска описывается одним из следующих значений: **Автоматический (Automatic)**, **Вручную (Manual)** или **Запрещен (Disabled)**.
   - Если шаблон не изменяет конфигурацию безопасности службы, в столбце **Разрешение (Permission)** стоит значение **Не определено (Not Defined)**. Иначе конфигурация безопасности определена значением **Настроено (Configured)**.
2. Щелкните дважды системную службу, чтобы открыть диалоговое окно ее свойств, показанное на рис. 6-4. Чтобы определить и применить параметр политики, установите флажок **Определить следующий параметр политики в шаблоне (Define This Policy Setting In The Template)**. Чтобы не применять политику, сбросьте этот флажок.

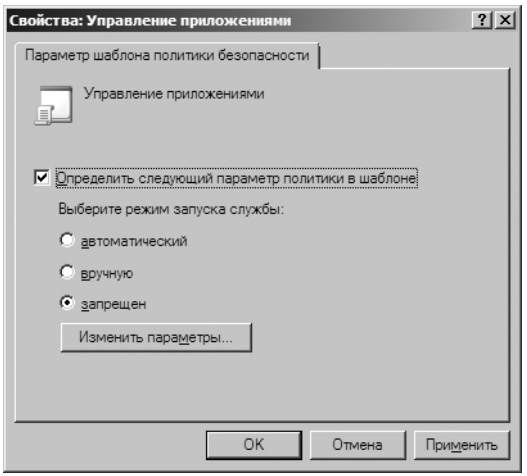


Рис. 6-4. Изменение параметров системных служб шаблона

3. Задайте способ запуска службы, установив переключатель **Автоматический (Automatic)**, **Вручную (Manual)** или **Запрещен (Disabled)**. При этом помните о следующем:
   - Автоматический запуск службы производится при запуске операционной системы. Такой режим следует устанавливать для основных

служб, в чьей надежности вы не сомневаетесь. Эти службы должны в обязательном порядке запускаться на компьютере, к которому применен шаблон.

- Ручной запуск означает, что автоматически служба запускать не будет. Выбирайте этот способ для ненужных или неиспользуемых служб, а также служб, в безопасности которых вы не уверены.
- Запрет запуска службы относится как к автоматическому, так и к ручному режиму. Задавайте этот параметр только для ненужных или неиспользуемых служб.

4. Если вам известна конфигурация безопасности, которую должна использовать служба, щелкните **Изменить параметры (Edit Security)** и задайте разрешения для службы в диалоговом окне **Безопасность для (Security For)**. Здесь вы можете разрешить отдельным пользователям и группам запускать, останавливать и приостанавливать службы на компьютере.
5. Щелкните **ОК**.

Настройка параметров безопасности для реестра и путей файловой системы

Параметры политики файловой системы отвечают за безопасность путей к локальным файлам и папкам. Параметры политики реестра определяют значения параметров реестра, связанных с безопасностью. Чтобы просматривать и изменять параметры безопасности реестра и путей файловой системы, выполните следующие действия:

1. В оснастке **Шаблоны безопасности (Security Templates)** выберите узел **Реестр (Registry)** или **Файловая система (File System)**. В правой панели перечислены все защищенные в данный момент пути.
2. Щелкните дважды раздел реестра или путь к файлу, чтобы просмотреть его текущие параметры (рис. 6-5).
3. Чтобы гарантировать неизменность разрешений раздела или пути, выберите **Запретить замену разрешений в этом разделе (Do Not Allow Permissions On This Key To Be Replaced)** и щелкните **ОК**. Пропустите остальные шаги.
4. Чтобы настроить путь или раздел с заменой разрешений, установите переключатель **Настроить этот раздел (Configure This Key Then)**. Далее выберите один из следующих вариантов:
   - **Распространить наследуемые разрешения на все подразделы (Propagate Inheritable Permissions To All)** Выберите этот вариант, чтобы применить все наследуемые разрешения к данному разделу или пути, а также ко всем вложенным в него разделам или путям. Существующие разрешения заменяются только в том случае, если они вступают в конфликт с набором разрешений безопасности для данного пути.
   - **Заменить текущие разрешения во всех подразделах наследуемыми (Replace Existing Permissions On All … With Inheritable Permissions)** Выберите этот вариант, чтобы заменить все существующие

разрешения для данного раздела реестра или пути, а также для всех вложенных в него разделов или путей. Все существующие разрешения удаляются, и остаются только текущие разрешения.

5. Щелкните **Изменить параметры (Edit Security)**. В диалоговом окне **Безопасность для (Security For)** настройте нужные разрешения для пользователей и групп. В вашем распоряжении те же разрешения, что и для файлов и папок NTFS. Подробнее о них — в главе 15.
6. Щелкните **ОК** дважды, чтобы сохранить параметры.

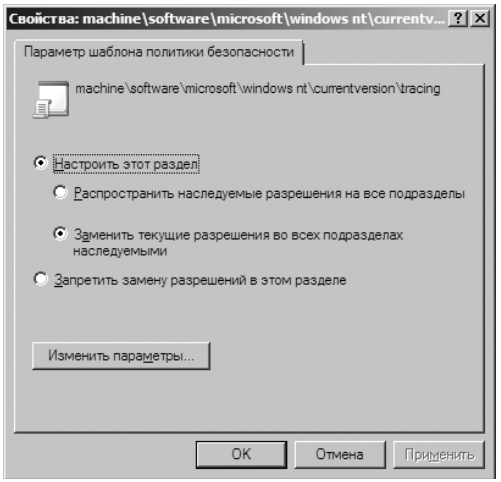


Рис. 6-5. Изменение параметров шаблона для путей и разделов реестра

Чтобы задать параметры безопасности для разделов реестра, выполните следующие действия:

1. В оснастке **Шаблоны безопасности (Security Templates)** выделите узел **Реестр (Registry)**, щелкните его правой кнопкой мыши и выберите команду **Добавить раздел (Add Key)**. Откроется диалоговое окно **Выбор раздела реестра (Select Registry Key)**, показанное на рис. 6-6.
2. Выберите нужный раздел или параметр, с которыми хотите работать, и щелкните **ОК**. Узел **CLASSES_ROOT** соответствует разделу HKEY_CLASSES_ROOT и т. п.
3. В диалоговом окне **Безопасность базы данных для (Database Security For)** определите разрешения для пользователей и групп. В вашем распоряжении те же разрешения, что и для файлов и папок NTFS. Подробнее о них — в главе 15.
4. Щелкните **ОК**. На экране появится диалоговое окно **Добавление объекта (Add Object)**. Чтобы исключить замену разрешений для этого раздела, установите переключатель **Запретить замену разрешений в этом разделе (Do Not Allow Permissions On This Key To Be Replaced)** и щелкните **ОК**. Пропустите остальные шаги.

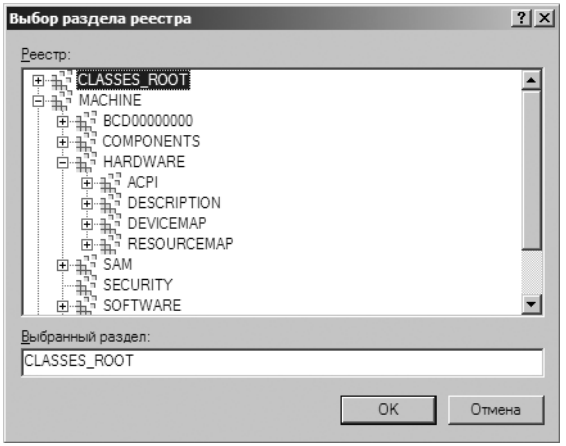


Рис. 6-6. Выберите раздел или параметр реестра, которые предполагается защитить

4. Чтобы настроить путь или раздел с заменой разрешений, установите переключатель **Настроить этот раздел (Configure This Key Then)**. Далее выберите один из следующих вариантов:
   - **Распространить наследуемые разрешения на все подразделы (Propagate Inheritable Permissions To All)** Выберите этот вариант, чтобы применить все наследуемые разрешения к данному разделу, а также ко всем вложенным в него разделам. Существующие разрешения заменяются только в том случае, если они вступают в конфликт с набором разрешений безопасности для данного раздела.
   - **Заменить текущие разрешения во всех подразделах наследуемыми (Replace Existing Permissions On All ... With Inheritable Permissions)** Выберите этот вариант, чтобы заменить все существующие разрешения для данного раздела, а также для всех вложенных в него разделов. Все существующие разрешения удаляются, и остаются только текущие разрешения.
5. Щелкните **ОК**.

Чтобы задать параметры безопасности для путей к файлам, выполните следующие действия:

1. В оснастке **Шаблоны безопасности (Security Templates)** щелкните правой кнопкой узел **Файловая система (File System)** и выберите команду **Добавить файл (Add File)**. Откроется диалоговое окно **Добавление файла или папки (Add A File Or Folder)**, показанное на рис. 6-7.
2. Укажите путь к файлу или папке и щелкните **ОК**.
3. В диалоговом окне **Безопасность базы данных для (Database Security For)** задайте разрешения для пользователей и групп. В вашем распоряжении те же разрешения, что и для файлов и папок NTFS. Подробнее о них — в главе 15.

4. Щелкните **ОК**. На экране появится диалоговое окно **Добавление объекта (Add Object)**. Чтобы исключить замену разрешений для этого пути, выберите **Запретить замену разрешения для этого файла или папки (Do Not Allow Permissions On This Key To Be Replaced)** и щелкните **ОК**. Пропустите остальные шаги.

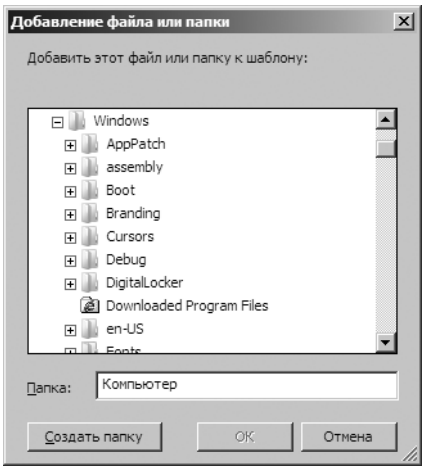


Рис. 6-7. Задайте путь к файлу или папке, которые предполагается защитить

5. Чтобы настроить путь и изменения разрешений, выберите **Настроить разрешения для этого файла или папки, а затем (Configure This Key Then)**. Далее выберите один из следующих вариантов:
   - **Распространить наследуемые разрешения на все файлы и папки (Propagate Inheritable Permissions To All)** Выберите этот вариант, чтобы применить все наследуемые разрешения к данному пути, а также ко всем вложенным в него путям. Существующие разрешения заменяются только в том случае, если они вступают в конфликт с набором разрешений безопасности для данного раздела.
   - **Заменить существующие разрешения для всех подпапок и файлов на наследуемые разрешения (Replace Existing Permissions On All … With Inheritable Permissions)** Выберите этот вариант, чтобы заменить все существующие разрешения для данного пути, а также для всех вложенных в него путей. Все существующие разрешения удаляются, и остаются только текущие разрешения.
6. Щелкните **ОК**.

Анализ, просмотр и применение шаблонов безопасности

Как уже говорилось, оснастка **Анализ и настройка безопасности (Security Configuration and Analysis)** используется для применения шаблонов, а также для сравнения параметров шаблона с текущими параметрами компьютера. Применение шаблона гарантирует приведение компьютера в соответст-

вие с определенной конфигурацией безопасности. Сравнение параметров помогает найти любые несоответствия между текущей настройкой компьютера и настройкой, определенной в шаблоне безопасности. Оно также помогает выявить изменения, внесенные в параметры безопасности после применения шаблона.

Ближе к реальности Основное неудобство оснастки **Анализ и настройка безопасности (Security Configuration and Analysis)** состоит в том, что она не позволяет настроить несколько компьютеров одновременно. Разрешается конфигурировать безопасность только того компьютера, на котором запущена оснастка. Поэтому, если вы захотите с помощью этого инструмента развернуть конфигурации безопасности, вам придется работать на каждом компьютере по отдельности. Эта методика приемлема для изолированных компьютеров, но в домене ее нельзя признать оптимальной. В домене следует импортировать параметры шаблона безопасности в GPO и уже с его помощью развернуть параметры безопасности на нескольких компьютеров. Подробнее — в следующем разделе.

Оснастка **Анализ и настройка безопасности (Security Configuration and Analysis)** использует рабочую базу данных для хранения параметров безопасности шаблона, после чего применяет параметры из этой базы данных. При анализе и сравнении параметров безопасности параметры из шаблона представлены как фактические параметры базы данных, а текущие параметры — как фактические параметры компьютера.

Чтобы произвести настройку и анализ нового или существующего шаблона, выполните следующие действия:

1. Откройте оснастку **Анализ и настройка безопасности (Security Configuration and Analysis)**.
2. Щелкните правой кнопкой узел **Анализ и настройка безопасности (Security Configuration and Analysis)** и выберите команду **Открыть базу данных (Open Database)**. Откроется одноименное диалоговое окно.
3. По умолчанию в этом окне открыта папка %SystemDrive%\Users\%UserName%\Documents\Security\Database. При необходимости перейдите в другое расположение. Ввведите в поле **Имя файла (File Name)** имя базы данных, например, **Current Config Comparison**, и щелкните кнопку **Открыть (Open)**. Будет создана база данных безопасности в формате **Файлы базы данных безопасности (Security Database Files)** с расширением .sdb.
4. В диалоговом окне **Импорт шаблона (Import Template)** отображается стандартный маршрут поиска %SystemDrive%\Users\%UserName%\Documents\Security\Templates. При необходимости перейдите в другое расположение. Выберите шаблон безопасности, которым хотите воспользоваться, и щелкните **Открыть (Open)**. Файлы шаблонов безопасности имеют расширение .inf.
5. Щелкните правой кнопкой узел **Анализ и настройка безопасности (Security Configuration and Analysis)** и выберите команду **Анализ компьютера (Analyze Computer Now)**. Введите путь для сохранения журнала ошибок или сразу щелкните **OK**, чтобы использовать стандартный путь.

6. Дождитесь завершения анализа шаблона. Если во время анализа произойдет ошибка, просмотрите журнал ошибок, щелкнув правой кнопкой узел **Анализ и настройка безопасности (Security Configuration and Analysis)** и выбрав команду **Показать файл журнала (View Log File)**.

В оснастке **Анализ и настройка безопасности (Security Configuration and Analysis)** вы можете просматривать различия между параметрами шаблона и текущими параметрами компьютера. Как показано на рис. 6-8, параметры шаблона, сохраненные в базе данных анализа, указаны в столбце **Параметр базы данных (Database Setting)**. Текущие параметры компьютера указаны в столбце **Параметр компьютера (Computer Setting)**. Если параметр не анализировался, у него стоит значение **Не анализировано (Not Analyzed)**.

Чтобы внести изменения в параметры базы данных, выполните следующие действия:

1. В оснастке **Анализ и настройка безопасности (Security Configuration and Analysis)** дважды щелкните параметр, с которым хотите работать.
2. В диалоговом окне свойств, показанном на рис. 6-9, текущее значение параметра приведено в поле **Параметр компьютера (Computer Setting)**. При необходимости прочитайте о назначении параметра на вкладке **Объяснение (Explain)**.
3. Чтобы задать и применить параметр политики, установите флажок **Определить следующую политику в базе данных (Define This Policy Setting In The Database)**. Чтобы не применять политику, сбросьте этот флажок.
4. Задайте способ использования политики, настроив дополнительные параметры.
5. При необходимости измените другие политики. Чтобы сохранить изменения базы данных, щелкните правой кнопкой узел **Анализ и настройка безопасности (Security Configuration and Analysis)** и выберите команду **Сохранить (Save)**.

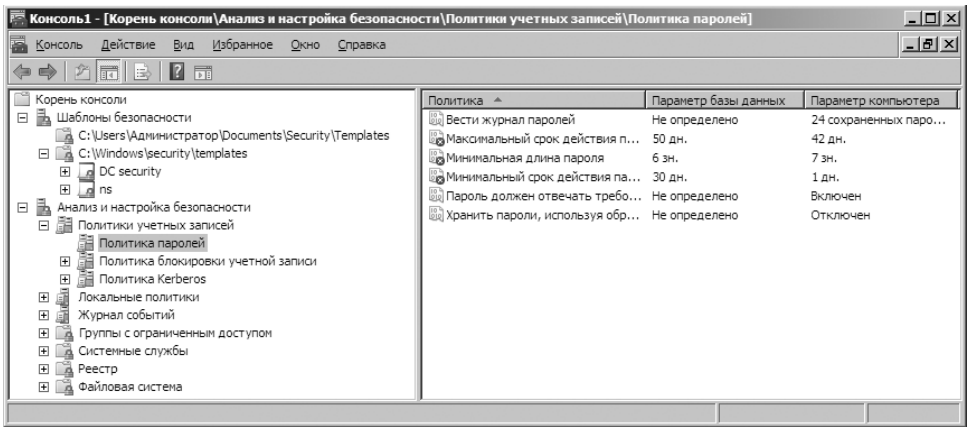


Рис. 6-8. Просмотр различий между параметрами шаблона и текущими параметрами компьютера

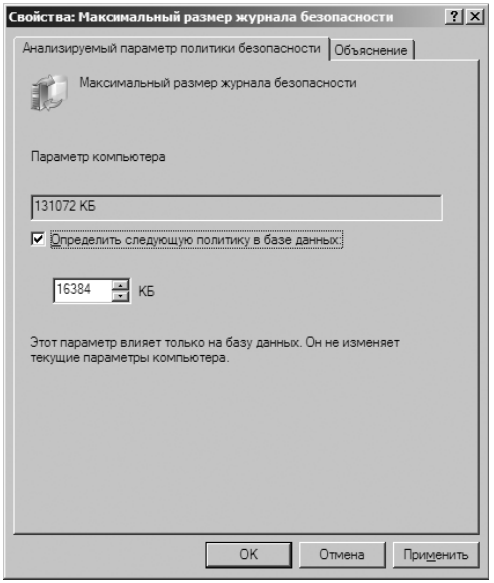


Рис. 6-9. Изменение параметра политики в базе данных перед применением шаблона

Перед применением шаблона имеется смысл создать шаблон для отката, позволяющий удалить большинство параметров, примененных в составе шаблона. Восстановить не удастся только параметры, затрагивающие списки управления доступом к путям файловой системы и реестра.

Шаблон для отката создается при помощи утилиты командной строки Secedit. Введите команду:

```
secedit /generaterollback /cfg Шаблон /rbk ШаблонОтката /log Журнал
```

где *Шаблон* — имя шаблона безопасности, для которого создается шаблон отката, *ШаблонОтката* — имя шаблона безопасности, в котором будут сохранены восстанавливаемые параметры, *Журнал* — имя необязательного системного журнала.

В следующем примере мы создадим шаблон отката для шаблона dc security:

```
secedit /generaterollback /cfg "dc security.inf" /rbk dc-orig.inf /log
rollback.log
```

Подготовившись к применению шаблона, щелкните правой кнопкой узел **Анализ и настройка безопасности (Security Configuration and Analysis)** и выберите команду **Настроить компьютер (Configure Computer Now)**. Задайте путь к файлу журнала ошибок или сразу щелкните **ОК**, чтобы принять стандартный путь. Чтобы просмотреть журнал ошибок, щелкните правой кнопкой узел **Анализ и настройка безопасности (Security Configuration and Analysis)** и выберите команду **Показать файл журнала (View Log File)**. Изучите возникшие проблемы и при необходимости примите меры.

Если перед применением шаблона безопасности вы создали шаблон отката, вы можете восстановить прежние значения параметров безопасности компьютера. Чтобы применить шаблон отката, выполните следующие действия:

1. В оснастке **Анализ и настройка безопасности (Security Configuration and Analysis)** щелкните правой кнопкой мыши узел **Анализ и настройка безопасности (Security Configuration and Analysis)** и выберите команду **Импорт шаблона (Import Template)**.
2. В диалоговом окне **Импорт шаблона (Import Template)** выберите шаблон отката.
3. Установите флажок **Очистить эту базу данных перед импортом (Clear This Database Before Importing)** и щелкните кнопку **Открыть (Open)**.
4. Щелкните правой кнопкой узел **Анализ и настройка безопасности (Security Configuration and Analysis)** и выберите команду **Настроить компьютер (Configure Computer Now)**. Щелкните **ОК**.

Восстановить не удастся только параметры, затрагивающие списки управления доступом к путям файловой системы и реестра. Отменять внесенные изменения придется вручную.

Развертывание шаблонов безопасности на нескольких компьютерах

Чтобы не применять шаблоны безопасности на каждом компьютере по отдельности, можно посредством групповой политики развернуть их на нескольких компьютеров. Для этого необходимо импортировать шаблон безопасности в объект групповой политики (GPO), обрабатываемый компьютерами, к которым должен быть применен шаблон. После обновления политики все компьютеры, находящиеся в сфере действия GPO, получат требуемые параметры безопасности.

Шаблоны безопасности применимы только к узлу групповой политики **Конфигурация компьютера (Computer Configuration)**. Прежде чем развернуть параметры безопасности, обратите особое внимание на структуру доменов и подразделений организации. При необходимости внесите изменения, гарантирующие применение параметров безопасности только к нужным компьютерам. По сути, это означает, что вам потребуется создать подразделения для различных типов компьютеров организации, а затем переместить в них учетные записи этих компьютеров. Затем вы создадите GPO и свяжете его с нужными подразделениями. Типичный набор подразделений выглядит примерно так:

- **Контроллеры домена** Подразделение для контроллеров домена; создается в домене автоматически.
- **Защищенные рядовые серверы** Подразделение для серверов, требующих уровня безопасности выше обычного.
- **Рядовые серверы** Подразделение для серверов с обычными параметрами безопасности.

- **Защищенные рабочие станции** Подразделение для рабочих станций, требующих уровня безопасности выше обычного.
- **Рабочие станции** Подразделение для рабочих станций с обычными параметрами безопасности.
- **Компьютеры удаленного доступа** Подразделение для компьютеров, пользующихся удаленным доступом к сети организации.
- **Компьютеры с ограниченным доступом** Подразделение для компьютеров, требующих ограничений по параметрам безопасности, например, для компьютеров в учебных аудиториях или лабораториях.

Ближе к реальности Развертывание шаблонов безопасности посредством GPO следует проводить с крайней осторожностью. Если вам не приходилось делать этого раньше, для начала потренируйтесь в тестовой среде. Также отработайте навыки восстановления на компьютерах первоначальных параметров безопасности. Если вы создали новый GPO и связали его с определенным уровнем структуры Active Directory, вы вернете компьютеры в исходной состояние, удалив связь GPO. Поэтому предпочтительно создать и связать новый GPO вместо использования существующего.

Чтобы развернуть шаблон безопасности в GPO компьютера, выполните следующие действия:

1. Настройте и протестируйте шаблон безопасности. Убедившись, что он вам подходит, откройте специально созданный GPO, связанный с определенным уровнем структуры Active Directory. В редакторе политики откройте узел **Конфигурация компьютера\Конфигурация Windows\ Параметры безопасности (Computer Configuration\Windows Settings\ Security Settings)**.
2. Щелкните правой кнопкой узел **Параметры безопасности (Security Settings)** и выберите в контекстном меню команду **Импорт политики (Import Policy)**.
3. В диалоговом окне **Импорт политики из (Import Policy From)** выберите шаблон безопасности и щелкните **Открыть (Open)**.
4. Убедившись, что импорт параметров прошел без неожиданностей, и проверив настройку параметров безопасности, закройте редактор политики. Повторите этот процесс для каждого шаблона безопасности и настроенного GPO компьютера. При стандартной конфигурации групповой политики передача параметров безопасности компьютерам организации произойдет в течение полутора-двух часов.

Мастер настройки безопасности

С помощью Мастера настройки безопасности (Security Configuration Wizard) вы легко создадите и примените исчерпывающую политику безопасности. Политика безопасности представляет собой файл с расширением .xml, который можно использовать для настройки служб, защиты сети, значений реестра и политики аудита. Поскольку политики безопасности основаны

на ролях и компонентах, в большинстве случаев вам придется создавать индивидуальную политику для каждой из стандартных серверных конфигураций. Например, если ваша организация использует контроллеры домена, файловые серверы и серверы печати, вам, вероятно, потребуется создать индивидуальную политику для каждого из этих типов. То же самое относится к почтовым серверам, серверам баз данных и пр.

Мастер настройки безопасности (Security Configuration Wizard) позволяет сделать следующее:

- создать новую политику безопасности;
- редактировать существующую политику безопасности;
- применить существующую политику безопасности;
- отменить последнюю примененную политику безопасности.

Политики безопасности могут включать в себя один или несколько шаблонов безопасности. С помощью групповой политики можно применить политику безопасности на нескольких компьютерах.

Создание политик безопасности

Мастер настройки безопасности (Security Configuration Wizard) позволяет настроить политику только для ролей и компонентов, установленных на компьютере во время запуска мастера. Конкретный процесс создания политики безопасности зависит от текущего набора ролей и компонентов. Впрочем, основные области настройки одинаковы для любой конфигурации компьютера.

В Мастере настройки безопасности (Security Configuration Wizard) имеются следующие разделы настройки безопасности:

- **Настройка служб на основе ролей (Role-Based Service Configuration)** Настройка режима запуска системных служб в зависимости от установленных ролей и компонентов сервера, заданных параметров и необходимых служб.
- **Сетевая безопасность (Network Security)** Настройка входящих и исходящих правил безопасности брандмауэра Windows в зависимости от установленных ролей и компонентов сервера.
- **Параметры реестра (Registry Settings)** Настройка протоколов для обмена данными с другими компьютерами.
- **Политика аудита (Audit Policy)** Настройка аудита на выбранном сервере.
- **Сохранение политики безопасности (Save Security Policy)** Сохранение и просмотр политики безопасности. В нее также можно включить один или несколько шаблонов безопасности.

Чтобы создать политику безопасности, выполните следующие действия:

1. Запустите Мастер настройки безопасности (Security Configuration Wizard). Для этого щелкните кнопку **Пуск (Start)**, **Администрирование**

(Administrative Tools) и **Мастер настройки безопасности (Security Configuration Wizard)**. На первой странице мастера щелкните **Далее (Next)**.

2. На странице **Действие настройки (Configuration Action)** просмотрите доступные действия (рис. 6-10). По умолчанию установлен переключатель **Создать новую политику безопасности (Create A New Security Policy)**. Щелкните **Далее (Next)**.

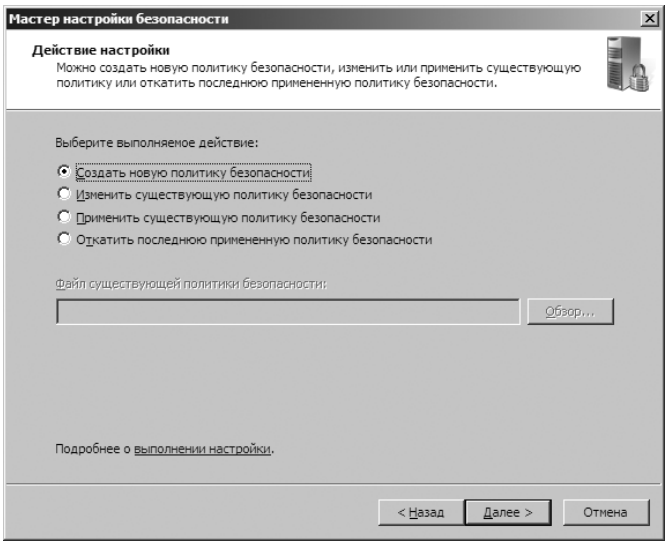


Рис. 6-10. Действия, которые можно выполнить при помощи мастера

3. На странице **Выбор сервера (Select Server)** укажите сервер, который должен использоваться в качестве базового для данной политики безопасности, то есть, сервер, на котором установлены нужные роли, компоненты и функции. По умолчанию выбран текущий компьютер. Чтобы выбрать другой компьютер, щелкните кнопку **Обзор (Browse)**. В диалоговом окне **Выбор: «Компьютер» (Select Computer)** введите имя компьютера и щелкните **Проверить имена (Check Names)**. Выделите нужную учетную запись компьютера и щелкните **ОК**.
4. Щелкните **Далее (Next)**. Мастер соберет конфигурацию безопасности и сохранит ее в базе данных настройки безопасности. Щелкните кнопку **Просмотр базы данных (View Configuration Database)** на странице **Обработка базы данных настройки безопасности (Processing Security Configuration Database)**, чтобы просмотреть параметры в базе данных. Просмотрев параметры, вернитесь в мастер и щелкните **Далее (Next)**.
5. Каждый раздел настройки начинается собственной заглавной страницей. Первая страница, которую вы увидите, — **Настройка служб на основе ролей (Role-Based Service Configuration)**. Щелкните **Далее (Next)**.

6. На странице **Выбор ролей сервера (Select Server Roles)**, показанной на рис. 6-11, показаны установленные роли сервера. Выберите роли, которые следует включить, и сбросьте роли, которые следует отключить. При выборе роли запускаются службы, входящие порты и параметры, требующиеся для этой роли. При сбросе роли соответствующие службы, входящие порты и параметры отключаются, при условии что они не требуются другой включенной роли.

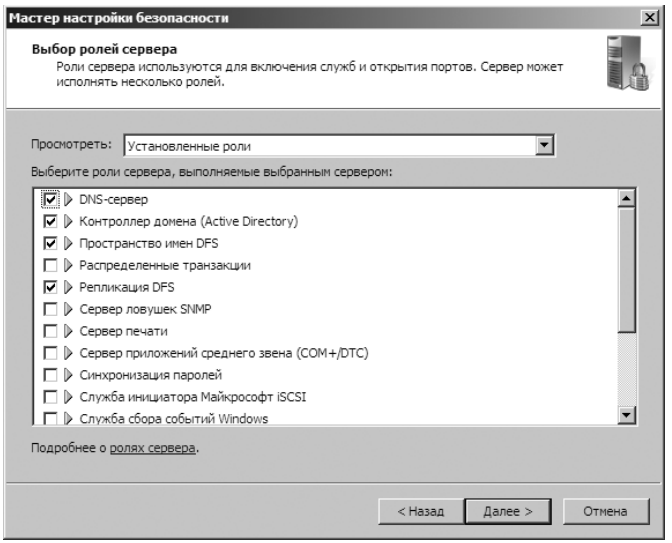


Рис. 6-11. Выберите роли сервера

7. На странице **Выбор клиентских возможностей (Select Client Features)** перечислены установленные клиентские компоненты, используемые для запуска служб. Выберите компоненты, которые нужно включить, и сбросьте компоненты, которые нужно отключить. При выборе компонента запускаются требующиеся ему службы. При отключении компонента требующиеся ему службы отключаются, при условии что они не требуются другому включенному компоненту.
8. На странице **Выбор управления и других параметров (Select Administration And Other Options)** перечислены установленные функции, используемые для запуска служб и открытия портов. Выберите функции, которые нужно включить, и сбросьте функции, которые нужно отключить. При выборе функции запускаются службы, требующиеся этой функции. При сбросе функции требующиеся ей службы отключаются, при условии что они не требуются другой включенной функции.
9. На странице **Выбор дополнительных служб (Select Additional Services)** показан список дополнительных служб, найденных на сервере во время обработки базы данных настройки безопасности. Выберите все службы, которые следует включить, и сбросьте все службы, которые нужно отключить.

10. На странице **Обработка неопределенных служб (Handling Unspecified Services)** определите, как следует обрабатывать неопределенные службы, то есть, службы, не установленные на выбранном сервере и не отраженные в базе данных настройки безопасности. По умолчанию режим запуска неопределенных служб не изменяется. Чтобы отключить неопределенные службы, установите переключатель **Отключить эту службу (Disable The Service)**. Щелкните **Далее (Next)**.
11. На странице **Подтверждение изменений для служб (Confirm Service Changes)** просмотрите список служб, которые будут изменены на выбранном сервере при применении политики безопасности. Обратите внимание на текущий режим запуска и режим запуска, заданный в политике.
12. На заглавной странице раздела **Сетевая безопасности (Network Security)** щелкните **Далее (Next)**. На странице **Правила сетевой безопасности (Network Security Rules)** отображен список правил брандмауэра, требуемых для ролей, компонентов и функций, выбранных вами ранее. Используя имеющиеся параметры, вы можете добавлять, изменять или удалять входящие и исходящие правила. Закончив настройку, щелкните **Далее (Next)**.
13. На заглавной странице раздела **Параметры реестра (Registry Settings)** щелкните **Далее (Next)**. На странице **Требовать цифровую подпись SMB (Require SMB Security Signatures)** просмотрите параметры подписей SMB. По умолчанию задано, что все компьютеры отвечают минимальным требованиям к ОС и сервер в состоянии обеспечить подписи трафика и печати. Изменять эти параметры не следует. Щелкните **ОК**.
14. На странице **Исходящие требования проверки подлинности (Outbound Authentication Methods)** задайте методы, используемые выбранным сервером для авторизации на удаленных компьютерах. Если компьютер обменивается данными только внутри домена, установите только флажок **Учетные записи в домене (Domain Accounts)**. Этим вы обеспечите наивысший уровень проверки подлинности. Если компьютер обменивается данными с компьютерами как в домене, так и в рабочей группе, установите флажки **Учетные записи в домене (Domain Accounts)** и **Локальные учетные записи на удаленных компьютерах (Local Accounts On The Remote Computers)**. В большинстве случаев не следует использовать пароли общего доступа, поскольку это наинизший уровень проверки подлинности. Щелкните **Далее (Next)**.
15. На странице **Исходящая проверка подлинности с использованием учетных записей домена (Outbound Authentication Using Domain Accounts)** задайте типы компьютеров, подключения которых будет принимать выбранный сервер. Если компьютер обменивается данными только с компьютерами под управлением Windows XP Professional или боле поздних версий Windows, сбросьте оба флажка, и ваш компьютер будет использовать наивысший уровень проверки подлинности. Если компьютер обме-

нивается данными с более старыми ПК, оставьте заданные по умолчанию параметры без изменения. Щелкните **Далее (Next)**.

16. На странице **Сводка параметров реестра (Registry Settings Summary)** просмотрите значения, которые будут изменены на выбранном сервере в случае применения политики. Сравните текущие значения и значения, заданные в политике. Щелкните **Далее (Next)**.
17. На заглавной странице **Политика аудита (Audit Policy)** щелкните **Далее (Next)**. На странице **Политика аудита системы (System Audit Policy)** задайте нужный уровень аудита. Для отключения аудита установите переключатель **Не выполнять аудит** (**Do Not Audit**). Чтобы включить аудит успешных событий, щелкните **Выполнять аудит успешных действий (Audit Successful Activities)**. Чтобы включить аудит всех событий, щелкните **Выполнять аудит как успешных, так и неуспешных действий (Audit Successful And Unsuccessful Activities)**. Щелкните **Далее (Next)**.
18. На странице **Сводка политики аудита (Audit Policy Summary)** просмотрите параметры, которые будут изменены на выбранном сервере в случае применения политики. Обратите внимание на текущие параметры и параметры, которые будут применены политикой. Щелкните **Далее (Next)**.
19. На заглавной странице **Сохранение политики безопасности (Save Security Policy)** щелкните **Далее (Next)**. На странице **Имя файла политики безопасности (Security Policy File Name)** задайте параметры сохранения политики безопасности и при необходимости добавьте в нее один или несколько шаблонов безопасности. Для просмотра политики безопасности щелкните кнопку **Просмотр политики безопасности (View Security Policy)**. Просмотрев политику, вернитесь в мастер.
20. Чтобы добавить в политику шаблоны безопасности, щелкните **Включение шаблонов безопасности (Include Security Templates)**. В диалоговом окне **Включение шаблонов безопасности (Include Security Templates)** щелкните кнопку **Добавить (Add)**. В диалоговом окне **Открыть (Open)** выберите шаблон безопасности, который будет включен в политику. При добавлении нескольких шаблонов вы можете назначить им приоритеты на случай возникновения конфликтов в параметрах безопасности. Параметры шаблонов, занимающих более высокое место в списке, соответственно, обладают более высоким приоритетом. Выберите шаблон и назначьте ему приоритет, щелкая кнопки-стрелки. Щелкните **OK**.
21. По умолчанию политика безопасности сохраняется в папке %SystemRoot%\Security\Msscw\Policies. При необходимости щелкните кнопку **Обзор (Browse)** и выберите другое место для сохранения. Введите имя политики безопасности и щелкните **Сохранить (Save)**. Путь к папке и имя файла отображаются в текстовом поле **Имя файла политики безопасности (Security Policy File Name)**.
22. Щелкните **Далее (Next)**. На странице **Применение политики безопас-**

ности (Apply Security Policy) укажите, применить политику сейчас или позднее. Щелкните **Далее (Next)** и **Готово (Finish)**.

Редактирование существующей политики безопасности

С помощью Мастера настройки безопасности (Security Configuration Wizard) вы можете редактировать существующую политику безопасности. Для этого выполните следующие действия:

1. Запустите Мастер настройки безопасности (Security Configuration Wizard). Для этого щелкните кнопку **Пуск (Start)**, **Администрирование (Administrative Tools)** и **Мастер настройки безопасности (Security Configuration Wizard)**. На первой странице мастера щелкните **Далее (Next)**.
2. На странице **Действие настройки (Configuration Action)** установите переключатель **Изменить существующую политику безопасности (Edit An Existing Security Policy)** и щелкните кнопку **Обзор (Browse)**. В диалоговом окне **Открыть (Open)** выберите политику безопасности, с которой хотите работать, и щелкните **Далее (Next)**. Политики безопасности хранятся в XML-файлах.
3. Выполните шаги 3–22 из предыдущего раздела, чтобы настроить политику безопасности.

Применение существующей политики безопасности

С помощью Мастера настройки безопасности (Security Configuration Wizard) вы можете применить существующую политику безопасности. Для этого выполните следующие действия:

1. Запустите Мастер настройки безопасности (Security Configuration Wizard). Для этого щелкните кнопку **Пуск (Start)**, **Администрирование (Administrative Tools)** и **Мастер настройки безопасности (Security Configuration Wizard)**. На первой странице мастера щелкните **Далее (Next)**.
2. На странице **Действие настройки (Configuration Action)** установите переключатель **Применить существующую политику безопасности (Apply An Existing Security Policy)** и щелкните кнопку **Обзор (Browse)**. В диалоговом окне **Открыть (Open)** выберите политику безопасности, с которой хотите работать, и щелкните **Далее (Next)**. Политики безопасности хранятся в XML-файлах.
3. На странице **Выбор сервера (Select Server)** выберите сервер, к которому хотите применить политику. По умолчанию выбран текущий компьютер. Чтобы выбрать другой компьютер, щелкните кнопку **Обзор (Browse)**. В диалоговом окне **Выбор: «Компьютер» (Select Computer)** введите имя компьютера и щелкните **Проверить имена (Check Names)**. Выделите нужную учетную запись компьютера и щелкните **ОК**.

4. Щелкните **Далее (Next)**. На странице **Применение политики безопасности (Apply Security Policy)** щелкните кнопку **Просмотр политики безопасности (View Security Policy)**, чтобы просмотреть политику. Затем вернитесь в мастер.
5. Щелкните **Далее (Next)**, чтобы применить политику к выбранному серверу. Когда мастер применит политику, щелкните **Далее (Next)** и **Готово (Finish)**.

Откат последней примененной политики

С помощью Мастера настройки безопасности (Security Configuration Wizard) вы можете откатить последнюю примененную политику безопасности. Для этого выполните следующие действия:

1. Запустите Мастер настройки безопасности (Security Configuration Wizard). Для этого щелкните кнопку **Пуск (Start)**, **Администрирование (Administrative Tools)** и **Мастер настройки безопасности (Security Configuration Wizard)**. На первой странице мастера щелкните **Далее (Next)**.
2. На странице **Действие настройки (Configuration Action)** установите переключатель **Откатить последнюю примененную политику безопасности (Rollback The Last Applied Security Policy** и щелкните **Далее (Next)**.
3. На странице **Выбор сервера (Select Server)** выберите сервер, на котором хотите выполнить откат. По умолчанию выбран текущий компьютер. Чтобы выбрать другой компьютер, щелкните кнопку **Обзор (Browse)**. В диалоговом окне **Выбор: «Компьютер» (Select Computer)** введите имя компьютера и щелкните **Проверить имена (Check Names)**. Выделите нужную учетную запись компьютера и щелкните **ОК**.
4. Щелкните **Далее (Next)**. На странице **Откат настройки безопасности (Rollback Security Configuration)** щелкните **Просмотр файла отката (View Rollback File)** для просмотра последней примененной политики. Просмотрев политику, вернитесь в мастер.
5. Щелкните **Далее (Next)**, чтобы выполнить откат политики на выбранном сервере. Когда мастер завершит откат, щелкните **Далее (Next)** и **Готово (Finish)**.

Развертывание политики безопасности на нескольких компьютерах

В организациях с большим количеством компьютеров вряд ли будет эффективно применять политику безопасности к каждому компьютеру по отдельности. Как уже говорилось ранее в этой главе, ее можно применять посредством групповой политики, создавая для этой цели специальные подразделения.

Создав необходимые подразделения, при помощи команды **transform** утилиты Scwcmd создайте GPO, который будет включать в себя параметры, заданные в политике безопасности, и все добавленные в нее шаблоны безопасности. На нескольких компьютерах параметры развертываются посредством связывания GPO с одним или несколькими подразделениями.

Команда для преобразования политики безопасности имеет следующий синтаксис:

```
scwcmd transform /p:ПолныйПутьКПолитике /g:ИмяGPO
```

где *ПолныйПутьКПолитике* — полный путь к XML-файлу политики безопасности, а *ИмяGPO* — отображаемое имя нового GPO. Например:

```
scwcmd transform /p:"c:\users\wrs\documents\fspolicy.xml" /g:"FileServer GPO"
```

Создав GPO, свяжите его с подразделением, выполнив следующие действия:

1. В консоли GPMC выберите подразделение, с которым хотите работать. На вкладке **Связанные объекты групповой политики (Linked Group Policy Objects)** отображены GPO, которые связаны с выбранным подразделением (если таковые имеются).
2. Щелкните правой кнопкой подразделение, с которым хотите связать ранее созданный GPO, и выберите команду **Связать существующий объект GPO (Link An Existing GPO)**. В диалоговом окне **Выбор объекта групповой политики (Select GPO)** выберите нужный GPO и щелкните **ОК**.

Параметры политики в GPO будут применены после обновления групповой политики на компьютерах соответствующего подразделения.

Поскольку вы создали новый GPO, а затем связали его с соответствующим уровнем структуры Active Directory, вы можете восстановить первоначальное состояние компьютеров, удалив связь с GPO. Для этого нужно выполнить следующие действия:

1. В консоли GPMC выберите подразделение, с которым хотите работать. На вкладке **Связанные объекты групповой политики (Linked Group Policy Objects)** отображены GPO, которые связаны с выбранным подразделением.
2. Щелкните правой кнопкой нужный GPO. В контекстном меню напротив команды **Связь включена (Link Enabled)** стоит флажок, указывающий на наличие связи. Сбросьте этот флажок.

Часть II

Администрирование службы каталога Windows Server 2008

Глава 7

Доменные службы Active Directory

Доменные службы Active Directory — открытая и расширяемая служба каталогов, применяемая для рационального управления ресурсами сети. Администратору следует очень хорошо разбираться в ее работе. Если вам раньше не приходилось сталкиваться с Active Directory, вы, пожалуй, даже поразитесь огромному количеству возможностей, которыми обладает эта технология. Чтобы помочь вам справиться с ее изучением, я начну с общего обзора Active Directory, а затем рассмотрю ее отдельные компоненты.

Знакомство с Active Directory

С самого момента выхода Windows 2000 служба Active Directory стала сердцем доменов на базе Windows. Почти любое выполняемое вами административное действие так или иначе затрагивает Active Directory. Технология Active Directory основана на стандартных протоколах Интернета и самой своей организацией помогает правильно выстроить структуру сети.

Active Directory и DNS

В службе каталогов Active Directory используется DNS (Domain Name System) — стандартная служба Интернета, которая объединяет группы компьютеров в домены, образующие иерархическую структуру. Иерархия доменов DNS определяется в масштабах Интернета, а различные уровни этой иерархии соответствуют компьютерам, корпоративным доменам и доменам верхнего уровня. Кроме того, DNS используется для преобразования имен хостов, например, *zeta.microsoft.com*, в числовые IP-адреса, наприме, 192.168.19.2. При помощи DNS иерархия домена Active Directory может стать частью Интернета или же остаться изолированной.

В подобных доменах при обращении к ресурсам компьютера используется его полностью определенное доменное имя (Fully Qualified Domain Name, FQDN), например, *zeta.microsoft.com*. Здесь *zeta* — имя конкретного компьютера, *microsoft* — корпоративный домен, а *com* — домен верхнего уровня. Домены верхнего уровня (top-level domain) лежат в основе иерархии DNS и организованы, главным образом, географически, с использованием двухбуквенных ко-

дов стран. Например, *ca* — код Канады. Домены верхнего уровня также могут обозначаться по типу организации (например, *com* для коммерческих организаций) или по ее назначению (например, *mil* для военных объектов).

Обычные домены, например, *microsoft.com*, называются также *родительскими* доменами, поскольку являются «родителями» организационной структуры. Родительские домены делятся на субдомены, которые могут находиться в различных офисах, отделах или местностях. Например, компьютеру, находящемуся в офисе Майкрософт в Сиэтле, может быть присвоено FQDN-имя *jacob.seattle.microsoft.com*. Здесь *jacob* — имя компьютера, *seattle* — субдомен, а *microsoft.com* — родительским доменом. Субдомены называют также *дочерними* доменами.

DNS — настолько неотъемлемая часть Active Directory, что перед установкой Active Directory необходимо произвести настройку DNS в сети. Работа с DNS подробно описана в главе 20.

В Windows Server 2008 установка Active Directory происходит в два этапа. Сначала вы добавляете на сервер роль доменных служб Active Directory, используя мастер добавления ролей. Затем вы запускаете мастер установки Active Directory, щелкнув **Пуск (Start)** и введя **dcpromo** в поле **Начать поиск (Search)**. Если DNS еще не установлена, вам будет предложено установить ее. Если домена не существует, мастер поможет создать домен и настроить Active Directory в новом домене, а также добавить дочерние домены в существующую структуру. Чтобы проверить правильность установки контроллера домена:

- проверьте журнал событий службы каталогов на предмет наличия ошибок;
- убедитесь, что клиентам доступен каталог Sysvol;
- убедитесь, что разрешение имен работает через DNS;
- проверьте репликацию изменений Active Directory.

Примечание В этой главе далее я часто буду использовать термины *каталог* и *домен* для обозначения, соответственно, Active Directory и доменов Active Directory. Когда мне понадобится отделить структуры Active Directory от DNS и прочих типов каталогов, я это оговорю.

Развертывание контроллера домена, доступного только для чтения

Как уже говорилось в главе 1, контроллеры доменов, работающие под управлением Windows Server 2008, могут быть настроены как контроллеры домена только для чтения (read-only domain controller, RODC). При установке DNS-сервера на RODC-контроллер он может выступать в качестве DNS-сервера только для чтения (read-only DNS, RODNS). В данной конфигурации справедливы следующие утверждения:

- Контроллер RODC реплицирует разделы каталога приложений, используемые DNS, включая разделы ForestDNSZones и DomainDNSZones. Клиент может запрашивать разрешение имен на RODNS-сервере. Од-

нако RODNS-сервер не поддерживает прямые клиентские обновления, поскольку не регистрирует записи ресурсов для любых размещенных на нем зон, интегрированных в Active Directory.

- Когда клиент пытается обновить DNS-записи, сервер возвращает ссылку. Клиент может попытаться произвести обновление на DNS-сервере, указанном в ссылке. Затем RODNS-сервер при помощи фоновой репликации предпримет попытку извлечь обновленную запись из DNS-сервера, выполнившего обновление. Запрос репликации относится только к измененной DNS-записи. В ходе такого специального запроса не производится репликация полного списка изменившихся данных зоны или домена.

Первый контроллер домена Windows Server 2008, установленный в лесе или домене, не может быть RODC-контроллером. Однако все последующие контроллеры домена уже можно настроить как RODC. При планировании помните о следующем:

- Перед добавлением доменных служб Active Directory (Active Directory Domain Services, AD DS) на сервер Windows Server 2008 в лесе Windows Server 2003 или Windows 2000 Server следует обновить схему на хозяине операций схемы (schema operations master) в лесе, запустив команду **adprep /forestprep**.
- Прежде чем установить AD DS на сервер Windows Server 2008 в домене Windows Server 2003 или Windows Server 2000, следует обновить хозяин инфраструктуры (infrastructure master) в домене, запустив команду **adprep /domainprep /gpprep**.
- Перед установкой AD DS с целью создания первого RODC в лесе следует подготовить лес, запустив команду **adprep /rodcprep**.

Windows Server 2008 и Windows NT 4.0

Функции домена Windows Server 2008 конструктивно не приспособлены для взаимодействия с функциями домена Windows NT 4.0. Контроллеры домена, работающие под управлением Windows NT Server 4.0, не поддерживаются в Windows Server 2008, и серверы Windows NT Server 4.0 не поддерживаются контроллерами домена Windows Server 2008. С учетом этих замечаний вам следует выполнить следующие действия:

- произвести обновление контроллеров домена Windows NT Server 4.0 перед развертыванием любых компьютеров Windows Server 2008;
- произвести обновление всех компьютеров Windows NT Server 4.0 перед развертыванием контроллеров домена Windows Server 2008.

Вы можете обновить Windows NT Server 4.0 до Windows 2000 Server или Windows Server 2003. Важно помнить, что даже после обновления всех компьютеров Windows NT Server 4.0 вам по-прежнему будет нужен хозяин операций эмулятора PDC.

Работа с доменной структурой

Active Directory организует как физическую, так и логическую структуру компонентов сети. Логическая структура помогает упорядочить объекты каталога, а также управлять сетевыми учетными записями и общими ресурсами. Компоненты логической структуры таковы:

- **Подразделение (organizational unit)** Подгруппа доменов, как правило, отображающая коммерческую или производственную структуру организации.
- **Домен (domain)** Группа компьютеров с общей базой данных каталога.
- **Дерево доменов (domain tree)** Один или несколько доменов с общим непрерывным пространством имен.
- **Лес доменов (domain forest)** Одно или несколько деревьев, использующих общую информацию каталога.

Физическая структура призвана оптимизировать сетевой обмен данными, а также установить физические границы сетевых ресурсов. Компоненты физической структуры таковы:

- **Подсеть (subnet)** Сетевая группа с конкретным диапазоном IP-адресов и маской.
- **Сайт (site)** Одна или несколько подсетей. Сайты используются для настройки доступа к каталогам и репликации.

Домены

Домен Active Directory — это группа компьютеров с общей базой данных каталога. Доменные имена Active Directory должны быть уникальными. К примеру, нельзя иметь два домена *microsoft.com*, но можно создать родительский домен *microsoft.com* и дочерние домены *seattle.microsoft.com* и *ny.microsoft.com*. Если создаваемый домен является частью закрытой сети, его имя не должно конфликтовать с именем существующего домена этой закрытой сети. Если домен является частью Интернета, присваиваемое ему имя не должно конфликтовать с именем существующего домена Интернета. Чтобы обеспечить уникальность имени в Интернете, перед использованием домена вы должны его зарегистрировать у любого уполномоченного регистратора. Список уполномоченных регистраторов вы найдете на сайте InterNIC (*http://www.internic.net*).

У каждого домена есть собственные политики безопасности и доверительные отношения с другими доменами. Домены могут охватывать несколько физических расположений. Это означает, что домен может состоять из нескольких сайтов, а сайты могут разделяться на несколько подсетей (рис. 7-1). В базе данных каталога домена содержатся объекты, представляющие учетные записи пользователей, групп и компьютеров, а также общие ресурсы, например, принтеры и папки.

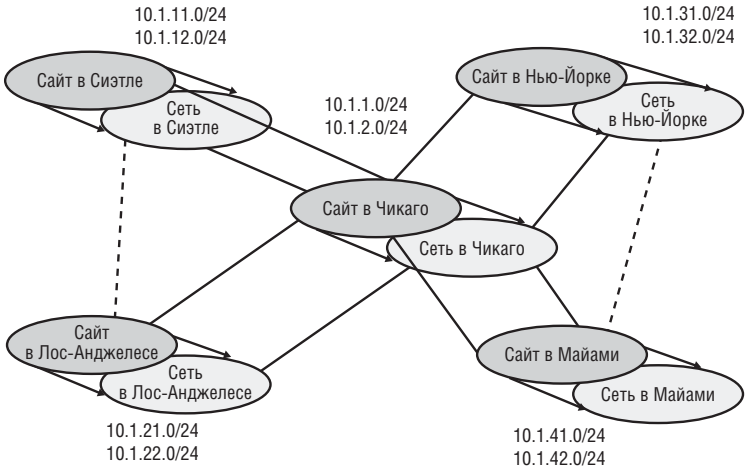


Рис. 7-1. Глобальная сеть (WAN) с несколькими сайтами и подсетями

Примечание Учетные записи пользователей и групп рассматриваются в главе 9. Учетные записи компьютеров и различные типы компьютеров, используемые в доменах Windows Server 2008, обсуждаются в разделе «Работа с доменами Active Directory» этой главы.

Функции домена ограничены и определяются режимом работы домена. Существует несколько режимов, в том числе:

- **Windows 2000 (смешанный режим) (Windows 2000 mixed)** Поддерживает контроллеры домена, работающие под управлением Windows NT 4.0 и более поздних выпусков Windows Server. Тем не менее, в нем нельзя совместно использовать контроллеры домена Windows NT 4.0 и Windows Server 2008, а также контроллеры домена Windows Server 2008 и серверы Windows NT 4.0.
- **Windows 2000 (основной режим) (Windows 2000 native)** Поддерживает контроллеры домена, работающие под управлением Windows 2000 и более поздних версий.
- **Windows Server 2003** Поддерживает контроллеры домена, работающие под управлением Windows Server 2003 и Windows Server 2008.
- **Windows Server 2008** Поддерживает контроллеры домена, работающие под управлением Windows Server 2008.

Дальнейшее обсуждение режимов работы домена вы найдете в разделе «Режимы работы домена» этой главы.

Леса и деревья

У каждого домена Active Directory есть DNS-имя, например, *microsoft.com*. Один или несколько доменов, использующих общие данные каталога, называются *лесом* (forest). Имена доменов внутри этого леса в иерархии DNS могут быть как смежными, так и несмежными.

Домены со смежной структурой имен находятся в одном *дереве* (tree), пример которого показан на рис. 7-2. В этом примере корневой домен *msnbc.com* имеет два дочерних домена — *seattle.msnbc.com* и *ny.msnbc.com*, которые, в свою очередь, разделены на субдомены. Все домены являются частью одного дерева, потому что у них общий корневой домен.

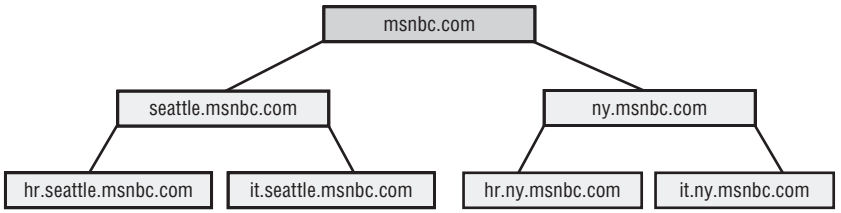


Рис. 7-2. Домены одного дерева используют смежную структуру имен

Если домены в лесу имеют несмежные DNS-имена, они образуют внутри этого леса отдельные доменные деревья. Как показано на рис. 7-3, в лесу доменов может быть одно или несколько деревьев. В данном примере домены *msnbc.com* и *microsoft.com* формируют корни различных деревьев домена в одном лесу.

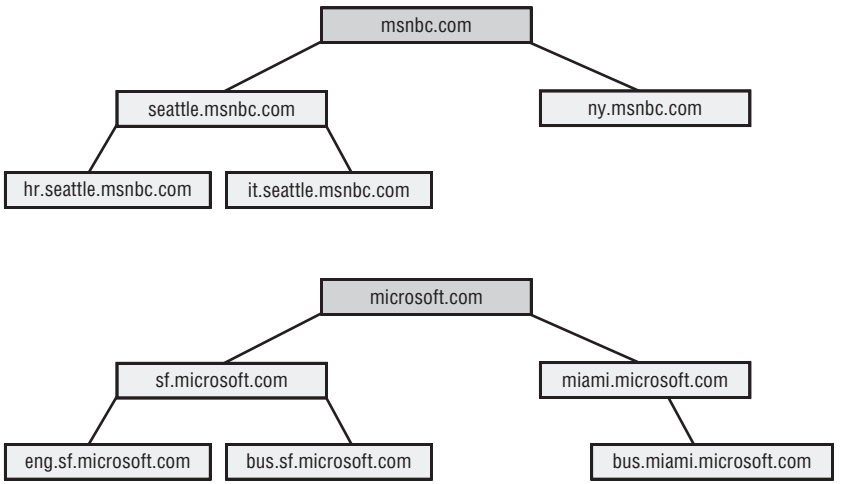


Рис. 7-3. Деревья в лесу обладают несмежной структурой имен

Доступ к доменным структурам осуществляется посредством консоли **Active Directory — домены и доверие (Active Directory Domains And Trusts)**, показанной на рис. 7-4. Она является оснасткой MMC, а также запускается при помощи меню **Администрирование (Administrative Tools)**. В ней вы найдете отдельные записи для каждого корневого домена.

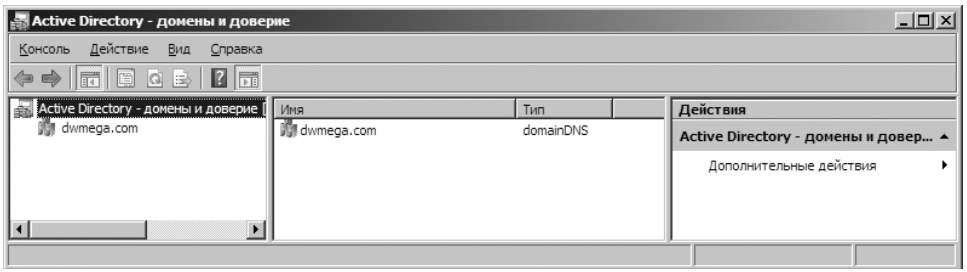


Рис. 7-4. Для работы с доменами, деревьями и лесами используется консоль Active Directory — домены и доверие (Active Directory Domains And Trusts)

Функции леса ограничены и регулируются режимом работы леса. Существует несколько режимов, в том числе:

- **Windows 2000** Поддерживает контроллеры домена, работающие под управлением Windows NT 4.0 и более поздних выпусков Windows Server. В нем нельзя совместно использовать контроллеры домена Windows NT 4.0 и Windows Server 2008, а также контроллеры домена Windows Server 2008 и серверы Windows NT 4.0.
- **Windows Server 2003** Поддерживает контроллеры домена под управлением Windows Server 2003 и Windows Server 2008.
- **Windows Server 2008** Поддерживает контроллеры домена под управлением Windows Server 2008.

Режим работы леса Windows Server 2003 обеспечивает более высокую производительность и располагает существенно более широкими возможностями Active Directory, чем режим работы Windows 2000. Если в этом режиме работают все домены леса, вы своими глазами увидите повышение эффективности репликации глобального каталога и данных Active Directory. Поскольку значения ссылок также реплицируются, улучшается и межсайтовая репликация. У вас имеется возможность отключать объекты и атрибуты класса схемы, использовать динамические вспомогательные классы, переименовывать домены и создавать односторонние, двухсторонние и транзитивные доверительные отношения между лесами.

В режиме работы Windows Server 2008 производительность и набор возможностей Active Directory по сравнению с режимом Windows Server 2003 еще более расширены. Если все домены леса работают в данном режиме, в пределах организации более эффективно будут осуществляться как межсайтовая, так и внутрисайтовая репликация. Кроме того, вместо FRS-репликации на контроллерах домена будет применяться DFS-репликация. Участники безопасности Windows Server 2008 не создаются, если хозяин операция эмулятора PDC в корневом домене леса работает не под управлением Windows Server 2008.

Подразделения

Подразделениями называются подгруппы внутри доменов, как правило, отражающие коммерческую или производственную структуру организации. Подразделения можно представить в виде контейнеров для размещения учетных записей, общих ресурсов и других подразделений. Например, можно создать в домене *microsoft.com* подразделения с названиями HumanResources, IT, Engineering и Marketing. Позже вы сможете расширить эту структуру, включив в нее дочерние подразделения, например, подразделения OnlineSales, ChannelSales и PrintSales для подразделения Marketing.

Объекты, помещенные в подразделение, могут принадлежать только его родительскому домену. Например, дочерние подразделения *seattle.microsoft.com* могут содержать только объекты этого домена. Нельзя добавить в них объекты домена *ny.microsoft.com*. Хотя главное назначение подразделений состоит в распределении объектов согласно структуре организации, это не единственная причина для их создания. Есть и другие преимущества:

- Подразделения позволяют назначать групповую политику небольшой части ресурсов домена, не применяя ее ко всему домену. Это помогает на должном уровне создавать групповые политики предприятия и управлять ими.
- Подразделения позволяют объединить объекты каталога в компактные и потому более управляемые группы.
- Подразделения позволяют делегировать права и управлять административным доступом к ресурсам домена, корректируя масштаб полномочий администратора домена. Можно, например, предоставить некоему пользователю права администратора подразделения, но не всего домена.

В консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** подразделения изображаются в виде папок (рис. 7-5). Эта консоль является оснасткой консоли MMC. Также ее можно запустить из меню **Администрирование (Administrative Tools)**.

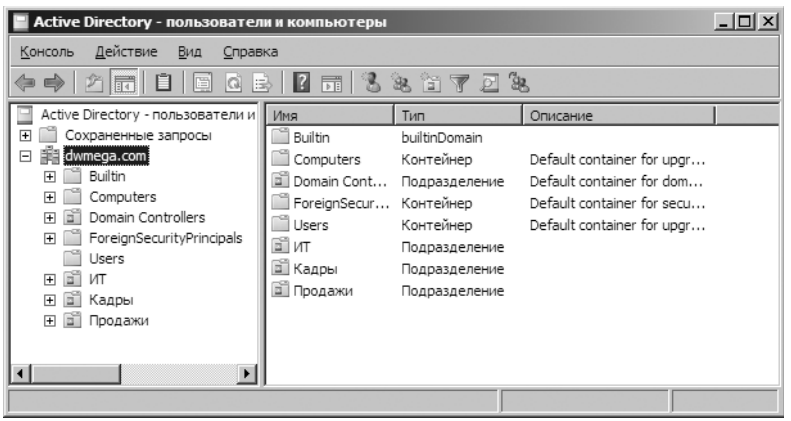


Рис. 7-5. Консоль Active Directory — пользователи и компьютеры (Active Directory Users And Computers) применяется для управления пользователями, группами, компьютерами и подразделениями

Сайты и подсети

Сайт — это группа компьютеров в одной или нескольких IP-подсетях. Сайты используются для отображения физической структуры сети. Структура сайтов не зависит от логической структуры доменов, поэтому очевидной связи между сайтами и доменами не существует. При помощи Active Directory вы можете создать несколько сайтов внутри одного домена или сайт, обслуживающий несколько доменов. Диапазон IP-адресов сайта и пространство имен домена также не связаны между собой.

Подсеть — это группа сетевых адресов. В отличие от сайтов, которые могут объединять несколько диапазонов IP-адресов, подсеть характеризуется конкретным диапазоном IP-адресов и сетевой маской. Имя подсети имеет формат *сеть/битовая маска*, например, 192.168.19.0/24. Здесь сетевой адрес 192.168.19.9 и маска подсети 255.255.255.0 объединены в имя подсети 192.168.19.0/24.

Примечание Вам совсем не обязательно знать, как создавать имя подсети. В большинстве случаев достаточно ввести сетевой адрес и маску подсети, и Windows Server 2008 сгенерирует имя подсети автоматически.

Компьютеры включаются в сайт на основании их расположения в подсети или совокупности подсетей. Если компьютеры в подсетях способны эффективно общаться друг с другом по сети, их называют хорошо связанными (well connected). В идеале, сайты состоят из хорошо связанных подсетей и компьютеров. Если не все подсети и компьютеры хорошо связаны, возможно, вам следует создать несколько сайтов. Связанность дает сайтам следующие преимущества:

- Когда клиент входит в домен, в процессе проверки подлинности сначала выполняется поиск контроллеров домена, находящихся в том же сайте, что и клиент. Это означает, что по возможности используются локальные контролеры домена, что сокращает сетевой трафик и ускоряет процесс проверки подлинности.
- Информация каталога чаще реплицируется внутри сайтов, чем между ними. Это сокращает сетевой трафик, связанный с репликацией, и в то же время гарантирует быструю передачу актуальной информации на локальные контроллеры домена. Для настройки репликации каталога между сайтами используйте ссылки сайта. Контроллер домена, предназначенный для выполнения межсайтовой репликации, называется *сервером-плацдармом* (bridghead server). Назначив сервер-плацдарм для выполнения межсайтовой репликации, вы возлагаете бремя репликации на специальный сервер, а не на любой доступный сервер сайта.

Доступ к сайтам и подсетям осуществляется при помощи консоли **Active Directory — сайты и службы (Active Directory Sites And Services)**, показанной на рис. 7-6. Это оснастка MMC, открыть которую также можно при помощи меню **Администрирование (Administrative Tools)**.

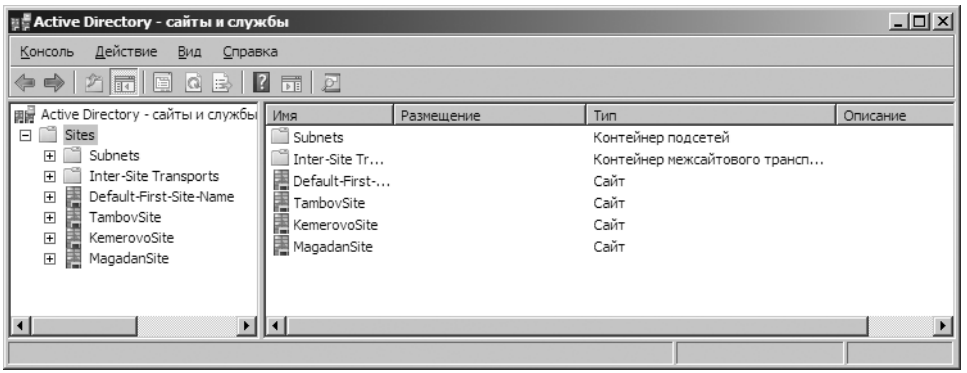


Рис. 7-6. Управление сайтами и подсетями в консоли Active Directory — сайты и службы (Active Directory Sites And Services)

Работа с доменами Active Directory

Хотя в сети Windows Server 2008 вы должны настраивать и Active Directory, и DNS, домены Active Directory и DNS служат разным целям. Домены Active Directory помогают управлять учетными записями, ресурсами и безопасностью. Домены DNS организуют иерархию доменов и используются, главным образом, для разрешения имен. ОС Windows Server 2008 использует DNS для преобразования имен хостов, например, *zeta.microsoft.com*, в числовые IP-адреса, например, 172.16.18.8. За дополнительными сведениями о DNS и доменах DNS обращайтесь в главу 20.

Использование в Active Directory ОС Windows 2000 и более поздних версий

Пользовательские компьютеры, работающие под управлением профессиональных версий Windows 2000, Windows XP и Windows Vista могут всецело использовать Active Directory. Такие компьютеры выходят в сеть в качестве клиентов Active Directory и имеют доступ ко всем возможностям каталога, а также могут использовать транзитивные доверительные отношения, существующие внутри дерева или леса. Транзитивные доверительные отношения устанавливаются неявно, точнее, автоматически, исходя из структуры леса и установленных в лесе разрешений. Эти отношения позволяют прошедшим проверку пользователям получать доступ к ресурсам любого домена в лесе.

Серверы, работающие под управлением Windows 2000 Server, Windows Server 2003 и Windows Server 2008, обслуживают другие системы и могут выступать в роли контроллеров домена или рядовых серверов. Контроллер домена отличается от рядового сервера тем, что на нем выполняются доменные службы Active Directory. Можно повысить рядовой сервер до уровня контроллеров домена, установив на него доменные службы Active Directory, или понизить контроллер домена до рядового сервера, удалив эти службы. Для добавления или удаления доменных служб Active Directory использу-

ются мастера добавления и удаления ролей. Повышение или понижение сервера производится с помощью утилиты dcpromo.exe.

В домене может быть несколько контроллеров. В этом случае контроллеры автоматически реплицируют данные каталога, используя модель репликации с несколькими хозяевами. Эта модель позволяет любому контроллеру домена обрабатывать изменения в каталоге и реплицировать эти изменения на другие контроллеры.

В структуре домена с несколькими хозяевами все контроллеры домена по умолчанию имеют одинаковые обязанности. Тем не менее, вы можете расширить обязанности некоторых контроллеров домена для выполнения определенных задач. Примером может быть сервер-плацдарм, обладающий приоритетом в репликации каталога на другие сайты. Кроме того, некоторые задачи выполнять на специально выделенном для них сервере. Сервер, выполняющий определенный тип задания, называется *хозяином операций* (operations master). Существует пять ролей FSMO (flexible single master operations), которые можно назначить различным контроллерам домена. Дополнительную информацию вы найдете в разделе «Роли хозяина операций» этой главы.

У всех компьютеров домена, работающих под управлением Windows 2000, Windows XP Professional, Windows Vista, Windows Server 2003 и Windows Server 2008, имеются учетные записи компьютеров. Подобно другим ресурсам, учетные записи компьютеров хранятся в Active Directory в качестве объектов и используются для управления доступом к сети и ее ресурсам. Компьютер получает доступ к домену, используя свою учетную запись, которая перед этим проходит проверку подлинности.

Ближе к реальности Контролеры домена используют для авторизации входа в домен компьютеров и пользователей глобальный каталог (global catalog, GC) Active Directory. Если глобальный каталог недоступен, доступ к домену могут получить только члены группы администраторов домена. Это объясняется тем, что в глобальном каталоге хранится информация о членстве в универсальных группах, необходимая для проверки подлинности. Решить эту проблему в Windows Server 2003 и Windows Server 2008 позволяет локальное кеширование членства в универсальных группах. Дополнительную информацию вы найдете в разделе «Структура каталога» этой главы.

Режимы работы домена

Всем компьютерам, работающим под управлением Windows NT, Windows 2000, Windows XP, Windows Vista, Windows Server 2003 и Windows Server 2008, для присоединения к домену необходимы учетные записи. Active Directory поддерживает несколько режимов работы домена, в том числе:

- **Windows 2000 (смешанный режим) (Windows 2000 mixed)** Этот режим не рекомендуется использовать с Windows Server 2008. Он не позволяет применять контроллеры домена под управлением Windows Server 2008, а рядовые серверы под управлением Windows Server 2008 могут испытывать проблемы при работе с контроллерами домена Windows NT.

Домены, работающие в смешанном режиме, не имеют доступа ко многим из более современных возможностей Active Directory, включая универсальные и вложенные группы, преобразование типов групп, простое переименование контроллера домена, номера версий ключей центра распространения ключей (key distribution center, KDC) Kerberos.

- **Windows 2000 (основной режим) (Windows 2000 native)** В основном режиме каталог поддерживает контроллеры домена, работающие под управлением Windows Server 2008, Windows Server 2003 и Windows 2000. Контроллеры домена под управлением Windows NT уже не поддерживаются. Домены, работающие в основном режиме, не поддерживают простое переименование контроллера домена и номера версий ключей центра распространения ключей Kerberos.
- **Windows Server 2003** В режиме Windows Server 2003 каталог поддерживает контроллеры домена, работающие по управлением Windows Server 2008 и Windows Server 2003. Контроллеры домена под управлением Windows NT и Windows 2000 не поддерживаются. Домен, работающий в режиме Windows Server 2003, имеет доступ ко многим новым функциям Active Directory, включая универсальные группы, вложенность групп, преобразование типов групп, простое переименование контроллера домена и номера версий ключей центра распространения ключей Kerberos.
- **Windows Server 2008** В режиме Windows Server 2008 каталог поддерживает контроллеры домена, работающие по управлением Windows Server 2008. Контроллеры домена под управлением Windows NT, Windows 2000 и Windows Server 2003 не поддерживаются. Однако взамен вы получаете поддержку всех новейших возможностей Active Directory, включая репликацию DFS, повышающую эффективность внутрисайтовой и межсайтовой репликации.

Работа в основном режиме Windows 2000

Если после обновления главного контроллера домена (primary domain controller, PDC), резервных контроллеров домена (backup domain controller, BDC) и прочих систем Windows NT у вас все еще остались ресурсы домена Windows 2000, перейдите в основной режим Windows 2000. После этого вы будете использовать в домене только ресурсы Windows 2000, Windows Server 2003 и Windows Server 2008. Из основного режима Windows 2000 вернуться к смешанному режиму уже нельзя. Поэтому осуществляйте переход, только если вы уверены в том, что вам больше не потребуются ни старая структура домена Windows NT, ни резервные контроллеры домена Windows NT.

Перейдя в основной режим Windows 2000, вы обнаружите следующие изменения:

- Основным механизмом проверки подлинности стал протокол Kerberos v5, а проверка подлинности NTLM более не используется.
- Эмулятор PDC более не синхронизирует данные с существующими BDC Windows NT.

- Вы не можете добавить в домен новые контроллеры домена Windows NT.

Переключение из смешанного в основной режим работы Windows 2000 происходит путем повышения функционального уровня домена.

Работа в режиме Windows Server 2003

Обновив структуру Windows NT, можете приступать к обновлению до домена Windows Server 2003. Для этого нужно обновить контроллеры домена Windows 2000 до Windows Server 2003 или Windows Server 2008. Затем при необходимости вы измените режим работы на Windows Server 2003.

Перед обновлением контроллеров домена, работающих под управлением Windows 2000, следует подготовить домен к обновлению. Для этого вам придется при помощи утилиты Adprep.exe обновить лес и схему домена, чтобы они стали совместимы с доменами Windows Server 2003. Ее нужно запустить на хозяине операций схемы в лесе, а затем на хозаяине операций инфраструктуры каждого домена леса. Как всегда, следует сначала проверить каждую процедуру в лабораторных условиях, и только потом выполнять в рабочей среде. Вы найдете Adprep в папке i386 на установочном диске Windows Server 2003.

Примечание Чтобы выявить сервер, являющийся текущим хозяином операций схемы, откройте окно командной строки и введите **dsquery server -hasfsmo schema**. Возвращаемая ею информация выглядит так:

```
"CN=CORPSERVER01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,
CN=Configuration,DC=microsoft,DC=com."
```

Из этой строки следует, что хозяином операций схемы является сервер COPRSERVER01 в домене *microsoft.com*.

Примечание Чтобы определить сервер, являющийся текущим хозяином операций инфраструктуры, введите **dsquery server -hasfsmo infr**.

После обновления серверов измените режим работы домена и леса, чтобы воспользоваться новейшими возможностями Active Directory. Однако после этого в домене вы сможете пользоваться только ресурсами Windows Server 2003 и Windows Server 2008 и не сможете вернуться ни к одному из ранее установленных режимов. Поэтому следует переходить в режим Windows Server 2003, только будучи уверенным в том, что старые структуры домена Windows NT, резервные контроллеры домена Windows NT или структуры домена Windows 2000 вам больше не понадобятся.

Работа в режиме Windows Server 2008

Обновив структуры Windows NT и Windows 2000, вы можете приступить к обновлению домена до Windows Server 2008. Для этого нужно обновить контроллеры домена Windows Server 2003 до Windows Server 2008. Затем при необходимости вы можете изменить режим работы на Windows Server 2008.

Перед обновлением контроллеров домена, работающих под управлением Windows Server 2003, следует подготовить домен к Windows Server 2008,

воспользовавшись утилитой Adprep.exe. Она обновит лес и схему домена, чтобы они стали совместимы с доменами Windows Server 2008. Выполните следующие действия:

1. На хозяине операций схемы в лесе скопируйте в локальную папку содержимое папки Sources\Adprep на установочном диске Windows Server 2008 и запустите команду **adprep /forestprep**. Если вы планируете устанавливать контроллеры домена только для чтения, следует также запустить **adprep /rodcprep**. Вам нужно будет зарегистрироваться с учетной записью администратора, которая является членом группы администраторов предприятия, администраторов схемы или администраторов домена в корневом домене леса.
2. На хозяине операций инфраструктуры каждого домена в лесе скопируйте содержимое папки Sources\Adprep на установочном диске Windows Server 2008 в локальную папку и запустите **adprep /domainprep**. Вам нужно будет зарегистрироваться с учетной записью, являющуюся членом группы администраторов домена в соответствующем домене.

Как всегда, следует сначала проверить каждую процедуру в лабораторных условиях и только потом выполнять в рабочей среде.

Обновив все контроллеры домена до Windows Server 2008, вы можете поднять режим работы домена и леса, чтобы воспользоваться новейшими возможностями Active Directory. Однако после этого вы сможете пользоваться в домене ресурсами только Windows Server 2008 и не сможете вернуться ни к одному из ранее установленных режимов. Поэтому следует переходить в режим Windows Server 2008, только будучи уверенным в том, что старые структуры домена Windows NT, резервные контроллеры домена Windows NT, структуры домена Windows 2000 или Windows Server 2003 вам больше не понадобятся.

Изменение режима работы домена и леса

Домены, работающие в режиме не ниже Windows Server 2003, имеют доступ ко многим усовершенствованиям доменов Active Directory, включая универсальные группы, вложенные группы, преобразование типов групп, простое переименование контроллера домена и номера версий ключей центра распространения ключей Kerberos. В этом режиме администраторы могут также выполнять следующие действия:

- переименовывать контроллеры домена без предварительного понижения;
- переименовывать домены, работающие на контроллерах Windows Server 2008;
- создавать расширенные двухсторонние доверительные отношения между лесами;
- переименовывать и перемещать домены в иерархии доменов;
- пользоваться усовершенствованиями в репликации отдельных членов групп и глобальных каталогов.

Леса, работающие в режиме не ниже Windows Server 2003, имеют доступ к усовершенствованиям лесов Active Directory, что означает повышенную эффективность репликации глобального каталога, репликации внутри сайтов и между сайтами, а также, возможность устанавливать односторонние, двухсторонние и транзитивные доверительные отношения между лесами.

Ближе к реальности Процесс обновления домена и леса генерирует значительный трафик, поскольку информация реплицируется по всей сети. Иногда весь процесс обновления занимает не менее 15 минут. В течение этого периода могут отмечаться задержки при подключении к серверу, а также повышенное время ожидания в сети. Поэтому следует планировать обновление на нерабочее время. Также неплохо перед выполнением этой операции всесторонне исследовать ее совместимость с существующими приложениями (особенно со старыми).

Чтобы изменить режим работы домена, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команды **Администрирование (Administrative Tools)** и **Active Directory — домены и доверие (Active Directory Domains And Trusts)**.
2. В дереве консоли щелкните правой кнопкой домен, с которым хотите работать, и выберите команду **Изменение режима работы домена (Raise Domain Functional Level)**. Откроется диалоговое окно **Повышение режима работы домена (Raise Domain Functional Level)**, в котором указаны имя и текущий режим работы домена.
3. Выберите в списке новый режим работы домена и щелкните кнопку **Повысить (Raise)**. Это действие отменить нельзя, поэтому тщательно продумайте его последствия.
4. Когда вы щелкнете **OK**, новый режим работы домена будет реплицирован на все его контроллеры. В больших организациях этот процесс может занять некоторое время.

Чтобы изменить режим работы леса, выполните следующие действия:

1. Щелкните кнопку **Пуск (Start)** и выберите команлы **Администрирование (Administrative Tools)** и **Active Directory — домены и доверие (Active Directory Domains And Trusts)**.
2. В дереве консоли щелкните правой кнопкой узел **Active Directory — домены и доверие (Active Directory Domains And Trusts)** и выберите команду **Изменение режима работы леса (Raise Forest Functional Level)**. Откроется диалоговое окно **Повышение режима работы леса (Raise Forest Functional Level)**, в котором указаны имя и текущий режим работы леса.
3. Выберите новый режим работы леса из списка и щелкните **Повысить (Raise)**. Это действие отменить нельзя, поэтому тщательно продумайте его последствия.
4. Когда вы щелкнете **OK**, новый режим работы леса будет реплицирован на каждый контроллер в каждом домене леса. В больших организациях этот процесс может занять некоторое время.

Структура каталога

Служба каталогов Active Directory состоит из многих компонентов и построена на множестве технологий. Данные каталога доступны пользователям и компьютерам благодаря хранилищам данных и глобальным каталогам. Хотя большинство действий, выполняемых в Active Directory, затрагивают хранилище данных, глобальные каталоги в равной степени важны, так как они используются при входе в систему и для поиска информации. Если глобальный каталог недоступен, обычные пользователи в домен войти не могут. Единственный способ изменить такое положение дел — локальное кеширование универсальной группы пользователей. Как вы, наверное, догадываетесь, кеширование универсальной группы пользователей имеет свои преимущества и недостатки, которые мы сейчас обсудим.

Вы получаете доступ к чужим данным и размещаете свои данные в Active Directory, используя репликацию и протоколы доступа к каталогу. Протоколы доступа к каталогу позволяют клиентам подключаться к компьютерам, на которых работает Active Directory. Репликация необходима для размещения обновленных данных на контроллерах домена. Основной способ распространения обновлений — репликация в модели с несколькими хозяевами. Некоторые изменения могут обрабатываться только специальными контроллерами домена — *хозяевами операций*. На способ репликации с несколькими хозяевами влияет также новая функция Windows Server 2008 — *разделы каталога приложений* (application directory partitions).

С помощью разделов каталога приложений администраторы предприятия, входящие в соответствующую группу, могут создавать в лесе домена разделы репликации, то есть, логические структуры, использующиеся для управления репликацией в пределах леса. Например, вы можете создать раздел для управления репликацией DNS внутри домена, не давая реплицировать информацию DNS другим системам домена.

Раздел каталога приложений может выступать в роли нового дерева в лесе, дочернего раздела домена или дочернего раздела другого раздела. Копии раздела каталога приложений можно сделать доступными на любом контроллере домена Active Directory, работающем под управлением Windows Server 2008, включая глобальные каталоги. Разделы каталога приложений полезны в больших доменах и лесах, однако они увеличивают накладные расходы, связанные с планированием, управлением и обслуживанием.

Знакомство с хранилищем данных

Хранилище данных содержит информацию о таких объектах, как учетные записи, общие ресурсы, подразделения и групповые политики. Хранилище данных также называется *каталогом* (directory), что роднит его с самой Active Directory.

На контроллерах домена каталог хранится в файле Ntds.dit, расположение которого задается во время установки Active Directory. Он должен

находиться на диске с файловой системой NTFS, отформатированном для использования в Windows Server 2008. Вы можете хранить данные каталога отдельно от главного хранилища данных. Это относится к групповым политикам, сценариям и другой открытой информации, хранящейся на общем системном томе (Sysvol).

Поскольку хранилище данных является контейнером для объектов, предоставление информации каталога в общее пользование называется *публикацией*. Например, вы публикуете информацию о принтере, предоставляя к нему общий доступ по сети.

Контроллеры домена реплицируют большую часть изменений в хранилище данных в модели с несколькими хозяевами. Администратору небольшой или средней организации редко приходится управлять репликацией хранилища данных, так как она выполняется автоматически. В крупных организациях или организациях с особыми требованиями ее можно настроить.

Реплицируются не все данные каталога, а только открытая информация, попадающая в одну из следующих категорий:

- **Данные домена** Информация об объектах домена: учетных записях, общих ресурсах, подразделениях и групповых политиках.
- **Данные конфигурации** Топология каталога: список доменов, деревьев и лесов, а также расположение контроллеров домена и серверов глобального каталога.
- **Данные схемы** Все объекты и типы данных, которые могут быть сохранены в каталоге. Стандартная схема, предусмотренная в Windows Server 2008, описывает объекты учетных записей, объекты общих ресурсов и пр. Вы вольны расширить стандартную схему, определив новые объекты и атрибуты или добавляя новые атрибуты для существующих объектов.

Знакомство с глобальным каталогом

Если членство в универсальной группе локально не кешируется, глобальные каталоги позволяют войти в сеть, предоставляя во время запуска процесса входа в сеть информацию о членстве в универсальной группе. Глобальные каталоги также позволяют производить поиски в каталогах по всем доменам леса. Контроллер домена, назначенный глобальным каталогом, хранит полную копию всех объектов каталога своего домена и частичную копию каталога остальных доменов леса.

Примечание Частичных копий достаточно, так как для входа в систему и поиска требуются только некоторые свойства объекта. Частичная копия также сокращает количество информации, передаваемой по сети.

По умолчанию глобальным каталогом назначается первый контроллер, установленный в домене. Если в домене есть только один контроллер, глобальный каталог и контроллер домена являются одним сервером. В противном случае глобальный каталог располагается на указанном вами контроллере домена. Вы также вольны добавлять в домен глобальные каталоги,

чтобы сократить время отклика при проверке подлинности и выполнении поиска. Рекомендуется иметь внутри домена по одному глобальному каталогу на сайт.

Контроллеры домена, выполняющие функции глобального каталога, должны быть хорошо связаны с контроллерами, выступающими в роли хозяев инфраструктуры. Роль хозяина инфраструктуры является одной из пяти ролей хозяина операций, которые можно назначить контроллеру домена. В домене хозяин инфраструктуры отвечает за обновление ссылок на объекты, сравнивая свои данные с данными глобального каталога. Если хозяин инфраструктуры находит устаревшие данные, он запрашивает обновленные данные в глобальном каталоге, а затем реплицирует изменения на другие контроллеры домена. Подробнее — в разделе «Роли хозяина операций» этой главы.

Если в домене всего один контроллер домена, вы можете сделать хозяином инфраструктуры и глобальным каталогом один и тот же компьютер. Если в домене несколько контроллеров, глобальный каталог и хозяин инфраструктуры должны располагаться на разных контроллерах. В противном случае, хозяин инфраструктуры не найдет устаревшие данные и не реплицирует изменения. Единственным исключением является случай, когда глобальный каталог размещен на всех контроллерах домена. В этом случае не имеет значения, какой контроллер домена выполняет роль хозяина инфраструктуры.

Одна из основных причин настройки дополнительных глобальных каталогов в домене заключается в обеспечении доступности каталога для входа в сеть и обработки запросов на поиск. Если в домене всего один глобальный каталог, который стал недоступен, и нет локального кеширования членства в универсальных группах, обычные пользователи не смогут войти в сеть, а вы не сможете произвести поиск в каталоге. При недоступном глобальном каталоге войти в домен могут только администраторы домена.

Поиск в глобальном каталоге очень эффективен. Каталог содержит информацию обо всех объектах всех доменов леса. Это позволяет выполнять запросы на поиск по каталогу в локальном домене, а не в домене на другом конце сети. Локальное выполнение поиска уменьшает загруженность сети и в большинстве случаев позволяет быстрее получить ответ.

Совет Если проверка подлинности или запросы на поиск стали выполняться дольше обычного, возможно, вам следует настроить дополнительные глобальные каталоги. Однако чем больше глобальных каталогов, тем больше данных передается по сети.

Кеширование членства в универсальной группе

В крупных организациях не всегда практично иметь глобальный каталог в каждом филиале. Однако отсутствие глобального каталога может стать источником проблемы. Если удаленный офис теряет связь с главным офисом или отделением, в котором находятся серверы глобального каталога, обыч-

ные пользователи не смогут войти в сеть, поскольку запросы на вход в систему должны направляться через сеть на сервер глобального каталога в другом офисе. В отсутствие связи эта задача невыполнима.

Как вы, наверное, догадываетесь, эту проблему можно решить несколькими способами. Во-первых, можно сделать один из контроллеров домена в филиале сервером глобального каталога, выполнив процедуру, описанную в разделе «Настройка глобального каталога» главы 8. Недостаток состоит в том, что такой сервер потребует дополнительных накладных расходов и ресурсов. Вам придется также тщательно следить за доступностью сервера глобального каталога.

Другой способ решения этой проблемы — локальное кеширование членства в универсальной группе. Благодаря ему любой контроллер домена может обрабатывать запросы на авторизацию локально, не обращаясь к серверу глобального каталога. Это ускоряет вход в сеть, а также снижает зависимость от выхода сервера из строя: домен более не зависит от единственного сервера или группы серверов для выполнения входа в сеть. Это решение также сокращает трафик репликации. Вместо периодической репликации всего глобального каталога обновляется только кешированная информация о членстве в универсальной группе. По умолчанию на каждом контроллере домена, локально кеширующем членство в группе, обновление происходит каждые восемь часов.

Членство в универсальной группе определяется в пределах сайта. Напомню, что сайтом называется физическая структура в каталоге, состоящая из одной или нескольких подсетей с конкретными диапазонами IP-адресов и масками. Контроллеры домена, работающие под управлением Windows Server 2008, и глобальный каталог, с которым они связаны, должны находиться в одном сайте. Если у вас несколько сайтова, вам следует настроить локальное кеширование в каждом из них. Кроме того, пользователи в сайте должны быть частью домена Windows Server 2008, работающего в режиме леса Windows Server 2008. Чтобы узнать, как настроить кеширование, читайте раздел «Настройка кеширования членства в универсальной группе» главы 8.

Репликация и Active Directory

Какую бы репликацию вы ни использовали (FRS или DFS), в каталоге хранятся данные трех типов: данные домена, данные схемы и данные конфигурации.

Данные домена реплицируются на все контроллеры внутри данного домена. Данные схемы и конфигурации реплицируются на все домены в дереве или лесе. Кроме того, все объекты конкретного домена и подмножество свойств объектов леса реплицируются в глобальный каталог.

Это означает, что контроллеры домена хранят и реплицируют следующие сведения:

- информацию о схеме доменного дерева или леса;
- информацию о конфигурации всех доменов дерева или леса;
- все объекты каталога и свойства соответствующих доменов.

На контроллерах домена с глобальным каталогом хранится и реплицируется информация схемы леса, информация о конфигурации всех доменов в лесе, подмножество свойств всех объектов каталога в лесе (оно реплицируется только между серверами глобального каталога) и все объекты каталога и свойства соответствующих доменов.

Чтобы лучше разобраться в репликации, рассмотрим следующий сценарий установки новой сети:

1. Вы устанавливаете первый контроллер в домене A. Сервер является единственным контроллером домена, а также содержит глобальный каталог. Репликация не производится, поскольку другие контроллеры домена отсутствуют.
2. Вы устанавливаете второй контроллер в домене A. Начинается репликация, поскольку контроллеров домена уже два. Чтобы гарантировать правильность репликации данных, настройте один контроллер домена как хозяин инфраструктуры, а другой — как глобальный каталог. Хозяин инфраструктуры следит за обновлениями глобального каталога и запрашивает обновления изменившихся объектов. Два контроллера домена также реплицируют схему и данные конфигурации.
3. Вы устанавливаете в домене A третий контроллер, который не является глобальным каталогом. Хозяин инфраструктуры следит за обновлениями глобального каталога и запрашивает обновления изменившихся объектов, а затем реплицирует эти изменения на третий контролер домена. Три контроллера домена также реплицируют схему и данные конфигурации.
4. Вы устанавливаете новый домен B и добавляете в него контроллеры. Хосты глобального каталога в доменах A и B начинают репликацию всей схемы и данных конфигурации, а также подмножества данных домена в каждом домене. Репликация в домене A продолжается, как было описано ранее. Начинается репликация в домене B.

Active Directory и LDAP

Протокол облегченного доступа к каталогам (Lightweight Directory Access Protocol, LDAP) — стандартный протокол взаимодействия в TCP/IP-сетях. Он специально предназначен для обеспечения доступа к службе каталогов с минимумом накладных расходов. В протоколе LDAP также определены действия, которые можно использовать для выполнения запросов и изменения информации каталога.

Клиенты Active Directory используют протокол LDAP для взаимодействия с компьютерами, на которых запущена Active Directory, при каждом входе в сеть или поиске ресурсов. Протокол LDAP также можно использовать для управления Active Directory.

Протокол LDAP — открытый стандарт, который может использоваться и другими службами каталогов. Это упрощает взаимодействие между каталогами и упрощает переход к Active Directory из других служб каталогов. Для повышения эффективности взаимодействия используйте интерфейс ADSI (Active Directory Service Interface), поддерживающий стандартные API-интерфейсы для LDAP, которые определены в RFC 1823. Вы также можете использовать ADSI с Windows Script Host для описания объектов в Active Directory.

Роли хозяина операций

Роли хозяина операций предназначены для выполнения задач, которые неудобно выполнять в модели с несколькими хозяевами. Есть пять ролей хозяина операций, которые можно назначить одному или нескольким контроллерам. Некоторые роли можно назначить только один раз во всем лесу, другие роли можно определить в каждом домене.

В каждом лесу Active Directory должны иметься следующие роли:

- **Хозяин схемы (schema master)** Отвечает за обновления и модификации схемы каталога. Чтобы обновить схему каталога, вам нужно получить доступ к хозяину схемы. Чтобы определить, какой сервер в данный момент является хозяином схемы в домене, введите в командной строке **dsquery server -hasfsmo schema**.
- **Хозяин именования доменов (domain naming master)** Управляет добавлением и удалением доменов леса. Чтобы добавить или удалить домен, вы должны получить доступ к хозяину именования доменов. Чтобы определить, какой сервер в данный момент является хозяином именования доменов, введите в командной строке **dsquery server -hasfsmo name**.

Эти роли имеют значение на уровне леса и должны быть уникальными, то есть, вы можете настроить только один хозяин схемы и один хозяин именования доменов на весь лес.

В каждом домене Active Directory должны иметься следующие роли:

- **Хозяин пула RID (relative ID master)** Назначает относительные идентификаторы контроллерам домена. Каждый раз, когда вы создаете пользователя, группу или компьютер, контроллер домена назначает им уникальные идентификаторы безопасности, состоящие из идентификатора безопасности домена и уникального относительного идентфикатора, который назначается хозяином пула RID. Чтобы определить, какой сервер в данный момент является хозяином пула RID, откройте командную строку и введите **dsquery server -hasfsmo rid**.
- **Эмулятор PDC (PDC emulator)** Когда вы используете смешанный или промежуточный режим работы, эмулятор PDC выступает в роли главного контроллера домена Windows NT. В его функции входят проверка подлинности при входе в систему Windows NT, обработка изменений пароля и репликация обновлений на резервный контроллер домена. Чтобы опреде-

лить, какой сервер в данный момент является эмулятором PDC в домене, откройте командную строку и введите **dsquery server -hasfsmo pdc**.

- **Хозяин инфраструктуры (infrastructure master)** Обновляет ссылки на объекты, сравнивая собственные данные каталога с данными глобального каталога. Если данные устарели, хозяин инфраструктуры запрашивает новые данные в глобальном каталоге, а затем реплицирует изменения на другие контроллеры домена. Чтобы определить, какой сервер в данный момент является хозяином инфраструктуры, откройте командную строку и введите **dsquery server -hasfsmo infr**.

Эти роли работают на уровне домена и должны быть уникальными в нем. Это означаетт, что в домене можно настроить только один хозяин пула RID, один эмулятор PDC и один хозяин инфраструктуры.

Роли хозяина операций, как правило, назначаются автоматически, но вы можете изменить назначения. Когда вы настраиваете сеть, все роли хозяина операций присваиваются первому контроллеру домена в первом домене. Если вы позднее создадите новый дочерний домен или корневой домен в новом дереве, первому контроллеру домена в новом домене также автоматически присваиваются роли хозяина операций. Все роли хозяина операций автоматически присваиваются контроллеру домена в новом лесе. Если новый домен находится в том же лесе, ему присваиваются роли хозяина пула RID, эмулятора PDC и хозяина инфраструктуры. Роли хозяина схемы и хозяина именования доменов остаются в первом домене леса.

Если в домене имеется всего один контроллер домена, он обрабатывает все роли хозяина операций. Если вы работаете с единственным сайтом, стандартного размещения ролей хозяина операций вполне достаточно. Однако по мере добавления контроллеров домена и новых доменов, стоит переместить роли хозяина операций на другие контроллеры.

В домене с двумя или несколькими контроллерами домена настройте для обработки ролей хозяина операций два контроллера, один из которых будет основным, а второй — резервным. Резервный хозяин операций используется в случае неисправности основного. Убедитесь, что контроллеры домена являются прямыми партнерами репликации и хорошо связаны.

По мере усложнения структуры домена вам придется разделить роли хозяина операций и разместить их на различных контроллерах. Это может повысить эффективность серверов. Уделите особое внимание текущим обязанностям контроллера домена, который собираетесь использовать в роли хозяина.

Ближе к реальности Не следует разделять роли хозяина схемы и хозяина именования доменов. Всегда назначайте их одному серверу. Для более эффективной работы следует также оставлять на одном сервере хозяин пула RID и эмулятор PDC, но эти роли при необходимости можно разделить. Например, в большой сети, где пиковые нагрузки приводят к проблемам с производительностью, стоит разместить хозяин пула RID и эмулятор PDC на разных контроллерах. Кроме того, как правило не следует помещать хозяин инфраструктуры на контроллер домена, выполняющий функцию глобального каталога. Подробнее — в разделе «Знакомство с глобальным каталогом» этой главы.

Глава 8

Основные методы администрирования Active Directory

Основные методы администрирования Active Directory тесно связаны с ключевыми задачами, которые вам предстоит регулярно решать при помощи доменных служб Active Directory. К этим задачам относятся, например, создание учетных записей компьютера и присоединение компьютеров к домену. В этой главе вы познакомитесь с инструментами, применяемыми для управления Active Directory, а также с особенностями управления компьютерами, контроллерами домена и подразделениями.

Средства управления Active Directory

Для управления Active Directory предназначено несколько наборов инструментов, как графических, так и запускаемых из командной строки.

Средства администрирования Active Directory

Средства администрирования Active Directory поставляются в виде оснасток консоли MMC. Ниже приведен список основных инструментов управления Active Directory:

- **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** Управление пользователями, группами, компьютерами и подразделениями.
- **Active Directory — домены и доверие (Active Directory Domains And Trusts)** Работа с доменами, деревьями и лесами.
- **Active Directory — сайты и службы (Active Directory Sites And Services)** Управление сайтами и подсетями.
- **Управление групповой политикой (Group Policy Management)** Управление использованием групповых политик и доступ к результирующей политике для моделирования и протоколирования.

Безопасность Администрированию при помощи консоли MMC может помешать брандмауэр Windows, включенный на удаленном компьютере. Если в сообщении об ошибке говорится, что у вас недостаточно прав, не найден сетевой путь или запрещен

доступ, попробуйте установить на удаленном компьютере исключение для порта 445 протокола TCP. Для этого можно включить параметр политики **Брандмауэр Windows: разрешить исключение для входящих сообщений удаленного администрирования (Windows Firewall: Allow Remote Administration Exception)** из раздела **Конфигурация компьютера\Административные шаблоны\Сеть\Сетевые подключения\Брандмауэр Windows\Профиль домена (Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile**) или ввести в командной строке удаленного компьютера команду **netsh firewall set portopening tcp 445 smb enable**. Дополнительную информацию вы найдете в статье 840634 базы знаний Майкрософт *(http://support.microsoft.com/default.aspx?scid=kb;en-us;840634)*.

Доступ к средствам администрирования Active Directory можно получить из меню **Администрирование (Administrative Tools)**. Вы также вольны добавить их в любую консоль MMC. Если вы работаете за другим компьютером, имеющим доступ в домен Windows Server 2008, перед использованием этих средств их необходимо установить. Сделать это можно при помощи Мастера добавления компонентов (Add Feature Wizard).

Каждый инструмент работает по-разному, однако в них используются общие приемы редактирования:

- **Выбор несмежных ресурсов** Удерживая нажатой клавишу Ctrl, щелкайте левой кнопкой мыши каждый объект, который хотите выделить.
- **Выбор смежных ресурсов** Удерживая нажатой клавишу Shift, щелкните первый и последний объект диапазона выделяемых ресурсов.
- **Перетаскивание ресурсов** Выделите объекты, которые хотите переместить, затем нажмите и удерживайте левую кнопку мыши, одновременно перемещая указатель в нужное место.
- **Редактирование свойств нескольких ресурсов одновременно** Выделите объекты, с которыми хотите работать, щелкните их правой кнопкой и выберите нужную команду, например, **Свойства (Properties)**.

Инструменты командной строки Active Directory

Существует несколько инструментов для управления Active Directory из командной строки:

- **ADPREP** Подготавливает лес или домен Windows 2000 к установке контроллеров домена Windows 2003. Для подготовки леса или домена используйте команды **adprep /forestprep** и **adprep /domainprep**, соответственно.

Безопасность В Windows Server 2003 SP1 и более поздних версиях, а также в Windows Server 2008 групповая политика домена автоматически не обновляется. Для подготовки групповой политики домена следует использовать команду **adprep /domainprep /gpprep**. Этим вы измените записи управления доступом (ACE) для всех папок объектов групповой политики (GPO) в папке Sysvol, чтобы разрешить их чтение всем контроллерам доменов предприятия. Это требуется для поддержки результирующей политики в сайтах. Это изменение в системе безопасности приводит к тому, что служба файловой репликации NT (NTFRS) повторно отправляет все объекты групповой политики на контроллеры домена. Поэтому использование команды **adprep /domainprep /gpprep** следует тщательно планировать.

- **DSADD** Добавляет в Active Directory компьютеры, контакты, группы, подразделения и пользователей. Для вывода справки по использованию команды введите в командной строке **dsadd *имяобъекта* /?**, например, **dsadd computer /?**.
- **DSGET** Отображает свойства компьютеров, контактов, групп, подразделений, пользователей и серверов Active Directory. Для вывода справки по использованию команды введите в командной строке **dsget *имяобъекта* /?**, например, **dsget server /?**.
- **DSMOVE** Перемещает один объект в новое расположение внутри того же домена или переименовывает объект, не перемещая его. Для вывода справки по использованию команды введите в командной строке **dsmove /?**.
- **DSQUERY** Выполняет в Active Directory поиск компьютеров, контактов, групп, подразделений, пользователей, сайтов, подсетей и серверов по заданному критерию. Для вывода справки по использованию команды введите в командной строке **dsquery /?**.
- **DSRM** Удаляет объекты из Active Directory. Для вывода справки по использованию команды введите в командной строке **dsrm /?**.
- **NTDSUTIL** Позволяет пользователям просматривать информацию о сайте, домене и сервере, управлять ролью хозяина операций, а также обслуживать базу данных Active Directory. Для вывода справки по использованию команды введите в командной строке **ntdsutil /?**.

Инструменты поддержки Active Directory

Вместе с Windows Server 2008 поставляются многие инструменты поддержки Active Directory. В табл. 8-1 перечислены наиболее популярные инструменты для настройки, управления и устранения неполадок Active Directory.

Табл. 8-1. Краткий список инструментов поддержки Active Directory

Инструмент	Исполняемый файл	Описание
ADSI Edit	Adsiedit.msc	Открывает и редактирует интерфейс служб Active Directory для домена, схемы и контейнеров конфигурации
Инструмент администрирования Active Directory	Ldp.exe	Выполняет операции протокола LDAP с Active Directory
Утилита списка управления доступом к службам каталога	Dsacls.exe	Управляет списками ACL для объектов из Active Directory
Утилита распределенной файловой системы	Dfsutil.exe	Управляет распределенной файловой системой (DFS) и отображает информацию о ней

Табл. 8-1. (*окончание*)

Инструмент	Исполняемый файл	Описание
Средство диагностики DNS	Dnscmd.exe	Управляет свойствами серверов, зон и записей ресурса DNS
Средство диагностики репликации	Repadmin.exe	Управляет репликацией из командной строки
Диспетчер доменов Windows	Netdom.exe	Управляет доменом и доверительными отношениями из командной строки

Active Directory — пользователи и компьютеры (Active Directory Users And Computers)

Консоль **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** основной инструмент для управления Active Directory. Она позволяет решать любые задачи, связанные с пользователями, группами и компьютерами, а также управлять подразделениями.

Для запуска консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** необходимо выбрать одноименную команду в меню **Администрирование (Administrative Tools)**. Кроме того, можно добавить оснастку **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** в любую обновляемую консоль.

Знакомство с консолью Active Directory — пользователи и компьютеры (Active Directory Users And Computers)

По умолчанию консоль **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** работает с доменом, к которому вы подключены в данный момент. Доступ к объектам компьютера или пользователя в данном домене открывает дерево консоли (рис. 8-1). Если вы не находите нужный контроллер домена или если нужный домен не отображен, вам необходимо подключиться к контроллеру домена в текущем или другом домене. К другим высокоуровневым задачам, которые выполняются посредством этой консоли, относятся просмотр дополнительных параметров и поиск объектов.

В консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** имеется следующий стандартный набор узлов:

- **Сохраненные запросы (Saved Queries)** Содержит сохраненные критерии поиска, что позволяет быстро проводить уже выполнявшиеся запросы к Active Directory.
- **Builtin** Список встроенных учетных записей пользователей.
- **Computers** Стандартный контейнер для учетных записей компьютеров.
- **Domain Controllers** Стандартный контейнер для контроллеров доменов.

- **ForeignSecurityPrincipals** Содержит информацию об объектах из доверенного внешнего домена. Обычно такие объекты создаются, когда в группу текущего домена добавляется объект из внешнего домена.
- **Users** Стандартный контейнер для пользователей.

В консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** имеются дополнительные возможности, не отображаемые по умолчанию. Для доступа к этим возможностям выберите в меню **Вид (View)** команду **Дополнительные компоненты (Advanced Features)**. Вы увидите следующие дополнительные узлы:

- **LostAndFound** Объекты без владельца. Вы можете удалить или восстановить их.
- **NTDS Quotas** Данные о квотах службы каталогов.
- **Program Data** Сохраненные данные Active Directory для приложений Microsoft.
- **System** Встроенные параметры системы.

Кроме того, сюда же добавляются папки подразделений. На рис. 8-1 в домен добавлено пять подразделений: Поддержка, Инженеры, Маркетинг, Продажи и Технологи.

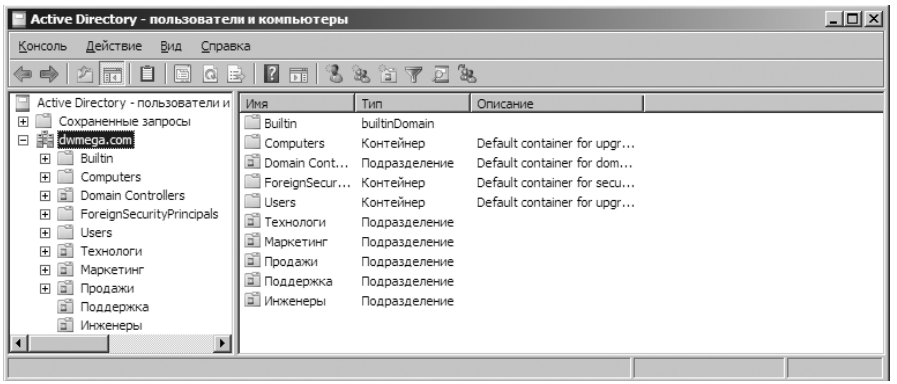


Рис. 8-1. Консоль Active Directory — пользователи и компьютеры (Active Directory Users And Computers) позволяет получать доступ к объектам компьютеров и пользователей

Подключение к контроллеру домена

Подключение к контроллеру домена преследует несколько целей. Если при открытии консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** вы не видите никаких объектов, подключение к контроллеру домена позволит вам получить доступ к его объектам пользователей, групп и компьютеров. Подключение к контроллеру домена может понадобиться при возникновении подозрений о неправильной репликации, когда вам нужно изучить объекты на том или ином контроллере. Установив подключение, вы увидите несоответствия в недавно обновленных объектах.

Чтобы подключиться к контроллеру домена, выполните следующие действия:

1. В дереве консоли щелкните правой кнопкой элемент **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** и выберите команду **Сменить контроллер домена (Change Domain Controller)**.
2. В диалоговом окне **Смена сервера каталогов (Change Domain Controller)**, показанном на рис. 8-2, будет отображен текущий домен и контроллер домена, с которым вы работаете.

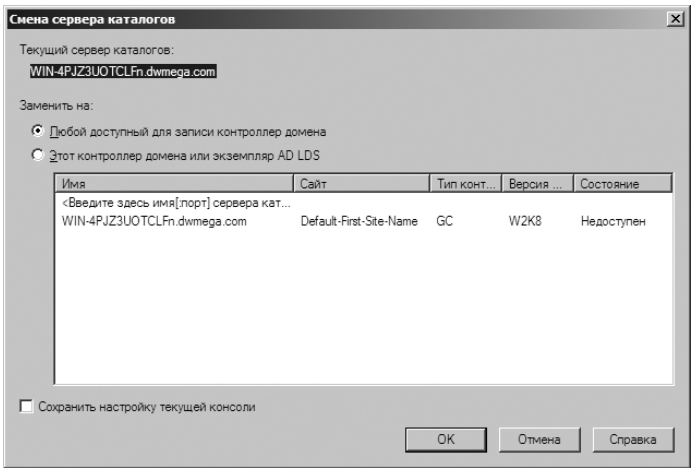


Рис. 8-2. Окно для выбора нового контроллера домена

3. В списке **Заменить на (Change To)** перечислены доступные контроллеры домена. По умолчанию установлен переключатель **Любой доступный для записи контроллер домена (Any Writable Domain Controller)**. Выбрав этот вариант, вы подключитесь к первому ответившему на ваш запрос контроллеру домена. Если же этот вариант неприемлем, укажите конкретный контроллер домена, к которому хотите подключиться.
4. Чтобы использовать выбранный контроллер при каждом запуске консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**, установите флажок **Сохранить настройку текущей консоли (Save This Setting For The Current Console)**.
5. Щелкните **OK**.

Примечание В диалоговом окне **Смена сервера каталогов (Change Domain Controller)** отображается сайт, связанный с контроллерами доменов, а также информация о типе, версии и состоянии контроллера домена. Если в столбце типа контроллера стоит GC, значит, контроллер содержит глобальный каталог.

Подключение к домену

Консоль **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** позволяет работать с любым доменом леса при нали-

чии соответствующих разрешений. Для подключения к домену выполните следующие действия:

1. В дереве консоли щелкните правой кнопкой **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** и выберите команду **Сменить домен (Change Domain)**.
2. В диалоговом окне **Смена домена (Change Domain)** отображен текущий домен или домен по умолчанию. Введите новое имя домена или найдите новый домен при помощи кнопки **Обзор (Browse)**. Затем щелкните **OK**.
3. Если вы хотите всегда использовать этот домен при работе с консолью **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**, установите флажок **Сохранить этот параметр домена для этой консоли (Save This Domain Setting For The Current Console)**.
4. Щелкните **OK**.

Поиск учетных записей и общих ресурсов

Консоль **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** обладает встроенной функцией поиска, с помощью которой можно найти учетные записи, общие ресурсы и другие объекты каталога.

Чтобы провести поиск объекта в каталоге, выполните следующие действия:

1. В дереве консоли щелкните правой кнопкой текущий домен или конкретный контейнер, в котором хотите провести поиск, и выберите команду **Найти (Find)**. Откроется диалоговое окно **Поиск (Find)**, показанное на рис. 8-3.

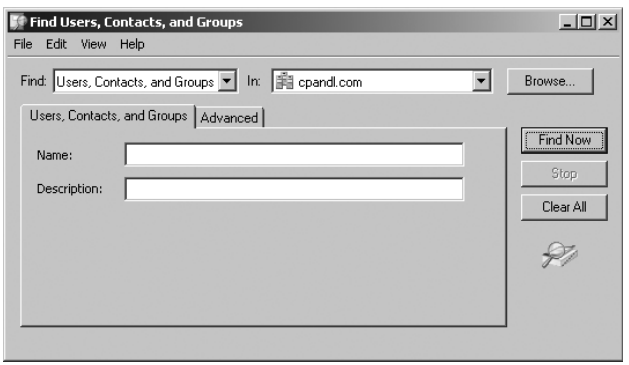


Рис. 8-3. Поиск ресурсов Active Directory

2. В списке **Найти (Find)** укажите желаемый тип поиска. Доступны следующие варианты:
   - **Пользователи, контакты и группы (Users, Contacts And Groups)** Поиск учетных записей пользователей и групп, а также контактов, перечисленных в службе каталогов.

- **Компьютеры (Computers)** Поиск учетных записей компьютеров по типу, имени и владельцу.
- **Принтеры (Printers)** Поиск принтеров по имени, модели и возможностям.
- **Общие папки (Shared Folders)** Поиск общих папок по имени или ключевым словам.
- **Организационные подразделения (Organizational Units)** Поиск подразделений по имени.
- **Пользовательский поиск (Custom Search)** Расширенный поиск или запрос по протоколу LDAP.
- **Общие запросы (Common Queries)** Быстрый поиск учетных записей по именам и описаниям, отключенных учетных записей, паролей с неограниченным сроком действия и по числу дней с момента последнего входа в систему.

3. В списке **Где (In)** укажите расположение, в котором хотите провести поиск. Если ранее вы щелкнули правой кнопкой контейнер, например, **Computers**, этот контейнер выбран по умолчанию. Чтобы провести поиск по всем объектам каталога, щелкните **Целиком Active Directory (Entire Directory)**.
4. Введите критерии поиска и щелкните **Найти (Find Now)**. Пример результатов поиска показан на рис. 8-4. Для просмотра или изменения свойств объекта дважды щелкните его. Для отображения контекстного меню с командами управления объектом щелкните его правой кнопкой.

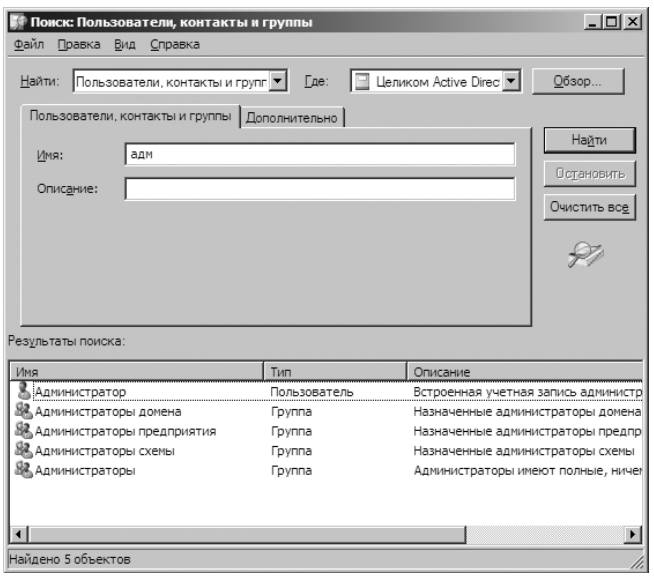


Рис. 8-4. Совпадения отображаются в результатах поиска. Для управления ими достаточно щелкнуть правой кнопкой выбранный объект

Примечание Доступные поля и вкладки в диалоговом окне **Поиск (Find)** определяются выбранным типом поиска. В большинстве случаев достаточно просто ввести имя искомого объекта в поле **Имя (Name)**. Однако существуют и другие возможности поиска. Например, вы можете выполнить поиск цветного принтера, принтера с возможностью печати на обеих сторонах листа, принтера, способного скреплять бумагу, и т. д.

Управление учетными записями компьютеров

Учетные записи компьютеров хранятся в Active Directory в качестве объектов. Они используются для регулирования доступа к сети и ее ресурсам. Вы можете добавлять учетные записи компьютеров в любой контейнер консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**, но наиболее подходят для этой цели контейнеры **Computers**, **Domain Controllers**, а также созданные вами подразделения.

Создание учетной записи компьютера на рабочей станции или сервере

Проще всего создать учетную запись компьютера следующим образом — войти на компьютер, который вы хотите настроить, и присоединить его к домену, как описано в разделе «Присоединение компьютера к домену или рабочей группе» этой главы. При этом необходимая учетная запись создается автоматически и помещается в контейнер **Computers** или **Domain Controllers** в соответствии со статусом компьютера. Кроме того, вы можете создавать учетные записи компьютеров непосредственно в консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**.

Создание учетных записей компьютеров в консоли Active Directory — пользователи и компьютеры (Active Directory Users And Computers)

Учетные записи компьютеров бывают двух типов: стандартные и управляемые. С помощью консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** вы легко создадите стандартную учетную запись компьютера, выполнив следующие действия:

1. В дереве консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** щелкните правой кнопкой контейнер, в котором хотите разместить учетную запись.
2. Выберите команды **Создать (New)** и **Компьютер (Computer)**. Откроется мастер Новый объект — Компьютер (New Object — Computer Wizard), показанный на рис. 8-5. Введите имя клиентского компьютера.
3. По умолчанию правом присоединять компьютеры к домену обладают только члены группы Администраторы домена (Domains Admins). Чтобы разрешить другим пользователям или группам присоединять компьютер к домену, щелкните кнопку **Изменить (Change)** и выберите учетную запись пользователя или группы в диалоговом окне **Выбор: «Пользователь» или «Группа» (Select User Or Group)**.

Примечание Вы вольны выбрать любую учетную запись пользователя или группы. Это позволяет предоставить другим пользователям право присоединить компьютер к домену.

4. Если использовать данную учетную запись могут системы под управлением Windows NT, установите флажок **Назначить учетной записи статус пред-Windows 2000 (Assign This Computer Account As A Pre–Windows 2000 Computer)**.
5. Два раза щелкните **Далее (Next)**, а затем **Готово (Finish)**.

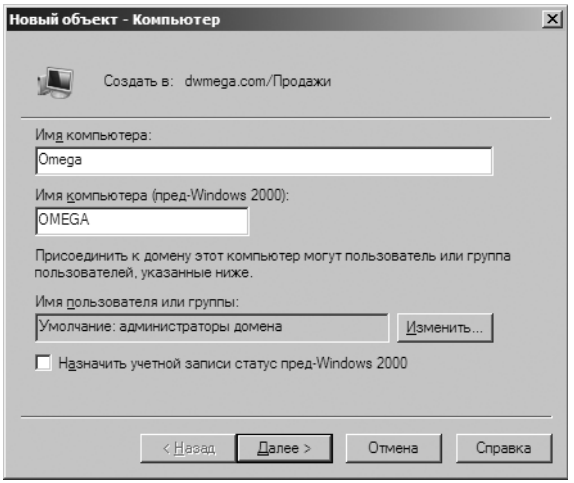


Рис. 8-5. Создание новой учетной записи компьютера

Управляемые (managed) учетные записи компьютеров используются для предварительной настройки компьютеров, которые предполагается настраивать автоматически при помощи серверов удаленной установки и служб развертывания Windows. Чтобы создать управляемую учетную запись компьютера в консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**, выполните следующие действия:

1. Выполните шаги 1–4 из предыдущей процедуры. Щелкните **Далее (Next)**, чтобы открыть страницу **Управляемый (Managed)**.
2. Установите флажок **Это управляемый компьютер (This Is A Managed Computer)** и введите идентификатор GUID/UUID компьютера. Значение GUID/UUID можно найти в системе BIOS; иногда его указывают на корпусе компьютера. Щелкните **Далее (Next)**.
3. На странице **Хост-сервер (Host Server)** укажите хост-сервер, который будет использоваться для удаленной установки, или разрешите использовать для удаленной установки любой доступный хост-сервер. Чтобы выбрать хост-сервер, установите переключатель **Следующий сервер удаленной установки (The Following Remote Installation Server)** и щелкните кнопку **Найти (Find)**. В диалоговом окне **Поиск (Find)** щелкните **Найти (Find Now)** для отображения списка доступных серверов удален-

ной установки. Выделите хост-сервер, который хотите использовать, и щелкните **OK**.

4. Щелкните **Далее (Next)** и **Готово (Finish)**.

Просмотр и редактирование свойств учетной записи компьютера

Чтобы просмотреть и отредактировать учетную запись компьютера, выполните следующие действия:

1. Откройте консоль **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**. В дереве консоли разверните узел домена.
2. Выберите контейнер подразделения, в котором расположена нужная учетная запись.
3. Щелкните правой кнопкой учетную запись, с которой собираетесь работать, и выберите команду **Свойства (Properties)**. Откроется диалоговое окно свойств, в котором вы сможете просмотреть и редактировать параметры.

Удаление, отключение и включение учетных записей компьютеров

Если вы более не нуждаетесь в учетной записи компьютера, вы можете навсегда удалить ее из Active Directory или временно отключить, а позднее снова включить и использовать.

Чтобы удалить, отключить или включить учетную запись компьютера, выполните следующие действия:

1. Откройте консоль **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**. В дереве консоли выберите контейнер, в котором расположена нужная учетная запись. Щелкните учетную запись правой кнопкой.
2. Выберите команду **Удалить (Delete)**, чтобы навсегда удалить учетную запись. Щелкните **Да (Yes)**, чтобы подтвердить удаление.
3. Выберите команду **Отключить учетную запись (Disable Account)**, чтобы временно отключить учетную запись. Щелкните **Да (Yes)**, чтобы подтвердить отключение.
4. Выберите команду **Включить учетную запись (Enable Account)**, чтобы включить учетную запись для дальнейшего использования.

Совет Если учетная запись в данный момент используется, вам, вероятно, не удастся ее отключить. Попробуйте выключить компьютер или прекратить его сеанс в узле **Сеансы (Sessions)** консоли **Управление компьютером (Computer Management)**.

Сброс заблокированных учетных записей компьютера

Учетные записи компьютеров обладают паролями, как и учетные записи пользователей. Но, в отличие от пользовательских учетных записей, управление и обслуживание учетных записей компьютеров производится автоматически. На компьютерах домена хранятся пароль учетной записи компьютера, который по умолчанию меняется каждые 30 дней, и пароль защищенного канала,

который служит для установки защищенного подключения к контроллерам домена. По умолчанию пароль защищенного канала также обновляется каждые 30 дней. Оба пароля должны быть синхронизованы. В случае сбоя в синхронизации паролей компьютеру не удастся войти в домен, а в службе Netlogon будет зарегистрировано сообщение об ошибке проверки подлинности при входе в домен с идентификатором события 3210 или 5722.

В этом случае необходимо переустановить пароль учетной записи компьютера. Щелкните правой кнопкой учетную запись компьютера в консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** и выберите команду **Переустановить учетную запись (Reset Account)**. Далее удалите компьютер из домена (сделав его членом рабочей группы или другого домена), а затем снова присоедините его к домену. Для переустановки пароля учетной записи компьютера можно также использовать утилиту командной строки NETDOM. Дополнительные сведения вы найдете в статье 325850 Базы знаний Майкрософт (*http://support.microsoft.com/default.aspx?scid=kb;en-us;325850*).

Чтобы переустановить пароль учетной записи рядового сервера, выполните следующие действия:

1. Локально войдите на компьютер. В командной строке введите **netdom resetpwd /s:ИмяСервера /ud:домен\ИмяПользователя /pd:***, где *ИмяСервера* — имя контроллера домена, который следует использовать для переустановки пароля, *домен\ИмяПользователя* определяет учетную запись администратора, обладающую правом изменять пароль, а символ * указывает, что для продолжения следует ввести пароль учетной записи.
2. Введите пароль администратора. Утилита NETDOM изменит пароль учетной записи компьютера локально и на контроллере домена. После этого контроллер домена распространит измененный пароль на другие контроллеры данного домена.
3. Перезагрузите компьютер.

На контроллере домена потребуется выполнить дополнительные шаги. Выполнив локальный вход, вы должны остановить службу Центр распространения ключей Kerberos (Kerberos Key Distribution Center) и задать для нее ручной запуск. Перезапустив компьютер и убедившись в успешности переустановки пароля, снова запустите службу Центр распространения ключей Kerberos (Kerberos Key Distribution Center) и задайте для нее автоматический запуск.

Перемещение учетных записей компьютеров

Учетные записи компьютеров обычно размещаются в контейнерах **Computers**, **Domain Controllers** или контейнерах подразделений, созданных пользователем. Чтобы переместить учетную запись в другой контейнер, выделите ее в консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** и перетащите ее в новое расположение с помощью мыши.

Кроме того, учетные записи компьютеров можно переместить следующим способом:

1. Откройте консоль **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**.
2. В дереве консоли щелкните контейнер, в котором расположена учетная запись компьютера.
3. Щелкните нужную учетную запись правой кнопкой и выберите команду **Переместить (Move)**. Откроется одноименное диалоговое окно, показанное на рис. 8-6.
4. В диалоговом окне **Переместить (Move)** разверните узел домена и выберите контейнер, в который хотите переместить учетную запись. Щелкните **OK**.

Рис. 8-6. Диалоговое окно Переместить (Move) позволяет перемещать учетные записи компьютера в другие контейнеры

Управление компьютерами

Назначение консоли **Управление компьютером (Computer Management)** однозначно вытекает из ее названия. Чтобы открыть консоль **Управление компьютером (Computer Management)** для конкретного компьютера из консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**, щелкните нужный компьютер правой кнопкой и выберите команду **Управление (Manage)**. Консоль **Управление компьютером (Computer Management)** автоматически установит соединение с выбранным компьютером.

Присоединение компьютера к домену или рабочей группе

Присоединение к домену или рабочей группе позволяет компьютеру под управлением Windows NT, Windows 2000, Windows XP, Windows Server 2003 или Windows Server 2008 авторизоваться и получать доступ к сети. Компьютеры под управлением Windows 95 и Windows 98 не нуждаются в учетной записи компьютера и не могут быть присоединены к домену. Вы

должны настроить компьютер под управлением Windows 95 и Windows 98 как клиент Active Directory.

Прежде всего убедитесь, что на компьютере корректно установлены сетевые компоненты. Они должны настраиваться в процессе установки операционной системы. Подробно о настройке сетевых подключений TCP/IP вы прочитаете в главе 17. Параметры TCP/IP должны обеспечивать связь между настраиваемым компьютером и контроллером домена. Если в сети настроены DHCP, WINS и DNS, рабочая станция не нуждается в присвоении статического IP-адреса и особом конфигурировании. Требуются только имя компьютера и имя домена, которые можно указать во время присоединения компьютера к домену.

Ближе к реальности Система Widows Server 2008 автоматически разрешает добавлять рабочие станции к домену всем членам неявной группы Прошедшие проверку (Authenticated Users). Это означает, что любой пользователь, вошедший в домен и прошедший проверку, может добавлять в домен рабочие станции, не обладая административными полномочиями. Однако в целях предосторожности число рабочих станций, которые пользователь может добавить в домен, ограничено десятью. Превысив этот предел, пользователь увидит сообщение об ошибке, причем на компьютерах под управлением Windows NT в сообщении говорится, что данная учетная запись компьютера не существует или недоступна. На рабочих станциях под управлением Windows 2000 или Windows XP сообщение более корректно и извещает пользователя, что компьютер не может быть присоединен к домену, поскольку пользователь превысил максимальное число учетных записей компьютеров, которые ему разрешено присоединить к этому домену. При помощи утилиты Ldp.exe из комплекта Windows Server 2008 Support Tools вы можете повысить лимит (заданный атрибутом *ms-DS-MachineAccountQuota*) на число компьютеров, которые зарегистрированный пользователь может присоединить к домену, но с точки зрения безопасности делать это не следует. Предпочтительнее заранее создать учетную запись компьютера в конкретном подразделении или предоставить пользователю дополнительное разрешение безопасности на создание объектов-компьютеров в определенном подразделении.

В процессе установки ОС сетевое подключение для вашего компьютера, возможно, уже было создано. Возможно также, что вы ранее уже присоединили компьютер к домену или рабочей группе. В этом случае вы можете присоединить компьютер к новому домену или рабочей группе. О том, как присоединить к домену компьютер под управлением Windows Vista или Windows Server 2008, читайте в разделе «Вкладка Имя компьютера (Computer Name)» главы 3. Этот процесс почти идентичен настройке компьютеров под управлением Windows 2000 Professional, Windows 2000 Server, Windows XP Professional и Windows Server 2003.

Если изменение имени прошло неудачно, на экране появится сообщение об этом или сообщение о том, что учетная запись уже существует. Подобная проблема может возникнуть при попытке изменения имени компьютера, присоединенного к домену, во время сеанса его работы в домене. Закройте приложения, которые могут использовать подключение к домену, например, проводник Windows, в котором открытая общая папка, и повторите переименование.

При возникновении других проблем в процессе присоединения компьютера к домену проверьте сетевую конфигурацию настраиваемого компьютера. На компьютере должны быть установлены сетевые службы, а в свойствах TCP/IP должны быть правильно заданы параметры DNS-сервера (подробнее — в главе 17).

Управление контроллерами домена, ролями и каталогами

В доменах Active Directory контроллеры домена выполняют множество важных функций, многие из которых уже затрагивались в главе 7.

Установка и понижение контроллеров домена

Установка контроллера домена состоит в настройке доменных служб Active Directory на рядовом сервере. Позднее, если вы более не хотите, чтобы сервер выполнял задачи контроллера, вы можете понизить его, и он снова станет рядовым сервером. Процессы установки и понижения серверов схожи, однако, приступая к работе, подумайте о том, как ваши действия повлияют на сеть, и прочитайте раздел «Структура каталога» главы 7.

Во время установки контроллера домена вам, скорее всего, придется перенести роли хозяина операций и перестроить структуру глобального каталога. Кроме того, перед установкой доменных служб Active Directory в сети уже должна работать служба DNS. Аналогично, перед понижением контроллера домена вы должны передать все основные обязанности этого контроллера другим контроллерам домена. Это означает перемещение глобального каталога и, при необходимости, передачу ролей хозяина операций. Вам также придется удалить все разделы каталогов приложений, существующие на сервере.

Ближе к реальности Следует отметить, что в Windows Server 2003 и Windows Server 2008 для переименования контроллера домена его не нужно понижать. Вы вольны переименовать контроллер домена в любое время. Единственная проблема заключается в том, что в процессе переименования сервер недоступен для пользователей, и вам, скорее всего, придется принудительно обновить каталог, чтобы заново установить связи клиентов с сервером. Переместить контроллер домена в другой домен нельзя. Вы должны сначала понизить его, обновить параметры принадлежности к домену на сервере и его учетную запись, а затем снова назначить сервер контроллером домена.

Чтобы установить контроллер домена, выполните следующие действия:

1. Зарегистрируйтесь на сервере, который хотите настроить. Выделите узел **Роли (Roles)** и щелкните ссылку **Добавить роли (Add Roles)** в правой панели диспетчере сервера. Откроется Мастер добавления ролей (Add Roles Wizard). Если первой страницей мастера является страница **Перед началом работы (Before You Begin)**, прочитайте ее и щелкните **Далее (Next)**.
2. На странице **Выбор ролей сервера (Select Server Roles)** установите флажок **Доменные службы Active Directory (Active Directory Domain Services)**, затем дважды щелкните **Далее (Next)** и **Установить (Install)**.

3. Щелкните кнопку **Пуск (Start)**, введите **dcpromo** в поле **Начать поиск (Search)** и нажмите Enter. Откроется Мастер установки доменных служб Active Directory (Active Directory Domain Services Installation Wizard).
4. Если в данный момент компьютер является рядовым сервером, мастер поможет вам установить Active Directory. Вам предстоит указать, будет компьютер контроллером в новом домене или дополнительным контролером в уже существующем домене. Для проверки правильности установки контроллера домена выполните следующее: проверьте журнал событий Служба каталогов (Directory Service) на наличие ошибок, убедитесь, что клиенты имеют доступ к папке Sysvol, убедитесь в работоспособности системы разрешения имен на сервере DNS, а также проверьте репликацию изменений в Active Directory.

Чтобы понизить контроллер домена, выполните следующие действия:

1. Зарегистрируйтесь на сервере, который хотите настроить. Щелкните кнопку **Пуск (Start)**, введите **dcpromo** в поле **Начать поиск (Search)** и нажмите Enter. Откроется Мастер установки доменных служб Active Directory (Active Directory Domain Services Installation Wizard).
2. Если в данный момент компьютер является контроллером домена, мастер понизит его. После понижения компьютер будет работать как рядовой сервер.
3. В диспетчере сервера выберите узел **Роли (Roles)** и щелкните ссылку **Удалить роли (Remove Roles)** в правой панели. Откроется Мастер удаления ролей (Remove Roles Wizard). Если первой страницей мастера является страница **Перед началом работы (Before You Begin)**, прочитайте ее и щелкните **Далее (Next)**.
4. На странице **Удаление ролей сервера (Remove Server Roles)** сбросьте флажок **Доменные службы Active Directory (Active Directory Domain Services)**, затем дважды щелкните **Далее (Next)**. Когда удаление завершится, щелкните **Готово (Finish)**.

Внимание! При понижении сервера с помощью DCPROMO выполняется плавная передача всех ролей сервера. В статье 332199 Базы знаний Майкрософт рассказывается о том, как выполнить принудительное понижение с использованием команды **dcpromo /forceremoval**. После применения этой команды роли FSMO остаются на пониженном сервере в неработоспособном состоянии, пока не будут заново назначены администратором. Если вы принудительно понижаете контроллер домена и операция понижения заканчивается неудачей, данные домена могут оказаться в рассогласованном состоянии. О том, как решить эту проблему, читайте в статье 216498 Базы знаний Майкрософт (*http://support.microsoft.com/kb/216498/en-us*).

Ближе к реальности Альтернативный способ настройки контроллеров домена — установка с диска резервного копирования. Это новинка Windows Server 2003 и Windows Server 2008. Чтобы установить контроллер домена с диска резервного копирования, создайте резервную копию данных о состоянии системы контроллера домена и восстановите их на другом сервере, работающем под управлением Windows Server 2003 или Windows Server 2008. Создавая контроллер домена с диска резервного копирования, вы

избавляетесь от необходимости реплицирования на новый контроллер домена всей БД каталога по сети. Это без преувеличения может сэкономить вам день работы, если у вас ограниченная полоса пропускания и БД каталога содержит тысячи записей.

Просмотр и передача ролей уровня домена

Для просмотра и изменения расположения ролей хозяина операций уровня домена используется консоль **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**. На уровне домена вы можете работать с ролями хозяина пула RID, эмулятора PDC и хозяина инфраструктуры.

Примечание О ролях хозяина операций рассказывается в разделе «Роли хозяина операций» главы 7. Для установки роли хозяина именования доменов используйте консоль **Active Directory — домены и доверие (Active Directory Domains And Trusts)**, а для изменения роли хозяина схемы — консоль **Схема Active Directory (Active Directory Schema)**. Проще всего определить текущее распределение ролей FSMO, введя в командной строке **netdom query fsmo**.

Чтобы просмотреть текущее распределение ролей хозяина операций, выполните следующие действия:

1. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** щелкните правой кнопкой узел **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**. В контекстном меню выберите команды **Все задачи (All Tasks)** и выберите **Хозяева операций (Operations Masters)**. Откроется диалоговое окно **Хозяева операций (Operations Masters)**, показанное на рис. 8-7.

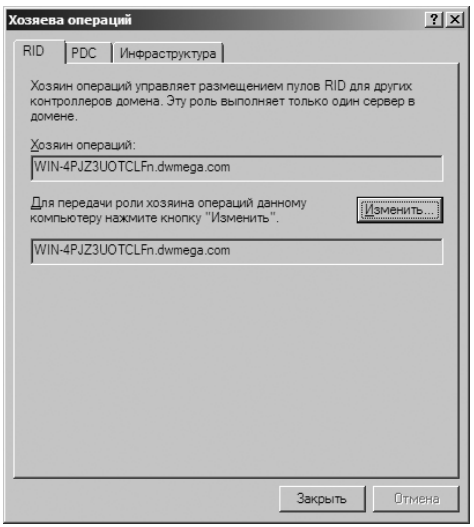


Рис. 8-7. В диалоговом окне Хозяева операций (Operations Masters) можно переместить роли хозяина операций на другие компьютеры или просто просмотреть их текущее расположение

2. В диалоговом окне **Хозяева операций (Operations Masters)** три вкладки. На вкладке **RID** отображено расположение текущего хозяина пула RID. На вкладке **PDC** показано расположение текущего эмулятора PDC. Вкладка **Инфраструктура (Infrastructure)** служит для отображения текущего хозяина инфраструктуры.

Чтобы переместить текущие роли хозяина операций, выполните следующие действия:

1. Запустите консоль **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**. В дереве консоли щелкните правой кнопкой узел **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** и выберите команду **Сменить контроллер домена (Change Domain Controller)**.
2. В диалоговом окне **Смена сервера каталогов (Change Domain Controller)** установите переключатель **Этот контроллер домена (This Domain Controller)**, выберите контроллер, которому хотите передать роль хозяина операций и щелкните **OK**.
3. В дереве консоли щелкните правой кнопкой узел **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**. В контекстном меню выберите команды **Все задачи (All Tasks)** и **Хозяева операций (Operations Masters)**.
4. В диалоговом окне **Хозяева операций (Operations Masters)** перейдите на вкладку **RID**, **PDC** или **Инфраструктура (Infrastructure)** в соответствии с ролью, которую собираетесь передать.
5. Для передачи роли на другой контроллер домена щелкните кнопку **Изменить (Change)**. Щелкните **OK**.

Просмотр и передача роли хозяина именования доменов

Для просмотра или изменения расположения роли хозяина именования доменов в лесе доменов используйте консоль **Active Directory — домены и доверие (Active Directory Domains And Trusts)**. Текущий домен отображается в корневом уровне дерева этой консоли.

Совет Чтобы подключиться к другому домену, установите подключение к контроллеру домена, выполнив шаги, описанные в разделе «Подключение к контроллеру домена» этой главы. Разница заключается лишь в том, что в данном случае вы щелкаете правой кнопкой узел **Active Directory — домены и доверие (Active Directory Domains And Trusts)** в дереве консоли.

Чтобы передать роль хозяина именования доменов, выполните следующие действия:

1. Откройте консоль **Active Directory — домены и доверие (Active Directory Domains And Trusts)**. В дереве консоли щелкните правой кнопкой узел **Active Directory — домены и доверие (Active Directory Domains And Trusts)** и выберите **Сменить контроллер домена Active Directory (Change Active Directory Domain Controller)**.

