Алексей Чекмарев

Microsoft® Windows Server 2008

Санкт-Петербург
«БХВ-Петербург»
2008

УДК 681.3.06
ББК 32.973.26-018.2
Ч-37

Чекмарев А. Н.

Ч-37 Microsoft Windows Server 2008. — СПб.: БХВ-Петербург, 2008. — 896 с.: ил. — (В подлиннике)

ISBN 978-5-9775-0260-3

Руководство по всем редакциям операционной системы Microsoft Windows Server 2008 для 32- и 64-разрядных платформ. Может использоваться при работе с английскими и русскими локализованными версиями. Рассматриваются все аспекты эксплуатации серверов в составе рабочих групп и доменов, подробно описаны традиционные и новые средства администрирования систем и многочисленных прикладных сервисов, включая файловые и сетевые службы, службы Интернета (IIS), службы каталогов Active Directory и т. д. Отдельные главы посвящены вопросам безопасности всех компонентов, а также средствам архивации и восстановления системы и данных.

Для системных администраторов и IT-специалистов

УДК 681.3.06
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Компьютерная верстка	*Натальи Смирновой*
Корректор	*Наталия Першакова*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 08.08.08.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 72,24.
Тираж 3000 экз. Заказ №
"БХВ-Петербург", 194354, Санкт-Петербург, ул. Есенина, 5Б.

Санитарно-эпидемиологическое заключение на продукцию № 77.99.60.953.Д.003650.04.08
от 14.04.2008 г. выдано Федеральной службой по надзору
в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 978-5-9775-0260-3

Оглавление

Введение
Общие сведения о системах Windows Server 2008

Этот обзорный раздел дает общее представление о возможностях операционных систем семейства Windows Server 2008. Рассматриваются особенности всех имеющихся редакций, что позволяет лучше понимать назначение отдельных компонентов и программ, входящих в конкретные версии Windows Server 2008, и степень их необходимости для пользовательских задач.

Версии Windows, предшествующие Windows Server 2008

Полезно знать некоторые детали создания операционной системы Windows Server 2008, поскольку это помогает в понимании связей между различными версиями Windows. Перечислим этапы в создании операционных систем, выпущенных компанией Microsoft за последнее десятилетие.

В декабре 1999 года была закончена разработка семейства кардинально новых систем *Windows 2000* (версия 5.0 build 2195), которые пришли на смену ОС Windows NT 4.0 и стали официально распространяться в начале 2000 года. Клиентская и серверная версии были выпущены одновременно.

Следующее поколение клиентских систем — *Windows XP* (версия 5.1 build 2600) — появилось в конце августа 2001 года, а его официальный выпуск состоялся в октябре 2001 года. Эту версию можно рассматривать как эволюционное развитие платформы Windows 2000. Соответствующая "поколению" Windows XP серверная платформа — *Windows Server 2003* (версия 5.2 build 3790) — была выпущена в конце марта 2003 года.

Летом 2002 года компания Microsoft объявила о появлении еще одного члена семейства систем Windows XP: впервые была анонсирована редакция *Windows XP Media Center Edition*, ориентированная на мультимедийные при-

ложения. Последняя версия этой системы — Windows XP Media Center Edition 2005 (ее ядро соответствует Windows XP Service Pack 2).

С момента выхода Windows XP компания Microsoft выпускала только пакеты обновлений (service pack) существующих клиентских систем, одновременно работая над операционными системами нового поколения, получившими общее кодовое название *Windows Longhorn*. Параллельно разрабатывались клиентская версия для рабочих станций и серверная платформа, которая была закончена на год позже выпуска клиентских ОС. В конце 2005 года клиентская версия системы проекта Longhorn получила название *Microsoft® Vista™*.

Официальный выпуск ОС Windows Vista (версия 6.0 build 6000) для широкого пользователя состоялся 30 января 2007. Компания Microsoft рассматривает эту систему как революционное обновление линейки ОС, предназначенных для клиентов всех уровней: от домашних до корпоративных.

В декабре 2005 года компания Microsoft запустила в производство обновленные версии серверной платформы, получившей название *Windows Server 2003 R2* (Release 2). В ее основу положен код Windows Server 2003 Service Pack 1, включены все последние обновления безопасности, а также дополнительные сетевые и серверные службы.

4 февраля 2008 года ОС Windows Server 2008 была сдана в производство (release to manufacturing, RTM), а ее официальный выход состоялся 27 февраля вместе с другими важнейшими программными продуктами Microsoft — SQL Server 2008 и Visual Studio 2008. ОС Windows Server 2008 на данный момент является последней версией Windows, выпущенной компанией Microsoft.

Редакции ОС Microsoft Windows Server 2008

Microsoft® Windows Server 2008™ — это общее имя для целого семейства операционных систем, которые выпускаются в нескольких редакциях, ориентированных на разные задачи и различные аппаратные платформы.

Различия между редакциями Windows Server 2008 определяются целевым сегментом рынка — т. е. набором выполняемых задач и условиями использования. Все редакции, за исключением Windows Server 2008 Web, могут устанавливаться в режиме Server Core и имеют вариант дистрибутива без компонента Hyper-V.

Windows Server 2008 Web. Предназначена для быстрого развертывания специализированных серверов, выполняющих роль веб-сервера. Включает службы IIS 7.0, средства ASP.NET и .NET Framework.

Windows Server 2008 Standard. Базовая система для использования во всех областях. Позволяет устанавливать любые роли, службы и компоненты.

Windows Server 2008 Enterprise. Система для развертывания критически важных приложений в корпоративной среде. Имеет улучшенные возможности кластеризации и замены процессоров, обеспечивает максимальную безопасность системы и процессов. Позволяет упростить развертывание приложений за счет использования механизмов виртуализации.

Windows Server 2008 Datacenter. Наиболее мощная платформа для развертывания ответственных приложений с высокими возможностями масштабирования нагрузки. Имеет неограниченное количество лицензий на использование средств виртуализации. Может поддерживать до 64 процессоров.

Itanium-системы. Системы, оптимизированные для больших баз данных и ответственных приложений. Имеют высокие возможности отказоустойчивости и масштабирования, поддерживают до 64 процессоров для обеспечения критически важных задач.

Все редакции Windows Server 2008 поставляются только на DVD-дисках, поскольку дистрибутивы имеют объем порядка 1,76 Гбайт (2,49 Гбайт для платформы x64). (Для сравнения — система Windows Server 2003 R2 поставляется на двух обычных CD-дисках.)

На дистрибутивном DVD-диске присутствует код практически всех редакций Windows Server 2008, и администратор может в тестовом режиме установить любую из редакций (*см. главу 1*, рис. 1.9). Однако для 32- и для 64-разрядных версий Windows Server 2008 дистрибутивные диски выпускаются отдельно.

Обзор функциональных возможностей Windows Server 2008

Рассмотрим назначение основных средств, функций и компонентов Windows Server 2008 — в дальнейшем это позволит лучше ориентироваться в материале книги (в скобках указаны номера глав, где упомянутое средство или функция рассматривается подробно).

Обзор разбит на три части: сначала перечислены принципиально новые функции систем Windows Server 2008, а затем — возможности, появившиеся в "родственной" системе Windows Vista, а также унаследованные от предыдущих версий, начиная с Windows 2000.

Новые средства

Хотя операционные системы Windows Vista и Windows Server 2008 разрабатывались в рамках одного проекта и имеют немало общих архитектурных решений и компонентов, многие службы (по понятным причинам) доступны только на серверных платформах; некоторые из них появились в качестве штатных компонентов системы только в Windows Server 2008. Начнем описание возможностей Windows Server 2008 именно с таких служб и возможностей. (Многие новые средства рассмотрены также в главах, посвященных конкретным службам или административным задачам; перечислить их в одном месте просто невозможно.)

> ***Службы мультимедиа***
>
> Роль *Streaming Media Services* (Потоковые службы мультимедиа) не включена в состав Windows Server 2008; этот программный пакет может загружаться и устанавливаться отдельно. В составе Windows Server 2008 имеется компонент Quality Windows Audio Video Experience (qWave), который обеспечивает некоторые возможности по передаче потоковых аудио- и видеофайлов.

Роли сервера

Установка и удаление служб и компонентов в системах Windows Server 2008 жестко увязана с понятием *роли сервера* (server role). Для управления ролями и службами используется новая оснастка **Server Manager** (Диспетчер сервера), которая также служит средством для централизованного мониторинга всех компонентов системы *(глава 3)*.

Режим установки основных компонентов сервера (Server Core)

Возможен режим развертывания операционной системы, при котором инсталлируются только нужные компоненты и службы без графического интерфейса пользователя. Это позволяет создавать серверы с большей защищенностью, требующие меньше внимания со стороны администратора *(глава 1)*.

Службы каталога Active Directory

Многие новшества Windows Server 2008 связаны со службами каталога Active Directory, которые могут использоваться для развертывания доменов, а также работать самостоятельно, в качестве информационного хранилища. Использованию служб каталога Active Directory целиком посвящена *глава 12*.

- Административные оснастки, используемые для управления доменными службами Active Directory, модернизированы и имеют новые функции. Множество утилит, входивших ранее в состав пакета Windows Support Tools, теперь являются частью системы. Имеется стандартное средство для централизованного управления групповыми политиками в доменах — оснастка **Group Policy Management** (Управление групповой политикой). Новые возможности групповых политик перечислены в *главе 13*.
- В доменах Active Directory можно устанавливать компьютеры, доступные только для чтения (Read-Only Domain Controller) и имеющие ограниченные возможности репликации каталога.
- Для эффективной репликации каталога Active Directory можно использовать службу *DFS Replication* (Репликация DFS). Это позволяет применять более эффективный механизм и снизить трафик репликации.
- Службы *Active Directory Certificate Services* (Службы сертификатов Active Directory) позволяют выдавать сертификаты и управлять ими, обеспечивая работу приложений и служб, использующих технологии открытых ключей (PKI).
- Службы *Active Directory Federation Services* (Службы федерации Active Directory) позволяют организовать проверку подлинности пользователей при доступе к нескольким связанным веб-приложениям. Для этого предоставляется безопасный общий доступ к цифровому удостоверению, который можно контролировать на границах разных организаций.
- Службы *Active Directory Rights Management Services* (Службы управления правами Active Directory (AD RMS) обеспечивают защиту конфиденциальной цифровой информации от несанкционированного использования и позволяют повысить безопасность документооборота (файлов, сообщений электронной почты и т. п.) внутри организации. Права доступа к документу всегда передаются вместе с ним, и документ остается защищенным даже за пределами организации.
- Имеются "автономные" службы каталога — *Active Directory Lightweight Directory Services (AD LDS)* (Службы Active Directory облегченного до-

ступа к каталогам), которые позволяют развертывать на сервере несколько экземпляров каталога Active Directory и никак не связаны с доменными службами Active Directory.

Технология виртуализации Hyper-V™

Средства виртуализации Hyper-V позволяют запускать на компьютере другие операционные системы (x86 и x64) и также прикладные программы, не поддерживаемые в Windows Server 2008. Эта роль сервера может устанавливаться только на процессорах x64, которые, кроме того, имеют аппаратную поддержку виртуализации Intel VT или AMD-V (список таких процессоров несложно найти на сайтах производителей). Материнская плата компьютера должна поддерживать Data Execution Protection (DEP).

Виртуальный компьютер (Virtual PC)

Подсистема *Virtual PC* позволяет эмулировать среду виртуального компьютера для запуска различных приложений, которые могут быть несовместимы с Windows Server 2008 и требовать специфических программных средств. Программу Virtual PC 2007 можно бесплатно скачать с веб-сайта Microsoft и устанавливать на x86-платформах, работающих под управлением Windows Server 2008.

Командный процессор Windows PowerShell

Новый командный процессор, позволяющий работать в интерактивном режиме или в режиме выполнения административных сценариев. Имеет расширенные возможности доступа к компонентам системы для получения от них информации, а также для управления *(глава 6)*.

Обновленные службы терминалов (Terminal Services)

Службы терминалов капитально модернизированы и включают в себя Terminal Services Gateway (Шлюз служб терминалов) и Remote Applications (Удаленные приложения). Шлюз обеспечивает беспрепятственный удаленный доступ к приложениям, установленным на сервере терминалов. Технология RemoteApps позволяет быстро развертывать приложения, доступные удаленным пользователям (в том числе и обращающимся к серверу через Интернет).

Защита доступа к сети (NAP)

Технология защиты доступа к сети *Network Access Protection* (NAP) позволяет предотвратить доступ к внутренней пользовательской сети со стороны небезопасного компьютера, который не отвечает определенным критериям безопасности (эти критерии могут задаваться с помощью групповых политик). Благодаря этому сеть становится менее уязвимой к атакам вирусов и червей, которые могут появиться на мобильных компьютерах, не имеющих последних обновлений безопасности, включенных средств защиты и т. п. Клиентский компонент, поддерживающий данную технологию, входит в состав Windows Vista и Windows XP Service Pack 3, а серверная часть должна располагаться на компьютерах, работающих под управлением Windows Server 2008.

Службы UDDI

Службы UDDI (Universal Description, Discovery and Integration) реализуют промышленный стандарт публикации и поиска сведений о распределенных веб-службах. Они позволяют бизнес-приложениям и разработчикам публиковать, обнаруживать и совместно использовать веб-службы в пределах нескольких организаций, а также непосредственно взаимодействовать с этими службами с помощью средств разработки.

Общие средства ОС Windows Vista и Windows Server 2008

Перечислим отдельно общие возможности, появившиеся в клиентских ОС Windows Vista и серверных ОС Windows Server 2008; это обусловлено тем фактом, что обе линейки систем построены на одном ядре и разрабатывались в рамках одного проекта. Некоторые средства относятся к возможностям рабочего стола и ориентированы на удобства пользователя; в системах Windows Server 2008 они появляются при установке соответствующего компонента *(см. главу 3)*.

Пользовательский интерфейс Windows Aero™

Новый пользовательский интерфейс (стиль, тема оформления), получивший название *Windows Aero*0, доступен и в серверных версиях Windows Server 2008. Этот интерфейс призван обеспечить максимальную производитель-

ность в работе с компьютером, его отличают современный дизайн с полупрозрачными окнами (Aero Glass), многочисленные визуальные эффекты, новые возможности при манипуляциях с открытыми окнами (включая функции трехмерного представления окон при их переключении — Flip и Flip 3D) и т. д. *(глава 2)*.

Новые типы учетных записей безопасности и контроль учетных записей (User Account Control, UAC)

Для повышения защищенности системы имеется механизм *контроля учетных записей пользователей* (User Account Control, UAC). Смысл его работы состоит в том, что пользовательские учетные записи делятся по привилегиям на несколько типов, и система строго контролирует операции, разрешенные тому или иному пользователю. В результате снижается риск повреждения системы или вероятность выполнения несанкционированных действий. Если, например, обычный пользователь компьютера запустит системную утилиту или попытается изменить параметры конфигурации, то система попросит ввести пароль администратора системы или откажет пользователю в доступе к запрошенным функциям *(глава 14)*.

Новые средства диагностики и мониторинга

Мощные средства мониторинга позволяют контролировать работу компонентов операционной системы (включая аппаратные средства) и прикладных программ. При наличии проблем информация может передаваться в компанию Microsoft, после чего пользователь имеет возможность узнать о наличии решений по устранению неисправностей и загрузить нужные обновления. Стандартная (но значительно модернизированная) оснастка **Event View** (Просмотр событий) и совершенно новый инструмент — оснастка **Reliability and Performance Monitor** (Монитор производительности и стабильности) — имеют множество новых возможностей, позволяющих анализировать все параметры системы и регистрировать их в системных журналах *(глава 5)*.

Поддержка протокола IPv6

Системы полностью поддерживают протокол IP version 6, позволяющий расширить возможности адресации компьютеров в Интернете, поскольку он предусматривает значительно большее адресное пространство, чем повсеместно распространенный в настоящее время протокол IP version 4 (в котором для адресации используются четыре двухбайтовых слова, например,

192.168.125.11). Все сетевые системные утилиты рассчитаны на работу с IPv6 (он устанавливается по умолчанию) и позволяют конфигурировать его параметры.

Планировщик задач (Task Scheduler)

Планировщик задач был значительно модернизирован и превратился в мощное средство диспетчеризации задач, имеющее множество возможностей и развитый интерфейс *(глава 4)*.

Средства поиска информации

Средства расширенного поиска (Windows Search Engine) позволяют искать информацию, содержащуюся в локальных и удаленных файлах, почтовых сообщениях и интернет-ссылках. При этом активно используется служба индексирования (что значительно сокращает время поиска), и поиск может осуществляться по имени или типу файлов, по автору создания документа и дате его создания, а также по множеству других параметров (для чего можно создавать сложные фильтры) *(глава 2)*.

Службы Интернета (IIS)

Набор служб Internet Information Services (IIS) позволяет установить на компьютере FTP- и веб-сервер; возможности этих служб используются многими другими компонентами операционной системы (например, службами печати или службами терминалов). В составе систем поставляются службы IIS версии 7.0 *(глава 11)*.

Браузер Internet Explorer 7.0

Среди множества новых функций Internet Explorer 7.0 следует отметить возможность одновременного просмотра нескольких веб-страниц на отдельных вкладках (tabs), средства фильтрации веб-сайтов (Phishing Filter), интегрированные средства поиска в Интернете, расширенные функции печати веб-страниц и поддержку XML-технологии Really Simple Syndication (RSS). Также имеются функция блокировки всплывающих окон (pop-ups) и средства управления устанавливаемыми компонентами (add-ons). Всеми настройками браузера можно управлять с помощью групповых политик.

Почтовый клиент Windows Mail

На смену стандартному почтовому клиенту Outlook Express пришла новая программа — Windows Mail (Почта Windows). Несмотря на новое имя, она является прямой наследницей Outlook Express (на это указывает и ее версия — 6.0.6000.16386). Помимо традиционных функций, программа имеет новые антиспамовые фильтры, а также возможность поиска в почтовых сообщениях из меню **Start** (Пуск).

Совместное использование факсов

Пользователи сети могут пользоваться факс-сервером или общим факсимильным аппаратом, подключенным к любому из компьютеров. Имеется новая клиентская программа для работы с факсами и сканерами *(глава 9)*.

Просмотр библиотеки графических изображений (Windows Photo Gallery)

Программа *Windows Photo Gallery* (Фотоальбом Windows) позволяет конечным пользователям упростить работу с большим количеством цифровых фотографий и графических изображений, а также выполнять простейшие манипуляции с самими картинками (например, улучшать качество картинки или форматировать ее). В системе имеется также программа просмотра изображений (Photo Gallery Viewer) (аналог программы Windows Picture and Fax Viewer (Программы просмотра изображений и факсов), входящей в состав предыдущих версий Windows), которая обладает аналогичными возможностями и похожим интерфейсом.

Проигрыватель Windows Media Player 11.0

Последняя версия проигрывателя файлов мультимедиа позволяет слушать и смотреть файлы самых разных форматов, переписывать аудиодиски на жесткий диск (форматы WMA, WMA lossless, MP3 и WAV) и записывать музыкальные сборники на CD-диски (в формате обычного аудиокомпакт-диска) или переносимое устройство (например, флэш-плеер). Имеется возможность записи на DVD-диски.

Календарь Windows (Windows Calendar)

Программа-органайзер "Календарь Windows" (Windows Calendar) представляет собой ежедневник, в который можно заносить все запланированные со-

бытия и мероприятия, причем эта информация может быть доступна коллегам, составляющим рабочую группу.

Образы установки

Формат *Windows Imaging* (WIM) позволяет хранить в одном файле один или несколько законченных образов установки систем. Для уменьшения пространства, занимаемого на диске, файл сжимается, и все файлы хранятся только в одном экземпляре. Использование образов позволяет уменьшить время развертывания систем в организации (чистая установка систем занимает около 20 минут) и уменьшить число возможных ошибок конфигурирования *(глава 1)*.

Восстановление с помощью архивного образа системы (Windows Complete PC)

Новая функция — *Windows Complete PC* — позволяет полностью восстановить систему в случае краха при загрузке с дистрибутивного диска (подобная функция — Automated System Recovery, ASR (Мастер аварийного восстановления системы) — существует и в предыдущих версиях Windows, однако теперь она полностью модифицирована). (Способы создания архива системы в Windows Vista и Windows Server 2008 немного различаются, при этом пользовательский интерфейс средств архивации и восстановления отличается весьма существенно.) Образ системы может сохраняться на жестком диске или записываться непосредственно на DVD-диск. В образ могут быть включены системный и загрузочный разделы, а также другие логические диски. С помощью этой функции легко перенести систему и данные на жесткий диск большего размера *(глава 15)*.

Встроенный брандмауэр Windows

Пользователей систем можно оградить от опасных вторжений из Интернета с помощью простого, но эффективного брандмауэра (Internet Connection Firewall). Возможности настройки брандмауэра заметно расширены, имеется возможность фильтрации исходящих подключений *(глава 8)*.

Защитник Windows (Windows Defender)

Программа Windows Defender является стандартным компонентом системы (в других версиях Windows ее можно устанавливать факультативно); она по-

зволяет защитить компьютер от разнообразных шпионских (spyware) программ, а также нежелательных приложений, которые могут нарушить работоспособность и безопасность системы *(глава 14)*.

Шифрование дисков Windows BitLocker™ Drive Encryption

Новая аппаратно-программная технология защиты данных на жестком диске позволяет предотвратить доступ к хранящейся на нем информации в том случае, если диск потерян или украден. Для ее работы требуется специальная микросхема — *Trusted Platform Module* (TPM), которая обычно устанавливается на материнскую плату компьютера. В ней хранятся ключи, пароли и цифровые сертификаты, причем доступ к этой информации сложно получить путем программных атак или в случае физической кражи компьютера.

Подсистема для UNIX-приложений

Подсистема Subsystem for UNIX-based Applications (SUA) позволяет запускать приложения, написанные для UNIX-систем.

Консоль управления Microsoft Management Console (MMC) 3.0

В состав систем входит новая версия консоли управления, представляющая собой программную оболочку для административных утилит, обеспечивающую универсальный пользовательский интерфейс для всех системных инструментов и средств администрирования, входящих в другие программные продукты. Возможностями консоли управления можно пользоваться из сценариев и командных файлов *(глава 3)*.

Новые интерфейсы программирования (API)

Имеется множество новых программных технологий, объединяющих в себе API для различных целевых областей: Windows Presentation Foundation (кодовое название "Avalon"), Windows Communication Foundation (кодовое название "Indigo"), Windows Workflow Foundation и Windows CardSpace. .NET Framework 3.0 входит в состав Windows Server 2008 (по умолчанию не активизирован, устанавливается как дополнительный компонент сервера — *см. главу 3*). Windows Presentation Foundation является подсистемой визуального представления информации и позволяет использовать единый подход при создании документов, графики и приложений. Windows Communication Foundation реализует аналогичные принципы для построения сетевых и распределенных бизнес-приложений (веб-служб).

Модернизированные средства, унаследованные от предыдущих версий Windows 2000/Windows XP/Windows Server 2003

В заключение отметим еще некоторые важные средства Windows Server 2008, которые были реализованы уже в предыдущих версиях Windows, начиная с Windows 2000 (*все* унаследованные возможности перечислить просто невозможно). Однако в системах Windows Vista и Windows Server 2008 эти средства были в той или иной степени модернизированы или имеют новые версии.

Быстрое переключение пользователей (Fast User Switching)

Это средство позволяет нескольким пользователям быть одновременно зарегистрированными на компьютере (даже если компьютер входит в домен). Можно, не выходя из системы и не закрывая работающие программы (они не будут остановлены), переключиться на другую учетную запись и работать в среде другого пользователя *(глава 2)*.

Определение действующих групповых политик (Resultant Policy)

При работе в домене Active Directory, где для администрирования пользователей применяются различные групповые политики, возникают сложности с определением результирующих параметров безопасности с учетом наследования и иерархии политик, организации подразделений в домене и подобных факторов. Оснастка **Resultant Set of Policy** (Результирующая политика) позволяет упростить проверку параметров групповых политик на отдельном компьютере, а оснастка **Group Policy Management** (Управление групповой политикой) имеет возможности для моделирования вариантов применения политик в сетях с развитой иерархией доменов. В системах Windows Vista и Windows Server 2008 появились сотни новых групповых политик, позволяющих управлять системными компонентами и программами *(глава 13)*.

Удаленный доступ к рабочему столу (Remote Desktop)

В составе многих систем Windows имеется "облегченная" версия служб терминалов (Terminal Services). Для использования их возможностей имеются две стандартных функции: *Remote Desktop* (Удаленный рабочий стол) позво-

ляет удаленно подключиться к компьютеру и использовать все его возможности (для решения задач администрирования или прикладных задач); *Remote Assistance* (Удаленный помощник) по запросу пользователя позволяет удаленному эксперту (из службы поддержки Microsoft, системному администратору или просто знакомому) наблюдать за тем, что происходит на экране компьютера, вести диалог с пользователем и при необходимости (и при получении соответствующего разрешения) самому выполнять нужные действия. В системах Windows Vista и Windows Server 2008 используются дополнительные механизмы защиты удаленных подключений *(глава 4)*.

Клиент и служба теневого копирования томов (Shadow Copy)

В системах Windows Server 2003 впервые появилась служба теневых копий томов, позволяющая "прозрачно" для пользователей делать резервные копии дисковых томов и при необходимости вернуться к предыдущим версиям файлов. Для того чтобы клиенты серверов могли пользоваться этой возможностью, на компьютерах должна быть установлена клиентская часть этой службы — Shadow Copy Client. Клиент теневых копий является стандартным компонентом последних версий Windows, как и *сама* служба теневого копирования томов (VSS), которая используется для создания точек состояния дисковых томов с целью их архивации, а также для поддержки функции предыдущих версий. Если в системе периодически создаются теневые копии, то пользователь при утрате файла или папки может восстановить их прежнюю версию *(глава 15)*.

Запись на диски CD-R/CD-RW и DVD-R/DVD-RW

Встроенная поддержка устройств записи на диски (с однократной или многократной записью) позволяет легко сохранять критические данные большого объема и создавать архивы. (В предыдущих версиях Windows диски DVD не поддерживаются встроенными программами.) При этом применяются распространенные стандарты, что позволяет использовать записанные диски на других компьютерах и устройствах *(глава 6)*.

Сервер сценариев (WSH)

Windows Scripting Host (WSH) версии 5.7 — средство для выполнения сценариев, запускаемое с рабочего стола или из командной строки. Поддерживаются языки VBScript и JScript.

Справка и поддержка (Help and Support)

Справочная служба в сочетании с функцией Remote Assistance (Удаленный помощник) и при наличии подключения к Интернету является достаточно эффективным средством поиска необходимых сведений как на локальном компьютере, так и в базе знаний Microsoft Knowledge Base. Непосредственно из окна справки пользователь может обратиться к информационным ресурсам Microsoft и телеконференциям (newsgroups). В системах Windows Vista и Windows Server 2008 справочная система существенно переделана *(глава 3)*.

Сравнение функциональных возможностей редакций Windows Server 2008 на различных платформах

Все редакции Windows Server 2008 выпускаются как в 32-разрядной (x86), так и в 64-разрядной (x64) версии; также имеются версии для платформы Itanium. Существуют планы компании Microsoft по полному переходу на 64-разрядные процессоры в следующих клиентских и серверных версиях Windows.

Каждая редакция Windows Server 2008 ориентирована на определенную область применения, и в первую очередь различия между редакциями состоят не в наборе компонентов и служб, а в возможностях масштабирования и соответствии большим нагрузкам. Возможности разных редакций Windows Server 2008 перечислены в табл. В1.

Таблица В1. *Основные функции, реализованные в различных редакциях Windows Server 2008*

	Windows Server 2008 Web	Windows Server 2008 Standard	Windows Server 2008 Enterprise	Windows Server 2008 Datacenter	Itanium-системы
x86 (процессоров)	4	4	8	32	-
x64 (процессоров)	4	4	8	64	-
IA64 (процессоров)	-	-	-	-	64
ОЗУ (32-разрядные системы)	4 Гб	4 Гб	64 Гб	64 Гб	-

Таблица В1 *(продолжение)*

	Windows Server 2008 Web	Windows Server 2008 Standard	Windows Server 2008 Enterprise	Windows Server 2008 Datacenter	Itanium-системы
ОЗУ (64-разрядные системы)	32 Гб	32 Гб	2 Тб	2 Тб	2 Тб
"Горячее" расширение ОЗУ	-	-	да	да	да
"Горячая" замена ОЗУ и добавление/замена процессоров	-	-	-	да	да
Количество кластеров	-	-	16	16	8
Репликация DFS (DFS-Replication) с использованием Cross-file RDC (Remote Differential Compression)	-	-	да	да	да
Network Access Protection (Защита доступа к сети)	-	да	да	да	-
Подключения удаленного доступа (RRAS)	-	250	не ограничено	не ограничено	2
Подключения через шлюз службы терминалов (TS Gateway)	-	250	65535	65535	-
AD Rights Management Services (RMS; Службы управления правами)	-	да	да	да	-
Windows Deployment Services (Службы установки Windows)	-	да	да	да	-
Медиа-сервер	базовый	базовый	полный	полный	-

Таблица В1 *(окончание)*

	Windows Server 2008 Web	Windows Server 2008 Standard	Windows Server 2008 Enterprise	Windows Server 2008 Datacenter	Itanium-системы
Виртуализация (Hyper-V, Viridian)	-	да	да	да	-
- Быстрая (live) миграция	-	-	да	да	-
- Кластеризация виртуальных образов	-	-	да	да	-
"Горячее" добавление/замена виртуальной памяти	-	-	да	да	-
"Горячее" добавление/замена виртуальных процессоров	-	-	да	да	-
Использование виртуальных образов	-	Хост+1 VM	Хост+4 VM	не ограничено	не ограничено
Режим установки Server Core	да	да	да	да	-

Реальный объем доступной памяти на x86-системах зависит от используемой материнской платы (чипсета и памяти) и наличия на ней механизма *Physical Address Extension* (PAE), позволяющего 32-разрядным системам использовать более 4 Гбайт физической памяти. Поэтому возможности работы системы с максимальным объемом памяти нужно проверять для каждой конкретной конфигурации (информацию нужно получать от производителя или искать на веб-сайте Microsoft).

Максимальный объем виртуального адресного пространства для каждого 32- или 64-разрядного процесса, работающего в пользовательском режиме (user mode), равен 2 Гбайт для x86-[1] и x64-систем (предел может быть выше за

[1] На 32-разрядных системах могут запускаться только 32-разрядные процессы; на 64-разрядных системах — и те, и другие.

счет особых механизмов; информацию можно найти на веб-сайте Microsoft в библиотеке MSDN).

Максимальный объем виртуального адресного пространства для режима ядра (kernel mode) равен 2 Гбайт для x86-систем и 8 Тбайт — для x64-систем.

Требования к аппаратным ресурсам

Перед установкой системы в первую очередь необходимо ознакомиться со списком минимальных требований, которые Windows Server 2008 предъявляет к оборудованию. Кроме того, рекомендуется проверить оборудование на совместимость с Windows Server 2008. (Для Windows Vista список различных устройств, сгруппированных по типу, — *Windows Logo'd Products List* — имеется на веб-странице **http://winqual.microsoft.com/hcl/**.)

Состав минимально необходимой для Windows Server 2008 аппаратной конфигурации представлен в табл. В2. Эти требования в значительной степени зависят от набора установленных ролей сервера.

Таблица В2. *Основные параметры аппаратных средств, необходимых для установки Windows Server 2008*

Компонент	Требования
Процессор	32-разрядный (x86) или 64-разрядный (x64) процессор с тактовой частотой 1 ГГц (1,4 ГГц для x64). Для комфортной работы рекомендуется 2 ГГц и выше
Оперативная память	Не менее 512 Мбайт; реально требуется 2 Гбайт и более
Монитор	Минимально поддерживаемое разрешение экрана 800 на 600, в реальности требуется 1024 на 768 и выше. Глубина цвета — 32 бита (при меньшей глубине цвета отключается стиль Aero Glass)
Видеоадаптер	Обязательна совместимость с DirectX 9.0. Желательна поддержка Pixel Shader 2.0, драйверы, отвечающие спецификации *Windows Vista Display Driver Model* (WDDM)[1], объем видеопамяти не менее 64 Мбайт

[1] Не следует путать эту аббревиатуру с WDM (Win32 Driver Model).

Таблица В2 *(окончание)*

Компонент	Требования
Жесткие диски	Раздел на жестком диске с объемом свободного пространства не менее 10 Гбайт[1] плюс файлы подкачки, гибернации и дампы памяти; рекомендуется 40 Гбайт и выше. (Не менее 8 Гбайт незанятого места требуется при обновлении системы.) При расчете объема свободного дискового пространства, необходимого для установки, следует учитывать объем ОЗУ, установленный на компьютере
Клавиатура	Стандартная
Мышь	Стандартная мышь или другое совместимое координатное устройство
DVD-ROM	Устройство DVD-ROM или DVR-RW (для записи архивов)
Сетевой адаптер	Совместимый сетевой адаптер (если компьютер будет подключен к локальной сети)

Дифференциация требований к графической подсистеме

Поскольку все возможности нового визуального интерфейса Aero Glass доступны и в ОС Windows Server 2008, укажем требования, предъявляемые к графической подсистеме. Эти требования совсем не обязательны, практически на любых компьютерах будут доступны стили *Windows Vista Basic* (Упрощенный стиль Windows Vista) или *Windows Classic* (Классический стиль). Можно определить три качественных уровня, определяющих возможности пользовательского графического интерфейса:

- базовый — сравнимый с интерфейсом Windows XP;
- улучшенный — использование возможностей WDDM-драйверов;

[1] Речь идет только об инсталляции самой системы и ее нормальной работе. При установке прикладных программ требуется дополнительное место; отдельная тема — файлы пользователей и свободное пространство, необходимое для работы приложений (например, при записи архивов на DVD-диски и т. п.).

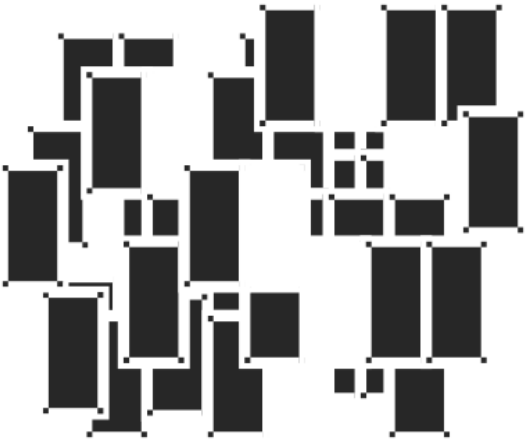
- максимальный — поддержка стиля Aero Glass ("гладкое" перемещение окон; эскизы; 3D-эффекты; масштабируемость интерфейса; визуальные стили, включающие прозрачные окна; улучшенные "переходные" эффекты и т. д.).

Минимальные требования к графическому адаптеру для использования стиля Aero Glass следующие (при наличии WDDM-драйвера):

- видеопамять 64 Мбайт (глубина цвета 32 бита);
- аппаратная поддержка DirectX 9 и Pixel Shader 2;
- AGP 4x и выше (скорость передачи данных на шине видеопамяти 1600 Мбайт/с и выше).

Объем необходимой видеопамяти определяется из требования "32 бита на пиксел". Поэтому в зависимости от используемого разрешения экрана ее минимальный объем будет следующим:

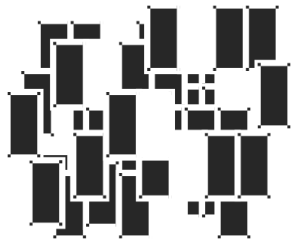
- 64 Мбайт для одного монитора с разрешением не выше 13 107 20 пикселов (1280 на 1024; скорость передачи не менее 1800 Мбайт/с);
- 128 Мбайт для одного монитора с разрешением не выше 2 304 000 пикселов (1920 на 1200);
- 256 Мбайт и выше для более высоких разрешений или нескольких экранов.



ЧАСТЬ I

Конфигурирование, администрирование и мониторинг серверов

Глава 1



Инсталляция систем и подготовка к работе

Эта глава посвящена различным способам установки операционных систем Windows Server 2008 и подготовке к эксплуатации. Рассматриваются самые важные вопросы, возникающие с момента планирования новой инсталляции и до ее готовности к использованию в рабочих условиях. Средства и возможности конфигурирования уже установленной системы, настройка ее компонентов и служб под конкретные задачи (роли сервера) рассматриваются отдельно в *главе 3*.

Подготовка к установке системы

Перед началом установки операционной системы необходимо определиться с некоторыми небольшими, но принципиальными вопросами, от которых будет зависеть выбор опций в процессе инсталляции и последовательность последующих действий. Это позволит избежать недоразумений или ошибок при инсталляции (что чревато необходимостью повторной установки, потерей пользовательских настроек или вынужденными ограничениями при дальнейшей работе с компьютером).

Системы Windows Vista и Windows Server 2008 не предъявляют каких-то особых требований к разметке дисков (разделов или томов) и без проблем могут существовать на одном физическом диске (но в разных логических разделах) с другими операционными системами. Хотя и имеются некоторые важные отличия и принципиальные моменты, о которых и будет рассказано в этом разделе (полезно также предварительно познакомиться с *главой 7*, поскольку в ней рассказывается об особенностях организации дисковых томов,

способах управления ими и имеющихся ограничениях — эта информация поможет правильно спланировать начальную разбивку дисков и без проблем эксплуатировать систему в дальнейшем).

Выбор режима инсталляции

Для систем Windows существуют два режима установки новой версии операционной системы:

- *установка новой копии* ("чистая" инсталляция) в чистый раздел диска. При этом отдельно нужно будет устанавливать прикладные программы и, возможно, переносить настройки и файлы приложений и пользователей из другой рабочей системы или с другого компьютера;
- *обновление уже существующей системы*. В этом случае все пользовательские настройки сохраняются и установленные приложения остаются работоспособными (во всяком случае те из них, которые поддерживаются в Windows Server 2008); по окончании обновления практически в неизменном виде сохраняется рабочая среда системы.

В первом случае возможен также вариант, когда на компьютере имеются уже установленные копии Windows[1] (неважно, какой версии) — получится *система с двойной* (или *множественной*) *загрузкой*, и нужную для работы систему можно будет выбирать перед загрузкой *(см. разд. "Организация систем с двойной загрузкой")*.

Систему Windows Vista или Windows Server 2008 нельзя установить в тот раздел, где уже имеется другая инсталляция Windows. Если точнее — установить можно (при наличии места), но существовавшая ранее система станет полностью неработоспособной (пользовательские файлы не теряются, но все "старые" системные файлы будут скопированы в специальную папку). Поэтому при организации систем с двойной загрузкой новые системы следует устанавливать только в чистые разделы (во всяком случае не имеющие системных папок *Windows*, *Program Files* и т. д.).

> ***Внимание!***
>
> При обновлении существующей системы необходимо временно отключить (лучше удалить) все антивирусное программное обеспечение, а также работающие сетевые сервисы и клиентское программное обеспечение третьих фирм.

[1] Возможно наличие и других операционных систем.

Конфигурирование разделов на жестком диске

В процессе инсталляции Windows Server 2008 программа установки предлагает пользователю выбрать диск или раздел жесткого диска для установки системы.

Создавать разделы на жестком диске можно тремя способами.

- Программа установки Windows Server 2008, загруженная с дистрибутивного компакт-диска, позволяет создать новый раздел для Windows Server 2008 (при условии, что на диске имеется свободное пространство), а также создавать, удалять и форматировать другие разделы и тома.

> ***Внимание!***
>
> Программа установки Windows Server 2008 создает на жестком диске только *основные* разделы *(см. главу 7)*. Если необходима более сложная конфигурация логических дисков, то ее нужно готовить заранее.

- Загрузившись с дистрибутивного диска и воспользовавшись опцией восстановления системы *(см. главу 15)*, можно открыть окно командной строки и запустить утилиту DiskPart, которая позволяет выполнять все операции по разметке дисков и подготовке разделов или томов.
- Если на компьютере уже установлена система Windows, то разделы на жестком диске можно создать с помощью административных средств этой операционной системы (обычно для этих целей используется оснастка **Disk Management** (Управление дисками) — *см. главу 7*).

Уместно вспомнить два определения, касающиеся названий разделов диска (можно также говорить о названиях логических дисков или томов).

Системным разделом (system partition) называется раздел жесткого диска, на котором располагаются файлы, необходимые для инициализации операции загрузки операционной системы (при установке систем Windows Vista и Windows Server 2008 здесь будет находиться диспетчер загрузки *Windows Boot Manager*). В качестве системного раздела может использоваться только основной (primary) раздел.

Загрузочный раздел (boot partition) — это раздел, который непосредственно содержит файлы самой операционной системы (имеются в виду папка *%SystemRoot%* и ее подкаталоги). Из этого раздела происходит загрузка системы и ее компонентов.

Если на жестком диске всего один раздел, то к нему будут относиться оба определения. Если на диске несколько разделов (или в системе несколько физических дисков), то загрузочный раздел может и не совпадать с системным (например, диск C: будет системным, а сама система будет установлена на диск D: или E:).

> ***Внимание!***
>
> При обновлении операционных систем Windows Server 2003 нужно учитывать, что для выполнения операции свободное пространство на загрузочном диске должно не менее чем в два раза превышать по объему системные папки.

Выбор файловой системы

Системы Windows Vista и Windows Server 2008 поддерживают все файловые системы, традиционно используемые в системах Windows: FAT12, FAT16, FAT32 и NTFS. Две файловые системы поддерживаются для CD- и DVD-приводов: Compact Disc File System (CDFS) и Universal Disk Format (UDF) (версии 1.5, 2.0, 2.1 и 2.5).

Относительно более новая файловая система — *exFAT* (расширенная FAT) — оптимизирована для использования в съемных флэш-устройствах большого объема и разработана для того, чтобы избавиться от проблем и ограничений, связанных с использованием FAT в накопителях подобного типа (например, снято ограничение на максимальный размер файлов, равный 4 Гбайт).

Проблема выбора файловой системы для диска, на который будет устанавливаться Windows Server 2008, не возникает, поскольку выбора, как такового, нет — системы Windows Server 2008 устанавливаются только на логические диски или разделы (тома), ***отформатированные под NTFS***. На других же дисках, используемых другими системами или для хранения данных, могут применяться любые из перечисленных выше файловых систем.

Причина такого жесткого ограничения на тип используемой файловой системы очень проста — только NTFS обеспечивает должную безопасность и надежность хранения информации (особенно на дисках большого размера) и предоставляет возможности для реализации многих функций системы (например, создание точек восстановления, работа со списками управления доступом, шифрованная файловая система EFS, потоки, используемые для хранения дополнительных свойств файлов, и т. д.).

Организация систем с двойной загрузкой

Системы Windows Vista и Windows Server 2008 без особых проблем можно установить на компьютеры, на которых уже имеются операционные системы Windows. (Некоторые сложности могут быть только из-за нового диспетчера загрузки, появившегося в Windows Vista/Windows Server 2008 — *см. далее*.) В этом случае компьютер конфигурируется как *система с двойной* (или множественной) *загрузкой* — пользователь будет иметь возможность выбирать операционную систему при запуске компьютера (в принципе, этих систем может быть две, три и более). Чтобы подобная конфигурация была работоспособной, соблюдайте простые правила, изложенные ниже.

- Устанавливайте каждую операционную систему на отдельный раздел — в этом случае системы будут совершенно независимыми друг от друга и для них можно выбирать разные файловые системы (FAT32 и NTFS), если это требуется (однако Windows Server 2008 можно ставить только на NTFS). Установка Windows Server 2008 в один раздел (логический диск) с уже существующей операционной системой невозможна; файлы "старой" системы будут перенесены в папку Windows.old, и эта система перестанет функционировать (хотя информация потеряна не будет).
- Операционные системы более ранних версий следует устанавливать первыми (хотя это требование и не строгое). Если, например, устанавливать любую предыдущую версию Windows (более раннюю, чем Windows Vista) после Windows Server 2008, то загрузочный сектор жесткого диска будет переписан, что сделает невозможной загрузку Windows Server 2008. Для восстановления возможности загрузки Windows Server 2008 придется воспользоваться опциями восстановления системы и утилитами, которые доступны при загрузке с дистрибутивного диска Windows Server 2008 *(см. главу 15)*.

Системы Windows Vista и Windows Server 2008 больше не используют загрузчик, который работает с файлом boot.ini, и имеют свой диспетчер загрузки Windows — *Windows Boot Manager*. Если на компьютере установлены только системы Windows Vista/Windows Server 2008, то файл boot.ini на компьютере будет вообще отсутствовать.

> ***Примечание***
>
> В системах с двойной загрузкой для переключения между старым загрузчиком NTLDR и диспетчером Windows Boot Manager используется утилита *Bootsect.exe*, которую можно найти на дистрибутивном диске системы в папке \boot. С ее помощью, например, можно восстановить работу диспет-

чера загрузки после того как на компьютер с Windows Server 2008 была установлена более ранняя версия Windows. Она также полезна, если нужно совсем удалить Windows Server 2008 и оставить другую версию Windows, использующую NTLDR и boot.ini.

На рис. 1.1 показано окно выбора загружаемой системы — окно диспетчера загрузки Windows. (Оно отображается, если только на компьютере установлено две системы или если успеть нажать клавишу <F8> при начальной загрузке системы.) Обратите внимание, что в окне имеется новая опция — **Windows Memory Diagnostic** (Диагностика памяти) (для переключения нужно нажать клавишу <Tab>). При ее выборе запускается двухпроходный тест памяти, после чего система перезагружается. При выполнении теста можно следить за ходом процесса (рис. 1.2). Клавиша <F1> в этом окне позволяет перейти к параметрам теста.

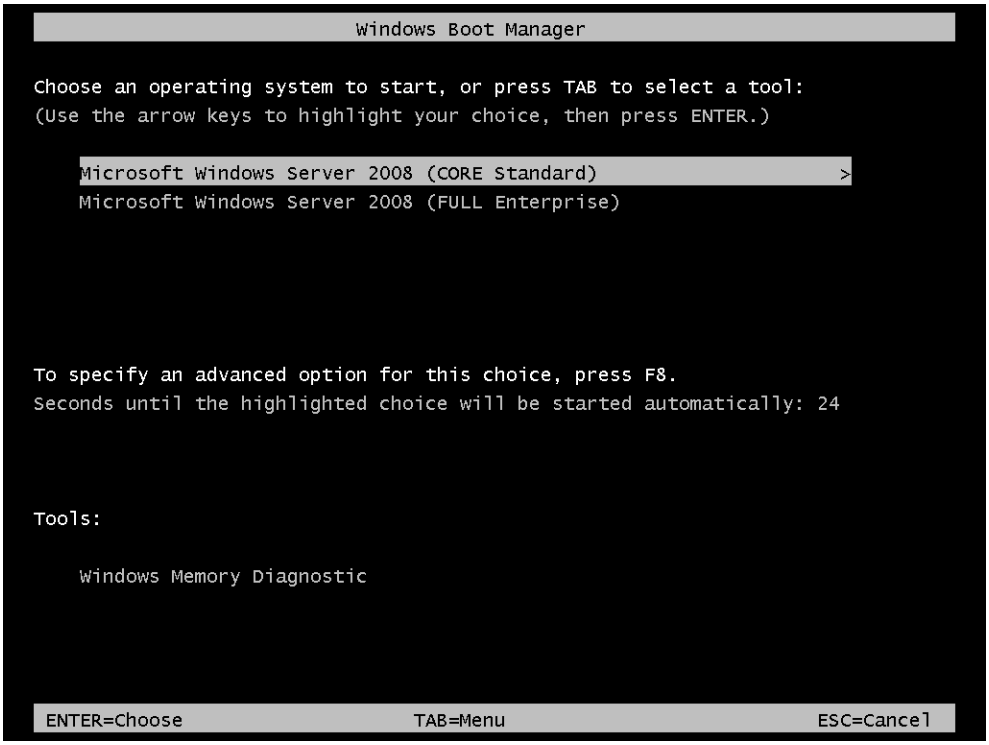


Рис. 1.1. Окно выбора загружаемой операционной системы

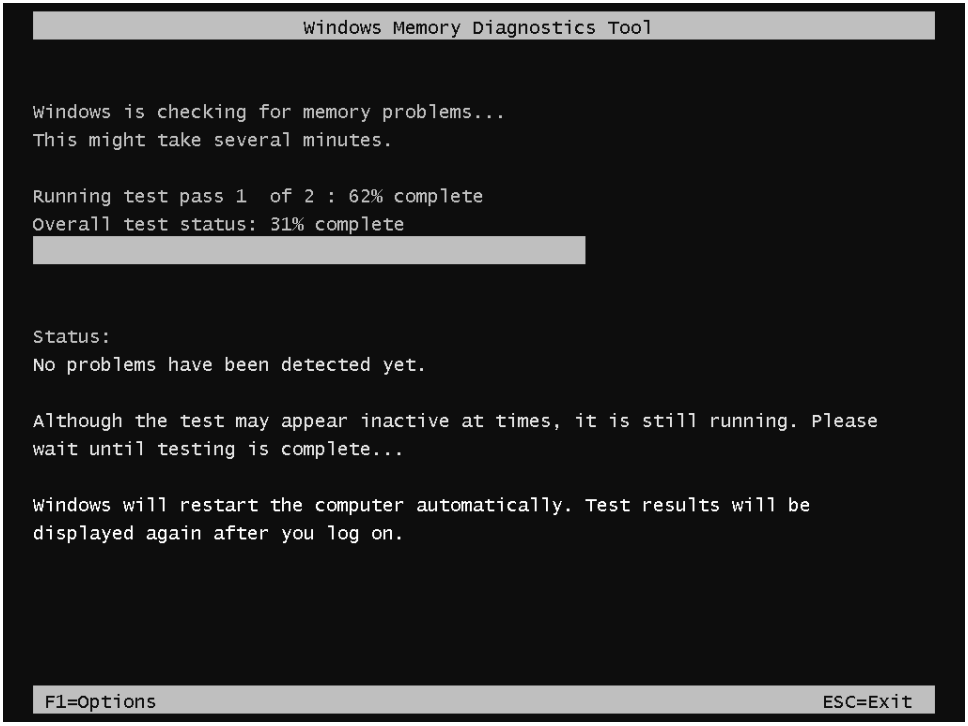


Рис. 1.2. Экран утилиты диагностики памяти

В окне параметров (рис. 1.3) можно выбрать подмножество тестов для диагностики (по умолчанию выполняется стандартный набор), указать режим использования кэша при выполнении тестов и количество проходов для выбранного подмножества тестов (по умолчанию 2).

После загрузки системы и регистрации пользователя на экране появляется сообщение, указывающее на выполнение теста и успешность результатов (рис. 1.4).

Запуск теста памяти можно инициировать и из самой системы, выбрав команду **Memory Diagnostic Tool** (Средство диагностики памяти) в подменю **Administrative Tools** (Администрирование). В этом случае имеются две возможности: можно сразу запросить перезагрузку системы и выполнение теста или же тест будет автоматически запущен при следующей перезагрузке компьютера.

На рис. 1.1 показан случай, когда на компьютере установлены две системы Windows Server 2008. Если до установки Windows Server 2008 существовала

система предыдущей версии (более ранней, чем Windows Vista), то в списке загружаемых систем помимо строки (строк) для системы Windows Server 2008 будет присутствовать опция **Ealier version of Windows** (Предыдущая версия Windows).

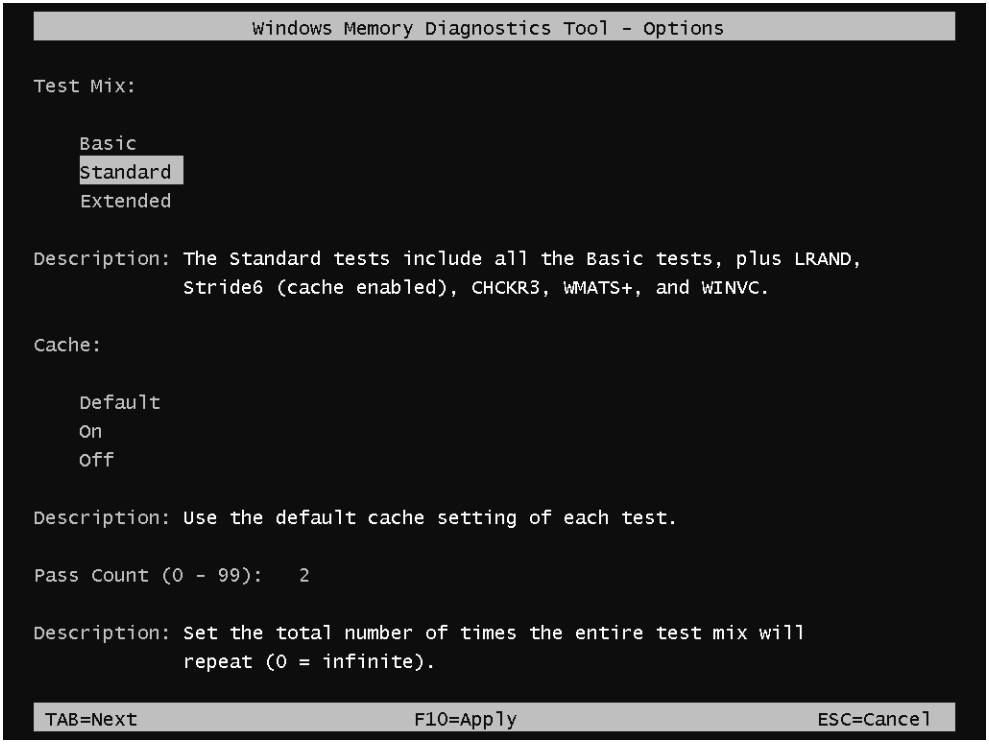


Рис. 1.3. Окно выбора параметров работы утилиты диагностики памяти

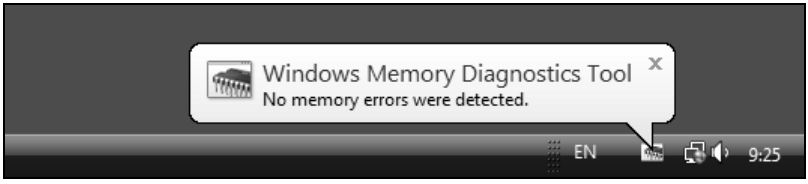


Рис. 1.4. Сообщение о результатах выполнения теста памяти

При ее выборе будет появляться дополнительное меню — традиционное меню загрузчика Windows, в котором будут присутствовать опции, хранящиеся

в файле boot.ini. При этом операционные системы можно будет загружать только из "своего" меню: Windows Vista и Windows Server 2008 — из главного меню (см. рис. 1.1), а предыдущие версии — из дополнительного (в этих системах сохраняются все возможности, касающиеся параметров и способов редактирования файла boot.ini).

Для редактирования сообщений, отображаемых диспетчером Windows Boot Manager, в системах Windows Vista и Windows Server 2008 имеется специальная утилита командной строки *BCDedit.exe*. С ней можно работать, ***только имея полномочия администратора*** (т. е. окно консоли необходимо открывать от имени администратора — в заголовке окна должно присутствовать слово Administrator (Администратор)).

Текущую конфигурацию диспетчера загрузки можно сохранить в файле с помощью следующей команды (при этом также появляются файлы вида `bcdbackup.LOG`):

```
bcdedit /export "c:\bcdbackup"
```

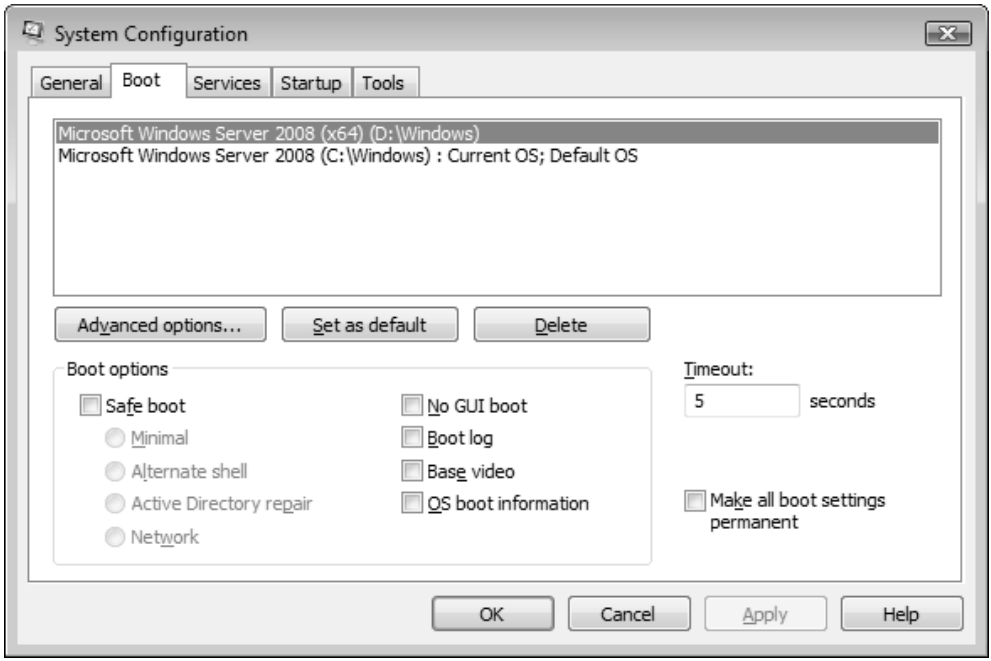


Рис. 1.5. Управление опциями диспетчера загрузки с помощью утилиты System Configuration

Следующая команда позволит поменять строку, отображаемую в меню выбора систем, для *загруженной в данный момент* системы:

```
bcdedit /set description "Windows Server 2008 (test configuration)"
```

Параметры команды можно узнать, выполнив команду `bcdedit /?`.