2. В диалоговом окне **Смена сервера каталогов (Change Active Directory Domain Controller)** установите переключатель **Этот контроллер домена (This Domain Controller)**, затем выберите контроллер домена, которому хотите передать роль хозяина именования доменов, и щелкните **OK**.
3. В дереве консоли щелкните правой кнопкой узел **Active Directory — домены и доверие (Active Directory Domains And Trusts)** и выберите команду **Хозяин операций (Operations Master)**. Откроется диалоговое окно **Хозяин операций (Change Operations Master)**.
4. В поле **Хозяин именования доменов (Domain Naming Operations Master)** отображен текущий хозяин именования доменов. Для передачи роли на ранее выбранный контроллер домена щелкните кнопку **Сменить (Change)**.
5. Щелкните **Закрыть (Close)**.

Просмотр и передача роли хозяина схемы

Для просмотра или изменения расположения роли хозяина схемы используется консоль **Схема Active Directory (Active Directory Schema)**, поставляемая с Windows Server 2008. Перед ее использованием введите в командной строке **regsvr32 schmmgmt.dll**. Затем выполните передачу роли хозяина схемы, выполнив следующие действия:

1. Добавьте оснастку **Схема Active Directory (Active Directory Schema)** в консоль MMC.
2. В дереве консоли щелкните правой кнопкой узел **Схема Active Directory (Active Directory Schema)** и выберите команду **Сменить контроллер домена Active Directory** (**Change Domain Controller**).
3. Установите переключатель **Любой доступный для записи контроллер домена (Any Domain Controller)**, чтобы предоставить Active Directory самостоятельно выбрать хозяин схемы. Или же выделите вариант **Введите здесь имя (Specify Name)** и введите имя нового хозяина схемы, например, **zeta.seattle.cpandl.com**.
4. Щелкните **OK**. В дереве консоли щелкните правой кнопкой узел **Схема Active Directory (Active Directory Schema)** и выберите **Хозяин операций (Operations Master)**.
5. В диалоговом окне **Смена хозяина схемы (Change Schema Master)** щелкните **Сменить (Change)**. Затем щелкните **OK** и **Закрыть (Close)**.

Передача ролей из командной строки

Еще один способ передачи ролей — использование утилиты NETDOM. Она применяется для перечисления текущих обладателей ролей FSMO и их передачи посредством Ntdsutil.exe. Утилита командной строки Ntdsutil.exe предназначена для управления Active Directory. Для передачи ролей при помощи командной строки выполните следующие действия:

1. Получите список текущих обладателей ролей FSMO. Для этого введите в командной строке **netdom query fsmo**.
2. Рекомендуется входить в систему с консоли сервера, который вы хотите назначить новым хозяином операций. Вы можете входить на консоль локально или с использованием удаленного рабочего стола.
3. Щелкните **Пуск (Start)**, выберите команду **Выполнить (Run)**, введите **cmd** в поле **Открыть (Open)** и щелкните **OK**.
4. В командной строке введите **ntdsutil**. Откроется командная строка этой утилиты.
5. Введите **roles**, переведя утилиту в режим обслуживания хозяев операций.
6. В приглашении *fsmo maintenance* введите **connections**. В приглашении *server connections* введите **connect to server** и укажите FQDN-имя контроллера домена, которому вы собираетесь назначить роль FSMO, например:

```
connect to server engdc01.technology.adatum.com
```

7. Установив подключение, введите команду **quit**, чтобы выйти из приглашения *server connections*. Затем в приглашении *fsmo maintenance* введите **transfer** и идентификатор передаваемой роли:
   - **pdc** эмулятор PDC;
   - **rid master** хозяин пула RID;
   - **infrastructure master** хозяин инфраструктуры;
   - **schema master** хозяин схемы;
   - **domain naming master** хозяин именования доменов.
8. В приглашении *fsmo maintenance* введите **quit**, затем введите **quit** в приглашении *ntdsutil*.

Захват ролей при помощи командной строки

Порой вы оказываетесь в ситуации, когда безболезненная передача серверных ролей невозможна, например, при выходе из строя диска на контроллере домена, выступающем в роли хозяина пула RID. Если быстро «оживить» сервер не удается, вам, скорее всего, придется выполнить захват роли хозяина пула RID и назначить ее другому контроллеру домена.

Внимание! Захват серверной роли — серьезная операция, которую следует использовать только в качестве последнего средства, если контроллер домена, управляющий данной ролью, недоступен продолжительное время. Единственный способ вернуть роль на исходный сервер — форматирование загрузочного диска и переустановка Windows Server 2008. После захвата роли FSMO контролера, которого более нет в домене, вы должны удалить из Active Directory связанные с ним данные. Дополнительные сведения вы найдете в статье 216498 Базы знаний Майкрософт (*http://support.microsoft.com/default.aspx?scid=kb;en-us;216498*).

Не выполняйте захват роли, пока не убедитесь, что информация на конечном контроллере домена актуальна по сравнению с информацией на

бывшем владельце роли. Служба каталогов Active Directory отслеживает изменения при репликации при помощи порядковых номеров обновления (USN). Поскольку репликация требует времени, может случиться так, что в какой-то момент времени будут обновлены не все контроллеры. Сравнив номер USN контроллера домена с аналогичными номерами на других серверах домена, вы установите, обновлен ли контроллер домена по отношению к предыдущему владельцу роли. Если контроллер домена обновлен, спокойно перемещайте роль. Если нет, подождите окончания репликации, после чего перемещайте роль на контроллер домена.

В систему Windows Server 2008 входит утилита Repadmin для работы с репликацией Active Directory. Чтобы отобразить наивысший USN для указанного контекста именования на каждом партнере репликации для определенного контроллера домена, введите в командной строке следующую команду:

```
repadmin /showutdvec ИмяКонтроллераДомена Контекст
```

Здесь *ИмяКонтроллераДомена* — FQDN-имя контролера домена, а *Контекст* — различающееся имя домена, в котором находится сервер, например:

```
repadmin /showutdvec server252.cpandl.com dc=cpandl,dc=com
```

Команда отображает наивысший номер USN среди партнеров по репликации раздела домена:

```
Default-First-Site-Name\SERVER252 @ USN 45164 @ Time 2008-03-30 14:25:36

Default-First-Site-Name\SERVER147 @ USN 45414 @ Time 2008-03-30 14:25:36
```

Если Server252 был предыдущим владельцем роли, а контроллер домена, который вы проверяете, обладает равным или большим номером USN, чем Server252, то контроллер домена обновлен. Если проверяемый контроллер домена обладает меньшим номером USN, чем Server252, сервер не обновлен, и вам следует подождать выполнения репликации до проведения захвата роли. Вы также можете провести принудительную репликацию контроллера домена при помощи команды **Repadmin /Syncall**.

Для захвата роли выполните следующие действия:

1. В командной строке введите **netdom query fsmo**, чтобы выяснить текущее распределение ролей FSMO.
2. Убедитесь, что контроллер домена, владеющий ролью, захват которой вы собираетесь выполнить, действительно недоступен. Если сервер можно вернуть в оперативный режим, не проводите захват (если, конечно, не собираетесь в любом случае полностью переустанавливать данный сервер).
3. Рекомендуется входить в систему с консоли сервера, который вы хотите назначить новым хозяином операций. Вы можете входить на консоль локально или с использованием удаленного рабочего стола.
4. Откройте окно командной строки.

5. В командной строке введите **ntdsutil**.
6. В приглашении *ntdsutil* введите **roles**, чтобы перейти в режим обслуживания хозяев операций.
7. В приглашении *fsmo maintenance* введите **connections**. В приглашении *server connections* введите **connect to server** и укажите FQDN-имя контроллера домена, которому собираетесь назначить роль FSMO, например:

```
connect to server engdc01.technology.adatum.com
```

8. Установив подключение, введите команду **quit**, чтобы выйти из приглашения *server connections*. В приглашении *fsmo maintenance* введите **seize** и идентификатор роли, захват которой выполняется:
   - **pdc** эмулятор PDC;
   - **rid master** хозяин пула RID;
   - **infrastructure master** хозяин инфраструктуры;
   - **schema master** хозяин схемы;
   - **domain naming master** хозяин именования доменов.
9. В приглашении *fsmo maintenance* введите **quit**, затем введите **quit** в приглашении *ntdsutil*.

Настройка глобального каталога

Глобальные каталоги играют в сети важнейшую роль, которая рассматривается в разделе «Структура каталога» главы 7. Настройка дополнительных глобальных каталогов производится путем предоставления контроллерам домена разрешения на размещение глобального каталога. Если оказалось, что в пределах одного сайта у вас есть несколько глобальных каталогов, вы, возможно, захотите отказаться от размещения глобального каталога на одном из контроллеров. Для этого глобальный каталог нужно отключить.

Чтобы включить или выключить глобальный каталог, выполните следующие действия:

1. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** разверните сайт, с которым хотите работать.
2. Разверните папку **Servers** этого сайта и выберите сервер, на котором хотите разместить глобальный каталог.
3. В области сведений щелкните правой кнопкой элемент **NTDS Settings** и выберите команду **Свойства (Properties)**.
4. Чтобы разрешить размещение на сервере глобального каталога, установите флажок **Глобальный каталог (Global Catalog)** на вкладке **Общие (General)**.
5. Чтобы отказаться от размещения глобального каталога, сбросьте флажок **Глобальный каталог (Global Catalog)** на вкладке **Общие (General)**.

Внимание! Не следует включать и выключать глобальные каталоги, не проанализировав влияние этого действия на сеть. В крупном предприятии назначение контроллера домена на роль глобального каталога может привести к репликации по сети данных, связанных с тысячами объектов Active Directory.

Настройка кеширования членства в универсальной группе

Кеширование членства в универсальной группе позволяет входить в систему независимо от доступности глобального каталога. Если в домене, работающем в режиме Windows Server 2008, включена эта функция, любой контроллер домена может разрешать запросы на вход в систему локально, не обращаясь к серверу глобального каталога. У этого способа входа есть свои преимущества и недостатки, о которых говорится в разделе «Кеширование членства в универсальной группе» главы 7.

Чтобы включить или отключить кеширование членства в универсальной группе, выполните следующие действия:

1. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** разверните и выделите сайт, с которым хотите работать.
2. В области сведений щелкните правой кнопкой элемент **NTDS Site Settings** и выберите команду **Свойства (Properties)**.
3. Чтобы включить кеширование членства в универсальной группе, установите флажок **Разрешить кэширование членства в универсальных группах (Enable Universal Group Membership Caching)** на вкладке **Параметры сайта (Site Settings)**. В списке **Обновлять кэш из (Refresh Cache From)** выберите сайт, из которого следует кешировать членство в универсальной группе. В выбранном сайте должен быть работающий сервер глобального каталога.
4. Чтобы отключить кеширование членства в универсальной группе, сбросьте флажок **Разрешить кэширование членства в универсальных группах (Enable Universal Group Membership Caching)** на вкладке **Параметры сайта (Site Settings)**.
5. Щелкните **OK.**

Управление подразделениями

Как уже говорилось в главе 7, подразделения служат для упорядочивания объектов, ограничения области действия групповой политики и т. д. В этом разделе говорится о том, как создавать и управлять подразделениями.

Создание подразделений

Обычно подразделения отражают коммерческую или производственную структуру организации. Кроме того, подразделения могут служить и целям администрирования, например, когда вам нужно передать некоторые права пользователям или администраторам. Подразделения можно создавать в домене или внутри других подразделений.

Чтобы создать подразделение, выполните следующие действия:

1. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** щелкните правой кнопкой домен или подразделение, где вы хотите создать новое подразделение. В контекстном меню выберите команды **Создать (New)** и **Подразделение (Organizational Unit)**.
2. Введите имя подразделения и щелкните **OK**.
3. Переместите в созданное подразделение учетные записи и общие ресурсы.

Просмотр и редактирование свойств подразделения

Для просмотра и редактирования свойств подразделения выполните следующие действия:

1. Откройте консоль **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**.
2. Щелкните правой кнопкой подразделение, с которым хотите работать, и выберите команду **Свойства (Properties)**.

Переименование и удаление подразделения

Чтобы переименовать или удалить подразделение, выполните следующие действия:

1. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** щелкните правой кнопкой подразделение, с которым хотите работать.
2. Чтобы удалить подразделение, выберите команду **Удалить (Delete)**. Щелкните **Да (Yes)**, чтобы подтвердить удаление.
3. Чтобы переименовать подразделение, выберите команду **Переименовать (Rename)**. Ведите новое имя подразделения и нажмите Enter.

Перемещение подразделений

Чтобы переместить подразделение в другое расположение, следует выделить его в консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** и перетащить в новое расположение.

То же действие можно выполнить другим способом:

1. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** щелкните правой кнопкой подразделение, которое хотите переместить. Выберите команду **Переместить (Move)**.
2. В диалоговом окне **Переместить (Move)** разверните домен и выберите контейнер, в который хотите переместить подразделение. Щелкните **OK**.

Управление сайтами

В процессе установки доменных служб Active Directory на первом контроллере домена в сайте мастер установки Active Directory устанавливает сайт

по умолчанию и связь сайта по умолчанию. Стандартный сайт называется Default-First-Site-Name, а стандартная связь сайта — DEFAULTIPSITELINK. При необходимости вы вольны переименовать стандартный сайт и связь сайта. Последующие сайты и связи вам придется создавать вручную.

Процесс настройки сайта состоит из нескольких этапов:

1. Создание сайта.
2. Создание одной или нескольких подсетей и их связывание с сайтом.
3. Связывание контроллера домена с сайтом.
4. Связывание сайта с другими сайтами при помощи связей сайтов. При необходимости создание мостов.

Далее мы подробно рассмотрим все эти задачи.

Создание сайта

Сайты может создавать любой администратор, являющийся членом группы администраторов предприятия. Чтобы создать новый сайт, выполните следующие действия:

1. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** щелкните правой кнопкой контейнер **Sites** в корне консоли и выберите команду **Создать сайт (New Site)**.
2. В диалоговом окне **Новый объект — Сайт (New Object — Site)**, показанном на рис. 8-8, введите имя сайта, например, *ChicagoSite*. В имени сайта не должно быть пробелов и специальных символов, за исключением дефиса.

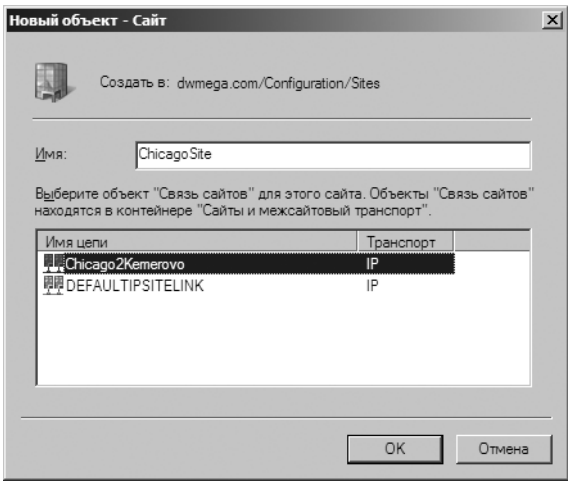


Рис. 8-8. Для создания сайта нужно задать его имя и указать его связь

3. Щелкните связь сайтов, которая будет использоваться для связывания этого сайта с остальными. Если связи, которую вы хотите использовать, не существует, выберите стандартную связь и позже измените ее параметры.

4. Щелкните **OK**. На экране появится окно с информацией о шагах, которые вам предстоит предпринять для завершения настройки сайта. Снова щелкните **OK**.
5. Выполните действия, описанные в информационном окне.

Совет При необходимости сайт можно в любой момент переименовать. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** щелкните сайт правой кнопкой и выберите команду **Переименовать (Rename)**. Введите новое имя сайта и нажмите Enter.

Создание подсетей

С каждым созданным вами сайтом необходимо связать подсети, описывающие сегменты сети, принадлежащие сайту. Считается, что в сайте находится любой компьютер, IP-адрес которого находится в сетевом сегменте, связанном с сайтом. С одним сайтом может быть связано несколько подсетей, но каждая подсеть может быть связана только с одним сайтом.

Чтобы создать подсеть и связать ее с сайтом, выполните следующие действия:

1. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** щелкните правой кнопкой контейнер **Subnet** в дереве консоли и выберите команду **Создать подсеть (New Subnet)**. На экране появится диалоговое окно **Новый объект — Подсеть (New Object – Subnet)**, показанное на рис. 8-9.

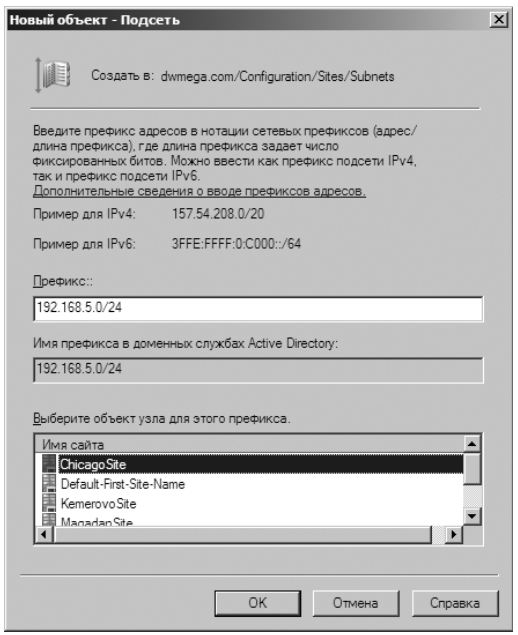


Рис. 8-9. Для создания подсети требуется ввести префикс и выбрать связанный с ней сайт

2. Введите в поле **Префикс (Prefix)** префикс сетевого адреса IPv4 или IPv6 в следующей нотации: идентификатор сети, косая черта и биты, которые следует использовать для сетевой идентификации. Допустим, идентификатор сети 192.168.5.0, и сетевой идентификатор определяют первые 24 бита, в качестве префикса вводится число **192.168.5.0/24**.
3. Выберите сайт, с которым следует связать подсеть, и щелкните **OK**.

Совет Сопоставление сайта можно в любой момент изменить. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** дважды щелкните подсеть в папке **Subnets** и на вкладке **Общие (General)** выберите другой сайт в списке **Сайт (Site)**.

Сопоставление контроллеров домена с сайтами

С каждым сайтом должен быть связан, по крайней мере, один контроллер домена. Добавляя в сайт второй контроллер домена, вы обеспечиваете отказоустойчивость и избыточность данных. Если хотя бы один контроллер домена в сайте является еще и сервером глобального каталога, трафик, связанный с поиском и проверкой подлинности, будет изолирован в пределах сайта.

Контроллеры домена добавляются в сайт автоматически или вручную. При связывании подсети с сайтом каждый вновь созданный контроллер домена будет автоматически добавлен к сайту при условии, что его IP-адрес лежит в диапазоне IP-адресов подсети. Существующие контроллеры домена автоматически с сайтами не связываются; это нужно делать вручную, перемещая в сайт объект контроллера домена.

До перемещения контроллера домена из одного сайта в другой, следует установить, в каком сайте контроллер домена располагается в данный момент. Проще всего выяснить это при помощи следующей команды:

```
dsquery server -s ИмяКонтроллераДомена | dsget server -site
```

где *ИмяКонтроллераДомена* — FQDN-имя контроллера домена, например:

```
dsquery server -s server241.cpandl.com | dsget server -site
```

Введя эту команду, вы узнаете имя сайта, в котором расположен указанный контроллер.

Чтобы переместить контроллер домена из одного сайта в другой, выполните следующие действия:

1. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** все контроллеры домена, связанные с сайтом, перечислены в узле **Servers**. Выделите сайт, с которым в настоящее время связан контроллер.
2. Щелкните правой кнопкой контроллер домена и выберите команду **Переместить (Move)**. В диалоговом окне **Перемещение сервера (Move Server)** щелкните сайт, в который следует переместить сервер, и щелкните **OK**.

Примечание Не перемещайте контроллер домена в сайт, если контроллер не принадлежит подсети, связанной с этим сайтом. Если вы изменяете связывание подсетей и сайтов, вам придется переместить контроллеры домена, находящиеся в этих подсетях, в контейнеры соответствующих сайтов.

Настройка связей сайтов

Сайтами называются группы IP-подсетей, соединенных между собой надежными высокоскоростными подключениями. Как правило, все подсети одной локальной сети являются частью одного и того же сайта. Сети с несколькими сайтами объединяются посредством связей сайтов (site link) — логических транзитивных соединений между двумя или несколькими сайтами. С каждой связью сайтов связаны расписание репликации, интервал репликации, стоимость и механизм репликации.

Поскольку связи сайтов организуются по каналам глобальных сетей, важную роль при их настройке играют соображения, связанные с пропускной способностью канала и его загруженностью. По умолчанию репликация данных по связям сайтов происходит 24 часа в сутки 7 дней в неделю с интервалом не менее трех часов. Если вы знаете, что у данной связи имеются ограничения по полосе пропускания, измените расписание так, чтобы в часы максимальной загруженности преимущество отдавалось трафику пользователей.

Если между сайтами имеется несколько связей, каждой из них следует назначить относительную стоимость (cost), исходя из доступности и надежности подключения. Стандартная стоимость связи равна 100. Если к сайту имеется несколько маршрутов, первым используется маршрут с наименьшей стоимостью. Поэтому самым надежным каналам с наибольшей пропускной способностью следует, как правило, назначать наименьшую стоимость связи.

В качестве транспортного протокола для связи сайтов можно настроить RPC через IP или SMTP. При использовании протокола IP контроллеры домена устанавливают подключение RPC через IP, допускающее репликацию с одним партнером, и синхронно реплицируют изменения Active Directory. Использовать RPC через IP следует при наличии надежных выделенных подключений между сайтами.

При использовании протокола SMTP контроллеры домена преобразуют весь трафик репликации в сообщения электронной почты, которые рассылаются между сайтами асинхронно. Благодаря этой асинхронности доступность обоих партнеров репликации во время установки подключения не требуется. Транзакции репликации сохраняются до тех пор, пока не станет доступен целевой сервер. Протокол SMTP следует использовать, если связи ненадежны или не всегда доступны.

Примечание Если вы планируете использовать SMTP, настройте центр сертификации. Выпускаемые им цифровые сертификаты используются для создания цифровой подписи и шифрования сообщений SMTP, посылаемых между сайтами. При использовании IP по умолчанию сертификаты не требуются.

Чтобы создать связь между двумя или несколькими сайтами, выполните следующие действия:

1. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** разверните контейнеры **Sites** и **Inter-Site Transports**.
2. Щелкните правой кнопкой контейнер транспортного протокола, который хотите использовать (**IP** или **SMTP**), и выберите команду **Создать связь с сайтом (New Site Link)**.
3. В диалоговом окне **Новый объект — Связь сайтов (New Object – Site Link)**, показанном на рис. 8-10, введите имя связи, например, **ChicagotoSeattleLink**. В имени связи не должно быть пробелов и специальных символов, за исключением дефиса.

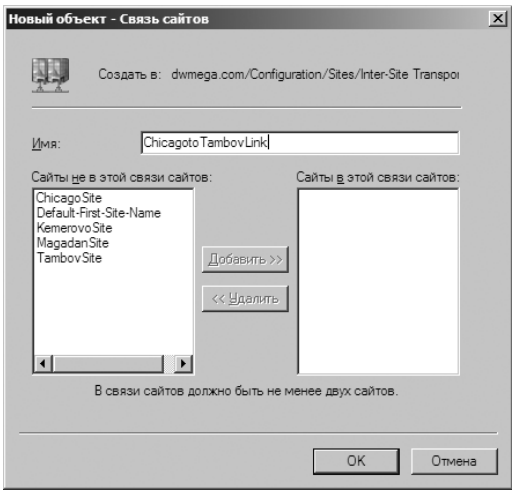


Рис. 8-10. Для создания связи задайте ее имя и выберите сопоставленные с ней сайты

4. В списке **Сайты не в этой связи сайтов (Sites Not In This Site Link)** выделите первый сайт, который следует включить в связь, и щелкните кнопку **Добавить (Add)**, чтобы добавить сайт в список **Сайты в этой связи сайтов (Sites In This Site Link)**. Повторите процесс для каждого сайта, который хотите добавить в связь. В связи должно быть не менее двух сайтов. Затем щелкните **OK**.

Завершив создание связи, настройте ее свойства — стоимость, расписание и интервал репликации. Чтобы настроить свойства связи, выполните следующие действия:

1. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** щелкните правой кнопкой нужную связь сайтов в области сведений и выберите команду **Свойства (Properties)**.
2. Диалоговое окно свойств по умолчанию открыто на вкладке **Общие (General)**. Введите в поле **Стоимость (Cost)** относительную стоимость связи. Стандартное значение — 100.

3. В поле **Реплицировать каждые (Replicate Every)** задайте интервал репликации. Интервал по умолчанию равен 180 минутам.
4. По умолчанию репликация проводится 24 часа в сутки, 7 дней в неделю. Чтобы задать другое расписание, щелкните кнопку **Изменить расписание (Change Schedule)** и настройте расписание репликации в диалоговом окне **Расписание для (Schedule For)**. Щелкните **OK**.

Чтобы изменить набор сайтов, сопоставленных со связью, выполните следующие действия:

1. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** щелкните правой кнопкой нужную связь сайтов в области сведений и выберите команду **Свойства (Properties)**.
2. Диалоговое окно свойств по умолчанию открыто на вкладке **Общие (General)**. В списке **Сайты не в этой связи сайтов (Sites Not In This Site Link)** выделите первый сайт, который следует включить в связь, и щелкните **Добавить (Add)**, чтобы добавить сайт в список **Сайты в этой связи сайтов (Sites In This Site Link)**. Повторите процесс для каждого сайта, который хотите добавить в связь.
3. В списке **Сайты не в этой связи сайтов** выделите первый сайт, который следует исключить из связи, и щелкните **Удалить (Remove)**, чтобы добавить сайт в список **Сайты не в этой связи сайтов (Sites Not In This Site Link)**. Повторите процесс для каждого сайта, который хотите убрать из связи, и щелкните **OK**.

Настройка мостов связей сайтов

По умолчанию связи сайтов транзитивны. Если связи репликации объединяют несколько сайтов и опираются на один и тот же транспортный протокол, установка мостов связей происходит автоматически. Благодаря транзитивности любые два контроллера домена могут установить подключение через ряд последовательных связей. Например, контроллер домена в Сайте А может подключиться к контроллеру домена в Сайте В через Сайт Б.

Маршрут связи, выбираемый контроллерами доменов для установки подключений, во многом определяется стоимостью моста связей, которая представляет собой сумму стоимостей всех связей, включенных в мост. Как правило, используется маршрут с наименьшей стоимостью.

Зная стоимости связей и мостов связей, легко посчитать последствия от нарушения связи и определить маршруты, которые будут использоваться при разрыве соединения. Допустим, контроллер домена в Сайте А обычно подключается к контроллеру домена в Сайте В через Сайт Б. В случае разрыва соединения с Сайтом Б два контроллера домена автоматически выберут альтернативный маршрут, если таковой имеется. Им может стать, например, маршрут, проходящий через Сайт Г и Сайт Д.

Топология межсайтовой репликации, по умолчанию, настроена максимум на три перехода. В крупных конфигурациях это может привести к не-

ожиданным последствиям, например, к многократному прохождению трафика репликации через одну и ту же связь. В этом случае вам следует отключить автоматическую установку мостов связей и настроить их вручную. В остальных случаях отключение автоматической установки мостов связей, как правило, не производится.

Внутри леса Active Directory вы можете включать или отключать транзитивность связей сайтов для каждого транспортного протокола в отдельности. Это означает, что все сайты, использующие тот или иной транспортный протокол, либо используют транзитивность, либо нет. Настройка транзитивности транспортного протокола выполняется следующим образом:

1. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** разверните контейнеры **Sites** и **Inter-Site Transports**.
2. Щелкните правой кнопкой контейнер транспортного протокола, который хотите использовать (**IP** или **SMTP**), и выберите команду **Свойства (Properties)**.
3. Чтобы включить транзитивность связей сайтов, установите флажок **Установить мост для всех связей сайтов (Bridge All Site Links)** и щелкните **OK**. При включенной транзитивности все созданные вами мосты связей для данного транспортного протокола игнорируются.
4. Чтобы отключить транзитивность связей сайтов, сбросьте флажок **Установить мост для всех связей сайтов (Bridge All Site Links)** и щелкните **OK**. Когда транзитивность связей отключена, вам следует вручную настроить мосты связей для данного протокола.

Отключив транзитивность связей, вы можете вручную создать мост связей между двумя или несколькими сайтами, выполнив следующие действия:

1. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** разверните контейнеры **Sites** и **Inter-Site Transports**.
2. Щелкните правой кнопкой контейнер транспортного протокола, который хотите использовать (**IP** или **SMTP**), и выберите команду **Создать мост связей сайтов (New Site Link Bridge)**.
3. В диалоговом окне **Новый объект — Мост связей сайтов (New Object – Site Link Bridge)** введите имя моста связей. В нем не должно содержаться пробелов и специальных символов, за исключением дефиса.
4. В списке **Связи сайтов, не входящие в данный мост (Site Links Not In This Site Link Bridge)** выберите связь, которую нужно включить в мост, и щелкните **Добавить (Add)**, чтобы добавить связь в список **Связи сайтов, входящие в данный мост (Site Links In This Site Link Bridge)**. Повторите процесс для каждой связи, которую хотите включить в мост. Мост должен состоять не менее чем из двух связей. Щелкните **OK**.

Чтобы изменить связи, связанные с мостом, выполните следующие действия:

1. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** щелкните правой кнопкой контейнер транспортного протокола, с которым хотите работать, и выберите команду **Свойства (Properties)**.

2. В диалоговом окне свойств по умолчанию выбрана вкладка **Общие (General)**. В списке **Связи сайтов, не входящие в данный мост (Site Links Not In This Site Link Bridge)** выделите первую связь, которую хотите включить в мост, и щелкните **Добавить (Add)**, чтобы добавить связь в список **Связи сайтов, входящие в данный мост (Site Links In This Site Link Bridge)**. Повторите процесс для каждой связи, которую хотите добавить в мост.
3. В списке **Связи сайтов, входящие в данный мост (Site Links In This Site Link Bridge)** выделите первую связь сайтов, которую хотите исключить из моста, и щелкните **Удалить (Remove)**, чтобы добавить связь в список **Связи сайтов, не входящие в данный мост (Site Links Not In This Site Link Bridge)**. Повторите процесс для каждой связи, которую хотите исключить из моста. Щелкните **OK**.

Обслуживание Active Directory

Правильная работа Active Directory невозможна без регулярного контроля и обслуживания системы. К счастью, существует целый ряд инструментов, которые помогут вам в проведении этих операций.

Оснастка Редактирование ADSI (ADSI Edit)

Для диагностики и устранения неисправностей Active Directory служит оснастка **Редактирование ADSI (ADSI Edit)**. Она используется для управления определениями классов объектов и их атрибутами в схеме. Кроме того, эта оснастка применяется для работы с другими контекстами именований, включая контекст по умолчанию, контекст Конфигурация (Configuration) и контекст RootDSE. Используйте ее, если хотите создать нестандартные атрибуты для пользователей и групп.

Чтобы добавить оснастку **Редактирование ADSI (ADSI Edit)** в консоль MMC, выполните следующие действия:

1. Щелкните **Пуск (Start)**, введите **mmc** в поле **Начать поиск (Search)** и нажмите Enter.
2. Выберите в меню **Консоль (File)** команду **Добавить или удалить оснастку (Add/Remove Snap-In)**.
3. В диалоговом окне **Добавление и удаление оснастки (Add Or Remove Snap-Ins)** выделите оснастку **Редактирование ADSI (ADSI Edit)** и щелкните **Добавить (Add)**. Затем щелкните **OK**.

Чтобы подключиться к нужному контексту именования, выполните следующие действия:

1. В дереве консоли MMC щелкните правой кнопкой узел **Редактирование ADSI (ADSI Edit)** и выберите команду **Подключение к (Connect To)**. Откроется диалоговое окно **Параметры подключения (Connection Settings)**, показанное на рис. 8-11.

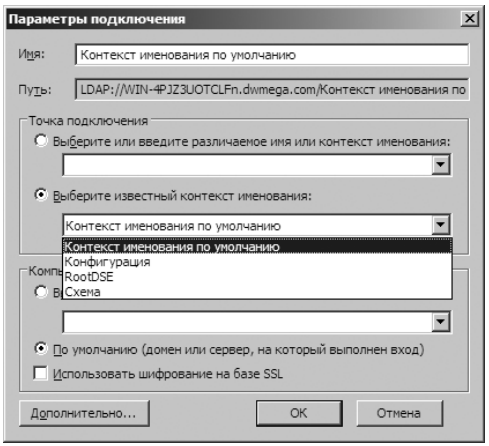


Рис. 8-11. Подключение к нужному контексту именования

2. В диалоговом окне **Параметры подключения (Connection Settings)** по умолчанию установлен переключатель **Выберите известный контекст именования (Select A Well Known Naming Context)**. В соответствующем раскрывающемся списке выберите контекст именования, с которым хотите работать.
3. Щелкнув **OK**, вы подключитесь к контроллеру текущего домена. Для подключения к другому домену или серверу установите переключатель **Выберите или введите домен или сервер (Select Or Type A Domain Or Server)** и выберите в раскрывающемся списке сервер или домен, с которым хотите работать, указав номер порта для подключения, например, **FileServer252.cpandl.com:389**. Порт 389 является стандартным портом протокола LDAP.

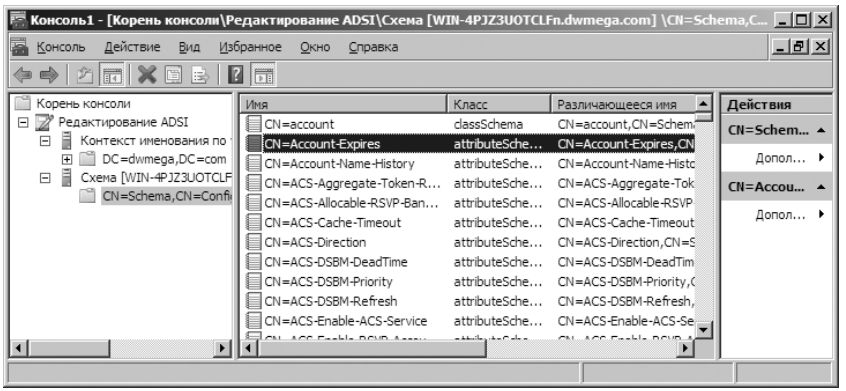


Рис. 8-12. Перемещайтесь по контекстам именования, чтобы проверить содержимое контейнеров и свойств

Выбрав контекст именования, домен и сервер, вы подключаетесь к серверу и вы можете приступать к работе с контекстом именования. Как показано на рис. 8-12, при подключении к нескольким контекстам именований

для управления каждым из них создается отдельный узел. При устранении неисправностей полезно подключиться к одному и тому же контексту на различных серверах одного домена. Сравнение значений свойств на одном сервере с аналогичными значениями на другом сервере поможет вам найти проблему репликации.

Исследование межсайтовой топологии

Генератор межсайтовой топологии (Iter-Site Topology Generator, ISTG) отвечает за формирование топологии репликации между сайтами. Формируя топологию репликации, ISTG занимает значительную часть вычислительной мощности, особенно, в большой сети. Поэтому следует внимательно следить за генераторами ISTG каждого сайта, чтобы не допускать их перегрузки.

Чтобы определить, какой контроллер домена выполняет функцию ISTG, выполните следующие действия:

1. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** разверните контейнер **Sites**, а затем разверните узел сайта, в котором хотите определить расположение ISTG.
2. В области сведений дважды щелкните элемент **NTDS Site Settings**. В открывшемся диалоговом окне свойств текущий ISGT отображен в разделе **Автоматическое формирование топологии между сайтами (Inter-Site Topology Generator)**.

Репликация между сайтами осуществляется серверами-плацдармами — контроллерами домена, которые ISTG выбрал для выполнения межсайтовой репликации. Если два сайта соединены между собой с помощью связи сайтов, ISTG выбирает по одному серверу-плацдарму в каждом сайте и создает для проведения межсайтовой репликации объекты связи между серверами, доступные только для входящих подключений.

Генератор ISTG настраивает сервер-плацдарм для каждого раздела Active Directory, требующего репликации, а также поддерживает собственные топологии репликации для каждого типа раздела. Хотя одиночный сервер-плацдарм может отвечать за репликацию нескольких разделов каталога, топология репликации для каждого раздела поддерживается отдельно.

Контроллеры домена, работающие в качестве сервера-плацдарма, несут дополнительную нагрузку, возрастающую пропорционально количеству и частоте репликационных изменений. Вам следует внимательно следить за серверами-плацдармами, чтобы не допускать их перегрузки. Чтобы найти серверы-плацдармы в сайте, введите в командной строке следующую команду:

```
repadmin /bridgeheads site:ИмяСайта
```

где *ИмяСайта* — имя сайта, например:

```
repadmin /bridgeheads site:SacramentoSite
```

Если текущие серверы-плацдармы перегружены или у вас есть контроллеры домена, которые лучше подходят на эту роль, вы можете назначить

предпочтительные серверы-плацдармы вручную. Когда вы это сделаете, ISTG будет использовать для репликации только назначенные вами предпочтительные серверы-плацдармы. Если предпочтительный сервер-плацдарм недоступен или по той или иной причине не может выполнить репликацию, она будет остановлена, пока сервер снова не станет доступен или пока вы не настроите другой предпочтительный сервер-плацдарм.

По возможности всегда настраивайте в каждом сайте несколько предпочтительных серверов. Генератор ISTG выберет для репликации один из них. При сбое в работе этого компьютера ISTG выберет из списка предпочтительных серверов-плацдармов другой сервер.

Свой сервер-плацдарм следует настроить для каждого реплицируемого раздела. Это значит, что вы должны настроить в качестве сервера-плацдарма хотя бы один контролер домена с репликой каждого раздела каталога. Если этого не сделать, репликации разделов не будет, а ISTG зарегистрирует событие в журнале Служба каталогов (Directory Services) с отчетом о сбое.

Чтобы сделать контроллер домена сервером-плацдармом, выполните следующие действия:

1. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** контроллеры домена, связанные с сайтом, собраны в узле **Servers**. Щелкните правой кнопкой сервер, который хотите сделать предпочтительным сервером-плацдармом, и выберите команду **Свойства (Properties)**.
2. В диалоговом окне свойств в списке **Транспорты для передачи данных между сайтами (Transports Available For Inter-Site Data Transfer)** выберите транспортный протокол, для которого производится настройка. Щелкните **Добавить (Add)**. Если необходимо указать оба протокола — IP и SMTP, — повторите процедуру. Щелкните **OK**.

Установив несколько серверов-плацдармов, в случае сбоя вы можете восстановить репликацию несколькими способами. Можно удалить неисправные серверы из списка предпочтительных, а на их место назначить другие. Кроме того, вы можете удалить из списка предпочтительных серверов-плацдармов все серверы и позволить ISTG самостоятельно выбрать серверы-плацдармы. Чтобы прекратить использование сервера в качестве предпочтительного плацдарма для того или иного протокола, выполните следующие действия:

1. В консоли **Active Directory — сайты и службы (Active Directory Sites And Services)** щелкните правой кнопкой сервер, который не должен более быть предпочтительным сервером-плацдармом, и выберите команду **Свойства (Properties)**.
2. Выделите транспортный протокол в списке **Это — сервер-плацдарм для следующих транспортов (This Server Is A Preferred Bridgehead Server For The Following Transports)** и щелкните **Удалить (Remove)**. Затем щелкните **OK**.

Устранение неисправностей Active Directory

Повседневное обслуживание среди прочего включает в себя наблюдение за контроллерами домена, серверами глобального каталога, серверами-плацдармами и связями сайтов. Если вы подозреваете сбой, в большинстве случаев диагностику и устранение неисправности следует начать с репликации. Настроив мониторинг внутрисайтовой и межсайтовой репликации Active Directory, вы диагностируете и разрешите большую часть проблем репликации. Не забывайте, что репликация Active Directory зависит от нескольких служб, в том числе LDAP, DNS, проверки подлинности Kerberos v5 и RPC.

Чтобы обновления каталога реплицировались своевременно, эти службы должны корректно функционировать. В процессе репликации Active Directory применяет различные порты TCP и UDP. По умолчанию они используются в следующем порядке:

- Протокол LDAP использует порт 389 протоколов TCP и UDP для стандартного трафика и порт 686 TCP для защищенного трафика.
- Глобальные каталоги используют порт 3268 протокола TCP. В технологии Kerberos v5 используется порт 88 TCP и UDP.
- Служба DNS использует порт 53 TCP и UDP.
- Протокол SMB через IP использует порт 445 TCP и UDP.

Кроме того, для репликации файлов в общих папках Sysvol на контроллерах домена Active Directory применяет либо службу репликации файлов (FRS), либо службу репликации распределенной файловой системы (DFS). Соответствующая служба репликации должна быть запущена и должным образом настроена.

Служба каталогов Active Directory отслеживает изменения при помощи порядковых номеров обновления (update sequence number, USN). Каждый раз при внесении изменения в каталог контроллер домена, обрабатывающий изменение, присваивает ему порядковый номер обновления. На каждом контроллере домена поддерживаются собственные локальные номера обновления, значения которых увеличиваются с каждым новым изменением. Контроллер домена также присваивает локальные порядковые номера изменениям атрибутов объектов. У каждого объекта есть атрибут *uSNChange*, который хранится вместе с объектом и представляет собой наивысшее значение USN, присвоенное любому атрибуту объекта.

Контроллер домена отслеживает локальные номера USN, а также номера USN других контроллеров. Во время репликации контроллеры домена сравнивают полученные значения USN с собственными значениями. Если текущее значение USN того или иного контроллера домена выше, чем локально сохраненное значение, изменения, связанные с этим контроллером домена следует реплицировать. Если текущее значение USN контроллера домена идентично сохраненному значению, изменения данного контроллера домена реплицировать ненужно.

Вы можете наблюдать за репликацией из командной строки при помощи утилиты Repadmin. В строке вызова Repadmin, как правило, указывается список контроллеров домена, с которыми вы хотите работать. Он называется DCList и определяется следующим образом:

- ***** Звездочка символизирует все контроллеры домена в организации.
- ***ЧастьИмени**** Все контроллеры, имена которых начинаются со строки «ЧастьИмени».
- **Site:*ИмяСайта*** Все контроллеры домена из сайта *ИмяСайта*.
- **Gc:** Все серверы глобального каталога в организации.

Утилита Repadmin обладает многими параметрами, и существует множество способов ее использования, однако некоторые задачи вам будут встречаться чаще, чем другие. Некоторые из них перечислены в табл. 8-2.

Табл. 8-2. Общие задачи репликации и связанные с ними команды

Задача	Команда
Принудительная проверка согласованности сведений (Knowledge Consistency Check, KCC) для пересчета топологии внутрисайтовой репликации заданного контроллера домена	`repadmin /kcc DCList [/async]`
Перечисление серверов-плацдармов из списка DCList.	`repadmin /bridgeheads DCList ] [/verbose]`
Список вызовов, сделанных заданным сервером и оставшихся без ответа	`repadmin /showoutcalls DCList`
Список доверенных доменов для указанного домена	`repadmin /showtrust DCList`
Список сбойных репликаций, обнаруженных проверкой KCC	`repadmin /failcache DCList`
Список объектов подключения для заданных контроллеров домена. По умолчанию работает для локального сайта	`repadmin /showconn DCList`
Список компьютеров, имеющих активное подключение к заданному контролеру домена	`repadmin /showctx DCList`
Вывод имени ISTG для заданного сайта	`repadmin istg DCList [/verbose]`
Список партнеров репликации для каждого раздела каталога на заданном контроллере	`repadmin /showrepl DCList`
Вывод отчета о состоянии репликации	`repadmin /replsummary DCList`
Список серверных сертификатов, загруженных на заданный контроллер домена	`repadmin /showcert DCList`
Список задач, ожидающих в очереди на репликацию	`repadmin /queue DCList`
Список временных промежутков между межсайтовыми репликациями с использованием метки времени ISTG Keep Alive	`repadmin /latency DCList [/verbose]`

Глава 9

Учетные записи пользователей и групп

Управление учетными записями — одна из основных задач администратора Windows Server 2008. Если в главе 8 говорилось об учетных записях компьютеров, то в этой главе рассматриваются учетные записи пользователей и групп. Учетные записи пользователей служат для предоставления отдельным пользователям прав входа в сеть и обращения к сетевым ресурсам. Учетные записи групп позволяют управлять доступом к ресурсам сразу нескольких пользователей. Разрешения и полномочия, предоставляемые пользователю или группе, определяют, какие действия могут выполнять пользователи, а также доступ к каким компьютерам они получают.

У вас может возникнуть искушение не ограничивать пользователей в возможностях. Однако лучше постараться найти золотую середину между свободным доступом к ресурсам и необходимостью защитить системную и конфиденциальную информацию. Например, не следует открывать общий доступ к платежной ведомости. Сделайте так, чтобы доступом к информации обладал только тот, кому она нужна для работы.

Модель безопасности Windows Server 2008

Модель безопасности Windows Server 2008 определяет, как именно осуществляется доступ к ресурсам сети. Ее ключевые компоненты — системы проверки подлинности и управления доступом.

Протоколы проверки подлинности

В Windows Server 2008 проверка подлинности реализована в виде двухступенчатого процесса, состоящего из интерактивного входа в систему и сетевой проверки подлинности. Когда пользователь выполняет вход на компьютер, используя учетную запись домена, в процессе интерактивного входа его подлинность подтверждается на локальном компьютере, и пользователю предоставляется доступ в службу каталогов Active Directory. После этого независимо от того, к каким ресурсам пользователь пытается получить доступ, используется сетевая проверка подлинности, при помощи которой определяется, имеет ли пользователь право на доступ к ресурсу.

Система Windows Server 2008 поддерживает многие протоколы проверки подлинности. Начиная с Windows 2000, в Active Directory в качестве стандартного протокола проверки подлинности используется Kerberos v5. Проверка подлинности по протоколу NTLM поддерживается только в целях обратной совместимости. При помощи групповой политики вы можете управлять использованием протокола NTLM, задавая параметр безопасности **Сетевая безопасность: уровень проверки подлинности LAN Manager (Network Security: LAN Manager Authentication Level)**. В большинстве случаев стандартным уровнем проверки подлинности является **Отправлять только NTLMv2 ответ (Send NTLMv2 Response Only)**, на котором клиенты используют для проверки подлинности и обеспечения безопасности сеанса протокол NTLM Version 2, если он поддерживается сервером. Кроме того, для проверки подлинности в Active Directory могут использоваться сертификаты клиентов.

Ключевой особенностью модели проверки подлинности Windows Server 2008 является поддержка единого входа в систему (Single Sign-On), которая работает следующим образом:

1. Пользователь входит в домен, введя имя и пароль или вставив смарт-карту в устройсто для чтения карт.
2. В процессе интерактивного входа в систему проводится проверка подлинности пользователя. При использовании локальной учетной записи подлинность учетных данных проверяется локально, и пользователь получает доступ к локальному компьютеру. При использовании учетной записи домена проверка подлинности происходит в Active Directory, и пользователь получает доступ к локальным и сетевым ресурсам.
3. Теперь при помощи сетевой проверки подлинности пользователь может входить на любой компьютер домена. Сетевая проверка подлинности доменной учетной записи, как правило, происходит автоматически (посредством единого входа). Пользователь, использовавший локальную учетную запись, должен вводить имя и пароль при каждом обращении к сетевому ресурсу.

В ОС Windows Server 2008 включены службы федерации Active Directory (Active Directory Federation Services, ADFS), которые распространяют действие единого входа в систему на доверенные ресурсы в Интернете. В их число могут входить партнеры, а также филиалы предприятия, разделенные территориально. После настройки серверов федерации пользователи смогут регистрироваться в сети организации, а затем автоматически подключаться к доверенным веб-приложениям, опубликованным партнерами в Интернете. Для обеспечения прямого доступа в федеративном едином входе применяется федеративная авторизация (Federated Authorization). Используемые в ней маркеры безопасности, помимо данных пользователя и учетной записи, содержат заявки на проверку подлинности с подробной информацией о пользователе и правах на доступ к приложениям.

Средства управления доступом

Служба каталогов Active Directory является объектно-ориентированной системой. Пользователи, компьютеры, группы, общие ресурсы и многие другие логические категории определяются в ней как объекты. Средства управления доступом применяются к объектам с использованием дескрипторов безопасности, выполняющих следующие функции:

- содержат список пользователей и групп, имеющих доступ к объекту;
- определяют разрешения, предоставленные пользователям и группам;
- отслеживают события аудита для объекта;
- определяют владельца объекта.

Отдельные записи в дескрипторе безопасности называются элементами управления доступом (access control entry, ACE). Объекты Active Directory могут наследовать элементы управления доступом от родительских объектов. Это означает, что разрешения родительского объекта применяются и к дочернему объекту. Например, все члены группы Администраторы домена (Domain Admins) наследуют разрешения, предоставленные этой группе.

Работая с элементами управления доступом, имейте в виду следующее:

- По умолчанию в элементах управления доступом включено наследование.
- Наследование вступает в силу сразу после создания элемента.
- Все элементы ACE содержат информацию о том, является ли данное разрешение наследуемым или было назначено явно.

Различия между учетными записями пользователей и групп

В системе Windows Server 2008 существуют учетные записи пользователей и учетные записи групп (членами которых могут быть пользователи). Пользовательские учетные записи предназначены для конкретных сотрудников. Учетные записи групп призваны облегчить управление большим количеством пользователей. Вход в систему можно выполнять только при помощи учетной записи пользователя. Обычно учетные записи групп называют просто группами.

Ближе к реальности ОС Windows Server 2008 поддерживает объект InetOrgPerson. По сути, этот объект — то же самое, что и объект-пользователь, и вы вольны применять его в этом качестве. Однако истинное назначение объекта InetOrgPerson — обеспечение совместимости и перехода со служб каталогов X.500 и LDAP сторонних организаций, использующих этот объект для представления пользователей. Если при переходе из такой службы каталогов у вас в результате получилось большое количество объектов InetOrgPerson, не беспокойтесь. Их можно использовать в качестве участников безопасности, как и учетные записи обычных пользователей. Возможности объекта InetOrgPerson реализуются полностью только при работе в режиме Windows Server 2008. В этом режиме вы может устанавливать пароли для объектов InetOrgPerson, а также, при необходимости, изменять их класс. При изменении класса объект InetOrgPerson преобразуется в объект-пользователь и в дальнейшем отобра-

жается в консоли Active Directory — пользователи и компьютеры (Active Directory Users And Computers) как объект User.

Учетные записи пользователей

В Windows Server 2008 используются учетные записи пользователя двух типов:

- **Доменные учетные записи** Учетные записи пользователей, определенные в Active Directory. Пройдя процедуру единого входа в систему владельцы доменных учетных записей получают доступ к ресурсам всего домена. Доменные учетные записи создаются в консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**.
- **Локальные учетные записи** Учетные записи пользователей, определенные на локальном компьютере и предоставляющие доступ только к его ресурсам. Прежде чем получить доступ к сетевому ресурсу, они обязаны авторизоваться. Локальные учетные записи пользователей создаются при помощи консоли **Локальные пользователи и группы (Local Users And Groups)**.

Примечание В домене локальные учетные записи пользователей и групп бывают только на рядовых серверах и рабочих станциях. На первом контроллере домена эти учетные записи перемещаются из БД диспетчера учетных записей (SAM) в Active Directory и преобразуются в доменные учетные записи.

Имена для входа, пароли и открытые сертификаты

Учетные записи пользователей идентифицируются по именам для входа. В Windows Server 2008 имя для входа состоит из двух частей:

- **Имя пользователя** Текстовое обозначение учетной записи.
- **Домен или рабочая группа пользователя** Рабочая группа или домен, в которых существует данная учетная запись пользователя.

Полное имя для входа в Windows Server 2008 для пользователя wrstanek, учетная запись которого создана в домене cpandl.com, выглядит как wrstanek@cpandl.com. Имя для входа в версиях Windows до Windows 2000 выглядит как CPANDL\wrstanek.

Работая с Active Directory, вы иногда должны будете указывать для пользователя *полностью определенное имя домена* (fuly qualified domain name, FQDN). FQDN-имя представляет собой комбинацию DNS-имени домена, контейнера или подразделения, в котором содержится пользователь, и имени пользователя. В имени пользователя *cpandl.com\users\wrstanek* к DNS-имени домена *cpandl.com* добавлены контейнер (или подразделение) *users* и имя пользователя *wrstanek*.

С учетными записями пользователей могут также связываться пароли и открытые сертификаты. Пароль — это строка символов для проверки подлинности учетной записи. В открытом сертификате для проверки подлинности пользователя используется сочетание открытого и закрытого ключа. С помощью пароля осуществляется интерактивный вход в систему, а откры-

тый сертификат позволяет выполнить вход при помощи смарт-карты и устройства для ее чтения.

Идентификаторы безопасности и учетные записи пользователей

Хотя в описаниях полномочий и разрешений пользователей Windows Server 2008 отображает их имена, ключевыми идентификаторами учетных записей являются *идентификаторы безопасности* (security identifier, SID) — уникальные идентификаторы, генерируемые при создании учетных записей. Каждый идентификатор SID учетной записи состоит из идентификатора безопасности домена и уникального относительного идентификатора (relative identifier, RID), назначаемого хозяином пула RID.

В Windows Sever 2008 идентификаторы SID используются для отслеживания учетных записей независимо от имен пользователей. Идентификаторы безопасности служат многим целям. Две наиболее важные из них — возможность изменить имя пользователя без потери разрешений и возможность удалять учетные записи, не опасаясь, что кто-то получит несанкционированный доступ к ресурсам, создав учетную запись с таким же именем.

Когда вы меняете имя пользователя, Windows Server 2008 сопоставляет с новым именем пользователя прежний идентификатор безопасности. При удалении учетной записи ее идентификатор SID становится недействительным. Даже если вы позже создадите учетную запись с таким же именем пользователя, ей будет назначен другой идентификатор SID, и потому новая учетная запись не будет обладать теми же полномочиями и разрешениями, что предыдущая.

Учетные записи групп

Кроме учетных записей пользователей, в Windows Server 2008 используются учетные записи групп. В целом, группы используются для предоставления разрешений сходным типам пользователей, а также для упрощения администрирования учетных записей. Если пользователь является членом группы, обладающей доступом к ресурсу, то и сам пользователь получает доступ к этому ресурсу. Таким образом, чтобы предоставить пользователю доступ к различным рабочим ресурсам, вы просто добавляете его в нужную группу. Следует помнить, что при помощи учетной записи пользователя можно войти на компьютер, а при помощи учетной записи группы — нет.

Поскольку в различных доменах Active Directory могут использоваться группы с совпадающими именами, в обозначение группы часто включают имя домена — *домен\имя_группы*. Например, *cpandl\gmarketing* является учетной записью группы *gmarketing* в домене *cpandl*. Для групп также можно указывать FQDN-имя — последовательность из DNS-имени домена, контейнера или подразделения, в котором содержится группа, и имени группы. В имени *cpandl.com\users\gmarketing* строка *cpandl.com* представляет собой DNS-именя домена, *users* — контейнер или подразделение, *gmarketing* — имя группы.

Ближе к реальности Сотрудникам отдела маркетинга, вероятно, нужен доступ ко всем ресурсам, связанным с маркетингом. Чтобы не предоставлять доступ к ресурсам индивидуально, сделайте этих пользователей членами группы marketing, и они автоматически получат полномочия данной группы. Позднее, если некий пользователь переходит в другой отдел, вы просто удаляете его из группы, аннулируя сразу все связанные с ней разрешения. Этот способ намного легче, чем ручная отмена разрешений для каждого ресурса в отдельности. Поэтому группы следует использовать максимально широко.

Типы групп

В Windows Server 2008 используются группы трех видов:

- **Локальные группы** Группы, определенные на локальном компьютере и используемые только на нем. Создаются при помощью консоли **Локальные пользователи и группы (Local Users And Groups)**.
- **Группы безопасности** Группы, с которыми сопоставлены дескрипторы безопасности. В доменах группы безопасности определяются при помощи консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**.
- **Группы распространения** Группы, используемые в качестве списка рассылки электронной почты. С ними не связаны дескрипторы безопасности. В доменах группы распространения также определяются при помощи консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**.

Примечание Как правило, говоря о группах, имеют в виду только локальные группы и группы безопасности, но не группы распространения. Группы распространения применяются только для рассылки электронной почты и не используются для управления доступом.

Область действия группы

В Active Directory группы различаются по областям действия — локальные доменные группы (domain local), встроенные локальные группы (built-in local), глобальные (global) и универсальные (universal) группы.

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

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

- **Универсальные группы** В основном, используются для определения наборов пользователей или компьютеров, которым требуется широкий спектр разрешений в домене или лесе. Членами универсальных групп могут быть учетные записи, глобальные группы и другие универсальные группы из любого домена дерева или леса. Универсальные группы безопасности доступны только при работе Active Directory в основном режиме Windows 2000 или в режиме Windows Server 2008. Универсальные группы распространения доступны в любом режиме работы домена.

Совет Универсальные группы полезны в больших предприятиях с несколькими доменами. При правильном планировании универсальные группы существенно облегчают процесс системного администрирования. Не следует часто менять членов универсальных групп. При каждом изменении членов универсальной группы вам следует реплицировать изменения во все глобальные каталоги доменного дерева или леса. Для сокращения объема изменений добавляйте в универсальную группу другие группы, а не пользователей. Подробнее — в разделе «Рекомендации по использованию локальных, глобальных и универсальных групп» этой главы.

Область действия группы определяет ваши возможности, краткая сводка которых приводится в табл. 9-1. Более подробно о создании групп рассказывается в главе 10.

Табл. 9-1. Область действия и возможности групп

Возможности группы	Локальная доменная группа	Глобальная группа	Универсальная группа
В основном режиме Windows 2000 или более высоком	Учетные записи, глобальные и универсальные группы из любого домена; локальные доменные группы только из того же домена	Учетные записи и глобальные группы только из того же домена	Учетные записи, а также глобальные и универсальные группы из любого домена
В смешанном режиме Windows 2000	Учетные записи и глобальные группы из любого домена	Только учетные записи из того же домена	Универсальные группы не могут создаваться в доменах, работающих в смешанном режиме
Членство в других группах	Может быть членом локальной группы другого домена; разрешения назначаются только в текущем домене	Может быть членом других группы; разрешения назначаются в любом домене	Может быть членом других групп; разрешения назначаются в любом домене

Табл. 9-1. (*окончание*)

Возможности группы	Локальная доменная группа	Глобальная группа	Универсальная группа
Изменение области действия	Может быть преобразована в универсальную при условии, что среди ее членов нет другой локальной доменной группы	Может быть преобразована в универсальную при условии, что сама не является членом универсальной группы	Область действия универсальной группы изменить нельзя

Идентификаторы безопасности и учетные записи групп

Учетные записи групп, как и учетные записи пользователей, обладают идентификаторами SID. Это означает, что вы не можете удалить ученую запись группы, а затем снова создать, сохранив все разрешения и полномочия. У новой группы будет новый идентификатор безопасности, и все разрешения и полномочия старой группы будут утеряны.

ОС Windows Server 2008 создает маркер безопасности для каждого имени входа. В маркер включается SID учетной записи пользователя, а также SID всех групп безопасности, к которым принадлежит учетная запись пользователя. С добавлением пользователя в новые группы безопасности размер маркера растет. Это приводит к следующим последствиям:

- Маркер безопасности нужно передавать процессу входа пользователя в систему до завершения этого процесса. Чем шире членство учетной записи в группах безопасности, тем больше времени требуется на вход в систему.
- Чтобы определить разрешения на доступ, маркер безопасности пересылается на каждый компьютер, доступ к которому получает пользователь. Поэтому размер маркера безопасности оказывает прямое влияние на объем сетевого трафика.

Примечание Членство в группах распространения не учитывается в маркерах безопасности и не отражается на их размерах.

Рекомендации по использованию локальных, глобальных и универсальных групп

Локальные доменные, глобальные и универсальные группы предоставляют широчайшие возможности для конфигурирования групп предприятия. Области действия этих групп призваны упростить администрирование, но ошибки в планировании легко превратят их использование в кошмар. В идеале вы должны использовать области действия групп для создания иерархии, которая отражала бы организационную структуру предприятия и обязанности отдельных пользовательских коллективов. Вот наиболее подходящие области применения локальных доменных, глобальных и универсальных групп:

- **Локальные группы домена** Обладают наименьшим охватом. Применяйте их для управления доступом к ресурсам, например, принтерам и общим папкам.
- **Глобальные группы** Подходят для управления учетными записями пользователей и компьютеров в отдельно взятом домене. Чтобы предоставить членам глобальной группы разрешение на доступ к ресурсу, сделайте ее членом соответствующей локальной доменной группы.
- **Универсальные группы** Обладают наибольшим охватом. Используйте их для объединения групп из различных доменов. Обычно для этого в универсальную группу включают глобальные группы. Даже если вы измените состав глобальных групп, изменения не нужно реплицировать в глобальные каталоги, поскольку состав универсальной группы не был изменен.

Совет Если в вашей организации всего один домен, универсальные группы вам, по большому счету, не нужны. Выстраивайте структуру групп при помощи локальных доменных и глобальных групп. Если в будущем в вашем доменном дереве появится еще один домен, вам не составит труда расширить групповую иерархию.

Чтобы лучше во всем разобраться, рассмотрим конкретный сценарий. Допустим, у вашей фирмы есть филиалы в Сиэтле, Чикаго и Нью-Йорке. У каждого офиса есть собственный домен, который является частью общего дерева или леса. Домены называются Seattle, Chicago и NY. Ваша задача: обеспечить возможность управления сетевыми ресурсами каждому администратору (из любого офиса). В каждом филиале вы создаете почти одинаковую групповую структуру. В компании имеются отделы ИТ, маркетинга и инженерно-технический, но мы для определенности сосредоточимся на маркетинге. В каждом офисе сотрудникам маркетингового отдела нужен доступ к общему принтеру MarketingPrinter и общей папке MarketingData. Кроме того, пользователям нужна возможность совместно работать над документами и печатать их. Например, Боб из Сиэтла должен иметь возможность распечатать документы на локальном принтере филиала в Нью-Йорке. Кроме того, Бобу нужен доступ к квартальному отчету, находящемуся в общей папке в нью-йоркском филиале.

Чтобы настроить группы отделов маркетинга во всех трех филиалах, выполните следующие действия:

1. Начните с создания глобальных групп для каждой маркетингового отдела. В домене Seattle создайте группу GMarketing и добавьте в нее сотрудников отдела маркетинга из Сиэтла. В домене Chicago создайте группу GMarketing и добавьте в нее сотрудников чикагского отдела маркетинга. Наконец, в домене NY создайте группу GMarketing и добавьте в нее сотрудников отдела маркетинга из Нью-Йорка.
2. В каждом филиале создайте локальные доменные группы с доступом к общим принтерам и общим папкам. Назовем группу с доступом к принтерам LocalMarketingPrinter, а группу с доступом к общим папкам —

LocalMarketingData. В доменах Seattle, Chicago и NY должны быть собственные локальные группы.

3. Создайте универсальную группу UMarketing в домене каждого филиала. Включите в нее группы Seattle\GMarketing, Chicago\GMarketing и NY\GMarketing.
4. Добавьте группу UMarketing в группы LocalMarketingPrinter и LocalMarketingData каждого филиала. Теперь сотрудники отдела маркетинга смогут совместно использовать данные и принтеры.

Стандартные учетные записи пользователей и групп

Во время установки ОС Windows Server 2008 создается ряд стандартных пользователей и групп. Их учетные записи станут основой дальнейшего развития вашей сети. Существует три типа стандартных учетных записей:

- **Встроенные (built-in)** Учетные записи пользователей и групп, устанавливаемые с ОС, приложениями и службами.
- **Предопределенные (predefined)** Учетные записи пользователей и групп, устанавливаемые с ОС.
- **Неявные (implicit)** Специальные группы, создаваемые неявно при осуществлении доступа к сетевым ресурсам.

Примечание Вы вольны изменить параметры стандартных пользователей и групп, но не можете удалить соответствующие учетные записи, созданные ОС.

Встроенные учетные записи пользователей

В ОС Windows Server 2008 каждая встроенная учетная запись имеет особое предназначение. Во всех ОС Windows Server 2008 имеется три встроенных учетных записи пользователя:

- **Локальная система (Local System)** Псевдозапись для запуска системных процессов и обработки задач системного уровня. Является членом группы Администраторы (Administrators) на сервере и обладает на нем всеми правами пользователя. Если вы настроите приложение или службу на работу от имени этой учетной записи, соответствующие процессы будут иметь полный доступ к серверу, что может представлять серьезную угрозу безопасности. От имени учетной записи Локальная система (LocalSystem) запускаются многие службы. В некоторых случаях у этих служб есть право взаимодействия с рабочим столом. Службы, требующие других полномочий или прав входа в систему, запускаются от имени учетных записей LocalService или NetworkService.
- **LocalService** Псевдозапись с ограниченными полномочиями, предоставляющая доступ только к локальной системе. Является членом группы Пользователи (Users) на сервере и обладает теми же правами, что и учетная запись NetworkService, за исключением того что она ограничена локальным компьютером. Настраивайте приложения и службы на ис-

пользование этой учетной записи, если соответствующие процессы не нуждаются в доступе к другим серверам.

- **NetworkService** Псевдозапись для запуска служб, требующих дополнительных полномочий и прав на вход в локальную систему и сеть. Эта учетная запись является членом группы Пользователи (Users) на сервере, и предоставляет меньше разрешений, чем группа Локальная система (LocalSystem), но больше, чем LocalService. В частности, запущенный от имени этой учетной записи процесс может взаимодействовать через сеть, используя данные учетной записи компьютера.

В процессе установки на сервер компонентов или других приложений иногда производится установка других стандартных учетных записей. Как правило, их можно удалять.

После установки IIS вы обнаружите несколько новых учетных записей, включая IUSR_*hostname*, где *hostname* — имя компьютера. Учетная запись IUSR_*hostname* представляет собой встроенную учетную запись для анонимного доступа к IIS. Данная учетная запись появляется в Active Directory, если вы настраиваете IIS в домене. При настройке ISS на рабочей станции или изолированном сервере эта учетная запись определяется как учетная запись локального пользователя.

Предопределенные учетные записи пользователей

В Windows Server 2008 имеется несколько предопределенных учетных записей пользователей, включая учетные записи Администратор (Administrator) и Гость (Guest). На рядовых серверах предопределенные учетные записи являются локальными для той системы, на которой они установлены.

У предопределенных учетных записей есть аналоги в Active Directory. Их права доступа определяются на уровне домена и полностью отделены от локальных учетных записей на отдельных системах.

Учетная запись Администратор (Administrator)

Предопределенная учетная запись Администратор (Administrator) предоставляет полный доступ к файлам, папкам, службам и прочим средствам. Удалить или отключить эту учетную запись невозможно. В Active Directory учетная запись Администратор (Administrator) обладает разрешениями и полномочиями на уровне домена. На локальном компьютере учетная запись Администратор (Administrator), в основном, имеет доступ только к локальной системе. Файлы и папки можно временно сделать недоступными для учетной записи Администратор (Administrator), но администратор всегда сможет без труда изменить разрешения на доступ в свою пользу. Дополнительную информацию вы найдете в главе 14.

Безопасность Чтобы предотвратить несанкционированный доступ к системе или домену, задайте для учетной записи администратора особенно сложный пароль. В качестве дополнительной меры предосторожности переименуйте ее, а также создайте фиктивную учетную запись с именем Администратор (Administrator), не предоставляя

ей никаких разрешений, прав и полномочий. Кроме того, чтобы ввести злоумышленников в заблуждение, отключите эту фиктивную учетную запись.

Как правило, менять основные параметры учетной записи Администратор (Administrator) не нужно. Вам может понадобиться изменить ее дополнительные параметры, например, членство в тех или иных группах. По умолчанию учетная запись Администратор (Administrator) в домене является членом следующих групп: Администраторы (Administrators), Администраторы домена (Domain Admins), Пользователи домена (Domain Users), Администраторы предприятия (Enterprise Admins), Владельцы-создатели групповой политики (Group Policy Creator Owners) и Администраторы схемы (Schema Admins). В следующем разделе содержится дополнительная информация об этих группах.

Ближе к реальности В доменной среде локальная учетная запись Администратор (Administrator) используется, в основном, для управления системой непосредственно после ее установки. Это позволяет настроить систему без риска быть заблокированным. Вполне возможно, что после установки системы вы больше никогда не будете использовать эту запись. Вместо этого сделайте своих администраторов членами группы Администраторы (Administrators). Это позволит отзывать административные полномочия, не меняя пароли всех учетных записей Администратор (Administrator).

В системе, являющейся частью рабочей группы, каждый компьютер управляется индивидуально. В большинстве случаев при выполнении обязанностей системного администратора вы будете использовать учетную запись Администратор (Administrator). Здесь будет уже неудобно создавать индивидуальные учетные записи для каждого человека, обладающего административным доступом к системе. Проще использовать одну учетную запись Администратор (Administrator) на каждом компьютере.

Учетная запись Гость (Guest)

Эта учетная запись предназначена для пользователей, которым необходим одноразовый или, по крайней мере, несистематический доступ к системе. Хотя гости обладают ограниченными системными полномочиями, использовать эту учетную запись следует крайне осторожно, поскольку во время ее использования вы все равно подвергаете безопасность системы потенциальному риску. Чтобы снизить этот риск, изначально после установки Windows Server 2008 учетная запись гостя отключена.

По умолчанию учетная запись Гость (Guest) является членом групп Гости домена (Domain Guests) и Гости (Guests). Кроме того, как и все остальные именованные учетные записи, она является членом неявной группы Все (Everyone). Обычно члены группы Все (Everyone) по умолчанию имеют доступ к файлам и папкам. Группа Все (Everyone) также обладает стандартным набором прав пользователя.

Безопасность Если вы решили включить учетную запись Гость (Guest), ограничьте ее использование, а также регулярно меняйте пароль. Как и в случае учетной записи Администратор (Administrator), в качестве дополнительной меры предосторожности следует переименовать гостевую учетную запись.

Встроенные и предопределенные группы

Встроенные и предопределенные группы устанавливаются вместе с ОС Windows Server 2008 и используются для предоставления пользователю определенного набора полномочий и разрешений. Допустим, можно предоставить пользователю административный доступ к системе, сделав его членом локальной группы Администраторы (Administrators).

Неявные группы и специальные идентификаторы

В Windows NT неявные группы назначались во время входа в систему на основании способа, которым пользователь получал доступ к сетевому ресурсу. Например, если пользователь осуществлял интерактивный вход в систему, он автоматически становился членом неявной группы Интерактивные (Interactive). В Windows 2000 и более поздних версиях объектно-ориентированный подход к структуре каталогов изменил первоначальные правила для неявных групп. Вы по-прежнему не можете просматривать состав неявных групп, но имеет право предоставлять членство в них пользователям, группам и компьютерам.

Чтобы отразить изменившуюся роль, неявные группы теперь часто называют *специальными идентификаторами* (special identity). Специальный идентификатор — это группа, членство в которой может быть задано как неявно, например, во время входа в систему, так и явно, посредством разрешений. Как и в случае других стандартных групп, доступность неявной группы зависит от текущей конфигурации. О неявных группах речь пойдет несколько позже.

Возможности учетной записи

Добавляя учетную запись пользователя, вы можете наделить ее владельца конкретными возможностями. Как правило, возможности предоставляются через членство в группах, благодаря чему пользователь обретает все полномочия этих групп. Вы лишаете пользователя возможностей, исключая его из группы.

В Windows Server 2008 учетная запись располагает возможностями следующих видов:

- **Полномочие (priviledge)** Разрешение на выполнение конкретной административной задачи. Полномочия предоставляются учетным записям как пользователей, так и групп. Примером полномочия является возможность завершать работу системы.
- **Право на вход в систему (logon right)** Разрешение на вход в систему. Право на вход может предоставляться как пользователям, так и группам. Примером права на вход является возможность выполнить вход в систему локально.
- **Стандартные возможности (built-in capabilities)** Назначаются группам автоматически. Стандартные возможности предопределены и неизменя-

емы, но их можно делегировать пользователям вместе с разрешением на управление объектами, подразделениями или другими контейнерами. Примером стандартной возможности является возможность создавать и удалять учетные записи пользователей, а также управлять. Она предоставлена администраторам и операторам учетных записей. Из этого следует, что если пользователь является членом группы Администраторы (Administrators), он имеет право на создание, удаление и управление учетными записями пользователей.

- **Разрешение на доступ (access permission)** Определяет действия, которые могут быть выполнены в отношении сетевых ресурсов. Разрешения на доступ предоставляются пользователям, компьютерам и группам. Примером разрешения на доступ является возможность создавать файл в папке. О разрешениях на доступ рассказывается в главе 15.

Администратору приходится ежедневно сталкиваться с возможностями учетной записи. Следующие разделы книги помогут не запутаться во встроенных возможностях. Помните, что вы не можете изменять встроенные возможности группы, но в вашей власти изменить ее стандартные права. Например, администратор может отозвать у группы право на сетевой доступ к компьютеру.

Полномочия

Полномочие представляет собой разрешение на выполнение конкретных административных задач. Полномочия предоставляются посредством групповых политик, которые применяются к отдельным компьютерам, подразделениям и доменам. Вы можете предоставлять полномочия как пользователям, так и группам, но в большинстве случаев полномочия назначаются группам. Назначение полномочий группам облегчает управление учетными записями пользователей.

В табл. 9-2 содержится краткое описание полномочий, которые могут предоставляться пользователям и группам. О назначении полномочий читайте в главе 10.

Табл. 9-2. Полномочия пользователей и групп в Windows Server 2008

Полномочие	Описание
Архивация файлов и каталогов (Back Up Files And Directories)	Позволяет пользователю проводить резервное копирование системы независимо от разрешений, заданных для файлов и каталогов
Блокировка страниц в памяти (Lock Pages In Memory)	Позволяет процессу хранить данные в физической памяти, не давая системе перемещать данные в виртуальную память на диске
Восстановление файлов и каталогов (Restore Files And Directories)	Позволяет пользователю восстанавливать файлы и папки из резервной копии независимо от разрешений, заданных для файлов и папок

Табл. 9-2. (*продолжение*)

Полномочие	Описание
Выполнение задач по обслуживанию томов (Perform Volume Maintenance Tasks)	Позволяет администрировать съемные носители, выполнять дефрагментацию диска и управлять диском
Добавление рабочих станций к домену (Add Workstations To Domain)	Позволяет пользователю добавлять компьютеры в домен
Завершение работы системы (Shut Down The System)	Позволяет пользователю завершать работу локального компьютера
Загрузка и выгрузка драйверов устройств (Load And Unload Device Drivers)	Позволяет пользователю устанавливать и удалять драйверы устройств Plug and Play. Это не касается драйверов других устройств, установить которые может только администратор
Замена маркера уровня процесса (Replace A Process Level Token)	Позволяет процессу заменять стандартные маркеры подпроцессов
Изменение метки объекта (Modify An Object Label)	Позволяет пользовательскому процессу изменять метку целостности объектов, например, файлов, разделов реестра или процессов, принадлежащих другим пользователям. Это полномочие может быть использовано для понижения приоритета других процессов. Процессы, выполняющиеся от имени учетной записи пользователя, могут модифицировать метку любого объекта, принадлежащего данному пользователю, не обладая этим полномочием
Изменение параметров среды изготовителя (Modify Firmware Environment Values)	Позволяет пользователю или процессу изменять переменные аппаратной среды
Изменение системного времени (Change The System Time)	Позволяет пользователю устанавливать время на системных часах
Изменение часового пояса (Change The Time Zone)	Позволяет пользователю устанавливать часовой пояс для системных часов. По умолчанию этим полномочием обладают все пользователи
Имитация клиента после проверки подлинности (Impersonate A Client After Authentication)	Позволяет веб-приложению выступать в роли клиента во время обработки запросов. Выступать в роли клиентов могут также службы и пользователи

Табл. 9-2. (*продолжение*)

Полномочие	Описание
Настройка квот памяти для процесса (Adjust Memory Quotas For A Process)	Позволяет пользователю изменять квоты на использование памяти процессами
Обход перекрестной проверки (Bypass Traverse Checking)	Позволяет пользователю проходить через папки, находящиеся на пути к объекту, независимо от заданных для них разрешений. Это полномочие не позволяет просматривать содержимое папок
Отключение компьютера от стыковочного узла (Remove Computer From Docking Station)	Позволяет отключать ноутбук от стыковочного узла и удалять его из сети
Отладка программ (Debug Programs)	Позволяет пользователю производить отладку
Принудительное удаленное завершение работы (Force Shutdown Of A Remote System)	Позволяет пользователю завершать работу компьютера из удаленного расположения в сети.
Профилирование одного процесса (Profile A Single Process)	Позволяет пользователю следить за выполнением несистемных процессов
Профилирование производительности системы (Profile System Performance)	Позволяет пользователю следить за выполнением системных процессов
Работа в режиме операционной системы (Act As Part Of The Operating System)	Позволяет процессу проходить проверку подлинности как обычному пользователю и точно так же получать доступ к ресурсам. Процесс, требующий такого полномочия, должен использовать учетную запись Локальная система (LocalSystem), которая им уже обладает
Разрешение доверия к учетным записям компьютеров и пользователей при делегировании (Enable User And Computer Accounts To Be Trusted For Delegation)	Позволяет пользователю или компьютеру изменять или применять параметр доверия для делегирования, при условии что у них есть доступ (разрешение на запись в объект)
Синхронизация данных службы каталогов (Synchronize Directory Service Data)	Позволяет пользователю синхронизировать данные службы каталогов на контроллерах домена

Табл. 9-2. (*окончание*)

Полномочие	Описание
Смена владельцев файлов и других объектов (Take Ownership Of Files Or Other Objects)	Позволяет пользователю устанавливать право собственности на файлы и иные объекты Active Directory
Создание аудитов безопасности (Generate Security Audits)	Позволяет процессу создавать записи в журнале безопасности для аудита доступа к объектам
Создание глобальных объектов (Create Global Objects)	Позволяет процессу создавать глобальные объекты. Этим полномочием по умолчанию обладают учетные записи LocalService и NetworkService
Создание маркерного объекта (Create A Token Object)	Позволяет процессу создавать объекты-маркеры, которые могут быть использованы для получения доступа к локальным ресурсам. Требующие данного полномочия процессы должны использовать учетную запись Локальная система (LocalSystem), которая им уже обладает
Создание постоянных общих объектов (Create Permanent Shared Objects)	Позволяет процессу создавать объекты каталога в диспетчере объектов. У большинства компонентов уже имеется это полномочие, и нет нужды присваивать его специально
Создание символических ссылок (Create Symbolic Link)	Позволяет приложению, запущенному пользователем, создавать символические ссылки. Ссылки создают видимость нахождения документа или папки в определенном расположении, тогда как на самом деле они находятся в другом месте. По умолчанию, использование символических ссылок ограничено по соображениям безопасности
Создание файла подкачки (Create A Pagefile)	Позволяет пользователю создавать файл подкачки для виртуальной памяти и изменять его размер
Увеличение приоритета выполнения (Increase Scheduling Priority)	Позволяет процессу повышать приоритет другого процесса, при условии что у него есть доступ (разрешение на запись в данный процесс)
Увеличение рабочего множества процесса (Increase A Process Working Set)	Позволяет пользовательскому приложению увеличивать объем памяти, используемой рабочим набором соответствующего приложения. Рабочий набор представляет собой совокупность страниц физической памяти, видимых процессом в данный момент времени. Увеличение количества страниц памяти уменьшает количество ошибок страниц и повышает производительность
Управление аудитом и журналом безопасности (Manage Auditing And Security Log)	Позволяет пользователю задавать параметры аудита и доступа к журналу безопасности. Предварительно требуется включить аудит в групповой политике

Права на вход в систему

Право на вход (logon right) предоставляется как учетным записям пользователей, так и группам. Как и полномочия, права на вход в систему предоставляются посредством групповых политик.

В табл. 9-3 содержится краткое описание прав на вход. О том, как их назначать, читайте в главе 10.

Табл. 9-3. Права на вход Windows Server 2008 для пользователей и групп

Право на вход	Описание
Вход в качестве пакетного задания (Log On As A Batch Job)	Разрешает вход в систему в качестве пакетного задания или сценария
Вход в качестве службы (Log On As A Service)	Разрешает вход в систему в качестве службы. Учетная запись Локальная система (LocalSystem) обладает этим правом. Службе, которая выполняется от имени другой учетной записью, следует это право предоставить
Доступ к диспетчеру учетных данных от имени доверенного вызывающего (Access Credential Manager As A Trusted Caller)	Разрешает устанавливать доверенное подключение к диспетчеру учетных данных (Credential Manager). Учетные данные, например, имя пользователя и пароль или смарт-карта, обеспечивают идентификацию и подтверждение идентификации
Доступ к компьютеру из сети (Access This Computer From The Network)	Разрешает удаленный доступ к компьютеру
Запретить вход в систему через службу терминалов (Deny Logon Through Terminal Services)	Запрещает вход в систему посредством служб терминалов
Запретить локальный вход (Deny Logon Locally)	Запрещает доступ к клавиатуре компьютера
Локальный вход в систему (Allow Log On Locally)	Предоставляет разрешение на доступ к клавиатуре компьютера. На серверах по умолчанию это право ограничено. Выполнить локальный вход могут только члены групп Администраторы (Administrators), Операторы учеты (Account Operators), Операторы архива (Backup Operators), Операторы печати (Print Operators) и Операторы сервера (Server Operators).
Отказать в доступе к этому компьютеру из сети (Deny Access To This Computer From The Network)	Запрещает удаленный доступ к компьютеру по сети

Табл. 9-3. (*окончание*)

Право на вход	Описание
Отказать во входе в качестве пакетного задания (Deny Logon As Batch Job)	Запрещает вход в систему посредством пакетного задания или сценария
Отказать во входе в качестве службы (Deny Logon As Service)	Запрещает вход в систему в качестве службы
Разрешать вход в систему через службу терминалов (Allow Log On Through Terminal Services)	Предоставляет доступ к системе через службу терминалов. Это необходимо для работы удаленного помощника и удаленного рабочего стола

Стандартные возможности групп Active Directory

Стандартные возможности групп Active Directory весьма обширны. В табл. 9-4 отображены стандартные пользовательские права для групп в доменах Active Directory (как полномочия, так и права на вход). Следует отметить, что любое действие, доступное группе Все (Everyone), доступно всем группам, включая группу Гости (Guests). Это означает, что хотя группа Гости (Guests) и не обладает явным разрешением на доступ к компьютеру или сети, ее члены все-таки могут получать доступ к системе, поскольку это право есть у группы Все (Everyone).

Табл. 9-4. Стандартные права групп Active Directory

Право	Группы, которым оно назначено
Архивация файлов и каталогов (Back Up Files And Directories)	Администраторы (Administrators), Операторы сервера (Server Operators), Операторы архива (Backup Operators)
Восстановление файлов и каталогов (Restore Files And Directories)	Администраторы (Administrators), Операторы сервера (Server Operators), Операторы архива (Backup Operators)
Вход в качестве пакетного задания (Log On As A Batch Job)	Администраторы (Administrators), Операторы архива (Backup Operators), Пользователи журналов производительности (Performance Log Users), IIS_IUSRS
Выполнение задач по обслуживанию томов (Perform Volume Maintenance Tasks)	Администраторы (Administrators)
Добавление рабочих станций к домену (Add Workstations To Domain)	Прошедшие проверку (Authenticated Users)

Табл. 9-4. (*продолжение*)

Право	Группы, которым оно назначено
Доступ к компьютеру из сети (Access This Computer From The Network)	Все (Everyone), Прошедшие проверку (Autentifica-ted Users), Администраторы (Administrators), Пред-Windows 2000 доступ (Pre-Windows 2000 Compatible Access), КОНТРОЛЛЕРЫ ДОМЕНА ПРЕДПРИЯТИЯ (ENTERPRISE DOMAIN CONTROLLERS)
Завершение работы системы (Shut Down The System)	Администраторы (Administrators), Операторы сервера (Server Operators), Операторы печати (Print Operators), Операторы архива (Backup Operators)
Загрузка и выгрузка драйверов устройств (Load And Unload Device Drivers)	Администраторы (Administrators), Операторы печати (Print Operators)
Замена маркера уровня процесса (Replace A Processlevel Token)	LOCAL SERVICE, NETWORK SERVICE
Изменение параметров среды изготовителя (Modify Firmware Environment Values)	Администраторы (Administrators)
Изменение системного времени (Change The System Time)	LOCAL SERVICE, Администраторы (Administrators), Операторы сервера (Server Operators)
Изменение часового пояса (Change The Time Zone)	LOCAL SERVICE, Администраторы (Administrators), Операторы сервера (Server Operators)
Имитация клиента после проверки подлинности (Impersonate A Client After Authentication)	LOCAL SERVICE, NETWORK SERVICE, Администраторы (Administrators), IIS_IUSRS, СЛУЖБА (SERVICE)
Локальный вход в систему (Allow Log On Locally)	Администраторы (Administrators), Операторы учета (Account Operators), Операторы сервера (Server Operators), Операторы печати (Print Operators), Операторы архива (Backup Operators)
Настройка квот памяти для процесса (Adjust Memory Quotas For A Process)	LOCAL SERVICE, NETWORK SERVICE, Администраторы (Administrators)
Обход перекрестной проверки (Bypass Traverse Checking)	Все (Everyone), Прошедшие проверку (Authentica-ted Users), LOCAL SERVICE, NETWORK SERVICE, Администраторы (Administrators), Пред-Windows 2000 доступ (Pre-Windows 2000 Compatible Access)
Отключение компьютера от стыковочного узла (Remove Computer From Docking Station)	Администраторы (Administrators)

Табл. 9-4. (*окончание*)

Право	Группы, которым оно назначено
Отладка программ (Debug Programs)	Администраторы (Administrators)
Принудительное удаленное завершение работы (Force Shutdown From A Remote System)	Администраторы (Administrators), Операторы сервера (Server Operators)
Профилирование одного процесса (Profile Single Process)	Администраторы (Administrators)
Профилирование производительности системы (Profile System Performance)	Администраторы (Administrators)
Разрешать вход в систему через службу терминалов (Allow Log On Through Terminal Services)	Администраторы (Administrators)
Разрешение доверия к учетным записям компьютеров и пользователей при делегировании (Enable User And Computer Accounts To Be Trusted For Delegation)	Администраторы (Administrators)
Смена владельцев файлов и других объектов (Take Ownership Of Files Or Other Objects)	Администраторы (Administrators)
Создание аудитов безопасности (Generate Security Audits)	LOCAL SERVICE, NETWORK SERVICE
Создание глобальных объектов (Create Global Objects)	LOCAL SERVICE, NETWORK SERVICE, Администраторы (Administrators), СЛУЖБА (SERVICE)
Создание символических ссылок (Create Symbolic Links)	Администраторы (Administrators)
Создание файла подкачки (Create A Pagefile)	Администраторы (Administrators)
Увеличение приоритета выполнения (Increase Scheduling Priority)	Администраторы (Administrators)
Увеличение рабочего множества процесса (Increase A Process Working Set)	Пользователи (Users)
Управление аудитом и журналом безопасности (Manage Auditing And Security Log)	Администраторы (Administrators)

В табл. 9-5 перечислены стандартные права пользователей для рабочих групп и рядовых серверов. Приведены как полномочия, так и права на вход.

Табл. 9-5. Стандартные права пользователей для рабочих групп и рядовых серверов

Право пользователя	Группы, которым оно назначено
Доступ к компьютеру из сети (Access This Computer From The Network)	Все (Everyone), Администраторы (Administrators), Пользователи (Users), Операторы архива (Backup Operators)
Настройка квот памяти для процесса (Adjust Memory Quotas For A Process)	LOCAL SERVICE, NETWORK SERVICE, Администраторы (Administrators)
Локальный вход в систему (Allow Log On Locally)	Администраторы (Administrators), Пользователи (Users), Операторы архива (Backup Operators)
Разрешать вход в систему через службу терминалов (Allow Log On Through Terminal Services)	Администраторы (Administrators), Пользователи удаленного рабочего стола (Remote Desktop Users)
Архивация файлов и каталогов (Back Up Files And Directories)	Администраторы (Administrators), Операторы архива (Backup Operators)
Обход перекрестной проверки (Bypass Traverse Checking)	Все (Everyone), LOCAL SERVICE, NETWORK SERVICE, Администраторы (Administrators), Пользователи (Users), Операторы архива (Backup Operators)
Изменение системного времени (Change The System Time)	LOCAL SERVICE, Администраторы (Administrators)
Изменение часового пояса (Change The Time Zone)	LOCAL SERVICE, Администраторы (Administrators)
Создание файла подкачки (Create A Pagefile)	Администраторы (Administrators)
Создание глобальных объектов (Create Global Objects)	LOCAL SERVICE, NETWORK SERVICE, Администраторы (Administrators), СЛУЖБА (SERVICE)
Создание символических ссылок (Create Symbolic Links)	Администраторы (Administrators)
Отладка программ (Debug Programs)	Администраторы (Administrators)
Принудительное удаленное завершение работы (Force Shutdown From A Remote System)	Администраторы (Administrators)
Создание аудитов безопасности (Generate Security Audits)	LOCAL SERVICE, NETWORK SERVICE
Имитация клиента после проверки подлинности (Impersonate A Client After Authentication)	LOCAL SERVICE, NETWORK SERVICE, Администраторы (Administrators), IIS_IUSRS, СЛУЖБА (SERVICE)

Табл. 9-5. (*окончание*)

Право пользователя	Группы, которым оно назначено
Увеличение рабочего множества процесса (Increase A Process Working Set)	Пользователи (Users)
Увеличение приоритета выполнения (Increase Scheduling Priority)	Администраторы (Administrators)
Загрузка и выгрузка драйверов устройств (Load And Unload Device Drivers)	Администраторы (Administrators)
Вход в качестве пакетного задания (Log On As A Batch Job)	Администраторы (Administrators), Операторы архива (Backup Operators), Пользователи журналов производительности (Performance Log Users), IIS_IUSRS
Управление аудитом и журналом безопасности (Manage Auditing And Security Log)	Администраторы (Administrators)
Изменение параметров среды изготовителя (Modify Firmware Environment Values)	Администраторы (Administrators)
Выполнение задач по обслуживанию томов (Perform Volume Maintenance Tasks)	Администраторы (Administrators)
Профилирование одного процесса (Profile Single Process)	Администраторы (Administrators)
Профилирование производительности системы (Profile System Performance)	Администраторы (Administrators)
Отключение компьютера от стыковочного узла (Remove Computer From Docking Station)	Администраторы (Administrators)
Замена маркера уровня процесса (Replace A Process-level Token)	LOCAL SERVICE, NETWORK SERVICE
Восстановление файлов и каталогов (Restore Files And Directories)	Администраторы (Administrators), Операторы архива (Backup Operators)
Завершение работы системы (Shut Down The System)	Администраторы (Administrators), Операторы архива (Backup Operators)
Смена владельцев файлов и других объектов (Take Ownership Of Files Or Other Objects)	Администраторы (Administrators)

В табл. 9-6 перечислены права, которые вы можете предоставить другим пользователям и группам. Изучая таблицу, обратите внимание, что к ограниченным учетным записям относится учетная запись Администратор (Administrator), учетные записи администраторов, а также учетные записи групп Администраторы (Administrators), Операторы сервера (Server Operators), Операторы учета (Account Operators), Операторы архива (Backup Operators) и Операторы печати (Print Operators). Операторы учета (Account Operators) не имеют права изменять эти учетные записи.

Табл. 9-6. Другие возможности встроенных и локальных групп

Задача	Описание	Группа, которой она часто присваивается
Выполнение криптографических операций (Perform Cryptographic Operations)	Позволяет пользователю управлять функциями шифрования	Администраторы Administrators), Криптографические операторы (Cryptographic Operators)
Изменение членства в группах (Modify The Membership Of A Group)	Позволяет пользователю добавлять и удалять пользователей из групп домена	Администраторы (Administrators), Операторы учета (Account Operators)
Наблюдение за журналами производительности (Monitor Performance Logs)	Позволяет пользователю осуществлять контроль за ведением журналов производительности	Администраторы (Administrators), Пользователи системного монитора (Performance Monitor Users)
Назначение прав пользователя (Assign User Rights)	Позволяет пользователю предоставлять права другим пользователям	Администраторы (Administrators)
Переустановка паролей учетных записей (Reset Passwords On User Accounts)	Позволяет пользователю задавать новые пароли для учетных записей пользователей	Администраторы (Administrators), Операторы учета (Account Operators)
Создание и удаление групп (Create And Delete Groups)	Позволяет пользователю создавать новые и удалять существующие группы	Администраторы (Administrators), Операторы учета (Account Operators)
Создание и удаление принтеров (Create And Delete Printers)	Позволяет пользователям создавать и удалять принтеры	Администраторы (Administrators), Операторы сервера (Server Operators), Операторы печати (Print Operators)

Табл. 9-6. (*окончание*)

Задача	Описание	Группа, которой она часто присваивается
Создание, удаление и управление учетными записями пользователей (Create, Delete, And Manage User Accounts)	Позволяет пользователям администрировать учетные записи домена	Администраторы (Administrators), Операторы учета (Account Operators)
Управление журналами производительности (Manage Performance Logs)	Позволяет пользователю настраивать ведение журналов производительности	Администраторы (Administrators), Пользователи журналов производительности (Performance Log Users)
Управление конфигурацией сети (Manage Network Configuration)	Позволяет пользователю настраивать подключение к сети	Администраторы (Administrators), Операторы настройки сети (Network Configuration Operators)
Управление принтерами (Manage Printers)	Позволяет пользователю изменять параметры принтера и управлять очередями на печать	Администраторы (Administrators), Операторы сервера (Server Operators), Операторы печати (Print Operators)
Управление ссылками на групповые политики (Manage Group Policy Links)	Позволяет пользователю применять групповые политики к сайтам, доменам и подразделениям, при условии что у пользователя есть разрешение на запись в соответствующие объекты	Администраторы (Administrators)
Чтение журналов событий (Read Event Logs)	Позволяет пользователю читать журналы событий	Администраторы (Administrators), Читатели журнала событий (Event Log Readers)
Чтение информации о всех пользователях (Read All User Information)	Позволяет пользователю просматривать информацию об учетных записях пользователя	Администраторы (Administrators), Операторы сервера (Server Operators), Операторы учета (Account Operators)

Использование стандартных учетных записей групп

Стандартные учетные записи групп рассчитаны на многоцелевое использование. Добавление пользователя в нужную группу способно существенно облегчить управление рабочей группой или доменом Windows Server 2008. К сожалению, при наличии большого количества групп трудно бывает понять назначение каждой из них. Я предлагаю вам более детально ознакомиться с административными и неявными группами.

Административные группы

Администратор имеет широкий доступ к ресурсам сети, может создавать учетные записи, изменять права пользователей, устанавливать принтеры, управлять общими ресурсами, а также многое другое. Основные административные группы таковы: Администраторы (Administrators), Администраторы домена (Domain Admins) и Администраторы предприятия (Enterprise Admins). В табл. 9-7 приводятся сравнительные характеристики различных административных групп.

Табл. 9-7. Обзор административных групп

Административная группа	Сетевая среда	Область действия	Состав	Администрирование учетной записи
Администраторы (Administrators)	Домены Active Directory	Локальная доменная	Администратор (Administrator), Администраторы домена (Domain Admins), Администраторы предприятия (Enterprise Admins)	Администраторы (Administrators)
Администраторы (Administrators)	Рабочие группы, компьютеры, не являющиеся частью домена	Локальная	Администратор (Administrator)	Администраторы (Administrators)
Администраторы домена (Domain Admins)	Домены Active Directory	Глобальная	Администратор (Administrator)	Администраторы (Administrators)
Администраторы предприятия (Enterprise Admins)	Домены Active Directory	Глобальная или универсальная	Администратор (Administrator)	Администраторы (Administrators)

Совет Локальная учетная запись Администратор (Administrator) и глобальные группы Администраторы домена (Domain Admins) и Администраторы предприятия (Enterprise Admins) являются членами группы Администраторы (Administrators). Учетная запись Администратор (Administrator) нужна для доступа к локальному компьютеру. Членство в группе Администраторы домена (Domain Admins) позволяет другим администраторам получать доступ к системе из любой точки домена. Членство в группе Администраторы предприятия (Enterprise Admins) позволяет другим администраторам получить доступ к системе из других доменов текущего доменного дерева или леса. Для предотвращения доступа к домену из других частей предприятия удалите группу Администраторы предприятия (Enterprise Admins) из группы Администраторы (Administrators).

Группа Администраторы (Administrators) — это локальная группа, предоставляющая полный административный доступ к отдельному компьютеру или домену (в зависимости от ее расположения). Относиться к добавлению пользователей в эту группу следует очень серьезно. Введя человека в эту группу, вы делаете его полноправным администратором локального компьютера или домена. Ее учетную запись могут изменять только члены группы Администраторы (Administrators).

Группа Администраторы домена (Domain Admins) — глобальная группа, созданная для администрирования всех компьютеров в домене. Она обладает административным контролем над всеми компьютерами домена, поскольку по умолчанию является членом группы Администраторы (Administrators). Чтобы сделать кого-либо администратором домена, добавьте его учетную запись в эту группу.

Совет В домене Windows Server 2008 локальный пользователь Администратор (Administrator) по умолчанию является членом группы Администраторы домена (Domain Admins). Это означает, что пользователь, входящий с учетной записью администратора на компьютер, который является членом домена, получает доступ ко всем ресурсам домена. Чтобы избежать этого, удалите локальную учетную запись Администратор (Administrator) из группы Администраторы домена (Domain Admins).

Глобальная группа Администраторы предприятия (Enterprise Admins) позволяет администрировать все компьютеры в дереве домена или лесе, поскольку по умолчанию является членом группы Администраторы (Administrators). Чтобы сделать кого-либо администратором предприятия, добавьте его учетную запись в эту группу.

Совет В домене Windows Server 2008 локальный пользователь Администратор (Administrator) по умолчанию является членом группы Администраторы предприятия (Enterprise Admins). Это означает, что пользователь, входящий с учетной записью администратора на компьютер, который является членом домена, получает доступ ко всем ресурсам дерева домена или леса. Чтобы избежать этого, удалите локальную учетную запись Администратор (Administrator) из группы Администраторы предприятия (Enterprise Admins).

Неявные группы и идентификаторы

В ОС Windows Server 2008 определено несколько специальных идентификаторов, которые в определенных ситуациях можно использовать для предоставления разрешений. Обычно разрешения для специальных идентификаторов назначаются неявно. Тем не менее, это можно сделать и путем редактирования объектов Active Directory. Имеются следующие специальные идентификаторы:

- **Proxy** Пользователи и компьютеры, получающие доступ к ресурсам через прокси. Эта группа применяется при использовании в сети прокси-сервера.
- **Self** Указывает на сам объект и позволяет объекту изменять самого себя.

- **System** Сама операционная система Windows Server 2008. Этот идентификатор используется, когда операционной системе требуется выполнить действие на уровне системы.
- **Анонимный вход (Anonymous Logon)** В эту группу зачисляется любой пользователь, получивший доступ к системе посредством анонимного входа. Она позволяет, например, осуществлять анонимный доступ к вебстраницам, опубликованным на корпоративных серверах.
- **Все (Everyone)** Членами группы Все (Everyone) являются все пользователи, выполнившие вход интерактивно, по сети, при помощи удаленного доступа или проверки подлинности. Это группа предоставляет широкий доступ к ресурсам системы.
- **Группа-создатель (Creator Group)** Windows Server 2008 использует эту группу, чтобы автоматически предоставлять доступ к файлу или папке пользователям, входящим в ту же группу, что и создатель (создатели) файла или папки.
- **Интерактивные (Interactive)** Любой пользователь, выполнивший локальный вход в систему. Данная группа позволяет предоставить доступ к ресурсу только локальным пользователям.
- **Контроллеры домена предприятия (Enterprise Domain Controllers)** Контроллеры домена, выполняющие роли уровня предприятия. Эта группа позволяет выполнять определенные задачи с использованием транзитивного доверия.
- **Ограниченные (Restricted)** Пользователи и компьютеры с ограниченными возможностями.
- **Пакетные файлы (Batch)** Любой пользователь или процесс, получивший доступ к системе в качестве пакетного задания. Эта группа позволяет пакетным заданиям выполнять запланированные задачи, например, очистку диска для удаления временных файлов, выполняющуюся по ночам.
- **Пользователь сервера терминалов (Terminal Server User)** Любой пользователь, выполнивший вход в систему при помощи служб терминалов. Эта группа позволяет пользователям сервера терминалов получать доступ к приложениям и выполнять необходимые действия с использованием служб терминалов.
- **Прошедшие проверку (Authenticated Users)** В эту группу зачисляется любой пользователь, получивший доступ к системе в результате проверки подлинности.
- **Сеть (Network)** Любой пользователь, выполнивший вход в систему по сети. Данная группа позволяет предоставить доступ к ресурсу только удаленным пользователям.
- **Служба (Service)** Любая служба, получившая доступ к системе. Эта группа обеспечивает доступ к процессам, выполняемым службами Windows Server 2008.

- **Создатель-владелец (Creator Owner)** Членом этой неявной группы является пользователь, создавший файл или папку. Она используется в Windows Server 2008 для автоматического предоставления пользователю разрешений на доступ к файлам и папкам, которые он создает.
- **Удаленный доступ (Dial-Up)** Любой пользователь, получивший доступ к системе посредством удаленного подключения. Эта группа отделяет пользователей удаленного доступа от других типов пользователей, прошедших проверку подлинности.

Глава 10

Создание учетных записей и групп

Создание учетных записей — ключевая часть работы администратора. Учетные записи пользователей и групп применяются в Windows Server 2008 для управления пользователями, включая назначение им разрешений и полномочии. Для создания учетных записей, как правило, используются следующие средства:

- Консоль Active Directory — пользователи и компьютеры (Active Directory Users And Computers) предназначена для управления учетными записями в домене службы каталогов Active Directory.
- Консоль Локальные пользователи и группы (Local Users And Groups) предназначена для управления учетными записями на локальном компьютере.

В этой главе речь пойдет как о создании учетных записей домена, так и о создании локальных пользователей и групп.

Настройка и организация учетных записей пользователя

Важным аспектом работы с учетными записями является их организация. Не продумав заблаговременно правила и политики, вы рискуете столкнуться с необходимостью переделывать все учетные записи. Поэтому, приступая к созданию учетных записей, заранее определите политику их настройки и размещения.

Правила именования учетных записей

Планирование системы учетных записей следует начать с разработки схемы их именования. У учетной записи пользователя есть отображаемое имя и имя для входа. *Отображаемое имя* (display name) — это имя, которое видят другие пользователи и которое отображается в сеансах пользователя. *Имя для входа* (logon name) в систему используется для входа в домен. Об именах для входа разговор уже заходил в разделе «Имена для входа, пароли и открытые сертификаты» главы 9.

Правила создания отображаемых имен

Обычно в отображаемое имя учетных записей домена включаются имя, первая буква отчества и фамилия, но вы вольны изменить этот порядок, при условии что в отображаемых именах соблюдаются следующие правила:

- Локальные отображаемые имена должны быть уникальными в пределах компьютера.
- Отображаемые имена домена должны быть уникальными в пределах домена.
- Длина отображаемого имени не должна превышать 64 символов.
- Отображаемое имя может состоять из букв, цифр и специальных символов.

Правила создания имен для входа

Имена для входа должны подчиняться следующим правилам:

- Локальные имена для входа должны быть уникальными в пределах компьютера, глобальные — в пределах домена.
- Имена для входа могут содержать до 256 символов, (хотя на практике редко используются имена длиннее 64 символов).
- Каждой учетной записи дается имя для входа на системы до Windows 2000. По умолчанию оно состоит из первых 20 символов имени для входа. Имена для входа в системы до Windows 2000 должны быть уникальными в пределах домена.
- Пользователи Windows 2000 и более поздних версий, входя в домен, могут использовать стандартные имена для входа или имена для предыдущих версий независимо от режима работы домена.
- Имена для входа не должны содержать следующих символов:
  " / \ [ ] ; | = , + * ? < >
- В именах для входа могут присутствовать все остальные специальные символы, включая пробелы, точки, тире и знаки подчеркивания. Однако пробелы в именах учетных записей лучше не использовать.

Примечание Windows Server 2008 хранит имена пользователей в том регистре, в котором вы их вводите, но при этом имена пользователей не чувствительны к регистру. Например, получить доступ к учетной записи Администратор (Administrator) можно при помощи имени Администратор (Administrator), администратор (administrator) или АДМИНИСТРАТОР (ADMINISTRATOR).

Схемы именования

В большинстве небольших организаций существует тенденция использовать в именах для входа фамилии или имена пользователей. Но в любой организации попадаются тезки, поэтому, чтобы избежать неразберихи с именами, раз и навсегда выберите хорошую схему, а также проследите, чтобы по ней работали и другие администраторы. Процедура именования учетных записей должна быть внутренне согласованной, допускать расширение базы пользователей, исключать возникновение конфликтов и обеспечивать бе-

зопасность имен учетных записей, чтобы их нелегко было угадать. Можно выделить следующие приемлемые схемы именования:

- имя и первая буква фамилии;
- первая буква имени и фамилия;
- инициалы и фамилия;
- инициалы и первые пять букв фамилии;
- имя и фамилия.

Безопасность В средах с повышенными требованиями к безопасности в качестве имени для входа можно использовать числовой код, состоящий, по крайней мере, из 20 символов. Объединив этот строгий способ именования со смарт-картами, вы избавите пользователей от необходимости для входа в домен вводить символы вручную. При этом у пользователей по-прежнему будут удобные для восприятия отображаемые имена.

Политики паролей и учетных записей

Для проверки подлинности учетных записей домена и предоставления доступа к ресурсам сети используются пароли и закрытые ключи. В этом разделе мы поговорим о паролях.

Безопасные пароли

Паролем называется строка, содержащая более 127 символов в Active Directory или до 14 знаков в диспетчере безопасности Windows NT. В паролях могут использоваться буквы (с различием верхнего и нижнего регистров), цифры и спецсимволы. После создания пароля учетной записи Windows Server 2008 сохраняет его в БД учетных записей в зашифрованном виде.

Просто иметь пароль недостаточно. Защитой от несанкционированного доступа к ресурсам сети служит только *безопасный* пароль. Различие между обычным и безопасным паролем заключается в том, что последний трудно подобрать и взломать. Трудные для подбора пароли создаются путем сочетания всех мыслимых типов знаков, включая буквы верхнего и нижнего регистра, цифры и спецсимволы. Например, в качестве пароля лучше использовать не обычное слово, например, happidays, а сложную комбинацию, например, haPPy2Days&, Ha**y!dayS или даже h*PPY%d*ys.

Кроме того, можно использовать в качестве паролей целые предложения, состоящие из нескольких слов и знаков препинания. Например, задайте в качестве пароля фразу: «Сколько будет 99 раз по 10?». Выражение, содержащее знаки препинания и числа, соответствует всем требованиям к сложности пароля. Взломать такой пароль будет совсем не просто.

К сожалению, как бы ни был безопасен пароль, изначально созданный вами, рано или поздно пользователь заменит его своим паролем. Поэтому следует установить такие политики учетных записей, которые вынудят пользователя и свой пароль также сделать максимально безопасным. Политики учетных записей настраиваются посредством групповой политики.

Настройка политик учетных записей

Из предыдущих глав вы уже знаете, что групповые политики применяются на различных уровнях сетевой структуры. Управление локальными групповыми политиками описано в разделе «Управление локальными групповыми политиками» главы 5. С управлением глобальными групповыми политиками вы познакомились в разделе «Управление политиками сайта, домена и подразделения» той же главы.

Политики учетных записей настраиваются в GPO с наивысшим приоритетом в домене. По умолчанию в домене самым высоким приоритетом обладает GPO-объект Default Domain Policy. Получив доступ к объекту Default Domain Policy или другому подходящему объекту GPO, настройте политики учетных записей, выполнив следующие действия:

1. В редакторе политики разверните узлы **Конфигурация компьютера (Computer Configuration)**, **Конфигурация Windows (Windows Settings)**, **Параметры безопасности (Security Settings)** и **Политики учетных записей (Account Policies)**, как показано на рис. 10-1. В дереве консоли указано имя компьютера или домена, который вы настраиваете. Убедитесь, что это именно тот ресурс, который вам нужен.

Примечание Политики домена обладают более высоким приоритетом, чем локальные политики. Объект GPO в домене с порядковым номером ссылки 1, будет всегда преобладать над другими объектами.

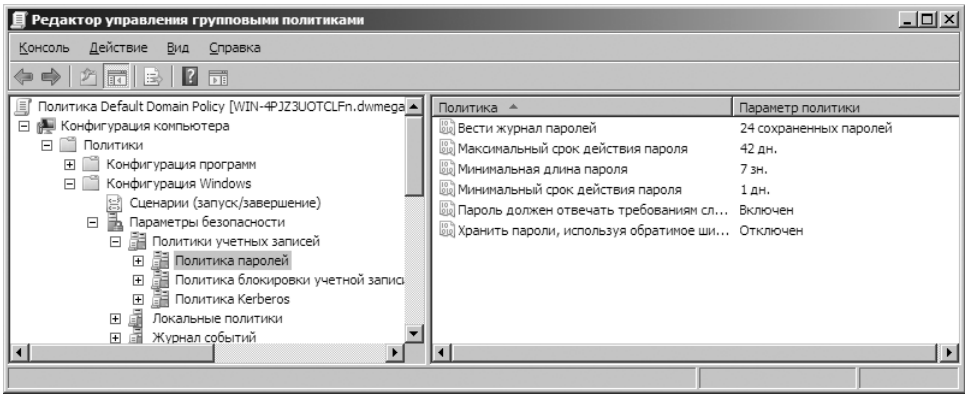


Рис. 10-1. Правила использования паролей и учетных записей задаются в узле Политики учетных записей (Account Policies)

2. Настройте параметры политик учетных записей в узлах **Политика паролей (Password Policy)**, **Политика блокировки учетной записи (Account Lockout Policy)** и **Политика Kerberos (Kerberos Policy)**. Чтобы настроить политику, дважды щелкните соответствующий элемент или щелкните его правой кнопкой и выберите команду **Свойства (Properties)**. Откроется диалоговое окно свойств политики, показанное на рис. 10-2.

Примечание Политики Kerberos не применяются на локальных компьютерах, и потому доступны только в групповых политиках уровня домена. Параметры локальной политики можно изменять на изолированных серверах, но не на контроллерах домена или рядовых серверах.

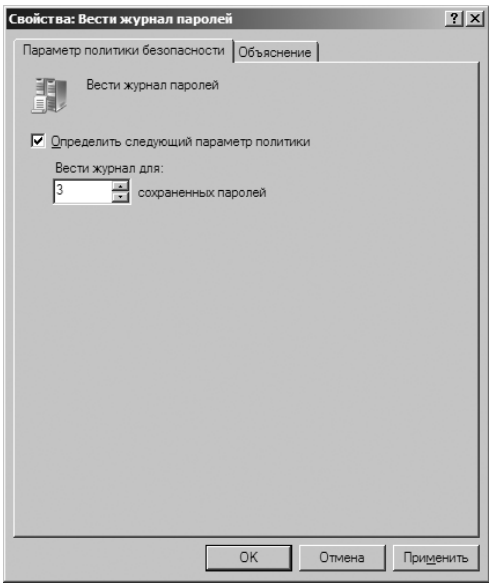


Рис.10-2. Настройка параметров глобальной групповой политики

3. Политика может быть задана (используется) или не задана (не используется). Политика, которая не определена в конкретном контейнере, может быть унаследована из другого контейнера. Установите или сбросьте флажок **Определить следующий параметр политики (Define This Policy Setting)**, чтобы задать политику или отказаться от ее использования.

Совет В окнах свойств политик могут присутствовать дополнительные параметры. Часто в нем имеются переключатели **Включен (Enabled)** и **Выключен (Disabled)**. Переключатель **Включен (Enabled)** активирует ограничение, налагаемое политикой. Переключатель **Выключен (Disabled)** отменяет ограничение. Некоторые политики сформулированы в форме отрицания, поэтому при их включении на самом деле происходит отключение какой-либо возможности. Например, политика **Отказать во входе в качестве службы (Disable Log On As A Service)** представляет собой отрицание политики **Вход в качестве службы (Log On As A Service)**.

Настройка политик учетных записей

Из предыдущего раздела вы знаете, что существует три типа политик учетных записей: политики паролей, политики блокировки учетных записей и политики Kerberos. Далее мы подробно поговорим о том, как настраивать каждую из перечисленных политик.

Настройка политик паролей

Безопасностью паролей управляют следующие политики паролей:

- Вести журнал паролей (Enforce Password History).
- Максимальный срок действия пароля (Maximum Password Age).
- Минимальный срок действия пароля (Minimum Password Age).
- Минимальная длина пароля (Minimum Password Length).
- Пароль должен отвечать требованиям сложности (Passwords Must Meet Complexity Requirements).
- Хранить пароли, используя обратимое шифрование (Store Password Using Reversible Encryption For All Users In The Domain).

В следующих разделах обсуждается использование этих политик.

Вести журнал паролей (Enforce Password History)

Политика Вести журнал паролей (Enforce Password History) устанавливает минимальное количество последовательно используемых неповторяющихся паролей. Она не дает пользователям попеременно использовать несколько паролей. В журнале паролей (password history) ОС Windows Server 2008 способна сохранять до 24 паролей для каждого пользователя.

Чтобы включить ведение журнала паролей, укажите его размер в поле **Сохраненных паролей (Passwords Remembered)**. Чтобы отключить журнал, введите в этой поле нулевое значение.

Примечание Чтобы не дать пользователям обойти политику Вести журнал паролей (Enforce Password History), запретите им изменять пароли немедленно. Иначе они смогут несколько раз подряд изменить пароль, чтобы вернуть ему старое значение. Время между двумя последовательными сменами пароля задается при помощи политики Минимальный срок действия пароля (Minimum Password Age), но об этом — немного позже.

Максимальный срок действия пароля (Maximum Password Age)

Политика Максимальный срок действия пароля (Maximum Password Age) определяет максимальный срок использования пароля, по истечении которого пользователь вынужден будет заменить его. Цель политики — заставить пользователей периодически менять пароли. Выбирайте длительность срока, исходя из потребностей вашей сети. Если безопасность очень важна, используется короткий промежуток времени, если нет — можно задать более длительный интервал.

Максимальный срок действия пароля может варьироваться от 0 до 999. Нулевое значение соответствует неограниченному сроку действия пароля. Не поддавайтесь соблазну не ограничивать срок действия паролей. Пользователи должны регулярно изменять их для укрепления безопасности сети. В сетях с повышенными требованиями к безопасности интервал может составлять 30, 60 или 90 дней. Если безопасность не столь критична, задайте максимальный срок действия пароля 120, 150 или даже 180 дней.

Примечание ОС Windows Server 2008 заблаговременно уведомляет пользователей об окончании срока действия пароля. Когда до истечения срока действия пароля остается менее 30 дней, при каждом входе в систему пользователь видит предупреждение о том, что пароль необходимо сменить в течение определенного количества дней.

Минимальный срок действия пароля (Minimum Password Age)

Политика Минимальный срок действия пароля (Minimum Password Age) определяет, сколько времени пользователь обязан использовать пароль, прежде чем ему разрешено будет его сменить. Эта политика применяется, чтобы не дать пользователю обойти требование смены паролей, введя новый пароль и тут же заменив его обратно на старый.

Если минимальный срок действия пароля равен нулю, пользователь может менять пароли друг за другом. Приемлемый срок действия — от 3 до 7 дней. Это лишит пользователя желания возвращать старые пароли, хотя, конечно, не до конца лишит его такой возможности. Имейте в виду, что минимальный срок действия пароля может помешать пользователю сменить ненадежный пароль. Если пользователь не может изменить пароль, администратору придется сделать это самому.

Минимальная длина пароля (Minimum Password Length)

Политика Минимальная длина пароля (Minimum Password Length) устанавливает минимально допустимое количество символов в пароле. Если вы еще не изменили стандартное значение, сделайте это немедленно. Иногда значение по умолчанию разрешает использовать пустые пароли (пароли с нулевым количеством символов), что, конечно, никуда не годится.

По соображениям безопасности в большинстве случаев следует использовать пароли, состоящие не менее чем из восьми символов. Причина проста: длинные пароли труднее взломать, чем короткие. Если вы хотите как следует укрепить безопасность, установите минимальную длину пароля 14 символов.

Пароль должен отвечать требованиям сложности (Passwords Must Meet Complexity Requirements)

Возможности Windows Server 2008 по управлению паролями не ограничиваются основными политиками паролей и учетных записей. Вы вправе потребовать соответствия паролей следующим правилам:

- Пароль должен быть не короче шести символов.
- Пароль не должен содержать имени пользователя, ни полностью, ни частично.
- В паролях должны быть задействованы, по крайней мере, три из четырех доступных типов символов: буквы верхнего регистра, буквы нижнего регистра, цифры и спецсимволы.

Чтобы обеспечить обязательное выполнение этих правил, включите политику Пароль должен отвечать требованиям сложности (Passwords Must Meet Complexity Requirements).

Хранить пароли, используя обратимое шифрование (Store Password Using Reversible Encryption For All Users In The Domain)

Пароли хранятся в БД в зашифрованном виде. Как правило, обратить шифрование нельзя. Изменение этого параметра потребуется, если в вашей организации используются приложения, которым требуется возможность чтения паролей. В этом случае включите политику Хранить пароли, используя обратимое шифрование (Store Password Using Reversible Encryption For All Users In The Domain).

Если эта политика включена, пароли можно с тем же успехом хранить и в виде простого текста. Это, конечно, представляет угрозу для безопасности. Лучше включать эту возможность только на уровне пользователя и только тогда, когда это действительно требуется.

Настройка политик блокировки учетной записи

Перечисленные ниже политики блокировки учетных записей определяют, как и когда происходит блокировка учетных записей в домене или в локальной системе:

- Пороговое значение блокировки (Account Lockout Threshold).
- Продолжительность блокировки учетной записи (Account Lockout Duration).
- Время до сброса счетчика блокировки (Reset Account Lockout Counter After).

  Эти политики обсуждаются в следующих разделах.

Пороговое значение блокировки (Account Lockout Threshold)

Политика Пороговое значение блокировки (Account Lockout Threshold) задает количество попыток входа в систему до того, как учетная запись будет заблокирована. Подберите для этого параметра компромиссное значение, чтобы желание защитить учетную запись от взлома не затруднило пользователям доступ к компьютерам.

Чаще всего пользователю не удается правильно ввести учетные данные с первого раза из-за забывчивости. Бывает, что вспомнить пароль удается лишь после нескольких попыток. Пользователь рабочей группы может столкнуться с проблемой доступа к удаленной системе, если его текущий пароль не совпадает с паролем, которого ожидает удаленная система. При этом удаленная система может зафиксировать несколько неудачных попыток входа, прежде чем пользователь получит приглашение на ввод правильного пароля, потому что Windows Server 2008 будет автоматически пытаться повторно выполнить вход на удаленную систему. Как правило, в домене этого не случается благодаря возможности единого входа (Single Log-On)

Значение порога блокировки варьируется от 0 до 999. Порог блокировки по умолчанию равен нулю. Это означает, что учетная запись не будет заблокирована при любом количестве неудачных попыток входа в систему. Любое другое значение устанавливает конкретный порог блокировки. Имейте

в виду: чем выше значение порога, тем выше риск взлома системы злоумышленником. Разумный диапазон значений заключен между 7 и 15. Этого достаточно, чтобы исправить ошибку пользователя и помешать злоумышленникам.

Продолжительность блокировки учетной записи (Account Lockout Duration)

Политика Продолжительность блокировки учетной записи (Account Lockout Duration) устанавливает время, на которое блокируется учетная запись, владелец которой нарушил правила входа. Вы можете задать блокировку на определенное время в интервале от 1 до 99999 минут или на неопределенный интервал, установив продолжительность блокировки, равную нулю.

С точки зрения безопасности лучше всего блокировать учетную запись на неопределенный срок. Разблокировать ее сможет только администратор. Таким образом вы предотвратите новые попытки злоумышленника получить доступ к системе, а также заставите заблокированного пользователя обратиться к администратору. Разговор с пользователем выявит, в чем он допустил ошибку, и поможет ему избежать подобной проблемы в дальнейшем.

Совет Чтобы разблокировать учетную запись, откройте диалоговое окно ее свойств при помощи консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**. Перейдите на вкладку **Учетная запись (Account)** и сбросьте флажок **Учетная запись заблокирована (Account Is Locked Out)**.

Время до сброса счетчика блокировки (Reset Account Lockout Counter After)

При каждой неудачной попытке войти в систему Windows Server 2008 увеличивает значение счетчика. Нужно понимать, что блокировка, бесспорно, необходимая из соображений безопасности, может произойти по простой неосторожности пользователя. Существует политика, определяющая, как долго следует «помнить» информацию о неудавшихся попытках входа в систему. Эта политика называется Время до сброса счетчика блокировки (Reset Account Lockout Counter After). Она позволяет сбросить счетчик неудачных попыток входа в систему до нуля по истечению определенного периода времени. Кроме того, счетчик неудавшихся попыток сбрасывается после успешного входа пользователя в систему.

Включив политику Время до сброса счетчика блокировки (Reset Account Lockout Counter After), задайте интервал от 1 до 99999 минут. Как и в случае с политикой Пороговое значение блокировки (Account Lockout Threshold), вам нужно выбрать значение, сочетающее потребности безопасности и нужды доступа пользователей. Разумное значение заключено между одним и двумя часами. Вряд ли у злоумышленника будет столько времени, чтобы дождаться разблокирования учетной записи.

Если политика Время до сброса счетчика блокировки (Reset Account Lockout Counter After) не установлена или отключена, сброс счетчика неудачных попыток входа происходит только после успешного входа пользователя в систему.

Примечание Счетчиком не учитываются неудачные попытки входа в систему из защищенной паролем экранной заставки. Также не учитываются попытки входа, после того как вы заблокировали сервер или рабочую станцию, нажав Ctrl+Alt+Delete.

Настройка политик Kerberos

Технология Kerberos v5 — основной механизм проверки подлинности в домене Active Directory. Для проверки идентификации пользователей и сетевых служб Kerberos v5 использует билеты (ticket), с зашифрованными данными, которые служат для проверки подлинности и авторизации.

Следующие политики позволяют управлять сроком действия, возобновлением и принудительным использованием билетов:

- Принудительные ограничения входа пользователей (Enforce User Logon Restrictions).
- Максимальный срок жизни билета службы (Maximum Lifetime For Service Ticket).
- Максимальный срок жизни билета пользователя (Maximum Lifetime For User Ticket).
- Максимальный срок жизни для возобновления билета пользователя (Maximum Lifetime For User Ticket Renewal).
- Максимальная погрешность синхронизации часов компьютера (Maximum Tolerance For Computer Clock Synchronization).

Эти политики рассмотрены в следующих разделах.

Безопасность Перечисленные выше политики должен изменять только администратор, глубоко разбирающийся в Kerberos. Если установленные вами параметры окажутся неэффективными, это может привести к серьезным проблемам в сети. В большинстве случаев вполне приемлемы параметры Kerberos по умолчанию.

Принудительные ограничения входа пользователей (Enforce User Logon Restrictions)

Политика Принудительные ограничения входа пользователей (Enforce User Logon Restriction) обеспечивает принудительное выполнение всех ограничений, наложенных на учетную запись пользователя. Например, если вход пользователя в систему ограничен по времени, то политика обеспечивает принудительное выполнение этого ограничения. По умолчанию, политика включена, и отключать ее следует только в редких случаях.

Максимальный срок жизни билета

Политики Максимальный срок жизни билета службы (Maximum Lifetime For Service Ticket) и Максимальный срок жизни билета пользователя (Maximum Lifetime For User Ticket) устанавливают максимальную продолжительность времени, в течение которого действителен билет. По умолчанию для билетов служб установлена максимальная продолжительность 600 минут, а для билетов пользователей — 10 часов.

Время жизни билетов можно изменять. Для билетов служб допустимый диапазон составляет от 0 до 99999 минут, для билетов пользователей — от 0 до 99999 часов. Значение «ноль» соответствует неограниченному времени жизни.

Билеты с истекшим сроком действия могут возобновляться, при условии что возобновление состоится в интервале времени, заданном политикой Максимальный срок жизни для возобновления билета пользователя (Maximum Lifetime For User Ticket Renewal). Стандартный срок возобновления составляет семь дней, но вы можете задать значение от 0 до 99999 дней. Значение «ноль» соответствует неограниченному сроку возобновления.

Допустимое отклонение часов при проведении синхронизации

Политика Максимальная погрешность синхронизации часов компьютера (Maximum Tolerance For Computer Clock Synchronization) — редкий пример политики Kerberos, которую, вероятно, придется изменить. По умолчанию компьютеры в домене должны синхронизироваться каждые пять минут. В противном случае происходит сбой проверки подлинности.

Если у вас есть удаленные пользователи, которые входят в систему без синхронизации часов с сетевым сервером времени, вам придется установить допустимое отклонение. Вы вольны задать любое значение от 0 до 99999. Значение «ноль» указывает, что допустимого отклонения разности часов не существует и удаленные пользователи должны быть точно синхронизированы по времени, иначе проверка подлинности не состоится.

Настройка прав пользователей

В главе 9 рассказывалось о встроенных возможностях и правах пользователей. Вы не вольны изменить встроенные возможности учетных записей, но можете администрировать права пользователей в учетных записях. Обычно вы предоставляете пользователям права, делая их членами соответствующей группы или групп. Кроме того, можно предоставлять права и напрямую.

Безопасность Все пользователи, входящие в группу, которой предоставлено определенное право, также обладают этим правом. Следует помнить, что изменения, вносимые в права пользователя, могут иметь далеко идущие последствия. Поэтому вносить изменения в права пользователя должны только опытные администраторы.

Назначение прав пользователей производится в узле **Локальные политики (Local Policies)** редактора групповой политики. Как видно из названия, локальные политики относятся к локальному компьютеру. Но это не помешает вам настроить локальные политики и импортировать их в Active Directory. Вы также можете настроить локальные политики как часть существующей групповой политики сайта, домена или подразделения. При этом локальные политики применяются к учетным записям компьютеров в сайте, домене или подразделении.

Чтобы настроить политики прав пользователей, выполните следующие действия:

1. Откройте групповую политику, с которой хотите работать. Последовательно разверните узлы **Конфигурация компьютера (Computer Configuration)**, **Конфигурация Windows (Windows Settings)**, **Параметры безопасности (Security Settings)** и **Локальные политики (Local Policies)**.
2. Выделите узел **Назначение прав пользователя (User Rights Assignment)**. Чтобы настроить право пользователя, щелкните его дважды или щелкните правой кнопкой и выберите команду **Свойства (Properties)**. Откроется диалоговое окно **Свойства (Properties)**.
3. Настройте право пользователя. Для настройки локальных прав выполните шаги 1–4 из раздела «Локальная настройка прав пользователя» этой главы. Для настройки глобальных прав выполните шаги 1–6 из следующего раздела.

Глобальная настройка прав пользователя

Чтобы настроить права пользователя в сайте, домене или подразделении, выполните следующие действия:

1. Откройте диалоговое окно свойств права пользователя, подобное тому, что показано на рис. 10-3. Если политика не определена, установите флажок **Определить следующие параметры политик (Define These Policy Settings)**.

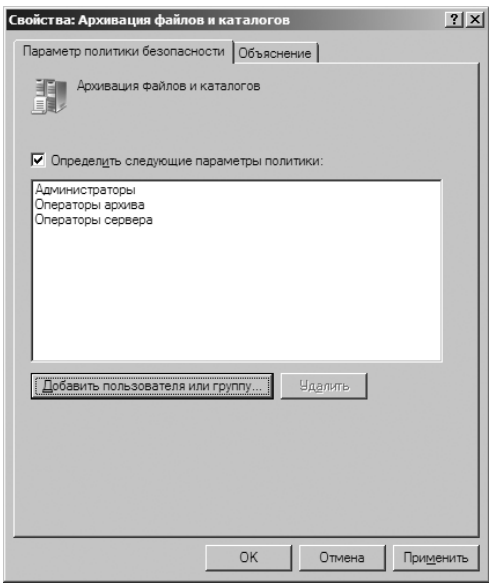


Рис. 10-3. Определите право пользователя и примените его к пользователям и группам

2. Чтобы применить право к пользователю или группе, щелкните кнопку **Добавить пользователя или группу (Add User Or Group)**. В диалоговом окне **Добавление пользователя или группы (Add User Or Group)** щелк-

ните кнопку **Обзор (Browse)**. Откроется диалоговое окно **Выбор: «Пользователи», «Компьютеры» или «Группы» (Select Users, Computers, Or Groups)**, показанное на рис. 10-4.

Безопасность Брандмауэр Windows, работающий на контроллере домена может помешать вам воспользоваться диалоговым окном **Выбор: «Пользователи», «Компьютеры» или «Группы» (Select Users, Computers, Or Groups)**, если вы работаете удаленно. Вам придется настроить на контроллере домена исключение для входящего порта TCP 445. Разверните узлы **Конфигурация компьютера\Административные шаблоны\Сеть\Сетевые подключения\Брандмауэр Windows\Профиль домена (Computer Configuration\Administrative Templates\Network\Network Connections\ Windows Firewall\Domain Profile)**. В области сведений дважды щелкните политику **Брандмауэр Windows: Разрешить исключение для входящих сообщений удаленного администрирования (Windows Firewall: Allow Remote Administration Exception)** и установите переключатель **Включен (Enabled)**. Существует и другой способ настройки исключения: введите в командной строке **netsh firewall set portopening tcp 445 smb enable**. Дополнительную информацию вы найдете в статье 840634 Базы знаний Майкрософт (*http://support.microsoft.com/default.aspx?scid=kb;en-us;840634*).

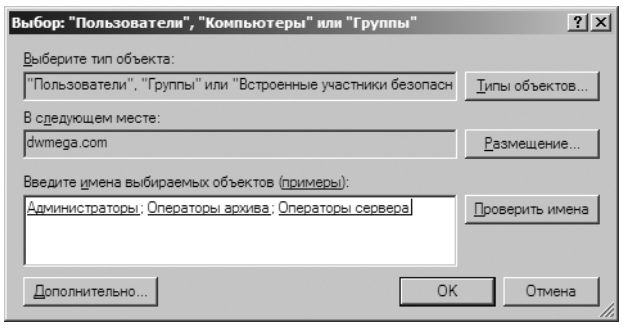


Рис. 10-4. Выберите нужных пользователей и группы

3. Введите имя пользователя или группы, которую хотите использовать, и щелкните **Проверить имена (Check Names)**. По умолчанию поиск проводится среди встроенных участников безопасности и учетных записей пользователей. Для добавления групп в область поиска щелкните кнопку **Типы объектов (Object Types)** в окне списка, установите флажок **Группы (Groups)** и щелкните **OK**.
4. Добавив все нужные имена учетных записей и групп, щелкните **OK**. Выбранные учетные записи будут отображены в диалоговом окне **Добавление пользователя или группы (Add User Or Group)**. Снова щелкните **OK**.
5. Ваш выбор будет отображен в диалоговом окне свойств. Если вы сделали ошибочный выбор, выделите имя и щелкните кнопку **Удалить (Remove)**.
6. Указав всех нужных пользователей, щелкните **OK**.

Локальная настройка прав пользователя

Чтобы применить права пользователя на локальном компьютере, выполните следующие действия:

1. Откройте диалоговое окно свойств права пользователя (см. рис. 10-5). Помните, что политики сайта, домена и подразделения обладают приоритетом по отношению к локальным политикам.
2. В диалоговом окне свойств отображены текущие пользователи и группы, которым предоставлено право. Чтобы удалить пользователя или группу из списка, выделите их и щелкните **Удалить (Remove)**.
3. Чтобы применить право пользователя к другим пользователям и группам, щелкните кнопку **Добавить пользователя или группу (Add User Or Group)**. В диалоговом окне **Добавление пользователя или группы (Add User Or Group)** щелкните кнопку **Обзор (Browse)**. Откроется диалоговое окно **Выбор: «Пользователи», «Компьютеры» или «Группы» (Select Users, Computers, Or Groups)**, показанное на рис. 10-4. Добавьте пользователей и группы.

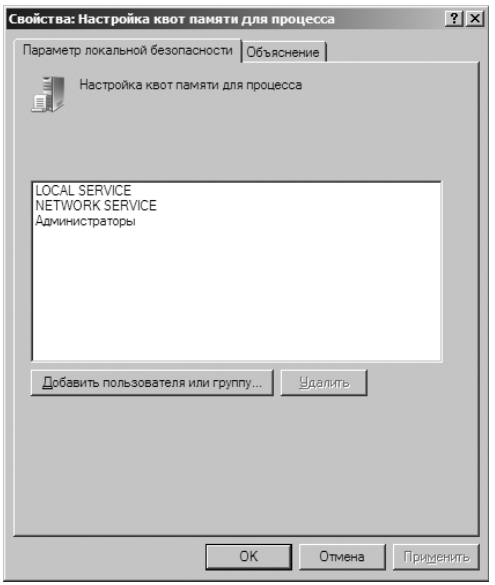


Рис. 10-5. Определите право пользователя и примените его к пользователям и группам

Добавление учетной записи пользователя

Для каждого пользователя, который будет использовать ресурсы вашей сети, требуется создать учетную запись. Учетные записи пользователей домена создаются в консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**. Локальные учетные записи пользователей создаются в консоли **Локальные пользователи и группы (Local Users And Groups)**.

Создание доменной учетной записи

Существует два основных способа создания доменной учетной записи:

- **Создание учетной записи пользователя «с нуля»** Чтобы создать учетную запись пользователя «с нуля», щелкните правой кнопкой контейнер, в который хотите поместить учетную запись, выберите команду **Создать (New)** и **Пользователь (User)**. Откроется мастер Новый объект — Пользователь (New Object — User Wizard), окно которого показано на рис. 10-6. При создании новой учетной записи используются стандартные системные параметры.
- **Создание новой учетной записи на основе существующей** В консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** щелкните правой кнопкой учетную запись пользователя, которую хотите взять за основу, и выберите команду **Копировать (Copy)**. Откроется мастер Копировать объект — Пользователь (Copy Object — User Wizard), который, в целом, похож на мастер Новый объект — Пользователь (New Object — User Wizard). Разница в том, что при копировании новая учетная запись принимает значения большинства параметров от существующей учетной записи. Дополнительную информацию о копировании учетных записей вы найдете в разделе «Копирование доменных учетных записей пользователя» главы 11.

Чтобы создать учетную запись в мастерах Новый объект — Пользователь (New Object — User Wizard) или Копировать объект — Пользователь (Copy Object — User Wizard), выполните следующие действия:

1. На первой странице мастера задаются отображаемое имя пользователя и имя для входа в систему (рис. 10-6). Введите в соответствующие поля имя пользователя, первую букву отчества и фамилию. Эти поля используются для создания полного отображаемого имени пользователя.

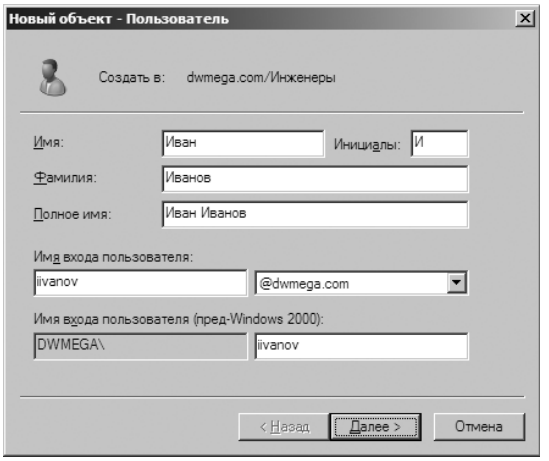


Рис. 10-6. Задайте отображаемое имя и имя для входа в систему

2. При необходимости внесите изменения в поле **Полное имя (Full Name)**. Полное имя должно быть уникальным в домене, и его длина не должна превышать 64 символов.
3. В поле **Имя входа пользователя (User Logon Name)** введите имя для входа пользователя. В раскрывающемся списке выберите домен, с которым будет связана учетная запись. Так будет задано полное имя для входа в систему.
4. Первые 20 символов имени входа используются для создания имени для входа в системы до Windows 2000. Это имя также должно быть уникальным в пределах домена. При необходимости измените имя, предназначенное для более ранних версий Windows.

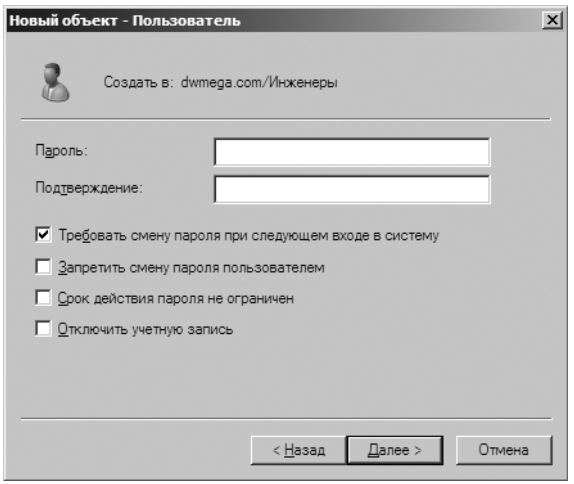


Рис. 10-7. Настройка пароля пользователя в мастере Новый объект — Пользователь (New Object — User Wizard)

5. Щелкните **Далее (Next)**. На странице мастера, показанной на рис.10-7, задайте пароль пользователя. Параметры этой страницы таковы:
   - **Пароль (Password)** Пароль учетной записи. Должен соответствовать правилам политики паролей.
   - **Подтверждение (Confirm Password)** Служит для проверки правильности ввода пароля. Введите пароль еще раз, чтобы подтвердить его.
   - **Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon)** Если установлен этот флажок, пользователь должен будет изменить пароль после входа в систему.
   - **Запретить смену пароля пользователем (User Cannot Change Password)** Если установлен этот флажок, пользователь не может изменять пароль.
   - **Срок действия пароля неограничен (Password Never Expires)** Если установлен этот флажок, пароль учетной записи не имеет срока дейст-

вия. Этот параметр перекрывает политику учетной записи домена. Лучше не создавать пароли без срока действия — при этом теряется смысл установки пароля как такового.

- **Отключить учетную запись (Account Is Disabled)** Если установлен этот флажок, учетная запись отключена и не может быть использована. Используйте это поле для наложения временного запрета на использование учетной записи.

6. Щелкните **Далее (Next)** и **Готово (Finish)**, чтобы создать учетную запись. При возникновении проблем в создании учетной записи вы увидите сообщение об этом. При необходимости щелкните **Назад (Back)**, чтобы ввести исправленную информацию.

Создав учетную запись, задайте ее дополнительные параметры. Подробнее — далее в этой главе.

Создание локальной учетной записи

Локальные учетные записи пользователей создаются в консоли **Локальные пользователи и группы (Local Users And Groups)**. Чтобы создать локальную учетную запись, выполните следующие действия:

1. Щелкните **Пуск (Click Start)**, **Все программы (All Programs)**, **Администрирование (Administrative Tools)** и **Управление компьютером (Computer Management)**.
2. Щелкните правой кнопкой узел **Управление компьютером (Computer Management)** в дереве консоли и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. Укажите систему, локальными учетными записями которой хотите управлять. На контроллерах домена не бывает локальных пользователей и групп.
3. Разверните узел **Служебные программы (System Tools)** и выделите элемент **Локальные пользователи и группы (Local Users And Groups)**.
4. Щелкните правой кнопкой элемент **Пользователи (Users)** и выберите команду **Новый пользователь (New User)**. Откроется одноименное диалоговое окно, показанное на рис. 10-8. Ниже приведены описания его полей:
   - **Пользователь (User Name)** Имя для входа в систему. Должно соответствовать принятым в компании правилам.
   - **Полное имя (Full Name)** Полное имя пользователя, например, William R. Stanek.
   - **Описание (Description)** Описание пользователя. Как правило, здесь вводится должность пользователя, например, веб-мастер. К должности можно добавить отдел.
   - **Пароль (Password)** Пароль учетной записи. Должен соответствовать правилам политики паролей.
   - **Подтверждение (Confirm Password)** Служит для проверки правильности ввода пароля. Введите пароль еще раз, чтобы подтвердить его.

- **Требовать смены пароля при следующем входе в систему (User Must Change Password At Next Logon)** Если установлен этот флажок, пользователь должен будет изменить пароль после входа в систему.
- **Запретить смену пароля пользователем (User Cannot Change Password)** Если установлен этот флажок, пользователь не сможет изменить пароль.
- **Срок действия пароля неограничен (Password Never Expires)** Если установлен этот флажок, пароль учетной записи не имеет срока действия. Этот параметр перекрывает политику локальной учетной записи.
- **Отключить учетную запись (Account Is Disabled)** Если установлен этот флажок, учетная запись отключена и не может быть использована. Используйте этот флажок для временного запрета на использование учетной записи.

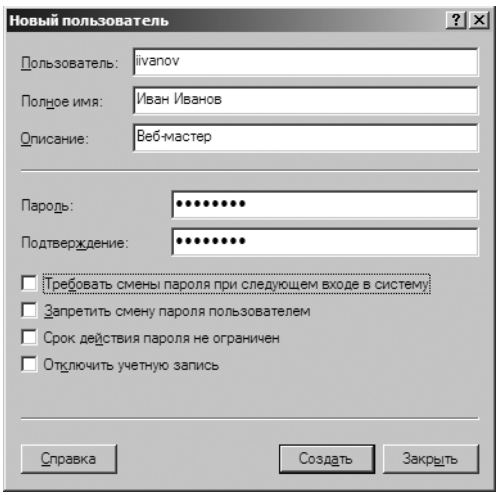


Рис. 10-8. Настройка локальной учетной записи отличается от настройки учетной записи пользователя домена

5. Завершив настройку новой учетной записи, щелкните **Создать (Create)**.

Добавление учетной записи группы

Группы используются для одновременного управления полномочиями нескольких пользователей. Учетные записи глобальных групп создаются в консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**. Учетные записи локальных групп создаются в консоли **Локальные пользователи и группы (Local Users And Groups)**.

Приступая к созданию учетных записей групп, помните, что вы создаете учетные записи для сходных типов пользователей. Создаваемые группы могут подразделяться на следующие типы:

- **Группы, представляющие отделы организации** В большинстве случаев пользователи, работающие в одном отделе, нуждаются в доступе к одним и тем же ресурсам. Поэтому вы можете создать группы на основе отделов, например, разработки, продаж, маркетинга и инженерно-технического.
- **Группы для пользователей отдельных приложений** Создавая группы на для конкретного приложения, вы обеспечите надлежащий доступ пользователей к необходимым ресурсам и файлам.
- **Группы, представляющие роли внутри организации** Кроме того, группы можно организовать в соответствии с ролью пользователя в организации. В частности, руководители наверняка нуждаются в доступе к иным ресурсам, чем обычные пользователи.

Создание глобальной группы

Чтобы создать глобальную группу, выполните следующие действия:

1. Откройте консоль **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**. Щелкните правой кнопкой контейнер, в котором хотите поместить учетную запись группы, и выберите команды **Создать (New)** и **Группа (Group)**. Откроется диалоговое окно **Новый объект — Группа (New Object — Group)**, показанное на рис. 10-9.

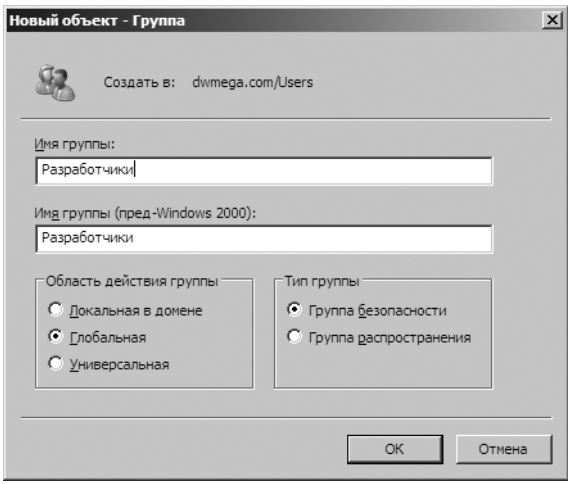


Рис. 10-9. Диалоговое окно Новый объект — Группа (New Object — Group) позволяет добавить в домен новую группу

2. Введите имя группы. Имена учетных записей групп должны следовать тем же правилам именования, что и отображаемые имена учетных записей пользователей. Регистр в них не различается. Они могут содержать до 64 символов.
3. Первые 20 символов имени группы используются для создания имени группы в системах до Windows 2000. Имя группы должно быть уникальным в пределах домена. При необходимости измените имя для ранних версий Windows.

4. Выберите область действия группы (локальная в домене, глобальная или универсальная).
5. Выберите тип группы (безопасности или распространения).
6. Щелкните **OK**, чтобы создать группу. Создав учетную запись, добавьте в нее членов и задайте дополнительные параметры. Подробнее — далее в этой главе.

Создание локальной группы и добавление в нее участников

Локальные группы создаются в консоли **Локальные пользователи и группы (Local Users And Groups)**. Выполните следующие действия:

1. Щелкните **Пуск (Click Start)**, **Все программы (All Programs)**, **Администрирование (Administrative Tools)** и **Управление компьютером (Computer Management)**.
2. Щелкните правой кнопкой узел **Управление компьютером (Computer Management)** в дереве консоли и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. Укажите систему, локальными учетными записями которой хотите управлять. На контроллерах домена не бывает локальных пользователей и групп.
3. Разверните узел **Служебные программы (System Tools)** и выделите элемент **Локальные пользователи и группы (Local Users And Groups)**.
4. Щелкните правой кнопкой элементы **Группы (Groups)** и выберите команду **Создать группу (New Group)**. Откроется диалоговое окно **Новая группа (New Group)**, показанное на рис. 10-10.

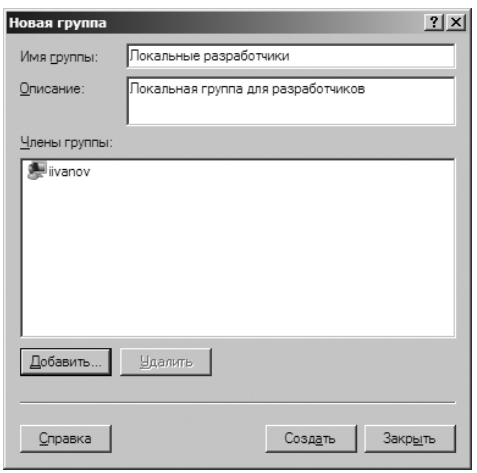


Рис. 10-10. В диалоговом окне Новая группа (New Group) вы добавляете на компьютер новую локальную группу

5. Введя имя и описание группы, щелкните кнопку **Добавить (Add)**, чтобы добавить членов группы. Откроется диалоговое окно **Выбор: «Пользователи» (Select Users)**.

6. Введите в поле **Имя (Name)** имя нужного пользователя и щелкните кнопку **Проверить имена (Check Names)**. Выделите нужную учетную запись и щелкните **OK**. Если совпадения не обнаружены, введите имя заново и попробуйте выполнить поиск еще раз. Выберите всех нужных пользователей и щелкните **OK**.
7. Если вы выбрали пользователя ошибочно, выделите его имя и щелкните кнопку **Удалить (Remove)**.
8. Завершив добавление и удаление членов группы, щелкните **Создать (Create)**.

Определение состава глобальной группы

Для настройки членства в группе используется консоль **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**. Работая с группами, имейте в виду следующее:

- Новые пользователи домена являются членами группы Пользователи домена (Domain Users). Это их основная группа.
- Новые рабочие станции и рядовые серверы домена являются членами группы Компьютеры домена (Domain Computers). Это их основная группа.
- Новые контроллеры домена являются членами группы Контроллеры домена (Domain Controllers). Это их основная группа.

В консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** имеется несколько способов управления членством в группах:

- выбор групп для учетной записи;
- выбор учетных записей для группы;
- установка основной группы для пользователей и компьютеров.

Выбор групп для учетной записи

Чтобы быстро добавить пользователя или группу в одну или несколько групп, щелкните правой кнопкой нужную учетную запись и выберите команду **Добавить в группу (Add To Group)**. Откроется диалоговое окно **Выбор: «Группы» (Select Groups)**, очень похожее на диалоговое окно **Выбор: «Пользователи» (Select Users Or Groups)**, о котором говорилось ранее. Укажите группы, членом которых должна быть выбранная учетная запись.

Чтобы управлять членством учетной записи любого типа, выполните следующие действия:

1. Дважды щелкните учетную запись пользователя, группы или компьютера в консоли Active Directory — **пользователи и компьютеры (Active Directory Users And Computers)**. Откроется диалоговое окно свойств учетной записи.
2. Перейдите на вкладку **Член групп (Member Of)**.

3. Чтобы сделать учетную запись членом группы, щелкните кнопку **Добавить (Add)**. Откроется диалоговое окно **Выбор: «Группы» (Select Groups)**. Укажите группы, членом которых должна быть выбранная учетная запись.
4. Чтобы удалить учетную запись из группы, выделите группу и щелкните кнопку **Удалить (Remove)**.
5. Щелкните **OK**.

Если вы работаете исключительно с учетными записями пользователей, добавляйте пользователей в группы при помощи следующих действий:

1. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** выделите все учетные записи пользователей, с которыми собираетесь работать.

Совет Чтобы выбрать несколько пользователей по отдельности, нажмите и удерживайте клавишу **Ctrl**, а затем щелкните левой кнопкой мыши все нужные вам учетные записи пользователя. Чтобы выделить несколько смежных учетных записей, удерживая нажатой клавишу **Shift**, щелкните первую и последнюю учетную запись.

2. Правой кнопкой щелкните одну из выбранных учетных записей и выберите команду **Добавить в группу (Add To Group)**. Откроется диалоговое окно **Выбор: «Группы» (Select Groups)**. Укажите группы, членами которых должны быть выбранные вами учетные записи.
3. Щелкните **OK**.

Выбор учетных записей для группы

Другой способ управления членством в группах предоставляет диалоговое окно свойств. В нем можно добавить или удалить несколько учетных записей, выполнив следующие действия:

1. Дважды щелкните элемент группы в консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**. Откроется диалоговое окно свойств группы.
2. Перейдите на вкладку **Члены группы (Members)**.
3. Щелкните кнопку **Добавить (Add)**. Откроется диалоговое окно **Выбор: «Пользователи», «Компьютеры» или «Группы» (Select Users, Computers, Or Groups)**. Укажите пользователей, компьютеры и группы, которые следует добавить в выбранную вами группу.
4. Чтобы удалить членов из группы, выберите соответствующую учетную запись и щелкните **Удалить (Remove)**.
5. Щелкните **OK**.

Установка основной группы для пользователей и компьютеров

Пользователи, получающие доступ к Windows Server 2008 через службы Macintosh, используют основные группы (primary group). Когда пользо-

ватель Macintosh создает файлы или папки в системе под управлением Windows Server 2008, этим файлам и папкам назначается основная группа.

Основная группа должна назначаться всем учетным записям пользователей и компьютеров, независимо от того, получают они доступ к системе Windows Server 2008 через Macintosh или нет. Эта группа быть глобальной или универсальной, как, например, группы Пользователи домена (Domain Users) или Компьютеры домена (Domain Computers).

Чтобы задать основную группу, выполните следующие действия:

1. Дважды щелкните элемент пользователя или компьютера в консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**. Откроется диалоговое окно свойств учетной записи.
2. Перейдите на вкладку **Член групп (Member Of)**
3. В списке **Член групп (Member Of)** выберите группу с глобальной или универсальной областью действия.
4. Щелкните кнопку **Задать основную группу (Set Primary Group)**.

Все пользователи обязаны быть членами, по крайней мере, одной основной группы. Нельзя аннулировать членство в основной группе, предварительно не зачислив пользователя в другую основную группу. Для этого выполните следующие действия:

1. В списке **Член групп (Member Of)** выберите другую группу с глобальной или универсальной областью действия и щелкните кнопку **Задать основную группу (Set Primary Group)**.
2. В списке **Член групп (Member Of)** выделите бывшую основную группу и щелкните **Удалить (Remove)**.

Глава 11

Управление учетными записями пользователей и групп

В идеальном мире, единожды создав учетные записи пользователей и групп, вы никогда более к ним не возвращаетесь. К сожалению, на практике создание учетных записей — это лишь начало пути, и в будущем вам предстоит потратить массу времени на управление ими. В этой главе содержатся инструкции и советы, призванные облегчить ваш труд.

Управление контактной информацией пользователя

Active Directory — это служба каталогов. Создавая учетные записи пользователей, вы можете сопроводить их подробной контактной информацией, которая будет доступна всем пользователям дерева или леса. Ее можно использовать для создания записей адресной книги или в качестве критерия для поиска пользователей.

Задание контактной информации

Чтобы задать контактную информацию учетной записи, выполните следующие действия:

1. Дважды щелкните имя пользователя в консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)**. Откроется диалоговое окно свойств учетной записи.
2. Перейдите на вкладку **Общие (General)**, показанную на рис. 11-1. Укажите контактную информацию в следующих полях:
   - **Имя (First Name), Инициалы (Initials), Фамилия (Last Name)** Полное имя пользователя.
   - **Выводимое имя (Display Name)** Имя пользователя, которое отображается в сеансах пользователя и в службе каталогов Active Directory.
   - **Описание (Description)** Описание пользователя.
   - **Комната (Office)** Расположение офиса пользователя.
   - **Номер телефона (Telephone Number)** Основной служебный номер телефона пользователя. Если у пользователя есть и другие номера

телефонов, которые нужно указать, щелкните **Другой (Other)** и введите дополнительные номера телефонов в диалоговом окне **Номер телефона (прочие) (Phone Number (Others))**.

- **Эл. почта (E-Mail)** Служебный адрес электронной почты.
- **Веб-страница (Web Page)** URL домашней страницы пользователя в Интернете или корпоративной интрасети. Если у пользователя есть и другие веб-страницы, которые нужно указать, щелкните **Другой (Other)** и введите дополнительные адреса веб-страниц в диалоговом окне **Адрес страницы в Интернете (прочие) (Web Page Address (Others))**.

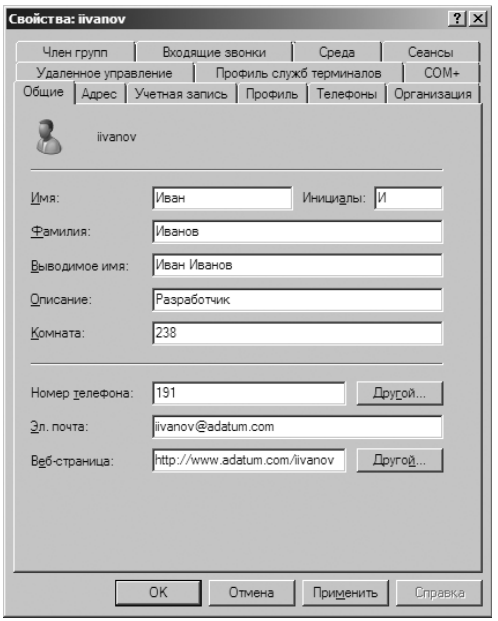


Рис. 11-1. Настройка общей информации о пользователе

Совет Если вы собираетесь использовать функции **Отправить почту (Send Mail)** и **Открыть домашнюю страницу (Open Home Page)** консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)**, обязательно заполните поля **Эл. почта (E-Mail)** и **Веб-страница (Web Page)**. Подробнее — в разделе «Обновление учетных записей пользователей и групп» этой главы.

3. Перейдите на вкладку **Адрес (Address)** и укажите служебный или домашний адрес пользователя. Обычно вводится служебный адрес, что позволяет отслеживать местоположения предприятий и почтовые адреса пользователей в различных офисах.

Примечание Прежде чем вводить домашний адрес пользователя, подумайте о его праве на личную жизнь. Обсудите этот вопрос с отделом кадров и юридическим отделом. Кроме того, для предоставления домашних адресов вам, вероятно, понадобится согласие самих пользователей.

4. Перейдите на вкладку **Телефоны (Telephones)**. Введите основные телефонные номера для связи с пользователем, например, номера домашнего и мобильного телефонов, пейджера, факса или Интернет-телефона.
5. При необходимости укажите другие номера для каждого типа телефонного номера, щелкнув соответствующую кнопку **Другой (Other)** и введя дополнительные номера телефонов в открывшемся диалоговом окне.
6. Перейдите на вкладку **Организация (Organization)**. Введите должность пользователя, отдел и компанию.
7. Чтобы указать руководителя пользователя, щелкните кнопку **Изменить (Change)** и выберите руководителя в диалоговом окне **Выбор: «Пользователь» или «Контакт» (Select User Or Contact)**. Когда вы укажете руководителя, пользователь будет отображен в учетной записи этого руководителя в качестве прямого подчиненного.
8. Щелкните **Применить (Apply)** или **OK**, чтобы изменения вступили в силу.

Поиск пользователей и групп в Active Directory

Чтобы найти пользователя или группу в Active Directory, выполните следующие действия:

1. В **консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** щелкните правой кнопкой нужный домен или контейнер и выберите команду **Найти (Find)**.
2. Выбранный домен или контейнер отображается в раскрывающемся списке **Где (In)** диалогового окна **Поиск: Пользователи, контакты и группы (Find Users, Contacts, And Groups)**. Чтобы провести поиск по всему каталогу, выберите **Целиком Active Directory (Entire Directory)**. Можно также выбрать для поиска другой домен или контейнер, щелкнув кнопку **Обзор (Browse)**.
3. На вкладке **Пользователи, контакты и группы (Users, Contacts, and Groups)** введите имя пользователя, контакта или группы, которых хотите найти.

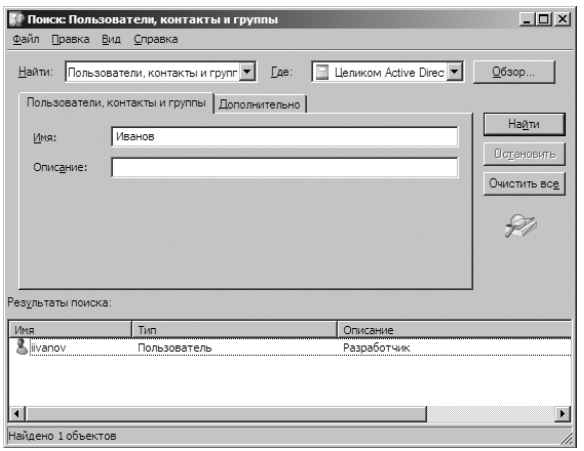


Рис. 11-2. Поиск пользователей в Active Directory

4. Щелкните **Найти (Find Now)**, чтобы начать поиск. Результаты поиска отображаются в окне, показанном на рис. 11-2. Если найти ничего не удалось, исправьте параметры поиска.
5. Чтобы просмотреть свойства найденной учетной записи, щелкните ее правой кнопкой и выберите команду **Свойства (Properties)**.

Настройка параметров среды пользователя

Помимо перечисленных выше параметров, с учетными записями пользователей могут быть связаны профили, сценарии входа и домашние папки. Чтобы настроить эти необязательные параметры, дважды щелкните отображаемое имя пользователя в консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** и перейдите на вкладку **Профиль (Profile)**, показанную на рис. 11-3. Здесь можно заполнить следующие поля:

- **Путь к профилю (Profile Path)** Путь к профилю пользователя, в котором хранятся параметры среды. При каждом входе пользователя на компьютер происходит обращение к его профилю, в ходе которого определяются параметры рабочего стола и панели управления, доступность команды меню приложений и многое другое. Настройка пути к профилю рассмотрена в разделе «Управление профилями пользователей» этой главы.

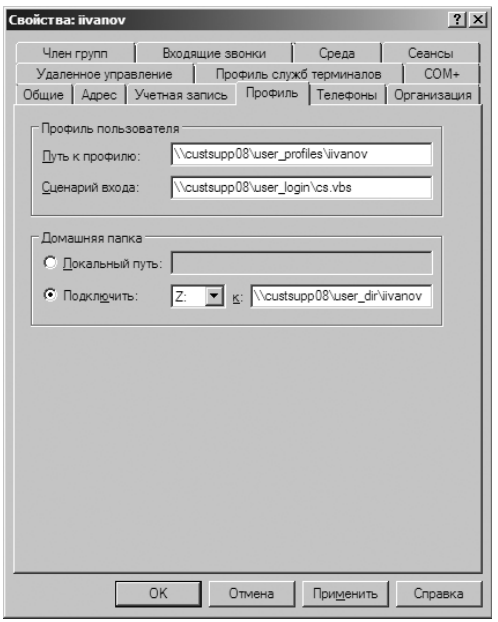


Рис. 11-3. Вкладка Профиль (Profile) позволяет настроить профиль пользователя

- **Сценарий входа (Logon Script)** Путь к сценарию входа пользователя — пакетному файлу, запускаемому при каждом входе пользователя в систему. Более подробно сценарии входа обсуждаются в главе 5.

- **Домашняя папка (Home Folder)** Папка для хранения файлов пользователя на локальном компьютере или сетевом диске. Если папка доступна по сети, пользователь может получить доступ к своим файлам с любого компьютера сети, в чем есть определенное преимущество.

Переменные системной среды

Переменные среды полезны при настройке рабочей среды пользователя, особенно, когда вы работаете со сценариями входа. Переменные среды используются для указания информации о путях, которая может время от времени изменяться. Чаще всего применяются следующие переменные среды:

- **%SystemRoot%** Основная папка операционной системы, например, C:\Windows. Используйте эту переменную на вкладке **Профиль (Profile)** диалогового окна свойств пользователя и в сценариях входа в систему.
- **%UserName%** Имя учетной записи пользователя, например, wrstanek. Используйте эту переменную на вкладке **Профиль (Profile)** диалогового окна свойств пользователя и в сценариях входа в систему.
- **%HomeDrive%** Буква диска, содержащего домашнюю папку пользователя, с двоеточием, например, «C:». Используется в сценариях входа.
- **%HomePath%** Полный путь к домашней папке без указания диска, например, \Users\Mkg\Georgej. Используется в сценариях входа.
- **%Processor_Architecture%** Архитектура процессора, установленного на компьютере пользователя, например, *x*86. Используется в сценариях входа.

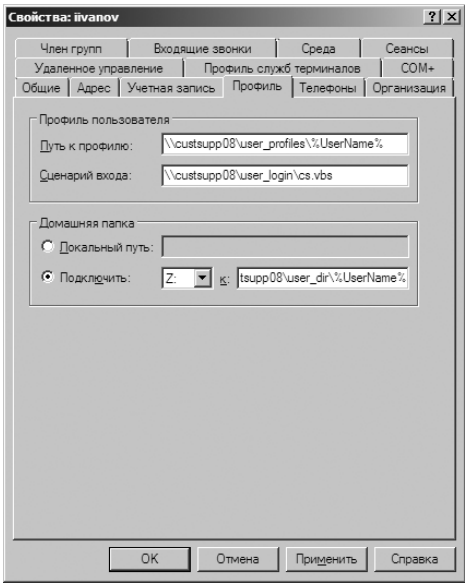


Рис. 11-4. Вкладка Профиль (Profile) позволяет сократить количество информации, вводимой вручную, особенно, при создании одной учетной записи на основе другой

На рис. 11-4 показан пример использования переменных среды при настройке учетных записей пользователя. Следует отметить, что переменная *%UserName%* позволяет системе определять информацию о полном пути для каждого пользователя. Данная методика позволяет использовать одну и ту же информацию о пути для нескольких пользователей, при этом, все пользователи будут иметь уникальные параметры.

Сценарии входа

В сценарий входа включаются команды, которые следует выполнять при каждом входе пользователя в систему. Их можно использовать для установки системного времени, путей к сетевым дискам, сетевых принтеров и прочих объектов. Хотя сценарии входа и подходят для одноразового выполнения команд, не следует устанавливать с их помощью переменные среды. Все параметры среды, использующиеся сценариями, не предназначены для последующего использования процессами пользователя. Также не следует использовать сценарии для запуска приложений, которые следует запускать при загрузке системы. Ярлыки таких программ следует поместить в папку **Автозагрузка (Startup)**.

В большинстве случаев в сценарии входа включаются команды Microsoft Windows, однако возможны и другие варианты:

- файлы сценариев Windows Script Host с расширениями .vbs, .js и др.;
- пакетные файлы с расширением .bat;
- командные файлы с расширением .cmd;
- исполняемые программы с расширением .exe.

Один сценарий входа может применяться несколькими пользователями. Использованием сценариев управляет администратор. Как следует из названия, сценарии входа выполняются во время входа пользователя в систему. Чтобы указать сценарий входа, выполните следующие действия:

1. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** откройте диалоговое окно свойств пользователя и перейдите на вкладку **Профиль (Profile)**.
2. Введите путь сценария входа в поле **Сценарий входа (Logon Script)**. Убедитесь, что введен полный путь к сценарию, например, **\\Zeta\User_Logon\Eng.vbs**.

Примечание Существуют другие способы задания сценариев входа и выхода из системы. Подробнее — в разделе «Управление сценариями пользователя и компьютера» главы 5.

Процесс создания сценариев входа не так сложен, как может показаться, особенно, если использовать командный язык Windows. В сценарии входа допустимы почти все команды, которые можно запускать из командной строки. Наиболее распространенные задачи, выполняемые в рамках сценариев, — это установка принтеров по умолчанию и подключение сетевых

дисков. Эта информация задается при помощи команды NET USE. Ниже приведены примеры задания сетевого принтера и диска:

```
net use lpt1: \\zeta\techmain
net use G: \\gamma\corp\files
```

Если вы включите эти команды в сценарий входа пользователя, у него будет сетевой принтер, подключенный к порту LPT1, и сетевая папка, доступная как диск G. Если вы предпочитаете VBScript, вам придется инициализировать переменные и объекты, которые вы планируете использовать, а затем вызвать соответствующие методы объекта *Network*. Рассмотрим пример:

```
Option Explicit
Dim wNetwork, printerPath
Set wNetwork = WScript.CreateObject("WScript.Network")

printerPath = "\\zeta\techmain"
wNetwork.AddWindowsPrinterConnection printerPath
wNetwork.SetDefaultPrinter printerPath

wNetwork.MapNetworkDrive "G:", "\\gamma\corpfiles"

Set wNetwork = vbEmpty
Set printerPath = vbEmpty
```

Здесь метод *AddWindowsPrinterConnection* используется для установки подключения к принтеру TechMain на сервере Zeta, а метод *SetDefaultPrinter* определяет данный принтер в качестве принтера по умолчанию. Далее метод *MapNetworkDrive* используется для определения сетевого диска G.

Назначение домашних папок

Система Windows Server 2008 позволяет назначать пользователям домашние папки для хранения личных файлов. Многие приложения используют домашнюю папку в качестве стандартного расположения для открытия и сохранения файлов, что облегчает поиск ресурсов. Кроме того, домашняя папка используется в командной строке в качестве начальной текущей папки.

Домашняя папка может находиться на локальном диске пользователя или на общем диске в сети. Папка на локальном диске доступна только на одной рабочей станции. Напротив, общие сетевые диски доступны с любого компьютера сети, что придает окружению пользователя универсальность.

Совет Одну и ту же домашнюю папку могут использовать несколько человек, но лучше этого не делать. В большинстве случаев следует предоставить отдельную домашнюю папку каждому пользователю.

Не следует создавать домашние папки пользователя «про запас». В нужный момент консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers) сделает это автоматически. Если же при со-

здании папки возникнут какие-либо проблемы, вам будут даны инструкции по созданию папки вручную.

Чтобы задать домашнюю папку на локальном компьютере, выполните следующие действия:

1. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** откройте диалоговое окно свойств пользователя и перейдите на вкладку **Профиль (Profile)**.
2. В разделе **Домашняя папка (Home Folder)** установите переключатель **Локальный путь (Local Path)** и введите в соответствующем текстовом поле путь к домашней папке, например, **C:\Home\%UserName%**.

Чтобы задать сетевую домашнюю папку, выполните следующие действия:

1. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** откройте диалоговое окно свойств пользователя и перейдите на вкладку **Профиль (Profile)**.
2. В разделе **Домашняя папка (Home Folder)** установите переключатель **Подключить (Connect)** и выберите букву диска для домашней папки. Для согласованности используйте одну букву диска для всех пользователей. Кроме того, убедитесь, что выбранная буква не конфликтует с существующими физическими или подключенными дисками. Во избежание проблем выбирайте букву ближе к концу алфавита.
3. Введите полный UNC-путь к домашней папке, например, **\\Gamma\User_Dirs\%UserName%**. Путь к диску включает имя сервера, что обеспечит доступность папки с любого компьютера сети.

Примечание Если домашняя папка не указана, Windows Server 2008 использует домашнюю папку по умолчанию. В системах, где ОС установлена как обновление, это, как правило, папка \Users\Default. В остальных случаях в роли домашней папки выступает корневой каталог.

Настройка возможностей и ограничений учетной записи

В арсенале Windows Server 2008 много способов управления учетными записями пользователей и их доступом в сеть. Вы можете определить часы, в течение которых пользователю разрешено входить в систему, рабочие станции, на которых ему разрешено это делать, параметры доступа по телефонной линии и многое другое.

Управление временем входа пользователя в сеть

Система Windows Server позволяет вам решать, когда пользователю разрешено войти в сеть. Чтобы укрепить безопасность, предотвратить взлом системы и другие действия злоумышленников в нерабочее время, запретите вход в систему в определенные часы.

В течение разрешенного времени входа пользователи могут нормально работать: входить в сеть и получать доступ к сетевым ресурсам. В часы огра-

ниченного входа в систему пользователи не могут работать, то есть, не могут войти в сеть и получить доступ к ее ресурсам. Если к моменту истечения действительного времени пользователи все еще находятся в системе, дальнейшее развитие событий зависит от установленной вами политики учетных записей. Как правило, реализуется один из двух вариантов:

- **С принудительным отключением** По истечении разрешенного времени входа в систему Windows Server 2008 принудительно отключает пользователей.
- **Без принудительного отключения** По истечении разрешенного времени входа пользователь не отключается от сети. Windows Server 2008 просто не позволяет ему устанавливать новые сетевые подключения.

Настройка времени входа в систему

Чтобы настроить время входа в систему, выполните следующие действия:

1. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** откройте диалоговое окно свойств пользователя и перейдите на вкладку **Учетная запись (Account)**.
2. Щелкните кнопку **Время входа (Logon Hours)**. Задайте приемлемые и неприемлемые часы входа в систему в диалоговом окне **Время входа (Logon Hours)**, показанном на рис. 11-5. В этом окне каждый час представлен в виде прямоугольной кнопки. Разрешенные часы — темные, запрещенные — белые.
3. Чтобы изменить возможность работы в конкретный час, щелкните его и выберите переключатель **Вход разрешен (Logon Permitted)** или **Вход запрещен (Logon Denied)**.

В таблице 11-1 перечислены функциональные возможности диалогового окна **Время входа (Logon Hours)**.

Табл. 1-1. Возможности диалогового окна Время входа (Logon Hours)

Элемент интерфейса	Описание
Все (All)	Позволяет выделить все интервалы времени
Кнопки дней недели	Позволяют выделить все часы определенного дня
Кнопки часов	Позволяют выделить определенный час всех дней недели
Вход разрешен (Logon Permitted)	Устанавливает разрешенные для входа часы
Вход запрещен (Logon Denied)	Устанавливает запрещенные для входа часы

Совет Вы сэкономите себе массу времени, если не будете слишком жестки в задании ограничений на доступное временное окно. Например, вместо строгого расписания с 9 до 17, добавьте по несколько часов с обеих сторон. Это позволит жаворонкам и совам эффективнее использовать рабочий день.

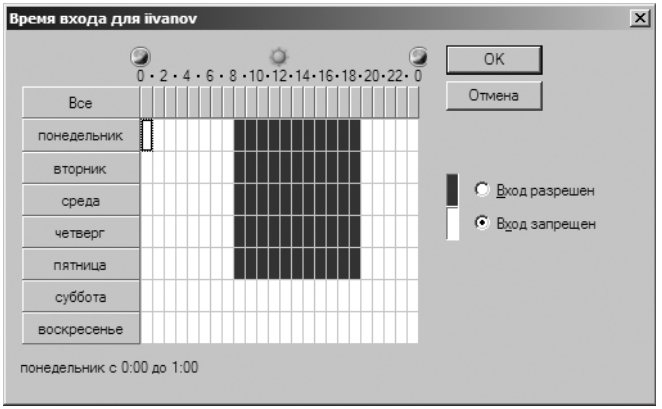


Рис. 11-5. Настройка разрешенного времени входа пользователей в систему

Действие по истечению разрешенного времени входа в систему

Чтобы принудительно отключить пользователей по истечению разрешенного времени входа в систему, выполните следующие действия:

1. Откройте нужную групповую политику. Об этом подробно рассказано в разделе «Управление политиками сайта, домена и подразделения» главы 5.
2. Последовательно разверните узлы **Конфигурация компьютера (Computer Configuration)**, **Конфигурация Windows (Windows Settings)**, **Параметры безопасности (Security Settings)** и **Локальные политики (Local Policies)**. Выделите элемент **Параметры безопасности (Security Options)**.
3. Дважды щелкните политику **Сетевая безопасность: Принудительный вывод из сеанса по истечении допустимых часов работы (Network Security: Force Logoff When Logon Hours Expire)**. Откроется диалоговое окно свойств политики.
4. Установите флажок **Определить следующий параметр политики (Define This Policy Setting)** и щелкните переключатель **Включен (Enabled)**. Затем щелкните **OK**.

Настройка разрешенных рабочих станций

В системе Windows Server 2008 существует формальная политика, позволяющая пользователям входить в систему локально, то есть, фактически находиться за клавиатурой компьютера. По умолчанию для локального входа на рабочую станцию можно использовать любую учетную запись, включая учетную запись гостя.

Несложно догадаться, что предоставление пользователям разрешения локального входа в систему на любой рабочей станции представляет собой угрозу безопасности. Любой обладатель имени пользователя и пароля может с помощью одной рабочей станции выполнить вход на любую рабочую станцию домена. Составление списка разрешенных рабочих станций позволяет

закрыть эту брешь. После этого злоумышленнику уже недостаточно будет иметь имя пользователя и пароль. Ему также придется найти разрешенный компьютер для своей учетной записи.

Примечание Ограничение нельзя применить к находящимся в домене компьютерам под управлением Windows 95 или Windows 98. Для входа в эти системы достаточно действующего имени пользователя и пароля.

Чтобы определить компьютеры, на которые разрешен вход пользователей домена, выполните следующие действия:

1. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** откройте диалоговое окно свойств учетной записи и перейдите на вкладку **Учетная запись (Account)**.
2. Щелкните кнопку **Вход на (Log On To)**, чтобы открыть диалоговое окно **Рабочие станции для входа в систему (Logon Workstations)**.
3. Установите переключатель **Только на указанные компьютеры (The Following Computers)**, как показано на рис. 11-6.
4. Введите имя разрешенной рабочей станции и щелкните **Добавить (Add)**. При необходимости повторите процедуру для других рабочих станций.
5. Допустив ошибку, выберите неверную запись и щелкните **Изменить (Edit)** или **Удалить (Remove)**.

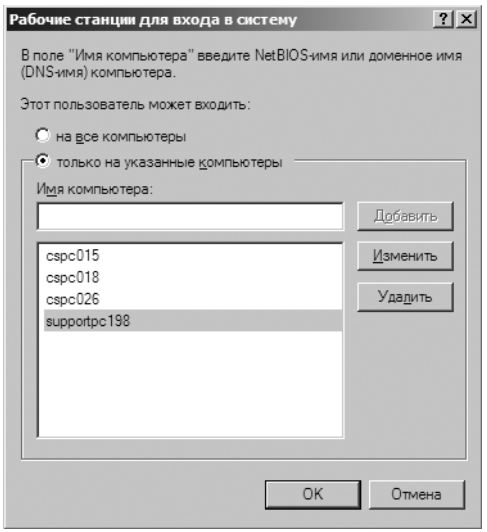


Рис. 11-6. Чтобы ограничить доступ в домен, определите рабочие станции, на которые разрешено входить

Настройка параметров подключения по телефонной линии и VPN

В ОС Windows Server 2008 параметры удаленного доступа задаются на вкладке **Входящие звонки (Dial-In)** диалогового окна свойств учетной записи. Ее параметры регулируют доступ к сети при помощи телефонной линии

или виртуальной частной сети (VPN). Как показано на рис. 11-7, параметры удаленного доступа по умолчанию регулируются политикой сети NPS. Этот метод управления удаленным доступом является предпочтительным. Чтобы явно предоставить или запретить доступ по телефонной линии, установите переключатель **Разрешить доступ (Allow Access)** или **Запретить доступ (Deny Access)**. В целом, прежде чем пользователи смогут получить удаленный доступ к сети, вы должны выполнить следующие действия:

1. При помощи диспетчера сервера добавьте роль **Службы политики сети и доступа (Network Policy and Access Services)**.
2. Чтобы разрешить подключения удаленного доступа, откройте для редактирования объект GPO нужного сайта, домена или подразделения. В редакторе политик последовательно разверните узлы **Конфигурация пользователя (User Configuration)**, **Административные шаблоны (Administrative Templates)** и **Сеть (Network)**. Затем выберите элемент **Сетевые подключения (Network Connections)** и настройте политики сетевых подключений сайта, домена или подразделения.
3. В консоли **Управление компьютером (Computer Management)** разверните узел **Службы и приложения (Services And Applications)** и выделите элемент **Маршрутизация и удаленный доступ (Routing And Remote Access)**. Выполните необходимые настройки маршрутизации и удаленного доступа.

Предоставив пользователю разрешение на удаленный доступ к сети, выполните следующие действия, чтобы настроить дополнительные параметры подключения по телефонной линии. В диалоговом окне свойств учетной записи перейдите на вкладку **Входящие звонки (Dial-In)**, показанную на рис. 11-7.

1. Если пользователь должен входить в сеть только с конкретного номера телефона, установите флажок **Проверять код звонящего (Verify Caller-ID)** и введите разрешенный номер телефона. Чтобы эта функция работала, ваша телефонная система должна поддерживать определение номеров.
2. Определите параметры ответного вызова:
   - **Ответный вызов не выполняется (No Callback)** Пользователь сам набирает номер и остается на связи. В этом случае, пользователю, возможно, придется оплачивать стоимость междугороднего звонка.
   - **Устанавливается вызывающим (Set By Caller)** Пользователь осуществляет набор прямого номера, и сервер предлагает ему ввести номер для ответного звонка. Затем пользователь отключается, а сервер выполняет ответный звонок по указанному пользователем номеру, чтобы восстановить подключение. При этом оплату междугороднего вызова производит компания.
   - **Всегда по этому номеру (Always Callback To)** Номер для ответного вызова задан жестко. Когда пользователь дозванивается до сервера, последний перезванивает по заранее установленному номеру. При этом компания оплачивает возможное междугороднее соединение. Риск несанкционированного доступа к сети уменьшается.

Примечание Не следует назначать ответный вызов пользователям, набирающим номер через коммутатор. Коммутатор может не позволить пользователю установить корректное подключение к сети.

3. При необходимости задайте статические IP-адреса и статические маршруты для телефонных подключений, щелкнув кнопки **Статические IP-адреса (Assign Static IP Address)** и **Статические маршруты (Apply Static Routes)**. Подробнее об IP-адресах и маршрутизации — в главе 17.

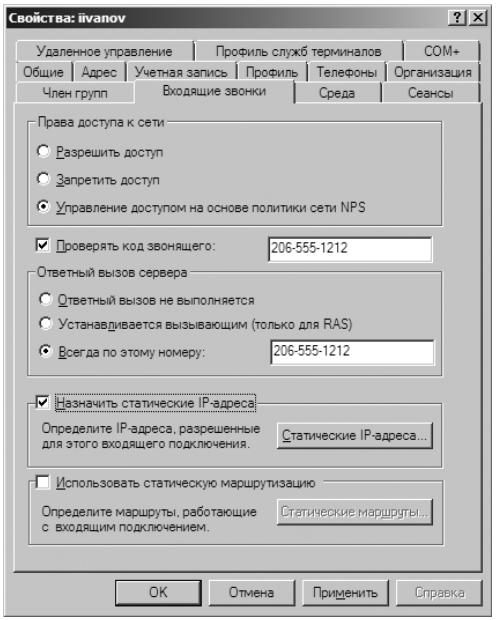


Рис. 11-7. Параметры удаленного доступа к сети

Настройка параметров безопасности учетной записи

Некоторые параметры вкладки **Учетная запись (Account)** диалогового окна свойств учетной записи призваны обеспечить безопасность сетевого окружения и регулировать использование учетных записей пользователей. Вот некоторые из этих параметров:

- **Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon)** Вынуждает пользователя изменить пароль при очередном входе в систему.
- **Запретить смену пароля пользователем (User Cannot Change Password)** Запрещает пользователю изменять пароль учетной записи.
- **Срок действия пароля не ограничен (Password Never Expires)** Обеспечивает бессрочное действие пароля, перекрывая обычный срок действия паролей.

Внимание! Эта возможность несет потенциальную угрозу безопасности сети. Старайтесь использовать бессрочные пароли только для учетных записей администраторов, но не обычных пользователей.

- **Хранить пароль, используя обратимое шифрование (Store Password Using Reversible Encryption)** Сохраняет пароль в виде зашифрованного простого текста.
- **Отключить учетную запись (Account Is Disabled)** Отключает учетную запись пользователя, не давая ему выполнить вход и получить доступ к сети.
- **Для интерактивного входа в сеть нужна смарт-карта (Smart Card Is Required For Interactive Logon)** Требует использовать смарт-карту для входа на рабочую станцию. Пользователь не сможет войти на компьютер, введя с клавиатуры имя и пароля.
- **Учетная запись важна и не может быть делегирована (Account Is Sensitive And Cannot Be Delegated)** Указывает, что учетные данные записи не могут быть делегированы посредством Kerberos. Используется для важных учетных записей, за которыми требуется особый контроль.
- **Используйте типы шифрования Kerberos DES для этой учетной записи (Use Kerberos DES Encryption Types For This Account)** Указывает, что в учетной записи пользователя будет использоваться стандарт шифрования DES.
- **Данная учетная запись поддерживает 128-разрядное шифрование Kerberos AES (This Account Supports Kerberos AES 128 Bit Encryption)** Учетная запись поддерживает 128-разрядный стандарт шифрования AES.
- **Данная учетная запись поддерживает 256-разрядное шифрование Kerberos AES (This Account Supports Kerberos AES 256 Bit Encryption)** Учетная запись поддерживает 256-разрядное шифрование AES.
- **Без предварительной проверки подлинности Kerberos (Do Not Require Kerberos Preauthentication)** Указывает, что для получения доступа к ресурсам сети учетная запись не нуждается в предварительной проверке подлинности. Предварительная проверка подлинности — часть процедуры безопасности Kerberos v5. Отказ от данной процедуры при входе разрешает проверку подлинности с клиентских компьютеров посредством предыдущих или нестандартных реализаций Kerberos.

Ближе к реальности Стандарты AES и DES — одни из нескольких стандартов шифрования. На большинстве компьютеров под управлением старых версий Windows поддерживается стандарт DES.

На компьютерах под управлением Windows Vista и Windows Server 2008 поддерживается стандарт AES, обеспечивающий более безопасный уровень шифрования, чем стандарт DES. Версии Windows Vista и Windows Server 2008, предназначенные для использования на территории США, поддерживают как 128-, так и 256-разрядное шифрование, тогда как версии для использования за пределами США, как правило, поддерживают только 128-разрядное шифрование.

Управление профилями пользователей

Профиль пользователя содержит такие параметры сетевого окружения, как конфигурацию рабочего стола и доступные команды меню. Иногда проблемы с профилем мешают пользователю выполнить вход в систему. Например, если заданное в профиле разрешение экрана недоступно на компьютере, с которого пользователь входит в систему, он рискует просто оказаться перед пустым экраном. В данном случае следует перезагрузить компьютер в режиме VGA и вручную исправить параметры дисплея. Однако не все проблемы с профилями решаются так же просто. Иногда требуется обновлять сам профиль.

В Windows Server 2008 предусмотрено несколько способов управления профилями пользователей:

- Пути к профилям назначаются в консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)**.
- Копирование, удаление и изменение типа существующего локального профиля производится при помощи утилиты **Система (System)** панели управления.
- Системные политики позволяют запретить пользователям изменять определенные параметры среды.

Локальные, перемещаемые и обязательные профили

В Windows Server 2008 у каждого пользователя есть свой профиль, который определяет компоненты, запускаемые в начале сеанса, программы и приложения, доступные пользователю, параметры рабочего стола и многое другое. Копия профиля пользователя хранится на каждом компьютере, который пользователь использует для входа. Пользователи, имеющие доступ к нескольким компьютерам, на каждом из них имеют профиль, которые называется *локальным* (local). Он недоступен с других компьютеров сети, и, как легко догадаться, в этом есть свои недостатки. Например, если пользователь входит на три различные рабочие станции, на каждой из них он может завести три достаточно различных профиля и, в результате, перепутать ресурсы, доступные на одной системе, с ресурсами другой системы.

Во избежание неразберихи с несколькими профилями желательно создать профиль, доступ к которому смогут получить и другие компьютеры. Такой профиль называется *перемещаемым* (roaming). Он позволяет пользователям в пределах домена работать с одним и тем же профилем независимо от используемого компьютера. Перемещаемые профили размещаются на серверах, причем, только под управлением Windows 2000, Windows Server 2003 или Windows Server 2008. Когда пользователь с перемещаемым профилем входит в систему, происходит загрузка профиля и создание его локальной копии на компьютере пользователя. При выходе пользователя изменения профиля переносятся в локальную копию и на сервер.

Ближе к реальности Если для обеспечения безопасности данных, ваша организация использует файловую систему EFS, использование перемещаемых профилей становится особенно важным, поскольку сертификаты шифрования, необходимые для работы с шифрованными файлами, хранятся именно в профилях. Если у пользователя есть шифрованные файлы, но нет перемещаемого профиля, он не сможет работать с этими файлами на другом компьютере.

Администратор может управлять профилями пользователей собственноручно или позволить осуществлять управление самим пользователям. Беря управление в свои руки, вы обеспечите единство сетевой конфигурации пользователей, что сократит число неполадок, связанных со средой.

Профили, управляемые администраторами, *обязательными* (mandatory). Пользователь с обязательным профилем может вносить в среду только временные изменения. При следующем входе в систему он опять вернется к исходному профилю. Смысл, разумеется, состоит в том, что пользователь, которому запрещено вносить постоянные изменения в сетевое окружение, не создаст своими изменениями никаких проблем. Ключевой недостаток обязательных профилей — невозможность для пользователя войти в систему, если профиль недоступен. Если сервер, на котором хранится профиль, по какой-то причине не работает, пользователю удастся выполнить вход, только если профиль сохранился в кеше. В этом случае пользователь увидит предупреждение, но сможет войти в локальную систему при помощи кешированного профиля.

Примечание Когда вы перезагружаете компьютер под управлением Windows XP, обязательные профили удаляются. При входе на компьютер под управлением Windows XP пользователь может получить доступ к неограниченному временному профилю. Это происходит, если нет доступного сетевого подключения к контроллеру домена и в кеше профиля тоже нет. Подробнее об этом читайте в в статье 893243 базы знаний Майкрософт по адресу *http://support.microsoft.com/default.aspx?scid=kb;en-us;893243*.

Создание локального профиля

В Windows 2000 и более поздних версиях профили пользователей хранятся в папке по умолчанию или в папке, заданной в поле **Путь к профилю (Profile Path)** диалогового окна свойств пользователя. В Windows Vista и Windows Server 2008 стандартное расположение профиля %*СистемныйДиск*%\Users\%*ИмяПользователя*%\Ntuser.dat, например, C:\Users\wrstanek\Ntuser.dat. Если вы не измените стандартное расположение, для пользователя будет создан локальный профиль.

Создание перемещаемого профиля

Перемещаемые профили хранятся на серверах под управлением Windows 2000, Windows Server 2003 или Windows Server 2008. Если пользователь собирается входить в систему с разных компьютеров, используя EFS, ему потребуется перемещаемый профиль. Он обеспечит доступность сертификатов, необходимых для работы с шифрованными файлами на других компьютерах.

Чтобы сделать профиль пользователя перемещаемым, задайте для него расположение на сервере, выполнив следующие действия:

1. Создайте общую папку на сервере под управлением Windows Server 2008 и убедитесь, что группа Все (Everyone) обладает, по крайней мере, разрешениями Изменение (Change) и Чтение (Read) для этой папки.
2. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)** откройте диалоговое окно свойств пользователя и перейдите на вкладку **Профиль (Profile)**. Введите путь к общей папке в поле **Путь к профилю (Profile Path)** в формате *имя сервера**имя папки профиля**имя пользователя*, например, \\Zeta\User_Profiles\Georgej, где *Zeta* — имя сервера, *User_Profiles* — общая папка и *Georgej* — имя пользователя.
3. Затем профиль сохраняется в заданной папке, в файле Ntuser.dat, например, \\Zeta\User_Profiles\Georgej\Ntuser.dat.

Примечание В большинстве случаев специально создавать папку для профиля конкретного пользователя не приходится, так как она создается автоматически при входе пользователя. Разрешения NTFS назначаются так, что доступ к папке имеет только пользователь. Вы можете одновременно задать расположение профиля для нескольких учетных записей. Выделите нужные записи при помощи клавиш Ctrl или Shift, щелкните правой кнопкой одного из выделенных пользователей и выберите команду **Свойства (Properties)**. Таким образом вы сможете редактировать свойства всех выбранных пользователей. Убедитесь, что в пути к профилю вы указали переменную среды %*UserName*%, например, \\Zeta\User_Profiles\%*UserName*%.

4. При необходимости создайте профиль для пользователя скопируйте существующий профиль в папку перемещаемого профиля пользователя. Если этого не сделать, при следующем входе в систему пользователь получит стандартный локальный профиль. Любые изменения, внесенные пользователем в этот профиль, при выходе из системы будут сохранены. Таким образом, при следующем входе в систему пользователь получит уже собственный профиль.

Создание обязательного профиля

Обязательные профили хранятся на серверах под управлением Windows Server 2008. Если вы хотите, чтобы пользователь обладал обязательным профилем, определите профиль следующим образом:

1. Выполните шаги 1-3 из предыдущего раздела.
2. Переименуйте файл Ntuser.dat в Ntuser.man. При следующем входе пользователя в систему, он получит обязательный профиль.

Примечание Файл Ntuser.dat содержит параметры реестра пользователя. Изменив расширение файла на .man, вы сообщаете Windows Server 2008, что данный профиль является обязательным.

Управление локальными профилями при помощи панели управления

Чтобы управлять локальными профилями, требуется войти на компьютер пользователя и воспользоваться утилитой Система (System) панели управления. Для просмотра информации о текущем профиле щелкните кнопку **Пуск (Start)** и выберите команду **Панель управления (Control Panel)**. Затем последовательно щелкните ссылки **Система и ее обслуживание (System And Maintenance)**, **Система (System)** и **Дополнительные параметры системы (Advanced System Settings)**, чтобы открыть диалоговое окно **Свойства системы (System Properties)**. В разделе **Профили пользователей (User Profiles)** щелкните кнопку **Параметры (Settings)**.

На рис. 11-8 показано диалоговое окно **Профили пользователей (User Profiles)**, в котором отображена информация о профилях, хранящихся в локальной системе. Эта информация полезна при управлении профилями.

В столбцах содержится следующая информация:

- **Имя (Name)** Имя профиля, как правило, включающее имя домена или компьютера и имя учетной записи пользователя. Например, имя ADATUM\Wrstanek говорит о том, что данный профиль находится в домене adatum, а имя пользователя — wrstanek.

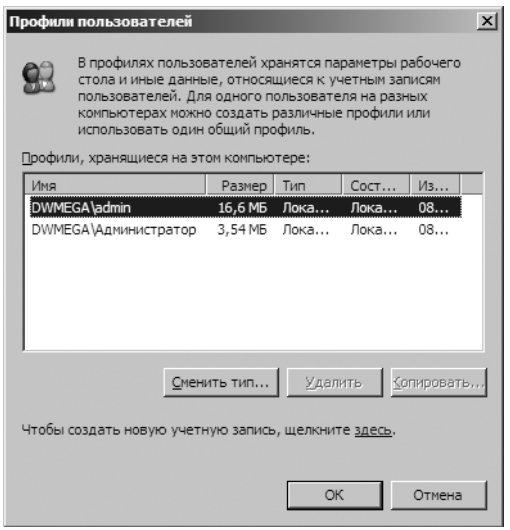


Рис. 11-8. Диалоговое окно Профили пользователя (Users Profiles) служит для управления локальными профилями

Примечание Если вы удалите учетную запись, но сохраните ее профиль, то увидите в этом окне элемент **Учетная запись удалена (Account Deleted)** или **Неизвестная учетная запись (Account Unknown)**. Обозначенный таким образом профиль доступен для копирования или удаления.

- **Размер (Size)** Как правило, чем больше профиль, тем значительнее он был изменен пользователем.
- **Тип (Type)** Тип профиля (локальный или перемещаемый).
- **Состояние (Status)** Текущее состояние профиля, например, извлечен ли он из локального кеша.
- **Изменение (Modified)** Дата последнего изменения профиля.

Создание профиля вручную

Чтобы создать профиль вручную, нужно войти в систему с учетной записью пользователя, настроить среду, а затем выйти. Конечно, такой способ создания учетных записей требует много времени. Лучше создать для этой цели базовую учетную запись с типичными настройками. Вы создаете базовую учетную запись, настраиваете ее среду, а затем используете полученный профиль как основу для профилей других учетных записей.

Копирование существующего профиля

Если у вас есть базовая учетная запись, вы можете скопировать ее профиль в новую учетную запись. Для этого используется утилита Система (System) панели управления. Выполните следующие действия:

1. Откройте панель управления. Последовательно щелкните ссылки **Система и ее обслуживание (System And Maintenance)**, **Система (System)** и **Дополнительные параметры системы (Advanced System Settings)**. В диалоговом окне **Свойства системы (System Properties)** щелкните кнопку **Параметры (Settings)** в разделе **Профили пользователей (User Profiles)**.
2. В списке **Профили, хранящиеся на этом компьютере (Profiles Stored On This Computer)** выберите профиль, который хотите копировать (рис. 11-8).
3. Щелкните кнопку **Копировать (Copy To)**. Далее введите путь к папке нового профиля в поле **Копировать профиль на (Copy Profile To)**, как показано на рис. 11-9. Например, пользователю georgej может соответствовать путь к профилю **\\Zeta\User_Profiles\Georgej**.

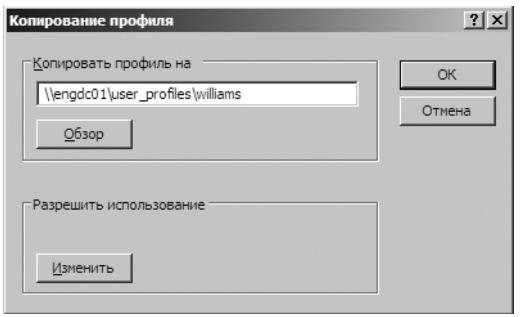


Рис. 11-9. В диалоговом окне Копирование (Copy To) введите путь к папке профиля и предоставьте разрешение на доступ к ней

4. Теперь следует предоставить пользователю разрешение на доступ к профилю. В разделе **Разрешить использование (Permitted To Use)** щелкните кнопку **Изменить (Change)** и в диалоговом окне **Выбор: «Пользователь» или «Группа» (Select User Or Group)** укажите нужную учетную запись.
5. Щелкните **OK**, чтобы закрыть диалоговое окно **Копирование (Copy To)**. Windows скопирует профиль в новое место.

Копирование или восстановление профиля

В рабочих группах, где управление каждым компьютером производится по отдельности, вам часто придется сталкиваться с копированием локального профиля с одного компьютера на другой. Такое копирование позволяет пользователям сохранять параметры среды на различных компьютерах. Безусловно, в домене Windows Server 2008 вы вольны воспользоваться перемещаемым профилем, доступ к которому можно получить из любого места в домене. Но и в этом случае вам иногда может понадобиться копия локального профиля для замены перемещаемого профиля пользователя (например, если перемещаемый профиль поврежден). Вы также можете скопировать существующий локальный профиль для создания перемещаемого профиля в другом домене.

Чтобы скопировать существующий профиль в новое расположение, выполните следующие действия:

1. Войдите на компьютер пользователя и откройте панель управления. Последовательно щелкните ссылки **Система и ее обслуживание (System And Maintenance)**, **Система (System)** и **Дополнительные параметры системы (Advanced System Settings)**. В диалоговом окне **Свойства системы (System Properties)** щелкните кнопку **Параметры (Settings)** в разделе **Профили пользователей (User Profiles)**.
2. В списке **Профили, хранящиеся на этом компьютере (Profiles Stored On This Computer)** выберите профиль, который хотите копировать.
3. Щелкните кнопку **Копировать (Copy To)**. Далее введите путь к папке нового профиля в поле **Копировать профиль на (Copy Profile To)**.
4. В разделе **Разрешить использование (Permitted To Use)** щелкните кнопку **Изменить (Change)** и в диалоговом окне **Выбор: «Пользователь» или «Группа» (Select User Or Group)** укажите нужную учетную запись.
5. Щелкните **OK**, чтобы закрыть диалоговое окно **Копирование (Copy To)**. Windows скопирует профиль в новое расположение.

Удаление локального профиля и назначение нового

Обращение к профилю происходит во время входа пользователя на компьютер. В Windows Server 2008 для всех пользователей, не имеющих перемещаемого профиля, используется локальный профиль. Кроме того, локальный профиль применяется, если он имеет более позднюю дату последнего изменения, чем перемещаемый профиль. Поэтому в ряде случаев локальный

профиль лучше удалить и назначить новый. Помните, что после удаления локального профиля, копии которого нет в домене, вы не сможете восстановить первоначальные параметры среды пользователя.

Чтобы удалить локальный профиль пользователя, выполните следующие действия:

1. Войдите на компьютер пользователя с учетной записью, обладающей административными полномочиями, и запустите утилиту **Система (System)**.
2. Щелкните ссылку **Дополнительные параметры системы (Advanced System Settings)**. В диалоговом окне **Свойства системы (System Properties)** щелкните кнопку **Параметры (Settings)** в разделе **Профили пользователей (User Profiles)**.
3. Выберите профиль, который хотите удалить, и щелкните кнопку **Удалить (Delete)**. Щелкните **Да (Yes)**, чтобы подтвердить удаление профиля.

Примечание Нельзя удалить профиль, используемый в данный момент. Если пользователь выполнил вход в локальную систему (компьютер, с которого вы хотите удалить профиль), прежде чем вы сможете удалить профиль, пользователь должен выйти из системы. В отдельных случаях Windows Server 2008 помечает как используемые профили, которые на самом деле таковыми не являются. Как правило, это происходит в результате изменения среды пользователя, которое не было корректно применено. Для решения проблемы достаточно перезагрузить компьютер.

При следующем входе пользователя в систему Windows Server 2008 выполнит одно из двух действий: предоставит пользователю стандартный локальный профиль системы или извлечет перемещаемый профиль пользователя, хранящийся на другом компьютере. Чтобы предотвратить использование указанных профилей, требуется назначить пользователю новый профиль. Это можно сделать одним из следующих способов:

- скопировать существующий профиль в папку профиля пользователя;
- обновить параметры профиля пользователя в консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)**.

Изменение типа профиля

Утилита **Система (System)** позволяет изменять тип профиля на компьютере пользователя. Выделите профиль и щелкните кнопку **Сменить тип (Change Type)**. В открывшемся диалоговом окне доступны следующие действия:

- **Преобразование перемещаемого профиля в локальный** Если вы хотите, чтобы на этом компьютере пользователь всегда работал с локальным профилем, преобразуйте профиль в локальный. После этого все вносимые в профиль изменения будут локальными, а первоначальный перемещаемый профиль не будет изменяться.
- **Преобразование локального профиля в перемещаемый (при условии что профиль изначально был определен как перемещаемый)** При следующем входе пользователя в систему будет использован его прежний перемещаемый профиль. После этого Windows Server 2008 будет обра-

щаться с ним, как и с любым другим перемещаемым профилем. Это означает, что все изменения локального профиля будут копироваться в перемещаемый профиль.

Примечание Если эти действия недоступны, профиль пользователя изначально определен как локальный.

Редактирование учетных записей пользователей и групп

Для редактирования учетных записей пользователей или групп домена используется консоль **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)**. Чтобы обновить учетную запись локального пользователя или группы, применяйте консоль **Локальные пользователи и группы (Local Users And Groups)**.

При работе с Active Directory вам довольно часто бывает нужно составить список определенных учетных записей для последующей работы с ними. Например, вам может понадобиться список учетных записей всех сотрудников организации, чтобы отключить учетные записи уволившихся пользователей. Ниже описан один из способов решения этой задачи:

1. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** щелкните правой кнопкой имя домена и выберите команду **Найти (Find)**.
2. В списке **Найти (Find)** выберите вариант **Пользовательский поиск (Custom Search)**. В диалоговом окне **Поиск (Find)** появится вкладка **Пользовательский поиск (Custom Search)**.
3. В списке **Где (In)** задайте область поиска. Чтобы выполнить поиск по всему предприятию, выберите вариант **Целиком Active Directory (Entire Directory)**.
4. Щелкните кнопку **Поле (Field)** и выберите команды **Пользователь (User)** и **Имя входа (пред-Windows 2000) (Logon Name (Pre-Windows 2000))**.

Совет Не перепутайте: выбирать нужно именно **Имя входа (пред-Windows 2000) (Logon Name (Pre–Windows 2000))**, а не просто **Имя для входа (Logon Name)**. У учетной записи может и не быть обычного имени входа, но имя для входа в систему до Windows 2000 у всех учетных записей есть обязательно.

5. В списке **Условие (Condition)** выберите вариант **Присутствует (Present)** и щелкните кнопку **Добавить (Add)**. Если система затребует подтверждение, щелкните **Да (Yes)**.
6. Щелкните **Найти (Find Now)**. Будет составлен список всех пользователей в указанной области.
7. Выделите запись или записи, с которыми собираетесь работать.
8. Щелкните правой кнопкой учетную запись пользователя и в контекстном меню выберите действие, например, **Отключить учетную запись (Disable Account)**.

Совет Вот действия, которые можно выполнить одновременно в отношении нескольких учетных записей: **Добавить в группу (Add To Group)**, **Включить учетную запись (Enable Account)**, **Отключить учетную запись (Disable Account)**, **Удалить (Delete)** и **Переместить (Move)**.

Та же процедура годится для составления списка компьютеров, групп или других ресурсов Active Directory. В случае поиска компьютеров щелкните кнопку **Поле (Field)** и выберите варианты **Компьютер (Computer)** и **Имя компьютера (пред-Windows 2000) (Computer Name (Pre-Windows 2000))**. Чтобы составить список групп, щелкните кнопку **Поле (Field)** и выберите варианты **Группа (Group)** и **Имя группы (пред-Windows 2000) (Group Name (Pre-Windows 2000))**.

В следующих разделах рассмотрены другие способы редактирования учетных записей (переименование, копирование, удаление и включение), а также изменение и переустановка паролей. Кроме того, вы узнаете, как устранять проблемы учетных записей, возникающие при входе в систему.

Переименование учетных записей пользователей и групп

Переименование учетной записи — не более чем присвоение ей новой метки. Как уже говорилось в главе 10, имена пользователей предназначены исключительно для облегчения управления учетными записями и работы с ними. Для реальной идентификации, сопровождения и обработки учетных записей Windows Server 2008 использует идентификаторы безопасности SID, не зависящие от имен пользователей. Идентификатор SID учетной записи уникален и генерируется во время ее создания.

Поскольку SID внутренне сопоставлены с именами учетных записей, вам не нужно изменять полномочия или разрешения переименованной учетной записи. Windows Server 2008 просто сопоставит SID с новым именем учетной записи.

Одна из распространенных причин изменения имени учетной записи — перемена фамилии. Допустим, Ким Акерс (kima) выходит замуж, берет фамилию мужа — Роллз — и, скорее всего, пожелает изменить имя пользователя на kimr. Изменение имени пользователя с kima на kimr будет отражено во всех связанных полномочиях и разрешениях. Если, например, просмотреть разрешения файла, к которому имела доступ Ким Акерс-Роллз, в списке разрешений будет стоять имя kimr, а имени kima в списке не будет.

Для облегчения переименования учетных записей в консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** предусмотрено диалоговое окно **Переименование пользователя (Rename User)**, которое позволяет изменить все компоненты имени. Чтобы переименовать учетную запись, выполните следующие действия:

1. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** найдите учетную запись, которую хотите переименовать.

2. Щелкните учетную запись правой кнопкой и выберите команду **Переименовать (Rename)**. Имя редактируемой учетной записи будет выделено. Нажмите клавишу Backspace или Delete, чтобы стереть существующее имя, затем нажмите клавишу Enter, чтобы открыть диалоговое окно **Переименование пользователя (Rename User)**.
3. Внесите необходимые изменения и щелкните **OK**. Если пользователь находится в системе, на экране появится предупреждение о том, что пользователю необходимо выполнить выход, а затем снова войти, используя новое имя для входа.
4. Поскольку при переименовании учетной записи SID не меняется, все разрешения записи остаются в силе. Тем не менее, вам, вероятно, все-таки придется внести некоторые изменения в диалоговом окне свойств учетной записи, в том числе:
   - **Путь к профилю** Измените путь к профилю в диалоговом окне свойств учетной записи, а затем переименуйте соответствующую папку на диске.
   - **Имя сценария входа** Измените имя сценария в диалоговом окне свойств учетной записи, а затем переименуйте сценарий на диске.
   - **Домашняя папка** Измените домашнюю папку в диалоговом окне свойств учетной записи, а затем переименуйте соответствующую папку на диске.

Примечание Редактирование информации о папках и файлах учетной записи во время сеанса пользователя может стать причиной сбоев. Поэтому лучше всего заниматься редактированием в конце рабочего дня, или попросить пользователя выйти из системы на несколько минут, а потом снова войти. В большинстве случаев возложить эти обязанности можно на простой сценарий Windows.

Копирование доменных учетных записей пользователя

Создание учетной записи пользователя домена с нуля — довольно утомительное занятие. Вместо этого воспользуйтесь в качестве отправной точки существующей учетной записью, выполнив следующие действия:

1. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** щелкните правой кнопкой учетную запись, которую хотите скопировать, и выберите команду **Копировать (Copy)**. Откроется диалоговое окно **Копировать объект — Пользователь (Copy Object — User)**.
2. Заполните поля с персональными данными пользователя. Затем при необходимости исправьте другие свойства учетной записи.

Легко догадаться, что при копировании учетной записи консоль **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** переносит в копию не всю информацию из исходной записи. Система копирует только ту информацию, которая будет вам нужна,

и отбрасывает информацию, которую вам все равно придется обновлять. Копируются следующие свойства:

- город, регион, почтовый индекс и страна, заданные на вкладке **Адрес (Address)**;
- компания и отдел, заданные на вкладке **Организация (Organization)**;
- параметры учетной записи, заданные в разделе **Параметры учетной записи (Account Options)** вкладки **Учетная запись (Account)**;
- время входа в систему и рабочие станции, с которых разрешен вход;
- срок действия учетной записи;
- членство в группах;
- параметры профиля;
- права на использование телефонного подключения.

Примечание Если в исходной учетной записи для указания параметров профиля вы использовали переменные среды, в копии учетной записи также используются переменные среды. Например, если в исходной учетной записи путь к профилю был задан при помощи переменной %*UserName*%, так же он будет задан и в копии.

Импорт и экспорт учетных записей

В состав Windows Server 2008 включена утилита командной строки CSVDE, предназначенная для импорта и экспорта объектов Active Directory. В качестве источника для импорта программа CSVDE использует текстовый файл с разделителями-запятыми. Общие параметры утилиты CSVDE таковы:

- **–i** Включает режим импорта (по умолчанию установлен режим экспорта).
- **–f** *имяфайла* Задает источник импорта или выходной файл экспорта.
- **–s** *имясервера* Задает сервер для импорта или экспорта (по умолчанию используется контроллер домена).
- **–v** Включает режим с детальным выводом.
- **–u** Включает поддержку Unicode (если в целевом или конечном файле должен применяться формат Unicode).

В ходе импорта первая строка файла-источника определяет список атрибутов LDAP для каждого определенного объекта. В последующих строках содержатся параметры конкретного импортируемого объекта в точном соответствии с заданным списком атрибутов. Например:

```
DN,objectClass,sAMAccoutName,sn,givenName,userPrincipalName
"CN=William Stanek,OU=Eng,DC=cpandl,DC=com",user,williams,William,Stanek,
williams@cpandl.com
```

Допустим, этот текст содержится в файле newusers.csv. Чтобы импортировать его в Active Directory, введите в командной строке с повышенными полномочиями следующую команду:

```
csvde -i -f newusers.csv
```

Выполняя экспорт, CSVDE записывает экспортируемые объекты в текстовый файл с разделителями-запятыми. Помимо уже перечисленных параметров, в ходе экспорта вам доступны дополнительные параметры, в том числе:

- **–d RootDN** Отправная точка экспорта, например, **–d "OU=Sales,DC=domain,DC=local"**. По умолчанию, текущий контекст именования.
- **–l** *список* Разделенный запятыми список выводимых атрибутов.
- **–r** *фильтр* Фильтр поиска LDAP, например, **–r "(objectClass=user)"**.
- **–m** Настраивает вывод для диспетчера учетных записей (SAM), а не для Active Directory.

Чтобы создать файл экспорта текущего контекста именования (домена по умолчанию), введите в командной строке команду:

```
csvde -f newusers.csv
```

Имейте в виду, что в этом случае файл экспорта может достигать гигантских размеров. В большинстве случаев следует дополнительно задать, как минимум, значение RootDN и фильтр объектов, например:

```
csvde -f newusers.csv -d "OU=Service,DC=cpandl,DC=com" -r
"(objectClass=user)"
```

Удаление учетных записей пользователей и групп

Удаляемая учетная запись действительно навсегда удаляется. Создав учетную запись с тем же именем, вы не получите прежнего набора разрешений, поскольку SID новой учетной записи не будет совпадать с SID старой учетной записи.

Удаление встроенных учетных записей может иметь далеко идущие последствия для домена, поэтому в Windows Server 2008 оно запрещено. Прочие типы учетных записей удалять можно. Для этого достаточно выделить запись и нажать клавишу Delete. Затем щелкните **OK** и **Да (Yes)**.

Примечание При удалении учетной записи пользователя Windows Server 2008 не удаляет профиль пользователя, личные файлы и домашнюю папку. Если вы желаете удалить их, вам придется сделать это вручную. При регулярном выполнении этой задачи стоит создать Windows-сценарий, который будет выполнять необходимые действия. Не забудьте перед удалением создать резервные копии нужных файлов или данных.

Изменение и переустановка паролей

Администратору часто приходится менять или переустанавливать пароли пользователей. Чаще всего это случается, когда пользователи забывают пароли или срок действия паролей истекает.

Чтобы изменить или переустановить пароль, выполните следующие действия:

1. Откройте консоль **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** или **Локальные пользователи и группы (Local Users And Groups)**.
2. Щелкните правой кнопкой учетную запись и выберите команду **Смена пароля (Reset Password)** или **Задать пароль (Set Password)**.
3. Введите новый пароль учетной записи и подтвердите его. Пароль должен соответствовать политике сложности, заданной на компьютере или в домене.
4. Дважды щелкните имя учетной записи и при необходимости сбросьте флажок **Учетная запись заблокирована (Account Is Locked Out)** или установите флажок **Разблокировать учетную запись (Unlock Account)**. Эти флажки находятся на вкладке **Учетная запись (Account)** диалогового окна свойств пользователя.

Включение учетной записи пользователя

Существует несколько причин, по которым учетная запись пользователя может быть отключена. Если пользователь забыл пароль и пытается подобрать его, он может превысить максимальное количество попыток входа в систему, заданное политикой учетной записи. Отключить учетную запись может другой администратор, например, на время отпуска пользователя. Может также истечь срок действия учетной записи. В следующих разделах рассказывается о том, что делать, если учетная запись отключена, заблокирована или просрочена.

Учетная запись отключена

В консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** отключенные учетные записи отмечены направленной вниз стрелкой рядом со значком пользователя. Чтобы включить отключенную учетную запись, выполните следующие действия:

1. Откройте консоль **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** или **Локальные пользователи и группы (Local Users And Groups)**.
2. Щелкните правой кнопкой имя учетной записи и выберите команду **Включить учетную запись (Enable Account)**.

Совет Чтобы оперативно составить список отключенных учетных записей в текущем домене, введите в командной строке **dsquery user –disabled**.

Учетная запись заблокирована

Чтобы разблокировать заблокированную учетную запись, выполните следующие действия:

1. Откройте консоль **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** или **Локальные пользователи и группы (Local Users And Groups)**.

2. Дважды щелкните имя учетной записи пользователя и установите флажок **Разблокировать учетную запись (Unlock Account)**. Он расположен на вкладке **Учетная запись (Account)** диалогового окна свойств пользователя.

Примечание Если блокировка учетных записей пользователей происходит слишком часто, подумайте о корректировке политик учетных записей в домене. Возможно, следует увеличить значение допустимых попыток входа или сократить время действия соответствующего счетчика. Дополнительную информацию о настройке политик учетных записей вы найдете в разделе «Настройка политик учетных записей» главы 10.

Истек срок действия учетной записи

Сроком действия обладают только доменные учетные записи. Локальные учетные записи пользователей не имеют срока действия. Чтобы исправить срок действия учетной записи, выполните следующие действия:

1. Откройте консоль **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)**.
2. Дважды щелкните имя учетной записи пользователя и перейдите на вкладку **Учетная запись (Account)**.
3. В разделе **Срок действия учетной записи (Account Expires)** установите переключатель **Истекает (End Of)** и щелкните стрелку соответствующего поля. Откроется календарь, с помощью которого вы сможете задать новый срок действия.

Управление несколькими учетными записями

Консоль **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** позволяет управлять несколькими учетными записями одновременно. Чтобы выделить несколько учетных записей, выполните следующие действия:

- Чтобы выделить произвольный набор учетных записей, нажмите клавишу Ctrl и по очереди щелкайте левой кнопкой все учетные записи, которые хотите выделить.
- Чтобы выделить группу смежных учетных записей, нажмите клавишу Shift, а затем щелкните первое и последнее имя пользователя в группе.

Закончив выделение учетных записей, щелкните их правой кнопкой для вывода контекстного меню. Оно содержит следующие команды:

- **Добавить в группу (Add To A Group)** Открывает диалоговое окно **Выбор: «Группы» (Select Group)** для выбора групп, членами которых должны стать выбранные пользователи.
- **Отключить учетную запись (Disable Account)** Отключает все выделенные учетные записи.
- **Включить учетную запись (Enable Account)** Включает все выделенные учетные записи.
- **Переместить (Move)** Перемещает выделенные учетные записи в новый контейнер или подразделение.

- **Свойства (Properties)** Позволяет настраивать ограниченный набор свойств одновременно для нескольких учетных записей

В следующих разделах мы подробно рассмотрим команду **Свойства (Properties)**. Как показано на рис. 11-10, интерфейс диалогового окна **Свойства множественных элементов (Properties For Multiple Objects)** отличается от интерфейса обычного диалогового окна свойств пользователя:

- Поля имени учетной записи и пароля отсутствуют. Вы можете указать DNS-имя домена (суффикс основного имени пользователя, UPN), время входа в систему, ограничения по компьютерам, параметры учетной записи, срок действия учетной записи и профили.
- Вы должны конкретно указать поля, с которыми собираетесь работать, ставя соответствующие флажки. Значение, вводимое вами в поле, будет применено ко всем выделенным учетным записям.

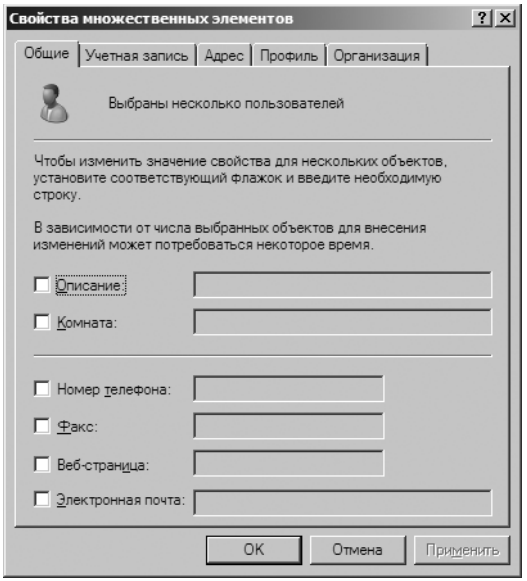


Рис. 11-10. При работе с несколькими учетными записями меняется интерфейс диалогового окна свойств

Назначение профилей нескольким учетным записям

Задание параметров профиля для нескольких учетных записей производится с помощью вкладки **Профиль (Profile)**. Собственно, именно возможность «одним махом» задать профили для нескольких пользователей наиболее часто становится стимулом для работы с несколькими учетными записями в консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)**. Как правило, это осуществляется при помощи переменной среды *%UserName%*, которая позволяет назначать пути и имена файлов на основе имен отдельных пользователей. Например, если задать имя

сценария входа *%UserName%*.cmd, Windows заменит значение переменной на имя пользователя для всех пользователей, учетными записями которых вы управляете. Таким образом, пользователям bobs, janew и ericl будут назначены индивидуальные сценарии входа: Bobs.cmd, Janew.cmd и Ericl.cmd.

На рис. 11-11 показан пример настройки параметров профиля для нескольких учетных записей. Обратите внимание на переменную *%UserName%* — с ее помощью назначаются путь к профилю, имя сценария входа и домашняя папка.

Как правило, каждому пользователю соответствуют собственные имена файлов и путей, но иногда нужно, чтобы они были одними и теми же для всех пользователей. Примером может служить использование обязательных профилей, когда лучше назначать одинаковый путь к профилю для всех пользователей.

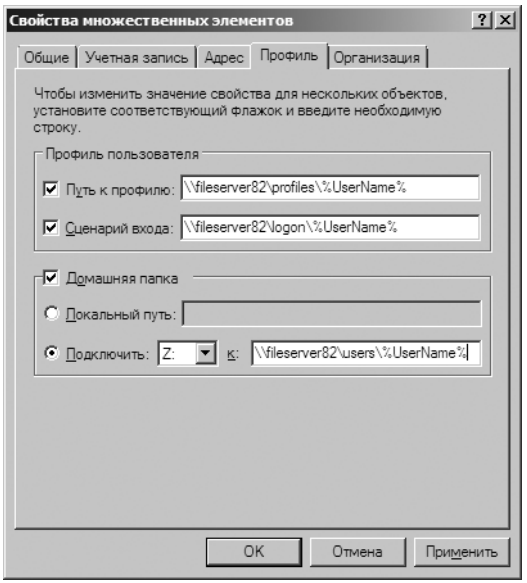


Рис. 11-11. Использование переменной среды %UserName% для назначения путей и имен файлов на основе имен пользователей

Настройка времени входа в систему для нескольких учетных записей

Выбрав несколько учетных записей пользователей в консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)**, можно единовременно настроить время их входа в систему. Выполните следующие действия:

1. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** выделите учетные записи, с которыми хотите работать.

2. Щелкните правой кнопкой выделенные учетные записи и выберите команду **Свойства (Properties)**. В диалоговом окне свойств перейдите на вкладку **Учетная запись (Account)**.
3. Установите флажок **Время входа (Logon Hours)** и щелкните одноименную кнопку. Теперь вы можете задать допустимое время входа в систему, как описано в разделе «Настройка времени входа в систему» этой главы.

Примечание Окно свойств нескольких учетных записей не содержит информации о том, какое время входа было назначено им ранее. В частности, оно не предупредит вас о том, что для разных учетных записей было установлено разное время входа.

Настройка разрешенных рабочих станций для нескольких учетных записей

Разрешенные рабочие станции для нескольких пользователей задаются в диалоговом окне **Рабочие станции для входа в систему (Logon Workstations)**. Чтобы открыть его, выполните следующие действия:

1. В консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** выделите учетные записи, с которыми хотите работать.
2. Щелкните правой кнопкой выделенные учетные записи и выберите команду **Свойства (Properties)**. В диалоговом окне свойств перейдите на вкладку **Учетная запись (Account)**.
3. Установите флажок **Ограничения компьютера (Computer Restrictions)** и щелкните кнопку **Вход на (Log On To)**.
4. Если вы хотите разрешить пользователям входить на все рабочие станции, установите переключатель **На все компьютеры (All Computers)**. Если вы хотите указать конкретные рабочие станции, на которых могут работать выделенные пользователи, щелкните переключатель **Только на указанные компьютеры (The Following Computers)**, а затем введите имена рабочих станций (не более восьми). Когда вы щелкнете **OK**, эти параметры будут применены ко всем выделенным учетным записям пользователей.

Настройка свойств входа, пароля и срока действия для нескольких учетных записей

У учетных записей пользователей есть много параметров, управляющих входом в систему, паролями и сроком действия. Эти параметры задаются на вкладке **Учетная запись (Account)**. Работая с несколькими учетными записями, вы должны активировать параметр, с которым хотите работать, установив соответствующий флажок в крайнем левом столбце. Далее у вас есть два варианта действия:

- Включить параметр, установив его флажок. Например, если вы установите флажок **Срок действия пароля не ограничен (Password Never Ex-**

pires), после щелчка кнопки **OK** пароли выбранных учетных записей будут иметь неограниченное время жизни.

- Не устанавливать флажок, фактически, отключая параметр. Например, если вы активируете параметр **Отключить учетную запись (Account Is Disabled)**, установив флажок слева, но оставите пустым флажок справа, после щелчка кнопки **OK** учетные записи выделенных пользователей будут включены.

Если вы хотите установить срок действия выделенных учетных записей, установите флажок **Срок действия учетной записи (Account Expires)**, а затем задайте подходящее значение срока действия. Переключатель **Никогда (Never)** отменяет любой заданный ранее срок действия. Для задания конкретной даты окончания срока действия установите переключатель **Истекает (End Of)**.

Устранение неполадок при входе в систему

В предыдущем разделе рассказывалось о ситуациях, когда учетные записи могут оказаться отключенными. Как вы уже знаете, чтобы включить отключенную учетную запись, ее нужно щелкнуть правой кнопкой в консоли **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)** и выбрать команду **Включить учетную запись (Enable Account)**.

Чтобы составить список всех отключенных учетных записей домена, введите в командной строке **dsquery user –disabled**. Чтобы включить отключенную учетную запись, введите **dsmod user UserDN –disabled no**.

Если учетная запись блокирована политикой учетных записей, ее нельзя использовать для входа в систему до истечения срока блокировки или пока администратор не сбросит ее. Если длительность блокировки не определена, единственный способ разблокировать учетную запись — прибегнуть к помощи администратора.

Система аудита Windows Server 2008 позволяет протоколировать удачные и неудачные попытки входа в систему. После включения аудита отказов входа в систему сведения об отказах записываются в журнал безопасности на контроллере домена, который был использован для входа. Политики аудита для GPO сайта, домена или подразделения доступны в разделе **Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\Локальные политики\Политика аудита (Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy)**.

Когда пользователь входит в сеть, достоверность учетных данных проверяется контроллером домена. По умолчанию пользователи могут входить в систему с доменными учетными записями, даже если подключение к контроллеру домена отсутствует или контроллер домена, выполняющий проверку подлинности, недоступен. Для этого необходимо, чтобы пользователь ранее уже входил на этот компьютер и имел действительные учетные данные,

сохраненные в кеше. Если в кеше компьютера нет учетных данных пользователя, а также нет подключения к контроллеру домена, пользователь выполнить вход не сможет. По умолчанию рядовой компьютер домена способен хранить в кеше до 10 учетных записей.

В домене, работающем в основном режиме Windows 2000 или Windows Server 2003, проверка подлинности может завершиться неудачей, если системное время рядового компьютера отличается от системного времени контроллера домена, причем, разница превышает предельно допустимое значение, заданное в политике Kerberos **Максимальная погрешность синхронизации часов компьютера (Maximum Tolerance For Computer Clock Synchronization)**. По умолчанию допустимое отклонение составляет 5 минут.

Кроме описанных выше типичных ситуаций отключения учетной записи, причиной отказа в доступе могут стать некоторые параметры системы. Следует обратить особое внимание на следующие варианты:

- **Пользователь видит сообщение, что ему не разрешено выполнить интерактивный вход** Пользователь не обладает правом на локальный вход в систему и не является членом группы, обладающей таким правом. Помните, что право на локальный вход, заданное для контроллера домена, распространяется на все контроллеры в домене. Будучи заданным на рядовом сервере, оно распространяется только на данный сервер. Если пользователю действительно нужен доступ к локальной системе, настройте право пользователя Локальный вход в систему (Logon Locally), как описано в разделе «Настройка прав пользователей» главы 10.
- **Пользователь видит сообщение, что не может войти в систему** Если вы уже проверили пароль и имя учетной записи, возможно, следует проверить тип учетной записи. Возможно, пользователь пытается войти в домен с локальной учетной записью. Не исключено также, что недоступен сервер глобального каталога, в результате чего войти в домен смогут только пользователи, обладающие административными полномочиями.
- **У пользователя обязательный профиль, а компьютер, на котором хранится профиль, в данный момент недоступен** Если пользователю назначен обязательный профиль, компьютер, на котором хранится профиль, должен быть доступен в процессе выполнения входа. Если компьютер выключен или недоступен по другой причине, пользователи с обязательными профилями, скорее всего, войти в систему не смогут. Подробнее о локальных, перемещаемых и обязательных профилях — ранее в этой главе.
- **Пользователь видит сообщение, что с данной учетной записью он не может войти на эту рабочую станцию** Пользователь пытается получить доступ к рабочей станции, вход на которую ему не разрешен. Если пользователь должен иметь доступ к этой рабочей станции, измените информацию о входе, как описано в разделе «Настройка разрешенных рабочих станций» этой главы.

Просмотр и установка разрешений Active Directory

В предыдущих разделах говорилось, что в Active Directory учетные записи пользователей, групп и компьютеров представлены в виде объектов. С объектами Active Directory связаны стандартные и дополнительные разрешения безопасности, которые предоставляют или запрещают доступ к этим объектам. Разрешения для объектов Active Directory не так просты, как прочие разрешения. Набор доступных разрешений может зависеть не только от типа объекта, но и от контейнера, в котором он размещается.

Чтобы просмотреть и настроить разрешения безопасности для объектов Active Directory, выполните следующие действия:

1. Откройте консоль **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)**. В меню **Вид (View)** выберите команду **Дополнительные компоненты (Advanced Features)**. Затем щелкните правой кнопкой учетную запись пользователя, группы или компьютера, с которой хотите работать, и в контекстном меню выберите команду **Свойства (Properties)**.
2. В диалоговом окне свойств перейдите на вкладку **Безопасность (Security)**. На ней приведен список групп и пользователей (рис. 11-12), которым были назначены разрешения для выделенного объекта. Если разрешения недоступны для выделения, значит, они унаследованы от родительского объекта.
3. Пользователи и группы с разрешениями на доступ приведены в списке **Группы или пользователи (Group Or User Names)**. Чтобы изменить разрешения для этих пользователей и групп, выполните следующие действия:
   - Выделите нужного пользователя или группу.
   - В списке **Разрешения (Permissions)** предоставьте или отклоните разрешения на доступ.
   - Если наследуемые разрешения недоступны для выделения, перекройте их, выбрав противоположные разрешения.
4. Чтобы задать разрешения для дополнительных пользователей, компьютеров или групп, щелкните кнопку **Добавить (Add)**. В диалоговом окне **Выбор: «Пользователи», «Компьютеры» или «Группы» (Select Users, Computers, Or Groups)**, добавьте пользователей, компьютеры или группы.
5. В списке **Группы или пользователи (Group Or User Names)** выделите только что добавленный элемент и предоставьте ему необходимые разрешения в списке **Разрешения (Permissions)**. При необходимости повторите эти действия для других пользователей, компьютеров или групп.
6. Завершив работу, щелкните **OK**.

Внимание! К работе с разрешениями следует допускать только администраторов, хорошо разбирающихся в Active Directory и разрешениях Active Directory. Неверно настроенные разрешения объектов могут привести к проблемам, которые будет крайне сложно диагностировать.

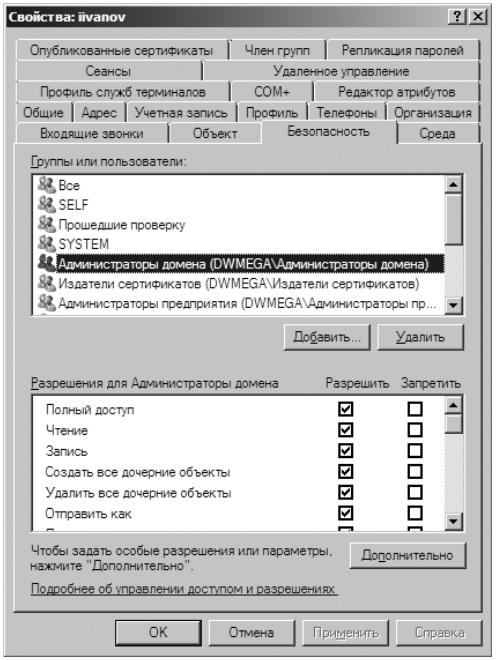


Рис. 11-12. Просмотр и настройка разрешений объектов на вкладке Безопасность (Security)

Чтобы просмотреть и настроить дополнительные разрешения безопасности для объектов Active Directory, выполните следующие действия:

1. Откройте консоль **Active Directory — пользователи и компьютеры (Active Directory Users and Computers)**. В меню **Вид (View)** выберите команду **Дополнительные компоненты (Advanced Features)**. Затем щелкните правой кнопкой учетную запись пользователя, группы или компьютера, с которой хотите работать, и в контекстном меню выберите команду **Свойства (Properties)**.
2. В диалоговом окне свойств перейдите на вкладку **Безопасность (Security)** и щелкните кнопку **Дополнительно (Advanced)**, чтобы отобразить список индивидуальных разрешений для выделенного объекта с информацией об их наследовании.
3. Чтобы просмотреть и настроить отдельные разрешения, выделите элемент и щелкните кнопку **Изменить (Edit)**.
4. Завершив работу, два раза щелкните **OK**.

Часть III

Администрирование данных в Windows Server 2008

Глава 12

Управление файловыми системами и дисками

Жесткий диск — наиболее распространенное устройство для хранения данных на рабочих станциях и серверах. На жестких дисках пользователи хранят текстовые документы, электронные таблицы и прочие типы сведений. Диски организованы в файловые системы, к которым пользователи получают локальный или удаленный доступ.

Локальные файловые системы устанавливаются на компьютерах пользователей. Примером локальной файловой системы может служить диск C, имеющийся на большинстве рабочих станций и серверов. Вы получаете доступ к диску C, используя путь C:\.

Доступ к удаленным системам вы осуществляете посредством сетевого подключения к удаленному ресурсу. Подключение к удаленной файловой системе можно установить при помощи команды **Подключить сетевой диск (Map Network Drive)** проводника Windows.

В задачу системного администратора входит управление дисковыми ресурсами независимо от их расположения. В этой главе рассказывается об инструментах и способах управления файловыми системами и дисками. Глава 13 посвящена наборам томов и отказоустойчивости. В главе 14 рассказывается о том, как управлять файлами и папками.

Управление ролью Файловые службы (File Services)

Файловый сервер — централизованное хранилище с предоставлением общего доступа к файлам по сети. Если вашим пользователям требуется доступ к одним и тем же файлам и данным приложений, настройте в домене один или несколько файловых серверов. В предыдущих версиях ОС Windows Server основные файловые службы устанавливались на все серверы. В Windows Server 2008 вы должны отдельно настроить файловый сервер, добавив на него роль Файловые службы (File Services) и настроив соответствующие службы роли.

В табл. 12-1 представлен обзор служб роли Файловые службы (File Services). Одновременно с этой ролью вам, вероятно, понадобиться установить и следующие компоненты:

- **Система архивации данных Windows Server (Windows Server Backup)** Новая программа резервного копирования, включенная в комплект Windows Server 2008.
- **Диспетчер хранилища для сетей SAN (Storage Manager for SANs)** Позволяет предоставлять пространство для сетей хранения данных (SAN).
- **Многопутевой ввод-вывод (Multipath IO)** Обеспечивает поддержку нескольких каналов между файловым сервером и накопителем. Серверы используют службу многопутевого ввода-вывода для обеспечения избыточности в случае сбоя одного из каналов и для повышения производительности передачи.

Табл. 12-1. Службы роли Файловые службы (File Services)

Служба роли	Описание
Управление общими ресурсами и хранилищами (Share and Storage Management)	Устанавливает консоль Управление общими ресурсами и хранилищами (Share and Storage Management) и настраивает сервер для ее использования. Консоль позволяет администраторам управлять общими папками, а пользователям — осуществлять доступ к общим папкам по сети. Также консоль можно использовать для настройки логических номеров устройств (LUN) в сетях хранения данных (SAN)
Распределенная файловая система DFS (Distributed File System (DFS))	Предоставляет инструменты и службы для служб Пространства имен DFS (DFS Namespaces) и Репликация DFS (DFS Replication). Репликация DFS — это новая и предпочтительная технология репликации. Если домен работает в режиме Windows Server 2008, контроллеры домена используют DFS для обеспечения более устойчивой и детализированной репликации каталога Sysvol
Пространства имен DFS (DFS Namespaces)	Позволяет группировать общие папки, расположенные на различных серверах, в одно или несколько логически взаимосвязанных пространств имен. Каждое пространство имен отображается как одна общая папка с серией подпапок, хотя реальная структура пространства имен может включать общие папки, расположенные на нескольких серверах в различных сайтах
Репликация DFS (DFS Replication)	Позволяет синхронизировать папки на нескольких серверах с помощью подключений по локальной или глобальной сети. Используется механизм репликации с несколькими хозяевами. При помощи протокола RDC (Remote Differential Compression) механизм репликации способен синхронизовать только фрагменты файлов, изменившиеся со времени последней репликации. Репликация DFS может использоваться совместно со службой Пространства имен DFS (DFS Namespaces) или без нее

Табл. 12-1. (*окончание*)

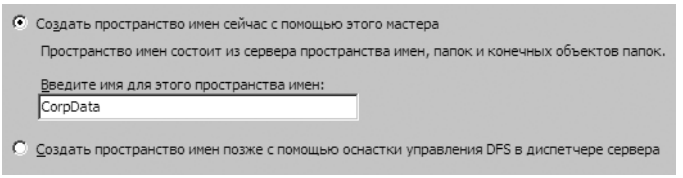
Служба роли	Описание
Диспетчер ресурсов файлового сервера (File Server Resource Manager (FSRM))	Устанавливает набор инструментальных средств для управления данными, хранящимися на сервере. При помощи FSRM администратор может составлять отчеты о хранилище, настраивать квоты и определять политики фильтрования файлов (file screening)
Службы для NFS (Services For Network File System)	Предоставляет решение для организации общего доступа к файлам на предприятиях со смешанными средами — Windows и UNIX. После установки служб для NFS пользователи смогут передавать файлы между ОС Windows Server 2008 и UNIX посредством протокола NFS
Служба поиска Windows (Windows Search Service)	Позволяет проводить быстрый поиск ресурсов на сервере с клиентских компьютеров, совместимых со службой поиска Windows. Эта функция предназначена, в основном, для настольных компьютеров и небольших офисов
Файловые службы Windows Server 2003 (Windows Server 2003 File Services)	Предоставляет файловые службы, совместимые с Windows Server 2003, что позволяет использовать сервер Windows Server 2008 совместно с серверами Windows Server 2003
Служба репликации файлов (File Replication Service (FRS))	Позволяет синхронизировать папки с файловыми серверами, использующими механизм репликации FRS. Также позволяет проводить синхронизацию с реализацией DFS из Windows 2000. Если в вашей организации имеется компьютер, использующий технологию FRS, вам может потребоваться установка этой службы роли для обеспечения совместимости с Windows Server 2008. Если домен работает в режиме Windows Server 2003, контроллеры домена, работающие под управлением Windows Server 2008, автоматически используют для репликации RFS
Служба индексирования (Indexing Service)	Позволяет индексировать файлы и папки для ускорения поиска. При помощи соответствующего языка запросов пользователи могут быстро найти интересующие файлы. Нельзя устанавливать службу индексирования и службу поиска на один и тот же компьютер

Чтобы добавить роль Файловые службы (File Services) на сервер, выполните следующие действия:

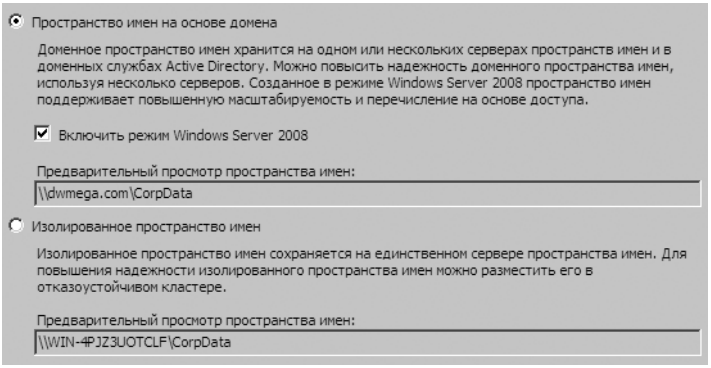
1. В дереве консоли **Диспетчер сервера (Server Manager)** выделите узел **Роли (Roles)** и щелкните ссылку **Добавить роли (Add Roles)**. Откроется Мастер добавления ролей (Add Roles Wizard). Если работа мастера начнется со страницы **Перед началом работы (Before You Begin)**, ознакомьтесь с вводным текстом и щелкните **Далее (Next)**.

Примечание В процессе установки на сервере создаются общие файлы. Если некая проблема привела к сбою в процессе установки, вы можете продолжить установку при помощи мастера Добавление ролей служб (Add Role Services). После повторного запуска диспетчера сервера в узле **Роли (Roles)** выделите узел **Файловые службы (File Services)** и прокрутите область сведений до ссылки **Добавить службы ролей (Add Role Services)**. Щелкните ее и продолжайте установку с шага 3. Если вы занимались настройкой распределенной файловой системы в рамках домена, вам нужно будет предоставить административные учетные данные.

2. На странице **Выбор ролей сервера (Select Server Roles)** установите флажок **Файловые службы (File Services)** и два раза щелкните **Далее (Next)**.
3. На странице **Выбор служб ролей (Select Role Services)** выделите одну или несколько служб. Их краткое описание приводится в табл. 12-1. Для обеспечения совместимости с UNIX обязательно установите флажок **Службы для NFS (Services For Network File System)**. Щелкните **Далее (Next)**.
4. Пространство имен DFS — это виртуальное представление общих папок, расположенных на различных серверах. В ходе установки службы роли Пространства имен DFS (DFS Namespaces) вы увидите три дополнительные страницы с параметрами:
   - На странице **Создание пространства имен DFS (Create A DFS Namespace)** задайте имя первого пространства имен или укажите, что пространство имен будет создано позже, как показано на следующем рисунке. Имя пространства имен должно быть простым для запоминания, например, CorpData. В большом предприятии вам, возможно, придется создать отдельные пространства имен для каждого крупного отдела.



   - На странице **Выберите тип пространства имен (Select Namespace Type)** укажите, какое пространство имен вы хотите создать: на основе домена или изолированное, как показано на следующем рисунке. Пространства имен на основе домена можно реплицировать на несколько серверов, обеспечив их высокую доступность, но в них можно иметь не более 5000 DFS-папок. Изолированное пространство имен может содержать до 50000 DFS-папок, но оно реплицируется только при использовании отказоустойчивых кластеров.

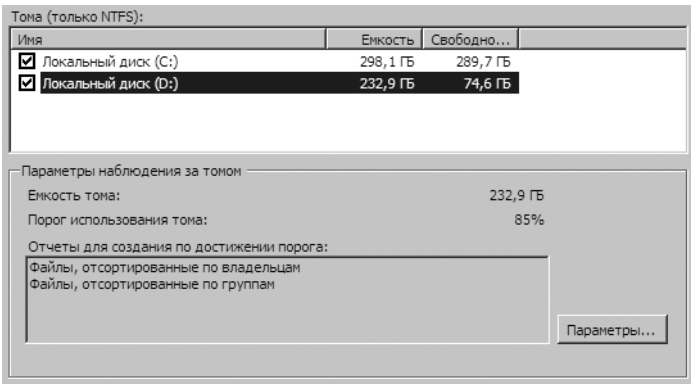


- На странице **Настройка пространства имен (Configure Namespace)** вы можете добавить в пространство имен общие папки, а также другие пространства имен, сопоставленные с DFS-папкой, как показано на следующем рисунке. Щелкните **Добавить (Add)**. В диалоговом окне **Добавление папки в пространство имен (Add Folder To Namespace)** щелкните кнопку **Обзор (Browse)**. В диалоговом окне **Обзор общих папок (Browse For Shared Folders)** выберите общую папку и щелкните **OK**. Введите имя добавляемой папки и щелкните **OK**. Введите имя папки в пространстве имен. Оно может совпадать с именем первоначальной папки или быть новым именем, которое будет сопоставлено с исходной папкой в пространстве имен. Введя имя, щелкните **OK**, чтобы добавить папку и завершить процесс.

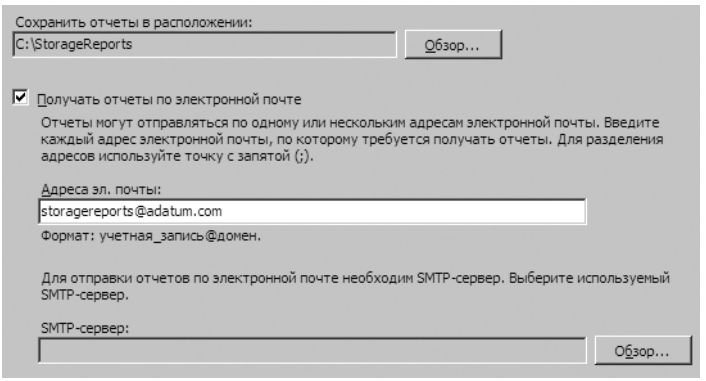
Примечание Настраивать службу Пространства имен DFS (DFS Namespaces) одновременно с установкой файлового сервера необязательно. Установив службы Пространства имен DFS (DFS Namespaces), Репликация DFS (DFS Replication) или обе сразу, вы сможете управлять соответствующими функциями в консоли **Управление DFS (DFS Management)**. Команда для ее вызова находится в меню **Администрирование (Administrative Tools)**. Подробнее — в главе 15.

5. Диспетчер ресурсов файлового сервера (File Server Resource Manager) позволяет наблюдать за объемом используемого пространства томов и создавать отчеты о хранилище. Если вы устанавливаете диспетчер ресурсов файлового сервера, вам будут предложены две дополнительные страницы:

- На странице **Настроить наблюдение за использованием хранилища (Configure Storage Usage Monitoring)** вы можете выбрать тома, наблюдение за которыми следует вести, как показано на следующем рисунке. Выбрав том и щелкнув кнопку **Параметры (Options)**, вы сможете задать порог использования тома и выбрать отчеты, которые будут создаваться при достижении порога использования тома. По умолчанию порог равен 85%.



- На странице **Настроить параметры отчета (Set Report Options)** задается расположение отчетов об использовании томов, как показано на следующем рисунке. Каждый раз при достижении томом порога, генерируется по одному отчету указанных вами типов. Автоматическое удаление старых отчетов не производится. По умолчанию для сохранения отчетов используется папка %SystemDrive%\StorageReports. Чтобы изменить стандартное расположение, щелкните кнопку **Обзор (Browse)** и задайте новое расположение в диалоговом окне **Обзор папок (Browse For Folders)**. Кроме того, вы можете задать отправку отчетов по электронной почте. Укажите адрес электронной почты получателя и сервер SMTP, который следует использовать.



Примечание Необязательно настраивать службу наблюдения и отчетов именно сейчас. Позже вы сможете использовать для этих целей консоль диспетчера ресурсов файлового сервера. Команда для ее вызова находится в меню **Администрирование (Administrative Tools)**. Подробнее — в главе 14.

6. Если вы устанавливаете Службу поиска Windows (Windows Search Service), вам будет предложено выбрать тома для индексирования. Индексирование тома, с одной стороны, позволяет пользователям производить быстрый поиск. С другой стороны, индексирование целого тома может отрицательно сказаться на производительности службы, в особенности, если речь идет о системном томе. Поэтому лучше индексировать лишь отдельные общие папки. Этим можно заняться позднее.

Примечание Необязательно настраивать службу индексирования именно сейчас. После установки Службы поиска Windows (Windows Search Service) вы можете использовать для этих целей утилиту Параметры индексирования (Indexing Options) панели управления.

7. Заполнив все страницы мастера с параметрами, щелкните **Далее (Next)**. На экране появится страница **Подтвердите выбранные элементы (Confirm Installation Options)**. Щелкните кнопку **Установить (Install)**, чтобы приступить к процессу установки. Когда установка сервера и выбранных вами служб завершится, на экране появится страница **Результаты установки (Installation Results)**. Просмотрите описание установки и убедитесь, что все этапы установки завершились успехом.

Если роль Файловые службы (File Services) уже установлена на сервер, но вы хотите установить дополнительные службы, разверните узел **Роли (Roles)** диспетчера сервера и щелкните узел **Файловые службы (File Services)**. Прокрутите область сведений, пока не дойдете до раздела **Службы ролей (Role Services)**. Щелкните ссылку **Добавить службы ролей (Add Role Services)** и добавляйте службы ролей, как описано выше, начиная с шага 3.

Добавление жестких дисков

Прежде чем сделать жесткий диск доступным для пользователей, следует настроить его и продумать, как он будет использоваться. Система Microsoft Windows Server 2008 позволяет настраивать жесткие диски разными способами. Способ, который следует выбрать вам, во многом зависит от типа данных, с которыми вы работаете, и требований сетевого окружения. Для обычных пользовательских данных, хранящихся на рабочих станциях, можно настроить в качестве автономных устройств хранения отдельные диски. При этом данные пользователя хранятся на локальном жестком диске рабочей станции, и к ним можно получить локальный доступ.

Несмотря на удобство хранения данных на одном диске, это все же не самый надежный способ. В целях повышения надежности и производительности, следует объединить диски в набор. ОС Windows Server 2008 подде-

рживает наборы и массивы дисков при помощи технологии RAID, которая встроена в систему.

Физические диски

Используете ли вы отдельные диски или дисковые массивы, в них всегда присутствуют физические диски — реальные устройства для хранения данных. Количество данных, которые можно сохранить на диске, зависит от его объема и от возможности сжатия. Обычные современные диски имеют вместимость от 100 Гб до 1 Тб. Для использования в ОС Windows Server 2008 подходят диски многих типов, в том числе, диски с интерфейсами SCSI, ATA и SATA.

Сокращения SCSI, PATA и SATA обозначают тип интерфейса, используемого для связи с контроллером диска. Диски SCSI работают с контроллерами SCSI, диски ATA — с контроллерами ATA, и т. д. Во время установки нового сервера следует хорошо продумать конфигурацию его дисков. Начните с выбора дисков или систем хранения данных, обеспечивающие требуемый уровень производительности. Между различными системами дисков существует значительная разница в скорости и производительности.

Помимо емкости следует руководствоваться следующими параметрами:

- **Частота вращения** Показатель скорости вращения диска.
- **Среднее время позиционирования** Время, требуемое для перевода головки с одной дорожки на другую во время последовательных операций ввода-вывода.

Вообще, при сравнении дисков с одинаковой спецификацией, например, Ultra320 SCSI или SATA II, предпочтение следует отдавать дискам с более высокой скоростью вращения и меньшим средним временем позиционирования. Например, диск со скоростью вращения 15000 об/мин обеспечит на 45%–50% операций ввода-вывода в секунду больше, чем диск со скоростью вращения 10000 об/мин, при условии что остальные показатели равны. У диска со временем позиционирования 3,5 мс время отклика будет на 25%–30% лучше, чем у диска со временем позиционирования 4,7 мс.

Далее перечислены другие показатели, на которые следует обратить внимание:

- **Максимальная скорость непрерывной передачи данных** Показатель количества данных, которое диск способен передавать непрерывно.
- **Наработка до отказа (mean time to failure, MTTF)** Предполагаемое количество часов, которые диск должен отработать до отказа.
- **Нерабочие температуры** Температуры, при которых диск не будет работать.

У большинства дисков сравнимого качества и показатели тоже сходные. Например, если сравнить диски Ultra320 SCSI со скоростью вращения 15000 об/мин, вероятно, у них обнаружатся сходные скорости передачи данных и MTTF. В частности, у диска Maxtor Atlas 15K II максимальная скорость непрерывной передачи данных составляет 98 мегабайт в секунду, тогда как

у диска Seagate Cheetah 15K.4 аналогичный показатель равен 96 Мб/с. У обоих дисков наработка до отказа равна 1,4 миллиона часов. Скорость передачи данных может выражаться и в гигабитах в секунду (Гбит/с). Скорость 1,5 Гбит/с соответствует скорости 188 Мб/с, а скорость 3,0 Гбит/с эквивалентна 375 Мб/с. Иногда в спецификации диска указывают максимально возможную скорость передачи данных (maximum external transfer rate) и среднюю скорость непрерывной передачи данных. Наиболее важным показателем является средняя скорость непрерывной передачи данных. Диск Seagate Barracuda 7200 SATA II имеет скорость вращения 7200 об/мин и среднюю скорость непрерывной передачи данных 58 Мб/с. При среднем времени позиционирования 8,5 мс и наработкой до отказа 1 млн часов, его производительность вполне сравнима с другими дисками SATA II со скоростью вращения 7200 об/мин. Тем не менее, большинство дисков Ultra320 SCSI обладают большей производительностью, и лучше выполняют многопользовательские операции чтения-записи.

Другой важный показатель, который следует учесть при выборе диска, это его рабочая температура. Однако не все администраторы придают ей значение. Как правило, чем быстрее вращается диск, тем горячее он становится. Это не всегда так, но этот фактор определенно следует учитывать при выборе диска. Например, большинство дисков серии 15K склонны к перегреву, поэтому следует внимательно регулировать температурный режим. Как Maxtor Atlas 15K II, так и Seagate Cheetah 15K.4 при температуре 70°C или выше могут отказать (как и большинство других дисков).

Подготовка физического диска к использованию

После установки диска требуется его настроить, создав разделы и, при необходимости, файловые системы в этих разделах. Разделом (partition) называется фрагмент физического диска, работающий как самостоятельная единица. Разделы бывают двух видов: с главной загрузочной записью (Master Boot Record, MBR) и с таблицей разделов глобально-универсальных идентификаторов (GUID Partition Table, GPT). Обе версии Windows Server 2008 — 32-разрядная и 64-разрядная — поддерживают как MBR, так и GPT. GPT-разделы нельзя читать в предыдущих версиях Windows Server для аппаратных платформ *x*86 или *x*64.

Главная загрузочная запись содержит таблицу разделов, в которой указано, в каких местах диска расположены разделы. В дисках этого типа первый сектор жесткого диска содержит главную загрузочную запись и двоичный код, который называется главным загрузочным кодом и используется для загрузки системы. Этот сектор не делится на разделы и скрыт от просмотра для защиты системы.

Диски MBR поддерживают тома размером до четырех терабайт (Тб) и разбиваются на разделы двух типов — первичные и расширенные. Каждый диск MBR может содержать до четырех первичных разделов или три первичных раздела и один расширенный. Первичный раздел — это раздел, к

которому можно получить непосредственный доступ для хранения файлов. Вы обеспечиваете доступ пользователей к первичному разделу, создавая на нем файловую систему. В отличие от первичных разделов, получить непосредственный доступ к расширенному разделу нельзя. На нем создаются один или несколько логических дисков, используемых для хранения файлов. Возможность разбивать расширенные разделы на логические диски позволяет создавать на физическом диске более четырех разделов.

Разделы GPT разрабатывались для высокопроизводительных компьютеров на базе Itanium. Эти разделы рекомендуется использовать для дисков объемом свыше 2 Тб на системах *x*86 и *x*64, а также для любых дисков, работающих на компьютерах на базе Itanium. Ключевое различие между разделами GPT и MBR связано со способом хранения данных раздела. В GPT важные данные раздела хранятся в отдельных разделах. Кроме того, для обеспечения целостности структуры используются избыточные основные и резервные таблицы. GPT-диски поддерживают тома объемом до 18 эксабайт (Эб) и могут содержать до 128 разделов. Несмотря на базовые различия между разделами GPT и MBR, большинство связанных с дисками задач выполняется одинаково в обоих случаях.

Оснастка Управление дисками (Disk Management)

Оснастка **Управление дисками (Disk Management)** упрощает работу с локальными и внешними дисками на локальной и удаленной системе. Она входит в состав консолей **Управление компьютером (Computer Management)** и **Диспетчер сервера (Server Manager)**. Кроме того, ее можно добавить в любую консоль MMC. Чтобы получить доступ к узлу **Управление дисками (Disk Management)** консолей **Управление компьютером (Computer Management)** и **Диспетчер сервера (Server Manager)**, нужно развернуть узел **Хранилище (Storage)**.

Оснастка **Управление дисками (Disk Management)** имеет три представления: Список дисков (Disk List), Графическое представление (Graphical View) и Список томов (Volume List). Существуют ограничения на выполнение некоторых задач на удаленных системах при помощи консоли **Управление дисками (Disk Management)**. К доступным задачам удаленного управления относятся просмотр сведений о диске, изменение букв и путей дисков и преобразование типов дисков. Для съемных носителей вы также можете выполнить дистанционное извлечение. Для более сложных манипуляций с удаленными дисками используйте утилиту командной строки DISKPART.

Примечание Прежде чем приступить к работе с консолью **Управление дисками (Disk Management)**, обратите внимание на следующие моменты. Если вы создаете раздел, но не форматируете его, он будет отмечен как свободное пространство. Если вы не назначили часть диска разделу, эта часть будет отмечена **Не распределен (Unallocated)**.

На рис. 12-1 представление Список томов (Volume List) находится в правом верхнем углу, а Графическое представление (Graphical View) — в правом нижнем углу. Это стандартная конфигурация. Вы можете изменить вид верхней или нижней панели следующим образом:

- Чтобы изменить верхнее представление, откройте меню **Вид (View)**, выберите команду **Верх (Top)** и укажите желаемое представление.
- Чтобы изменить нижнее представление, откройте меню **Вид (View)**, выберите команду **Низ (Bottom)** и укажите желаемое представление.
- Чтобы скрыть нижнее представление, откройте меню **Вид (View)** и выберите команды **Низ (Bottom)** и **Скрыть (Hidden)**.

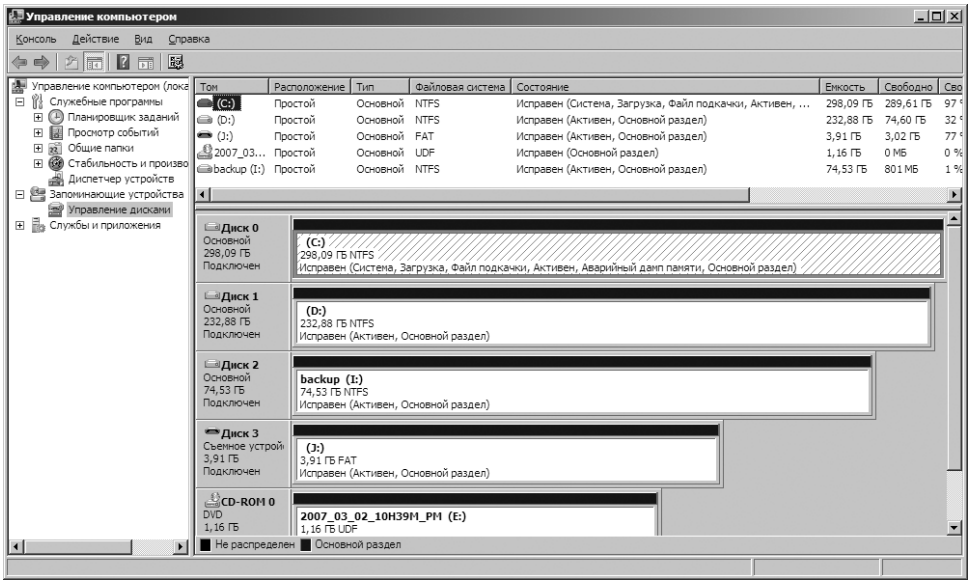


Рис. 12-1. В верхней части оснастки Управление дисками (Disk Management) отображается сводка обо всех дисках компьютера. В нижней части приводятся более подробные сведения о тех же дисках

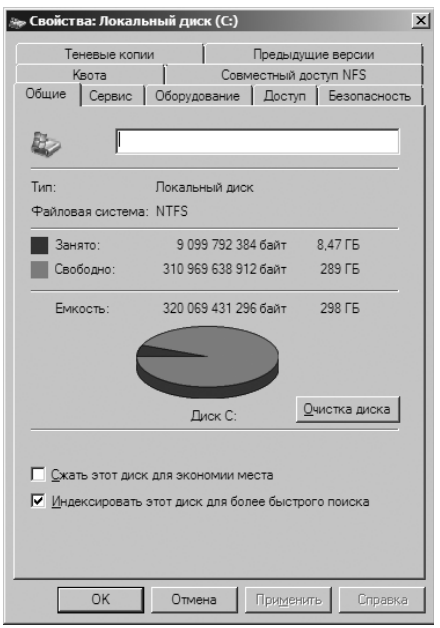
В ОС Windows Server 2008 поддерживаются три типа дисков:

- **Основной (Basic)** Обычный несъемный диск, как в предыдущих версиях Windows. Основные диски разбиваются на разделы и могут использоваться с предыдущими версиями Windows.
- **Динамический (Dynamic)** Усовершенствованный несъемный диск для Windows Server 2008, который в большинстве случаев можно обновлять без перезагрузки системы. Динамические диски делятся на тома, их можно использовать только в Windows 2000 и более поздних версиях.
- **Съемный (Removable)** Стандартный диск, связанный со съемным накопителем данных. Съемные устройства хранения данных могут форматироваться в exFAT, FAT16, FAT32 или NTFS.

Ближе к реальности Файловая система exFAT для съемных накопителей поддерживается в ОС Windows Vista SP1 или более поздних, а также в Windows Server 2008. Файловая система exFAT — новое поколение файловых систем FAT (FAT12/16 и FAT32). Вобрав в себя преимущества простой файловой системы FAT32, exFAT позволяет преодолеть присущий FAT32 4-гигабайтное ограничение на размер файла и 32-гигабайтный предел на объем раздела. Файловая система exFAT также поддерживает единицы выделения памяти размером до 32768 Кб.

Система exFAT годится для использования с любой совместимой ОС или устройством. Это значит, что вы можете удалить накопитель exFAT из совместимой камеры и вставить его в совместимый телефон и т. д., не прибегая к повторному форматированию. Это также означает, что вы можете извлечь накопитель exFAT из компьютера под управлением Mac OS или Linux и подключить его к компьютеру под управлением Windows.

Чтобы получить более подробную информацию о разделе диска в консоли **Управление дисками (Disk Management)**, щелкните раздел правой кнопкой и в контекстном меню выберите команду **Свойства (Properties)**. Откроется диалоговое окно, примерный вид которого для локальных дисков показан на рис. 12-2 слева, а справа показан вид того же окна, но для съемных дисков. Это точно такое же диалоговое окно которое открывается в Проводнике Windows (Windows Explorer), если выделить на диске папку верхнего уровня и выбрать в меню **Файл (File)** команду **Свойства (Properties)**.



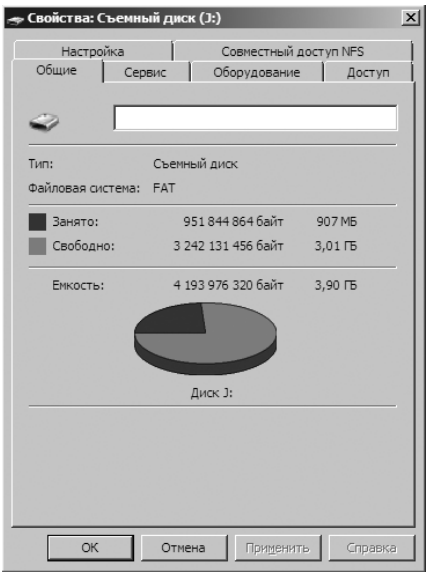


Рис. 12-2. Подробная информация о диске на вкладке Общие (General) диалогового окна Свойства (Properties)

Съемные накопители

Съемные накопители могут форматироваться в NTFS, FAT, FAT32 и exFAT. Они обычно подключаются к компьютеру извне и допускают оперативное включение и выключение. Большинство внешних накопителей имеют интерфейс USB или FireWire. С точки зрения пользователя, скорость передачи данных и общая производительность оборудования с интерфейсами USB и FireWire зависит, в основном, от поддерживаемой версии. В данный момент используется несколько версий USB и FireWire, включая USB 1.0, USB 1.1, USB 2.0, FireWire 400 и FireWire 800.

Интерфейс USB 2.0 — это промышленный стандарт, поддерживающий передачу данных с максимальной скоростью 480 Мб/с. Скорость непрерывной передачи данных колеблется от 10 до 30 Мб/с. Реальное значение скорости передачи зависит от многих факторов, например, типа устройства, типа передаваемых данных и быстродействия компьютера. Все USB-контроллеры компьютера обладают постоянной пропускной способностью, которую делят между собой все устройства, подключенные к данному контроллеру. Скорость передачи данных будет значительно ниже, если на компьютере установлен USB-порт более ранней версии, чем у используемого устройства. Допустим, вы подключаете устройство с интерфейсом USB 2.0 к порту USB 1.0. В результате, устройство будет работать на значительно меньше скорости интерфейса USB 1.0.

Порты USB 1.0, 1.1 и 2.0 выглядят одинаково. Надежнее всего определить тип USB-портов компьютера можно, заглянув в его документацию. В будущем порты USB 2.0 будут устанавливаться на ЖК-мониторах, к которым также можно будет подключать устройства. При подключении USB-устройства к монитору, последний будет выступать в роли USB-концентратора. Все устройства, подключенные к концентратору, будут делить между собой один канал. Общая ширина канала определяется скоростью входа USB, к которому подключен концентратор.

Интерфейс FireWire (IEEE 1394) — высокопроизводительный стандарт подключения с одноранговой архитектурой. Между периферийными устройствами на шине возникают конфликты, в результате которых определяется устройство, способное лучше управлять передачей данных. Как и в случае USB, сегодня используется несколько версий интерфейса FireWire, например, FireWire 400 и FireWire 800. Максимальная скорость непрерывной передачи для интерфейса FireWire 400 (IEEE 1394a) может достигать 400 Мб/с, а для интерфейса FireWire 800 (IEEE 1394b) — 800 Мб/с. При подключении устройства FireWire 800 к порту FireWire 400 или наоборот, устройство будет работать на низкой скорости интерфейса FireWire 400.

Порты и кабели FireWire 400 и FireWire 800 различны по форме, так что их проще отличить друг от друга (если вы знаете, что ищете). Внешне кабели и порты FireWire 400 выглядят точно так же, как и ранние версии FireWire, применявшиеся до окончательного формирования спецификаций IEEE 1394a и

IEEE 1394b. Однако в ранних вариантах FireWire в соединительных кабелях было другое количество контактов, а в портах было иное количество разъемов. Поэтому ранний интерфейс FireWire нетрудно отличить от FireWire 400 — достаточно посмотреть на кабели и порты. Кабели и порты ранних версий FireWire имеют четыре штырька и четыре разъема. В портах и кабелях интерфейса FireWire 400 имеется шесть штырьков и шесть разъемов.

При покупке внешнего устройства для компьютера обратите внимание на интерфейсы, поддерживаемые устройством. Встречаются устройства с двойным интерфейсом, поддерживающие USB 2.0 и FireWire 400, а также с тройным — USB 2.0, FireWire 400 и FireWire 800. Устройства с двойным или тройным интерфейсом более функциональны.

Работа со съемными дисками мало отличается от работы с несъемными носителями. Вы можете выполнить следующие действия:

- Щелкните диск правой кнопкой и выберите команду **Открыть (Open)** или **Проводник (Explore)**, чтобы просмотреть содержимое диска в Проводнике Windows (Windows Explorer).
- Щелкните диск правой кнопкой и выберите команду **Форматировать (Format)**, чтобы отформатировать диск, как описано в разделе «Форматирование разделов» этой главы. Как правило, на съемном диске создается единственный раздел.
- Щелкните диск правой кнопкой и выберите команду **Свойства (Properties)** для просмотра и редактирования свойств диска. На вкладке **Общие (General)** диалогового окна **Свойства (Properties)** вы можете задать метку тома, о чем рассказано в разделе «Изменение или удаление метки тома».

Работая со съемными носителями, можно настраивать виды диска и папок. Щелкните правой кнопкой диск или папку, выберите команду **Свойства (Properties)** и перейдите на вкладку **Настройка (Customize)**. Здесь вы можете настроить шаблон папки, который позволяет управлять отображаемыми сведениями. В частности, можно задать шаблоны **Документы (Documents)** или **Изображения и видео (Pictures And Videos)** и настроить рисунки и значки папок.

На съемных дисках поддерживается общий сетевой доступ к файлам и папкам. Он настраивается точно так же, как и обычный общий доступ к файлам: с разрешениями, кешированием для автономного использования и ограничением на количество одновременных подключений. Можно предоставить общий доступ ко всему съемному диску или к отдельным его папкам. Для одной папки можно создать несколько общих ресурсов.

Общий доступ к съемным дискам отличается от общего доступа к NTFS тем, что на них может отсутствовать архитектура безопасности. В файловых системах exFAT, FAT и FAT32 папки и файлы не обладают разрешениями или другими параметрами безопасности, за исключением стандартных атрибутов «только чтение» или «скрытый».

Установка и проверка нового диска

Функция «горячей» замены позволяет отключать устройства без выключения компьютера. Обычно устройства с возможностью «горячей» замены подключаются на передней панели компьютера. Если ваш компьютер поддерживает «горячую» замену дисков, вы можете устанавливать диски, не выключая компьютер. Подключив диск, откройте оснастку **Управление дисками (Disk Management)** и в меню **Действие (Action)** выберите команду **Повторить проверку дисков (Rescan Disks)**. Найденные новые диски будут добавлены в список с соответствующим типом. Если установленный вами диск не найден, перезагрузите компьютер.

Если компьютер не поддерживает «горячую» замену дисков, вы должны выключить его и установить новые диски. Далее выполните поиск дисков, как описано выше. Если вы работаете с дисками, не прошедшими инициализацию (то есть, у них отсутствуют подписи), откройте оснастку Управление дисками (Disk Management). При обнаружении новых дисков будет запущен Мастер инициализации и преобразования дисков (Initialize And Convert Disk Wizard).

Чтобы инициализировать новые диски при помощи Мастера инициализации и преобразования дисков (Initialize And Convert Disk Wizard), выполните следующие действия:

1. Щелкните **Далее (Next)** на стартовой странице. На странице **Выбор диска для инициализации (Select Disks To Initialize)** автоматически задана инициализация добавленных вами дисков. Если вы не хотите инициализировать тот или иной диск, сбросьте соответствующий флажок.
2. Щелкните **Далее (Next)**, чтобы перейти на страницу **Выбор дисков для преобразования (Select Disks To Convert)**. На этой странице приводится список новых дисков, а также всех несистемных или загрузочных дисков, которые можно преобразовать в динамические диски. Новые диски по умолчанию не выбраны. Если вы хотите преобразовать диски, выделите их и щелкните **Далее (Next)**.
3. На заключительной странице перечислены выбранные вами параметры и указаны действия, которые будут выполнены в отношении каждого диска. Если параметры заданы правильно, щелкните **Готово (Finish)**. Компьютер приступит к выполнению намеченных действий. Если вы выбрали инициализацию диска, мастер запишет на диск подпись. Если вы выбрали преобразование диска, мастер выполнит его.

Если вы не хотите работать с мастером Мастера инициализации и преобразования дисков (Initialize And Convert Disk Wizard), закройте его и продолжайте работу с дисками в оснастке **Управление дисками (Disk Management)**. В представлении **Список дисков (Disk List)** рядом с диском будет стоять красный восклицательный знак, а в столбце с состоянием диска будет стоять значение Не проинициализирован (Not Initialized). Щелкните значок диска правой кнопкой и выберите команду **Инициализировать диск**

(Initialize Disk). Подтвердите свой выбор и при необходимости добавьте другие диски для инициализации, а затем щелкните **OK**. Преобразование диска в динамический рассматривается в разделе «Преобразование основного диска в динамический» этой главы.

Состояние диска

Информация о состоянии диска полезна во время его установки или при диагностике диска. Оснастка **Управление дисками (Disk Management)** отображает состояние диска в представлениях **Графическое представление (Graphical View)** и **Список томов (Volume List)**. В табл. 12-2 приводится краткое описание наиболее распространенных состояний.

Табл. 12-2. Основные состояния диска

Состояние	Описание	Действие
Подключен (Online)	Обычное состояние диска. На диске нет неисправностей, и он доступен. Это состояние присуще как динамическим, так и основным дискам	На диске нет ни одной из известных неисправностей. Он не нуждается в исправ-лениях
Работает (ошибки) (Online (Errors))	На динамическом диске обнаружены ошибки ввода-вывода	Попытайтесь исправить временные ошибки, щелкнув диск правой кнопкой и выбрав команду **Реактивизировать диск (Reactivate Disk)**. Если это не удалось, возможно, на диске имеется аппаратная неисправность. Запустите полную проверку диска
Не подключен (Offline)	Нет доступа к диску. Диск поврежден или временно недоступен. Если имя диска изменено на **Отсутствует (Missing)**, система не может обнаружить или идентифицировать диск	Проверьте диск, контроллер и кабели. Убедитесь, что к диску подведено питание и он правильно подключен. Для перевода диска в оперативный режим (если это возможно) используйте команду **Реактивизировать диск (Reactivate Disk)**.
Инородный (Foreign)	Диск был перемещен на компьютер, но не был импортирован. Иногда этот состояние назначается неисправному диску, переведенному в оперативный режим	Чтобы добавить диск в систему, щелкните его правой кнопкой и выберите команду **Импорт чужих дисков (Import Foreign Disks)**

Табл. 12-2. (*продолжение*)

Состояние	Описание	Действие
Не читается (Unreadable)	В данный момент нет доступа к диску. Это происходит, например, во время проверки дисков. Это состояние присуще как динамическим, так и основным дискам	Это состояние может отображаться для устройств FireWire/USB чтения смарт-карт, если карта не отформатирована или отформатирована неверно. Кроме того, это состояние отображается после извлечения смарт-карты из устройства. Если проверка дисков в данный момент не проводится, на диске могут быть неисправности или ошибки ввода-вывода. Чтобы устранить неисправность, щелкните диск правой кнопкой и выберите в меню **Действие (Action)** команду **Повторить проверку дисков (Rescan Disks)**. Возможно, придется перезагрузить систему
Неопознан (Unrecognized)	Диск относится к неизвестному типу и не может использоваться в системе. Такое состояние может отображаться для диска из ОС, отличной от Windows	Если диск использовался с другой ОС, ничего не делайте. Вы не сможете использовать данный диск, поэтому попробуйте установить другой. Чтобы подготовить диск к использованию в Windows Server 2008, щелкните его правой кнопкой и выберите команду **Инициализировать диск (Initialize Disk)**
Не проинициализирован (Not Initialized)	На диске нет действительной подписи. Такое состояние может отображаться для диска из ОС, отличной от Windows	Если диск использовался с другой ОС, ничего не делайте. Вы не сможете использовать данный диск, поэтому попробуйте установить другой. Чтобы подготовить диск к использованию в Windows Server 2008, щелкните его правой кнопкой и выберите команду **Инициализировать диск (Initialize Disk)**

Табл. 12-2. (*окончание*)

Состояние	Описание	Действие
Нет носителя (No Media)	Отсутствует или извлечен носитель из CD-ROM-дисковода или съемного диска. Это состояние отображается только для CD-ROM-дисководов и съемных дисков	Для перевода диска в оперативный режим вставьте компакт-диск, дискету или съемный накопитель. Для кардридеров с интерфейсом FireWire/USB этот состояние обычно (но не всегда) отображается при извлечении карты

Работа с основными и динамическими дисками

В ОС Windows Server 2008 поддерживаются два типа конфигураций локальных дисков:

- **Основной** Обычный тип диска, как и в предыдущих версиях Windows. Основные диски разбиваются на разделы и могут использоваться с предыдущими версиями Windows.
- **Динамический** Улучшенный тип диска для Windows Server 2008. В большинстве случаев такой диск можно обновлять без перезагрузки системы. Динамические диски делятся на тома, их можно использовать только с Windows 2000 и более поздними версиями.

Примечание Нельзя использовать динамические диски на портативных компьютерах или съемных носителях.

Применение основных и динамических дисков

Когда вы переходите в Windows Server 2008, диски с разделами инициализируются как основные. При установке Windows Server 2008 на новый компьютер, на дисках которого нет разделов, вы вольны инициализировать диски как основные или как динамические.

В основных дисках поддерживаются стандартные функции отказоустойчивости. Их можно использовать для поддержки или удаления существующих составных, зеркальных и чередующихся конфигураций. А вот создавать новые отказоустойчивые наборы основные диски не позволяют. Для этого их нужно преобразовать в динамические, а затем создать тома с зеркалированием или чередованием. Функции отказоустойчивости и возможность изменения дисков без перезагрузки компьютера — ключевые отличия между основными и динамическими дисками. Прочие доступные функции зависят от формата диска.

На одном компьютере можно использовать как основные, так и динамические диски, но наборы томов должны состоять из однотипных дисков. Например, если у вас имеются зеркалированные диски C и D, созданные в Windows NT 4.0, их можно использовать в Windows Server 2008. Если вы

захотите преобразовать диск C в динамический тип, преобразовать придется и диск D. О преобразовании основного диска в динамический читайте в разделе «Изменение типов дисков» этой главы.

Основные и динамические диски позволяют решать различные задачи конфигурирования дисков. С основными дисками можно выполнять следующие действия:

- форматировать разделы и помечать их, как активные;
- создавать и удалять первичные и расширенные разделы;
- создавать и удалять логические диски в расширенных разделах;
- преобразовать основной диск в динамический.

Динамические диски позволяют выполнять следующие действия:

- создавать и удалять простые, чередующиеся, составные, зеркальные тома и тома RAID-5;
- удалять зеркало из зеркального тома;
- расширять простые и составные тома;
- разбивать том на два тома;
- устранять неисправности зеркалированных томов и томов RAID-5;
- повторно активировать отсутствующий или отключенный диск;
- преобразовывать динамический диск в основной (требуется удаление томов и повторная загрузка);

С дисками любых типов можно выполнять следующие действия:

- просматривать свойства дисков, разделов и томов;
- назначать букву диска;
- настраивать безопасность и общий доступ к диску.