Некоторые дополнительные возможности для работы с диспетчером Windows Boot Manager имеет утилита System Configuration (Конфигурация системы; msconfig.exe), которую можно запустить из подменю **Administrative Tools** (Администрирование). На вкладке **Boot** (Загрузка) (рис. 1.5) перечислены опции меню выбора операционных систем и можно устанавливать особые режимы загрузки.

Еще бóльшие возможности по конфигурированию опций загрузки Windows Vista/Windows Server 2008 имеют специализированные утилиты, которые несложно найти в Интернете: например, *EasyBCD* или *VistaBootPro*. Эти утилиты могут устанавливаться и работать и в предыдущих версиях Windows.

Интерактивная установка Windows Server 2008

После решения всех вопросов, касающихся планирования установки операционной системы, можно приступать непосредственно к инсталляции. Благодаря тому, что используются *образы инсталляции* (файлы в формате Windows Imaging (WIM)), время установки систем Windows Vista и Windows Server 2008 значительно сокращено: на компьютере средней производительности на эту операцию требуется приблизительно 20 минут (вместо 60 для предыдущих версий). (Однако процедура обновления Windows Server 2003 до Windows Server 2008 по-прежнему занимает не менее часа, причем без учета дополнительного времени, необходимого для миграции параметров прикладных сервисов.)

Установка системных файлов происходит в папку \Windows на указанном диске или разделе. Все профили пользователей располагаются в папке \Users, а в папки \Program Files и \Program Data будут копироваться файлы системных приложений (и, по умолчанию, пользовательских программ).

Дистрибутив Windows Server 2008 имеет размер порядка 1,76 Гбайт (2,49 Гбайт для платформы x64); сам файл образа (install.wim) имеет размер 1,47 Гбайт (2,16 Гбайт для x64). Традиционная папка \i386 на дистрибутивном диске от-

сутствует, как нет теперь и программ установки Winnt.exe и Winnt32.exe. Для инсталляции системы запускается программа Setup.exe, а все дистрибутивные файлы находятся на диске в папке \sources.

Все системные библиотеки и программы хранятся в двух больших файлах — *boot.wim* и *install.wim* (последний из них, по сути, и является дистрибутивом системы).

Установка Windows Server 2008 в режиме Server Core

Установка серверов в режиме Server Core ничем не отличается от стандартной процедуры инсталляции систем. Первое отличие этого режима — отсутствие графического интерфейса, т. е. после установки системы, загрузки и регистрации администратор увидит только пустой экран с окном консоли, средства рабочего стола (включая меню **Start** (Пуск) и панель задач) будут отсутствовать.

Другое важное отличие — полное отсутствие оснасток администрирования; можно использовать только утилиты командной строки. Работает диспетчер задач, возможно обычное переключение задач по нажатию клавиш <Alt>+<Tab>, можно использовать "заветные" три клавиши <Ctrl>+<Alt>+<Del>.

Несложно сымитировать работу полной версии Windows Server 2008 в режиме Server Core. Запустите редактор реестра, и в разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` замените стандартное значение переменной `Shell`, где записана строка `explorer.exe`, на другое — `cmd /c "cd /d "%USERPROFILE%" & start cmd.exe /k runonce.exe /AlternateShellStartup"` (с сохранением всех кавычек). После этого нужно перезагрузиться. Теперь можно будет *приблизительно*[1] посмотреть, как выглядит рабочая среда сервера. Чтобы вернуться к обычной среде, необходимо отредактировать реестр и вернуть переменной `Shell` исходное значение `explorer.exe`.

Новая установка системы с загрузочного компакт-диска

Рассмотрим процедуру установки системы на самом простом примере — когда используется загрузочный дистрибутивный компакт-диск Windows Server

[1] Повторим, что это лишь *имитация* режима Server Core. Для более полной достоверности попробуйте теперь совершенно не пользоваться оснастками (*.msc), панелями управления (*.cpl) и программой Windows Explorer (Проводник; explorer.exe).

2008[1] и выполняется инсталляция системы на свободный раздел диска ("чистая" установка). Нужно отметить, что процесс установки системы стал значительно проще, и не требуется периодически отвечать на вопросы, возникающие у системы, — достаточно запустить инсталляцию и вернуться к компьютеру через некоторое время для конфигурирования уже установленной системы.

Как можно будет увидеть, некоторые этапы, существовавшие в предыдущих версиях Windows, отсутствуют и изначально параметры (например, сетевые установки и принадлежность к определенной рабочей группе) выбираются по умолчанию; затем их можно поменять с панели управления или из окна новой специальной утилиты *Initial Configuration Tasks* (Задачи начальной настройки; oobe.exe — *см. далее*).

Рис. 1.6. Окно выбора региональных стандартов

[1] Системы Windows Vista и Windows Server 2008 распространяются только на DVD-дисках.

Последовательность этапов установки системы выглядит следующим образом.

1. Чтобы начать установку Windows Server 2008, необходимо загрузиться с дистрибутивного компакт-диска. Устанавливается ядро системы и появляется окно выбора региональных стандартов (рис. 1.6): необходимо указать формат представления дат и времени, а также раскладку клавиатуры. Для локализованной версии автоматически устанавливается русский язык (помимо стандартного английского, который присутствует всегда). При выборе русской раскладки клавиатуры имя компьютера, первого пользователя и его пароль будут по умолчанию вводиться по-русски; в окне регистрации в системе (на экране приветствия, Welcome Screen — см. рис. 2.10) также будет выбран русский язык. Если указать раскладку US (США), то по умолчанию задается английский язык. Можно оставить параметры, предлагаемые по умолчанию, и нажать кнопку **Next** (Далее). (В любом случае язык ввода на экране приветствия можно потом изменить или добавить кнопку переключения языков — см. рис. 2.11.)

Рис. 1.7. Первое окно программы установки Windows Server 2008

2. В первом окне программы установки Windows (рис. 1.7) ссылка **What to know before installing Windows** (Что следует знать перед выполнением установки Windows) позволяет увидеть файл справки, в котором перечислены требования и рекомендации для выполнения операции. Ссылка **Repair your computer** (Восстановление системы) позволяет перейти в меню функций восстановления системы (мы рассмотрим их в *главе 15*). Для запуска инсталляции нажмите кнопку **Install now** (Установить).

Рис. 1.8. Ввод серийного номера

3. Введите серийный номер версии Windows Server 2008 (рис. 1.8). В зависимости от указанного номера программа установки сама определяет *редакцию* инсталлируемой системы (после чего выполняется переход к этапу подтверждения лицензионного соглашения). Обратите внимание на то, что в этом окне установлен флажок активации (**Automatically activate Windows when I'm online**) — активация системы произойдет автоматически в течение 3 дней при наличии подключения компьютера к Интернету.

Флажок можно снять, если активация будет выполняться по телефону или иным образом, а также, если серийный номер изначально вводиться не будет (в этом случае флажок ***обязательно*** нужно сбросить).

При установке систем Windows Server 2008 можно не вводить сразу серийный номер и выбрать для инсталляции *любую* из редакций, имеющихся на дистрибутивном диске. Этот режим удобен при работе с trial-версиями, которые можно скачать с веб-сайта Windows Vista. Система может функционировать без активации в течение 60[1] дней, после чего работа станет невозможной — потребуется активация с указанием серийного номера, либо систему придется переустанавливать с потерей всех настроек. Время "испытательного периода" для Windows Server 2008 можно продлевать с помощью сценария slmgr *(см. далее)*.

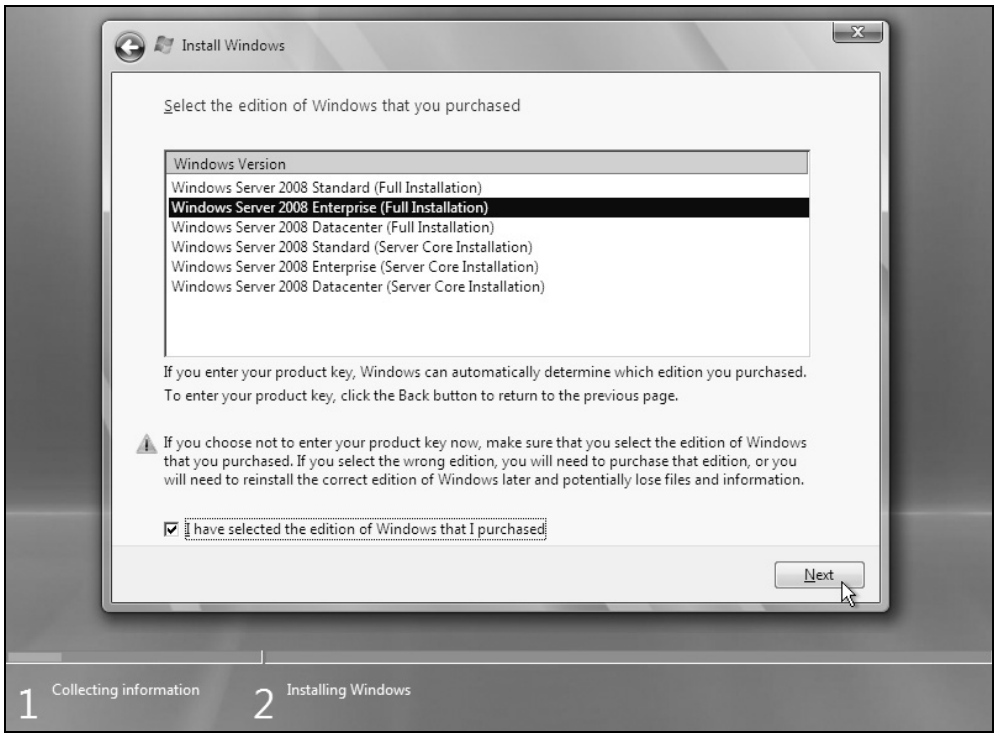


Рис. 1.9. Выбор версии устанавливаемой системы

[1] Для Windows Vista это время составляет 30 дней; любую версию Windows Vista с дистрибутивного диска также можно устанавливать без ключа.

Если поле серийного номера оставить пустым, то на следующем шаге появится запрос: "Do you want to enter your product key now?" (Ввести код продукта сейчас?). Нажав кнопку **No** (Нет), пользователь может выбрать для установки любую редакцию Windows Server 2008 (рис. 1.9); при этом обязательно нужно отметить флажок **I have selected the edition of Windows that I purchased** (Выбран приобретенный выпуск Windows).

4. Затем программа установки отображает на экране лицензионное соглашение (License Agreement), которое следует принять. В случае несогласия с условиями лицензионного соглашения пользователь должен отказаться от установки, и программа установки прервет свою работу.

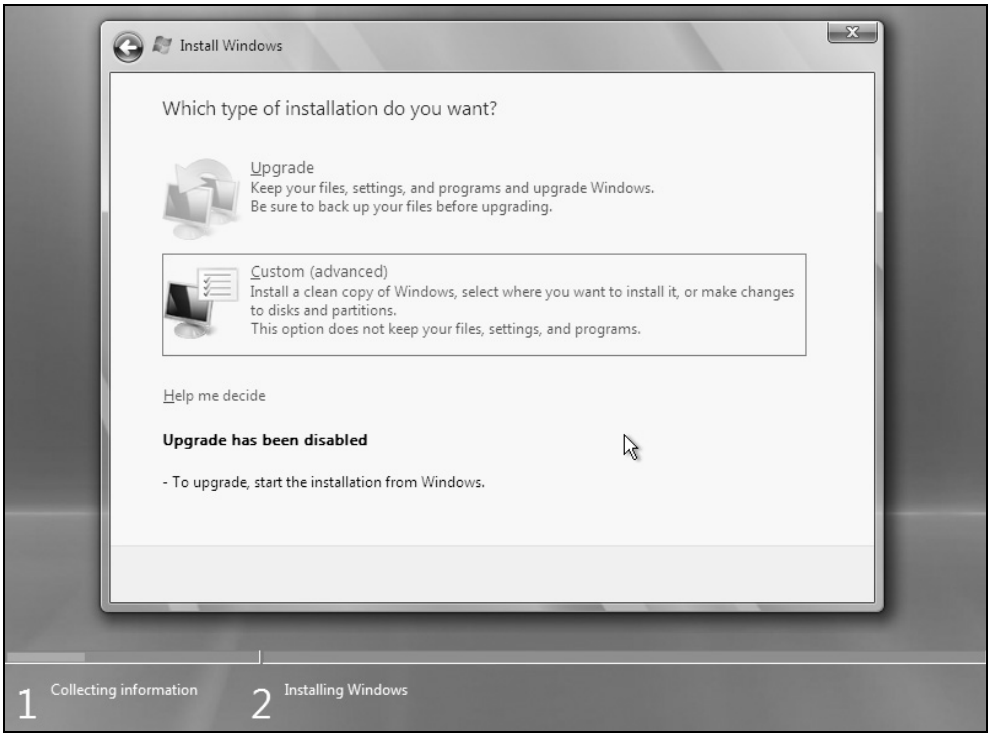


Рис. 1.10. Обновление невозможно, доступна лишь опция чистой установки системы

5. Далее предлагается выбрать способ установки системы: обновление (upgrade) или "чистая" (custom) установка (рис. 1.10). На этом шаге выбора фактически нет, поскольку для обновления уже инсталлированной сис-

темы программу установки нужно запускать *непосредственно из* этой системы *(см. далее)*. Для продолжения инсталляции выберите опцию **Custom (advanced)** (Полная установка (дополнительные параметры)).

6. На следующем шаге программа установки отображает имеющийся в системе диск (диски) или список разделов, уже существующих на жестком диске. Можно выбрать раздел для инсталляции из числа уже существующих, удалить один из существующих разделов, чтобы создать новые разделы на основе освободившегося пространства, или (при наличии достаточного объема свободного пространства, не принадлежащего ни одному разделу) создать новый раздел. Если нужны какие-то манипуляции с разделами (создание и форматирование раздела и т. п.), то щелкните по ссылке **Drive options (advanced)** (Настройка диска) — в этом случае в окне появятся дополнительные команды (см. рис. 1.11). *Вновь созданный* для установки раздел обязательно форматируется, при этом возможность выбора типа файловой системы отсутствует.

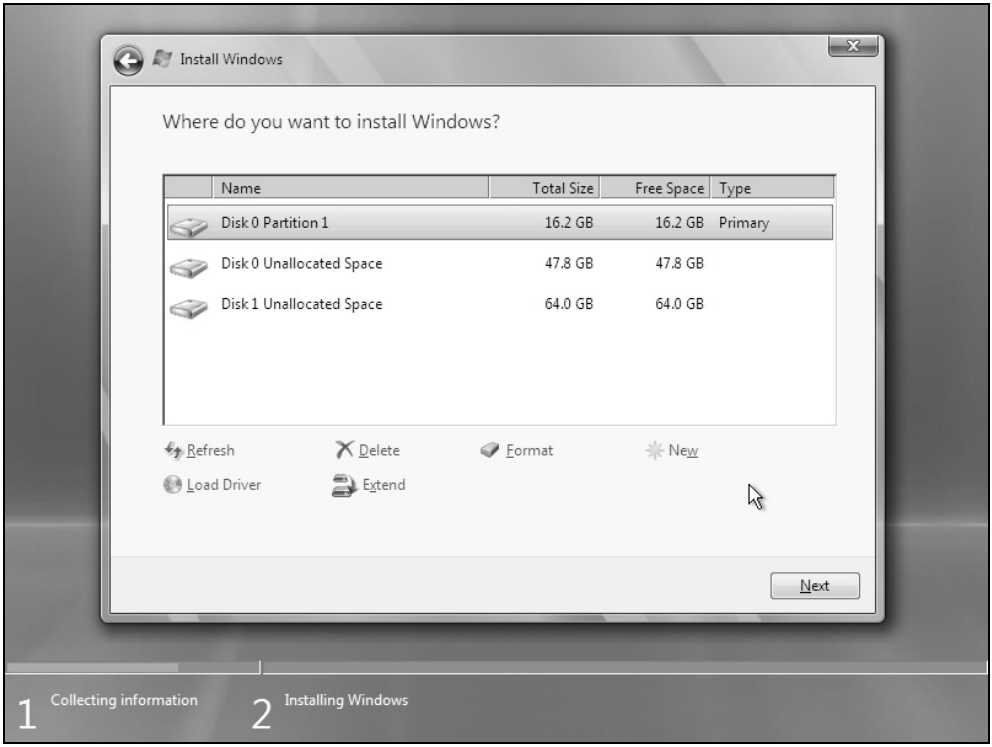


Рис. 1.11. Выбор раздела для установки

Внимание!

Программа установки Windows Server 2008 создает только основные разделы. Если требуется сложная конфигурация со множеством логических дисков (разделов), то лучше создавать ее перед установкой системы — *см. выше разд. "Конфигурирование разделов на жестком диске".*

Рис. 1.12. Выполнение инсталляционных процедур

На рис. 1.11 в качестве примера показан случай, когда раздел для установки системы уже подготовлен, при этом он занимает не весь диск (что вовсе не является обязательным или рекомендуемым вариантом — раздел может быть единственным и занимать все свободное пространство на физическом диске). Кнопка **Next** (Далее) станет активной, только когда имеется и *выбран* раздел, пригодный для установки системы (наличие необходимого свободного пространства определяется автоматически).

7. Теперь в течение 15—20 минут[1] компьютер не требует никакого внимания, поскольку все дальнейшие действия выполняются в автоматическом режиме. На экране отображается процесс выполнения инсталляционных процедур (рис. 1.12), во время которых компьютер может несколько раз перезагружаться. Два самых длительных по времени этапа — это извлечение файлов (до 10 минут) и установка компонентов (около 5 минут).

По завершении инсталляции системы программа установки в последний раз перезагружает компьютер, после чего нужно выполнить вход в систему и конфигурирование рабочей среды сервера *(см. далее)*.

Обновление систем Windows Server 2003

Список систем, для которых возможно обновление до Windows Server 2008, относительно невелик — в нем присутствуют только системы Windows Server 2003 и старше (разумеется, исключая Windows Vista). Ниже перечислены поддерживаемые операционные системы и указаны редакции Windows Server 2008, до которых их можно обновить:

- **Windows Server 2003 Standard Edition** (с пакетами обновлений Service Pack 1 или Service Pack 2) — Windows Server 2008 Standard, Windows Server 2008 Enterprise;
- **Windows Server 2003 R2 Standard Edition** — Windows Server 2008 Standard, Windows Server 2008 Enterprise;
- **Windows Server 2003 Enterprise Edition** (SP1 или SP2) — Windows Server 2008 Enterprise, Windows Server 2008 Datacenter;
- **Windows Server 2003 R2 Enterprise Edition** — Windows Server 2008 Enterprise, Windows Server 2008 Datacenter;
- **Windows Server 2003 Datacenter Edition** (SP1 или SP2) — Windows Server 2008 Datacenter;
- **Windows Server 2003 R2 Datacenter Edition** — Windows Server 2008 Datacenter.

Таким образом, "минимальной" версией Windows, для которой поддерживаются обновления, является Windows Server 2003 SP1.

---

[1] Временны́е оценки длительности операций довольно приблизительны и сделаны для компьютера средней производительности (с точки зрения Windows Server 2008).

Возможно обновление некоторых редакций Windows Server 2008 до более старших версий:

- **Windows Server 2008 Standard** — Windows Server 2008 Enterprise;
- **Windows Server 2008 Enterprise** — Windows Server 2008 Datacenter.

При всех вариантах обновления систем необходимо, чтобы совпадали языки установленной системы и новой системы (т. е. нельзя, к примеру, русскую версию Windows 2003 обновить до английской Windows Server 2008).

Невозможно обновление 32-разрядных версий системы до 64-разрядных или наоборот. Нельзя также делать обновления до Windows Server 2008 в режиме Server Core. Не поддерживается обновление для систем Windows Server 2003 на платформе Itanium и версии Windows Server 2003 Web Edition.

В процессе обновления сохраняются многие роли сервера — данные и конфигурация соответствующих служб переносятся в новую систему. Некоторые роли переносятся лучше и не требуют дополнительных операций, некоторые службы требуют повторного конфигурирования. В любом случае перед выполнением обновления рекомендуется выполнить сохранение всей информации и параметров, а после него следует проверить все настройки служб.

Выполнение процедуры обновления

Обновление уже установленных систем имеет некоторые особенности. Чтобы начать эту операцию, необходимо загрузить обновляемую операционную систему, вставить дистрибутивный диск Windows Server 2008 и запустить программу установки.

Нажав кнопку **Install now** (Установить) в первом окне программы установки (см. рис. 1.7), можно начать процедуру обновления имеющейся операционной системы. Программа предложит выполнить подключение к Интернету и загрузить последние обновления, необходимые для выполнения операции (рис. 1.13). Лучше разрешить эту возможность; однако в этом случае компьютер должен оставаться подключенным к Интернету в течение всего процесса обновления системы, который, в отличие от чистой установки, длится около часа и более (в зависимости от наличия дополнительных серверных служб). После загрузки обновлений программа установки будет перезапущена.

Затем процедура установки Windows Server 2008 будет выполняться так же, как и при новой установке системы: потребуется серийный номер, подтверждение лицензионного соглашения и т. д. При возникновении проблем программа укажет причину невозможности обновления (например, может быть

недостаточно свободного места на диске или может не поддерживаться обновление имеющейся операционной системы до выбранной редакции Windows Server 2008). Если какие-то приложения не поддерживаются в Windows Server 2008, то рекомендуется их удалить перед обновлением системы. В противном случае возможна неработоспособность этих программ и потеря их параметров (настроек). Если все нормально, то появится окно, в котором можно выбрать тип установки (рис. 1.14): теперь помимо полной установки, возможно обновление системы (сравните с рис. 1.10).

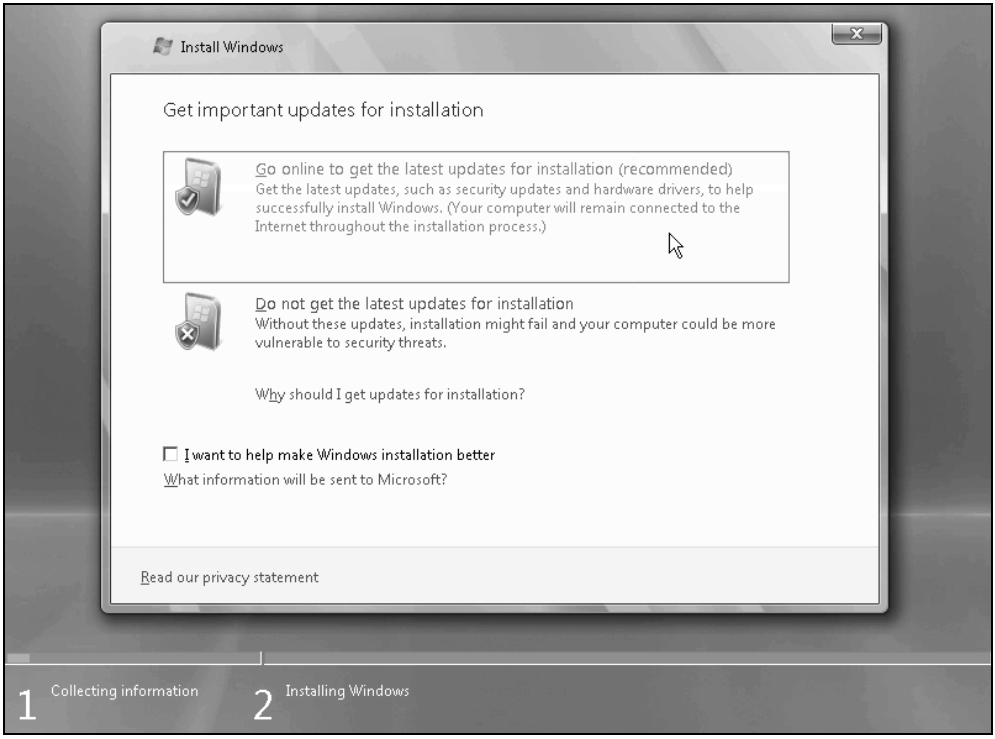


Рис. 1.13. Запрос на получение обновленных файлов для установки системы

При выполнении обновления программа установки может сообщить о наличии потенциальных проблем, которые не будут препятствовать операции. После этого установка пойдет обычным образом — начнется копирование и извлечение файлов, установка компонентов и т. д. (см. рис. 1.12). Напомним, что обновление длится существенно дольше (в несколько раз), чем обычная установка новой системы.

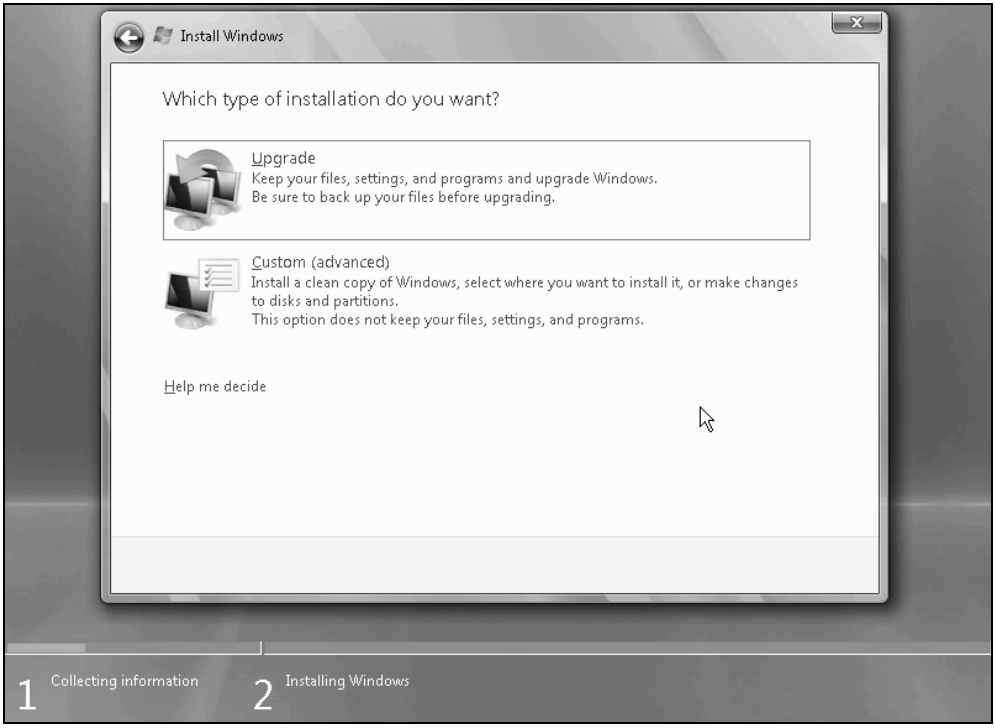


Рис. 1.14. Выбор типа установки в том случае, когда возможно обновление

Примечание

Особенности обновления контроллеров доменов Active Directory будут рассмотрены в *главе 12*, посвященной службам каталога.

Когда операция закончится, администратор может войти в систему с обычным именем и паролем. Начальное конфигурирование после обновления системы не требуется, рекомендуется лишь проверить параметры служб, обеспечивающих выполнение дополнительных ролей сервера.

Постинсталляционные задачи

После полной установки системы необходимо выполнить некоторые обязательные и рекомендуемые операции по настройке системных параметров. Только после этого можно начинать полноценную работу на сервере.

Установка пароля

После загрузки только что установленной системы перед первым входом в систему требуется смена пароля учетной записи Administrator (Администратор) (рис. 1.15) (это верно, поскольку никакого пароля в процессе установки не задавалось). Необходимо установить и подтвердить пароль; можно сразу создать дискету восстановления пароля *(см. разд. "Сохранение и восстановление паролей пользователей" главы 4)*. После появления сообщения об успешном изменении пароля можно входить в систему.

Рис. 1.15. Сообщение о необходимости смены пароля администратора перед первым входом в систему

Нужно помнить о том, что по умолчанию требуется сложный пароль, поскольку установлена политика **Password must meet complexity requirements** (Пароль должен отвечать требованиям сложности). Такой пароль включает, например, строчные и заглавные буквы, а также цифры или служебные символы.

Начальное конфигурирование системы

При первом входе в систему администратор видит окно программы *Initial Configuration Tasks* (Задачи начальной настройки) (рис. 1.16; на рисунке показаны исходные значения параметров, до внесения каких-либо изменений). Здесь собраны все основные параметры системы, и можно выполнить их настройку, щелкнув по соответствующей ссылке. Это удобно тем, что не нужно искать различные средства конфигурирования и сложнее забыть о необходимости выбора какого-то параметра.

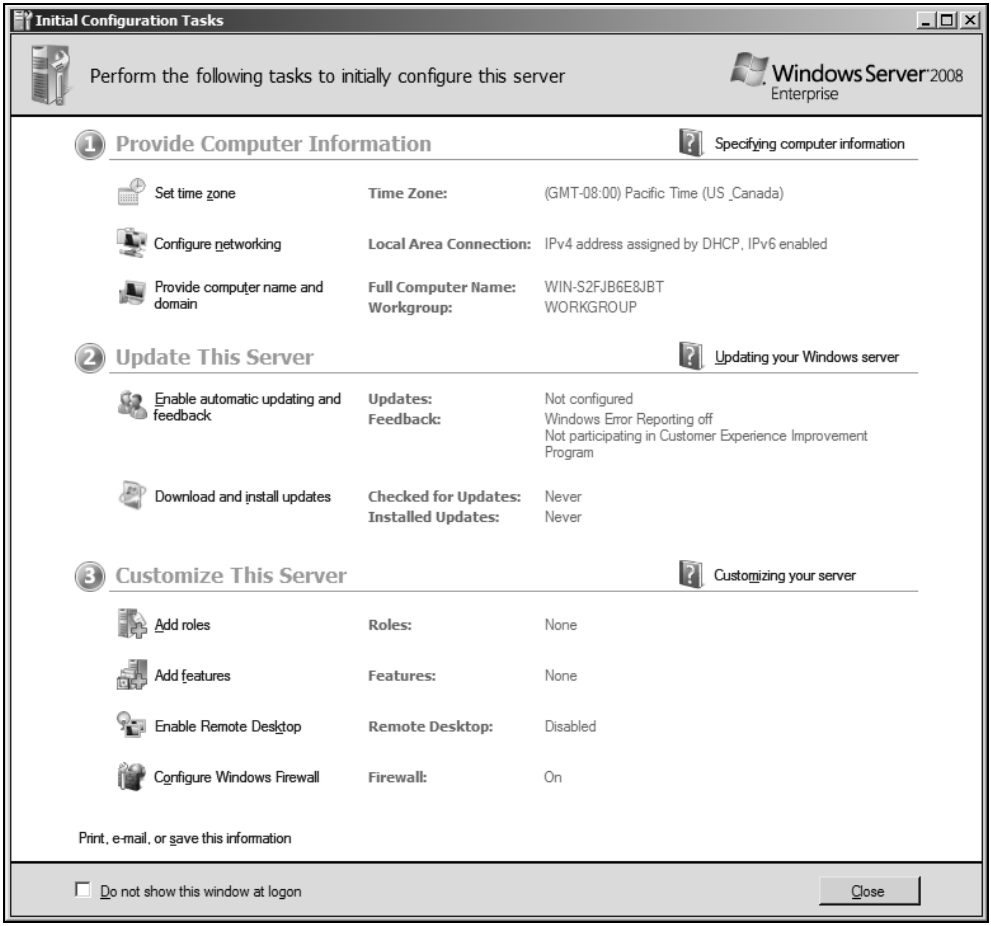


Рис. 1.16. Программа начальной настройки позволяет установить основные рабочие параметры системы

Самые важные задачи составляют первую группу — необходимо установить следующие параметры:

- часовой пояс;
- параметры сети (если они не получаются от DHCP-сервера);
- имя компьютера и его принадлежность к рабочей группе или домену.

Затем рекомендуется выбрать параметры для службы обновлений Windows Update *(см. также далее разд. "Выбор параметров автоматического обновления Windows")*.

Сразу же можно добавить роли и компоненты сервера; можно включить удаленный доступ к рабочему столу.

Когда все операции будут выполнены, можно установить флажок **Do not show this windows at logon** (Не показывать это окно при входе в систему) и закрыть окно. В противном случае оно будет появляться при каждом входе в систему и напоминать о необходимости выполнения настроек.

Примечание

Окончательно закрытое окно программы Initial Configuration Tasks (Задачи начальной настройки) можно вызвать снова при помощи команды `oobe`, введенной в меню **Start** (Пуск).

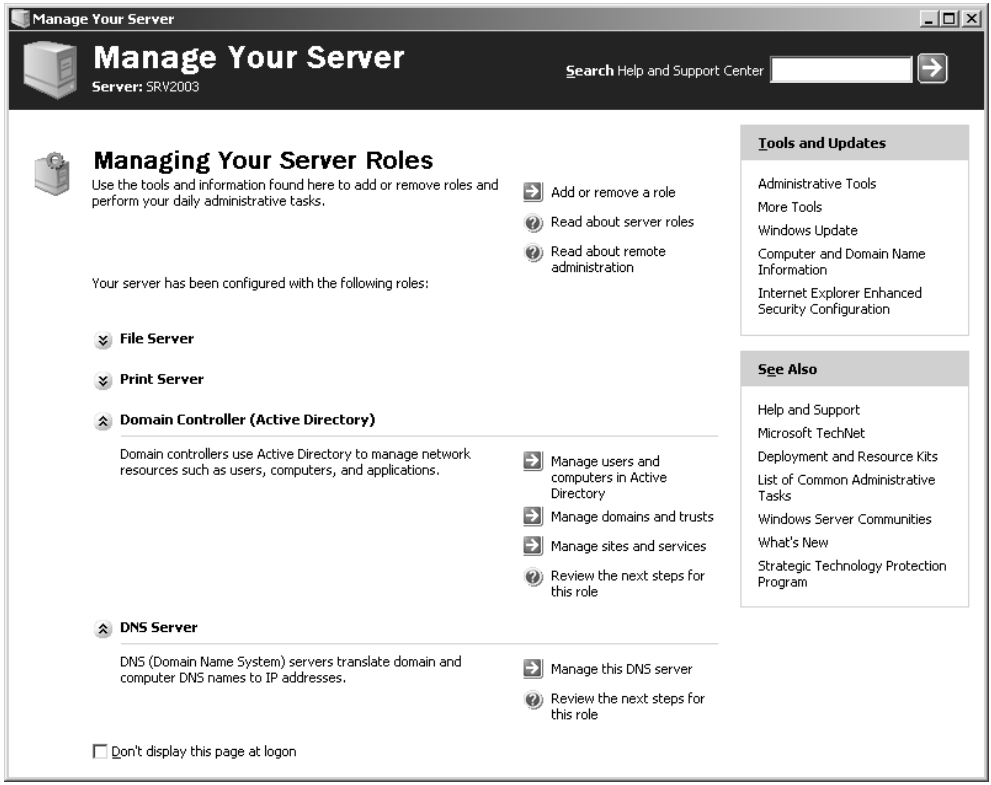


Рис. 1.17. Окно программы Manage Your Server в системах Windows Server 2003

После того как при первом входе в систему будет закрыто окно задач начальной настройки, на экране появится окно главного средства администрирования — окно оснастки **Server Manager** (Диспетчер сервера) (см. рис. 1.18).

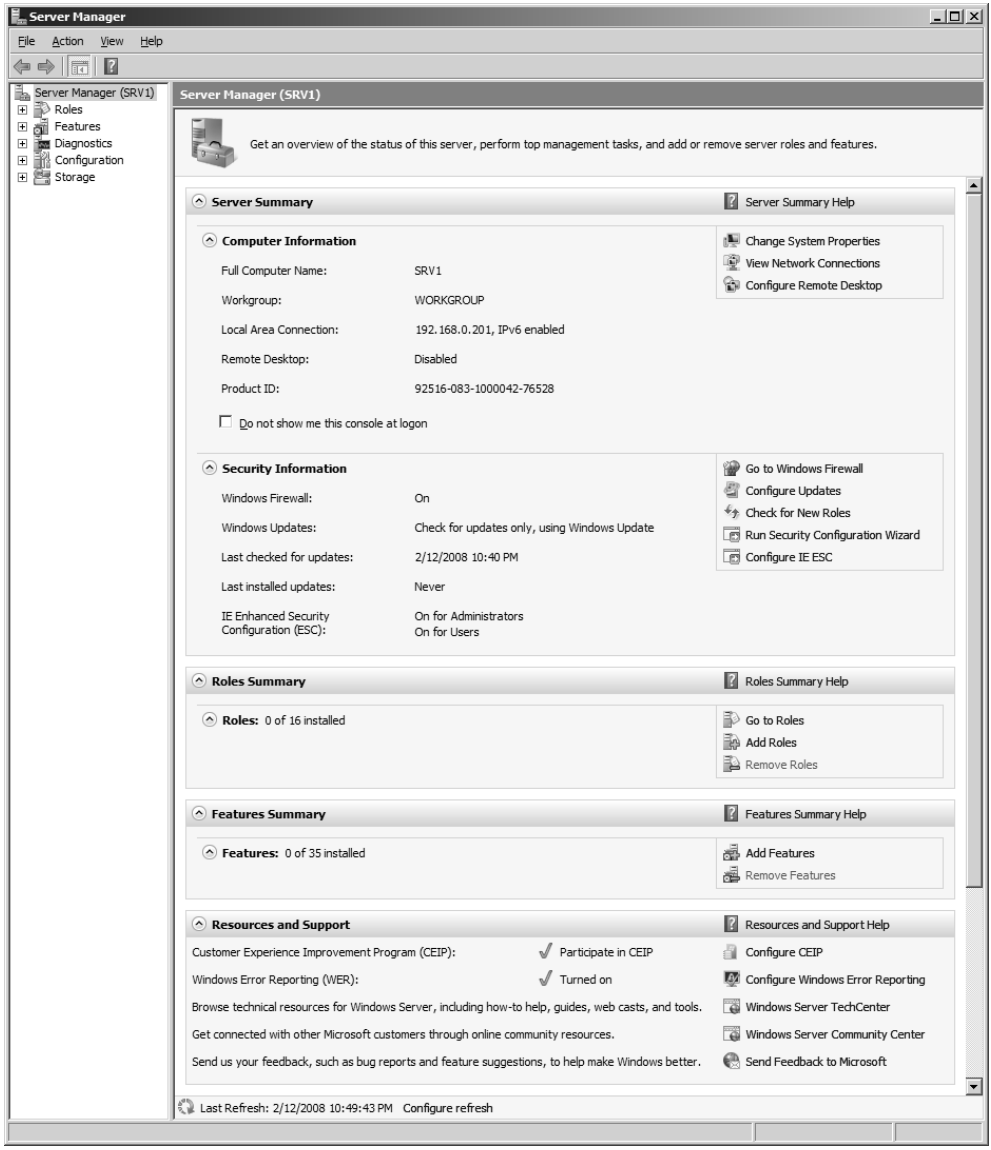


Рис. 1.18. Начальный вид оснастки **Server Manager**

Похожее средство под названием *Manage Your Server* имеется в системах Windows Server 2003 (рис. 1.17). С его помощью можно устанавливать роли сервера (устанавливая соответствующие компоненты) и вызывать административные оснастки, управляющие этими ролями. Эта программа удобна для централизованного управления сервером, но скорее факультативна и не обеспечивает доступ ко всем основным средствам администрирования.

Оснастка **Server Manager** (Диспетчер сервера) (рис. 1.18) в системах Windows Server 2008 имеет значительно бóльшие возможности и позволяет в своем окне управлять практически всеми ролями сервера, службами и компонентами. В других главах эта оснастка будет часто упоминаться, будет рассказано о способах ее использования.

При первом запуске в окне оснастки **Server Manager** (Диспетчер сервера) можно видеть общую информацию о компьютере (включая параметры, заданные с помощью программы Initial Configuration Tasks (Задачи начальной настройки) — например, имя компьютер, рабочую группу, IP-адрес и т. д.) и параметры безопасности (состояние брандмауэра и службы обновления). Оснастка позволяет устанавливать роли сервера, службы и компоненты, более того — в Windows Server 2008 она является ***единственным средством*** (если не считать утилиты ServerManagerCmd.exe), позволяющим устанавливать дополнительные компоненты Windows или серверные службы.

Подробно процедура установки ролей и компонентов сервера с использованием оснастки **Server Manager** (Диспетчер сервера) рассматривается в *главе 3*.

Окно оснастки **Server Manager** (Диспетчер сервера) будет появляться на экране до тех пор, пока не будет установлен флажок **Do not show me this console at logon** (Не показывать эту консоль при входе в систему). Команда для запуска оснастки по умолчанию присутствует в меню **Start** (Пуск), а ее значок имеется на панели быстрого запуска. Также ее можно запустить непосредственно, введя в окне консоли или в меню **Start** (Пуск) строку `compmgmtlauncher`.

Выбор параметров автоматического обновления Windows

Функция автоматического обновления Windows Update (сервис wuauserv; исполняемый файл утилиты настройки — wuapp.exe) представляет собой системный сервис, который позволяет пользователям, обладающим административными правами в системе, выполнять автоматическую загрузку и установку обновлений Windows.

Если функция автоматического обновления не блокирована, то сервис стартует автоматически и выполняет сканирование системы, чтобы определить, имеются ли на сайте Windows Update обновления, доступные для загрузки. По умолчанию загрузка обновлений осуществляется в фоновом режиме, и по ее завершении установка может выполняться автоматически или с уведомлением пользователя, который имеет возможность отложить этот процесс, поскольку некоторые обновления могут потребовать перезагрузки компьютера. Сервис автоматического обновления выполняет все необходимые проверки, налагаемые системой безопасности.

В доменах опции автоматического обновления можно устанавливать с помощью групповых политик — в соответствии с корпоративными требованиями и в зависимости от наличия или отсутствия программных продуктов типа *Microsoft Windows Server Update Services* (WSUS) ((см. узел **Computer Configuration** | **Administrative Templates** | **Windows Components** | **Windows Update** (Конфигурация компьютера | Административные шаблоны | Компоненты Windows | Центр обновления Windows)).

Очень важно, чтобы обновления устанавливались в системе оперативно, поэтому выбор параметров автоматического обновления является важной задачей после установки системы (впоследствии эти параметры можно менять в любой момент). Для изменения параметров требуются следующие операции:

1. Откройте окно *Центра обновления Windows* (Windows Update) (рис. 1.19), выполнив одноименную команду в меню **Start** (Пуск) или выбрав соответствующую задачу на панели управления (также можно непосредственно ввести имя программы `wuapp`). В этом окне можно видеть наличие новых обновлений, время последней операции поиска обновлений и параметры сервиса обновлений, которые можно выбрать, щелкнув по ссылке **Change settings** (Изменить параметры). Также указывается, для каких программ проверяются обновления — только для Windows или для Windows и других программных продуктов из Microsoft Update.
2. В окне параметров сервиса автоматического обновления (рис. 1.20) имеются следующие опции (в примере показаны рекомендованные значения; в реальных условиях предпочтения могут быть совсем иными):
   - рекомендуемая опция — **Install updates automatically** (Устанавливать обновления автоматически). При этом обновления загружаются в фоновом режиме и устанавливаются в указанное время (желательно, чтобы это не мешало работе пользователей и служб, поскольку иногда требуется перезагрузка);

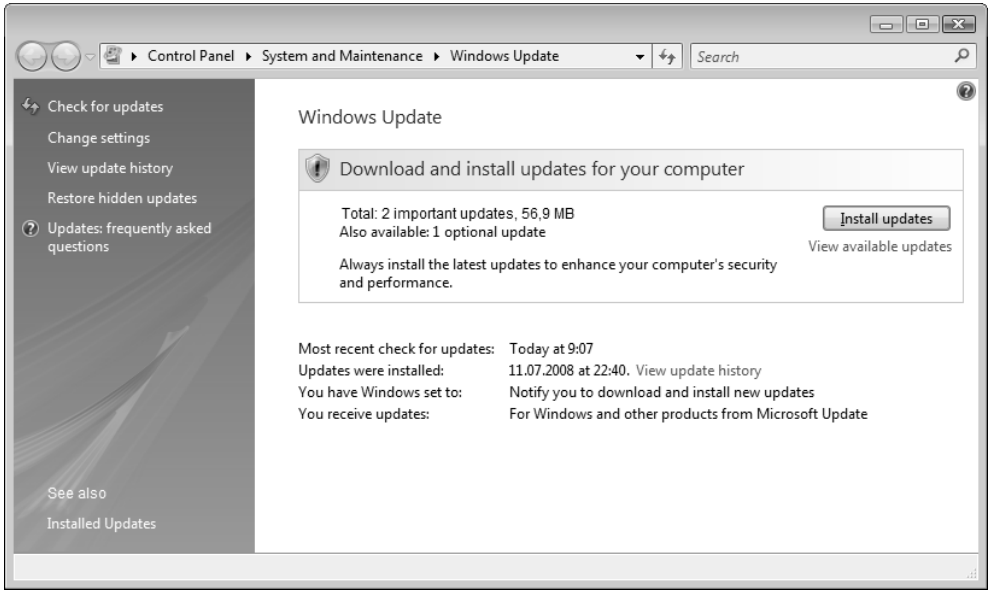


Рис. 1.19. Главное окно Центра обновлений Windows

- при выборе опции **Download updates but let me choose whether to install them** (Загружать обновления, но предоставить мне выбрать, надо ли устанавливать их) администратор сначала уведомляется о готовности загруженных обновлений к инсталляции (эта опция может быть оптимальной для автономной системы при наличии быстрого доступа к Интернету);
- если администратор хочет сначала увидеть список обновлений, а только потом загружать и устанавливать их, то следует выбрать опцию **Check for updates but let me choose whether to download and install them** (Проверять наличие обновлений, но предоставить мне выбрать, надо ли загружать и устанавливать их). Эта опция, возможно, самая оптимальная для автономной системы, поскольку обеспечивает оперативность информирования администратора и полный контроль за скачиванием и установкой обновлений;
- последняя опция — **Never check for updates** (Не проверять наличие обновлений) — позволяет вообще отключить автоматическое обновление и выполнять все операции по обновлению системы вручную, с помощью ссылки **Check for updates** (Проверка обновлений) в главном окне Центра обновлений Windows.

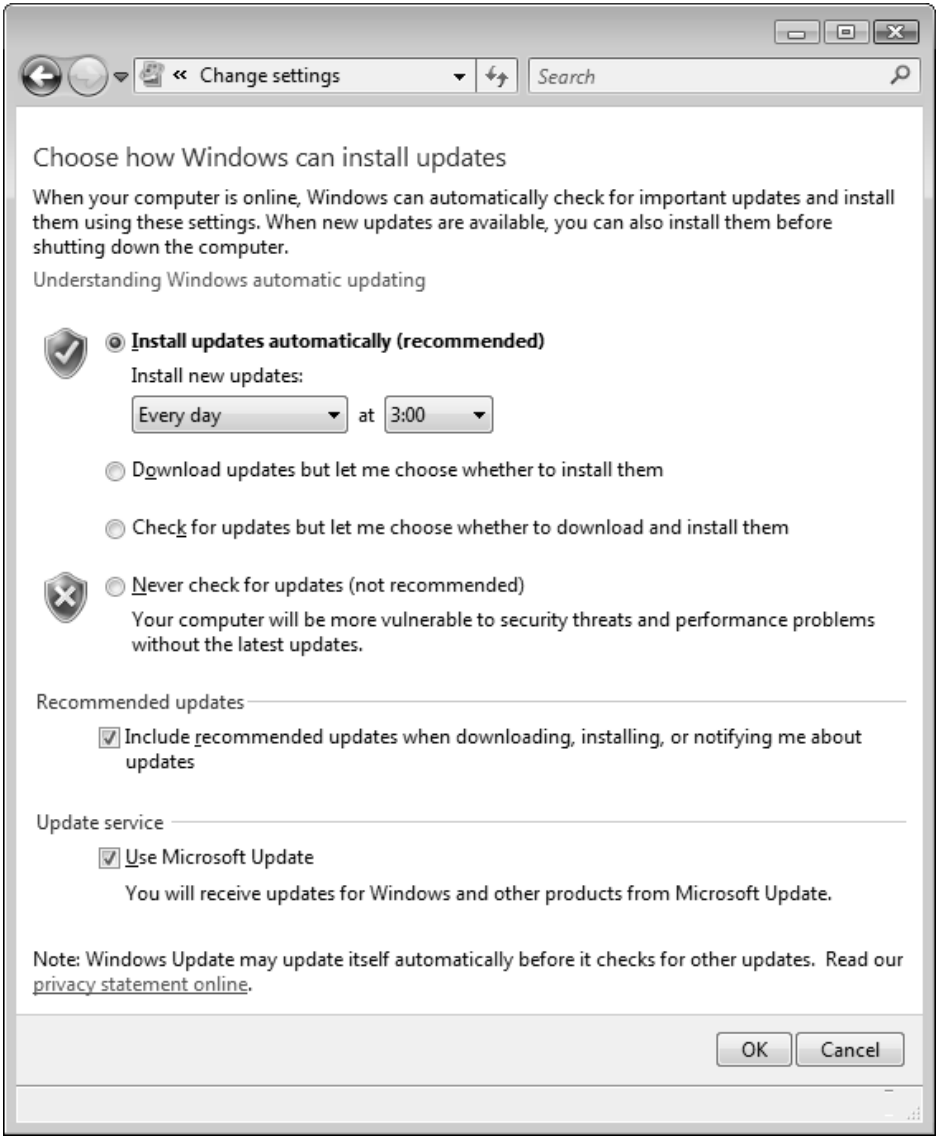


Рис. 1.20. Окно параметров автоматического обновления системы

Также имеются дополнительные параметры:

- флажок **Install recommended updates…** (Включать рекомендуемые обновления…) указывает на необходимость проверки наличия некритических обновлений;

- флажок **Use Microsoft Update** (Использовать Microsoft Update) указывает на необходимость проверки других программных продуктов Microsoft, помимо Windows. Этот флажок появится, если только в главном окне центра обновлений щелкнуть по ссылке **Get updates for more products** (Получить обновления для других продуктов) и на открывшейся в окне браузера веб-странице Microsoft Update согласиться с условиями предоставления услуг (при этом будет выполнена установка компонента Microsoft Update). После этого указанная ссылка больше отображаться не будет.

3. Выберите параметры, наиболее подходящие для конкретных условий работы, и закройте окно, нажав кнопку **ОК**.

> ***Внимание!***
>
> По умолчанию в системах Windows Server 2008 проверка наличия обязательных и не критических обновлений не задана, поскольку подразумевается, что администратор должен самостоятельно выбрать параметры обновления для каждой конкретной инсталляции сервера.

Активация системы

Если при установке системы была разрешена автоматическая активация, то система пытается сразу же выполнить ее через Интернет.

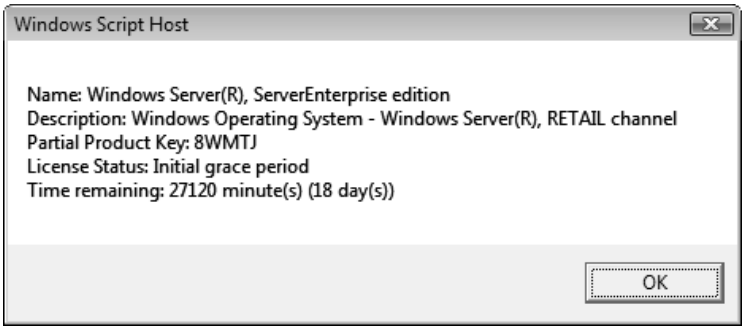


Рис. 1.21. Сообщение о лицензионном статусе системы

Если флажок разрешения активации был сброшен (например, при использовании пробной (trial) версии, скачанной с веб-сайта Microsoft), то в течение

60 дней периодически будет появляться сообщение, напоминающее о необходимости активации. Нужно помнить о том, что для выполнения активации потребуется серийный номер, если он не вводился при установке системы!

Время, остающееся до момента обязательной активации, указывается в окне свойств системы (см. рис. 3.7), либо его можно получить от службы лицензирования, запустив в окне командной строки сценарий `slmgr.vbs` с параметром `-dli` или `-dlv`. Пример результата показан на рис. 1.21.

Период работы пробной версии можно продлить на 60 дней с помощью команды `slmgr -rearm` (после ее выполнения требуется перезагрузка). Эту операцию можно повторять два раза (продлевая общее время работы до 180 дней в сумме).

Автоматическая инсталляция системы

Главным средством для развертывания систем Windows Vista и Windows Server 2008 в крупных сетях является пакет *Windows Automated Installation Kit* (Windows AIK или WAIK; Пакет автоматической установки Windows). Это весьма сложный продукт, и мы ограничимся только упоминанием основных его возможностей.

Пакет Windows AIK можно свободно скачать с веб-сайта Microsoft (ссылку легко найти, выполнив поиск строки *WAIK* на главной странице Центра загрузки Microsoft — см. ссылки в *приложении*). Пакет хранится в виде образа (IMG) диска, его размер для английской версии составляет 1375,9 Мбайт. После загрузки необходимо образ записать на DVD-болванку и запустить с нее программу установки — на рис. 1.22 показано главное окно этой оболочки.

Для установки на компьютер основных средств пакета следует выбрать опцию **Windows AIK Setup**. По окончании инсталляции всех программ в меню **Start** (Пуск) появится группа **Microsoft Windows AIK**, содержащая ссылки на программы и документацию (рис. 1.23).

Основным средством подготовки *файлов ответов* (answer files) для автоматической установки (unattended setup) является программа *Windows System Image Manager* (рис. 1.24).

Файл ответов, обычно называемый Unattend.xml, содержит параметры и значения, необходимые для программы установки Windows (Windows Setup). Для Windows Server 2008 этот файл имеет формат XML.

Рис. 1.22. Главное окно программы установки средств Windows Automated Installation Kit

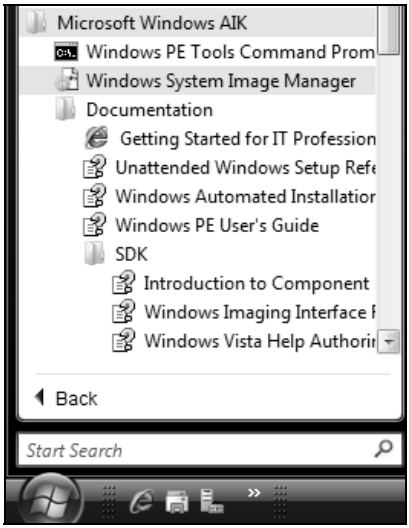


Рис. 1.23. Средства пакета Windows AIK, устанавленные на компьютере

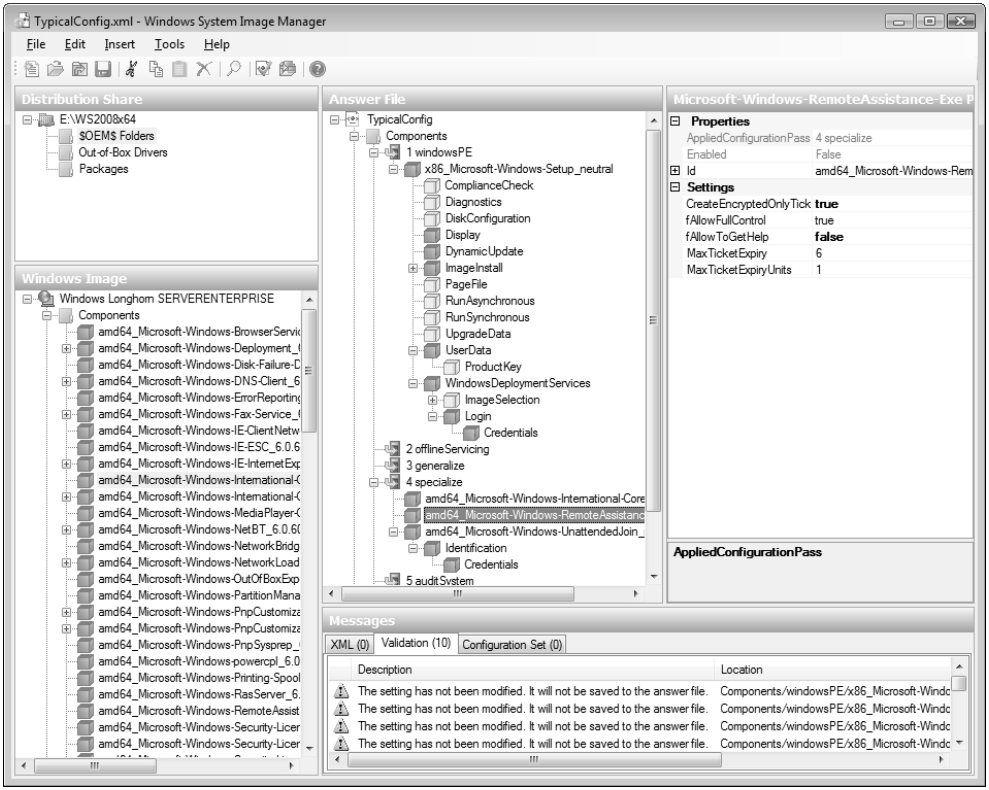


Рис. 1.24. Главное окно программы Windows System Image Manager

В папке support\samples на диске Windows AIK имеется файл headlessunattend.xml, который можно использовать в качестве примера файла ответов. Его можно просмотреть в любом текстовом редакторе или открыть в программе Windows System Image Manager.

Подробное описание всех технологий, используемых для установки Windows Server 2008, утилит и параметров служебных файлов (включая файлы ответов), содержится в весьма информативной и объемной сопроводительной документации к пакету Windows AIK. Для подготовки автоматической инсталляции Windows Server 2008 требуется серьезное предварительное знакомство с используемой терминологией (где очень много новых понятий), технологиями и программными средствами.

Службы развертывания Windows (WDS)

Службы *Windows Deployment Services* (WDS; Службы развертывания Windows) пришли на смену службам удаленной установки (Remote Installation Services, RIS), входящим в состав Windows Server 2003. Они предназначены для централизованной установки операционных систем на клиентских компьютерах, при этом на каждой подключаемой к сети рабочей станции помимо самой ОС может быть установлен стандартный набор компонентов и приложений. Автоматизация процесса установки предполагает сведение к минимуму участия пользователя и администратора.

Службы WDS на базе Windows Server 2008 в первую очередь ориентированы на установку операционных систем Windows Vista и Windows Server 2008, хотя с их помощью можно устанавливать образы и других версий Windows.

Для функционирования служб WDS необходимо обязательное присутствие в сети трех компонентов:

- службы каталога Active Directory;
- сервера DNS;
- сервера DHCP.

Клиентские компьютеры должны поддерживать протокол *Preboot eXecution Environment* (PXE), обеспечивающий возможность загрузки с удаленного сервера, либо нужно использовать Windows Server 2008-версию среды *Windows Preinstallation Environment* (Windows PE; Среда предустановки Windows). Сервер, на котором устанавливаются службы WDS, должен быть членом домена.

Для передачи данных используется протокол *Trivial File Transfer Protocol*, TFTP (Простейший протокол передачи файлов). Протокол TFTP используется службами WDS как транспортный механизм, посредством которого клиенту передаются необходимые для инициации процесса удаленной установки файлы. При этом аутентификация не используется.

Для управления службами WDS и хранилищем образов используется оснастка **Windows Deployment Services** (Службы развертывания Windows; WdsMgmt.msc) (см. рис. 1.27).

Примечание

Службы WDS на базе Windows Server 2008 не используют *Single Instance Store*, SIS (Хранилище единственных копий) — средство для хранения образов установки, применяемое службами RIS.

Установка служб и конфигурирование WDS-сервера

Чтобы начать развертывание служб WDS, необходимо с помощью оснастки **Server Manager** (Диспетчер сервера) установить роль *Windows Deployment Services* (Службы развертывания Windows). В ее состав входят два компонента: *Deployment Server* (Сервер развертывания) и *Transport Server* (Транспортный сервер). Для базовых конфигураций требуются оба компонента.

При установке роли необходимо выполнить конфигурирование WDS-сервера. Для этого следует запустить оснастку **Windows Deployment Services** (Службы развертывания Windows), выбрать новый сервер и выполнить команду **Configure Server** (Настроить сервер) из меню **Action** (Действие). (Для настройки WDS-сервера также можно использовать утилиту *WDSUtil.exe*.)

Рис. 1.25. Определение политики ответов на запросы клиентов

Процесс конфигурирования состоит из следующих этапов:

1. Нужно указать местоположение папки в разделе NTFS, где будут храниться образы систем, устанавливаемых с данного сервера. По умолчанию это папка C:\RemoteInstall.
2. Необходимо определить политику ответов сервера на запросы известных и неизвестных клиентов. (Для известных клиентов в каталоге Active Directory имеется заранее созданная учетная запись компьютера.) По умолчанию сервер вообще не отвечает на запросы клиентов (рис. 1.25). Эту политику можно потом поменять в окне свойств WDS-сервера на вкладке **PXE Response Settings** (Параметры PXE-ответа) (см. рис. 1.28).

Добавление образов

После нажатия кнопки **Finish** (Готово) в последнем окне мастера конфигурирования (см. рис. 1.25) выполняется настройка WDS-сервера, а затем мастер установки предлагает сразу же добавить в хранилище образы системы. Эта процедура выглядит следующим образом:

1. Необходимо указать путь к файлам boot.wim и install.wim. В простейшем случае можно вставить в DVD-привод дистрибутивный диск и указать букву дисковода.
2. Следует дать имя новой группе образов (это образы одной операционной системы разных редакций). Указанное имя будет дано папке в хранилище, куда будут скопированы схожие образы.
3. Если все параметры указаны верно, мастер найдет образы в заданной папке, и затем необходимо указать, какие образы будут копироваться в хранилище (рис. 1.26).

После копирования информации из указанной папки имена загрузочного и установочных образов будут помещены в соответствующие папки в окне оснастки **Windows Deployment Services** (Службы развертывания Windows) (рис. 1.27). Для работы WDS-сервера необходимы, как минимум, один загрузочный образ и один установочный образ. Загрузочные образы соответствуют платформе — x86 и x64, и один образ используется для установки всех систем, работающих на данной платформе.

Загрузочный (boot.wim) или установочный (install.wim) образ можно добавить в хранилище в любой момент; для этого нужно выбрать соответствующую папку (**Boot Images** или **Install Images**) или группу образов и в

меню **Action** (Действие) выполнить команду **Add Boot Image** или **Add Install Image**.

В папке **Legacy Images** (Устаревшие образы) размещаются образы служб RIS, оставшиеся после обновления операционной системы Windows Server 2003, где были развернуты эти службы. Напрямую их использовать нельзя, а необходимо конвертировать с помощью специальной утилиты.

Службы WDS позволяют использовать заказные (custom) образы установки для любых версий Windows, включая Windows Vista и более ранние системы. Для этого с помощью утилиты *Sysprep.exe* (она имеется на любом компьютере с системой Windows Server 2008 в папке *%SystemRoot%*\System32\sysprep) необходимо подготовить эталонный компьютер, а затем снять с него образ операционной системы с помощью мастера *Image Capture Wizard*.

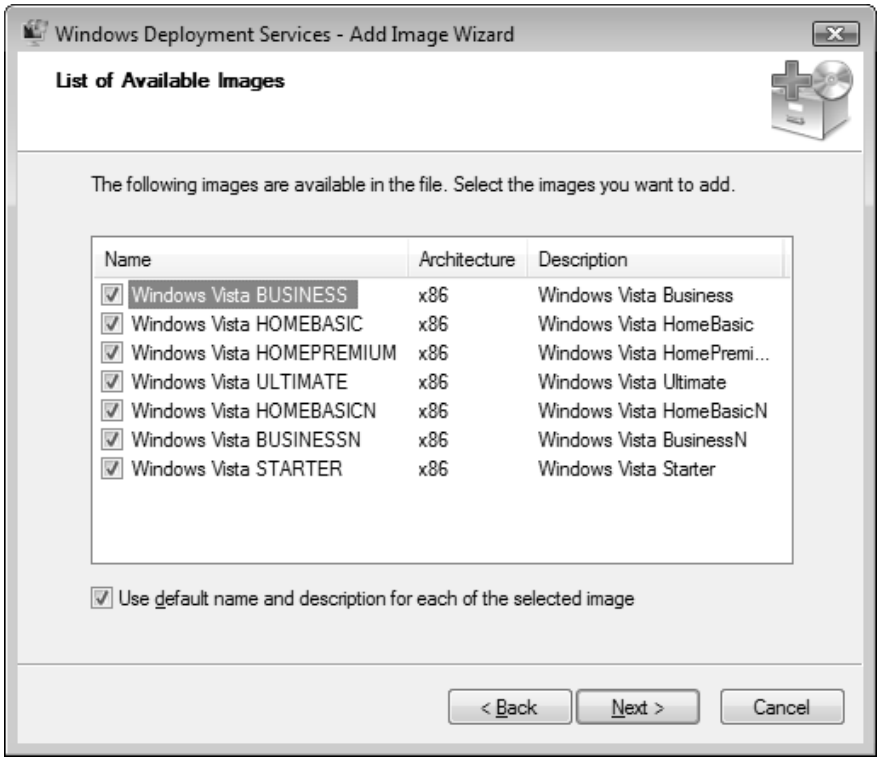


Рис. 1.26. Выбор образов, помещаемых в хранилище образов

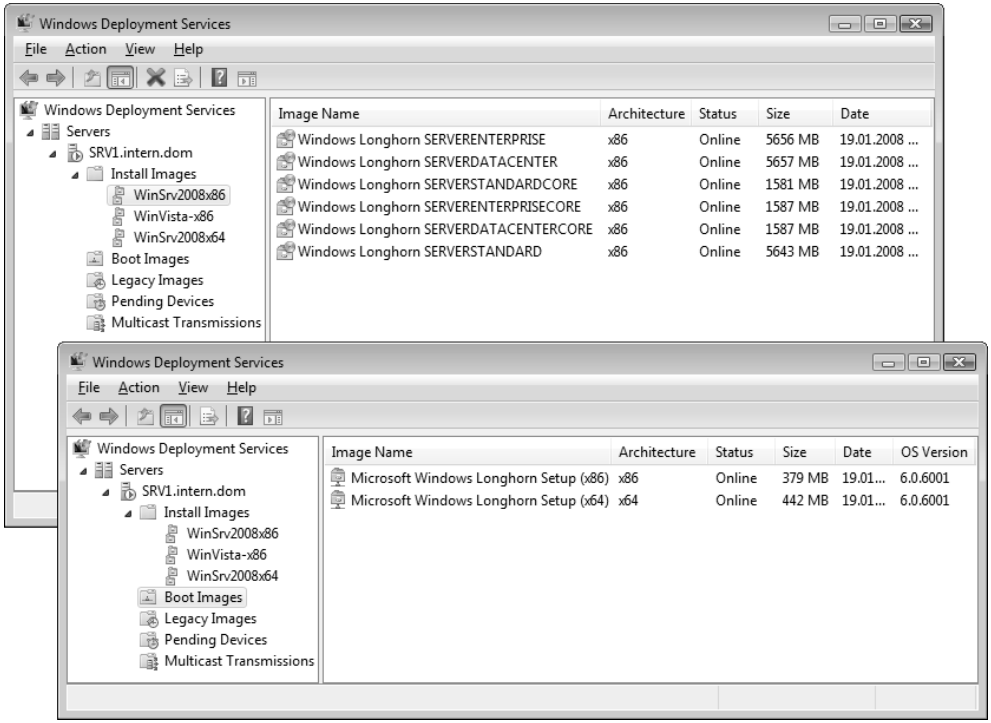


Рис. 1.27. Папки, содержащие загрузочные и установочные образы

Образы можно модифицировать (добавляя файлы, драйверы и другие компоненты) с помощью средств пакета Windows AIK.

Дополнительная настройка параметров WDS-сервера

Установленный и сконфигурированный WDS-сервер готов к работе и может использоваться для установки операционных систем на клиентских компьютерах. Однако некоторые параметры его работы могут меняться в процессе эксплуатации служб WDS (например, порядок обработки пользовательских запросов: будет ли WDS-сервер отвечать на запросы *всех* клиентов или только на запросы тех клиентов, с которыми в каталоге ассоциированы соответствующие объекты). Кроме того, с помощью групповых политик можно определить свои параметры удаленной установки для различных групп пользователей.

Если в окне оснастки **Windows Deployment Services** (Службы развертывания Windows) выбрать WDS-сервер и открыть окно его свойств, то на многочисленных вкладках можно выбирать параметры, определяющие работу сервера и функционирование служб WDS в целом.

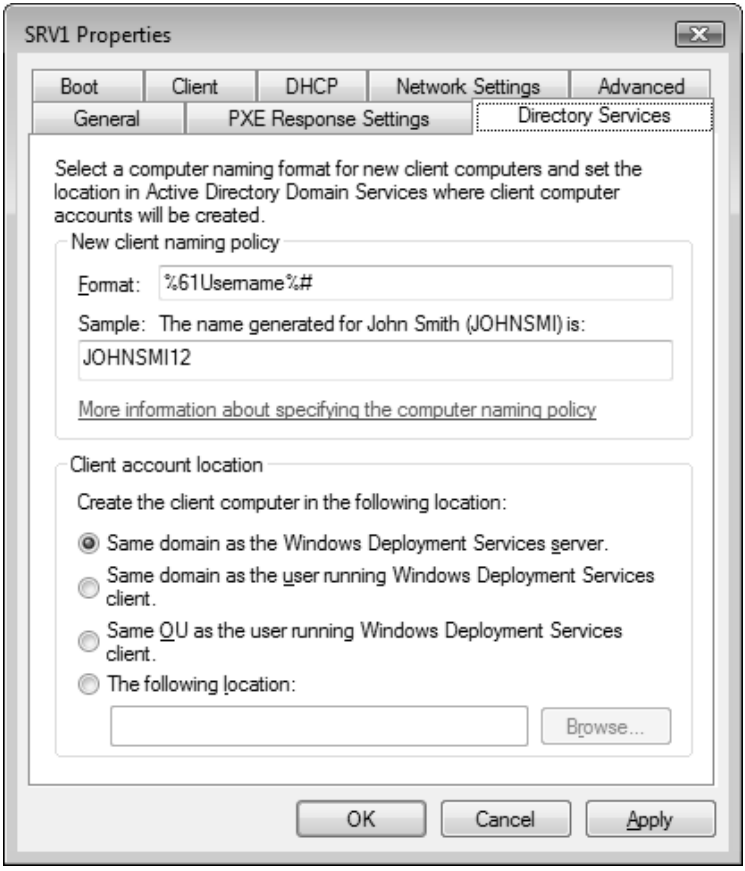


Рис. 1.28. Окно свойств WDS-сервера

Например, на вкладке **Directory Service** (Служба каталога) (рис. 1.28) задается порядок формирования имен для клиентских компьютеров, а также доменное местоположение учетных записей, создаваемых для этих компьютеров. На вкладке **PXE Response Settings** (Параметры PXE-ответа) определяется политика ответов сервера на запросы клиентов.

Установка устройств в работающей системе

Традиционная для систем Windows технология Plug and Play позволяет операционной системе распознавать изменения аппаратной конфигурации без вмешательства пользователя, устанавливать драйверы устройств и задавать их рабочие параметры. Обычно при этом не требуется перезагрузка компьютера. Обычно драйверы для всех устройств, имеющихся в компьютере, автоматически загружаются при установке системы, однако иногда требуется ручная их установка — если в системе отсутствуют нужные драйверы или если устройство подключается в процессе работы, уже после инсталляции операционной системы.

В системах Windows Server 2008 средства для работы с устройствами и способы установки драйверов практически не изменились по сравнению с предыдущими версиями Windows. Несколько отличается только пользовательский интерфейс операций, требующих выбора драйвера при оперативном подключении устройства.

Диспетчер устройств

Основным инструментом для конфигурирования аппаратных средства традиционно остается оснастка **Device Manager** (Диспетчер устройств, devmgmt.msc), которая преимущественно используется для проверки состояния аппаратных устройств (компонентов) и обновления (иногда установки) драйверов устройств, установленных на компьютере.

В окне оснастки (см. рис. 1.29) в виде дерева объектов отображаются все аппаратные устройства, установленные на компьютере. С ее помощью можно выполнить следующие задачи:

- определять правильность работы установленных устройств;
- изменять конфигурационные настройки оборудования;
- идентифицировать драйверы устройств, которые загружены для каждого устройства, и получить информацию о драйверах всех устройств;
- обновлять драйверы устройств;
- отключать и активизировать устройства;
- возвратиться к предыдущей версии драйвера устройства.

Для запуска диспетчера устройств можно воспользоваться панелью управления или же ссылкой **Device Manager** (Диспетчер устройств) в окне свойств системы *(см. главу 3)*. Другой путь — ввести строку `devmgmt.msc` в окне **Run** (Выполнить) или непосредственно в меню **Start** (Пуск). Оснастку можно добавить к пользовательской консоли MMC *(см. главу 3)*, в этом случае ее можно подключить и к удаленному компьютеру.

Примечание

Большинство всех функций оснастки **Device Manager** (Диспетчер устройств), касающихся управления устройствами, реализованы в утилите командной строки *Devcon.exe*, которая входит в состав пакета Windows Support Tools. С помощью этой утилиты можно, например, изменить состояние устройства, удалить его или, наоборот, вручную установить. Параметры утилиты можно получить из встроенной справки.

Много ценной информации об устройствах и драйверах можно получить с помощью утилиты *System Information* (Сведения о системе) *(см. главу 3)*, в частности — список всех имеющихся драйверов, их состояние и режим запуска. Информацию о драйверах можно также получить с помощью утилиты командной строки *DriverQuery.exe*.

Основные параметры видиосистемы компьютера и режимы DirectX легко увидеть, воспользовавшись стандартным средством диагностики DirectX — утилитой *DxDiag.exe*, которая запускается из командной строки.

Проверка состояния устройств и драйверов

Чтобы просмотреть параметры конфигурациии конкретного устройства, дважды щелкните по его названию в окне оснастки **Device Manager** (Диспетчер устройств) (см. рис. 1.29) — появится окно свойств данного устройства, раскрытое на вкладке **General** (Общие). На этой вкладке отображается общая информация об устройстве, включая его название, тип, фирму-производителя, размещение на шине или название контроллера и статус (дополнительная информация о занимаемых ресурсах и возможных аппаратных конфликтах содержится на вкладке **Resources**). Особое внимание здесь следует обратить на панель **Device status** (Состояние устройства). Если устройство совместимо с операционной системой, правильно установлено и не конфликтует с другими аппаратными средствами, то отображается следующая строка:

```
This device is working properly
(Устройство работает нормально)
```

Если же в работе устройства имеют место неполадки и проблемы, то на панели отображается код ошибки и ее краткое описание. Такие устройства в окне диспетчера помечаются желтым треугольником с восклицательным знаком. В этом случае следует попробовать переустановить устройство или поменять для него драйверы *(см. далее)*.

Примечание

В меню **View** (Вид) имеются команды способа отображения устройств и ресурсов в окне оснастки **Device Manager** (Диспетчер устройств). Здесь также имеется команда **Show hidden devices** (Показать скрытые устройства), с помощью которой можно увидеть устройства, удаленные когда-то из системы, но "оставившие следы". Эта информация бывает полезной в случае возникновения конфликтов при повторной установке устройств аналогичного типа (например, сетевых плат).

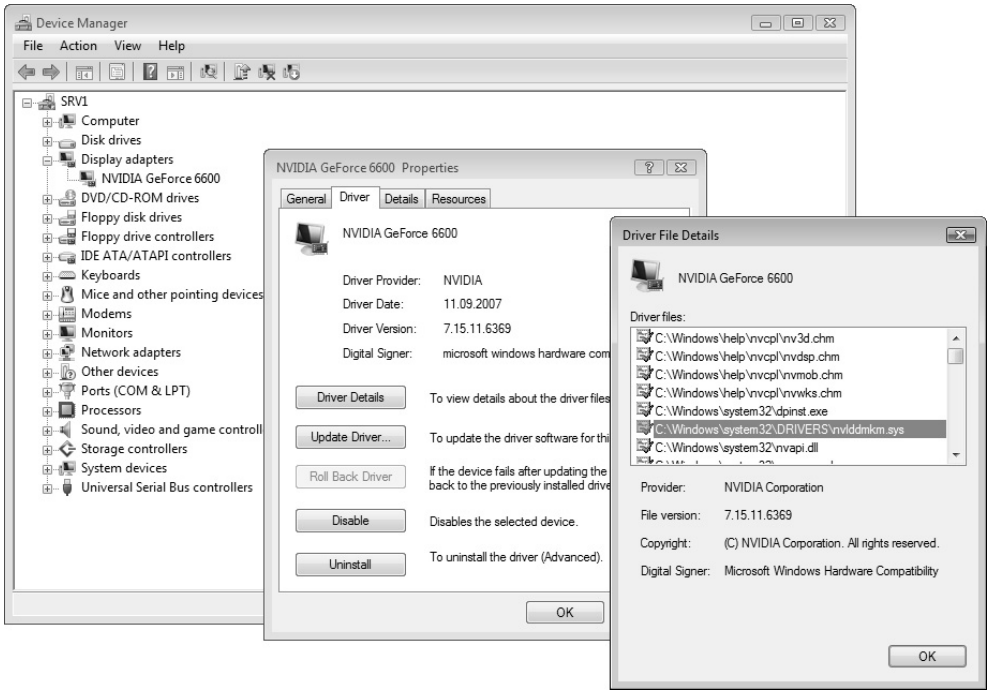


Рис. 1.29. Просмотр сведений
о драйвере выбранного аппаратного устройства

На вкладке **Driver** (Драйвер) (рис. 1.29) отображается базовая информация о драйвере устройства (название поставщика, дата выпуска, версия драйвера; расширенную информацию о драйвере можно получить, нажав кнопку **Driver Details** (Сведения)). Здесь же с помощью соответствующих кнопок можно запустить обновление драйвера устройства (будет использоваться та же процедура, что и при установке драйверов — *см. далее*), удалить драйвер из системы или отключить устройство. Обратите внимание, что если после обновления драйвера в работе устройства будут обнаружены неполадки, то можно вернуться к использованию предыдущей версии драйвера, нажав кнопку **Roll Back Driver** (Откатить).

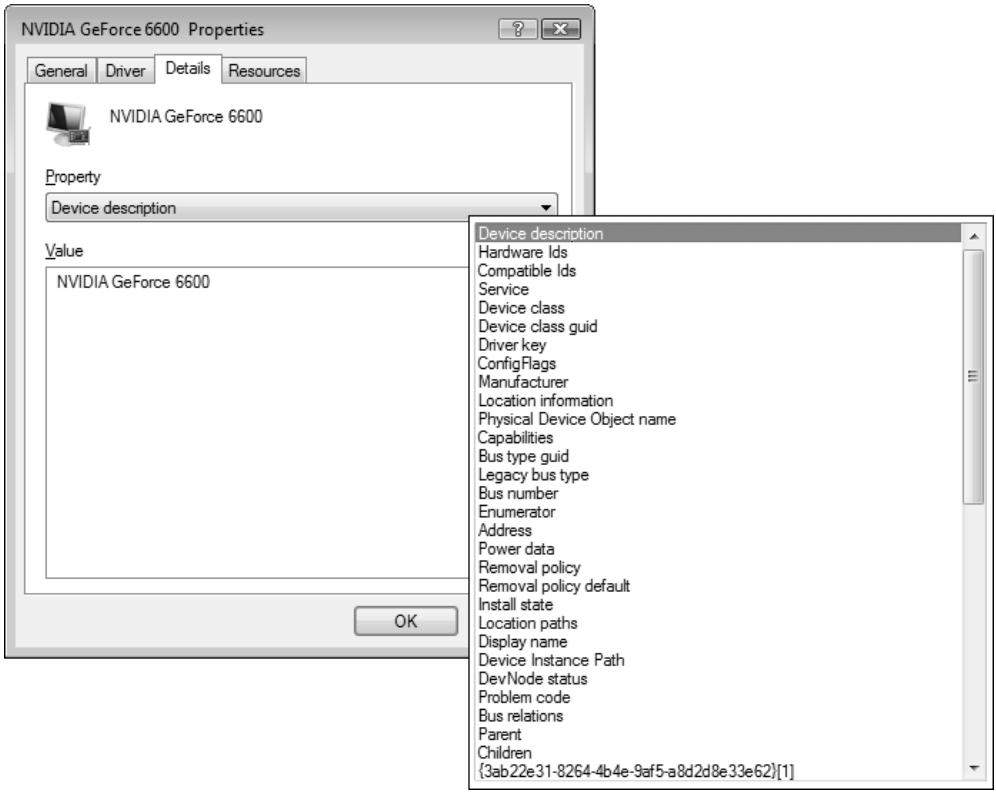


Рис. 1.30. Список свойств устройства

Внимание!

В системах Windows Vista и Windows Server 2008 нельзя создавать профили оборудования (hardware profile), существующие в системах Windows

2000/XP и позволяющие определять наборы используемых аппаратных средств (для этого в окне свойств каждого устройства имеется возможность выбора применяемого профиля). Скрытые профили имеются только для переносимых компьютеров, подключаемых к док-станции.

На вкладке **Details** (Сведения) (рис. 1.30) в виде длинного раскрывающегося списка (см. врезку) представлены многочисленные свойства устройства. Некоторые из них могут быть полезными для диагностики или при работе с утилитой Devcon.exe (например, идентификаторы Hardware IDs (ИД оборудования) используются для обращения к конкретному устройству).

Установка драйверов для подключенных устройств

При подключении к компьютеру нового устройства (например, флэш-накопителя, внешнего диска, принтера и т. д.) система пытается распознать устройство, и в случае успеха на панели задач в области уведомлений появляется индикатор мастера установки нового оборудования и выводится всплывающее сообщение, информирующее пользователя об обнаружении нового устройства. При этом система автоматически установит драйвер успешно распознанного устройства, сконфигурирует устройство для работы и через несколько секунд выведет всплывающее сообщение, информирующее о том, что новое устройство готово к работе.

Для некоторого оборудования (например, для принтеров, сканеров и т. д.) непосредственная установка драйверов и служебных утилит должна выполняться заранее — до того, как устройство подключается к системе (по требованиям производителей оборудования). Затем, при физическом включении устройства, все равно выполняется стандартная процедура распознавания устройства, и система конфигурирует уже имеющийся у нее драйвер.

Совет

Иногда возникают проблемы при установке вполне работоспособных драйверов, но не предназначенных специально для системы Windows Server 2008. Можно предложить следующую рекомендацию, которая нередко помогает в данной ситуации. Найдите на дистрибутивном носителе драйверов все запускаемые файлы (типа setup.exe и т. п.; иногда таких файлов может быть несколько, для разных служебных программ, поставляемых вместе с устройством), которые выполняют установку, откройте для них окно свойств

файла и установите режим совместимости с Windows XP Service Pack 2. После этого запускайте программу установки от имени администратора (с помощью соответствующей команды в контекстном меню файла).

Если после загрузки система обнаруживает новое устройство, то появляется запрос, показанный на рис. 1.31. Можно отказаться от установки драйверов в данный момент или вообще, но если драйверы имеются, то их следует установить; можно также попытаться найти драйверы на сайте Microsoft (в этом случае в специальном всплывающем окне можно будет видеть, как выполняются поиск и загрузка драйвера). Для этого следует выбрать первую в списке опцию.

Рис. 1.31. Запрос на установку драйвера для обнаруженного устройства

Если система успешно находит, загружает и устанавливает драйвер в автоматическом режиме, то этот процесс заканчивается появлением специального сообщения (рис. 1.32) (если драйвер имеется на локальном диске, то система находит и устанавливает его сама, без всяких запросов). В противном случае драйвер нужно устанавливать вручную.

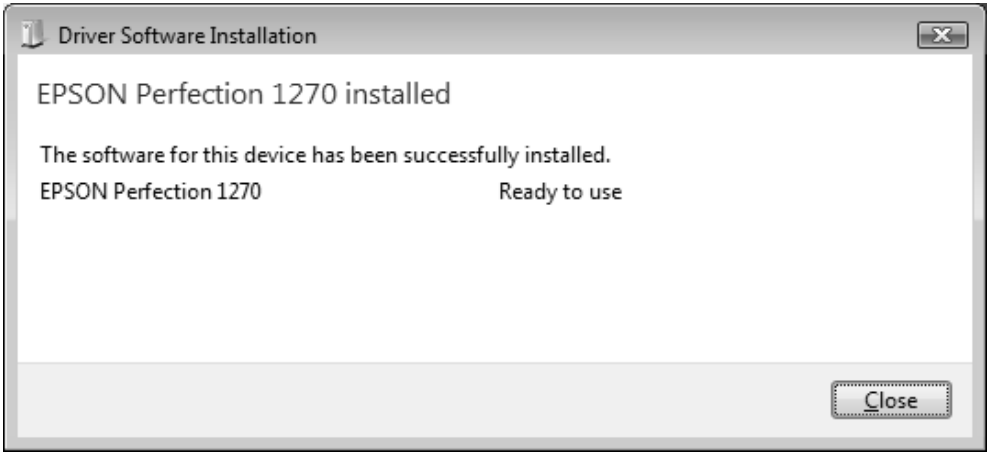


Рис. 1.32. Сообщение о загрузке и успешной установке драйвера для нового устройства

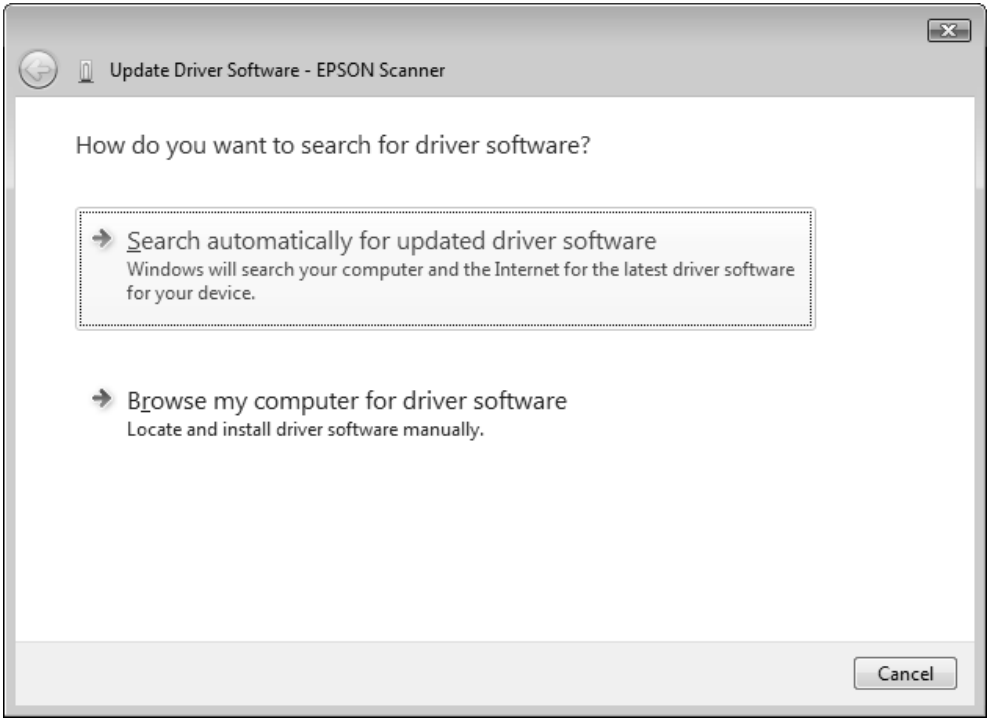


Рис. 1.33. Выбор способа поиска драйвера

При ручной установке драйвера или необходимости его обновлении (в этом случае в окне диспетчера устройств нужно выбрать устройство и в контекстном меню выполнить команду **Update Driver Software** (Обновить драйверы)) следует определить способ поиска драйвера — автоматический или ручной (рис. 1.33). Автоматический поиск осуществляется сначала в стандартном хранилище драйверов (это папка *%SystemRoot%*\System32\ DriverStore), а затем — в Интернете (на сайте Windows Update). Ручной поиск выбирается, если драйверы хранятся в других папках на диске или на дистрибутивном носителе.

Рис. 1.34. Определение местоположения драйвера или выбор драйвера из списка

При выборе опции поиска драйверов на компьютер на следующем шаге нужно определить местоположение драйверов (рис. 1.34) — они могут находиться на локальном диске или на сменном носителе. Можно указывать корневую папку (с поиском во вложенных подкаталогах) или конкретный каталог. Также можно просто выбрать устройства из списка устройств, для которых в

системе имеются стандартные драйверы (ссылка **Let me pick from a list of device drivers on my computer**).

Если требуется установить драйвер из числа уже имеющихся в системе, то на следующих шагах следует выбрать тип устройства (рис. 1.35), а затем — конкретную модель (рис. 1.36). Также имеется возможность использования установочного диска.

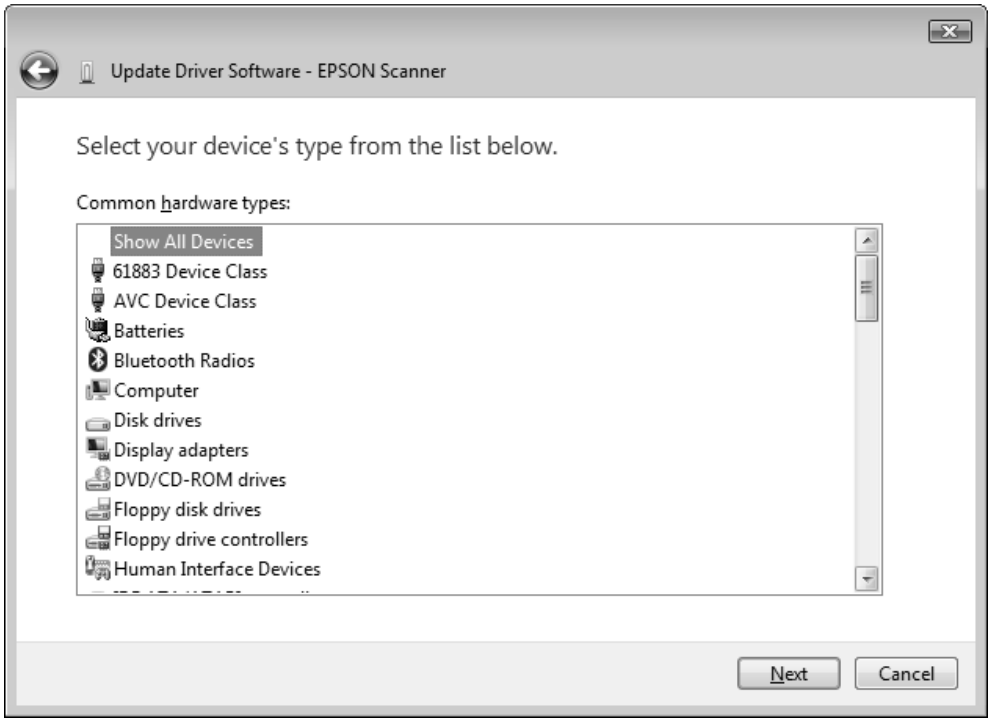


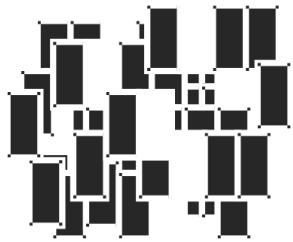
Рис. 1.35. Выбор типа устройства, для которого будет устанавливаться драйвер

После того как в результате выполнения описанных выше процедур выбран тот или иной способ поиска драйвера для нового устройства, система попытается обнаружить подходящий драйвер и установить его. Если драйвер не подписан, то появляется предупреждение, и пользователь может либо разрешить его установку, либо отказаться. В случае успешной установки окно диспетчера устройств обновляется, и имя устройства появляется в соответствующей группе, если выбрана сортировка по типу устройств. Если драйвер

не обнаружен, то устройство остается в неработоспособном (неподключенном) состоянии, и нужно искать для него другие драйверы.

Рис. 1.36. Выбор модели подключаемого устройства

Глава 2



Пользовательский интерфейс и рабочая среда

Эффективная работа в системе требует хорошего знания элементов пользовательского интерфейса и методов правильного взаимодействия компонентов системы. Это важно как для клиентских операционных систем, так и для серверных платформ. Поскольку интерфейс систем Windows Server 2008 заметно отличается от предыдущей версии (Windows Server 2003), мы решили уделить ему особое внимание — данная глава полностью посвящена описанию рабочей среды: интерфейсу системы и ее основных компонентов, представлению объектов файловой системы в программе Windows Explorer (Проводник) и операциям с ними и т. п.

Базовые концепции визуального интерфейса Windows сохранились и в последних версиях — системах Windows Vista и Windows Server 2008, однако многие элементы и детали реализации являются новыми и требуют определенного привыкания и изучения. Пользователю, знакомому с Windows Vista, легко будет работать в среде Windows Server 2008, хотя имеются и некоторые отличия в исходных (default) настройках и поведении этих систем.

В системах Windows Server 2008 многие новые элементы пользовательского интерфейса по умолчанию не установлены, однако при необходимости и наличии технических (аппаратных) возможностей можно включить *все* эффектные и удобные средства, имеющиеся в Windows Vista (включая Aero Glass, Windows Flip 3D и т. д.).

> ***Внимание!***
>
> Все иллюстрации в книге (снимки экранов, screenshots) даны с использованием стиля (темы) *Windows Vista Basic* (Windows Vista – упрощенный стиль) *(см. далее)*. Он выглядит лучше, чем устанавливаемый по умолчанию стиль

Windows Classic, и при этом не так требователен к характеристикам видеоадаптера, как стиль *Windows Aero*.

Прежде всего мы уделим внимание новой концепции построения пользовательского интерфейса, которая была специально разработана для систем Windows Vista/Server 2008, — речь идет о стиле Aero. Затем будут описаны компоненты рабочей среды, включая способы их настройки, и особенности выполнения типовых операций, таких как манипуляции с файлами (просмотр, сохранение, поиск и т. д.), средства поиска информации, переключение между окнами работающих программ и т. п. В следующей главе будут описаны дополнительные средства конфигурирования различных элементов графического интерфейса.

Стиль Aero — ключевая особенность нового пользовательского интерфейса Windows

Компания Microsoft постаралась сделать пользовательский интерфейс своих новых операционных систем Windows Vista и Windows Server 2008 максимально привлекательным и удобным для конечных пользователей, а также управляемым и функционально полным с точки зрения разработчиков приложений. Для этого в рамках глобальной программы создания этих систем, имевших общее кодовое название *Longhorn*, был предусмотрен проект с названием *Aero*. Этот проект представлял собой совокупность концепций, соглашений и требований, в соответствии с которыми были модернизированы все компоненты интерфейса пользователя.

Внимание!

Необходимы некоторые уточнения, чтобы не было путаницы в терминологии. Далее мы будем говорить о *стиле Aero* как о концепции нового интерфейса систем Windows Vista/Windows Server 2008, которая охватывает все элементы рабочей среды — от вида и разновидностей окон до расположения кнопок и подписей внутри них. В списке стилей (тем) этот стиль фигурирует как *Windows Vista* (см. рис. 3.36). Существует составная часть общей концепции нового интерфейса, получившая название *Aero Glass*; она предусматривает возможность использования трехмерной графики, прозрачных окон, эффектов анимации и т. п. Другие элементы интерфейса стиль Aero Glass не затрагивает (если говорить о типах окон, расположении на них элементов, используемых значках, шрифтах и т. д.). Поэтому возможны варианты, когда Aero Glass используется (этот стиль (цветовая схе-

ма) называется *Windows Aero* — см. рис. 3.39) и когда Aero Glass *не* используется (*Windows Vista Basic* (Windows Vista – упрощенный стиль); см. рис. 3.39). Помимо этого, существует *классический стиль* (тема) и классическая цветовая схема — *Windows Classic* (см. рис. 3.36 и 3.39), при котором не применяются Aero Glass и другие новшества в оформлении окон и других элементов пользовательского интерфейса, но при этом *сохраняются* многие новые решения, предлагаемые в рамках общей концепции стиля Aero — например, типы диалоговых окон, панелей управления и программ-мастеров, поле поиска и разновидности меню **Start** (Пуск), используемые значки, панели просмотра и т. д.

В книге мы будем использовать то название стиля, которое наиболее точно подходит по смыслу к содержанию текста.

Далее мы рассмотрим основные идеи, заложенные в эстетику стиля Aero, и покажем, как они реализованы в элементах интерфейса.

Эстетика Aero

Новый стиль интерфейса должен быть привлекательным для пользователя и обеспечивать эффективную работу с системой. "Изюминкой" этого стиля является концепция *Aero Glass*, которая предусматривает использование свойства прозрачности окон, многочисленных анимационных эффектов (плавных переходов от одного вида к другому), высококачественной графики и 3-мерных изображений. Aero Glass — это одновременно и составляющая часть концепции визуального представления элементов интерфейса, и функция, которую в системах Windows Vista/Windows Server 2008 можно включать и отключать.

Примечание

Именно для реализации Aero Glass системы Windows Vista/Windows Server 2008 предъявляют повышенные требования к видеосистеме компьютеров *(см. Введение)*. Эти системы можно устанавливать и на компьютеры с более скромными характеристиками, однако в этом случае некоторые визуальные возможности интерфейса будут отключены и будет использоваться *упрощенный стиль Windows Vista* (Windows Vista Basic) или *классический стиль* (Windows Classic).

Покажем на примерах отличия и привлекательные особенности нового стиля Aero, хотя черно-белые иллюстрации и не очень наглядно передают все детали. На рис. 2.1 и 2.2 для сравнения показано окно программы Windows Ex-

plorer (Проводник) в классическом стиле (устанавливаемом по умолчанию) и в стиле Windows Aero (т. е. с включенной функцией Aero Glass).

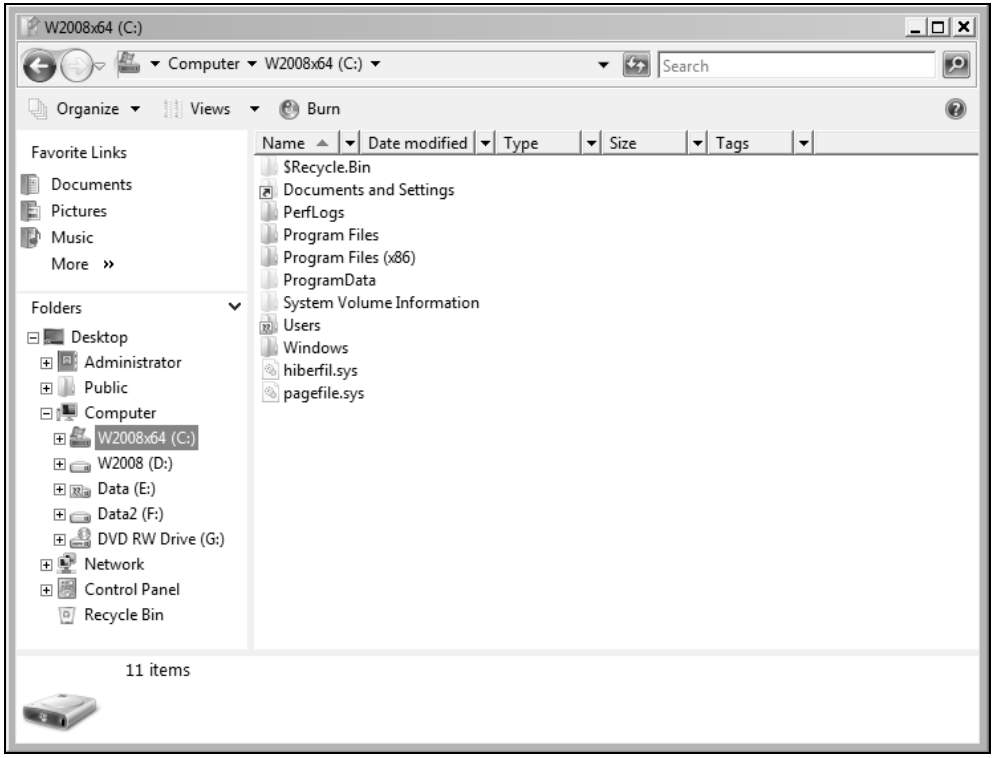


Рис. 2.1. Вид окна программы Windows Explorer при использовании классического стиля (Windows Classic)

Можно видеть, что содержание окна не меняется, неизменными остаются все поля, списки, панели и многие значки. Меняется лишь их вид — во втором случае появляется прозрачность заголовка и рамки окна. (Обратите внимание на вид заголовка и рамки окна, а также на форму кнопок управления окном и вид панели поиска.) Все новые функции присутствуют в обоих случаях — панели просмотра и подробностей, панель задач и меню видов с возможностью плавного изменения размера значков, меню выбора папок в поле адреса, поле поиска, заголовки просматриваемых столбцов и т. д.

За исключением отдельных вспомогательных операций (например, предпросмотр окон на панели задач или Windows Flip 3D), для пользователя не имеет

принципиального значения, какой стиль оформления он выбирает — функциональные возможности системы и приложений от этого не меняются.

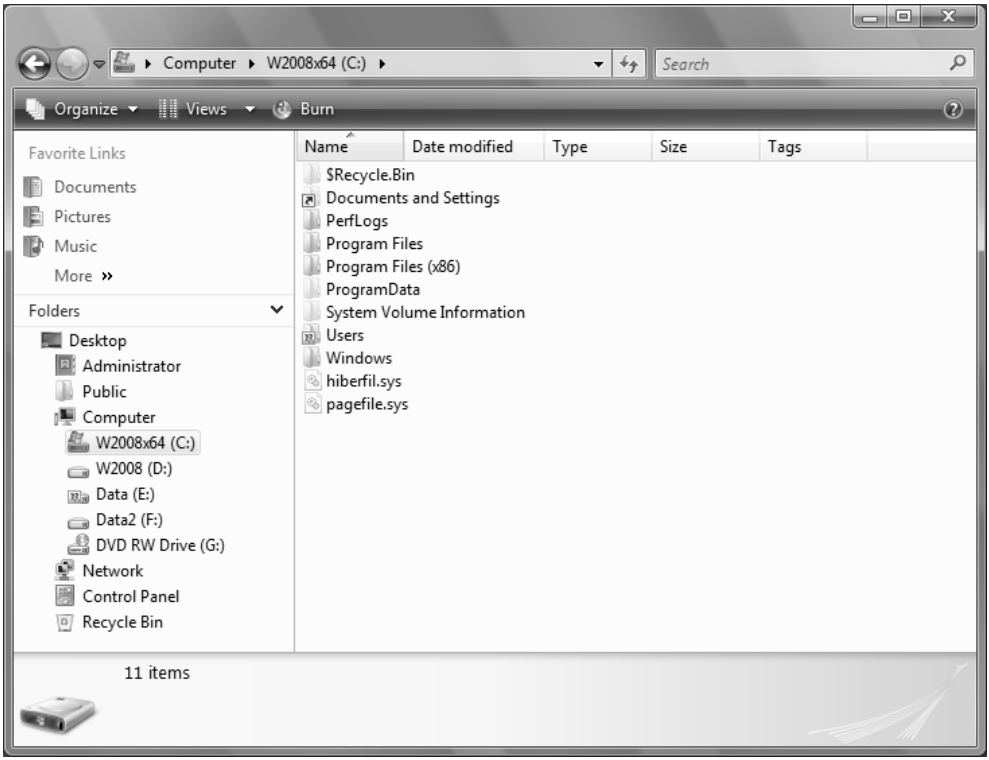


Рис. 2.2. Вид окна программы Windows Explorer при использовании стиля Windows Aero

Эффект от использования функции Aero Glass не очень заметен на иллюстрациях. На рис. 2.3 показан фрагмент стандартного окна: вверху — при включенной функции (стиль Windows Aero), внизу — при выключенной (упрощенный стиль Windows Vista). Можно заметить, что во втором случае (нижняя картинка) область заголовка становится непрозрачной, матовой и без "муарового" перелива; значки управления окном имеют меньший размер и другое расположение, выбранная кнопка меняет цвет, но область вокруг нее не подсвечивается. Кроме того, отсутствует тень вокруг окна.

Еще лучше прозрачность окон видна на рис. 2.4, где масштаб немного увеличен — сквозь заголовок окна просвечивает лежащее под ним изображение

(степень прозрачности можно менять), и заметнее эффект от подсвечивания кнопок управления окном. Эффект от использования Aero Glass гораздо заметнее в других случаях — например, *см. далее разд. "Окна уведомлений"* и *"Переключение задач"*.

Рис. 2.3. Включенный (вверху) и выключенный (внизу) режим Aero Glass

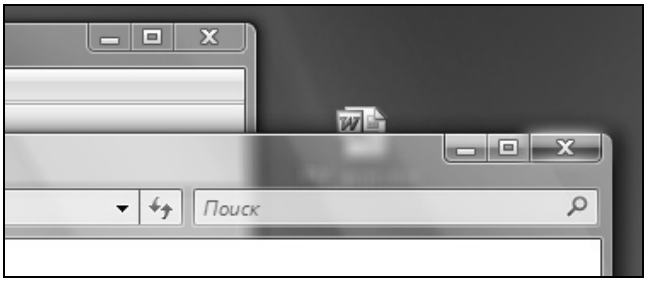


Рис. 2.4. Прозрачные заголовки и окантовка окон

Универсальные элементы управления

Стиль Aero предусматривает новый дизайн всех стандартных элементов пользовательского интерфейса, к которым относятся текстовые окна, переключатели, флажки, командные кнопки, обычные и раскрывающиеся списки, древовидные структуры (trees), вкладки, ползунки (sliders), индикаторы хода процесса (progress bars) и другие компоненты. Здесь мы не будем специально приводить примеры, поскольку изображения таких элементов встречаются на иллюстрациях практически в каждой главе книги, и всегда можно сравнить их вид с интерфейсом предыдущих версий Windows.

Диалоговые окна задач

Новый элемент пользовательского интерфейса Aero — *окна задач* (task dialog). Они используются для стандартизованного (унифицированного) представления выбора при решении той или иной задачи (вопроса). Окно задачи состоит из названия задачи, ее описания и нескольких командных кнопок, которые определяют выбор действий по выбору пользователя. Разработчики приложений могут применять окна задач для эффективного общения с конечным пользователем. Примером окна задачи может служить запрос на установку драйвера для обнаруженного устройства — *см. разд. "Установка драйверов для подключенных устройств" главы 1*.

Поле поиска

Стандартное *поле поиска* (Search) (рис. 2.5) встроено в большинство диалоговых окон и стандартных программ Windows Server 2008. Например, оно присутствует в меню **Start** (Пуск), программе Windows Explorer (Проводник), на панели управления (Control Panel), в папке **Network** (Сеть), в окнах **Open** (Открыть) и **Save As** (Сохранить как) и т. д.

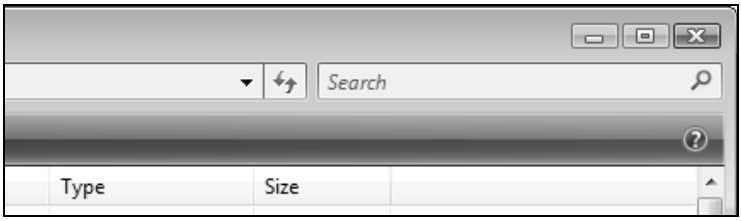


Рис. 2.5. Панель поиска присутствует во многих диалоговых окнах

Благодаря полю поиска пользователи могут осуществлять контекстный поиск информации в любой "точке" интерфейса, при этом они будут получать результаты, логически зависящие от контекста (назначения) открытого окна или запущенной программы.

Программы-мастера

Программы-мастера (wizards) используются для выполнения типовых задач, не требующих от пользователя какой-либо квалификации. Они представляют собой последовательность окон, в которых представлены элементарные шаги и действия, необходимые со стороны пользователя. Стиль Aero предусматри-

вает стандартизованный подход к созданию мастеров, что позволяет пользователю легче ориентироваться в различных ситуациях, поскольку решение задач разбивается на понятные шаги и стиль представления этих шагов единообразен для всего интерфейса.

Универсальные диалоговые окна для работы с файлами

Многие системные программы и пользовательские приложения работают с файлами, для чего существуют стандартные окна для выбора открываемых файлов (окно **Open**) и для указания местоположения сохраняемых данных (окна **Save** и **Save As**).

Стандартный вид этих окон упрощает пользователю работу с файлами, делая привычными эти манипуляции в разных по назначению приложениях. На рис. 2.6 для примера показано стандартное окно сохранения документов — **Save As** (Сохранить как) (по умолчанию используется компактный, упрощенный вид окна). Дизайн этого окна не зависит от типа сохраняемого файла.

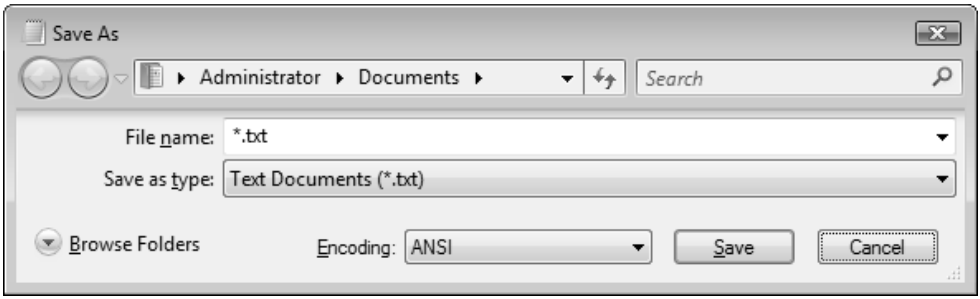


Рис. 2.6. Стандартное окно **Save As**

Если в окне **Save As** (Сохранить как) (см. рис. 2.6) щелкнуть по стрелке **Browse Folders** (Обзор папок), то можно получить доступ к структуре локальных и сетевых папок для выбора целевой папки (рис. 2.7). В окне имеется также панель избранных ссылок (Favorite Links), соответствующих стандартным папкам пользовательского профиля.

Внимание!

Ссылка **Recent Places** (Недавние места) присутствует в окнах **Save As** (Сохранить как) и подобных, если только в системе установлен компонент Desktop Experience (Возможности рабочего стола) *(см. главу 3)*.

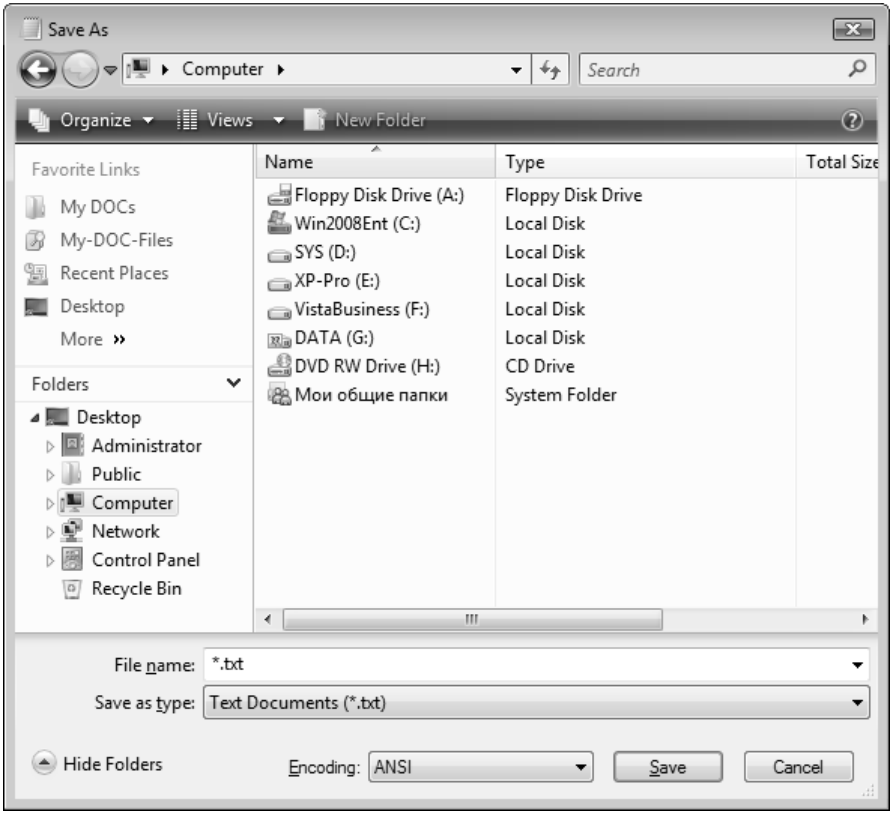


Рис. 2.7. Окно **Save As** с возможностью просмотра папок

Панели управления

Панели задач или *панели управления* (control panels) служат для изменения системных параметров (например, для установки аппаратных и программных средств, управления учетными записями, настройки безопасности и т. п.) и выполнения связанных с этим задач. Стиль Aero предусматривает стандартизованный подход к созданию и оформлению панелей управления.

Хороший пример нового дизайна панелей управления можно видеть на рис. 3.5, где изображены одна из категорий задач панели управления Windows Server 2008 и входящие в эту категорию подзадачи. Другим примером является новое окно **Windows Update** (Центр обновления Windows) (см. рис. 3.10). Панель управления может делиться на две половины: слева показаны объекты или относящиеся к ним задачи управления, а справа — ко-

мандные кнопки для выполнения нужных действий или ссылки на окна свойств, в которых можно модифицировать системные параметры.

Значки

Значки (icons) широко используются в интерфейсе операционной системы для визуального представления программ, объектов, действий и т. п. и помогают пользователю идентифицировать объекты и мнемонически запоминать их назначение.

В системах Windows Vista/Windows Server 2008 значки выглядят более реалистично по сравнению с Windows XP/Windows Server 2003, при этом они не напоминают фотографии[1]. Максимальный размер значков равен 256 на 256 пикселов, что делает их пригодными при работе с мониторами, имеющими высокое разрешение; при этом размер отображаемых значков можно плавно менять. Прикладные программы могут использовать любые системные значки.

Новые значки используются не только при выборе темы Windows Vista (с цветовыми схемами Windows Vista Basic или Windows Aero), но и с другими темами, включая классический стиль *(см. главу 3)*.

Системный шрифт Segoe UI

Стиль Aero предусматривает широкое использование нового системного шрифта *Segoe UI*, при этом размер шрифта по сравнению с системами Windows XP/Windows Server 2003 увеличен до 9 пунктов (в системах Windows XP/Windows Server 2003 применяется шрифт Tahoma размером 8 пунктов; в Windows Vista/Windows Server 2008 этот шрифт используется при выборе классического стиля). Новые параметры системного шрифта можно видеть в окне тонкой настройки элементов пользовательского интерфейса (см. рис. 3.39).