Особенности основных и динамических дисков

Работая с основными и динамическими дисками, следует помнить о пяти типах разделов:

- **Аварийный дамп памяти (crash dump)** Раздел, на который производится запись дампов памяти в случае зависания системы. По умолчанию файлы дампа записываются в папку %SystemRoot%, но могут располагаться в любом разделе или томе.
- **Активный (active)** Активный раздел или том, предназначенный для системного кеша и запуска системы. Активный раздел можно размещать на некоторых устройствах со съемными накопителями.
- **Загрузочный (boot)** Содержит ОС и поддерживающие ее файлы. Может совпадать с системным разделом или томом.
- **Системный (system)** Системный раздел или том содержит файлы, относящиеся к оборудованию, требующиеся для загрузки ОС. Системный раздел или том не может быть частью чередующихся или составных томов.
- **Файл подкачки (page file)** Раздел, содержащий файл подкачки. Благодаря возможности распределять страничную память по различным дис-

кам на компьютере может существовать несколько разделов или томов файла подкачки.

Примечание На компьютерах x86 можно пометить раздел как активный при помощи оснастки **Управление дисками (Disk Management)**. Щелкните правой кнопкой первичный раздел, который хотите сделать активным и выберите команду **Сделать раздел активным (Mark Partition As Active)**. Нельзя делать активными динамические тома. В процессе преобразования основного диска с активным разделом в динамический, раздел становится простым томом, который сам по себе автоматически активен.

Изменение типов дисков

Основные диски разработаны для использования в предыдущих версиях Windows. Динамические диски призваны использовать преимущества современных возможностей Windows. Использовать динамические диски можно на компьютерах под управлением Windows 2000 или более поздних версий. Тем не менее, вы вольны использовать динамические диски и в других ОС, например, UNIX. Для этого вам придется создать отдельный том для ОС, отличной от Windows. Динамические диски нельзя использовать на портативных компьютерах.

В арсенале Windows Server 2008 имеются инструменты для преобразования основного диска в динамический и обратно. В ходе преобразования основного диска в динамический разделы автоматически становятся томами соответствующего типа. Обратное преобразование томов в разделы невозможно. Вам придется удалить тома на динамическом диске и только потом сделать диск основным. При удалении томов уничтожается вся информация на диске.

Преобразование основного диска в динамический

Прежде чем заняться преобразованием основного диска в динамический, убедитесь, что на компьютере не загружается никакая другая версия Windows. Использовать динамические диски можно только на компьютерах под управлением Windows 2000 и более поздних версий.

Если вы используете MBR-диски, убедитесь, что в конце диска имеется 1 Мб свободного пространства. Оснастка **Управление дисками (Disk Management)** автоматически резервирует свободное пространство во время создания разделов и томов, но инструменты управления дисками из других ОС могут этого и не делать. При отсутствии свободного пространства в конце диска преобразование не состоится.

На дисках GPT должны иметься непрерывные распознаваемые разделы данных. Если GPT-диск содержит разделы, нераспознаваемые Windows, допустим, разделы, созданные другой ОС, вы не сможете преобразовать диск в динамический.

Для любых типов дисков справедливы следующие утверждения:

- Нельзя преобразовать диски с секторами, размер которых превышает 512 байт. Если размер секторов на диске слишком велик, вам придется переформатировать диск перед преобразованием.

- Нельзя создать динамические диски на портативных компьютерах или съемных носителях. Здесь можно использовать только основные диски с первичными разделами.
- Нельзя преобразовать диск, если системный или загрузочный раздел является частью составного, чередующегося, зеркального тома или тома RAID-5. Придется удалить набор и только потом выполнить преобразование.
- Не следует преобразовывать диск, если на нем установлено несколько версий ОС Windows. В противном случае, в дальнейшем вы сможете запускать компьютер только в Windows Server 2008.
- Вы можете преобразовать диски с разделами других типов, которые являются частью составных, чередующихся, зеркальных томов или томов RAID-5. Эти тома станут динамическими томами того же типа. Все диски набора необходимо преобразовывать одновременно.

Чтобы преобразовать основной диск в динамический, выполните следующие действия:

1. В оснастке **Управление дисками (Disk Management)** щелкните правой кнопкой основной диск, который хотите преобразовать, в представлении Список дисков (Disk List) или в левой панели Графического представления (Graphical View). Выберите команду **Преобразовать в динамический диск (Convert To Dynamic Disk)**.
2. В диалоговом окне **Преобразование в динамические диски (Convert To Dynamic Disk)** поставьте флажки напротив дисков, которые хотите преобразовать. Преобразуя составной, чередующийся, зеркальный том или том RAID-5, проверьте, что выбрали все диски в наборе. Щелкните **OK**.
3. В диалоговом окне **Диски для преобразования (Disks To Convert)** отображены преобразуемые диски. В этом диалоговом окне содержатся следующие столбцы и элементы управления:
   - **Имя (Name)** Номер диска.
   - **Оглавление диска (Disk Contents)** Тип и состояние разделов, например, загрузочный, активный или использующийся.
   - **Будет преобразован (Will Convert)** Указывает на возможность преобразования диска. Если диск не удовлетворяет требованиям, он не будет преобразован. Вам придется исправить ситуацию, как описано ранее.
   - **Сведения (Details)** Тома на выбранном диске.
   - **Преобразовать (Convert)** Запуск преобразования.
4. Чтобы начать преобразование, щелкните **Преобразовать (Convert)**. Вы получите предупреждение, что после завершения преобразования не сможете загрузить предыдущие версии Windows, находящиеся на выбранных дисках. Щелкните **Да (Yes)**, чтобы продолжить преобразование.
5. Если на выбранном диске содержится загрузочный раздел, системный раздел, или использующийся раздел, оснастка **Управление дисками (Disk Management)** перезагрузит компьютер.

Обратное преобразование динамического диска в основной

Перед обратным преобразованием динамического диска в основной с диска должны быть удалены все динамические тома. Затем щелкните правой кнопкой диск и выберите команду **Преобразовать в базовый диск (Convert To Basic Disk)**. Динамический диск будет преобразован в основной, на котором впоследствии можно будет создать новые разделы и логические диски.

Повторная активация динамических дисков

Если динамический диск находится в состоянии **Работает (ошибки) (Online (Errors))** или **Не подключен (Offline)**, зачастую устранить проблему можно повторной активацией диска, выполнив следующие действия:

1. В оснастке **Управление дисками (Disk Management)** щелкните правой кнопкой динамический диск, который хотите повторно активировать, выберите команду **Реактивизировать диск (Reactivate Disk)** и подтвердите выбранное действие.
2. Если состояние диска не изменится, перезагрузите компьютер. Если устранить проблему не удается, проверьте диск, контроллер диска и кабели. Кроме того, убедитесь, что к диску подведено питание и он правильно подключен.

Повторный поиск дисков

Повторный поиск обновляет информацию о конфигурации дисков компьютера и иногда помогает устранить проблемы, связанные с дисками, находящимися в состоянии **Не читается (Unreadable)**. Для повторного поиска дисков на компьютере выберите в меню **Действие (Action)** команду **Повторить проверку дисков (Rescan Disks)**.

Перемещение диска на другую систему

Серьезное преимущество динамических дисков перед основными состоит в том, что их можно без труда перемещать с одного компьютера на другой. Допустим, настроив компьютер, вы решили, что дополнительный жесткий диск на нем вам не нужен. Перенесите диск на другой компьютер, где от него будет больше пользы.

Система Windows Server 2008 значительно упрощает перемещение дисков на другую систему. Перед переносом выполните следующие действия:

1. Откройте оснастку **Управление дисками (Disk Management)** на том компьютере, где в данный момент установлен динамический диск. Проверьте состояние диска и убедитесь, что он исправен. В противном случае перед перемещением диска следует исправить разделы и тома на нем.

Примечание Этим способом нельзя перемещать диски, зашифрованные при помощи BitLocker. Функция шифрования BitLocker обнаруживает попытку автономного доступа, и диск блокируется до тех пор, пока администратор не разблокирует его.

2. Проверьте подсистемы жестких дисков на исходном и целевом компьютерах. Оба компьютера должны иметь идентичные подсистемы. В противном случае идентификатор Plug and Play диска исходного компьютера не совпадет с ожидаемым идентификатором на целевом компьютере. В результате целевой компьютер не сможет загрузить нужные драйверы, и загрузка может завершиться неудачей.
3. Проверьте, не является ли перемещаемый динамический диск частью составного, расширенного или чередующегося набора. Если это так, пометьте диски, входящие в состав набора, и запланируйте одновременный перенос всего набора дисков. Если вы перемещаете только часть набора дисков, помните о последствиях. При перемещении части составного, расширенного или чередующегося тома он станет непригоден для дальнейшего использования как на текущем компьютере, так и на компьютере, на который вы собираетесь переместить диски.

Подготовившись к перемещению дисков, выполните следующие действия:

1. На исходном компьютере откройте консоль **Управление компьютером (Computer Management)**. Выделите узел **Диспетчер устройств (Device Manager)**. В списке устройств разверните узел **Дисковые устройства (Disk Drives)**. В окне будет отображен список всех физических дисков компьютера. Щелкайте правой кнопкой все диски, которые хотите переместить, и выбирайте команду **Отключить (Uninstall)**. Если вы не точно знаете, какие диски нужно удалить, щелкните правой кнопкой каждый диск и выберите команду **Свойства (Properties)**. В диалоговом окне свойств перейдите на вкладку **Тома (Volumes)** и щелкните кнопку **Заполнить (Populate)**. На экране отобразятся тома выбранного диска.
2. Выделите узел **Управление дисками (Disk Management)** в консоли **Управление компьютером (Computer Management)** на исходном компьютере. Щелкайте правой кнопкой все диски, которые хотите переместить, и выбирайте команду **Удалить (Remove Disk)**.
3. Выполнив эту процедуру, переместите динамические диски. Если диски обладают функцией «горячей» замены, и эта функция поддерживается на обоих компьютерах, извлеките диски из исходного компьютера и установите их на целевом компьютере. В противном случае, выключите оба компьютера, извлеките все диски из исходного компьютера и установите их на целевом компьютере. Затем перезагрузите компьютеры.
4. Откройте оснастку **Управление дисками (Disk Management)** на целевом компьютере и выберите в меню **Действие (Action)** команду **Повторить проверку дисков (Rescan Disks)**. Когда просмотр дисков завершится, щелкайте правой кнопкой все диски с состоянием **Инородный (Foreign)** и выбирайте команду **Импортировать (Import)**. Теперь вы можете получить доступ к дискам и их томам на целевом компьютере.

Примечание В большинстве случаев динамические диски сохраняют буквы, назначенные им на исходном компьютере. Однако если данная буква диска уже используется на целевом компьютере, том получает ближайшую доступную букву. Если динамический том на исходном компьютере не имел буквы диска, при перемещении на другой компьютер буква ему также не будет присвоена. Кроме того, если отключена функция автоподключения, вам придется подключать тома и назначать им буквы вручную.

Основные диски и разделы

Во время установки нового или обновления старого компьютера часто требуется создание разделов на дисках компьютера. Создание разделов выполняется в оснастке **Управление дисками (Disk Management)**.

Создание основных разделов

В ОС Windows Server 2008 физический диск с MBR-разделами может иметь до четырех первичных разделов и один расширенный. Таким образом, существует два способа настройки MBR-дисков: создание от одного до четырех первичных разделов, или создание от одного до трех первичных и одного расширенного раздела. Первичный раздел может занимать весь диск или его часть. В расширенном разделе можно создать один или несколько логических дисков. Логический диск — это часть раздела со своей файловой системой. Вообще, логические диски используются для разбиения большого диска на части. Например, вы вольны разбить расширенный раздел объемом 600 Гб на три логических диска по 200 Гб каждый. На физических GPT-дисках может быть до 128 разделов.

После разбиения диска на разделы выполняется форматирование разделов и присвоение им букв. Предпочтительно использовать высокоуровневое форматирование, в ходе которого создается структура файловой системы. Вам, вероятно, очень хорошо знаком диск C, но это лишь указатель на раздел диска. Если вы разобьете диск на несколько разделов, каждый раздел получит свою букву диска. Буквы дисков используются для доступа к файловым системам различных разделов. В отличие от MS-DOS, которая автоматически присваивала буквы, начиная с C, Windows Server 2008 позволяет задавать буквы произвольно. Как правило, для использования доступны буквы от C до Z.

Примечание Буква A всегда назначена накопителю для гибких дисков. Если в системе есть второй накопитель для гибких дисков, ему назначается буква B, поэтому вам доступны только буквы от C до Z. Не забывайте, что для CD-дисководов, Zip-накопителей и других типов носителей также требуются буквы. Общее число букв, которые можно использовать одновременно, составляет 24. Если вам требуются дополнительные тома, их можно настроить при помощи путей.

Буквы позволяют иметь только 24 активных тома. Чтобы преодолеть этот барьер, подключайте диски к путям. При этом доступ к диску осуществляется как к папке на другом диске. В частности, вы можете подключить дополнительные диски, как E:\Data1, E:\Data2 и E:\Data3. Пути можно ис-

пользовать как с основными, так и с динамическими дисками. Единственное ограничение состоит в том, что диски можно подключать только к пустым папкам, расположенным на дисках с файловой системой NTFS.

Чтобы вам проще было различить первичные разделы и расширенные разделы с локальными дисками, в оснастке **Управление дисками (Disk Management)** они обозначены различными цветами. Например, первичные разделы маркируются темно-синей полосой, а логические диски на расширенных разделах — светло-синей полосой. Расшифровка цветовой схемы показана в нижней части окна **Управление дисками (Disk Management)**. Чтобы изменить схему, выберите в меню **Вид (View)** команду **Параметры (Settings)**.

Создание разделов и простых томов

В Windows Server 2008 пользовательский интерфейс оснастки **Управление дисками (Disk Management)** упрощен за счет использования одного набора диалоговых окон и мастеров как для разделов, так и для томов. Первые три тома основного диска автоматически создаются как первичные разделы. При попытке создать на основном диске четвертый том, оставшееся свободное пространство автоматически преобразуется в расширенный раздел с логическим диском.

В оснастке **Управление дисками (Disk Management)** разделы, локальные диски и простые тома создаются следующим образом:

1. В графическом представлении оснастки **Управление дисками (Disk Management)** щелкните правой кнопкой неразмеченную или свободную область и выберите команду **Создать простой том (New Simple Volume)**. Откроется Мастер создания простых томов (New Simple Volume Wizard). Прочитайте приветственную страницу и щелкните **Далее (Next)**.
2. На странице **Указание размера тома (Specify Volume Size)**, показанной на рис. 12-3, указаны допустимые наибольший и наименьший размеры тома в мегабайтах (Мб). Задайте размер тома и щелкните **Далее (Next)**.

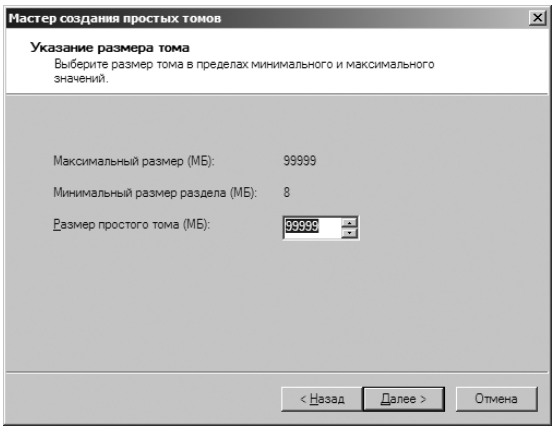


Рис. 12-3. Определение размера тома на странице Указание размера тома (Specify Volume Size)

3. На странице **Назначение буквы диска или пути (Assign Drive Letter Or Path)**, показанной на рис. 12-4, укажите букву или путь к диску и щелкните **Далее (Next)**. В вашем распоряжении следующие возможности:
   - **Назначить букву диска (Assign The Following Drive Letter)** Установите этот переключатель и выберите доступную букву диска в списке. По умолчанию Windows Server 2008 выбирает букву диска с наименьшим значением, исключая зарезервированные буквы и буквы, уже назначенные сетевым дискам.
   - **Подключить том как пустую NTFS-папку (Mount In The Following Empty NTFS Folder)** Установите этот переключатель для подключения раздела к пустой NTFS-папке. Вы должны ввести путь к папке или найти ее, щелкнув кнопку **Обзор (Browse)**.
   - **Не назначать буквы диска или пути диска (Do Not Assign A Drive Letter Or Drive Path)** Установите этот переключатель, чтобы создать раздел, не присваивая ему буквы диска или пути. Вы сможете назначить букву или путь позднее.

Примечание Вы не обязаны назначать томам букву или путь. При этом том считается неподключенным и, фактически, неиспользуемым. Назначить тому букву или путь можно позже. Подробнее — в разделе «Назначение букв и путей к дискам» этой главы.

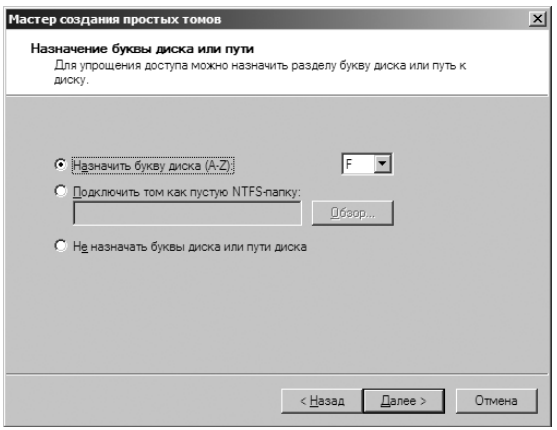


Рис. 12-4. На странице Назначение буквы диска или пути (Assign Drive Letter Or Path) назначьте букву или путь к диску

4. На странице **Форматирование раздела (Format Partition)**, которая показана на рис. 12-5, укажите, следует ли форматировать том и каким способом. Если вы хотите форматировать том, установите переключатель **Форматировать этот том следующим образом (Format This Volume With The Following Settings)** и задайте следующие параметры:
   - **Файловая система (File System)** Тип файловой системы: FAT, FAT32 или NTFS. В большинстве случаев по умолчанию выбрана файловая система NTFS. Создав файловую систему FAT или FAT32, позже вы сможете преобразовать ее в NTFS. Преобразовать NTFS в FAT или FAT32 нельзя.

- **Размер кластера (Allocation Unit Size)** Размер кластера — базовой единицы распределения дискового пространства. Стандартный размер кластера зависит от размера тома и по умолчанию задается динамически перед форматированием. Вы вольны выбрать собственный размер кластера. Если вы используете много небольших файлов, вам стоит работать с кластерами небольшого размера, например, 512 или 1024 байт. Такие параметры позволяют сэкономить дисковое пространство при работе с небольшими файлами.
- **Метка тома (Volume Label)** Текстовая метка раздела, по умолчанию имеющая значение Новый том (New Volume). Чтобы изменить метку тома, щелкните том правой кнопкой в Проводнике Windows (Windows Explorer), выберите **Свойства (Properties)** и введите новое значение в текстовое поле на вкладке **Общие (General)**.
- **Быстрое форматирование (Perform A Quick Format)** Система Windows Server 2008 выполнит быстрое форматирование, не проверяя том на наличие ошибок. При форматировании больших разделов эта функция сэкономит вам несколько минут, но лучше не отказываться от проверки. В ее ходе оснастка **Управление дисками (Disk Management)** отмечает на диске секторы с ошибками и блокирует их.
- **Применять сжатие файлов и папок (Enable File And Folder Compression)** Включает функцию сжатия данных на диске. Встроенная возможность сжатия данных доступна только для NTFS-томов. В NTFS сжатие происходит незаметно для пользователей, и они осуществляют доступ к сжатым файлам точно так же, как и к обычным. Если вы установите этот флажок, файлы и папки на диске будут автоматически сжиматься. Подробнее о сжатии дисков, файлов и папок — в разделе «Сжатие дисков и данных» этой главы.

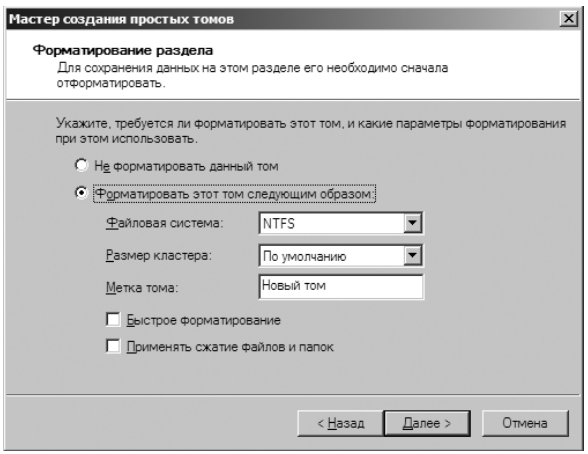


Рис. 12-5. Задание параметров форматирования на странице Форматирование раздела (Format Partition)

5. Щелкните **Далее (Next)**, проверьте заданные параметры и щелкните **Готово (Finish)**.

Форматирование разделов

Форматирование создает в разделе файловую систему и навсегда удаляет все существующие данные. Предпочтительнее проводить высокоуровневое форматирование, при котором только создается структура файловой системы, а не низкоуровневое форматирование, которое инициализирует диск. Чтобы форматировать раздел, щелкните его правой кнопкой и выберите команду **Форматировать (Format)**. Откроется диалоговое окно **Форматирование (Format)**, показанное на рис. 12-6.

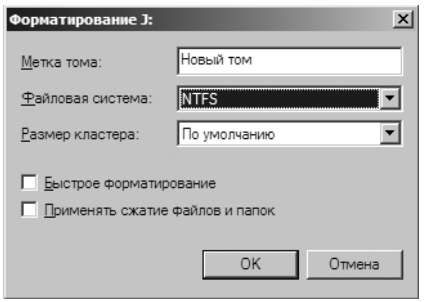


Рис. 12-6. Задайте параметры форматирования раздела в диалоговом окне Форматирование (Format)

Задайте следующие параметры форматирования:

- **Метка тома (Volume Label)** Текстовая метка раздела, имя тома.
- **Файловая система (File System)** Тип файловой системы: exFAT, FAT, FAT32 или NTFS. Файловая система FAT поддерживается MS-DOS, а также Microsoft Windows 3.1, Windows 95, Windows 98 и Windows Me. Файловая система NTFS — оригинальная файловая система Microsoft Windows NT и более поздних выпусков Windows.
- **Размер кластера (Allocation Unit Size)** Размер кластера — базовой единицы распределения дискового пространства. Стандартный размер кластера зависит от размера тома и по умолчанию задается динамически перед форматированием. Вы вольны выбрать собственный размер кластера. Если вы используете много небольших файлов, вам стоит работать с кластерами небольшого размера, например, 512 или 1024 байт. Такие параметры позволяют сэкономить дисковое пространство при работе с небольшими файлами.
- **Быстрое форматировани (Perform A Quick Format)** Система Windows Server 2008 выполнит быстрое форматирование, не проверяя том на наличие ошибок. При форматировании больших разделов эта функция сэкономит вам несколько минут, но лучше не отказываться от проверки. В ее ходе оснастка **Управление дисками (Disk Management)** отмечает на диске секторы с ошибками и блокирует их.

- **Применять сжатие файлов и папок (Enable File And Folder Compression)** Включает функцию сжатия данных на диске. Встроенная возможность сжатия данных доступна только для NTFS-томов. В NTFS сжатие происходит незаметно для пользователей, и они осуществляют доступ к сжатым файлам точно так же, как и к обычным. Если вы установите этот флажок, файлы и папки на диске будут автоматически сжиматься. Подробнее о сжатии дисков, файлов и папок — в разделе «Сжатие дисков и данных» этой главы.

Щелкните **OK**. Форматирование раздела уничтожит все существующие данные, поэтому оснастка **Управление дисками (Disk Management)** предоставит вам последний шанс отменить процедуру. Щелкните **OK**, чтобы начать форматирование раздела. О завершении форматирования вы узнаете по изменившемуся состоянию диска.

Управление существующими разделами и дисками

Оснастка **Управление дисками (Disk Management)** предоставляет несколько возможностей по управлению существующими разделами и дисками. Вы можете назначать буквы дисков, удалять разделы, устанавливать активные разделы и делать многое другое. Кроме того, Windows Server 2008 оснащена другими утилитами для выполнения типичных задач, например, для преобразование NTFS-томов, проверки диска на наличие ошибок и освобождения неиспользуемого дискового пространства.

Примечание Система Windows Server 2008, как и Windows Vista, поддерживает устройства с возможностью «горячего» подключения, работающие с NTFS-томами. Эта новая возможность позволяет форматировать флеш-накопители USB и другие подобные носители в файловой системе NTFS. Система Windows Vista SP1 обладает усовершенствованиями, позволяющими избежать потери данных при извлечении съемных носителей, форматированных в NTFS.

Назначение букв и путей к дискам

Вы можете назначить диску одну букву, а также один или несколько путей, при условии что пути к дискам находятся на NTFS-дисках. Вы не обязаны назначать диску букву или путь. В отсутствие указателя том считается неподключенным. Вы можете подключить его, назначив ему букву или путь. Прежде чем перемещать диск на другой компьютер, его следует отключить.

Система Windows не позволяет изменять букву системного тома, загрузочного тома и тома, на котором расположен файл подкачки. Чтобы изменить букву системного или загрузочного тома, потребуется редактировать реестр. Эта процедура описана в статье 223188 базы знаний Майкрософт, в (*http://support.microsoft.com/kb/223188/en-us*). Прежде чем изменить букву тома, использующегося файлом подкачки, вам придется переместить файл подкачки на другой том.

Чтобы управлять буквами и путями к дискам, в оснастке **Управление дисками (Disk Management)** щелкните правой кнопкой диск, который хотите настроить, и выберите команду **Изменить букву диска или путь к диску (Change Drive Letter And Paths)**. Откроется диалоговое окно, показанное на рис. 12-7. Здесь вы можете выполнить следующие действия:

- **Добавить путь к диску** Щелкните кнопку **Добавить (Add)**, установите переключатель **Установить том как пустую NTFS-папку (Mount In The Following Empty NTFS Folder)**, а затем введите путь к существующей папке или щелкните **Обзор (Browse)**, чтобы найти или создать папку.
- **Удалить путь к диску** Выберите удаляемый путь к диску и щелкните **Удалить (Remove)**, а затем щелкните **Да (Yes)**.
- **Назначить букву диска** Щелкните кнопку **Добавить (Add)**, установите переключатель **Назначить букву диска (Assign The Following Drive Letter)** и выберите доступную букву.
- **Изменить букву диска** Выделите текущую букву диска и щелкните **Изменить (Change)**. Установите переключатель **Назначить букву диска (Assign The Following Drive Letter)** и выберите доступную букву.
- **Удалить букву диска** Выберите текущую букву диска и щелкните **Удалить (Remove)**, а затем щелкните **Да (Yes)**.

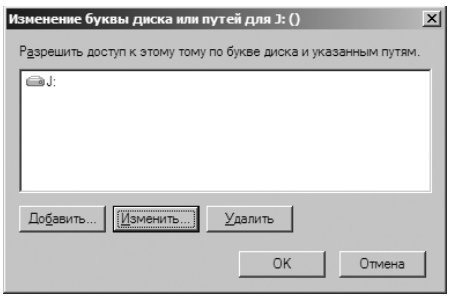


Рис. 12-7. Диалоговое окно Изменение буквы диска или путей (Change Drive Letter And Paths) позволяет изменить букву и путь к диску

Примечание При попытке изменить букву использующегося диска Windows Server 2008 выдаст предупреждение. Закройте программы, использующие диск, и повторите попытку или разрешите оснастке **Управление дисками (Disk Management)** принудительно применить изменение, щелкнув **Да (Yes)**.

Изменение или удаление метки тома

Метка тома — это текстовый идентификатор диска. В файловых системах FAT и FAT32 метка тома может содержать до 11 символов и включать пробелы. В файловой системе NTFS метка тома может содержать до 32 символов. Кроме того, FAT и FAT32 не допускают использование некоторых специальных символов, например, * / \ [ ] : ; | = , . + “ ? < >. В свою очередь, NTFS допускает использование этих символов.

Метка тома отображается при обращении к диску различных программ Windows Server 2008, например, Проводника Windows (Windows Explorer), поэтому в ней удобно размещать информацию о содержимом диска. Изменить или удалить метку тома можно при помощи оснастки **Управление дисками (Disk Management)** или Проводника Windows (Windows Explorer).

Чтобы изменить или удалить метку в оснастке **Управление дисками (Disk Management)**, выполните следующие действия:

1. Щелкните раздел правой кнопкой и выберите команду **Свойства (Properties)**.
2. На вкладке **Общие (General)** диалогового окна **Свойства (Properties)** введите новую метку тома в текстовое поле или удалите существующую метку. Щелкните **OK**.

Чтобы изменить или удалить метку в Проводнике Windows (Windows Explorer), выполните следующие действия:

1. Щелкните правой кнопкой значок диска и выберите команду **Свойства (Properties)**.
2. На вкладке **Общие (General)** диалогового окна **Свойства (Properties)** введите новую метку тома в текстовое поле или удалите существующую метку. Щелкните **OK**.

Удаление разделов и дисков

Чтобы изменить конфигурацию существующего полностью распределенного диска, требуется удалить существующие разделы и локальные диски. Удаление раздела или диска влечет за собой удаление связанной с ним файловой системы, что приведет к полной потере данных, содержащихся в файловой системе. Поэтому перед удалением раздела или диска следует создать резервные копии всех файлов и папок, содержащихся на нем.

Примечание В целях защиты целостности системы не допускается удаление системного или загрузочного раздела. Однако Windows Server 2008 разрешит удалить активный раздел, если он не является системным или загрузочным. Всегда проверяйте удаляемый раздел или том на наличие важных данных или файлов.

Чтобы удалить первичный раздел, том или логический диск, выполните следующие действия:

1. В оснастке **Управление дисками (Disk Management)** щелкните правой кнопкой раздел, том или логический диск, который хотите удалить, и выберите команду **Проводник (Explore)**. В Проводнике Windows (Windows Explorer) переместите все данные на другой том или проверьте наличие резервных копий данных.
2. В оснастке **Управление дисками (Disk Management)** снова щелкните раздел, том или диск правой кнопкой и выберите нужную команду: **Удалить раздел (Delete Partition)**, **Удалить том (Delete Volume)** или **Удалить логический диск (Delete Logical Drive)**.

3. Подтвердите удаление выбранного объекта, щелкнув **Да (Yes)**.

Удаление расширенного раздела немного отличается от удаления первичного раздела или логического диска. Чтобы удалить расширенный раздел, выполните следующие действия:

1. Удалите все логические диски в разделе, выполнив шаги из предыдущей процедуры.
2. Выберите сам расширенный раздел и удалите его.

Преобразование файловой системы тома в NTFS

В ОС Windows Server 2008 включена программа для преобразования FAT-томов в NTFS. Она называется Convert и находится в папке %SystemRoot%. При использовании этого инструмента для преобразования тома структура файлов и папок сохраняется, и данные остаются без изменения. Тем не менее, следует учесть, что в Windows Server 2008 отсутствуют утилиты для преобразования NTFS в FAT. Единственный способ преобразовать NTFS в FAT — удалить раздел и воссоздать его как том в формате FAT.

Синтаксис программы Convert

Программа Convert запускается из командной строки. Если вы хотите преобразовать диск, используйте следующий синтаксис:

```
convert том /FS:NTFS
```

где *том* — буква диска с двоеточием, путь к диску или имя тома. Допустим, вам нужно преобразовать в NTFS диск D. Используйте следующую команду:

```
convert D: /FS:NTFS
```

Ниже приводится полный синтаксис утилиты Convert:

```
convert том /FS:NTFS [/V] [/X] [/CvtArea:имя_файла] [/NoSecurity]
```

Эти параметры описаны в таблице:

том	Том, с которым следует работать
/FS:NTFS	Преобразование в NTFS
/V	Режим вывода подробного отчета о работе
/X	При необходимости задает принудительное отключение тома
/CvtArea: *имя_файла*	Определяет имя непрерывного файла в корневой папке для резервирования места под системные файлы NTFS
/NoSecurity	Удаляет все атрибуты безопасности и делает файлы и папки доступными для группы Все (Everyone)

Применение программы Convert

Перед использованием программы Convert выясните, используется ли раздел в качестве активного загрузочного или системного раздела, содержащего файлы ОС. Системы на базе Intel *x*86 позволяют выполнить преобразование

активного загрузочного раздела в формат NTFS. В этом случае системе требуется исключительный доступ к разделу. Это можно осуществить только во время запуска. Если вы пытаетесь преобразовать активный загрузочный раздел в формат NTFS, система предложит вам запланировать преобразование диска на следующую загрузку системы. Щелкнув **Да (Yes)**, вы сможете перезагрузить систему и начать процесс преобразования.

Совет Часто для полного завершения преобразования активного загрузочного раздела требуется несколько раз перезагружать систему. Не паникуйте! Дайте системе закончить преобразование.

Перед началом преобразования диска в NTFS утилита Convert проверяет наличие на диске свободного места, достаточного для преобразования. Вообще, для преобразования требуется примерно 25% общего объема используемого пространства. Например, если на диске можно хранить 200 Гб данных, для работы Convert потребуется около 50 Гб. Если свободного места недостаточно, Convert отменяет операцию и сообщает о том, что необходимо освободить место на диске. Если на диске достаточно свободного места, Convert приступает к преобразованию. Наберитесь терпения. Процесс преобразования займет несколько минут (в зависимости от объема диска). Не обращайтесь к расположенным на диске файлам или программам в ходе преобразования.

Чтобы увеличить производительность тома, включите параметр /CvtArea, позволяющий зарезервировать место для главной файловой таблицы (master file table, MFT) и тем самым предотвратить фрагментацию MFT. Как? Со временем размер MFT может увеличиться и выйти за рамки отведенного для нее места. Из-за этого ОС придется расширять MFT на другие области диска. Утилита дефрагментации диска способна дефрагментировать MFT, однако она не может переместить первую секцию MFT.

В некоторых случаях, чтобы избежать фрагментации, нужно резервировать под MFT больше места (чем стандартные 12,5% от размера тома). В частности, увеличение размера MFT может потребоваться, если том содержит большое количество небольших файлов, а не несколько больших файлов. Для определения величины резервируемого пространства используйте программу FSUtil. С ее помощью создается файл-заполнитель, который по размеру равен создаваемой MFT. Затем преобразуйте том в NTFS, указав имя файла-заполнителя в параметре /CvtArea.

В следующем примере FSUtil используется для создания файла-заполнителя Temp.txt размером 1,5 Гб:

```
fsutil file createnew c:\temp.txt 1500000000
```

Чтобы использовать файл-заполнитель для MFT во время преобразования диска C в формат NTFS, введите следующую команду:

```
convert c: /fs:ntfs /cvtarea:temp.txt
```

Обратите внимание, что файл-заполнитель создается в преобразуемом разделе или томе. В процессе преобразования файл будет перезаписан метаданными NTFS, и все неиспользуемое место в файле будет зарезервировано для будущей таблицы MFT.

Изменение размера разделов и томов

Для загрузки Windows Server 2008 не используются файлы Ntldr и Boot.ini. Вместо них Windows Server 2008 применяет предзагрузочную среду, в которой запуском и загрузкой выбранного загрузочного приложения руководит диспетчер загрузки Windows (Windows Boot Manager). Диспетчер загрузки освобождает ОС семейства Windows от наследия MS-DOS, что дает возможность взглянуть на работу с дисками под другим углом. Система Windows Server 2008 позволяет расширять и сжимать как основные, так и динамические диски. Для расширения и сжатия томов можно использовать оснастку **Управление дисками (Disk Management)** или программу DiskPart. Нельзя сжимать чередующиеся диски.

В процессе расширения тома происходит преобразование неразмеченных областей с их последующим добавлением к существующему тому. Пространство для составных томов на динамических дисках может быть взято с любого доступного динамического диска, не только из дисков, на которых был изначально создан том. Таким образом, вы можете объединить свободные области на нескольких динамических дисках и использовать их для увеличения размера существующего тома.

Внимание! Приступая к расширению тома, помните о некоторых ограничениях. Вы можете расширять простые и составные тома только в том случае, если они отформатированы в файловой системе NTFS. Чередующиеся тома расширять нельзя. Невозможно расширять неформатированные тома или тома, форматированные в FAT или FAT32. Кроме того, независимо от конфигурации нельзя расширить системный или загрузочный том.

Чтобы сжать простой или составной том, выполните следующие действия:

1. В оснастке Управление дисками (Disk Management) щелкните правой кнопкой том, который хотите сжать, и выберите команду **Сжать том (Shrink Volume)**. Это команда доступна, если том удовлетворяет перечисленным выше условиям.
2. В диалоговом окне **Сжать (Shrink)**, показанном на рис. 12-8, введите объем сжимаемого пространства. Здесь отображена следующая информация:
   - **Общий размер до сжатия (МБ) (Total Size Before Shrink In MB)** Суммарный объем тома в мегабайтах. Это — форматированный размер тома.
   - **Доступное для сжатия пространство (МБ) (Size Of Available Shrink Space In MB)** Наибольший объем, на который можно сжать том.

Эта величина характеризует не общее свободное пространство тома, а, скорее, представляет объем, который можно удалить. Этот объем не включает данные, зарезервированные для главной файловой таблицы, снимки тома, файлы подкачки и временные файлы.

- **Размер сжимаемого пространства (МБ) (Amount of Space To Shrink In MB)** Суммарный объем освобождаемого пространства тома. Значение по умолчанию равно максимальному объему, который можно удалить из тома. Для оптимальной производительности диска следует проследить, чтобы после сжатия на диске осталось, по крайней мере, 10% свободного места.
- **Общий размер после сжатия (МБ) (Total Size After Shrink In MB)** Суммарный объем тома в мегабайтах после сжатия. Это новый форматированный размер тома.

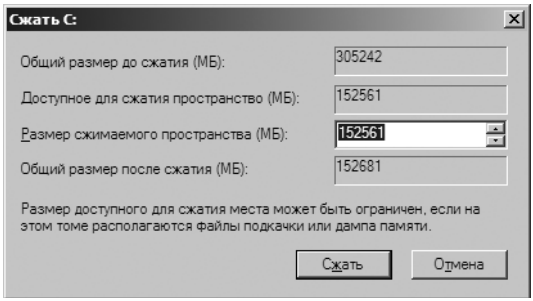


Рис. 12-8. Укажите величину сжимаемого пространства

3. Щелкните кнопку **Сжать (Shrink)**, чтобы выполнить сжатие.

Для расширения простого или составного тома выполните следующие действия:

1. В оснастке **Управление дисками (Disk Management)** щелкните правой кнопкой расширяемый том и выберите команду **Расширить том (Extend Volume)**. Это команда доступна только в том случае, если том удовлетворяет ранее описанным условиям и если на одном или более дисках системы имеется свободное место.
2. В окне Мастера расширения тома (Extend Volume Wizard) прочитайте вводную информацию и щелкните **Далее (Next)**.
3. На странице **Выбор дисков (Select Disks)** выберите диск или диски, свободное пространство которых хотите распределить. Все использующиеся томом диски будут выбраны автоматически. По умолчанию для расширения будет выбрано все имеющееся на этих дисках свободное пространство.
4. В случае динамических дисков вы можете указать дополнительное пространство на других дисках, которое следует использовать. Выполните следующие действия:
   - Щелкните диск, затем щелкните **Добавить (Add)**, чтобы добавить диск в список **Выбраны (Selected)**.

- Последовательно выбирайте все диски в списке **Выбраны (Selected)** и в поле **Выберите размер выделяемого пространства (МБ) (Select The Amount Of Space In MB)** указывайте размер неразмеченного пространства, которое следует использовать на выбранном диске.

5. Щелкните **Далее (Next)**, проверьте выбранные параметры и щелкните кнопку **Готово (Finish)**.

Исправление ошибок на диске

Функциональные расширения Windows Server 2008 позволяют сократить объем ручного труда при обслуживании дисковых накопителей. Наибольшее влияние на работу с дисками оказывают следующие расширения:

- Transactional NTFS;
- Self-Healing NTFS.

Расширение Transactional NTFS позволяет проводить операции с файлами на томах NTFS в режиме транзакций. Это означает, что программы могут группировать наборы файловых и реестровых операций в транзакцию. Пока транзакция активна, изменения за пределами транзакции не видны. Изменения фиксируются и полностью записываются на диск только после успешного завершения транзакции. Если транзакция завершается неудачно или выполняется не полностью, программа производит откат транзакции, восстанавливая файловую систему до состояния, предшествующего транзакции.

Транзакции, объединяющие несколько томов, координируются диспетчером транзакций ядра (Kernel Transaction Manager, KTM). Диспетчер транзакций поддерживает независимое восстановление томов в случае сбоя транзакции. Локальный менеджер ресурсов тома ведет отдельный журнал регистрации транзакций. Он отвечает за отделение потоков транзакций от потоков, выполняющих работу с файлами.

Традиционно для исправления ошибок и сбоев на NTFS-томах используется инструмент Check Disk. Однако его применение может нарушить доступность системы Windows, и потому в Windows Server 2008 используется Self-Healing NTFS, которая защищает файловую систему без привлечения специальных инструментальных средств для устранения неисправностей. Значительная часть процесса самовосстановления активизируется и выполняется автоматически, поэтому ваше участие в обслуживании тома требуется только в случаях, когда ОС не может устранить проблему автоматически. При возникновении подобной ошибки Windows Server 2008 уведомит вас о проблеме и предложит возможные пути решений.

Самовосстанавливающаяся NTFS (Self-Healing NTFS) обладает многими преимуществами перед программой Check Disk, включая следующие:

- Программа Check Disk должна иметь исключительный доступ к томам. Это означает, что системные и загрузочные тома можно проверять только во время запуска системы. С другой стороны, при работе Self-Healing

NTFS файловая система всегда доступна и в большинстве случаев не требует отключения для исправления ошибок.

- В случае повреждения данных Self-Healing NTFS старается сохранить как можно больше информации, а также сокращает возможности подключения сбойной файловой системы, что могло происходить раньше. Во время перезагрузки Self-Healing NTFS немедленно исправляет том, так что его можно сразу же подключать.
- Программа Self-Healing NTFS сообщает об изменениях, внесенных в том во время исправления, с помощью существующих механизмов Chkdsk.exe, уведомлений каталога, а также последовательных номеров обновлений (USN). Она также позволяет прошедшим проверку пользователям и администраторам отслеживать операции исправления ошибок при помощи сообщений Verification, Waiting For Repair Completion и Progress Status.
- Программа Self-Healing NTFS способна восстановить том, если загрузочный сектор читается, но не идентифицирует NTFS-том. В этом случае вы должны запустить автономную утилиту для исправления загрузочного сектора, а затем позволить Self-Healing NTFS начать восстановление.

Несмотря на всю мощь расширения Self-Healing NTFS, иногда приходится проверять целостность диска вручную. В этом случае воспользуйтесь программой Check Disk (Chkdsk.exe) для проверки и исправления ошибок, найденных в томах FAT, FAT32 и NTFS. Программа Check Disk способна находить и исправлять множество типов ошибок, но, главным образом, она проводит поиск непоследовательностей в файловой системе и связанных с ней метаданных. Один из способов обнаружения ошибок программой Check Disk — сравнение битовой карты тома с дисковыми секторами, назначенными файлам в файловой системе. В остальном функциональность Check Disk весьма ограничена. В частности, она не способна исправлять поврежденные данные, находящиеся внутри файлов, которые кажутся неповрежденными.

Запуск Check Disk из командной строки

Запускать программу Check Disk можно как из командной строки, так и из других утилит. Запустив следующую команду, вы проверите целостность диска E:

```
chkdsk E:
```

Для поиска и исправления ошибок на диске E используйте следующую команду:

```
chkdsk /f E:
```

Примечание Программа Check Disk не способна исправить том, используемый в данный момент. Если том используется, программа Check Disk предложит вам запланировать проверку тома при следующем перезапуске системы. Щелкните **Да (Yes)**, чтобы запланировать проверку.

Далее приведен полный синтаксис команды Check Disk:

```
chkdsk [том[[путь]имя_файла]]] [/F] [/V] [/R] [/X] [/I] [/C] [/L[:размер]]
```

Далее описаны параметры утилиты Check Disk:

том	Том, с которым следует работать
имя_файла	Только FAT/FAT32: файлы для проверки на фрагментацию
/F	Исправлять ошибки на диске
/V	FAT/FAT32: отображение полного пути и имени каждого файла на диске. NTFS: Выводит сообщения об очистке (если таковые имеются)
/R	Определять расположение поврежденных секторов и восстанавливать уцелевшую информацию (используется одновременно с /F)
/L:*размер*	Только NTFS: изменяет размер файла журнала
/X	При необходимости принудительно отключать том (используется одновременно /F).
/I	Только NTFS: выполнять минимальную проверку элементов индекса
/C	Только NTFS: пропускать проверку циклов внутри структуры папки

Интерактивный запуск Check Disk

Программу Check Disk можно запускать при помощи интерфейса Проводника Windows (Windows Explorer) или оснастки **Управление дисками (Disk Management)**. Выполните следующие действия:

1. Щелкните правой кнопкой диск и выберите команду **Свойства (Properties)**.
2. В диалоговом окне **Свойства (Properties)** на вкладке **Сервис (Tools)** щелкните кнопку **Выполнить проверку (Check Now)**.

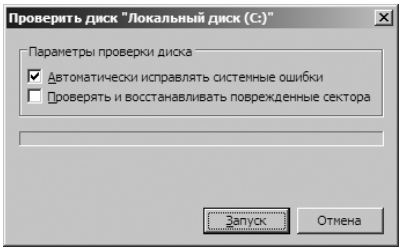


Рис. 12-9. Поиск и исправление ошибок на диске при помощи Check Disk

3. Как показано на рис. 12-9, вы можете выполнить следующие действия:
   - **Поиск ошибок без исправления** Щелкните **Запуск (Start)**, не устанавливая ни один из флажков.
   - **Поиск и исправление ошибок** Установите соответствующие флажки для исправления ошибок файловой системы или восстановления поврежденных секторов. Затем щелкните **Запуск (Start)**.

Дефрагментация дисков

Каждый раз при добавлении и удалении файлов с диска может возникнуть фрагментация имеющихся на диске данных. Фрагментация препятствует записи больших файлов в одну последовательную область. В результате ОС вынуждена распределять файл по нескольким небольшим областям диска, что увеличивает время, требующееся на чтение файла с диска. Windows Server 2008 позволяет вручную или автоматически через заданный период выполнять дефрагментацию дисков с помощью программы Дефрагментация диска (Disk Defragmenter). Чем чаще обновляются данные на дисках, тем чаще следует запускать этот инструмент.

Чтобы вручную дефрагментировать диск, выполните следующие действия:

1. В консоли **Диспетчер сервера (Server Manager)** разверните узел **Хранилище (Storage)** и щелкните узел **Управление дисками (Disc Management)**. Щелкните диск правой кнопкой и выберите команду **Свойства (Properties)**.
2. На вкладке **Сервис (Tools)** щелкните кнопку **Выполнить дефрагментацию (Defragment Now)**. Программа Дефрагментация диска (Disk Defragmenter) проанализирует диски сервера, чтобы определить, следует ли проводить дефрагментацию. Если требуется произвести дефрагментацию, рекомендуется сделать это немедленно.
3. В диалоговом окне **Дефрагментация диска (Disk Defragmenter)** щелкните **Выполнить дефрагментацию (Defragment Now)**. Затем укажите дефрагментируемые диски и щелкните **OK**.

Примечание В зависимости от размера диска дефрагментация может занять несколько часов. Для остановки дефрагментации щелкните кнопку **Отменить дефрагментацию (Cancel Defragmentation)**.

Если включить автоматическую дефрагментацию, Windows Server 2008 будет автоматически запускать дефрагментацию дисков каждую среду в 01.00. Автоматическая дефрагментация будет выполняться, пока на компьютере установлено время автоматического выполнения. Следующие шаги помогут вам настроить и управлять автоматической дефрагментацией:

1. В консоли **Диспетчер сервера (Server Manager)** разверните узел **Хранилище (Storage)** и щелкните узел **Управление дисками (Disc Management)**. Щелкните диск правой кнопкой и выберите команду **Свойства (Properties)**.
2. На вкладке **Сервис (Tools)** щелкните кнопку **Выполнить дефрагментацию (Defragment Now)**. Откроется диалоговое окно **Дефрагментация диска (Disk Defragmenter)**, показанное на рис. 12-10.

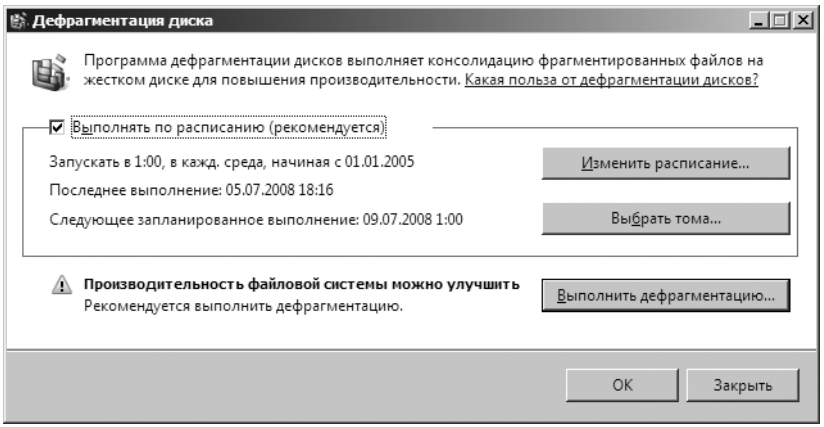


Рис. 12-10. Программа Дефрагментация диска (Disk Defragmenter) проводит анализ и дефрагментацию дисков

3. Для отмены автоматической дефрагментации сбросьте флажок **Выполнять по расписанию (Run On A Schedule)** и два раза щелкните **OK**. Пропустите оставшиеся шаги.
4. Чтобы включить автоматическую дефрагментацию, установите флажок **Выполнять по расписанию (Run On A Schedule)**. При этом в окне отображается стандартное или последнее настроенное расписание.
5. Если вы хотите изменить расписание, щелкните кнопку **Изменить расписание (Modify Schedule)**. В диалоговом окне **Изменение расписания (Modify Schedule)**, показанном на рис. 12-11, настройте желаемое расписание и щелкните **OK**. В списке **Как часто (How Often)** выберите периодичность **Ежедневно (Daily)**, **Еженедельно (Weekly)** или **Ежемесячно (Monthly)**. При настройке еженедельной или ежемесячной дефрагментации необходимо выбрать в списке **В какие дни (What Day)** день недели или месяца, в который она будет производиться. Наконец, в списке **В какое время (What Time)** задайте время суток, в которое должна проводиться дефрагментация.

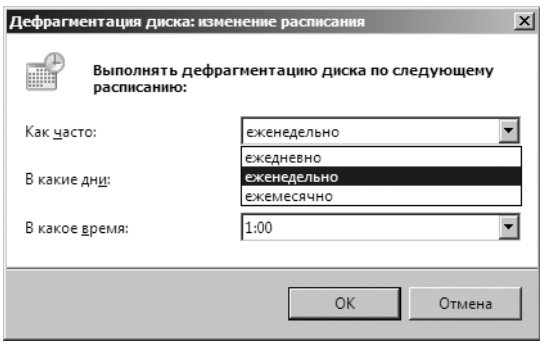


Рис. 12-11. Настройте расписание запуска автоматической дефрагментации

6. Если вы хотите определить диски, дефрагментацию которых следует проводить, щелкните кнопку **Выбрать тома (Select Volumes)**. В диалоговом окне **Дополнительные параметры (Advanced Options)** укажите дефрагментируемые тома. По умолчанию дефрагментируются все установленные на компьютере или подключенные к нему диски. Все новые диски будут также автоматически дефрагментированы. В списке **Диски для дефрагментации (Disks To Defragment)** установите флажки для дисков, дефрагментацию которых следует выполнять автоматически, и сбросьте флажки дисков, которые не следует дефрагментировать автоматически. Щелкните **OK**.
2. Два раза щелкните **OK**, чтобы сохранить параметры.

Примечание Системы Windows Vista SP1 и более поздние версии, а также Windows Server 2008 автоматически выполняют дефрагментацию с продолжением. При остановке и повторном запуске дефрагментации по расписанию автоматически выбирается ближайший том с неоконченной дефрагментацией, стоящий в очереди.

Сжатие дисков и данных

Во время форматирования диска в формате NTFS Windows Server 2008 позволяет включить встроенную функцию сжатия. При этом все хранящиеся на диске файлы автоматически сжимаются при их создании. Сжатие происходит незаметно для пользователей, и доступ к сжатым файлам происходит точно так же, как и к обычным. Различие заключается в том, что диск со сжатием позволяет хранить больше информации, чем обычный несжатый диск.

Ближе к реальности Безусловно, сжатие очень полезно для экономии дискового пространства, однако шифрование сжатых данных невозможно. Сжатие и шифрование — две взаимоисключающие функции. Вы можете применить либо только сжатие, либо только шифрование. Нельзя использовать обе технологии одновременно. Дополнительную информацию о шифровании вы найдете в разделе «Шифрование дисков и данных» этой главы. Если вы попытаетесь сжать шифрованные данные, Windows Server 2008 автоматически отменит шифрование, а затем сожмет данные. Подобным же образом, при попытке зашифровать сжатые данные Windows Server 2008 восстановит данные и применит к ним шифрование.

Сжатие дисков

Чтобы сжать диск и все его содержимое, выполните следующие действия:

1. В окне Проводника Windows (Windows Explorer) или оснастки **Управление дисками (Disk Management)** щелкните правой кнопкой диск, который хотите сжать, и выберите команду **Свойства (Properties)**.
2. Установите флажок **Сжать этот диск для экономии места (Compress Drive To Save Disk Space)** и щелкните **OK**.

Сжатие папок и файлов

Если вы не хотите сжимать весь диск, Windows Server 2008 позволяет производить выборочное сжатие папок и файлов. Чтобы сжать файл или папку, выполните следующие действия:

1. В окне Проводника Windows (Windows Explorer) щелкните правой кнопкой файл или папку, которую хотите сжать, и выберите команду **Свойства (Properties)**.
2. На вкладке **Общие (General)** диалогового окна **Свойства (Properties)** щелкните кнопку **Другие (Advanced)**. В диалоговом окне **Дополнительные атрибуты (Advanced Attributes)** установите флажок **Сжимать содержимое для экономии места на диске (Compress Contents To Save Disk Space)**, как показано на рис. 12-12. Два раза щелкните **OK**.

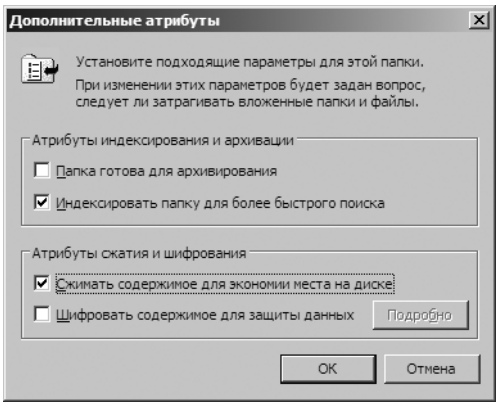


Рис. 12-12. Чтобы сжать файл или папку, установите флажок Сжимать содержимое для экономии места на диске (Compress Contents To Save Disk Space) в диалоговом окне Дополнительные атрибуты (Advanced Attributes)

В случае отдельного файла Windows Server 2008 помечает файл как сжатый, а затем сжимает его. В случае папки Windows Server 2008 помечает папку, как сжатую, после чего сжимает все содержащиеся в ней файлы. Если в папке есть подпапки, Windows Server 2008 выводит диалоговое окно, позволяющее сжать также все подпапки текущей папки. Установите переключатель **К данной папке и ко всем вложенным папкам и файлам (Apply Changes To This Folder, Subfolders, And Files)** и щелкните **OK**. После сжатия папки все файлы, добавляемые или копируемые в нее, сжимаются автоматически.

Примечание Если переместить в сжатую папку несжатый файл из другого диска, файл будет сжат. При перемещении несжатого файла в сжатую папку в пределах одного NTFS-диска сжатие файла не выполняется. Помните также, что к сжатым файлам нельзя применить шифрование.

Восстановление сжатых дисков

Чтобы отменить сжатие диска, выполните следующие действия:

1. В окне Проводника Windows (Windows Explorer) или оснастки **Управление дисками (Disk Management)** щелкните правой кнопкой диск, который хотите восстановить, и выберите команду **Свойства (Properties)**.

2. Сбросьте флажок **Сжать этот диск для экономии места (Compress Drive To Save Disk Space)** и щелкните **OK**.

Совет Перед восстановлением сжатых данных Windows всегда выполняет проверку наличия свободного места на диске. Вы тоже следите за этим. Если объем свободного пространства меньше, чем объем использованного, восстановление может не состояться. Например, если сжатый диск занимает 150 Гб, при свободных 70 Гб у вас не будет достаточно места для восстановления диска.

Восстановление сжатых папок и файлов

Чтобы восстановить сжатый файл или папку, выполните следующие действия:

1. В окне Проводника Windows (Windows Explorer) щелкните правой кнопкой файл или папку, которую хотите сжать, и выберите команду **Свойства (Properties)**.
2. На вкладке **Общие (General)** диалогового окна **Свойства (Properties)** щелкните кнопку **Другие (Advanced)**. В диалоговом окне **Дополнительные атрибуты (Advanced Attributes)** сбросьте флажок **Сжимать содержимое для экономии места на диске (Compress Contents To Save Disk Space)**. Два раза щелкните **OK**.

Windows Server 2008 отменит сжатие и восстановит файлы. При восстановлении папок система восстанавливает все файлы, находящиеся в папке. Если в папке находятся подпапки, вам будет предложено восстановить подпапки. Установите переключатель **К данной папке и ко всем вложенным папкам и файлам (Apply Changes To This Folder, Subfolders, And Files)** и щелкните **OK**.

Совет В Windows Server 2008 имеются утилиты командной строки для сжатия и восстановления данных. Утилита для сжатия называется Compact.exe, утилита для восстановления — Expand.exe.

Шифрование дисков и данных

Файловая система NTFS обладает многими преимуществами по сравнению с другими файловыми системами. Одно из главных преимуществ — способность автоматически шифровать и расшифровывать данные при помощи шифрующей файловой системы (EFS). Шифрование — дополнительный уровень защиты уязвимых данных, не позволяющий другим пользователям читать содержимое шифрованных файлов. Доступ к данным может получить только конкретный пользователь. Это преимущество может, правда, обернуться недостатком, когда необходимо обеспечить доступ к данным других авторизованных пользователей.

Примечание Из предыдущего раздела вы знаете, что невозможно сжимать шифрованные данные. Функции шифрования и сжатия NTFS взаимно исключают друг друга. Вы можете использовать обе функции по отдельности, но не вместе.

Шифрование и шифрующая файловая система

Шифрование файлов поддерживается на уровне папки или файла. Каждый файл, помещаемый в папку, помеченную как зашифрованная, автоматически шифруется. Файлы в шифрованном формате может читать только применивший шифрование пользователь. Чтобы шифрованный файл смогли прочитать другие пользователи, пользователь должен снять с него шифрование.

С каждым шифрованным файлом связан уникальный ключ шифрования. Это означает, что шифрованный файл можно копировать, перемещать и переименовывать, как и любые другие файлы, и это, в большинстве случаев, не повлияет на шифрование данных (подробнее — в разделе «Работа с шифрованными файлами и папками» этой главы). Пользователь, применивший шифрование к файлу, всегда имеет к нему доступ, при условии, что компьютере имеется сертификат открытого ключа пользователя. Для этого пользователя процесс шифрования и расшифровки выполняется автоматически и прозрачно.

Шифрованием и дешифрованием управляет шифрующая файловая система (EFS). Стандартные параметры EFS позволяют пользователю шифровать файлы без специального разрешения. Шифрование файлов выполняется с помощью открытого и секретного ключа, автоматически создаваемых EFS для каждого пользователя.

Сертификаты шифрования хранятся в профилях пользователей. Если пользователь желает работать на нескольких компьютерах, используя шифрование, администратору нужно настроить для этого пользователя перемещаемый профиль, который обеспечивает доступ пользователя к данным профиля и сертификатам открытого ключа с других компьютеров. Без него пользователи не смогут получить доступ к своим шифрованным файлам с другого компьютера.

Безопасность Альтернативой перемещаемому профилю может служить копирование сертификата шифрования пользователя на компьютер, за которым он работает. Для этого можно использовать резервное копирование и восстановление сертификатов, о котором рассказывается в разделе «Резервное копирование и восстановление состояния системы» главы 16. Создайте резервную копию сертификата на исходном компьютере пользователя, а затем восстановите сертификат на каждом компьютере, на который входит пользователь.

В EFS существует встроенная система восстановления данных, предотвращающая их потерю. Эта система обеспечивает восстановление данных в случае потери или удаления сертификата открытого ключа пользователя. Чаще всего это случается, когда пользователь покидает компанию и удаляется его учетная запись. Менеджер должен иметь возможность войти в систему с учетной записью пользователя, проверить информацию и сохранить нужные файлы в других папках. Но если учетная запись удалена, доступ к шифрованным файлам можно получить только после снятия шифрования или путем перемещения файлов на том FAT или FAT32 (где шифрование не поддерживается).

Для доступа к шифрованным файлам в случае удаления учетной записи пользователя вам потребуется агент восстановления (recovery agent). Он имеет доступ к ключу шифрования файла, который необходим для разблокирования данных. Тем не менее, для защиты уязвимых данных у агента восстановления нет доступа к секретному ключу пользователя и к любой информации о ключе.

ОС Windows Server 2008 не будет шифровать файлы без соответствующих агентов восстановления EFS. Поэтому агенты восстановления назначаются автоматически. Необходимые сертификаты восстановления также создаются автоматически. Это обеспечивает возможность восстановления шифрованных данных.

Настройка агентов восстановления EFS происходит на двух уровнях:

- **Домен** Агент восстановления домена настраивается автоматически во время установки первого контроллера домена под управлением Windows Server 2008. По умолчанию агентом восстановления считается администратор домена. Посредством групповой политики администраторы домена могут назначать дополнительных агентов восстановления, а также делегировать полномочия агентов восстановления назначенным администраторам безопасности.
- **Локальный компьютер** Если компьютер входит в рабочую группу или работает автономно, по умолчанию агентом восстановления является администратор локального компьютера. Могут быть назначены и дополнительные агенты восстановления. Если даже в среде домена вам больше подходят локальные агенты восстановления, а не агенты восстановления уровня домена, удалите политику восстановления из групповой политики домена.

Удалите агентов восстановления, если не желаете их использовать. Однако при удалении всех агентов восстановления EFS перестанет шифровать файлы. Для нормального функционирования EFS необходимы один или несколько агентов восстановления.

Шифрование папок и файлов

На NTFS-томах ОС Windows Server 2008 позволяет выбирать файлы и папки для шифрования. В процессе шифрования файлов данные преобразуются в шифрованный формат, прочитать который может только пользователь, применивший шифрование. Пользователь может шифровать файлы, только если у него есть соответствующее разрешение. Когда вы применяете шифрование к папке, папка лишь помечается как шифрованная, на самом деле шифруются находящиеся внутри нее файлы. Все создаваемые в папке или добавляемые в нее файлы шифруются автоматически.

Для применения шифрования к файлу или папке выполните следующие действия:

1. Щелкните правой кнопкой файл или папку, которую хотите зашифровать, и выберите команду **Свойства (Properties)**.

2. В диалоговом окне **Свойства (Properties)** на вкладке **Общие (General)** щелкните кнопку **Другие (Advanced)**. Затем установите флажок **Шифровать содержимое для защиты данных (Encrypt Contents To Secure Data)**. Два раза щелкните **OK**.

Примечание Нельзя шифровать сжатые, системные файлы, а также файлы с доступом только для чтения. При попытке зашифровать сжатые файлы они сначала автоматически восстанавливаются, а затем шифруются. При попытке шифрования системных файлов произойдет ошибка.

Отдельный файл помечается Windows Server 2008 как шифрованный, а затем шифруется. При шифровании папки Windows Server 2008 помечает ее как шифрованную, а затем шифрует все содержащиеся в ней файлы. Если в папке есть подпапки, Windows Server 2008 выводит диалоговое окно, позволяющее зашифровать все подпапки, связанные с текущей папкой. Установите переключатель **К данной папке и ко всем вложенным папкам и файлам (Apply Changes To This Folder, Subfolders, And Files)** и щелкните **OK**.

Примечание На NTFS-томах файлы остаются шифрованными, даже если их переместить, копировать или переименовать. Если вы переместите шифрованный файл на диск FAT или FAT32, перед копированием файл будет автоматически дешифрован. Соответственно, для перемещения файла у вас должны иметься необходимые разрешения.

Работа с шифрованными файлами и папками

Ранее я говорил, что вы можете копировать, перемешать и переименовывать шифрованные файлы и папки, как и любые другие файлы и папки, но вы наверняка заметили не большое уточнение — «в большинстве случаев». У вас не возникнет особых проблем, пока вы работаете с зашифрованными файлами на NTFS-томах одного компьютера. Проблемы начнутся при работе с другой файловой системой или другими компьютерами. Вот два наиболее распространенных сценария:

- **Копирование между томами одного компьютера** При копировании или перемещении шифрованного файла или папки из одного NTFS-тома в другой NTFS-том в пределах одного компьютера файлы остаются в зашифрованными. Однако, если вы копируете или перемещаете шифрованные файлы в тома FAT или FAT32, перед перемещением происходит дешифрование файлов, после чего они перемещаются уже как обычные файлы. Файловые системы FAT и FAT32 не поддерживают шифрование.
- **Копирование между томами различных компьютеров** При копирова-нии или перемещении шифрованного файла или папки из NTFS-тома в NTFS-том, расположенный на другом компьютере, файлы остаются в зашифрованными, если конечный компьютер поддерживает шифрование, а удаленный компьютер является доверенным для делегирования. В противном случае файлы расшифровываются и перемещаются как обычные файлы. Это справедливо и в случае копирования или перемещения

шифрованных файлов в том FAT или FAT32, расположенный на другом компьютере. Файловые системы FAT и FAT32 не поддерживают шифрование.

После перемещения важного файла, к которому было применено шифрование, стоит проверить, что он остался зашифрованным и после копирования. Щелкните файл правой кнопкой и выберите команду **Свойства (Properties)**. В диалоговом окне **Свойства (Properties)** на вкладке **Общие (General)** щелкните кнопку **Другие (Advanced)**. Флажок **Шифровать содержимое для защиты данных (Encrypt Contents To Secure Data)** должен быть установлен.

Настройка политики восстановления

Политики восстановления для контроллеров домена и рабочих станций настраиваются автоматически. По умолчанию администраторы домена назначаются агентами восстановления доменов, а локальные администраторы назначаются агентами восстановления для изолированных рабочих станций.

Чтобы просматривать, назначать и удалять агентов восстановления, выполните следующие действия:

1. Откройте редактор групповой политики для локального компьютера, сайта, домена или подразделения, с которым вы хотите работать. Подробнее — в разделе «Групповые политики» главы 5.
2. Разверните узлы **Конфигурация компьютера (Computer Configuration)**, **Конфигурация Windows (Windows Settings)**, **Параметры безопасности (Security Settings)**, **Политики открытого ключа (Public Key Policies)**, **Шифрующая файловая система (Encrypting File System)** и **Агенты восстановления шифрованных данных (Encrypted Data Recovery Agents)**.
3. На правой панели будут отображены сертификаты восстановления, назначенные в данный момент, в соответствии с тем, кто их создал, для кого они выпущены, со сроком действия, целью и прочими критериями.
4. Чтобы назначить дополнительного агента восстановления, щелкните правой кнопкой узел **Шифрующая файловая система (Encrypting File System)** и выберите команду **Добавить агент восстановления данных (Add Data Recovery Agent)**. Откроется Мастер добавления агента восстановления (Add Recovery Agent Wizard), который поможет выбрать ранее сгенерированный сертификат, который был назначен пользователю, и пометить его как сертификат восстановления. Щелкните **Далее (Next)**.
5. На странице **Выбор агентов восстановления (Select Recovery Agents)** щелкните кнопку **Обзор каталога (Browse Directory)** и выберите пользователя, с которым хотите работать.

Безопасность Прежде чем вы сможете добавлять агентов восстановления, вы должны установить в домене корневой центр сертификации. После этого вы должны сгенерировать личный сертификат в оснастке **Сертификаты (Certificates)** на основе шаблона **Агент восстановления EFS (EFS Recovery Agent)**. Корневой центр сертификации утверждает запрос на предоставление сертификата, после чего сертификат можно использовать.

6. Чтобы удалить агент восстановления, на правой панели выберите сертификат агента и нажмите клавишу **Delete**. Щелкните **Да (Yes)**, чтобы окончательно удалить сертификат. Если политика восстановления пуста (то есть, других назначенных агентов восстановления не существует), EFS будет отключена, и с этого момента шифрование файлов производиться не будет.

Расшифровка файлов и папок

Чтобы снять шифрование с файла или папки, выполните следующие действия:

1. В окне Проводника Windows (Windows Explorer) щелкните правой кнопкой файл или папку.
2. В диалоговом окне **Свойства (Properties)** на вкладке **Общие (General)** щелкните кнопку **Другие (Advanced)**. Сбросьте флажок **Шифровать содержимое для защиты данных (Encrypt Contents To Secure Data)**. Два раза щелкните **OK**.

Windows Server 2008 снимет шифрование с файла и восстановит его первоначальную форму. Если вы снимаете шифрование с папки, Windows Server 2008 отменит шифрование всех находящихся в папке файлов. Если в папке находятся подпапки, вам будет предложено расшифровать их, установив переключатель **К данной папке и ко всем вложенным папкам и файлам (Apply Changes To This Folder, Subfolders, And Files)** и щелкнув **OK.**

Совет Шифрование и расшифровку данных можно производить при помощи утилиты командной строки Cipher.exe, которая входит в состав Windows Server 2008. Введя в командной строке команду cipher без дополнительных параметров, вы получите информацию о шифровании всех папок в текущей папке.

Глава 13

Администрирование наборов томов и массивов RAID

Во время работы с постоянными дисковыми накопителями в ОС Microsoft Windows Server 2008 вам предстоит часто выполнять дополнительные действия по настройке дисков. К ним относятся создание набора томов и установка массива избыточных независимых дисков (RAID).

Набор томов (volume set) позволяет создать один том из нескольких накопителей. Пользователи будут обращаться к тому, как будто он представляет собой один диск, независимо от того сколько реальных дисков охватывает том. Том, расположенный на одном диске, называется *простым* (simple). Том, состоящий из нескольких накопителей, называется *составным* (spanned).

Массивы RAID позволяют защитить важную деловую информацию, а иногда и повысить производительность дисков. Система Windows Server 2008 поддерживает три уровня RAID — 0, 1 и 5. Массивы RAID реализованы как зеркальные, чередующиеся тома и чередующиеся тома с контролем четности.

Наборы томов и RAID-массивы создаются на динамических дисках, работающих только в Windows 2000 и более поздних выпусках. Если на вашем компьютере с двухвариантной загрузкой установлена более ранняя версия Windows, из нее динамические диски будут не видны. Тем не менее, компьютеры под управлением более ранних версий Windows могут получить доступ к дискам по сети, как и к любому сетевому диску.

Тома и наборы томов

Создание и управление томами и разделами мало чем отличаются друг от друга. Том представляет собой раздел диска, используемый непосредственно для хранения данных.

Примечание Работая с составными и чередующимися томами на основных дисках, вы можете удалить том, но не можете создавать или расширять тома. Работая с зеркальными томами на основных дисках, вы можете удалять зеркало, исправлять его и повторно синхронизировать. Вы также можете разбить зеркало. Работая с чередующимися томами с контролем четности (RAID5) на основных дисках, вы можете удалять или исправлять тома, но не можете создавать новые тома.

Основные сведения о томах

В оснастке **Управление дисками (Disk Management)** тома маркированы цветом, как и разделы. На рис. 13-1 показаны параметры томов:

- **Расположение (Layout)** Простой, составной, зеркальный, чередующийся или чередующийся по четности.
- **Тип (Type)** Тип тома всегда динамический.
- **Файловая система (File System)** По аналогии с разделами, каждый том может иметь собственную файловую систему: FAT, FAT32 или NTFS.
- **Состояние (Status)** Состояние накопителя. В Графическом представлении (Graphical View) состояние выражается значениями Исправен (Healthy), Отказавшая избыточность (Failed Redundancy) и т. д.
- **Емкость (Capacity)** Полный объем диска.

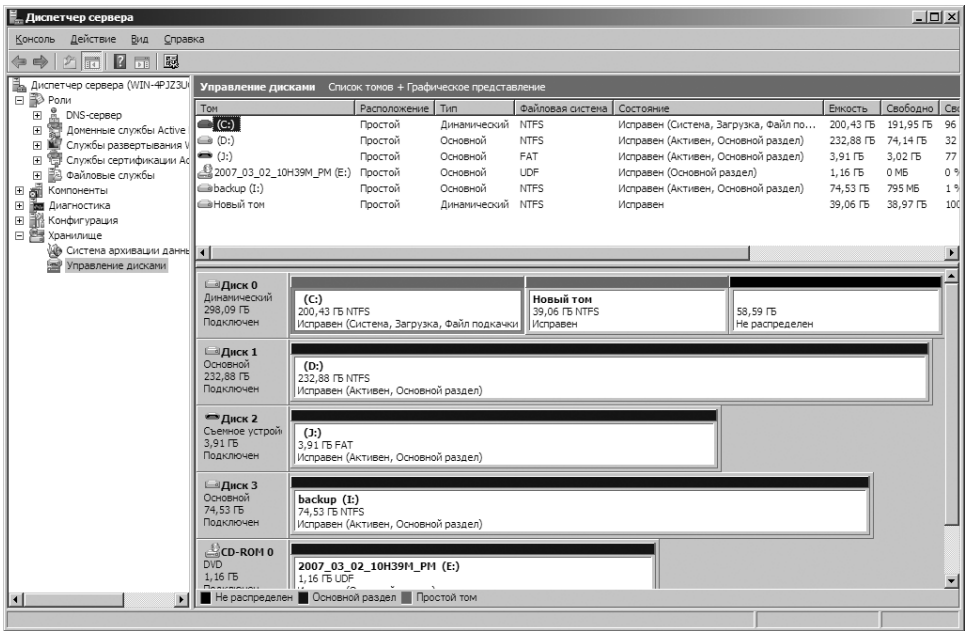


Рис. 13-1. В оснастке Управление дисками (Disk Management) отображение томов очень похоже на отображение разделов

Преимущество динамических разделов перед основными состоит в том, что они в большинстве случаев позволяют вносить изменения в тома и накопители без последующей перезагрузки системы. Кроме того, тома позволяют использовать расширения отказоустойчивости Windows Server 2008. Вы можете установить в качестве альтернативы Windows Server 2008 другую операционную систему. Для другой ОС вам придется создать отдельный том. Например, можно установить Windows Server 2008 на том C и Windows Vista на том D.

С томами можно выполнять следующие действия (подробнее — в главе 12):

- назначать буквы дисков;
- назначать пути к дискам;
- создавать любое количество томов на диске (при наличии свободного пространства);
- создавать тома, объединяющие два или несколько дисков, при необходимости, настраивая отказоустойчивость;
- расширять тома с целью увеличения их объема;
- настраивать активные, системные и загрузочные тома.

Наборы томов

Наборы позволяют создавать тома, охватывающие несколько дисков. Свободное пространство на нескольких накопителях объединяется и представляется пользователю в виде единого тома. Файлы располагаются в томе посегментно: для хранения файлов сначала используется первый сегмент свободного пространства, потом второй сегмент и т. д.

Для создания набора томов можно использовать свободное пространство до 32 жестких дисков. Ключевое преимущество наборов томов заключается в том, что вы получаете доступ к неиспользуемому свободному пространству и создаете на нем нормальную файловую систему. Ключевой недостаток состоит в том, что при возникновении неисправности в одном из дисков набора весь набор становится неработоспособным. По сути, это означает потерю всех данных в наборе томов.

При установке новых томов или устранении неисправностей полезно понимание состояния тома. Состояние диска отображается в представлениях Графическое представление (Graphical View) и Список томов (Volume List) оснастки **Управление дисками (Disk Management)**. В табл. 13-1 приводится обзор состояний динамических дисков.

Табл. 13-1. Состояние тома

Состояние	Описание	Решение
Неполные данные (Data Incomplete)	Составной том на инородном диске не завершен. Возможно, вы забыли добавить другие диски из набора составного тома	Добавьте диски, содержащие остаток составного тома, а затем одновременно импортируйте все диски
Нет избыточности данных (Data Not Redundant)	Отказоустойчивый том на инородном диске не завершен. Возможно, вы забыли добавить другие диски зеркала или набора RAID-5	Добавьте оставшиеся диски, а затем одновременно импортируйте все диски

Табл. 13-1. (*продолжение*)

Состояние	Описание	Решение
Неисправен (Failed)	На диске есть ошибка. Диск недоступен или поврежден	Убедитесь, что динамический диск подключен. При необходимости щелкните том правой кнопкой и выберите команду **Реактивизировать том (Reactivate Volume)**. В случае с основным диском проверьте правильность подключения диска
Отказавшая избыточность (Failed Redundancy)	Состояние свидетельствует о наличии ошибки на диске. Не подключен один из дисков зеркала или набора RAID-5	Убедитесь, что динамический диск подключен. При необходимости реактивируйте том. Далее вам, возможно, придется заменить неисправное зеркало или том RAID-5
Форматирование (Formatting)	Временное состояние, указывающее на форматирование тома	Дождитесь окончания форматирования. Завершенность форматирования указывается в процентах
Исправен (Healthy)	Нормальное состояние тома	На томе нет ни одной из известных неисправностей. Делать ничего не нужно
Исправен (под угрозой) (Healthy (At Risk))	У Windows возникли проблемы с чтением или записью на физический диск, на котором расположен динамический том. Состояние свидетельствует о наличии ошибки на диске	Щелкните том правой кнопкой и выберите команду **Реактивизировать том (Reactivate Volume)**. Если состояние диска не изменилось или появляется периодически, возможно, диск неисправен и вам следует выполнить резервное копирование всех данных на диске
Исправен (неизвестный раздел) (Healthy (Unknown Partition))	Системе не удается распознать раздел. Это происходит, если ранее раздел использовался другой ОС или является разделом, который создан производителем диска для хранения системных файлов	Исправление не требуется
Инициализация (Initializing)	Временное состояние, указывающее на инициализацию диска	Дождитесь окончания инициализации

Табл. 13-1. (*окончание*)

Состояние	Описание	Решение
Регенерация (Regenerating)	Временное состояние, указывающее на восстановление данных и четности тома из массива RAID-5	Дождитесь окончания регенерации. Состояние тома должно измениться на Исправен (Healthy)
Ресинхронизация (Resynching)	Временное состояние, указывающее на синхронизацию зеркального набора	Дождитесь окончания ресинхронизации. Состояние тома должно измениться на Исправен (Healthy)
Устаревшие данные (Stale Data)	Асинхронность данных на инородных отказоустойчивых дисках	Выполните повторный поиск дисков или перезагрузите компьютер, а затем проверьте состояние. Оно должно измениться, например, на Отказавшая избыточность (Failed Redundancy)
Неизвестный (Unknown)	Нет доступа к тому. Скорее всего, поврежден загрузочный сектор	В загрузочном секторе тома может находится вирус. Проверьте том обновленной антивирусной программой. Выполните повторный поиск дисков или перезагрузите компьютер, а затем проверьте состояние

Создание томов и наборов томов

Простые тома можно форматировать в FAT, FAT32 или NTFS. Чтобы облегчить управление, тома, охватывающие несколько дисков, следует форматировать в NTFS. Такое форматирование позволяет при необходимости расширить набор томов. Если вам потребуется больше места на диске, расширяйте простые и составные тома. Вся процедура сводится к поиску свободного пространства и его добавлению к тому. Простой том можно расширять как в пределах одного диска, так и распространить его на другие диски. При этом вы создаете составной диск, который должен быть отформатирован в NTFS.

Для создания тома или набора томов выполните следующие действия:

1. В графическом представлении оснастки **Управление дисками (Disk Management)** щелкните правой кнопкой нераспределенную область и выберите команду **Новый составной том (New Spanned Volume)**. Прочитайте вводную страницу и щелкните **Далее (Next)**.
2. Откроется страница **Выбор дисков (Select Disks)**, показанная на рис. 13-2. Выберите диски, из которых будет состоять том, и укажите размер фрагментов тома на этих дисках.

3. Доступные диски отображены в списке **Доступны (Available)**. При необходимости выберите диск в этом списке и щелкните кнопку **Добавить (Add)**, чтобы добавить диск в список **Выбраны (Selected)**. Если вы ошибочно выбрали диск, выделите его в списке **Выбраны (Selected)** и щелкните **Удалить (Remove)**.

Внимание! В отличие от предыдущих версий Windows, мастера для работы с дисками в Windows Server 2008 отображают как основные, так и динамические диски с доступным дисковым пространством. При добавлении пространства из основного диска перед созданием набора томов мастер преобразует диск в динамический. Прежде чем щелкнуть **Да (Yes)**, подумайте, действительно ли вы хотите выполнить это действие, поскольку оно способно повлиять на работу ОС с дисками.

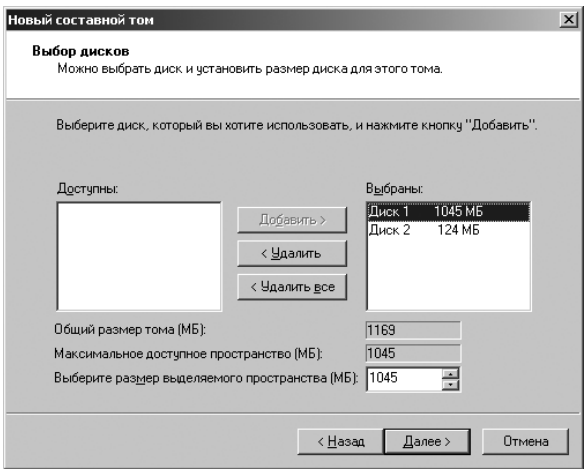


Рис. 13-2. На странице Выбор дисков (Select Disks) выберите диски, которые станут частью тома

4. Выберите диск в списке **Выбраны (Selected)** и в поле **Выберите размер выделяемого пространств (МБ) (Select The Amount Of Space In MB)** укажите размер фрагмента тома на выбранном диске. В поле **Максимальное доступное пространство (Maximum available space)** показана наибольшая область свободного пространства на выбранном диске. В поле **Общий размер тома (Total Volume Size)** показано суммарное дисковое пространство тома. Щелкните **Далее (Next)**.

Совет Вы вольны устанавливать размер тома любым удобным для вас способом, однако подумайте, каким образом будут использоваться наборы томов в системе. Простые и составные тома не являются отказоустойчивыми. Поэтому вместо создания одного гигантского тома, охватывающего все доступное свободное пространство, лучше создать несколько меньших по размеру томов. Таким образом, потеря одного тома не будет означать потерю всех данных.

5. Укажите, будет ли назначена тому буква диска или путь, и щелкните **Далее (Next)**. Доступны следующие варианты:

- **Назначить букву диска (Assign The Following Drive Letter)** Установите этот переключатель, чтобы назначить букву диска, и выберите незанятую диска в списке.
- **Подключить том как пустую NTFS-папку (Mount In The Following Empty NTFS Folder)** Установите этот переключатель, чтобы назначить путь к диску. Затем введите путь к существующей папке на NTFS-диске или щелкните **Обзор (Browse)**, чтобы найти или создать папку.
- **Не назначать буквы диска или пути диска (Don't Assign A Drive Letter Or Drive Path)** Установите этот переключатель, чтобы создать том, не присваивая ему буквы диска или пути. Вы сможете назначить букву или путь позже.

6. Укажите, следует ли форматировать том (рис. 13-3), и задайте следующие параметры форматирования:
   - **Файловая система (File System)** Тип файловой системы. Здесь вам доступен единственный вариант — NTFS.
   - **Размер кластера (Allocation Unit Size)** Размер кластера — базовой единицы распределения дискового пространства. Стандартный размер кластера зависит от размера тома и по умолчанию задается динамически перед форматированием. Вы вольны выбрать собственный размер кластера. Если вы используете много небольших файлов, вам стоит работать с кластерами небольшого размера, например, 512 или 1024 байт. Такие параметры позволяют сэкономить дисковое пространство при работе с небольшими файлами.
   - **Метка тома (Volume Label)** Текстовая метка раздела.
   - **Быстрое форматирование (Perform A Quick Format)** Система Windows Server 2008 выполнит быстрое форматирование, не проверяя том на наличие ошибок. При форматировании больших разделов эта функция сэкономит вам несколько минут, но лучше не отказываться от проверки. В ее ходе оснастка **Управление дисками (Disk Management)** отмечает на диске секторы с ошибками и блокирует их.
   - **Применять сжатие файлов и папок (Enable File And Folder Compression)** Включает функцию сжатия данных на диске. Встроенная возможность сжатия данных доступна только для NTFS-томов. В NTFS сжатие происходит незаметно для пользователей, и они осуществляют доступ к сжатым файлам точно так же, как и к обычным. Если вы установите этот флажок, файлы и папки на диске будут автоматически сжиматься. Подробнее о сжатии дисков, файлов и папок — в разделе «Сжатие дисков и данных» главы 12.
7. Щелкните **Далее (Next)** и **Готово (Finish)**.

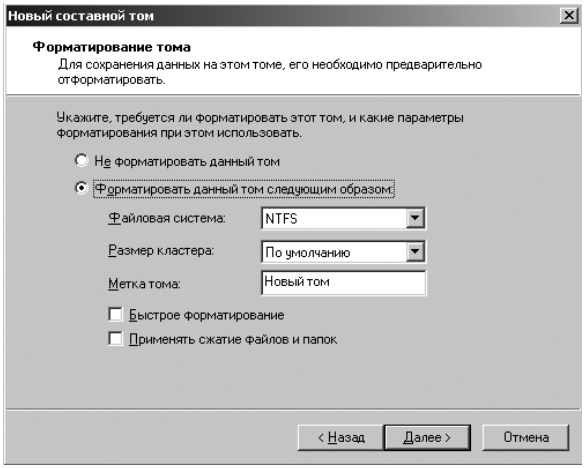


Рис. 13-3. Укажите размер кластера и метку тома

Удаление томов и наборов томов

Существует единый способ удаления простых, составных, зеркальных, чередующихся томов и томов RAID-5. При удалении набора томов удаляется соответствующая файловая система, и теряются все данные. Поэтому прежде чем удалить набор томов, создайте резервные копии всех файлов и папок, содержащихся в наборе. Нельзя удалить том, содержащий системные, загрузочные или активные файлы подкачки Windows Server 2008.

Чтобы удалить том, выполните следующие действия:

1. В оснастке **Управление дисками (Disk Management)** щелкните правой кнопкой любой том набора и выберите команду **Удалить том (Delete Volume)**. Нельзя удалить часть составного тома, не удалив весь том.
2. Щелкните **Да (Yes)**, чтобы подтвердить удаление тома.

Управление томами

Управление томами мало чем отличается от управления разделами. Подробнее — в разделе «Управление существующими разделами и дисками» главы 12.

Повышение производительности и отказоустойчивости с помощью RAID

Часто возникает необходимость защитить важные данные от потери из-за неисправности дисков. Для этого можно воспользоваться технологией RAID, которая обеспечивает отказоустойчивость файловых систем. Она повышает целостность и доступность данных путем создания их избыточных копий. Кроме того, технологию RAID можно использовать для повышения производительности дисков.

Существуют различные реализации технологии RAID, описываемые определенными уровнями. На данный момент определены уровни RAID от 0 до 5. Каждый уровень RAID обладает различными возможностями. Система Windows Server 2008 поддерживает уровни RAID 0, 1 и 5. При помощи RAID 0 вы повысите производительность дисков. Для обеспечения отказоустойчивости используются RAID 1 и RAID 5.

В табл. 13-2 содержится краткий обзор уровней RAID. Поддержка целиком и полностью осуществляется на программном уровне.

Табл. 13-2. Уровни RAID, поддерживаемые в Windows Server 2008

Уровень RAID	Тип RAID	Описание	Основные преимущества
0	Чередование дисков	Два или несколько томов, каждый на отдельном диске, сконфигурированы как чередующийся набор. Диск разбивается на блоки, которые называются полосами (strip). Запись выполняется последовательно на все диски чередующегося набора	Скорость и производительность
1	Зеркалирование дисков	На двух дисках создается два одинаковых тома. Запись данных производится на оба диска. В случае неисправности потери данных не происходит, потому что данные имеются на другом диске. (Нет чередования дисков.)	Избыточность. Большее быстродействие при записи, чем у чередующихся дисков с контролем четности
5	Чередование дисков с контролем четности	Задействовано три и более томов, каждый на отдельном диске. Создается чередующийся набор с проверкой ошибок по четности. При возникновении неисправности данные могут быть восстановлены	Отказоустойчивость при меньших затратах по сравнению с зеркалированием. Большее быстродействие при чтении, чем у зеркальных томов

На серверах Windows Server 2008 чаще всего встречаются массивы RAID 1 (зеркала) и RAID 5 (чередование с контролем четности). Наиболее экономичным способом защиты данных посредством избыточности является создание зеркальных дисков. Здесь для создания избыточного набора данных применяются два идентичных тома на разных накопителях. В случае неисправности одного накопителя вы сможете получить данные с другого.

Чередование дисков с контролем четности требует больше дисков — как минимум, трех. Но в то же время, накладные расходы на отказоустойчивость в этом случае меньше, чем в зеркальных дисках. При выходе из строя одного

из дисков вы восстановите данные, объединив блоки данных на оставшихся дисках, используя контроль четности — способ проверки ошибок, в котором операция исключающего ИЛИ применяется для вычисления контрольной суммы каждого блока записываемых на диск данных. Контрольная сумма используется для восстановления данных в случае неисправности.

Ближе к реальности Хотя первоначальные затраты на создание зеркальных наборов ниже, чем на создание чередующихся наборов с контролем четности, реальная стоимость мегабайта при работе с зеркалами может оказаться выше. Накладные расходы при использовании зеркал составляют 50%. Например, при зеркальном отображении двух накопителей объемом 300 Гб (суммарный объем 600 Гб) полезный объем составит 300 Гб. С другой стороны, накладные расходы на чередующиеся диски с контролем четности составляют около 33%. В частности, при создании массива RAID-5 на трех накопителях по 300 Гб каждый (суммарный объем 900 Гб) полезный объем (за вычетом одной трети на накладные расходы) составит 600 Гб.

Реализация RAID в Windows Server 2008

Система Windows Server 2008 поддерживает зеркалирование, чередование и чередование с контролем четности. В следующих разделах речь пойдет о реализации технологий RAID.

Внимание! Некоторые ОС, например, MS-DOS, не поддерживают RAID. В случае двухвариантной загрузки одной из таких несовместимых ОС диски с настроенными RAID-массивами будут недоступны.

RAID 0: чередование

Технология RAID уровня 0 представляет собой чередование дисков, когда два или несколько томов (каждый на отдельном накопителе) объединены в чередующийся набор. Записываемые на чередующийся набор данные разбиваются на блоки, которые называются *полосами* (stripe). Полосы последовательно записываются на все диски чередующегося набора. В чередующемся наборе можно разместить до 32 дисков, но в большинстве случаев наибольший рост производительности обеспечивают наборы, состоящие из 2–5 томов. При большем количестве дисков рост производительности значительно снижается.

Основное преимущество чередующихся дисков заключается в быстродействии. Доступ к данным осуществляется на нескольких дисках с использованием нескольких головок, что значительно увеличивает производительность. Тем не менее, подобное повышение производительности обходится недешево. Как и в случае с наборами томов, при неисправности одного из дисковых накопителей весь набор выходит из строя. По сути, это означает потерю данных всего чередующегося набора. Потребуется повторное создание чередующегося набора и восстановление данных из резервных копий. Резервное копирование и восстановление данных рассмотрены в главе 16.

Внимание! Загрузочные и системные тома не должны быть частью чередующегося набора. Не применяйте чередование к этим томам.

Для создания чередующегося набора используйте приблизительно равные по размеру тома. Оснастка **Управление дисками (Disk Management)** устанавливает общий размер чередующегося набора по размеру наименьшего тома. В частности, максимальный размер чередующегося набора кратен размеру наименьшего тома. Например, если размер самого маленького тома составляет 50 Мб, максимальный размер чередующегося набора равен 150 Мб.

Существуют способы повышения производительности чередующихся наборов:

- Используйте диски на разных контроллерах. Это позволит системе одновременно обращаться к разным накопителям.
- Не используйте диски, содержащие чередующийся набор, для других целей. Это позволит диску отдавать все свое время чередующемуся набору.

Чтобы создать чередующийся набор, выполните следующие действия:

1. В графическом представлении оснастки **Управление дисками (Disk Management)** щелкните правой кнопкой нераспределенную область динамического диска. Выберите команду **Новый чередующийся том (New Striped Volume)**. Откроется Мастер создания чередующихся томов (New Striped Volume Wizard). Прочитайте вводную страницу и щелкните **Далее (Next)**.
2. Создайте том, как описано в разделе «Создание томов и наборов томов» этой главы. Ключевое отличие заключается в том, что для создания чередующегося тома требуется, по меньшей мере, два динамических диска.
3. Создав чередующийся том, используйте его, как любой другой том. После создания чередующегося набора его расширение невозможно. Поэтому перед созданием набора тщательно все продумайте.

RAID 1: зеркалирование

Технология RAID уровня 1 представляет собой зеркальное отображение дисков. Для него используются идентичные по размеру тома на двух отдельных накопителях с целью создания избыточного набора данных. На диски записываются одинаковые наборы информации. В случае неисправности одного накопителя вы получите данные с другого.

Зеркальное отображение обеспечивает примерно тот же уровень отказоустойчивости, что и чередование дисков с контролем четности. Зеркальным дискам не требуется запись сведений о четности, поэтому в большинстве случаев они обеспечивают большее быстродействие при записи. С другой стороны, чередование дисков с контролем четности обеспечивает лучшую производительность при чтении, потому что операции чтения распределены между несколькими дисками.

Серьезным недостатком зеркалирования является тот факт, что оно вдвое уменьшает пространство для хранения данных. Например, чтобы зеркально

отобразить диск объемом 500 Гб, вам потребуется еще один диск того же объема. Это значит, что для хранения 500 Гб информации будет использовано 1000 Гб дискового пространства.

Совет Если есть возможность, старайтесь создавать зеркала загрузочного и системного томов. Это гарантирует возможность загрузить сервер в случае неисправности одного из дисков.

Как и в случае чередующихся дисков, как правило, зеркальные диски лучше размещать на отдельных контроллерах. Это обеспечивает защиту от сбоя контроллера диска. В случае выхода из строя одного контроллера диск на другом контроллере продолжает работать. Технически, при использовании двух отдельных контроллеров вы реализуете механизм, известный как *дуплексирование дисков* (disk duplexing). На рис. 13-4 показаны отличия двух технологий. Если для зеркалирования обычно используется один контроллер диска, в дуплексирование дисков вовлечено два контроллера. В остальном обе технологии очень похожи.

При выходе из строя одного зеркального диска, работа может продолжаться. При чтении и записи данных пользователями информация записывается на оставшийся диск. Чтобы отремонтировать зеркало, сначала его следует разбить. Подробнее — в разделе «Управление RAID и восстановление после сбоя» этой главы.

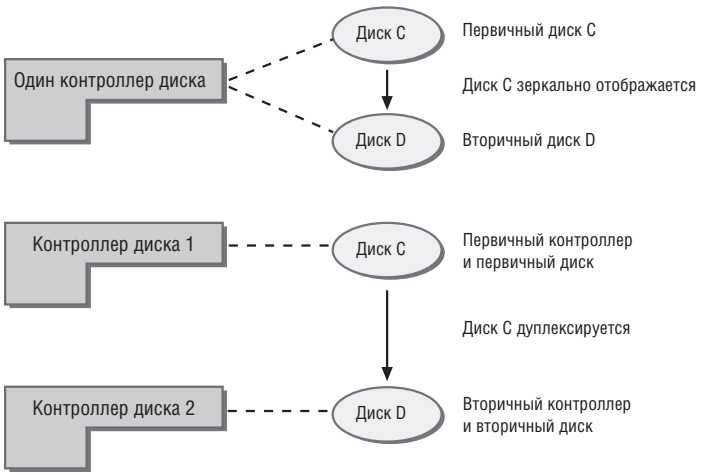


Рис. 13-4. Для зеркалирования обычно используется один контроллер диска, а в дуплексирование вовлечено два контроллера

Создание зеркального набора томов

Чтобы создать зеркальный набор томов, выполните следующие действия:

1. В графическом представлении оснастки **Управление дисками (Disk Management)** щелкните правой кнопкой нераспределенную область динамического диска. Выберите команду **Создать зеркальный том (New Mirrored Volume)**. Откроется Мастер создания образа (New Mirrored Vol-

ume Wizard). Прочитайте вводную страницу и щелкните **Далее (Next)**.

2. Создайте том, как описано в разделе «Создание томов и наборов томов» этой главы. Ключевое отличие состоит в том, что вы должны создать два одинаковых по размеру тома и эти тома должны находиться на разных динамических дисках. Вы не сможете продолжить, пока не выберете в списке **Выбраны (Selected)** два диска, с которыми хотите работать.
3. Подобно другим уровням RAID, зеркалирование работает прозрачно для пользователей. Пользователи видят зеркальный набор, как один диск, обращение к которому происходит так же, как и к обычному накопителю.

Примечание Нормальное состояние зеркала — **Исправен (Healthy)**. В процессе создания зеркала отображается состояние **Ресинхронизация (Resynching)**. Оно свидетельствует о создании зеркала оснасткой **Управление дисками (Disk Management)**.

Создание зеркала существующего тома

Для создания набора зеркал необязательно создавать новый зеркальный том, можно воспользоваться и существующим. Том, который вы хотите отобразить, должен быть простым, а на втором динамическом диске у вас должна иметься неразмеченная область, равная или превосходящая по размеру существующий том.

Чтобы создать зеркальное отображение существующего тома в оснастке **Управление дисками (Disk Management)**, выполните следующие действия:

1. Щелкните правой кнопкой существующий том, который собираетесь отобразить, и выберите команду **Добавить зеркало (Add Mirror)**. Откроется диалоговое окно **Добавить зеркальный том (Add Mirror)**.

   В списке **Диски (Disks)**, показанном на рис. 13-5, выберите расположение зеркала и щелкните кнопку **Добавить зеркальный том (Add Mirror)**.
2. Система Windows Server 2008 начнет процесс создания зеркала. В окне **Управление дисками (Disk Management)** оба тома будут находиться в состоянии **Ресинхронизация (Resynching)**. Диск, на котором создается зеркальный том, будет помечен значком предупреждения.

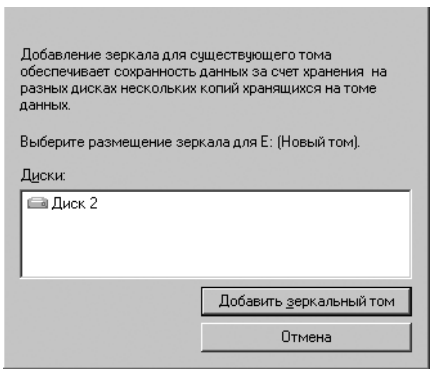


Рис. 13-5. Выберите расположение зеркала

RAID 5: чередование дисков с контролем четности

Технология RAID уровня 5 — это чередование дисков с контролем четности. Для настройки отказоустойчивости по этой технологии требуется, по меньшей мере, три дисковых накопителя. Оснастка **Управление дисками (Disk Management)** определяет одинаковые размеры для томов, расположенных на этих дисках.

Вообще, RAID 5 — это улучшенная версия RAID 1, дополненная отказоустойчивостью, которая обеспечивает работу набора дисков даже при возникновении неисправности в одном из них. Диски продолжают функционировать, а дисковые операции направляются на оставшиеся тома набора.

Чтобы реализовать отказоустойчивость RAID 5, вместе с блоками данных записываются контрольные суммы. При выходе из строя одного из накопителей чередующегося набора вы можете восстановить данные с помощью информации о четности. Этот процесс называется восстановлением чередующегося набора и обсуждается в разделе «Управление RAID и восстановление после сбоя» этой главы. В случае неисправности двух дисков для восстановления данных информации о четности будет недостаточно. Вам придется восстанавливать чередующийся набор из резервных копий.

Создание чередующегося набора с контролем четности

Чтобы создать чередующийся набор с контролем четности в оснастке **Управление дисками (Disk Management)**, выполните следующие действия:

1. В графическом представлении оснастки **Управление дисками (Disk Management)** щелкните правой кнопкой нераспределенную область динамического диска. Выберите команду **Новый том RAID-5 (New RAID-5 Volume)**. Откроется Мастер создания томов RAID-5 (New RAID-5 Volume Wizard). Прочитайте вводную страницу и щелкните **Далее (Next)**.
2. Создайте том, как описано в разделе «Создание томов и наборов томов» этой главы. Ключевое отличие состоит в том, что вы должны выбрать три области на трех разных динамических дисках.

Когда вы создадите набор RAID-5, пользователи смогут работать с ним, как с обычным диском. Помните, что чередующийся набор с контролем четности нельзя расширить. Поэтому перед его созданием все тщательно продумайте.

Управление RAID и восстановление после сбоя

Управление зеркальными дисками и чередующимися наборами несколько отличается от управления томами на других накопителях, особенно, в части восстановления после сбоя. В данном разделе описано управление RAID-массивами и их восстановление.

Резервное копирование зеркального набора

Существует две причины, по которым требуется разделить зеркало:

- С выходом из строя одного зеркального диска работа дисков набора может продолжаться. Для записи и чтения данных используется оставшийся диск. Но все-таки рано или поздно зеркало придется чинить. Для этого потребуется сначала разделить зеркало, а затем восстановить его.
- Если вы хотите отказаться от зеркального отображения дисков, вам также придется разделить зеркальный набор. Это позволит использовать дисковое пространство для других целей.

Совет Хотя разделение зеркального набора не удаляет его данных, перед выполнением этой процедуры следует проводить резервное копирование. Оно обеспечит возможность восстановления данных, если что-то пойдет не так.

Чтобы разделить зеркальный набор в оснастке **Управление дисками (Disk Management)**, выполните следующие действия:

1. Щелкните правой кнопкой один из томов зеркального набора и выберите команду **Разделить зеркальный том (Break Mirrored Volume)**.
2. Подтвердите разделение, щелкнув **Да (Yes)**. Если том используется, вы получите еще одно предупреждение. Подтвердите продолжение операции, щелкнув **Да (Yes)**.
3. Система Windows Server 2008 разобьет набор, создав два независимых тома.

Ресинхронизация и восстановление зеркального набора

Система Windows Server 2008 автоматически синхронизирует зеркальные тома на динамических дисках. Тем не менее, на зеркальных дисках может произойти сбой синхронизации данных. Например, в случае отключения одного из дисков все данные записываются на работающий диск.

Чтобы ресинхронизировать и восстановить зеркальный набор, вы должны использовать диски с тем же самым стилем разделов — MBR или GPT. Оба диска набора должны быть подключены. Зеркальный набор должен находиться в состоянии **Отказавшая избыточность (Failed Redundancy)**. Требующееся корректирующее воздействие зависит от статуса неисправного тома:

- Если том находится в состоянии **Отсутствует (Missing)** или **Не подключен (Offline)**, проверьте питание диска и правильность подключения. Затем откройте оснастку **Управление дисками (Disk Management)**, щелкните правой кнопкой сбойный том и выберите команду **Реактивизировать том (Reactivate Volume)**. Состояние диска должно измениться на **Регенерация (Regenerating)**, а затем — на **Исправен (Healthy)**. Если диск не переходит в состояние **Исправен (Healthy)**, щелкните том правой кнопкой и выберите команду **Ресинхронизация зеркала (Resynchronize Mirror)**.
- Если диск находится в состоянии **Работает (ошибки) (Online (Errors))**, щелкните том правой кнопкой и выберите команду **Реактивизировать том**

(Reactivate Volume). Состояние диска должно измениться на **Регенерация (Regenerating)**, а затем — на **Исправен (Healthy)**. Если диск не переходит в состояние **Исправен (Healthy)**, щелкните том правой кнопкой и выберите команду **Ресинхронизация зеркала (Resynchronize Mirror)**.

- Если один из дисков находится в состоянии **Не читается (Unreadable)**, выполните повторный поиск дисков в системе. Для этого в меню **Действие (Action)** оснастки **Управление дисками (Disk Management)** выберите команду **Повторить проверку дисков (Rescan Disks)**. Если состояние диска не изменится, перезагрузите компьютер.
- Если один из дисков так и не удается подключить, щелкните неисправный том правой кнопкой и выберите команду **Удалить зеркало (Remove Mirror)**. Далее щелкните правой кнопкой оставшийся том и выберите команду **Добавить зеркало (Add Mirror)**. Затем отобразите том на нераспределенную область свободного пространства. При отсутствии свободного пространства придется его создать, удалив другие тома или заменив неисправный диск.

Восстановление зеркалированного системного тома

Неисправность зеркального накопителя может помешать загрузке системы. Как правило, это случается, когда вы создаете зеркальные копии системного, загрузочного или обоих томов и первичный зеркальный том выходит из строя. В предыдущих версиях ОС Windows для восстановления системы требовалось выполнить несколько процедур. В Windows Server 2008, в большинстве случаев, вопрос неисправности первичного зеркала решается гораздо проще.

Во время создания зеркальной копии системного тома ОС должна добавить запись в **Диспетчер загрузки (Boot Manager)**, которая позволит загружаться со вторичного зеркала. Благодаря этой записи неисправность первичного зеркала намного легче устранить. Все, что от вас требуется, это выбрать загрузку со вторичного зеркала. Если во время зеркального копирования загрузочного тома запись о вторичном зеркале не была создана, вы можете создать ее при помощи BCD Editor (bcdedit.exe).

Если вам не удается загрузить систему с первичного системного тома, перезагрузите систему и выберите вариант загрузки **Вторичный плекс загрузочного зеркального тома (Boot Mirror – Secondary Plex)** для ОС, которую вы хотите запустить. Система должна начать работать нормально. После успешной загрузки системы со вторичного диска вы, при желании, можете запланировать мероприятия по восстановлению зеркала. Вам потребуется выполнить следующие действия:

1. Завершите работу системы и замените сбойный диск или добавьте новый. Перезапустите систему.
2. Разделите зеркальный набор и вновь создайте зеркало на замененном диске. Как правило, это диск 0. Щелкните правой кнопкой оставшийся

диск, который был частью первоначального зеркала, и выберите команду **Добавить зеркало (Add Mirror)**. Затем следуйте инструкциям из раздела «Создание зеркала существующего тома» этой главы.

3. Если вы хотите, чтобы первичное зеркало располагалось на добавленном или замененном диске, снова разделите зеркальный набор в оснастке **Управление дисками (Disk Management)**. Убедитесь, что буква первичного диска первоначального набора зеркал соответствует букве, назначенной ранее всему зеркалу. В случае несоответствия назначьте нужную букву.
4. Щелкните правой кнопкой первоначальный системный том и выберите команду **Добавить зеркало (Add Mirror)**. Теперь создайте зеркало повторно.
5. Проверьте файл Boot.ini и убедитесь, что загрузка системы производится с оригинального системного тома. Для этого вам может понадобиться отредактировать файл Boot.ini.

Удаление набора зеркал

Оснастка Управление дисками (Disk Management) позволяет удалять тома из набора зеркал. На удаляемом зеркале стираются все данные, а занимаемое им место помечается как нераспределенное.

Чтобы удалить зеркало, выполните следующие действия:

1. В оснастке Управление дисками (Disk Management) щелкните правой кнопкой один из томов зеркального набора и выберите команду **Удалить зеркало (Remove Mirror)**. Откроется одноименное диалоговое окно.
2. Выберите диск, с которого следует удалить том.
3. Подтвердите выбранное действие. Произойдет стирание всех данных удаляемого зеркала.

Восстановление чередующегося набора без контроля четности

Чередующийся набор дисков без контроля четности не обладает отказоустойчивостью. В случае неисправности диска, входящего в состав чередующегося набора, выходит из строя весь набор. Прежде чем предпринять попытку восстановления чередующегося набора, исправьте или замените сбойный диск. Затем потребуется заново создать чередующийся набор и восстановить содержавшиеся в нем данные из резервной копии.

Восстановление чередующегося набора с контролем четности

Технология RAID 5 позволяет восстанавливать чередующийся набор с контролем четности в случае выхода из строя одного из дисков. О неисправности одного из дисков набора вы узнаете по изменившемуся состоянию набора — **Отказавшая избыточность (Failed Redundancy)**. Состояние отдельного тома изменится на **Отсутствует (Missing)**, **Не подключен (Offline)** или **Работает (ошибки) (Online (Errors))**.

Для восстановления набора RAID 5 должны использоваться диски с идентичным типом разделов — MBR или GPT. Все диски RAID-5 должны быть подключены. Набор должен находиться в состоянии **Отказавшая избыточность (Failed Redundancy)**. Требуемое действие зависит от состояния неисправного тома:

- Если диск находится в состоянии **Отсутствует (Missing)** или **Не подключен (Offline)**, проверьте питание диска и правильность подключения. Затем откройте оснастку **Управление дисками (Disk Management)**, щелкните правой кнопкой сбойный том и выберите команду **Реактивизировать том (Reactivate Volume)**. Состояние диска должно измениться на **Регенерация (Regenerating)**, а затем на **Исправен (Healthy)**. Если диск не переходит в состояние **Исправен (Healthy)**, щелкните том правой кнопкой и выберите команду **Восстановить четность (Regenerate Parity)**.
- Если диск находится в состоянии **Работает (ошибки) (Online (Errors))**, щелкните том правой кнопкой и выберите команду **Реактивизировать том (Reactivate Volume)**. Состояние диска должно измениться на **Регенерация (Regenerating)**, а затем на **Исправен (Healthy)**. Если диск не переходит в состояние **Исправен (Healthy)**, щелкните том правой кнопкой и выберите команду **Восстановить четность (Regenerate Parity)**.
- Если один из дисков находится в состоянии **Не читается (Unreadable)**, выполните повторный поиск дисков в системе. Для этого в меню **Действие (Action)** оснастки **Управление дисками (Disk Management)** выберите команду **Повторить проверку дисков (Rescan Disks)**. Если состояние диска не изменится, перезагрузите компьютер.
- Если один из дисков так и не удается подключить, требуется исправить сбойный участок набора RIAD 5. Щелкните правой кнопкой неисправный том и выберите команду **Удалить том (Remove Volume)**. Теперь выберите нераспределенный участок для набора RAID 5 на отдельном динамическом диске. Размер участка должен быть, по меньшей мере, равен размеру сбойного участка и не может находиться на диске, уже используемом в наборе RAID 5. Если свободного места недостаточно, команда **Восстановить том (Repair Volume)** будет недоступна, и вам придется освободить место, удалив другие тома или заменив накопитель.

Совет По возможности перед выполнением этой процедуры создайте резервные копии данных. Они обеспечат возможность восстановления данных, если что-то пойдет не так.

Управление номерами LUN в сетях хранения данных

Логический номер устройства (LUN) — это логическая ссылка на часть подсистемы хранилища в сетях хранения данных (SAN). Номера LUN очень похожи на тома, поскольку используются для обозначения всего диска или его части, а также для обозначения всего дискового массива или его части. По

аналогии с томами, для каждого LUN можно организовать доступ и управлять полномочиями.

Как и тома, номера LUN делятся на несколько видов:

- **Простой** Занимает один физический диск или часть физического диска.
- **Составной** Охватывает несколько физических дисков.
- **Чередующийся** Записывает данные на несколько физических дисков. Чередующиеся LUN не обладают отказоустойчивостью, их невозможно расширить или создать зеркальную копию. Выход из строя одного из дисков, содержащих чередующийся LUN, приводит к отказу всего LUN.
- **Зеркальный** Отказоустойчивый LUN, обеспечивающий избыточность данных путем создания идентичных копий LUN на двух физических дисках. В случае неисправности одного из физических дисков данные на неисправном диске становятся недоступны, однако LUN будет доступен за счет исправного диска.
- **Чередующийся с контролем четности** Отказоустойчивый LUN, в котором данные пользователя и данные о четности по очереди распределяются по трем или более физическим дискам. С выходом из строя части физического диска, вы можете восстановить данные, имевшиеся на сбойной части, по оставшимся данным и информации о четности.

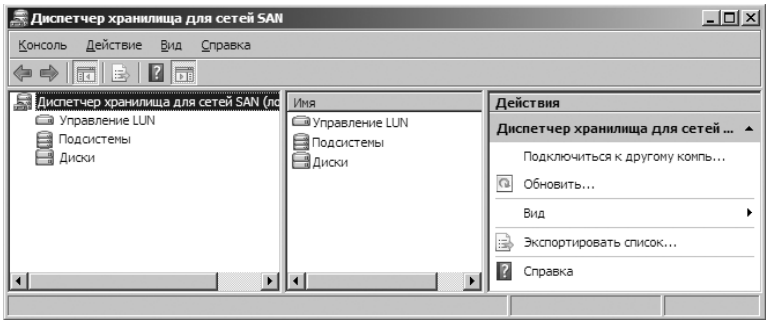


Рис. 13-6. Управление протоколами Fibre Channel и iSCSI SANs при помощи Диспетчера хранилища для сетей SAN (Storage Manager For SANs)

В Windows Server 2008 имеется консоль **Диспетчер хранилища для сетей SAN (Storage Manager For SANs)**, показанная на рис. 13-6. Она служит для управления сетями SAN на базе протоколов Fibre Channel и Internet Small Computer System Interface (iSCSI), которые поддерживают службу виртуальных дисков (VDS) и обладают настроенным поставщиком оборудования VDS. Чтобы работать с этой консолью, на сервер следует добавить компонент Диспетчер хранилища для сетей SAN (Storage Manager For SANs) при помощи Мастера добавления компонентов (Add Features Wizard). Чтобы открыть консоль, выберите соответствующую команду в меню **Администрирование (Administrative Tools)** или разверните узел **Хранилище (Storage)** консоли **Диспетчер сервера (Server Manager)** и щелкните узел **Диспетчер хранилища для сетей SAN (Storage Manager For SANs)**.

Настройка подключения к SAN по протоколу Fibre Channel

В сетях хранения данных на базе протокола Fibre Channel сервер, подключенный к SAN, получает доступ к LUN непосредственно через один или несколько портов адаптеров главной шины (host bus adapter, HBA). Поэтому от вас требуется только идентифицировать сервер, который будет обращаться к LUN, а затем определить, какие HBA-порты этого сервера будут использоваться для трафика LUN. Когда вы указываете сервер, консоль **Диспетчер хранилища для сетей SAN (Storage Manager For SANs)** пытается автоматически обнаружить на нем доступные HBA-порты Fibre Channel. Можно также добавлять порты вручную, используя их WWN-имена.

Чтобы добавить и настроить сервер с подключениями по протоколу Fibre Channel, выполните следующие действия:

1. В консоли **Диспетчер хранилища для сетей SAN (Storage Manager For SANs)** выделите узел **Управление LUN (LUN Management)**. В области действий или в меню **Действие (Action)** выберите команду **Управление подключениями сервера (Manage Server Connections)**.
2. В диалоговом окне **Управление подключениями сервера (Manage Server Connections)** щелкните **Добавить (Add)**.
3. В диалоговом окне **Добавление сервера (Add Server)** введите имя или IP-адрес добавляемого сервера. Вы можете также осуществить поиск сервера.
4. При необходимости введите описание сервера.
5. Щелкните **OK**. Теперь сервер должен отображаться в окне консоли. Все найденные автоматически порты перечислены на вкладке **Порт оптоволоконного канала (Fibre Channel Ports)**.

Чтобы вручную добавить порт, выполните следующие действия:

1. В консоли **Диспетчер хранилища для сетей SAN (Storage Manager For SANs)** выделите узел **Управление LUN (LUN Management)**. В области действий или в меню **Действие (Action)** выберите команду **Управление подключениями сервера (Manage Server Connections)**.
2. Выделите в списке ранее настроенный сервер. На вкладке **Порт оптоволоконного канала (Fibre Channel Ports)** щелкните **Добавить (Add)** и введите WWN-имя нового порта.
3. При необходимости введите описание нового порта.
4. Щелкните **OK**.

Чтобы открыть порты Fibre Channel для доступа к LUN, выполните следующие действия:

1. В консоли **Диспетчер хранилища для сетей SAN (Storage Manager For SANs)** выделите узел **Управление LUN (LUN Management)**. В области действий или в меню **Действие (Action)** выберите команду **Управление подключениями сервера (Manage Server Connections)**.

2. Выберите в списке ранее настроенный сервер. На вкладке **Порт оптоволоконного канала (Fibre Channel Ports)** выделите порты, которые следует включить.
3. Щелкните **OK**.

Примечание Прежде чем выбрать несколько инициаторов, убедитесь, что на сервере настроен интерфейс многопутевого ввода-вывода. Отсутствие настройки многопутевого ввода-вывода может привести к повреждению данных.

Настройка подключения к SAN по протоколу iSCSI

При использовании протокола iSCSI номера LUN, создаваемые в подсистеме накопителя iSCSI, не назначаются непосредственно серверу. Они назначаются логическим объектам, которые называются *конечными объектами* (target). Конечные объекты служат для управления подключением между устройством iSCSI и сервером, которому нужно получить доступ к устройству. Конечный объект идентифицирует порталы IP-адресов, которые могут использоваться при подключении к устройству iSCSI, а также всех соответствующих параметров безопасности, которые требуются iSCSI-устройству для проверки подлинности серверов, запрашивающих доступ к ресурсам.

В основном, создание и управление конечными объектами производится вручную. Однако в некоторых сетях хранения данных iSCSI поддерживается только простая конфигурация, когда необходимые конечные объекты создаются автоматически во время создания LUN. При использовании простой конфигурации от вас требуется только идентифицировать сервер или серверы, которым нужен доступ к конкретному LUN.

Сервер, подключенный к сети SAN на базе iSCSI, получает доступ к LUN посредством инициатора iSCSI. После указания сервера, которому требуется доступ к LUN, консоль **Диспетчер хранилища для сетей SAN (Storage Manager For SANs)** пытается автоматически обнаружить инициатор iSCSI, который следует использовать для обмена данными, и перечисляет все адаптеры, доступные для конкретного инициатора. После этого вы указываете, какой адаптер следует использовать для LUN.

Чтобы добавить и настроить сервер с подключениями iSCSI, выполните следующие действия:

1. В консоли **Диспетчер хранилища для сетей SAN (Storage Manager For SANs)** выделите узел **Управление LUN (LUN Management)**. В области действий или в меню **Действие (Action)** выберите команду **Управление подключениями сервера (Manage Server Connections)**.
2. В диалоговом окне **Управление подключениями сервера (Manage Server Connections)** щелкните **Добавить (Add)**.
3. В диалоговом окне **Добавление сервера (Add Server)** введите имя или IP-адрес добавляемого сервера. Вы можете также осуществить поиск сервера.
4. При необходимости введите описание сервера.

5. Щелкните **OK**. Теперь сервер должен отображаться в окне консоли. Все найденные автоматически инициаторы перечислены на вкладке **Адаптеры-инициаторы (Initiator Adapters)**.

Чтобы включить адаптеры инициатора iSCSI для доступа к LUN, выполните следующие действия:

1. В консоли **Диспетчер хранилища для сетей SAN (Storage Manager For SANs)** выделите узел **Управление LUN (LUN Management)**. В области действий или в меню **Действие (Action)** выберите команду **Управление подключениями сервера (Manage Server Connections)**.
2. Выберите в списке ранее настроенный сервер. На вкладке **Адаптеры-инициаторы (Initiator Adapters)** выберите адаптеры, которые следует включить.

Примечание Прежде чем выбрать несколько инициаторов, убедитесь, что на сервере настроен интерфейс многопутевого ввода-вывода. Отсутствие многопутевого ввода-вывода может привести к повреждению данных.

3. Щелкните **OK**.

Добавление и удаление конечных объектов

Работая с iSCSI, вы можете выполнять разнообразные задачи в разделе **Управление конечными объектами iSCSI (Manage iSCSI Targets)**. В консоли Диспетчер хранилища для сетей SAN (Storage Manager For SANs) выделите узел **Управление LUN (LUN Management)**. В области действий или в меню **Действие (Action)** выберите команду **Управление конечными объектами iSCSI (Manage iSCSI Targets)**. Выбрав подсистему, которой вы хотите управлять, вы сможете сделать следующее:

- Щелкните **Добавить (Add)**, чтобы добавить конечный объект iSCSI. В диалоговом окне **Добавление конечного объекта (Add Target)** введите понятное имя для объекта, выберите порталы IP-адресов, которые следует включить для конечного объекта, и щелкните **OK**.
- Выберите существующий конечный объект iSCSIи щелкните **Удалить (Remove)**, чтобы удалить его. В диалоговом окне **Удаление конечного объекта (Remove Target)** подтвердите удаление, установив соответствующий флажок и щелкнув **OK**.

Создание, расширение, назначение и удаление LUN

Настроив требуемые подключения SAN, можете выполнять различные действия в разделе **Управление подключениями сервера (Manage Server Connections)**. В консоли **Диспетчер хранилища для сетей SAN (Storage Manager For SANs)** выделите узел **Управление LUN (LUN Management)**. В области действий или в меню **Действие (Action)** выберите команду **Управление подключениями сервера (Manage Server Connections)**. После этого вы сможете выполнить следующие действия:

- Щелкните **Создать LUN (Create LUN)**, чтобы запустить Мастер создания нового LUN (Create LUN Wizard). Здесь вы сможете выбрать подсис-

тему, для которой следует создать LUN, а также указать тип, размер и имя LUN. При необходимости вы можете назначить LUN конечному объекту, серверу или кластеру, а также указать тип форматирования тома LUN. По окончанию настройки щелкните **Создать LUN (Create LUN)**, чтобы запустить процесс создания LUN.

- Откройте меню **Действие (Action)** и выберите команду **Расширить LUN (Extend LUN)**. В открывшемся диалоговом окне вы сможете ввести новый размер LUN.
- Откройте меню **Действие (Action)** и выберите команду **Назначить LUN (Assign LUN)**, чтобы запустить Мастер назначения LUN (Assign LUN Wizard). Здесь вы сможете выбрать сервер, конечный объект или кластер, которому нужно назначить LUN. Щелкните **Назначить LUN (Assign LUN)** для завершения процесса.
- Откройте меню **Действие (Action)** и выберите команду **Удалить LUN (Delete LUN)**. Подтвердите удаление LUN, установив соответствующий флажок и щелкнув **OK**.

Определение серверных кластеров в Диспетчере хранилища для сетей SAN (Storage Manager For SANs)

Доступ к LUN может получить и группа серверов, объединенных в кластер. Кластеры определяются в консоли **Диспетчер хранилища для сетей SAN (Storage Manager For SANs)**. Кроме того, на каждом сервере кластера необходимо включить службы кластеризации. Каждый сервер должен быть членом только одного кластера. Создав кластер, вы можете назначить кластеру LUN так же, как вы назначали LUN отдельным серверам.

Чтобы определить кластер серверов в **консоли Диспетчер хранилища для сетей SAN (Storage Manager For SANs)**, выполните следующие действия:

1. В консоли **Диспетчер хранилища для сетей SAN (Storage Manager For SANs)** выделите узел **Управление LUN (LUN Management)**. В области действий или в меню **Действие (Action)** выберите команду **Управление подключениями сервера (Manage Server Connections)**.
2. В диалоговом окне **Управление подключениями сервера (Manage Server Connections)** щелкните **Управление кластерами (Manage Clusters)**.
3. В диалоговом окне **Управление кластерами (Manage Clusters)** щелкните **Добавить (Add)**.
4. Введите имя кластера или общее описание, с помощью которого его можно будет распознать.
5. В списке серверов выберите все серверы, которые хотите включить в кластер.
6. Щелкните **OK**, чтобы создать новый кластер. Затем еще раз щелкните **OK**.

Теперь, новый кластер будет отображен в списке **Управление подключениями сервера (Manage Server Connections)**. Назначьте кластеру LUN, как описано ранее в этой главе.

Глава 14

Блокировка файлов и отчеты хранилищ

Система Windows Server 2008 — надежная среда для работы с файлами и папками. Как правило, для обеспечения управляемости и гибкости тома форматируются в NTFS, что открывает множество дополнительных возможностей, включая блокировку файлов и отчеты хранилищ. Чтобы воспользоваться этими возможностями, добавьте на сервер службу роли Диспетчер ресурсов файлового сервера (File Server Resource Manager), входящую в состав роли Файловые службы (File Services).

Введение в блокировку файлов и отчеты хранилищ

Блокировка файлов (file screening) предназначена для защиты сетей от вредоносных программ и несанкционированных типов содержимого. Файловые фильтры можно использовать в сочетании с квотами и отчетами хранилищ, о чем подробно говорится в главе 15. Фильтры позволяют отслеживать и блокировать использование определенных типов файлов. Существует два режима блокировки файлов:

- **Активная блокировка** Пользователям не разрешается сохранять файлы несанкционированных типов.
- **Пассивная блокировка** Пользователям разрешено сохранять файлы несанкционированных типов, однако эти действия отслеживаются и (или) сопровождаются предупреждениями об их использовании.

Активная и пассивная блокировка файлов осуществляется посредством определения файловых фильтров. С каждым фильтром сопоставлен *путь фильтра блокировки файлов* — папка, определяющая основной путь, к которому применяется фильтр. Блокировка применяется к данной папке и всем ее подпапкам. Детали работы и параметры фильтра выводятся из исходного шаблона, определяющего свойства блокировки.

Шаблоны имеющихся в Windows Server 2008 фильтров перечислены в табл. 14-1. Диспетчер ресурсов файлового сервера (File Server Resource Manager) позволяет без труда определять дополнительные шаблоны. Кроме того, вы вольны задать индивидуальный фильтр, предназначенный для одного пользователя.

Табл. 14-1. Шаблоны файловых фильтров

Название шаблона	Тип блокировки	Действие
Блокировать исполняемые файлы (Block Executable Files)	Активная	Блокирует исполняемые файлы
Блокировать файлы аудио и видео (Block Audio And Video Files)	Активная	Блокирует аудио- и видео-файлы
Блокировать файлы изображений (Block Image Files)	Активная	Блокирует файлы изображений
Блокировать файлы электронной почты (Block E-Mail Files)	Активная	Блокирует файлы электронной почты
Отслеживать выполняемые и системные файлы (Monitor Executable And System Files)	Пассивная	Предупреждает об исполняемых и системных файлах

При помощи шаблонов или вручную вы задаете следующие параметры:

- тип блокировки (активная или пассивная);
- группы файлов, к которым применяется фильтр;
- способ уведомления (сообщение электронной почты, запись в журнале событий, запуск команды, отчете, а также любая комбинация).

В табл. 14-2 приведены стандартные группы файлов, к которым применяются фильтры. При помощи **Диспетчера ресурсов файлового сервера (File Server Resource Manager)** вы можете изменять имеющиеся типы файлов и или создавать собственные группы файлов.

Табл. 14-2. Группы блокируемых файлов и включенные в них типы файлов

Группа файлов	Включенные расширения
Аудио- и видео-файлы	.aac, .aif, .aifft, .asf, .asx, .au, .avi, .flac, .m3u, .mid, .midi, .mov, .mp1, .mp2, .mp3, .mp4, .mpa, .mpe, .mpeg, .mpeg2, .mpeg3, .mpg, .ogg, .qt, .qtw, .ram, .rm, .rmi, .rmvb, .snd, .swf, .vob, .wav, .wax, .wma, .wmv, .wvx
Временные файлы	.temp, .tmp, ~*
Исполняемые файлы	.bat, .cmd, .com, .cpl, .exe, .inf, .js, .jse, .msh, .msi, .msp, .ocx, .pif, .pl, .scr, .vb, .vbs, .wsf, .wsh
Резервные копии	.bak, .bck, .bkf, .old
Сжатые файлы	.ace, .arc, .arj, .bhx, .bz2, .cab, .gz, .gzip, .hpk, .hqx, .jar, .lha, .lzh, .lzx, .pak, .pit, .rar, .sea, .sit, .sqz, .tgz, .uu, .uue, .z, .zip, .zoo
Системные файлы	.acm, .dll, .ocx, .sys, .vxd
Текстовые файлы	.asc, .text, .txt
Файлы Office	.doc, .dot, .mad, .maf, .mda, .mdb, .mdm, .mdt, .mdw, .mdz, .mpd, .mpp, .mpt, .pot, .ppa, .pps, .ppt, .pwz, .rqy, .rtf, .rwz, .slk, .vdx, .vsd, .vsl, .vss, .vst, .vsu, .vsw, .vsx, .vtx,.wbk, .wri, .xla, .xlb, .xlc, .xld, .xlk, .xll, .xlm, .xls, .xlt, .xlv, .xlw

Табл. 14-2. (*окончание*)

Группа файлов	Включенные расширения
Файлы веб-страниц	.asp, .aspx, .cgi, .css, .dhtml, .hta, .htm, .html, .mht, .php, .php3, .shtml, .url
Файлы изображений	.bmp, .dib, .eps, .gif, .img, .jfif, .jpe, .jpeg, .jpg, .pcx, .png, .ps, .psd, .raw, .rif, .spiff, .tif, .tiff
Файлы электронной почты	.eml, .idx, .mbox, .mbx, .msg, .ost, .otf, .pab, .pst

Вы также можете настраивать пути исключений и задавать конкретные расположения для сохранения блокируемых типов файлов. Можно разрешить отдельным пользователям сохранять блокируемые типы файлов в указанных расположениях или разрешить всем пользователям сохранять несанкционированные типы файлов в этих расположениях. Например, вы можете ограничить незаконную загрузку музыки и фильмов. Для этого достаточно запретить пользователям сохранять аудио- и видеофайлы. Однако, если в вашей организации есть отдел, работающий с аудио- и видеоматериалами, настройте исключение, разрешающее сохранение файлов в папке, доступ к которой имеют только члены данной группы.

Отчеты хранилищ создаются в рамках управления квотами и блокировкой файлов. В табл. 14-3 приведен обзор стандартных отчетов хранилища и решаемых ими задачах. Взяв за основу стандартные отчеты, вы создадите отчеты трех основных типов:

- **Отчеты об инцидентах** Создаются автоматически при попытке пользователя сохранить несанкционированный файл или при превышении пользователем квоты.
- **Запланированные отчеты** Создаются в соответствии с запланированным заданием
- **Отчеты по запросу** Создаются вручную, по требованию.

Табл. 14-3. Стандартные отчеты хранилища

Название отчета	Описание
Аудит блокировки файлов (File Screening Audit)	Список событий аудита блокировки файлов за определенный период. Помогает установить пользователей и приложения, нарушающие политики блокировки. Вы можете ограничить отчет по наименьшему количеству дней с момента блокировки, а также по пользователям
Большие файлы (Large Files)	Список файлов указанного размера или большего. Помогает установить файлы, занимающие большие объемы дискового пространства. Вы можете задать минимальный размер файла, при котором он считается большим. По умолчанию большими считаются файлы размером более 5 Мб. Можно также включать и исключать файлы по шаблону имени

Табл. 14-3. (*окончание*)

Название отчета	Описание
Давно не открывавшиеся файлы (Least Recently Accessed Files)	Список файлов, к которым давно не осуществлялся доступ. Помогает установить файлы, которые можно удалить или отправить в архив. Вы можете задать, какие файлы следует считать давно неиспользуемыми. По умолчанию давно неиспользуемым файлом считается любой файл, обращение к которому не производилось за последние 90 дней. Можно также включать и исключать файлы по шаблону имени
Использование квоты (Quota Usage)	Список квот, превысивших минимальное значение использования квот. Помогает определить использование файлов по квотам. Вы можете задать квоты, которые следует включать в отчет, в соответствии с процентом использованного лимита
Недавно открывавшиеся файлы (Most Recently Accessed Files)	Список файлов, доступ к которым осуществлялся недавно. Помогает выявить часто используемые файлы. Вы можете задать, какие файлы следует считать последними по времени использования. По умолчанию таковым считается любой файл, обращение к которому производилось за последние семь дней. Можно включать и исключать файлы по шаблону имени
Файлы по владельцам (Files By Owner)	Список файлов по владельцам. Помогает установить пользователей, использующих много дискового пространства. Вы можете задать параметры, позволяющие включать и исключать отдельных пользователей, а также файлы по шаблону имени
Файлы по группам (Files By File Group)	Список файлов по группам. Помогает установить закономерности использования и типы файлов, занимающих большие объемы дискового пространства. Вы можете задать параметры, позволяющие включать и исключать отдельные группы файлов
Файлы-дубликаты (Duplicate Files)	Список файлов, которые кажутся дубликатами исходя из размера файла и времени последнего изменения. Помогает избежать лишних трат дискового пространства из-за дублирования

Управление блокировкой файлов и отчетами хранилища осуществляется при помощи диспетчера ресурсов файлового сервера. Эта консоль устанавливается и запускается из меню **Администрирование (Administrative Tools)** после добавления на сервер службы роли Диспетчер ресурсов файлового сервера (File Server Resource Manager) в составе роли Файловые службы (File Services). Выбрав корневой узел консоли **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**, вы увидите на экране три дополнительных узла (рис. 14-1):

- **Управление квотами (Quota Management)** Используется для управления квотами Windows Server 2008 (подробнее — в главе 15).
- **Управление блокировкой файлов (File Screening Management)** Используется для управления блокировкой файлов.
- **Управление ресурсами хранилища (Storage Reports Management)** Используется для управления отчетами хранилища Windows Server 2008.

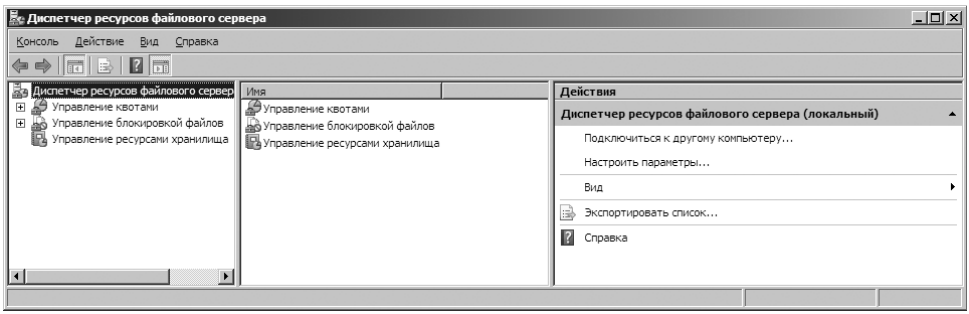


Рис. 14-1. Диспетчер ресурсов файлового сервера (File Server Resource Manager) используется для управления квотами, блокировкой и отчетами

Управление блокировкой файлов и отчетами

Параметры управления блокировкой и отчетами можно разделить на следующие ключевые области:

- **Глобальные параметры** Уведомления по электронной почте, стандартные параметры отчета хранилища, расположение отчетов и аудит блокировки файлов.
- **Группы файлов** Типы файлов, к которым применяются ограничения.
- **Шаблоны блокировки файлов** Свойства фильтров: тип блокировки (активный или пассивный), группы файлов, к которым применяются ограничения, уведомления (электронная почта, журнал событий или и то, и другое).
- **Пути блокировки файлов** Пути, к которым применяется блокировка.
- **Исключения блокировки файлов** Пути, к которым не применяются файловые фильтры.
- **Генерация отчетов** Параметры создания отчетов хранилища.

В следующих разделах обсуждается каждая из этих областей.

Глобальные параметры файловых ресурсов

Глобальные параметры файловых ресурсов применяются для настройки уведомлений по электронной почте, стандартных параметров отчетов, расположения отчетов и аудита блокировки файлов. Глобальные параметры следует настраивать перед настройкой квот, фильтров и отчетов.

Настройка уведомлений по электронной почте

Уведомления и отчеты хранилища передаются через SMTP-сервер. Чтобы этот процесс работал, вы должны указать, какой SMTP-сервер следует использовать, задать получателей-администраторов по умолчанию, а также адрес отправителя для уведомлений и отчетов. Чтобы настроить эти параметры, выполните следующие действия:

1. Откройте консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**. В меню **Действие (Action)** или в области действий щелкните команду **Настроить параметры (Configure Options)**. Откроется диалоговое окно **Параметры диспетчера ресурсов файлового сервера (File Server Resource Manager Options)**. По умолчанию окно открыто на вкладке **Уведомления (Email Notifications)**, показанной на рис. 14-2.

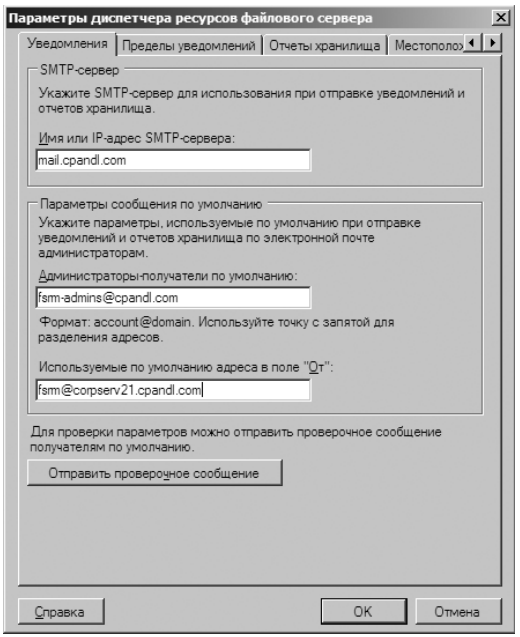


Рис. 14-2. Настройка почтовых уведомлений и других глобальных параметров на вкладке Уведомления (Email Notifications)

2. В поле **Имя или IP-адрес SMTP-сервера (SMTP Server Name Or IP Address)** введите FQDN-имя почтового сервера организации, например, mail.cpandl.com, или IP-адрес этого сервера, например, **192.168.10.52**.
3. В поле **Администраторы-получатели по умолчанию (Default Administrator Recipients)** введите адрес электронной почты администратора для получения уведомлений, например, filescreens@cpandl.com. Обычно это специальный почтовый ящик, просматриваемый администратором или группой распространения, которая выполняет особую административную функцию — управление ресурсами файлового сервера. При необхо-

димости введите несколько адресов электронной почты. Не забывайте отделять их друг от друга точкой с запятой.

4. В поле **Используемые по умолчанию адреса в поле «От» (Default «From» E-Mail Address)** введите адрес электронной почты, который будет использован сервером в качестве обратного адреса. Помните, что получать уведомления могут не только администраторы, но и обычные пользователи.
5. Чтобы протестировать параметры, щелкните **Отправить проверочное сообщение (Send Test E-Mail)**. Тестовое сообщение будет доставлено указанным получателям почти мгновенно. Если этого не произошло, проверьте используемые адреса получателей, а также допустимость обратного адреса на используемом SMTP-сервере.
6. Щелкните **OK**.

Настройка пределов для уведомлений

В случае превышения квоты или обнаружения несанкционированного файла консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** посылает администраторам уведомление одним из следующих образов:

- Отправка сообщения электронной почты пользователю, который пытался сохранить несанкционированный файл, администратору или и тому, и другому.
- Запись предупреждения в журнал событий.
- Выполнение команды от имени учетной записи Local Service, Network Service или Локальная система (Local System).
- Создание одного или нескольких отчетов об уведомлении с возможной отправкой отчетов по электронной почте.

Чтобы сократить количество уведомлений, задайте предельные временные промежутки между уведомлениями, касающимися одного и того же события. Стандартные интервалы уведомлений составляют по одному часу для уведомления по электронной почте, для записей в журнале событий, для запуска команды и для генерации отчета.

Чтобы настроить пределы уведомлений, выполните следующие действия:

1. Откройте консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**. В меню **Действие (Action)** или в области действий щелкните **Настроить параметры (Configure Options)**.
2. В диалоговом окне **Параметры диспетчера ресурсов файлового сервера (File Server Resource Manager Options)** перейдите на вкладку **Пределы уведомлений (Notification Limits)**.
3. Настройте пределы для следующих типов уведомлений:
   - **Уведомление почты (Email Notification)** Интервал между уведомлениями по электронной почте.
   - **Уведомление журнала событий (Event Log Notification)** Интервал между уведомлениями, записываемыми в журнал событий.

- **Уведомление команды (Command Notification)** Интервал между запусками команды.
- **Уведомление отчета (Report Notification)** Интервал между генерацией отчетов.

4. Щелкните **OK**.

Просмотр отчетов и настройка параметров отчета хранилища

Каждый отчет хранилища имеет стандартную конфигурацию, параметры которой можно изменить в диалоговом окне **Параметры диспетчера ресурсов файлового сервера (File Server Resource Manager Options)**. Изменения, внесенные в эти параметры, применяются ко всем будущим отчетам, использующим стандартную конфигурацию. При необходимости вы вольны перекрыть стандартные параметры, запланировав создание отчета по расписанию или создавая отчет по запросу.

Чтобы изменить параметры стандартных отчетов хранилища, выполните следующие действия:

1. Откройте консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**. В меню **Действие (Action)** или в области действий щелкните **Настроить параметры (Configure Options)**.
2. В диалоговом окне **Параметры диспетчера ресурсов файлового сервера (File Server Resource Manager Options)** перейдите на вкладку **Отчеты хранилища** (**Storage Reports**).
3. Чтобы познакомиться с текущими параметрами отчета, выделите имя отчета в списке **Отчеты (Reports)** и щелкните **Просмотреть отчеты (Review Reports)**.
4. Чтобы изменить стандартные параметры отчета, выделите имя отчета в списке **Отчеты (Reports)** и щелкните **Изменить параметры (Edit Parameters)**.
5. Завершив работу, щелкните **Закрыть (Close)** или **OK**.

Настройка расположения отчетов

По умолчанию отчеты об инцидентах, запланированные отчеты и отчеты по запросу хранятся на целевом сервере в отдельных подпапках папки %SystemDrive%\StorageReports. Чтобы изменить это правило, выполните следующие действия:

1. Откройте консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**. В меню **Действие (Action)** или в области действий щелкните команду **Настроить параметры (Configure Options)**.
2. В диалоговом окне **Параметры диспетчера ресурсов файлового сервера (File Server Resource Manager Options)** перейдите на вкладку **Местоположения отчетов (Report Locations)**.
3. Настроенные в данный момент папки отчетов перечислены в разделе **Местоположения отчетов (Report Locations)**. Чтобы указать другую

локальную папку для отчетов конкретного типа, введите новый путь или щелкните **Обзор (Browse)**, чтобы найти нужную папку.

4. Щелкните **OK**.

Примечание Для хранения отчетов можно использовать только локальные папки. Нелокальные пути будут считаться недействительными.

Настройка аудита блокировки файлов

У вас есть возможность записывать все действия, предпринимаемые файловыми фильтрами, в БД аудита, чтобы позже их можно было просмотреть в отчете Аудит блокировки файлов (File Screen Auditing Report). Данные аудита отслеживаются на каждом сервере. Чтобы включить или выключить аудит блокировки файлов, выполните следующие действия:

1. Откройте консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**. В меню **Действие (Action)** или в области действий щелкните команду **Настроить параметры (Configure Options)**.
2. В диалоговом окне **Параметры диспетчера ресурсов файлового сервера (File Server Resource Manager Options)** перейдите на вкладку **Аудит фильтра блокировки файлов (File Screen Audit)**.
3. Чтобы включить аудит, установите флажок **Записывать операции по блокировке файлов в базу данных аудита (Record File Screening Activity In Auditing Database)**. Чтобы отключить аудит, сбросьте этот флажок.
4. Щелкните **OK**.

Управление группами файлов для применения фильтров

Файловые группы используются для объединения сходных типов файлов, к которым должны применяться блокировки. Консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** позволяет просматривать текущие группы файлов. Для этого нужно развернуть узлы **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** и **Управление блокировкой файлов (File Screening Management)**, а затем выбрать **Группы файлов (File Groups)**. Стандартные группы файлов и входящие в них типы файлов приведены в табл. 14-2.

Чтобы изменить существующие группы файлов, выполните следующие действия:

1. Откройте консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**. Разверните узлы **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** и **Управление блокировкой файлов (File Screening Management)**, а затем выберите **Группы файлов (File Groups)**. Появится список определенных в данный момент групп, а также включенных и исключенных файлов.
2. Чтобы изменить свойства группы, дважды щелкните ее имя . Откроется диалоговое окно свойств, показанное на рис. 14-3.

3. В текстовом поле **Включить файлы (Files To Include)** введите расширение файла, для которого следует организовать блокировку, например, **.pdf**. Либо введите шаблон имени файла, например, **Archive*.***. Щелкните **Добавить (Add)**. Повторите эти действия, чтобы задать блокировки для других типов файлов.
4. В текстовом поле **Исключить файлы (Files To Exclude)** введите расширение файла, для которого следует сделать исключение, например, **.doc**. Либо введите шаблон имени файла, например, **Report*.***. Щелкните **Добавить (Add)**. Повторите эти действия, чтобы указать другие типы файлов, для которых следует делать исключение.
5. Щелкните **OK**.

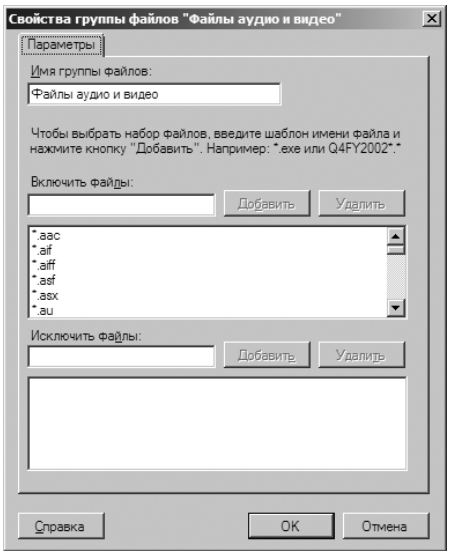


Рис. 14-3. Добавление и удаление типов файлов

Чтобы создать новую группу файлов для блокировки, выполните следующие действия:

1. Откройте консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**. Разверните узлы **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** и **Управление блокировкой файлов** (**File Screening Management**), а затем выберите **Группы файлов (File Groups)**.
2. В меню **Действие (Action)** или в области действий щелкните команду **Создать группу файлов (Create File Group)**. Откроется диалоговое окно **Создание свойств группы файлов (Create File Group Properties)**.
3. В поле **Имя группы файлов (File Group Name)** введите имя создаваемой группы файлов.
4. В текстовом поле **Включить файлы (Files To Include)** введите расширение файла, для которого следует организовать блокировку, например,

.pdf. Либо введите шаблон имени файла, например, **Archive*.***. Щелкните **Добавить (Add)**. Повторите эти действия, чтобы задать блокировки для других типов файлов.

5. В текстовом поле **Исключить файлы (Files To Exclude)** введите расширение файла, для которого следует сделать исключение, например, **.doc**. Либо введите шаблон имени файла, например, **Report*.***. Щелкните **Добавить (Add)**. Повторите эти действия, чтобы указать другие типы файлов, для которых следует делать исключение.
6. Щелкните **OK**.

Управление шаблонами фильтров блокировки

Шаблоны фильтров используются для определения свойств блокировки, в том числе, типа блокировки, группы файлов, к которым применяется блокировка, и уведомления. Чтобы просматривать текущие шаблоны блокировки в консоли **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**, разверните узлы **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** и **Управление блокировкой файлов (File Screening Management)**, а затем выберите элемент **Шаблоны фильтра блокировки файлов (File Screen Templates)**. Информация о стандартных шаблонах содержится в табл. 14-1.

Чтобы изменить существующие шаблоны блокировки, выполните следующие действия:

1. Откройте консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**. Разверните узлы **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** и **Управление блокировкой файлов (File Screening Management)**, а затем выберите **Шаблоны фильтра блокировки файлов (File Screen Templates)**. Появится список заданных шаблонов блокировки с именами, типами блокировки и группами файлов, к которым применяется блокировка.
2. Чтобы изменить свойства шаблона блокировки, дважды щелкните имя шаблона. Откроется диалоговое окно свойств, показанное на рис. 14-4.
3. На вкладке **Параметры (Settings)** задайте имя шаблона, тип блокировки и группы файлов, к которым применяется блокировка.
4. На вкладке **Сообщение электронной почты (E-mail Message)** настройте одно из следующих уведомлений:
   - Чтобы уведомлять администратора о срабатывании блокировки, установите флажок **Посылать сообщения следующим администраторам (Send E-Mail To The Following Administrators)** и введите адреса электронной почты. Не забывайте отделять адреса точками с запятой. Значение **[Admin Email]** используется для установки адреса администратора по умолчанию, ранее настроенного в глобальных параметрах.

- Чтобы уведомлять пользователей, установите флажок **Отправить сообщение пользователю, попытавшемуся сохранить несанкционированный файл (Send E-Mail To The User Who Attempted To Save An Unauthorized File)**. Затем в полях **Тема (Subject)** и **Текст сообщения (Message Body)** задайте содержание уведомления для пользователя. В табл. 14-4 приведены доступные переменные и их значения.

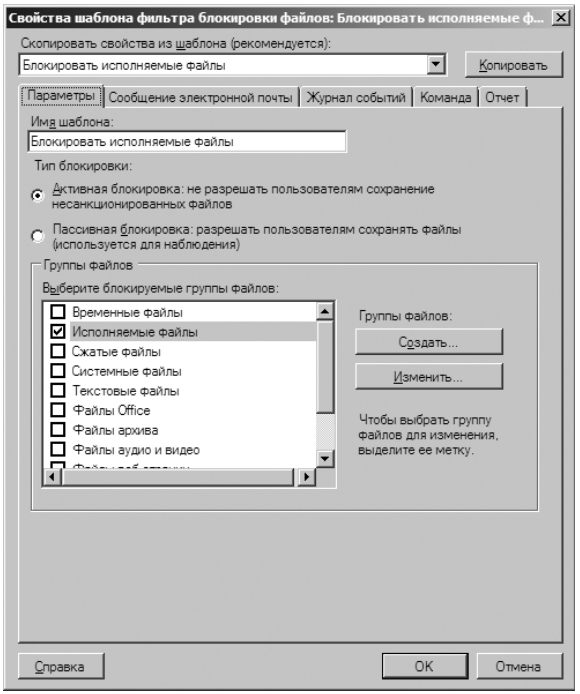


Рис. 14-4. Настройка типа блокировки, группы файлов, к которым она применяется, и способа уведомления

5. На вкладке **Журнал событий (Event Log)** задается запись событий в журнал. Установите переключатель **Записывать предупреждения в журнал (Send Warning To Event Log)**, чтобы включить запись событий. Текст записи задайте в поле **Запись журнала (Log Entry)** задайте текст записи в журнале. Доступные переменные и их значения приведены в табл. 14-4.
6. На вкладке **Отчет (Report)** установите флажок **Создать отчет (Generate Reports)**, чтобы включить создание отчетов о событиях. Установите флажки напротив нужных типов отчетов. Отчеты об инцидентах по умолчанию сохраняются в папке %SystemDrive%\StorageReports\Incident. Кроме того, их можно отправлять администраторам и пользователям, попытавшимся сохранить несанкционированный файл. Значение [Admin Email] используется для ввода адреса администратора по умолчанию, заданного в глобальных параметрах.
7. Щелкните **OK**.

Табл. 14-4. Переменные файловых фильтров

Имя переменной	Описание
[Admin Email]	Адрес электронной почты администраторов, заданный в глобальных параметрах
[File Screen Path]	Локальный путь, в котором пользователь попытался сохранить файл, например, C:\Data
[File Screen Remote Path]	Удаленный путь, в котором пользователь попытался сохранить файл, например, \\server\share
[File Screen System Path]	Канонический путь, в котором пользователь попытался сохранить файл, например, \\?\VolumeGUID
[Server Domain]	Домен сервера, на котором произошло событие
[Server]	Сервер, на котором произошло событие
[Source File Owner Email]	Адрес электронной почты владельца несанкционированного файла
[Source File Owner]	Имя владельца несанкционированного файла
[Source File Path]	Путь к несанкционированному файлу
[Source Io Owner Email]	Адрес электронной почты пользователя, действия которого привели к созданию уведомления
[Source Io Owner]	Имя пользователя, действия которого привели к созданию уведомления
[Source Process Id]	Идентификатор процесса (PID), приведшего к созданию уведомления
[Source Process Image]	Исполняемый файл процесса, который привел к созданию уведомления
[Violated File Group]	Имя группы файлов, в которой тип файла определен как несанкционированный

Чтобы создать новый файловый фильтр, выполните следующие действия:

1. Откройте консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**. Разверните узлы **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** и **Управление блокировкой файлов (File Screening Management)**, а затем выберите **Шаблоны фильтра блокировки файлов (File Screen Templates)**.
2. В меню **Действие (Action)** или в области действий щелкните команду **Создать шаблон фильтра блокировки файлов (Create File Screen Template)**. Откроется диалоговое окно **Создание шаблона фильтра блокировки файлов (Create File Screen Template)**.
3. Выполните шаги 4–8 из предыдущей процедуры.

Создание файловых фильтров

Фильтры блокировки файлов обозначают пути к файлам, к которым применяется блокировка. Консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** позволяет просматривать текущие файловые фильтры. Для этого нужно развернуть узлы **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** и **Управление блокировкой файлов (File Screening Management)**, а затем выбрать **Фильтры блокировки файлов (File Screens)**. Прежде чем определить файловые фильтры, следует указать группы и шаблоны блокировки, которые следует использовать. Об этом говорилось выше.

Определив необходимые группы и шаблоны, создайте фильтр блокировки, выполнив следующие действия:

1. Откройте консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**. Разверните узлы **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** и **Управление блокировкой файлов (File Screening Management)**, а затем выберите **Фильтры блокировки файлов (File Screens)**.
2. В меню **Действие (Action)** или в области действий щелкните команду **Создать фильтр блокировки файлов (Create File Screen)**.
3. В диалоговом окне **Создание фильтра блокировки файлов (Create File Screen)** введите путь фильтра на локальном компьютере или щелкните **Обзор (Browse)** и выберите путь в диалоговом окне **Обзор папок (Browse For Shared Folder)**.
4. В списке **Наследовать свойства (Derive Properties)** выберите шаблон, определяющий нужную вам блокировку.
5. Щелкните **Создать (Create)**.

Определение исключений для файловых фильтров

Пути исключений обозначают папки, в которых разрешено сохранять блокируемые типы файлов. Используя разрешения NTFS, вы можете разрешить отдельным или всем пользователям сохранять блокируемые типы файлов в указанных расположениях.

Чтобы создать исключение для файлового фильтра, выполните следующие действия:

1. Откройте консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**. Разверните узлы **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** и **Управление блокировкой файлов (File Screening Management)**, а затем выберите **Фильтры блокировки файлов (File Screens)**.
2. В меню **Действие (Action)** или в области действий щелкните команду **Создать исключение для фильтра блокировки файлов (Create File Screen Exception)**.

3. В диалоговом окне **Создание исключения для фильтра блокировки файлов (Create File Screen Exception)** задайте локальный путь или щелкните **Обзор (Browse)** и найдите путь исключения в диалоговом окне **Обзор папок (Browse For Folder)**.
4. Выберите группы файлов, с которых нужно снять блокировку в указанном пути.
5. Щелкните **OK**.

Планирование и создание отчетов хранилища

Отчеты об инцидентах создаются автоматически при наступлении определенного события, как задано на вкладке **Отчет (Report)** окна свойств шаблона файлового фильтра. Настройка запланированных отчетов и отчетов по запросу выполняется отдельно. Консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** позволяет просматривать текущие запланированные отчеты. Для этого нужно развернуть узел **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** и выбрать **Управление ресурсами хранилища (Storage Reports Management)**.

Чтобы запланировать отчеты для тома или папки, выполните следующие действия:

1. Откройте консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**. Разверните узлы **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** и **Управление ресурсами хранилища (Storage Reports Management)**.

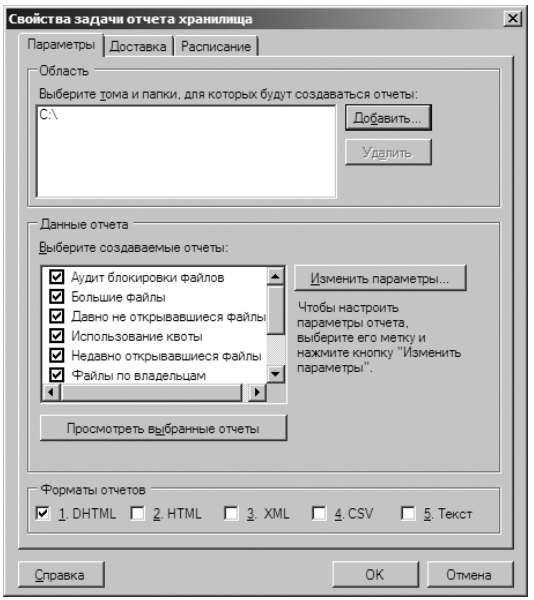


Рис. 14-5. Создание расписания отчетов для томов и папок

2. В меню **Действие (Action)** или в области действий щелкните команду **Запланировать новую задачу отчета (Schedule A New Report Task)**. Откроется диалоговое окно **Свойства задачи отчета хранилища (Storage Reports Task Properties)**, показанное на рис. 14-5.
3. На вкладке **Параметры (Settings)**, в разделе **Область (Scope)** щелкните **Добавить (Add)**. В диалоговом окне **Обзор папок (Browse For Folder)** выберите том или папку, для которых хотите создавать запланированные отчеты. Повторите действия, чтобы добавить другие тома или папки.
4. В разделе **Данные отчета (Report Data)** выберите создаваемые типы отчетов.
5. В разделе **Форматы отчетов (Report Formats)** выберите формат отчета, например, DHTML.
6. По умолчанию Windows Server 2008 сохраняет создаваемые запланированные отчеты о хранении в папке %SystemDrive%\StorageReports\Scheduled. Если вы хотите также доставлять отчеты администраторам по электронной почте, перейдите на вкладку **Доставка (Delivery)** и установите флажок **Посылать отчеты следующим администраторам (Send Reports To The Following Administrators)**. Введите адреса электронной почты, по которым следует доставлять отчеты, не забывая отделять их точкой с запятой.
7. На вкладке **Расписание (Schedule)** щелкните кнопку **Создать расписание (Create Schedule)**. В диалоговом окне **Расписание (Schedule)** щелкните **Создать (New)** и задайте время генерации отчетов.
8. Два раза щелкните **OK**.

Для создания отчета по запросу выполните следующие действия:

1. Откройте консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**. Разверните узлы **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** и **Управление ресурсами хранилища (Storage Reports Management)**.
2. В меню **Действие (Action)** или в области действий щелкните команду **Создать отчеты (Generate Reports Now)**. Откроется диалоговое окно **Свойства задачи отчета хранилища (Storage Reports Task Properties)**.
3. На вкладке **Параметры (Settings)**, в разделе **Область (Scope)** щелкните **Добавить (Add)**. В диалоговом окне **Обзор папок (Browse For Folder)** выберите том или папку, для которых хотите создавать запланированные отчеты. Повторите действия, чтобы добавить другие тома или папки.
4. В разделе **Данные отчета (Report Data)** выберите создаваемые типы отчетов.
5. В разделе **Форматы отчетов (Report Formats)** выберите формат отчета, например, DHTML.
6. По умолчанию Windows Server 2008 сохраняет создаваемые отчеты по запросу в папке %SystemDrive%\StorageReports\Interactive. Если вы хоти-

те также доставлять отчеты администраторам по электронной почте, перейдите на вкладку **Доставка (Delivery)** и установите флажок **Посылать отчеты следующим администраторам (Send Reports To The Following Administrators)**. Введите адреса электронной почты, по которым следует доставлять отчеты, не забывая отделять их точкой с запятой.

7. Щелкните **OK**. Укажите, нужно ли ожидать создания отчетов и затем отображать их, или же отчеты должны создаваться в фоновом режиме. Щелкните **OK**.

Глава 15

Общий доступ, безопасность и аудит

Microsoft Windows Server 2008 поддерживает две модели совместного использования файлов: обычный общий доступ и общий доступ к файлам из папки Общие (Public). Обычный общий доступ открывает удаленным пользователям доступ к ресурсам сети, например, файлам, папкам и дискам. Предоставляя общий доступ к папке или диску, вы делаете все содержащиеся в них файлы и подпапки доступными для определенного круга пользователей. При этом перемещение файлов из их текущего расположения не требуется.

Обычный общий доступ можно организовать на съемных носителях, форматированных в exFAT, FAT или FAT32, а также на любых дисках в формате NTFS. К съемным дискам в формате exFAT, FAT или FAT32 применяется единственный набор полномочий: разрешения общего ресурса. К дискам, форматированным в NTFS, применяются два набора полномочий: разрешения NTFS и разрешения общего ресурса. Два набора полномочий позволяют точно определить тех, кто обладает доступом к совместно используемым файлам, и соответствующий уровень доступа. В обоих случаях вам не нужно никуда перемещать файлы, к которым вы предоставляете общий доступ.

Вторая модель общего доступа к файлам подразумевает использование папки Общие (Public). Для предоставления доступа достаточно скопировать или переместить файлы в папку Общие (Public). Файлы в папке Общие (Public) доступны каждому, кто выполнил локальный вход на компьютер, независимо от типа учетной записи (обычная или административная). Кроме того, к папке Общие (Public) можно открыть сетевой доступ. Однако при этом не существует никаких ограничений доступа: общая папка и ее содержимое открыты всем, кто может получить доступ к компьютеру по локальной сети.

Организация общего доступа к файлам

Способ, которым осуществляется совместное использование файлов, определяется параметрами общего доступа. Две модели совместного использования ресурсов, поддерживаемые Windows 2008, различаются в следующем:

- **Обычный общий доступ** Позволяет удаленным пользователям обращаться к файлам, папкам и дискам по сети. Предоставляя общий доступ к папке или диску, вы делаете все содержащиеся в них файлы и подпапки доступными для определенного круга пользователей. Регулировать доступ к совместно используемым файлам позволяют разрешения общего ресурса и разрешения NTFS. Перемещать совместно используемые файлы не требуется.
- **Общий доступ из папки Общие (Public)** Позволяет всем локальным, а при необходимости, и удаленным пользователям обращаться ко всем файлам, расположенным в папке *%СистемныйДиск%*\Users\Public. Для определения списка пользователей и групп, которые имеют доступ к файлам этой папки, а также уровень доступа, используются разрешения доступа для папки Общие (Public). Во время копирования или перемещения файлов в папку Общие (Public) разрешения на доступ к ним приводятся в соответствие с папкой Общие (Public), и добавляются некоторые дополнительные разрешения. Если компьютер входит в рабочую группу, вы можете защитить папку Общие (Public) паролем. В домене отдельная защита паролем не нужна, поскольку доступ к данным папки Общие (Public) могут получить только пользователи домена.

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

Использование общей папки предоставляет возможность совместно работать с файлами и папками в одном расположении. Чтобы открыть общую папку в Проводнике Windows (Windows Explorer), щелкните кнопку **Пуск (Start)** и выберите команду **Компьютер (Computer)**. Щелкните крайнюю левую стрелку в строке адреса и выберите вариант **Общие (Public)**. Копируйте или перемещайте файлы, к которым хотите предоставить общий доступ, в папку *%СистемныйДиск%*\Users\Public.

В папке Общие (Public) есть несколько подпапок, которые помогут вам упорядочить общие файлы:

- **Общий рабочий стол (Public Desktop)** Содержит элементы общего рабочего стола. Ярлыки файлов и программ, находящиеся в папке Общий рабочий стол (Public Desktop), присутствуют на рабочих столах всех пользователей, входящих на компьютер, и сетевых пользователей, если к папке Общие (Public) открыт сетевой доступ.
- **Общие документы (Public Documents), Общая музыка (Public Music), Общие изображения (Public Pictures), Общие видео (Public Videos)**

Предназначены для общих документов и медиа-файлов. Все файлы, помещенные в эти подпапки, доступны всем пользователям, входящим на компьютер локально, и всем сетевым пользователям, если к папке Общие (Public) открыт сетевой доступ.

- **Общие загруженные файлы (Public Downloads)** Содержит общие загруженные файлы. Все файлы, помещенные в подпапку Общие загруженные файлы (Public Downloads), доступны всем пользователям, входящим на компьютер локально, и всем сетевым пользователям, если к папке Общие (Public) открыт сетевой доступ.

По умолчанию доступ к папке Общие (Public) открыт для всех пользователей, имеющих на компьютере учетную запись пользователя и пароль. Во время копирования или перемещения файлов в папку Общие (Public) разрешения доступа приводятся в соответствие с параметрами папки Общие (Public), а также добавляются некоторые дополнительные разрешения.

Есть два способа изменить стандартную конфигурацию совместного доступа к папке Общие (Public):

- Разрешить сетевым пользователям просматривать и открывать общие файлы, запретив им изменять, создавать или удалять общие файлы. Если вы используете эту возможность, неявной группе Все (Everyone) предоставляются разрешения Чтение и выполнение (Read & Execute) и Чтение (Read) для общих файлов, а также разрешения Чтение и выполнение (Read & Execute), Список содержимого папки (List Folder Contents) и Чтение (Read) для папок.
- Разрешить сетевым пользователям управлять общими файлами, то есть, открывать, изменять, создавать и удалять общие файлы. При настройке этой возможности скрытой группе Все (Everyone) предоставляется разрешение Полный доступ (Full Control) для общих файлов и папок.

Windows Server 2008 позволяет использовать любую модель общего доступа, но обычный общий доступ обеспечивает большую безопасность и защиту, чем папка Общие (Public). При использовании обычного общего доступа разрешения общего ресурса применяются только при попытке обратиться к файлу или папке по сети, а разрешения доступа используются всегда, как при консольном входе, так и при обращении к файлу или папке с удаленной системы. При удаленном доступе к данным сначала применяются разрешения общего ресурса, а затем разрешения доступа.

Центр управления сетями и общим доступом (Network And Sharing Center) позволяет настраивать основные параметры общего доступа к файлам. Управление доступом к файлам, общим папкам и принтерам осуществляется отдельно. Состояние каждого элемента отображается обозначениями **Вкл (On)** или **Выкл (Off)**, как показано на рис. 15-1.

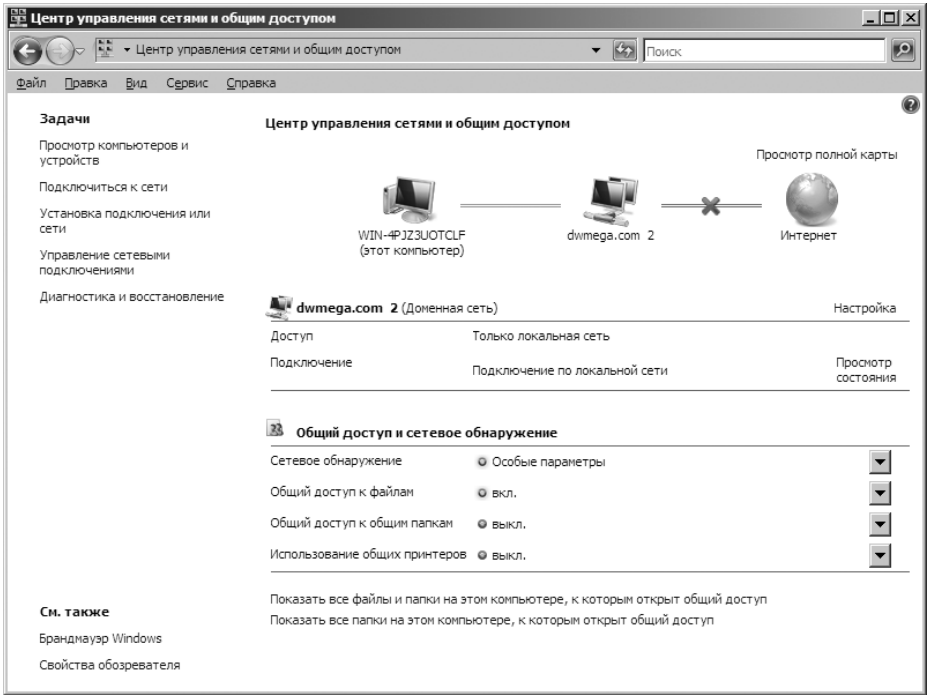


Рис. 15-1. Текущая конфигурация общего доступа в Центре управления сетями и общим доступом (Network And Sharing Center)

Чтобы управлять конфигурацией совместного доступа на компьютере, выполните следующие действия:

1. Откройте Центр управления сетями и общим доступом (Network And Sharing Center), щелкнув **Пуск (Start)** и **Сеть (Network)**, а затем на панели инструментов консоли **Сеть (Network)** щелкнув команду **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. Элемент **Общий доступ к файлам (File Sharing)** управляет сетевым доступом к общим ресурсам. Чтобы настроить обычный общий доступ, щелкните кнопку со стрелкой, соответствующую элементу **Общий доступ к файлам (File Sharing)**. Выполните одно из следующих действий, а затем щелкните **Применить (Apply)**:
   - Установите переключатель **Включить общий доступ к файлам (Turn On File Sharing)**, чтобы включить общий доступ к файлам.
   - Установите переключатель **Отключить общий доступ к файлам (Turn Off File Sharing)**, чтобы отключить общий доступ к файлам.
3. Чтобы настроить общий доступ к папке Общие (Public), щелкните кнопку со стрелкой, соответствующую элементу **Общий доступ к общим папкам (Public Folder Sharing)**. Выберите одну из следующих возможностей, а затем щелкните **Применить (Apply)**:

- **Включить общий доступ, чтобы сетевые пользователи могли открывать файлы (Turn On Sharing So Anyone With Network Access Can Open Files)** Включает общий доступ к папке Общие (Public) с предоставлением разрешения на ее чтение каждому, кто имеет доступ к компьютеру по сети. Параметры брандмауэра Windows могут перекрыть внешний доступ.
- **Включить общий доступ, чтобы сетевые пользователи могли открывать, изменять и создавать файлы (Turn On Sharing So Anyone With Network Access Can Open, Change, And Create Files)** Включает общий доступ к папке Общие (Public), делая всех пользователей, имеющих доступ к компьютеру по сети, совладельцами папки. Параметры брандмауэра Windows могут перекрыть внешний доступ.
- **Отключить общий доступ (Turn Off Sharing)** Отключает общий доступ к папке Общие (Public), запрещая любой доступ к ней извне. Пользователи, вошедшие на компьютер локально, по-прежнему имеют доступ к папке Общие (Public) и всем ее файлам.

4. Элемент **Использование общих принтеров (Printer Sharing)** управляет доступом к принтерам компьютера. Для настройки общего доступа к принтерам щелкните на соответствующую кнопку со стрелкой. Выполните одно из следующих действий, а затем щелкните **Применить (Apply)**:
   - Установите переключатель **Включить общий доступ к принтерам (Turn On Printer Sharing)**, чтобы включить общий доступ к принтерам.
   - Установите переключатель **Выключить общий доступ к принтерам (Turn Off Printer Sharing)**, чтобы отключить общий доступ к принтерам.
5. Пароль позволяет ограничить доступ в пределах рабочей группы, так что доступ к общим ресурсам будет только у пользователей, имеющих учетная запись и пароль на этом компьютере. Чтобы настроить общий доступ, защищенный паролем, щелкните кнопку со стрелкой, соответствующую элементу **Общий доступ с парольной защитой (Password Protected Sharing)**. Выполните одно из следующих действий, а затем щелкните **Применить (Apply)**:
   - Установите переключатель **Включить общий доступ с парольной защитой (Select Turn On Password Protected Sharing)**, чтобы включить защищенный паролем доступ.
   - Установите переключатель **Отключить общий доступ с парольной защитой (Select Turn Off Password Protected Sharing)**, чтобы отключить защищенный паролем доступ.

Настройка обычного общего доступа

Общие ресурсы служат для управления доступом удаленных пользователей. Разрешения на доступ к общим папкам не затрагивают пользователей, локально вошедших на сервер или рабочую станцию, содержащую общие папки.

Просмотр общих ресурсов

Для работы с общими ресурсами можно использовать консоли **Управление компьютером (Computer Management)** и **Управление общими ресурсами и хранилищами (Share And Storage Management)**. Кроме того, текущие общие ресурсы можно просмотреть, введя в командной строке **net share**.

Чтобы просмотреть общие папки в консоли **Управление компьютером (Computer Management)**, выполните следующие действия:

1. По умолчанию вы подключены к локальному компьютеру. Чтобы подключиться к другому компьютеру, щелкните правой кнопкой узел **Управление компьютером (Computer Management)** и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. Установите переключатель **Другим компьютером (Another Computer)**, введите имя или IP-адрес компьютера, к которому хотите подключиться, и щелкните **OK**.
2. В дереве консоли последовательно разверните узлы **Служебные программы (System Tools)** и **Общие папки (Shared Folders)**, а затем выберите элемент **Общие ресурсы (Shares)**. На экране отобразятся текущие общие ресурсы системы (рис. 15-2).

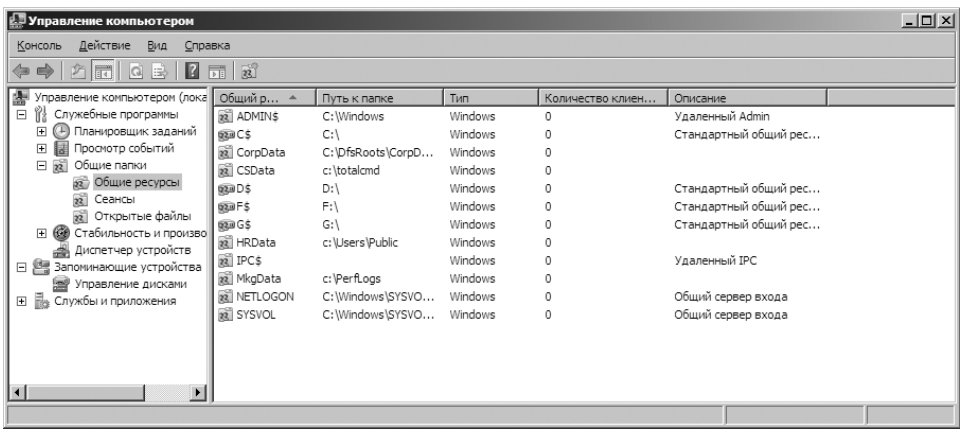


Рис. 15-2. Доступные общие ресурсы приведены в узле Общие папки (Shared Folders)

В столбцах узла **Общие ресурсы (Shares)** содержится следующая информация:

- **Общий ресурс (Share Name)** Имя общей папки.
- **Путь к папке (Folder Path)** Полный путь к папке на локальной системе.
- **Тип (Type)** Платформы, которые могут использовать общий ресурс, например, Macintosh или Windows.
- **Количество клиентских подключений (# Client Connections)** Число клиентов, обращающихся к ресурсу в данный момент.
- **Описание (Description)** Описание общего ресурса.

Примечание Запись **Windows** в столбце **Тип (Type)** означает, что общий ресурс могут использовать все клиенты, работающие под управлением ОС Windows или Macintosh. Запись **Macintosh** в столбце **Тип (Type)** означает, что использовать общий ресурс могут только клиенты Macintosh.

Чтобы просмотреть общие папки в консоли **Управление общими ресурсами и хранилищами (Share And Storage Management)**, выполните следующие действия:

1. По умолчанию вы подключены к локальному компьютеру. Чтобы подключиться к удаленному компьютеру, щелкните правой кнопкой узел **Управление общими ресурсами и хранилищами (Share And Storage Management)** и выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. Установите переключатель **Другим компьютером (Another Computer)**, введите имя или IP-адрес компьютера, к которому хотите подключиться, и щелкните **OK**.

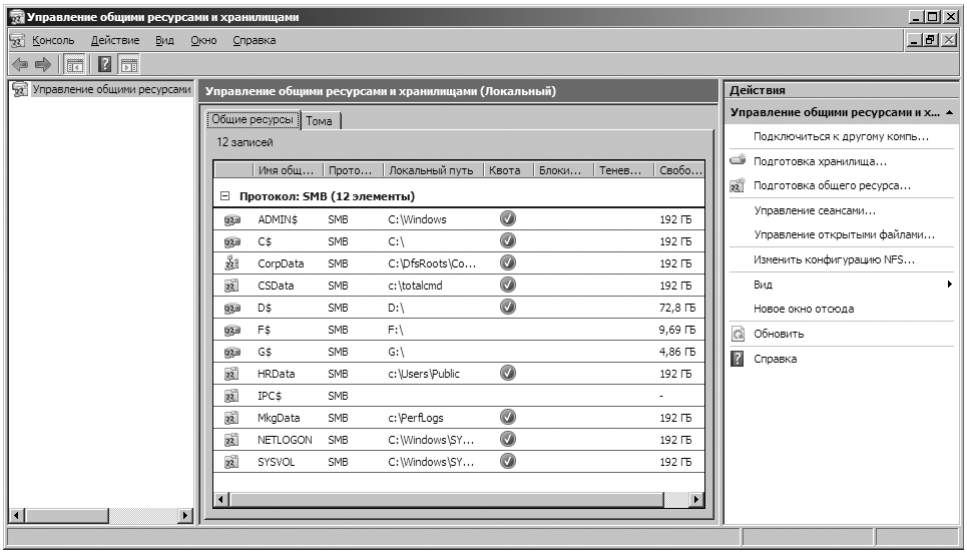


Рис. 15-3. Перейдите на вкладку Общие ресурсы (Shares), чтобы просмотреть доступные общие ресурсы

2. Перейдите на вкладку **Общие ресурсы (Shares)** основной панели и просмотрите текущие общие ресурсы системы (рис. 15-3). В столбцах на вкладке **Общие ресурсы** содержится следующая информация:
   - **Имя общего ресурса (Share Name)** Имя общей папки.
   - **Протокол (Protocol)** Протокол, используемый для совместного доступа (SMB или NFS).
   - **Локальный путь (Local Path)** Полный путь к папке в локальной системе.
   - **Квота (Quota)** Суммарное состояние квот, установленных для общей папки.

- **Блокировка файлов (File Screening)** Суммарное состояние файловых фильтров, примененных к общей папке.
- **Теневые копии (Shadow Copies)** Суммарное состояние теневых копий, примененных к общей папке.
- **Свободно (Free Space)** Объем неиспользованного (свободного) пространства соответствующего диска, если не применены квоты. Если применяются квоты, информация о свободном пространстве отображается в соответствии с заданными ограничениями.

Ближе к реальности Протокол NFS используется для предоставления общего доступа к файлам в ОС UNIX. Из раздела «Настройка общего доступа NFS» этой главы вы узнаете, что для включения поддержки NFS в конфигурации файлового сервера требуется установить службу роли **Службы для NFS (Services for Network File System)**. Протокол SMB используется для предоставления общего доступа в ОС Windows. Системы Windows Vista и Windows Server 2008 поддерживают протокол SMB version 2, обладающий большей производительностью по сравнению с первой версией протокола. Системы Windows Vista SP1 или более поздние версии, а также Windows Server 2008, поддерживают SMB Helper Class, входящий в состав Network Diagnostics Framework (NDF). Этот класс предоставляет диагностическую информацию, весьма полезную при устранении неполадок подключения к общим файловым ресурсам. В частности, он позволяет диагностировать неисправности, когда (а) пользователь пытается получить доступ к несуществующему серверу, (б) пользователь пытается получить доступ к несуществующему общему ресурсу на существующем сервере, (в) пользователь с ошибкой вводит имя общего ресурса, при том что существует общий ресурс с похожим именем.

Создание общих папок

Система Windows Server 2008 позволяет открывать общий доступ к папкам несколькими способами — при помощи Проводника Windows (Windows Explorer), консоли **Управление компьютером (Computer Management)** и консоли **Управление общими ресурсами и хранилищами (Share And Storage Management)**.

Создавая общий ресурс в консоли **Управление компьютером (Computer Management)**, вы можете настроить разрешения общего ресурса и параметры автономной работы. Создавая общий ресурс в консоли **Управление общими ресурсами и хранилищами (Share And Storage Management)**, вы задаете все параметры совместного использования: разрешения NTFS, протоколы общего доступа, ограничения пользователей, параметры автономной работы и разрешения общего ресурса. Кроме того, вы можете настроить квоты диспетчера ресурсов, блокировку файлов, разрешения NFS и публикацию пространства имен DFS.

Чтобы предоставить общий доступ к папкам на сервере Windows Server 2008, вы должны быть членом групп Администраторы (Administrators) или Операторы сервера (Server Operators). Чтобы открыть общий доступ к папке при помощи консоли **Управление компьютером (Computer Management)**, выполните следующие действия:

1. Подключитесь к нужному компьютеру. В дереве консоли последовательно разверните узлы **Служебные программы (System Tools)**, **Общие папки (Shared Folders)**, а затем выберите элемент **Общие ресурсы (Shares)**. На экране отобразятся текущие общие ресурсы системы.
2. Щелкните правой кнопкой элемент **Общие ресурсы (Shares)** и выберите команду **Новый общий ресурс (New Share)**. Откроется **Мастер создания общей папки (Create A Shared Folder Wizard)**. Щелкните **Далее (Next)**.
3. В поле **Путь к папке (Folder Path)** введите локальный путь папки, к которой хотите открыть общий доступ. Путь должен быть точным, например, **C:\Data\CorpDocuments**. Если вы не знаете точный путь, щелкните кнопку **Обзор (Browse)**, чтобы найти папку в диалоговом окне **Обзор папок (Browse For Folder)**. Щелкните **OK** и **Далее (Next)**.

Совет Если путь не существует, мастер предложит его создать. Щелкните **Да (Yes)**.

4. В поле **Общий ресурс (Share Name)** введите имя общего ресурса, как показано на рис. 15-4. Это имя папки, по которому к ней будут подключаться пользователи. В каждой системе имена общих ресурсов должны быть уникальными.

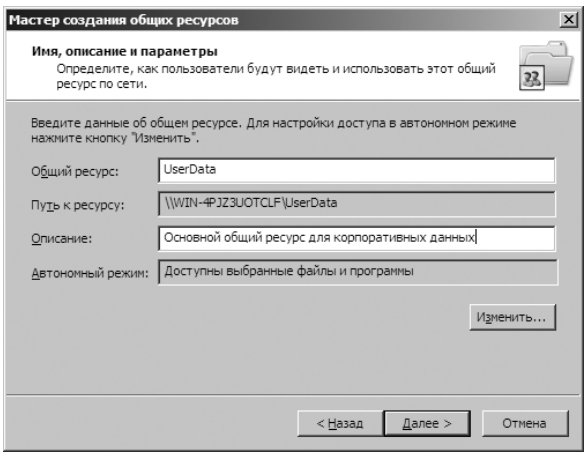


Рис. 15-4. Настройку основных свойств общего ресурса выполняйте в Мастере создания общей папки (Create A Shared Folder Wizard)

Совет Если вы хотите скрыть общий ресурс от пользователей, чтобы он не отображался при попытке найти его в Проводнике Windows (Windows Explorer) или командной строке, в качестве последнего символа имени ресурса введите **$**. Например, можно создать общий ресурс PrivEngData$, который будет скрыт от Проводника Windows (Windows Explorer), команды Net View и прочих подобных программ. Пользователи смогут подключаться к ресурсу и обращаться к его данным, при условии что у них есть разрешение доступа и они знают имя общего ресурса. Обратите внимание, что символ **$** должен вводиться как часть имени общего ресурса при подключении к нему.

5. При необходимости введите описание общего ресурса в поле **Описание (Description)**. Позже, во время просмотра общих ресурсов на компьютере, описание отображается в консоли **Управление компьютером (Computer Management)**.
6. По умолчанию в автономном режиме доступны только указанные пользователем файлы и программы. Если вы хотите запретить автономное использование файлов или, напротив, разрешить автономное использование всех файлов и программ, щелкните кнопку **Изменить (Change)** и задайте нужные параметры в диалоговом окне **Настройка автономного режима (Offline Settings)**.

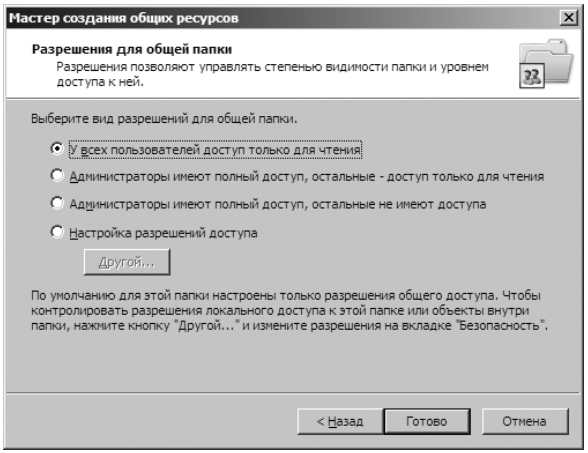


Рис. 15-5. Установка разрешений общего ресурса на странице Разрешения для общей папки (Permissions)

7. Щелкните **Далее (Next)** и задайте базовые разрешения для общего ресурса. Полезные указания вы найдете в разделе «Управление разрешениями общего ресурса» этой главы. Ниже приведены доступные параметры (рис. 15-5):
   - **У всех пользователей доступ только для чтения (All Users Have Read-Only Access)** Предоставляет пользователям доступ для просмотра файлов и чтения данных. Они не могут создавать, изменять или удалять файлы и папки.
   - **Администраторы имеют полный доступ, остальные — доступ только для чтения (Administrators Have Full Access; Other Users Have Read-Only Access)** Предоставляет администраторам полный контроль над общим ресурсом. Они могут создавать, изменять и удалять файлы и папки. В NTFS администраторы также имеют право изменять разрешения и становиться владельцами файлов и папок. Другие пользователи могут лишь просматривать файлы и читать данные, но не могут создавать, изменять или удалять файлы и папки.

- **Администраторы имеют полный доступ, остальные не имеют доступа (Administrators Have Full Access; Other Users Have No Access)** Предоставляет администраторам полный контроль над общим ресурсом и запрещает доступ к нему других пользователей.
- **Настройка разрешений доступа (Customize Permissions)** В большинстве случаев это оптимальный вариант настройки, позволяющий индивидуально управлять доступом отдельных пользователей и групп. Установка разрешений общего доступа подробно рассмотрена далее, в разделе «Управление разрешениями общего ресурса» этой главы.

8. Щелкните кнопку **Готово (Finish)**. На экране появится страница с отчетом **Ресурс успешно сделан общим (Sharing Was Successful)**. Еще раз щелкните **Готово (Finish)**.

Примечание Если теперь посмотреть на общую папку в Проводнике Windows (Windows Explorer), к ее значку будет добавлено изображение руки — символ общего ресурса.

Совет Создав ресурс для всеобщего использования и доступа, опубликуйте его в Active Directory. Это облегчит пользователям его поиск. Чтобы опубликовать общий ресурс в Active Directory, щелкните его правой кнопкой в консоли **Управление компьютером (Computer Management)** и выберите команду **Свойства (Properties)**. На вкладке **Публикация (Publish)** установите флажок **Опубликовать этот общий ресурс в Active Directory (Publish This Share In Active Directory)** и при необходимости добавьте описание и информацию о владельце. Щелкните **OK**.

Создание дополнительных общих ресурсов

Одной и той же папке может соответствовать несколько общих ресурсов со своими именами и наборами разрешений доступа. Чтобы создать дополнительные общие ресурсы для уже существующего общего ресурса, выполните шаги из предыдущего раздела, описывающие создание общего ресурса, внеся в них следующие коррективы:

- На шаге 4, присваивая имя общему ресурсу, проследите, чтобы оно было другим.
- На шаге 5, добавляя описание общего ресурса, постарайтесь объяснить, для чего используется ресурс и чем он отличается от других общих ресурсов для данной папки.

Управление разрешениями общего ресурса

Разрешения общего ресурса определяют допустимые действия в отношении общей папки. По умолчанию при создании общего ресурса каждый сетевой пользователь получает разрешение Чтение (Read) для содержимого общего ресурса. В этом заключается немаловажное новшество системы безопасности — в предыдущих версиях стандартным разрешением был Полный доступ (Full Control).

В целях дальнейшего ужесточения ограничений общего ресурса на томах NTFS допускается применение разрешений файлов и папок, владения, а также разрешений общих ресурсов. На томах FAT доступ управляется только разрешениями общих ресурсов.

Разрешения общего доступа

Разрешения общего ресурса перечислены в порядке убывания ограничений:

- **Нет доступа (No Access)** Разрешения на доступ к общему ресурсу не предоставляются.
- **Чтение (Read)** Это разрешение позволяет:
  - просматривать имена файлов и подпапок;
  - обращаться к подпапкам общего ресурса;
  - читать данные и атрибуты файла;
  - запускать файлы программ.
- **Изменение (Change)** Пользователи обладают разрешением Чтение (Read), а также могут делать следующее:
  - создавать файлы и подпапки;
  - изменять файлы;
  - изменять атрибуты файлов и подпапок;
  - удалять файлы и подпапки.
- **Полный доступ (Full Control)** Пользователи обладают разрешениями Чтение (Read) и Изменение (Change), а также могут делать следующее (на NTFS-томах):
  - изменять разрешения файлов и папок;
  - становиться владельцами файлов и папок.

Вы можете назначать полномочия пользователям и группам, в том числе, неявным группам. Дополнительные сведения о неявных группах вы найдете в разделе «Неявные группы и идентификаторы» главы 9.

Просмотр разрешений общего ресурса

Чтобы просмотреть разрешения общего ресурса, выполните следующие действия:

1. В консоли **Управление компьютером (Computer Management)** подключитесь к компьютеру, на котором создан общий ресурс.
2. В дереве консоли последовательно разверните узлы **Служебные программы (System Tools)** и **Общие папки (Shared Folders)**, а затем выберите элемент **Общие ресурсы (Shares)**.
3. Щелкните правой кнопкой ресурс, который хотите просмотреть, и выберите команду **Свойства (Properties)**.
4. В диалоговом окне свойств перейдите на вкладку **Разрешения для общего ресурса (Share Permissions)**, показанную на рис. 15-6. Просмотрите

пользователей и группы, имеющие доступ к общему ресурсу, а также тип предоставленного им доступа.

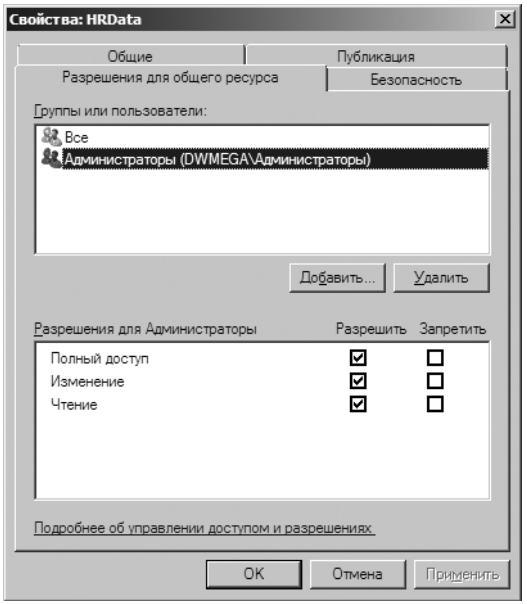


Рис. 15-6. На вкладке Разрешения для общего ресурса (Share Permissions) отображены пользователи и группы, имеющие доступ к общему ресурсу

Настройка разрешений общего ресурса

Чтобы задать разрешения общего ресурса для пользователей, компьютеров и групп в консоли **Управление компьютером (Computer Management)**, выполните следующие действия:

1. Щелкните правой кнопкой общий ресурс, который хотите настроить, и выберите команду **Свойства (Properties)**.
2. В диалоговом окне свойств перейдите на вкладку **Разрешения для общего ресурса (Share Permissions)**.
3. Щелкните **Добавить (Add)**. Откроется диалоговое окно **Выбор: «Пользователи», «Компьютеры» или «Группы» (Select Users, Computers, Or Groups)**, показанное на рис. 15-7.

   Введите имя пользователя, компьютера или группы в текущем домене и щелкните **Проверить имена (Check Names)**.

   - Если обнаружится одно совпадение, соответствующее имя пользователя будет автоматически добавлено в диалоговое окно.
   - Если совпадений не найдено, вы ввели ошибочное имя или работаете в неверном расположении. Исправьте имя или щелкните кнопку **Размещение (Locations)**, чтобы задать другое место для поиска.

- Если найдено несколько совпадений, выберите нужное имя или имена и щелкните **OK**. Чтобы предоставить разрешения другим пользователям, компьютерам или группам, поставьте после найденного имени точку с запятой и повторите поиск.

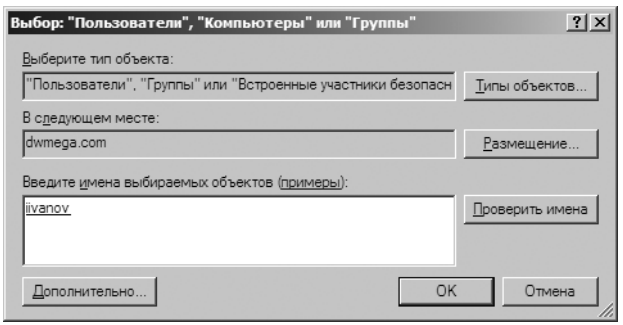


Рис. 15-7. Добавление пользователей и групп, имеющих доступ к общему ресурсу

Примечание Кнопка **Размещение (Locations)** позволяет получить доступ к учетным записям из других доменов. Щелкните ее, чтобы просмотреть доступные размещения. Благодаря транзитивным доверительным отношениям в Windows Server 2008 вы сможете выбирать записи из большинства доменов дерева или леса.

4. Щелкните **OK**. Пользователи и группы будут добавлены в список **Группы или пользователи (Group Or User Names)**.
5. Настройте разрешения доступа для каждого пользователя, компьютера и группы. Выделите соответствующую учетную запись и предоставьте или отзовите разрешения. Помните, что для конкретной учетной записи вы задаете предельно допустимые разрешения.
6. Завершив настройку, щелкните **OK**. О том, как предоставить дополнительные разрешения безопасности NTFS, читайте в разделе «Разрешения файлов и папок» этой главы.

Изменение существующих разрешений общего ресурса

Чтобы изменить разрешения общего ресурса, предоставленные пользователям, компьютерам и группам, при помощи консоли **Управление компьютером (Computer Management)**, выполните следующие действия:

1. Щелкните правой кнопкой общий ресурс, который хотите настроить, и выберите команду **Свойства (Properties)**.
2. В диалоговом окне свойств перейдите на вкладку **Разрешения для общего ресурса (Share Permissions)**.
3. В списке **Группы или пользователи (Group Or User Names)** выберите пользователя, компьютер или группу, разрешения которых хотите изменить.
4. Предоставьте или отзовите разрешения при помощи флажков в разделе **Разрешения (Permissions)**.

5. Повторите действие для других пользователей, компьютеров или групп. Завершив настройку, щелкните **OK**.

Удаление разрешений общего ресурса

При помощи консоли **Управление компьютером (Computer Management)** вы можете удалить разрешения общего ресурса, предоставленные пользователям, компьютерам и группам, выполнив следующие действия:

1. Щелкните правой кнопкой общий ресурс, который хотите настроить, и выберите команду **Свойства (Properties)**.
2. В диалоговом окне свойств перейдите на вкладку **Разрешения для общего ресурса (Share Permissions)**.
3. В списка **Группы или пользователи (Group Or User Names)** выберите пользователя, компьютер или группу и щелкните **Удалить (Remove)**.
4. При необходимости повторите действие для других пользователей или групп. Завершив настройку, щелкните **OK**.

Управление общими ресурсами

В этом разделе описаны распространенные административные задачи по управлению общими ресурсами.

Специальные общие ресурсы

В процессе установки Windows Server 2008 ОС автоматически создает специальные общие ресурсы — *административные общие ресурсы* (administrative shares) и *скрытые общие ресурсы* (hidden shares), — предназначенные для упрощения администрирования системы. Вы не можете задавать разрешения доступа для автоматически создаваемых общих ресурсов, этим занимается Windows Server 2008. (Вы вольны сами создавать скрытые общие ресурсы, вводя символ **$** в конце имени ресурса.)

Вы можете временно удалять специальные общие ресурсы, если уверены, что они вам не нужны. Однако при следующей загрузке ОС они будут автоматически воссозданы. Чтобы навсегда отключить административные общие ресурсы, присвойте следующим параметрам реестра нулевые значения:

```
HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\
AutoShareServer
HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareWks
```

Набор специальных общих ресурсов зависит от конфигурации системы. В табл. 15-1 приведен список специальных общих ресурсов и их предназначение.

Табл. 15-1. Специальные общие ресурсы Windows Server 2008

Специальный общий ресурс	Описание	Применение
ADMIN$	Общий ресурс, используемый при удаленном администрировании системы. Предоставляет доступ к корневой папке ОС (%SystemRoot%)	На рабочих станциях и серверах доступ к ресурсу имеют администраторы и операторы архива. На контроллерах домена доступ также имеют операторы сервера
FAX$	Поддерживает сетевые факсы	Используется факс-клиентами во время отправки факсов
IPC$	Поддерживает именованные каналы во время удаленного взаимодействия процессов (IPC)	Используется программами во время проведения удаленного администрирования и просмотра совместно используемых ресурсов
NETLOGON	Поддерживает службу Net Logon	Используется службой Net Logon для обработки запросов на вход в домен. Группа Все (Everyone) имеет разрешение Чтение (Read)
PRINT$	Поддерживает общие принтеры, предоставляя доступ к драйверам	Используется общими принтерами. Группа Все (Everyone) имеет разрешение Чтение (Read). Администраторы, операторы сервера и операторы печати имеют разрешение Полный доступ (Full Control)
PUBLIC	Поддерживает общий доступ к папки Общие (Public)	Используется для хранения общих данных
SYSVOL	Поддерживает Active Directory	Используется для хранения данных и объектов Active Directory
БуквaДиска$	Общий ресурс, позволяющий администраторам подключаться к корневой папке диска. Имена этих ресурсов имеют вид C$, D$, E$ и т. д.	На рабочих станциях и серверах доступ к этим ресурсам имеют администраторы и операторы архива. На контроллерах домена доступ также имеют операторы сервера

Подключение к специальным общим ресурсам

Имена специальных общих ресурсов оканчиваются символом $. Эти ресурсы не отображаются в Проводнике Windows (Windows Explorer), но, тем не менее, администраторы и некоторые операторы могут к ним подключаться. Для подключения к специальному общему ресурсу выполните следующие действия:

1. Щелкните **Пуск (Start)** и **Компьютер (Computer)**. На панели инструментов консоли **Компьютер (Computer)** щелкните команду **Подключить сетевой диск (Map Network Drive)**. На экране появится окно, показанное на рис. 15-8.

2. В раскрывающемся списке **Диск (Drive)** выберите свободную букву диска. Эта буква нужна для доступа к специальному общему ресурсу.
3. В поле Папка (Folder) введите UNC-путь к ресурсу. Например, для доступа к общему ресурсу C$ на сервере Twiddle следует ввести **TWIDDLE\C$**.
4. Щелкните **Готово (Finish)**.

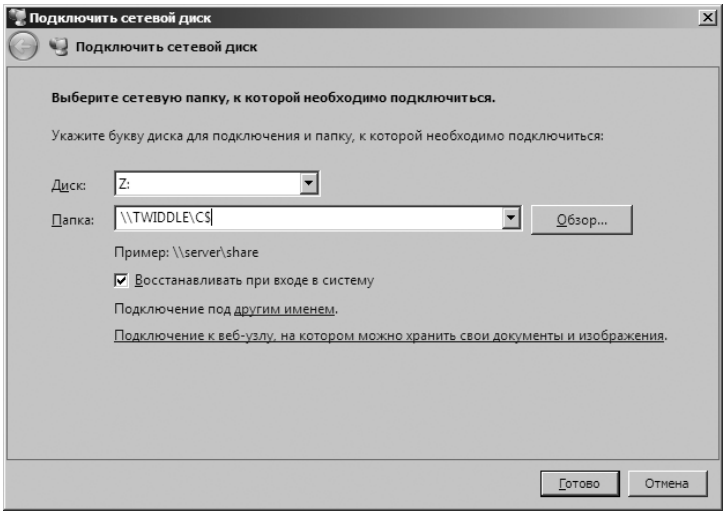


Рис. 15-8. Подключение к специальному общему ресурсу

Подключившись к специальному общему ресурсу, вы можете обращаться к нему, как и к любому другому диску. Специальные общие ресурсы защищены, поэтому не беспокойтесь, что обычные пользователи смогут получить к ним доступ. При первом подключении к общему ресурсу вам, возможно, придется ввести имя пользователя и пароль.

Просмотр сеансов пользователя и компьютера

В консоли **Управление компьютером (Computer Management)** можно отследить все подключения к общим ресурсам Windows Server 2008. Каждое подключение пользователя или компьютера к общему ресурсу Windows Server 2008 заносит в список, находящийся в узле **Сеансы (Sessions)**.

Для просмотра подключений к общим ресурсам введите в командной строке **net session** или выполните следующие действия:

1. В консоли **Управление компьютером (Computer Management)** подключитесь к компьютеру, на котором создан общий ресурс.
2. В дереве консоли последовательно разверните узлы **Служебные программы (System Tools)** и **Общие папки (Shared Folders)**, а затем выберите **Сеансы (Sessions)**. Здесь можно просмотреть подключения пользователей и компьютеров к общим ресурсам. В столбцах узла **Сеансы (Sessions)** содержится следующая информация:

- **Пользователь (User)** Имя пользователя или компьютера, подключившегося к общим ресурсам. Имена компьютеров отображаются с суффиксом $, что отличает их от имен пользователей.
- **Компьютер (Computer)** Имя используемого компьютера.
- **Тип (Type)** Тип сетевого подключения.
- **Количество открытых файлов (# Open Files)** Число файлов, с которыми работает пользователь. Для получения более подробной информации откройте узел **Открытые файлы (Open Files)**.
- **Время подсоединения (Connected Time)** Время, прошедшее с момента установки подключения.
- **Время простоя (Idle Time)** Время, прошедшее с момента последнего использования подключения.
- **Гость (Guest)** Указывает, вошел ли пользователь в систему как гость.

Управление сеансами и общими ресурсами

Управление сеансами и общими ресурсами представляет собой типичную административную задачу. Перед завершением работы сервера или запущенного на нем приложения вам, возможно, придется отключить пользователей от общих ресурсов. Кроме того, отключение пользователей может потребоваться для изменения разрешений доступа, при удалении общего ресурса, для снятия блокировки с файлов. Отключение пользователей от общих ресурсов происходит посредством завершения сеансов соответствующих пользователей.

Редактирование отдельных сеансов

Чтобы отключить отдельных пользователей от общих ресурсов, введите в командной строке **net session \\ИмяКомпьютера /delete** или выполните следующие действия:

1. В консоли **Управление компьютером (Computer Management)** подключитесь к компьютеру, на котором создан общий ресурс.
2. В дереве консоли последовательно разверните узлы **Служебные программы (System Tools)** и **Общие папки (Shared Folders)**, а затем выберите **Сеансы (Sessions)**.
3. Щелкните правой кнопкой сеанс, который хотите завершить и выберите команду **Закрыть сеанс (Close Session)**.
4. Для подтверждения действия щелкните **Да (Yes)**.

Закрытие всех сеансов

Чтобы отключить всех пользователей от общих ресурсов, выполните следующие действия:

1. В консоли **Управление компьютером (Computer Management)** подключитесь к компьютеру, на котором создан общий ресурс.

2. В дереве консоли последовательно разверните узлы **Служебные программы (System Tools)** и **Общие папки (Shared Folders)**, а щелкните правой кнопкой элемент **Сеансы (Sessions)**.
3. Выберите команду **Отключить все сеансы (Disconnect All Sessions)** и щелкните **Да (Yes)**, чтобы подтвердить действие.

Примечание Помните, что вы отключаете пользователей от общих ресурсов, а не от домена. Принудительный вывод из домена возможен, только если вы задали допустимые часы работы при помощи групповой политики.

Управление открытыми ресурсами

Каждый раз, когда пользователи подключаются к общим ресурсам, файлы и объекты, с которыми они работают, отображаются в узле **Открытые файлы (Open Files)**. В том числе, в узле **Открытые файлы (Open Files)** отображаются файлы, открытые пользователем, но не редактируемые в данный момент.

Чтобы открыть узел **Открытые файлы (Open Files)**, выполните следующие действия:

1. В консоли **Управление компьютером (Computer Management)** подключитесь к компьютеру, на котором находится общий ресурс.
2. В дереве консоли последовательно разверните узлы **Служебные программы (System Tools)** и **Общие папки (Shared Folders)**, а затем выберите **Открытые файлы (Open Files)**. Откроется панель, в которой представлена следующая информация об использовании ресурсов:
   - **Открытый файл (Open File)** Локальный путь к открытому файлу или папке. Также это может быть именованный канал, например, \PIPE\spools, использующийся для очереди принтера.
   - **Пользователь (Accessed By)** Имя пользователя, открывшего файл.
   - **Тип (Type)** Тип сетевого подключения.
   - **Блокир. (# Locks)** Число блокировок ресурса.
   - **Режим открытия (Open Mode)** Режим доступа к ресурсу, например, чтение, запись или чтение/запись.

Закрытие открытого файла

Чтобы закрыть открытый файл в общем ресурсе компьютера, выполните следующие действия:

1. В консоли **Управление компьютером (Computer Management)** подключитесь к нужному компьютеру.
2. В дереве консоли последовательно разверните узлы **Служебные программы (System Tools)** и **Общие папки (Shared Folders)**, а затем выберите **Открытые файлы (Open Files)**.
3. Щелкните правой кнопкой открытый файл, который хотите закрыть, и выберите команду **Закрыть открытый файл (Close Open File)**.
4. Для подтверждения действия щелкните **Да (Yes)**.

Закрытие всех открытых файлов

Чтобы закрыть все открытые файлы в общих ресурсах компьютера, выполните следующие действия:

1. В консоли **Управление компьютером (Computer Management)** подключитесь к нужному компьютеру.
2. В дереве консоли последовательно разверните узлы **Служебные программы (System Tools)** и **Общие папки (Shared Folders)**, а затем щелкните правой кнопкой элемент **Открытые файлы (Open Files)**.
3. Выберите команду **Отключить все открытые файлы (Disconnect All Open Files)** и щелкните **Да (Yes)**, чтобы подтвердить действие.

Прекращение общего доступа к файлам и папкам

Чтобы прекратить общий доступ к папке, выполните следующие действия:

1. В консоли **Управление компьютером (Computer Management)** подключитесь к компьютеру, на котором находится общий ресурс, и откройте узел **Общие ресурсы (Shares)**.
2. Щелкните правой кнопкой общий ресурс, который хотите удалить, и выберите команду **Прекратить общий доступ (Stop Sharing)**. Для подтверждения действия щелкните **Да (Yes)**.

Внимание! Не удаляйте папку общего ресурса, предварительно не прекратив к ней доступ. Если вы не остановите общий доступ, при следующей загрузке компьютера Windows Server 2008 попытается восстановить ресурс. В журнал событий **Система (System)** будет занесена ошибка.

Настройка общего доступа NFS

В разделе «Управление файловыми системами и дисками» главы 12 говорилось о возможности установки на файловый сервер службы роли **Службы для NFS (Services for Network File System)**. Эта служба роли представляет собой решение совместного использования файлов на предприятиях со смешанной средой Windows/UNIX, которое позволяет перемещать файлы между ОС Windows Server 2008 и UNIX при помощи протокола NFS.

Проводник Windows (Windows Explorer) позволяет настроить общий доступ по протоколу NFS к локальным папкам, расположенным на NTFS-томах. Кроме того, вы можете настроить общий доступ к локальным и удаленным папкам на NTFS-томах по протоколу NFS в консоли **Управление общими ресурсами и хранилищами (Share And Storage Management)**. Чтобы включить и настроить общий доступ для NFS в Проводнике Windows (Windows Explorer), выполните следующие действия:

1. Щелкните правой кнопкой общий ресурс, который хотите настроить, и выберите команду **Свойства (Properties)**. Откроется диалоговое окно свойств общего ресурса.

2. На вкладке **Совместный доступ NFS (NFS Sharing)** щелкните кнопку **Управление доступом NFS (Manage NFS Sharing)**.
3. В диалоговом окне **Дополнительные параметры общего доступа NFS (NFS Advanced Sharing)** установите флажок **Открыть общий доступ к этой папке (Share This Folder)**, как показано на рис. 15-9.

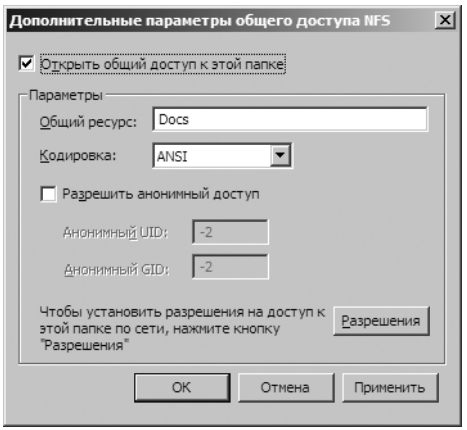


Рис. 15-9. Общий доступ NFS служит для совместного использования ресурсов компьютерами под управлением Windows и UNIX

4. В поле **Общий ресурс (Share Name)** введите имя общего ресурса, то есть, имя, по которому к папке будут подключаться пользователи UNIX. Имена общих ресурсов NFS должны быть уникальны в пределах каждой системы, но могут совпадать с именами, используемыми для обычного общего доступа к файлам.
5. По умолчанию для кодировки текста, связанного со списками и именами файлов, используется кодировка ANSI. Если на компьютерах UNIX используется другая кодировка, выберите ее в списке **Кодировка (Encoding)**.
6. Если вы хотите разрешить анонимный доступ к общему ресурсу NFS, установите флажок **Разрешить анонимный доступ (Allow Anonymous Access)**, а затем введите идентификаторы анонимного пользователя и анонимной группы.
7. По умолчанию компьютеры под управлением UNIX обладают доступом только для чтения к общим ресурсам NFS. Чтобы изменить стандартные разрешения, щелкните кнопку **Разрешения (Permissions)**, в диалоговом окне **Разрешения для общей папки NFS (NFS Share Permissions)** задайте желаемые разрешения, а затем щелкните **OK**. Вы можете запретить доступ пользователям и группам, открыть доступ только для чтения, а также предоставить доступ для чтения и записи.
8. Два раза щелкните **OK**, чтобы закрыть все открытые диалоговые окна и сохранить параметры.

Чтобы отключить общий доступ NFS в Проводнике Windows (Windows Explorer), выполните следующие действия:

1. Щелкните правой кнопкой общий ресурс, который хотите настроить, и выберите команду **Свойства (Properties)**. Откроется диалоговое окно свойств общего ресурса.
2. На вкладке **Совместный доступ NFS (NFS Sharing)** щелкните кнопку **Управление доступом NFS (Manage NFS Sharing)**.
3. В диалоговом окне **Дополнительные параметры общего доступа NFS (NFS Advanced Sharing)** сбросьте флажок **Открыть общий доступ к этой папке (Share This Folder)**.

В консоли **Управление общими ресурсами и хранилищами (Share And Storage Management)** можно настроить разрешения NFS в рамках начальной настройки NFS.

- Щелкните правой кнопкой общий ресурс NFS на вкладке **Общие ресурсы (Shares)** и выберите команду **Свойства (Properties)**. В диалоговом окне свойств ресурса вы можете выбрать другую кодировку в списке **Кодировка (Encoding)** на вкладке **Совместный доступ NFS (NFS Sharing)**. Чтобы управлять разрешениями NFS, щелкните кнопку **Разрешения NFS (NFS Permissions)** на вкладке **Разрешения (Permissions)**.
- Чтобы прекратить общий доступ к папке посредством NFS, щелкните правой кнопкой общий ресурс NFS на вкладке **Общие ресурсы (Shares)** и выберите команду **Прекратить общий доступ (Stop Sharing)**. Щелкните **Да (Yes)**, чтобы подтвердить действие.

Теневые копии

Если в вашей организации используются общие папки, подумайте о создании теневых копий этих папок — одномоментных резервных копий файлов, к которым обращаются пользователи. Подобного рода копии сэкономят вам и другим администраторам организации массу времени, особенно благодаря возможности восстановления из резервных копий потерянных, перезаписанных или поврежденных данных. Обычно процедура восстановления из теневой копии заключается в работе со вкладкой **Предыдущие версии (Previous Versions)** или клиентом теневого копирования. В Windows Server 2008 включено расширение, позволяющее восстановить любой том (кроме системного) к состоянию на момент создания предыдущей теневой копии.

Знакомство с теневыми копиями

Теневые копии создаются только на NTFS-томах. Функция теневого копирования предназначена для автоматического создания резервных копий файлов, расположенных в общих папках на томах NTFS. Допустим, на файловом сервере есть три тома NTFS, на каждом из которых есть общие папки. В этом случае потребуется отдельная настройка этой функции на каждом томе.

Если функция включена со стандартными параметрами, теневые копии создаются дважды за каждый рабочий день (с понедельника по пятницу), в 7:00 и в 24:00. Для создания первой теневой копии тома требуется не менее 100 Мб свободного пространства. Объем дополнительного дискового пространства зависит от количества данных, содержащихся в общих папках тома. Вы вольны ограничить объем дискового пространства, занятого теневыми копиями, задав предельный размер копий.

Просмотреть и настроить текущие параметры теневого копирования можно в диалоговом окне свойств диска, на вкладке **Теневые копии (Shadow Copies)**. Щелкните правой кнопкой значок диска, который хотите настроить, в Проводнике Windows (Windows Explorer) или консоли **Управление компьютером (Computer Management)**. Выберите команду **Свойства (Properties)** и перейдите на вкладку **Теневые копии (Shadow Copies)**. На панели **Выберите том (Select A Volume)** отображена следующая информация:

- **Том (Volume)** Метки NTFS-томов на выбранном диске.
- **Время следующего запуска (Next Run Time)** Состояние функции теневого копирования — **Отключено (Disabled)** или время создания очередной теневой копии тома.
- **Общие ресурсы (Shares)** Количество общих папок в томе.
- **Использовано (Used)** Объем дискового пространства, занятый теневой копией.

Отдельные теневые копии для выбранного тома перечислены на панели **Теневые копии выбранного тома (Shadow Copies Of Selected Volume)**, отсортированные по дате и времени.

Создание теневых копий

Чтобы создать теневую копию NTFS-тома, выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)**. При необходимости подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел **Запоминающие устройства (Storage)** и выберите **Управление дисками (Disk Management)**. Тома на выбранном компьютере отображаются в области сведений.
3. Щелкните правой кнопкой элемент **Управление дисками (Disk Management)**, раскройте подменю **Все задачи (All Tasks)** и выберите команду **Настроить теневые копии (Configure Shadow Copies)**.
4. На вкладке **Теневые копии (Shadow Copies)** в списке **Выберите том (Select A Volume)** выберите том, с которым хотите работать.
5. Щелкните кнопку **Параметры (Settings)**, чтобы задать максимальный размер всех теневых копий данного тома и изменить стандартное расписание. Завершив работу, щелкните **OK**.
6. При необходимости, настроив теневое копирование на томе, щелкните **Включить (Enable)**. Щелкните **Да (Yes)**, чтобы подтвердить действие.

Таким образом, будет создана первая теневая копия, и задано расписание для последующего теневого копирования.

Примечание Если в процессе настройки параметров теневого копирования вы создаете расписание запуска, включение теневого копирования происходит автоматически, когда вы щелкнете **OK**, чтобы закрыть диалоговое окно **Параметры (Settings)**.

Восстановление теневой копии

Пользователи на клиентских компьютерах работают с теневыми копиями отдельных общих папок посредством вкладки **Предыдущие версии (Previous Versions)** или клиента теневого копирования. Чтобы получить доступ к резервной копии на клиентском компьютере, выполните следующие действия:

1. Щелкните правой кнопкой общий ресурс, доступ к прежним версиям файлов которого хотите получить. Выберите команду **Свойства (Properties)** и перейдите на вкладку **Предыдущие версии (Previous Versions)**.
2. Выберите нужную версию папки. Каждая версия помечена датой и временем. Затем щелкните кнопку, соответствующую действию, которое вы хотите выполнить:
   - **Открыть (Open)** Открывает теневую копию в Проводнике Windows (Windows Explorer).
   - **Копировать (Copy)** Открывает диалоговое окно **Копирование элементов (Copy Items)**, позволяющее копировать снимок состояния папки в заданное положение.
   - **Восстановить (Restore)** Возвращает общую папку к состоянию на момент создания выбранной теневой копии.

Возврат тома к предыдущей теневой копии

В Windows Server 2008 вколючено расширение, позволяющее вернуть весь том в состояние на момент создания конкретной теневой копии. Нельзя восстановить только тома, содержащие ОС, поэтому том, который вы хотите вернуть в прежнее состояние, не должен быть системным.

Чтобы вернуть весь том в прежнее состояние, выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)**. При необходимости подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел **Запоминающие устройства (Storage)**. Щелкните правой кнопкой элемент **Управление дисками (Disk Management)**, раскройте подменю **Все задачи (All Tasks)** и выберите команду **Настроить теневые копии (Configure Shadow Copies)**.
3. На вкладке **Теневые копии (Shadow Copies)** в списке **Выберите том (Select A Volume)** выберите том, с которым хотите работать.

4. Отдельные теневые копии выбранного тома отображены в списке **Теневые копии выбранного тома (Shadow Copies Of Selected Volume)**. Выберите теневую копию со датой и временем, на которое вы хотите восстановить состояние тома, и щелкните **Восстановить (Revert)**.
5. Подтвердите действие, установив флажок **Выполнить откат состояния этого тома (Check Here If You Want To Revert This Volume)**, и щелкните **Откатить (Revert Now)**. Щелкните **OK**.

Удаление теневых копий

Обслуживание каждой резервной копии, созданной в данный момент времени, выполняется отдельно. При необходимости вы можете удалять теневые копии тома. Этим вы освободите занимаемое ими дисковое пространство.

Чтобы удалить теневую копию, выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)**. При необходимости подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел **Запоминающие устройства (Storage)**. Щелкните правой кнопкой элемент **Управление дисками (Disk Management)**, раскройте подменю **Все задачи (All Tasks)** и выберите команду **Настроить теневые копии (Configure Shadow Copies)**.
3. На вкладке **Теневые копии (Shadow Copies)** в списке **Выберите том (Select A Volume)** выберите том, с которым хотите работать.

Выберите в списке **Теневые копии выбранного тома (Shadow Copies Of Selected Volume)** теневую копию, которую хотите удалить, и щелкните **Удалить (Delete Now)**.

Отключение теневых копий

Чтобы прекратить поддержку теневых копий тома, отключите функцию теневого копирования. Выполнение расписания автоматического копирования будет остановлено, а все существующие теневые копии будут удалены.

Чтобы отключить теневое копирование, выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)**. При необходимости подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел **Запоминающие устройства (Storage)**. Щелкните правой кнопкой элемент **Управление дисками (Disk Management)**, раскройте подменю **Все задачи (All Tasks)** и выберите команду **Настроить теневые копии (Configure Shadow Copies)**.
3. На вкладке **Теневые копии (Shadow Copies)** в списке **Выберите том (Select A Volume)** выберите том, с которым хотите работать, и щелкните **Отключить (Disable)**.
4. Щелкните **Да (Yes)**, чтобы подтвердить действие. Щелкните **OK**.

Подключение к сетевым дискам

Пользователи могут подключаться к сетевым дискам и общим сетевым ресурсам. Такое подключение отображается в виде диска, доступ к которому пользователи получают как к обычному диску.

Примечание Подключение пользователей к сетевым дискам зависит не только от набора разрешений общих ресурсов, но и от разрешений файлов и папок Windows Server 2008. Различия между наборами разрешений часто становятся причиной того, что пользователи не могут получить доступ к тому или иному файлу или подпапке сетевого диска.

Подключение сетевого диска

Подключение к сетевому диску в Windows Server 2008 осуществляется при помощи команды NET USE:

```
net use Диск \\ИмяКомпьютера\ИмяОбщегоРесурса
```

где *Диск* — буква диска или символ *, соответствующий ближайшей незанятой букве, а *\\ИмяКомпьютера\ИмяОбщегоРесурса* — UNC-путь к общему ресурсу, например:

```
net use g: \\ROMEO\DOCS
```

или

```
net use * \\ROMEO\DOCS
```

Примечание Чтобы восстанавливать подключение к диску при каждом входе пользователя в систему, используйте параметр /Persistent:Yes.

Если клиентский компьютер работает под управлением Windows Vista, для подключения сетевого диска можно воспользоваться следующими действиями:

1. Войдите на компьютер от имени пользователя и откройте Проводник Windows (Windows Explorer).
2. В меню **Сервис (Tools)** выберите команду **Подключить сетевой диск (Map Network Drive)**. Откроется одноименное окно.
3. В раскрывающемся списке **Диск (Drive)** выберите диск для общего ресурса — любую незанятую букву.
4. В поле **Папка (Folder)** введите UNC-путь к нужному общему ресурсу. Например, для доступа к общему ресурсу DOCS на сервере ROMEO, следует ввести **\\ROMEO\DOCS**. Если вы не знаете расположение общего ресурса, щелкните **Обзор (Browse)**. Найдя ресурс, щелкните **OK**, чтобы закрыть диалоговое окно **Обзор папок (Browse For Folder)**.
5. Если вы хотите, чтобы сетевой диск автоматически подключался в следующих сеансах, установите флажок **Восстанавливать при входе в систему (Reconnect At Logon)**. Если вы предпочитаете устанавливать соединение вручную, сбросьте этот флажок.
6. Чтобы создать подключение для другого пользователя, щелкните ссылку **Подключение под другим именем (Different User Name)** и введите имя

пользователя и пароль. Щелкните **OK**, чтобы закрыть диалоговое окно **Подключение от имени (Connect As)**.

7. Щелкните **Готово (Finish)**, чтобы подключить сетевой диск.

Отключение сетевого диска

Для отключения сетевого диска выполните следующие действия:

1. Войдите на компьютер от имени пользователя и откройте Проводник Windows (Windows Explorer).
2. Выберите в меню **Сервис (Tools)** команду **Отключить сетевой диск (Disconnect Network Drive)**. Откроется диалоговое окно **Отключение сетевых дисков (Disconnect Network Drive)**.
3. Выделите диск, который хотите отключить, и щелкните **OK**.

Управление объектами, владение и наследование

В ОС Windows Server 2008 используется объектно-ориентированный подход к описанию ресурсов и управлению разрешениями. Объекты, описывающие ресурсы, определяются на NTFS-томах и в Active Directory. Тома NTFS позволяют задавать разрешения для файлов и папок. В Active Directory вы можете устанавливать разрешения для объектов других типов, например, пользователей, компьютеров и групп. Эти разрешения предназначены для тонкой настройки доступа.

Объекты и диспетчеры объектов

Где бы ни был определен объекта — на NTFS-томе или в Active Directory, — каждому типу объектов соответствует диспетчер объектов и основные инструменты управления. Диспетчер объектов управляет параметрами и разрешениями объекта. Объекты, их диспетчеры и инструментальные средства управления приведены в табл. 15-2.

Табл. 15-2. Объекты Windows Server 2008

Тип объекта	Диспетчер объекта	Средство управления
Файлы и папки	NTFS	Проводник Windows (Windows Explorer)
Общие ресурсы	Служба Server	Проводник Windows (Windows Explorer), консоль **Управление компьютером (Computer Management)**
Параметры реестра	Реестр Windows	Редактор реестра (Registry Editor)
Службы	Контроллеры служб	Набор утилит настройки безопасности (Security Configuration Tool Set)
Принтеры	Диспетчер очереди	Утилита **Принтеры (Printers)** панели управления

Владение и перемещение объектов

Очень важно понимать идею владения объектами. В Windows Server 2008 владельцем объекта не обязательно является его создатель. Владелец объекта — это человек, обладающий правом прямого управления данным объектом. Владельцы объектов могут предоставлять другим пользователям разрешения доступа, а также передавать право владения объектом.

Часто становиться владельцем сетевых объектов приходится администратору. Это позволяет ему преодолевать блокировки файлов, папок, принтеров и других ресурсов. Однако, став владельцем файла, вы в большинстве случаев не сможете вернуть файл в собственность первоначального владельца. Это не дает администратору получать доступ к файлам, оставаясь незамеченным.

Первоначальный выбор владельца зависит от расположения создаваемого ресурса. В большинстве случаев в роли текущего владельца выступает группа Администраторы (Administrators), а настоящий создатель объекта отмечен как лицо, которое может стать владельцем объекта.

Передавать право владения можно несколькими способами:

- Если изначально владельцем объекта является группа Администраторы (Administrators), владельцем может стать создатель объекта, при условии что его не опередит кто-либо другой.
- Текущий владелец объекта может предоставить другим пользователям разрешение Смена владельца (Take Ownership), которое позволит им стать владельцами объекта.
- Владельцем объекта может стать администратор, при условии что объект входит в область его административной компетенции.

Чтобы стать владельцем объекта, выполните следующие действия:

1. Запустите средство управления объектом. Например, для работы с файлами и папками откройте Проводник Windows (Windows Explorer).
2. Щелкните правой кнопкой объект, владельцем которого хотите стать.
3. В контекстном меню выберите команду **Свойства (Properties)**. В диалоговом окне свойств перейдите на вкладку **Безопасность (Security)**.
4. Откройте диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**, щелкнув кнопку **Дополнительно (Advanced)**.
5. На вкладке **Владелец (Owner)** щелкните кнопку **Изменить (Edit)**, чтобы перейти в редактируемую версию вкладки **Владелец (Owner)**, показанную на рис. 15-10.
6. В списке **Изменить владельца на (Change Owner To)** выберите нового владельца и щелкните **OK**.

Совет Становясь владельцем папки, вы можете одновременно стать владельцем всех подпапок и файлов, находящихся в ней, установив флажок **Заменить владельца подконтейнеров и объектов (Replace Owner On Subcontainers And Objects)**. Эта возможность применима и к другим объектам, содержащим вложенные объекты: вы всегда можете вступить во владение всеми дочерними объектами.

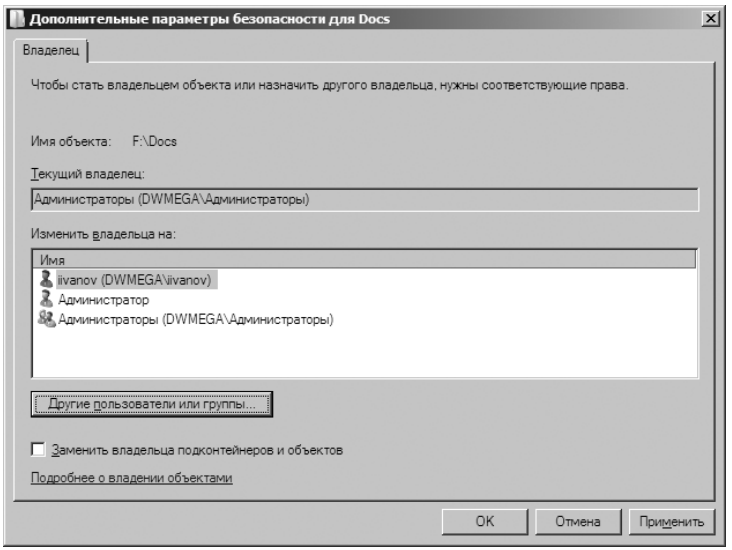


Рис. 15-10. Изменение владельца файла на вкладке Владелец (Owner)

Наследование объектов

Объекты выстроены в структуру с родительскими и дочерними элементами. Родительский объект — объект верхнего уровня. Дочерний объект находится в иерархии под родительским объектом. Например, папка C:\ является родительской для папок C:\Data и C:\Backups. Все подпапки, создаваемые в C:\Data и C:\Backups, становятся дочерними объектами этих папок, и дочерними объектами второго уровня для папки C:\.

Дочерние объекты могут наследовать разрешения от родительских. Больше того, наследование при создании объектов Windows Server 2008 включено по умолчанию. Это означает, что дочерний объект наследует разрешения родительского автоматически. Поэтому доступ к дочерним объектам регулируется разрешениями родительского объекта. Чтобы изменить разрешения дочернего объекта, выполните следующие действия:

1. Отредактируйте разрешения родительского объекта.
2. Отмените наследование разрешений родительского объекта, а затем задайте разрешения дочернего объекта.
3. Чтобы перекрыть наследуемые разрешения, выбирайте противоположные разрешения. Например, если родитель разрешает действие, для дочернего объекта его следует запретить.

Чтобы включить или отменить наследование разрешений родительского объекта, выполните следующие действия:

1. Запустите средство управления объектом. Например, для работы с файлами и папками откройте Проводник Windows (Windows Explorer).
2. Щелкните правой кнопкой объект, с которым хотите работать.

3. Выберите в контекстном меню команду **Свойства (Properties)**. В диалоговом окне свойств перейдите на вкладку **Безопасность (Security)**.
4. Щелкните кнопку **Дополнительно (Advanced)**, чтобы открыть диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**.
5. На вкладке **Разрешения (Permissions)** щелкните кнопку **Изменить (Edit)**, чтобы перейти в редактируемую версию вкладки **Разрешения (Permissions)**.
6. Установите или сбросьте флажок **Добавить разрешения, наследуемые от родительских объектов (Include Inheritable Permissions From This Object's Parent)**. Щелкните **OK**.

Разрешения файлов и папок

На томах NTFS можно задавать разрешения доступа для файлов и папок, открывающие или закрывающие доступ к ним. Чтобы просмотреть разрешения доступа для файлов и папок, выполните следующие действия:

1. В Проводнике Windows (Windows Explorer) щелкните правой кнопкой нужный файл или папку.
2. В контекстном меню выберите команду **Свойства (Properties)**. В диалоговом окне свойств перейдите на вкладку **Безопасность (Security)**.
3. Выделите пользователя, компьютер или группу, разрешения которых хотите просмотреть. Если разрешения недоступны для выделения, они наследуются от родительского объекта.

Введение в разрешения файлов и папок

Основные разрешения для файлов и папок перечислены в табл. 15-3. К разрешениям файлов относятся Полный доступ (Full Control), Изменение (Modify), Чтение и выполнение (Read & Execute), Чтение (Read) и Запись (Write). К разрешениям папок относятся Полный доступ (Full Control), Изменение (Modify), Чтение и выполнение (Read & Execute), Список содержимого папки (List Folder Contents), Чтение (Read) и Запись (Write).

Табл. 15-3. Разрешения файлов и папок в Windows Server 2008

Разрешение	Значение для папок	Значение для файлов
Чтение (Read)	Разрешает просмотр и вывод списка файлов и подпапок	Разрешает просмотр или доступ к содержимому файла
Запись (Write)	Разрешает добавление файлов и подпапок	Разрешает запись в файл
Чтение и выполнение (Read & Execute)	Разрешает просмотр и вывод списка файлов и подпапок, а также выполнение файлов; наследуется файлами и папками	Разрешает просмотр или доступ к содержимому файла, а также выполнение файла

Табл. 15-3. (*окончание*)

Разрешение	Значение для папок	Значение для файлов
Список содержимого папки (List Folder Contents)	Разрешает просмотр и вывод списка файлов и подпапок, а также выполнение файлов; наследуется только папками	Недоступно
Изменение (Modify)	Разрешает чтение и запись в файлы и папки; разрешает удаление папки	Разрешает чтение и запись в файлы; разрешает удаление файла
Полный доступ (Full Control)	Разрешает чтение, запись, изменение и удаление файлов и подпапок	Разрешает чтение, запись, изменение и удаление файла

Работая с файлами, помните о следующем:

- Для запуска сценария достаточно разрешения Чтение (Read). Разрешения на выполнение не требуется.
- Для доступа к ярлыку и целевому объекту требуется разрешение Чтение (Read).
- Разрешение на запись, но не на удаление файла не запрещает пользователю удалить все содержимое файла.
- Если пользователь имеет полный доступ к папке, он может удалять файлы в ней независимо от разрешений файлов.

Основные разрешения создаются путем объединения особых разрешений в логические группы. В табл. 15-4 перечислены особые разрешения, из которых создаются основные разрешения для файлов. При необходимости вы можете назначать особые разрешения индивидуально, используя для этого дополнительные параметры безопасности. Рассматривая особые разрешения, помните о следующем:

- По умолчанию, если доступ явным образом ни предоставлен, ни запрещен, он считается запрещенным.
- Действия, доступные пользователю, основаны на сумме всех разрешений, предоставленных пользователю и всем группам, членом которых он является. В частности, если пользователь GeorgeJ имеет разрешение Чтение (Read) и является членом группы Techies, имеющей разрешение Изменение (Modify), GeorgeJ будет предоставлено разрешение Изменение (Modify). Если группа Techies, в свою очередь, является членом группы Администраторы (Administrators), которая обладает разрешением Полный доступ (Full Control), у GeorgeJ будет полный доступ к файлу.

Табл. 15-4. Особые разрешения для файлов

	Основные разрешения				
Особые разрешения	**Полный доступ (Full Control)**	**Изменение (Modify)**	**Чтение и выполнение (Read & Execute)**	**Чтение (Read)**	**Запись (Write)**
Траверс папок / выполнение файлов (Traverse Folder / Execute File)	Да	Да	Да		
Содержание папки / выполнение данных (List Folder / Read Data)	Да	Да	Да	Да	
Чтение атрибутов (Read Attributes)	Да	Да	Да	Да	
Чтение дополнительных атрибутов (Read Extended Attributes)	Да	Да	Да	Да	
Создание файлов / запись данных (Create Files/Write Data)	Да	Да			Да
Создание файлов / дозапись данных (Create Folders/ Append Data)	Да	Да			Да
Запись атрибутов (Write Attributes)	Да	Да			Да
Запись дополнительных атрибутов (Write Extended Attributes)	Да	Да			Да
Удаление подпапок и файлов (Delete Subfolders and Files)	Да				
Удаление (Delete)	Да	Да			
Чтение разрешений (Read Permissions)	Да	Да	Да	Да	Да
Смена разрешений (Change Permissions)	Да				
Смена владельца (Take Ownership)	Да				

В табл. 15-5 приведены особые разрешения, из которых создаются основные полномочия для папок. При назначении особых полномочий имейте ввиду следующее:

- Задавая разрешения для родительских папок, вы можете включить принудительное наследование разрешений для всех файлов и подпапок внутри папки, установив флажок **Заменить все наследуемые разрешения для всех потомков на новые наследуемые разрешения от этого объекта (Reset Permissions On All Child Objects And Enable Propagation Of Inheritable Permissions)**.
- Создаваемые вами файлы и папки наследуют определенные разрешения. Эти разрешения отображены в виде разрешений файлов по умолчанию.

Табл. 15-5. Особые разрешения папок

	Основные разрешения					
Особые разрешения	**Полный доступ (Full Control)**	**Изменение (Modify)**	**Чтение и выполнение (Read & Execute)**	**Список содержимого папки (List Folder Contents)**	**Чтение (Read)**	**Запись (Write)**
Траверс папок/выполнение файлов (Traverse Folder/Execute File)	Да	Да	Да	Да		
Содержание папки /выполнение данных (List Folder /Read Data)	Да	Да	Да	Да	Да	
Чтение атрибутов (Read Attributes)	Да	Да	Да	Да	Да	
Чтение дополнительных атрибутов (Read Extended Attributes)	Да	Да	Да	Да	Да	
Создание файлов /запись данных (Create Files/ Write Data)	Да	Да				Да
Создание файлов /дозапись данных (Create Folders /Append Data)	Да	Да				Да
Запись атрибутов (Write Attributes)	Да	Да				Да

Табл. 15-5. (*окончание*)

	Основные разрешения					
Особые разрешения	**Полный доступ (Full Control)**	**Изменение (Modify)**	**Чтение и выполнение (Read & Execute)**	**Список содержимого папки (List Folder Contents)**	**Чтение (Read)**	**Запись (Write)**
Запись дополнительных атрибутов (Write Extended Attributes)	Да	Да				Да
Удаление подпапок и файлов (Delete Subfolders And Files)	Да					
Удаление (Delete)	Да	Да				
Чтение разрешений (Read Permissions)	Да	Да	Да	Да	Да	Да
Смена разрешений (Change Permissions)	Да					
Смена владельца (Take Ownership)	Да					

Настройка разрешений файлов и папок

Чтобы задать разрешения для файлов и папок, выполните следующие действия:

1. В Проводнике Windows (Windows Explorer) щелкните правой кнопкой нужный файл или папку.
2. В контекстном меню выберите **Свойства (Properties)**. В диалоговом окне свойств перейдите на вкладку **Безопасность (Security)**.
3. Щелкните кнопку **Изменить (Edit)**, чтобы перейти к редактируемой версии вкладки **Безопасность (Security)**, показанной на рис. 15-11.
4. Пользователи и группы, уже обладающие доступом к файлу или папке, перечислены в списке **Группы или пользователи (Group Or User Names)**. Следующие действия помогут вам изменить разрешения этих пользователей и групп:
   - Выберите пользователя или группу, которую хотите изменить.

- В списке **Разрешения (Permissions)** предоставьте или отзовите разрешения доступа.

Совет Наследуемые разрешения недоступны для редактирования. Чтобы перекрыть наследуемое разрешение, установите противоположное разрешение.

Рис. 15-11. Настройка основных разрешений файлов и папок на вкладке Безопасность (Security)

5. Чтобы задать разрешения доступа для других пользователей, компьютеров и групп, щелкните **Добавить (Add)**. Откроется диалоговое окно **Выбор: «Пользователи», «Компьютеры» или «Группы» (Select Users, Computers, Or Groups)**, показанное на рис. 15-12.

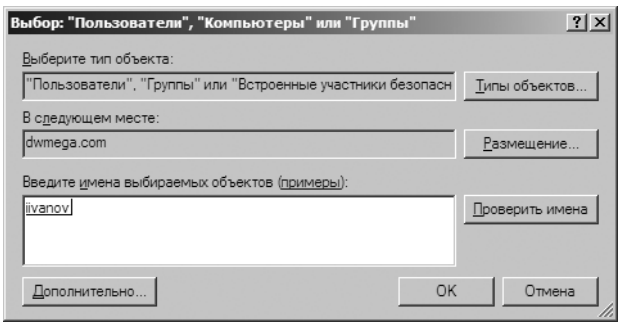


Рис. 15-12. Выберите пользователей, компьютеры или группы, которым следует предоставить или запретить доступ

6. Введите имя пользователя, компьютера или группы в текущем домене и щелкните **Проверить имена (Check Names)**.
   - Если обнаружится одно совпадение, соответствующее имя пользователя будет автоматически добавлено в диалоговое окно.

- Если совпадений не найдено, вы ввели ошибочное имя или работаете в неверном расположении. Исправьте имя или щелкните кнопку **Размещение (Locations)**, чтобы задать другое место для поиска.
- Если найдено несколько совпадений, выберите нужное имя или имена и щелкните **OK**. Чтобы предоставить разрешения другим пользователям, компьютерам или группам, поставьте после найденного имени точку с запятой и повторите поиск.

Примечание Кнопка **Размещение (Locations)** позволяет получить доступ к учетным записям из других доменов. Щелкните ее, чтобы просмотреть доступные размещения. Благодаря транзитивным доверительным отношениям в Windows Server 2008 вы сможете выбирать записи из большинства доменов дерева или леса.

7. В списке имен выберите пользователя, компьютер или группу, которую хотите настроить. Далее устанавливайте или сбрасывайте флажки в области **Разрешения (Permissions)**, разрешая или запрещая соответствующие действия. Повторите действие для других пользователей, компьютеров или групп.
8. Завершив настройку, щелкните **OK**.

Аудит системных ресурсов

Лучший способ проследить за тем, что делается в системе Windows Server 2008, — это аудит, с помощью которого вы собираете информацию об использовании ресурсов, например, о доступе к файлам, входе в систему и об изменениях системной конфигурации. Каждый раз, когда происходит действие, для которого настроен аудит, информация об этом записывается в системный журнал безопасности. Журнал безопасности можно просмотреть в консоли **Просмотр событий (Event Viewer)**.

Примечание В большинстве случаев, чтобы изменять политики аудита, необходимо использовать учетную запись, принадлежащую к группе Администраторы (Administrators), или любую запись, которой при помощи групповой политики предоставлено право Управление аудитом и журналом безопасности (Manage Auditing And Security Log).

Настройка политик аудита

Политики аудита необходимы для обеспечения безопасности и целостности системы. Практически на всех компьютерах сети необходим какой-либо способ регистрации событий системы безопасности. Для отдельных компьютерах политики аудита настраиваются при помощи локальных групповых политик, а для всех компьютеров домена — при помощи групповой политики Active Directory. Групповая политика позволяет задавать политики аудита в масштабах всего сайта, домена или подразделения. Вы также можете настроить политики для отдельной рабочей станции или сервера.

Получив доступ к объекту GPO, с которым вы хотите работать, выполните следующие действия для настройки политики аудита:

1. В дереве консоли редактора групповой политики последовательно разверните узлы **Конфигурация компьютера (Computer Configuration)**, **Конфигурация Windows (Windows Settings)**, **Параметры безопасности (Security Settings)** и **Локальные политики (Local Policies)**. Затем выделите узел **Политика аудита (Audit Policy)**, как показано на рис. 15-13.

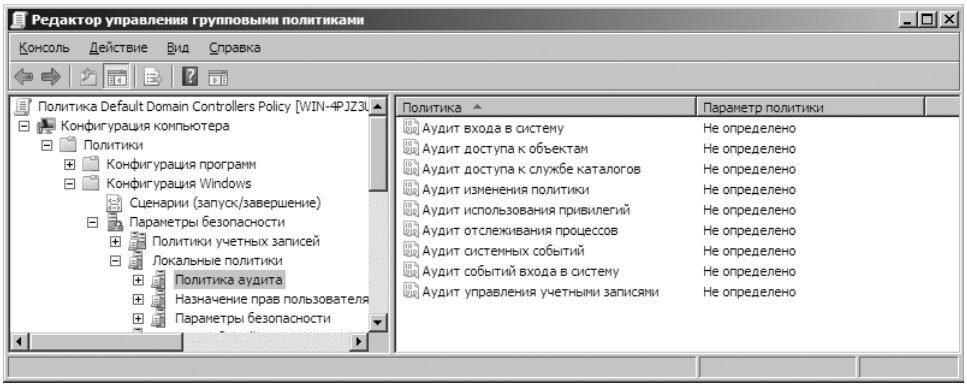


Рис. 15-13. Настройка политик аудита при помощи редактора групповой политики

2. Настройте следующие возможности аудита:
   - **Аудит входа в систему (Audit Logon Events)** Отслеживание событий, относящихся к входу и выходу пользователя из системы, а также к удаленным подключениям к сетевым системам.
   - **Аудит доступа к объектам (Audit Object Access)** Наблюдение за использованием файлов, папок, общих ресурсов, принтеров и объектов Active Directory.
   - **Аудит доступа к службе каталогов (Audit Directory Service Access)** Наблюдение за доступом к Active Directory. События создаются при каждом обращении пользователей или компьютеров к каталогу.
   - **Аудит изменения политики (Audit Policy Change)** Отслеживание изменений в правах пользователя, аудите и доверительных отношениях.
   - **Аудит использования привилегий (Audit Privilege Use)** Наблюдение за использованием прав и привилегий пользователей, таких как право на резервное копирование файлов и каталогов.

Примечание Политика **Аудит использования привилегий (Audit Privilege Use)** не отслеживает события, относящиеся к доступу в систему, например, использование права на интерактивный вход или права на доступ к компьютеру по сети. Эти события отслеживаются при помощи аудита входа и выхода.

   - **Аудит отслеживания процессов (Audit Process Tracking)** Отслеживание системных процессов и используемых ими ресурсов.
   - **Аудит системных событий (Audit System Events)** Отслеживание запуска, завершения работы и перезагрузки системы, а также действий, затрагивающих безопасность системы или журнал безопасности.

- **Аудит событий входа в систему (Audit Account Logon Events)** Отслеживание событий, относящихся к входу и выходу пользователя из системы.
- **Аудит управления учетными записями (Audit Account Management)** Отслеживание управления учетными записями средствами консоли **Active Directory — пользователи и компьютеры (Active Directory Users And Computers)**. События создаются при каждом создании, изменении или удалении учетной записи пользователя, компьютера или группы.

3. Чтобы настроить политику аудита, дважды щелкните ее или щелкните правой кнопкой и выберите команду **Свойства (Properties)**. Откроется диалоговое окно свойств политики.
4. Установите флажок **Определить следующие параметры политики (Define These Policy Settings)**, а затем установите флажок **Успех (Success)**, **Отказ (Failure)** или оба флажка. Аудит успехов регистрирует успешные события, например, успешный вход в систему. Аудит отказов фиксирует неудачи, например, неудачные попытки входа в систему.
5. Завершив настройку, щелкните **OK**.

При включенном аудите в журнале Безопасность (Security Event) будет отображаться следующие события:

- события с кодами 560 и 562, относящиеся к аудиту пользователей;
- события с кодами 592 и 593, относящиеся к аудиту процессов.

Аудит файлов и папок

Если вы настраиваете групповую политику для включения политики Аудит доступа к объектам (Audit Object Access), имейте в виду, что уровень аудита можно задавать для отдельных файлов и папок. Это позволяет детально отслеживать использование папок и файлов. Аудит такого рода возможен только на NTFS-томах.

Чтобы настроить аудит файлов и папок, выполните следующие действия:

1. В Проводнике Windows (Windows Explorer) щелкните правой кнопкой файл или папку, для которых хотите настроить аудит. В контекстном меню выберите команду **Свойства (Properties)**.
2. Перейдите на вкладку **Безопасность (Security)** и щелкните кнопку **Дополнительно (Advanced)**. Откроется диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**.
3. На вкладке **Аудит (Auditing)** щелкните кнопку **Изменить (Edit)**. Теперь вы можете приступить к просмотру и управлению параметрами аудита посредством параметров, показанных на рис. 15-14.

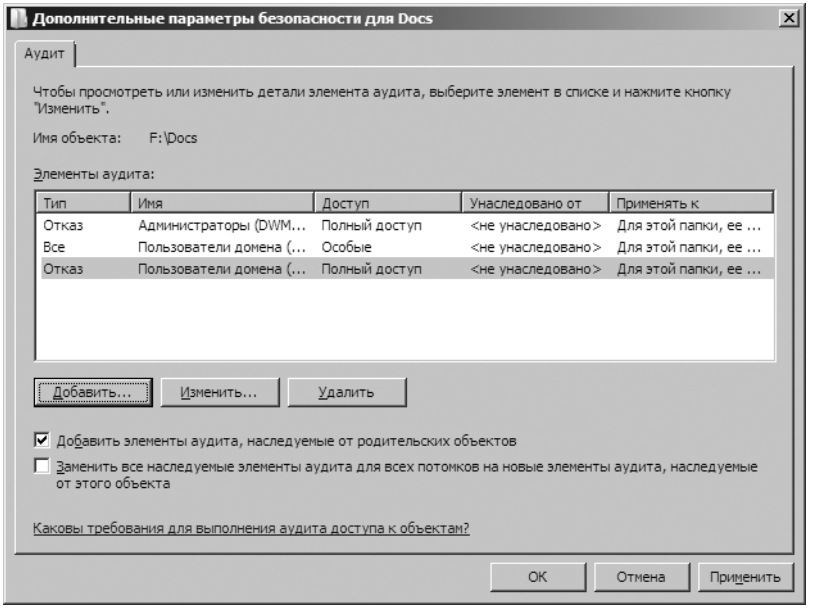


Рис. 15-14. Настройте аудит отдельных файлов и папок на вкладке Аудит (Auditing)

4. Если требуется наследование параметров аудита от родительского объекта, убедитесь, что установлен флажок **Добавить элементы аудита, наследуемые от родительских объектов (Include Inheritable Auditing Entries From This Object's Parent)**.
5. Если требуется, чтобы дочерние объекты текущего объекта наследовали его параметры, установите флажок **Заменить все наследуемые элементы аудита для всех потомков на новые элементы аудита, наследуемые от этого объекта (Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object)**.
6. В список **Элементы аудита (Auditing Entries)** включите пользователей, группы или компьютеры, действия которых хотите отслеживать. Чтобы удалить учетную запись, выделите ее в списке **Элементы аудита (Auditing Entries)** и щелкните **Удалить (Remove)**.
7. Чтобы добавить новые учетные записи, щелкните **Добавить (Add)** и в диалоговом окне **Выбор: «Пользователь», «Компьютер» или «Группа» (Select User, Computer, Or Group)** укажите имя добавляемой учетной записи. Щелкнув **OK**, вы увидите диалоговое окно **Элемент аудита для (Auditing Entry For)**, показанное на рис. 15-15.

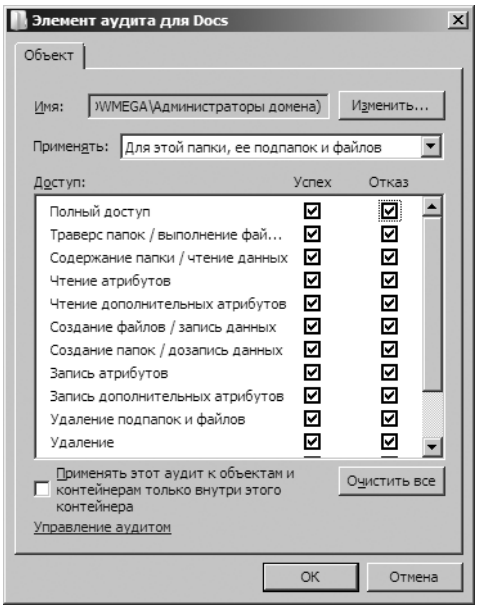


Рис. 15-15. Задайте элементы аудита для пользователя, компьютера или группы

Совет Если вы хотите осуществлять аудит действий всех пользователей, используйте специальную группу Все (Everyone). В противном случае выберите определенных пользователей или группы (или тех и других), аудит которых вы хотите проводить.

8. При необходимости укажите область выполнения аудита в раскрывающемся списке **Применять (Apply Onto)**.
9. Установите флажки в столбцах **Успех (Successful)** или **Отказ (Failed)** (или в обоих столбцах) напротив каждого события, аудит которого хотите осуществлять. Аудит успехов соответствует успешным событиям, например, удачному чтению файла. Аудит отказов регистрирует неудачи, например, неудачные удаления файлов. События, подлежащие аудиту, совпадают со специальными разрешениями, перечисленными в табл. 15-5, за исключением того что аудит синхронизации автономных файлов и папок невозможен. Для важных файлов и папок обычно следует контролировать следующие задачи аудита:
   - Запись атрибутов (Write Attributes) — успех;
   - Запись дополнительных атрибутов (Write Extended Attributes) — успех;
   - Удаление подпапок и файлов (Delete Subfolders and Files) — успех;
   - Удаление (Delete) — успех;
   - Смена разрешений (Change Permissions) — успех.
10. Завершив настройку, щелкните **OK**. Повторите действия для настройки аудита других пользователей, групп или компьютеров.

Аудит реестра

Включив политику Аудит доступа к объектам (Audit Object Access), вы можете настроить аудит разделов реестра. Это позволяет отследить изменение значений параметров, создание подразделов и удаление разделов.

Чтобы настроить аудит реестра, выполните следующие действия:

1. В командной строке введите команду **regedit**.
2. Найдите раздел, аудит которого хотите настроить. Выберите в меню **Правка (Edit)** команду **Разрешения (Permissions)**.
3. В диалоговом окне **Разрешения для (Permissions For)** щелкните кнопку **Дополнительно (Advanced)**. В диалоговом окне **Дополнительные параметры безопасности (Advanced Security Settings)** перейдите на вкладку **Аудит (Auditing)**.
4. Щелкните **Добавить (Add)**. В диалоговом окне **Выбор: «Пользователь», «Компьютер» или «Группа» (Select User, Computer, Or Group)** введите **Все (Everyone)**, щелкните **Проверить имена (Check Names)** и **OK**.
5. В диалоговом окне **Элемент аудита для (Auditing Entry For)** выберите действия, аудит которых хотите выполнять. Существуют следующие типичные задачи аудита:
   - Задание значения (Set Value) — успех и отказ;
   - Создание подраздела (Create Subkey) — успех и отказ;
   - Удаление (Delete) — успех и отказ.
6. Щелкните **OK**.
7. Два раза щелкните **OK**, чтобы закрыть все открытые диалоговые окна и применить параметры аудита.

Аудит объектов Active Directory

Включив политику Аудит доступа к объектам (Audit Object Access), вы можете настроить аудит объектов Active Directory. Это позволяет детально следить за использованием объектов.

Чтобы настроить аудит объектов Active Directory, выполните следующие действия:

1. В консоли Active Directory — пользователи и компьютеры (Active Directory Users And Computers) выберите в меню **Вид (View)** команду **Дополнительные компоненты (Advanced Features)**, если она еще не выбрана, и откройте нужный контейнер.
2. Щелкните правой кнопкой объект, подлежащий аудиту, и выберите в контекстном меню команду **Свойства (Properties)**.
3. Перейдите на вкладку **Безопасность (Security)** и щелкните **Дополнительно (Advanced)**.
4. В диалоговом окне **Дополнительные параметры безопасности (Advanced Security Settings)** перейдите на вкладку **Аудит (Auditing)**. Если

требуется наследование параметров аудита от родительского объекта, убедитесь, что установлен флажок **Добавить элементы аудита, наследуемые от родительских объектов (Include Inheritable Auditing Entries From This Object's Parent)**.

5. В список **Элементы аудита (Auditing Entries)** включите пользователей, группы или компьютеры, действия которых хотите отслеживать. Чтобы удалить учетную запись, выделите ее в списке **Элементы аудита (Auditing Entries)** и щелкните **Удалить (Remove)**.
6. Чтобы добавить новые учетные записи, щелкните **Добавить (Add)** и в диалоговом окне **Выбор: «Пользователь», «Компьютер» или «Группа» (Select User, Computer, Or Group)** укажите имя добавляемой учетной записи. Щелкнув **OK**, вы увидите диалоговое окно **Элемент аудита для (Auditing Entry For)**.
7. При необходимости укажите область выполнения аудита в раскрывающемся списке **Применять (Apply Onto)**.
8. Установите флажки в столбцах **Успех (Successful)** или **Отказ (Failed)** (или в обоих столбцах) напротив каждого события, аудит которого хотите осуществлять. Аудит успехов соответствует успешным событиям, например, удачному изменению разрешений файлов. Аудит отказов регистрирует неудачи, например, неудачные попытки изменения владельца объекта.
9. Завершив настройку, щелкните **OK**. Повторите действия для настройки аудита других пользователей, групп или компьютеров.

Дисковые квоты NTFS

Система Windows Server 2008 поддерживает два типа дисковых квот:

- **Дисковые квоты NTFS** Поддерживаются всеми версиями Windows Server 2008 и позволяют управлять использованием дискового пространства. Дисковые квоты настраиваются для каждого тома. Превысившие лимит пользователи получают уведомления, администраторы же узнают о превышении квоты из журналов событий.
- **Дисковые квоты диспетчера ресурсов** Поддерживаются Windows Server 2008 и позволяют управлять использованием дискового пространства в папке или на томе. Пользователи, приблизившиеся к пределу или превысившие его, могут автоматически оповещаться по электронной почте. Система оповещения также способна уведомлять администраторов по электронной почте, создавать отчеты об инцидентах, выполнять команды и регистрировать события.

  В следующем разделе рассказывается о дисковых квотах NTFS.

Примечание Квоты обоих типов настраиваются только на томах NTFS. Нельзя создать квоты для томов FAT или FAT32.

Использование дисковых квот NTFS

Администраторы применяют дисковые квоты NTFS, чтобы управлять использованием дискового пространства на важных томах, в частности, томах, содержащих корпоративные и пользовательские общие ресурсы. В процессе настройки дисковых квот NTFS вы задаете два значения:

- **Предел дисковой квоты (disk quota limit)** Верхняя граница использования дискового пространства, используется для предотвращения записи на том чрезмерных объемов данных, для регистрации событий превышения предела или для того и другого сразу.
- **Предупреждение дисковой квоты (disk quota warning)** Уведомляет пользователя о скором превышении квоты и записывает соответствующее предупреждение в журнал.

Совет Установка дисковой квоты не обязательно подразумевает запрет на превышение предела. Иногда достаточно просто следить за использованием дискового пространства конкретными пользователями, своевременно узнавая о превышении ими определенного предела. Когда это происходит, вы не отказываете пользователю в дополнительном пространстве, но записываете событие в журнал приложения. После этого пользователю можно послать уведомление или придумать другие способы экономии дискового пространства.

Дисковые квоты NTFS применимы только к конечным пользователям, но не к администраторам. Администратору нельзя отказать в использовании дискового пространства, даже если он превысил ограничение.

В типичной среде используемое дисковое пространство измеряется в мегабайтах или гигабайтах данных. Например, на общем корпоративном ресурсе, который используется несколькими пользователями отдела, вы можете задать предел квоты от 20 до 100 Гб. На пользовательском общем ресурсе допустим более низкий порог, например, от 5 до 25 Гб, который не даст пользователю накапливать большие объемы личных данных. Предупреждения дисковых квот часто задаются в зависимости от доли использования квоты. Например, вы можете задать выдачу предупреждения об использовании 90–95% от предела дисковой квоты.

Дисковые квоты NTFS на каждом томе отслеживаются для конкретного пользователя. Поэтому дисковое пространство, используемое одним пользователем, не влияет на дисковые квоты других. В случае превышения пользователем предела все налагаемые на него ограничения не затрагивают других пользователей. Если пользователь превысит предел дисковой квоты, например, в 1Гб, а настройки тома запрещают запись в случае превышения квоты, пользователь не сможет записывать данные на том. Но ему разрешено удалять из тома файлы и папки, чтобы освободить дисковое пространство, а также перемещать файлы и папки в сжатую область тома или сжимая сами файлы. Перемещение файлов в другое расположение на томе не влияет на квоту. Объем занятого пользователем пространства останется прежним, пока он не переместит несжатые файлы и папки в сжатые папки. В любом случае, огра-

ничения одного пользователя не влияют на возможности других пользователей выполнять запись на том (если на томе есть свободное место).

Дисковые квоты NTFS применяются к следующим объектам:

- **Локальные тома** Чтобы управлять дисковыми квотами на локальных томах, следует настраивать сами диски. При установке дисковых квот на локальном томе системные файлы Windows расцениваются как использование тома пользователем, установившим Windows. В некоторых случаях это приводит к превышению пользователем предела дисковой квоты. Во избежание этого ограничения следует увеличить предел квоты на использование тома локальной рабочей станции.
- **Удаленные тома** Чтобы управлять дисковыми квотами на удаленных томах, следует открыть общий доступ к корневой папке тома и установить дисковые квоты для тома. Помните, что вы задаете квоты для конкретного тома. Если на удаленном файловом сервере для разных типов данных предназначены отдельные тома, например, тома корпоративных и пользовательских данных, дисковые квоты на этих томах будут отличаться.

Настраивать дисковые квоты имеют право только члены групп с полномочиями администраторов домена или локальных администраторов. Первый шаг в использовании квот — это их включение в групповой политике. Существует два уровня включения квот:

- **Локальный уровень** Дисковые квоты для отдельного компьютера включаются посредством локальной групповой политики.
- **Уровень предприятия** Дисковые квоты для групп пользователей и компьютеров включаются посредством групповой политики сайта, домена и подразделения.

Отслеживание дисковых квот приводит к появлению на компьютерах некоторого количества служебных данных. Их объем зависит от числа включенных дисковых квот, общего размера томов и объема информации на них, а также от числа пользователей, к которым применены дисковые квоты.

Хотя внешне дисковые квоты отслеживаются по именам пользователей, на самом деле Windows Server 2008 управляет дисковыми квотами на основании идентификаторов безопасности SID. Поэтому вы можете спокойно менять имена пользователей, не влияя на конфигурацию квот. При просмотре статистики дисковых квот использование SID приводит к некоторой дополнительной нагрузке на компьютер, так как ОС Windows Server 2008 должна сопоставить SID с именами учетных записей для отображения в окне. Это подразумевает обмен данными между диспетчером локальных пользователей и контроллером домена Active Directory.

Проведя поиск имен, Windows Server 2008 кеширует их в локальном файле, поэтому при следующем обращении доступ к ним будет мгновенный. Обновление кеша запросов происходит не часто. Если вы заметили несоответствие между отображаемыми и реальными настройками, обновите информацию. Обычно для этого нужно выбрать команду **Обновить (Refresh)** в меню **Вид (View)** или нажать клавишу F5.

Настройка политик дисковых квот NTFS

Эффективнее всего настраивать дисковые квоты NTFS посредством групповой политики. При этом вы определяете общие политики, настраиваемые автоматически, когда вы включаете управление квотами на отдельных томах. Вместо индивидуальной настройки каждого тома вы можете взять один набор правил и применять его к каждому тому, которым управляете.

Политики, управляющие дисковыми квотами NTFS, применяются на уровне системы и находятся в узле **Конфигурация компьютера\Административные шаблоны\Система\Дисковые квоты (Computer Configuration\Administrative Templates\System\Disk Quotas)**. Доступные политики перечислены в табл. 15-6.

Табл. 15-6. Политики дисковых квот NTFS

Имя политики	Описание
Включить дисковые квоты (Enable Disk Quotas)	Включает или отключает дисковые квоты на всех NTFS-томах компьютера и не дает пользователям изменять данный параметр
Задать предел дисковой квоты (Enforce Disk Quota Limit)	Задает принудительное применение пределов квоты. В случае превышения квоты пользователю будет отказано в дисковом пространстве. При этом перекрывается параметр, установленный на вкладке **Квота (Quota)** окна свойств NTFS-тома
Предел квоты по умолчанию и уровень предупреждения (Default Quota Limit And Warning Level)	Задает стандартный предел и порог предупреждения для всех пользователей. Этот параметр перекрывает другие параметры и влияет только на новых пользователей
Записывать в журнал события при превышении предела квоты (Log Event When Quota Limit Exceeded)	Определяет, следует ли записывать в журнал события превышения предела и запрещает пользователям изменять параметры протоколирования событий
Записывать в журнал события, возникающие при превышении уровня предупреждения квоты (Log Event When Quota Warning Level Exceeded)	Определяет, следует ли записывать в журнал события достижения пользователями порога предупреждения
Применить политику к съемным носителям (Apply Policy To Removable Media)	Определяет, следует ли применять политики квот к NTFS-томам на съемных дисках. Если не включить эту политику, пределы квот будут действовать только на несъемных дисковых накопителях

В работе с пределами квот всегда следует придерживаться стандартного набора политик на всех системах. Как правило, включают не все политики, а лишь некоторые. Затем для управления квотами на различных томах ис-

пользуются стандартные функции NTFS. Чтобы включить пределы квот, выполните следующие действия:

1. Откройте в редакторе нужную групповую политику, например, для файлового сервера. Затем разверните узел **Конфигурация компьютера\Административные шаблоны\Система (Computer Configuration\Administrative Templates\System)** и выберите элемент **Дисковые квоты (Disk Quotas)**.
2. Дважды щелкните политику **Включить дисковые квоты (Enable Disk Quotas)**. На вкладке **Параметр (Setting)** установите переключатель **Включен (Enabled)** и щелкните **OK**.
3. Дважды щелкните политику **Задать предел дисковой квоты (Enforce Disk Quota Limit)**. Если вы хотите ограничить использование пространства на всех NTFS-томах данного компьютера, установите переключатель **Включен (Enabled)**. В противном случае установите переключатель **Отключен (Disabled)** и задайте пределы для отдельных томов. Щелкните **OK**.
4. Дважды щелкните политику **Предел квоты по умолчанию и уровень предупреждения (Default Quota Limit And Warning Level)**. В диалоговом окне свойств, показанном на рис. 15-16, установите переключатель **Включен (Enabled)**.

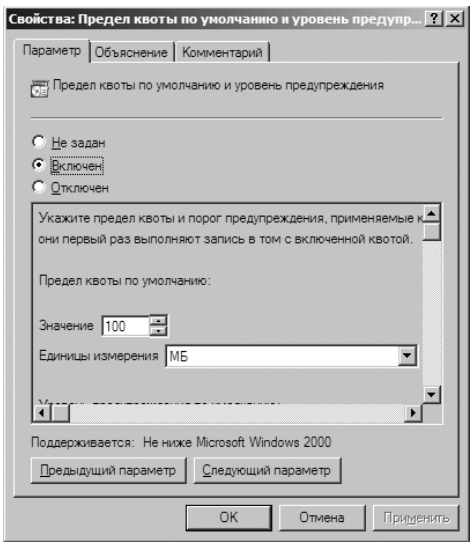


Рис. 15-16. Ограничение использования дискового пространства в диалоговом окне свойств политики Предел квоты по умолчанию и уровень предупреждения (Default Quota Limit And Warning Level)

5. В разделе **Предел квоты по умолчанию (Default Quota Limit)** задайте предел по умолчанию, назначаемый пользователям при первой записи в том с включенными квотами. Этот предел не применяется к текущим пользователям и не затрагивает текущие пределы тома. На корпоративном общем ресурсе типичные значения предела составляют 500–1000 Мб.

Конечно, все зависит от размера файлов, с которыми обычно работают пользователи, количества пользователей и объема диска. Дизайнерам и инженерам по обработке данных может потребоваться гораздо больше дискового пространства.

6. Чтобы установить уровень предупреждения, прокрутите подокно на вкладке **Параметр (Setting)**. Типичный уровень предупреждения составляет приметно 90% от предела квоты. Это означает, что при стандартном пределе в 1000 Мб следует установить уровень предупреждения 900 Мб. Щелкните **OK**.
7. Дважды щелкните политику **Записывать в журнал события при превышении предела квоты (Log Event When Quota Limit Exceeded)**. Чтобы записывать события квоты в журнал Приложение (Application), установите переключатель **Включен (Enabled)** и щелкните **OK**.
8. Дважды щелкните политику **Записывать в журнал события, возникающие при превышении уровня предупреждения квоты (Log Event When Quota Warning Level Exceeded)**. Чтобы записывать предупреждения в журнал Приложение (Application), установите переключатель **Включен (Enabled)** и щелкните **OK**.
9. Дважды щелкните политику **Применить политику к съемным носителям (Apply Policy To Removable Media)** и установите переключатель **Отключен (Disabled)**, чтобы ограничения квот применялись только к томам на несъемных носителях.

Совет Чтобы обеспечить немедленное принудительное применение политик, откройте узел **Конфигурация компьютера\Административные шаблоны\Система\Групповая политика (Computer Configuration\Administrative Templates\System\Group Policy)**, затем дважды щелкните политику **Обработка политики дисковых квот (Disk Quota Policy Processing)**. Установите переключатель **Включен (Enabled)** и флажок **Обрабатывать, даже если объекты групповой политики не изменились (Process Even If The Group Policy Objects Have Not Changed)**. Щелкните **OK**.

Включение квот файловой системы на NTFS-томах

Дисковые квоты NTFS настраиваются отдельно для каждого тома и могут существовать только на NTFS-томах. Настроив соответствующие групповые политики, вы настроите дисковые квоты для локальных и удаленных томов при помощи консоли **Управление компьютером (Computer Management)**.

Примечание Если для ограничения использования дискового пространства вы включили политику **Задать предел дисковой квоты (Enforce Disk Quota Limit)**, при превышении квоты пользователям будет отказано в дисковом пространстве. Действие параметра, заданного на вкладке **Квота (Quota)** окна свойств NTFS-тома, перекрывается.

Чтобы включить дисковые квоты на NTFS-томе, выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)**. При необходимости подключитесь к удаленному компьютеру.

2. В дереве консоли разверните узел **Запоминающие устройства (Storage)** и выберите элемент **Управление дисками (Disk Management)**. Тома, настроенные на выбранном компьютере, отображаются в области сведений.
3. В представлении **Список томов (Volume List)** или **Графическое представление (Graphical View)** щелкните правой кнопкой том, с которым хотите работать, и выберите команду **Свойства (Properties)**.
4. На вкладке **Квота (Quota)** установите флажок **Включить управление квотами (Enable Quota Management)**, как показано на рис. 15-17. Если вы уже задали значения параметров управления квотами в групповой политике, параметры вкладки **Квота (Quota)** будут недоступны, и вы не сможете изменить их. Вместо этого вам придется изменять параметры самой групповой политики.

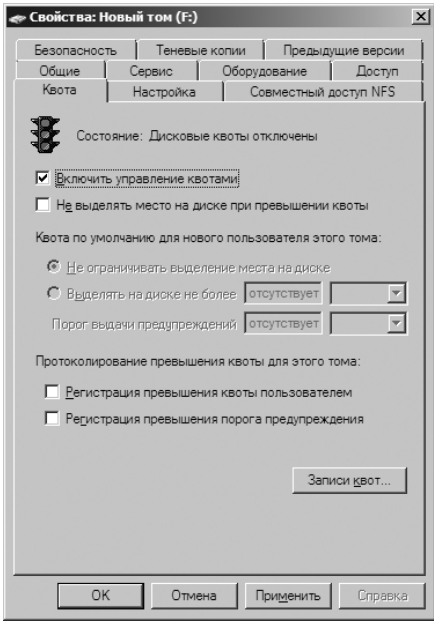


Рис. 15-17. Включив управление квотами, вы можете настроить пределы и предупреждения квот для всех пользователей

Примечание Работая с вкладкой **Квота (Quota)**, обращайте особое внимание на поле **Состояние (Status)** и расположенный радом значок светофора. Оба элемента изменяются в соответствии с состоянием управления квотами. Если квоты не настроены, на светофоре горит красный сигнал, а в поле **Состояние (Status)** написано, что квоты отключены. Если квоты находятся в процессе создания или обновления, на светофоре горит желтый сигнал, а в поле **Состояние (Status)** отображается действие, выполняемое в данный момент. Когда квоты настроены, на светофоре горит зеленый сигнал.

5. Чтобы установить квоту по умолчанию для всех пользователей, установите переключатель **Выделять на диске не более (Limit Disk Space To)**, а в расположенных рядом полях задайте предел в Кб, Мб, Гб, Тб, Пб или

Эб. Затем задайте уровень предупреждения в поле **Порог выдачи предупреждений (Set Warning Level To)**. Напомню, что уровень предупреждения обычно составляет 90-95% от дисковой квоты.

Совет Хотя стандартные ограничения и пороги предупреждения квот касаются всех пользователей, вы также можете настроить различные пределы для разных пользователей. Это делается в диалоговом окне **Записи квот (Quota Entries)**. Если вы создали много уникальных записей квот и не желаете заново создавать их на томе со сходными характеристиками, экспортируйте записи и импортируйте их на другом томе.

6. Чтобы ограничить выделение места на диске и не дать пользователям превысить предел, установите флажок **Не выделять место на диске при превышении квоты (Deny Disk Space To Users Exceeding Quota Limit)**. Помните, что этим вы создадите реальные физические ограничения для пользователей (не для администраторов).
7. Чтобы задать регистрацию превышений квоты или уровня предупреждения, установите флажки **Регистрация превышения (Log Event)**. Щелкните **OK**, чтобы сохранить изменения.
8. Если система квот в данный момент выключена, вам будет предложено включить ее. Щелкните **OK**, чтобы разрешить Windows Server 2008 повторно просмотреть том и обновить статистику использования диска. К пользователям, превысившим текущий предел или уровень предупреждения, могут быть приняты меры, включающие запрет записи на том дополнительных данных, уведомление во время следующего обращения к тому и запись соответствующих событий в журнал Приложение (Application).

Просмотр записей квот

Использование дискового пространства отслеживается на уровне пользователя. Когда дисковые квоты включены, каждому пользователю, хранящему данные на диске, соответствует запись в файле квот диска. Запись периодически обновляется, отображая используемое пространство на текущем диске, предел квоты, уровень предупреждения и долю использования допустимого пространства. Администратор может изменять записи квот, чтобы задать для отдельных пользователей другие пределы и уровни предупреждения. Вы также вольны создать записи квот для пользователей, еще не хранящих данные на диске. К моменту начала использования тома пользователем для него уже будут заданы предел и уровень предупреждения.

Чтобы просмотреть текущие записи квот, выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)**. При необходимости подключитесь к удаленному компьютеру.
2. В дереве консоли разверните узел **Запоминающие устройства (Storage)** и выберите элемент **Управление дисками (Disk Management)**. Тома, настроенные на выбранном компьютере, отображаются в области сведений.

3. В представлении **Список томов (Volume List)** или **Графическое представление (Graphical View)** щелкните правой кнопкой том, с которым хотите работать, и выберите команду **Свойства (Properties)**.
4. На вкладке **Квота (Quota)** щелкните **Записи квот (Quota Entries)**. Откроется одноименное диалоговое окно. Для каждой записи указано ее состояние, по которому можно быстро выявить пользователей, превысивших ограничения. Состояние **OK** означает, что пользователь работает в пределах квоты. Любое другое состояние, как правило, свидетельствует о достижении пользователем уровня предупреждения или предела квоты.

Создание записей дисковых квот

Можно создавать записи квот для пользователей, еще не хранящих данные на диске. Это позволяет задать индивидуальные пределы и уровни предупреждения для отдельных пользователей. Эта возможность используется, в основном, когда некий пользователь часто хранит больше информации, чем остальные, и вы хотите разрешить ему выходить за общие пределы. Этим же способом можно установить ограничение для администраторов. Как вы помните, администраторы не подлежат ограничениям дисковых квот. Если вы все-таки хотите ограничить выделение дискового пространства для некоторых администраторов, создайте для каждого из них записи дисковых квот.

Ближе к реальности Не стоит создавать индивидуальные дисковые квоты беспорядочно. Тщательно отслеживайте отдельные записи, а лучше всего, ведите журнал, отображающий все индивидуальные записи так, чтобы другие администраторы могли разобраться в текущих политиках и в том, как они применяются. Изменив основные правила квот тома, перепроверьте отдельные записи: соответствуют ли они новым правилам, не нужно ли их обновить. Мой опыт показывает, что некоторые типы пользователей чаще других становятся исключениями, поэтому иногда стоит размещать различные классы пользователей на разных томах, а потом применить дисковые квоты к каждому тому. Таким образом, у каждого класса или категории пользователей будет собственный предел квоты, соответствующий их типичным потребностям. При этом станет меньше исключений (возможно, даже не станет совсем). В частности, следует использовать отдельные тома для руководства, менеджеров и пользователей или для руководства, дизайнеров, инженеров и всех остальных пользователей.

Чтобы создать запись квоты тома, выполните следующие действия:

1. Откройте диалоговое окно **Записи квот (Quota Entries)**, как описано в предыдущем разделе. Здесь перечислены текущие записи квот всех пользователей. Чтобы обновить список, нажмите **F5** или выберите в меню **Вид (View)** команду **Обновить (Refresh)**.
2. Если у пользователя нет записи, создайте ее. Выберите в меню **Квота (Quota)** команду **Создать запись квоты (New Quota Entry)**. Откроется диалоговое окно **Выбор: «Пользователи» (Select Users)**.
3. Введите имя пользователя в текстовое поле и щелкните **Проверить имена (Check Names)**. Если совпадение обнаружено, выберите нужную учетную запись и щелкните **OK**. Если совпадений не найдено, исправьте имя и выполните поиск еще раз. Завершив выбор, щелкните **OK**.

4. Когда вы выберете пользователя, откроется диалоговое окно **Добавление новой квоты (Add New Quota Entry)**, показанное на рис. 15-18. Чтобы удалить все ограничения квот для данного пользователя, установите флажок **Не ограничивать выделение места на диске (Do Not Limit Disk Usage)**. Чтобы задать для пользователя предел и уровень предупреждения, установите переключатель **Выделять на диске не более (Limit Disk Space To)** и введите соответствующие значения. Щелкните **OK**.