Окна уведомлений

Всплывающие *окна уведомлений* (notifications)[2] информируют пользователя о системных событиях (например, о наличии сообщений от системы безопасности компьютера), а также используются прикладными программами, значки которых отображаются в области уведомлений на панели задач. В систе-

[1] Это принципиальное решение разработчиков стиля Aero.

[2] В английском языке такие окна называются *balloons*.

мах Windows Vista/Windows Server 2008 при использовании стиля Windows Aero такие окна исчезают постепенно, некоторое время находясь в полупрозрачном состоянии.

Вход в систему и ее выключение

Пользовательский интерфейс, используемый в Windows Server 2008 при входе в систему, заметно отличается от тех возможностей, которые имеются в предыдущих версиях Windows. В системах Windows XP/Windows Server 2003 существуют два способа интерактивного входа в систему:

- *экран приветствия* (Welcome screen) — заданный по умолчанию способ входа в систему, при котором на мониторе отображаются имена всех имеющихся на компьютере пользователей; для регистрации достаточно выбрать мышью нужное имя (и, возможно, ввести пароль);
- обычное *окно регистрации* в системе — традиционный способ входа в системы Windows NT и Windows 2000, он всегда используется на компьютерах — членах домена; в этом случае для регистрации пользователь вводит имя своей учетной записи и пароль, может также указывать имя домена. (Имя последнего работавшего пользователя при этом может не отображаться.)

Экран приветствия позволяет использовать механизм *быстрого переключения пользователей* (Fast User Switching). Эта возможность, появившаяся впервые в системах Windows XP, реализована на базе встроенных служб терминалов (Terminal Services). Она позволяет нескольким пользователям быть одновременно зарегистрированными на компьютере; при этом сохраняется их рабочая среда и при переключении не останавливаются программы, запущенные другим пользователем.

Для быстрого переключения пользователей необходимо, чтобы экран приветствия (Welcome screen) было включен. В системах Windows XP его можно включать и отключать по желанию администратора. Быстрое переключение и экран приветствия всегда отключаются, когда компьютер входит в домен (при этом используется традиционное окно регистрации).

В системах Windows Vista/Windows Server 2008 ***экран приветствия включен всегда***, и его нельзя запретить, поскольку он используется и на автономном компьютере (члене рабочей группы), и на компьютерах, входящих в домен — несколько меняется лишь вид окна. ***Механизм быстрого переключения пользователей также всегда включен***, и его ***нельзя блокировать***

(можно только запретить элементы интерфейса, позволяющие выполнять эту функцию — *см. далее*). Переключение пользователей возможно даже на компьютерах — членах домена.

После загрузки системы Windows Server 2008 — автономной или входящей в домен — пользователь видит экран регистрации (рис. 2.8) с предложением нажать клавиши <Ctrl>+<Alt>+<Delete>. (Обязательность выполнения этого требования определяется тем, что по умолчанию включена политика безопасности **Local Policies** | **Security Options** | **Interactive logon: Do not require CTRL+ALT+DEL** (Локальные политики | Параметры безопасности | Интерактивный вход: не требовать нажатия сочетания клавиш CTRL+ALT+DEL).) По умолчанию кнопка выбора языка ввода не отображается — используется основной язык системы (английский или локализованной версии). В принципе, язык ввода может потребоваться при вводе пароля; в некоторых режимах вводится и имя пользователя, поэтому выбор языка тоже может потребоваться в этом окне. Изменить ситуацию можно путем редактирования реестра *(см. далее)*.

Рис. 2.8. Экран регистрации в системах Windows Server 2008

Левая кнопка позволяет включить специальные возможности, необходимые людям с ослабленным зрением или ограниченными физическими возможностями (рис. 2.9): например, модуль озвучивания текста (Narrator), увеличительное стекло (Magnifier), клавиатура, отображаемая на экране (On-Screen Keyboard) и т. д.

После нажатия клавиш <Ctrl>+<Alt>+<Delete> появляется экран приветствия (рис. 2.10). В нашем примере можно видеть на рисунке три пиктограммы, соответствующие учетным записям пользователей, имеющимся на компьютере (сразу же после установки пользователь только один — *см. разд. "Установка пароля" главы 1*). Для входа в систему надо щелкнуть по нужной пиктограмме и ввести соответствующий пароль. (Напомним, что пароль администратора задается при первой регистрации в системе после ее установки.)

Правая кнопка (см. рис. 2.10) позволяет выключить компьютер, а щелчок по стрелочке открывает меню, в котором можно выбрать команды перезагрузки (**Restart**) и перехода в спящий режим (**Sleep**) (если этот режим поддерживается). По умолчанию эта кнопка отсутствует, поскольку запрещена политика безопасности **Local Policies** | **Security Options** | **Shutdown: Allow system to be shut down without having to log on** (Локальные политики | Параметры безопасности | Завершение работы: разрешить завершение работы системы без выполнения входа в систему).

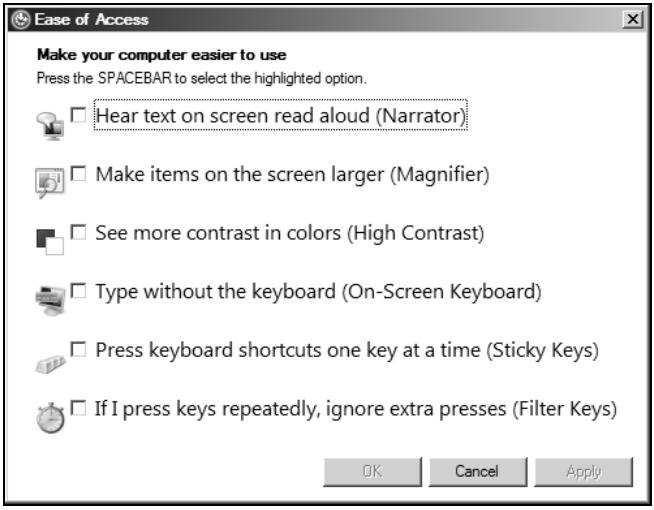


Рис. 2.9. Окно выбора специальных возможностей

На экране приветствия для ввода символов может использоваться язык локализованной версии или английский язык. Для английской версии системы язык ввода только один, и кнопка выбора языка вообще отсутствует. Включить дополнительные языки или изменить порядок языков ввода на экране приветствия можно, изменив в реестре раздел `HKEY_USERS\.DEFAULT\Keyboard Layout\Preload`.

Рис. 2.10. Экран приветствия в системах Windows Server 2008

Порядок языков ввода (номеров кодовых таблиц) определяется значениями параметров: в примере, показанном на рис. 2.11, по умолчанию выбирается английский язык (код 409), а русский язык будет дополнительным (код 419). Если поменять значения, то поменяется и порядок языков. В английской версии системы параметр вообще только один (код 409), потому и отсутствует кнопка выбора языка на экране приветствия. При необходимости можно вручную создать в реестре строковый параметр с нужным значением кода.

Если компьютер входит в состав домена Windows, то имя пользователя на экране задается полностью, в формате *<имяДомена>\<имяПользователя>*. В нашем примере на рис. 2.12 ранее использовался локальный вход в систему, поэтому в качестве домена указано имя самого компьютера.

Если нужно войти под другим именем (или в другой домен), то следует нажать кнопку **Switch User** (Сменить пользователя) (см. рис. 2.12). После этого на экране помимо кнопки последнего регистрировавшегося пользователя

(локального или доменного) появится кнопка **Other User** (Другой пользователь) (рис. 2.13). Нажав ее, вы попадете в окно, где можно ввести произвольное имя (см. рис. 2.14).

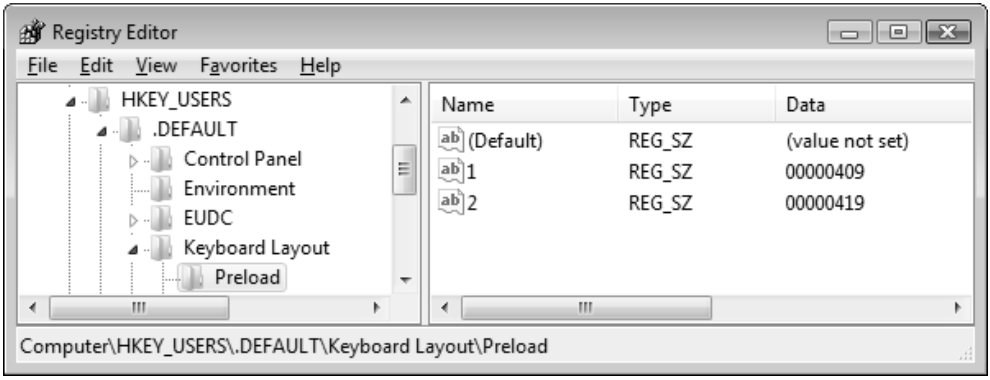


Рис. 2.11. Параметры реестра, определяющие выбор языка ввода при входе в систему

Рис. 2.12. Вход в систему на компьютере, подключенном к домену

Как можно видеть на рис. 2.14, по умолчанию предлагается вход в тот домен, к которому подключен компьютер (в нашем примере — INTERN; указывается NetBIOS-имя домена). Если щелкнуть по ссылке **How do I log on to another domain?** (Как войти в другой домен?), то можно получить подсказку, где указан формат имени. (Таким образом, имя домена или локального компьютера в Windows Server 2008 задается только в составе полного имени пользователя.) После ввода имени и пароля нужно щелкнуть по стрелке, расположенной справа от поля пароля, или нажать клавишу <Enter>.

Рис. 2.13. Вход в систему под другим именем, отличным от имени текущего пользователя

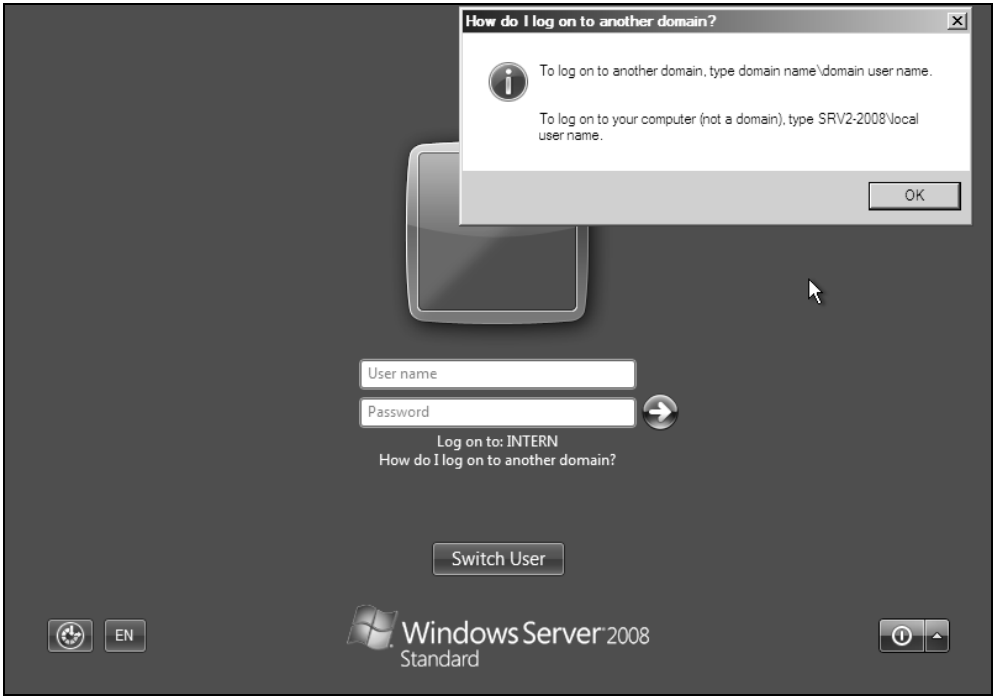


Рис. 2.14. Окно входа в систему под другим именем

Окно, аналогичное изображенному на рис. 2.14, будет *всегда* использоваться, если на компьютере запретить отображение последнего имени пользователя. Для этого в локальных политиках компьютера или домена в разделе **Security**

Options (Параметры безопасности) нужно включить политику **Interactive logon: Do not display last user name** (Интерактивный вход в систему: не отображать последнее имя пользователя).

Как уже говорилось, в системах Windows Vista/Windows Server 2008 саму функцию быстрого переключения пользователей нельзя запретить, однако можно запретить пользователям выполнять эту операцию, скрыв от них соответствующие элементы интерфейса (кнопки, опции меню и т. п.). Для этого нужно включить политику **Computer Configuration** | **Administrative Templates** | **System** | **Logon** | **Hide entry points for Fast User Switching** (Конфигурация компьютера | Административные шаблоны | Система | Вход в систему | Скрыть точки входа для быстрого переключения пользователей) и перезагрузить компьютер.

Блокировка компьютера

Для блокировки рабочего стола в моменты отсутствия интерактивной активности используются быстрые клавиши <Win>+<L> (также имеется специальная кнопка (с изображением замка) в меню **Start** (Пуск)).

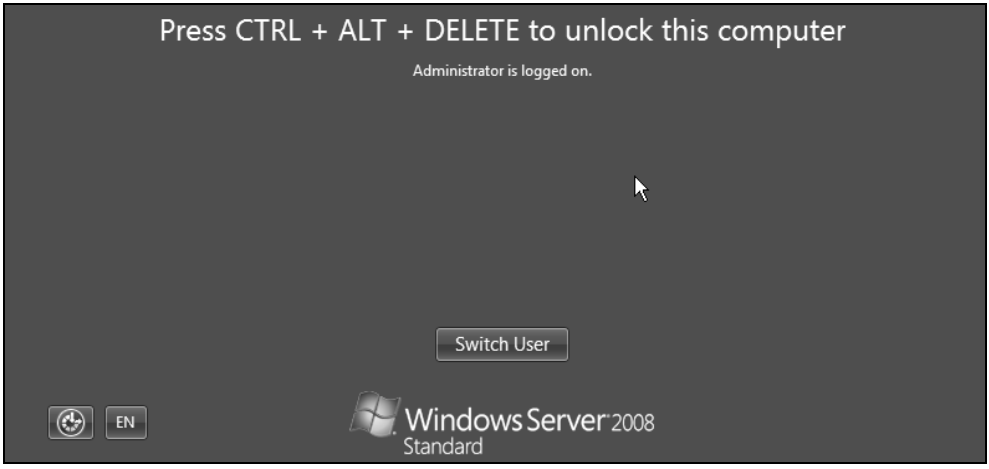


Рис. 2.15. Компьютер заблокирован зарегистрированным пользователем

Поскольку быстрое переключение пользователей включено, то выполняется следующая операция: сеанс текущего пользователя остается активным (работа запущенных приложений при блокировке не прекращается) и появляется экран

регистрации (рис. 2.15), где можно войти в систему под другим именем (нажав кнопку **Switch User** (Сменить пользователя)) или вернуться к текущему сеансу, введя пароль своей учетной записи. Выключить компьютер при этом нельзя.

Если в процессе работы с системой одновременно нажать клавиши <Ctrl>+<Alt>+<Del>, то появится экран безопасности системы (рис. 2.16), на котором имеются команды блокировки компьютера, переключения пользователей, выхода из системы, изменения пароля текущей учетной записи и запуска диспетчера задач (Task Manager).

Рис. 2.16. Экран безопасности системы

Выключение компьютера

Для завершения работы в системах Windows Server 2008 имеются две кнопки, встроенные в меню **Start** (Пуск) (см. рис. 3.16, сверху): левая кнопка по умолчанию полностью выключает компьютер[1], а правая — блокирует его. Действие, выполняемое после нажатия левой кнопки, можно выбрать с помощью задачи **Power Options** (Электропитание) на панели управления *(см. главу 3)*; оно указывается в окне подсказки, появляющейся при наведении на кнопку курсора мыши. При этом если кнопка имеет крас-

[1] В системах Windows Vista данная кнопка по умолчанию переводит компьютер в спящий режим (при этом запущенные приложения из памяти не выгружаются и готовы к работе сразу после возврата компьютера в рабочее состояние), если таковой поддерживается.

ный оттенок, то при нажатии кнопки компьютер будет выключаться полностью, а если цвет зеленоватый, то будет использоваться спящий режим или гибернация (hibernation).

Кроме того, щелкнув по стрелке, расположенной справа от этих кнопок, можно открыть меню с дополнительными командами (см. рис. 3.16, сверху): переключения пользователей (**Switch User**), выхода из системы (**Log Off**), перезагрузки (**Restart**) и выключения компьютера (**Shut Down**). Также в этом меню могут присутствовать команды перехода в спящий режим (**Sleep**) и режим гибернации (**Hibernate**) — это зависит от возможностей материнской платы и параметров BIOS.

Если при открытом рабочем столе нажать клавиши <Alt>+<F4>, то появится стандартное окно выключения компьютера (см. рис. 3.16, снизу), в котором можно выбрать необходимую команду.

Все особенности выключения компьютера и перехода в энергосберегающие режимы рассматриваются в *главе 3*. В этом плане у систем Windows Vista/Windows Server 2008 много нового.

Основные компоненты пользовательского интерфейса

Рассмотрим основные элементы интерфейса, посредством которого пользователь взаимодействует с системой, а также определим, как этот интерфейс можно настроить в соответствии со своими задачами и предпочтениями (некоторые вопросы конфигурирования рабочей среды будут рассматриваться в следующей главе).

Рабочий стол

После регистрации в системе пользователь видит *рабочий стол* (desktop) — область, где могут располагаться служебные значки и пиктограммы, представляющие файлы и программы, чаще всего необходимые пользователю. По умолчанию рабочий стол систем Windows Server 2008 (рис. 2.17) пуст и на нем присутствует только значок **Recycle Bin** (Корзина).

В нижней части экрана видна выделенная полоса — *панель задач*, на которой слева находится изображение кнопки **Start** (Пуск), а рядом с ней — значки, помещенные на *панель быстрого запуска* (Quick Lunch). В правой части па-

нели задач находятся *языковая панель*, представленная символьным изображением выбранного языка ввода (EN/RU), и *область уведомлений* (notification area), в которой располагаются различные значки компонентов системы, часы, а также служебные значки установленных программ, для которых необходим мониторинг.

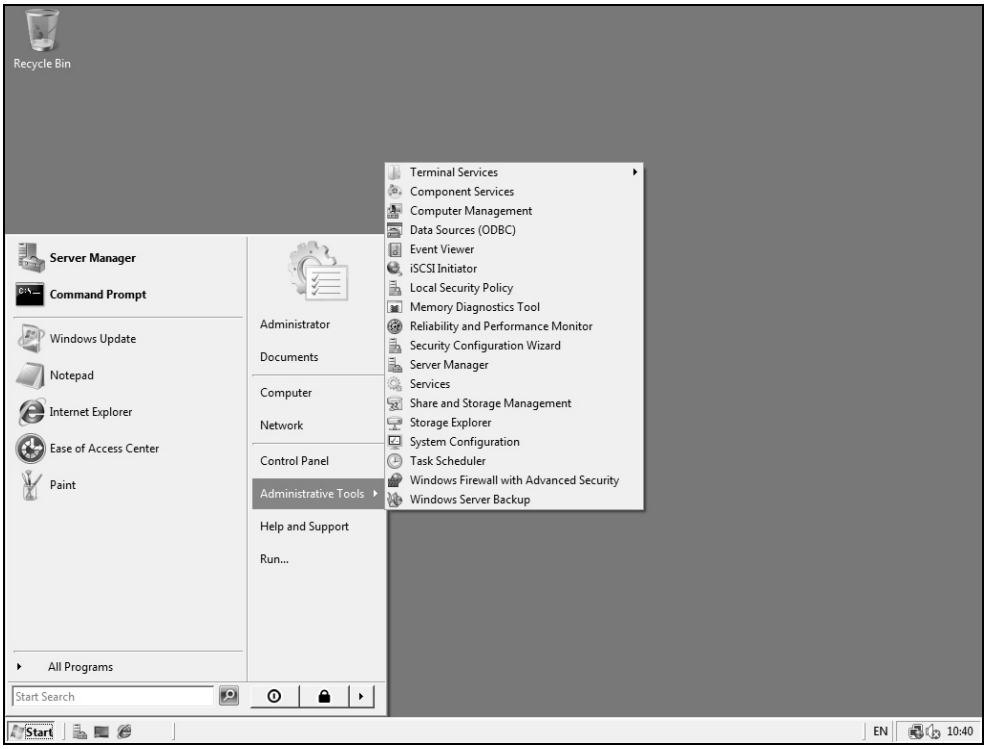


Рис. 2.17. Исходный вид рабочего стола и меню **Start** в системах Windows Server 2008

Изначально, после установки системы, используется классический стиль оформления (см. рис. 2.17). При выборе темы Windows Vista меню **Start** (Пуск) и панель задач будут выглядеть несколько иначе (рис. 2.18). Все изменения касаются только внешнего вида элементов, принципиальных функциональных различий нет[1].

[1] В классическом стиле отсутствует кнопка и сама функция переключения окон, что можно заметить по разному набору значков на панели быстрого запуска на рис. 2.17 и 2.18.

Рис. 2.18. Вид меню **Start** и панели задач при использовании стиля (темы) Windows Vista

Способы настройки глобальных параметров пользовательского интерфейса — стиля (темы), цветов, экранной заставки, фонового рисунка (обоев) рабочего стола и т. д. — будут описаны в *главе 3* в соответствующих разделах. Сейчас же мы подробно рассмотрим основные компоненты пользовательского интерфейса и их параметры.

Настройка опций корзины

В контекстном меню значка **Recycle Bin** (Корзина) кроме других прочих имеются две команды: **Empty Recycle Bin** (Очистить корзину) и **Delete** (Удалить) (т. е. удалить сам значок с рабочего стола). Если вместо очистки корзины по ошибке удален сам значок, то его несложно восстановить, открыв окно

Personalization (Персонализация) и изменив отображение значков на рабочем столе (см. рис. 3.35).

По сравнению с предыдущими версиями Windows, в системе Windows Server 2008 окно настройки параметров корзины (рис. 2.19) изменилось. Для каждого диска задается размер папки, где будут храниться удаленные объекты файловой системы (файлы, папки, ссылки и т. д.). Обычно система автоматически выделяет 10% от объема диска (для больших дисков это значение меньше). При необходимости указанную величину можно изменить.

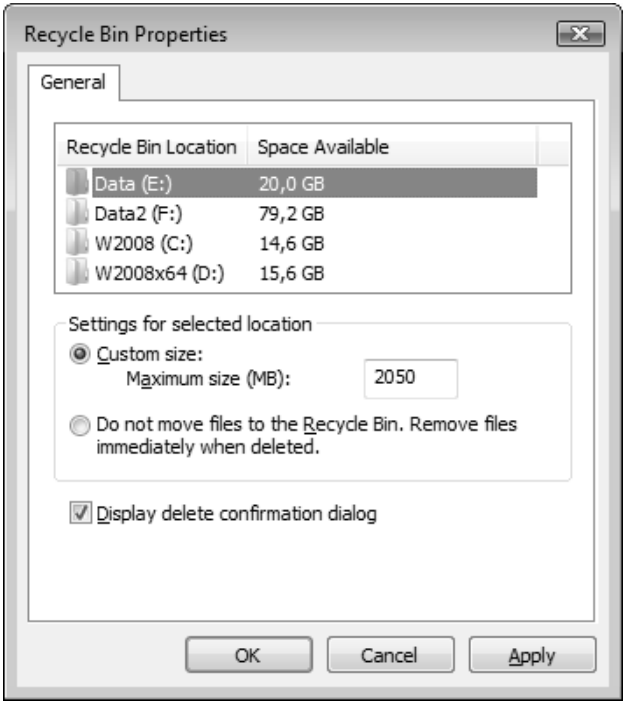


Рис. 2.19. Параметры корзины и опции операций удаления файлов или папок

Размер папки и возможность удаления файлов без копирования в корзину (переключатель **Do not move files to the Recycle Bin**) задаются для каждого диска индивидуально. (В обычном состоянии для полного удаления выбранных объектов нужно нажать клавиши <Shift> + <Delete> — в этом случае объекты удаляются сразу, без перемещения в корзину.) По умолчанию при удалении объектов появляется предупреждение, от которого можно отказать-

ся, сбросив флажок **Display delete confirmation dialog** (Запрашивать подтверждение на удаление).

Меню *Start* и панель задач

На первый взгляд меню **Start** (Пуск) (его содержимое после первой регистрации пользователя в системе можно видеть на рис. 2.17) в системах Windows Vista/Windows Server 2008 мало изменилось по сравнению с Windows XP/Windows Server 2003. В заголовке меню указывается имя и отображается пиктограмма зарегистрированного пользователя. В левой половине окна меню находятся закрепленные и наиболее часто запускаемые программы, а в правой — ссылки на системные папки (**Documents** (Документы), **Computer** (Компьютер), **Pictures** (Изображения), **Music** (Музыка) и т. д.[1]), а также на панель управления (**Control Panel**) и справочную систему (**Help and Support**).

Главное новшество меню **Start** (Пуск) в системах Windows Vista/Windows Server 2008 состоит в том, что список установленных приложений (папка **All Programs** (Все программы)) не раскрывается на новой панели, а "встроен" в основное окно меню **Start** (Пуск) (рис. 2.20). Из основного меню в него можно попасть, щелкнув по ссылке **All Programs** (Все программы) (см. рис. 2.17), а ссылка **Back** (Назад) (см. рис. 2.20) позволяет вернуться в основное меню.

> ***Примечание***
>
> Некоторые элементы в нашем примере меню **Start** (Пуск), показанном на рис. 2.20, выделены цветом. По умолчанию так отмечаются все вновь установленные в системе приложения. В данном случае можно видеть, какие программы появляются в системе после установки компонента Desktop Experience (Возможности рабочего стола) *(см. главу 3)*.

Для сравнения на рис. 2.21 изображен классический вид меню **Start** (Пуск)[2], привычный для многих предыдущих версий Windows. В этом случае все элементы (ссылки) группируются в виде иерархических меню, раскрывающихся

---

[1] По умолчанию отображаются только две первые из перечисленных папок; дополнительные ссылки включаются самим пользователем.

[2] Не следует путать классический стиль *меню* **Start** (Пуск) и классический стиль (тему) *пользовательского интерфейса* (Windows Classic): каждая тема позволяет выбирать *любой* стиль меню.

последовательно на отдельных панелях. Обратите внимание на то, что при выборе классического стиля меню **Start** (Пуск) на рабочем столе автоматически включается отображение значков компьютера, панели управления, сети и т. д.

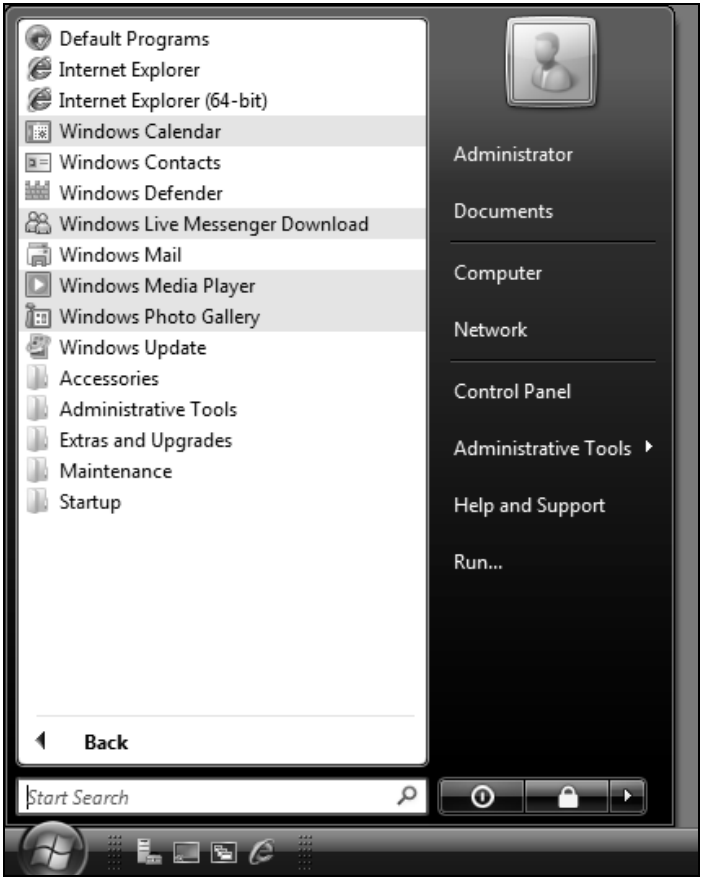


Рис. 2.20. Меню **Start** и панель установленных в системе приложений **All Programs**

Примечание

Список программ в меню **Start** (Пуск) всегда упорядочен по алфавиту, что облегчает поиск нужных программ (хотя эту сортировку можно отключить и располагать ссылки на программы в другом порядке — *см. след. разд.*).

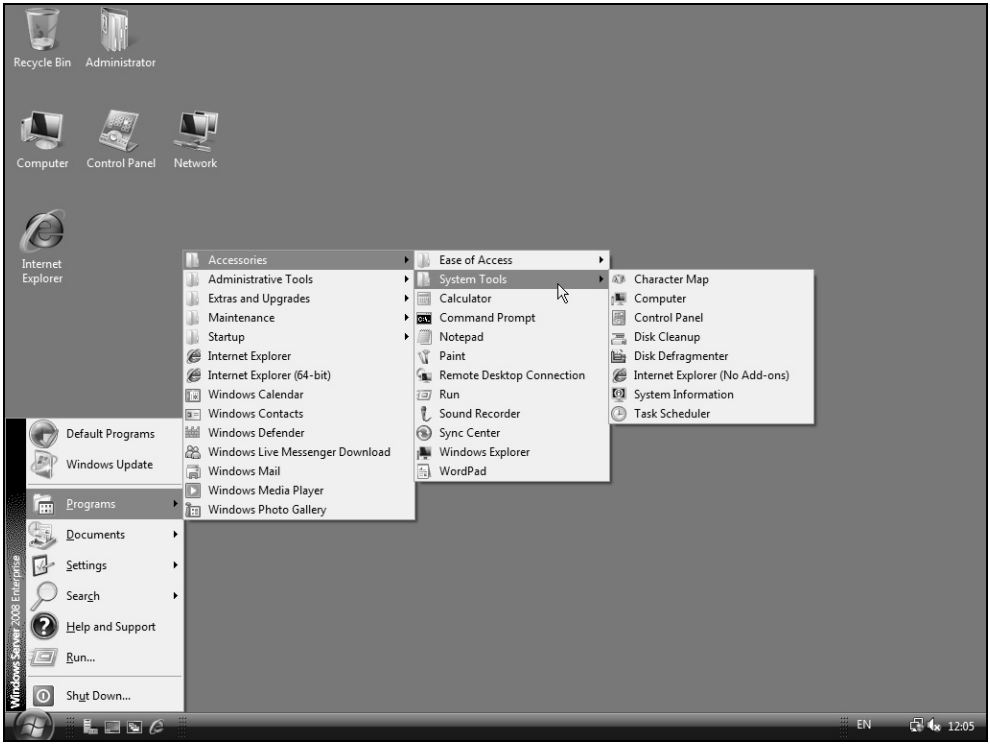


Рис. 2.21. Меню **Start** в классическом варианте

Большим достоинством нового меню **Start** (Пуск) является возможность быстрого поиска нужной программы или файла: для этого в поле **Start Search** (Начать поиск) нужно ввести имя или название (достаточно одного из ключевых слов) — система выполняет поиск после ввода каждого символа и отображает обнаруженные элементы в левой половине меню **Start** (Пуск) (рис. 2.22). Такой подход — особенно при большом количестве установленных программ — может значительно сократить поиск приложения, которое присутствует в системе, но используется нечасто. Поиск ведется не только среди программ, но и среди файлов, расположенных в пользовательских или индексируемых папках (о поиске и индексации речь еще пойдет далее), причем поиск выполняется не только по именам, но и по содержимому файлов и ключевым словам. Как видно в нашем примере, поиск введенной строки выполнялся в программных группах (**Programs**), ссылках веб-браузера (**Favorites and History**), файлах (**Files**), почтовых сообщениях и контактах (**Communications**).

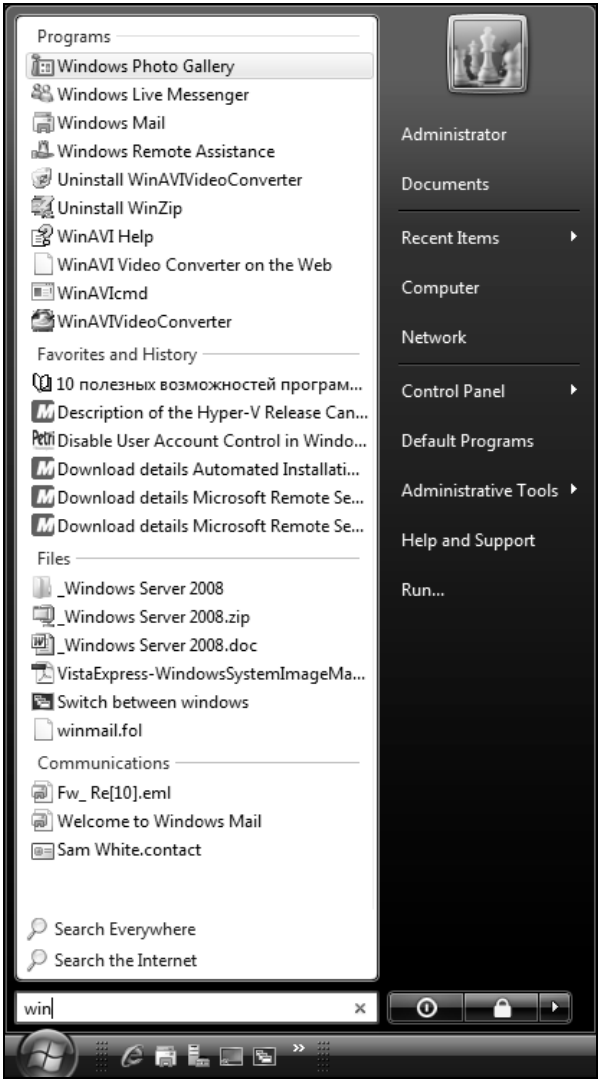


Рис. 2.22. Поиск по ключевому слову из меню **Start**

Настройка меню *Start*

Для настройки внешнего вида меню **Start** (Пуск):

1. Переместите курсор на свободное (черное) поле меню **Start** (Пуск) или панели задач, щелкните правой кнопкой мыши и выберите пункт **Properties** (Свойства).

2. В открывшемся окне перейдите на вкладку **Start Menu** (Меню "Пуск") (рис. 2.23).

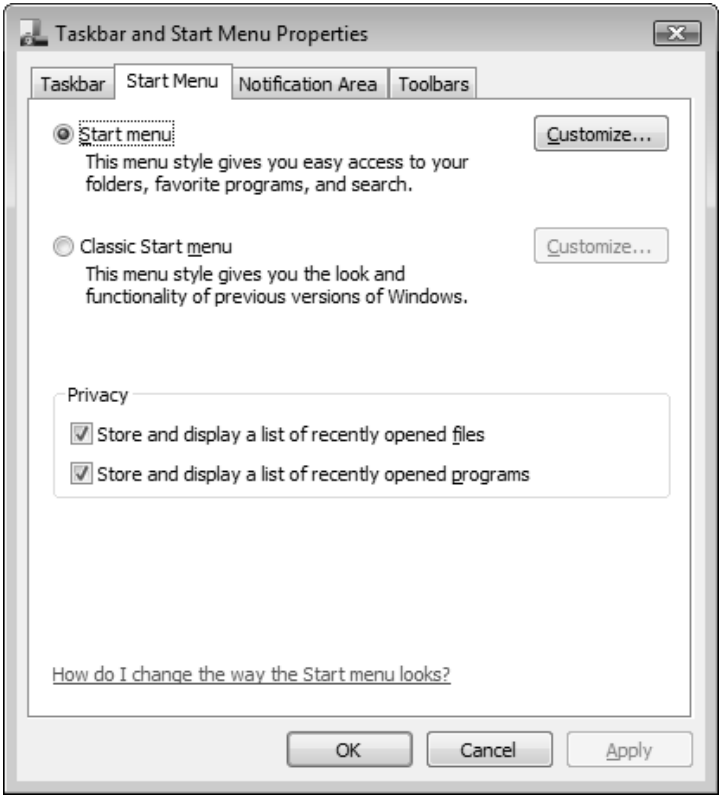


Рис. 2.23. Окно настройки меню **Пуск**

Внимание!

Для выбора классического вида меню **Start** (Пуск) следует установить переключатель **Classic Start menu** (Классическое меню "Пуск"). В этом случае меню будет выглядеть как в системах Windows 2000 и более ранних версиях (см. рис. 2.21). Настройка классического меню **Start** (Пуск) производится с помощью кнопки **Customize** (Настроить), расположенной справа от названного переключателя.

3. Нажмите кнопку **Customize** (Настроить). В появившемся окне (рис. 2.24) можно настроить каждый элемент меню **Start** (Пуск), указать количество

отображаемых в меню значков часто используемых программ, а также выбрать программы, которые будут применяться для работы с Интернетом и электронной почтой.

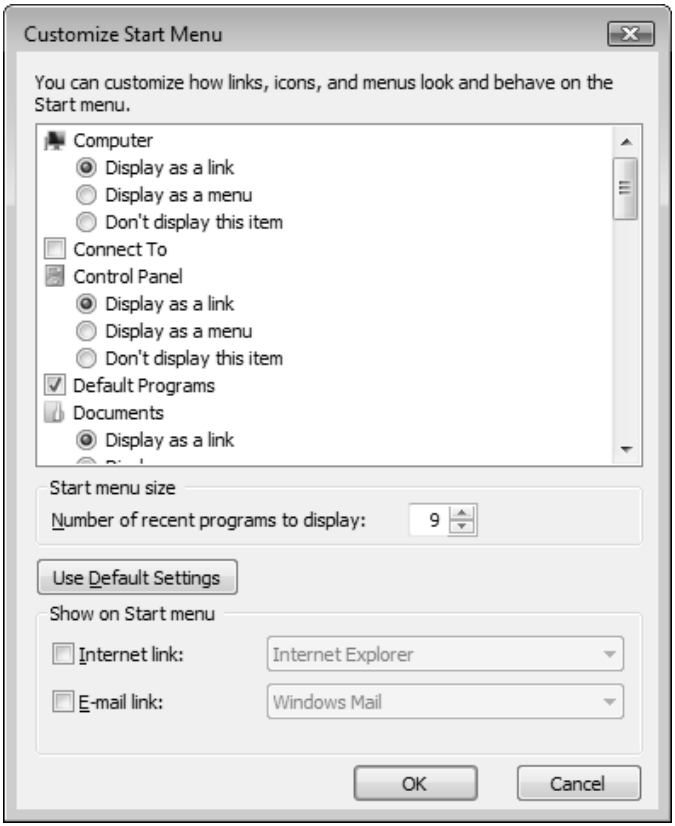


Рис. 2.24. В этом окне выбираются отображаемые элементы меню **Start**

4. В списке элементов меню **Start** (Пуск) для многих элементов предлагаются три опции:

   - **Display as a link** (Отображать как ссылку) — отображать как ссылку на папку (по умолчанию);
   - **Display as a menu** (Отображать как меню) — отображать как меню. Это очень удобно для быстрого доступа к любому объекту данного элемента (например, при выборе этой опции для панели управления

(Control Panel) легко непосредственно обращаться к нужным настройкам);

- **Don't display this item** (Не отображать этот элемент) — элемент не отображается.

Внимание!

В списке опций настройки меню **Start** (Пуск) (см. рис. 2.24) обратите особое внимание на флажок выбора размера значков, отображаемых в меню, флажок включения/отключения сортировки элементов меню по именам (по умолчанию все названия команд в меню сортируются), флажок команды **Run** (Выполнить) и опции поиска.

Окно тонкой настройки *классического* меню **Start** (Пуск) изображено на рис. 2.25. Обратите внимание на наличие кнопки сортировки (**Sort**) — с ее помощью можно упорядочить элементы меню.

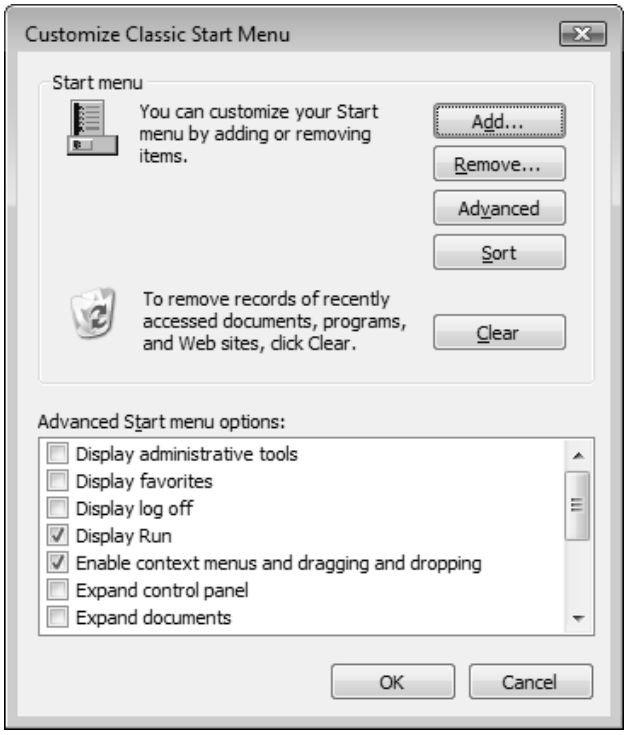


Рис. 2.25. Настройка опций классического меню **Start**

Для того чтобы ускорить обращение к программам, с которыми часто приходится работать, нужно выполнить следующую операцию:

1. Щелкните по имени программы правой кнопкой мыши (значок программы можно выбрать в меню **Start** | **All Programs** (Пуск | Все программы), в окне Проводника (Windows Explorer) или на рабочем столе).
2. В контекстном меню выберите команду **Pin to Start Menu** (Закрепить в меню "Пуск").

Теперь значок программы будет всегда находиться в верхней части левой половины меню **Start** (Пуск) (см. рис. 2.17), и часто используемую программу можно будет запускать, щелкнув мышью по ее названию. (Аналогичную задачу решает панель быстрого запуска (Quick Launch), описываемая далее.)

Для удаления ссылки на программу из меню **Start** (Пуск) щелкните по значку программы правой кнопкой мыши и выберите команду **Unpin from Start menu** (Изъять из меню "Пуск").

Настройка панели задач

Окно настройки панели задач (Taskbar) в системах Windows Vista/Windows Server 2008 несколько модифицировано: параметры распределены по четырем вкладкам.

Процедура настройки панели задач выглядит следующим образом:

1. Выберите курсором свободную часть панели задач, щелкните правой кнопкой мыши и в контекстном меню выберите команду **Properties** (Свойства).
2. В открывшемся окне будет выбрана вкладка **Taskbar** (Панель задач) (рис. 2.26).

Рассмотрим назначение флажков, определяющих работу панели управления.

- **Lock the taskbar** (Закрепить панель задач). На эту команду следует обратить внимание, если в процессе работы размеры панели задач меняются, и это нежелательно для пользователя. При установке флажка панель задач всегда будет видна на экране, и ее высоту нельзя изменить. Нельзя будет менять и размер панелей инструментов, если таковые имеются на панели задач.
- **Auto-hide the taskbar** (Автоматически скрывать панель задач). Панель задач будет автоматически исчезать с экрана и появляться только при перемещении курсора к нижней кромке экрана — это позволяет увеличить

площадь окон запущенных приложений и не отвлекаться при работе с программами.

Рис. 2.26. Окно настройки панели задач и меню **Start**

- **Keep the taskbar on the top of other windows** (Отображать панель задач поверх остальных окон). При установленном флажке панель задач всегда видна, и ее не могут перекрыть открытые окна приложений.
- **Group similar taskbar buttons** (Группировать сходные кнопки панели задач). При большом количестве запущенных одновременно однотипных приложений (например, при редактировании множества документов или картинок) панель задач оказывается заполненной ссылками на работающие программы, что может мешать быстрому выбору нужной программы. При установке данного флажка начинает работу механизм группирования задач.

Когда панель задач полностью заполняется, система начинает группировать открытые файлы по приложениям. Например, если одновременно редактируется четыре картинки, то на панели задач будет присутствовать только одна кнопка программы Paint. Если флажок **Show windows previews (thumbnails)** (Отображать образцы окон (эскизы)) установлен, то при *наведении курсора* на кнопку будет отображаться миниатюрное изображение окна запущенной программы, а также будет указано число работающих копий этой программы (рис. 2.27). Если *щелкнуть* по кнопке, то раскроется список открытых документов, а при выборе некоторой строки в этом списке появится эскиз окна соответствующей копии программы (рис. 2.28). Такой механизм упрощает выбор окон при большом количестве работающих экземпляров приложения.

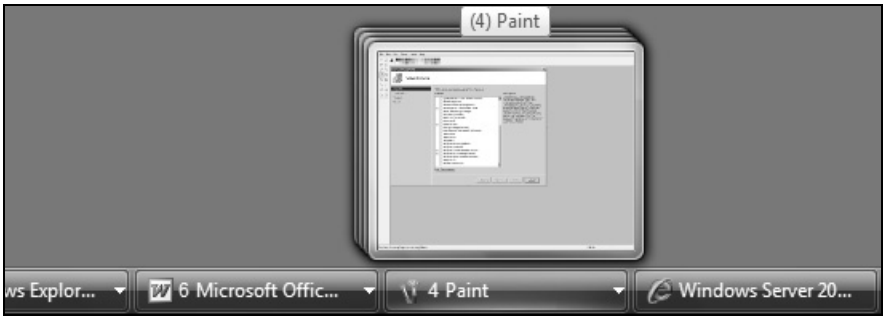


Рис. 2.27. Группирование эскизов экранов однотипных документов на панели задач

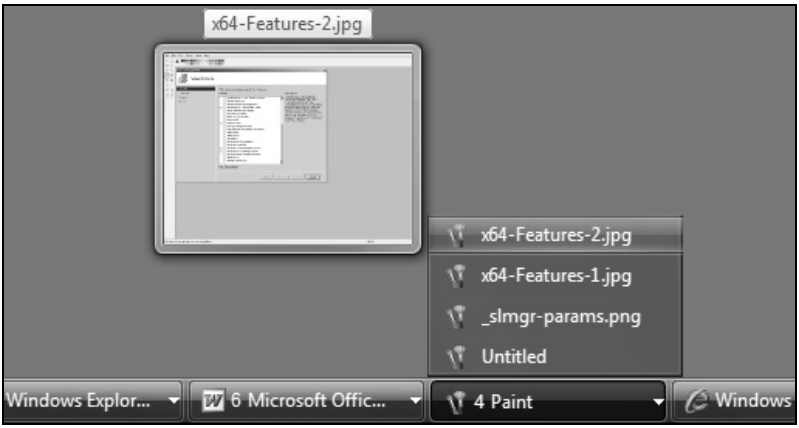


Рис. 2.28. Список однотипных документов на панели задач и эскиз выбранного документа

Группу файлов можно закрыть одним щелчком мыши. Для этого щелкните по группе правой кнопкой мыши и выберите команду **Close Group** (Закрыть группу).

Внимание!

Функция отображения образцов окон (эскизов) (Thumbnails) работает только при выборе стиля Windows Aero (с включенной функцией Aero Glass). В остальных случаях вместо эскиза отображается только название приложения *(см. далее разд. "Переключение задач")*.

Настройка области уведомлений

На вкладке **Notification Area** (Область уведомлений) (рис. 2.29) в окне **Taskbar and Start Menu Properties** (Свойства панели задач и меню "Пуск")

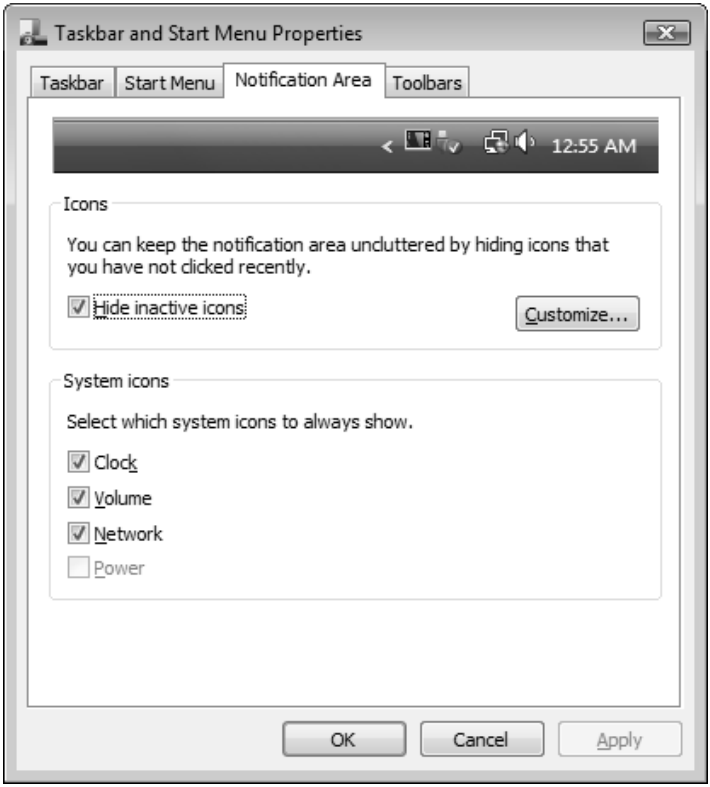


Рис. 2.29. Окно настройки значков в области уведомлений на панели задач

можно настраивать отображение значков в области *системных уведомлений* (system tray) на панели задач. Эти значки служат для управления различными системными сервисами, а также запущенными приложениями.

В данной области могут, например, находиться значки регулятора громкости, индикатора раскладки клавиатуры, индикатора сетевых подключений, часов и т. д. При наличии большого количества программ, имеющих значки в области уведомлений, панель задач может оказаться сильно перегруженной.

Для освобождения свободного места на панели задач редко используемые значки можно скрывать. Для этого нужно установить флажок **Hide inactive icons** (Скрывать неиспользуемые значки). После этого область системных значков будет находиться в "минимизированном" состоянии, отображая только задействованные значки. Открыть область целиком можно, щелкнув по кнопке со стрелкой (<).

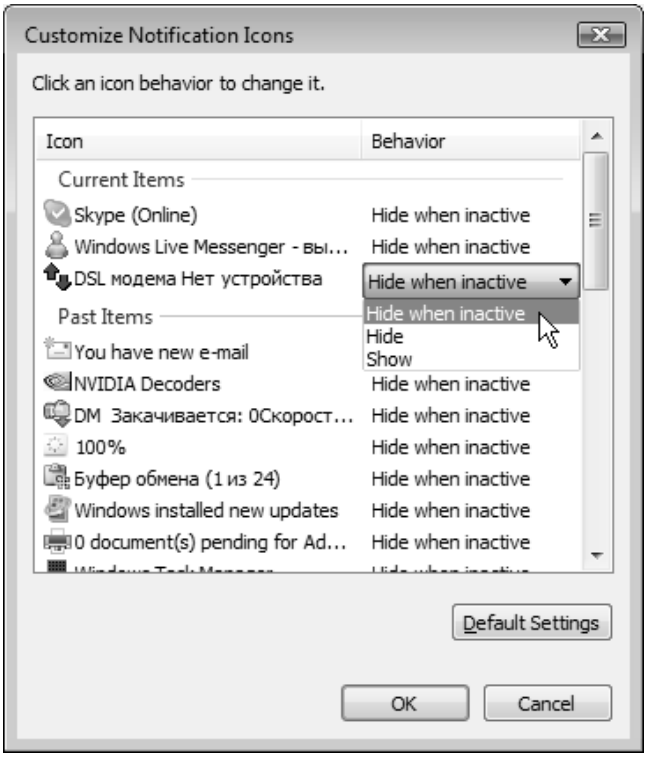


Рис. 2.30. Окно настройки отображения системных уведомлений на панели задач

Если неиспользуемые значки скрываются, то для настройки поведения системных уведомлений можно нажать кнопку **Customize** (Настроить) (см. рис. 2.29). В окне **Customize Notification Icons** (Настройка значков уведомлений) (рис. 2.30) можно выбрать режим отображения уведомлений (колонка **Behavior** (Поведение)) — указать нужную опцию для выбранного значка.

Настройка и синхронизация системных часов

Во всех системах Windows в правом углу на панели задач обычно находятся часы, показывающие текущее время.

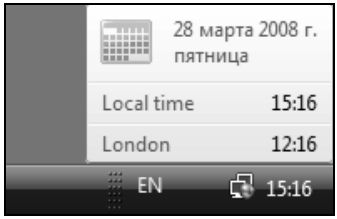


Рис. 2.31. Отображение системного времени для локального и дополнительного часовых поясов

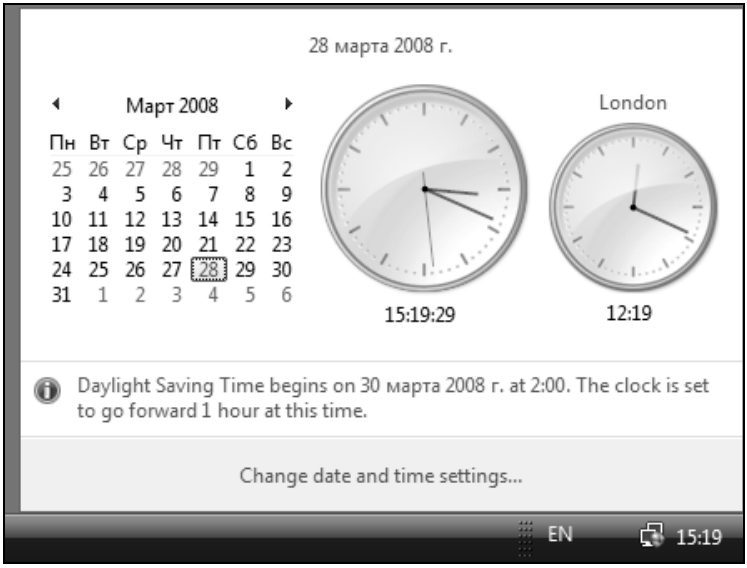


Рис. 2.32. Календарь и часы для локального времени и дополнительного часового пояса

Показания этих часов основаны на данных системных часов компьютера. Однако эти данные не всегда являются достоверными, и системные часы могут показывать неверное время. Если компьютер является членом домена, то системные часы автоматически синхронизируются со временем контроллера домена. Для автономного компьютера часы можно синхронизировать через Интернет.

Если *щелкнуть мышью* по показаниям часов, то календарь и часы отображаются полностью (рис. 2.32). Чтобы настроить календарь и часы, следует щелкнуть по ссылке **Change date and time settings** (Изменение настройки даты и времени). В окне **Date and Time** (Дата и время) (рис. 2.33) можно настроить все необходимые параметры.

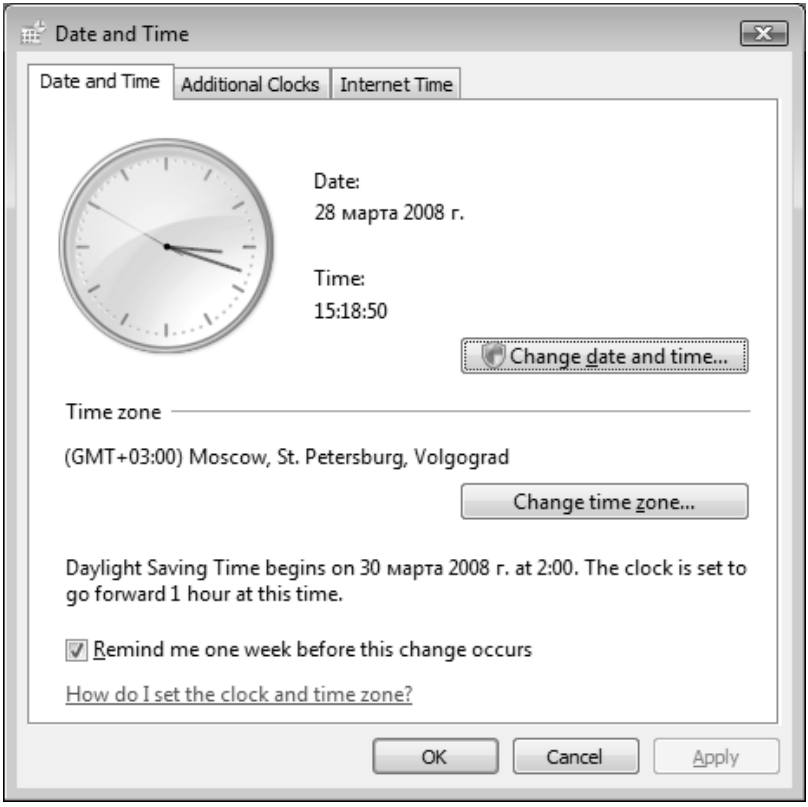


Рис. 2.33. Окно настройки календаря и часов

В системах Windows Vista/Windows Server 2008 функции отображения системного времени дополнены новыми возможностями. Если *задержать кур-*

cop на показаниях часов на панели задач, то отображается окно, в котором показаны текущая дата и системное время, при этом имеется возможность использования дополнительных часов для других часовых поясов (рис. 2.31) (таких часов может быть двое).

Дополнительные часы включаются и настраиваются на соответствующей вкладке — **Additional Clocks** (рис. 2.34) — необходимо лишь разрешить их отображение и выбрать часовой пояс (а также ввести отображаемое название).

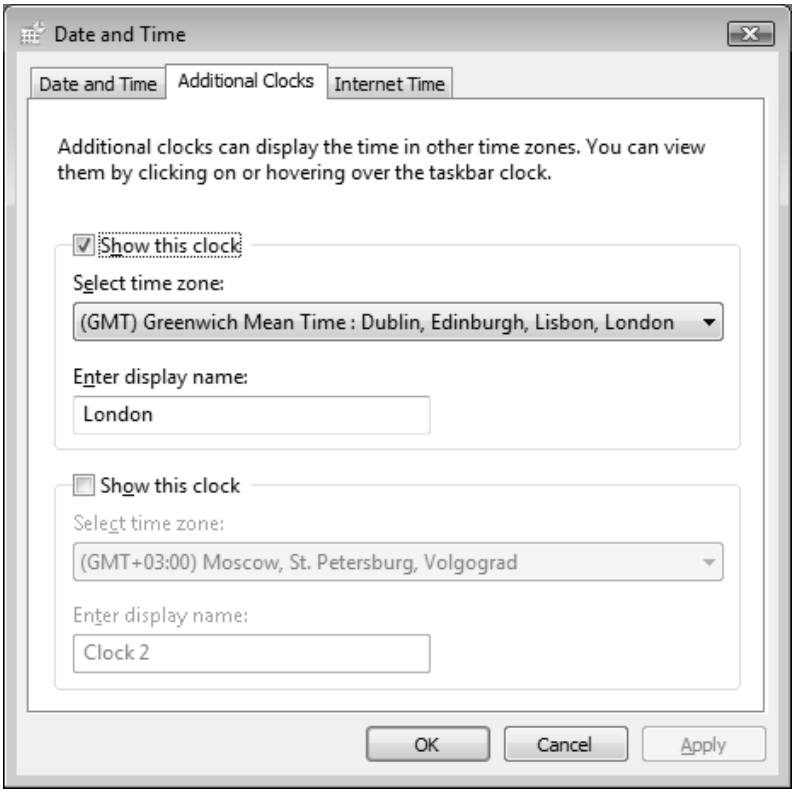


Рис. 2.34. Включение и настройка дополнительных часов для других временных поясов

Чтобы настроить параметры синхронизации времени с Интернетом, выполните следующие действия:

1. В окне **Date and Time** (Дата и время) (см. рис. 2.33) перейдите на вкладку **Internet Time** (Время Интернета).

2. Щелкните по ссылке **Change Settings** (Изменить параметры).
3. В окне **Internet Time Settings** (Настройка времени Интернета) (рис. 2.35) установите флажок **Synchronize with an Internet time server** (Синхронизация с сервером времени в Интернете).

Рис. 2.35. Окно настройки параметров синхронизации часов через Интернет

4. В списке **Server** (Сервер) выберите сервер времени, который будет использоваться для синхронизации. Если имя нужного сервера времени отсутствует в списке, его можно ввести с клавиатуры. Синхронизация часов проходит только с серверами, использующими протокол SNTP. Сервер time.windows.com управляется корпорацией Microsoft, другие серверы контролируются правительственными организациями.
5. Нажав кнопку **Update Now** (Обновить сейчас), можно осуществить внеплановую синхронизацию времени.
6. Для сохранения изменений нажмите кнопку **OK**.

Внимание!

Вкладка **Internet Time** (Время Интернета) присутствует в окне настроек времени, только если компьютер не входит в состав домена Windows (и не является контроллером домена). В доменах синхронизация часов выполняется от контроллера домена, и их ручная корректировка невозможна.

Встроенные и пользовательские панели инструментов

Помимо стандартной панели задач (расположенной в нижней части рабочего стола), имеется несколько встроенных *панелей инструментов* (toolbars), которые могут помещаться только на панели задач (а не в любом месте рабочего стола, как это было в Windows XP/Windows Server 2003). Чтобы открыть дополнительные панели инструментов, щелкните правой кнопкой мыши на панели задач и в контекстном меню выберите подменю **Toolbars** (Панели) (рис. 2.36). Здесь перечислены все стандартные панели инструментов, а также те, которые создал сам пользователь. Выберите любую панель, и она сразу же появится на панели задач (выбранные панели отмечаются галочкой).

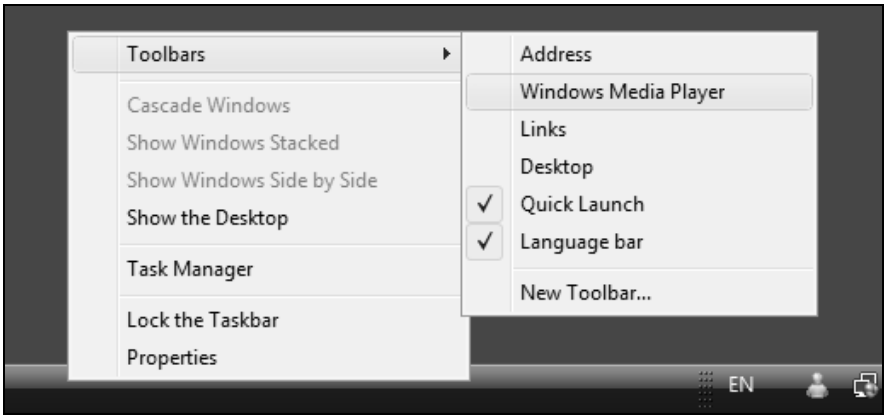


Рис. 2.36. Включение и выключение отображаемых панелей

Внимание!

Концепция панелей инструментов в Windows Vista/Windows Server 2008 заметно изменилась по сравнению с Windows XP/Windows Server 2003. Теперь любую панель инструментов нельзя свободно перемещать по экрану: одни панели (см. рис. 2.36) могут находиться только на панели задач, а другие — на рабочем столе (как автономные окна или панели, закрепленные у края экрана слева, вверху или справа).

Также панели можно включать и отключать, открыв окно **Taskbar and Start Menu Properties** (Свойства панели задач и меню "Пуск") и перейдя на вкладку **Toolbars** (Панели инструментов) (рис. 2.37), где перечислены все стан-

дартные и пользовательские (если таковые имеются) панели инструментов. Обратите внимание на флажок **Windows Media Player** (Проигрыватель Windows Media) — если он установлен, то при сворачивании окна проигрывателя Windows Media Player на панели задач будет появляться маленькая панель, позволяющая осуществлять операции по управлению воспроизведением музыки (пуск, стоп, вперед, назад и т. п.).

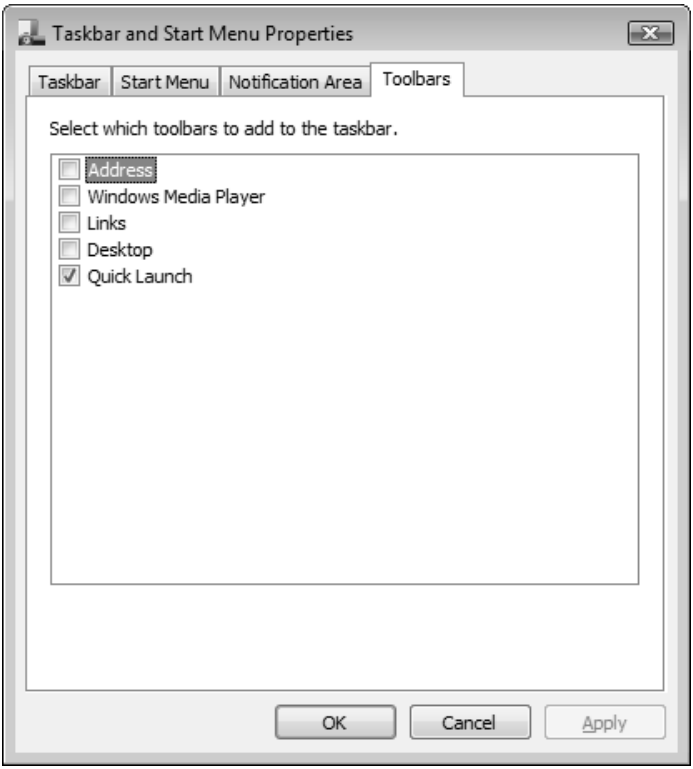


Рис. 2.37. Выбор панелей инструментов

Встроенные панели облегчают работу, поскольку позволяют быстро выполнять необходимые задачи: открывать рабочий стол, запускать наиболее часто используемые программы или загружать сайты из Интернета. Например, с помощью панели **Quick Launch** (Быстрый запуск) (рис. 2.38) можно быстро свернуть все окна (кнопка **Show desktop** (Свернуть все окна)[1]), переключить-

[1] Эта кнопка отсутствует при использовании классического стиля оформления.

ся в окно нужной программы *(см. далее)* или запустить браузер Internet Explorer. На эту панель можно также поместить ярлыки других программ.

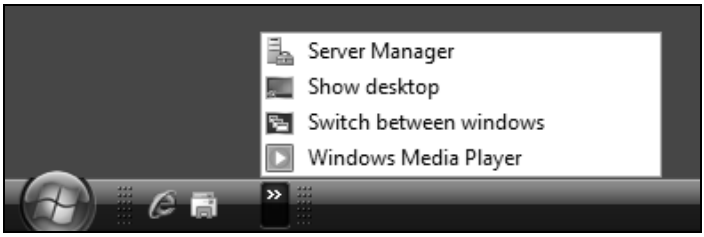


Рис. 2.38. Панель быстрого запуска позволяет ускорить запуск часто используемых программ

Для того чтобы получить возможность вызова программ с панели быстрого запуска, достаточно перетащить значок программы (или ссылку в меню **Start** (Пуск)) на эту панель. Имеется и другое решение: нужно выбрать программу в меню **Start** (Пуск) и в контекстном меню выполнить команду **Add to Quick Lunch** (Добавление на панель быстрого запуска).

Помимо стандартных панелей инструментов можно создавать и использовать собственные. В системах Windows Vista/Windows Server 2008 для этого имеются две возможности: пользовательская панель может находиться либо на панели задач, либо на рабочем столе (у кромки экрана или в произвольном месте).

Для добавления новой панели, *отображаемой на панели задач*, щелкните правой кнопкой мыши на панели задач и в контекстном меню выберите команду **Toolbars** | **New Toolbar** (Панели | Создать панель инструментов) (см. рис. 2.36). В открывшемся диалоговом окне **New Toolbar** (Новая панель) будет предложено выбрать любую папку из числа имеющихся на диске. Ссылки на файлы (папки) из указанной папки и станут содержанием новой панели.

Чтобы создать панель, *отображаемую на рабочем столе*, проделайте следующие операции:

1. В окне Проводника выберите нужную папку, щелкните правой кнопкой мыши и в контекстном меню выполните команду **Send To** | **Desktop (create shortcut)** (Отправить | Рабочий стол (создать ярлык)).
2. Появившийся на рабочем столе ярлык папки перетащите к самой кромке экрана (по выбору — левой, верхней или правой).

3. Отрегулируйте ширину панели, захватывая мышью ее *свободный* край (при этом вместо курсора отображается двунаправленная стрелочка); выберите в контекстном меню параметры отображения панели: наличие подписей и заголовка и т. д.

Панель может автоматически убираться с экрана (опция **Auto-Hide**), если она не используется (при перемещении курсора к краю она снова появляется). Если установлен флажок **Always on Top** (Поверх остальных окон), то панель уменьшает площадь рабочего стола и все значки и открытые окна сдвигаются в сторону (опция автоматического скрытия панели должна при этом быть выключена). В противном случае панель просто отображается поверх других окон и под нее могут попасть значки и часть открытых окон программ.

Если созданную панель нужно свободно перемещать по рабочему столу, то необходимо навести курсор на ту часть рамки окна, которая прилегает к кромке экрана, щелкнуть левой кнопкой мыши и потянуть панель в нужную сторону рабочего стола. При этом окно панели инструментов из прикрепленного превращается в автономное.

Чтобы совсем удалить пользовательскую панель с рабочего стола, нужно выполнить команду **Close Toolbar** (Закрыть панель инструментов).

Пользовательские панели инструментов не отображаются в списке панелей, который открывается с панели задач (см. рис. 2.36). Однако команда **Toolbars** (Панели), имеющаяся в контекстном меню пользовательской панели, позволяет видеть перечень *всех* панелей инструментов: и созданных на рабочем столе, и имеющихся на панели задач.

Просмотр объектов файловой системы, локальных и сетевых ресурсов

Для просмотра файлов и папок, хранящихся на компьютере или в общих сетевых папках, используется традиционная для всех систем Windows программа Windows Explorer (Проводник), которую можно вызывать непосредственно или открывая папки **Computer** (Компьютер), **Documents** (Документы) и другие папки, доступ к которым можно получить из меню **Start** (Пуск) (см. рис. 2.17) или с рабочего стола. В системах Windows Vista/Windows Server 2008 программа Windows Explorer (Проводник) существенно модифицирована и имеет много новых функций, которые будут подробно описаны ниже.

Папка **Computer** (Компьютер) позволяет просматривать жесткие и сменные диски компьютера, а также сетевые ресурсы. Все файлы пользователя по умолчанию сохраняются в папке **Documents** (Документы). Для хранения графических, звуковых и видеофайлов предусмотрены специальные папки **Pictures** (Изображения) и **Music** (Музыка). Папка **Network** (Сеть) позволяет просматривать сетевые ресурсы (компьютеры, совместно используемые диски, папки и принтеры). Все личные пользовательские папки хранятся в профиле пользователя, они недоступны для других пользователей системы *(см. далее разд. "Профили пользователей и виртуальные папки")*.

Программа Windows Explorer (Проводник) и ее новые возможности

Программа Windows Explorer (Проводник) является универсальным средством систем Windows для работы с объектами файловой структуры локального компьютера или общими сетевыми ресурсами. Ее можно запустить из меню **Start** (Пуск), хотя проще одновременно нажать клавиши <Win>+<E>.

В системах Windows Vista/Windows Server 2008 интерфейс программы заметно изменился, как изменились и способы выполнения многих операций с папками и файлами. Тем не менее, базовая идеология "копировать-и-вставить" (copy-and-paste) осталась незыблемой, как и многие другие основополагающие концепции оконного интерфейса Windows.

Работа с компакт-дисками (CD и DVD)

Поскольку в системах имеется встроенная поддержка записываемых CD- и DVD-дисков, операции копирования информации на диск можно выполнять непосредственно из окна программы Windows Explorer (Проводник). Все вопросы, связанные с режимами и возможностями записи на CD- и DVD-диски, подробно рассматриваются в *главе 6*.

Окно программы Windows Explorer (Проводник) (рис. 2.39) — как и в предыдущих версиях Windows — делится на две части: слева отображается древовидный список ресурсов (он называется *Navigation Pane* (Панель навигации)), а справа — *содержимое* выбранного объекта: компьютера, диска или папки. Обратите внимание на то, что в структуре локальных папок вместо традиционной папки **My Documents** (Мои документы) отображается папка с именем зарегистрированного пользователя (в нашем примере — Administrator) — в этой папке и находится вся личная информация (документы, изображения и т. д.).

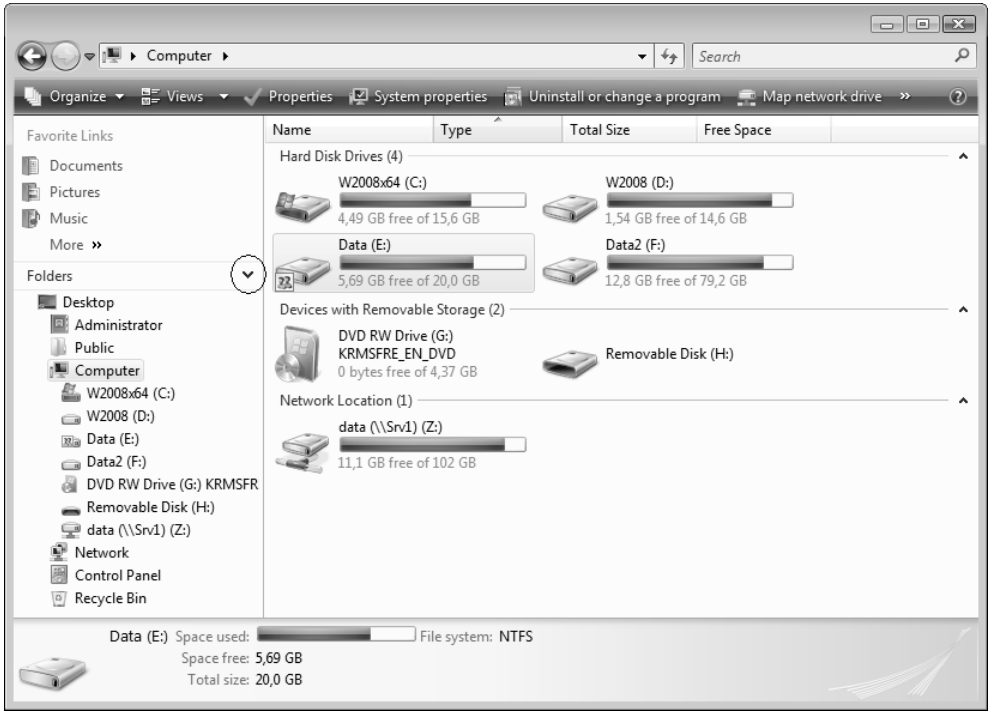


Рис. 2.39. Окно программы Windows Explorer, в котором отображаются локальные ресурсы компьютера и подключенные устройства

На панели навигации, в свою очередь, располагаются *панель избранных ссылок* (Favorite Links; работа с этой панелью описывается далее, в разделе, посвященном концепции виртуальных папок) и *панель папок* (Folders). Границу между этими панелями можно передвигать мышью, а можно вообще закрыть одну из панелей, сдвинув границу вверх или вниз до конца. Щелкнув по заголовку панели со стрелочкой, панель можно быстро закрыть или, наоборот, раскрыть.

Рассмотрим подробнее главные особенности нового дизайна программы Windows Explorer (Проводник) и начнем описывать окно сверху вниз.

Поле адреса

В строке адреса (поле выбранной папки) реальное имя папки (включающее имя диска, символы наклонной черты и имена родительских папок) "скрыва-

ется" и вместо него названия отображаются как цепочка объектов. Очень удобно то, что, щелкнув *по стрелке* справа от названия папки, можно раскрыть список вложенных объектов. Например, если выполнить эту операцию для объекта **Computer** (Компьютер), можно получить список локальных и подключенных дисков (рис. 2.40). Щелкнув *по самому имени* папки, мы увидим ее содержимое. Таким образом, строка адреса совмещает в себе сразу несколько возможностей древовидного списка: непосредственно видны родительские объекты выбранной папки, а можно также увидеть все дочерние объекты на любом вышестоящем уровне и сразу выбирать их.

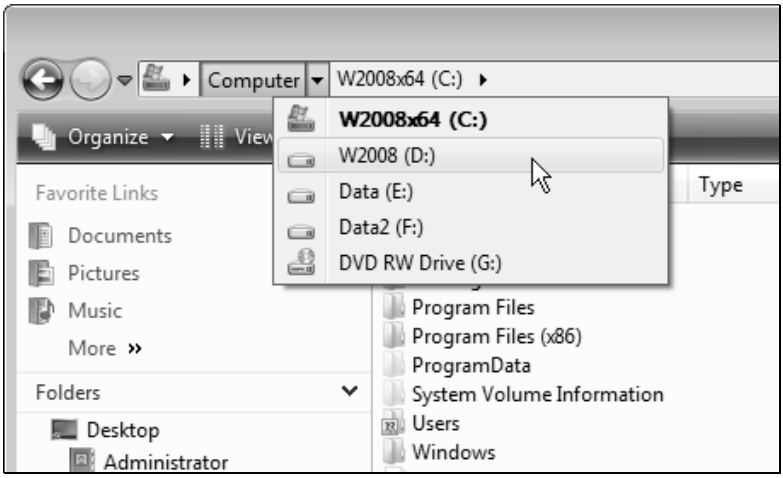


Рис. 2.40. Вид иерархии папок в поле адреса

Чтобы в поле адреса увидеть реальное физическое имя папки, нужно щелкнуть мышью в свободной части этого поля. Тогда все графические элементы пропадут, и появится традиционное имя типа C:\Users\Administrator\AppData\Roaming\Microsoft\Windows (см. пример на рис. 2.68).

Внимание!

Слева от поля адреса находятся кнопки перехода вперед и назад, позволяющие возвращаться к уже просмотренным папкам (контейнерам). Кнопка перехода на один уровень вверх (к родительской папке) теперь отсутствует; эту операцию можно выполнять, одновременно нажимая клавиши <Alt>+ +<Стрелка вверх>.

Поле поиска

Традиционное для многих окон, имеющихся в интерфейсе систем Windows Vista/Windows Server 2008, поле поиска в правом верхнем углу программы позволяет выполнять поиск в текущей выбранной папке (эту операцию мы подробно рассмотрим далее). Поиск начинается с момента ввода первого символа, и результаты операции обновляются при вводе каждого следующего символа. Помимо поля поиска, в окне программы Windows Explorer (Проводник) может отображаться еще и *панель* поиска *(см. далее)*, на которой можно указывать тип файлов, которые будут выбираться для поиска.

Классическое меню

Во всех приведенных выше примерах в окне программы Windows Explorer (Проводник) отсутствует классическое меню (хотя по умолчанию оно отображается — *см. разд. "Настройка вида папок"*), поскольку теперь необходимость в нем возникает очень редко. В тех случаях, когда требуются специфические команды, выполняемые с помощью меню, это меню можно на время включить, нажав клавишу <Alt> (при повторном нажатии меню исчезает)[1]. На рис. 2.41 можно видеть, как в окне программы появляется дополнительная строка меню (подменю **File**, **Edit**...).

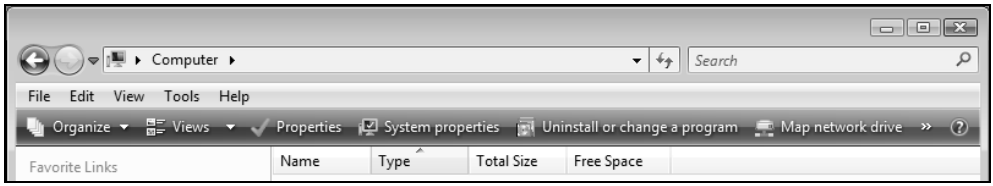


Рис. 2.41. Отображение классического меню в окне программы Windows Explorer

Панель поиска

Специальная *Панель поиска* (Search Pane) отображается, если в окне программы Windows Explorer (Проводник) папки **Computer** (Компьютер) выполнить команду **Layout** | **Search Pane** (Раскладка | Панель поиска) в меню

[1] Аналогичным образом отображением классического меню можно управлять и в программе Internet Explorer 7.0, в окне панели управления, в Центре управления сетями и т. д.

Organize (Упорядочить). На этой панели (рис. 2.42) можно выбирать тип просматриваемых файлов при выполнении поиска, а также включить функцию расширенного поиска. Данная панель всегда присутствует в стандартном окне поиска или появляется при выборе операции расширенного поиска *(см. далее разд. "Средства поиска информации, хранящейся на сервере")*.

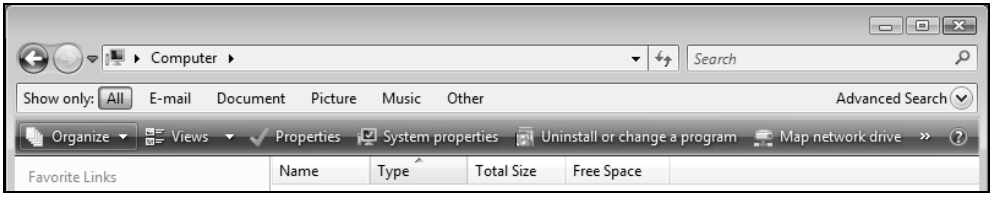


Рис. 2.42. Панель поиска

Панель задач программы Windows Explorer

В новой версии программы Windows Explorer (Проводник) отсутствует боковая панель, существующая в системах Windows XP/Windows Server 2003 (на этой панели, которая может отображаться слева вместо панели **Folders** (Папки), перечисляются типовые задачи, имеющиеся для выбранной папки). Вместо боковой панели появилась *панель задач*, располагающаяся под панелями адреса и поиска; ее функции такие же, как и у боковой панели Windows XP/Windows Server 2003.

Набор задач, присутствующих на панели задач программы Windows Explorer (Проводник), меняется в зависимости от выбранного объекта. Например, на рис. 2.41 можно видеть панель задач при выборе папки **Computer** (Компьютер). Панели задач для других окон, операций или типов файлов можно видеть в разных главах книги, например, задачи для окна поиска — см. рис. 2.52.

Специальные панели просмотра

Имеются две совершенно новых панели программы Windows Explorer (Проводник), которые появились в Windows Vista/Windows Server 2008: *Details Pane* (Панель подробностей) и *Preview Pane* (Панель просмотра). Для управления ими используются команды в меню **Organize** | **Layout** (Упорядочить | Раскладка) (см. рис. 2.43).

Внимание!

Для того чтобы эти панели были доступны, в окне свойств папок должен быть установлен переключатель **Show preview and filters** (Отображать образцы и фильтры) — *см. далее разд. "Настройка вида папок"*.

Панель просмотра обычно включена и находится в нижней части окна программы (пример можно видеть на рис. 2.39). На ней отображается эскиз страницы (thumbnail) выбранного файла (маленькая картинка) и приводятся свойства файла или объекта (размер, дата создания и изменения, автор, ключевые слова, рейтинг и т. п.). Высоту панели можно плавно менять, "потянув" мышью за верхний край панели.

Примечание

Ниже панели просмотра может отображаться строка состояния (Status Bar). Чтобы ее включить, нужно открыть классическое меню и установить флажок **View | Status Bar** (Вид | Строка состояния).

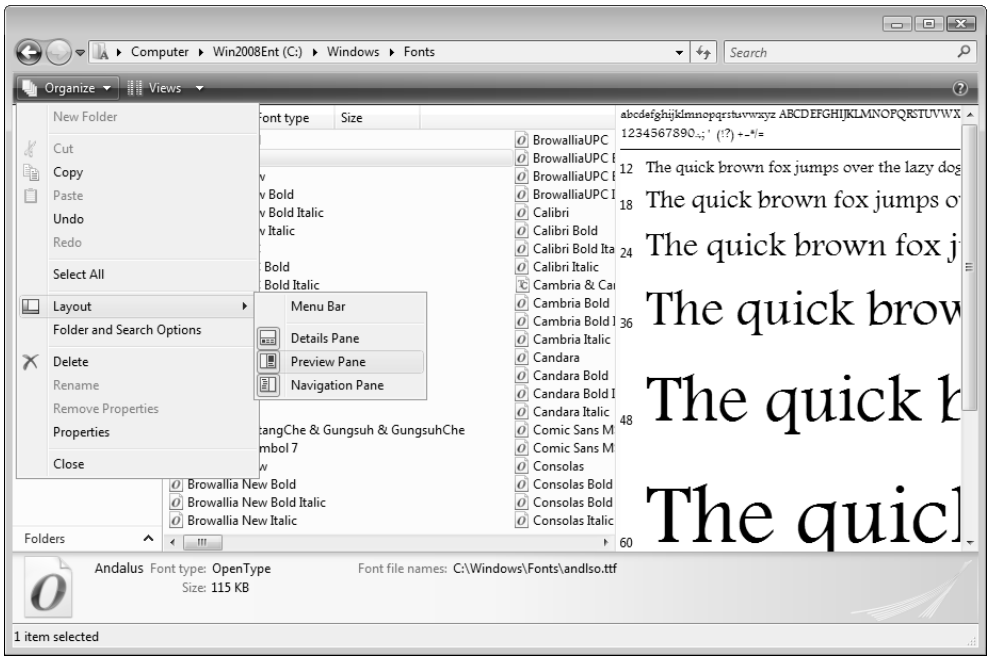


Рис. 2.43. Меню управления панелями программы Windows Explorer и панель просмотра

Панель просмотра отображается в правой части окна программы (ее размер тоже можно менять, перетаскивая границу). На этой панели в увеличенном масштабе показано содержимое выбранного файла — это может быть текст, картинка, аудио- или видеоклип. Для двух последних имеется возможность непосредственного воспроизведения. На рис. 2.43 в качестве примера показана панель просмотра, на которой отображаются образцы выбранного шрифта; также можно видеть меню, позволяющее включать и отключать панели программы Windows Explorer (Проводник).

Вид содержимого папки

Режим просмотра файлов и подкаталогов в выбранной папке можно установить с помощью команд меню **Views** (Виды) (рис. 2.44). Это меню имеет три основных фиксированные опции — **Tiles** (Плитка), **Details** (Таблица) и **List** (Список), а также несколько опций отображения значков файлов (Icons). С помощью ползунка в меню **Views** (Виды) размер значков можно менять плавно, выбирая оптимальный вид для конкретного случая. Особенно это полезно, если просматриваемая папка содержит графические файлы и нужно видеть их эскизы (thumbnails). При выборе для папок крупных и огромных значков помимо имени папки можно видеть образцы его содержимого (тексты, картинки и т. д.).

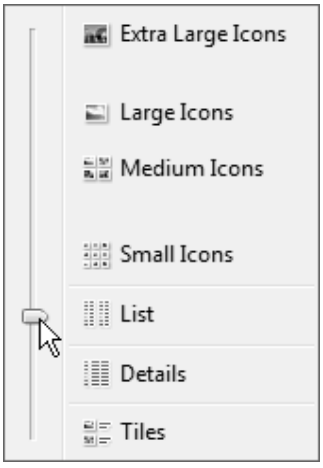


Рис. 2.44. Меню выбора представления файлов и папок при просмотре объектов файловой структуры

Примечание

Если при просмотре папки курсор находится в правой половине окна программы Windows Explorer (Проводник), то для изменения размера значков в окне можно нажать клавишу <Ctrl> и вращать колесико мыши.

Настройка вида папок

Для тонкой настройки способов отображения информации в окне программы Windows Explorer (Проводник) нужно открыть окно **Folder Options** (Свойства папки) (см. рис. 2.46). Параметров, управляющих работой программы, довольно много. Например, по умолчанию не отображаются расширения файлов, скрытые и системные файлы и папки, хотя иногда возникает в этом необходимость. Можно разрешить постоянное отображение классического меню, определить вид для конкретной папки или для однотипных папок и т. д.

Для перехода к окну параметров настройки можно воспользоваться командой **Folder and Search Options** (Свойства папок и поиска) в меню **Organize** (Упорядочить) (см. рис. 2.43) или же, открыв классическое меню, выполнить команду **Folder Options** (Свойства папки) в меню **Tools** (Сервис). Можно также открыть панель управления и выполнить задачу **Folder Options** (Свойства папки) (категория **Appearance and Personalization** (Оформление и персонализация)). Для прямого доступа к окну свойств папки служит командная строка `rundll32 shell32,Options_RunDLL`.

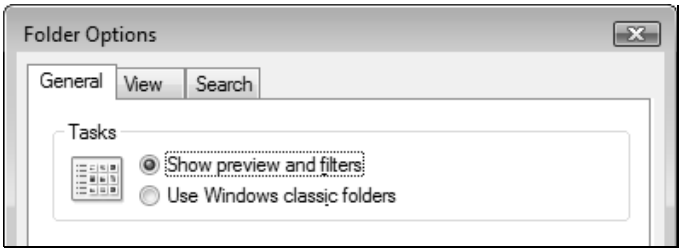


Рис. 2.45. Переключатели, определяющие общий вид панелей программы Windows Explorer

В окне **Folder Options** (Свойства папки) важные переключатели имеются на вкладке **General** (Общие) в группе **Tasks** (Задачи) (рис. 2.45). По умолчанию установлен переключатель **Use Windows classic folders** (Использовать обычные папки Windows). В этом случае в окне программы Windows Explorer (Проводник) и других системных окнах всегда присутствует классическое

меню, а специальные панели просмотра недоступны. Переключатель **Show preview and filters** (Отображать образцы и фильтры) позволяет использовать все новые средства программы (при этом отображением классического меню можно управлять с помощью параметра на вкладке **View** (Вид), а дополнительные панели можно включать с помощью флажков в меню **Organize** | **Layout** (Упорядочить | Раскладка)).

На вкладке **View** (Вид) располагаются параметры, определяющие вид объектов файловой системы в окне программы; на рис. 2.46 показаны значения некоторых параметров, заданные по умолчанию.

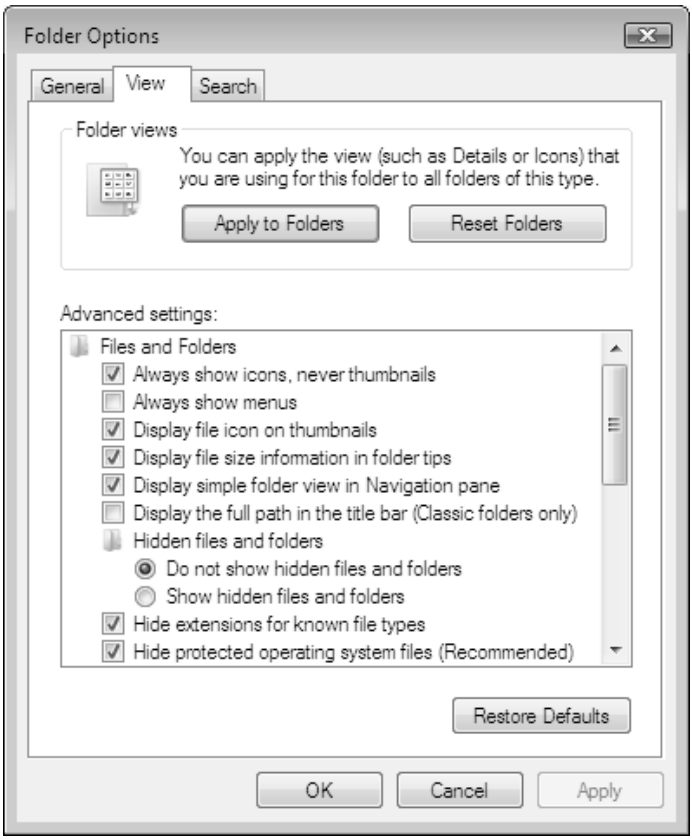


Рис. 2.46. Окно настройки вида папок

Флажок **Always show icons, never thumbnails** (Всегда отображать значки, а не эскизы) в серверных системах установлен — это ускоряет работу системы,

поскольку не требуется генерировать эскизы просматриваемых папок. Эти эскизы не будут отображаться ни в режиме просмотра файлов в основном окне программы, ни на панели подробностей (Details Pane). При частой работе с графическими файлами этот флажок лучше сбросить.

Если установить флажок **Always show menus** (Всегда отображать меню), то классические меню будут всегда отображаться в окне программы Windows Explorer (Проводник) и других системных окнах (на панели управления, в Центре управления сетями и т. д.).

Флажок **Display simple folder view in Navigation pane** (Отображать простой вид папок в списке папок "Проводника") определяет способ отображения структуры папок в окне программы. По умолчанию флажок установлен, и папки располагаются в виде простого списка: возле открытой папки виден черный треугольник; папки, содержащие вложенные папки, отмечены незакрашенной стрелкой. Если флажок сбросить, то помимо названных элементов будут отображаться пунктирные линии, соединяющие папки одного уровня. Иногда такой вид предпочтительнее при просмотре многоуровневых структур с большим числом вложенных папок.

Большое значение для удобства просмотра папок имеет их тип. По умолчанию система автоматически определяет тип папки на основании расширений файлов, содержащихся в этой папке, и в соответствии с типом выбирает стандартный набор столбцов: например, для фотографий важны дата съемки, ключевые слова и оценка, а для документов дата изменения и автор; у аудио- и видеофайлов еще больше параметров.

Тип папки и вид можно задать вручную. Для этого нужно открыть окно свойств папки, перейти на вкладку **Customize** (Настройка) и выбрать тип папки, наиболее подходящий для содержащейся в папке информации (рис. 2.47). Если установить флажок **Also apply this template to all subfolders** (Применять этот же шаблон ко всем подпапкам), то сделанный выбор распространится и на все вложенные папки.

Теперь нужно в меню **Views** (Виды) выбрать наиболее удобный вид содержимого папки, после чего открыть окно **Folder Options** (Свойства папки), перейти на вкладку **View** (Вид) (см. рис. 2.46) и нажать кнопку **Apply to Folders** (Применить к папкам). Теперь все папки, имеющие такой же тип, как и текущая папка (для которой задавался тип), будут иметь одинаковый вид.

Другими словами — настройки внешнего вида папки распространяются только на папки одного типа. В системах Windows Vista/Windows Server 2008 нельзя выбрать один вид папки (например, List (Список)) и применить его ко *всем* папкам локальной системы (как это возможно в Windows XP/Windows Server 2003).

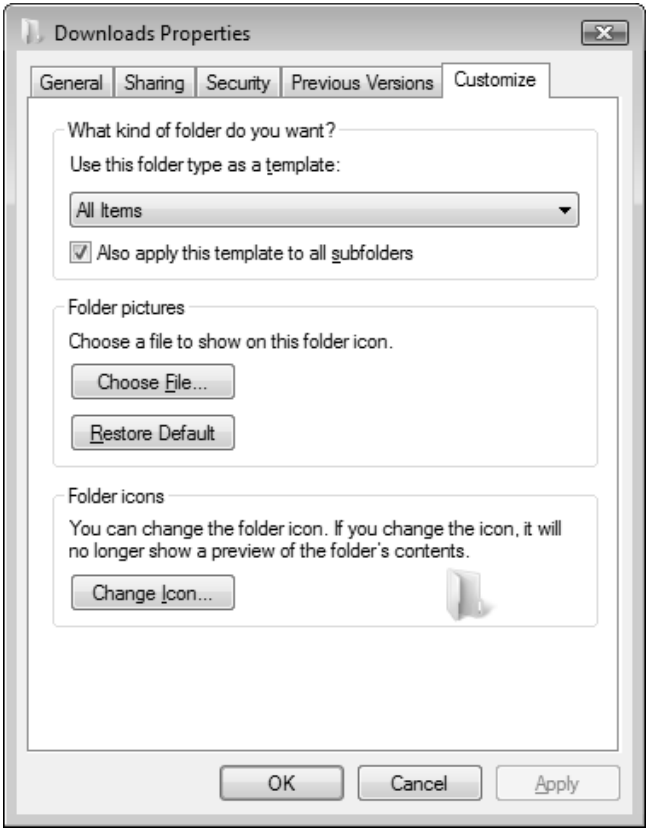


Рис. 2.47. Панель настройки оформления папки

Для папки можно выбрать индивидуальный значок и пиктограмму (icon), которая будет отображаться в режиме обычных, крупных и огромных значков (опции **Choose File** (Выбор файла) и **Change Icon** (Сменить значок)).

Работа с объектами файловой системы в программе Windows Explorer

Программа Windows Explorer (Проводник) в системах Windows Vista/Windows Server 2008 имеет множество новых функций, упрощающих работу с файлами. Рассмотрим их подробнее.

Многие операции с файлами — например, переименование, копирование, удаление и др. — можно отменить, нажав клавиши <Ctrl>+<Z> или выполнив

команду **Undo** (Отменить) в подменю **Edit** (Правка) классического меню программы. Команда **Redo** (Вернуть) позволяет возвратиться к сделанным изменениям (например, если вы переименовали файл и отказались от изменений, то с помощью этой команды можно вернуться к имени, данному в результате переименования).

В окне программы Windows Explorer (Проводник) во всех видах представления файлов постоянно присутствуют названия самых важных атрибутов файлов (рис. 2.48) (список отображаемых столбцов можно менять; он зависит от типа папки — см. рис. 2.47). Это очень удобно для сортировки файлов (не нужно каждый раз переключаться в режим Details (Таблица)) — достаточно щелкнуть мышью по заголовку нужного столбца. Кроме того, легко группировать файлы по выбранному признаку, например, по типу (как показано на рисунке).

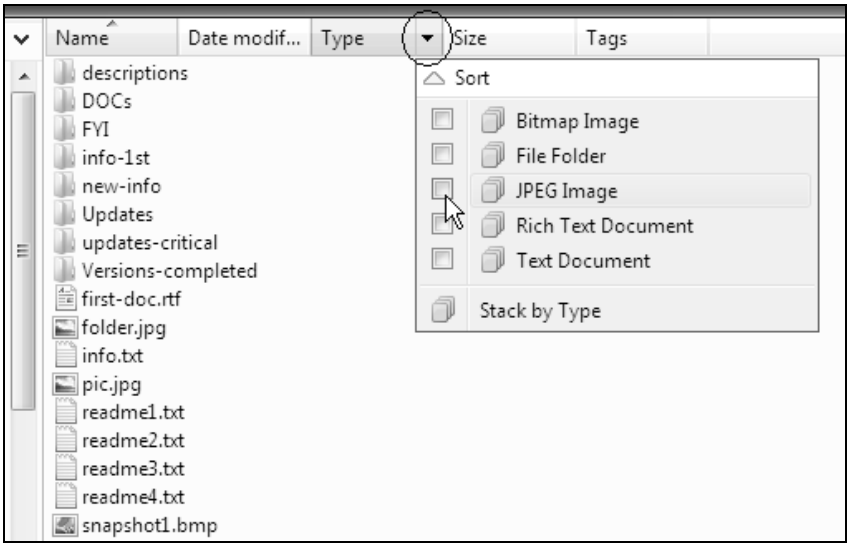


Рис. 2.48. Выбор режима сортировки по типам файлов

Если имена файлов и другие атрибуты достаточно длинные, то в режиме Details (Таблица) они могут обрезаться. Если щелкнуть по любому заголовку столбца таблицы правой кнопкой мыши, то в контекстном меню можно увидеть две команды:

- **Size Column to Fit** (Столбец по размеру содержимого) — расширяет *выбранный* столбец так, чтобы все названия были видны полностью;

- **Size All Columns to Fit** (Все столбцы по размеру содержимого) — расширяет *все* столбцы, позволяя видеть поля целиком.

Также в контекстном меню заголовков столбцов имеются флажки для выбора отображаемых атрибутов — основных и дополнительных.

В программе Windows Explorer (Проводник) изменился интерфейс операций копирования и перемещения файлов, выполняемых с помощью мыши. Всплывающее окно указывает имя выбранной целевой папки, а при одновременном выделении нескольких файлов еще указывается и их число (рис. 2.49). В случае *копирования* файлов около курсора также отображается знак "плюс". Вся эта вспомогательная информация позволяет контролировать правильность выполняемых действий.

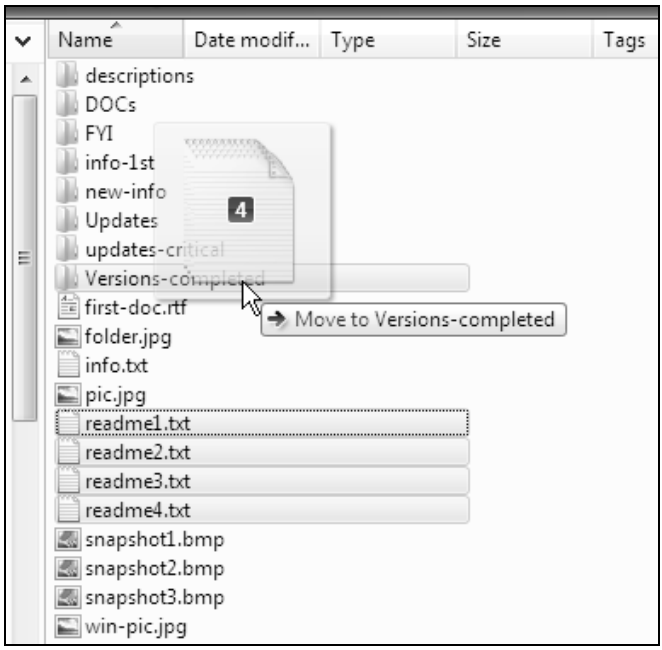


Рис. 2.49. Отображение количества перемещаемых файлов и имени целевой папки

Изменилось окно предупреждения о конфликте имен при копировании файлов. Можно видеть атрибуты файлов и выбрать один из трех вариантов выполнения операции (рис. 2.50). Опция **Don't move** (Не перемещать) имеет смысл для операций с несколькими файлами или папками, для одиночных

объектов она эквивалентна отказу от операции, т. е. нажатию кнопки **Cancel** (Отмена).

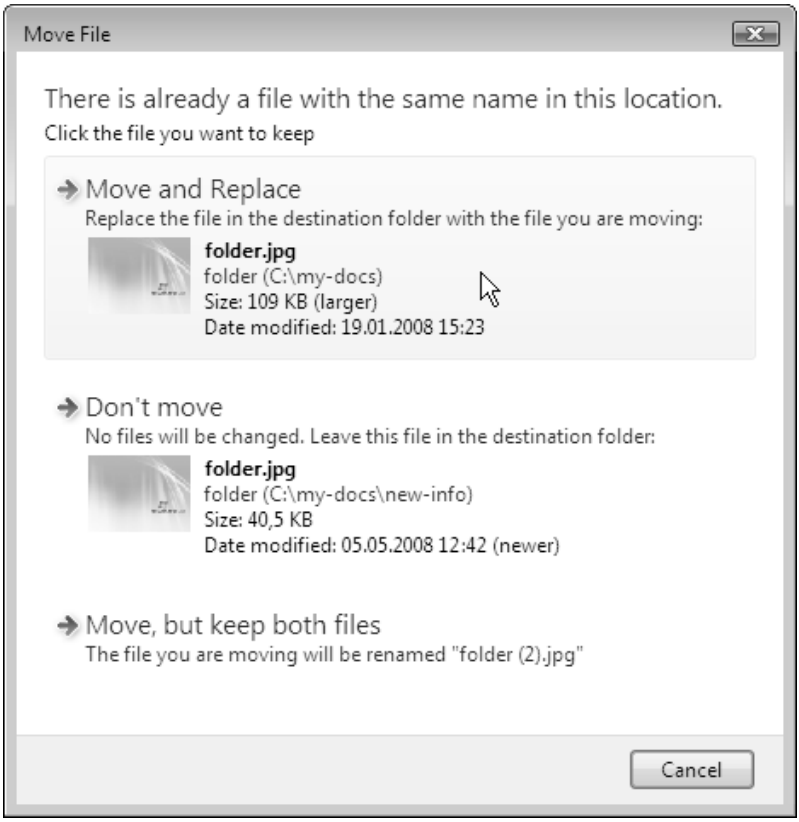


Рис. 2.50. Опции копирования при совпадении имен файлов

Если конфликт возникает при выполнении операции копирования или перемещения *множества* объектов, то в окне предупреждения появляется дополнительный флажок, установив который, можно распространить выбранную опцию на все последующие конфликтующие файлы или папки.

По-новому реализована операция переименования файла: по умолчанию выделяется не все имя, а только основная его часть, без расширения. Вводимые символы заменяют старое имя, не затрагивая тип файла. Это удобно, поскольку уменьшается риск случайного изменения *типа* файла (который не имеет никакого отношения к операции *переименования*).

Для любой папки, выбранной в поле содержимого (в правой половине окна программы Windows Explorer (Проводник)), можно быстро открыть окно командной строки. Для этого нужно, удерживая нажатой клавишу <Shift>, щелкнуть по имени папки правой кнопкой мыши и выбрать в контекстном меню команду **Open Command Window Here** (Открыть окно команд). В открывающемся окне командной строки будет виден полный путь к выбранной папке.

Аналогичным образом можно получить доступ к команде **Copy as Path** (Копировать как путь), позволяющей скопировать в буфер обмена полное физическое имя выбранной папки или файла (включая имя диска и все имена подкаталогов).

Поиск информации, хранящейся на сервере

Средства поиска в системах Windows Vista/Windows Server 2008 обеспечивают поиск данных любого типа и по любым критериям — как на локальных ресурсах, так и в сети. Эти средства активно используют службу *Windows Search* (Служба поиска Windows; сервис WSearch), которая предварительно просматривает все файлы на локальном компьютере, что ускоряет поиск.

> ***Примечание***
>
> В системах Windows Server 2008 *Служба индексирования* (Indexing Service), входящая в состав Windows Server 2003, сохранена только для совместимости с предыдущими версиями и может устанавливаться дополнительно в составе роли сервера File Services (Файловые службы).

Поиск возможен в разных режимах и из разных программ. Рассмотрим эти варианты поочередно. Рекомендуем до конца разобраться во всех функциях, описанных ниже, и опробовать их в реальных условиях. Операция поиска выполняется очень часто, и неправильные или неожиданные результаты могут серьезно осложнить работу. Это тем более важно, что новые средства поиска сильно отличаются от тех, которые имелись в предыдущих версиях Windows.

> ***Внимание!***
>
> Опции поиска, выполняющегося непосредственно из меню **Start** (Пуск), выбираются в окне свойств панели задач и меню **Start** (рис. 2.51). По умолча-

нию (индексированный) поиск выполняется только в личных папках пользователя, но можно указать, чтобы просматривался *весь* индекс.

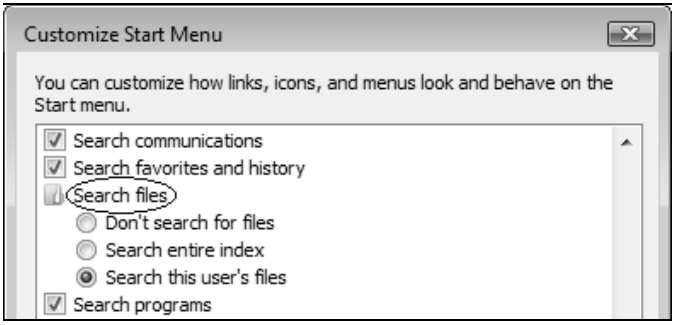


Рис. 2.51. Настройка способов поиска из меню **Start**

В плане реализации возможностей поиска системы Windows Server 2008 заметно отличаются от Windows Vista; сходство наблюдается, если только на Windows Vista установить пакет обновлений Service Pack 1 (в системах Windows Server 2008 он уже имеется).

Отметим самые важные особенности, касающиеся функций поиска в Windows Server 2008:

- опция **Search** (Поиск) отсутствует в меню **Start** (Пуск) и в контекстных меню всех контейнеров (папок, дисков и т. д.);
- после выполнения поиска непосредственно из меню **Start** (Пуск) появляется ссылка **Search Everywhere** (Искать везде) (см. пример на рис. 2.22), позволяющая перейти в окно поиска по всем индексированным папкам (аналогичный результат получается при нажатии клавиш <Win>+<F>);
- в окне параметров индексирования имеется кнопка **Pause** (Пауза), позволяющая приостановить работу по индексированию файлов и папок на 15 минут.

Выполнение операций поиска

Для запуска функции поиска можно нажать клавиши <Win>+<F> или нажать клавишу <F3> (или <Ctrl>+<F>), выбрав папку в окне Проводника. В первом случае поиск выполняется в индексе, построенном для *всех* заданных папок (причем индексированный поиск самый эффективный!); во втором — поиск

осуществляется *только* в пределах выбранной папки (это может быть медленно, если папка не индексирована).

При любом способе вызова операции в появляющемся окне нужно ввести строку или условие поиска в стандартном поле поиска (в правом верхнем углу). Операция поиска начинается сразу же после нажатия первой клавиши, и результат обновляется при вводе каждого следующего символа. Полученные результаты (рис. 2.52) можно просматривать в таблице и фильтровать, выбирая типы файлов (все, почта, документы и т. п.) на панели поиска. Любой найденный файл можно тут же открыть.

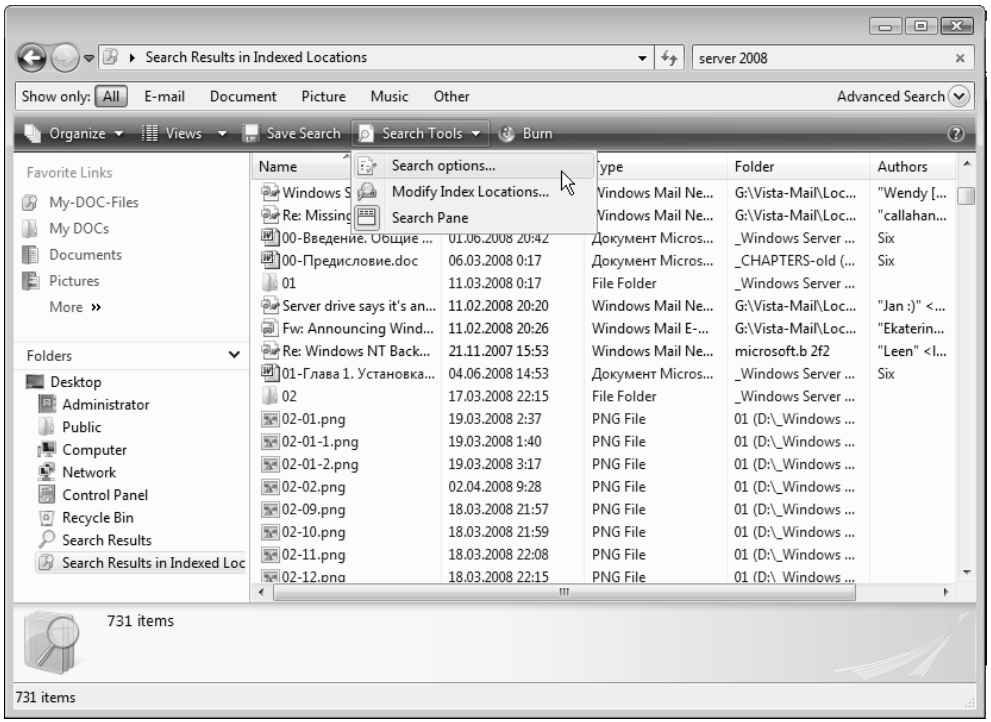


Рис. 2.52. Окно результатов выполнения операции поиска

Совет

При выполнении поиска по сложному критерию обращайте внимание на количество найденных файлов (см. рис. 2.52, левый нижний угол). Это позволит следить за правильностью формирования строки поиска и понимать, влияет ли изменение параметров поиска на получаемые при этом резуль-

таты (например, если для нашего примера в строке поиска ввести строки `server 2008`, `file:server 2008` или `"file:server 2008"`, то результаты будут принципиально разными).

С помощью кнопки **Save Search** (Сохранить условия поиска), имеющейся на панели задач в окне поиска (см. рис. 2.52), создается хранимый запрос, который можно использовать в дальнейшем *(см. далее разд. "Виртуальные папки и панель избранных ссылок")*.

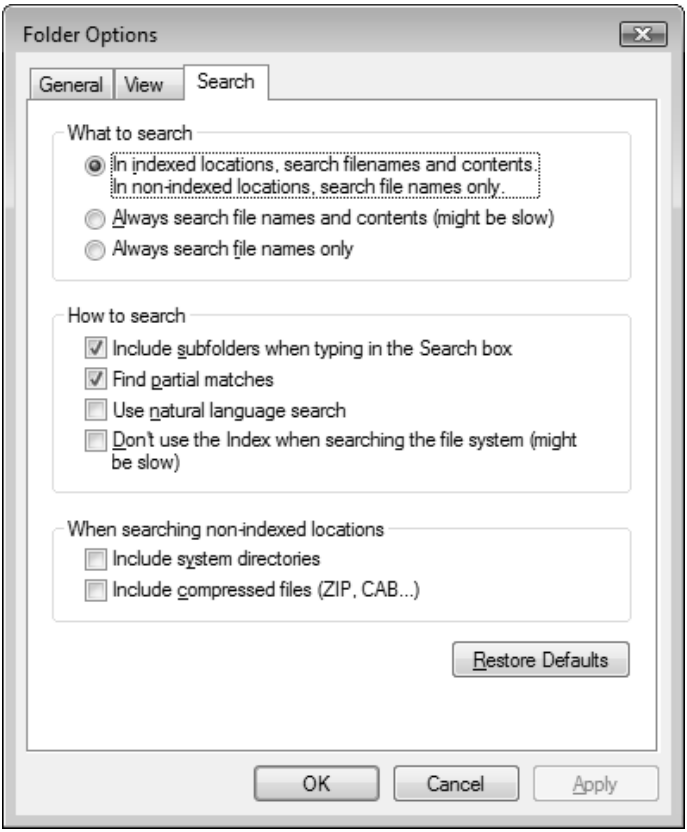


Рис. 2.53. Настройка общих параметров поиска

В меню кнопки **Search Tools** (Средства поиска) на панели задач имеются две команды для настройки параметров поиска. Команда **Search Options** (Параметры поиска) открывает окно, в котором определяются общие параметры поиска (рис. 2.53). Здесь очень важно понять, что в индексированных папках

информация ищется по именам файлов и их содержимому (включая ключевые слова). В тех папках, которые не включены в индекс, *содержимое* файлов не просматривается. Об этом следует помнить и не удивляться, если какая-то информация не находится. Также видно, что по умолчанию не просматриваются системные папки и архивы, расположенные в неиндексируемых папках.

Конфигурирование службы Windows Search

После нажатия кнопки **Modify Index Locations** (Изменение индексируемых мест) в окне результатов поиска (см. рис. 2.52) открывается окно параметров индексирования (рис. 2.54), в котором перечислены все папки, включенные в индекс (в остальных папках поиск будет выполняться медленно, только по именам файлов). В окне постоянно отображается ход процесса индексации: файлы могут быть уже индексированы полностью или индексация может продолжаться[1]. Обычно индексация выполняется при простое и снижается, когда пользователь работает. Кнопка **Pause** (Пауза) позволяет приостановить индексирование на 15 минут.

Примечание

Окно индексируемых папок можно также открыть с панели управления, выбрав задачу **Indexing Options** (Параметры индексирования) (категория **System and Maintenance** (Система и ее обслуживание)). Также из этого окна можно получить доступ к настройкам службы Windows Search.

Внимание!