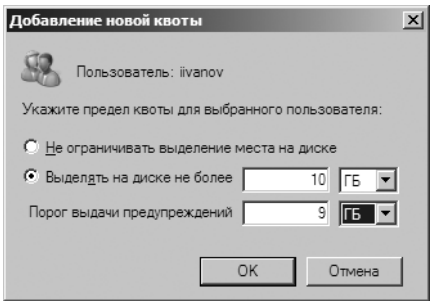


Рис. 15-18. В диалоговом окне Добавление новой квоты (Add New Quota Entry) вы можете задать для пользователя предел квоты и уровень предупреждения или, напротив, снять с него все ограничения

Удаление записей дисковых квот

Если пользователю больше не требуется доступ к тому, удалите соответствующую запись квоты. Во время удаления записи квоты все файлы, которыми владеет пользователь, отображаются в диалоговом окне. Вы можете удалить файлы, стать их владельцем или переместить файлы в папку на другом томе.

Чтобы удалить запись квоты пользователя и определить дальнейшую судьбу его файлов, выполните следующие действия:

1. Откройте диалоговое окно **Записи квот (Quota Entries)**, как описано в разделе «Просмотр записей квот» этой главы. В нем перечислены текущие записи квот всех пользователей. Чтобы обновить список, нажмите **F5** или выберите в меню **Вид (View)** команду **Обновить (Refresh)**.
2. Выделите запись дисковой квоты, которую хотите удалить, и нажмите **Delete** или в меню **Квота (Quota)** выберите команду **Удалить запись квоты (Delete Quota Entry)**. С помощью клавиш **Shift** и **Ctrl** вы можете выделить несколько записей.
3. Щелкните **Да (Yes)**, чтобы подтвердить удаление. Откроется диалоговое окно **Дисковая квота (Disk Quota)** со списком файлов, владельцем которых является пользователь.
4. В списке **Файлы, которыми владеет (List Files Owned By)** отображены файлы пользователя, запись квоты которого вы удаляете. Укажите, что делать с файлами пользователя. Можно обрабатывать каждый файл по

отдельности или выбрать несколько файлов при помощи клавиш **Shift** и **Ctrl**. В вашем распоряжении следующие возможности:

- **Окончательно удалить файлы (Permanently Delete Files)** Выделите удаляемые файлы и щелкните кнопку **Удалить (Delete)**. Щелкните **Да (Yes)**, чтобы подтвердить действие
- **Стать владельцем файлов (Take Ownership Of Files)** Выделите файлы, владельцем которых хотите стать, и щелкните кнопку **Смена владельца (Take Ownership)**.
- **Переместить в (Move Files To)** Выделите файлы, которые хотите переместить и введите путь к папке на другом томе. Если вы не знаете путь, щелкните **Обзор (Browse)**, чтобы найти папку в диалоговом окне **Обзор папок (Browse For Folder)**. Найдя нужную папку, щелкните **Переместить (Move)**.

5. Завершив работу, щелкните **OK**. Если вы указали действие для всех файлов пользователя, записи дисковых квот будут удалены.

Экспорт и импорт параметров дисковых квот NTFS

Чтобы не создавать одинаковые записи квот на разных томах, экспортируйте параметры из исходного тома и импортируйте их на другой том. Оба тома должны быть отформатированы в NTFS. Чтобы экспортировать и импортировать записи дисковых квот, выполните следующие действия:

1. Откройте диалоговое окно **Записи квот (Quota Entries)**, как описано в разделе «Просмотр записей квот» этой главы. В нем перечислены текущие записи квот всех пользователей. Чтобы обновить список, нажмите **F5** или выберите в меню **Вид (View)** команду **Обновить (Refresh)**.
2. В меню **Квота (Quota)** выберите команду **Экспорт (Export)**. Откроется диалоговое окно **Параметры экспорта квоты (Export Quota Settings)**. В адресной строке выберите место, куда будет сохранен файл, содержащий параметры квоты, затем введите имя файла в поле **Имя файла (File Name)**. Щелкните **Сохранить (Save)**.

Совет Сразу сохраните файл параметров на целевом томе. Тем самым вы облегчите себе жизнь при импорте параметров. Файлы квот, как правило, невелики и не займут много места на диске.

3. Выберите в меню **Квота (Quota)** команду **Закрыть (Close)**, чтобы выйти из диалогового окна **Записи квот (Quota Entries)**.
4. В дереве консоли щелкните правой кнопкой элемент **Управление компьютером (Computer Management)**. В контекстном меню выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. В диалоговом окне **Выбор компьютера (Select Computer)** выберите компьютер, на котором содержится целевой том, то есть, том, на котором вы хотите применить экспортируемые параметры.

5. Откройте диалоговое окно свойств целевого тома. На вкладке **Квота (Quota)** щелкните кнопку **Записи квот (Quota Entries)**. Откроется диалоговое окно **Записи квот (Quota Entries)** целевого тома.
6. В меню **Квота (Quota)** выберите команду **Импорт (Import)**. В диалоговом окне **Параметры импорта квоты (Import Quota Settings)** выберите сохраненный ранее файл параметров квот. Щелкните **Открыть (Open)**.
7. Если на томе остались предыдущие записи квот, у вас будет возможность заменить существующие записи или сохранить их. Когда вам будет предложено разрешить конфликт, щелкните **Да (Yes)**, чтобы заменить существующую запись, или **Нет (No)**, чтобы сохранить ее.

Отключение дисковых квот NTFS

Квоты можно отключать как для отдельных пользователей, так и для всех пользователей тома. При отключении квот для конкретного пользователя предел больше не применяется к этому пользователю, но сохраняется для других пользователей. При отключении квот в томе управление квотами полностью прекращается. Чтобы отключить квоты для конкретного пользователя, следуйте инструкциям, приведенным в разделе «Просмотр записей квот» этой главы. Чтобы отключить управление квотами в томе, выполните следующие действия:

1. Откройте консоль **Управление компьютером (Computer Management)**. При необходимости подключитесь к удаленному компьютеру.
2. Откройте диалоговое окно свойств тома, на котором хотите отключить дисковые квоты.
3. На вкладке **Квота (Quota)** сбросьте флажок **Включить управление квотами (Enable Quota Management)**. Щелкните **OK**. В запросе о подтверждении также щелкните **OK**.

Дисковые квоты диспетчера ресурсов

В Windows Server 2008 поддерживается усовершенствованная система управления квотами — консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)**. С ее помощью также можно регулировать использование дискового пространства в папке и томе.

Совет Управление дисковыми квотами диспетчера ресурсов осуществляется отдельно от дисковых квот NTFS, теоретически можно настроить обе системы квот на одном томе. Однако на практике рекомендуется пользоваться одной системой квот, а не обеими сразу. Возможен также такой вариант: используйте дисковые квоты NTFS для томов и дисковые квоты диспетчера ресурсов для важных папок.

Знакомство с дисковыми квотами диспетчера ресурсов

Дисковые квоты диспетчера ресурсов — альтернативный инструмент Windows Server 2008 для управления использованием диска. Они настраиваются для тома или для папки и бывают жесткими (превышение невозможно) и мягкими (превышение возможно).

Жесткие ограничения применяются, когда требуется предотвратить чрезмерное использование диска. Мягкие ограничения применяются, когда достаточно проследить за использованием диска и просто предупредить пользователя, превысившего или близкого к превышению рекомендуемых рамок. Квота применяется к тому или к папке и ко всем подпапкам тома или папки. Детали работы квот, а также способ предупреждения пользователей, выводятся из исходного шаблона квоты.

Шаблоны квот Windows Server 2008 перечислены в табл. 15-7. **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** позволяет определять дополнительные шаблоны для определения квот. Кроме того, определяя квоту, вы всегда можете задать индивидуальные свойства для конкретного пользователя.

Табл. 15-7. Шаблоны дисковых квот

Шаблон квоты	Ограничение	Тип квоты	Описание
Предел 100 МБ (100 MB Limit)	100 Мб	Жесткая	Посылает пользователям предупреждения по мере приближения к пределу и при его достижении
Предел 200 МБ с уведомлением пользователя (200 MB Limit Reports To User)	200 Мб	Жесткая	Посылает пользователям, превысившим предел, отчеты хранилища
Предел 200 МБ с расширением 50 МБ (200 MB Limit With 50 MB Extension)	200 Мб	Жесткая	При помощи команды DIRQUOTA предоставляет пользователям, превысившим предел, единовременное автоматическое расширение квоты на 50 Мб
Расширенный предел 250 МБ (250 MB Extended Limit)	250 Мб	Жесткая	Предназначен для пользователей, у которых предел был увеличен с 200 Мб до 250 Мб
Наблюдение за томом размером 200 ГБ (Monitor 200 GB Volume Usage)	200 Гб	Мягкая	Отслеживает использование тома и предупреждает о приближении к пределу и его превышении
Наблюдение за общим ресурсом размером 500 МБ (Monitor 500 MB Share)	500 Мб	Мягкая	Отслеживает использование общего ресурса и предупреждает о приближении к пределу и его превышении

В шаблоне квоты определены следующие свойства:

- **Предел** Предел использования дискового пространства.
- **Тип квоты** Жесткая или мягкая.
- **Порог уведомления** Типы уведомлений об использовании определенной доли от предела.

Вы можете задать несколько порогов уведомления или пределов. Порогом уведомления считается любой порог меньше 100%. Предельному порогу соответствует достижение 100% предела. Например, вы можете определить пороги уведомления, составляющие 85% и 90% от предела, и предельный порог при достижении 100% предела.

Пользователи, приблизившиеся к пределу или превысившие его, могут автоматически оповещаться по электронной почте. Система оповещения также способна уведомлять администраторов по электронной почте, генерировать отчеты об инцидентах, выполнять команды и записывать события в журнал.

Управление шаблонами дисковых квот

Шаблоны дисковых квот используются для определения свойств квоты, включая предел, тип квоты и пороги уведомлений. Консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** позволяет просматривать определенные в данный момент шаблоны дисковых квот. Для этого нужно развернуть узел **Управление квотами (Quota Management)** и выбрать элемент **Шаблоны квот (Quota Templates)**. Краткое описание стандартных шаблонов дисковых квот приведено в табл. 15-7.

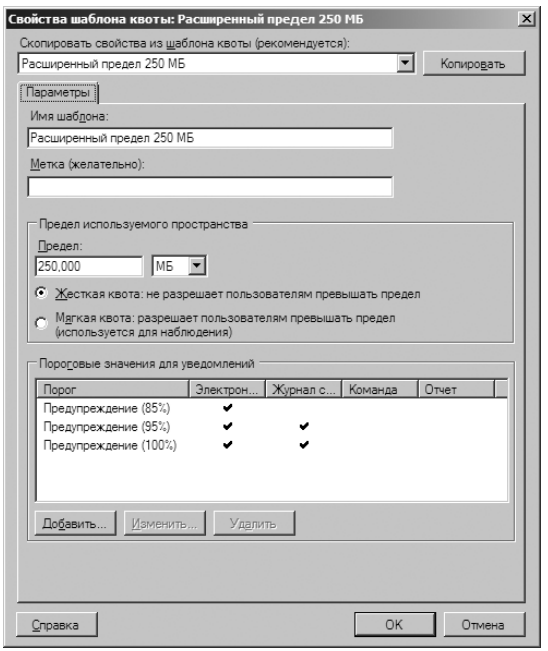


Рис. 15-19. Настройка предела, типа квоты и порога уведомления в свойствах дисковой квоты

Чтобы изменить существующие шаблоны дисковых квот, выполните следующие действия:

1. В консоли **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** разверните узел **Управление квотами (Quota Management)** и выберите **Шаблоны квот (Quota Templates)**.

Для каждого шаблона в списке приведены имя, предел и тип квоты.

2. Чтобы изменить свойства шаблона дисковой квоты, дважды щелкните его имя. Откроется диалоговое окно свойств, показанное на рис. 15-19.
3. На вкладке **Параметры (Settings)** задайте имя шаблона, предел и тип квоты. В окне перечислены текущие пороги уведомлений. Чтобы изменить существующий порог, выделите его и щелкните **Изменить (Edit)**. Чтобы задать новый порог, щелкните **Добавить (Add)**.
4. Завершив изменение шаблона, щелкните **OK**, чтобы сохранить изменения.

Чтобы создать новый шаблон дисковой квоты, выполните следующие действия:

1. В консоли **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** разверните узел **Управление квотами (Quota Management)** и выберите **Шаблоны квот (Quota Templates)**.
2. В меню **Действие (Action)** или в области действий щелкните команду **Создать шаблон квоты (Create Quota Template)**. Откроется диалоговое окно **Создание шаблона квоты (Create Quota Template)**.
3. На вкладке **Параметры (Settings)** задайте имя шаблона, предел и тип квоты. Сначала следует задать предел, а затем пороги уведомления. Введите желаемый предел в поле **Предел (Limit)**. В списке единиц измерения укажите требуемые единицы: килобайты, мегабайты, гигабайты или терабайты.
4. Щелкните **Добавить (Add)**, чтобы добавить пороги уведомлений. В диалоговом окне **Добавление порога (Add Threshold)** задайте значение в поле **Создавать уведомления, когда использование достигает (Generate Notifications When Usage Reaches)**. Порогом уведомления может служить любая доля предела меньше 100%.
5. На вкладке **Сообщение электронной почты (E-mail Message)** настройте следующие параметры:
   - Чтобы уведомлять администратора о срабатывании квоты, установите флажок **Посылать сообщения следующим администраторам (Send E-Mail To The Following Administrators)** и введите адреса электронной почты, отделяя их друг от друга точками с запятой. Значение [Admin Email] соответствует адресу администратора по умолчанию, заданному в глобальных параметрах.
   - Чтобы уведомлять пользователей, установите флажок **Посылать сообщения пользователям, превысившим порог (Send E-Mail To The User Who Exceeded The Threshold)**.
   - Задайте содержимое уведомления в полях **Тема (Subject)** и **Текст сообщения (Message Body)**. Доступные переменные и их значения приведены в табл. 14-6.
6. На вкладке **Журнал событий (Event Log)** настройте запись событий в журнал. Установите флажок **Записывать предупреждения в жур-**

нал (Send Warning To Event Log) и задайте текст записи в поле **Запись журнала (Log Entry)**. Доступные переменные и их значения приведены в табл. 14-6.

7. На вкладке **Отчет (Report)** установите флажок **Создать отчет (Generate Reports)**, чтобы включить создание отчетов об инцидентах. Выберите соответствующие типы отчетов. По умолчанию отчеты об инцидентах хранятся в папке *%SystemDrive%*\StorageReports\Incident. Кроме того, они могут быть отправлены указанным администраторам. Значение [Admin Email] соответствует адресу администратора по умолчанию, заданному в глобальных параметрах
8. Повторите шаги 5–7, чтобы задать дополнительные пороги уведомлений.
9. Завершив создание шаблона, щелкните **OK**.

Создание дисковых квот диспетчера ресурсов

Дисковые квоты используются для введения особых ограничений на использование определенных папок. Консоль **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** позволяет просматривать текущие дисковые квоты. Для этого нужно развернуть узел **Управление квотами (Quota Management)** и выбрать элемент **Квоты (Quotas)**. Прежде чем определить дисковые квоты, следует указать группы блокировки файлов и шаблоны дисковых квот, которыми вы будете пользоваться.

Определив необходимые группы блокировки и шаблоны дисковых квот, создайте дисковую квоту, выполнив следующие действия:

1. В консоли **Диспетчер ресурсов файлового сервера (File Server Resource Manager)** разверните узел **Управление квотами (Quota Management)** и выберите элемент **Квоты (Quotas)**.
2. В меню **Действие (Action)** или в области действий щелкните команду **Создать квоту (Create Quota)**.
3. В диалоговом окне **Создание квоты (Create Quota)** укажите путь на локальном компьютере. Щелкните кнопку **Обзор (Browse)** и в диалоговом окне **Обзор папок (Browse For Folder)** выберите нужный путь, например, C:\Data. Щелкните **OK**.
4. В списке **Наследовать свойства из следующего шаблона квоты (Derive Properties From This Quota Template)** выберите шаблон, определяющий нужные свойства квоты.
5. Щелкните **Создать (Create)**.

Глава 16

Архивация и восстановление данных

Данные — сердце предприятия, а их защита — первостепенная задача администратора. Для защиты данных предприятия нужно среди прочего разработать план архивации и восстановления. Архивация — это средство защиты данных от случайной потери, повреждения БД, аппаратных сбоев и даже стихийных бедствий. В задачу администратора входит создание и безопасное хранение резервных копий.

Разработка плана архивации и восстановления

Архивация данных — это ваша страховка. То и дело случайно удаляются важные файлы. Возникают сбои в данных, необходимых для решения ответственных задач. На ваш офис может обрушиться удар стихии... Если у вас есть план архивации и восстановления, вы переживете любую неприятность. Если такого плана нет, вы лишены главной опоры.

Подготовка плана архивации

На создание и внедрение плана архивации требуется время. Следует рассчитать, какие данные следует копировать, частоту создания копий и многое другое. Составить план вам помогут ответы на следующие вопросы:

- **Насколько важны или конфиденциальны данные?** От важности данных зависит целесообразность их архивации, а также ее сроки и способы. Для критических данных, например, баз данных, следует иметь избыточные наборы резервных копий, охватывающих несколько периодов архивации. В случае конфиденциальных данных следует обеспечить физическую безопасность копий или их шифрование. Для менее важных данных, например, файлов пользователей, тщательной разработки плана не требуется. Тем не менее, и в этом случае следует регулярно проводить архивацию и обеспечить простоту восстановления данных.
- **Какие сведения содержатся в данных?** Данные, кажущиеся вам незначительными, могут оказаться очень важными для другого сотрудника. От типа информации зависит целесообразность архивации, а также ее сроки и способы.

- **Как часто обновляются данные?** Частота изменения влияет на частоту архивации данных. В частности, данные, обновляемые ежедневно, следует архивировать каждый день.
- **Можете ли вы дополнить архивацию теневыми копиями?** Теневые копии — это одномоментные копии документов в общих папках. Они облегчают восстановление документов, позволяя в случае удаления или случайной перезаписи документа без труда вернуться к прежней версии. Теневое копирование используется в качестве дополнения к обычным резервным копиям, но не вместо них.
- **Как быстро требуется восстановить данные?** Важным фактором при составлении плана архивации является время. Критические системы нужно быстро возвращать в оперативный режим. Для этого вам, возможно, придется изменить план архивации.
- **Есть ли у вас подходящее оборудование для архивации?** Для регулярного копирования следует иметь несколько устройств и несколько наборов резервных носителей. К архивационному оборудованию относятся накопители на магнитной ленте (НМЛ), оптические накопители и съемные диски. Как правило, НМЛ стоят дешевле, но работают медленнее накопителей других типов.
- **Кто отвечает за план архивации и восстановления?** В идеале, в организации должен быть специальный сотрудник, отвечающий за архивацию и восстановление данных.
- **На какое время лучше планировать архивацию?** Понятно, что архивация в часы наименьшей загруженности системы ускорит процесс создания копий. Однако сделать это получается не всегда. Поэтому следует тщательно планировать время создания копий ключевых данных системы.
- **Нужно ли хранить резервные копии вне системы?** Сохранение резервных копий отдельно от системы необходимо на случай стихийного бедствия. Во внешнее хранилище следует также поместить и копии ПО, необходимого для восстановления работы системы.

Основные виды архивации

Существует много способов архивации файлов. Способ, который выберете вы, зависит от типа копируемых данных, от того, насколько удобным должен быть процесс восстановления, и т. д.

Заглянув в свойства файла или папки в Проводнике Windows (Windows Explorer), вы увидите атрибут Архивный (Archive). Он часто используется, чтобы определить, следует ли выполнять архивацию файла или папки. Если этот атрибут задан, файл или папка нуждаются в архивации. Существуют следующие основные типы архивации:

- **Нормальная, или полная, архивация** Архивация всех выбранных файлов выполняется независимо от значения атрибута Архивный (Archive). После создания резервной копии файла атрибут Архивный (Archive)

снимается. В случае последующего изменения файла, этот атрибут восстанавливается, указывая на необходимость архивации файла.

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

План архивации обычно состоит из еженедельной полной архивации, дополненной ежедневной, разностной или добавочной архивацией. При проведении ежемесячной или ежеквартальной архивации может оказаться полезным создание расширенных резервных копий, включающих дополнительные файлы, которые не копируются регулярно.

Совет Зачастую пропажа файла или источника данных обнаруживается спустя недели или даже месяцы. При этом важность некоторых типов данных вовсе не умаляется редкостью их использования. Поэтому не забывайте о пользе создания дополнительных наборов резервных копий, создаваемых ежемесячно или ежеквартально. Они обеспечат восстановление важных данных даже по прошествии значительного времени.

Разностная и добавочная архивация

Между разностной и добавочной архивацией есть очень важное различие. Чтобы лучше разобраться в нем, изучите табл. 16-1. Как видите, при разностной архивации создаются копии всех файлов, изменившихся с момента прошлой полной архивации (это означает, что размер разностных резервных копий со временем растет). В процессе добавочной архивации копируются только файлы, изменившиеся со времени последней полной или добавочной

архивации (это означает, что размер добавочной резервной копии, как правило, значительно меньше размера полной резервной копии).

Табл. 16-1. Способы добавочной и разностной архивации

День недели	Еженедельная полная архивация с ежедневной разностной архивацией	Еженедельная полная архивация с ежедневной добавочной архивацией
Воскресенье	Выполняется полная архивация	Выполняется полная архивация
Понедельник	Разностная копия содержит все изменения, произошедшие с воскресенья	Добавочная копия содержит изменения, произошедшие с воскресенья
Вторник	Разностная копия содержит все изменения, произошедшие с воскресенья	Добавочная копия содержит изменения, произошедшие с понедельника
Среда	Разностная копия содержит все изменения, произошедшие с воскресенья	Добавочная копия содержит изменения, произошедшие со вторника
Четверг	Разностная копия содержит все изменения, произошедшие с воскресенья	Добавочная копия содержит изменения, произошедшие со среды
Пятница	Разностная копия содержит все изменения, произошедшие с воскресенья	Добавочная копия содержит изменения, произошедшие с четверга
Суббота	Разностная копия содержит все изменения, произошедшие с воскресенья	Добавочная копия содержит изменения, произошедшие с пятницы

Определив, архивацию каких данных и как часто вы собираетесь выполнять, выберите соответствующие архивные устройства и носители. О них пойдет речь в следующем разделе.

Выбор устройств и носителей

Существует много устройств для архивации файлов. Некоторые из них работают быстро и стоят недешево. Другие — медленны, но надежны. Выбор решения архивации для вашей компании зависит от многих факторов, в том числе:

- **Объем** Количество данных, резервные копии которых следует создавать регулярно. Сможет ли архивное оборудование выдержать требуемую нагрузку с учетом ограничений по времени и ресурсам?
- **Надежность** Надежность архивного оборудования и носителей. Можете ли вы позволить себе пожертвовать надежностью ради бюджета или времени?

- **Расширяемость** Будет ли решение удовлетворять потребностям роста организации?
- **Скорость** Скорость, с которой будут выполняться архивация и восстановление данных. Можете ли вы позволить себе пожертвовать скоростью в угоду экономии?
- **Стоимость** По силам ли вашему бюджету выбранное решение архивации?

Типичные решения архивации

Емкость, надежность, расширяемость, скорость и стоимость — вот краеугольные камни плана архивации. Если вы разберетесь, как эти аспекты проявляют себя в вашей организации, то без труда подберете приемлемое решение. Некоторые из наиболее часто используемых решений архивации перечислены ниже:

- **Накопители на магнитной ленте (НМЛ)** Наиболее типичные архивные накопители, в которых для хранения данных используются кассеты с магнитной лентой. НМЛ относительно дешевы, но не очень надежны. Лента рвется, растягивается, часто со временем теряет информацию. Средний объем кассет варьируется от 24 Гб до 72 Гб. По сравнению с другими решениями НМЛ достаточно медленны. Их основное достоинство — низкая стоимость.
- **Накопители на лентах DAT** Накопители DAT постепенно приходят на смену НМЛ в качестве предпочтительных устройств архивации. Существует множество форматов DAT. Наиболее широко распространены форматы DLT или SDLT. Ленты формата SDLT 320 или 600 обладают емкостью 160 или 300 Гб для несжатых данных и 320 или 600 Гб для сжатых данных. В больших организациях целесообразно использовать технологии лент LTO. Ленты LTO-3 обладают емкостью 400 Гб для несжатых данных и 800 Гб для сжатых данных.
- **Ленточные накопители с автозагрузкой** Накопители с автозагрузкой состоят из магазина лент и способны создавать расширенные архивные тома, удовлетворяющие потребности любого предприятия. В системе автозагрузки ленты внутри магазина в процессе архивации или восстановления меняются автоматически, по мере надобности. Большинство накопителей с автозагрузкой работают с лентами DAT в форматах DLT, SDLT или LTO. Типичные накопители DLT способны записывать до 45 Гб в час. Чтобы увеличить скорость, приобретите ленточную библиотеку с несколькими накопителями. Это позволит одновременно производить запись на несколько лент. Большинство накопителей SDLT и LTO записывают более 100 Гб в час, а с помощью нескольких накопителей в системе вы доведете скорость записи до сотен Гб в час.
- **Дисковые накопители** Обеспечивают один из самых быстрых способов архивации и восстановления файлов, зачастую позволяя за считанные ми-

нуты справится с заданием, на которое при работе с НМЛ уйдут часы. Если успешность бизнеса невозможна без быстрого восстановления данные, дисковые накопители вне всякой конкуренции. Их недостаток состоит в более высокой стоимости по сравнению с ленточными накопителями.

- **Системы архивации на основе дисков** Представляют собой исчерпывающее решение архивации и восстановления с использованием больших производительных дисковых массивов. Высокая надежность достигается при работе с массивами RAID, обеспечивающими избыточность и отказоустойчивость. Типичные дисковые системы архивации опираются на технологию виртуальной библиотеки, благодаря чему Windows «видит» их как ленточные библиотеки с автозагрузкой. Это облегчает работу с ними. Обычная система из 20 дисков способна записывать до 500 Гб/час, система из 40 дисков — до 2 Тб/час.

Примечание Диски и дисковые архивные системы на предприятиях, как правило, используются в качестве промежуточного этапа между архивируемым сервером и ленточным накопителем с автозагрузкой. Резервные копии сервера сначала создаются на диске, потому что диски по сравнению с лентой работают с более высокой скоростью. Затем выполняется архивация на НМЛ с автозагрузкой. Хранение данных на магнитных лентах облегчает процесс ротации резервных копий и их перенос во внешнее хранилище.

Перед началом работы с архивным устройством его следует установить. Во время установки архивных устройств, отличных от обычных НМЛ и накопителей DAT, вы должны сообщить ОС об используемых контроллерах и драйверах.

Приобретение архивных носителей и работа с ними

Выбор архивного устройства — важный шаг в реализации плана архивации и восстановления. Но для осуществления плана необходимо также приобрести носители — ленты или диски. Требуемое количество носителей зависит от объема архивируемых данных, частоты архивации, а также от сроков хранения дополнительных наборов данных.

Обычно при работе с резервными лентами создается расписание ротации двух или нескольких наборов лент. Это позволяет увеличить срок службы лент за счет сокращения их использования, одновременно уменьшив количество лент, необходимое для сохранности старых данных.

В одном из наиболее распространенных расписаний ротации используется десять лент. Эти ленты делятся на два набора по 5 лент (по одной на каждый рабочий день). Первый набор используется в первую неделю, второй — во вторую неделю. По пятницам выполняется полная архивация, с понедельника по четверг — добавочная архивация. Если добавить еще один набор лент, вы сможете размещать во внешнем хранилище набор, не используемый в текущую неделю.

Расписание на основе десяти лент предназначено для организации, работающей 8 часов в день 5 дней в неделю. Если вы работаете по графику 24/7, вам

придется добавить ленты на субботу и воскресение. В этом случае вы будете использовать 14 лент: два набора по 7 лент. Полную архивацию планируйте на воскресение. С понедельника по субботу проводится добавочная архивация.

По мере падения цены на дисковые накопители некоторые организации переходят с кассетных на дисковые архивные накопители. Расписание ротации дисков похоже на расписание ротации лент, но может потребовать и некоторой коррекции. Главное — обязательно поочередно переносите наборы архивных дисков во внешнее хранилище.

Выбор программы архивации

Система Windows Server 2008 поддерживает многие решения в области архивации и восстановления. При выборе ПО для архивации помните о нужных вам типах резервных копий и о типе данных, архивацию которых вы производите. В Windows Server 2008 есть три компонента для архивации и восстановления:

- **Система архивации данных Windows Server (Windows Server Backup)** Основная, очень простая в использовании утилита архивации и восстановления. Если этот компонент установлен на сервере, вы найдете команду для его вызова в меню **Администрирование (Administrative Tools)**. Кроме того, программа добавляется в консоль **Диспетчер сервера (Server Manager)**.
- **Программы командной строки для архивации** Набор команд для архивации и восстановления, работающих из командной строки Wbadmin. Утилита Wbadmin запускается из командной строки с повышенными полномочиями. Для вывода полного списка поддерживаемых команд введите **wbadmin /?**.
- **Среда восстановления Windows** Если функции восстановления, предоставляемые производителем сервера, почему-либо недоступны, воспользуйтесь этой средой.

Чаще других используется программа Система архивации данных Windows Server (Windows Server Backup). С ее помощью вы можете создавать полные и добавочные копии, а также проводить архивацию копированием — как на локальной, так и на удаленной системе. С помощью Системы архивации данных Windows Server (Windows Server Backup) нельзя создавать разностные резервные копии. Программа Система архивации данных Windows Server (Windows Server Backup) использует службу VSS (Volume Shadow Copy Service) для быстрого создания резервных копий операционной системы, файлов и папок, а также томов на уровне блоков. Создав первую резервную копию, вы затем можете настроить Систему архивации данных Windows Server (Windows Server Backup) на автоматический запуск по расписанию полной или добавочной архивации.

При работе с Системой архивации данных Windows Server (Windows Server Backup) вам потребуются носители, специально выделенные для хра-

нения архивов. Архивы можно создавать на внешних дисках, внутренних дисках, DVD или в общих папках. Поддержка архивации на DVD — новая возможность программы. Архивы на DVD позволяют восстанавливать целые тома, однако с их помощью нельзя восстановить отдельные файлы, папки или данные приложений.

Примечание Программа Система архивации данных Windows Server (Windows Server Backup) не поддерживает архивацию на магнитную ленту. Для архивации на магнитную ленту потребуется ПО сторонних производителей.

С помощью Системы архивации данных Windows Server (Windows Server Backup) можно без труда восстанавливать отдельные файлы и папки. Если файлы хранятся в добавочных архивах, то вместо восстановления вручную файлов из нескольких архивов, можно восстановить файлы и папки, выбрав дату создания резервной копии восстанавливаемого элемента. Кроме того, Система архивации данных Windows Server (Windows Server Backup) работает с новыми инструментами восстановления Windows, тем самым, упрощая восстановление ОС. Восстановление можно выполнить на тот же или на новый сервер, на котором нет никакой ОС. Благодаря использованию VSS Система архивации данных Windows Server (Windows Server Backup) без труда восстанавливает данные совместимых приложений, например, Microsoft SQL Server и Windows SharePoint Services.

Программа Система архивации данных Windows Server (Windows Server Backup) включает в себя автоматическое управление дисками. Вы можете выполнять архивацию на несколько дисков попеременно, просто добавляя очередной диск в качестве расположения плановой резервной копии. Когда вы настроите диск как расположение резервной копии, Система архивации данных Windows Server (Windows Server Backup) автоматически возьмет на себя управление этим диском. Вам не придется беспокоиться о наличии на нем свободного места. Создавая новые резервные копии, программа Система архивации данных Windows Server (Windows Server Backup) автоматически перезаписывает старые архивы. Чтобы помочь вам в планировании, Система архивации данных Windows Server (Windows Server Backup) отображает доступные архивные диски и текущую информацию об их использовании.

Архивация данных: основы

Для создания резервных копий на локальных и удаленных системах в Windows Server 2008 существует программа Система архивации данных Windows Server (Windows Server Backup). Система архивации служит для создания резервных копий файлов и папок, восстановления архивных файлов и папок, создания снимков состояния системы для архивации и восстановления, а также для автоматизированного создания плановых резервных копий.

Установка утилит архивации и восстановления

Средства архивации и восстановления Windows Server доступны во всех версиях Windows Server 2008, как в 32-разрядных, так и в 64-разрядных. Графические версии этих средств нельзя установить на Windows Server 2008 Core. На серверах, работающих под управлением версии Windows Server Core, управление архивами осуществляется из командной строки или с удаленного компьютера.

Чтобы установить средства архивации и восстановления Windows, выполните следующие действия:

1. В консоли Диспетчер сервера (Server Manager) выберите узел **Компоненты (Features)** и щелкните команду **Добавить компоненты (Add Features)**. Откроется Мастер добавления компонентов (Add Features Wizard).
2. На странице **Выбор компонентов (Select Features)** установите флажок **Возможности системы архивации данных Windows (Windows Server Backup Features)**. При этом будут выбраны компоненты **Система архивации данных Windows Server (Windows Server Backup)** и **Программы командной строки (Command-Line Tools)**. Щелкните **Далее (Next)**.
3. Щелкните **Установить (Install)**. По завершению установки щелкните **Закрыть (Close)**. После этого в меню **Администрирование (Administrative Tools)** появится команда **Система архивации данных Windows Server (Windows Server Backup)**.

Совет С помощью Системы архивации данных Windows Server (Windows Server Backup) (Wbadmin.exe) нельзя восстановить резервные копии, созданные в предыдущей программе архивации (Ntbackup.exe). Версию Ntbackup.exe для Windows Server 2008 вы найдете в Центре загрузки Майкрософт. Размещенная там версия Ntbackup.exe предназначена только для восстановления резервных копий, созданных в старых версиях Windows. Ее нельзя использовать для создания новых резервных копий в Windows Server 2008.

Знакомство с системой архивации данных Windows Server

Первый раз открыв программу Система архивации данных Windows Server (Windows Server Backup), вы увидите предупреждение о том, что на этом компьютере архивация еще не настроена (рис. 16-1). Чтобы убрать это предупреждение, создайте резервную копию с помощью команды **Однократная архивация (Backup Once)** или запланируйте автоматическое создание архива при помощи команды **Расписание архивации (Backup Schedule)**.

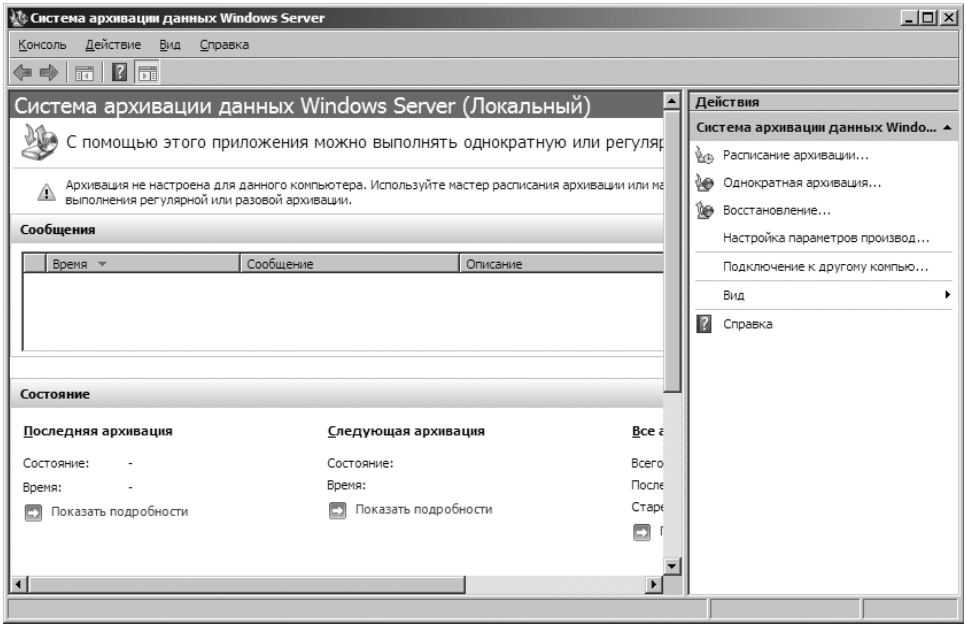


Рис. 16-1. Система архивации данных Windows Server обладает удобным интерфейсом, помогающим проводить архивацию и восстановление

Для выполнения архивации и восстановления вы должны обладать определенными разрешениями и правами пользователя. Члены групп Администраторы (Administrators) и Операторы архива (Backup Operators) имеют право выполнять архивацию и восстановление файлов любого типа независимо от владельца и разрешений файла. Пользователь, которому предоставлен доступ к файлу, также может выполнять его архивацию, при условии что он является владельцем файла или обладает разрешениями Чтение (Read), Чтение и выполнение (Read & Execute), Изменение (Modify) или Полный доступ (Full Control).

Примечание Помните, что локальные учетные записи работают только на локальном компьютере, а учетные записи домена обладают полномочиями в масштабах домена. Поэтому член группы локальных администраторов может работать только с файлами на локальной системе, а член группы Администраторы домена (Domain Administrators) может работать с файлами в пределах домена.

В системе архивации имеются расширения, позволяющие работать со следующими специальными типами данных:

- **Данные состояния системы** Системные файлы, необходимые для восстановления локальной системы. Для полного восстановления работы системы необходимо создавать их резервные копии наряду с другими файлами.
- **Данные приложений** Файлы данных приложений. Их нужно архивировать, чтобы иметь возможность полностью восстановить приложение.

Система архивации данных Windows Server создает поблоковые резервные копии данных приложений при помощи службы VSS.

Исходная реализация Системы архивации данных Windows Server (Windows Server Backup) позволяет создавать полные и добавочные копии, а также проводить архивацию копированием. Вы можете проводить полную или добавочную архивацию один или несколько раз в день, но программа не позволяет создавать отдельные расписания для выполнения обоих типов архивации сразу. Более того, вы не можете установить день или дни недели для выполнения архивации, поскольку у каждого сервера есть свое главное расписание, выполняющееся один или несколько раз в день. Ожидается обновление программы Система архивации данных Windows Server (Windows Server Backup), которое позволит создавать несколько главных расписаний на каждый день недели или месяца. Установив это обновление, вы сможете настраивать отдельные расписания полной и добавочной архивации на одном и том же сервере, а также задавать дни недели или месяца для выполнения архивации. Если у вашего сервера имеется одно главное расписание, вы можете обойти это ограничение. Настройте систему архивации данных Windows Server на ежедневное выполнение добавочной архивации, а затем создайте задание в Планировщике заданий (Task Scheduler) на создание полной резервной копии при помощи Wbadmin в нужный вам день недели или месяца.

Во время запуска консоли **Система архивации данных Windows Server (Windows Server Backup)** по умолчанию программа подключается к локальному компьютеру. Чтобы управлять архивацией на удаленном компьютере, выполните следующие действия:

1. Запустите консоль **Система архивации данных Windows Server (Windows Server Backup)**. В области действий или в меню **Действие (Action)** щелкните команду **Подключение к другому компьютеру (Connect To Another Computer)**.
2. Установите переключатель **Другой компьютер (Another Computer)**, а затем введите имя сервера или IP-адрес. Если включено сетевое обнаружение, щелкните кнопку **Обзор (Browse)**, найдите удаленный компьютер в открывшемся диалоговом окне и щелкните **OK**.
3. Щелкните **Готово (Finish)**, чтобы установить сетевое подключение к удаленному компьютеру.

При работе с программой Система архивации данных Windows Server (Windows Server Backup) первая резервная копия сервера — всегда полная копия. Это делается для очистки атрибута Архивный (Archive), чтобы впоследствии программа могла проследить за обновлением файлов. Будет ли следующая архивация полной или добавочной, зависит от заданных вами параметров производительности. Чтобы настроить стандартные параметры производительности, выполните следующие действия:

1. Запустите консоль **Система архивации данных Windows Server (Windows Server Backup)**. В области действий или в меню **Действие (Action)**

щелкните команду **Настройка параметров производительности (Configure Performance Settings)**. Откроется диалоговое окно **Оптимизация производительности архивации (Optimize Backup Performance)**, показанное на рис. 16-2.

2. Выполните одно из следующих действий, а затем щелкните **OK**:
   - Установите переключатель **Всегда выполнять полную архивацию (Always Perform Full Backup)** для создания полных резервных копий всех подключенных дисков.
   - Установите переключатель **Всегда выполнять добавочную архивацию (Always Perform Incremental Backup)** для создания добавочных резервных копий всех подключенных дисков.
   - Установите переключатель **Выборочная (Custom)**, а затем укажите в списке, какую архивацию следует выполнять для отдельных подключенных дисков — полную или добавочную.
3. Настроив стандартные параметры производительности, запустите полную архивацию или архивацию копированием. Для этого в меню **Действие (Action)** или в области действий щелкните команду **Однократная архивация (Backup Once)**. Чтобы настроить расписание архивации, в меню **Действие (Action)** или в области действий щелкните команду **Расписание архивации (Backup Schedule)**.

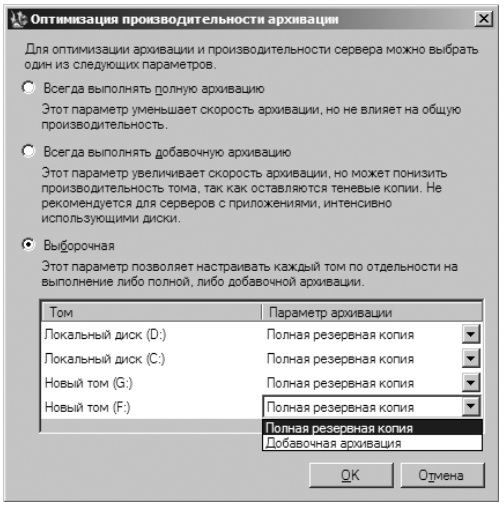


Рис. 16-2. Настройка стандартных параметров архивации

Запуск архивации из командной строки

Программа Wbadmin представляет собой аналог системы архивации данных Windows Server для командной строки. Эта утилита позволяет управлять всеми аспектами настройки архивации, которые настраиваются в системе архивации данных, а значит, для архивации и восстановления подойдет любая из этих двух программ.

Установив компонент Программы командной строки (Backup Command-Line Tools), о котором говорилось ранее в этой главе, вы сможете выполнять архивацию и восстановление при помощи утилиты Wbadmin из папки %SystemRoot%\System32\. Вот что нужно сделать, чтобы ее запустить:

1. Щелкните кнопку **Пуск (Start)** и разверните меню **Все программы (All Programs)** и **Стандартные (Accessories)**.
2. Щелкните правой кнопкой команду **Командная строка (Command Prompt)** и выберите команду **Запуск от имени администратора (Run As Administrator)**.
3. В окне командной строки запустите команду Wbadmin или вызывающий ее сценарий.

   С утилитой Wbadmin связанно несколько команд, перечисленных в табл. 16-2.

Табл. 16-2. Команды управления архивацией Wbadmin

Команда	Описание
DELETE SYSTEMSTATEBACKUP	Удаляет резервную копию состояния системы из заданного расположения
DISABLE BACKUP	Отключает плановые ежедневные архивации
ENABLE BACKUP	Включает или изменяет плановую ежедневную архивацию
GET DISKS	Выдает список подключенных дисков локального компьютера с их именами, типами, номерами диска, GUID, емкостью и имеющимися томами
GET ITEMS	Выдает список элементов в конкретной резервной копии
GET STATUS	Отображает состояние выполняющейся в данный момент архивации или восстановления
GET VERSIONS	Выдает сведения о доступных резервных копиях, хранящихся в конкретном расположении, включая время создания и целевую папку
START BACKUP	Запускает архивацию с заданными параметрами. Если параметры не заданы, но включена плановая архивация, используются ее параметры
START RECOVERY	Запускает восстановление томов, приложений или файлов по заданным параметрам
START SYSTEMSTATEBACKUP	Запускает архивацию состояния системы по заданным параметрам
START SYSTEMSTATERECOVERY	Запускает восстановление состояния системы по заданным параметрам
STOP JOB	Останавливает выполняющуюся в данный момент архивацию или восстановление. Выполнение остановленных задач нельзя продолжить

Чтобы получить справку по командам программы Wbadmin, выполните следующие действия:

- Чтобы просмотреть список управляющих команд, введите **wbadmin /?**.
- Чтобы просмотреть синтаксис той или иной команды, введите **wbadmin команда /?**, где команда — имя интересующей вас команды, например, **wbadmin stop job /?**.

Почти у всех команд есть параметры, уточняющие их действие. В качестве примера рассмотрим следующий синтаксис:

```
wbadmin get versions [-backupTarget:{ИмяТома | СетевойПутьОбщегоРесурса}]
[-machine:ИмяКомпьютера]
```

Квадратными скобками в данном случае отмечены необязательные параметры –backupTarget и –machine. Вообще, чтобы получить информацию о рабочих резервных копиях на локальном компьютере, достаточно ввести команду:

```
wbadmin get versions
```

Для получения информации о рабочих резервных копиях на диске F: введите команду:

```
wbadmin get versions -backuptarget:f:
```

Для получения информации о рабочих резервных копиях на диске F: компьютера Server96 введите команду:

```
wbadmin get versions -backuptarget:f: -machine:server96
```

Чаще всего используются параметры –backupTarget и –machine. Параметр **–backuptarget** — это расположение, с которым вы хотите работать. Он может выражаться именем локального тома, например, F:, или путем к общему сетевому ресурсу, например, \\FileServer32\backups\Server85. Параметр **–machine** обозначает компьютер, с которым вы хотите работать.

Работа с командами Wbadmin

Команды утилиты Wbadmin используются для управления архивацией серверов и работают с конкретным набором параметров. В следующих разделах содержатся сведения о командах и наиболее распространенные примеры синтаксиса.

Команды общего назначения

Следующие команды предназначены для сбора информации о резервных копиях и системе, с которой вы работаете:

- **GET DISKS** Выдает список подключенных дисков локального компьютера с их именами, типами, номерами диска, GUID, емкостью и имеющимися томами.

  ```
  wbadmin get disks
  ```

- **GET ITEMS** Выдает список элементов в конкретной резервной копии.

```
wbadmin get items -version:ИдентификаторВерсии
 [-backupTarget:{ИмяТома | СетевойПутьОбщегоРесурса}]
 [-machine:ИмяКомпьютера]
```

- **GET STATUS** Отображает состояние выполняющейся в данный момент архивации или восстановления.

```
wbadmin get status
```

- **GET VERSIONS** Выдает сведения о доступных резервных копиях, хранящихся в конкретном расположении, включая время создания и целевую папку.

```
wbadmin get versions [-backupTarget:{ИмяТома | СетевойПутьОбщегоРесурса}]
 [-machine:ИмяКомпьютера]
```

Команды для управления архивацией

Управление архивацией и ее параметрами осуществляется с помощью следующего синтаксиса:

- **DELETE SYSTEMSTATEBACKUP** Удаляет резервную копию состояния системы из заданного расположения.

```
wbadmin delete systemstateBackup [-backupTarget:{ИмяТома}]
 [-machine:ИмяКомпьютера]
 [-keepVersions:ЧислоСохраняемыхРезервныхКопий | -version:
ИдентификаторВерсии |
 -deleteOldest]
 [-quiet]
```

- **DISABLE BACKUP** Отключает плановые ежедневные архивации.

```
wbadmin disable backup [-quiet]
```

- **ENABLE BACKUP** Включает или изменяет плановую ежедневную архивацию.

```
wbadmin enable backup [-addTarget:{КонечныйДискРезервногоКопирования}]
 [-removeTarget:{КонечныйДискРезервногоКопирования}]
 [-schedule:ВремяЗапускаРезервногоКопирования]
 [-include:КопируемыеТома]
 [-allCritical]
 [-quiet]
```

- **START BACKUP** Запускает архивацию с заданными параметрами. Если параметры не заданы, но включена плановая архивация, используются ее параметры.

```
wbadmin start backup [-backupTarget:{КонечныйТом | КонечныйОбщийРесурсСети}]
 [-include:КопируемыеТома]
```

```
 [-allCritical]
 [-noVerify]
 [-user:имя_пользователя]
 [-password:пароль]
 [-noinheritAcl]
 [-vssFull]
 [-quiet]
```

- **STOP JOB** Останавливает выполняющуюся в данный момент архивацию или восстановление. Выполнение остановленных задач нельзя продолжить.

```
wbadmin stop job [-quiet]
```

Команды для управления восстановлением

Восстановление компьютеров и данных осуществляется с помощью следующего синтаксиса:

- **START RECOVERY** Запускает восстановление томов, приложений или файлов по заданным параметрам.

```
wbadmin start recovery -version:ИдентификаторВерсии
 -items:ВосстанавливаемыеТома | ВосстанавливаемыеПриложения | Восстанавл
иваемыеПапкиИлиФайлы
 -itemType:{том | приложение | файл}
 [-backupTarget:{ТомРезервнойКопии | СетевойРесурсРезервнойКопии}]
 [-machine:ИмяКомпьютера]
 [-recoveryTarget:ВосстанавливаемыйТом | ВосстанавливаемыйПуть]
 [-recursive]
 [-overwrite:{Перезаписать | СоздатьКопию | Пропустить}]
 [-notRestoreAcl]
 [-skipBadClusterCheck]
 [-noRollForward]
 [-quiet]
```

- **START SYSTEMSTATEBACKUP** Запускает архивацию состояния системы по заданным параметрам.

```
wbadmin start systemstateBackup -backupTarget:{ИмяТома}
 [-quiet]
```

- **START SYSTEMSTATERECOVERY** Запускает восстановление состояния системы по заданным параметрам.

```
wbadmin start systemstateRecovery -version:ИдентификаторВерсии
 -showSummary
 [-backupTarget:{ИмяТома | СетевойПутьОбщегоРесурса}]
 [-machine:ИмяКомпьютера]
 [-recoveryTarget:КонечныйПутьВосстановления]
 [-authSysvol]
 [-quiet]
```

Архивация сервера

Вы можете выполнять архивацию как локального сервера, так и удаленных серверов. Возможно, для нормальной работы с удаленным компьютером вам придется настроить исключение брандмауэра Windows. В рамках плана архивации для каждого сервера вы должны решить, какие тома следует архивировать, включать ли в архив данные состояния системы, данные приложений или и то, и другое.

Вручную вы можете создавать резервные копии на общих томах или DVD, но для запуска архивации по расписанию вам потребуется специально предназначенный для этого жесткий диск. Когда вы настроите диск для плановой архивации, управлять его работой, перезаписывая старые архивы, будет программа архивации. Распланировав архивацию, не забывайте проводить периодические проверки ее выполнения и при необходимости корректировать расписание.

Создавая расписание архивации, вы должны указать тома, которые следует включить в архив, а это повлияет на способы восстановления серверов и данных. Возможны следующие варианты:

- **Все тома с данными приложений** Архивируйте все тома с данными приложений, если вам нужна возможность полного восстановления сервера, включая состояние системы и данные приложений. Поскольку вы архивируете все файлы, состояние системы и данные приложений, вы сможете полностью восстановить сервер, пользуясь исключительно средствами восстановления Windows.
- **Все тома без данных приложений** Архивируйте все тома без данных приложений, если собираетесь восстанавливать сервер отдельно от приложений. При этом следует сначала архивировать сервер при помощи инструментов Windows, а затем архивировать приложения при помощи программ сторонних производителей или собственных возможностей приложений. При помощи средств Windows вы полностью восстановите сервер, а затем воспользуетесь программами сторонних производителей для восстановления данных приложений.
- **Критические тома** Архивируйте только критические тома, если хотите восстановить только операционную систему.
- **Некритические тома** Архивируйте конкретные некритические тома, если вам требуется восстанавливать только файлы, приложения или данные с этих томов.

В процессе архивации вы также указываете место хранения резервных копий. Выбирая хранилище, имейте в виду следующее:

- Если для хранения резервных копий используется внутренний жесткий диск, вы ограничены в способах восстановления системы. Вы сможете восстановить данные тома, но не сможете воссоздать структуру диска.
- Если вы используете для хранения резервных копий внешний жесткий диск, диск будет предназначен исключительно для хранения архивов и не

будет отображаться в Проводнике Windows (Windows Explorer). Перед архивацией диск будет отформатирован, в результате чего с него будут удалены все данные.

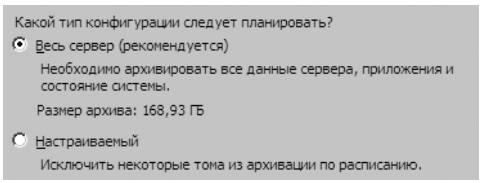
- В случае использования для хранения резервных копий удаленной общей папки при каждом создании нового архива старый архив будет перезаписываться. Не выбирайте этот вариант, если хотите хранить несколько резервных копий каждого сервера.
- Съемные носители и DVD позволяют восстанавливать только тома целиком, но не приложения или отдельные файлы. Емкость используемого носителя не должна быть меньше 1 Гб.

В следующем разделе рассмотрены способы выполнения архивации. Алгоритмы архивации сервера в Системе архивации данных Windows Server (Windows Server Backup) и Wbadmin очень похожи.

Настройка архивации по расписанию

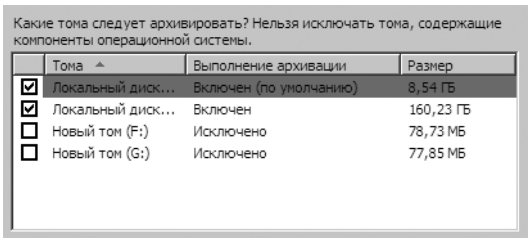
Программа Система архивации данных Windows Server (Windows Server Backup) позволяет запланировать автоматическую архивацию сервера. Выполните следующие действия:

1. В консоли **Система архивации данных Windows Server (Windows Server Backup)** вы по умолчанию подключены к локальному серверу. При необходимости подключитесь к удаленному серверу.
2. В меню **Действие (Action)** или в области действий щелкните команду **Расписание архивации (Backup Schedule)**. Откроется Мастер расписания архивации (Backup Schedule Wizard). Щелкните **Далее (Next)**.
3. На странице **Выбор конфигурации архивации (Select Backup Type)**, показанной на следующем рисунке, обратите внимание на размер архива под переключателем **Весь сервер (Full Server)**. Это пространство, необходимое для архивации данных сервера, приложений и состояния системы. Для архивации всех томов сервера установите переключатель **Весь сервер (Full Server)** и щелкните **Далее (Next)**. Для архивации избранных томов сервера установите переключатель **Настраиваемый (Custom)** и щелкните **Далее (Next)**.

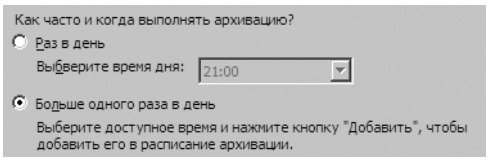


Примечание Тома, содержащие файлы операционной системы или приложений, автоматически включены в архив, и исключить их оттуда нельзя. К сожалению, это означает, что на сервере, где ОС Windows Server 2008 установлена на диске D, вам придется также архивировать и весь диск C, потому что он содержит диспетчер загрузки и другие загрузочные файлы.

4. Если вы установили переключатель **Настраиваемый (Custom)**, откроется страница **Выбор элементов для архивации (Select Backup Items)**. Установите флажки напротив томов, которые нужно архивировать, и сбросьте флажки томов, не подлежащих архивации, как показано на следующем рисунке.



5. На странице **Укажите время архивации (Specify Backup Time)** задайте периодичность и время проведения архивации. Для ежедневной архивации в установленное время установите переключатель **Раз в день (Once A Day)** и задайте время начала ежедневной архивации. Для проведения архивации по несколько раз в день установите переключатель **Больше одного раза в день (More Than Once A Day)**, как показано на следующем рисунке. В разделе **Доступное время (Available Time)** выберите время начала архивации, после чего щелкните **Добавить (Add)**, чтобы переместить время в раздел **Назначенное время (Scheduled Time)**. Повторите действие для каждого назначаемого времени запуска. Щелкните **Далее (Next)**.



6. На странице **Выберите диск назначения (Select Destination Disk)** выберите диск, который будет использоваться для архивации. Если в списке нет нужного вам диска, щелкните кнопку **Показать все доступные диски (Show All Available Disks)**. Установите флажок рядом с диском, на котором хотите хранить резервные копии.

Примечание На каждом диске можно хранить до 512 резервных копий, в зависимости от объема данных в каждом архиве. Вы можете выбрать несколько дисков. В этом случае Система архивации данных Windows Server (Windows Server Backup) будет чередовать диски.

7. Когда вы щелкнете кнопку **Далее (Next)**, на экране появится предупреждение о том, что выбранные диски будут отформатированы, а все имеющиеся на них данные — удалены. Щелкните **Да (Yes)**.

8. На странице **Маркировка диска назначения (Destination Disk)** отображен выбранный вами диск. Ему назначена метка, отображающая тип диска, имя сервера, текущую дату и время, а также размер диска. Эта информация потребуется вам для идентификации диска, поэтому обязательно запишите ее. На внешние диски можно наклеить ярлычок с этими сведениями.
9. На странице **Подтверждение операций (Confirmation)** просмотрите заданные параметры, затем щелкните **Готово (Finish)**. После этого мастер приступит к форматированию диска. В зависимости от размера диска процесс форматирования может занять несколько минут или более долгое время.
10. Когда мастер завершит работу, щелкните **Закрыть (Close)**. Теперь вы запланировали архивацию выбранного вами сервера.

В программе Wbadmin для планирования архивации используется команда ENABLE BACKUP. Она поддерживает следующие параметры:

- **–addTarget** Место хранения резервных копий в соответствии с GUID диска, который вы предполагаете использовать. Чтобы узнать идентификатор GUID диска, запустите команду GET DISKS.
- **–removeTarget** Место хранения, которое требуется удалить из расписания архивации, также в соответствии с GUID диска.
- **–include** Список букв томов, разделенных запятыми, их точки подключения и идентификаторы GUID.
- **–allCritical** Автоматическое включение в архив всех томов операционной системы.
- **–quiet** Отказ от вывода сообщений для пользователя в ходе выполнения команды.

Далее показаны примеры использования команды ENABLE BACKUP. Чтобы ежедневно в 21:00 проводить архивацию дисков C: и D:, введите команду:

```
wbadmin enable backup -addtarget:{06d88776-0000-0000-0000-000000000000}
 -schedule:18:00 -include:c:,d:
```

Чтобы назначить ежедневную архивацию всех томов ОС в 6:00 и 21:00, введите команду:

```
wbadmin enable backup -addtarget:{06d88776-0000-0000-0000-000000000000}
 -schedule:06:00,18:00 -allcritical
```

Изменение или остановка архивации по расписанию

Чтобы изменить расписание архивации или остановить его выполнение, выполните следующие действия:

1. Запустите консоль **Система архивации данных Windows Server (Windows Server Backup)**. По умолчанию вы подключены к локальному серверу. При необходимости подключитесь к удаленному серверу.

2. В меню **Действие (Action)** или в области действий щелкните команду **Расписание архивации (Backup Schedule)**. Откроется Мастер расписания архивации (Backup Schedule Wizard). Щелкните **Далее (Next)**.
3. На странице **Параметры архивации по расписанию (Schedule Backup Settings)** установите переключатель **Изменить архив (Modify Backup)**, чтобы добавить или удалить элементы архивации, изменить время или целевые тома. Затем приступайте к шагу 4. Чтобы остановить выполнение архивации по расписанию, установите переключатель **Прекратить архивацию (Stop Backup)**. Щелкните **Далее (Next)** и **Готово (Finish)**. Пропустите оставшиеся шаги.

Примечание Остановка архивации освобождает диск для обычного использования. Архивы не удаляются и по-прежнему доступны для восстановления.

4. На странице **Выбор конфигурации архивации (Select Backup Type)**, показанной на следующем рисунке, обратите внимание на размер архива под переключателем **Весь сервер (Full Server)**. Это пространство, необходимое для архивации данных сервера, приложений и состояния системы. Для архивации всех томов сервера установите переключатель **Весь сервер (Full Server)** и щелкните **Далее (Next)**. Для архивации избранных томов сервера установите переключатель **Настраиваемый (Custom)** и щелкните **Далее (Next)**.
5. Если вы установили переключатель **Настраиваемый (Custom)**, откроется страница **Выбор элементов для архивации (Select Backup Items)**. Установите флажки напротив томов, которые нужно архивировать, и сбросьте флажки томов, не подлежащих архивации.
6. На странице **Укажите время архивации (Specify Backup Time)** задайте периодичность и время проведения архивации. Для ежедневной архивации в установленное время установите переключатель **Раз в день (Once A Day)** и задайте время начала ежедневной архивации. Для проведения архивации по несколько раз в день установите переключатель **Больше одного раза в день (More Than Once A Day)**, как показано на следующем рисунке. В разделе **Доступное время (Available Time)** выберите время начала архивации, после чего щелкните **Добавить (Add)**, чтобы переместить время в раздел **Назначенное время (Scheduled Time)**. Повторите действие для каждого назначаемого времени запуска. Щелкните **Далее (Next)**.
7. На странице **Добавление или удаление дисков архивации (Add Or Remove Backup Disks)** выполните одно из следующих действий, а затем щелкните **Далее (Next)**:
   - Установите переключатель **Действие не требуется (Do Nothing)**, если не хотите изменять целевые диски архивации.
   - Установите переключатель **Добавить диски (Add More Disks)**, чтобы добавить один или несколько дисков для архивации. На странице **Выберите диск назначения (Select Destination Disk)** поставьте

флажки напротив дисков, которые хотите использовать в качестве архивных. Когда вы щелкнете кнопку **Далее (Next)**, на экране появится предупреждение о том, что выбранные диски будут отформатированы, а все имеющиеся на них данные — удалены. Щелкните **Да (Yes)**. На странице **Маркировка диска назначения (Destination Disk)** отображены все выбранные вами диски. Щелкните **Далее (Next)**.

- Установите переключатель **Удаление текущих дисков (Remove Current Disks)**, чтобы удалить один или несколько установленных в данный момент архивных дисков. На странице **Удаление текущих дисков (Remove Current Disks)** установите флажки дисков, которые вы более не хотите использовать для хранения архивов.

8. На странице **Подтверждение (Confirmation)** просмотрите заданные параметры и щелкните **Готово (Finish)**. Мастер изменит расписание и отформатирует добавленные диски. На странице **Сводка (Summary)** щелкните **Закрыть (Close)**.

Программа Wbadmin позволяет изменять запланированную архивацию при помощи команды ENABLE BACKUP. Для изменения резервных дисков применяются параметры **–addTarget** и **–removeTarget**. Для изменения расписания запуска и списка включенных томов достаточно задать новые значения. Рассмотрим примеры.

Чтобы удалить диск из архивации по расписанию, введите команду:

```
wbadmin enable backup -removetarget:{06d88776-0000-0000-0000-000000000000}
```

Чтобы добавить диск в архивацию по расписанию, введите команду:

```
wbadmin enable backup -addtarget:{41cd2567-0000-0000-0000-000000000000}
```

Чтобы изменить расписание запуска и список включенных томов, введите команду:

```
wbadmin enable backup -schedule:03:00 -include:c:,d:,e:
```

Создание архивов и расписания при помощи Wbadmin

Чтобы выполнить архивацию вручную, запустите команду START BACKUP в программе Wbadmin. Она имеет следующие параметры:

- **–backupTarget** Место хранения резервных копий. Задается в виде буквы диска или UNC-пути к общей папке на удаленном сервере, соответствующим универсальному соглашению об именовании.
- **–include** Список букв томов, разделенных запятыми, их точки подключения и идентификаторы GUID.
- **–allCritical** Автоматическое включение в архив всех томов операционной системы.
- **–inheritAcl** Указывает, что архивная папка в удаленной общей папке должна наследовать полномочия доступа общей папки. Если этот пара-

метр не задан, доступ к резервной папке будут иметь только пользователи, заданные в параметре **–user**, а также администраторы и операторы архива.

- **–noVerify** Указывает, что резервные копии, записываемые на съемные носители, не требуют проверки. Если этот параметр не задан, выполняется проверка архивов, записываемых на съемные носители.
- **–password** Пароль для подключения к удаленной общей папке.
- **–quiet** Отказ от вывода сообщений для пользователя в ходе выполнения команды.
- **–user** Имя пользователя для подключения к удаленной общей папке.
- **–vssFull** Указывает на необходимость выполнения полной архивации при помощи VSS. Это обеспечит сохранность всех данных сервера и приложений. Не включайте этот параметр, если для архивации приложений вы используете программы сторонних производителей.

В следующих примерах иллюстрируется использование команды START BACKUP:

Полная архивация сервера:

```
wbadmin start backup -backuptarget:f: -vssfull
```

Архивация дисков C: и D: на диск F:

```
wbadmin start backup -backuptarget:f: -include:c:,d:
```

Архивация всех критических томов:

```
wbadmin start backup -backuptarget:f: -allcritical
```

Архивация дисков C: и D: в удаленную общую папку:

```
wbadmin start backup -backuptarget:\\fileserver27\backups -include:c:,d:
 -user:williams
```

Чтобы запланировать архивацию на различные дни и время, создайте задания на выполнение этой команды в Планировщике заданий (Task Scheduler), выполнив следующие действия:

1. Последовательно щелкните **Пуск (Start)**, **Администрирование (Administrative Tools)** и **Планировщик заданий (Task Scheduler)**. По умолчанию вы подключены к локальному компьютеру. При необходимости подключитесь к нужному удаленному компьютеру.
2. Щелкните правой кнопкой узел **Планировщик заданий (Task Scheduler)** и выберите команду **Создать задачу (Create Task)**. Откроется диалоговое окно **Создание задачи (Create Task)**.
3. На вкладке **Общие (General)** введите имя задания и задайте его параметры безопасности.
   - Если задание следует запускать от имени другого пользователя, щелкните кнопку **Изменить (Change)**. В диалоговом окне **Выбор:**

«Пользователь» или «Группа» (Select User Or Group) выберите пользователя или группу, от имени которой следует выполнять задание. По требованию системы подтвердите свои полномочия.

- Установите другие параметры запуска. По умолчанию выполнение задания производится, когда пользователь находится в системе. Чтобы выполнять задание независимо от нахождения пользователя в системе, установите флажок **Выполнять вне зависимости от регистрации пользователя (Run Whether User Is Logged On Or Not)**. Кроме того, вы можете установить запуск с наивысшими правами, а также настроить задание для более ранних версий Windows.

4. На вкладке **Триггеры (Triggers)** щелкните кнопку **Создать (New)**. В диалоговом окне **Создание триггера (New Trigger)** в раскрывающемся списке **Начать задачу (Begin The Task)** выберите вариант **По расписанию (On A Schedule)**. С помощью имеющихся параметров задайте расписание и щелкните **OK**.
5. На вкладке **Действия (Actions)** щелкните **Создать (New)**. В диалоговом окне **Создание действия (New Action)** в раскрывающемся списке **Действие (Action)** выберите вариант **Запуск программы (Start A Program)**.
6. В поле **Программа или сценарий (Programm/Script)** введите **%windir%\System32\wbadmin.exe**.
7. В поле **Добавить аргументы (Add Arguments)** введите команду START BACKUP и ее параметры, например:

```
start backup -backuptarget:f: -include:c:,d:,e:\mountpoint,\\?\
volume{be345a23-32b2-432d-43d2-7867ff3e3432}\
```

8. Щелкните **OK**, чтобы закрыть диалоговое окно **Создание действия (New Action)**.
9. На вкладке **Условия (Conditions)** укажите условия запуска и останова задачи.
10. На вкладке **Параметры (Settings)** задайте дополнительные параметры задания.
11. Щелкните **OK**, чтобы создать задание.

Запуск архивации вручную

Чтобы выполнить архивацию сервера вручную, выполните следующие действия:

1. Запустите консоль **Система архивации данных Windows Server (Windows Server Backup)**. По умолчанию вы подключены к локальному серверу. При необходимости подключитесь к удаленному серверу.
2. В меню **Действие (Action)** или в области действий щелкните команду **Однократная архивация (Backup Once)**. Откроется Мастер однократной архивации (Backup Once Wizard). Щелкните **Далее (Next)**.

3. Если для архивации сервера следует использовать те же параметры, что использовались в Мастере расписания архивации (Backup Schedule Wizard), установите переключатель **Те же параметры (The Same Options)**. Щелкните **Далее (Next)** и **Архивировать (Backup)**, чтобы выполнить архивацию. Пропустите оставшиеся шаги.
4. Если для архивации сервера следует использовать другие параметры, установите переключатель **Другие параметры (Different Options)** и щелкните **Далее (Next)**.
5. На странице **Выбор конфигурации архивации (Select Backup Type)** обратите внимание на размер резервной копии под переключателем **Весь сервер (Full Server)**. Это пространство, необходимое для архивации данных сервера, приложений и состояния системы. Чтобы архивировать все тома сервера, установите переключатель **Весь сервер (Full Server)** и щелкните **Далее (Next)**. Для архивации избранных томов сервера установите переключатель **Настраиваемый (Custom)** и щелкните **Далее (Next)**.
6. Если вы установили переключатель **Настраиваемый (Custom)**, откроется страница **Выбор элементов для архивации (Select Backup Items)**. Установите флажки томов, которые вы хотите архивировать, и сбросьте флажки томов, не подлежащих архивации. Чтобы создать резервную копию состояния системы и всех критических томов ОС, установите флажок **Включить восстановление системы (Enable System Recovery)**. Щелкните **Далее (Next)**.
7. На странице **Укажите тип места назначения (Specify Destination Type)** выполните одно из следующих действий:
   - Для создания резервной копии на локальных дисках установите переключатель **Локальные диски (Local Drives)** и щелкните **Далее (Next)**. На странице **Выбор места назначения архивации (Backup Destination)** выберите внутренний, внешний или DVD-диск для использования в качестве резервного диска. При сохранении на DVD-диске резервные копии сжимаются. В результате размер архива на DVD может оказаться меньше, чем размер тома на сервере. Если в качестве резервного используется съемный диск, после выполнения мастером записи архивов автоматически проводится их проверка. Чтобы не проводить проверку, сбросьте флажок **Проверять после записи (Verify After Writing)**. Щелкните **Далее (Next)**.
   - Для архивации в удаленную общую папку установите переключатель **Удаленная общая папка (Remote Shared Folder)** и щелкните **Далее (Next)**. На странице **Укажите удаленную папку (Specify Remote Folder)** введите UNC-путь к удаленной папке, например, \\FileServer43\Backups. Если вы хотите, чтобы резервная копия была доступна для всех пользователей, имеющих доступ к общей папке, в разделе **Управление доступом (Access Control)** установите переключатель **Наследовать (Inherit)**. Для ограничения доступа

к общей папке текущим пользователем, администраторами и операторами архива установите переключатель **Не наследовать (Do Not Inherit)**. Щелкните **Далее (Next)**. Когда вам будет предложено ввести учетные данные, введите имя пользователя и пароль учетной записи, имеющей доступ на запись в общую папку.

8. На странице **Укажите дополнительный параметр (Specify VSS Backup Type)** укажите, следует ли выполнять архивацию копированием или полную архивацию посредством VSS. Установите переключатель **Копирующая архивация VSS (Copy Backup)**, если для архивации данных приложений используется отдельная программа. В противном случае установите переключатель **Полная архивация VSS (VSS Full Backup)** для полной архивации выбранных томов вместе с данными приложений.
9. Щелкните **Далее (Next)** и **Архивировать (Backup)**. Ход выполнения архивации отображается в диалоговом окне. Если вы щелкнете кнопку **Закрыть (Close)**, архивация продолжится в фоновом режиме.

Восстановление сервера после сбоя или неудачной загрузки

Подобно Windows Vista, Windows Server 2008 располагает обширной архитектурой диагностики и разрешения проблем. Эти компоненты позволяют восстанавливать систему после большинства аппаратных сбоев, ошибок памяти и проблем с производительностью. Устранение неисправностей происходит либо автоматически, либо система помогает пользователям в процессе их устранения.

Система Windows Server 2008 оснащена более надежными и производительными драйверами устройств, позволяющими избежать многих известных случаев зависаний и отказов системы. Улучшенное прерывание ввода-вывода для драйверов устройств обеспечивает восстановление ОС после блокирующих вызовов. Кроме того, сократилось количество блокирующих операций ввода/вывода диска.

Для уменьшения времени простоя и числа перезагрузок, требующихся при установке приложений, в Windows Server 2008 применяется процесс обновления, помечающий используемые файлы, подлежащие обновлению. Файлы автоматически заменяются при следующем запуске приложения. В некоторых случаях Windows Server 2008 может сохранить данные приложения, закрыть приложение, обновить используемые файлы, а затем снова открыть приложение. Для увеличения общей производительности и улучшения отклика системы в Windows Server 2008 более эффективно используется память, обеспечено упорядоченное выполнение групп потоков и введен новый механизм управления процессами. Оптимизация использования памяти и процессов приводит к тому, что фоновые процессы не оказывают столь сильного влияния на производительность системы.

Система Windows Server 2008 предоставляет больше информации о причинах зависания программ. Наличие дополнительных сведений об ошибках

в журналах событий ОС облегчает идентификацию и разрешение проблем. Гораздо эффективнее, чем в предшествующих системах, в Windows Server 2008 для автоматического восстановления служб после сбоя используются политики восстановления служб. Восстанавливая отказавшую службу, Windows Server 2008 автоматически обрабатывает все виды зависимостей. Перед запуском отказавшей службы запускаются все необходимые зависимые службы и компоненты системы.

В предыдущих версиях Windows в случае фатального сбоя или зависания приложения пользователю сообщалось, что приложение не отвечает. Пользователю приходилось самостоятельно закрывать и заново запускать приложение. Windows Server 2008 пытается автоматически решать проблему неотвечающих приложений при помощи Диспетчера перезапуска (Restart Manager). Он автоматически закрывает и перезапускает приложения. Благодаря этому диспетчеру вам, скорее всего, не придется самому решать проблемы зависших приложений.

Неудачная установка и зависшие приложения и драйверы отслеживаются в консоли **Отчеты о проблемах и их решениях (Problem Reports And Solutions)**. В случае возникновения проблемы встроенная система диагностики выдает предупреждение, щелкнув которое вы откроете диалоговое окно **Отчеты о проблемах и их решениях (Problem Reports And Solutions)**. Оно позволяет провести поиск решений проблем в Интернете. Чтобы просмотреть список текущих проблем, выполните следующие действия:

1. Щелкните **Пуск (Start)** и **Панель управления (Control Panel)**.
2. В панели управления щелкните ссылку **Система и ее обслуживание (System Maintenance)**, а затем — **Отчеты о проблемах и их решениях (Problem Reports And Solutions)**.
3. В консоли **Отчеты о проблемах и их решениях (Problem Reports And Solutions)** щелкните ссылку **Показать проверяемые проблемы (See Problems To Check)** на левой панели.
4. На экране появится список известных проблем. Установите флажок рядом с проблемой и щелкните кнопку **Искать решения (Check For Solutions)**, чтобы провести поиск имеющихся решений на веб-сайте Майкрософт.

Система Windows Server 2008 пытается решать проблемы, происходящие из-за недостатка виртуальной памяти, при помощи функции Resource Exhaustion Detection And Recovery. Эта функция отслеживает использование системной виртуальной памяти и предупреждает об истощении виртуальной памяти. Чтобы помочь устранить проблему, она также выявляет процессы, потребляющие наибольший объем памяти, и выводит диалоговое окно, позволяющее закрыть любое приложение, использующее много памяти. Предупреждение об истощении памяти также записывается в журнал Система (System).

В прежних версиях Windows одной из распространенных причин неудачной загрузки системы было повреждение системных файлов. В Windows

Server 2008 имеются встроенные средства диагностики, которые автоматически выявляют поврежденные файлы системы в ходе загрузки и помогают выполнить ручное или автоматическое восстановление. Для устранения проблем, возникающих на этапе загрузки системы, в Windows Server 2008 применяется средство Startup Repair Tool (StR), которое устанавливается автоматически и запускается при неудачной попытке загрузить систему. После запуска StR пытается установить причину сбоя загрузки, анализируя журналы загрузки и отчеты об ошибках, и пытается решить проблему автоматически. Если StR не в состоянии справиться с проблемой, она выполняет восстановление системы до последнего известного рабочего состояния, после чего предоставляет диагностическую и справочную информацию для дальнейшего устранения неисправностей.

К числу проблем оборудования, обрабатываемых встроенными средствами диагностики, относятся ошибки и сбои на диске. Если в устройстве имеются неисправности, средства диагностики оборудования выявят обстоятельства возникновения проблемы и устранят неисправность автоматически или проведут пользователя по этапам процесса восстановления. В случае дисковых накопителей средства диагностики оборудования могут использовать отчеты о неисправностях, предоставляемые дисками, чтобы обнаружить потенциальный сбой и заблаговременно предупредить вас. Больше того, предупредив о неисправности диска, средства диагностики оборудования помогут вам выполнить архивацию.

Проблемы производительности, решаемые встроенными средствами диагностики, включают медленный запуск приложений, медленную загрузку, медленный переход в режим ожидания и обратно, а также медленное закрытие. При ухудшении производительности компьютера средства диагностики производительности помогут обнаружить проблему и предоставят возможные пути ее решения. Решая более сложные проблемы производительности, отслеживайте соответствующие данные о производительности и стабильности в консоли **Монитор надежности и производительности (Reliability And Performance Monitor)**, о которой подробно рассказывается в главе 4.

К проблемам памяти, входящим в компетенцию встроенных средств диагностики, относятся утечки памяти и ошибки памяти. Утечки памяти происходят, когда приложение или системный компонент не полностью освобождают области физической памяти, завершив работу с ними. Если вы подозреваете, что на компьютере имеются проблемы памяти, не обнаруженные автоматически, вручную запустите Средство диагностики памяти Windows (Windows Memory Diagnostics) во время загрузки, выбрав для этого соответствующую команду. Если команда отсутствует, запустите программу вручную, выполнив следующие действия:

1. Щелкните **Пуск (Start)**. В поле **Начать поиск (Search)** введите **mdsched.exe** и нажмите Enter.
2. Выберите немедленную перезагрузку и запуск средства или запланируйте проверку на время следующей загрузки.

3. После перезагрузки компьютера Средство диагностики памяти Windows (Windows Memory Diagnostics) запускается автоматически. Вы сможете выбрать один из трех типов тестирования: от базового до полного.

Для выявления возможности полного отказа системы из-за ошибки памяти средство диагностики подключается к инструменту Microsoft Online Crash Analysis. В случае отказа компьютера из-за ошибки памяти, обнаруженной средством диагностики памяти, вам будет предложено запланировать тестирование памяти на время следующей перезагрузки системы.

Запуск сервера в безопасном режиме

Если система не загружается нормально, безопасный режим поможет вам ее восстановить или найти неисправность. В безопасном режиме Windows Server 2008 загружает только основные файлы, службы и драйверы — мыши, монитора, клавиатуры, накопителя и видео. Сетевые службы и драйверы не запускаются, если не выбрана загрузка в безопасном режиме с поддержкой сети. В безопасном режиме загружается только ограниченный набор информации о конфигурации, что позволяет найти неисправность. Как правило, следует сначала загрузить компьютер в безопасном режиме и лишь потом пытаться использовать аварийный диск или запускать консоль восстановления.

Чтобы запустить систему в безопасном режиме, выполните следующие действия:

1. Запустите или перезагрузите сбойную систему.
2. В ходе загрузки нажмите клавишу F8, чтобы отобразить меню **Дополнительные варианты загрузки (Advanced Boot Options)**.
3. Выберите безопасный режим, в котором хотите работать, и нажмите Enter. Выбор режима зависит от типа возникшей проблемы. Возможные варианты таковы:
   - **Безопасный режим (Safe Mode)** Во время последовательности инициализации происходит загрузка только основных файлов, служб и драйверов. Загружаются драйверы мыши, монитора, клавиатуры, накопителя и видео. Сетевые службы и драйверы не запускаются.
   - **Безопасный режим с загрузкой сетевых драйверов (Safe Mode With Networking)** Загружаются основные файлы, службы и драйверы, а также службы и драйверы, необходимые для работы в сети.
   - **Безопасный режим с поддержкой командной строки (Safe Mode With Command Prompt)** Загружаются основные файлы, службы и драйверы, после чего вместо графического интерфейса Windows запускается командная строка. Сетевые службы и драйверы не запускаются.

Совет В Безопасном режиме с поддержкой командной строки (Safe Mode With Command Prompt) вы можете запустить оболочку Explorer из командного интерфейса. Нажмите клавиши Ctrl+Shift+Esc, выберите в меню **Файл (File)** Диспетчера задач (Task Manager) команду **Новая задача (New Process)** и введите **explorer.exe**.

- **Ведение журнала загрузки (Enable Boot Logging)** Позволяет создавать записывать все события, происходящие во время загрузки, в журнал загрузки.
- **Включение видеорежима с низким разрешением (Enable Low Resolution Video)** Запускает систему с низким разрешением экрана (640x480). Это полезно, если установлен режим дисплея, не поддерживаемый текущим монитором.
- **Последняя удачная конфигурация (Last Known Good Configuration)** Запускает компьютер в безопасном режиме, используя информацию из реестра, сохраненную Windows во время последнего завершения работы. Загружается только раздел HKEY_CURRENT_CONFIG с информацией о конфигурации оборудования, позволившей ранее успешно запустить компьютер.
- **Режим отладки (Debugging Mode)** Запускает систему в режиме исправления ошибок. Применяется только для поиска ошибок в операционной системе.
- **Режим восстановления служб каталогов (Directory Services Recovery Mode)** Запускает систему в безопасном режиме и позволяет восстановить службу каталогов. Эта возможность доступна на контроллерах домена Windows Server 2008.
- **Отключить автоматическую перезагрузку при отказе системы (Disable Automatic Restart On System Failure)** Препятствует автоматической перезагрузке Windows Server 2008 при полном отказе ОС.
- **Отключение обязательной проверки подписи драйверов (Disable Driver Signature Enforcement)** Запускает компьютер в безопасном режиме, игнорируя политику цифровых подписей для драйверов. Если ошибку запуска вызвал драйвер с недействительной или отсутствующей цифровой подписью, это временно решит проблему, позволив запустить компьютер и устранить неполадку путем установки нового драйвера или изменения параметров проверки цифровых подписей.

Если в безопасном режиме проблема не возникает, вычеркните стандартные параметры и драйверы основных устройств из списка возможных причин сбоя. Если причиной проблемы является добавленное устройство, безопасный режим позволяет удалить устройство или откатить обновление.

Продолжение работы после неудачного запуска

Подобно Windows Vista, Windows Server 2008 после неудачного запуска автоматически входит в режим Восстановление после ошибок Windows (Windows Error Recovery). Ваши возможности в этом режиме схожи с возможностями меню дополнительных вариантов загрузки. Для устранения неисправностей вы можете загрузить систему в Безопасном режиме (Safe Mode), Безопасном режиме с загрузкой сетевых драйверов (Safe Mode With

Networking) или Безопасном режиме с поддержкой командной строки (Safe Mode With Command Prompt). Вы также можете выбрать загрузку последней удачной конфигурации или обычную загрузку Windows. Подробнее — в предыдущем разделе.

Совет Если вы предпочитаете работать с меню **Дополнительные варианты загрузки (Advanced Boot Options)**, перезагрузите сервер, а затем нажмите **F8** до инициализации режима Восстановление после ошибок Windows (Windows Error Recovery).

Архивация и восстановление состояния системы

В Windows Server 2008 имеется порядка 50000 файлов состояния системы, которые в стандартной установке на базе компьютера *x*86 занимают около 4 Гб дискового пространства. Быстрее и проще архивировать и восстанавливать состояние системы сервера при помощи программы Wbadmin. В ней для создания резервной копии состояния системы компьютера служит команда START SYSTEMSTATEBACKUP, а команда START SYSTEMSTATERECOVERY восстанавливает состояние системы на компьютере.

Совет Для восстановления состояния системы на контроллере домена вы должны работать в Режиме восстановления служб каталогов (Directory Services Restore). О восстановлении Active Directory речь пойдет в следующем разделе.

Для архивации состояния сервера введите в командной строке с расширенными полномочиями команду:

```
wbadmin start systemstatebackup -backupTarget:ИмяТома
```

где *ИмяТома* — диск для сохранения резервной копии, например, F:.

Чтобы восстановить состояние сервера введите в командной строке с расширенными полномочиями команду:

```
wbadmin start systemstaterecovery -backupTarget:ИмяТома
```

где *ИмяТома* — расположение, в котором хранится резервная копия, например, F:. Кроме того, вы можете сделать следующее:

- Задайте параметр –**recoveryTarget**, чтобы провести восстановление в другое расположение.
- Задайте параметр –**machine**, чтобы указать имя восстанавливаемого компьютера, если в архивном расположении содержатся резервные копии для нескольких компьютеров.
- Задайте параметр –**authorsysvol** для принудительного восстановления каталога Sysvol.

Восстановление Active Directory

Восстанавливая состояние системы на контроллере домена, вы должны решить, какое восстановление выполнять — принудительное или непринудительное. Стандартный вариант — непринудительное восстановление. В этом

режиме Active Directory и другие реплицируемые данные восстанавливаются из резервной копии, а все изменения реплицируются с другого контроллера домена. Таким образом, вы восстанавливаете сбойный контроллер домена, не перезаписывая последнюю информацию Active Directory. С другой стороны, при восстановлении Active Directory по сети при помощи архивных данных следует проводить принудительное восстановление. При этом данные восстанавливаются на текущий контроллер домена, а затем реплицируются на другие контроллеры.

Внимание! Принудительное восстановление перезаписывает все данные Active Directory в домене. Прежде чем выполнять его, убедитесь, что данные архива действительно можно распространить в домене, а текущие данные на других контроллерах домена неверны, устарели или повреждены.

Чтобы восстановить Active Directory на контроллере домена и включить репликацию восстановленных данных по сети, выполните следующие действия:

1. Убедитесь, что контроллер домена выключен.
2. Запустите контроллер домена. Нажмите F8, чтобы открыть меню **Дополнительные варианты загрузки (Advanced Boot Options)**.
3. Выберите команду **Режим восстановления служб каталогов (Directory Services Restore Mode)**.
4. После загрузки системы восстановите состояние системы и другие важные файлы при помощи системы архивации.
5. После восстановления данных, но перед перезагрузкой сервера, сделайте объекты полномочными при помощи средства Ntdsutil. Полностью проверьте данные Active Directory.
6. Перезагрузите сервер. По завершению загрузки системы начнется репликация данных Active Directory в домене.

Восстановление операционной системы и всей системы

Как говорилось ранее, Windows Server 2008 обладает функциональными возможностями по исправлению ошибок запуска, которые способны восстановить сервер в случае повреждения или отсутствия системных файлов. Процесс восстановления запуска также способен исправить некоторые ошибки загрузки, включая ошибки диспетчера загрузки. В случае сбоя этих процессов, если причина отказа системы заключается в диспетчере загрузки, вы можете восстановить диспетчер загрузки и запустить систему при помощи установочного диска Windows Server 2008 или восстановительного раздела.

В среде восстановления Windows имеются следующие инструментальные средства:

- **Восстановление архива Windows Complete PC (Windows Complete PC Restore)** Позволяет восстановить ОС сервера или выполнить полное восстановление системы. Убедитесь в доступности архивных данных и

в том, что вы можете войти на компьютер с учетной записью, имеющей соответствующие полномочия. При полном восстановлении системы имейте в виду, что существующие данные, которых нет в резервных копиях, в ходе восстановления будут удалены. К ним относятся все используемые тома, отсутствующие в резервной копии.

- **Средство диагностики памяти Windows (Windows Memory Diagnostics)** Позволяет проводить диагностику неисправностей физической памяти сервера. Существует три уровня тестирования памяти: базовый, стандартный и полный.

Кроме того, вы можете работать в командной строке, используя инструменты, доступные во время установки, а также дополнительные программы.

- **X:\Sources\Recovery\StartRep.exe (Startup Repair)** Обычно этот инструмент запускается автоматически при сбое загрузки, если Windows обнаруживает неполадку в загрузочном секторе, диспетчере загрузки или хранилище данных конфигурации загрузки (BCD).
- **X:\Sources\Recovery\recenv.exe (Startup Recovery Options)** Позволяет запустить мастер Startup Recovery Options. Если ранее вы ввели неверные параметры восстановления, вы сможете изменить их.

Восстановить ОС сервера или выполнить полное восстановление системы можно при помощи установочного диска Windows и резервной копии, созданной в программе **Система архивации данных Windows Server (Windows Server Backup)**. В ходе восстановления ОС восстанавливаются все критические тома. Несистемные тома не восстанавливаются. Если вы восстанавливаете всю систему, система архивации данных Windows Server переформатирует все диски, создает на них новые разделы и подключает их к серверу. Этот способ следует использовать только в случаях, когда вы хотите восстановить данные сервера на другом оборудовании или когда все попытки восстановить сервер на существующем оборудовании потерпели неудачу.

Примечание При восстановлении ОС или всей системы убедитесь в доступности архивных данных и в том, что вы можете войти на компьютер с учетной записью, обладающей соответствующими полномочиями. При полном восстановлении системы имейте в виду, что существующие данные, которых нет в резервных копиях, будут удалены в ходе восстановления. К ним относятся и все используемые сервером тома, которых нет в резервной копии.

Для восстановления ОС сервера или полного восстановления системы выполните следующие действия:

1. Вставьте диск Windows в CD- или DVD-дисковод и перезапустите компьютер. Нажмите на соответствующую клавишу, чтобы загружаться с компакт-диска. На экране появится мастер установки Windows.
2. Задайте языковые параметры и щелкните **Далее (Next)**.
3. Щелкните **Восстановление системы (Repair Your Computer)**. Будет выполнен поиск существующей установки Windows на жестких дисках. Результаты будут отображены в окне мастера **Параметры восстановления**

системы (System Recovery Options Wizard). Если вы восстанавливаете ОС на другом оборудовании, список должен быть пустым: на компьютере нет операционных систем. Щелкните **Далее (Next)**.

4. На странице **Параметры восстановления системы (System Recovery Options)** щелкните ссылку **Восстановление архива Windows Complete PC (Windows Complete PC Restore)**. Откроется одноименный мастер.
5. Установите переключатель **Использовать последний доступный архив (рекомендуется) (Use The Latest Available Backup (Recommended))** или **Восстановить другой архив (Restore A Different Backup)**. Затем щелкните **Далее (Next)**.
6. Если вы выбрали восстановление из другой резервной копии, на странице **Выберите расположение резервной копии (Select The Location Of The Backup)** выполните одно из следующих действий:
   - Щелкните компьютер, на котором содержится резервная копия для восстановления, затем щелкните **Далее (Next)**. На странице **Выберите резервную копию для восстановления (Select The Backup To Restore)** щелкните нужную резервную копию, а затем щелкните **Далее (Next)**.
   - Щелкните **Дополнительно (Advanced)** для поиска резервной копии в сети, после чего щелкните **Далее (Next)**. Найдите и выберите резервную копию в сети. Щелкните **Далее (Next)**.
7. На странице **Выберите тип восстановления резервной копии (Choose How To Restore The Backup)** выполните следующие необязательные действия и щелкните **Далее (Next)**:
   - Установите флажок **Форматировать и разбить на разделы диски (Format And Repartition Disks)**, чтобы удалить существующие разделы и переформатировать целевые диски в соответствии с резервной копией.
   - Щелкните кнопку **Исключить диски (Exclude Disks)** и установите флажки дисков, форматирование и создание разделов на которых нужно отменить. Диски, на которых хранятся используемые данные, исключаются автоматически.
   - Щелкните **Установить драйверы (Install Drivers)**, чтобы установить драйверы восстанавливаемых устройств.
   - Щелкните **Дополнительно (Advanced)**, чтобы указать, требуется ли перезагрузка компьютера и проверка дисков на наличие ошибок после завершения восстановления.
8. Просмотрите параметры восстановления и щелкните **Готово (Finish)**. После этого мастер Восстановление архива Windows Complete PC (Windows Complete PC Restore) восстановит ОС или весь сервер в соответствии с заданными параметрами.

Восстановление приложений, несистемных томов, файлов и папок

В Windows Server 2008 для восстановления состояния системы, полного восстановления сервера и восстановления отдельных томов, файлов и папок используются различные процессы. Чтобы восстановить несистемные тома, файлы и папки, воспользуйтесь Мастером восстановления (Recovery Wizard) из консоли **Система архивации данных Windows Server (Windows Server Backup)**. Прежде чем начать работу, убедитесь, компьютер, на который вы восстанавливаете файлы, работает под управлением Windows Server 2008. Если вы хотите восстановить отдельные файлы и папки, убедитесь также, что на внутреннем или внешнем диске или в удаленной общей папке имеется, по крайней мере, одна резервная копия. Нельзя восстановить отдельные файлы и папки из архивов, сохраненных на DVD или съемных носителях.

Чтобы восстановить несистемные тома, файлы, папки или данные приложений, выполните следующие действия:

1. Запустите консоль **Система архивации данных Windows Server (Windows Server Backup)**. В области действий или в меню **Действие (Action)** щелкните команду **Восстановление (Recover)**. Откроется Мастер восстановления (Recovery Wizard).
2. На странице **Приступая к работе (Getting Started)** укажите, данные какого компьютера будут восстановлены (локального или другого), и щелкните **Далее (Next)**. Допустим, вы вошли на компьютер FileServer18 и хотите восстановить данные с WebServer84. Установите переключатель **Другой сервер (Another Server)**, независимо от того, хранятся ли данные для сервера на локальном диске или удаленном общем ресурсе.
3. Если вы восстанавливаете данные другого компьютера, укажите, находятся ли восстанавливаемые данные на локальном накопителе или в удаленной общей папке. Щелкните **Далее (Next)**, а затем задайте параметры расположения. При восстановлении с локального диска на странице **Укажите тип размещения (Select Backup Location)** выберите в раскрывающемся списке расположение резервной копии. При восстановлении из удаленной общей папки на странице **Укажите удаленную папку (Specify Remote Folder)** введите путь к папке, содержащей резервную копию. В удаленной папке резервная копия должна храниться в подпапке \WindowsImageBackup*ComputerName*.
4. При восстановлении с локального компьютера, при наличии нескольких резервных копий, на странице **Выберите расположение резервной копии (Select Backup Location)** выберите архив в раскрывающемся списке.
5. На странице **Выбор даты архивации (Select Backup Date)** выберите дату и время создания резервной копии, которую хотите восстановить. Даты создания доступных резервных копий в календаре выделены полужирным. Щелкните **Далее (Next)**.
6. На странице **Выберите тип восстановления (Select Recovery Type)** выполните одно из следующих действий:

- Для восстановления отдельных файлов и папок установите переключатель **Файлы и папки (Files And Folders)** и щелкните **Далее (Next)**. На странице **Выберите элементы для восстановления (Select Items To Recover)** в разделе **Доступные элементы (Available Items)** щелкните значок «+», чтобы развернуть список и найти нужную папку. Щелкните папку, чтобы отобразить ее содержимое на соседней панели. Щелкните каждый элемент, который хотите восстановить, а затем щелкните **Далее (Next)**.
- Чтобы восстановить некритические тома, на которых нет ОС, установите переключатель **Тома (Volumes)** и щелкните **Далее (Next)**. На странице **Выберите тома (Select Volumes)** приведен список исходных и целевых томов. Установите флажки рядом с исходными томами, которые хотите восстановить. Затем в раскрывающемся списке **Конечный том (Destination Volume)**, выберите расположение, в котором хотите восстановить том. Щелкните **Далее (Next)**.
- Для восстановления данных приложений установите переключатель **Приложения (Applications)** и щелкните **Далее (Next)**. На странице **Выберите приложение (Select Application)** в разделе **Приложение (Application)** щелкните приложение, которое хотите восстановить. Щелкните **Далее (Next)**. Все данные на конечном томе после выполнения восстановления будут утеряны, поэтому убедитесь, что конечный том пуст или не содержит информации, которая может понадобиться впоследствии.

7. На странице **Укажите параметры восстановления (Specify Recovery Options)** в разделе **Конечные объекты восстановления (Recovery Destination)** укажите, куда следует восстанавливать данные: в исходное расположение (только для несистемных файлов) или в другое расположение. Выбрав другое расположение, введите путь к расположению восстановления или щелкните **Обзор (Browse)**, чтобы указать его. Данные приложений можно копировать в другое расположение, но восстановить приложения в другое расположение или на другой компьютер нельзя.
8. В разделе **Когда мастер обнаруживает файлы и папки в расположении восстановления (When Backup Finds Existing Files And Folders)** выберите действие, которое следует выполнить, если файлы и папки уже существуют в конечном расположении. Можно сохранить обе версии файла или папки, перезаписать существующие файлы восстановленными или пропустить повторяющиеся файлы и папки, чтобы сохранить существующие файлы.
9. На странице **Подтверждение (Confirmation)** проверьте параметры и щелкните **Восстановить (Recover)**, чтобы восстановить заданные объекты.

Политика восстановления шифрования

Если ваша организация использует шифрующую файловую систему EFS, план восстановления в аварийных ситуациях должен включать дополнительные процедуры. Следует принять во внимание вопросы, связанные с личными сертификатами шифрования, агентами восстановления EFS и политикой восстановления EFS. Эти вопросы рассмотрены в следующих разделах.

Сертификаты шифрования и политика восстановления

Шифрование файлов осуществляется на уровне папки или файла. Каждый файл, помещаемый в шифрованную папку, автоматически шифруется. Зашифрованные файлы может читать только пользователь, применивший шифрование. Чтобы файл могли читать другие люди, пользователь должен снять с него шифрование.

Каждому зашифрованному файлу соответствует уникальный ключ шифрования. Это означает, что зашифрованные файлы можно копировать, перемещать и переименовывать, как и любые другие файлы, и это в большинстве случаев не повлияет на шифрование данных. У пользователя, зашифровавшего файл, всегда есть к нему доступ, при условии что в профиле пользователя на компьютере имеется секретный ключ или пользователь обладает перемещаемыми учетными данными. Для этого пользователя процесс шифрования и дешифрования выполняется автоматически и прозрачно.

Процессом шифрования и дешифрования управляет шифрующая файловая система (EFS). Стандартные параметры EFS позволяют пользователю шифровать файлы без специального разрешения. Шифрование файлов выполняется с помощью открытого и секретного ключей, автоматически создаваемых EFS на уровне пользователя. По умолчанию в Windows XP SP1 и более поздних версиях Windows для шифрования используется алгоритм AES. Стандарт AES не поддерживается Windows 2000 или версиями Windows XP до SP1. Файлы, зашифрованные посредством AES, могут отображаться на этих компьютерах, как поврежденные, хотя на самом деле это не так. По умолчанию IIS 7 использует поставщика AES для шифрования паролей.

Сертификаты шифрования хранятся в профилях пользователей. Если пользователь хочет использовать шифрование на нескольких компьютерах, администратору нужно настроить для этого пользователя перемещаемый профиль, который обеспечивает доступ к данным профиля и сертификатам открытого ключа с других компьютеров. Без него пользователь не сможет получить доступ к своим шифрованным файлам с другого компьютера.

Совет У перемещаемого профиля есть альтернатива — копирование сертификата шифрования пользователя на компьютеры, за которыми он работает. Для этого можно использовать процесс архивации и восстановления сертификатов, о котором пойдет речь в разделе «Архивация и восстановление шифрованных данных и сертификатов» этой главы. Создайте резервную копию сертификата на исходном компьютере пользователя, а затем восстановите сертификат на каждом компьютере, где пользователь предполагает работать.

В EFS имеется встроенная система восстановления, предотвращающая потерю данных. Эта система обеспечивает восстановление зашифрованных данных, если сертификат открытого ключа пользователя потерян или удален. Это часто случается, когда пользователь покидает компанию и его учетная запись удаляется. Менеджер, конечно, мог войти в систему с учетной записью пользователя и сохранить нужные файлы в других папках. Но доступ к ним все равно можно получить только после снятия шифрования или после перемещения файлов на том FAT или FAT32 (где шифрование не поддерживается).

Для доступа к зашифрованным файлам после удаления учетной записи пользователя требуется агент восстановления (recovery agent). Агенты восстановления имеют доступ к ключу шифрования, который необходим для разблокирования данных в шифрованном файле, но не имеют доступа к секретному ключу пользователя или к любой информации о ключе.

Агенты восстановления назначаются автоматически. Необходимые сертификаты восстановления также создаются автоматически. Это обеспечивает возможность восстановления шифрованных данных.

Настройка агентов восстановления EFS происходит на двух уровнях:

- **Домен** Агент восстановления домена настраивается автоматически во время установки первого контроллера домена под управлением Windows Server 2008. По умолчанию агентом восстановления является администратор домена. При помощи групповой политики администраторы домена могут назначать дополнительных агентов восстановления, а также делегировать полномочия агентов восстановления назначенным администраторам безопасности.
- **Локальный компьютер** Если компьютер входит в рабочую группу или работает автономно, по умолчанию агентом восстановления является администратор локального компьютера. Вы можете назначить дополнительных агентов восстановления. Если даже в домене вам более подходят локальные агенты восстановления, а не агенты восстановления уровня домена, вы должны удалить политику восстановления из групповой политики домена.

Удалите политики восстановления, если хотите, чтобы они стали недоступны.

Настройка политики восстановления EFS

Политики восстановления для контроллеров домена и рабочих станций настраиваются автоматически. По умолчанию администраторы домена назначаются агентами восстановления домена, а локальные администраторы — агентами восстановления для изолированных рабочих станций.

Чтобы просматривать, назначать и удалять агентов восстановления в редакторе групповой политики, выполните следующие действия:

1. Откройте редактор групповой политики для локального компьютера, сайта, домена или подразделения, с которыми хотите работать. Подробнее об этом — в главе 5
2. Последовательно разверните узлы **Конфигурация компьютера (Computer Configuration)**, **Конфигурация Windows (Windows Settings)**, **Параметры безопасности (Security Settings)** и **Политики открытого ключа (Public Key Policies)**. Затем щелкните элемент **Шифрующая файловая система (Encrypting File System)**, чтобы открыть список агентов восстановления EFS. В правой панели будут отображены сертификаты восстановления, назначенные в данный момент. Для каждого сертификата указано, кому он назначен, кем выпущен, каков его срок действия, цель и пр.
3. Чтобы назначить дополнительного агента восстановления, щелкните правой кнопкой элемент **Шифрующая файловая система (Encrypting File System)** и выберите команду **Добавить агент восстановления данных (Add Data Recovery Agent)**. Откроется Мастер добавления агента восстановления (Add Recovery Agent Wizard), который поможет выбрать ранее созданный сертификат, который был назначен пользователю, и сделать его назначенным сертификатом восстановления. Щелкните **Далее (Next)**. На странице **Выбор агентов восстановления (Select Recovery Agents)** щелкните **Обзор каталога (Browse Directory)** и выберите пользователя в диалоговом окне **Поиск: Пользователи, контакты и группы (Find Users, Contacts, And Groups)**. Щелкните **OK**, **Далее (Next)** и **Готово (Finish)**.

Примечание Прежде чем назначить дополнительных агентов восстановления, установите в домене корневой центр сертификации. Затем сгенерируйте в оснастке **Сертификаты (Certificates)** личный сертификат на основе шаблона Агент восстановления EFS (EFS Recovery Agent). Корневой центр сертификации подтверждает запрос на предоставление сертификата, после чего сертификат можно будет использовать. Для генерирования ключа агента восстановления EFS и сертификата можно также использовать утилиту Cipher.exe.

4. Чтобы удалить агента восстановления, выберите сертификат агента на правой панели и нажмите клавишу Delete. Щелкните **Да (Yes)**, чтобы подтвердить действие. Если других назначенных агентов восстановления не существует, EFS будет отключена, и пользователь не сможет шифровать файлы.

Архивация и восстановление шифрованных данных и сертификатов

Зашифрованные данные, как любые другие данные, можно архивировать и восстанавливать. Ключевой момент состоит в том, что вы должны использовать программы архивации, которые понимают EFS, например, встроенные инструменты архивации и восстановления. Однако при работе с подобным ПО следует соблюдать особую осторожность.

Не всегда в процессе архивации (или восстановления) архивируется (или восстанавливается) сертификат, необходимый для работы с зашифрованными данными и хранящийся в профиле пользователя. Если учетная запись пользователя существует и необходимый сертификат содержится в профиле, пользователь сможет продолжить работу с шифрованными данными. Если учетная запись пользователя существует и вы восстановили профиль пользователя из ранее созданной резервной копии, чтобы восстановить удаленный сертификат, пользователь также сможет работать с шифрованными данными. Однако другого способа обеспечить работу с шифрованными данными не существует. Если восстановить профиль из резервной копии невозможно, вам придется предоставить доступ к файлам назначенным агентам восстановления, чтобы снять шифрование.

Архивация и восстановление сертификатов — важная часть любого плана восстановления в аварийных ситуациях. В следующем разделе рассмотрены способы выполнения этих задач.

Архивация сертификата шифрования

Для архивации и восстановления личных сертификатов используется оснастка **Сертификаты (Certificates)**. Личные сертификаты сохраняются в формате .pfx.

Чтобы архивировать сертификаты, выполните следующие действия:

1. Войдите на компьютер, где хранится нужный личный сертификат, как пользователь. Щелкните **Пуск (Start)**, в поле **Начать поиск (Search)** введите **mmc** и нажмите Enter. Откроется консоль управления MMC.
2. В меню **Консоль (File)** выберите команду **Добавить или удалить оснастку (Add/Remove Snap-In)**. Откроется диалоговое окно **Добавление и удаление оснастки (Add Or Remove Snap-Ins)**.
3. В списке **Доступные оснастки (Available Snap-Ins)** выберите **Сертификаты (Certificates)** и щелкните кнопку **Добавить (Add)**. Установите переключатель **Моей учетной записи пользователя (My User Account)** и щелкните **Готово (Finish)**. Оснастка **Сертификаты (Certificates)** будет отображена в списке **Выбранные оснастки (Selected Snap-Ins)**.
4. Щелкните **OK**, чтобы закрыть диалоговое окно **Добавление и удаление оснастки (Add Or Remove Snap-Ins)**.
5. Последовательно разверните узлы **Сертификаты — текущий пользователь (Certificates – Current User)** и **Личное (Personal)**, а затем выберите элемент **Сертификаты (Certificates)**. Щелкните правой кнопкой сертификат, который хотите сохранить, раскройте подменю **Все задачи (All Tasks)** и выберите команду **Экспорт (Export)**. Откроется Мастер экспорта сертификатов (Certificate Export Wizard).
6. Щелкните **Далее (Next)** и установите переключатель **Да, экспортировать закрытый ключ (Yes, Export The Private Key)**. Щелкните **Далее (Next)**.

7. Щелкните **Далее (Next)**, чтобы принять стандартные параметры, и введите пароль сертификата.
8. Укажите расположение файла сертификата. Убедитесь в безопасности этого расположения — не стоит подвергать риску безопасность системы. Файл сохраняется с расширением .pfx.
9. Щелкните **Далее (Next)** и **Готово (Finish)**. Если процесс экспорта завершился успешно, вы увидите сообщение об этом. Щелкните **OK**, чтобы закрыть окно сообщения.

Восстановление сертификатов шифрования

При наличии резервной копии сертификата вы можете восстановить сертификат на любом компьютере сети, а не только на исходном. Так что процесс архивации и восстановления — это, по сути, способ перемещения сертификатов с одного компьютера на другой.

Чтобы восстановить личный сертификат, выполните следующие действия:

1. Скопируйте pfx-файл на дискету и войдите в качестве пользователя на компьютер, где хотите использовать сертификат.

Примечание Войдите на конечный компьютер как пользователь восстанавливаемого сертификата. Если этого не сделать, пользователь не сможет работать со своими зашифрованными данными.

2. Откройте оснастку **Сертификаты (Certificate)** с установленным переключателем **Моей учетной записи пользователя (My User Account)**, как описано ранее.
3. Разверните узел **Сертификаты — текущий пользователь (Certificates – Current User)** и щелкните правой кнопкой элемент **Личное (Personal)**. Раскройте подменю **Все задачи (All Tasks)** и выберите команду **Импорт (Import)**. Откроется Мастер импорта сертификатов (Certificate Import Wizard).
4. Щелкните **Далее (Next)** и вставьте дискету в дисковод.
5. В диалоговом окне **Открыть (Open)** щелкните кнопку **Обзор (Browse)** и найдите личный сертификат на дискете. Выделите файл и щелкните **Открыть (Open)**.
6. Щелкните **Далее (Next)**. Введите пароль личного сертификата и снова щелкните **Далее (Next)**.
7. По умолчанию сертификат будет помещен в хранилище **Личное (Personal)**. Щелкните **Далее (Next)** и **Готово (Finish)**. Если процесс импорта завершился успешно, вы увидите сообщение об этом. Щелкните **OK**.

Часть IV

Администрирование сетей в Windows Server 2008

Глава 17

Управление сетями TCP/IP

Администратор организует обмен данными между компьютерами сети при помощи основных сетевых протоколов, встроенных в Microsoft Windows Server 2008. Ключевой среди них — протокол TCP/IP. Точнее, TCP/IP представляет собой набор протоколов и служб, используемых для сетевого взаимодействия. По сравнению с другими сетевыми протоколами настройка TCP/IP достаточно сложна, однако именно он является наиболее универсальным из всех имеющихся протоколов .

Примечание Помешать установке и управлению сетями TCP/IP могут параметры групповой политики. Основные политики, которые следует проверять, находятся в узлах **Конфигурация пользователя\Административные шаблоны\Сеть\Сетевые подключения (User Configuration\Administrative Templates\Network\Network Connections)** и **Конфигурация компьютера \Административные шаблоны\Система\Групповая политика (Computer Configuration\Administrative Templates\System\ Group Policy)**. Подробнее о групповой политике — в главе 5.

Работа с сетями в Windows Server 2008

Сетевые возможности Microsoft Windows Server 2008 отличаются от возможностей предыдущих версий Windows. Система Windows Server 2008 оснащена новым набором сетевых инструментальных средств, в том числе:

- **Обозреватель сети (Network Explorer)** Центральная консоль для обзора компьютеров и устройств сети.
- **Центр управления сетями и общим доступом (Network And Sharing Center)** Центральная консоль для просмотра и управления конфигурацией сети и общего доступа.
- **Карта сети (Network Map)** Графическая карта сети, изображающая подключения компьютеров и устройств.
- **Диагностика сети (Network Diagnostics)** Средство автоматической диагностики и помощи в устранении сетевых неполадок.

Прежде чем приступить к обсуждению сетевых инструментов, обратим внимание на компоненты Windows Server 2008, необходимые для работы этих инструментов:

- **Сетевое обнаружение (Network Discovery)** Компонент Windows Server 2008, управляющий способностью видеть другие компьютеры и устройства.
- **Служба сетевого расположения (Network Awareness)** Компонент Windows Server 2008, уведомляющий об изменениях в подключениях узлов и конфигурации сети.

Ближе к реальности ОС Windows Vista SP1 и более поздние версии, а также Windows Server 2008, поддерживают расширения службы сетевого расположения. Эти расширения позволяют компьютеру, подключенному к одной или нескольким сетям посредством двух или нескольких интерфейсов (как проводных, так и беспроводных), выбирать маршрут, обеспечивающий наилучшую производительность для конкретной операции передачи данных. В рамках определения лучшего маршрута Windows выбирает для передачи наиболее эффективный интерфейс (проводной или беспроводной).

Параметры сетевого обнаружения компьютера, на котором вы работаете, определяют какие компьютеры и устройства вы сможете просматривать в сетевых инструментах Windows Server 2008. Параметры обнаружения работают в сочетании с брандмауэром Windows и способны блокировать или разрешать следующие действия:

- обнаружение сетевых компьютеров и устройств;
- обнаружение вашего компьютера другими системами.

Параметры сетевого обнаружения должны обеспечить надлежащий уровень безопасности для каждой из категорий сетей, к которым подключен компьютер. Существует три категории сетей:

- **Доменная сеть** Обозначает сеть, в которой компьютеры подключены к домену. По умолчанию в доменной сети обнаружение разрешено. Это сокращает ограничения и позволяет компьютерам обнаруживать другие компьютеры и устройства сети.
- **Частная сеть** Обозначает сеть, компьютеры которой являются членами рабочей группы и лишены прямого выхода в Интернет. По умолчанию в частной сети обнаружение разрешено. Это сокращает ограничения и позволяет компьютерам обнаруживать другие компьютеры и устройства сети.
- **Публичная сеть** Обозначает сеть в общественном месте, например, в кафе или аэропорту. По умолчанию в публичной сети обнаружение блокировано. Это повышает безопасность, запрещая компьютерам публичной сети обнаруживать другие компьютеры и устройства.

Компьютер отдельно хранит параметры для сетей каждой категории. Поэтому для каждой категории могут использоваться различные блокирующие и разрешающие параметры. При первом подключении к сети на экране появляется диалоговое окно, позволяющее указать категорию сети — частная или публичная. Если вы указали, что сеть является частной, и компьютер обнаружит подключение к домену, членом которого он является, сети будет назначена категория доменной.

Опираясь на категорию сети, Windows Server 2008 автоматически настраивает параметры обнаружения. Если режим обнаружения включен, то:

- компьютер может обнаруживать другие компьютеры и устройства в сети;
- другие компьютеры и устройства в сети могут обнаруживать этот компьютер.

Если режим обнаружения выключен, то:

- компьютер не способен обнаруживать другие компьютеры и устройства в сети;
- другие компьютеры и устройства в сети не могут обнаруживать этот компьютер.

В консоли **Сеть (Network)**, показанной на рис. 17-1, отображается список обнаруженных в сети компьютеров и устройств. Чтобы открыть Обозреватель сети (Network Explorer), щелкните кнопку **Пуск (Start)** и выберите команду **Сеть (Network)**. Список отображенных в Обозревателе сети (Network Explorer) компьютеров и устройств зависит от параметров сетевого обнаружения компьютера. Если обнаружение заблокировано, вы увидите соответствующее предупреждение. Щелкните его и выберите команду **Включить сетевое обнаружение (Turn On Network Discovery)**, чтобы включить сетевое обнаружение. При этом будут открыты соответствующие порты брандмауэра Windows. Если никаких дополнительных изменений в параметры сетевого обнаружения не вносилось, компьютер будет находиться в состоянии «только обнаружение». Вам придется вручную настроить общий доступ к принтерам, файлам и накопителям, как описано в главе 15.

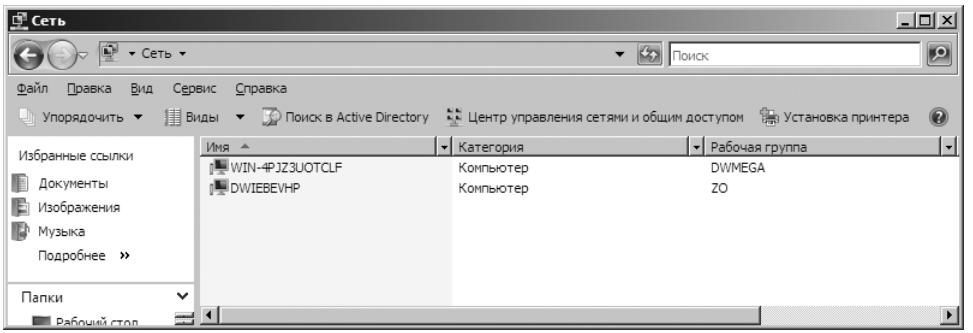


Рис. 17-1. Просмотр сетевых ресурсов в Обозревателе сети (Network Explorer)

Консоль **Центр управления сетями и общим доступом (Network And Sharing Center)**, показанная на рис. 17-2, показывает текущее состояние сети и текущую сетевую конфигурацию. Чтобы открыть консоль **Центр управления сетями и общим доступом (Network And Sharing Center)**, последовательно щелкните **Пуск (Start)** и **Сеть (Network)**. Затем щелкните кнопку **Центр управления сетями и общим доступом (Network And Sharing Center)** на панели инструментов Обозревателя сети (Network Explorer).

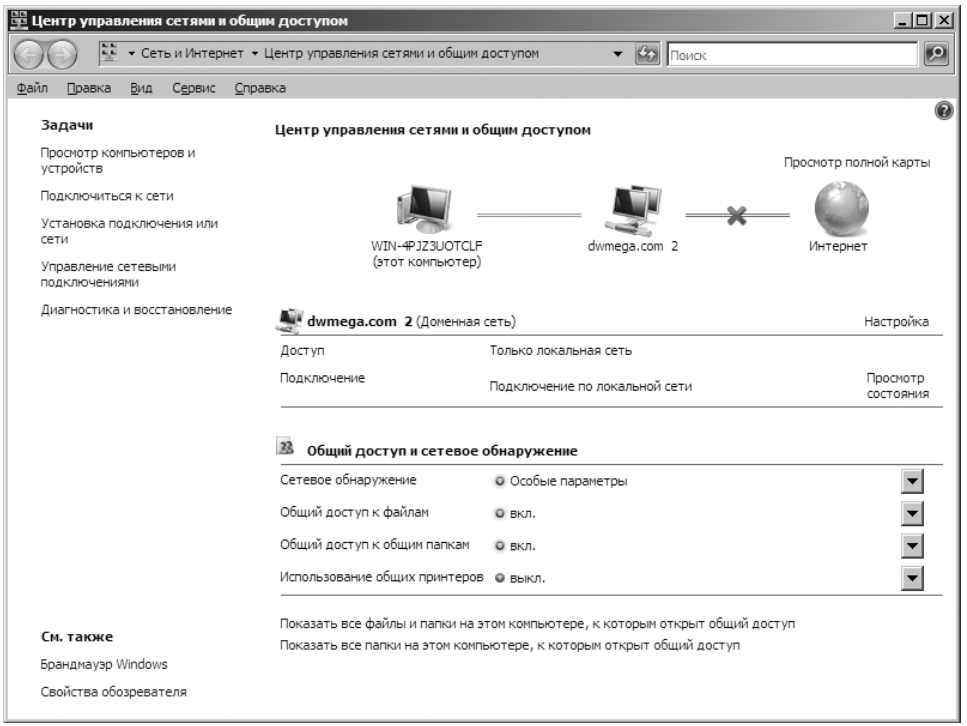


Рис. 17-2. Просмотр и управление параметрами сети в Центре управления сетями и общим доступом (Network And Sharing Center)

Окно **Центр управления сетями и общим доступом (Network And Sharing Center)** разделено на три главных области:

- **Краткая карта сети** Графическое изображение конфигурации сети и сетевых подключений. Нормальное состояние подключение отображается в виде линии, соединяющей различные сегменты сети. Любые проблемы сети отмечаются предупреждающими значками. Желтый значок предупреждения указывает на возможную неполадку конфигурации. Красный крестик говорит об отсутствии подключения к данному сегменту сети. Щелкнув ссылку **Просмотр полной карты (View Full Map)**, вы откроете окно **Карта сети (Network Map)** с расширенным отображением вида сети.
- **Подробные сведения о сети** Имя текущей сети и ее параметры. В скобках за именем сети указана ее категория: доменная, частная или публичная. В поле **Доступ (Access)** указан способ подключения компьютера к текущей сети: **Только локальная сеть (Local Only)**, **Локальная сеть и Интернет (Local And Internet)** или **Только Интернет (Internet Only)**. В поле **Подключение (Connection)** отображается имя подключения, используемого для работы в текущей сети. Щелкнув ссылку **Настройка (Customize)**, вы сможете изменить имя сети, категорию (только для частных и публичных сетей) и значок сети. Щелкнув ссылку **Просмотр состояния (View Status)**, вы откроете диалоговое окно **Состояние — Подключение по локальной сети (Local Area Connection Status)**.

- **Общий доступ и сетевое обнаружение** Позволяет настраивать параметры общего доступа и обнаружения компьютера и отображает текущее состояние каждого параметры. Чтобы изменить значение параметра, щелкните соответствующую кнопку со стрелкой вниз, установите нужный параметр, а затем щелкните кнопку **Применить (Apply)**. Например, чтобы включить или выключить сетевое обнаружение, разверните раздел **Сетевое обнаружение (Network Discovery)**, установите переключатель **Включить сетевое обнаружение (Turn On Network Discovery)** или **Отключить сетевое обнаружение (Turn Off Network Discovery)**. Затем щелкните **Применить (Apply)**.

В окне **Центр управления сетями и общим доступом (Network And Sharing Center)** можно провести диагностику предупреждений. Щелкните значок предупреждения, чтобы открыть окно **Диагностика сетей Windows (Windows Network Diagnostics)**. Будет произведена попытка определить неисправность сети и предложить возможное решение.

Примечание Центр управления сетями и общим доступом (Network And Sharing Center) позволяет в любой момент запустить средство диагностики вручную. Щелкните ссылку **Диагностика и восстановление (Diagnose And Repair)** в области задач.

Расширение сетевых возможностей в Windows Vista и Windows Server 2008

В редакторе групповой политики Windows Vista и Windows Server 2008 политики управления проводными и беспроводными (IEEE 802.11) сетями находятся в узле **Конфигурация компьютера\Конфигурация Windows\ Параметры безопасности (Computer Configuration\Windows Settings\ Security Settings)**. Щелкнув правой кнопкой узел **Политики проводной сети (IEEE 802.3) (Wired Network (IEEE 802.3))**, вы сможете создать политику для компьютеров под управлением Windows Vista и более поздних версий, которая позволяет использовать проверку подлинности по стандарту IEEE 802.1X для проводных сетей. Щелкнув правой кнопкой узел **Политики беспроводной сети (IEEE 802.11) (Wired Network (IEEE 802.11))**, вы сможете создать отдельные политики для компьютеров Windows XP и компьютеров Windows Vista или более поздних версий, включающих автоматическую настройку WLAN, определить используемые сети и установить сетевые полномочия.

ОС Windows Vista SP1 и более поздние версии, а также Windows Server 2008, поддерживают несколько усовершенствований для проводных и беспроводных сетей. Эти изменения позволяют пользователям изменять пароли при подключении к проводным и беспроводным сетям (без использования функции изменения пароля Winlogon), исправлять неправильно введенный пароль, а также сбрасывать пароль с истекшим сроком действия — все это в рамках входа в систему.

ОС Windows Vista SP1 и более поздние версии, а также Windows Server 2008, поддерживают много других расширений сетевой безопасности, в том числе:

- протокол SSTP (Secure Socket Tunneling Protocol);
- безопасный удаленный доступ SRA (Secure Remote Access);
- интерфейс CAPI2 (CryptoAPI Version 2);
- расширения протокола OCSP (Online Certificate Status Protocol);
- резервирование порта для протокола Teredo;
- подписывание файлов по протоколу RDP (Remote Desktop Protocol).

Протокол SSTP позволяет осуществлять передачу данных на канальном уровне по протоколу HTTP через подключение HTTPS. Протокол SRA обеспечивает защищенный доступ к удаленным сетям по HTTPS. Вместе две этих технологии позволяют пользователям получать защищенный доступ к частной сети по Интернету. Протоколы SSTP и SRA представляют собой модификации протоколов PPTP и L2TP/IPSec. Для защищенного веб-трафика они используют стандартные порты TCP/IP, что позволяет им проходить большинство брандмауэров, а также NAT и прокси.

В протоколе SSTP используется HTTP через SSL (TCP-порт 443), часто применяемый для защищенных подключений к коммерческим веб-сайтам. Каждый раз, когда пользователи подключаются к веб-адресу, который начинается на *https://*, они используют протокол HTTPS через SSL. Использование HTTP через SSL устраняет многие проблемы VPN-подключений. Протокол SSTP поддерживает как IPv4, так и IPv6, поэтому пользователи могут устанавливать безопасные туннели при помощи любой из IP-технологий. По сути, результатом является технология VPN, которая работает всегда и везде. Это означает значительное сокращение числа обращений в службу поддержки.

Протокол CAPI2 расширяет поддержку сертификатов PKI и X.509 и обеспечивает дополнительную функциональность для проверки пути сертификата, хранилищ сертификатов и проверки подписи. Один из этапов проверки пути сертификата — проверка отзыва. В нее входит проверка состояния сертификата на предмет его отзыва издателем. Здесь в дело вступает протокол OCSP.

Протокол OCSP используется для проверки состояния отзыва сертификатов. Кроме того, CAPI2 поддерживает независимые цепочки подписей OCSP и позволяет указать дополнительные источники загрузки OCSP для каждого издателя. Независимые цепочки подписей OCSP изменяют первоначальную реализацию OCSP. Она обретает возможность работать с откликами OCSP, подписанными доверенными источниками OCSP, которые не связаны с издателем проверяемого сертификата. Дополнительные источники загрузки OCSP позволяют указывать источники загрузки OCSP для выпуска сертификатов ЦС в виде URL, которые добавляются к сертификатам ЦС в виде свойств.

Для поддержки совместного существования протоколов IPv4-IPv6 в Windows Vista SP1 и более поздние версии, а также в Windows Server 2008, включены расширения, позволяющие приложениям использовать IPv6 в сети IPv4, например, резервирование порта для Teredo. Протокол Teredo — это технология туннелирования на базе UDP, способная проходить NAT. Она позволяет установить связь между симметричными NAT с резервированием портов и прочими типами NAT. Механизм NAT с резервированием портов использует внешний порт с тем же номером, что и внутренний.

В Windows Vista SP1 и более поздних версиях, а также в Windows Server 2008, используется клиент RDP 6.1, который позволяет подписывать файлы RDP для предотвращения открытия или запуска пользователями потенциально опасных файлов из неизвестных источников. Администраторы могут подписывать файлы RDP при помощи специального инструментария Майкрософт. В групповой политике или реестре могут быть настроены три связанных параметра: разделенный запятыми список хешей сертификатов, которым доверяют администраторы (список доверенных издателей), параметр, позволяющий пользователям принимать недоверенных издателей (включен по умолчанию), а также параметр, позволяющий принимать неподписанные файлы (включен по умолчанию).

Установка сетей TCP/IP

Чтобы установить сеть на компьютере, вы должны установить сетевой протокол TCP/IP и сетевой адаптер. В системе Windows Server 2008 TCP/IP используется в качестве стандартного протокола глобальных сетей. Обычно установка сети происходит одновременно с установкой Windows Server 2008. Вы также можете установить TCP/IP в свойствах подключения по локальной сети.

Если вы устанавливаете TCP/IP после установки Windows Server 2008, войдите на компьютер с административной учетной записью и выполните следующие действия:

1. Щелкните **Пуск (Start)** и **Сеть (Network)**. В консоли **Сеть (Network)** щелкните кнопку **Центр управления сетями и общим доступом (Network And Sharing Center)** на панели инструментов.
2. В окне **Центр управления сетями и общим доступом (Network And Sharing Center)** щелкните ссылку **Управление сетевыми подключениями (Manage Network Connections)**.
3. В окне **Сетевые подключения (Network Connections)** щелкните правой кнопкой нужное подключение и выберите команду **Свойства (Properties)**. Откроется диалоговое окно **Подключение по локальной сети — свойства (Local Area Connection Properties)**, показанное на рис. 17-3.

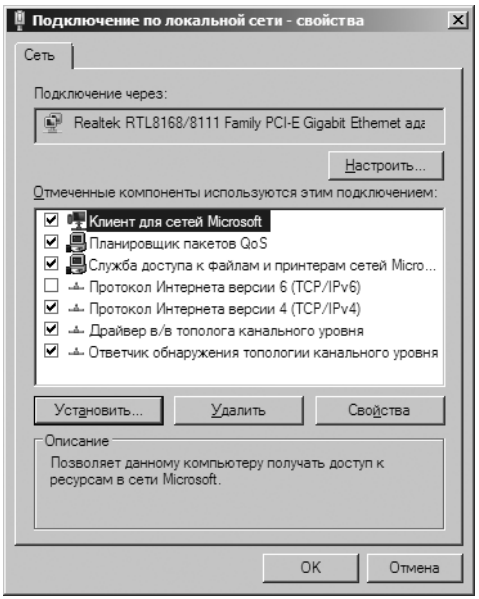


Рис. 17-3. Настройка параметров TCP/IP в диалоговом окне Подключение по локальной сети — свойства (Local Area Connection Properties)

4. Изначально протоколы IPv6 и IPv4 отсутствуют в списке установленных компонентов. Их нужно установить. Щелкните кнопку **Установить (Install)**. Выделите элемент **Протокол (Protocol)** и щелкните **Добавить (Add)**. В диалоговом окне **Выбор сетевого протокола (Select Network Protocol)** выберите устанавливаемый протокол и щелкните **OK**. Если вы устанавливаете оба протокола (IPv6 и IPv4), повторите процедуру для каждого из них.
5. Убедитесь, что в диалоговом окне **Подключение по локальной сети — свойства (Local Area Connection Properties)** выбран хотя бы один из протоколов IPv6 и IPv4. Затем щелкните **OK**.
6. При необходимости выполните инструкции из следующего раздела для настройки подключения по локальной сети.

Настройка сетей TCP/IP

Подключение по локальной сети создается автоматически, если в компьютере есть сетевой адаптер и он подключен к сети. Если на компьютере установлено несколько сетевых адаптеров, у каждого из них будет собственное подключение к локальной сети. Если доступных сетевых подключений не существует, вам следует подключить компьютер к сети или создать подключение другого типа.

Для работы по протоколу TCP/IP компьютеру необходим IP-адрес. В Windows Server 2008 существует несколько способов настройки IP-адреса:

- **Вручную** IP-адреса, назначаемые вручную, называются статическими IP-адресами. Такие фиксированные адреса не изменяются, пока вы не измените их. Как правило, статические IP-адреса назначаются серверам Windows. При этом следует настроить также ряд дополнительных параметров.
- **Динамически** Динамические IP-адреса назначаются во время запуска компьютера DHCP-сервером (если он установлен в сети). Время от времени такие адреса могут изменяться. По умолчанию все IP-адреса компьютера считаются динамическими.
- **Альтернативный адрес (только для IPv4)** Когда компьютер настроен на использование DHCPv4, но в сети нет доступного DHCPv4-сервера, Windows Server 2008 автоматически назначает компьютеру частный альтернативный IP-адрес. По умолчанию альтернативный адрес IPv4 заключен в диапазоне от 169.254.0.1 до 169.254.255.254 с маской подсети 255.255.0.0. Вы также можете назначить пользовательский альтернативный IPv4-адрес, что особенно полезно, если вы работаете на ноутбуке.

Настройка статического IP-адреса

На компьютере со статическим IP-адресом помимо собственно IP-адреса вы должны указать маску подсети, а также, при необходимости, шлюз по умолчанию. IP-адрес — это числовой идентификатор компьютера. Схемы предоставления IP-адресов различаются в зависимости от настройки сети, но в большинстве случаев они назначаются на основе конкретных сетевых сегментов.

Адреса IPv6 сильно отличаются от адресов IPv4. В IPv6-адресах первые 64 бита представляют идентификатор сети, а оставшиеся 64 бита — сетевой интерфейс. В IPv4-адресах переменное число первых битов обозначает идентификатор сети, а остальные биты — идентификатор хоста. Допустим, вы используете протокол IPv4 и компьютер в сегменте сети 10.0.10.0 с маской подсети 255.255.255.0. Первые три группы битов обозначают сетевой идентификатор, а доступные для хостов адреса находятся в диапазоне от 10.0.10.1 до 10.0.10.254. Адрес 10.0.10.255 зарезервирован для широковещательной передачи.

Если вы находитесь в частной сети, не имеющей прямого выхода в Интернет, следует использовать частные IPv4-адреса, приведенные в табл. 17-1.

Табл. 17-1. Частные сетевые IPv4-адреса

Идентификатор частной сети	Маска подсети	Диапазон сетевых адресов
10.0.0.0	255.0.0.0	10.0.0.0–10.255.255.255
172.16.0.0	255.240.0.0	172.16.0.0–172.31.255.255
192.168.0.0	255.255.0.0	192.168.0.0–192.168.255.255

Все остальные сетевые IPv4-адреса являются публичными и должны арендоваться или приобретаться. Если сеть подключена напрямую

к Интернету, получите диапазон IPv4-адресов от поставщика Интернета и назначайте их вашим компьютерам.

Проверка адреса с помощью команды PING

Прежде чем назначить статический IP-адрес, убедитесь, что он не используется и не зарезервирован для использования с DHCP. Проверить использование адреса можно при помощи команды PING. Откройте командную строку и введите ping с IP-адресом, который хотите проверить. Например, для проверки IPv4-адреса 10.0.10.12 нужно ввести команду:

```
ping 10.0.10.12
```

Команда для проверки IPv6-адреса FEC0::02BC:FF:BECB:FE4F:961D выглядит так:

```
ping FEC0::02BC:FF:BECB:FE4F:961D
```

Если команда PING даст положительный ответ, данный IP-адрес уже используется, и вам нужно проверить другой адрес. Если время запроса всех четырех попыток команды PING истекло, а отклик от компьютера так и не получен, IP-адрес в настоящий момент не активен и, возможно, не используется. Однако запросы PING могут блокироваться брандмауэром. Информацию об использовании адреса также может предоставить сетевой администратор компании.

Настройка статических адресов IPv4 или IPv6

Каждый установленный сетевой адаптер может быть подключен к одной локальной сети. Подключения создаются автоматически. Для настройки IP-адреса конкретного подключения выполните следующие действия:

1. Щелкните **Пуск (Start)** и **Сеть (Network)**. В консоли **Сеть (Network)** щелкните кнопку **Центр управления сетями и общим доступом (Network And Sharing Center)** на панели инструментов.
2. В окне **Центр управления сетями и общим доступом (Network And Sharing Center)** щелкните ссылку **Управление сетевыми подключениями (Manage Network Connections)**. В окне **Сетевые подключения (Network Connections)** щелкните правой кнопкой нужное подключение и выберите команду **Свойства (Properties)**.
3. Дважды щелкните протокол, соответствующий типу настраиваемого IP-адреса — **TCP/IPv6** или **TCP/IPv4**.
4. Настройте адрес IPv6:
   - Установите переключатель **Использовать следующий IPv6-адрес (Use The Following IPv6 Address)** и введите IPv6-адрес в поле **IPv6-адрес (IPv6 Address)**. Этот IPv6-адрес должен быть уникален в пределах сети.
   - Нажмите на клавишу Tab. Поле **Длина префикса сети (Subnet Prefix Length)** обеспечивает нормальный доступ компьютера к сети. Система вставляет в поле **Длина префикса сети (Subnet Prefix Length)** стандарт-

ное значение префикса. Если в сети не используются подсети переменной длины, стандартное значение должно сработать. В противном случае вам придется привести значение в соответствии с вашей сетью.

5. Настройте адрес IPv4:
   - Установите переключатель **Использовать следующий IP-адрес (Use The Following IP Address)** и введите IPv4-адрес в поле **IP-адрес (IP Address)**. Назначаемый компьютеру IPv4-адрес должен быть уникален в пределах сети.
   - Нажмите на клавишу Tab. Поле **Маска подсети (Subnet Mask)** обеспечивает нормальный доступ компьютера к сети. Система сама вставляет в поле значение маски по умолчанию, которое подходит в большинстве ситуаций. При необходимости задайте другое значение, соответствующее вашей сети.
6. Если компьютеру необходим выход в другие TCP/IP-сети, в Интернет или другие подсети, укажите IP-адрес шлюза по умолчанию в поле **Основной шлюз (Default Gateway)**.
7. Для разрешения доменных имен требуется DNS. В соответствующие поля введите IP-адреса основного и альтернативного DNS-серверов.
8. Завершив настройку, щелкните **OK** и **Закрыть (Close)**. Повторите процесс для других сетевых адаптеров и IP-протоколов, которые требуется настроить.
9. При необходимости настройте WINS для IPv4-адресов.

Настройка динамических и альтернативных IP-адресов

Хотя на рабочих станциях вполне могут использоваться статические IP-адреса, большинство рабочих станций работает с динамическими или альтернативными IP-адресами или с их комбинациями. Для настройки динамического и альтернативного IP-адреса выполните следующие действия:

1. Щелкните **Пуск (Start)** и **Сеть (Network)**. В консоли **Сеть (Network)** щелкните кнопку **Центр управления сетями и общим доступом (Network And Sharing Center)** на панели инструментов.
2. В окне **Центр управления сетями и общим доступом (Network And Sharing Center)** щелкните ссылку **Управление сетевыми подключениями (Manage Network Connections)**. В окне **Сетевые подключения (Network Connections)** для каждого установленного сетевого адаптера отображается одно подключение по локальной сети. Подключения создаются автоматически. Если для установленного адаптера сетевое подключение не отображается, проверьте драйвер адаптера. Возможно, он установлен неправильно. Щелкните правой кнопкой нужное подключение и выберите **Свойства (Properties)**.
3. Дважды щелкните протокол, соответствующий типу настраиваемого IP-адреса — **TCP/IPv6** или **TCP/IPv4**.

4. Установите переключатель **Получить IPv6-адрес автоматически (Obtain An IPv6 Address Automatically)** или **Получить IP-адрес автоматически (Obtain An IP Address Automatically)** — в соответствии с типом настраиваемого IP-адреса. При необходимости установите также переключатель **Получить адрес DNS-сервера автоматически (Obtain DNS Server Address Automatically)** или **Использовать следующие адреса DNS-серверов (Use The Following DNS Server Addresses)**, а затем введите адреса основного и альтернативного DNS-серверов.
5. При использовании динамического IPv4-адреса на настольном компьютере следует настроить также автоматический альтернативный адрес. На вкладке **Альтернативная конфигурация (Alternate Configuration)** установите переключатель **Автоматический частный IP-адрес (Automatic Private IP Address)**. Щелкните **OK**, затем **Закрыть (Close)** и пропустите оставшиеся шаги.
6. При использовании динамического IPv4-адреса на портативном компьютере, как правило, альтернативный адрес настраивается вручную. Для использования этой конфигурации на вкладке **Альтернативная конфигурация (Alternate Configuration)** установите переключатель **Настраиваемый пользователем (User Configured)** и введите в поле **IP-адрес (IP Address)** нужный IP-адрес. Он должен входить в диапазон, указанный в табл. 17-1, и быть уникальным.
7. Введите маску подсети, основной шлюз и параметры WINS. Завершив настройку, щелкните **OK** и **Закрыть (Close)**.