По умолчанию служба Windows Search (сервис WSearch) не запущена (на это указывает соответствующее сообщение в верхней части окна параметров индексирования — см. рис. 2.54).

Для подготовки службы к работе нужно запустить Server Manager (Диспетчер сервера), в списке ролей выбрать узел **File Services** (Файловые службы) и добавить службу Windows Search Service (Служба поиска Windows). Программа-мастер предложит выбрать дисковые тома, которые будут индексироваться — можно сразу указать нужные тома или выполнить конфигурирование позже *(см. далее)*. (По умолчанию индексируются только меню **Start** (пуск) и папка **Users** (Пользователи)).

---

[1] Нагрузку на систему в процессе индексирования несложно оценить с помощью Системного монитора (Performance Monitor) *(см. главу 5)*.

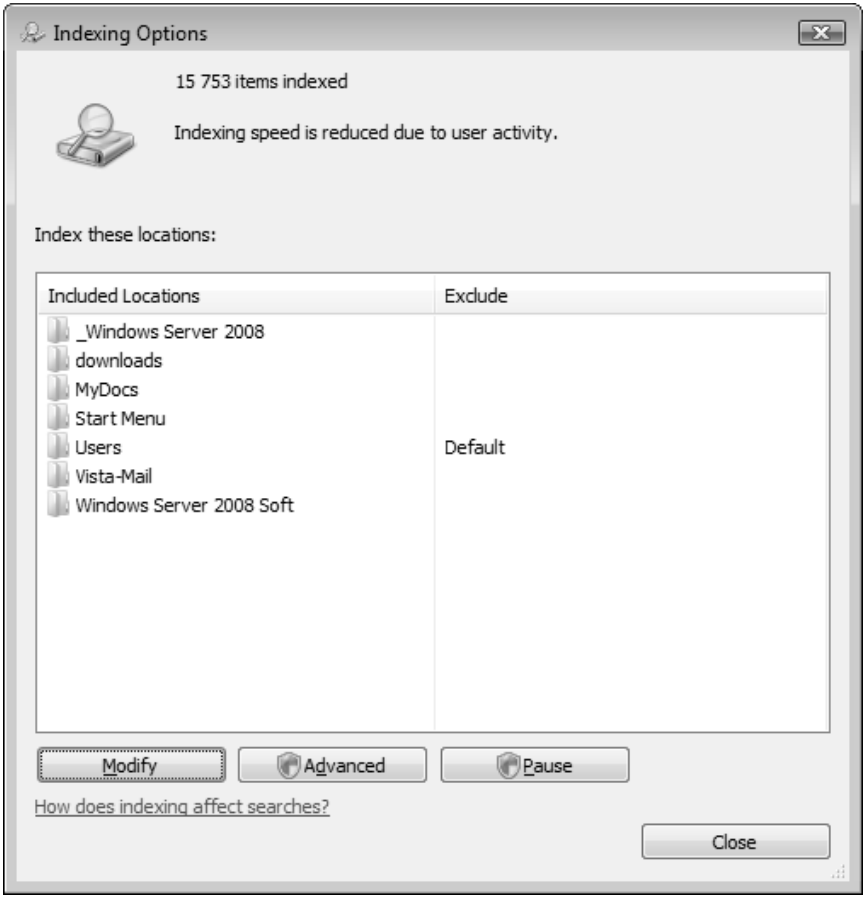


Рис. 2.54. Список индексируемых папок

Рекомендуется перед началом работы в системе выбрать все папки, в которых будет выполняться поиск, включить их в индекс и дождаться завершения операции. Тогда можно рассчитывать на то, что поиск всегда будет успешным.

Чтобы расширить список индексируемых папок, нужно в окне параметров (см. рис. 2.54) нажать кнопку **Modify** (Изменить) и в следующем окне (рис. 2.55) отметить флажками все нужные папки. Список всех уже выбранных папок виден в нижней части окна. Такой точный выбор области поиска позволяет сократить время операции и в то же время обеспечивает ее гибкость.

По умолчанию файл индекса создается в папке C:\ProgramData\Microsoft. Его местоположение можно изменить, нажав кнопку **Advanced** (Другие); в окне

дополнительных параметров можно выполнить тонкую настройку службы Windows Search.

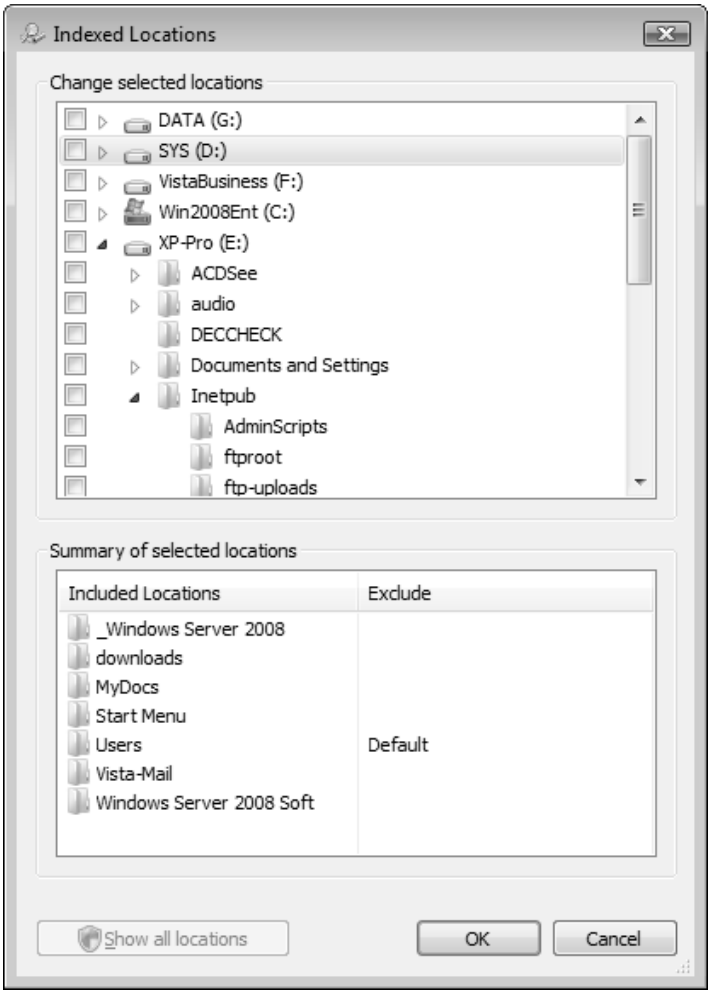


Рис. 2.55. Окно выбора индексируемых папок

Второй распространенный способ поиска — когда *произвольная* папка выбирается на панели навигации в окне программы Windows Explorer (Проводник) и строка вводится в поле поиска (рис. 2.56). Как правило, в таких случаях появляется предупреждение о замедлении поиска в неиндексируемых папках. Поиск выполняется медленно, ход процесса отображается в виде зе-

леного столбика в поле адреса. Если щелкнуть мышью по строке предупреждения о замедлении поиска, то появится меню (рис. 2.57), в котором можно выбрать команду включения текущей папки в индекс (это, конечно, не означает, что поиск сразу будет быстрым — на построение индекса нужно время). Поэтому рекомендуется все часто используемые папки заранее включать в индекс.

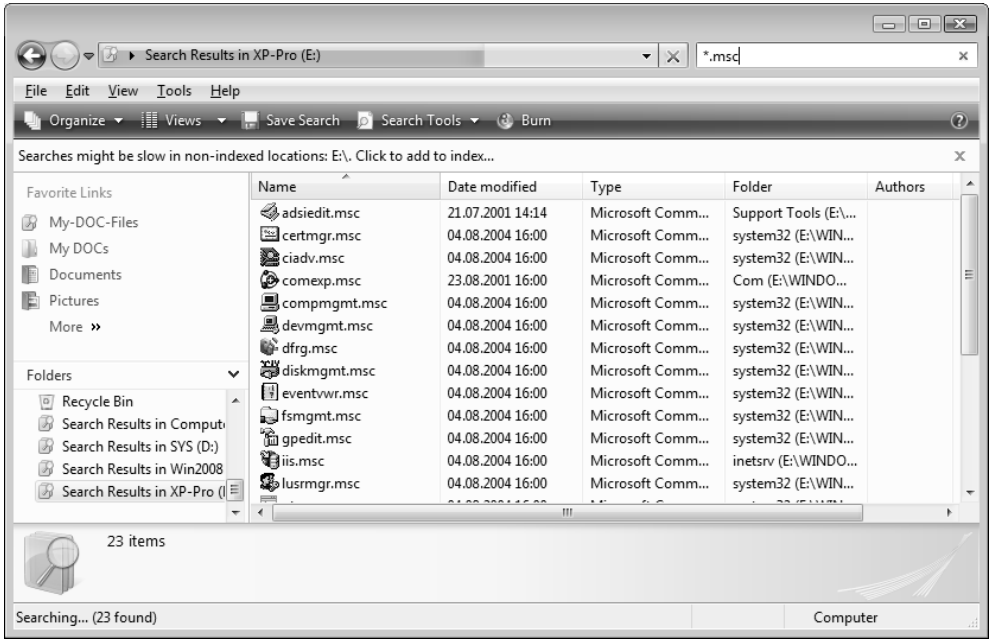


Рис. 2.56. Поиск в произвольной папке

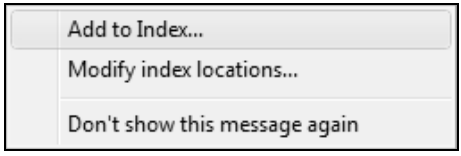


Рис. 2.57. Меню операций по выбору папок для индексирования

По окончании поиска в конце результирующего списка отображается панель (рис. 2.58), с которой можно запустить дополнительный поиск по содержимому файлов или включить опцию расширенного поиска.

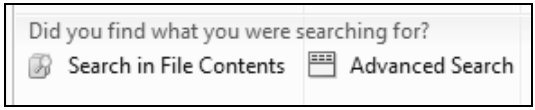


Рис. 2.58. Дополнительные возможности поиска

В окне расширенного поиска (рис. 2.59) можно указывать тип просматриваемых файлов, задавать ключевые слова и другие дополнительные критерии поиска, а также разрешить поиск в неиндексированных и системных файлах. В этом случае нужно сначала ввести строку поиска, выбрать все параметры, а потом начать операцию, нажав кнопку **Search** (Найти).

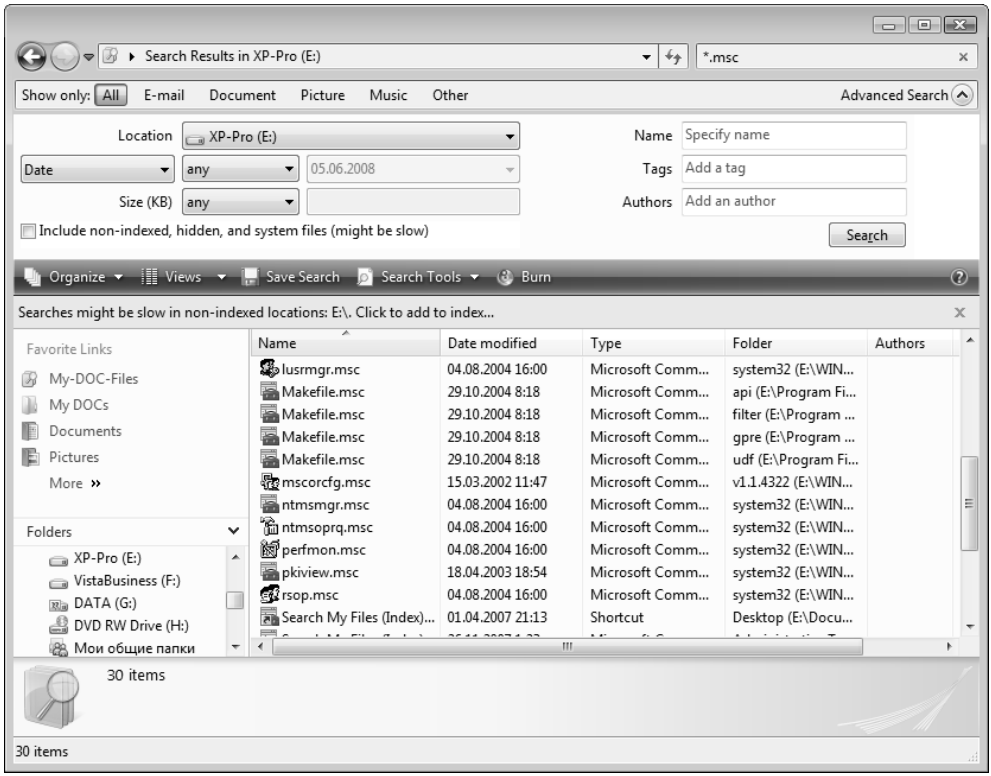


Рис. 2.59. Окно расширенного поиска

Примечание

Обратите внимание на то, что кнопка **Advanced Search** (Расширенный поиск) имеется и в стандартном окне поиск в индексированных папках, которое вызывается при нажатии клавиш <Win>+<F> (см. рис. 2.52). Поэтому дополнительные возможности поиска доступны всегда.

Правила и примеры поиска

Стандартные возможности поиска в системах Windows Vista/Windows Server 2008 значительно расширились по сравнению с Windows XP/Windows Server 2003, однако для того, чтобы быстро получать правильные (и ожидаемые) результаты, необходимо знать некоторые правила выполнения поиска и ключевые слова, которые при этом могут использоваться. Правила поиска распространяются на все случаи; неважно, каким способом операция поиска инициируется. Рассмотрим на примерах формат строки, вводимой в поле поиска (*графический* интерфейс для определения некоторых параметров поиска — например, по тегам, по дате или размеру — реализован в окне расширенного поиска (см. рис. 2.59)).

По умолчанию поиск осуществляется в именах файлов, их содержимом и ключевых словах (тегах). Введенные через пробел слова объединяются логической операцией "И", т. е. в найденных файлах должны присутствовать *все* слова, указанные в строке поиска (эти слова могут встречаться в именах файлов, их содержимом или в ключевых словах). Например, при вводе строки *Windows Server* (строчные и прописные буквы не различаются!) будут найдены все файлы и документы, в которых имеется одновременно и слово Windows, и слово Server. Если нужно искать конкретную *строку*, то все входящие слова следует заключить в двойные кавычки, например, *"Windows Server"*.

Если в строке поиска ввести *Windows OR Server* (OR обязательно заглавными буквами!), то будут найдены все файлы, содержащие первое слово, а также все файлы, содержащие второе слово; т. е. указанные слова объединяются логической операцией "ИЛИ".

Строка *Windows NOT Server* (NOT заглавными буквами!) позволит найти файлы, содержащие слово Windows и ***не*** содержащие слово Server.

Для того чтобы конкретизировать область поиска, используются служебные слова (регистр значения не имеет; в скобках указан русскоязычный эквивалент):

- *file* (имя) — для поиска в именах файлов;
- *ext* (расширение) — для поиска в расширениях файлов;

- *tag* (ключевое слово) — для поиска среди ключевых слов (тегов);
- *date* (изменен) — для поиска по дате изменения файла;
- *author* (автор) — для поиска файлов, созданных данным автором.

Таким образом, строка *file:Windows file:Server* позволит найти все файлы, в *именах* которых встречаются *оба* указанных слова. Для поиска MP2-файлов, в имени которых содержится слово Video, можно использовать строку *ext:mp2 file:Video*.

Служебные слова и символы логических операций можно комбинировать, получая сложные условия поиска. Напомним, что эти условия можно сохранить и обращаться к ним впоследствии повторно.

Переключение окон работающих приложений

Названия всех запущенных в системе программ можно видеть на панели задач. Щелкнув мышью по названию задачи, пользователь может открыть окно любого работающего приложения. Системы Windows Vista/Windows Server 2008 — при использовании стиля Windows Aero! — предлагают новую функцию (task bar previews), которая позволяет в уменьшенном масштабе видеть окна работающих приложений (рис. 2.60). Это упрощает выбор нужной задачи (особенно, если одно приложение запущено в нескольких копиях), поскольку помимо названия задачи, можно видеть и ее экран.

Рис. 2.60. Предпросмотр окон запущенных приложений на панели задач

Чтобы отключить функцию предпросмотра, нужно сбросить флажок **Show window previews (thumbnails)** (Отображать образцы окон (эскизы)) в окне свойств панели задач и меню **Start** (Пуск) (см. рис. 2.26).

Во всех системах Windows задачи можно переключать, последовательно нажимая клавиши <Alt>+<Tab> (или <Alt>+<Shift>+<Tab>). При этом на экра-

не появляется всплывающее окно, где отображаются значки программ и названия открытых документов — нужную программу можно выбрать последовательным нажатием названных клавиш.

В системах Windows Vista/Windows Server 2008 для выполнения данной задачи имеются две совершенно новые функции, которые активны только при выборе стиля Windows Vista. Эти функции названы *Windows Flip* и *Windows Flip 3D*.

Функция Windows Flip, вызываемая при нажатии клавиш <Alt>+<Tab>, позволяет помимо имени текущей программы или документа, видеть одновременно окна программ (рис. 2.61). Благодаря этому пользователь может быстро ориентироваться и выбирать нужное окно. На рис. 2.62 для сравнения показана панель переключения задач при выключенной функции Aero Glass (выбран упрощенный стиль Windows Vista Basic), а на рис. 2.63 изображена аналогичная панель при использовании классического стиля.

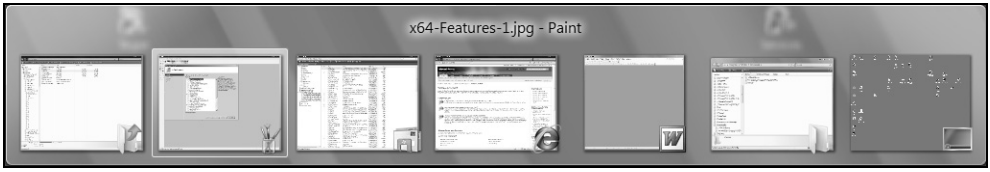


Рис. 2.61. Переключение задач по клавишам <Alt>+<Tab> при использовании стиля Windows Aero

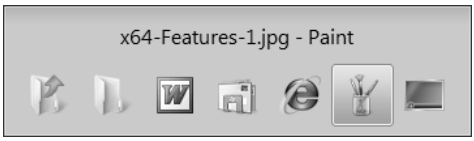


Рис. 2.62. Переключение задач при использовании стиля Windows Vista Basic (Windows Vista – упрощенный стиль)

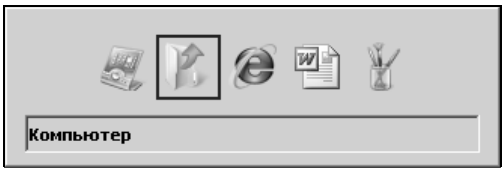


Рис. 2.63. Переключение задач при использовании классического стиля (Windows Classic)

Функция Windows Flip 3D реализована только при использовании стиля Windows Aero; она активизируется при нажатии клавиш <Win>+<Tab> (или <Win>+<Shift>+<Tab>). В этом случае окна запущенных приложений представлены в трехмерной проекции, при этом они уменьшены по сравнению с натуральным размером (рис. 2.64). При повторном нажатии клавиш следующее за первым окно "выезжает" на передний план, и пользователь может просматривать содержимое каждого окна, выбирая нужное. При отпускании клавиш переднее окно разворачивается в натуральную величину.

Если нажать клавиши <Win>+<Ctrl>+<Tab>, то при отпускании клавиш изображение не меняется (клавиши "залипают"), и перебирать окна можно, нажимая одну только клавишу <Tab> (или стрелки влево/вправо). (Аналогичный эффект наблюдается, если использовать кнопку **Switch between windows** (Переключение между окнами) на панели быстрого запуска — см. рис. 2.38.) При щелчке мышью или нажатии клавиши <Enter> раскрывается первое окно.

Рис. 2.64. Переключение задач с помощью функции Windows Flip 3D (клавиши <Win>+<Tab>)

Профили пользователей и виртуальные папки

Рассмотрим некоторые особенности реализации механизма пользовательских профилей в системах Windows Server 2008, а также совершенно новую концепцию *виртуальных папок*, которая значительно повышает возможности организации документов и объектов файловой системы самого разного типа. Эти сведения весьма важны при организации работы в среде Windows Server 2008, поскольку каждый пользователь должен понимать, где ему хранить файлы и как обеспечивается защита его данных — какая информация будет закрыта от других пользователей, а какая доступна всем.

Профили пользователей

Рабочая среда пользователя определяется настройками рабочего стола (например, цвета экрана, курсора мыши, размера и расположения окон), параметрами подключенных сетевых устройств и принтеров, переменными среды, параметрами реестра, наборов доступных приложений и т. д.

Все настройки рабочей среды компьютера хранятся в *профиле пользователя* (user profile) и определяются самим пользователем. Они автоматически сохраняются в папке, имя которой в системах Windows Vista/Windows Server 2008 по умолчанию выглядит следующим образом: *%SystemDrive%*\Users\<*имяПользователя*> (*%SystemDrive%* — имя загрузочного диска, на котором находятся файлы системы; для указанных систем это почти всегда диск C:\).

> ***Внимание!***
>
> Напомним, что в системах Windows 2000/XP Windows Server 2003 для хранения профилей пользователей используется папка *%SystemDrive%*\Documents and Settings\<*имяПользователя*>. Папка **Documents and Settings** присутствует в Windows Vista/Windows Server 2008 для совместимости, но не представляет собой реальную папку файловой системы.

Локальные профили создаются автоматически для каждого пользователя в процессе его первой регистрации на компьютере. При входе пользователя в систему рабочая среда имеет ту же конфигурацию, какая существовала в момент предыдущего выхода пользователя из системы. Благодаря наличию профилей несколько пользователей могут работать на одном и том же компьютере в индивидуальных средах, не влияя друг на друга.

На рис. 2.65 показан пример папки **Users** (Пользователи) (если на компьютере работают несколько пользователей). Как можно видеть, помимо папок профилей администратора компьютера и пользователя, созданного в момент начального конфигурирования системы, имеется также папка **Public** (Общие), которая предназначается для хранения информации, с которой могут работать как все локальные пользователи, так и пользователи удаленных компьютеров (к этой папке по умолчанию разрешен общий доступ). Подробнее назначение этой папки мы рассмотрим далее.

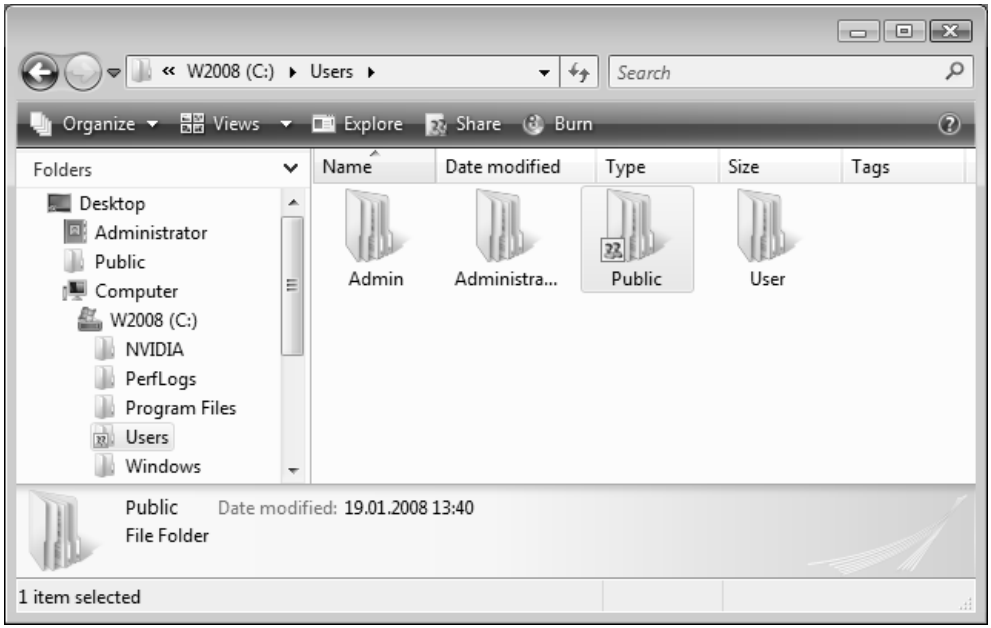


Рис. 2.65. Папка **Users**, в которой хранятся профили пользователей

Структура профиля пользователя

Профиль пользователя создается на основе профиля, назначаемого по умолчанию. Скрытые системные папки **Default** и **All Users**, используемые для определения параметров стандартного профиля, присутствуют в Windows Server 2008 и представляют собой реальные папки файловой системы. Папка **Default User** оставлена для совместимости и является ссылкой. Эти папки, как и папки пользовательских профилей, также хранятся в папке **Users** (Пользователи) корневого каталога загрузочного диска.

На рис. 2.66 показана структура локального профиля пользователя (для наглядности изображены все имеющиеся папки и ссылки). Многие объекты являются скрытыми и по умолчанию не видны в окне программы Проводник (на рисунке эти папки более светлые и не имеют особой пиктограммы — например, папка **AppData**), некоторые из них на самом деле представляют собой не файловые папки, а *ссылки* (junction point) (что видно по изображению стрелки на значке папки — например, папка **Local Settings**) и доступ к ним невозможен (их имена используются для совместимости только прикладными программами).

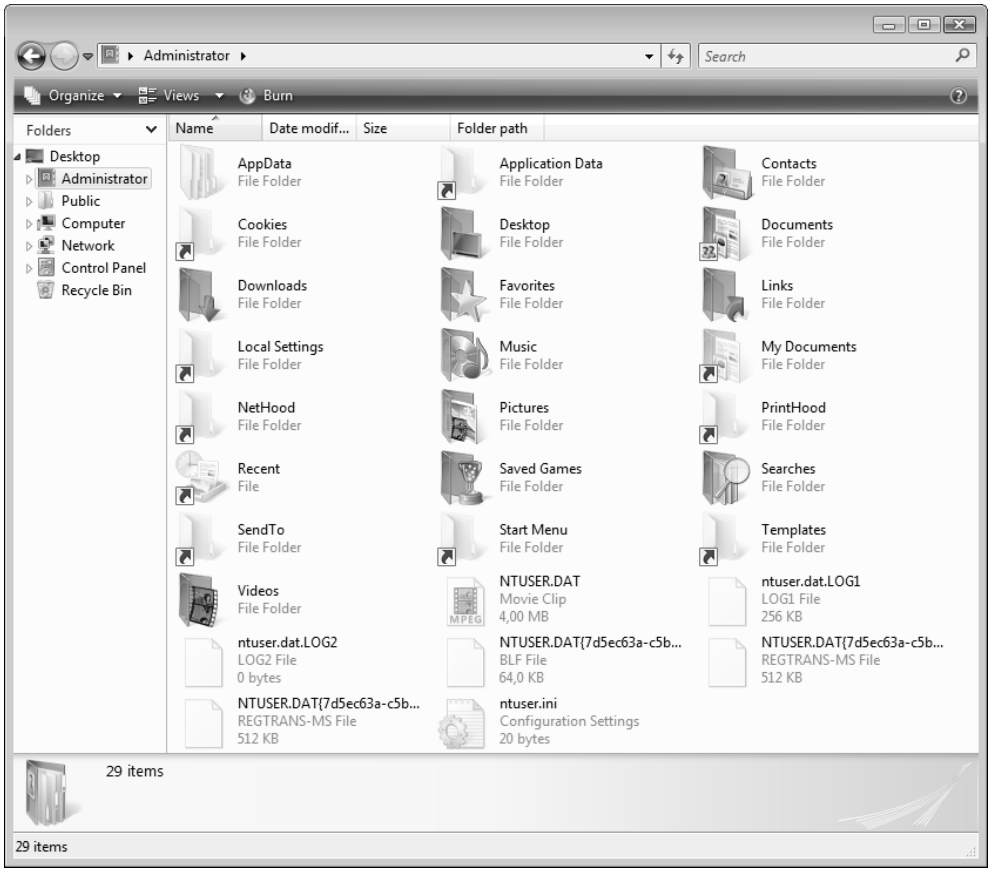


Рис. 2.66. Структура локального профиля пользователя

Папки, представляющие собой *точки повторной обработки* (junction points), а не реальные физические папки, можно увидеть в окне командной строки с

помощью специального параметра команды `dir` — ниже приведены некоторые примеры (строки, не имеющие отношения к делу, не показаны):

```
C:\>dir /AL
 Directory of C:\
19.01.2008  15:47    <JUNCTION>     Documents and Settings [C:\Users]
...
C:\>cd users
C:\Users>dir /AL
 Directory of C:\Users
19.01.2008  15:47    <SYMLINKD>     All Users [C:\ProgramData]
19.01.2008  15:47    <JUNCTION>     Default User [C:\Users\Default]
```

В приведенных строках можно видеть имя, которое фигурирует в окне программы Проводник и доступно прикладным программам, а в квадратных скобках — имя физической папки, связанной с данным объектом.

> ***Внимание!***
>
> Ссылки невозможно удалить с помощью обычных операций удаления в окне программы Windows Explorer (Проводник) или в командной строке. В случае такой необходимости следует использовать утилиту `fsutil` с параметрами `reparsepoint delete`.

В табл. 3.1 перечислены реальные (физические) подкаталоги, находящиеся внутри папки локального профиля пользователя, и описано их назначение.

Таблица 3.1. *Содержимое папки локального профиля пользователя*

Подкаталог	Содержимое
AppData	Данные, относящиеся к конкретным приложениям, например, индивидуальный словарь. Разработчики приложений сами принимают решение, какие данные должны быть сохранены в папке профиля пользователя
Contacts (Контакты)	Контакты, используемые почтовой программой Windows Mail
Desktop (Рабочий стол)	Объекты рабочего стола, включая файлы и ярлыки
Documents (Документы)	Документы, создаваемые пользователем

Таблица 3.1 *(окончание)*

Подкаталог	Содержимое
Downloads (Загрузка)	Файлы, загруженные с веб-сайтов
Favorites (Избранное)	Ярлыки часто используемых программ и папок, сохраненные веб-ссылки
Links (Ссылки)	Ссылки, отображаемые на панели избранных ссылок (Favorite Links) программы Windows Explorer (Проводник) *(см. далее разд. "Виртуальные папки и панель избранных ссылок")*
Music (Музыка)	Папка, в которую по умолчанию копируются все аудиофайлы
Pictures (Изображения)	Изображения и цифровые фотографии, созданные и импортированные пользователем
Saved Games (Сохраненные игры)[1]	Параметры сохраненных игр
Searches (Поиски)	Сохраненные запросы поиска
Videos (Видео)	Импортированные видеоклипы и телепрограммы

Некоторые папки пользовательского профиля систем Windows XP/Windows Server 2003 теперь отсутствуют, их аналоги в Windows Server 2008 можно найти внутри папки C:\Users\<*имяПользователя*>\AppData\Roaming\Microsoft\Windows. В табл. 3.2 перечислены некоторые из этих папок и указано их новое полное имя.

Таблица 3.2. *Дополнительные папки, входящие в профиль пользователя*

Папка	Содержимое и полный путь
Cookies	Служебные файлы, получаемые с посещенных веб-серверов C:\Users\<*имяПользователя*>\AppData\Roaming\Microsoft\Windows\Cookies
Recent (Недавние документы)	Данные о документах и графических файлах, открытых пользователем в течение последнего времени C:\Users\<*имяПользователя*>\AppData\Roaming\Microsoft\Windows\Recent

[1] Даже в серверных системах такая папка имеется!

Таблица 3.2 *(окончание)*

Папка	Содержимое и полный путь
SendTo	Ярлыки объектов, куда могут посылаться документы C:\Users\<*имяПользователя*>\AppData\Roaming\Microsoft\Windows\SendTo В эту папку можно поместить ярлыки программы, которые будут открываться при вызове контекстного меню для файла или папки и выборе команды **Send To** (Отправить). Например, такой программой может быть специфический текстовый редактор или программа, не запускаемая по умолчанию для данного типа файлов
Start Menu (Главное меню)	Ярлыки программ C:\Users\<*имяПользователя*>\AppData\Roaming\Microsoft\Windows\Start Menu

Личные и общие папки

Внутри папки пользовательского профиля имеется множество специализированных папок для хранения разного рода данных (рис. 2.67).

Назначение папок понятно из их названия. Все показанные на рисунке папки являются реальными папками файловой системы. Можно обеспечить доступ к этим папкам со стороны удаленных пользователей, но по умолчанию личные папки закрыты для любых других пользователей.

При работе с личными (и общими) пользовательскими папками следует, однако, учитывать тот факт, что полные имена файлов "маскируются" в поле адреса окна программы Windows Explorer (Проводник). Если мы хотим увидеть реальное имя папки, следует щелкнуть мышью по полю адреса — после этого будет отображаться физический путь к папке (иногда именно он нужен для работы). Это проиллюстрировано на рис. 2.68: вверху показано представление по умолчанию, внизу — реальное имя папки.

Как уже говорилось, внутри папки **Users** (Пользователи) имеется папка **Public** (Общие), в которой пользователи могут сохранять информацию, доступную другим пользователям. Подкаталоги этой папки показаны на рис. 2.69 (обратите внимание на строку **Shared with: Everyone** ("Общий доступ для: Все")). Пользователь может с помощью несложной операции обеспечить доступ к любому подкаталогу папки **Public** (Общие), указав при этом права доступа к информации *(см. главу 7)*.

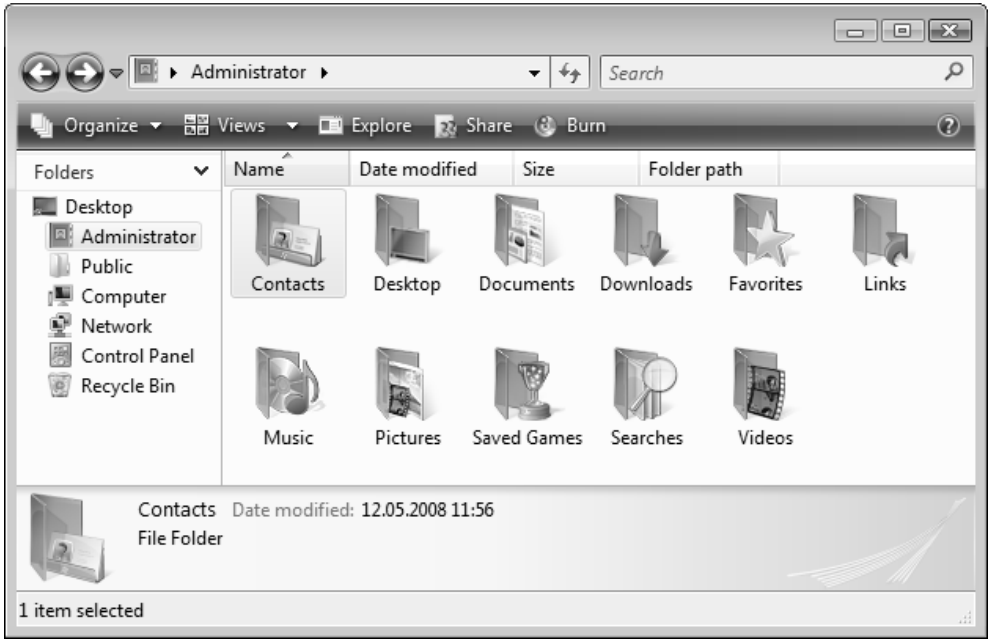


Рис. 2.67. Личные папки пользователя

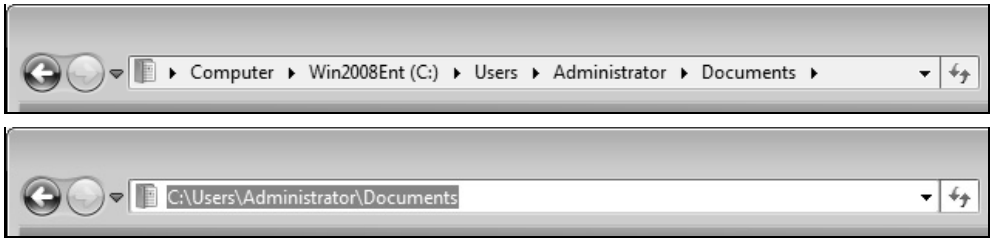


Рис. 2.68. Представление адреса папки в окне программы Windows Explorer и ее реальное физическое имя

Внимание!

При необходимости стандартное местоположение любой (отдельной) личной и общей папки можно изменить и перенести папку, скажем, на другой логический диск. Для этого следует открыть окно свойств нужной папки, перейти на вкладку **Location** (Папка), нажать кнопку **Move** (Переместить) и выбрать новое местоположение для папки. Система предложит перенести файлы из старой папки в новую. Нажав кнопку **Restore Default** (По умолчанию), можно в любой момент вернуть все в исходное состояние. Подобная

возможность отсутствует в системах Windows, предшествующих Windows Vista/Windows Server 2008: там папку **My Documents** (Мои документы) можно переместить только целиком, со всем ее содержимым.

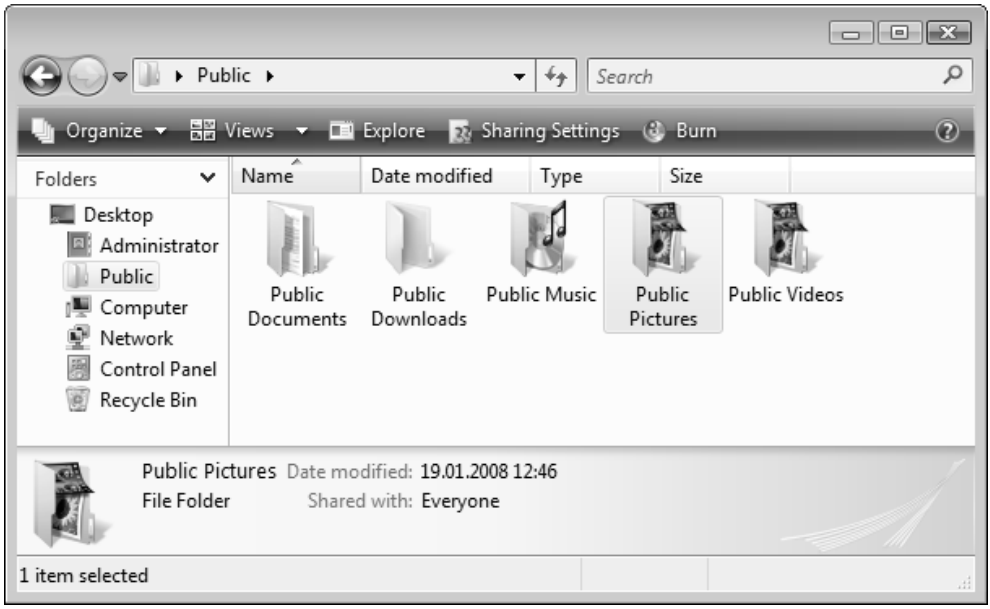


Рис. 2.69. Стандартные папки для общего доступа

Виртуальные папки и панель избранных ссылок

В системах Windows Vista/Windows Server 2008 реализована новая концепция организации информации на диске, получившая название *виртуальных папок* (Virtual Folder). Эти папки, по сути, представляют собой хранящийся запрос, который мгновенно выполняется в тот момент, когда пользователь открывает папку. Содержимое виртуальной папки является списком файлов, отвечающих условиям поиска или фильтрации. В составе систем имеются стандартные виртуальные папки, однако их можно создавать и самостоятельно.

Чтобы самому создать виртуальную папку, необходимо выполнить операцию поиска информации, хранящейся на диске, и в окне результатов поиска нажать кнопку **Save Search** (Сохранить условия поиска) на панели задач. Запрос можно сохранить в любой папке или на рабочем столе, а также на пане-

ли избранных ссылок программы Windows Explorer (Проводник) (эту операцию мы рассмотрим позже). Реально запрос представляет собой XML-файл с расширением .search-ms.

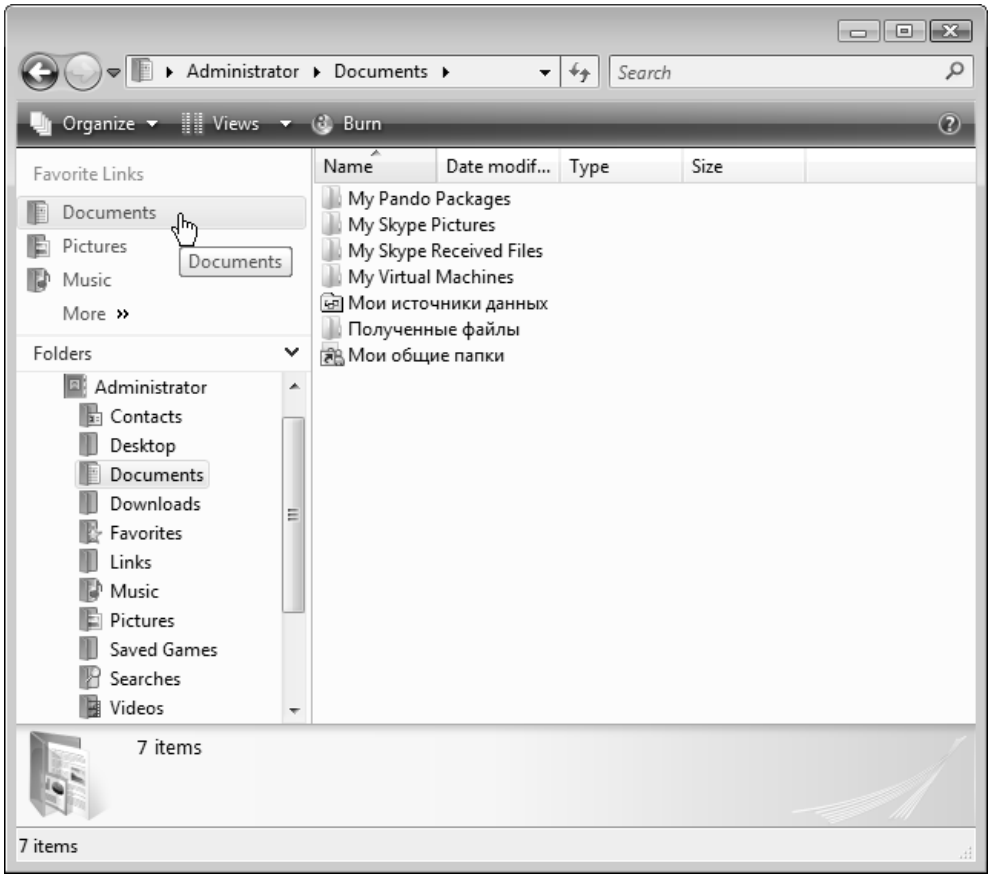


Рис. 2.70. Папка на панели навигации является ссылкой на некоторую папку жесткого диска

Панель **Favorite Links** (Избранные ссылки), расположенная выше панели **Folders** (Папки) в левой части окна программы Windows Explorer (Проводник) (на панели навигации), позволяет быстро переходить к файлам, хранящимся в некоторой папке или отвечающим определенным условиям фильтрации. Как можно видеть на рис. 2.70, при выборе элемента **Documents** (Документы) на панели ссылок мы видим содержимое одноименной папки в

профиле пользователя. Хранятся элементы данной панели в папке **Links** (Ссылки) профиля пользователя. Понимая этот механизм, можно эффективно организовывать способы представления файлов и папок на жестком диске. Покажем это на примере.

Допустим, нам нужно иметь быстрый доступ к папке, где хранятся рабочие документы (где реально находится эта папка на диске — значения не имеет). Создадим ярлык для этой папки, **My DOCs**, и переместим его в папку **Links** (Ссылки) — можно просто с помощью мыши перетащить папку на панель избранных ссылок (при этом в процессе перемещения значка папки возле курсора появится всплывающая подсказка со стрелочкой и подписью **Create link in Links** (Создать ссылку в Ссылки); при отпускании левой кнопки мыши на панели будет создана ссылка на выбранную папку). (Чтобы создать обычную ссылку, следует выбрать папку в окне программы Windows Explorer (Проводник), щелкнуть правой кнопкой мыши и в контекстном меню выполнить команду **Create Shortcut** (Создать ярлык).)

Рис. 2.71. Новое содержимое папки **Links** в профиле пользователя

Кроме того, нам нужно видеть список всех документов Word (*.doc), независимо от того, в каких папках на диске эти документы находятся. Выполним операцию поиска на диске или в определенной корневой папке (вообще, фильтр поиска может быть достаточно сложным!) и сохраним ее результат в виде виртуальной папки — например, как файл My-DOC-Files (с расширением .search-ms). Сохранять файл нужно непосредственно в папке **Links** (Ссылки). Результат этих операций — новое содержимое папки — показан на рис. 2.71. (Обратите внимание на пиктограммы с изображением увеличительного стекла — их несколько.)

Теперь на панели избранных ссылок появились два новых элемента (рис. 2.72) — **My-DOC-Files** и **My-Docs**. При выборе первого мы увидим список *всех* имеющихся DOC-файлов, а при выборе второго элемента будет отображаться содержимое *конкретной* папки My-Docs.

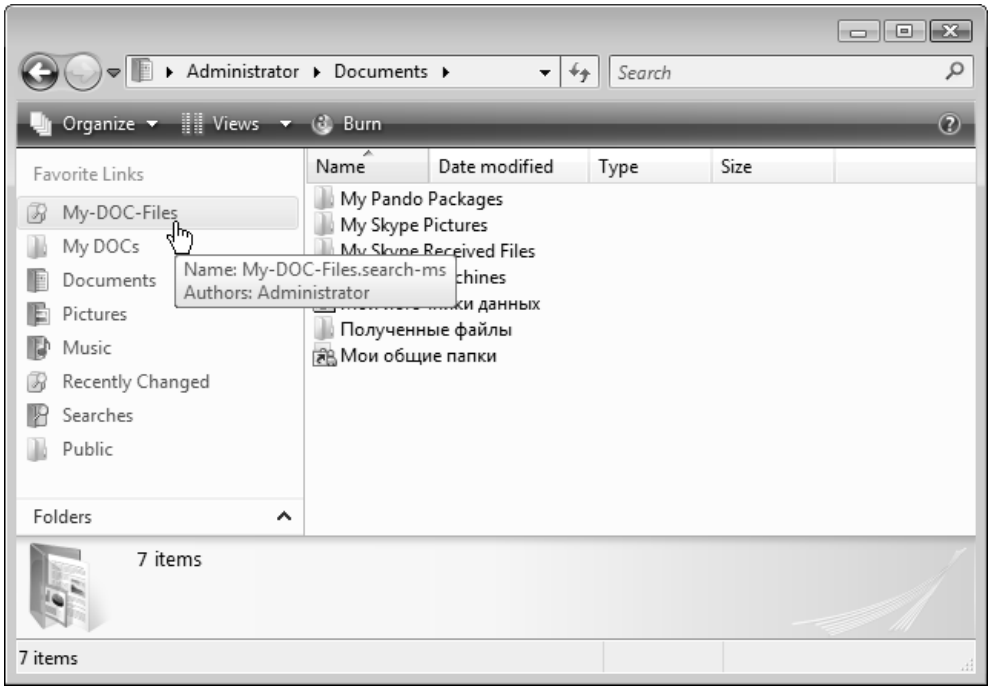


Рис. 2.72. Модифицированная панель избранных ссылок

Пиктограмма для первого элемента указывает на то, что он является запросом (на всплывающей подсказке видно имя файла сохраненного запроса и

имя автора). Для второго элемента используется обычный значок папки, поскольку он и является обычной ссылкой на локальную папку.

Любой значок с панели избранных ссылок можно удалить, выбрав его и выполнив команду **Remove Link** (Удалить ссылку) в контекстном меню. Эта операция никак не влияет на *содержимое* папки, с которой связан удаляемый значок.

Описанная выше процедура позволяет сформировать набор нужных папок и документов, предоставляя также возможность быстрого перехода между папками. Выполните сами все рассмотренные операции, и вы поймете, что этот механизм прост и эффективен.

Справочная система Windows Server 2008

В заключение этой главы рассмотрим, какие средства система Windows Server 2008 предоставляет в помощь пользователю для получения информации и решения возникающих проблем.

Справочная система — *Windows Help and Support* (Справка и поддержка) — представляет собой справочно-консультативный центр, который не только содержит много полезной информации о системе и приемах эффективной работы, но и позволяет находить ответы на возникающие вопросы и решать появляющиеся в процессе работы проблемы. В справочной системе Windows Server 2008 наличие подключения к Интернету особенно важно, поскольку дополнительная информация с сайта Microsoft может поступать при каждом обращении к справке, при выполнении запросов (при поиске) и переходах по ссылкам.

Для запуска справочной системы выберите в меню **Start** (Пуск) команду **Help and Support** (Справка и поддержка). На экране появится главное окно справки (рис. 2.73). Поле поиска (Search Help) позволяет находить требуемую информацию в локальной справочной системе, при этом обновление справки может выполняться через Интернет с веб-ресурсов Microsoft.

Возможность обращения к онлайновым ресурсам определяется переключателем в нижнем правом углу окна справки. (В автономном режиме справка работает быстрее, но ее информационное наполнение может оказаться недостаточным для некоторых вопросов.) Кнопка **Options** (Параметры) позволяет настроить функцию поиска и выполнить типовые операции по работе со справкой.

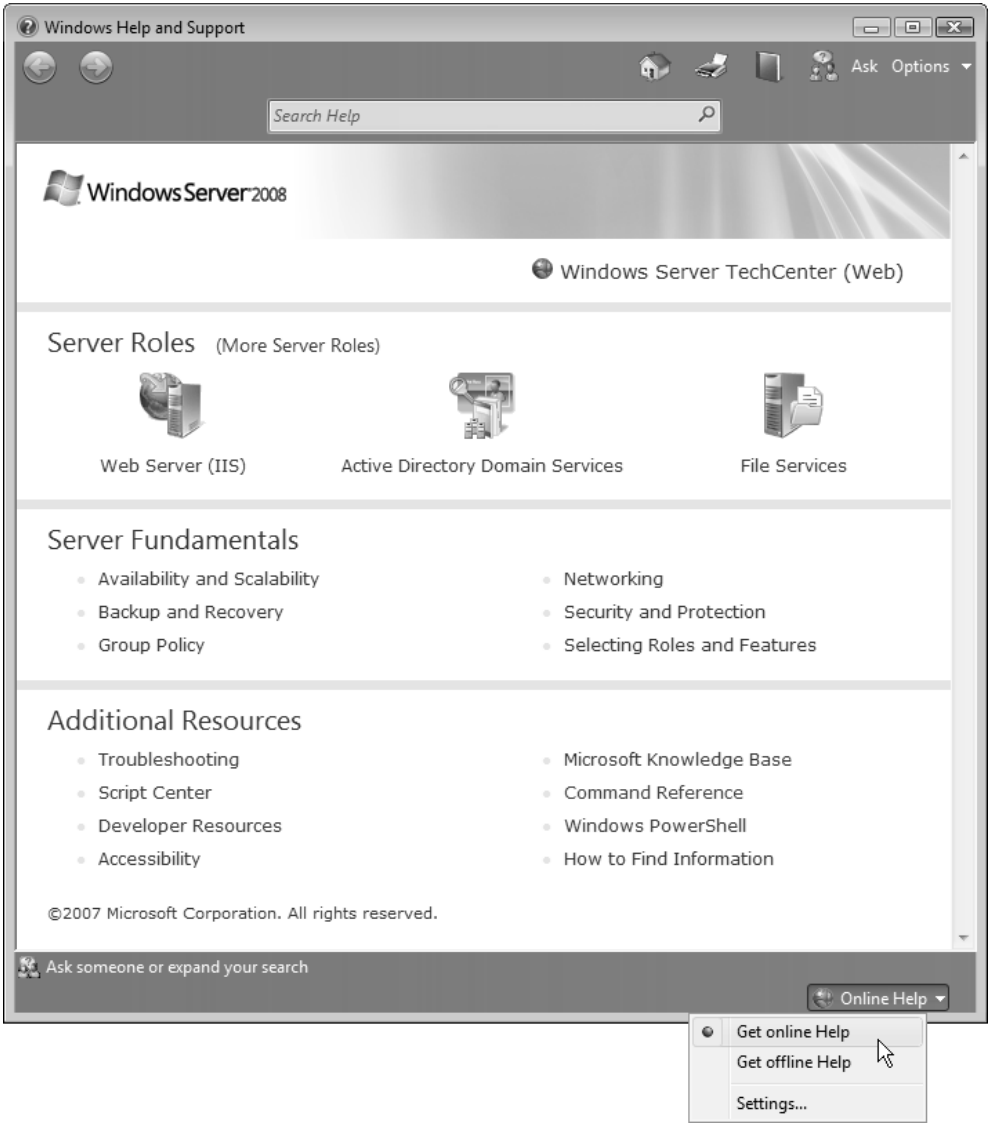


Рис. 2.73. Главное окно справочной системы Windows Server 2008

Справка не имеет, как такового, структурированного *оглавления* имеющихся статей; доступ к разделам осуществляется по ссылкам или с помощью поиска по ключевым словам.

Если для решения проблемы требуется дополнительная информация, то пользователь может нажать кнопку **Ask** (Спросить) или щелкнуть по ссылке **Ask someone or expand your search** (Спросить другого пользователя или расширить область поиска). На странице дополнительной поддержки (рис. 2.74) можно видеть ссылки на онлайновые ресурсы Microsoft, где можно найти расширенную техническую информацию. В системах Windows Vista аналогичная страница справки позволяет также вызвать средство *Remote Assistance* (Удаленный помощник), но в сервере такая возможность отсутствует и используются другие методы запуска удаленного помощника.

Функция Remote Assistance (Удаленный помощник) позволяет другому пользователю или администратору подключиться через сеть или Интернет к локальному компьютеру, обсудить в диалоговом режиме возникшие вопросы и увидеть экран компьютера. Удаленному пользователю также могут быть предоставлены все полномочия для управления компьютером. Подробнее средство Remote Assistance описано в *главе 4*.

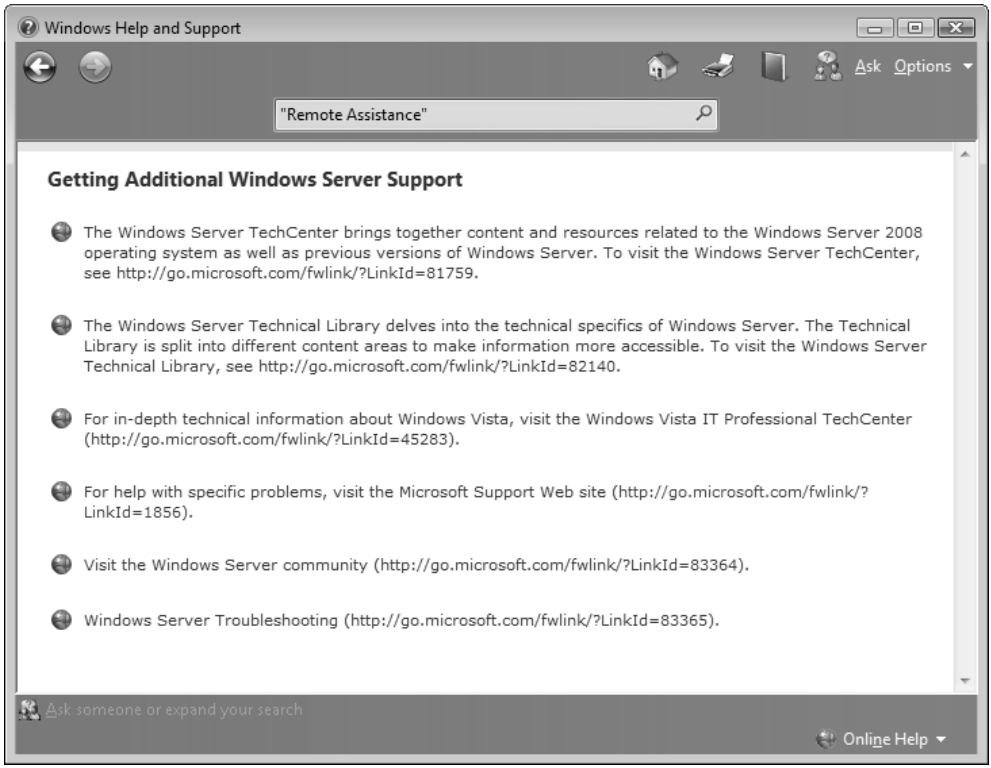
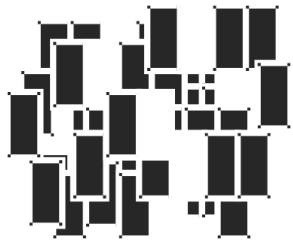


Рис. 2.74. Ссылки на дополнительные онлайновые информационные ресурсы

Глава 3



Конфигурирование системы и средства администрирования

В этой главе рассматриваются способы настройки разнообразных параметров систем Windows Server 2008 и ее компонентов — элементов рабочего стола, свойств монитора и других устройств ввода и отображения информации, языков и региональных стандартов, даты, времени и т. д. Для этого имеется множество разнообразных утилит, которые обладают дружественным пользовательским интерфейсом и уменьшают потенциальные опасности от неправильного выбора параметров. Различные системные средства рассматриваются по мере необходимости и в других главах книги.

Некоторые из рассматриваемых в главе утилит отсутствуют как в предыдущих серверных версиях Windows, так и в близкой по ядру и программному коду операционной системе Windows Vista (хотя *большинство* из описываемых далее параметров настраиваются одинаково в Windows Vista и Windows Server 2008). Отличия от Windows Vista, в первую очередь, определяются необходимостью конфигурирования специфических серверных служб.