Настройка нескольких шлюзов

Для обеспечения отказоустойчивости в случае выхода из строя маршрутизатора вы можете настроить компьютер под управлением Windows Server 2008 на использование нескольких шлюзов по умолчанию. При этом для выбора используемого шлюза Windows Server 2008 использует метрику шлюза. Метрика шлюза характеризует затраты на маршрутизацию для данного шлюза. Первым используется шлюз с наименьшей метрикой. Если компьютер не может установить связь с этим шлюзом, Windows Server 2008 пытается использовать шлюз, следующий по возрастанию метрики.

Выбор способа настройки нескольких шлюзов зависит от конфигурации сети. Если компьютеры в вашей организации настраиваются при помощи DHCP, вероятно, лучше задавать дополнительные шлюзы через параметры на DHCP-сервере. Если на компьютерах применяются статические IP-адреса или если вы хотите задавать IP-адреса шлюзов самостоятельно, выполните следующие действия:

1. Щелкните **Пуск (Start)** и **Сеть (Network)**. На панели инструментов консоли **Сеть (Network)** щелкните кнопку **Центр управления сетями и общим доступом (Network And Sharing Center)**.

2. В окне **Центр управления сетями и общим доступом (Network And Sharing Center)** щелкните ссылку **Управление сетевыми подключениями (Manage Network Connections)**. В окне **Сетевые подключения (Network Connections)** щелкните правой кнопкой нужное подключение и выберите **Свойства (Properties)**.
3. Дважды щелкните протокол, соответствующий типу настраиваемого IP-адреса — **TCP/IPv6** или **TCP/IPv4**.
4. Щелкните **Дополнительно (Advanced)**, чтобы открыть диалоговое окно **Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)**, показанное на рис. 17-4.

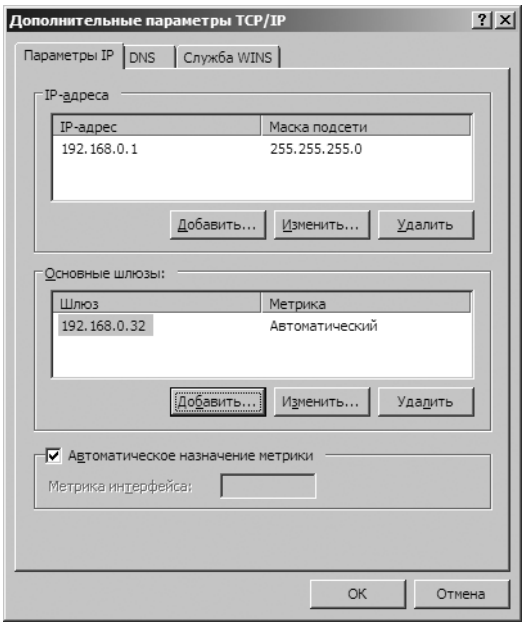


Рис. 17-4. Настройка нескольких шлюзов в диалоговом окне Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)

5. В разделе **Основные шлюзы (Default Gateway)** показаны шлюзы, которые были настроены вручную (если таковые имеются). При необходимости введите адреса дополнительных шлюзов. Щелкните кнопку **Добавить (Add)** и введите адрес шлюза в поле **Шлюз (Gateway)**.
6. По умолчанию Windows Server 2008 назначает метрику шлюзу автоматически, но вы вольны задать ее вручную. Сбросьте флажок **Автоматическое назначение метрики (Automatic Metric)** и введите метрику в соответствующее поле.
7. Повторите шаги 5–6 для каждого добавляемого шлюза.
8. Щелкните **OK** и **Закрыть (Close)**.

Управление сетевыми подключениями

Подключения по локальной сети позволяют компьютерам получать доступ к ресурсам в сети и Интернете. Для каждого установленного на компьютере сетевого адаптера автоматически устанавливается одно подключение по локальной сети. В этом разделе рассмотрены способы управления подключениями.

Проверка состояния, скорости и активности сетевого подключения

Чтобы проверить состояние подключения по локальной сети, выполните следующие действия:

1. Щелкните **Пуск (Start)** и **Сеть (Network)**. На панели инструментов консоли **Сеть (Network)** щелкните кнопку **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. В окне **Центр управления сетями и общим доступом (Network And Sharing Center)** щелкните ссылку **Управление сетевыми подключениями (Manage Network Connections)**. В окне **Сетевые подключения (Network Connections)** щелкните правой кнопкой нужное подключение и выберите **Состояние (Status)**. Откроется диалоговое окно **Состояние — Подключение по локальной сети (Local Area Connection Status)**.
3. Если подключение отключено или отсоединен кабель, диалоговое окно не откроется. Для устранения неисправности включите подключение или присоедините сетевой кабель. Затем еще раз попытайтесь открыть диалоговое окно **Состояние (Status)**.

Включение и выключение сетевого подключения

Создание подключений и установка связи по локальной сети происходит автоматически. Чтобы отключить подключение, выполните следующие действия:

1. Щелкните **Пуск (Start)** и **Сеть (Network)**. На панели инструментов консоли **Сеть (Network)** щелкните кнопку **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. В окне **Центр управления сетями и общим доступом (Network And Sharing Center)** щелкните ссылку **Управление сетевыми подключениями (Manage Network Connections)**. В окне **Сетевые подключения (Network Connections)** щелкните правой кнопкой нужное подключение и выберите **Отключить (Disable)**.
3. Чтобы снова включить подключение, щелкните его правой кнопкой в окне **Сетевые подключения (Network Connections)** и выберите команду **Включить (Enable)**.

Если вы хотите отключиться от сети и установить другое подключение (как правило, удаленного доступа), выполните следующие действия:

1. Щелкните **Пуск (Start)** и **Сеть (Network)**. На панели инструментов консоли **Сеть (Network)** щелкните кнопку **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. В окне **Центр управления сетями и общим доступом (Network And Sharing Center)** щелкните ссылку **Управление сетевыми подключениями (Manage Network Connections)**. В окне **Сетевые подключения (Network Connections)** щелкните правой кнопкой нужное подключение и выберите **Отключить (Disconnect)**.
3. Чтобы позже активировать подключение, щелкните его правой кнопкой в окне **Сетевые подключения (Network Connections)** и выберите команду **Подключить (Connect)**.

Переименование сетевого подключения

Изначально Windows Server 2008 назначает подключениям по локальной сети стандартные имена. Чтобы переименовать подключение, откройте окно **Сетевые подключения (Network Connections)**, щелкните правой кнопкой нужное подключение, выберите команду **Переименовать (Rename)** и введите новое имя подключения. Если на компьютере имеется несколько подключений по локальной сети, их понятные имена помогут вам и другим пользователям понять предназначение того или иного подключения.

Глава 18

Администрирование сетевых принтеров и служб печати

Чтобы обеспечить сетевой доступ пользователей к устройству печати, подключенному к компьютеру Microsoft Windows Server 2008, администратор должен сделать две важные вещи: установить сервер печати и открыть с его помощью общий доступ к сетевому принтеру.

В этой главе приводятся основные сведения по установке устройств печати и организации общего доступа к ним. Здесь вы также найдете советы по администрированию и поиску неисправностей принтеров.

Управление ролью Службы печати (Print Services)

Сервер печати позволяет централизованно управлять общим доступом к сетевым принтерам. Если в вашем домене многие пользователи нуждаются в доступе к одним и тем же принтерам, вам следует настроить серверы печати. В прежних версиях Windows Server базовые службы печати устанавливались на всех серверах. В Windows Server 2008 вам придется специально настроить сервер для работы в качестве сервера печати.

Работа с устройствами печати

В сети применяются устройства печати двух типов:

- **Локальное** Устройство печати, физически подключенное к компьютеру пользователя и доступное только пользователю, выполнившему вход на компьютер.
- **Сетевое** Устройство печати, настроенное для удаленного использования по сети. Сетевое устройство печати может подключаться к серверу печати или напрямую к сети посредством собственного сетевого адаптера.

Примечание Ключевое отличие локального принтера от сетевого заключается в том, что к локальному принтеру нет общего доступа. Локальный принтер можно легко превратить в сетевой. Подробнее — в разделе «Открытие и закрытие общего доступа к принтерам» этой главы.

Сетевые принтеры устанавливаются на серверах печати или в качестве отдельных устройств, подключенных к сети. Сервер печати представляет собой рабочую станцию или сервер, обеспечивающие общий доступ к одному или нескольким принтерам. Физически эти принтеры могут быть подключены как к компьютеру, так и к сети. Недостаток рабочей станции по сравнению с сервером заключается в количестве допустимых подключений. Windows Server 2008 позволяет вовсе забыть об ограничениях на подключения.

Основная работа сервера печати состоит в организации общего доступа к устройству печати и обработке вывода на печать. К основным преимуществам сервера печати относятся наличие централизованно управляемой очереди печати и отсутствие необходимости в установке драйверов принтеров на клиентских системах.

Тем не менее, работать с сервером печати совсем не обязательно. Вы можете подключать пользователей напрямую к сетевому принтеру. При этом работа с ним будет очень напоминать работу с локальным принтером, подключенным к компьютеру напрямую. Ключевое отличие состоит в том, что к принтеру могут подключаться несколько пользователей, у каждого из которых имеется своя очередь печати. Управление каждой индивидуальной очередью осуществляется отдельно, что усложняет администрирование и затрудняет поиск неисправностей.

Основы печати

Понимание принципов работы печати пригодится вам в процессе поиска и устранения неисправностей принтера. В печати документа задействовано много процессов, драйверов и устройств. В частности, в печати на принтере, подключенном к серверу печати, участвуют следующие компоненты:

- **Драйвер принтера** Когда вы печатаете документ из приложения, компьютер загружает драйвер принтера. Если устройство печати подключено к компьютеру физически, драйвер принтера загружается с локального диска. Если устройство печати расположено на удаленном компьютере, драйвер принтера может быть загружен с удаленного компьютера. Доступность драйверов принтера на удаленном компьютере изменяется в зависимости от ОС и архитектуры процессора. Если компьютеру не удается получить новейший драйвер принтера, возможно, администратор не установил драйвер для ОС компьютера. Подробнее — в разделе «Управление драйверами принтеров» этой главы.
- **Локальная очередь и процессор печати** С помощью драйвера принтера приложение, из которого вы печатаете, переводит документ в формат, понятный выбранному устройству печати. Затем компьютер передает документ в локальную очередь печати, а она, в свою очередь, передает документ процессору печати, который создает исходные данные, необходимые для печати на принтере.

- **Маршрутизатор печати и очередь печати на сервере** Подготовленные к печати данные передаются обратно в локальную очередь или в очередь на сервере печати, если вы печатаете на удаленном принтере. В Windows Server 2008 на маршрутизатор печати (Winspool.drv) возлагаются задачи поиска удаленного принтера, маршрутизации заданий на печать и, при необходимости, загрузки драйвера принтера на локальную систему. Сбой при выполнении любой из перечисленных задач, как правило, происходит по вине маршрутизатора. О возможных способах устранения этой проблемы читайте в разделах «Устранение неисправностей очереди» и «Установка разрешений на доступ к принтеру» этой главы. Если описанные там процедуры не сработают, возможно, вам придется заменить или восстановить Winspool.drv.

  Главный довод в пользу загрузки драйверов принтера на клиентские ПК состоит в создании единого расположения для установки обновлений драйверов. Вместо того чтобы устанавливать новый драйвер на все клиентские системы, вы устанавливаете драйвер на сервер печати, а клиенты при необходимости автоматически загружают его. Подробнее о работе с драйверами принтера — в разделе «Управление драйверами принтеров» этой главы.
- **Принтер (очередь печати)** Из очереди документ поступает в стек печати, который в некоторых ОС также называется очередью. Помещенный в очередь документ называется *заданием* (job). Время, проводимое документом в очереди принтера, зависит от приоритета документа и его положения в очереди. Подробнее — в разделе «Расписание выполнения и приоритет заданий печати» этой главы.
- **Монитор печати** Когда документ переходит на первое место в очереди принтера, монитор печати отсылает документ на устройство, где и происходит печать. Если принтер настроен на уведомление пользователей о печати документа, вы увидите соответствующее сообщение.

  Конкретный монитор печати, используемый в Windows Server 2008, зависит от конфигурации и типа устройства. Часто собственные мониторы предоставляют производители устройств печати. Без DLL-файла монитора осуществить печать на устройстве невозможно. Если DLL-файл поврежден или отсутствует, его придется переустановить.
- **Устройство печати** Само физическое устройство, печатающее документы. К основным проблемам и ошибкам устройства печати относятся: отсутствие бумаги, недостаточное количество или отсутствие тонера (чернил), замятие бумаги.

  На возможность установки и управления принтерами может повлиять групповая политика. Если вы подозреваете, что с ней связаны определенные проблемы, просмотрите политики в следующих узлах:
  - Конфигурация компьютера\Административные шаблоны\Принтеры (Computer Configuration\Administrative Templates\Printers).

- Конфигурация пользователя\Административные шаблоны\Панель управления\Принтеры (User Configuration\Administrative Templates\Control Panel\Printers).
- Конфигурация пользователя\Административные шаблоны\Меню «Пуск» и панель задач (User Configuration\Administrative Templates\Start Menu And Taskbar).

Настройка серверов печати

Чтобы настроить сервер как сервер печати, добавьте роль Службы печати (Print Services) и настройте одну или несколько из перечисленных ниже служб роли:

- **Сервер печати (Print Server)** Настраивает сервер как сервер печати и устанавливает консоль **Управление печатью (Print Management)** для управления несколькими принтерами и серверами печати, для переноса принтеров на другие серверы печати и обратно, а также для управления заданиями печати.
- **Служба LPD (LPD Service)** Позволяет компьютерам на базе UNIX и другим компьютерам использовать службу LPR для печати на общих принтерах сервера.
- **Печать через Интернет (Internet Printing)** Создает веб-сайт, посредством которого авторизованные пользователи могут управлять заданиями на печать. Кроме того, позволяет пользователям, у которых установлен клиент печати через Интернет, печатать на общих принтерах сервера при помощи протокола IPP. Стандартный Интернет-адрес для службы печати через Интернет — *http://*ИмяСервера*/Printers*, где *ИмяСервера* — имя реального внутреннего или внешнего сервера, например, *http://PrintServer15/Printers* или *http://www.cpandl.com/Printers*.

Чтобы добавить роль Службы печати (Print Services) на сервер, выполните следующие действия:

1. В консоли **Диспетчер сервера (Server Manager)** выберите узел **Роли (Roles)** и щелкните ссылку **Добавить роли (Add Roles)**. Откроется Мастер добавления ролей (Add Roles Wizard). Если работа мастера начинается со страницы **Перед началом работы (Before You Begin)**, ознакомьтесь с вводным текстом и щелкните **Далее (Next)**.
2. На странице **Выбор ролей сервера (Select Server Roles)** выберите **Службы печати (Print Services)** и два раза щелкните **Далее (Next)**.
3. На странице **Выбор служб ролей (Select Role Services)** задайте установку одной или нескольких служб. Для обеспечения функциональной совместимости с UNIX обязательно добавьте службу **Служба LPD (LPD Service)**. Щелкните **Далее (Next)**.
4. При установке службы **Печать через Интернет (Internet Printing)** следует также установить роль Веб-сервер (IIS) (Web Server (IIS)) и компонент Служба активации процессов Windows (Windows Process Activation

Service). Подтвердите их установку, и у вас появится возможность добавить другие службы для роли Веб-сервер (IIS) (Web Server (IIS)).

Примечание Службы IIS предоставляют базовую функциональность для размещения серверов, веб-приложений и служб Windows SharePoint. Подробнее — в книге *Microsoft IIS 7 Administrator's Pocket Consultant* (Microsoft, 2008).

5. Щелкните **Далее (Next)**. На экране появится страница **Подтвердите выбранные элементы (Confirm Installation Options)**. Щелкните **Установить (Install)**. Когда мастер завершит установку сервера и выбранных вами функций, на экране появится страница **Результаты установки (Installation Results)**. Убедитесь, что все этапы установки завершились успешно.

Включение и выключение общего доступа к принтерам

В Windows Server 2008 совместное использование принтеров по умолчанию выключено. Чтобы управлять конфигурацией общего доступа к принтеру, выполните следующие действия:

1. Щелкните **Пуск (Start)** и **Сеть (Network)**. На панели инструментов Обозревателя сети (Network Explorer) щелкните кнопку **Центр управления сетями и общим доступом (Network And Sharing Center)**.
2. Разверните раздел **Использование общих принтеров (Printer Sharing)**, щелкнув соответствующую кнопку со стрелкой вниз. Выполните одно из следующих действий и щелкните **Применить (Apply)**:
   - Установите переключатель **Включить общий доступ к принтерам (Turn On Printer Sharing)**, чтобы включить общий доступ к принтерам.
   - Установите переключатель **Выключить общий доступ к принтерам (Turn Off Printer Sharing)**, чтобы отказаться от общего доступа к принтерам.

Консоль Управление печатью (Print Management)

Консоль **Управление печатью (Print Management)** — основной инструмент для работы с принтерами и серверами печати. После установки роли Службы печати (Print Services) консоль **Управление печатью (Print Management)** доступна в меню **Администрирование (Administrative Tools)**. Вы также можете добавить ее как оснастку в любую пользовательскую консоль.

С помощью консоли **Управление печатью (Print Management)**, показанной на рис.18-1, можно устанавливать, просматривать и управлять всеми принтерами и серверами печати организации. Кроме того, в ней отображается состояние принтеров и серверов печати. Если у принтера есть веб-интерфейс управления, в консоли **Управление печатью (Print Management)** указана дополнительная информация о печати, включая информацию о количестве тонера и бумаги.

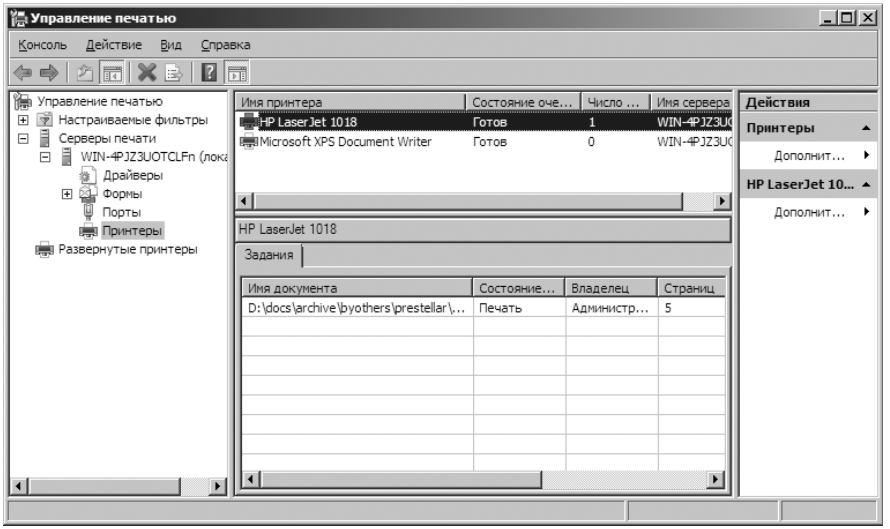


Рис. 18-1. Консоль Управление печатью (Print Management) предназначена для работы с серверами печати и принтерами

По умолчанию консоль **Управление печатью (Print Management)** настроена на управление локальным сервером печати, но вы можете управлять и другими серверами печати организации, добавив их в консоль. Эти серверы печати должны работать под управлением Windows 2000 или более поздней версии. Кроме того, чтобы управлять удаленным сервером печати, вы должны быть членом локальной группы Администраторы (Administrators) этого сервера или членом группы администраторов домена, членом которого является сервер.

Развернув узел **Принтеры (Printers)** для данного сервера печати, на главной панели вы увидите список очередей печати с именами принтеров, состоянием очереди, количеством заданий в очереди и именем сервера. Если щелкнуть правой кнопкой узел **Принтеры (Printers)** и выбрать команду **Показать расширенное представление (Show Extended View)**, вы перейдете в расширенное представление, содержащее информацию о состоянии задания, его владельце, количестве страниц, размере задания, времени постановки в очередь, номере порта и приоритете задания.

Если у принтера есть веб-страница, в расширенном представлении отображается вкладка **Веб-страница принтера (Printer Web Page)**, позволяющая получить непосредственный доступ к странице. На веб-странице вы найдете сведения о состоянии принтера, его свойствах и конфигурации. Иногда на веб-странице можно также выполнять удаленное администрирование.

Чтобы добавить сервер печати в консоль **Управление печатью (Print Management)**, выполните следующее действие:

1. В консоли **Управление печатью (Print Management)** щелкните правой кнопкой узел **Серверы печати (Print Servers)** и выберите команду **Добавление и удаление серверов (Add/Remove Servers)**.

2. В диалоговом окне **Добавление и удаление серверов (Add/Remove Servers)**, показанном на рис. 18-2, показан список добавленных ранее серверов печати.

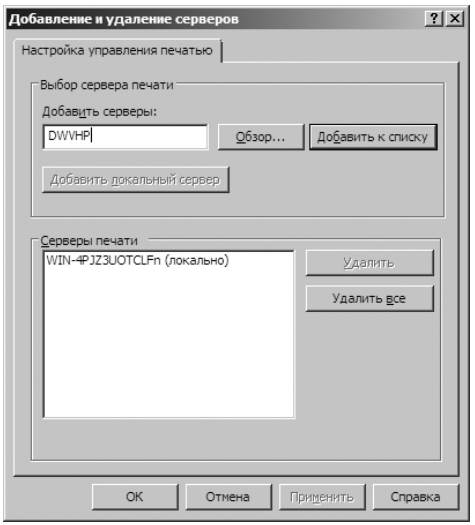


Рис. 18-2. Добавление серверов печати в консоль Управление печатью (Print Management)

3. Выполните одно из следующих действий, а затем щелкните **Добавить к списку (Add To List)**:
   - Введите имена добавляемых серверов печати в поле **Добавить серверы (Add Servers)**. Для разделения имен используются запятые.
   - Щелкните **Обзор (Browse)**, чтобы открыть диалоговое окно **Выберите сервер печати (Select Print Server)**. Выделите нужный сервер и щелкните **Выбор сервера (Select Server)**.
4. При необходимости повторите предыдущий шаг, а затем щелкните **OK**.

Чтобы удалить серверы печати из консоли **Управление печатью (Print Management)**, выполните следующие действия:

1. В консоли **Управление печатью (Print Management)** щелкните правой кнопкой узел **Серверы печати (Print Servers)** и выберите команду **Добавление и удаление серверов (Add/Remove Servers)**.
2. В диалоговом окне **Добавление и удаление серверов (Add/Remove Servers)** отображен список серверов печати. Выберите один или несколько серверов и щелкните кнопку **Удалить (Remove)**.

Установка принтеров

В следующих разделах рассмотрены способы установки принтеров. Система Windows Server 2008 позволяет устанавливать и управлять принтерами в любом месте сети. Чтобы установить и настроить принтер в Windows Server 2008, вы должны быть членом группы Администраторы (Administrators),

Операторы печати (Print Operators) или Операторы сервера (Server Operators). Для печати документов на принтере вы должны обладать соответствующими разрешениями. Подробнее — в разделе «Установка разрешений на доступ к принтеру» этой главы.

Автоматическое добавление в консоль Управление печатью (Print Management)

Консоль **Управление печатью (Print Management)** способна обнаруживать и устанавливать сетевые принтеры, расположенные в той же подсети, что и компьютер, на котором она запущена. Обнаружив принтер, консоль **Управление печатью (Print Management)** автоматически установит подходящие драйверы, настроит очередь печати и организует общий доступ к принтеру. Чтобы автоматически установить сетевые принтеры и настроить сервер печати, выполните следующие действия:

1. Откройте консоль **Управление печатью (Print Management)** при помощи одноименной команды меню **Администрирование (Administrative Tools)**.
2. Разверните узел **Серверы печати (Print Servers)** и щелкните правой кнопкой локальный или удаленный сервер печати, с которым хотите работать.
3. Выберите команду **Добавить принтер (Add Printer)**. Откроется Мастер установки сетевых принтеров (Network Printer Installation Wizard).
4. На странице **Установка принтера (Print Installation)** установите переключатель **Выполнить поиск принтеров в сети (Search The Network For Printers)** и щелкните **Далее (Next)**.
5. Мастер произведет поиск сетевых принтеров. Найденные принтеры будут отображены в списке с именами, IP-адресами и информацией о состоянии. Щелкните принтер, который следует установить, и щелкните **Далее (Next)**.
6. Если для обнаруженного принтера имеется несколько драйверов, вам будет предложено выбрать нужный драйвер. Затем щелкните **Закрыть (Close)**.

Установка и настройка физически подключенных устройств печати

Физически подключенные устройства печати соединяются с компьютером при помощи последовательного или параллельного кабеля, кабеля USB или через инфракрасный порт. Физически подключенные принтеры можно настроить как локальные или как сетевые устройства печати. Ключевое различие состоит в том, что доступ к локальному устройству могут получить только пользователи, вошедшие на компьютер, а сетевые устройства доступны всем пользователям сети. Помните, что рабочая станция или сервер, на который вы вошли, становится сервером печати для настраиваемого устройства.

Если компьютер находится в спящем режиме или выключен, принтер будет недоступен.

Вы можете установить физически подключенное устройство печати локально, войдя на настраиваемый сервер печати, или удаленно, при помощи удаленного рабочего стола. Если вы настраиваете локальный принтер «plug and play», выполнив вход на сервер печати, установка устройства проходит легко. Установив принтер, следует настроить его для дальнейшего использования.

Чтобы установить и настроить устройство печати, выполните следующие действия:

1. Подключите устройство печати к серверу при помощи последовательного, параллельного или USB-кабеля. Включите принтер.
2. Если Windows Server 2008 обнаружит устройство печати автоматически, начнется установка устройства и необходимых драйверов. Если системе не удается найти необходимые драйверы, вам понадобится диск с драйверами принтера.
3. Если Windows Server 2008 не обнаружит устройство автоматически, потребуется ручная установка принтера, описанная далее.
4. После установки принтера настройте его. В консоли **Управление печатью (Print Management)** разверните узел **Серверы печати (Print Servers)** и узел сервера, с которым хотите работать. Выделив узел **Принтеры (Printers)** настраиваемого сервера, на главной панели вы увидите список доступных принтеров. Щелкните правой кнопкой принтер, который хотите настроить, и выберите команду **Управление доступом (Manage Sharing)**. Диалоговое окно свойств принтера откроется на вкладке **Доступ (Sharing)**, показанной на рис. 18-3.
5. Когда вы установите флажок **Совместный доступ к принтеру (Share this Printer)**, в качестве общего имени для принтера Windows Server 2008 установит стандартное имя общего ресурса. При желании, измените имя общего принтера в поле **Сетевое имя (Share Name)**.

Примечание Имена общих ресурсов в Windows NT могут состоять не более чем из восьми символов и не могут содержать пробелов. Имена общих ресурсов в Windows 2000 и более поздних версиях могут состоять из 256 символов, включая пробелы. В больших организациях имена общих ресурсов должны нести смысловую нагрузку, помогающую найти принтер.

6. Публикация общего принтера в Active Directory упростит пользователям его поиск. Если вы хотите поместить общий принтер в Active Directory, установите флажок **Внести в Active Directory (List In The Directory)**.
7. Открывая общий доступ к принтеру, Windows Server 2008 автоматически открывает также доступ к драйверам для их загрузки пользователями при первом подключении к принтеру. В большинстве случаев по умолчанию доступны только драйверы для систем *x*86. Чтобы открыть доступ к дополнительным драйверам, щелкните кнопку **Дополнительные драй-**

веры (Additional Drivers). В диалоговом окне **Дополнительные драйверы (Additional Drivers)** выберите ОС, из которой будет загружаться дополнительный драйвер. При необходимости вставьте компакт-диск Windows Server 2008, диск с драйверами принтера или оба диска. На компакт-диске Windows Server 2008 есть драйверы для большинства версий Windows. Затем два раза щелкните **OK**.

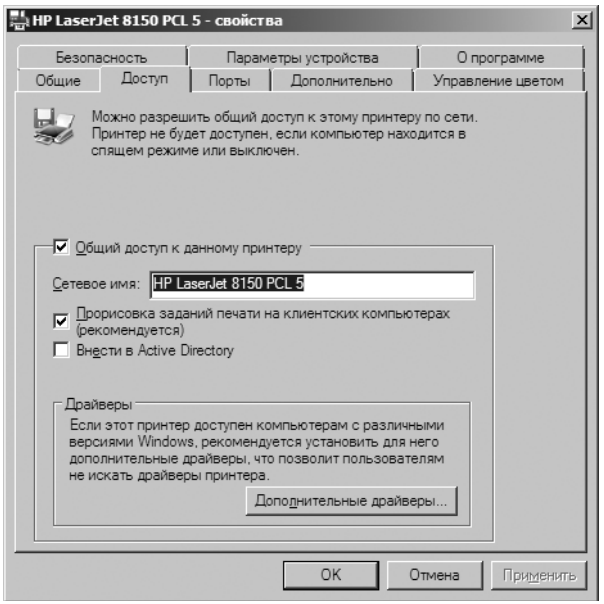


Рис. 18-3. Настройка принтера в диалоговом окне свойств

Случается, что Windows не обнаруживает принтер. В этом случае для установки устройства печати нужно выполнить следующие действия:

1. В консоли **Управление печатью (Print Management)** разверните узел **Серверы печати (Print Servers)** и узел сервера, с которым вы хотите работать.
2. Щелкните правой кнопкой узел **Принтеры (Printers)** нужного сервера и выберите команду **Добавить принтер (Add Printer)**. Откроется Мастер установки сетевых принтеров (Network Printer Installation Wizard).
3. На странице **Установка принтера (Print Installation)**, показанной на рис. 18-4, установите переключатель **Добавить новый принтер, используя существующий порт (Add A New Printer Using An Existing Port)**, а затем выберите соответствующий порт (LPT, COM или USB). Кроме того, вы можете выполнять печать в файл. В этом случае перед каждой отправкой документа на печать Windows Server 2008 будет запрашивать у пользователя имя файла. Щелкните **Далее (Next)**.

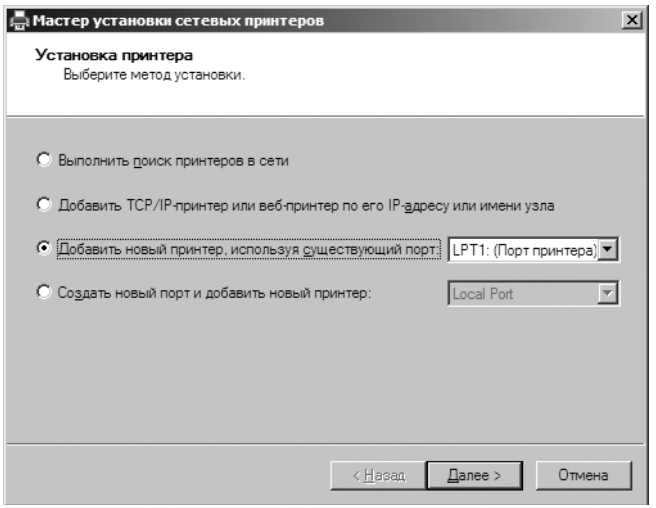


Рис. 18-4. Выбор порта для принтера

4. На странице **Драйвер принтера (Printer Driver)** выберите одну из следующих возможностей:
   - Если Windows удалось обнаружить принтер на выбранном порте и был автоматически найден совместимый драйвер, драйвер принтера будет внесен в список с информацией о производителе и модели принтера. Переключатель **Использовать драйвер принтера, выбранный мастером установки (Use The Printer Driver That The Wizard Selected)** будет установлен автоматически. Чтобы принять этот вариант, просто щелкните **Далее (Next)**.
   - Если совместимый драйвер не найден и вы хотите выбрать существующий драйвер, установленный на компьютере, установите переключатель **Использовать имеющийся на этом компьютере драйвер (Use An Existing Driver)**. Выбрав подходящий драйвер в списке, щелкните **Далее (Next)**.
   - Если совместимый драйвер не найден и вы хотите установить новый драйвер, установите переключатель **Установить новый драйвер (Install A New Driver)**. Как показано на рис. 18-5, от вас потребуется указать производителя и модель принтера. Допустим, вы устанавливаете принтер HP LaserJet 8150 PCL 5. В списке производителей вы должны указать HP, а списке принтеров — HP LaserJet 8150 PCL 5. Затем щелкните **Далее (Next)**. Windows Server 2008 назначит драйвер устройству печати. Если нужные производитель и модель отсутствуют в списке, для установки нового драйвера щелкните кнопку **Установить с диска (Have Disk)**.

Примечание Если у вас нет драйвера для той или иной модели принтера, воспользуйтесь стандартным драйвером или драйвером для похожего принтера. Дополнительные указания вы найдете в документации устройства печати.

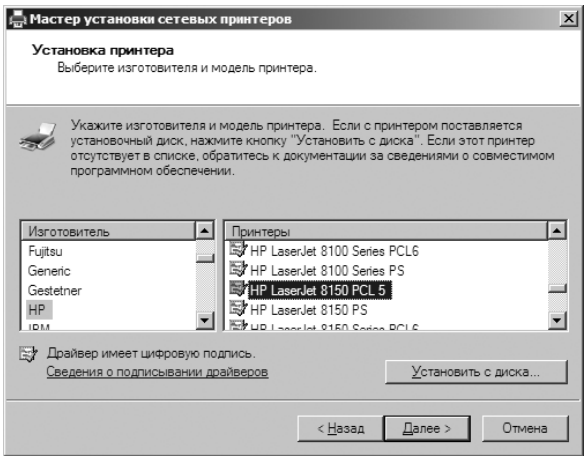


Рис. 18-5. Выбор производителя и модели устройства печати

5. Задайте имя принтера. Оно будет отображаться в консоли **Управление печатью (Print Management)**.
6. Укажите, будет ли доступен принтер удаленным пользователям. Чтобы открыть общий доступ к принтеру, установите флажок **Совместный доступ к принтеру (Share This Printer)** и введите имя общего ресурса. В больших организациях имена общих ресурсов должны нести смысловую нагрузку, помогающую найти принтер.
7. При необходимости укажите расположение принтера и добавьте его описание. Эта информация поможет пользователям найти принтер и определить его возможности.
8. На последней странице проверьте параметры и щелкните **Далее (Next)**.
9. Когда Windows установит и настроит принтер, убедитесь, что установка прошла успешно. При наличии ошибок придется устранить неисправности и повторить процесс установки. Чтобы испытать принтер, установите флажок **Напечатать пробную страницу (Print Test Page)** и щелкните **Готово (Finish)**. Чтобы установить другой принтер, установите флажок **Добавить другой принтер (Add Another Printer)** и щелкните **Готово (Finish)**.

Когда установка нового принтера в Мастере установки сетевых принтеров (Network Printer Installation Wizard) закончится, в папке **Принтеры (Printers)** появится новый значок с заданным вами именем. С его помощью вы сможете изменить свойства и проверить состояние принтера. Подробнее — в разделе «Управление драйверами принтеров» этой главы.

Совет Повторив те же действия, можно создать несколько принтеров для одного устройства печати. Для этого достаточно изменить имя принтера и общего ресурса. Несколько принтеров для одного устройства печати позволяют задавать различные параметры для различных целей. Например, можно создать высокоприоритетный принтер для немедленной печати и принтер с низким приоритетом для печати несрочных заданий.

Установка сетевых устройств печати

Сетевое устройство печати — это печатающее устройство, при помощи собственного сетевого адаптера подключенное непосредственно к сети. Подключенные к сети принтеры настраиваются как сетевые устройства печати и доступны пользователям сети как общие принтеры. Помните, что сервер, на котором вы настраиваете устройство печати, становится сервером печати для этого устройства.

Чтобы установить сетевое устройство печати, выполните следующие действия:

1. В консоли **Управление печатью (Print Management)** разверните узел **Серверы печати (Print Servers)** и узел сервера, с которым хотите работать.
2. Щелкните правой кнопкой узел **Принтеры (Printers)** и выберите команду **Добавить принтер (Add Printer)**. Откроется Мастер установки сетевых принтеров (Network Printer Installation Wizard).
3. На странице **Установка принтера (Print Installation)** установите переключатель **Добавить TCP/IP-принтер или веб-принтер по его IP-адресу или имени узла (Add A TCP/IP Or Web Services Printer By IP Address Or Hostname)** и щелкните **Далее (Next)**.
4. На странице **Адрес принтера (Printer Address)** выберите в списке **Тип устройства (Type Of Device)** один из следующих вариантов:
   - **Автообнаружение (Autodetect)** Установите этот переключатель, если не уверены в типе устройства печати. Windows Server 2008 попытается определить тип устройства автоматически.
   - **Устройство TCP/IP (TCP/IP Device)** Установите этот переключатель, если уверены, что принтер относится к TCP/IP-устройствам.
   - **Принтер веб-служб (Web Services Printer)** Установите этот переключатель, если уверены, что принтер позволяет выполнять печать через Интернет.
5. Введите имя хоста или IP-адрес принтера, например, 192.168.1.90. Если вы установили переключатели **Автообнаружение (Autodetect)** или **Устройство TCP/IP (TCP/IP Device)**, мастер задаст такое же имя порта. При желании вы вольны изменить имя.

Совет Имя порта не имеет особого значения, оно должно лишь быть уникальным в пределах системы. Если вы настраиваете несколько принтеров на сервере печати, запишите сопоставления портов и принтеров.

6. Щелкните **Далее (Next)**. Мастер попытается автоматически обнаружить устройство печати. Если это не удалось, проверьте следующее:
   - правильно ли вы выбрали тип устройства печати;
   - включено ли питание устройства печати и подключено ли оно к сети;
   - правильно ли настроен принтер;
   - нет ли ошибки в IP-адресе или имени принтера.

7. Если в типе, IP-адресе или имени устройства допущена ошибка, щелкните **Назад (Back)** и повторно введите информацию.
8. Если информация введена правильно, потребуется дальнейшая идентификация устройства. В разделе **Тип устройства (Device Type)** на странице **Требуются дополнительные сведения о порте (Additional Port Information Required)** установите переключатель **Обычное (Standard)** и выберите модель принтера или тип используемого принтером сетевого адаптера. Или установите переключатель **Особое (Custom)** и щелкните кнопку **Параметры (Settings)**, чтобы задать специальные параметры принтера, например, протокол и состояние SNMP.
9. На странице **Драйвер принтера (Printer Driver)** выберите одну из следующих возможностей:
   - Если Windows удалось обнаружить принтер на выбранном порте и был автоматически найден совместимый драйвер, драйвер принтера будет внесен в список с информацией о производителе и модели принтера. Переключатель **Использовать драйвер принтера, выбранный мастером установки (Use The Printer Driver That The Wizard Selected)** будет установлен автоматически. Чтобы принять этот вариант, просто щелкните **Далее (Next)**.
   - Если совместимый драйвер не найден и вы хотите выбрать существующий драйвер, установленный на компьютере, установите переключатель **Использовать имеющийся на компьютере драйвер (Use An Existing Driver)**. Выбрав подходящий драйвер в списке, щелкните **Далее (Next)**.
   - Если совместимый драйвер не найден и вы хотите установить новый драйвер, установите переключатель **Установить новый драйвер (Install A New Driver)**. От вас потребуется указать производителя и модель принтера. Допустим, вы устанавливаете принтер HP LaserJet 8150 PCL 5. В списке производителей вы должны указать HP, а списке принтеров — HP LaserJet 8150 PCL 5. Затем щелкните **Далее (Next)**. Windows Server 2008 назначит драйвер устройству печати. Если нужные производитель и модель отсутствуют в списке, для установки нового драйвера щелкните кнопку **Установить с диска (Have Disk)**.
10. Назначьте принтеру имя, которое будет отображаться в консоли **Управление печатью (Print Management)**.
11. Укажите, будет ли принтер доступен удаленным пользователям. Чтобы сделать принтер общим, установите переключатель **Имя ресурса (Share Name)** и введите имя общего ресурса. В больших организациях имена общих ресурсов должны нести смысловую нагрузку, помогающую найти принтер.
12. При необходимости укажите расположение принтера и добавьте его описание. Эта информация поможет пользователям найти принтер и определить его возможности.

13. На последней странице проверьте параметры и щелкните **Далее (Next)**.
14. Когда Windows установит и настроит принтер, убедитесь, что установка прошла успешно. При наличии ошибок придется устранить неисправности и повторить процесс установки. Чтобы испытать принтер, щелкните **Напечатать пробную страницу (Print Test Page)** и щелкните **Готово (Finish)**. Чтобы установить другой принтер, щелкните **Добавить другой принтер (Add Another Printer)** и щелкните **Готово (Finish)**.

Когда установка нового принтера в Мастере установки сетевых принтеров (Network Printer Installation Wizard) закончится, в папке **Принтеры (Printers)** появится новый значок с заданным вами именем. С его помощью вы сможете изменить свойства и проверить состояние принтера. Подробнее — в разделе «Управление драйверами принтеров» этой главы.

Совет В этом случае также можно создать несколько принтеров для одного устройства печати.

Подключение к сетевому принтеру

Когда вы создали сетевой принтер, удаленные пользователи подключаются к нему, как к любому другому принтеру. Вы или сами пользователи должны будете создать подключения отдельно для каждого пользователя. Чтобы создать подключение к принтеру в системе Windows Vista, выполните следующие действия:

1. Войдя в систему с учетной записью пользователя, щелкните **Пуск (Start)** и **Панель управления (Control Panel)**. Затем дважды щелкните значок **Принтеры (Printers)**, чтобы открыть одноименную папку.
2. На панели инструментов щелкните кнопку **Установка принтера (Add A Printer)**, чтобы запустить мастер Установка принтера (Add Printer Wizard). Щелкните кнопку **Добавить сетевой, беспроводной или Bluetooth-принтер (A Network, Wireless Or Bluetooth Printer)** и щелкните **Далее (Next)**.
3. Если нужный принтер имеется в списке **Выберите принтер (Select A Printer)**, выделите его и щелкните **Далее (Next)**.
4. Если в списке **Выберите принтер (Select A Printer)** нет нужного принтера, щелкните **Нужный принтер отсутствует в списке (The Printer That I Want Isn't Listed)**. На странице **Найти принтер по имени или TCP/IP-адресу (Find A Printer By Name Or TCP/IP Address)** выполните одно из следующих действий:
   - Для поиска общих принтеров в сети установите переключатель **Обзор принтеров (Browse For A Printer)**, а затем щелкните **Далее (Next)**. Выделите нужный принтер и щелкните **Выделить (Select)**.
   - Чтобы указать принтер, используя путь к общему ресурсу, установите переключатель **Выбрать общий принтер по его имени (Select A Shared Printer By Name)**. Введите путь к общему принтеру в формате

UNC, например, **PrintServer12\Twelfth Floor NE**, или сетевой путь к принтеру в Интернете, например, **http://PrintServer12/Printers/IPrinter52/.printer**.

- Чтобы найти принтер по TCP/IP-адресу или имени хоста, установите переключатель **Добавить принтер по его TCP/IP-адресу или имени узла (Add A Printer Using A TCP/IP Address Or Hostname)**. Щелкните **Далее (Next)**. Укажите тип устройства, затем введите имя хоста или IP-адрес принтера, например, 192.168.1.90. Для типов устройства **Автовыбор (Autodetect)** и **Устройство TCP/IP (TCP/IP Device)** мастер установит такое же значение имени порта. При желании измените имя порта и щелкните **Далее (Next)**.

5. На странице **Введите имя принтера или IP-адрес (Type A Printer Hostname Or IP Address)** установлено стандартное имя принтера. Оставьте его неизменным или введите новое. Щелкните **Далее (Next)** и **Готово (Finish)**. Теперь пользователь сможет печатать на сетевом принтере. В папке **Принтеры (Printers)** на компьютере пользователя появится новый сетевой принтер.

Чтобы создать подключение к принтеру в системе Windows XP, выполните эти шаги:

1. Войдя в систему с учетной записью пользователя, откройте папку **Принтеры и факсы (Printers And Faxes)**.
2. Щелкните команду **Установка принтера (Add Printer)**, чтобы открыть Мастер установки принтеров (Add Printer Wizard). На второй странице мастера установите переключатель **Сетевой принтер (A Network Printer)** и щелкните **Далее (Next)**.
3. В диалоговом окне **Укажите принтер (Specify A Printer)** укажите способ поиска сетевого принтера. В вашем распоряжении следующие варианты:
   - **Найти принтер в Active Directory (Find A Printer In The Directory)** Установите этот переключатель, чтобы найти принтер в Active Directory.
   - **Введите имя принтера или нажмите кнопку «Далее» для обзора принтеров (Type The Printer Name, Or Click Next To Browse For A Printer)** Установите этот переключатель, чтобы найти общие принтеры в сети с помощью окна поиска.
   - **Подключиться к принтеру в Интернете или в вашей интрасети (Connect To A Printer On The Internet Or On Your Intranet)** Установите этот переключатель, чтобы ввести URL Интернет-принтера.
4. Выберите принтер и щелкните **OK**.
5. Укажите, будет ли принтер использоваться по умолчанию, щелкнув **Да (Yes)** или **Нет (No)**, и щелкните **Далее (Next)**.
6. Щелкните **Готово (Finish)**, чтобы завершить установку. Теперь пользователь сможет печатать на сетевом принтере, а в папке Принтеры и факсы

(Printers And Faxes) на компьютере пользователя появится значок нового сетевого принтера. С его помощью вы сможете настроить локальные параметры. По умолчанию имя принтера имеет формат *Принтер* на *ИмяКомпьютера*, например, HP DeskJet на ENGSVR01.

Развертывание подключений к принтерам

Осуществить подключение к принтерам довольно легко, но вы можете еще более упростить процесс, развертывая подключения к принтерам при помощи групповой политики. Если вы хотите организовать доступ к принтеру для определенных пользователей с любого компьютера, развертывайте принтер для группы пользователей. Если вы хотите организовать доступ к принтеру для любого пользователя, зарегистрировавшегося на определенных компьютерах, развертывайте принтер для группы компьютеров. Подключения компьютеров к принтерам Windows добавляет или удаляет при запуске компьютера. Подключения пользователей к принтерам добавляются и удаляются при входе пользователя в систему.

Чтобы развернуть подключения к принтерам на компьютерах под управлением версий Windows до Windows Vista, выполните следующие действия:

1. В консоли **Управление групповой политикой (Group Policy Management Console)** щелкните правой кнопкой GPO сайта, домена или подразделения, с которым вы хотите работать, и выберите команду **Изменить (Edit)**. Откроется редактор групповой политики.
2. В окне редактора выполните одно из следующих действий:
   - Чтобы развернуть подключение к принтеру для конкретных компьютеров, разверните узел **Конфигурация компьютера (Computer Configuration)** дважды щелкните узел **Конфигурация Windows (Windows Settings)**. Затем щелкните **Сценарии (Scripts)**.
   - Чтобы развернуть подключение к принтеру для конкретных пользователей, разверните узел **Конфигурация пользователя (User Configuration)** дважды щелкните узел **Конфигурация Windows (Windows Settings)**. Затем щелкните **Сценарии (Scripts)**.
3. Скопируйте файл PushPrinterConnections.exe из папки %SystemRoot%\System32 в папку Machine\Scripts\Startup, User\Scripts\Logon или User\Scripts\Logoff соответствующей политики. Политики хранятся на контроллере домена, в папке %SystemRoot%\Sysvol\Domain\Policies.
4. В окне редактора групповой политики щелкните правой кнопкой элемент **Автозагрузка (Startup)** или **Вход в систему (Logon)** и выберите команду **Свойства (Properties)**.
5. В диалоговом окне **Свойства: Автозагрузка (Startup Properties)** или **Свойства: Вход в систему (Logon Properties)** щелкните кнопку **Показать файлы (Show Files)**. Если вы скопировали исполняемый файл в правильное расположение в папке Policies, он будет отображен в диалоговом окне.

6. В диалоговом окне **Свойства: Автозагрузка (Startup Properties)** или **Свойства: Вход в систему (Logon Properties)** щелкните кнопку **Добавить (Add)**. Откроется диалоговое окно **Добавление сценария (Add Script)**.
7. В поле **Имя сценария (Script Name)** введите **PushPrinterConnections.exe** и щелкните **OK**.

Чтобы развернуть подключения к принтеру на компьютерах под управлением Windows Vista и более поздних версий, выполните следующие действия:

1. В консоли **Управление печатью (Print Management)** разверните узел **Серверы печати (Print Servers)** и узел сервера, с которым вы хотите работать.
2. Выделите узел **Принтеры (Printers)**. На главной панели щелкните правой кнопкой принтер, который хотите развернуть, и выберите команду **Развернуть с помощью групповой политики (Deploy With Group Policy)**. Откроется диалоговое окно **Развертывание с помощью групповой политики (Deploy With Group Policy)**, показанное на рис. 18-6.

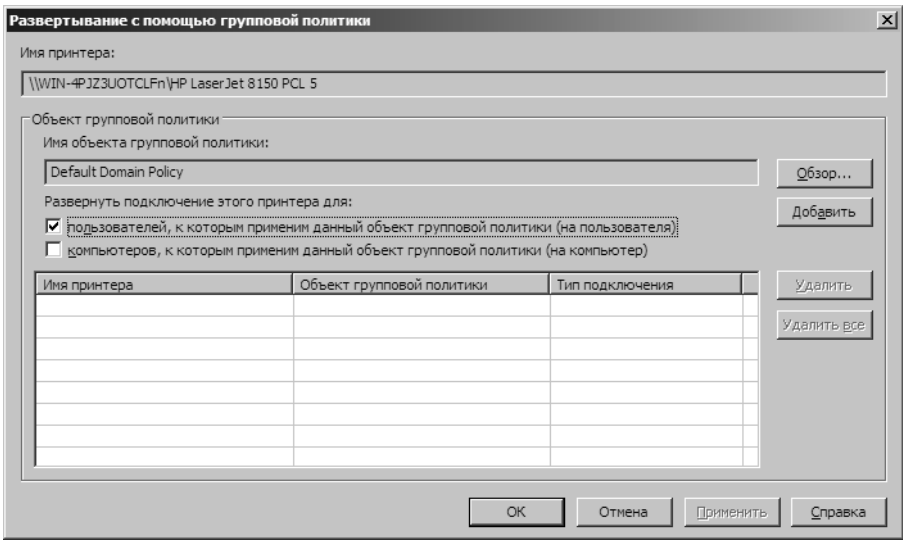


Рис. 18-6. Выбор GPO для развертывания принтера

3. Щелкните кнопку **Обзор (Browse)**. В диалоговом окне **Поиск объекта групповой политики (Browse For Group Policy Object)** выберите нужный GPO и щелкните **OK**.
4. В разделе **Развернуть подключение этого принтера для (Deploy This Printer Connection To The Following)** установите один или оба флажка:
   - Чтобы распространить подключение к принтеру на пользователей, установите флажок **Пользователей, к которым применим данный объект групповой политики (The Users That This GPO Applies To)**.
   - Чтобы распространить подключение к принтеру на компьютеры, установите флажок **Компьютеров, к которым применим данный объект групповой политики (The Computers That This GPO Applies To)**.

5. Щелкните **Добавить (Add)**.
6. Повторите шаги 3–5, чтобы развернуть принтера в других GPO.
7. Щелкните **OK**, чтобы сохранить изменения в объектах GPO. Убедитесь, что операция завершена успешно. При возникновении ошибки щелкните кнопку **Сведения (Details)**. Наиболее часто ошибки связаны с разрешениями на редактирование GPO, с которым вы работаете. Если используемая вами учетная запись не обладает соответствующими разрешениями, используйте учетную запись с дополнительными полномочиями.

Ограничения указания и печати

Параметр групповой политики Ограничения указания и печати (Point and Print Restrictions) управляет несколькими важными аспектами безопасности принтера. В Windows XP Professional и более поздних версиях этот параметр определяет серверы, к которым клиентский компьютер может подключаться при помощи функции указания и печати. В Windows Vista и более поздних версиях он управляет предупреждениями системы безопасности и запросами на повышение полномочий, когда пользователь применяет функцию указания и печати или когда следует настроить драйверы для подключения принтера. Применение данного параметра описано в табл. 18-1.

Табл. 18-1. Ограничения указания и печати

Параметр политики...	Политика работает следующим образом
Включен	Клиенты под управлением Windows XP и Windows Server 2003 могут использовать указание и печать только на явно заданном списке серверов леса. Клиенты под управлением Windows Vista и более поздних версий могут использовать указание и печать на всех серверах. На клиентах Windows Vista и более поздних версий можно настроить отображение или сокрытие предупреждений или запросов на повышение полномочий в ходе указания и печати или на обновление драйвера существующего подключения принтера
Не настроен	Клиенты под управлением Windows XP и более поздних версий могут использовать указание и печать на любом сервере леса. Клиенты Windows Vista и более поздних версий в ходе указания и печати не будут выдавать предупреждения и запросы на повышение полномочий пользователей или на обновление драйвера существующего подключения принтера
Отключен	Клиенты под управлением Windows XP и более поздних версий могут использовать указание и печать на любом сервере. Клиенты Windows Vista и более поздних версий в ходе указания и печати не будут выдавать предупреждения и запросы на повышение полномочий пользователей или на обновление драйвера существующего подключения принтера

По умолчанию, Windows Vista и Windows Server 2008 позволяют пользователям, не являющимся членами группы с административными привилеги-

ями, устанавливать только надежные драйвера принтеров. Например, драйвера, поставляющиеся с Windows, либо, имеющие цифровую подпись пакеты драйверов принтера. Включая параметр Ограничения указания и печати (Point and Print Restrictions), вы также разрешаете пользователям, не являющимся членами локальной группы с административными полномочиями, устанавливать подключения к принтеру, развернутые с помощью групповой политики. При этом, пользователи смогут устанавливать дополнительные или обновленные неподписанные драйвера принтера. Если данный параметр отключен, пользователям придется предоставлять для этого полномочия учетной записи, обладающей административными полномочиями.

Чтобы включить и настроить параметр Ограничения указания и печати (Point and Print Restrictions) в редакторе групповой политики, выполните следующие действия:

1. В консоли **Управление групповой политикой (Group Policy Management Console)** щелкните правой кнопкой GPO сайта, домена или подразделения, с которым хотите работать, и выберите команду **Изменить (Edit)**. Откроется редактор групповой политики.
2. В окне редактора разверните узлы **Конфигурация пользователя\Административные шаблоны\Панель управления (User Configuration\Administrative Templates\Control Panel)** и выберите узел **Принтеры (Printers)**.
3. В главной панели дважды щелкните политику **Ограничения указания и печати (Point and Print Restrictions)**.
4. В диалоговом окне **Свойства: Ограничения указания и печати (Point And Print Restrictions Properties)**, показанном на рис. 18-7, установите переключатель **Включен (Enabled)**.

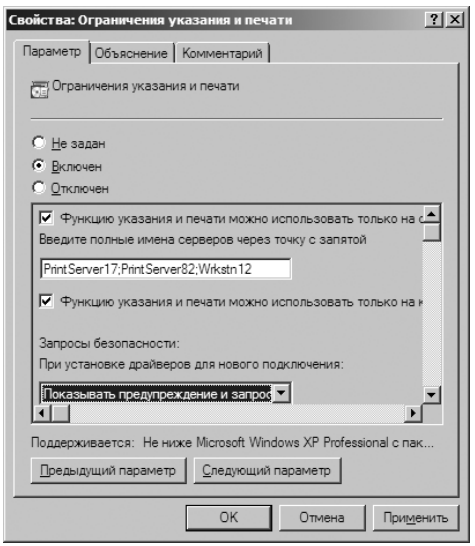


Рис. 18-7. Настройка свойств указания и печати

5. Включив политику, вы можете настроить ее таким образом, что пользователи смогут печатать только на заданном списке серверов. Чтобы ввести это ограничение, установите соответствующий флажок и введите список FQDN-имен серверов, разделенных точкой с запятой. Для снятия ограничения сбросьте соответствующий флажок.
6. Вы можете настроить политику таким образом, что пользователи смогут печатать удаленно на серверах в своем лесе. Чтобы ввести это ограничение, установите соответствующий флажок. Для снятия ограничения сбросьте флажок.
7. При установке драйверов для нового подключения клиенты под управлением Windows Vista и более поздних версий могут выдавать или не выдавать предупреждения и запросы на повышение полномочий. Задайте нужный вариант в соответствующем списке.
8. В ходе обновления драйверов существующего подключения клиенты под управлением Windows Vista и более поздних версий могут выдавать или не выдавать предупреждения и запросы на повышение полномочий. Задайте нужный вариант в соответствующем списке.
9. Щелкните **OK**.

Перенос принтеров на новый сервер печати

Перенос очередей, драйверов, процессоров печати, а также портов принтера с одного сервера печати на другой, осуществляется с помощью мастера Миграция принтеров (Printer Migration Wizard). Это эффективный способ объединения нескольких серверов печати или замены старого сервера.

При переносе принтера сервер, на котором расположен принтер в данный момент, называется исходным сервером, а сервер, на который выполняется перемещение, — целевым сервером. Чтобы переместить принтеры на новый сервер печати, выполните следующие действия:

1. В консоли **Управление печатью (Print Management)** щелкните правой кнопкой исходный сервер и выберите команду **Экспортировать принтеры в файл (Export Printers To A File)**. Откроется мастер Миграция принтеров (Printer Migration Wizard).
2. На первой странице указаны связанные с принтером объекты, экспорт которых будет произведен. Щелкните **Далее (Next)**.
3. На странице **Выберите расположение файла (Select The File Location)** щелкните **Обзор (Browse)**. В открывшемся диалоговом окне укажите место, в котором следует сохранить файл. Введите имя файла и щелкните **Открыть (Open)**.
4. Файлы переноса принтеров имеют расширение .printerExport. Чтобы принять этот вариант, щелкните **Далее (Next)**.
5. Когда мастер завершит процесс экспорта, щелкните кнопку **Открыть просмотр событий (Open Event Viewer)**, чтобы просмотреть события, сгене-

рированные в процессе экспорта. Если в процессе экспорта произошла ошибка, записи о событиях помогут вам ее выявить и выработать возможные действия по ее устранению. Затем закройте консоль **Просмотр событий (Event Viewer)**.

6. На странице **Экспорт (Exporting)** щелкните **Готово (Finish)**, чтобы закрыть мастер **Миграция принтеров (Printer Migration Wizard)**.
7. В консоли **Управление печатью (Print Management)** щелкните правой кнопкой конечный сервер и выберите команду **Импортировать принтеры из файла (Import Printers From A File)**. Откроется мастер Миграция принтеров (Printer Migration Wizard).
8. На странице **Выберите расположение файла (Select The File Location)** щелкните **Обзор (Browse)**. В открывшемся диалоговом окне выберите ранее созданный файл переноса принтера и щелкните **Открыть (Open)**.
9. Щелкните **Далее (Next)**. Просмотрите объекты, импорт которых будет произведен, и щелкните **Далее (Next)**. На странице **Выберите параметры импорта (Select Import Options)** в списке **Режим импорта (Import Mode)** выберите один из следующих вариантов:
   - **Сохранить существующие принтеры; импортировать копии (Keep Existing Printers; Import Copies)** Если существующие очереди печати имеют те же имена, что и импортируемые очереди, мастер создаст копии. Это обеспечит доступность как исходных, так и импортируемых очередей печати.
   - **Перезаписать существующие принтеры (Overwrite Existing Printers)** Если существующие очереди печати имеют те же имена, что и импортируемые очереди, мастер перезапишет существующие очереди информацией из импортируемых очередей.
10. В списке **Перечислить в каталоге (List In The Directory)** выберите один из следующих вариантов:
    - **Составить список тех принтеров, которые были в списке раньше (List Printers That Were Previously Listed)** В Active Directory будут помещены только принтеры, которые и ранее там присутствовали.
    - **Составить список всех принтеров (List All Printers)** В Active Directory помещаются все принтеры.
    - **Не составлять список принтеров (Don't List Any Printers)** Принтеры не вносятся в Active Directory.
11. Щелкните **Далее (Next)**, чтобы запустить импорт. Когда мастер завершит процесс импорта, щелкните кнопку **Открыть просмотр событий (Open Event Viewer)**, чтобы просмотреть события, сгенерированные в процессе импорта. Если в процессе импорта произошла ошибка, записи о событиях помогут вам ее выявить и выработать возможные действия по ее устранению. Затем закройте консоль **Просмотр событий (Event Viewer)**.

12. На странице **Импорт (Importing)** щелкните **Готово (Finish)**, чтобы закрыть мастер Миграция принтеров (Printer Migration Wizard).

Автоматический мониторинг принтеров и очередей печати

Фильтры принтеров позволяют отображать только те принтеры, очереди и драйверы, которые удовлетворяют определенным критериям. Фильтры можно использовать для автоматизации наблюдения за принтерами.

Консоль **Управление печатью (Print Management)** позволяет просматривать существующие фильтры в узле **Настраиваемые фильтры (Custom Filters)**. Если развернуть узел **Настраиваемые фильтры (Custom Filters)** и выбрать фильтр, на главной панели будут отображены только принтеры и драйверы принтеров, удовлетворяющее критерию фильтра. В консоли **Управление печатью (Print Management)** имеются следующие фильтры:

- **Все принтеры (All Printers)** Все принтеры, связанные с серверами печати, которые были добавлены в консоль.
- **Все драйверы (All Drivers)** Все драйверы принтеров, связанных с серверами печати, которые были добавлены в консоль.
- **В состоянии «Не готов» (Printers Not Ready)** Все принтеры, находящиеся в состоянии «Не готов» (Not Ready), например, принтеры с ошибками.
- **С заданиями печати (Printers With Jobs)** Все принтеры, связанные с серверами печати, у которых есть активные или отложенные задания.

Чтобы создать пользовательский фильтр, выполните следующие действия:

1. В консоли **Управление печатью (Print Management)** щелкните правой кнопкой узел **Настраиваемые фильтры (Custom Filters)** и выберите команду **Добавить новый фильтр принтеров (Add New Printer Filter)**. Откроется Мастер создания фильтра принтеров (New Filter Wizard).
2. На странице **Имя и описание фильтра принтеров (Printer Filter Name And Description)** введите имя и описание фильтра. Если вы хотите, чтобы рядом с именем фильтра отображалось число элементов, соответствующих критерию, установите флажок **Показывать общее число принтеров после имени фильтра принтеров (Display The Total Number Of Printers)**. Щелкните **Далее (Next)**.
3. На странице **Определить фильтр принтеров (Define A Printer Filter)** задайте фильтр, указав в первой строке поле, условие и значение. При необходимости определите дополнительные критерии во второй, третьей и следующих строках. Щелкните **Далее (Next)**.

Примечание Создавая фильтры для мониторинга, вы чаще всего будете использовать поле **Состояние очереди (Queue Status)**. Это позволит вам своевременно узнавать об определенном состоянии принтера. Вы можете следить за возникновением следующих состояний: Выходной лоток полон (Output Bin Full), Готов (Ready), Занят (Busy), Застряла бумага (Paper Jam), Идет ввод-вывод (IO Active), Инициализация (Initializing), Недостаточно памяти (Out Of Memory), Недоступен (Not Available), Неполадки с бумагой (Paper Problem), Нет бумаги (Out Of Paper), Нет тонера или чернил (No Toner/Ink), Обра-

ботка (Processing), Ожидание (Waiting), Отключен (Offline), Открыта дверца (Door Open), Ошибка (Error), Печать (Printing), Приостановлен (Paused), Прогрев (Warming Up), Тонер или чернила на исходе (Toner/Ink Low), Требуется вмешательство (User Intervention Required), Требуется ручная подача (Manual Feed Required), Удаление (Deleting).

Совет Вы можете следить как за выполнением, так и за невыполнением условия. Например, если вы хотите узнавать только о состояниях, требующих внимания, задавайте в фильтре условие несовпадения состояния очереди со значениями Готов (Ready), Инициализация (Initializing), Обработка (Processing), Печать (Printing), Прогрев (Warming Up), Удаление (Deleting).

4. На странице **Настроить уведомления (Set Notification)** задайте действие, которое следует выполнять при выполнении критерия — отправлять сообщение по электронной почте, запускать сценарий или выполнять оба этих действия. Щелкните **Готово (Finish)**, чтобы завершить настройку.

Чтобы изменить пользовательский фильтр, выполните следующие действия:

1. В консоли **Управление печатью (Print Management)** разверните узел **Настраиваемые фильтры (Custom Filters)**. Выделите и щелкните правой кнопкой фильтр, который хотите настроить. В контекстном меню выберите команду **Свойства (Properties)**.
2. В диалоговом окне свойств фильтра настройте параметры фильтра. В этом окне есть три вкладки:
   - **Общие (General)** Имя и описание принтера. Здесь можно ввести новое имя и описание.
   - **Критерии фильтрации (Filter Criteria)** Отображает параметры фильтра. Здесь можно задать новый критерий фильтра.
   - **Уведомление (Notification)** Параметры уведомления по электронной почте и при помощи сценария. Здесь можно изменить параметры уведомления.

Устранение неисправностей очереди

Управление очередью заданий печати в Windows Server 2008 осуществляется при помощи службы Диспетчер печати (Print Spooler). Если она не запущена, задания печати в очередь добавляться не будут. Чтобы проверить состояние службы Диспетчер печати (Print Spooler), воспользуйтесь консолью **Службы (Services)**. Для проверки и перезапуска службы Диспетчер печати (Print Spooler) выполните следующие действия:

1. В меню **Администрирование (Administrative Tools)** выберите команду **Управление компьютером (Computer Management)**.
2. Если вы хотите подключиться к удаленному компьютеру, щелкните правой кнопкой элемент **Управление компьютером (Computer Management)** в дереве консоли и в контекстном меню выберите команду **Подключиться к другому компьютеру (Connect To Another Computer)**. Выберите систему, службами которой хотите управлять.

3. Разверните узел **Службы и приложения (Services And Applications)** и выберите элемент **Службы (Services)**.
4. Выделите службу Диспетчер печати (Print Spooler). В столбце состояния службы должно стоять значение **Работает (Restarted)**. Если это не так, щелкните службу Диспетчер печати (Print Spooler) и выберите команду **Запустить (Start)**. В столбце **Тип запуска (Startup Type)** должно стоять значение **Авто (Automatic)**. Если это не так, дважды щелкните службу Диспетчер печати (Print Spooler) и выберите в списке **Тип запуска (Startup Type)** значение **Авто (Automatic)**.

Совет В работе диспетчера печати случаются сбои. Среди симптомов — остановка принтера или прекращение отправки заданий на устройство печати. Иногда устройство печатает страницы с искажениями. В большинстве случаев решить проблему помогает остановка и повторный запуск службы Диспетчер печати (Print Spooler). Другие проблемы диспетчера могут быть связаны с разрешениями. Подробнее — в разделе «Установка разрешений на доступ к принтеру» этой главы.

Настройка свойств принтера

Этот раздел посвящен настройке основных свойств принтера. Чтобы открыть диалоговое окно свойств принтера, выполните следующие действия:

1. В консоли **Управление печатью (Print Management)** разверните узел **Серверы печати (Print Servers)** и узел сервера, с которым вы хотите работать.
2. Выделите узел **Принтеры (Printers)**. Щелкните правой кнопкой нужный принтер и выберите команду **Свойства (Properties)**. Теперь вы можете задать свойства принтера.

Добавление описания и информации о размещении

Чтобы облегчить поиск принтера, добавьте в его свойства описание и информацию о размещении принтера. В описание включается общая информация о принтере, например, тип устройства печати и ответственный за его работу. В информации о размещении описано место, где находится устройство печати. Эти поля могут отображаться в приложениях. Например, Microsoft Word отображает эту информацию в окне **Печать (Print)**.

Описание и информация о размещении принтера добавляются на вкладке **Общие (General)** диалогового окна свойств принтера, в полях **Комментарий (Comments)** и **Размещение (Location)**.

Публикация принтеров в Active Directory

Внесение принтеров в Active Directory облегчает пользователям их поиск и установку. Чтобы внести принтер в Active Directory, выполните следующие действия:

1. Откройте диалоговое окно свойств принтера и перейдите на вкладку **Доступ (Sharing)**.

2. Установите флажок **Внести в Active Directory (List In Directory)** и щелкните **OK**.

Управление драйверами принтеров

В домене Windows Server 2008 настраивать и обновлять драйвера принтеров требуется только на сервере печати. Обновление драйверов принтеров на клиентах под управлением Windows не требуется. При необходимости клиентские системы обеспечиваются драйверами посредством настройки сетевого принтера.

Обновление драйвера принтера

Чтобы обновить драйвер принтера, выполните следующие действия:

1. Откройте диалоговое окно свойств принтера и перейдите на вкладку **Дополнительно (Advanced)**.
2. В списке **Драйвер (Driver)** выберите нужный драйвер из установленных в данный момент драйверов.
3. Если нужный драйвер отсутствует в списке или если у вас есть новый драйвер, щелкните кнопку **Сменить (New Driver)**. Запустится Мастер дополнительных драйверов принтера (Add Printer Driver Wizard). Щелкните **Далее (Next)**.
4. Щелкните кнопку **Установить с диска (Have Disk)**, чтобы установить новый драйвер из файла или с диска.
5. В диалоговом окне **Установка с диска (Install From Disk)** введите путь к папке, содержащей драйвер принтера, или щелкните **Обзор (Browse)**, чтобы найти файл драйвера в диалоговом окне **Поиск файла (Locate File)**. Щелкните **OK**.
6. Щелкните **Далее (Next)** и **Готово (Finish)**.

Настройка драйверов для сетевых клиентов

Когда вы установили принтер и сменили драйвер, вам, возможно, понадобится указать операционные системы, которые должны загружать этот драйвер с сервера печати. Предоставляя клиентам возможность загружать драйвер с сервера, вы организуете единое расположение для установки обновлений драйверов. Таким образом, вместо того, чтобы устанавливать новый драйвер на все клиентские системы, вы устанавливаете его один раз — на сервере печати.

Чтобы разрешить клиентам загружать новый драйвер принтера, выполните следующие действия:

1. Щелкните правой кнопкой значок принтера, который хотите настроить, и выберите команду **Свойства (Properties)**.
2. Перейдите на вкладку **Доступ (Sharing)** и щелкните кнопку **Дополнительные драйверы (Additional Drivers)**.
3. В диалоговом окне **Дополнительные драйверы (Additional Drivers)** выберите ОС, из которой будет загружаться дополнительный драйвер. При необходимости вставьте компакт-диск Windows Server 2008, диск с драй-

верами принтера или оба диска. На компакт-диске Windows Server 2008 есть драйверы для большинства ОС Windows.

Установка страницы-разделителя и изменение режима устройства печати

В ОС Windows Server 2008 страницы-разделители применяются в двух целях:

- в начале задания, чтобы проще было найти документ среди других документов на принтере;
- для изменения режима работы устройства, в частности, языка, используемого принтером (PostScript или PCL).

Чтобы задать страницу-разделитель на устройстве печати, выполните следующие действия:

1. В диалоговом окне свойств принтера на вкладке **Дополнительно (Advanced)**, щелкните кнопку **Страница-разделитель (Separator Page)**.
2. В диалоговом окне **Страница-разделитель (Separator Page)** введите имя файла страницы разделителя. В основном, используются следующие файлы:
   - **Pcl.sep** Переводит устройство печати в режим PCL и печатает страницу-разделитель перед каждым документом.
   - **Pscript.sep** Переводит устройство печати в режим PostScript, но не печатает страницу-разделитель.
   - **Sysprint.sep** Переводит устройство печати в режим PostScript и печатает страницу-разделитель перед каждым документом.

Примечание Страница Sysprintj.sep — это вариант страницы Sysprint.sep. Если в системе имеются японские шрифты, и вы хотите ими воспользоваться, применяйте страницу Sysprintj.sep.

3. Чтобы отказаться от печати страницы-разделителя, откройте диалоговое окно **Страница-разделитель (Separator Page)** и удалите имя файла.

Примечание Если вы, работая на локальном сервере, щелкнете кнопку **Обзор (Browse)** в диалоговом окне **Страница-разделитель (Separator Page)**, откроется папка %SystemRoot%\Windows\System32. Здесь вы можете выбрать страницу-разделитель. При работе на удаленном сервере кнопка **Обзор (Browse)**, как правило, недоступна. В этом случае вам придется ввести точное имя файла страницы-разделителя.

Изменение порта принтера

Чтобы изменить порт, используемый устройством печати, воспользуйтесь диалоговым окном свойств принтера. Перейдите на вкладку **Порты (Ports)**. Здесь, чтобы задействовать порт для печати или удалить его, нужно установить или сбросить соответствующий флажок. Чтобы добавить новый тип порта, щелкните **Добавить порт (Add Port)**. В диалоговом окне **Порты принтера (Printer Ports)** выберите тип порта и щелкните **Новый порт (New**

Port). Введите имя порта и щелкните **OK**. Чтобы окончательно удалить порт, выделите его и щелкните **Удалить порт (Delete Port)**.

Расписание выполнения и приоритет заданий печати

Диалоговое окно свойств принтера позволяет задать стандартные параметры приоритета и расписания заданий печати. Перейдите на вкладку **Дополнительно (Advanced)**, показанную на рис. 18-8, и настройте стандартное расписание и параметры приоритета. О каждом из этих полей речь пойдет в следующих разделах.

График доступности принтера

Принтеры могут быть доступны всегда или только в определенные часы. Чтобы принтер был доступен всегда, на вкладке **Дополнительно (Advanced)** установите переключатель **Доступен всегда (Always Available)**. Чтобы указать допустимые часы работы, установите переключатель **Доступен с (Available From)**.

Установка приоритета

В поле **Приоритет (Priority)** вкладки **Дополнительно (Advanced)** задайте стандартный приоритет заданий. Выполнение заданий на печать всегда происходит в соответствии с приоритетом. Задания с более высоким приоритетом выполняются в первую очередь.

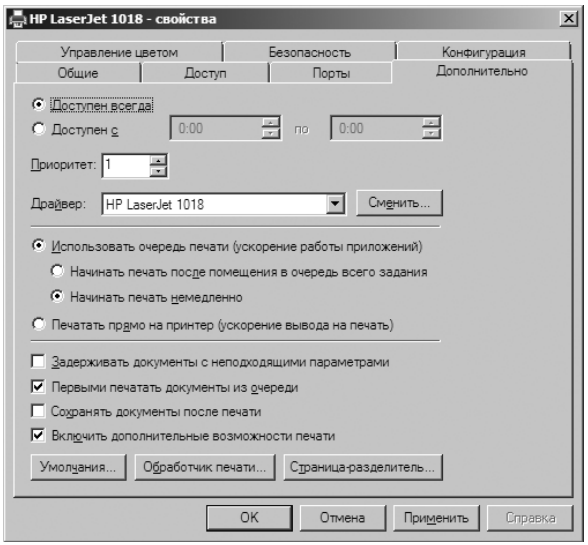


Рис. 18-8. Конфигурирование расписания и приоритета выполнения заданий на печать выполняется на вкладке Дополнительно (Advanced)

Настройка очереди печати

В устройствах печати, подключенных к сети, как правило, используется не прямая печать, а очередь, позволяющая управлять заданиями печати при помощи принтера.

Существует несколько возможностей включения очереди:

- **Использовать очередь печати (ускорение работы приложений) (Spool Print Documents So Program Finishes Printing Faster)** Установите этот переключатель, чтобы организовать очередь заданий.
- **Начинать печать после помещения в очередь всего задания (Start Printing After Last Page Is Spooled)** Загрузка в очередь всего документа до начала печати. Если по какой-либо причине печать отменяется или не может быть завершена, задание не будет напечатано.
- **Начинать печать немедленно (Start Printing Immediately)** Это переключатель позволяет начать печать немедленно, если устройство печати не используется. Эта позволяет оперативнее выполнять задания печати и быстрее возвращать управление приложением пользователю.

Чтобы отключить очередь печати, установите переключатель **Печатать прямо на принтер (Print Directly To The Printer)**. Настроить другие параметры очереди вам помогут дополнительные флажки:

- **Задерживать документы с неподходящими параметрами (Hold Mismatched Documents)** Принтер задерживает задания, не удовлетворяющие параметрам устройства печати. Этот параметр удобен, если вы часто меняете формат бумаги или используемый лоток.
- **Первыми печатать документы из очереди (Print Spooled Documents First)** Этот флажок позволяет печатать сначала помещенные в очередь документы, а затем документы, находящиеся в процессе помещения в очередь, независимо от приоритета заданий.
- **Сохранять документы после печати (Keep Printed Documents)** Обычно после выполнения печати документы удаляются из очереди. Чтобы сохранять копии документов на принтере, установите этот флажок. Эта возможность полезна при печати файлов, которые нелегко создать заново. Вы сможете повторно напечатать документ, не воссоздавая его. Подробнее — в разделе «Приостановка, возобновление и перезапуск печати отдельных документов» этой главы.
- **Включить дополнительные возможности печати (Enable Advanced Printing Features)** Данная опция позволяет использовать дополнительные возможности печати (если они есть), например, изменение порядка страниц или числа страниц на листе. Обнаружив проблемы при использовании дополнительных возможностей, отключите их, сбросив этот флажок.

Открытие и закрытие общего доступа к принтерам

Общий доступ к принтеру открывается в диалоговом окне его свойств. Щелкните правой кнопкой значок принтера, который хотите настроить, и выберите команду **Управление доступом (Manage Sharing)**. Диалоговое окно свойств принтера откроется на вкладке **Доступ (Sharing)**, где вы можете изменить имя сетевого принтера, а также открыть или прекратить об-

щий доступ к принтеру. Основные задачи по управлению общим доступом к принтеру таковы:

- **Открытие общего доступа к локальному принтеру** Чтобы открыть общий доступ к локальному принтеру (тем самым, принтер становится сетевым), установите флажок **Совместный доступ к принтеру (Share This Printer)** и укажите имя общего ресурса в поле **Сетевое имя (Share Name)**. Затем щелкните **OK**.
- **Изменение сетевого имени принтера** Чтобы изменить сетевое имя принтера, введите новое имя в поле **Сетевое имя (Share Name)** и щелкните **OK**.
- **Прекращение общего доступа к принтеру** Чтобы прекратить совместное использование принтера, сбросьте флажок **Совместный доступ к принтеру (Share This Printer)**. Затем щелкните **OK**.

Установка разрешений на доступ к принтеру

Сетевой принтер — это общий ресурс, и потому для него можно задать разрешения доступа. Для этого используется диалоговое окно свойств настраиваемого принтера, точнее, его вкладка **Безопасность (Security)**. Для принтеров можно предоставить или отозвать следующие разрешения: Печать (Print), Управление документами (Manage Documents) и Управление принтерами (Manage Printers). В табл. 18-2 содержится краткое описание этих разрешений.

Для каждого создаваемого принтера используются стандартные полномочия:

- Члены групп Администраторы (Administrators), Операторы печати (Print Operators) и Операторы сервера (Server Operators) по умолчанию имеют полный доступ к принтерам. Это позволяет администрировать принтер и его задания на печать.
- Создатель или владелец документа может управлять своим документом — изменять параметры документа и удалять его из очереди.
- Члены группы Все (Everyone) могут печатать на принтере. Это делает принтер доступным для всех пользователей сети.

Табл. 18-2. Разрешения принтера в Windows Server 2008

Разрешение	Печать (Print)	Управление документами (Manage Documents)	Управление принтерами (Manage Printers)
Печать документов	X	X	X
Приостановка, перезапуск, продолжение и отмена печати своих документов	X	X	X

Табл. 18-2. (*окончание*)

Разрешение	Печать (Print)	Управление документами (Manage Documents)	Управление принтерами (Manage Printers)
Подключение к принтерам	X	X	X
Управление параметрами заданий на печать		X	X
Приостановка, перезапуск и удаление заданий на печать		X	X
Предоставление общего доступа к принтерам			X
Изменение свойств принтера			X
Изменение разрешений принтера			X
Удаление принтера			X

Как и другие разрешения, базовые разрешения для принтеров создаются путем объединения особых разрешений в логические группы. В табл. 18-3 описаны особые разрешения, из которых формируются основные разрешения принтеров. При необходимости вы можете назначать особые разрешения индивидуально.

Табл. 18-3. Особые разрешения для принтеров

Особые полномочия	Печать (Print)	Управление документами (Manage Documents)	Управление принтерами (Manage Printers)
Печать (Print)	X		X
Управление документами (Manage Documents)		X	
Управление принтерами (Manage Printers)			X
Чтение разрешений (Read Permissions)	X	X	X
Смена разрешений (Change Permissions)		X	X
Смена владельца (Take Ownership)		X	X

Аудит заданий печати

Система Windows Server 2008 позволяет проводить аудит общих заданий печати. Выполните следующие действия:

1. Откройте диалоговое окно свойств принтера и перейдите на вкладку **Безопасность (Security)**. Щелкните кнопку **Дополнительно (Advanced)**, чтобы открыть диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)**.

Примечание Аудит действий не выполняется по умолчанию. Сначала вы должны включить аудит, настроив групповую политику аудита принтера.

2. На вкладке **аудит (Auditing)** при помощи кнопки **Добавить (Add)** добавьте имена пользователей или групп, аудит которых хотите проводить. Имена лишних пользователей или групп удалите при помощи кнопки **Удалить (Remove)**.
3. Выберите события аудита, установив флажки в столбцах **Успех (Successful)** и **Отказ (Failed)**.
4. Щелкните **OK**.

Установка стандартных параметров документов

Стандартные параметры документа используются только при печати из приложений, не входящих в состав Windows, например, при печати из строки MS-DOS. Чтобы установить параметры печати документов по умолчанию, выполните следующие действия:

1. Откройте диалоговое окно свойств принтера на вкладке **Общие (General)**.
2. Щелкните кнопку **Настройка печати (Printer Preferences)**.
3. Настройте стандартные параметры в открывшемся диалоговом окне.

Настройка свойств сервера печати

Система Windows Server 2008 позволяет управлять глобальными параметрами серверов печати с помощью диалогового окна **Свойства: Сервер печати (Print Server Properties)**. Открыть его можно одним из следующих способов:

- Откройте папку **Принтеры (Printers)** на сервере печати и выберите в меню **Файл (File)** команду **Свойства сервера (Server Properties)** или щелкните правой кнопкой свободную область окна и выберите команду **Свойства сервера (Server Properties)** в контекстном меню.
- В консоли **Управление печатью (Print Management)** щелкните правой кнопкой нужный сервер печати и выберите команду **Свойства (Properties)**. Если сервер отсутствует в списке, добавьте его при помощи диалогового окна **Добавление и удаление серверов (Add/Remove Servers)**: щелкните правой кнопкой элемент **Серверы печати (Print**

Servers) и выберите команду **Добавление и удаление серверов (Add/Remove Servers)**.

В следующих разделах рассмотрены некоторые свойства серверов печати.

Размещение папки Spool и включение печати в NTFS

Папка Spool содержит копии всех документов очереди принтера. По умолчанию она находится в папке %SystemRoot%\System32\Spool\PRINTERS. В файловой системе NTFS для доступа к принтеру все пользователи должны иметь разрешение Изменение (Change) для этой папки. Иначе они не смогут печатать документы.

При возникновении проблем проверьте разрешения для этой папки, выполнив следующие действия:

1. Откройте диалоговое окно **Свойства: Сервер печати (Print Server Properties)**.
2. Перейдите на вкладку **Дополнительные параметры (Advanced)**. Расположение папки Spool показано в поле **Папка очереди печати (Spool Folder)**. Запомните его.
3. Щелкните папку Spool правой кнопкой в окне Проводника Windows (Windows Explorer) и выберите команду **Свойства (Properties)**.
4. Перейдите на вкладку **Безопасность (Security)** и проверьте правильность предоставленных разрешений.

Управление массовой печатью

На принтерах, установленных в корпоративной среде, ежедневно печатаются сотни и тысячи документов. Большие объемы печати перегружают серверы и могут стать причиной задержек печати, повреждения документов и других проблем. Чтобы облегчить нагрузку на сервер печати, выполните следующие действия:

- Используйте принтеры, подключенные непосредственно к сети, вместо принтеров, подключенных через последовательные, параллельные, инфракрасные, а также USB-порты. Принтеры, подключенные по сети, потребляют меньше системных ресурсов, чем другие принтеры.
- Избавьте сервер печати от любых других обязанностей. Если сервер печати выполняет другие сетевые задачи, он может задерживать отклики на запросы печати и управления. Чтобы сократить время отклика, переместите прочие сетевые задачи на другие серверы.
- Переместите папку Spool на специальный диск. По умолчанию папка Spool находится в той же файловой системе, что и ОС. Для повышения эффективности ввода-вывода разместите ее на диске с отдельным контроллером.

Регистрация событий принтера

Настройка регистрации событий принтера выполняется в диалоговом окне **Свойства: Сервер печати (Print Server Properties)**. Перейдите на вкладку **Дополнительные параметры (Advanced)** и с помощью имеющихся флажков определите, какие события очереди следует регистрировать.

Включение уведомления об ошибке задания на печать

Серверы печати могут уведомлять пользователя о неудачной печати удаленного документа звуковым сигналом. По умолчанию эта функция выключена, т. к. некоторых она может раздражать. Чтобы активировать удаленное уведомление, откройте диалоговое окно **Свойства: Сервер печати (Print Server Properties)** и установите или сбросьте флажок **Звуковой сигнал при ошибках удаленной печати документов (Beep On Errors Of Remote Documents)** на вкладке **Дополнительные параметры (Advanced)**.

Управление заданиями на локальных и удаленных принтерах

Управление заданиями печати и принтерами осуществляется в окне управления печатью. Если принтер настроен в вашей системе, вы можете открыть окно управления печатью одним из следующих способов:

- Откройте папку Принтеры (Printers) на сервере печати. Дважды щелкните значок принтера, с которым вы хотите работать. Если принтер не настроен в вашей системе, им можно управлять удаленно. Для этого щелкните **Пуск (Start)**, затем — **Сеть (Network)**. Дважды щелкните значок сервера печати, с которым хотите работать, а затем дважды щелкните папку Принтеры (Printers) и значок нужного принтера.
- В окне консоли **Управление печатью (Print Management)** разверните узел **Серверы печати (Print Servers)**. Дважды щелкните элемент сервера печати. Выберите узел **Принтеры (Printers)**. Щелкните правой кнопкой нужный принтер и выберите **Открыть очередь печати (Open Printer Queue)**.
- В консоли **Управление печатью (Print Management)** щелкните правой кнопкой узел **Принтеры (Printers)** и выберите команду **Показать расширенное представление (Show Extended View)**.

Просмотр очередей и заданий печати

Для управления заданиями печати и принтерами используется окно управления печатью, показанное на рис. 18-9. В этом окне отображена информация о печатаемых документах, в том числе:

- **Документ (Document Name)** Имя документа; может включать имя приложения, из которого напечатан документ.
- **Состояние (Status)** Состояние задания, включающее состояние документа и состояние принтера.

- **Владелец (Owner)** Владелец документа
- **Число страниц (Pages)** Количество страниц в документе.
- **Размер (Size)** Размер документа, кб или Мб.
- **Поставлено в очередь (Submitted)** Время и дата поступления задания печати.
- **Порт (Port)** Порт, используемый для печати, например, LPT1, COM3, файл или IP-адрес (если есть).

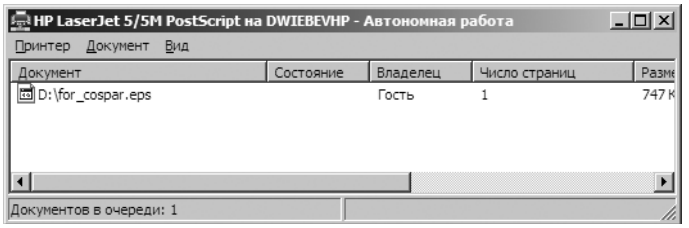


Рис. 18-9. Управление заданиями печати и принтерами в окне управления печатью

Приостановка принтера и продолжение печати

Иногда требуется приостановить принтер. В окне управления печатью для этого нужно выбрать в меню **Принтер (Printer)** или **Действие (Action)** команду **Приостановить печать (Pause Printing)**. О том, что печать уже приостановлена, свидетельствует галочка рядом с командой. Когда вы приостанавливаете принтер, он завершает текущее задание и замораживает выполнение других заданий.

Для возобновления печати выберите команду **Приостановить печать (Pause Printing)** еще раз. Галочка рядом с командой будет удалена.

Очистка очереди печати

Чтобы очистить очередь печати и удалить все ее содержимое в окне управления печатью, выберите в меню **Принтер (Printer)** или **Действие (Action)** команду **Очистить очередь печати (Cancel All Documents)**.

Приостановка, возобновление и перезапуск печати отдельных документов

В окне управления печатью состояние отдельных документов устанавливается в меню **Документ (Document)**. Чтобы изменить состояние документа, щелкните его правой кнопкой и выберите одну из следующих возможностей, чтобы изменить состояние задания:

- **Приостановить (Pause)** Приостанавливает печать документа и продолжает печать других документов.
- **Продолжить (Resume)** Сообщает принтеру, что следует продолжить печать документа с места приостановки.

- **Перезапустить (Restart)** Сообщает принтеру, что следует заново начать печать документа.

Удаление документа и отмена задания печати

Чтобы удалить документ из принтера или отменить задание печати, выделите документ в окне управления печатью, щелкните его правой кнопкой и выберите команду или нажмите клавишу Delete.

Примечание Когда вы отменяете задание на печать, выполняемое в данный момент, устройство печати может продолжить печатать документ полностью или частично. Это происходит из-за того, что устройства печати кешируют документы во внутренний буфер. Таким образом, устройство продолжает печатать содержимое документа из кеша.

Проверка свойств документов в принтере

Свойства документа могут многое рассказать о документах, находящихся в принтере, например, об источнике бумаги, ориентации и размере страницы. Чтобы проверить свойства документа в принтере, выполните одно из следующих действий:

- Щелкните правой кнопкой документ в окне управления печатью. В контекстном меню выберите команду **Свойства (Properties)**.
- В окне управления печатью дважды щелкните имя документа.

Установка приоритета отдельных документов

Приоритет определяет время печати документа. Документы с более высоким приоритетом выполняются в первую очередь. Чтобы задать приоритет отдельных документов в принтере, выполните следующие действия:

1. Щелкните правой кнопкой документ в окне управления печатью. В контекстном меню выберите команду **Свойства (Properties)**.
2. На вкладке **Общие (General)** с помощью бегунка измените приоритет документа. Значение наименьшего приоритета равно 1, наивысшего — 99.

Планирование печати отдельных документов

В загруженной среде печати полезно планировать печать документов на принтере. Например, печать больших заданий или заданий с низким приоритетом можно организовать ночью. Чтобы задать расписание печати, выполните следующие действия:

1. Щелкните правой кнопкой документ в окне управления печатью. В контекстном меню выберите команду **Свойства (Properties)**.
2. На вкладке **Общие (General)** установите переключатель **Только с (Only From)** и укажите временной интервал, когда можно выполнять печать. Например, можно задать выполнение печати только в промежутке между 24.00 и 5.00 часами.

Глава 19

Серверы и клиенты DHCP

Из этой главы вы узнаете о том, как протокол динамической настройки хоста DHCP облегчает администрирование доменов Active Directory. Протокол DHCP используется для динамического назначения сетевым клиентам параметров TCP/IP. Это экономит время и позволяет централизованно управлять обновлением конфигурации. Чтобы включить протокол DHCP в сети, требуется установить и настроить DHCP-сервер.

Протокол DHCP

Протокол DHCP позволяет централизовано управлять IP-адресами и не только ими. Установив DHCP, вы возлагаете на DHCP-сервер обязанности по предоставлению всей базовой информации для формирования сетей TCP/IP: IP-адресов, масок подсетей и адресов шлюзов, основных и альтернативных DNS-серверов, основных и альтернативных серверов WINS, а также DNS-имени домена. В Windows Server 2008 серверы DHCP способны назначать адреса IPv4 и IPv6 (или и те, и другие) любым сетевым адаптерам компьютера.

Динамическая адресация и настройка IPv4

Компьютер, использующий динамическую адресацию и настройку параметров протокола IPv4, называется клиентом DHCPv4. Во время загрузки DHCPv4-клиента, из пула IPv4-адресов, выделенного DHCP-серверу, извлекается 32-разрядный IPv4-адрес и назначается клиенту на определенный период времени, называемый сроком аренды. По истечении примерно половины срока аренды клиент пытается ее продлить. Если попытка не удалась, до истечения срока аренды клиент ее повторит. В случае неудачи клиент попытается связаться с другим DHCP-сервером. IPv4-адреса, аренда которых не продлена, возвращаются в пул адресов. Если клиенту удается связаться с сервером DHCP, но нет возможности продлить аренду текущего IP-адреса, DHCP-сервер назначает клиенту новый IPv4-адрес.

Доступность DHCP-сервера не влияет на запуск или вход в систему (в большинстве случаев). Запуск клиентов DHCPv4 и вход пользователей на локальный компьютер может выполняться, даже если DHCP-сервер не

доступен. Во время запуска клиент DHCPv4 производит поиск DHCP-сервера. Если DHCP-сервер доступен, клиент получает у него информацию о настройках. Если DHCP-сервер недоступен, но срок аренды еще не истек, клиент «пингует» основной шлюз, записанный в параметрах аренды. Успех операции свидетельствует, что клиент находится в той же сети, в которой он был на момент предоставления аренды. Клиент продолжает пользоваться арендой, как было описано ранее. Неудача команды ping говорит о том, что клиент находится в другой сети. В этом случае клиент использует автоматическую настройку IPv4. Она также используется, если DHCP-сервер не доступен, а срок предыдущей аренды истек.

Автоматическая настройка IPv4 работает следующим образом:

1. Клиентский компьютер выбирает IP-адрес из подсети класса B 169.254.0.0 с маской подсети 255.255.0.0, зарезервированной Майкрософт. Перед использованием IPv4-адреса клиент при помощи протокола ARP проверяет, что данный IPv4-адрес не занят другим клиентом.
2. Если адрес занят, клиент повторяет шаг 1. После десяти неудачных попыток произойдет ошибка. Если клиент отключен от сети, результат ARP-тестирования всегда будет успешным, поэтому клиент получит первый попавшийся IPv4-адрес.
3. Если выбранный IPv4-адрес доступен, клиент соответствующим образом настраивает сетевой адаптер. Далее, клиент пытается связаться с DHCP-сервером, каждые пять минут посылая в сеть запрос. После успешной установки связи клиента с сервером, клиент получает аренду и заново настраивает сетевой интерфейс.

Динамическая адресация и настройка IPv6

Если в процессе установки Microsoft Windows Vista и Windows Server 2008 на компьютере обнаружено сетевое оборудование, по умолчанию включаются оба протокола (IPv4 и IPv6). Как уже говорилось в главах 1 и 17, протокол IPv4 представляет собой первую версию протокола IP и используется в большинстве сетей, а IPv6 представляет собой следующее поколение протокола IP. В протоколе IPv6 используются 128-разрядные адреса. В стандартной конфигурации первые 64 бита — это идентификатор сети, а последние 64 бита — сетевой интерфейс на клиентском компьютере.

Существует два основных способа настройки IPv6 посредством DHCP:

- **Режим с отслеживанием состояния (Stateful)** DHCPv6-клиенты получают IPv6-адреса и параметры настройки сети от DHCPv6-сервера.
- **Режим без отслеживания состояния (Stateless)** DHCPv6-клиенты получают IP-адреса при помощи автоматической настройки, а параметры сетевой конфигурации — при помощи DHCPv6.

Компьютер, получающий от DHCPv6-сервера IPv6-адрес и (или) сетевые настройки, называется DHCPv6-клиентом. Как и в случае DHCPv4, инфраструктура DHCPv6 состоит из DHCPv6-клиентов, запрашивающих

параметры, DHCPv6-серверов, предоставляющих параметры, и агентов-ретрансляторов DHCPv6, которые обеспечивают обмен данными между клиентами и серверами, когда клиенты находятся в подсетях, не имеющих DHCPv6-сервера.

В отличие от DHCPv4, для поддержки DHCPv6 вам придется настроить IPv6-маршрутизаторы. В основе автоматической настройки DHCPv6 лежат следующие флаги в сообщении, посылаемом ближайшим маршрутизатором:

- **Флаг *Managed Address Configuration* (флаг M)** Если этот флаг имеет значение 1, он предписывает клиенту использовать протокол для получения адресов с отслеживанием состояния.
- **Флаг *Other Stateful Configuration* (флаг O)** Если этот флаг имеет значение 1, он предписывает клиенту использовать протокол для получения других параметров.

Клиент DHCPv6 имеется и в Window Vista, и в Windows Server 2008. Он выстраивает конфигурацию на основе DHCPv6 в зависимости от значений флагов M и O в объявлениях маршрутизатора. Если в данной сети несколько объявляющих маршрутизаторов, их следует настроить так, чтобы для флагов M и O объявлялись одинаковые значения и префиксы адреса без отслеживания состояния. У клиентов IPv6 под управлением Windows XP или Windows Server 2003 нет DHCPv6-клиента, поэтому они игнорируют флаги M и O в объявлениях маршрутизаторов.

Вы можете настроить маршрутизатор IPv6, работающий под управлением Windows Vista или Windows Server 2008, на установку в объявлениях значения 1 для флага M. Для этого в командной строке с повышенными полномочиями нужно ввести команду **netsh interface ipv6 set interface *ИмяИнтерфейса* managedaddress=enabled**, где *ИмяИнтерфейса* — фактическое имя интерфейса. Аналогичным способом можно установить значение 1 для флага O в объявлениях, введя в командной строке с повышенными полномочиями команду **netsh interface ipv6 set interface *ИмяИнтерфейса* otherstateful=enabled**. Если в имени интерфейса присутствуют пробелы, его следует заключить в кавычки, как в следующем примере:

```
netsh interface ipv6 set interface “Connection 2” managedaddress=enabled
```

Работая с флагами M и O, помните о следующем:

- Если оба флага имеют значение 0, считается, что в сети нет инфраструктуры DHCPv6. Клиенты используют объявления маршрутизатора для настройки нелокальных адресов и ручную настройку других параметров.
- Если оба флага имеют значение 1, DHCPv6 используется для назначения как IP-адресов, так и других параметров конфигурации. Эта комбинация известна, как режим с отслеживанием состояния, при котором DHCPv6 назначает IPv6-клиентам адреса.
- Если значение флага M равно 0, а значение флага O — 1, DHCPv6 используется только для назначения прочих параметров конфигурации. Соседние

маршрутизаторы настроены на объявление префиксов нелокальных адресов, из которых клиенты IPv6 получают адреса без отслеживания состояния. Эта комбинация известна как режим без отслеживания состояния.

- Если значение флага M равно 1, а значение флага O — 0, DHCPv6 используется для настройки IP-адресов, но не других параметров. Поскольку IPv6-адреса следует, как правило, настраивать вместе с другими параметрами, например, IPv6-адресами DNS-серверов, данная комбинация используется редко.

Системы Windows Vista и Windows Server 2008 получают динамические IPv6-адреса примерно так же, как и адреса IPv4. Обычно автоматическая настройка IPv6 для клиентов DHCPv6 в режиме с отслеживанием состояния происходит так:

1. Клиентский компьютер получает индивидуальный локальный IPv6-адрес с отслеживанием состояния. Перед использованием IPv6-адреса клиент при помощи ARP проверяет, что данный IPv6-адрес не используется другим клиентом.
2. Если адрес занят, клиент повторяет шаг 1. Помните, что если клиент отключен от сети, результат ARP-тестирования всегда успешный. Поэтому клиент получает первый попавшийся IPv6-адрес.
3. Если выбранный IPv6-адрес доступен, клиент соответствующим образом настраивает сетевой адаптер. Далее клиент пытается связаться с DHCP-сервером, каждые пять минут посылая в сеть запрос. После успешной установки связи клиента с сервером клиент получает аренду и заново настраивает сетевой интерфейс.

Иначе работает автоматическая настройка параметров IPv6 на клиентах DHCPv6 в режиме без отслеживания состояния. В этом случае клиенты DHCPv6 настраивают как локальные адреса, так и дополнительные нелокальные адреса, обмениваясь запросами и объявлениями с соседними маршрутизаторами.

Как и в случае DHCPv4, в протоколе DHCPv6 используются сообщения UDP. Клиенты DHCPv6 принимают сообщения на UDP-порт 546. Серверы и агенты-ретрансляторы DHCPv6 принимают сообщения на UDP-порт 547. Структура сообщений DHCPv6 намного проще, чем структура сообщений DHCPv4 — наследника протокола BOOTP, который служит для поддержки бездисковых рабочих станций.

Сообщения DHCPv6 начинаются с 1-байтового поля *Msg-Type* (тип сообщения). Далее следует 3-байтовое поле *Transaction-ID*, определяемое клиентом и служащее для группирования сообщений DHCPv6. За полем *Transaction-ID* следуют параметры DHCPv6 — идентификаторы сервера и клиента, адреса и прочие параметры. С каждым параметром DHCPv6 связано три поля. Поле *Option-Code* (2 байта) идентифицирует параметр. Поле *Option-Len* (2 байта) указывает на длину поля *Option-Data* в байтах. Поле *Option-Data* содержит данные соответствующего параметра.

Иную структуру имеют сообщения, пересылаемые между агентами-ретрансляторами и серверами. Поле *Hop-Count* (1 байт) указывает на количество агентов-ретрансляторов, получивших сообщение. Агент, получивший сообщение, может отбросить его, если значение счетчика переходов превысило заданный предел. Поле *Link-Address* (16 байт) содержит нелокальный адрес интерфейса, подключенному к подсети, в которой расположен клиент. На основе информации из поля *Link-Address* сервер устанавливает корректный диапазон, из которого следует извлекать адрес. Поле *Peer-Address* (16 байт) содержит IPv6-адрес клиента, пославшего сообщение, или агента, ретранслировавшего это сообщение. За полем *Peer-Address* следуют параметры DHCPv6. Основной параметр Relay Message обеспечивает инкапсуляцию сообщений, передаваемых между клиентом и сервером.

У протокола IPv6 нет широковещательных адресов. На смену широковещательному адресу, используемому в некоторых сообщениях DHCPv4, в DHCPv6 пришел адрес All_DHCP_Relay_Agents_and_Servers, значение которого равно FF02::1:2. Чтобы обнаружить расположение DHCPv6-сервера в сети, клиент DHCPv6 отправляет запрос со своего локального адреса. Если в подсети клиента есть DHCPv6-сервер, он получает запрос и отправляет соответствующий ответ. Если клиент и сервер находятся в различных подсетях, агент-ретранслятор DHCPv6 в подсети клиента, который получает запрос, перешлет его на DHCPv6-сервер.

Проверка назначений IP-адресов

Для проверки текущих IP-адресов и прочей информации используется команда IPCONFIG. Чтобы получить информацию обо всех имеющихся на компьютере сетевых адаптерах, введите в командной строке **ipconfig /all** . Если IP-адрес присваивается автоматически, вы увидите пункт Автонастройка IP-адреса (Autoconfiguration IP Address). В этом примере автоматически настраиваемый IPv4-адрес — 169.254.98.59:

```
Настройка протокола IP для Windows

   Имя компьютера.................: DELTA
   Основной DNS-суффикс...........: microsoft.com
   Тип узла.......................: Гибридный
   IP-маршрутизация включена......: Нет
   WINS-прокси включен............: Нет
   Порядок просмотра суффиксов DNS.: microsoft.com

Ethernet adapter Подключение по локальной сети:
   DNS-суффикс подключения.........:
   Описание.......................: Intel Pro/1000 Network Connection
   Физический адрес...............: 23-17-C6-F8-FD-67
   DHCP включен...................: Да
   Автонастройка включена.........: Да
   Автонастройка IPv4-адреса:.....: 169.254.98.59
```

```
Маска подсети.....................: 255.255.0.0
Основной шлюз.....................:
DNS-серверы.......................:
```

Области адресов

Области (scope) адресов — это пулы IPv4 и IPv6-адресов, которые могут арендовать клиенты. Протокол DHCP также позволяет предоставлять адреса в бессрочную аренду. Чтобы зарезервировать конкретный IPv4-адрес, свяжите его с MAC-адресом компьютера, которому должен назначаться этот IPv4-адрес. Впоследствии клиентский ПК с указанным MAC-адресом будет всегда получать заданный IPv4-адрес. В протоколе IPv6 резервирование осуществляется посредством указания бессрочной аренды.

Области создаются, чтобы определить диапазоны IP-адресов, доступных DHCP-клиентам. Например, вы можете назначить диапазон IP-адресов от 192.168.12.2 до 192.168.12.250 для области Enterprise Primary. В областях допускается использование открытых или частных IPv4-адресов в следующих сетях:

- Сети класса A IP адреса в диапазоне от 1.0.0.0 до 126.255.255.255
- Сети класса B IP-адреса в диапазоне от 128.0.0.0 до 191.255.255.255
- Сети класса C IP-адреса в диапазоне от 192.0.0.0 до 223.255.255.255
- Сети класса D IP-адреса в диапазоне от 224.0.0.0 до 239.255.255.255

Примечание Адрес IP 127.0.0.1 используется для замыкания на себя.

В областях можно также использовать локальные одноадресные IPv6-адреса, глобальные одноадресные и многоадресные IPv6-адреса. Локальные одноадресные адреса начинаются с FE80. Многоадресные адреса начинаются с FF00. Глобальные (в пределах сайта) индивидуальные адреса включают все остальные адреса за исключением :: (не определено) и ::1 (замыкание на себя).

Один DHCP-сервер может управлять несколькими областями. Для IPv4-адресов доступно три типа областей:

- **Обычные области (normal scope)** Используются для назначения адресов в сетях классов A, B и C.
- **Многоадресные области (multicast scope)** Используются для назначения IP-адресов в сетях IPv4 класса D. Многоадресные IP-адреса применяются в качестве второстепенных, в дополнение к стандартным IP-адресам.
- **Суперобласти** Это контейнеры для других областей, которые упрощают управление несколькими областями.

В IPv6 доступны только обычные области. Хотя можно создавать области, охватывающие несколько сегментов сети, обычно эти сегменты принадлежат к одному классу сети, например, к классу C.

Совет Не забудьте настроить ретрансляторы DHCPv4 и DHCPv6 для передачи широковещательных запросов DHCPv4 и DHCPv6 между сегментами сети. Агенты-ретрансляторы можно настроить при помощи службы маршрутизации и удаленного доступа (RRAS) и службы агента-ретранслятора DHCP. Для использования в качестве агентов-ретрансляторов можно также настроить некоторые маршрутизаторы.

Установка DHCP-сервера

Динамическое назначение IP-адресов возможно лишь в том случае, когда в сети установлен DHCP-сервер. Мастер добавления ролей (Add Roles Wizard) позволяет установить роль DHCP-сервера, настроить его начальные параметры и авторизовать сервер в Active Directory. Только авторизованные DHCP-серверы могут предоставлять клиентам динамические IP-адреса.

Установка компонентов DHCP

Чтобы настроить сервер под управлением Microsoft Windows Server 2008 в качестве DHCP-сервера, выполните следующие действия:

1. Серверу DHCP должны быть назначены статические IPv4 или IPv6-адреса в каждой обслуживаемой ими подсети. Убедитесь, что у сервера есть статические IPv4 или IPv6-адреса.
2. В консоли **Диспетчер сервера (Server Manager)** выделите узел **Роли (Roles)** и щелкните команду **Добавить роли (Add Roles)**. Откроется Мастер добавления ролей (Add Roles Wizard). Если работа мастера начинается с вводной страницы, ознакомьтесь с ее содержимым и щелкните **Далее (Next)**.
3. На странице **Выбор ролей сервера (Select Server Roles)** установите флажок **DHCP-сервер (DHCP Server)** и два раза щелкните **Далее (Next)**.
4. На странице **Выбор привязки сетевого подключения (Network Bindings)** выведен список сетевых подключений со статическими IPv4-адресами. Выберите сетевые подключения, при помощи которых сервер будет обслуживать DHCPv4-клиентов, и щелкните **Далее (Next)**.
5. На странице **Указать параметры IPv4 DNS-сервера (Specify IPv4 DNS Server Settings)**, показанной на рис. 19-1, введите стандартные параметры DNS, которые сервер будет передавать DHCPv4-клиентам для автоматической настройки DNS. В поле **Родительский домен (Parent Domain)** введите DNS-имя родительского домена, например, **cpandl.com**. В поля **IPv4-адрес основного DNS-сервера (Preferred DNS Server)** и **IPv4-адрес дополнительного DNS-сервера (Alternate DNS Server)** введите IPv4-адреса основного и альтернативного DNS-серверов. Щелкните кнопку **Проверить (Validate)**, чтобы проверить правильность ввода DNS-адреса. Затем щелкните **Далее (Next)**.
6. На странице **Задать параметры IPv4 WINS-сервера (Specify IPv4 WINS Server Settings)** укажите, требуется ли служба WINS для приложений в сети. Если она нужна, введите IP-адреса основного и дополнительного WINS-серверов в поля **IP-адрес основного WINS-сервера (Preferred WINS Server)** и **IP-адрес дополнительного WINS-сервера (Alternate WINS Server)**. Затем щелкните **Далее (Next)**.

Ближе к реальности В Windows Server 2008 сервер WINS является компонентом и устанавливается при помощи Мастера добавления компонентов (Add Features Wizard). Если в вашей сети нет приложений или систем, предшествующих Windows 2000, служба WINS вам не нужна. Вместо нее для однорангового разрешения имен устройств с IPv4 и (или) IPv6-адресами можно воспользоваться службой LLMNR (Link-Local Multicast Name Resolution). Чтобы включить LLMNR, требуется установить компонент Протокол PNRP (Peer Name Resolution Protocol).

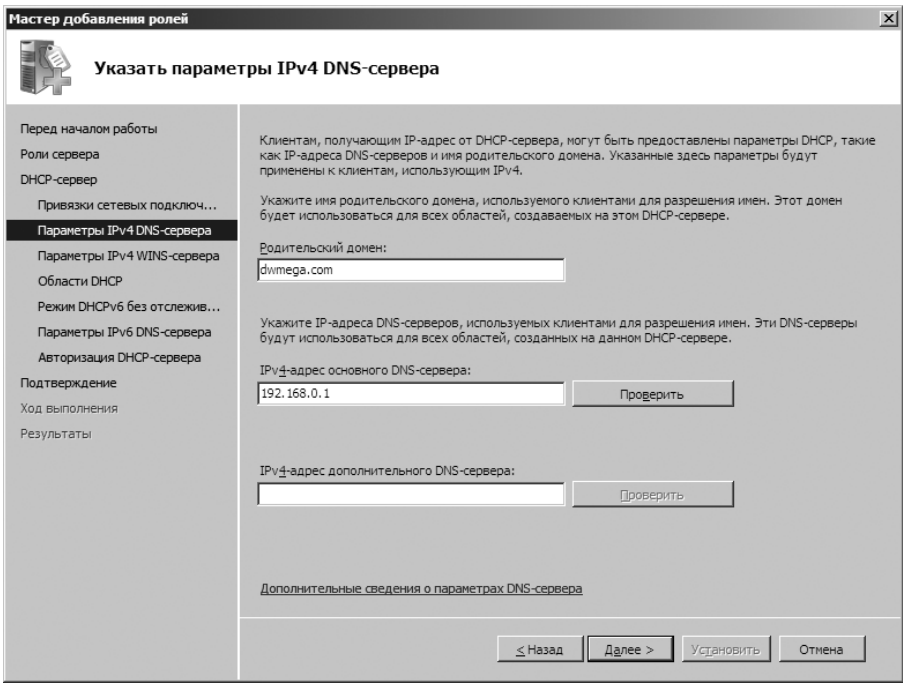


Рис. 19-1. Настройка стандартных параметров DNS для DHCPv4-клиентов

7. На странице **Добавление или изменение DHCP-областей (Add Or Edit Scopes)** создайте первоначальные области для DHCP-сервера, щелкнув кнопку **Добавить (Add)** и выполнив действия, описанные в разделе «Создание областей и управление ими» этой главы. Если вы намерены создать необходимые области DHCP позднее, щелкните **Далее (Next)**.
8. На странице **Настроить режим DHCPv6 без отслеживания состояния (Configure DHCPv6 Stateless Mode)** укажите, нужно ли включить режим без отслеживания состояния. Если вы хотите, чтобы DHCPv6-клиенты получали IPv6-адреса и параметры конфигурации от DHCPv6, отключите этот режим. Если вы включите режим без отслеживания состояния, клиенты будут получать через DHCPv6 только параметры конфигурации. Щелкните **Далее (Next)**.
9. На странице **Укажите параметры DNS-сервера IPv6 (Specify IPv6 DNS Server Settings)**, показанной на рис. 19-2, введите стандартные параметры DNS, которые сервер будет передавать DHCPv6-клиентам. В поле

Родительский домен (Parent Domain) введите DNS-имя родительского домена, например, **cpandl.com**. В поля **IPv6-адрес основного DNS-сервера (Preferred DNS Server)** и **IPv6-адрес основного DNS-сервера (Alternate DNS Server)** введите IPv6-адреса основного и альтернативного DNS-серверов. Щелкните кнопку **Проверить (Validate)**, чтобы проверить введенный адрес. Затем щелкните **Далее (Next)**.

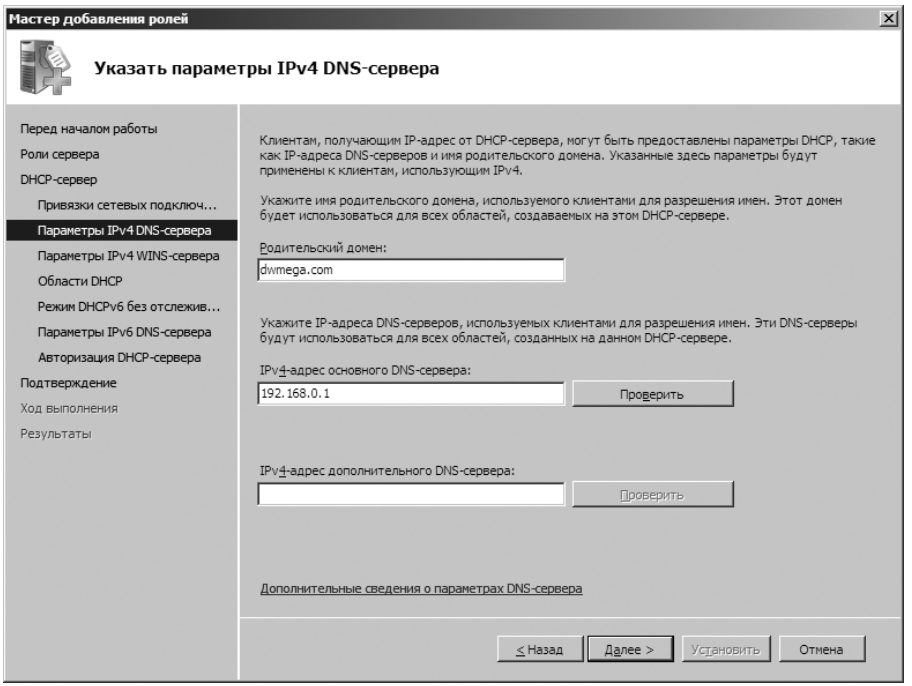


Рис. 19-2. Настройка стандартных параметров DNS для DHCPv6-клиентов

10. На странице Авторизация DHCP-сервера (Authorize DHCP Server) задайте учетные данные для авторизации DHCP-сервера в Active Directory:
    - В поле **Имя пользователя (User Name)** отображено текущее имя пользователя. Если вы обладаете административными полномочиями в домене, членом которого является DHCP-сервер, щелкните **Далее (Next)**, чтобы авторизовать сервер при помощи текущих учетных данных.
    - Если вам не удалось авторизовать сервер при помощи текущих учетных данных или вы хотите воспользоваться другими учетными данными, установите переключатель **Использовать другие учетные данные (Use Alternate Credentials)** и щелкните **Указать (Specify)**. В диалоговом окне **Безопасность Windows (Windows Security)** введите имя пользователя и пароль нужной учетной записи и щелкните **OK**. Затем щелкните **Далее (Next)**.
    - Чтобы авторизовать DHCP-сервер позднее, установите переключатель **Пропустить авторизацию этого DHCP-сервера в AD DS (Skip Autho-**

rization) и щелкните **OK**. Помните, что предоставлять клиентам динамические IP-адреса могут только авторизованные DHCP-серверы.

11. Щелкните **Установить (Install)**. Мастер приступит к установке и настройке сервера. Чтобы сервер заработал, его нужно авторизовать в домене, о чем пойдет речь в разделе «Авторизация DHCP-сервера в Active Directory» этой главы. Вы также должны создать и активировать области DHCP, с которыми будет работать сервер. Подробнее — в разделе «Создание областей и управление ими» этой главы.

Работа в консоли DHCP

После установки DHCP-сервера настройка и управление динамической IP-адресацией происходит в консоли DHCP. Чтобы открыть ее, щелкните **Пуск (Start)**, **Администрирование (Administrative Tools)** и **DHCP**. Главное окно консоли **DHCP** показано на рис. 19-3. На его левой панели перечислены DHCP-серверы домена. Развернув узел сервера, вы увидите подузлы **IPv4** и **IPv6**. Развернув их, вы получите доступ к возможностям соответствующей версии IP. На правой панели отображается развернутый вид выбранного элемента.

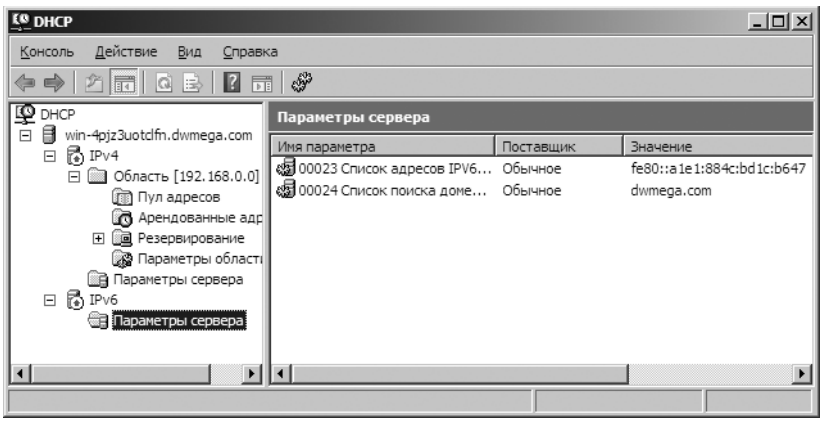


Рис. 19-3. Консоль DHCP используется для управления DHCP-сервером

Значки на узлах отображают их текущее состояние. На узлах сервера и протокола IP могут отображаться следующие значки:

- Зеленая стрелка вверх указывает, что служба DHCP работает и сервер активен.
- Красный крестик указывает, что консоль не может подключиться к серверу. Служба DHCP остановлена или сервер недоступен.
- Красная стрелка вниз указывает, что DHCP-сервер не авторизован.
- Синий значок предупреждения указывает на изменение в состоянии сервера.

На элементах областей могут отображаться следующие значки:

- Красная стрелка вниз указывает, что область не включена.
- Синий значок предупреждения указывает на изменение в состоянии области.

Подключение к удаленным DHCP-серверам

Открыв консоль **DHCP**, вы подключаетесь к локальному DHCP-серверу. Элементы удаленных DHCP-серверов не отображаются. Для подключения к удаленным серверам выполните следующие действия:

1. Щелкните правой кнопкой элемент **DHCP** в дереве консоли и выберите команду **Добавить сервер (Add Server)**. Откроется диалоговое окно, показанное на рис. 19-4.

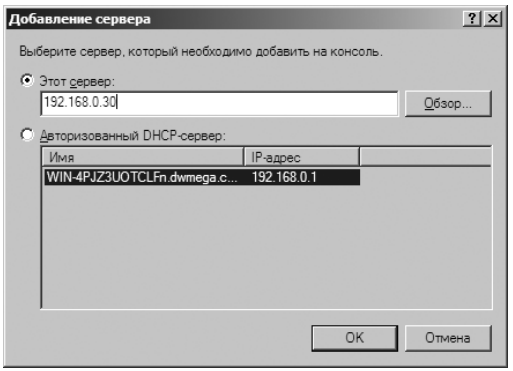


Рис. 19-4. Если в списке отсутствует нужный DHCP-сервер, добавьте в консоль DHCP

2. Установите переключатель **Этот сервер (This Server)** и введите IP-адрес или имя компьютера, на котором установлен нужный DHCP-сервер.
3. Щелкните **OK**. Сервер DHCP будет добавлен в дерево консоли.

Совет При работе с удаленными серверами некоторые возможности могут быть недоступны. Решить проблему позволяет обновление информации о сервере: щелкните правой кнопкой узел сервера и выберите команду **Обновить (Refresh)**.

Запуск и остановка DHCP-сервера

Управление DHCP-серверами осуществляется при помощи службы DHCP-сервер (DHCP Server). Как и любую другую службу, ее можно запустить, остановить, приостановить и перезапустить в узле **Конфигурация\Службы (Configuration\Services)** консоли **Диспетчер сервера (Server Manager)** или из командной строки. Кроме того, службой DHCP-сервер (DHCP Server) можно управлять в консоли **DHCP**. Щелкните правой кнопкой сервер, которым хотите управлять, разверните подменю **Все задачи (All Tasks)** и выберите нужную команду: **Запустить (Start)**, **Остановить (Stop)**, **Приостановить (Pause)**, **Продолжить (Resume)** или **Перезапустить (Restart)**.

Примечание Чтобы запустить или остановить DHCP-сервер в консоли **Диспетчер сервера (Server Manager)**, разверните узлы **Роли (Roles)** и **DHCP-сервер (DHCP Server)**. Щелкните сервер правой кнопкой, разверните подменю **Все задачи (All Tasks)** и выберите нужную команду: **Запустить (Start)**, **Остановить (Stop)**, **Приостановить (Pause)**, **Продолжить (Resume)** или **Перезапустить (Restart)**.

Авторизация DHCP-сервера в Active Directory

Прежде чем использовать DHCP-сервер в домене, вы должны авторизовать его в Active Directory. Авторизация сервера означает, что серверу разрешено назначать динамические IP-адреса в домене. В Windows Server 2008 авторизация требуется для предотвращения обслуживания клиентов неавторизованными DHCP-серверами.

Чтобы авторизовать DHCP-сервер, щелкните правой кнопкой элемент сервера в дереве консоли **DHCP** и выберите команду **Авторизовать (Authorize)**. Чтобы лишить сервер авторизации, щелкните его правой кнопкой и выберите команду **Запретить (Unauthorize)**.

Примечание Чтобы авторизовать DHCP-сервер в консоли **Диспетчер сервера (Server Manager)**, разверните узлы **Роли (Roles)** и **DHCP-сервер (DHCP Server)**, щелкните сервер правой кнопкой и выберите команду **Авторизовать (Authorize)**. Наберитесь терпения — процесс авторизации может занять несколько минут. Нажмите клавишу **F5**, чтобы обновить представление. Если DHCP-сервер авторизован, в дереве консоли будет отображена зеленая стрелка вверх. Чтобы отменить авторизацию, разверните узлы **Роли (Roles)** и **DHCP-сервер (DHCP Server)**, щелкните сервер правой кнопкой и выберите команду **Запретить (Unauthorize)**.

Совет Возможно, для авторизации DHCP-сервера в Active Directory вам придется выполнить войти на контроллер домена или подключиться к нему удаленно. Получив доступ к контроллеру домена, откройте консоль DHCP и подключитесь к серверу, который хотите авторизовать. Щелкните сервер правой кнопкой и выберите команду **Авторизовать (Authorize)**.

Настройка DHCP-сервера

В процессе установки DHCP-сервера возможности настройки IP автоматически оптимизируются для данного сетевого окружения. Возможности протоколов PIv4 и IPv6 различны. Как правило, менять эти параметры не нужно, если вы испытываете проблем с производительностью. Если же проблемы возникли, вам, возможно, придется добавить или удалить некоторые возможности.

Привязка DHCP-сервера с несколькими сетевыми адаптерами к конкретному IP-адресу

На сервере с несколькими сетевыми адаптерами имеется несколько подключений по локальной сети, по каждому из которых он может предоставлять параметры DHCP. Иногда работа DHCP на всех доступных подключениях вам не требуется. Допустим, на сервере имеется два подключения — 100 Мбит/с и 1000 Мбит/с. Трафик DHCP лучше пропускать через подключение со скоростью 1000 Мбит/с.

Чтобы связать DHCP с конкретным подключением, выполните следующие действия:

1. В консоли DHCP разверните узел сервера, с которым хотите работать. Щелкните правой кнопкой узел **IPv4** или **IPv6** и выберите **Свойства (Properties)**.
2. В диалоговом окне свойств IPv4 или IPv6 перейдите на вкладку **Дополнительно (Advanced)** щелкните кнопку **Привязки (Bindings)**.
3. В диалоговом окне **Привязки (Bindings)** отображен список доступных сетевых подключений DHCP-сервера. Чтобы DHCP-сервер использовал подключение, установите соответствующий флажок. Чтобы служба не использовала подключение, сбросьте соответствующий флажок.
4. Два раза щелкните **OK**.

Обновление статистики DHCP

В консоли **DHCP** представлена статистика доступности и использования адресов IPv4 и IPv6. По умолчанию обновление статистики происходит только запуске консоли DHCP, а также если выбрать сервер и щелкнуть кнопку **Обновить (Refresh)** на панели инструментов. Если вы хотите постоянно следить за DHCP, вам потребуется автоматическое обновление статистики. Чтобы настроить его, выполните следующие действия:

1. В консоли DHCP разверните узел нужного сервера. Щелкните правой кнопкой узел **IPv4** или **IPv6** и выберите команду **Свойства (Properties)**.
2. На вкладке **Общие (General)** установите флажок **Автоматически обновлять статистику каждые (Automatically Update Statistics Every)** и введите интервал обновления в часах и минутах. Щелкните **OK**.

Аудит и устранение неисправностей DHCP

По умолчанию в Windows Server 2008 настроен аудит DHCP-процессов с записью информации в журналы.

Аудит DHCP

В устранении неисправностей DHCP-сервера вам помогут журналы аудита. По умолчанию оба протокола — IPv4 и IPv6 — производят запись в одни и те же журналы, но вы вольны настроить и раздельный аудит. Стандартное расположение журналов DHCP — %SystemRoot%\System32\DHCP. В этой папке помещены журналы для каждого дня недели. Файл журнала понедельника называется DhcpSrvLog-Mon.log, файл журнала вторника — DhcpSrvLog-Tue.log и т. д.

При запуске DHCP-сервера или наступлении нового дня в файл журнала записывается заголовок. В заголовке содержится сводка событий DHCP и значение событий. При остановке и запуске службы DHCP-сервер (DHCP Server) очистка файла журнала может не произойти. Она обязательно происходит по прошествии 24 часов с момента последней записи в журнал. Вам не нужно отслеживать использование дискового пространства службой DHCP-сервер (DHCP Server). Она по умолчанию настроена на ограничение используемого пространства.

Включение и отключение аудита DHCP

Чтобы включить или отключить аудит DHCP, выполните следующие действия:

1. В консоли DHCP разверните узел нужного сервера. Щелкните правой кнопкой узел **IPv4** или **IPv6** и выберите **Свойства (Properties)**.
2. На вкладке **Общие (General)** установите или сбросьте флажок **Вести журнал аудита DHCP (Enable DHCP Audit Logging)**. Щелкните **OK**.

Изменение расположения журналов аудита DHCP

По умолчанию журналы DHCP хранятся в папке %SystemRoot%\System32\DHCP. Чтобы изменить расположение журналов DHCP, выполните следующие действия:

1. В консоли DHCP разверните узел нужного сервера. Щелкните правой кнопкой узел **IPv4** или **IPv6** и выберите **Свойства (Properties)**.
2. Перейдите на вкладку **Дополнительно (Advanced)**. В поле **Журнал аудита (Audit Log File Path)** отображен текущий путь папки с файлами журналов. Введите новое расположение или укажите его при помощи кнопки **Обзор (Browse)**.
3. Щелкните **OK**. Системе Windows Server 2008 потребуется перезапустить службу DHCP-сервер (DHCP Server). Щелкните **Да (Yes)**, чтобы подтвердить действие. Служба будет остановлена и заново запущена.

Изменение используемого журналом пространства

В службе DHCP-сервер (DHCP Server) имеется система самоконтроля, проверяющая использование дискового пространства. По умолчанию максимальный размер всех журналов DHCP-сервера составляет 70 Мб. Размер каждого журнала составляет одну седьмую часть от этого пространства. При достижении сервером предела в 70 Мб или при превышении отдельным журналом выделенного для него пространства регистрация деятельности DHCP прекращается, пока не будут очищены файлы журналов или место не освободится каким-либо иным способом. Обычно это происходит в начале нового дня, когда сервер очищает файл журнала прошлой недели.

Параметры реестра, регулирующие объем журнала и другие параметры DHCP, находятся в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters.

Следующие параметры управляют регистрацией событий:

- **DhcpLogFilesMaxSize** Максимальный размер всех журналов. Стандартное значение — 70 Мб.
- **DhcpLogDiskSpaceCleanupInterval** Частота проверки использования диска и очистки журнала. Стандартный интервал — 60 мин.
- **DhcpLogMinSpaceOnDisk** Порог свободного пространства, необходимый для записи в журнал. Если свободное пространство на диске меньше установленного значения, запись в журнал временно прекращается. Стандартное значение — 20 Мб.

Параметр *DhcpLogMinSpaceOnDisk* не создается автоматически. Вы должны сами создать его и задать подходящее для вашей сети значение.

Интеграция DHCP и DNS

Служба DNS предназначена для разрешения имен компьютеров в доменах Active Directory и в Интернете. Благодаря протоколу динамического обновления DNS, вы избавлены от необходимости регистрировать DHCP-клиентов в DNS вручную. Протокол позволяет клиенту или DHCP-серверу при необходимости регистрировать в DNS записи прямого и обратного просмотра. При работе DHCP по стандартной схеме DHCP-клиенты Windows Server 2008 автоматически обновляют соответствующие DNS-записи после получения IP-адреса в аренду. Записи клиентов, работающих в предыдущих версиях Windows, после предоставления аренды обновляет DHCP-сервер. Вы можете изменить этот порядок для DHCP-сервера в целом или для конкретной области.

Совет Серверы DNS под управлением Microsoft Windows NT 4.0 не поддерживают протокол динамического обновления, и записи не обновляются автоматически. Один из способов разрешения проблемы — включить WINS для DHCP-клиентов, использующих NetBIOS. Это позволит клиенту находить другие компьютеры посредством WINS. Более надежное решение — обновить DNS-серверы до Windows Server 2008.

Чтобы просмотреть и изменить глобальные параметры интеграции с DNS, выполните следующие действия:

1. В консоли **DHCP** разверните узел нужного сервера. Щелкните правой кнопкой узел **IPv4** и выберите **Свойства (Properties)**.

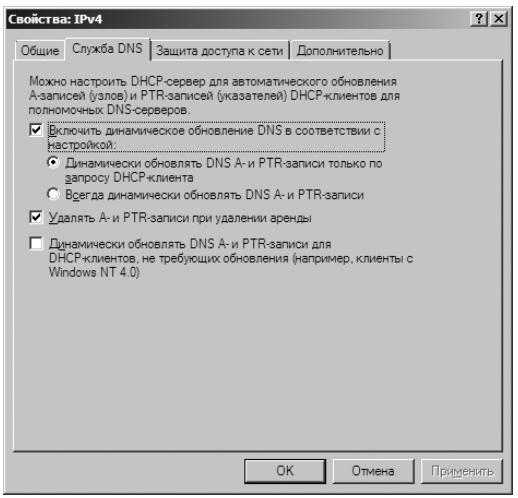


Рис. 19-5. На вкладке Служба DNS (DNS) показаны стандартные параметры интеграции DNS и DHCP

2. Перейдите на вкладку **Служба DNS (DNS)**. На рис. 19-5 показаны стандартные параметры интеграции DNS и DHCP. В большинстве случаев изменять стандартную конфигурацию не требуется.

Чтобы просмотреть и изменить параметры интеграции с DNS для областей, выполните следующие действия:

1. В консоли **DHCP** разверните узел нужного сервера. Затем разверните узел **IPv4**.
2. Щелкните правой кнопкой нужную область и выберите **Свойства (Properties)**.
3. Перейдите на вкладку **Служба DNS (DNS)**. Ее параметры показаны на рис. 19-5. В большинстве случаев изменять стандартную конфигурацию не требуется.

Интеграция DHCP и NAP

Платформа NAP (Network Access Protection) призвана защитить сеть от клиентов, не имеющих достаточных собственных средств защиты. Простейший способ включить NAP на DHCP — настроить DHCP-сервер как сервер политики сети (Network Policy Server, NPS). Для этого нужно установить консоль Сервер политики сети (Network Policy Server), настроить политику объединения DHCP и NAP и включить NAP на DHCP. При этом на сетевых компьютерах осуществляется включение платформы NAP, но не ее настройка.

Чтобы создать политику интеграции NAP и DHCP, выполните следующие действия:

1. На сервере, который будет выполнять роль сервера политики сети запустите Мастер добавления компонентов (Add Features Wizard), чтобы установить консоль **Сервер политики сети (Network Policy Server)**.
2. В дереве консоли **Сервер политики сети (Network Policy Server)** выделите узел **NPS (Локально) (NPS (Local))** и щелкните ссылку **Настройка NAP (Configure NAP)** на главной панели. Запустится мастер Настройка NAP (Configure NAP Wizard).
3. В списке **Способ сетевого подключения (Network Connection Method)** выберите вариант **Протокол DHCP (Dynamic Host Configuration Protocol (DHCP))**. Этот способ подключения будет использован для NAP-совместимых клиентов. Как показано на рис. 19-6, заданное по умолчанию имя политики — NAP DHCP. Щелкните **Далее (Next)**.
4. На странице **Укажите серверы принудительной защиты доступа к сети под управлением DHCP-сервера (Specify NAP Enforcement Servers Running DHCP Server)** укажите все удаленные DHCP-серверы вашей сети:
   - Щелкните **Добавить (Add)**. В диалоговом окне **Новый RADIUS-клиент (Add New RADIUS Client)** введите понятное имя удаленного сервера в поле **Понятное имя (Friendly Name)**. В поле **Адрес (Address)** введите DNS-имя или IP-адрес удаленного сервера DHCP. Для проверки адреса щелкните **Проверить (Verify)**.
   - В разделе **Общий секрет (Shared Secret)** установите переключатель **Создать (Generate)**. Затем щелкните кнопку **Создать (Generate)**, чтобы создать длинный пароль с общим секретом. Вам нужно будет ввести эту фразу в политику NAP DHCP на всех удаленных DHCP-серверах. Поэтому обязательно запишите ее или сохраните в файле, в безопасном расположении. Щелкните **OK**.

5. Щелкните **Далее (Next)**. На странице **Укажите DHCP-области (Specify DHCP Scopes)** вы можете задать области DHCP, к которым будет применена политика. Если области не указаны, политика применяется ко всем областям на выбранных DHCP-серверах, в которых включена NAP. Два раза щелкните **Далее (Next)**.

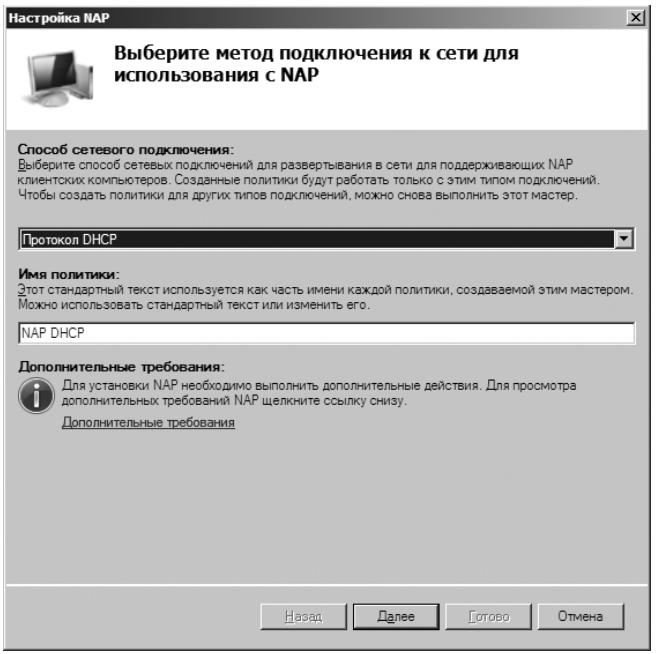


Рис. 19-6. Настройка политики для локального DHCP-сервера

6. На странице **Задайте группу сервера исправлений NAP и URL-адрес (Specify A NAP Remediation Server Group And URL)** выберите группу серверов обновлений или щелкните **Создать группу (New Group)**, чтобы задать группу серверов исправлений. На этих серверах хранятся обновления ПО для NAP-клиентов. В текстовое поле введите URL веб-страницы с инструкцией, как привести компьютер в соответствие с политикой NAP. Убедитесь, что клиенты DHCP могут открыть эту страницу. Щелкните **Далее (Next)**.
7. На странице **Определите политику работоспособности NAP (Define NAP Health Policy)** задайте, как будет работать политика работоспособности NAP. В большинстве случаев можно оставить стандартные параметры, которые запрещают вход в сеть клиентам, не совместимым с NAP. Для NAP-совместимых клиентов проводится проверка работоспособности и автоматическое исправление. Это позволяет им получить необходимые обновления ПО. Щелкните **Далее (Next)** и **Готово (Finish)**.

Вы можете настроить параметры NAP для всего DHCP-сервера или для отдельных областей. Чтобы просмотреть или изменить глобальные параметры NAP, выполните следующие действия:

1. В консоли DHCP разверните узел нужного сервера. Щелкните правой кнопкой узел IPv4 и выберите **Свойства (Properties)**.
2. На вкладке **Защита доступа к сети (Network Access Protection)**, показанной на рис. 19-7, щелкните кнопку **Включить во всех областях (Enable On All Scopes)** или **Отключить во всех областях (Disable On All Scopes)**, чтобы включить или отключить NAP для всех областей сервера.