Для решения множества административных задач, связанных с управлением системой и службами, имеются дополнительные инструменты: так называемая *консоль управления* (MMC) и *оснастки*. Им посвящается завершающая часть главы.

Панель управления — административный центр системы

Практически все средства конфигурирования компонентов и сервисов систем Windows сосредоточены на *панели управления* (Control Panel), с которой так-

же можно получить доступ и ко всем административным оснасткам. Чтобы открыть панель управления, нужно в меню **Start** (Пуск) выполнить команду **Control Panel** (Панель управления). При необходимости меню **Start** (Пуск) можно настроить так, что панель управления будет отображаться как подменю, в котором можно сразу выбрать конкретную задачу или группу параметров *(см. главу 2)*.

На первый взгляд панель управления систем Windows Vista/Windows Server 2008 принципиально почти не изменилась по сравнению с Windows XP или Windows Server 2003. В Windows Vista все задачи, выполняемые с панели управления, разделены по категориям: например, все операции, связанные с настройкой параметров системы, сосредоточены в одном окне, а команды по конфигурированию элементов пользовательского интерфейса — в другом.

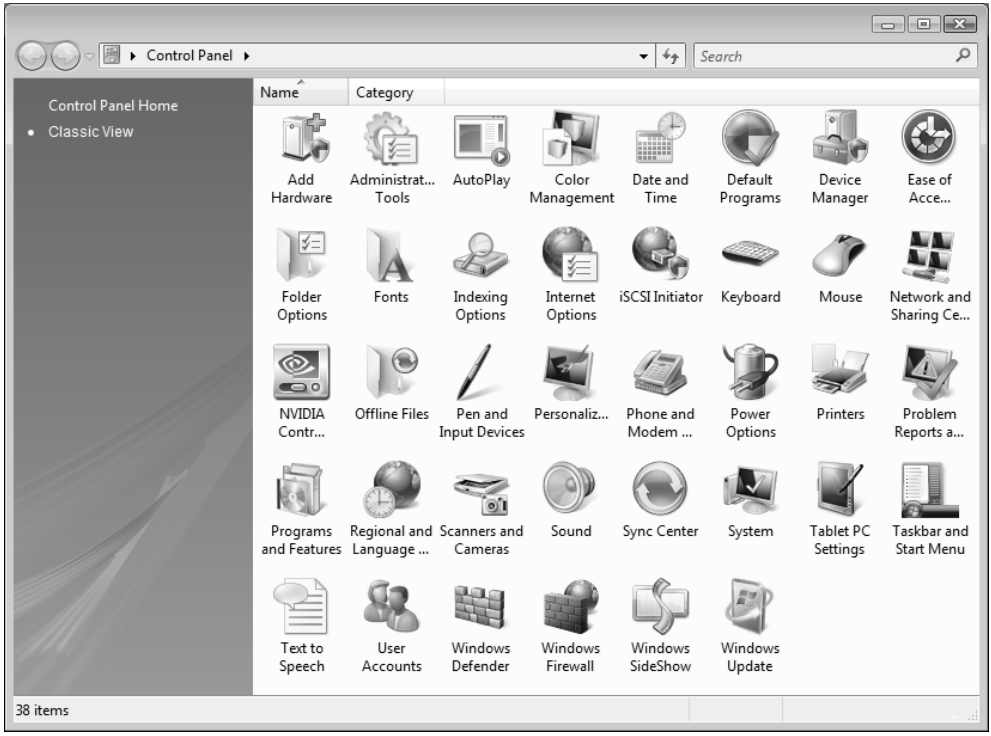


Рис. 3.1. Исходный (классический) вид панели управления систем Windows Server 2008

В Windows Server 2008 по умолчанию используется более традиционный для серверных систем способ представления задач — когда все они представлены в виде списка (который значительно больше, чем в системах Windows XP/Windows Server 2003) (рис. 3.1). Для опытного пользователя удобнее, если на панели управления одновременно отображаются значки всех утилит — в этом случае можно сразу выбрать конкретную задачу и не искать ее по тематическим категориям.

Если переместить курсор на свободное пространство окна панели управления и щелкнуть правой кнопкой мыши, то появится контекстное меню, в котором в подменю **View** (Вид) можно выбрать вид значков задач: от самого крупного до мелкого — пользователь легко может выбрать привычный и удобный для себя вид окна. На рис. 3.2 показана панель управления в режиме Details (Таблица) — в этом случае помимо имени задачи указывается категория (таким образом, список задач можно отсортировать по именам или категориям).

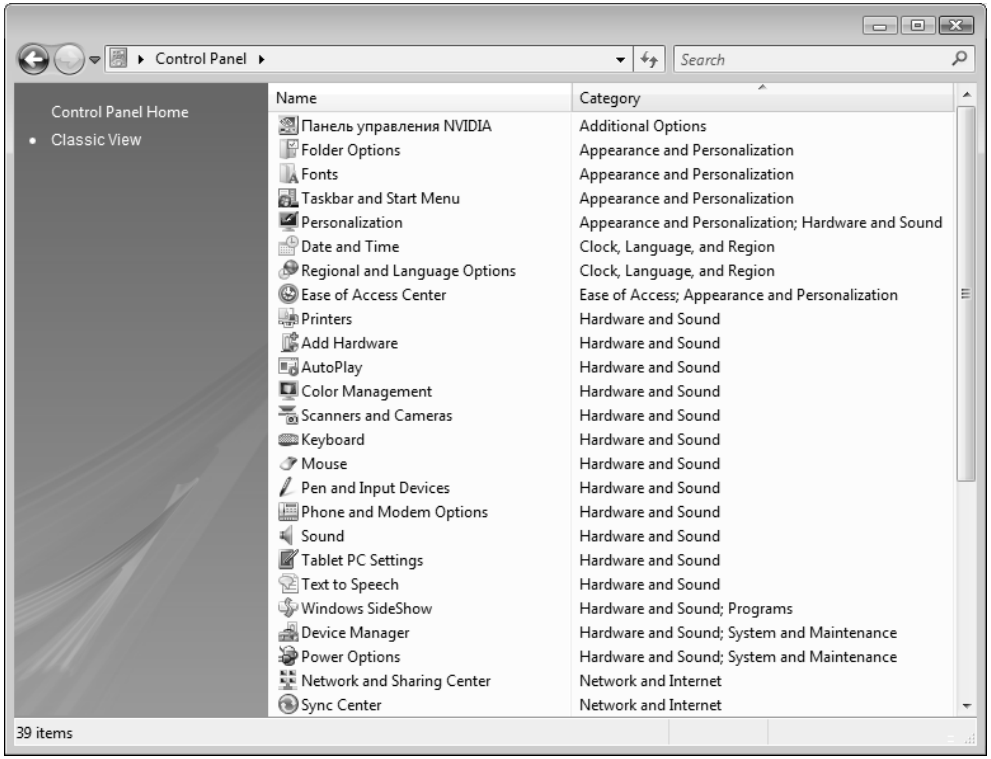


Рис. 3.2. Детальное представление задач на панели управления

В окне программы Windows Explorer (Проводник) все категории задач панели управления отображаются как узлы в дереве локальных папок (рис. 3.3). Благодаря этому можно быстро найти и выполнить нужную задачу, не отрываясь от просмотра содержимого папок. Если используется вид панели управления с делением по категориям *(см. далее)*, то и список задач в окне программы будет другим — менее детализованным.

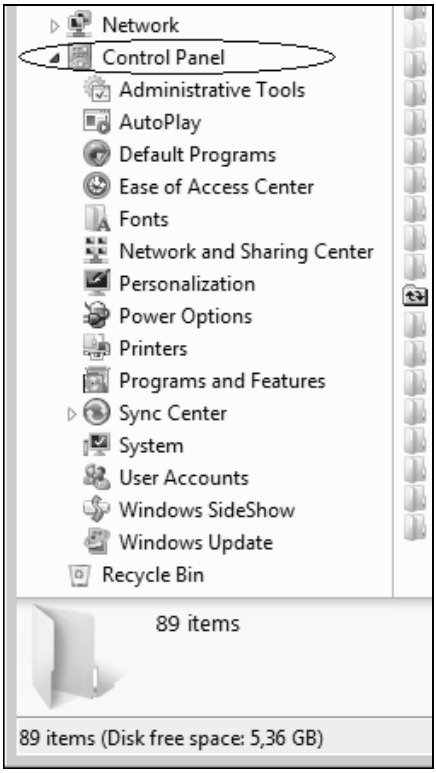


Рис. 3.3. Представление задач панели управления в окне локальных ресурсов компьютера

Выбор представления задач на панели управления

В системах Windows Server 2008 сохраняется возможность просмотра задач управления с группировкой по категориям, используемая по умолчанию в

Windows Vista. Для перехода к такому виду представления задач нужно на панели управления щелкнуть по ссылке **Control Panel Home** (Панель управления – домашняя страница) в левой части окна. В окне будут представлены все категории задач (рис. 3.4).

Рис. 3.4. Вид панели управления, когда задачи сгруппированы по категориям

Чтобы получить дополнительную информацию о категории, нужно подвести курсор мыши к значку соответствующей категории, и во всплывающем окне отобразится ее описание (см. рис. 3.4). Каждая категория представлена группой ссылок (основной и вспомогательными), поэтому для того чтобы открыть список подзадач, относящихся к некоторой категории, достаточно один раз щелкнуть мышью по основной ссылке.

На рис. 3.4 обратите внимание на то, что помимо названий категорий, показаны ссылки на некоторые часто используемые задачи, относящиеся к данной категории. Щелкнув по ссылке, можно сразу перейти к выполнению выбранной задачи конфигурирования системы (например, в категории **Hardware and Sound** (Оборудование и звук) можно сразу выбрать команды

настройки принтеров или мыши — ссылки **Printer** (Принтер) и **Mouse** (Мышь) соответственно). При этом новое окно не открывается, а все параметры отображаются в уже открытом окне панели управления. При необходимости можно вернуться к предыдущему окну, нажав кнопку со стрелкой на панели навигации (в верхнем правом углу окна).

Внимание!

Возле названий некоторых задач, показанных на рис. 3.4, виден значок с изображением щита  (такой значок встречается во многих окнах пользовательского интерфейса Windows Server 2008). Это означает, что для выполнения указанной задачи требуются права администратора, обычному пользователю она недоступна *(см. главу 14)*. Подобные значки отображаются всегда, вне зависимости от того, выключен контроль учетных записей (UAC) или нет.

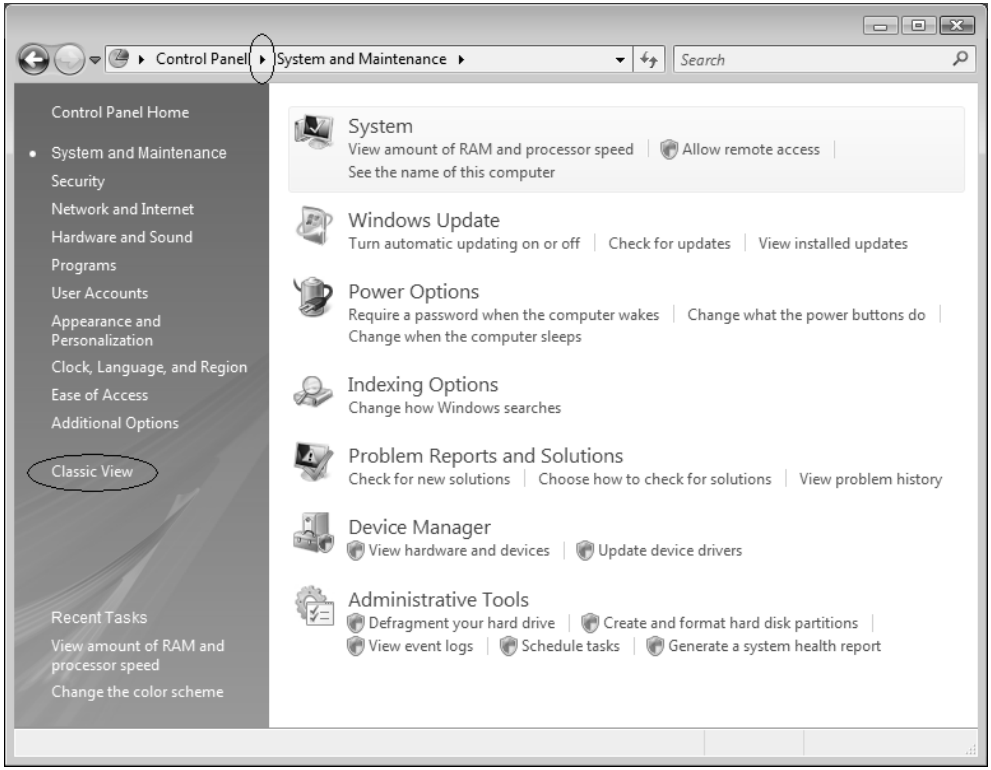


Рис. 3.5. Панель управления в режиме выбора задач по категориям

При работе с задачами, сгруппированными по категориям, удобнее пользоваться другим режимом представления панели управления (рис. 3.5): если выбрать любую категорию, то список категорий будет отображаться слева, при этом справа перечисляются все задачи, относящиеся к выбранной категории.

В этом случае можно одновременно видеть и имеющиеся категории, и их "содержание". Ссылка **Classic View** (Классический вид) позволяет вернуться к исходному виду панели управления, раздел **Recent Tasks** (Недавние задания) в левой нижней части окна содержит названия трех последних выполненных задач. Для быстрого перехода к категориям задач можно также пользоваться раскрывающимися списками в адресной строке: достаточно щелкнуть по стрелочке в виде треугольника (см. рис. 3.5) — и откроется список категорий или подзадач (рис. 3.6).

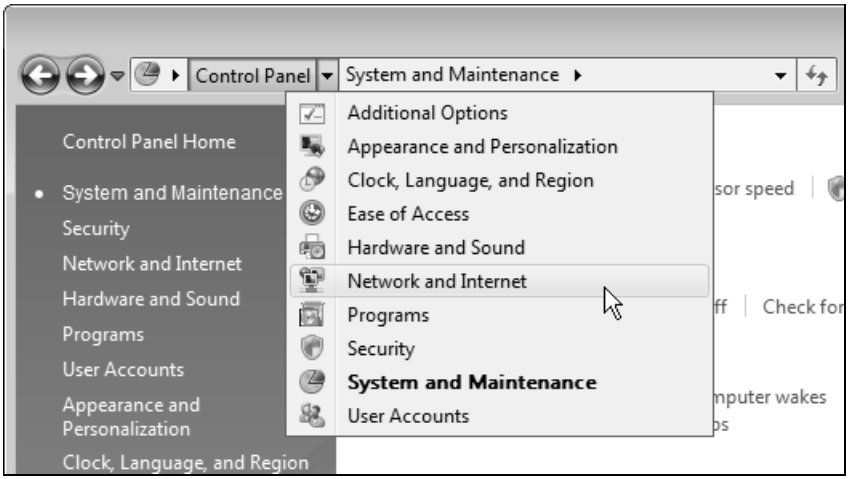


Рис. 3.6. Быстрый переход к определенной категории задач управления

Категории задач управления

Дадим краткое описание всех категорий задач, имеющихся на панели управления, включая перечень утилит, которые входят в их состав. Это позволит составить общее представление об имеющихся настройках системы и их группировке. (Обратите внимание на то, что некоторые задачи могут одновременно входить в разные категории.) Некоторые задачи — например,

Центр управления сетями, свойства панели задач, настройки времени и т. д. — можно быстро вызвать с помощью других значков и команд, имеющихся в пользовательском интерфейсе.

> ***Внимание!***
>
> Некоторые задачи (например, архивация и восстановление, Шифрование дисков BitLocker (BitLocker Drive Encryption) и т. д.) появляются на панели управления только после установки на сервере соответствующих компонентов.

В скобках, помимо названия, принятого в локализованной русской версии, указано имя панели управления, если ее можно запускать непосредственно (например, appwiz.cpl). Альтернативный вариант прямого доступа к задачам панели управления описан далее в *разд. "Непосредственный доступ к задачам панели управления"*.

- **System and Maintenance** (Система и ее обслуживание). Настройка и конфигурирование параметров работы компьютера, управление подсистемами, мониторинг производительности системы. Состав:
  - **System** (Система, sysdm.cpl);
  - **Windows Update** (Центр обновления Windows);
  - **Power Options** (Электропитание);
  - **Indexing Options** (Параметры индексирования);
  - **Problem Reports and Solutions** (Отчеты о проблемах и их решениях);
  - **Device Manager** (Диспетчер устройств);
  - **Administrative Tools** (Администрирование).

> ***Примечание***
>
> В системах Windows Server 2008 (как и в Windows Vista) отсутствует оснастка **Disk Defragmenter** (Дефрагментация дисков), входящая в состав Windows XP/Windows Server 2003.

- **Security** (Безопасность). Конфигурирование средств, обеспечивающих безопасность системы и информации. Состав:
  - **Windows Firewall** (Брандмауэр Windows);
  - **Windows Update** (Центр обновления Windows);

- **Windows Defender** (Защитник Windows);
- **Internet Options** (Свойства обозревателя, inetcpl.cpl).

Примечание

В отличие от систем Windows Vista, в Windows Server 2008 отсутствуют Security Center (Центр обеспечения безопасности, wscui.cpl) и соответствующая задача панели управления.

- **Network and Internet** (Сеть и Интернет). Подключение к Интернету, настройка веб-браузера Internet Explorer, локальной сети и доступа к общим ресурсам. Состав:
  - **Network and Sharing Center** (Центр управления сетями и общим доступом);
  - **Internet Options** (Свойства обозревателя, inetcpl.cpl);
  - **Offline Files** (Автономные файлы);
  - **Windows Firewall** (Брандмауэр Windows, Firewall.cpl);
  - **Sync Center** (Центр синхронизации).
- **Hardware and Sound** (Оборудование и звук). Конфигурирование параметров принтеров, клавиатуры, мыши, сканеров и другого подключаемого оборудования. Состав:
  - **Printers** (Принтеры);
  - **AutoPlay** (Автопуск);
  - **Sound** (Звук, mmsys.cpl);
  - **Mouse** (Мышь, main.cpl);
  - **Power Options** (Электропитание, powercfg.cpl);
  - **Personalization** (Персонализация);
  - **Scanners and Cameras** (Сканеры и камеры);
  - **Keyboard** (Клавиатура);
  - **Device Manager** (Диспетчер устройств);
  - **Phone and Modem Options** (Телефон и модем, telephon.cpl);
  - **Windows SideShow** — управление задачами, работающими на дополнительном экране;
  - **Pen and Input Devices** (Перо и устройства ввода);

- **Color Management** (Управление цветом);
- **Tablet PC Settings** (Параметры планшетного компьютера, TabletPC.cpl).

❒ **Programs** (Программы). Установка и удаление программ и компонентов Windows. Состав:

- **Programs and Features** (Программы и компоненты, appwiz.cpl);
- **Windows Defender** (Защитник Windows);
- **Default Programs** (Программы по умолчанию);
- **Windows SideShow**;
- **Get Programs Online** (Приобретение программ через Интернет).

❒ **User Accounts** (Учетные записи пользователей). Создание и конфигурирование пользовательских учетных записей. Содержит единственную, одноименную задачу.

❒ **Appearance and Personalization** (Оформление и персонализация). Настройка вида рабочего стола, выбор стиля пользовательского интерфейса, выбор заставки экрана. Настройка параметров меню **Start** (Пуск) и панели задач. Состав:

- **Personalization** (Персонализация);
- **Taskbar and Start Menu** (Панель задач и меню "Пуск");
- **Ease of Access Center** (Центр специальных возможностей);
- **Folder Options** (Свойства папки);
- **Fonts** (Шрифты).

❒ **Clock, Language, and Region** (Часы, язык и регион). Настройка региональных опций и параметров многоязычной поддержки. Состав:

- **Date and Time** (Дата и время, timedate.cpl);
- **Regional and Language Options** (Язык и региональные стандарты, intl.cpl).

❒ **Ease of Access** (Специальные возможности). Настройка опций для пользователей с плохим зрением, слухом или ограниченной подвижностью. Содержит единственную задачу:

- **Ease of Access Center** (Центр специальных возможностей).

❒ **Additional Options** (Дополнительные параметры). Здесь могут располагаться ссылки на управляющие программы, устанавливаемые производителями аппаратных и программных средств, например, утилиты управления видеоадаптером и т. п.

В последующих разделах мы познакомимся с важнейшими операциями по настройке параметров системы (в главах, посвященных администрированию и сетевым средствам, некоторые средства и оснастки будут рассмотрены особо).

Непосредственный доступ к задачам панели управления

Иногда пользователю необходимо иметь быстрый доступ к тем или иным средствам настройки системы (например, при частом просмотре и/или изменении параметров). Для любой задачи, имеющейся на панели управления, можно создать значок на рабочем столе или в произвольной папке:

1. Выберите задачу на панели управления, представленной в классическом виде.
2. Щелкните правой кнопкой мыши и в контекстном меню выполните команду **Create Shortcut** (Создать ярлык).
3. При необходимости значок можно с рабочего стола перетащить мышью в меню **Start** (Пуск) и запускать задачу из списка "закрепленных" программ.

Некоторые задачи конфигурирования системы отсутствуют на панели управления, однако их можно запустить, указав имя в меню **Start** (Пуск) или в командной строке:

desk.cpl	Display Settings (Параметры дисплея)
hdwwiz.cpl	Add Hardware Wizard (Мастер установки оборудования)
ncpa.cpl	Network Connections (Сетевые подключения)

С помощью следующей командной строки можно открыть окно **Folder Options** (Свойства папки) (см. рис. 2.45):

```
rundll32 shell32,Options_RunDLL
```

К любой задаче панели управления можно обратиться напрямую (например, из командной строки или из меню **Start** (Пуск), используя строку следующего вида: `control /name Microsoft.`*<английскоеНазваниеЗадачи>*[1]. Необходимо лишь удалить из имени все пробелы. Ниже перечислены примеры командных

[1] В локализованных версиях системы также нужно использовать английские названия.

строк, которые можно использовать для непосредственного вызова соответствующих задач:

```
control /name Microsoft.WindowsUpdate
control /name Microsoft.Personalization
control /name Microsoft.ProgramsAndFeatures
control /name Microsoft.System
control /name Microsoft.ProblemReportsAndSolutions
```

Свойства системы

Традиционное для систем Windows окно свойств системы в версиях Windows Vista/Windows Server 2008 претерпело значительную модернизацию. Для быстрого вызова этого окна обычно используют клавиши <Win>+<Pause/Break>; также можно выполнять команду **System** (Система) на панели управления.

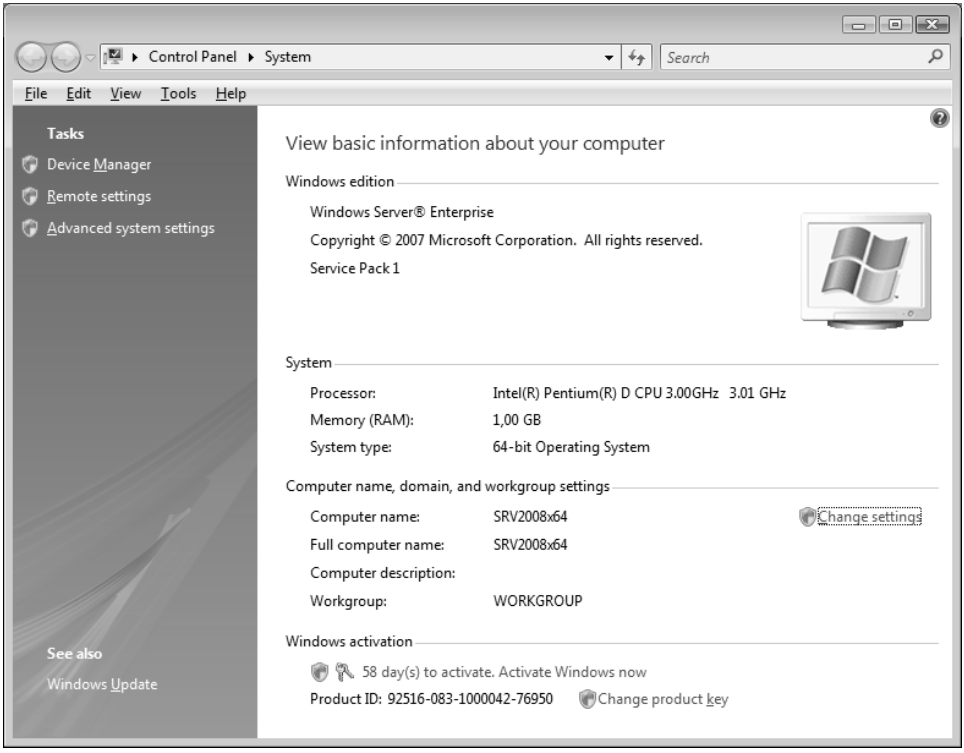


Рис. 3.7. Общие сведения о системе и компьютере

В открывающемся окне отображаются общие сведения о системе и компьютере, в том числе — редакция системы, основные параметры аппаратных средств, состояние активации (оставшееся время или логотип подлинности "Genuine Windows") и т. д. (рис. 3.7). Ссылки в левой части окна позволяют обратиться к различным средствам настройки аппаратных средств и подсистем — мы рассмотрим их подробнее в других разделах, посвященных администрированию систем.

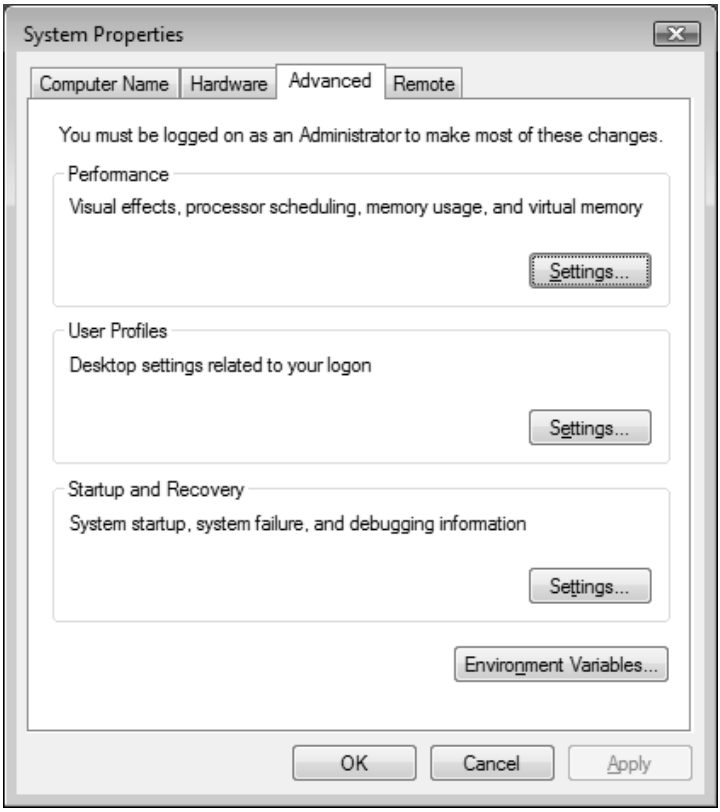


Рис. 3.8. Дополнительные возможности конфигурирования системы

Примечание

На рис. 3.7 обратите внимание на то, что системы Windows Server 2008 имеют в своем составе пакет обновлений Service Pack 1 (команда `winver` сообщает, что система имеет Version 6.0 (Build 6001: Service Pack1)).

Индексы производительности Windows (Windows System Performance Rating), определяемые для систем Windows Vista, в Windows Server 2008 не используются, поэтому в окне свойств системы нет никаких оценок.

Щелкнув по ссылке **Advanced system settings** (Дополнительные параметры системы), можно получить доступ к очень важному окну свойств системы (рис. 3.8), аналогичному тому, которое обычно используется в Windows XP/Windows Server 2003 (sysdm.cpl). Например, показанная на рисунке вкладка **Advanced** (Дополнительно) позволяет, среди прочего, настроить визуальные эффекты пользовательского интерфейса, изменить местоположение файла подкачки, управлять профилями пользователей, изменять опции загрузки систем и системные переменные.

Конфигурирование аппаратных средств

С вкладки **Hardware** (Оборудование) в окне свойств системы (см. рис. 3.8) можно запустить диспетчер устройств или определить поведение системы при поиске драйверов для устройств (для этого используется кнопка **Windows Update Driver Settings** (Поиск драйверов в Центре обновления Windows)).

Рис. 3.9. Выбор способа поиска драйверов для новых устройств

По умолчанию поиск выполняется автоматически (рис. 3.9), но при необходимости такое поведение можно и переопределить.

Диспетчер устройств можно запустить и непосредственно из окна системы — ссылка **Device Manager** (Диспетчер устройств) (см. рис. 3.7). В системе Windows Server 2008 он не претерпел практически никаких изменений по сравнению с Windows XP/Windows Server 2003. Диспетчер позволяет обнаруживать неработающие устройства, обновлять драйверы устройств и просматривать системные ресурсы, выделенные тому или иному устройству. Внешний вид программы и ее использование рассматривались в *главе 1*.

Центр обновления Windows (Windows Update)

В окне **Windows Update** (Центр обновления Windows) (рис. 3.10) можно проверить наличие на веб-сайте Microsoft обновлений для установленной операционной системы, настроить параметры проверки и загрузки этих обновлений, а также просмотреть журнал установки обновлений на компьютер. Это окно можно открыть из панели управления или непосредственно из меню **Start** (Пуск), выполнив одноименную команду в группе **All Programs** (Все программы).

Нужно отметить, что по команде **Windows Update** (Центр обновления Windows) из меню **Start** (Пуск) не происходит обращения к веб-сайту Windows Update (или Microsoft Update), как это реализовано в предыдущих версиях Windows — в системах Windows Vista/Windows Server 2008 все "лишние" операции скрыты от глаз пользователя.

По умолчанию предлагается автоматическая загрузка обновлений, однако порядок действий и расписание несложно изменить в любой момент *(см. главу 1)*. Помимо того, щелкнув по ссылке **Check for updates** (Проверка обновлений), можно в любой момент принудительно запустить проверку на наличие обновлений, после чего просмотреть список имеющихся обновлений и загрузить нужные на компьютер — процесс загрузки обновлений также отображается в окне центра обновления.

При наличии новых обновлений можно просмотреть их список и дополнительную информацию (для этого нужно дважды щелкнуть по названию обновления), и если какие-то необязательные обновления вам не требуются, их можно скрыть. Для этого нужно вызвать контекстное меню и выполнить соответствующую команду (**Hide update**). Ссылка **Restore hidden updates** (Восстановить скрытые обновления) (см. рис. 3.10) позволяет увидеть перечень тех об-

новлений, которые по каким-то причинам не устанавливались, а по ссылке **View update history** (Просмотр журнала обновлений) можно попасть в окно, где перечислены все полученные и установленные исправления, и удалить те, после появления которых работа системы или приложений стала неудовлетворительной *(см. разд. "Установка приложений и компонентов Windows")*.

Рис. 3.10. Центр обновления Windows предлагает загрузить и установить имеющиеся обновления

Если после установки обновлений требуется перезагрузка компьютера, соответствующий запрос выводится на экран для пользователя. Если по каким-то причинам перезагрузка откладывается, то будет появляться сообщение, напоминающее о необходимости выполнения этой операции — пользователь должен предпринять соответствующие действия.

Управление электропитанием

В системах Windows Vista/Windows Server 2008 существенно изменились механизм управления электропитанием и способы настройки параметров. Вме-

сто понятия *схемы электропитания* (power scheme) введен термин *план электропитания* (power plan), при этом вместо шести типовых схем электропитания Windows XP/Windows Server 2003 предлагается всего три стандартных плана (рис. 3.11) (можно создавать и собственные планы; обычно отображаются три плана, включая действующий, остальные скрываются).

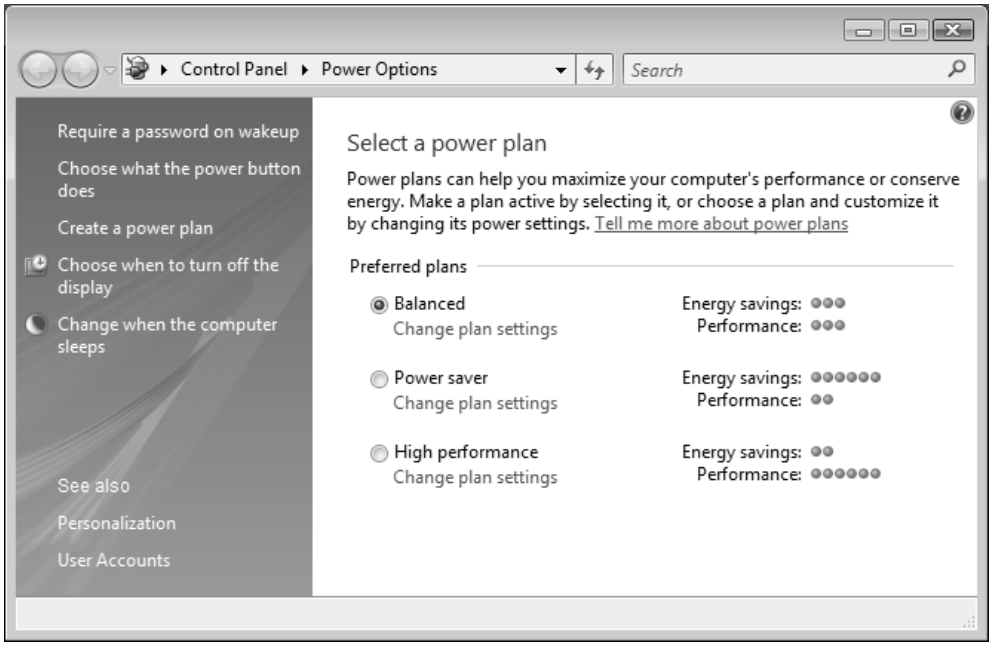


Рис. 3.11. Выбор плана электропитания

Количеством кружков визуально представлены основные характеристики каждого плана электропитания: сбережение энергии (что особо важно для компьютеров, питающихся от батарей) и производительность (быстрота реакции на действия пользователя). По умолчанию выбран сбалансированный план. Выбор плана осуществляется простым выбором переключателя в окне параметров (см. рис. 3.11), при этом указанный план сразу начинает действовать — ***никаких дополнительных подтверждений не требуется***.

Щелкнув по ссылке **Change plan settings** (Изменение параметров плана), можно открыть окно редактирования параметров выбранного плана электропитания (рис. 3.12). Здесь видны значения основных характеристик каждого стандартного плана. Для более детальной настройки режима энергосбереже-

ния нужно щелкнуть по ссылке **Change advanced power settings** (Изменить дополнительные параметры питания).

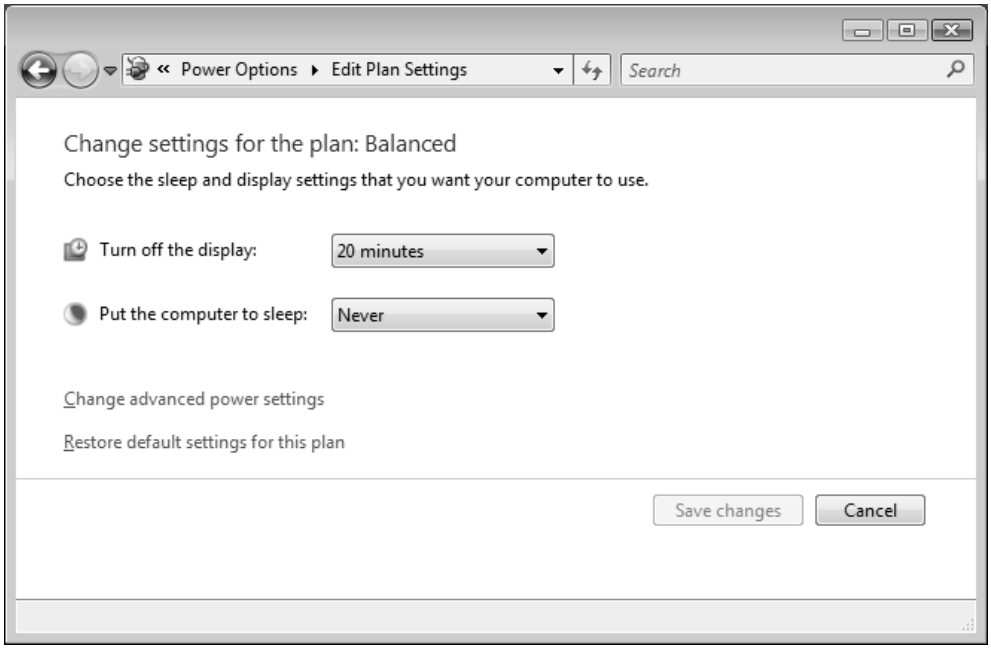


Рис. 3.12. Настройка параметров выбранного плана электропитания

В окне дополнительных параметров (рис. 3.13) можно определить поведение компонентов и самой системы для каждого режима или действия. Обратите внимание на то, что опция включения режимов *гибридного сна* (hybrid sleep) и *гибернации* (hibernate) присутствует в списке параметров (а также в списке опций кнопки питания — *см. ниже*), если только гибернация включена *(см. далее)*! Также нужно заметить, что при нажатии кнопки питания в меню **Start** (Пуск) (см. рис. 3.16) могут выполняться различные действия — для их выбора используется параметр **Start menu power button** (Кнопка питания меню "Пуск") (рис. 3.14). Системы Windows Server 2008 по умолчанию полностью выключаются.

В основном окне **Power Options** (Электропитание) можно также определить реакцию компьютера на нажатие кнопки питания (power button) на системном блоке — ссылка **Choose what the power button does** (Укажите действие кнопки питания). В специальном окне (рис. 3.15) помимо заданной операции, также указывается, нужен ли пароль при выходе из режима

сна. (В системах Windows Vista можно также индивидуально указывать действие для кнопки сна.)

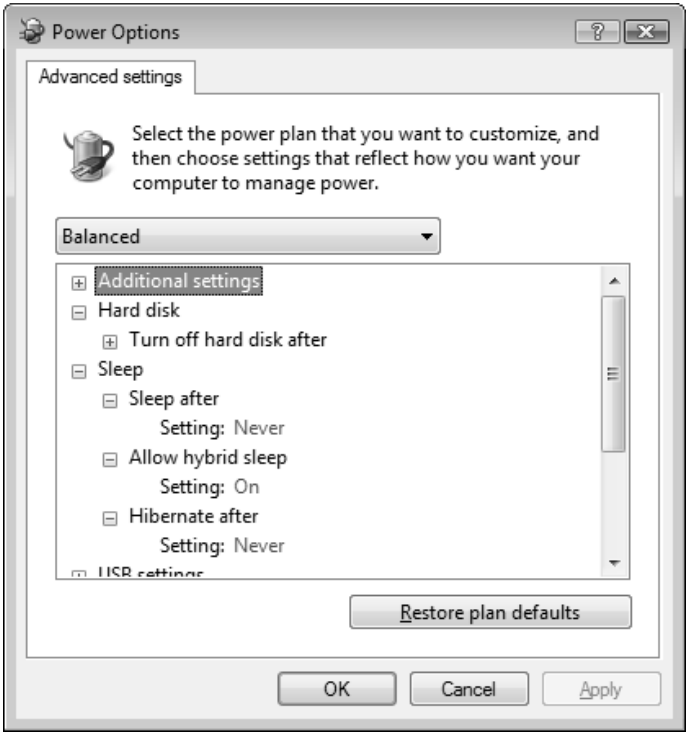


Рис. 3.13. Настройка дополнительных параметров электропитания

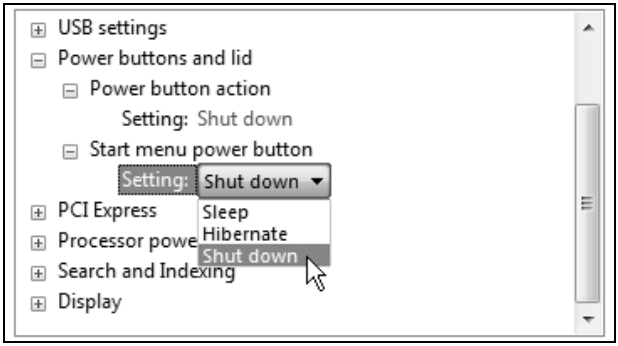


Рис. 3.14. Выбор действия, которое будет выполняться при нажатии кнопки питания в меню **Start**

Рис. 3.15. Определение действий при нажатии кнопки питания

В системах Windows Server 2008 при выключении компьютера с использованием меню **Start** (Пуск) (рис. 3.16, вверху, левая кнопка) пользователь может выбрать только то действие, которое определено для кнопки питания меню **Start** (Пуск) (в системах Windows Vista доступны также опции сна и гибернации). В меню, появляющемся после нажатия клавиш <Alt>+<F4> при закрытом рабочем столе (рис. 3.16, внизу), у пользователя имеются дополнительные возможности сохранения текущего рабочего состояния системы — опции **Sleep** (Сон) и **Hibernate** (Гибернация)[1]. В этих случаях все запущенные приложения и открытые окна будут восстановлены при включении системы (выход из режимов сна происходит, если несколько раз нажать на клавишу клавиатуры или повторно нажать кнопку питания — различия между режимами описываются в следующем разделе).

[1] Эта опция присутствует, если только компьютер ***не*** поддерживает *гибридный спящий режим*.

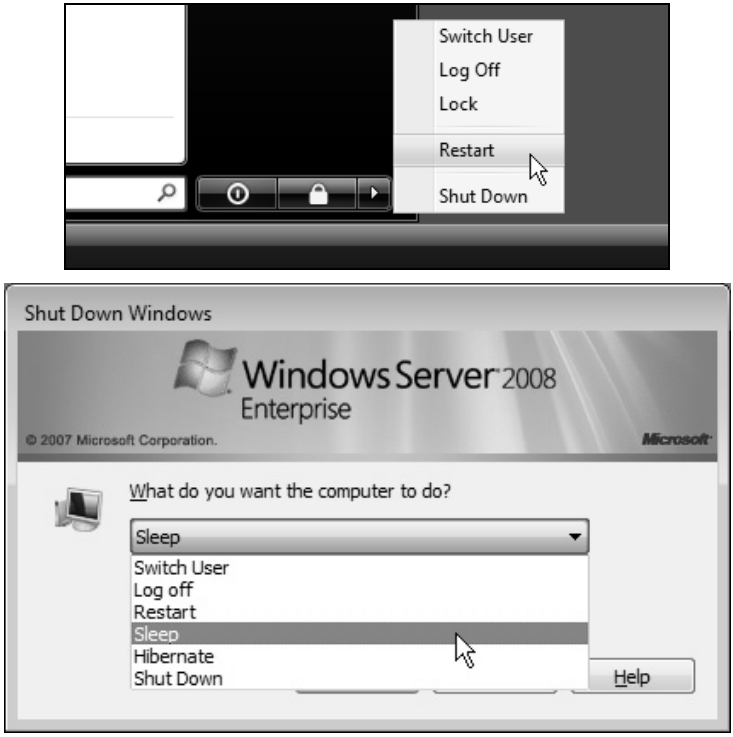


Рис. 3.16. Опции завершения работы
(выход из системы и выключение компьютера)

Рекомендуется при кратковременном (на несколько часов) прекращении работы с помощью кнопки выключения питания в меню **Start** (Пуск) переводить компьютер в режим сна (это может осуществляться и автоматически), а при длительном перерыве или при отключении питания пользоваться режимом гибернации, указывая эту опцию в меню завершения работы.

Энергосберегающие режимы Windows Server 2008

Поясним смысл некоторых новых терминов, связанных с энергосберегающими режимами систем Windows Vista/Windows Server 2008, поскольку некоторые возможности отсутствовали в предыдущих версиях и нужно хорошо понимать, что происходит в системе при использовании того или иного режима.

Системы Windows Vista/Windows Server 2008 поддерживают три следующих режима энергосбережения (в настольных системах и на портативных компьютерах):

- **сон**, спящий режим (Sleep, suspend-to-RAM) — рабочие данные (системные и прикладные) сохраняются *в памяти*, которая переключается в режим пониженного энергопотребления. Жесткий диск и монитор отключаются. Процессор может переключаться в режим пониженного энергопотребления или вообще отключаться — это зависит от параметров БИОСа (BIOS) компьютера; вентилятор блока питания работает. При включении системы данные считываются из памяти и через несколько секунд компьютер готов к работе — экран загорается, и все рабочие окна и приложения оказываются "на своих местах". Если "спящий" компьютер полностью отключить от сети, то начинается полная загрузка: на экране появится меню выбора систем (если их несколько), при загрузке системы будет сообщение о ее аварийном выключении;
- **гибернация**[1] (Hibernate, suspend-to-disk) — рабочие данные сохраняются *на жестком диске*. Процессор, память и диск выключаются, обычно при этом автоматически отключается и вентилятор блока питания[2] (при этом на лицевой панели индикатор питания может мигать, указывая на то, что компьютер не выключен окончательно). После включения питания вся информация считывается с жесткого диска и восстанавливается в памяти (при этом на экране монитора на темно-синем фоне появляется сообщение "Восстановление Windows"), система — включая приложения и открытые окна — возвращается в исходное рабочее состояние, однако на это требуется значительно больше времени, чем при выходе из спящего режима (почти как при обычной загрузке);
- **гибридный спящий режим** (Hybrid sleep) объединяет оба вышеназванных режима: данные сохраняются и *в памяти*, и *на жестком диске*, компьютер переходит в режим пониженного энергопотребления, вентиляторы отключаются. Если компьютер не обесточивается полностью (скажем, провод не выдергивается из сети), то при включении выполняется быстрый выход из режима сна; если же компьютер выключался полностью, то

---

[1] Такой термин используется в локализованной русской версии.

[2] Нужно помнить о том, что на современных компьютерах выключение питания (кнопкой на передней панели) не означает полное обесточивание устройств, которое достигается лишь при отключении сетевого провода или при использовании дополнительного выключателя на блоке питания (с задней части системного блока).

система восстанавливается из режима гибернации. Такой подход обеспечивает быстрое выключение системы при отсутствии риска потери данных (при полном отключении питания).

В системах Windows Server 2008 гибридный спящий режим является основным, и если он поддерживается БИОСом компьютера, то опция **Hibernate** (Гибернация) в меню выключения компьютера (см. рис. 3.16, внизу) вообще не появляется: при выборе опции **Sleep** (Сон) выполняется переход в данный режим.

Для использования режима гибернации и гибридного спящего режима требуется файл hiberfil.sys, создаваемый на загрузочном диске (обычно это диск C: — местоположение файла изменить нельзя!); в этом файле сохраняется содержимое оперативной памяти. Размер этого файла примерно равен объему оперативной памяти, установленной на компьютере.

Энергосберегающие режимы Windows Server 2008 тесно связаны с возможностями материнской платы и настройками БИОСа компьютера. (На возможность использования режима гибернации может также влиять работа некоторых аппаратных средств.) Команда `powercfg /a`, выполненная в окне командной строки, позволяет получить информацию о доступных режимах. Пример сообщений команды приведен ниже.

```
C:\>powercfg /a

The following sleep states are available on this system: Standby
 ( S1 S3 ) Hibernate Hybrid Sleep

The following sleep states are not available on this system:

Standby (S2)

        The system firmware does not support this standby state.

[В данной системе доступны следующие состояния спящего режима: Standby
 ( S1 S3 ) Hibernate Гибридный спящий

Следующие состояния спящего режима недоступны в данной системе:

Standby (S2)

        Системные микропрограммы не поддерживают ждущий режим.]
```

В данном случае опция **Hibernate** (Гибернация) в системе отсутствует, и всегда используется гибридный спящий режим (Hybrid Sleep). Если этот режим не поддерживается, то выбор опции **Sleep** (Сон) означает перевод компьютера в режим сна, а наличие опции **Hibernate** (Гибернация) зависит от возможностей материнской платы и параметров электропитания, выбранных в системе.

Внимание!

При необходимости для включения/отключения режима гибернации можно использовать команды `powercfg -H ON` и `powercfg -H OFF`. При отключении режима файл hiberfil.sys удаляется с загрузочного диска. (Отключить гибернацию и удалить файл hiberfil.sys можно также при помощи утилиты *Disk Cleanup* (Очистка диска), имеющейся в составе программной группы **All Programs** | **Accessories** | **System Tools** (Все программы | Стандартные | Служебные).)

Диагностика и устранение неполадок

В системах Windows Vista/Windows Server 2008 появились новые встроенные средства для выявления и решения проблем, возникающих как в работе самой системы (на аппаратном и/или программном уровне), так и при взаимодействии с подключенными устройствами.

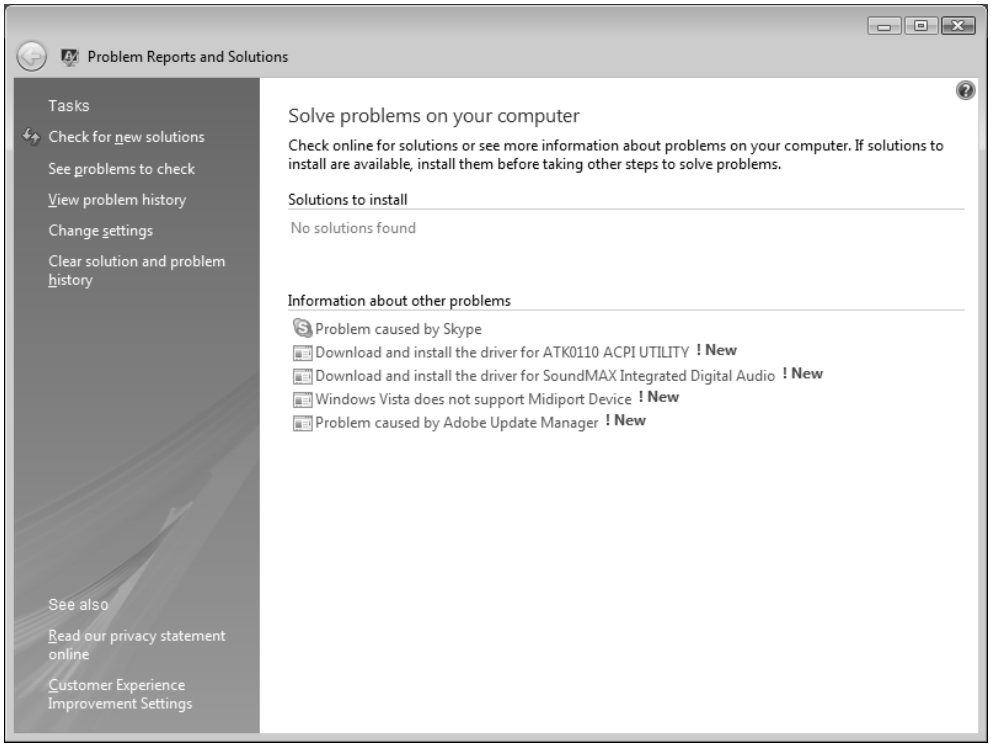


Рис. 3.17. Окно решений для устранения обнаруженных проблем

При подключении компьютера к Интернету средства диагностики позволяют сообщить компании Microsoft о возникших неполадках и получить рекомендации по их устранению (а также скачать обновления или новые драйверы).

Для того чтобы ознакомиться с информацией, собранной средствами диагностики, нужно на панель управления запустить задачу **Problem Reports and Solutions** (Отчеты о проблемах и их решениях) (категория **System and Maintenance** (Система и ее обслуживание)). В открывшемся окне (рис. 3.17) можно видеть результаты работы средств диагностики и проверить наличие проблем, а также решений для их устранения (в разделе **Solutions to install** (Устанавливаемые решения) отображаются имена обновлений и других файлов, которые следует загрузить с веб-сайта Microsoft). Если проблема ликвидирована, то решение можно удалить из списка.

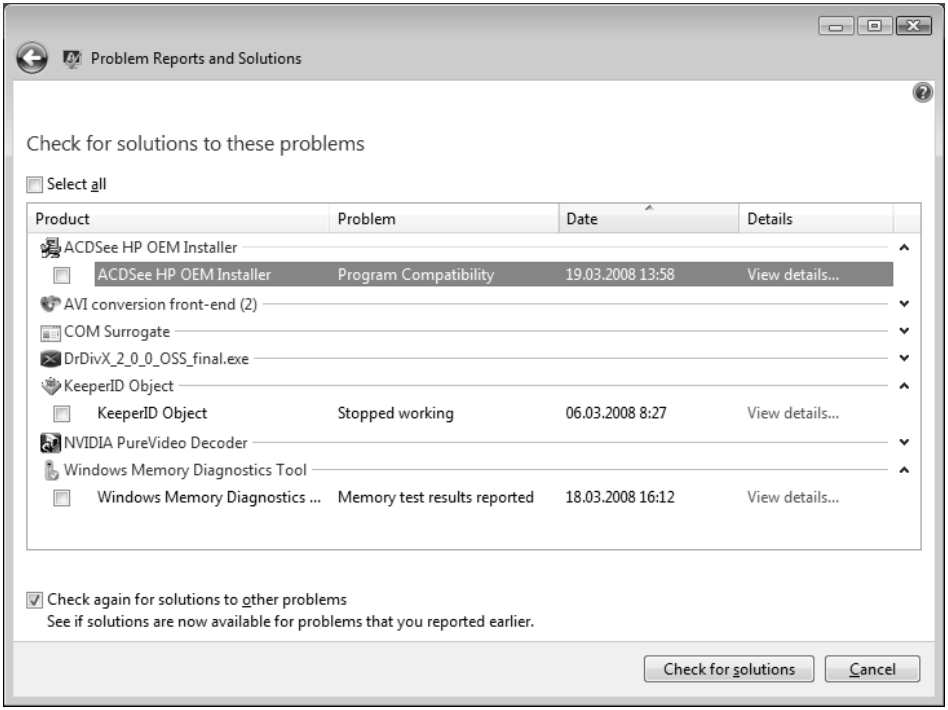


Рис. 3.18. Перечень проблем, обнаруженных в системе, для которых еще не выполнялся поиск решений

В разделе **Information about other problems** (Информация о других проблемах) на рис. 3.17 можно увидеть перечень решений, которые система предла-

гает для обнаруженных программных и аппаратных ошибок (также сообщается о наличии обновлений для установленных приложений). Если щелкнуть по ссылке, то появляется окно с описанием конкретной проблемы и ее решением. Например, может сообщаться о наличии драйвера устройства, который отсутствовал при установке системы, но который можно скачать, используя процедуру обновления Windows (Windows Update).

Если в списке проблем (рис. 3.18) (он отображается при выборе ссылки **See problems to check** (Показать проверяемые решения) в основном окне **Problem Reports and Solutions** (Отчеты о проблемах и решениях) окажутся такие, для которых не выполнялся поиск решений, то можно, устанавливая соответствующие флажки, выбрать строку, описывающую возникшую проблему, и нажать кнопку **Check for a solution** (Найти решение). По умолчанию решения ищутся автоматически, по мере появления неисправностей. В процессе поиска решений могут появляться запросы на отправку в компанию Microsoft дополнительной информации, необходимой для анализа ошибки — в этом случае можно увидеть, какая информация передается, после чего согласиться с выполнением операции или отказаться от нее.

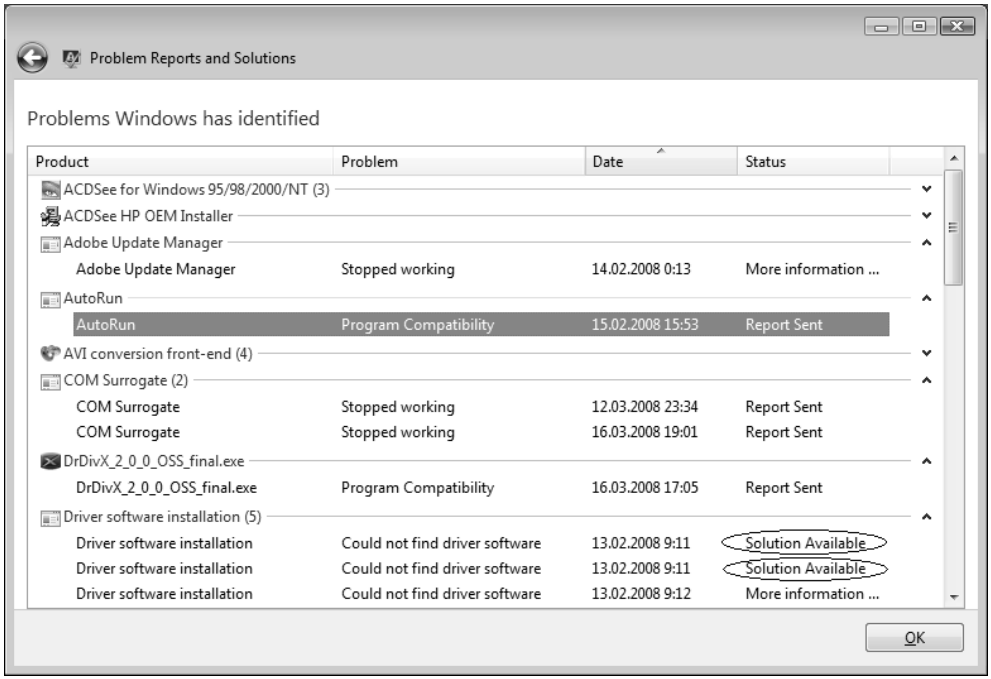


Рис. 3.19. Перечень проблем, обнаруженных в системе, с указанием наличия соответствующих решений

Периодически система Windows Server 2008 посредством всплывающих сообщений в области извещений на панели задач сама предлагает проверить "здоровье" системы и открыть окно **Problem Reports and Solutions** (Отчеты о проблемах и решениях). Рекомендуется периодически проверять сообщения диагностики и своевременно устранять обнаруженные проблемы.