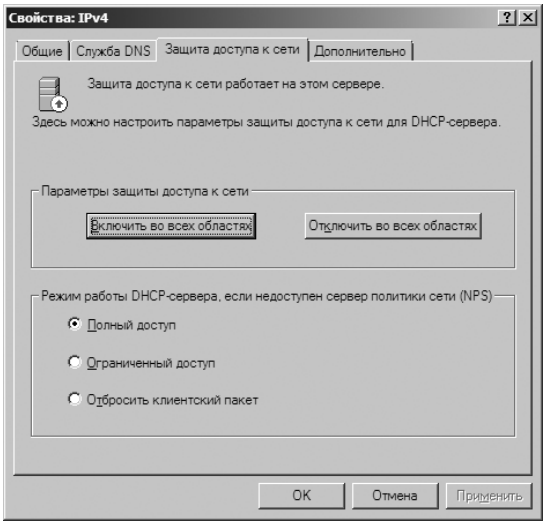


Рис. 19-7. Вкладка Защита доступа к сети (Network Access Protection) управляет возможностями защиты DHCP

Примечание Если локальный DHCP-сервер выступает в роли сервера NPS, он должен быть всегда доступен. Если вы не настроили сервер как сервер NPS или DHCP-сервер не может установить связь с назначенным сервером NPS, на вкладке **Защита доступа к сети (Network Access Protection)** будет отображено сообщение об ошибке.

Выберите один из следующих переключателей, чтобы указать, как должен действовать DHCP-сервер, если NPS-сервер недоступен. Затем щелкните **OK**.

- **Полный доступ (Full Access)** Предоставляет DHCP-клиентам полный доступ к сети. Клиентам позволено выполнять любые разрешенные действия.
- **Ограниченный доступ (Restricted Access)** Предоставляет DHCP-клиентам ограниченный доступ к сети. Клиенты могут работать только с тем сервером, к которому они подключены.
- **Отбросить клиентский пакет (Drop Client Packet)** Блокирует запросы клиентов и запрещает выход клиентов в сеть. У клиентов нет доступа к ресурсам сети.

Чтобы просмотреть и изменить параметры NAP для отдельных областей, выполниет следующие действия:

1. В консоли DHCP разверните узел нужного сервера. Затем разверните узел **IPv4**.
2. Щелкните правой кнопкой нужную область и выберите **Свойства (Properties)**.
3. На вкладке **Защита доступа к сети (Network Access Protection)** установите переключатель **Включить для этой области (Enable For This Scope)** или **Отключить для этой области (Disable For This Scope)**, чтобы включить или отключить NAP для данной области.
4. Если вы включили NAP и хотите использовать профиль NAP отличный от стандартного, установите переключатель **Использовать особый профиль (Use Custom Profile)** и введите имя профиля, например, **Alternate NAP DHCP**.
5. Щелкните **OK**, чтобы сохранить параметры.

Профилактика конфликтов IP-адресов

Часто причиной проблем с DHCP становятся конфликты IPv4-адресов. Двум компьютерам в сети нельзя иметь один IP-адрес. Если компьютеру назначен уже использованный IPv4-адрес, один или оба компьютера могут быть отключены от сети. Чтобы своевременно обнаруживать конфликты, а еще лучше, избежать их, включите обнаружение конфликтов IPv4-адресов, выполнив следующие действия:

1. В консоли DHCP разверните узел нужного сервера. Щелкните правой кнопкой узел **IPv4** и выберите **Свойства (Properties)**.
2. На вкладке **Дополнительно (Advanced)** присвойте параметру **Число попыток определения конфликтов (Conflict Detection Attempts)** отличное от нуля значение. Оно определяет количество проверок IP-адреса, которые DHCP-сервер проводит перед предоставлением адресу клиенту. Сервер DHCP проверяет IP-адреса, отправляя по сети запросы PING.

Ближе к реальности Индивидуальный IPv4-адрес — это стандартный IP-адрес для сетей классов A, B и C. Когда DHCP-клиент запрашивает аренду, DHCP-сервер проверяет пул адресов и предоставляет клиенту в аренду доступный IPv4-адрес. По умолчанию сервер проверяет только отсутствие адреса в текущем списке аренды. Настоящая проверка сети на предмет использования адреса не проводится. Но в оживленном сетевом окружении администратор мог вручную назначить этот же IPv4-адрес другому компьютеру. Возможно также, что при включении компьютера с этим IPv4-адресом возникнет несогласованность между компьютером и DHCP-сервером: клиент будет считать, что аренда еще продолжается, тогда как с точки зрения DHCP-сервера срок аренды уже истек. В любом случае произойдет конфликт адресов, который приведет к сбою в сети.

Сохранение и восстановление конфигурации DHCP

Настроив необходимые параметры DHCP, сохраните заданную конфигурацию, чтобы потом ее можно было восстановить на DHCP-сервере. Чтобы сохранить конфигурацию, введите в командной строке следующую команду:

```
netsh dump dchp >dhcpconfig.dmp
```

В этом примере, *dhcpconfig.dmp* — это имя сценария конфигурации, который вы хотите создать. Создав сценарий, вы можете восстановить конфигурацию, в командной строке введя следующую команду:

```
netsh exec dhcpconfig.dmp
```

Совет Этот метод можно использовать при установке другого DHCP-сервера с такой же конфигурацией. Скопируйте сценарий конфигурации в папку на конечном компьютере, а затем выполните его.

Управление областями DHCP

После установки DHCP-сервера требуется настроить области, которые он будет использовать. Области адресов — это пулы IP-адресов, которые могут арендовать клиенты. Как уже говорилось, вы можете создавать области трех типов: суперобласти и многоадресные области для Ipv4-адресов, а также обычные области для IPv4- и Ipv6-адресов.

Создание суперобласти и управление ею

Суперобласть служит контейнером для областей IPv4 так же, как подразделение служит контейнером для объектов Active Directory. Суперобласти помогают управлять имеющимися в сети областями, например, позволяют одновременно включать или выключать сразу несколько областей. Кроме того, в суперобласти можно просматривать статистику для нескольких областей, вместо того чтобы проверять статистику для каждой области отдельно.

Создание суперобласти

Создайте, по крайней мере, одну обычную или многоадресную область IPv4. Затем, чтобы создать суперобласть, выполните следующие действия:

1. В консоли DHCP разверните узел нужного сервера. Щелкните правой кнопкой узел **IPv4** и выберите команду **Создать суперобласть (New Superscope)**. Откроется Мастер создания суперобласти (New Superscope Wizard). Щелкните **Далее (Next)**.
2. Введите имя суперобласти и щелкните **Далее (Next)**.
3. Выберите области, которые следует добавить в суперобласть, щелкая их в списке **Имеющиеся области (Available Scopes)**. Чтобы выбрать несколько областей, щелкайте их при нажатых клавишах Shift или Ctrl.
4. Щелкните **Далее (Next)** и **Готово (Finish)**.

Добавление областей в суперобласть

Добавлять области в суперобласть можно как в процессе ее создания, так и позже. Чтобы добавить область в существующую суперобласть, выполните следующие действия:

1. Правой кнопкой щелкните область, которую хотите добавить в существующую суперобласть, и выберите команду **Добавить в суперобласть (Add To Superscope)**.
2. В диалоговом окне **Добавление области… к суперобласти (Add Scope … To A Superscope)** выберите суперобласть.
3. Щелкните **OK**.

Удаление областей из суперобласти

Чтобы удалить область из суперобласти, выполните следующие действия:

1. Правой кнопкой щелкните область, которую хотите удалить из суперобласти, и выберите команду **Удалить из суперобласти (Remove From Superscope)**.
2. Щелкните **Да (Yes)**, чтобы подтвердить действие. Если это была последняя область, суперобласть автоматически удаляется.

Включение и отключение суперобласти

Включая и отключая суперобласть, вы включаете или отключаете сразу все входящие в нее области. Чтобы включить суперобласть, щелкните ее правой кнопкой и выберите команду **Активировать (Activate)**. Чтобы отключить суперобласть, щелкните ее правой кнопкой и выберите команду **Деактивировать (Deactivate)**.

Удаление суперобласти

При удаления суперобласти удаляется контейнер для хранения областей, но не сами области. Если вы хотите удалить области, которые входят в состав контейнера, сначала следует удалить суперобласть. Чтобы удалить суперобласть, щелкните ее правой кнопкой и выберите команду **Удалить (Delete)**. Щелкните **Да (Yes)**, чтобы подтвердить действие.

Создание областей и управление ими

Область предоставляет пул адресов для выделения DHCP-клиентам. Обычная область — это область с адресами сетей класса A, B и C. Многоадресная область — это область с адресами сетей класса D. Хотя обычные и многоадресные области создаются по-разному, в управлении они мало чем отличаются друг от друга. Ключевые отличия состоят в том, что многоадресные области не позволяют резервировать адреса, а также задавать дополнительные параметры WINS, DNS, маршрутизации и т. д.

Создание обычной области IPv4-адресов

Чтобы создать обычную область IPv4-адресов, выполните следующие действия:

1. В консоли DHCP разверните узел нужного сервера. Выделите и разверните узел **IPv4**. Если вы хотите, чтобы новая область была автоматически добавлена в суперобласть, выделите и щелкните правой кнопкой нужную суперобласть.

2. В контекстном меню выберите команду **Создать область (New Scope)**. Откроется Мастер создания области (New Scope Wizard). Щелкните **Далее (Next)**.
3. Введите имя и описание области и щелкните **Далее (Next)**.
4. На странице **Диапазон адресов (IP Address Range)** введите начальный и конечный адреса в поля **Начальный IP-адрес (Start IP Address)** и **Конечный IP-адрес (End IP Address)**.

Примечание Обычно в область не включают адреса *x.x.x*.0 и *x.x.x*.255. В большинстве случаев они резервируются, соответственно, для сетевых адресов и широковещательных сообщений. Поэтому вы можете использовать диапазон от 192.168.10.1 до 192.168.10.254, но не от 192.168.10.0 до 192.168.10.255.

5. Когда вы вводите диапазон IP-адресов, длина идентификатора сети и маска подсети заполняются автоматически (рис. 19-8). Если вы не используете подсети, оставьте стандартные значения.

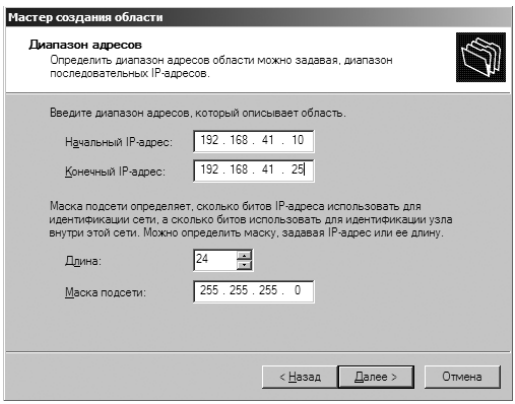


Рис. 19-8. Введите диапазон IP-адресов для области в Мастере создания области (New Scope Wizard),

6. Щелкните **Далее (Next)**. Если введенный вами диапазон охватывает разные сети, вам будет предоставлена возможность создать суперобласть, содержащую различные области для каждой сети. Установите переключатель **Да (Yes)**, чтобы принять это предложение, и перейдите к шагу 8. Если вы допустили ошибку, щелкните **Назад (Back)**, чтобы исправить введенный диапазон IP-адресов.
7. Определите диапазоны IP-адресов, которые следует исключить из области. На странице **Добавление исключений (Add Exclusion)** задайте исключения в полях **Начальный IP-адрес (Start IP Address)** и **Конечный IP-адрес (End IP Address)**:
   - Чтобы определить диапазон, введите начальный и конечный адреса в поля **Начальный IP-адрес (Start IP Address)** и **Конечный IP-адрес (End IP Address)** и щелкните **Добавить (Add)**. Чтобы исключить один IP-адрес, введите его и как начальный, и как конечный IP-адрес.

Повторите эти действия, чтобы исключить еще один диапазон.

- Исключенные диапазоны адресов отображаются в списке **Исключаемый диапазон адресов (Excluded Address Range)**.
- Чтобы удалить исключение, выделите диапазон в списке **Исключаемый диапазон адресов (Excluded Address Range)** и щелкните **удалить (Remove)**.

8. Щелкните **Далее (Next)**. Задайте продолжительность аренды в полях **Дней (Day(s))**, **Часов (Hour(s))** и **Минут (Minutes)**. Стандартная продолжительность составляет восемь дней. Щелкните **Далее (Next)**.

Совет Продумайте продолжительность аренды. Установив слишком продолжительный срок, вы снизите эффективность DHCP, поскольку рискуете исчерпать имеющиеся IP-адреса, особенно в сетях с мобильными пользователями или другими типами компьютеров, не являющихся постоянными членами сети. В большинстве сетей нормальный срок аренды составляет от трех до семи дней.

9. У вас есть возможность установить общие параметры DHCP для DNS, WINS, шлюзов и т. п. Если вы хотите задать эти параметры сейчас, установите переключатель **Да, настроить эти параметры сейчас (Yes, I Want To Configure These Options Now)**. В противном случае, установите переключатель **Нет, настроить эти параметры позже (No, I Will Configure These Options Later)** и пропустите шаги 10–14.
10. Щелкните **Далее (Next)**. Первый параметр, который можно настроить, — это основной шлюз. В поле **IP-адрес (IP Address)** введите IP-адрес первого основного шлюза. Щелкните **Добавить (Add)**. Повторите процесс для других шлюзов.

    Сначала клиенты пытаются использовать первый шлюз из списка. Если он недоступен, клиенты пытаются получить доступ к другому шлюзу и т. д. При помощи кнопок **Вверх (Up)** и **Вниз (Down)** можно изменить порядок шлюзов.

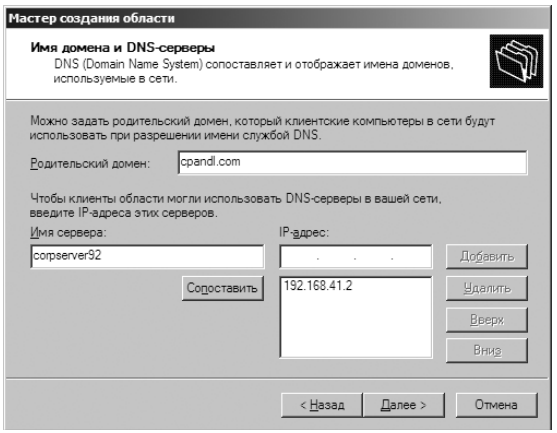


Рис. 19-9. Стандартные параметры DNS задаются на странице Имя домена и DNS-серверы (Domain Name And DNS Servers)

11. Щелкните **Далее (Next)**. Как показано на рис. 19-9, настройте стандартные параметры DNS для клиентов DHCP. Введите имя родительского домена, который следует использовать для разрешения не полностью определенных имен компьютеров.
12. В поле **IP-адрес (IP Address)** введите IP-адрес основного DNS-сервера. Щелкните **Добавить (Add)**. Повторите процесс, чтобы указать дополнительные DNS-серверы. Здесь опять же порядок записей определяет, какой из IP-адресов будет использован в первую очередь. При необходимости, измените порядок с помощью кнопок **Вверх (Up)** и **Вниз (Down)**. Щелкните **Далее (Next)**.

Совет Если вам известно имя DNS-сервера, введите его вместо IP-адреса в поле **Имя сервера (Server Name)** и щелкните кнопку **Сопоставить (Resolve)**. В случае удачного сопоставления IP-адрес будет введен в поле **IP-адрес (IP Address)**. Добавьте сервер, щелкнув кнопку **Добавить (Add)**.

13. Аналогичным способом задайте стандартные параметры WINS. Щелкните **Далее (Next)**.
14. Чтобы активировать область, установите переключатель **Да, я хочу активировать эту область сейчас (Yes, I Want To Activate This Scope Now)** и щелкните **Далее (Next)**. В противном случае, установите переключатель **Нет, я активирую эту область позже (No, I Will Activate This Scope Later)** и щелкните **Далее (Next)**.
15. Щелкните **Готово (Finish)**, чтобы завершить процесс.

Создание обычной области IPv6-адресов

Обычные области IPv6-адресов создаются при помощи Мастера создания области (New Scope Wizard). Во время настройки DHCP для IPv6-адресов вы должны ввести идентификатор сети и значение предпочтения. Обычно сеть идентифицируют первые 64 бита IPv6-адреса. Мастер создания области (New Scope Wizard) ждет от вас ввода именно 64-разрядного значения. Значение предпочтения устанавливает приоритет области по отношению к другим областям. Область с наименьшим предпочтением будет использована в первую очередь. Область со следующим по величине предпочтением будет использована во вторую очередь и т. д.

Чтобы создать обычную область IPv6-адресов, выполните следующие действия:

1. В консоли **DHCP** разверните узел нужного сервера. Выделите узел **IPv6** и щелкните его правой кнопкой.
2. В контекстном меню выберите команду **Создать область (New Scope)**. Откроется Мастер создания области (New Scope Wizard). Щелкните **Далее (Next)**.
3. Введите имя и описание области и щелкните **Далее (Next)**.
4. На странице **Префикс области (Scope Prefix)**, показанной на рис. 19-10, введите 64-разрядный сетевой префикс и значение предпочтения. Щелкните **Далее (Next)**.

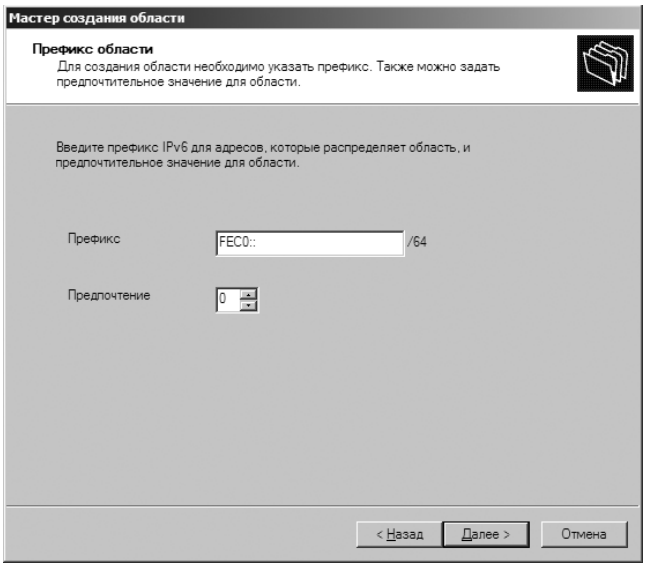


Рис. 19-10. Введите сетевой префикс и предпочтение в Мастере создания области (New Scope Wizard)

5. На странице **Добавление исключений (Add Exclusion)** определите диапазоны IPv6-адресов, которые следует исключить из области, в полях **Начальный IPv6-адрес (Start IPv6 Address)** и **Конечный IPv6-адрес (End IPv6 Address)**. Вы можете исключить несколько адресов следующим образом:
   - Чтобы определить диапазон исключения, в разделе **Исключаемый диапазон адресов (Exclusion Range)** введите начальный и конечный адреса в поля **Начальный IPv6-адрес (Start IPv6 Address)** и **Конечный IPv6-адрес (End IPv6 Address)** и щелкните **Добавить (Add)**. Чтобы исключить один IPv6-адрес, введите его как начальный IPv6-адрес и щелкните **Добавить (Add)**.
   - Отследить исключенные диапазоны адресов можно в списке **Исключаемый диапазон адресов (Excluded Address Range)**.
   - Чтобы удалить исключение, выделите диапазон в списке **Исключаемый диапазон адресов (Excluded Address Range)** и щелкните **Удалить (Remove)**.
6. Щелкните **Далее (Next)**. Динамические IPv6-адреса бывают временными и постоянными. Постоянный адрес похож на зарезервированный адрес. На странице **Аренда области (Scope Lease)**, показанной на рис. 19-11, укажите сроки аренды для временных и постоянных адресов в разделах **Основное время жизни (Preferred Lifetime)** и **Допустимое время жизни (Valid Lifetime)**. Основное время жизни — это типичный интервал, в течение которого будет действительна аренда. Допустимое время жизни — это максимальный интервал, в течение которого будет действительна аренда. Щелкните **Далее (Next)**.

Совет В большинстве сетей IPv6 нормальный срок постоянной аренды составляет от 8 до 30 дней.

7. Чтобы активировать область, установите переключатель **Да (Yes)** в разделе **Активировать область сейчас (Activate Scope Now)** и щелкните **Готово (Finish)**. В противном случае установите переключатель **Нет (No)** и щелкните **Готово (Finish)**.

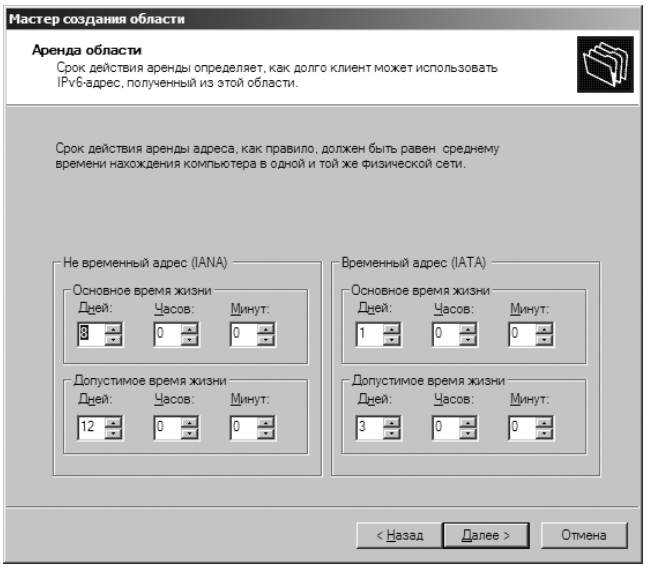


Рис 19-11. Укажите продолжительность временной и постоянной аренды

Создание многоадресной области

Чтобы создать многоадресную область, выполните следующие шаги:

1. В консоли DHCP разверните узел нужного сервера. Выделите и щелкните правой кнопкой узел **IPv4**.
2. В контекстном меню выберите команду **Создать многоадресную область (New Multicast Scope)**. Откроется Мастер создания многоадресной области (New Multicast Scope Wizard). Щелкните **Далее (Next)**.
3. Введите имя и описание области и щелкните **Далее (Next)**.
4. Поля **Начальный IP-адрес (Start IP Address)** и **Конечный IP-адрес (End IP Address)** определяют диапазон IP-адресов для области. Многоадресные области определяются IP-адресами класса D. Это значит, что допустимый диапазон IP-адресов лежит в пределах от 224.0.0.0 до 239.255.255.255.
5. Сообщения, посылаемые компьютерами при помощи многоадресных IP-адресов, имеют определенное время жизни (Time to Live, TTL). Им определяется максимальное количество маршрутизаторов, через которые может пройти сообщение. Стандартное значение TTL равно 32. В большинстве сетей этого достаточно, но если у вас большая сеть, увеличьте это значение, чтобы оно соответствовало реальному количеству маршрутизаторов.

6. Щелкните **Далее (Next)**. Если вы допустили ошибку, щелкните **Назад (Back)**, чтобы исправить введенный диапазон IP-адресов.
7. На странице **Добавление исключений (Exclusion Range)** задайте диапазоны IP-адресов, которые следует исключить из области. Можно исключить несколько диапазонов.
   - Чтобы определить исключаемый диапазон, введите начальный и конечный адреса в поля **Начальный IP-адрес (Start IP Address)** и **Конечный IP-адрес (End IP Address)** и щелкните **Добавить (Add)**.
   - Исключенные диапазоны адресов перечислены в списка **Исключаемые адреса (Excluded Addresses)**.
   - Чтобы удалить исключенный диапазон, выделите диапазон в списке **Исключаемые адреса (Excluded Addresses)** и щелкните **Удалить (Remove)**.
8. Щелкните **Далее (Next)**. Укажите продолжительность аренды в полях **Дней (Day(s))**, **Часов (Hour(s))** и **Минут (Minutes)**. Стандартная продолжительность составляет 30 дней. Щелкните **Далее (Next)**.

Совет Если вам нечасто приходится работать с многоадресной передачей, лучше измените стандартное значение. Многоадресная аренда используется несколько иначе, чем обычная. Многоадресный IP-адрес можно назначить нескольким компьютерам, и каждый из них может получить его в аренду. В большинстве сетей типичный срок многоадресной аренды составляет от 30 до 60 дней.

9. Чтобы активировать область, установите переключатель **Да (Yes)** и щелкните **Далее (Next)**. В противном случае, щелкните **Нет (No)** и **Далее (Next)**.
10. Щелкните **Готово (Finish)**, чтобы завершить процесс.

Настройка параметров области

Параметры области позволяют детально управлять ее работой и задать стандартные параметры TCP/IP для клиентов, использующих область. Например, вы можете позволить клиентам автоматически находить в сети DNS-сервер, а также определить основные шлюзы, WINS и многое другое. Параметры области применимы только к обычным областям, но не к многоадресным.

Задать параметры области можно любым из следующих способов:

- сразу для всех областей, задав стандартные параметры сервера;
- для конкретной области;
- для конкретного клиента, задав параметры резервирования;
- для класса клиентов, настроив параметры для конкретных пользователей или поставщиков.

Протоколам IPv4 и IPv6 соответствуют различные параметры области. Порядок применения параметров области определяется их положением в иерархии, которая отображена в предыдущем списке. Главным образом, это означает, что:

- параметры области перекрывают глобальные параметры;
- параметры клиента перекрывают параметры области и глобальные параметры;
- параметры класса клиента перекрывают все остальные параметры.

Просмотр и назначение параметров сервера

Параметры сервера применяются ко всем областям, настроенным на конкретном DHCP-сервере. Чтобы просмотреть и изменить параметры сервера, выполнив следующие действия:

1. В консоли **DHCP** дважды щелкните нужный сервер. В дереве консоли разверните узел **IPv4** или **IPv6**.
2. Чтобы просмотреть текущие параметры, в папке IPv4 или IPv6 выберите узел **Параметры сервера (Server Options)**. Настроенные в данный момент параметры будут отображены на правой панели.
3. Чтобы назначить новые параметры, щелкните правой кнопкой элемент **Параметры сервера (Server Options)** и выберите команду **Настроить параметры (Configure Options)**. Откроется диалоговое окно **Параметры: сервер (Server Options)**. В разделе **Доступный параметр (Available Options)**, установите флажок первого настраиваемого параметры. Далее введите нужную информацию в поля раздела **Данные (Data Entry)**. Повторите эти действия для настройки других параметров.
4. Щелкните **OK**.

Просмотр и назначение параметров области

Параметры области действуют для конкретной области и перекрывают стандартные параметры сервера. Чтобы просматривать и изменять параметры области, выполните следующие действия:

1. В консоли **DHCP** разверните элемент нужной области.
2. Чтобы просмотреть текущие параметры, выделите узел **Параметры области (Scope Options)**. Настроенные в данный момент опции будут отображены на правой панели.
3. Чтобы назначить новые параметры, щелкните правой кнопкой элемент **Параметры области (Scope Options)** и выберите команду **Настроить параметры (Configure Options)**. Откроется диалоговое окно **Параметры: область (Scope Options)**. В разделе **Доступный параметр (Available Options)** установите флажок первого настраиваемого параметра и введите нужную информацию в поля раздела **Данные (Data Entry)**, как показано на рис. 19-12. Повторите этот шаг для настройки других параметров.
4. Щелкните **OK**.

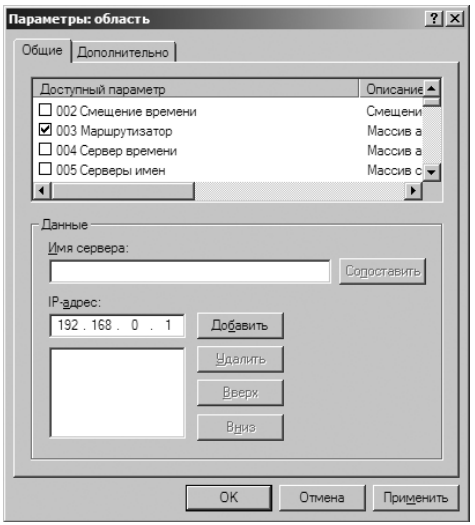


Рис. 19-12. Выберите параметр, который хотите настроить, и введите нужную информацию в поля раздела Данные (Data Entry)

Просмотр и назначение параметров резервирования

Параметры резервирования можно назначить клиенту, у которого есть зарезервированные IPv6- или IPv4-адреса. Эти параметры закрепляются за конкретным клиентом и перекрывают параметры сервера и области. Чтобы просмотреть и изменить параметры резервирования, выполните следующие действия:

1. В консоли **DHCP** разверните нужную область.
2. Дважды щелкните папку **Резервирование (Reservations)** области.
3. Чтобы просмотреть текущие параметры, щелкните нужное резервирование. Настроенные параметры будут отображены в правой панели.
4. Чтобы назначить новые параметры, щелкните правой кнопкой резервирование и выберите команду **Настроить параметры (Configure Options)**. Откроется диалоговое окно **Параметры: резервирование (Reservation Options)**. В разделе **Доступный параметр (Available Options)** установите флажок первого настраиваемого параметра и введите нужную информацию в поля раздела **Данные (Data Entry)**. Повторите этот шаг для настройки других параметров.

Изменение области

Чтобы изменить существующую область, выполните следующие действия:

1. В консоли **DHCP** дважды щелкните нужный сервер. В дереве консоли разверните папки **IPv4** и **IPv6**. Будут отображены области, настроенные на сервере.
2. Щелкните правой кнопкой область, которую хотите изменить, и выберите **Свойства (Properties)**.

3. Теперь вы можете изменить свойства области. Имейте в виду следующее:
   - При изменении обычной области IPv4 у вас есть возможность задать неограниченный срок аренды. Это отрицательно сказывается на эффективности выделения IP-адресов DHCP-сервером. Постоянная аренда не заканчивается, пока вы не отключите ее физически или не отключите область. В результате вы рискуете постепенно исчерпать все адреса, в особенности, если ваша сеть растет. Удачной альтернативой неограниченному сроку аренды является использование резервирований, причем, только для тех клиентов, которые действительно нуждаются в постоянном IP-адресе.
   - При изменении многоадресных областей у вас есть возможность задать время жизни области. Оно определяет количество времени, в течение которого будет действительна область. По умолчанию многоадресные области действительны, пока они включены. Чтобы изменить этот параметр, перейдите на вкладку **Время жизни многоадресной области (Lifetime)**, установите переключатель **Срок действия многоадресной области истекает (Multicast Scope Expires On)** и задайте срок действия.

Включение и отключение областей

В консоли **DHCP** отключенные области отмечены значком с красной стрелкой вниз. Включенные области отображены в виде обычных значков папки. Чтобы включить неактивную область в консоли **DHCP**, щелкните ее правой кнопкой и выберите команду **Активировать (Activate)**. Чтобы отключить активную область в консоли **DHCP**, щелкните ее правой кнопкой и выберите команду **Деактивировать (Deactivate)**.

Совет Отключение деактивирует выключает область, но не аннулирует текущие аренды клиентов. О том, как аннулировать аренды, читайте в разделе «Освобождение адресов и аренды» этой главы.

Включение протокола BOOTP

Протокол динамической адресации BOOTP предшествует DHCP. Обычные области не поддерживают BOOTP. Чтобы включить поддержку BOOTP в области, выполните следующие действия:

1. Щелкните правой кнопкой область IPv4-адресов, которую хотите изменить, и выберите **Свойства (Properties)**.
2. На вкладке **Дополнительно (Advanced)** установите переключатель **Обоих типов серверов (Both)**, чтобы обеспечить поддержку клиентов DHCP и BOOTP.
3. При необходимости задайте срок аренды для BOOTP-клиентов и щелкните **OK**.

Удаление области

Удаляемая область навсегда удаляется с DHCP-сервера. Чтобы удалить область, выполните следующие действия:

1. В консоли **DHCP** щелкните правой кнопкой область, которую хотите удалить, и выберите команду **Удалить (Delete)**.
2. Подтвердите удаление области, щелкнув **Да (Yes)**.

Настройка нескольких областей в сети

В одной сети можно настроить несколько областей. Обслуживать эти области может как один, так и несколько DHCP-серверов. Тем не менее, при работе с несколькими областями, крайне важно не допускать перекрытия их диапазонов адресов. Каждая область должна иметь собственный диапазон. В противном случае, может произойти назначение одного IP-адреса двум DHCP-клиентам, что приведет к серьезным проблемам в сети.

Чтобы лучше разобраться, как работать с несколькими областями, рассмотрим подсеть, в которой каждый DHCP-сервер выделяет IP-адреса из своего диапазона.

Сервер	Диапазон IP-адресов в области DHCP
A	192.168.10.1 до 192.168.10.99
B	192.168.10.100 до 192.168.10.199
C	192.168.10.200 до 192.168.10.254

Каждый сервер будет отвечать на запросы DHCP, и все они смогут назначать клиентам IP-адреса. В случае неисправности одного из серверов сеть продолжат обслуживать другие DHCP-серверы.

Управление пулом адресов, арендой и резервированиями

В каждой области есть папки с пулом адресов, арендами и резервированиями. В этих папках вы найдете соответствующие данные и сможете управлять существующими записями.

Просмотр статистики области

В статистике области содержится информация об пуле адресов пространстве текущей области или суперобласти. Для просмотра статистики щелкните область или суперобласть правой кнопкой и выберите команду **Отобразить статистику (Display Statistics)**.

Далее описаны поля открывшегося диалогового окна:

- **Всего областей (Total Scopes)** Количество областей в суперобласти.
- **Всего адресов (Total Addresses)** Количество IP-адресов в области.
- **Используется (In Use)** Общее количество используемых адресов (в числовом и процентном выражении). Если это значение достигает 85% и более, стоит подумать о выделении дополнительных адресов или освобождении существующих.
- **Доступен (Available)** Общее количество доступных адресов (в числовом и процентном выражении).

Создание нового диапазона исключений

Вы можете исключить из области диапазон IPv4- или IP-адресов. В областях может быть несколько диапазонов исключений. Чтобы определить диапазон исключений в области IPv4-адресов, выполните следующие действия:

1. В консоли **DHCP** разверните нужную область и щелкните правой кнопкой папку **Пул адресов (Address Pool)** и выберите команду **Диапазон исключений (New Exclusion Range)**.
2. Введите начальный и конечный адреса в поля **Начальный IP-адрес (Start IP Address)** и **Конечный IP-адрес (End IP Address)** и щелкните **Добавить (Add)**. Указанный диапазон должен быть подмножеством диапазона текущей области и в данный момент не должен использоваться. Повторите этот шаг, чтобы добавить другие диапазоны исключений.
3. Завершив настройку, щелкните **Закрыть (Close)**.

Чтобы определить диапазон исключений для области IPv6-адресов, выполните следующие действия:

1. В консоли DHCP разверните нужную область и щелкните правой кнопкой папку **Исключения (Exclusions)**. В контекстном меню выберите команду **Диапазон исключения (New Exclusion Range)**.
2. Введите начальный и конечный адреса в поля **Начальный IPv6-адрес (Start IPv6 Address)** и **Конечный IPv6-адрес (End IPv6 Address)** и щелкните **Добавить (Add)**. Указанный диапазон должен быть подмножеством диапазона текущей области и в данный момент не должен использоваться. Повторите этот шаг, чтобы добавить другие диапазоны исключений.
3. Завершив настройку, щелкните **Закрыть (Close)**.

Удаление диапазона исключений

Если вам больше не нужно исключение, вы можете его удалить. Выберите папку **Пул адресов (Address Pool)** или **Исключения (Exclusions)**. Щелкните исключение правой кнопкой и выберите команду **Удалить (Delete)**. Подтвердите действие, щелкнув **Да (Yes)**.

Резервирование DHCP-адресов

Протокол DHCP позволяет назначать постоянные адреса клиентам несколькими способами. В частности, с помощью переключателя **Без ограничений (Unlimited)** в диалоговом окне свойств области можно назначить постоянный адрес всем клиентам, использующим данную область. Кроме того, можно зарезервировать DHCP-адрес для конкретного клиента. В результате резервирования сервер DHCP всегда назначает клиенту один и тот же IP-адрес, сохраняя возможность централизованного управления, в чем и состоит преимущество DHCP.

Чтобы зарезервировать IP-адрес для клиента, выполните следующие действия:

1. В консоли **DHCP** разверните нужную область и щелкните правой кнопкой папку **Резервирование (Reservations)**. В контекстном меню выберите команду **Создать резервирование (New Reservation)**.
2. В поле **Имя клиента (Reservation Name)** введите короткое, но понятное имя резервирования. Это поле служит только для идентификации.
3. В поле **IP-адрес (IP Address)** введите IPv4-адрес, который хотите зарезервировать для клиента.

Примечание Обратите внимание, что IP-адрес должен находиться в пределах диапазона адресов выбранной области.

4. Поле **MAC-адрес (MAC Address)** содержит аппаратный адрес сетевого адаптера клиентского компьютера. Чтобы узнать MAC-адрес, введите команду **ipconfig /all** в командной строке клиентского компьютера. В пункте Физический адрес (Physical Address) содержится MAC-адрес клиента. Вы должны ввести это значение без ошибок, иначе резервирование не будет работать.
5. В поле **Описание (Description)** введите комментарий, если сочтете нужным.
6. По умолчанию поддерживаются как DHCP-клиенты, так и BOOTP-клиенты. Это очень удобно, и отказываться от этой возможности следует, только если вы хотите исключить клиентов определенного типа.
7. Щелкните **Добавить (Add)**, чтобы создать резервирование. Повторите этот шаг, чтобы добавить другие резервирования.
8. Завершив настройку, щелкните **Закрыть (Close)**.

Чтобы зарезервировать IPv6-адрес для клиента, выполните следующие действия:

1. В консоли DHCP разверните нужную область и щелкните правой кнопкой папку **Резервирование (Reservations)**. В контекстном меню выберите **Создать резервирование (New Reservation)**.
2. В поле **Имя клиента (Reservation)** введите короткое, но понятное имя. Это поле служит только для идентификации.
3. В поле **IPv6-адрес (IPv6 Address)** введите IPv6-адрес, который хотите закрепить за клиентом.

Примечание Обратите внимание, что IP-адрес должен находиться в пределах диапазона адресов выбранной области.

4. В поле уникального идентификатора устройства DUID (Device Unique Identifier) нужно ввести MAC-адрес сетевого адаптера клиентского компьютера. Чтобы узнать MAC-адрес, введите команду **ipconfig /all** в командной строк клиентского компьютера. В пункте **Физический адрес (Physical Address)** содержится MAC-адрес клиента. Вы должны ввести это значение без ошибок, иначе резервирование не будет работать.
5. Идентификатор IAID устанавливает уникальный префикс идентификатора клиента. Как правило, это значение состоит из 9 цифр.

6. В поле **Описание (Description)** введите комментарий, если сочтете нужным.
7. Щелкните **Добавить (Add)**, чтобы создать резервирование. Повторите этот шаг, чтобы добавить другие резервирования.
8. Завершив настройку, щелкните **Закрыть (Close)**.

Освобождение адресов и аренды

Работая с зарезервированными адресами, помните о двух нюансах:

- Зарезервированные адреса не переназначаются автоматически. Чтобы передать используемый адрес другому клиенту, адрес придется освободить. Чтобы освободить адрес, аннулируйте аренду или введите на клиентском компьютере команду **ipconfig /release**.
- Клиенты не переходят на зарезервированные адреса автоматически. Если клиент уже использует другой IP-адрес, вам нужно заставить его освободить текущую аренду и запросить новую. Чтобы освободить адрес, аннулируйте аренду или введите на клиентском компьютере команду **ipconfig /release**.

Изменение свойств резервирования

Чтобы изменять свойства резервирования, выполните следующие действия:

1. В консоли **DHCP** разверните нужную область и щелкните папку **Резервирование (Reservations)**.
2. Щелкните правой кнопкой нужное резервирование и выберите **Свойства (Properties)**. Измените свойства резервирования. Затененные поля изменять нельзя, зато другие поля вы можете изменять. Это те самые поля, о которых рассказывалось ранее.

Удаление аренды и резервирования

Чтобы удалить активную аренду и резервирование, выполните следующие действия:

1. В консоли DHCP разверните нужную область и щелкните папку **Арендованные адреса (Address Leases)** или **Резервирование (Reservations)**.
2. Щелкните правой кнопкой аренду или резервировании, которое хотите удалить, и выберите **Удалить (Delete)**.
3. Подтвердите удаление, щелкнув **Да (Yes)**.
4. Теперь аренда или резервирование удалены из DHCP. Однако клиент еще не освободил IP-адрес. Чтобы освободить адрес, введите на клиентском компьютере команду **ipconfig /release**.

Архивация и восстановление базы данных DHCP

На серверах DHCP в файлах БД хранится информация об аренде и резервировании DHCP. По умолчанию эти файлы находятся в папке %SystemRoot%\System32\DHCP. Вот описание основных файлов:

- **Dhcp.mdb** Основной файл БД DHCP-сервера.
- **J50.log** Журнал регистрации транзакций, используемый для восстановления незавершенных транзакций в случае сбоя сервера.
- **J50.chk** Файл контрольной точки, используемый при усечении журнала регистрации транзакций DHCP-сервера.
- **Res1.log** Зарезервированный файл журнала DHCP-сервера.
- **Res2.log** Зарезервированный файл журнала DHCP-сервера.
- **Tmp.edb** Временный рабочий файл DHCP-сервера.

Архивация БД DHCP

Архивная папка в папке %SystemRoot%\System32\DHCP содержит информацию о конфигурации и базе данных DHCP. По умолчанию БД DHCP архивируется автоматически каждые 60 минут. Чтобы архивировать БД DHCP в произвольное время, выполните следующие действия:

1. В консоли **DHCP** щелкните правой кнопкой сервер, который хотите архивировать, и выберите команду **Архивировать (Backup)**.
2. В диалоговом окне **Обзор папок (Browse For Folder)** выберите папку, в которой будет содержаться архивная БД DHCP, и щелкните **OK**.

Параметры реестра, управляющие расположением архива, расписанием архивации, а также другими параметрами архивации DHCP, хранятся в разделе:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters
```

Следующие параметры управляют БД DHCP и параметрами архивации:

- **BackupDatabasePath** Расположение БД DHCP. Этот параметр задается в окне свойств сервера DHCP. Перейдите на вкладку **Дополнительно (Advanced)** и установите требуемое значение в поле **Путь к базе данных (Database Path)**.
- **DatabaseName** Имя основного файла БД DHCP. Значение по умолчанию — DHCP.mdb.
- **BackupInterval** Интервал архивации в минутах. Значение по умолчанию — 60 мин.
- **DatabaseCleanupInterval** Интервал очистки записей в БД. Значение по умолчанию — 60 мин.

Восстановление БД DHCP из архивной копии

Восстанавливая сервер после аварийного отказа, вы должны будете восстановить, а затем согласовать БД DHCP. Чтобы восстановить БД DHCP из архивной копии, выполните следующие действия:

1. При необходимости восстановите из архива копию папки %SystemRoot%\System32\DHCP\backup. Затем откройте консоль **DHCP**, щелкните правой кнопкой сервер, который хотите восстановить, и выберите команду **Восстановить (Restore)**.

2. В диалоговом окне **Обзор папок (Browse For Folder)** выберите папку, в которой содержится нужная архиваня копия, и щелкните **OK**.
3. На время восстановления БД служба DHCP-сервер (DHCP Server) останавливается. В результате DHCP-клиенты временно не смогут устанавливать связь с DHCP-сервером и получать IP-адреса.

Перемещение БД DHCP на новый сервер при помощи архивации и восстановления

Если вы хотите перенастроить DHCP-сервер, вам придется переместить DHCP-службы на другой сервер. Для этого потребуется выполнить несколько задач на исходном и конечном серверах. На конечном сервере выполните следующие действия:

1. Установите службу DHCP-сервер (DHCP Server) на конечном сервере и перезагрузите сервер.
2. Остановите службу DHCP-сервер (DHCP Server) в консоли **Службы (Services)**.
3. Удалите содержимое папки %SystemRoot%\System32\DHCP.

Выполните следующие действия на исходном сервере:

1. Остановите службу DHCP-сервер (DHCP Server) в консоли **Службы (Services)**.
2. После остановки службы DHCP-сервер (DHCP Server) отключите ее запуск, чтобы ее нельзя было запустить в дальнейшем.
3. Скопируйте все содержимое папки %SystemRoot%\System32\DHCP в папку %SystemRoot%\System32\DHCP на конечном сервере.

Теперь все необходимые папки находятся на конечном сервере. Запустите службу DHCP-сервер (DHCP Server) на конечном сервере, чтобы завершить перенос.

Регенерация БД DHCP

Если БД DHCP повреждена и Windows не может исправить ее простой остановкой и перезапуском службы DHCP-сервер (DHCP Server), попытайтечь восстановить БД способом, описанным в разделе «Восстановление БД DHCP из архивной копии» этой главы. В случае неудачи создайте новую БД, выполнив следующие действия:

1. Остановите службу DHCP-сервер (DHCP Server) в консоли **Службы (Services)**.
2. Удалите содержимое папки %SystemRoot%\System32\DHCP. Если вы хотите провести полное восстановление БД и не дать серверу восстановить архивную копию, удалите также содержимое архивной папки.

Внимание! Если в результате сбоя повреждены параметры раздела реестра DHCP-Server, не удаляйте файлы DHCP. Они понадобятся для восстановления БД DHCP.

3. Перезапустите службу DHCP-сервер (DHCP Server).

4. В консоли **DHCP** не будет никаких активных аренд или другой информации об областях. Чтобы восстановить активные аренды, вы должны согласовать области сервера, о чем пойдет речь в следующем разделе.
5. Чтобы предотвратить конфликты с арендами, назначенными ранее, на несколько следующих дней включите обнаружение конфликтов адреса. Подробнее — в разделе «Профилактика конфликтов IP-адресов» этой главы.

Согласование аренд и резервирований

В процессе согласования аренды и резервирования клиентов сверяются с БД DHCP на сервере. При обнаружения несоответствий между тем, что записано в реестре Windows, и данными БД DHCP-сервера, вы можете выбрать и согласовать все противоречивые записи. После согласования DHCP либо возвращает IP-адрес прежнему владельцу, либо создает временное резервирование IP-адреса. По истечению срока аренды адрес восстанавливается для дальнейшего использования.

Можно согласовывать отдельные области или все области на сервере. Чтобы согласовать отдельную область, выполните следующие действия:

1. В консоли DHCP щелкните правой кнопкой нужную область и выберите команду **Согласование (Reconcile)**.
2. В диалоговом окне **Согласовать (Reconcile)** щелкните кнопку **Проверить (Verify)**.
3. Найденные противоречия приводятся в окне состояния. Для их исправления нужно выбрать адрес и щелкнуть **Согласовать (Reconcile)**.
4. Если противоречий не найдено, щелкните **OK**.

Чтобы согласовать все области на сервере, выполните следующие действия:

1. В консоли **DHCP** щелкните правой кнопкой элемент нужного протокола и выберите команду **Согласовать все области (Reconcile All Scopes)**.
2. В диалоговом окне **Согласование всех областей (Reconcile All Scopes)** щелкните **Проверить (Verify)**.
3. Найденные противоречия приводятся в окне состояния. Для их исправления нужно выбрать адрес и щелкнуть **Согласовать (Reconcile)**.
4. Если противоречий не найдено, щелкните **OK**.

Глава 20

Оптимизация DNS

В этой главе рассказывается об установке системы DNS и управлении ею. Система DNS — это служба разрешения имен, которая преобразует имена компьютеров в IP-адреса, позволяющие компьютерам находить и идентифицировать друг друга. Система DNS работает через стек протоколов TCP/IP и может интегрироваться с WINS, DHCP и Active Directory. Тесная интеграция с сетевыми возможностями Microsoft Windows делает работу DNS в доменах Active Directory максимально эффективной.

Как работает DNS

Система DNS объединяет группы компьютеров в домены, организованные в иерархическую структуру, которая для публичных сетей определяется в Интернете, а для частных (интрасетей, экстрасетей) — на уровне предприятия. Различные уровни иерархии соответствуют отдельным компьютерам, доменам организаций и доменам более высокого уровня. В полностью определенном имени хоста *omega.microsoft.com*, — имя отдельного компьютера, *microsoft* — домен организации, *com* — домен верхнего уровня.

Домены верхнего уровня лежат в основе иерархии DNS, поэтому их часто называют корневыми. Эти домены упорядочены географически, по типу организации и назначению. Обычные домены, например, *microsoft.com*, также именуются родительскими доменами, так как они являются «родителями» для структуры подразделений. Родительские домены можно делить на поддомены, предназначенные для групп или отделов внутри организации.

Поддомены часто называют дочерними доменами. Например, полностью определенное доменное имя компьютера, принадлежащего отделу кадров компании, может выглядеть так: *jacob.hr.microsoft.com*. Здесь *jacob* — имя хоста, *hr* — дочерний домен, *microsoft.com* — родительский домен.

Интеграция Active Directory с DNS

Как говорилось в главе 7, именно DNS используется в доменах Active Directory для построения иерархии и структуры имен. Служба каталогов Active Directory и DNS настолько тесно взаимосвязаны, что перед установ-

кой доменных служб Active Directory (Active Directory DS) вы должны установить в сети DNS.

При установке первого контроллера домена в сети Active Directory вам предоставляется возможность автоматически установить DNS, если в сети не обнаружен DNS-сервер. Кроме того, вы можете указать, следует ли полностью интегрировать DNS и Active Directory. В большинстве случаев на оба вопроса следует дать утвердительный ответ. При полной интеграции информация DNS хранится в Active Directory, что позволяет воспользоваться преимуществами Active Directory. Важно понимать различия между частичной и полной интеграцией:

- **Частичная интеграция** При частичной интеграции для хранения информации DNS используется стандартное хранилище — текстовые файлы с расширением .dns в заданной по умолчанию папке %SystemRoot%\System32\Dns. Обновления DNS проводятся через единственный полномочный DNS-сервер. Этот сервер задан как основной DNS-сервер конкретного домена или области внутри домена, которая называется *зоной* (zone). Клиенты, использующие динамическое обновление DNS через DHCP, должны быть настроены на работу с основным DNS-сервером зоны. В противном случае DNS-информация на них обновляться не будет. Более того, если в сети отсутствует основной DNS-сервер, проводить динамические обновления через DHCP нельзя.
- **Полная интеграция** При полной интеграции информация DNS хранится непосредственно в Active Directory, в контейнере dnsZone. Поскольку информация является частью Active Directory, получить доступ к данным DNS может любой контроллер домена, и динамические обновления через DHCP можно проводить по модели с несколькими хозяевами. Это позволяет любому контроллеру домена, на котором запущена служба DNS-сервер (DNS Server), обрабатывать динамические обновления. К тому же, клиенты, использующие динамические обновления DNS через DHCP, могут работать с любым DNS-сервером внутри зоны. Еще одно преимущество интеграции с каталогом состоит в возможности управлять доступом к DNS-информации при помощи системы безопасности каталога.

Присмотревшись внимательнее к способу репликации информации DNS по сети, можно найти и другие преимущества полной интеграции с Active Directory. При частичной интеграции информация DNS хранится и реплицируется отдельно от Active Directory. Имея две отдельные структуры, вы снижаете эффективность как DNS, так и Active Directory, чем усложняете репликацию. С точки зрения репликации изменений DNS менее эффективна, чем Active Directory, поэтому репликация изменений DNS может занять больше ресурсов и времени.

В прежних версиях DNS-сервера для Windows Server перезапуск DNS-сервера в больших организациях со значительным количеством зон, интегрированных в AD DS, мог занимать час и даже больше. Это происходило потому,

что данные зон загружались не в фоновом режиме одновременно с запуском службы DNS. В целях повышения эффективности DNS-серверов в Windows Server 2008 они существенно доработаны и теперь в ходе перезагрузки загружают данные зон из AD DS в фоновом режиме. Это гарантирует способность DNS-сервера отвечать на запросы, в том числе, и из других зон.

В ходе загрузки DNS-серверы, работающие под управлением Windows Server 2008, выполняют следующие задачи:

- перечисляют все загружаемые зоны;
- загружают корневые ссылки из файлов или хранилища AD DS;
- загружают все зоны, хранящиеся в файлах, а не в AD DS;
- начинают отвечать на запросы и вызовы RPC;
- создают один или несколько потоков для загрузки зон, хранящихся в AD DS.

Поскольку данные зоны загружаются отдельными потоками, DNS-сервер способен во время загрузки зон отвечать на запросы. Если DNS-клиент посылает запрос относительно хоста в уже загруженной зоне, DNS-сервер отвечает ему. Если запрос касается компьютера, который еще не загружен в память, DNS-сервер считывает данные хоста из AD DS и соответствующим образом обновляет список записей.

Включение DNS

Чтобы включить DNS в сети, нужно настроить клиенты и серверы DNS. Настройка DNS-клиентов состоит в том, что вы сообщаете им IP-адреса DNS-серверов сети. По этим адресам клиенты связываются с DNS-серверами в любой части сети, даже если серверы находятся в других подсетях.

Примечание Настройка DNS-клиента описана в разделе «Настройка сетей TCP/IP» главы 17. О настройке DNS-сервера речь пойдет в следующем разделе этой главы.

Клиент DNS, встроенный в Windows Vista и Windows Server 2008, поддерживает DNS-трафик по протоколам IPv4 и IPv6. По умолчанию при использовании IPv6 серверам DNS назначаются хорошо известные локальные адреса FEC0:0:0:FFFF::1, FEC0:0:0:FFFF::2 и FEC0:0:0:FFFF::3. Чтобы указать IPv6-адреса DNS-серверов на клиенте, измените параметры TCP/IPv6 при помощи консоли **Сетевые подключения (Network Connections)** или команды IPV6 ADD DNS утилиты *netsh*.

Серверы DNS под управлением Windows Server 2008 теперь в равной степени поддерживают IPv6-адреса и IPv4-адреса. В консоли **Диспетчер DNS (DNS Manager)** адреса хостов отображаются как IPv4 или IPv6-адреса, соответственно. Утилита командной строки Dnscmd также поддерживает оба формата. Кроме того, теперь DNS-серверы способны посылать рекурсивные запросы на серверы с поддержкой только протокола IPv6, тогда как список пересылки сервера может содержать и IPv4-, и IPv6-адреса. И наконец, DNS-серверы поддерживают доменное пространство имен *ip6.arpa* для обратного просмотра.

Если в сети используется DHCP, его следует настроить для работы с DNS. Клиенты DHCP способны регистрировать IPv6-адреса как вместе с IPv4-адресами, так и вместо них. Для обеспечения надлежащей интеграции DHCP и DNS задайте параметры области DHCP, как описано в предыдущей главе. Для IPv4 следует задать параметры области **006 DNS-серверы (006 DNS Servers)** и **015 DNS-имя домена (015 DNS Domain Name)**. Для IPv6 следует установить параметры области **00023 Список адресов IPv6 рекурсивных серверов имен DNS (00023 DNS Recursive Name Server IPV6 Address)** и **00024 Список поиска доменов (00024 Domain Search List)**. Кроме того, если вам нужно организовать доступ к компьютерам сети из других доменов Active Directory, создайте для них записи в DNS. Записи DNS упорядочены по зонам, где зона — просто область внутри домена.

Если DNS-сервер не доступен, DNS-клиент, работающий под управлением Windows Vista или Windows Server 2008, для разрешения имен в локальном сегменте сети может использовать протокол многоадресного разрешения имен локальных ссылок LLMNR. Кроме того, он периодически проводит поиск контроллеров домена, членом которого является. Это позволяет избежать проблем с производительностью, которые могут возникнуть, когда DNS-клиент устанавливает связь с удаленным контроллером домена на медленном канале, а не с локальным контроллером, который оказался временно недоступен из-за сбоя сети или сервера. Ранее такая связь поддерживалась до тех пор, пока клиент не проводил вынужденный поиск нового контроллера домена, например, после того клиентский ПК был надолго отключен от сети. Периодическое обновление связи с контроллером домена сокращает вероятность того, что DNS-клиент будет ассоциирован с неправильным доменом.

Примечание Вы можете настроить клиентский компьютер DNS, работающий под управлением Windows Vista или Windows Server 2008, чтобы он определял расположение ближайшего контроллера домена, а не выполнял случайный поиск. Это повышает производительность в сетях, содержащих домены, связанные медленными каналами. С другой стороны, в процессе поиска генерируется сетевой трафик, поэтому обнаружение ближайшего контроллера домена может иметь и негативные последствия для производительности сети.

В системе Windows Server 2008 введены основные зоны только для чтения и зона GlobalNames. Основная зона только для чтения автоматически создается для поддержки контроллера домена, доступного только для чтения (RODC). Когда компьютер становится RODC-контроллером, он реплицирует с доступом только для чтения полную копию всех разделов каталога приложений, используемых DNS, включая раздел домена, а также зоны DNS леса и домена. Это гарантирует наличие на DNS-сервере RODC полной копии всех зон DNS. Администратор RODC может просматривать содержимое основной зоны, но не может изменять его. Редактировать содержимое зоны можно только на стандартном контроллере домена.

Для поддержки всех сред DNS и разрешения однокомпонентных имен создается зона GlobalNames. Чтобы обеспечить оптимальную производи-

тельность и поддержку в различных лесах, интегрируйте эту зону с AD DS и настройте каждый полномочный DNS-сервер при помощи локальной копии. Если вы публикуете расположение зоны GlobalNames при помощи записи ресурса Расположение службы (SRV) (Service Location (SRV)), зона предоставляет уникальные однокомпонентные имена по всему лесу. В отличие от WINS, зона GlobalNames предназначена для разрешения однокомпонентных имен для подмножества имен хостов, обычно записей ресурса CNAME для корпоративных серверов. Зона GlobalNames не предназначена для разрешения одноранговых имен, например, разрешения имен рабочих станций. Для этого существует LLMNR.

Если зона GlobalNames настроена правильно, разрешение однокомпонентных имен работает следующим образом:

1. К однокомпонентному имени, которое запрашивает клиент, добавляется основной DNS-суффикс клиента. Затем запрос передается DNS-серверу.
2. Если полное имя компьютера не удается разрешить, клиент запрашивает разрешение при помощи списков поиска DNS-суффикса, если они имеются.
3. Если ни один из вариантов имени не удается разрешить, клиент запрашивает разрешение посредством однокомпонентного имени.
4. Если однокомпонентное имя имеется в зоне GlobalNames, имя разрешает DNS-сервер, на котором размещена зона. В противном случае, запрос передается в WINS.

Зона GlobalNames обеспечивает разрешение однокомпонентных имен только при условии, что все уполномоченные DNS-серверы работают под управлением Windows Server 2008. Впрочем, иные DNS-серверы, которые не являются уполномоченными ни в одной зоне, могут работать под управлением других ОС. Динамические обновления в зоне GlobalNames не поддерживаются.

Настройка разрешения имен на DNS-клиентах

Способ настройки разрешения имен на DNS-клиентов зависит от конфигурации сети. Если в ней применяется DHCP, настройка DNS осуществляется при помощи параметров DHCP-сервера. Если на компьютерах используются статические IP-адреса или вы хотите особо настроить DNS для отдельного пользователя или системы, придется настроить DNS вручную.

Параметры DNS задаются на вкладке **DNS** диалогового окна **Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)**. Чтобы открыть это окно, выполните следующие действия:

1. В окне **Центр управления сетями и общим доступом (Network And Sharing Center)** щелкните ссылку **Управление сетевыми подключениями (Manage Network Connections)**. В окне **Сетевые подключения (Network Connections)** щелкните правой кнопкой нужное подключение и выберите команду **Свойства (Properties)**.
2. Дважды щелкните протокол, соответствующий типу настраиваемого IP-адреса — **TCP/IPv6** или **TCP/IPv4**.

3. Если вы используете DHCP и хотите, чтобы адрес DNS-сервера был задан посредством DHCP, установите переключатель **Получить адрес DNS-сервера автоматически (Obtain DNS Server Address Automatically)**. В противном случае установите переключатель **Использовать следующие адреса DNS-серверов (Use The Following DNS Server Addresses)**, а затем введите адреса основного и дополнительного DNS-серверов в соответствующих полях.
4. Щелкните кнопку **Дополнительно (Advanced)**, чтобы открыть диалоговое окно **Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)**. Перейдите на вкладку **DNS**.

Далее описаны параметры вкладки **DNS**:

- **Адреса DNS-серверов, в порядке использования (DNS Server Addresses, In Order Of Use)** Укажите IP-адрес каждого DNS-сервера, используемого для разрешения доменных имен. Чтобы добавить IP-адрес сервера в список, щелкните **Добавить (Add)**. Щелкните **Удалить (Remove)**, чтобы удалить адрес выделенного сервера из списка. Для редактирования выделенной записи щелкните **Изменить (Edit)**. Если вы указываете несколько серверов DNS, их приоритет определяется очередностью в списке. Если первый сервер не может ответить на запрос о разрешении имени хоста, запрос посылается на следующий DNS-сервер и т. д. Чтобы изменить положение сервера в списке, выделите его и воспользуйтесь кнопками со стрелками вверх и вниз.
- **Дописывать основной DNS-суффикс и суффикс подключения (Append Primary And Connection Specific DNS Suffixes)** Обычно по умолчанию этот переключатель установлен. Он применяется для разрешения неполных имен компьютеров в основном домене. Допустим, вы обращаетесь к компьютеру Gandolf в родительском домене microsoft.com. Для разрешения имя компьютера будет автоматически дополнено суффиксом DNS — gandolf.microsoft.com. Если в основном домене компьютера с таким именем нет, запрос не выполняется. Основной домен задается на вкладке **Имя компьютера (Computer Name)** диалогового окна **Свойства системы (System Properties)**.
- **Дописывать родительские суффиксы основного DNS-суффикса (Append Parent Suffixes Of The Primary DNS Suffix)** По умолчанию этот флажок установлен. Он используется для разрешения неполных имен компьютеров в иерархии родительских и дочерних доменов. В случае неудачного запроса в ближайшем родительском домене, для попытки разрешения запроса используется суффикс родительского домена более высокого уровня. Этот процесс продолжается, пока не будет достигнута вершина иерархии доменов DNS. Допустим, в запросе указано имя компьютера Gandolf в родительском домене dev.microsoft.com. Сначала DNS пытается разрешить имя компьютера gandolf.dev.microsoft.com, а потом, в случае неудачи, пытается разрешить имя gandolf.microsoft.com.

- **Дописывать следующие DNS-суффиксы (по порядку) (Append These DNS Suffixes (In Order))** Установите этот переключатель, чтобы задать использование особых DNS-суффиксов вместо имени родительского домена. Щелкните **Добавить (Add)**, чтобы добавить суффикс домена в список. Щелкните **Удалить (Remove)**, чтобы удалить выделенный суффикс домена из списка. Для редактирования выделенной записи щелкните **Изменить (Edit)**. Вы можете указать несколько суффиксов домена. Если первый суффикс не позволяет разрешить имя, DNS применяет следующий суффикс из списка. В случае неудачи берется следующий суффикс и т. д. Чтобы изменить очередность суффиксов домена, выберите нужный суффикс и измените его положение кнопками со стрелками вверх и вниз.
- **DNS-суффикс подключения (DNS Suffix For This Connection)** В этом поле задается DNS-суффикс подключения, перекрывающий DNS-имена, уже настроенные на использование с данным подключением.
- **Зарегистрировать адреса этого подключения в DNS (Register This Connection's Addresses In DNS)** Установите этот флажок, если хотите, чтобы все IP-адреса данного подключения регистрировались в DNS с FQDN-именами компьютеров. Этот флажок по умолчанию установлен.

Примечание Динамические обновления DNS в сочетании с DHCP применяются, чтобы позволить клиенту обновлять свою запись A (Host Address) в случае изменения IP-адреса, а также чтобы позволить DHCP-серверу обновлять запись PTR (Pointer) клиента на DHCP-сервере. Вы также можете настроить DHCP-серверы на обновление обеих записей (A и PTR) от имени клиента. Динамические обновления DNS поддерживаются только BIND 5.1 или более высокими версиями DNS-серверов, а также Microsoft Windows 2000 Server, Microsoft Windows Server 2003 и более поздними серверными версиями Windows. Эта функциональная возможность не поддерживается в Microsoft Windows NT Server 4.

- **Использовать DNS-суффикс подключения при регистрации в DNS (Use This Connection's DNS Suffix In DNS Registration)** Установите этот флажок, если хотите, чтобы все IP-адреса для данного подключения регистрировались в DNS родительского домена.

Установка DNS-сервера

Вы можете настроить систему Windows Server 2008 как DNS-сервер одного из четырех типов:

- **Основной сервер, интегрированный в Active Directory (Active Directory-integrated primary server)** Сервер DNS, полностью интегрированный в Active Directory. Все данные DNS хранятся непосредственно в Active Directory.
- **Основной сервер (primary server)** Основной DNS-сервер домена, частично интегрированный в Active Directory. На таком сервере основная копия записей DNS и файлы конфигурации домена — текстовые файлы с расширением .dns.

- **Дополнительный сервер (secondary server)** Резервный сервер DNS. Хранит копию DNS-записей, полученную с основного сервера и передачи зон для обновлений. Дополнительный сервер при запуске получает всю информацию DNS с основного сервера. Эта информация хранится до обновления или до истечения срока действия.
- **Сервер пересылки (forwarding-only server)** Сервер, кеширующий информацию DNS после просмотров и всегда передающий запросы на другие серверы. Сервер пересылки хранит информацию DNS до обновления, до истечения срока действия или до перезапуска сервера. В отличие от дополнительных серверов сервер пересылки не запрашивает полную копию файлов БД зоны. Это означает, что при запуске сервера пересылки его БД пуста.

Перед настройкой DNS-сервера требуется установить службу DNS-сервер (DNS Server).

Установка и настройка службы DNS-сервер (DNS Server)

В роли DNS-сервера могут выступать все контроллеры домена, и вам было предложено установить и настроить DNS в ходе установки контроллера домена. Если вы ответили положительно, DNS у вас уже установлена с автоматически заданной стандартной конфигурацией. Переустановки не требуется.

Если вы работаете не с контроллером домена, а с рядовым сервером, или если служба DNS не установлена, выполните следующие действия:

1. В консоли **Диспетчер сервера (Server Manager)** выберите узел **Роли (Roles)** и щелкните ссылку **Добавить роли (Add Roles)**. Откроется Мастер добавления ролей (Add Roles Wizard). Если работа мастера начинается с вводной страницы, ознакомьтесь с ее содержанием и щелкните **Далее (Next)**.
2. На странице **Выбор ролей сервера (Select Server Roles)** выберите **DNS-сервер (DNS Server)** и два раза щелкните **Далее (Next)**.
3. Щелкните **Установить (Install)**. По окончанию установки служба DNS-сервер (DNS Server) будет запускаться автоматически при каждой перезагрузке сервера. Если служба не запускается, выполните запуск вручную. Подробнее — в разделе «Запуск и остановка DNS-сервера».

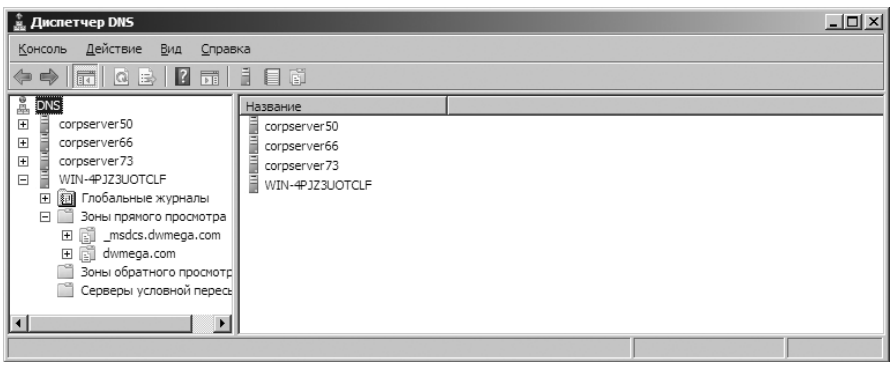


Рис. 20-1. Консоль Диспетчер DNS (DNS Manager) предназначена для управления DNS-серверами сети

4. Откройте консоль **Диспетчер DNS (DNS Manager)**, выбрав команду **DNS** в меню **Администрирование (Administrative Tools)**. Консоль **Диспетчер DNS (DNS Manager)** показана на рис. 20-1.
5. Если настраиваемый сервер отсутствует в дереве консоли, к нему нужно подключиться. Щелкните правой кнопкой элемент **DNS** и выберите команду **Подключение к DNS-серверу (Connect To DNS Server)**. Затем выполните одно из следующих действий:
   - Если вы подключаетесь к локальному серверу, установите переключатель **Этот компьютер (This Computer)** и щелкните **OK**.
   - Чтобы подключиться к удаленному серверу, установите переключатель **Другой компьютер (The Following Computer)** и введите имя или IP-адрес сервера. Затем щелкните **OK**.
6. Запись DNS-сервера будет включена в дерево консоли **Диспетчер DNS (DNS Manager)**. Щелкните правой кнопкой запись сервера и выберите в контекстном меню команду **Настроить DNS-сервер (Configure A DNS Server)**. Откроется Мастер настройки DNS-сервера (Configure A DNS Server Wizard). Щелкните **Далее (Next)**.
7. На странице **Выбор действия по настройке (Select Configuration Action)**, показанной на стр. 20-2, установите переключатель **Настроить только корневые ссылки (Configure Root Hints Only)**. Этим вы укажете, что в данный момент следует создать только основу структуры DNS.

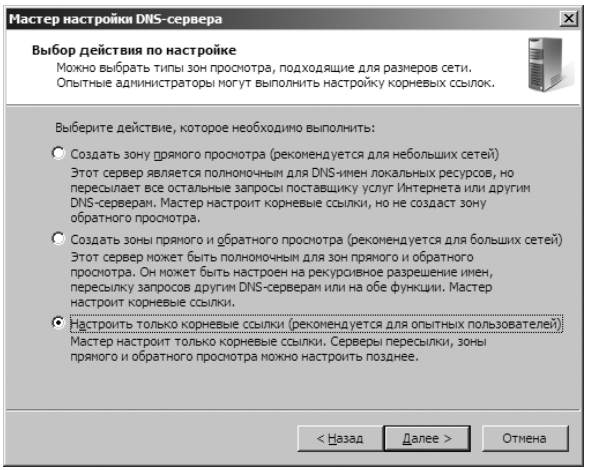


Рис. 20-2. Настройка корневых ссылок DNS

8. Щелкните **Далее (Next)**. Мастер проведет поиск существующих корневых ссылок DNS и при необходимости настроит их.
9. Щелкните **Готово (Finish)**.

Настройка основного DNS-сервера

Основной DNS-сервер — интегрированный в Active Directory или обычный основной сервер — должен быть в каждом домене. На основном сервере должны быть зоны прямого и обратного просмотра. Прямой просмотр служит для разрешения доменных имен в IP-адреса. Обратный просмотр нужен для проверки подлинности DNS-запросов посредством разрешения IP-адресов в доменные или хост-имена.

Чтобы настроить основной сервер после установки службы DNS-сервер (DNS Server), выполните следующие действия:

1. Откройте консоль **Диспетчер DNS (DNS Manager)** и подключитесь к серверу, который хотите настроить.
2. Щелкните правой кнопкой сервер в дереве консоли и выберите команду **Создать новую зону (New Zone)**. Откроется Мастер создания новой зоны (New Zone Wizard). Щелкните **Далее (Next)**.

Примечание Альтернативой консоли **Диспетчер DNS (DNS Manager)** может стать узел DNS-сервер (DNS Server) консоли **Диспетчер сервера (Server Manager)**. Откройте его и щелкните подузел **DNS**.

3. Выберите тип зоны (рис. 20-3). Если вы настраиваете основной сервер, интегрированный с Active Directory, установите переключатель **Основная зона (Primary Zone)** и убедитесь, что установлен флажок **Сохранять зону в Active Directory (Store The Zone In Active Directory)**. Если вы не хотите интегрировать DNS в Active Directory, установите переключатель **Основная зона (Primary Zone)** и сбросьте флажок **Сохранять зону в Active Directory (Store The Zone In Active Directory)**. Щелкните **Далее (Next)**.

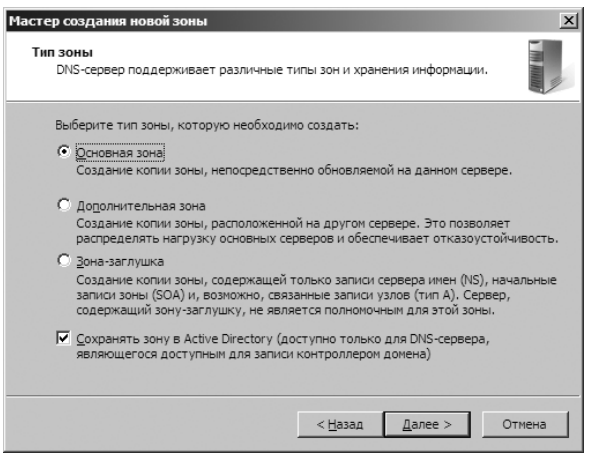


Рис. 20-3. Выбор типа зоны в Мастере создания новой зоны (New Zone Wizard)

4. Если вы интегрируете зону с Active Directory, выберите стратегию репликации. В противном случае, перейдите к шагу 6.

- **Для всех DNS-серверов в этом лесу (To All DNS Servers In This Forest)** Это обширнейшая стратегия репликации. Помните, что лес Active Directory включает все деревья доменов, использующие данные каталога совместно с текущим доменом.
- **Для всех DNS-серверов в этом домене (To All DNS Servers In This Domain)** Выберите эту стратегию, чтобы реплицировать информацию DNS внутри текущего домена и его дочерних доменов.
- **Для всех контроллеров домена в этом домене (To All Domain Controllers In This Domain)** Выберите эту стратегию, если хотите реплицировать информацию DNS на все контроллеры домена внутри текущего домена и его дочерних доменов. Хотя эта стратегия обеспечивает более широкую репликацию информации DNS внутри домена, не каждый контролер домена является DNS-сервером (вам и не нужно настраивать каждый контроллер домена как DNS-сервер).

5. Щелкните **Далее (Next)**. Установите переключатель **Зона прямого просмотра (Forward Lookup Zone)** и щелкните **Далее (Next)**.
6. Введите полное DNS-имя зоны. Оно помогает определить, как сервер или зона вписываются в доменную иерархию DNS. Например, если вы создаете основной сервер для домена microsoft.com, в качестве имени зоны следует ввести microsoft.com. Щелкните **Далее (Next)**.
7. Если вы настраиваете основную зону, не интегрированную в Active Directory, вам нужно задать имя зонного файла. Имя файла БД зоны DNS по умолчанию должно быть уже введено. Оставьте это имя без изменений или введите новое. Щелкните **Далее (Next)**.
8. Укажите, следует ли разрешить динамические обновления. У вас есть три возможности:
   - **Разрешить только безопасные динамические обновления (Allow Only Secure Dynamic Updates)** Если зона интегрирована в Active Directory, вы можете воспользоваться списками ACL, чтобы ограничить круг клиентов, которые могут выполнять динамические обновления. Если вы установите этот переключатель, динамически обновлять записи ресурсов смогут только клиенты с учетными записями компьютеров, прошедшими проверку, и одобренными ACL.
   - **Разрешить любые динамические обновления (Allow Both Nonsecure And Secure Dynamic Updates)** Установите этот переключатель, чтобы позволить любому клиенту обновлять его записи ресурса в DNS при наличии изменений.
   - **Запретить динамические обновления (Do Not Allow Dynamic Updates)** Этот переключатель отключает динамические обновления DNS. Его следует использовать только при отсутствии интеграции зоны с Active Directory.

9. Щелкните **Далее (Next)**, затем щелкните **Готово (Finish)**, чтобы завершить процесс. Новая зона добавляется на сервер, и автоматически создаются базовые DNS-записи.
10. Один DNS-сервер может предоставлять услуги DNS в нескольких доменах. Если у вас есть несколько родительских доменов, например, microsoft.com и msn.com, настройте другие зоны прямого просмотра, повторив описанные выше действия. Создание зон обратного просмотра описано в разделе «Настройка обратного просмотра».
11. Создайте дополнительные записи для компьютеров, к которым хотите открыть доступ из других DNS-доменов, выполнив действия, описанные в разделе «Управление DNS-записями».

Ближе к реальности В большинстве сетей используются закрытые и открытые области. В открытых областях сети расположены веб-, FTP- и внешний почтовый серверы. Доступ к открытым областям сети организации не должен быть неограниченным. Открытые области сети должны быть настроены как часть сетей периметра, защищенных брандмауэром, имеющих ограниченный внешний доступ и не предоставляющих доступа во внутреннюю сеть. Открытая область сети может также полностью отделяться от внутренней сети.

Закрытая область сети — это область, в которой расположены внутренние серверы и рабочие станции организации. Параметры DNS открытой области находятся в общем Интернет-пространстве. Здесь вы можете использовать DNS-имена .com, .org или .net и общие IP-адреса, приобретенные или арендованные. В закрытых областях сети параметры DNS относятся к закрытому пространству сети. Здесь вы можете использовать adatum.com в качестве DNS-имени организации и применять частные IP-адреса. Подробнее в разделе — «Настройка сетей TCP/IP» главы 17.

Настройка дополнительного DNS-сервера

Дополнительные серверы обеспечивают отказоустойчивость DNS-службы сети. Если вы используете полную интеграцию с Active Directory, настраивать дополнительные серверы вам не нужно. Достаточно запустить службу DNS на нескольких контроллерах домена, и Active Directory будет реплицировать информацию DNS на все контроллеры. При использовании частичной интеграции следует настроить дополнительные серверы, чтобы уменьшить нагрузку на основной сервер. В небольшой или средней сети можно использовать в качестве дополнительных серверов DNS-серверы поставщика услуг Интернет. Свяжитесь с провайдером, чтобы узнать подробности.

На дополнительных серверах для большинства типов запросов используются зоны прямого просмотра, поэтому зоны обратного просмотра вам, вероятно, не понадобятся. Но не забывайте, что они необходимы основным серверам, поэтому вы должны настроить зоны обратного просмотра, чтобы обеспечить корректное разрешение доменных имен.

Чтобы установить дополнительные серверы для повышения отказоустойчивости и балансировки нагрузки, выполните следующие действия:

1. Откройте консоль **Диспетчер DNS (DNS Manager)** и подключитесь к нужному серверу.
2. Щелкните правой кнопкой элемент сервера и выберите команду **Создать новую зону (New Zone)**. Откроется Мастер создания новой зоны (New Zone Wizard). Щелкните **Далее (Next)**.
3. На странице **Тип зоны (Zone Type)** установите переключатель **Дополнительная зона (Secondary Zone)**. Щелкните **Далее (Next)**.
4. На дополнительных серверах используются зоны как прямого, так и обратного просмотра. В первую очередь создаются зоны прямого просмотра, поэтому установите переключатель **Зона прямого просмотра (Forward Lookup Zone)** и щелкните **Далее (Next)**.
5. Введите полное DNS-имя зоны и щелкните **Далее (Next)**.
6. В списке **Основные серверы (Master Servers)** введите IP-адрес основного сервера зоны и нажмите Enter. Мастер попытается проверить сервер. Если произошла ошибка, убедитесь, что сервер подключен к сети и вы ввели правильный IP-адрес. Если вы хотите скопировать данные зоны из других серверов на случай недоступности первого сервера, повторите этот шаг.
7. Щелкните **Далее (Next)** и **Готово (Finish)**. В большой сети вам, возможно, потребуется настройка зон обратного просмотра на дополнительных серверах. Подробнее — в следующем разделе.

Настройка обратного просмотра

Прямой просмотр нужен для разрешения доменных имен в IP-адреса, обратный просмотр — для разрешения IP-адресов в доменные имена. В каждом сегменте сети должна быть зона обратного просмотра. В частности, если у вас есть подсети 192.168.10.0, 192.168.11.0 и 192.168.12.0, у вас должно быть три зоны обратного просмотра.

Стандартное имя зоны обратного просмотра составляется из идентификатора сети, выстроенного в обратном порядке, и суффикса in-addr.arpa. Зоны обратного просмотра из предыдущего примера будут называться 10.168.192.in-addr.arpa, 11.168.192.in-addr.arpa и 12.168.192.in-addr.arpa. Записи зон обратного и прямого просмотра должны быть синхронизированы. В случае сбоя синхронизации в домене может произойти сбой проверки подлинности.

Чтобы создать зону обратного просмотра, выполните следующие действия:

1. Откройте консоль **Диспетчер DNS (DNS Manager)** и подключитесь к нужному серверу.
2. Щелкните правой кнопкой элемент сервера и выберите команду **Создать новую зону (New Zone)**. Откроется Мастер создания новой зоны (New Zone Wizard). Щелкните **Далее (Next)**.
3. Если вы настраиваете основной сервер, интегрированный с Active Directory, установите переключатель **Основная зона (Primary Zone)** и убеди-

тесь, что установлен флажок **Сохранять зону в Active Directory (Store The Zone In Active Directory)**. Если вы не хотите интегрировать DNS в Active Directory, установите переключатель **Основная зона (Primary Zone)** и сбросьте флажок **Сохранять зону в Active Directory (Store The Zone In Active Directory)**. Щелкните **Далее (Next)**.

4. Если вы настраиваете зону обратного просмотра для дополнительного сервера, установите переключатель **Дополнительная зона (Secondary Zone)** и щелкните **Далее (Next)**.
5. Если вы интегрируете зону с Active Directory, выберите одну из следующих стратегий репликации:
   - **Для всех DNS-серверов в этом лесу (To All DNS Servers In This Forest)** Это обширнейшая стратегия репликации. Помните, что лес Active Directory включает все деревья доменов, использующие данные каталога совместно с текущим доменом.
   - **Для всех DNS-серверов в этом домене (To All DNS Servers In This Domain)** Выберите эту стратегию, чтобы реплицировать информацию DNS внутри текущего домена и его дочерних доменов.
   - **Для всех контроллеров домена в этом домене (To All Domain Controllers In This Domain)** Выберите эту стратегию, если хотите реплицировать информацию DNS на все контроллеры домена внутри текущего домена и его дочерних доменов. Хотя эта стратегия обеспечивает более широкую репликацию информации DNS внутри домена, не каждый контроллер домена является DNS-сервером (вам и не нужно настраивать каждый контроллер домена как DNS-сервер).
6. Установите переключатель **Зона обратного просмотра (Reverse Lookup Zone)**. Щелкните **Далее (Next)**.
7. Укажите, для каких адресов вы хотите создать зону обратного просмотра (**IPv4** или **IPv6**) и щелкните **Далее (Next)**. Выполните одно из следующих действий:
   - Если вы проводите настройку для IPv4, введите идентификатор сети для зоны обратного просмотра. Вводимые значения определяют стандартное имя зоны обратного просмотра. Щелкните **Далее (Next)**.

Примечание Если в одной и той же сети существует несколько подсетей, например, 192.168.10 и 192.168.11, в имя зоны можно ввести только сетевую часть имени. В нашем примере можно использовать 168.192.in-addr.arpa, позволив консоли **Диспетчер DNS (DNS Manager)** самостоятельно создать необходимые зоны подсети.

   - Если вы проводите настройку для IPv6, введите префикс сети для зоны обратного просмотра. Имена зон автоматически генерируются на основе вводимых значений. В зависимости от введенного префикса вы можете создать до восьми зон. Щелкните **Далее (Next)**.

8. Если вы настраиваете основной или дополнительный сервер, не интегрированный в Active Directory, задайте имя файла зоны. Стандартное имя файла для БД зоны DNS должно быть уже введено. Оставьте его неизменным или введите новое имя. Щелкните **Далее (Next)**.
9. Укажите, следует ли разрешить динамические обновления. У вас есть три возможности:
   - **Разрешить только безопасные динамические обновления (Allow Only Secure Dynamic Updates)** Если зона интегрирована в Active Directory, вы можете воспользоваться списками ACL, чтобы ограничить круг клиентов, которые могут выполнять динамические обновления. Если вы установите этот переключатель, динамически обновлять записи ресурсов смогут только клиенты с учетными записями компьютеров, прошедшими проверку, и одобренными ACL.
   - **Разрешить любые динамические обновления (Allow Both Nonsecure And Secure Dynamic Updates)** Установите этот переключатель, чтобы позволить любому клиенту обновлять его записи ресурса в DNS при наличии изменений.
   - **Запретить динамические обновления (Do Not Allow Dynamic Updates)** Этот переключатель отключает динамические обновления DNS. Его следует использовать только при отсутствии интеграции зоны с Active Directory.
10. Щелкните **Далее (Next)**, затем щелкните **Готово (Finish)**, чтобы завершить процесс. Новая зона добавляется на сервер, и автоматически создаются базовые DNS-записи.

После установки зон обратного просмотра необходимо убедится в правильности обработки делегирования для зоны. Свяжитесь с информационным отделом или поставщиком услуг Интернета, чтобы проверить регистрацию зон в родительском домене.

Настройка глобальных имен

Зона GlobalNames — это специальная зона прямого просмотра, которую нужно интегрировать в AD DS. Если все ваши DNS-серверы работают под управлением Windows Server 2008, при развертывании зоны GlobalNames WINS не используется — создаются статические глобальные записи с однокомпонентными именами. Это позволяет пользователям получать доступ к хостам по однокомпонентным именам, не прибегая к FQDN-именам. Использовать зону GlobalNames нужно в случаях, если вы все разрешение имен решили возложить на DNS, например, отказавшись от WINS, чтобы в перспективе полностью перейти на IPv6. Поскольку для регистрации обновлений в зоне GlobalNames нельзя использовать динамические обновления, настраивать разрешение однокомпонентных имен следует только для основных серверов.

Чтобы развернуть зону GlobalNames, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** щелкните правой кнопкой узел **Зоны прямого просмотра (Forward Lookup Zones)** и выберите команду **Создать новую зону (New Zone)**. В Мастере создания новой зоны (New Zone Wizard) щелкните **Далее (Next)**, чтобы по умолчанию создать основную зону, интегрированную с AD DS. На странице **Область репликации зоны, интегрированной в Active Directory (Active Directory Zone Replication Scope)** задайте репликацию зоны в лесе и щелкните **Далее (Next)**. На странице **Имя зоны (Zone Name)** введите имя **GlobalNames**. Два раза щелкните **Далее (Next)** и **Готово (Finish)**.
2. На каждом полномочном DNS-сервере леса введите в командной строке с повышенными полномочиями следующую команду:

   ```
   dnscmd ИмяСервера /enableglobalnamessupport 1
   ```

   где *ИмяСервера* — имя DNS-сервера, на котором расположена зона GlobalNames. Чтобы указать локальный компьютер, вместо имени сервера поставьте точку (.), наример, **dnscmd . /enableglobalnamessupport 1.**
3. Для каждого сервера, доступ к которому должны иметь пользователи, в зону GlobalNames добавьте запись CNAME: в консоли **Диспетчер DNS (DNS Manager)** щелкните правой кнопкой узел **GlobalNames**, выберите команду **Создать псевдоним (CNAME) (New Alias (CNAME))** и создайте новую запись ресурса в открывшемся диалоговом окне.

Примечание Полномочный DNS-сервер разрешает запросы в следующем порядке: 1) по данным локальной зоны, 2) по данным зоны GlobalNames, 3) при помощи DNS-суффиксов, 4) при помощи WINS. Выполняя динамические обновления, полномочный DNS-сервер сначала проверяет зону GlobalNames, затем — локальную зону.

Совет Если вы хотите, чтобы DNS-клиенты в другом лесе использовали для разрешения имен зону GlobalNames, добавьте запись ресурса **Расположение службы (SRV) (Service Location (SRV))** с указанием имени службы _globalnames._msdcs в DNS-раздел, охватывающий весь лес. Запись должна содержать полное доменное имя DNS-сервера, на котором размещена зона GlobalNames.

Управление DNS-серверами

Консоль **Диспетчер DNS (DNS Manager)** позволяет управлять локальными и удаленными DNS-серверами. Как показано на рис. 20-4, главное окно консоли состоит из двух панелей. Левая панель открывает доступ к DNS-серверам и их зонам. На правой панели отображены сведения о выбранном элементе. Есть три способа работы с консолью **Диспетчер DNS (DNS Manager)**:

- Дважды щелкните элемент на левой панели, чтобы развернуть список файлов для этого элемента.
- Выделите элемент на левой панели, чтобы просмотреть на правой панели сведения о нем, например, состояние зоны и доменные записи.

- Щелкните элемент правой кнопкой, чтобы открыть контекстное меню с доступными командами.

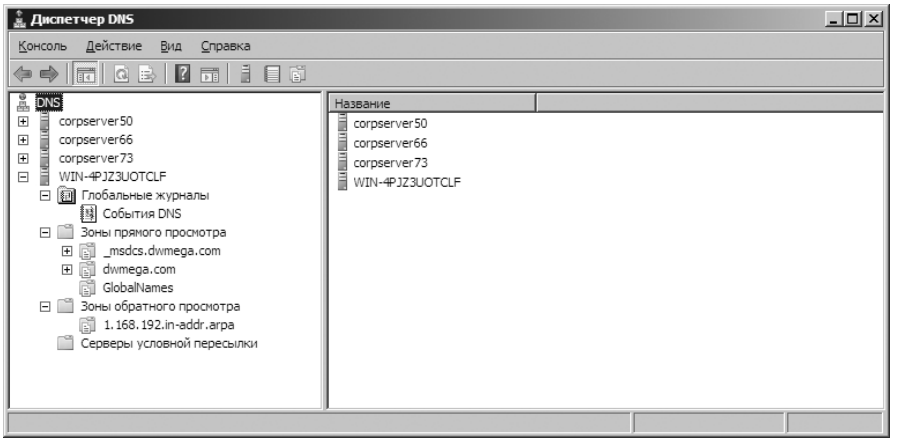


Рис. 20-4. Управление доменами в папках Зоны прямого просмотра (Forward Lookup Zones) и Зоны обратного просмотра (Reverse Lookup Zones)

Папки **Зоны прямого просмотра (Forward Lookup Zones)** и **Зоны обратного просмотра (Reverse Lookup Zones)** открывают доступ к доменам и подсетям, настроенным для использования на данном сервере. Выбирая папки домена или подсети в левой панели, вы сможете управлять соответствующими DNS-записями.

Добавление удаленных серверов в консоль Диспетчер DNS (DNS Manager)

Чтобы управлять удаленными DNS-серверами из консоли **Диспетчер DNS (DNS Manager)**, выполните следующие действия:

1. В дереве консоли щелкните правой кнопкой **DNS** и выберите команду **Подключение к DNS-серверу (Connect To DNS Server)**.
2. Если вы подключаетесь к локальному компьютеру, установите переключатель **Этот компьютер (This Computer)**. В противном случае установите переключатель **Другой компьютер (The Following Computer)** и введите IP-адрес или FQDN-имя удаленного компьютера, к которому вы хотите подключиться.
3. Щелкните **OK**. Система Windows Server 2008 попытается подключиться к серверу. В случае успеха сервер будет добавлен в консоль.

Примечание Если сервер отключен от сети или недоступен по другим причинам — из-за ограничений системы безопасности или сбоя службы процедуры удаленного вызова (RPC), — подключение не состоится. Но вы вольны добавить сервер в консоль без подключения, щелкнув **Да (Yes)** в ответ на предложение системы.

Удаление сервера из консоли DNS

Чтобы удалить сервер из консоли **Диспетчер DNS (DNS Manager)**, достаточно выделить его запись и нажать Delete. Щелкните **OK**, чтобы подтвердить удаление. Удаление сервера только стирает его запись в дереве консоли. Сам сервер не удаляется.

Запуск и остановка DNS-сервера

Для управления DNS-серверами используется служба DNS-сервер (DNS Server). Вы можете включить, остановить, приостановить, продолжить и перезапустить службу DNS-сервер (DNS Server) из консоли **Диспетчер сервера (Server Manager)** или из командной строки. Кроме того, службой DNS-сервер (DNS Server) можно управлять в консоли **Диспетчер DNS (DNS Manager)**. Щелкните правой кнопкой сервер, которым хотите управлять, раскройте подменю **Все задачи (All Tasks)** и выберите команду **Запустить (Start)**, **Остановить (Stop)**, **Приостановить (Pause)**, **Продолжить (Resume)** или **Перезапустить (Restart)**.

Создание дочерних доменов внутри зон

Консоль **Диспетчер DNS (DNS Manager)** позволяет создавать внутри зоны дочерние домены. Допустим, вы создали основную зону — *microsoft.com*. В этой зоне можно создать поддомены *hr.microsoft.com* и *mis.microsoft.com*. Чтобы создать дочерний домен, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** разверните папку **Зоны прямого просмотра (Forward Lookup Zones)** нужного сервера.
2. Щелкните правой кнопкой запись родительского домена и выберите в контекстном меню команду **Создать домен (New Domain)**.
3. Введите имя нового домена и щелкните **OK**. Например, чтобы создать домен hr.microsoft.com, введите **hr**.

Создание дочерних доменов в отдельных зонах

По мере роста организации иногда нужно разделить пространство имен DNS на отдельные зоны. Штаб-квартира корпорации может находиться в зоне родительского домена (*microsoft.com*). Филиалы могут иметь зону для каждого офиса, например, *memphis.microsoft.com*, *newyork.microsoft.com* и *la.microsoft.com*.

Чтобы создать дочерние домены в раздельных зонах, выполните следующие действия:

1. В каждом дочернем домене установите DNS-сервер и создайте необходимые зоны прямого и обратного просмотра для дочернего домена.
2. Делегируйте полномочия для каждого дочернего домена на полномочном DNS-сервере родительского домена. Делегирование полномочий позволяет дочернему домену разрешать и отвечать на DNS-запросы компьютеров, находящихся внутри и за пределами локальной подсети.

Чтобы делегировать полномочия дочернему домену, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** разверните папку **Зоны прямого просмотра (Forward Lookup Zones)** нужного сервера.
2. Щелкните правой кнопкой запись родительского домена и выберите в контекстном меню команду **Создать делегирование (New Delegation)**. Откроется Мастер делегирования (New Delegation Wizard). Щелкните **Далее (Next)**.
3. Введите имя домена, например, **hr** (рис. 20-5) и щелкните **Далее (Next)**. Введенное имя будет отражено в поле **Полное доменное имя (Fully Qualified Domain Name)**.

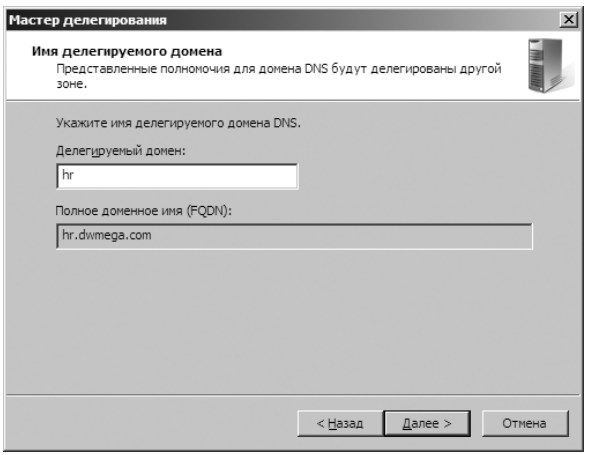


Рис. 20-5. Введя имя делегируемого домена, вы задаете полностью определенное доменное имя

4. Щелкните **Добавить (Add)**. Откроется диалоговое окно **Новая запись сервера имен (New Name Server Record)**.
5. В поле **Полное доменное имя сервера (Server Fully Qualified Domain Name)** введите полное хост-имя DNS-сервера дочернего домена, например, **corpserver01.memphis.adatum.com**. Щелкните **Разрешить в адрес (Resolve)**. Сервер пошлет запрос и добавит разрешенный IP-адрес в список **IP-адрес (IP Address)**.
6. Повторите шаг 5, чтобы указать дополнительные серверы имен. Порядок записей определяет, какой из IP-адресов будет использован первым. При необходимости измените порядок с помощью кнопок **Вверх (Up)** и **Вниз (Down)**. Щелкните **OK**, чтобы закрыть диалоговое окно **Новая запись сервера имен (New Name Server Record)**.
7. Щелкните **Далее (Next)** и **Готово (Finish)**.

Удаление домена или подсети

Удаление домена или подсети окончательно удаляет их из DNS-сервера. Чтобы удалить домен или подсеть, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** щелкните правой кнопкой запись домена или подсети.
2. В контекстном меню выберите команду **Удалить (Delete)**. Подтвердите действие, щелкнув **Да (Yes)**.
3. Если домен или подсеть интегрирован в Active Directory, на экране появится предупреждение. Подтвердите удаление домена или подсети из Active Directory, щелкнув **Да (Yes)**.

Примечание Удаление домена или подсети приводит к удалению всех DNS-записей в зонном файле, но не удаляет сам зонный файл на основном или дополнительном сервере, интегрированном в Active Directory. Он остается в папке %SystemRoot%\System32\Dns. Этот файл можно удалить, после того как вы удалите зоны из консоли **Диспетчер DNS (DNS Manager)**.

Управление DNS-записями

Создав необходимые зонные файлы, вы можете добавить в зоны записи. Компьютеры, доступ к которым требуется из Active Directory и DNS-доменов, должны иметь DNS-записи. Существует много различных типов DNS-записей, но большинство из них используется редко. Мы не будем зря тратить время и рассмотрим только те типы, с которыми вам реально предстоит работать:

- **Узел A (IPv4-адрес)** Сопоставляет хост-имя с IPv4-адресом. Если на компьютере установлено несколько сетевых адаптеров или у него есть несколько IPv4-адресов (или то и другое), он должен иметь несколько записей A.
- **Узел AAAA (IPv6-адрес)** Сопоставляет хост-имя с IPv6-адресом. Если на компьютере установлено несколько сетевых адаптеров или у него есть несколько IPv6-адресов (или то и другое), он должен иметь несколько записей AAAA.
- **Псевдоним (CNAME)** Задает псевдоним для хост-имени. Например, эта запись позволяет *zeta.microsoft.com* иметь псевдоним *www.microsoft.com*.
- **Почтовый обменник (MX)** Задает почтовый сервер домена, что позволяет точно доставлять почту на почтовые серверы домена.
- **Сервер имен (NS)** Задает сервер имен домена, что позволяет выполнять просмотры DNS в различных зонах. В этих записях должны объявляться все основные и дополнительные серверы.
- **Указатель (PTR)** Создает указатель, сопоставляющий IP-адрес хост-имени при обратном просмотре.
- **Начальная запись зоны (SOA)** Объявляет хост, обладающий наибольшими полномочиями в зоне, и потому являющийся наилучшим источ-

ником DNS-информации в зоне. Начальная запись зоны (SOA) должна быть в каждом зонном файле (который создается автоматически при добавлении зоны).

Добавление записей адреса и указателя

Записи типов A и AAAA используются для сопоставления имен хостов с IP-адресами, а запись PTR создает указатель на хост для обратного просмотра. Записи адреса или указателя можно создавать одновременно или по отдельности.

Чтобы создать новый элемент хоста при помощи записей адреса и указателя, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** разверните папку **Зоны прямого просмотра (Forward Lookup Zones)** для нужного сервера.
2. Щелкните правой кнопкой домен, который хотите обновить, и в контекстном меню выберите команду **Создать узел (A или AAAA) (New Host (A Or AAAA))**. Откроется диалоговое окно, показанное на рис. 20-6.

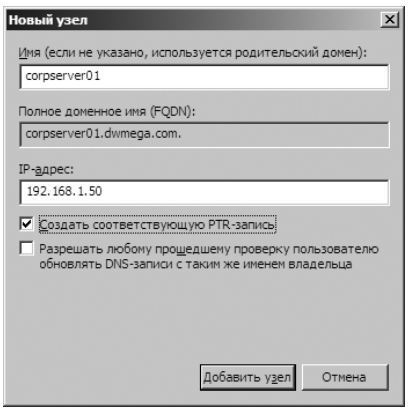


Рис. 20-6. Диалоговое окно Новый узел (New Host) позволяет одновременно создавать записи адреса и указателя

3. Введите имя компьютера, например, **corpserver01**, и IP-адрес, например, 192.168.1.50.
4. Установите флажок **Создать соответствующую PTR-запись (Create Associated Pointer (PTR) Record)**.

Примечание Создавать PTR-записи можно только при наличии соответствующей зоны обратного просмотра. Для создания этого файла выполните шаги, описанные в разделе «Настройка обратного просмотра». Флажок **Разрешать любому прошедшему проверку пользователю... (Allow Any Authenticated Users...)** доступен, если DNS-сервер настроен на контроллере домена.

5. Щелкните кнопку **Добавить узел (Add Host)** и щелкните **OK**. При необходимости повторите процесс, чтобы добавить другие узлы.
6. Завершив работу, щелкните **Готово (Done)**.

Добавление PTR-записи

Чтобы добавить PTR-запись для узла, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** разверните папку **Зоны обратного просмотра (Reverse Lookup Zones)** для нужного вам сервера.
2. Щелкните правой кнопкой подсеть, которую вы хотите обновить, и в контекстном меню выберите команду **Создать указатель (New Pointer (PTR))**. Откроется диалоговое окно, показанное на рис. 20-7.

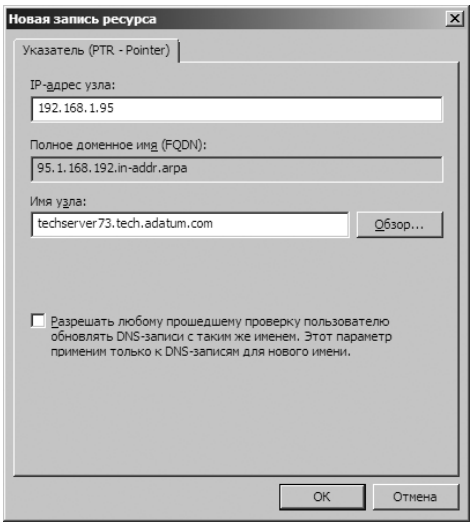


Рис. 20-7. При необходимости вы можете добавить PTR-запись позже при помощи диалогового окна Новая запись ресурса (New Resource Record)

3. Введите **IP-адрес узла (Host IP Address)**, например, **192.168.1.95**, и **Имя узла (Host Name)**, например, **techserver09.tech.adatum.com**. Щелкните **OK**.

Добавление DNS-псевдонимов CNAME

Псевдонимы задаются при помощи CNAME-записей и позволяют одному хост-компьютеру выдавать себя за несколько хост-компьютеров. Например, узел *gamma.microsoft.com* может выглядеть извне как *www.microsoft.com* и как *ftp.microsoft.com*.

Чтобы создать CNAME-запись, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** разверните папку **Зоны прямого просмотра (Forward Lookup Zones)** для нужного сервера.
2. Щелкните правой кнопкой домен, который хотите обновить, и в контекстном меню выберите команду **Создать псевдоним (CNAME) (New Alias (CNAME))**. Откроется диалоговое окно, показанное на рис. 20-8.
3. В поле **Псевдоним (Alias Name)** введите псевдоним — хост-имя, состоящее из одного компонента, например, **www** или **ftp**.

4. В поле **Полное доменное имя (FQDN) конечного узла (Fully Qualified Domain Name (FQDN) For Target Host)** введите полное хост-имя компьютера, для которого предназначен псевдоним.
5. Щелкните **OK**.

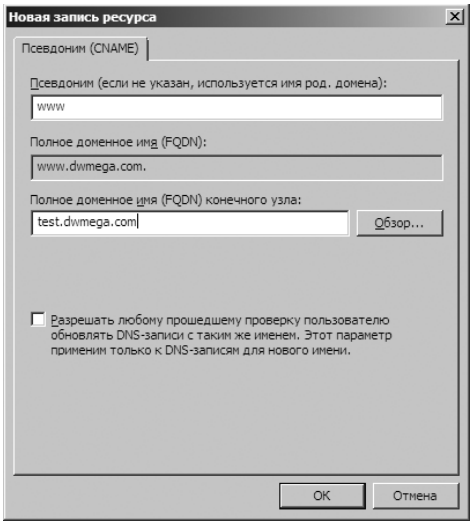


Рис. 20-8. В CNAME-запись вводится однокомпонентное хост-имя и полное имя хоста

Добавление почтового обменника

Записи MX служат для идентификации серверов обмена почтовыми сообщениями домена, которые отвечают за обработку или пересылку почты внутри домена. Создавая MX-запись, вы должны указать номер предпочтения почтового сервера — число от 0 до 65535, указывающее на приоритет почтового сервера в домене. Почтовый сервер с наименьшим предпочтением обладает наибольшим приоритетом и получает почту в первую очередь. В случае сбоя доставки почты, используется следующий предпочитаемый номер по возрастанию.

Чтобы создать MX-запись, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** разверните папку **Зоны прямого просмотра (Forward Lookup Zones)** для нужного сервера.
2. Щелкните правой кнопкой домен, который хотите обновить, и в контекстном меню выберите команду **Создать почтовый обменник (MX) (New Mail Exchanger (MX))**. Откроется диалоговое окно, показанное на рис 20-9.
3. Создайте запись почтового сервера, заполнив следующие поля:
   - **Узел или дочерний домен (Host Or Child Domain)** При желании введите однокомпонентное имя почтового сервера. В большинстве случаев можно оставить это поле незаполненным. Это означает, что имя почтового обменника совпадает с именем родительского домена.

- **Полное доменное имя (FQDN) (Fully Qualified Domain Name (FQDN))** Здесь стоит полное имя домена, к которому относится запись почтового обменника, например, **tech.adatum.com**.
- **Полное доменное имя (FQDN) почтового сервера (Fully Qualified Domain Name (FQDN) Of Mail Server)** Введите полное имя почтового сервера, который будет обрабатывать прием и доставку почты, например, **corpmail.tech.adatum.com**. Сообщения для ранее указанного домена передаются на этот сервер с целью доставки.
- **Приоритет почтового сервера (Mail Server Priority)** Введите приоритет хоста — от 0 до 65535.

Примечание Назначая приоритет, учитывайте будущий рост компании. Например, для сервера с наивысшим приоритетом задайте значение 10, для следующего — 20, далее — 30.

4. Щелкните **OK**.

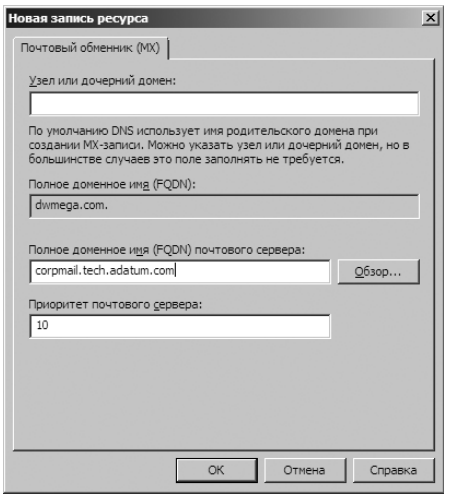


Рис. 20-9. Почтовые серверы с наименьшим номером предпочтения обладают самым большим приоритетом

Добавление сервера имен

В записях NS задаются серверы имен домена. В записи NS должен быть объявлен каждый основной и дополнительный сервер. Если вы получили адреса дополнительных серверов имен от Интернет-провайдера, убедитесь, что ввели требуемые NS-записи.

Чтобы создать NS-запись, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** разверните папку **Зоны прямого просмотра (Forward Lookup Zones)** нужного сервера.
2. Отобразите DNS-записи домена, развернув его узел в дереве консоли.

3. Щелкните правой кнопкой существующую NS-запись в области просмотра и выберите команду **Свойства (Properties)**. Диалоговое окно свойств домена откроется на вкладке **Серверы имен (Name Servers)**, показанной на рис. 20-10.

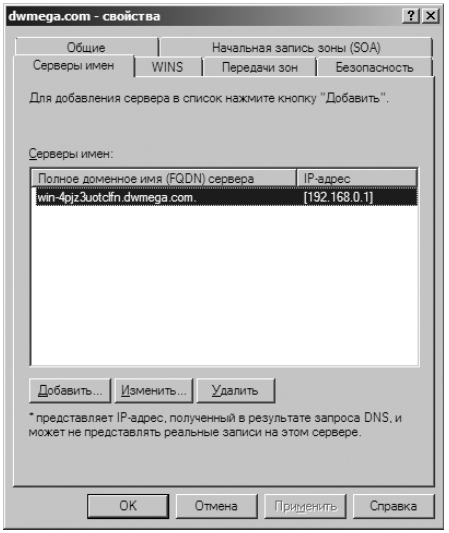


Рис. 20-10. Настройка серверов имен в диалоговом окне свойств домена

4. Щелкните **Добавить (Add)**. Откроется диалоговое окно **Новая запись сервера имен (New Name Server Record)**.
5. В поле **Полное доменное имя сервера (Server Fully Qualified Domain Name)** введите полное хост-имя DNS-сервера дочернего домена, например, **corpserver01.adatum.com**. Щелкните **Разрешить в адрес (Resolve)**. Сервер пошлет запрос на просмотр и добавит разрешенный IP-адрес в список **IP-адрес (IP Address)**.
6. Повторите шаг 5, чтобы указать дополнительные серверы имен. Порядок записей определяет, какой из IP-адресов будет использован первым. При необходимости измените порядок с помощью кнопок **Вверх (Up)** и **Вниз (Down)**. Щелкните **OK**, чтобы закрыть диалоговое окно **Новая запись сервера имен (New Name Server Record)**.
7. Щелкните **OK**, чтобы сохранить изменения.

Просмотр и обновление DNS-записей

Чтобы просмотреть или обновить DNS-записи, выполните следующие действия:

1. Дважды щелкните нужную зону. Записи зоны отобразятся в правой панели.
2. Дважды щелкните DNS-запись, которую хотите просмотреть или обновить. Откроется диалоговое окно свойств записи. Внесите необходимые изменения и щелкните **OK**.

Обновление свойств и начальной записи зоны

У каждой зоны есть свойства, задающие общие параметры зоны — начальную запись зоны (SOA), уведомление об изменениях, интеграцию с WINS. Чтобы настроить свойства зоны в консоли **Диспетчер DNS (DNS Manager)**, выполните следующие действия:

- Щелкните правой кнопкой зону, которую хотите обновить, и выберите в контекстном меню команду **Свойства (Properties)**.
- Выделите зону и выберите в меню **Действие (Action)** команду **Свойства (Properties)**.

Окна свойств зон прямого и обратного просмотра одинаковы, за исключением вкладок **WINS** и **WINS-R**. В зонах прямого просмотра вкладка **WINS** служит для настройки просмотров имен NetBIOS. В зонах обратного просмотра вкладка **WINS-R** предназначена для настройки обратных просмотров имен NetBIOS.

Изменение начальной записи зоны

В начальной записи зоны объявляется полномочный сервер имен зоны и устанавливаются общие свойства зоны, например, интервалы повторов и обновлений. Чтобы изменить эти параметры, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** щелкните правой кнопкой зону, которую хотите обновить, и в контекстном меню выберите **Свойства (Properties)**.
2. Перейдите на вкладку **Начальная запись зоны (SOA) (Start Of Authority (SOA))** и обновите параметры, показанные на рис. 20-11.

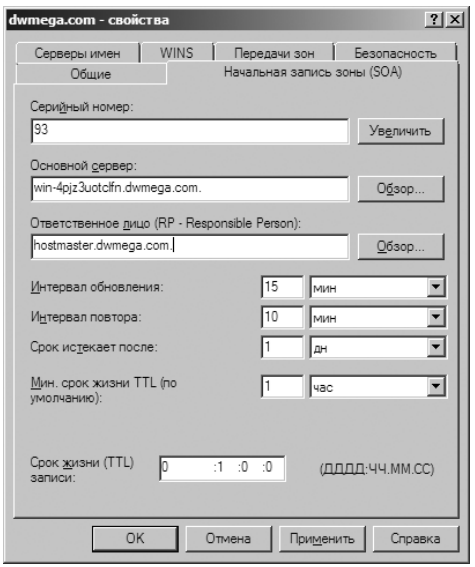


Рис. 20-11. В диалоговом окне свойств зоны задайте общие свойства зоны и обновите SOA-запись

На вкладке **Начальная запись зоны (SOA) (Start Of Authority (SOA))** доступны следующие параметры:

- **Серийный номер (Serial Number)** Серийный номер отражает версию файлов БД DNS. Номер обновляется автоматически при внесении изменений в файлы зоны, но вы можете обновить его и вручную. По этому номеру дополнительные серверы определяют, изменилась ли зона. Если серийный номер основного сервера превышает серийный номер дополнительного сервера, записи изменились, и дополнительный сервер может запросить DNS-записи зоны. Кроме того, вы можете настроить DNS на уведомление дополнительных серверов об изменениях (что ускоряет процесс обновления).
- **Основной сервер (Primary Server)** Полное доменное имя сервера, в конце которого стоит точка. Точка обозначает конец имени и гарантирует, что к записи не будет добавлена информация о домене.
- **Ответственное лицо (Responsible Person)** Адрес электронной почты лица, ответственного за домен. По умолчанию здесь стоит имя *hostmaster*, за которым следует точка. Это обозначает адрес hostmaster@ваш_домен.com. Если вы введете здесь другой адрес, замените точкой символ @ в адресе электронной почты и в конце адреса также поставьте точку.
- **Интервал обновления (Refresh Interval)** Интервал, через который дополнительный сервер проводит проверку обновлений зоны. Уменьшив его значение, вы сокращаете сетевой трафик. С другой стороны, его нельзя делать слишком большим, так как изменения NS-записей должны своевременно распространяться на дополнительный сервер.
- **Интервал повтора (Retry Interval)** Время после сбоя, в течение которого дополнительный сервер не загружает БД зоны. Если задан интервал 10 минут, после сбоя передачи БД зоны дополнительный сервер ждет 10 минут, прежде чем отправить новый запрос.
- **Срок жизни истекает после (Expires After)** Период времени, в течение которого информация зоны на дополнительном сервере считается достоверной. Если дополнительный сервер в течение этого времени не может загрузить данные с основного сервера, данные в кеше дополнительного сервера устаревают, и дополнительный сервер перестает отвечать на DNS-запросы.
- **Мин. срок жизни TTL (по умолчанию) (Minimum (Default) TTL)** Минимальное время жизни кешированных записей на дополнительном сервере. Когда это время заканчивается, дополнительный сервер считает срок действия соответствующей записи истекшим и сбрасывает ее. После этого необходимо отправлять очередной запрос на основной сервер. Делайте минимальный срок жизни относительно большим, скажем, 24 часа. Это сократит сетевой трафик и повысит производительность. С другой стороны, нужно помните, что высокое значение замедляет распространение обновлений через Интернет.

- **Срок жизни (TTL) записи (TTL For This Record)** Время жизни конкретной SOA-записи в формате: ДД: ЧЧ: ММ: СС. Как правило, оно должно совпадать с минимальным временем жизни всех записей.

Разрешение и ограничение передач зон

Передачи зоны отправляют копию информации зоны на другие DNS-серверы в том же или в других доменах. По соображениям безопасности в Windows Server 2008 передачи зон отключены. Чтобы включить их для дополнительных серверов, настроенных вами или поставщиком Интернета, требуется разрешить передачи зоны, а затем указать типы серверов, на которые они могут осуществляться.

Вы можете разрешить передачи зон на любой сервер, однако это подвергает риску безопасность сервера. Ограничьте доступ к информации о зонах, чтобы запрашивать обновления с основного сервера зоны могли только указанные вами серверы. Это позволит ограничить запросы определенной группой дополнительных серверов, например, серверов имен поставщика Интернета, а также скрыть внутреннюю сеть от внешнего мира.

Чтобы разрешить передачи зоны и ограничить доступ к БД основной зоны, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** щелкните правой кнопкой домен или подсеть, которую хотите обновить, и в контекстном меню выберите **Свойства (Properties)**.
2. Перейдите на вкладку **Передачи зон (Zone Transfer)**, показанную на рис. 20-12.

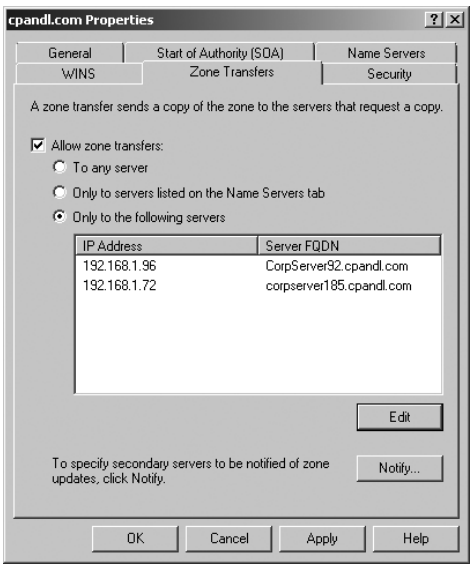


Рис. 20-12. На вкладке Передачи зон (Zone Transfers) можно разрешить зонные переносы на все или только на указанные серверы

3. Чтобы ограничить переносы серверами имен, перечисленными на вкладке **Серверы имен (Name Servers)**, установите флажок **Разрешить передачи зон (Allow Zone Transfers)** и установите переключатель **Только на серверы, перечисленные на странице серверов имен (Only To Servers Listed On The Name Servers Tab)**.
4. Чтобы ограничить переносы указанными серверами, установите флажок **Разрешить передачи зон (Allow Zone Transfers)** и переключатель **Только на серверы из этого списка (Only To The Following Servers)**. Затем щелкните **Изменить (Edit)**, чтобы открыть диалоговое окно **Разрешить передачи зон (Allow Zone Transfers)**. Щелкните поле **IP-адрес (IP Address)**, введите IP-адрес дополнительного сервера зоны и нажмите Enter. Система проверит сервер. В случае ошибки убедитесь, что сервер подключен к сети и вы ввели правильный IP-адрес. Если вы хотите копировать данные зоны из других серверов на случай недоступности первого сервера, добавьте IP-адреса и других серверов. Щелкните **OK**.
5. Щелкните **OK**, чтобы сохранить изменения.

Уведомление дополнительных серверов об изменениях

Свойства зоны устанавливаются при помощи SOA-записи. Они регулируют распространение информации DNS по сети. Вы также можете указать основному серверу, чтобы он рассылал уведомления дополнительным серверам имен при наличии изменений в БД зоны. Для этого выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** щелкните правой кнопкой домен или подсеть, которую хотите настроить, и в контекстном меню выберите **Свойства (Properties)**.
2. На вкладке **Передачи зон (Zone Transfers)** щелкните кнопку **Уведомить (Notify)**. Откроется диалоговое окно, показанное на рис. 20-13.

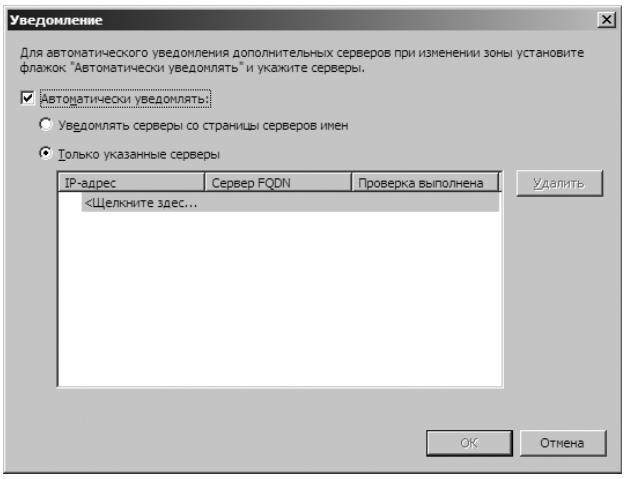


Рис. 20-13. Уведомление всех дополнительных серверов, перечисленных на вкладке Серверы имен (Name Servers), или только серверов, указанных вами

3. Чтобы уведомлять серверы имен, перечисленные на вкладке **Серверы имен (Name Servers)**, установите флажок **Автоматически уведомлять (Automatically Notify)** и переключатель **Уведомлять серверы со страницы серверов имен (Only To Servers Listed On The Name Servers Tab)**.
4. Чтобы указать серверы для получения уведомлений, установите флажок **Автоматически уведомлять (Automatically Notify)** и переключатель **Только указанные серверы (Following Servers)**. Щелкните списке **IP-адрес (IP Address)**, введите IP-адрес дополнительного сервера зоны и нажмите Enter. Система проверит сервер. В случае ошибки убедитесь, что сервер подключен к сети и вы ввели правильный IP-адрес. Если вы хотите уведомлять другие серверы, добавьте их IP-адреса.
5. Два раза щелкните **OK**.

Установка типа зоны

Чтобы изменить тип зоны и режим интеграции с Active Directory, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** щелкните правой кнопкой домен или подсеть, которую хотите настроить, и в контекстном меню выберите **Свойства (Properties)**.
2. На вкладке **Общие (General)** щелкните кнопку **Изменить (Change)** в разделе **Тип (Type)**. В диалоговом окне **Изменение типа зоны (Change Zone Type)** выберите новый тип зоны.
3. Для интеграции зоны с Active Directory установите флажок **Хранить зону в Active Directory (Store The Zone In Active Directory)**.
4. Чтобы удалить зону из Active Directory, сбросьте флажок **Хранить зону в Active Directory (Store The Zone In Active Directory)**.
5. Два раза щелкните **OK**.

Включение и выключение динамических обновлений

Динамические обновления позволяют DNS-клиентам регистрировать и поддерживать собственные записи адресов и указателей. Это полезно, если компьютеры настраиваются динамически при помощи DHCP. Включив динамические обновления, вы поможете динамически настроенным компьютерам определить положение друг друга в сети. Если зона интегрирована в Active Directory, у вас есть возможность включить запрос на безопасные обновления. При безопасных обновлениях определение компьютеров и пользователей, которым позволено динамически обновлять DNS, происходит при помощи списков ACL.

Чтобы включить или отключить динамические обновления, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** щелкните правой кнопкой домен или подсеть, которую хотите настроить, и в контекстном меню выберите **Свойства (Properties)**.

2. На вкладке **Общие (General)** в раскрывающемся списке **Динамическое обновление (Dynamic Updates)** выберите один из вариантов для включения или отключения динамических обновлений:
   - **Никакие (None)** Отключение динамических обновлений.
   - **Небезопасные и безопасные (Nonsecure And Secure)** Включение небезопасных и безопасных обновлений.
   - **Только безопасные (Secure Only)** Включение динамических обновлений с использованием системы безопасности Active Directory. Доступно только при интеграции с Active Directory.
3. Щелкните **OK**.

Примечание Параметры интеграции DNS должны быть настроены и для DHCP. Подробнее об этом — в разделе «Интеграция DHCP и DNS» главы 19.

Управление конфигурацией и безопасностью DNS-сервера

Управление основной конфигурацией DNS-серверов осуществляется в диалоговом окне свойств сервера. В нем можно включать и выключать IP-адреса сервера и регулировать доступ к DNS-серверам за пределами организации. Кроме того, вы можете настроить мониторинг, протоколирование и дополнительные возможности.

Включение и выключение IP-адресов для DNS-сервера

По умолчанию многосетевые DNS-серверы отвечают на DNS-запросы на всех доступных сетевых интерфейсах и IP-адресах, использование которых на них настроено.

Консоль **Диспетчер DNS (DNS Manager)** позволяет указать серверу отвечать на запросы только с заданных IP-адресов. Для этого выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** щелкните правой кнопкой нужный сервер и выберите в контекстном меню команду **Свойства (Properties)**.
2. На вкладке **Интерфейсы (Interfaces)** установите переключатель **Только по указанным IP-адресам (Only The Following IP Addresses)**. Выберите IP-адрес, по которому нужно отвечать на DNS-запросы. Сбросьте флажок IP-адреса, по которому не нужно отвечать на DNS-запросы. Для DNS будут использоваться только выбранные IP-адреса. DNS на всех остальных IP-адресах будет отключена.
3. Щелкните **OK**.

Управление доступом к внешним DNS-серверам

Ограничение доступа к информации зоны позволяет указать, какие внутренние и внешние серверы могут получать доступ к основному серверу. Для

внешних серверов это означает управление возможностью подключения из внешнего мира. Также вы можете задать, какие DNS-серверы вашей организации могут получать доступ к серверам за ее пределами. Для этого следует настроить внутри домена DNS-пересылку.

С точки зрения пересылки серверы DNS в домене можно настроить одним из следующих образов:

- **Серверы без пересылки (Nonforwarders)** Серверы должны передавать DNS-запросы, которые они не смогли разрешить, на заданные серверы пересылки. В целом, эти серверы выступают в роли DNS-клиентов для серверов пересылки.
- **Только пересылка (Forwarding-only)** Серверы способны только кешировать ответы и передавать запросы на серверы пересылки. Известны также как *кеширующие* DNS-серверы.
- **Серверы пересылки (Forwarders)** Серверы, получающие запросы от серверов без пересылки или только с пересылкой. Для разрешения запросов серверы пересылки используют нормальные способы коммуникаций DNS.
- **Серверы условной переписки (Conditional forwarders)** Серверы, перенаправляющие запросы на основе домена DNS. Условное перенаправление удобно, когда в организации есть несколько внутренних доменов.

Примечание Нельзя сделать корневой сервер домена сервером пересылки (за исключением условного перенаправления, используемого при внутреннем разрешении имен). Все остальные серверы можно настроить на пересылку.

Создание серверов без пересылки и только с пересылкой

Чтобы настроить DNS-сервер без пересылки, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** щелкните правой кнопкой настраиваемый сервер и в контекстном меню выберите **Свойства (Properties)**.
2. Перейдите на вкладку **Дополнительно (Advanced)**. Чтобы настроить сервер без пересылки, убедитесь, что флажок **Отключить рекурсию (Disable Recursion)** сброшен. Чтобы настроить сервер только для пересылки, убедитесь, что флажок **Отключить рекурсию (Disable Recursion)** установлен.
3. На вкладке **Пересылка (Forwarders)** щелкните кнопку **Изменить (Edit)**. Откроется диалоговое окно **Редактировать пересылки (Edit Forwarders)**.
4. Щелкните список **IP-адрес (IP Address)**, введите IP-адрес сервера пересылки сети и нажмите Enter. Система проверит сервер. В случае ошибки убедитесь, что сервер подключен к сети и вы ввели правильный IP-адрес. Повторите процесс, чтобы задать IP-адреса других серверов пересылки.
5. Задайте время ожидания пересылки, то есть, время, в течение которого сервер без пересылки повторяет попытки опросить текущий сервер пе-

ресылки при отсутствии ответа. По истечению времени ожидания сервер без пересылки пытается запросить следующий сервер пересылок из списка. Стандартный таймаут составляет 5 секунд. Щелкните **OK**.

Создание сервера пересылки

Выступать в роли сервера пересылок способен любой DNS-сервер, если он не настроен в качестве сервера без пересылок или сервера только для пересылки. На серверах пересылки в сети убедитесь в том, что флажок **Отключить рекурсию (Disable Recursion)** не задан и что вы не настроили сервер на перенаправление запросов на другие DNS-серверы в домене.

Настройка условной пересылки

Если у вас несколько внутренних доменов, вам стоит подумать о настройке условной пересылки. Она позволяет направлять запросы конкретных доменов для разрешения на конкретные DNS-серверы. Условная пересылка полезна, если в вашей организации есть несколько внутренних доменов и вам требуется разрешать запросы между ними.

Чтобы настроить условную пересылку, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** щелкните правой кнопкой папку **Серверы условной пересылки (Conditional Forwarders)** нужного вам сервера. В контекстном меню выберите команду **Создать условную пересылку (Conditional Forwarder)**.
2. В диалоговом окне **Создать сервер условной пересылки (New Conditional Forwarder)** введите имя домена, в который следует пересылать запросы, например, **adatum.com**.
3. Щелкните список **IP-адрес (IP Address)**, введите IP-адрес полномочного DNS-сервера в указанном домене и нажмите Enter. Повторите процесс, чтобы указать дополнительные IP-адреса.
4. При использовании интеграции DNS с Active Directory установите флажок **Сохранять условную пересылку в Active Directory (Store This Conditional Forwarder In Active Directory)** и выберите одну из следующих стратегий репликации.
   - **Все DNS-серверы в этом лесу (All DNS Servers In This Forest)** Это обширнейшая стратегия репликации. Помните, что лес Active Directory включает все деревья доменов, использующие данные каталога совместно с текущим доменом.
   - **Все DNS-серверы в этом домене (All DNS Servers In This Domain)** Выберите эту стратегию, чтобы реплицировать информацию DNS внутри текущего домена и его дочерних доменов.
   - **Все контроллеры домена в этом домене (All Domain Controllers In This Domain)** Выберите эту стратегию, если хотите реплицировать информацию DNS на все контроллеры домена внутри текущего домена и его дочерних доменов. Хотя эта стратегия обеспечивает более широкую репликацию информации DNS внутри домена, не

каждый контролер домена является DNS-сервером (вам и не нужно настраивать каждый контроллер домена как DNS-сервер).

5. Задайте время ожидания пересылки, то есть, время, в течение которого сервер пытается запросить сервер пересылки в случае отсутствия ответа. По истечении времени ожидания сервер пытается запросить следующий полномочный сервер из списка. Стандартное время ожидания составляет пять секунд. Щелкните **OK**.
6. Повторите процедуру, чтобы настроить условную пересылку для других доменов.

Включение и выключение протоколирования событий

По умолчанию служба DNS отслеживает все события в журнале событий DNS-сервера. Вы можете изменить параметры ведения журнала, выполнив следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** щелкните правой кнопкой нужный сервер и в контекстном меню выберите **Свойства (Properties)**.
2. Настройка ведения журнала событий DNS выполняется на вкладке **Журнал событий (Event Logging)**. Чтобы отключить запись событий, установите переключатель **Не заносить никакие события (No Events)**.
3. Щелкните **OK**.

Отладочное протоколирование и отслеживание активности DNS

Как правило, журнал событий **DNS-сервер (DNS Server)** используется для наблюдения за деятельностью DNS-сервера. В этом журнале записаны все события DNS, а просмотреть его можно в узле **Просмотр событий (Event View)** консоли **Управление компьютером (Computer Management)**. При поиске неисправностей DNS весьма полезной может оказаться настройка временного журнала для отслеживания определенных событий DNS. Не забывайте очищать события после окончания отладки.

Чтобы настроить отладку, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** щелкните правой кнопкой нужный сервер и в контекстном меню выберите **Свойства (Properties)**.
2. На вкладке **Ведение журнала отладки (Debug Logging)**, показанной на рис. 20-14, установите флажок **Записывать пакеты в журнал для отладки (Log Packets For Debugging)**. Затем установите флажки событий, временное наблюдение за которыми хотите вести.
3. В поле **Имя и путь к файлу (File Path And Name)** введите имя файла журнала, например, **dns.log**. По умолчанию журналы хранятся в папке %SystemRoot%\System32\Dns.
4. Щелкните **OK**. Завершив отладку, отключите протоколирование, сбросив флажок **Записывать пакеты в журнал для отладки (Log Packets For Debugging)**.

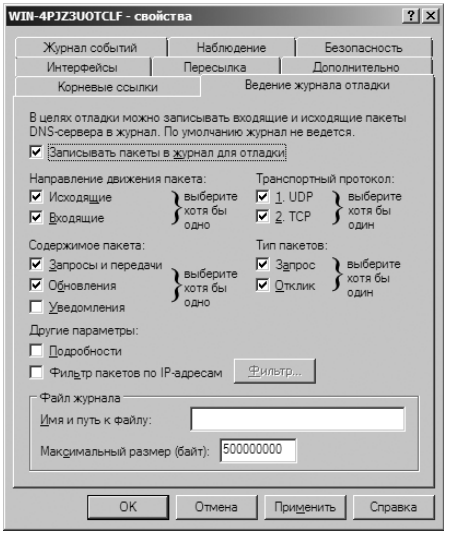


Рис. 20-14. Протоколируемые события устанавливаются на вкладке Ведение журнала отладки (Debug Logging)

Мониторинг DNS-сервера

В Windows Server 2008 имеется встроенная возможность мониторинга DNS-сервера для проверки правильности настройки разрешения имен.

Чтобы настроить ручное или автоматическое выполнение мониторинга, выполните следующие действия:

1. В консоли **Диспетчер DNS (DNS Manager)** щелкните правой кнопкой нужный сервер и в контекстном меню выберите **Свойства (Properties)**.

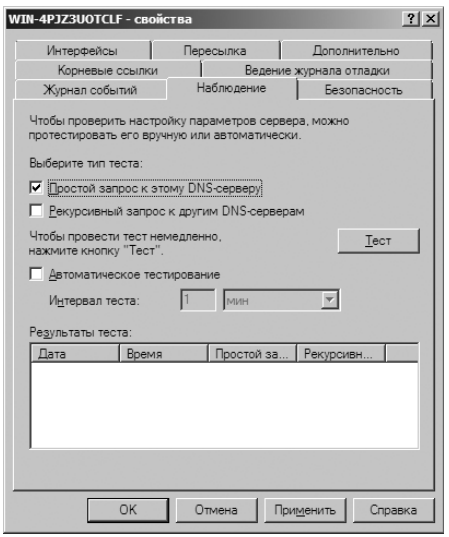


Рис. 20-15. Настройка ручного или автоматического мониторинга DNS-сервера

2. Перейдите на вкладку **Наблюдение (Monitoring)**, показанную на рис. 20-15. Вы можете провести два типа тестов. Чтобы проверить разрешение DNS на текущем сервере, установите флажок **Простой запрос к этому DNS-серверу (A Simple Query Against This DNS Server)**. Чтобы проверить разрешение DNS в домене, установите флажок **Рекурсивный запрос к другим DNS-серверам (A Recursive Query To Other DNS Servers)**.
3. Чтобы провести тестирование вручную, щелкните кнопку **Тест (Test Now)**. Чтобы запланировать автоматический мониторинг, установите флажок **Автоматическое тестирование (Perform Automatic Testing At The Following Interval)** и интервал в секундах, минутах или часах.
4. Результаты тестирования отображены в разделе **Результаты теста (Test Results)**. Здесь указаны дата и время проведения теста, а также его результаты, например, **Пройден (Pass)**. Причиной отдельного сбоя может стать временная неисправность. Несколько сбоев, скорее всего, указывают на проблему с разрешением имен.

Примечание Если все рекурсивные тесты завершились неудачей, попробуйте отключить рекурсию на вкладке **Дополнительно (Advanced)** окна свойств сервера.

Ближе к реальности Если вы в данный момент занимаетесь диагностикой конкретной неисправности DNS, вам стоит настроить проведение тестирования через каждые 10-15 сек. Так вы быстрее узнаете об устранении неисправности. Если вы проводите мониторинг неисправностей DNS в рамках повседневной работы, лучше установить более продолжительный интервал — примерно два-три часа.

Об авторе

Уильям Р. Станек (William R. Stanek) (*http://www.williamstanek.com/*) обладает более чем двадцатилетним практическим опытом в области программирования и разработки. Он ведущий эксперт по компьютерным технологиям, автор, книги которого завоевали множество наград, и блестящий преподаватель. На протяжении многих лет его практические советы помогают миллионам профессионалов во всем мире. Он написал более 65 книг, включая *Microsoft Exchange Server 2007 Administrator's Pocket Consultant (Microsoft Exchange Server 2007. Справочник администратора, Русская Редакция, БХВ-Петербург, 2008) Microsoft Windows Vista Administrator's Pocket Consultant (Microsoft Windows Vista. Справочник администратора, Русская Редакция, БХВ-Петербург, 2007), Windows Server 2008 Administrator's Pocket Consultant (Windows Server 2008. Справочник администратора, Русская Редакция, БХВ-Петербург, 2008) и Windows Server 2008 Inside Out.*

Уильям Станек участвует в коммерческом Интернет-сообществе с 1991 г. Основу его делового и технологического опыта составили 11 лет военной службы. Он также обладает значительным опытом в разработке серверных технологий, шифрования и решений Интернета. Им написано множество руководств и учебных курсов по самым разнообразным вопросам. Он часто выступает в роли эксперта и консультанта.

Уильям Станек с отличием защитил степень магистра информационных систем и степень бакалавра информатики. Он гордится тем, что во время войны в Персидском заливе принимал участие в боевых действиях в составе экипажа самолета радиоэлектронной борьбы. Он неоднократно совершал боевые вылеты в Ирак и награжден девятью медалями, включая одну из высочайших наград США — крест Air Force Distinguished Flying Cross. В настоящее время он живет на северо-западе США с женой и детьми.

Windows Server® 2008

Справочник администратора

Это практическое пособие поможет быстро найти ответы на вопросы, возникающие при администрировании Windows Server 2008. Подробные таблицы, пошаговые инструкции, примеры кода и списки параметров предоставят точную информацию, позволяющую администратору моментально устранить проблему и выполнить необходимые операции.

В этой книге:

- развертывание Windows Server 2008;
- настройка серверных ролей;
- настройка и обслуживание Active Directory;
- создание учетных записей пользователей и групп, управление правами и разрешениями;
- управление файловыми системами, дисками и массивами RAID;
- настройка сетей TCP/IP, а также клиентов и серверов DHCP и DNS;
- диагностика работы принтеров и серверов печати;
- мониторинг и настройка производительности сети;
- архивация и восстановление системы.

Каждая книга серии **Справочник администратора** (Administrator's Pocket Consultant) объединяет в себе руководство по эксплуатации и подробный справочник по основным функциям и параметрам системы.

Компактный справочник администратора — ваш идеальный помощник в повседневной работе!

Microsoft Windows Server System

ISBN 978-5-9775-0009-8

9 785977 500098

Издательство
БХВ-Петербург
Санкт-Петербург,
ул. Есенина, 5Б
Тел./факс: (812) 591-6243
E-mail: mail@bhv.ru
Internet: www.bhv.ru

Издательство
Русская Редакция
Москва, Шелепихинская наб., 32
Тел.: (495) 638-5-638
Тел./факс: (495) 256-7145
E-mail: info@rusedit.com
Internet: www.rusedit.com

bhv®

РУССКАЯ РЕДАКЦИЯ