Щелкнув по ссылке **View problem history** (Показать журнал проблем), можно просмотреть список всех отправленных отчетов (с описанием проблемы) и полученных решений (рис. 3.19). Все записи в этом журнале сгруппированы по названию приложений, с которыми возникли проблемы. Записи можно также сортировать по описанию проблемы, дате возникновения и состоянию (в списке легко увидеть, для каких проблем имеется решение (статус Solution Available)). Дважды щелкнув по записи, можно получить подробную информацию о проблеме.

Установка приложений и компонентов Windows

Категория **Programs** (Программы) на панели управления систем Windows Vista/Windows Server 2008 содержит различные задачи, относящиеся к установленным на компьютере приложениям и обновлениям системы. В основном, они реализуют те же возможности, для реализации которых в системах Windows XP/Windows Server 2003 служит утилита Установка/Удаление программ (Add or Remove Programs).

При выборе задачи **Programs and Features** (Программы и компоненты) открывается окно, в котором перечислены все приложения, установленные в системе (рис. 3.20). Для удаления программы используется соответствующая команда, появляющаяся на панели задач при выборе этой программы. Ссылка **View installed updates** (Просмотр установленных обновлений) в левой части окна позволяет увидеть результаты работы службы обновления Windows — при выборе ссылки в окне появится список всех обновлений, которые можно при необходимости удалить (рис. 3.21).

Большое значение имеет задача **Turn Windows features on or off** (Включение или отключение компонентов Windows) — аналог кнопки **Add/Remove Windows Components** (Добавить/Удалить компоненты Windows) в окне **Add or Remove Programs** (Установка или удаление программ), имеющемся в системах Windows XP/Windows Server 2003.

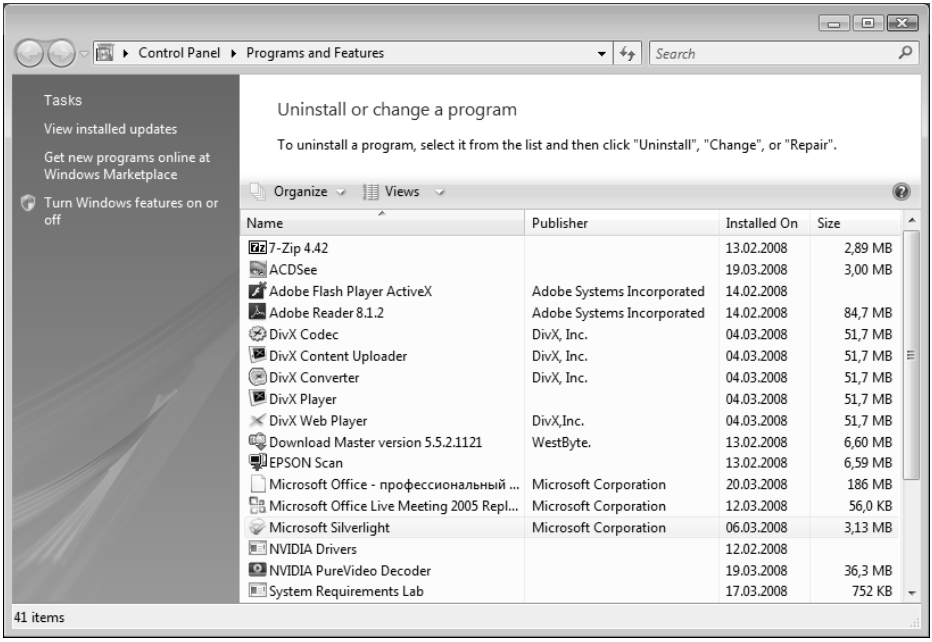


Рис. 3.20. Список установленных приложений

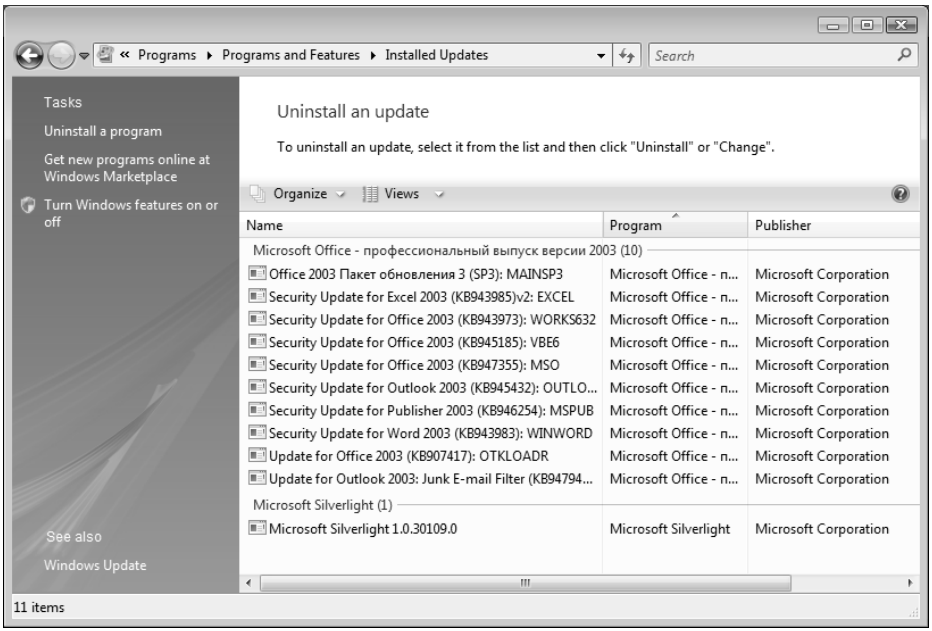


Рис. 3.21. Перечень установленных обновлений, которые можно удалять

В системах Windows Vista с помощью этой задачи можно изменить конфигурацию установленных компонентов и служб Windows — в системах Windows Server 2008 для этих целей используется совершенно новый механизм, реализуемый с помощью утилиты Server Manager (Диспетчер сервера), описываемой ниже.

Роли и компоненты сервера

В системах Windows Server 2003 имеется утилита *Manage Your Server* (Управление данным сервером), с помощью которой можно осуществлять централизованное управление установленными на сервере службами, а также обращаться к вспомогательным инструментам и службам поддержки, находить информацию об обновлениях, способах решения проблем и т. п. Эта утилита особенно полезна начинающим администраторам, поскольку она упрощает настройку и сопровождение сервера. Опытные администраторы могут сразу обращаться к специализированным оснасткам, необходимым для конкретных задач.

Тогда достаточно широко стало использоваться понятие *роли сервера* (server role), которое связывалось с определенными прикладными службами, работающими на сервере. Например, сервер мог выполнять роль DNS-сервера или контроллера домена Active Directory. В системах Windows Server 2008 концепция ролевого управления серверами и настройки системных сервисов получила дальнейшее развитие и привела к появлению принципиально новых средств администрирования, которым уже не стало альтернативы. Например, полностью изменился механизм установки компонентов Windows, который в предыдущих версиях запускался с панели управления при выборе опции **Add or Remove Programs** (Установка или удаление программ).

В системах Windows Server 2008 широко используются два новых термина:

- **роль** (Role) — совокупность системных сервисов и их настроек, используемая для реализации прикладной службы (см. список ролей). Применение определенной службы, например, службы печати, влечет за собой изменения в параметрах других служб — в частности, в настройках брандмауэра сетевого подключения. Установка роли приводит к согласованному изменению параметров системы, что упрощает задачу администратору и уменьшает вероятность ошибок. В состав роли входят определенные *службы роли* (Role Services), которые выбираются и запускаются индивидуально;

- **компонент** (Feature) — программный модуль или средство, используемые для выполнения частных административных задач или обеспечивающие дополнительные функциональные возможности (см. список компонентов).

Основным средством для управления сервером и установки/удаления ролей и компонентов систем Windows Server 2008 является оснастка **Server Manager** (Диспетчер сервера) (см. рис. 3.22), для которой в меню **Start** (Пуск) имеется закрепленный значок, а также соответствующий значок присутствует на панели быстрого запуска *(см. главу 2)*.

По умолчанию в системах Windows Server 2008 имеется 16 ролей; на x64-системах имеется дополнительная роль — Hyper-V. По умолчанию частично установлена только одна роль — File Services (Файловые службы). Список ролей приведен в табл. 3.1; он достаточно информативен сам по себе и не требует дополнительных комментариев — большинство ролей будут рассматриваться в других главах книги.

Таблица 3.1. *Роли серверов Windows Server 2008*

Active Directory Certificate Services (AD CS) (Службы сертификации Active Directory)
Active Directory Domain Services (AD DS) (Доменные службы Active Directory)
Active Directory Federation Services (AD FS) (Службы федерации Active Directory)
Active Directory Lightweight Directory Services (AD LDS) (Службы Active Directory облегченного доступа к каталогам)
Active Directory Rights Management Services (AD RMS) (Службы управления правами Active Directory)
Application Server (Сервер приложений)
DHCP Server (DHCP-сервер)
DNS Server (DNS-сервер)
Fax Server (Факс-сервер)
File Services (Файловые службы)
Hyper-V
Network Policy and Access Services (Службы политики сети и доступа)
Print Services (Службы печати)

Таблица 3.1 *(окончание)*

Terminal Services (Службы терминалов)
UDDI Services (Службы UDDI)
Web Server (IIS) (Веб-сервер (IIS))
Windows Deployment Services (Службы развертывания Windows)

В системах Windows Server 2008 по умолчанию имеются 35 компонентов (feature); изначально ни один из них не установлен. Список компонентов приведен в табл. 3.2. Многие компоненты будут рассматриваться подробно в соответствующих главах при описании тех или иных административных задач или прикладных служб.

Таблица 3.2. *Компоненты серверов Windows Server 2008*

.NET Framework 3.0 Features (Возможности .NET Framework 3.0)
BitLocker Drive Encryption (Шифрование диска BitLocker)
BITS Server Extensions (Серверные расширения BITS)
Connection Manager Administration Kit (CMAK) (Пакет администрирования диспетчера подключений)
Desktop Experience (Возможности рабочего стола)
Failover Clustering (Средство отказоустойчивости кластеров)
Group Policy Management (Управление групповой политикой)
Internet Printing Client (Клиент печати через Интернет)
Internet Storage Name Server (Сервер службы имен хранилищ Интернета)
LPR Port Monitor (Монитор LPR-портов)
Message Queuing (Очередь сообщений)
Multipath I/O (Многопутевой ввод-вывод)
Network Load Balancing (NLB; Балансировка сетевой нагрузки)
Peer Name Resolution Protocol (Протокол PNRP)
Quality Windows Audio Video Experience (qWave)

Таблица 3.2 *(окончание)*

Remote Assistance (Удаленный помощник)
Remote Differential Compression (Удаленное разностное сжатие)
Remote Server Administration Tools (Средства удаленного администрирования сервера)
Removable Storage Manager (RSM) (Диспетчер съемных носителей)
RPC over HTTP Proxy (RPC через HTTP-прокси)
Simple TCP/IP Services (Простые службы TCP/IP)
SMTP Server (Сервер SMTP)
SNMP Services (Службы SNMP)
Storage Manager for SANs (Диспетчер хранилища для сетей SAN)
Subsystem for UNIX-based Applications (Подсистема для UNIX-приложений)
Telnet Client (Клиент Telnet)
Telnet Server (Сервер Telnet)
TFTP Client (Клиент TFTP)
Windows Internal Database (Внутренняя база данных Windows)
Windows PowerShell
Windows Process Activation Service (Служба активации процессов Windows)
Windows Server Backup Features (Возможности системы архивации данных Windows Server)
Windows System Resource Manager (WSRM) (Диспетчер системных ресурсов)
WINS Server (WINS-сервер)
Wireless LAN Service (Служба беспроводной локальной сети)

Примечание

Важным элементом для работы в системе является компонент *Desktop Experience* (Возможности рабочего стола). При его установке в системе появляются новые стандартные приложения: программа-органайзер *Windows Calendar* (Календарь Windows), программы просмотра изображений *Windows Photo Gallery* (Фотоальбом Windows) и *Photo Gallery Viewer*, а также

проигрыватель *Windows Media Player*. Что очень важно — появляется возможность использования стиля (темы) Windows Vista *(см. главу 2)* со всеми ее дополнительными возможностями.

Установка ролей и компонентов

Окно оснастки **Server Manager** (Диспетчер сервера) представлено на рис. 3.22. Как можно видеть, в ее состав входят многие средства, которые традиционно входили (и продолжают входить) в состав главного инструмента администратора — оснастки **Computer Management** (Управление компьютером).

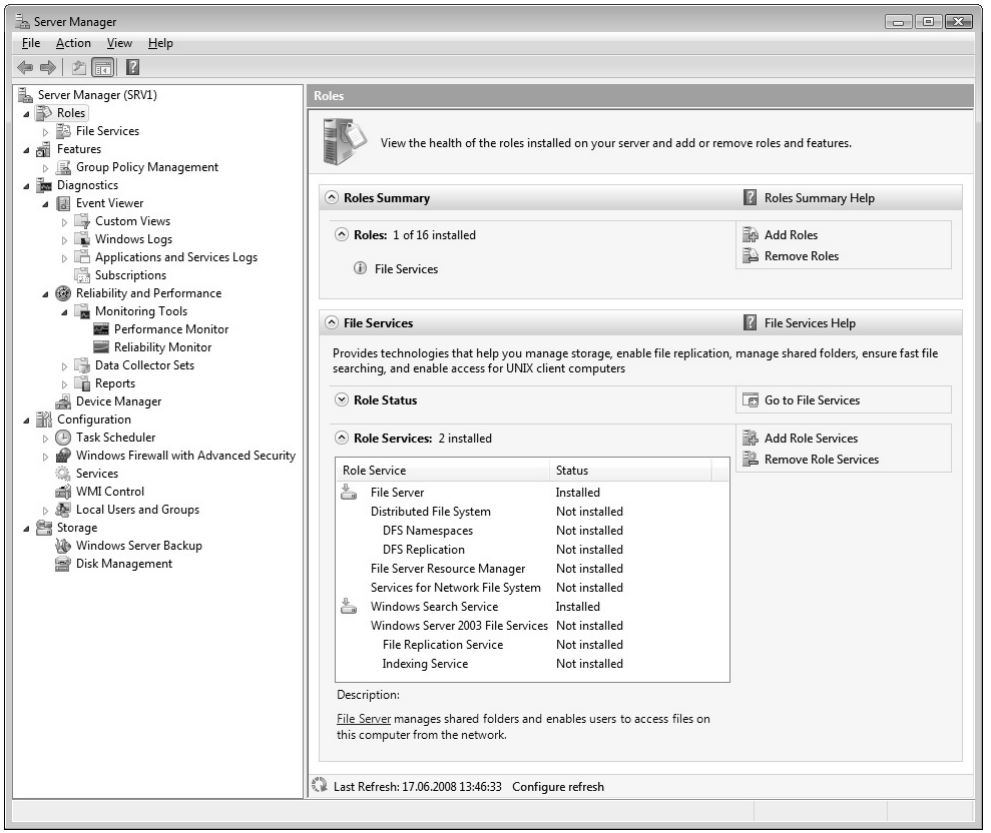


Рис. 3.22. Основное окно оснастки **Server Manager**

К числу этих средств относятся оснастки **Event Viewer** (Просмотр событий), **Device Manager** (Диспетчер устройств) и т. д. (сравните с рис. 3.52). Уникальной же возможностью оснастки **Server Manager** (Диспетчер сервера) является то, что только с ее помощью можно устанавливать и удалять роли и компоненты сервера. Возможности мониторинга установленных ролей (например, файловых служб) будут рассматриваться в соответствующих главах книги.

Все установленные на сервере роли видны в разделе **Roles Summary** (Сводка по ролям), также они представлены в дереве объектов в составе узла **Roles** (Роли). (Панели в окне оснастки можно скрывать и раскрывать, щелкая по стрелке, расположенной слева от названия панели.) Ниже перечня ролей располагаются информационные панели для каждой роли, где отображается состояние роли **Roles Status** (включающее число информационных и других сообщений), а также список служб роли (**Role Services**), если в состав роли входят несколько служб. Для компонентов отображается только одна панель, где указано количество и названия установленных элементов (рис. 3.23).

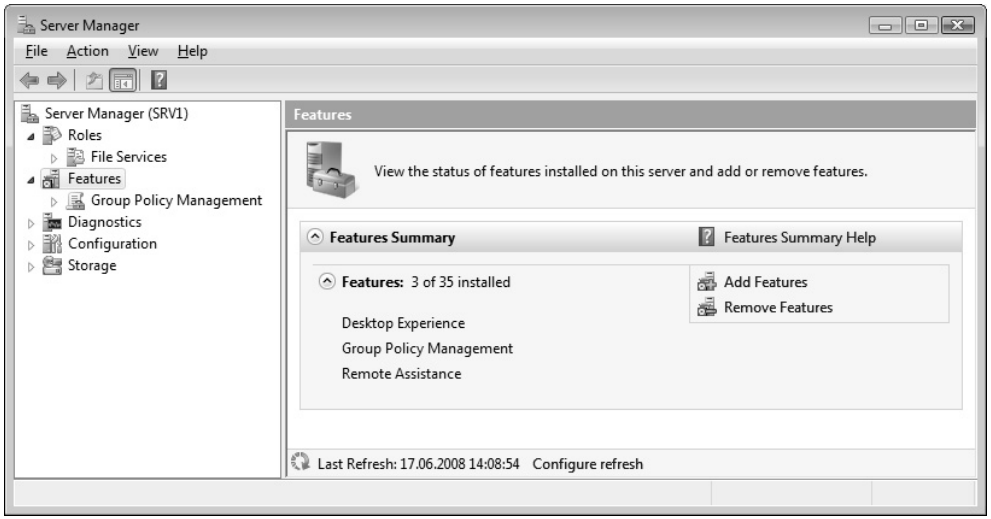


Рис. 3.23. Панель установленных компонентов

Обратите внимание на ссылки, имеющиеся на панелях в правой части, — с их помощью устанавливаются и удаляются роли и компоненты, а также отдельные службы роли.

Чтобы установить роль сервера, следует выбрать узел **Roles** (Роли) и щелкнуть по ссылке **Add Roles** (Добавить роли). В окне мастера добавления ролей

(рис. 3.24) нужно установить флажки около названий нужных ролей (обратите внимание на то, что для каждой роли имеется подробное описание), после чего нажать кнопку **Install** (Установить). (Уже установленные роли отмечены галочками; для их удаления следует использовать соответствующую ссылку на панели ролей.) После установки многих ролей требуется перезагрузка компьютера, в этом случае в окне мастера появляется предупреждение.

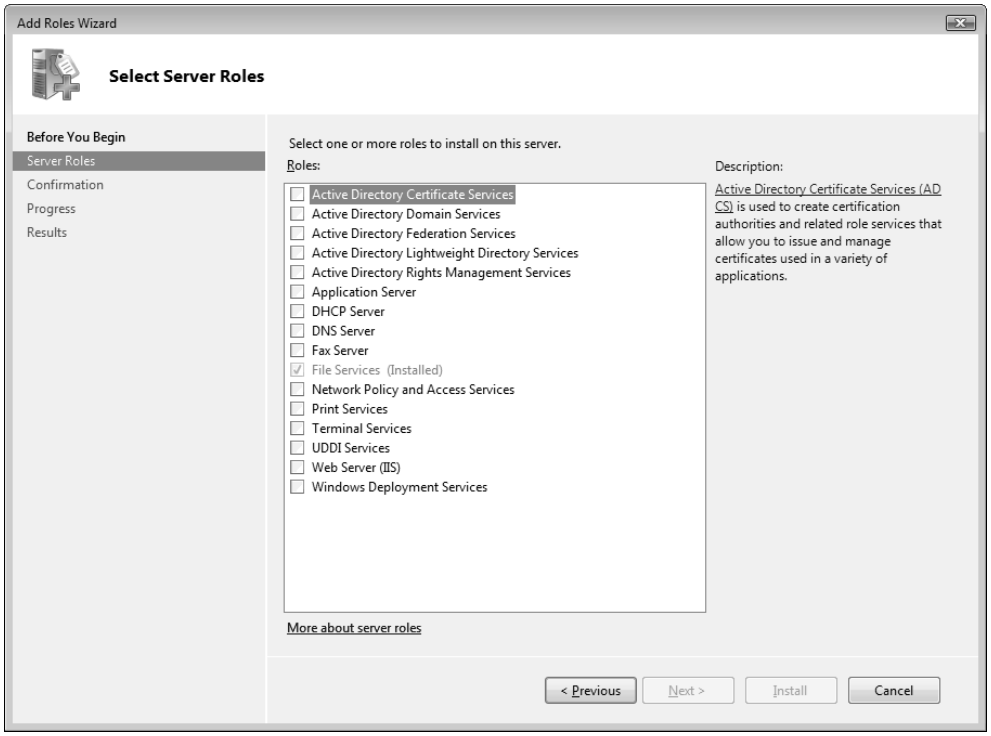


Рис. 3.24. Окно мастера добавления ролей

В процессе установки роли мастер может предложить на выбор список устанавливаемых *служб роли*. Например, в составе файловых служб имеется много разных сервисов (см. рис. 3.22), и при установке роли можно указать лишь некоторые из них. Службы роли можно добавлять или удалять и позднее, уже после установки роли.

Аналогичным образом добавляются компоненты сервера: в окне оснастки нужно выбрать узел **Features** (Компоненты) и щелкнуть по ссылке **Add Features** (Добавить компоненты). Затем в окне мастера добавления компонентов

(рис. 3.25) следует установить галочки для нужных компонентов и нажать кнопку **Install** (Установить).

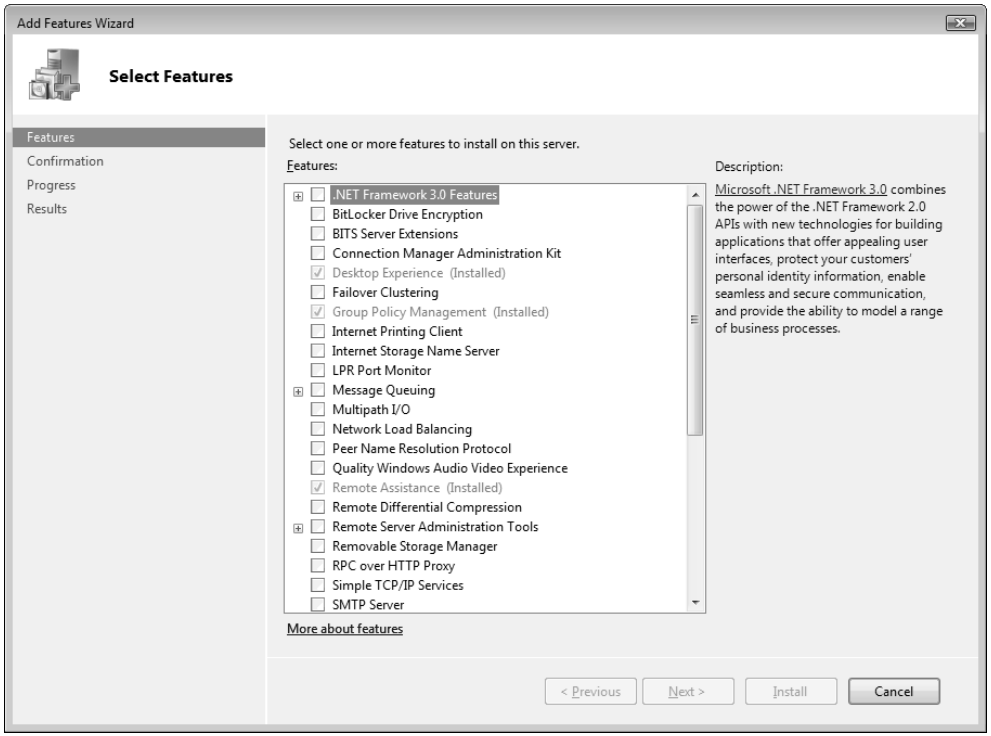


Рис. 3.25. Окно мастера добавления компонентов

Примечание

При установке компонентов могут появляться окна запросов на разрешение дополнительных действий или сообщения о выполненных изменениях: например, при установке компонента Remote Assistance (Удаленный помощник) меняются настройки встроенного брандмауэра, о чем сообщается в отдельном окне.

Для удаления ролей (или отдельных служб роли) и компонентов используются соответствующие ссылки на панелях **Roles Summary** (Сводка по ролям) и **Features Summary** (Сводка компонентов).

Программы по умолчанию

Задача **Default Programs** (Программы по умолчанию) или одноименный раздел в категории **Programs** (Программы) содержит подзадачи, связанные с установлением отношений между приложениями и типами файлов или носителей, работающими с этими приложениями (рис. 3.26).

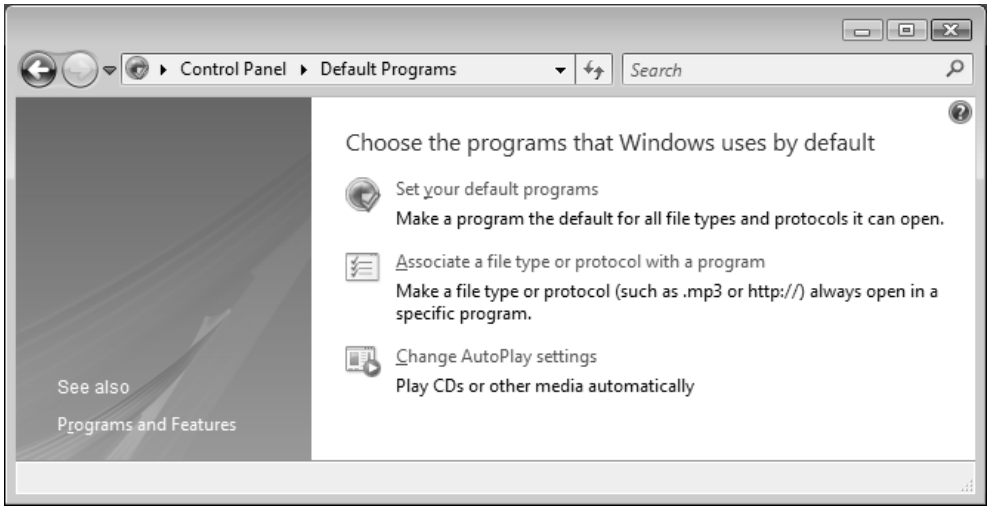


Рис. 3.26. Выбор программ для работы с файлами, протоколами или носителями

Задача **Set your default programs** (Задание используемых по умолчанию программ) позволяет указать, с какими файлами (расширениями файлов) связаны стандартные приложения Windows, например, такие как Windows Media Player, Windows Photo Gallery ("Фотоальбом Windows") и т. д. Можно выбрать программу для открытия *всех* типов файлов, которые выбранная программа поддерживает, а можно указать только конкретные форматы.

Задача **Associate a file type or protocol with a program** (Сопоставление типов файлов или протоколов…) выполняет функции отсутствующей в Windows Server 2008 вкладки **File Types** (Типы файлов) в окне **Folder Options** (Свойства папки) (это окно можно открыть с помощью команды **Tools** | **Folder Options** (Сервис | Свойства папки) в окне программы Windows Explorer (Проводника) — *см. главу 2*). В специальном окне (рис. 3.27) перечислены все известные системе типы файлов, указаны их название и программы, которые по умолчанию запускаются при открытии файла конкретного типа, но при

необходимости можно выбрать и другие программы. (Для быстрого поиска нужного расширения можно ввести с клавиатуры символ точки и первые символы расширения.)

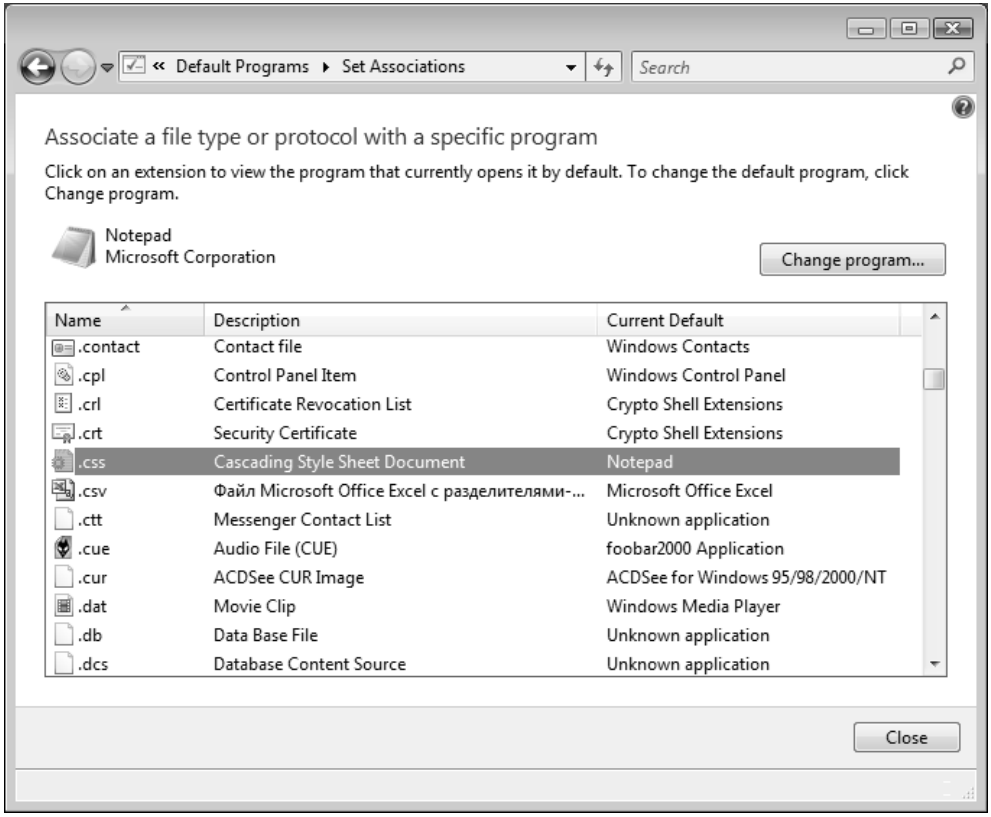


Рис. 3.27. Связь между форматами файлов и программами, используемыми для работы с ними по умолчанию

Выбрать или изменить программу, с помощью которой нужно открыть конкретный файл, можно в любой момент. Для этого в окне программы Windows Explorer (Проводника) нужно щелкнуть по имени файла правой кнопкой мыши и в контекстном меню выбрать команду **Open With** | **Choose Default Program** (Открыть с помощью | Выбрать программу). В открывающемся окне (рис. 3.28) перечислены рекомендуемые программы. Щелкнув по стрелке, отмеченной на рисунке кружком, можно выбрать любую другую программу из числа зарегистрированных в системе, а нажав кнопку **Browse** (Обзор),

можно выбрать любой исполняемый файл, хранящийся на диске. По умолчанию указанная программа будет использоваться для всех файлов выбранного типа, т. е. изменится сопоставление типов файлов (см. рис. 3.27). Если программа требуется лишь в частном случае, то флажок **Always use the selected program to open this kind of file** (Использовать выбранную программу для всех файлов такого типа) следует снять.

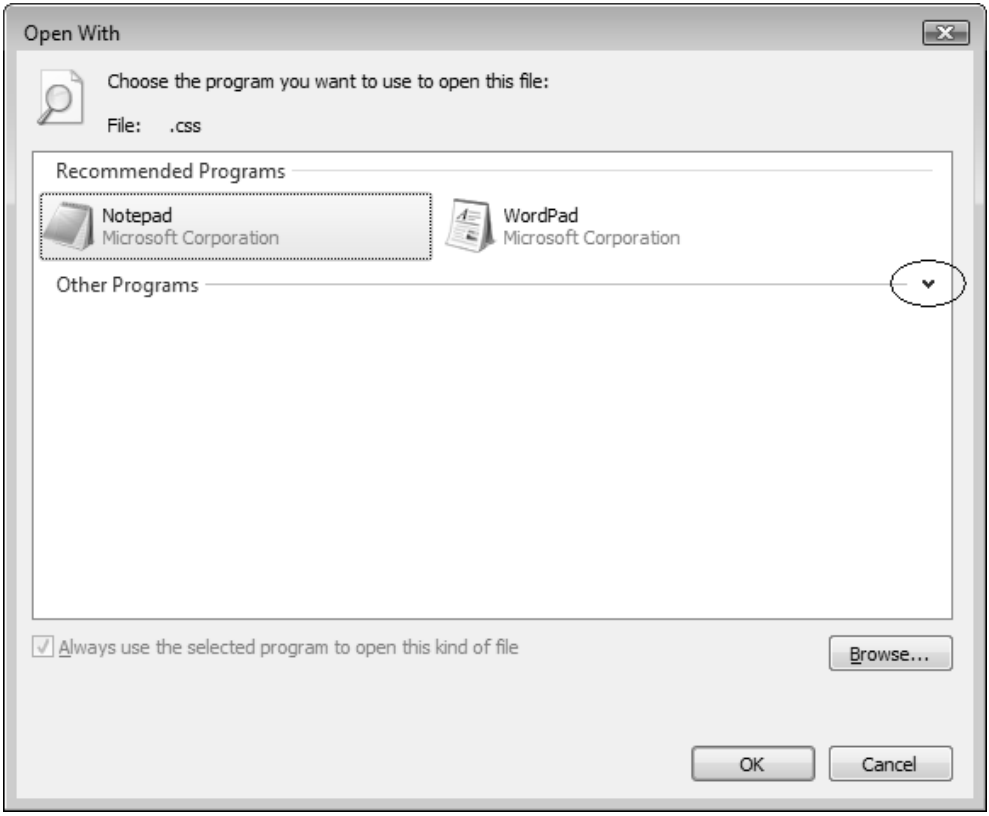


Рис. 3.28. Окно выбора программы, используемой для открытия конкретного файла или всех файлов данного типа

Открыть окно сопоставления типов файлов можно и с помощью командной строки следующего вида:

```
rundll32 shell32,OpenAs_RunDLL <расширениеФайла>
```

Например, для файлов формата PNG используется такая строка:

```
rundll32 shell32,OpenAs_RunDLL .png
```

После выполнения приведенной команды откроется окно, аналогичное показанному на рис. 3.28, и в нем можно выбрать нужную программу.

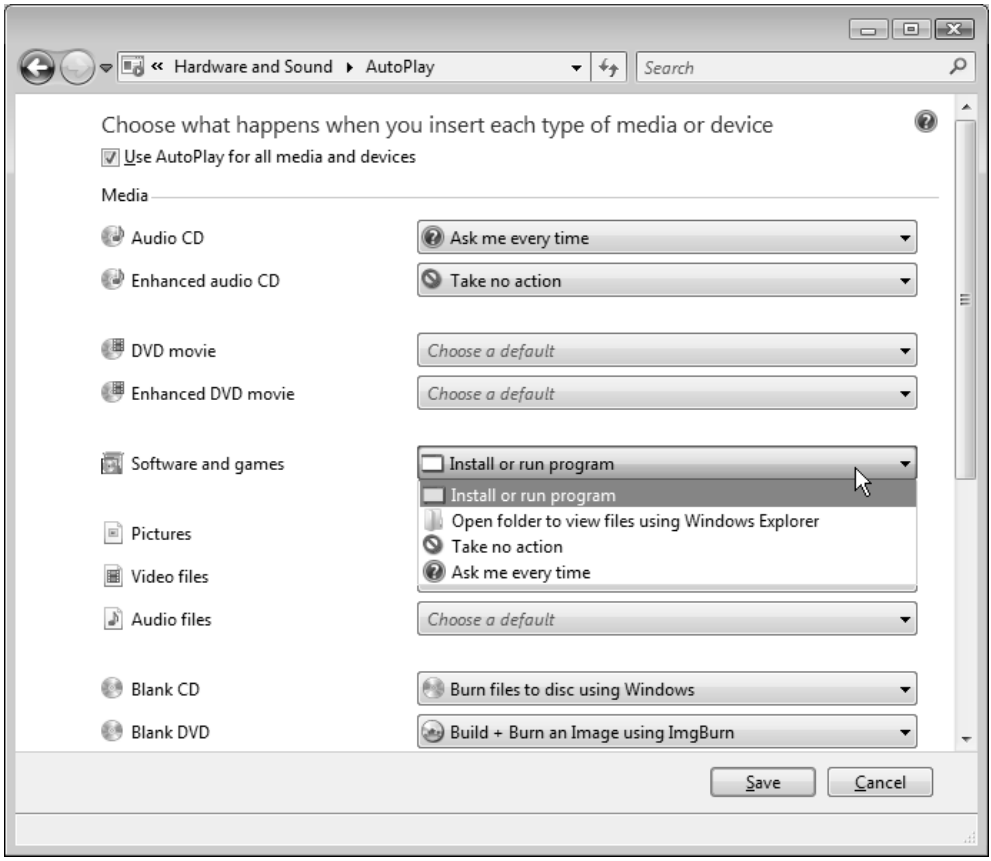


Рис. 3.29. Параметры автозапуска для различных типов носителей

Еще одна важная задача раздела **Default Programs** (Программы по умолчанию) — **Change AutoPlay settings** (Настройка параметров автозапуска). Она позволяет указать, какие действия будут (или не будут) выполняться при установке носителей различного типа или при подключении съемных или внешних устройств (рис. 3.29). Для каждого из перечисленных в окне носителей можно указать программу, которая будет запускаться; можно выбрать

опцию **Take no action** (Не выполнять никаких действий) или оставить действие по умолчанию. При выборе опции **Ask me every time** (Спрашивать каждый раз) окно для выбора выполняемой программы будет появляться каждый раз при смене носителя. В нижней части списка носителей и устройств имеется кнопка **Reset all defaults** (Восстановить умолчания), позволяющая сбросить все выбранные опции.

Режим совместимости программ

Рассмотрим еще одну возможность, которая не относится непосредственно к панели управления, однако непосредственно связана с работой приложений в среде операционной системы.

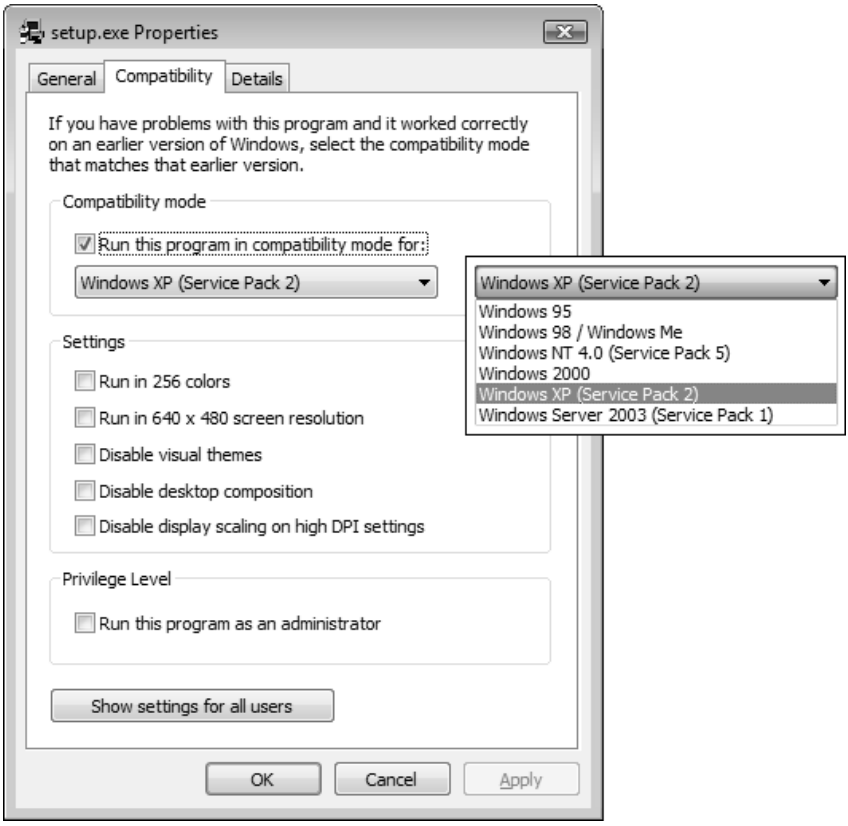


Рис. 3.30. Режим совместимости программ — выбор операционной системы и параметров экрана

Для установки и запуска программ, выпущенных до появления Windows Server 2008, имеется так называемый *режим совместимости*, который устанавливается индивидуально для любого исполняемого файла. Этот режим позволяет установить драйверы для устройств, не сертифицированных под Windows Server 2008, или запустить программы, которые проверяют версию операционной системы.

Чтобы задать режим совместимости, нужно открыть окно свойств исполняемого файла и перейти на вкладку **Compatibility** (Совместимость) (рис. 3.30). Установив флажок **Run this program in compatibility mode** (Запустить программу в режиме совместимости), следует в раскрывающемся списке выбрать операционную систему, для которой разработана данная программа (имеющиеся опции показаны на рисунке во врезке). Кроме того (необязательно), можно задать дополнительные параметры, относящиеся к разрешению экрана. Иногда для установки программы целесообразно повысить полномочия, и запускать ее от имени администратора. Оптимальные параметры для каждой конкретной программы определяются опытным путем, и здесь сложно дать общие рекомендации.

Настройка элементов пользовательского интерфейса

Подход к настройке параметров дисплея и элементов оформления в Windows Server 2008 несколько изменился: в системах Windows XP/Windows Server 2003 это делается в окне свойств экрана (**Display Properties**), а в Windows Vista/Windows Server 2008 появилось новое окно настроек, в которое можно попасть, щелкнув правой кнопкой мыши на рабочем столе и выбрав в контекстном меню команду **Personalize** (Персонализация). В окно личных настроек (рис. 3.31) можно также попасть с панели управления, выбрав задачу **Personalization** (Персонализация) (категория **Appearance and Personalization** (Оформление и персонализация) — *см. далее*). Все настройки, за исключением параметров дисплея, являются личными для каждого пользователя.

В окне **Personalization** (Персонализация) обратите внимание на ссылку **Adjust font size (DPI)** (Изменить размер шрифта) — она позволяет получить доступ к настройкам системных шрифтов (рис. 3.32), используемых в раз-

личных компонентах пользовательского интерфейса (эти параметры являются глобальными для всех элементов интерфейса, стилей, цветовых схем и т. п.). При увеличении масштаба все текстовые сообщения, заголовки окон и т. п. будут отображаться крупнее, что может быть удобно при ослабленном зрении или при работе с дисплеем, имеющим очень высокое разрешение. В этом случае "зернистость" отображения каждого символа будет меньше, поскольку для его представления используется больше точек (пикселов экрана).

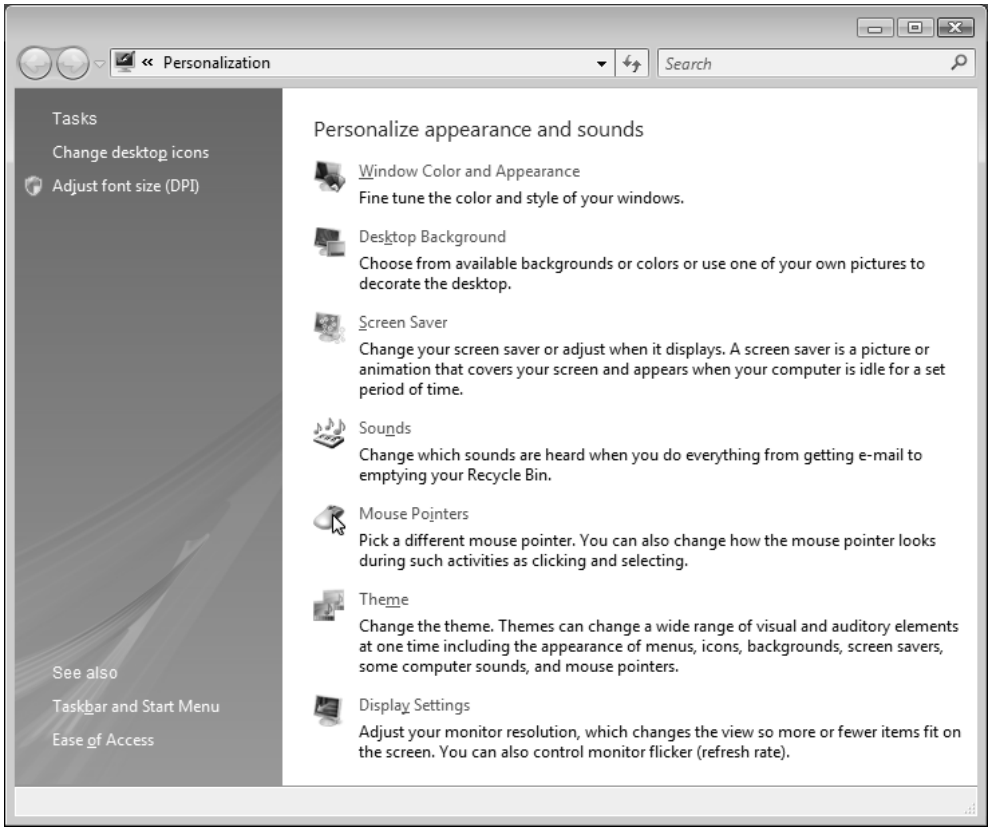


Рис. 3.31. Окно выбора личных параметров дисплея, оформления, звуковых эффектов и указателей мыши

Далее настройка параметров всех элементов пользовательского интерфейса системы будет рассмотрена подробно.

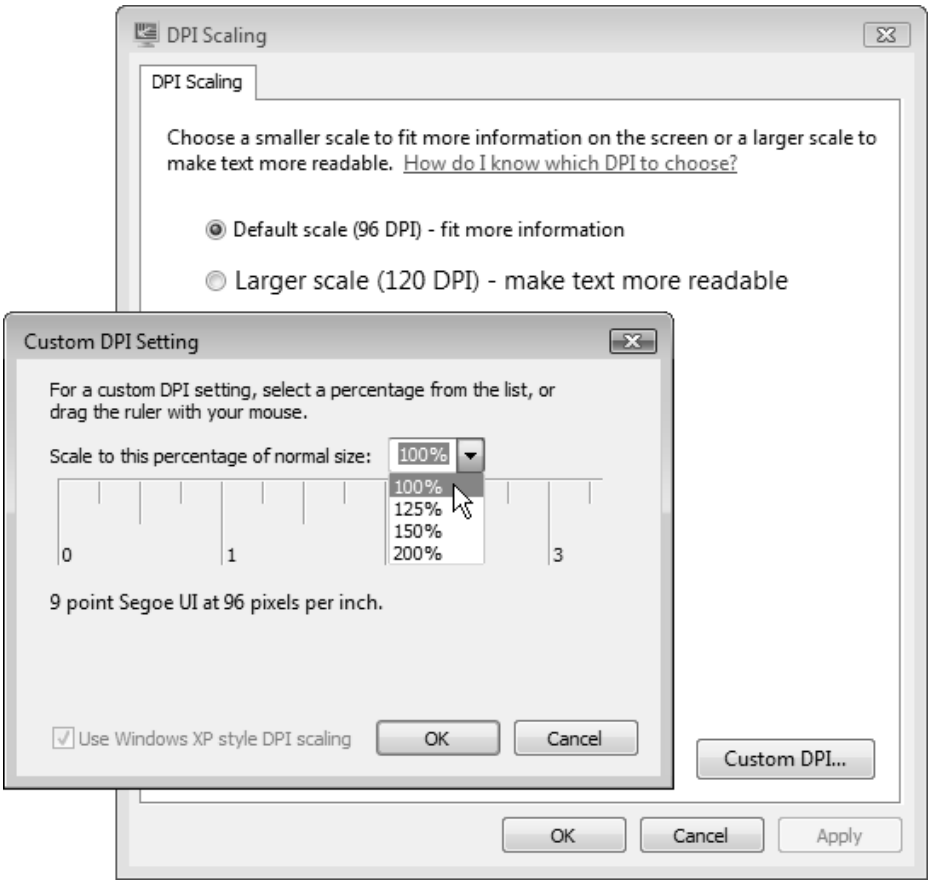


Рис. 3.32. Окно выбора размера системных шрифтов

Настройка параметров монитора

Важной и первоочередной задачей после установки системы, а также и в процессе работы с компьютером является настройка видеосистемы (поскольку не всегда устройства могут быть распознаны правильно при инсталляции системы или при их замене). Для осуществления этой операции в окне **Personalization** (Персонализация) (см. рис. 3.31) следует выбрать задачу **Display Settings** (Параметры дисплея). В окне настроек (рис. 3.33) можно менять разрешение экрана, глубину цвета, а также частоту развертки и другие параметры видеоадаптера и дисплея. При подключении *нескольких* устройств

отображения (от ЭЛТ-мониторов до плазменных панелей и проекторов) в этом окне можно индивидуально задать настройки для каждого дисплея и разрешить на них отображение рабочего стола; все операции будут одинаковыми для любого типа монитора.

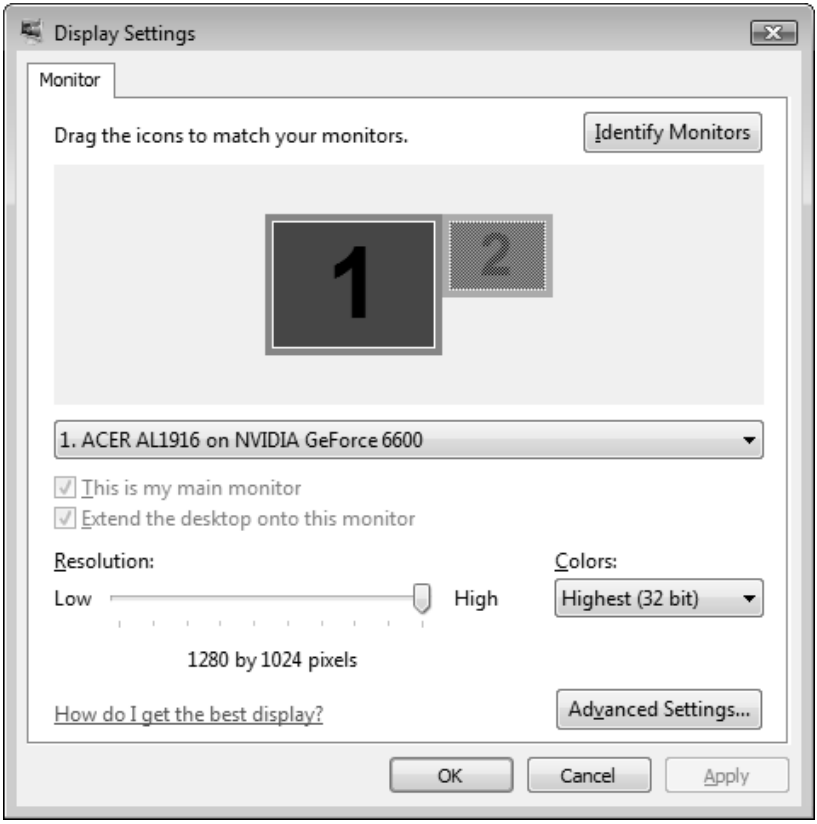


Рис. 3.33. Окно настройки параметров монитора (мониторов)

При необходимости можно более точно выбрать разрешение и частоту обновления экрана. Для этого следует нажать кнопку **Advanced Settings** (Дополнительно) и на вкладке **Adapter** (Адаптер) (рис. 3.34) установить разрешение, нажав кнопку **List All Modes** (Список всех режимов) и выбрав параметры в списке. Драйвер дисплея можно поменять, нажав кнопку **Properties** (Свойства) на вкладке **Monitor** (Монитор) — после этого в окне свойств монитора на вкладке **Driver** (Драйвер) нужно нажать кнопку **Update**

Driver (Обновить) и следовать указаниям стандартного мастера установки драйверов *(см. главу 1)*.

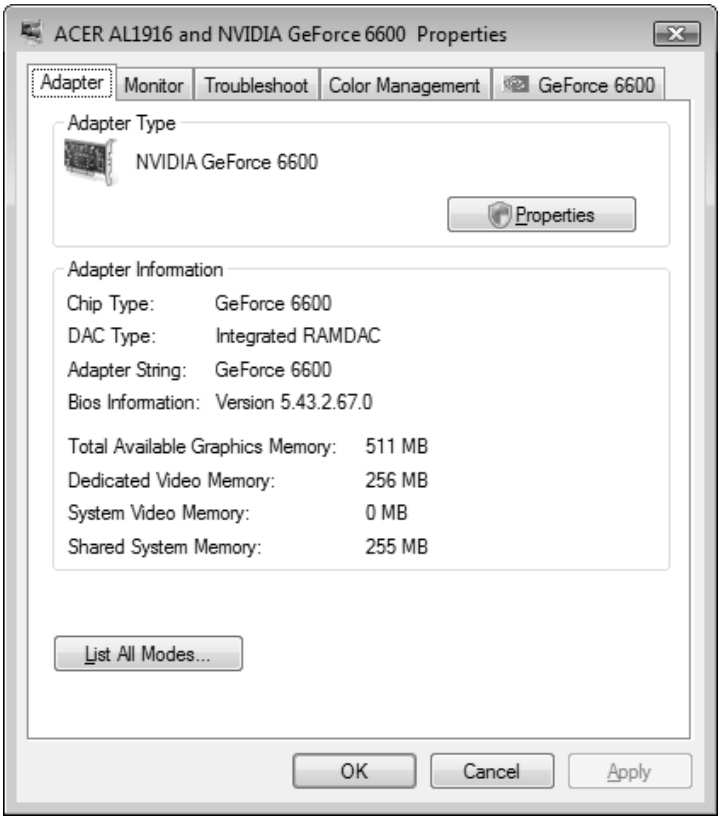


Рис. 3.34. Окно точной настройки параметров видеоадаптера и монитора

Выбор значков, отображаемых на рабочем столе

Изначально рабочий стол каждого пользователя, регистрирующегося в системе, пуст *(см. главу 2)* и на нем отображается единственный значок — **Recycle Bin** (Корзина). Тем не менее, присутствие на рабочем столе некоторых других служебных значков может оказаться полезным и желательным, поэтому пользователь может сам выбрать значки, которые будут отображаться на рабочем столе.

Для этого нужно выполнить следующие операции:

1. Откройте окно **Personalization** (Персонализация) (см. рис. 3.31) и щелкните по ссылке **Change desktop icons** (Изменить значки рабочего стола).
2. В открывшемся окне (рис. 3.35) поставьте флажки рядом с теми значками, которые должны отображаться на рабочем столе.

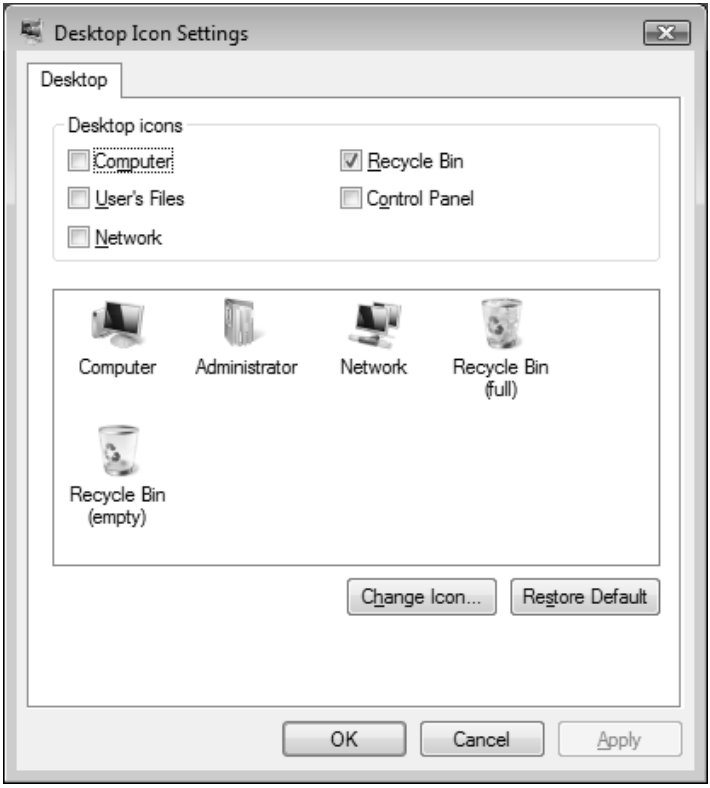


Рис. 3.35. Окно выбора значков, отображаемых на рабочем столе

3. Если предлагаемый набор изображений для отображения значков вас не устраивает, выделите значок, который вы собираетесь сменить, и нажмите кнопку **Change Icon** (Сменить значок). Кнопка **Restore Default** (Обычный значок) позволяет восстановить стандартное изображение выбранного значка.
4. После выполнения всех изменений закройте окно, нажав кнопку **ОК**.

Для настройки *размера* значков, отображаемых на рабочем столе, имеются два подхода. Щелкните на рабочем столе правой кнопкой мыши и выберите нужный размер в подменю **View** (Вид) — *классические* значки будут самыми маленькими из предлагаемых вариантов.

Второй подход менее очевиден. Откройте рабочий стол (свернув все открытые окна приложений), нажмите клавишу <Ctrl> и покрутите колесико мыши (если оно имеется) — размер значков будет меняться в бóльшую или меньшую сторону. В этом случае диапазон возможных размеров еще выше, чем при выборе из меню.

> ***Совет***
>
> Описанный выше прием изменения масштаба изображения в окне с нажатием клавиши <Ctrl> и использованием колесика мыши применим и к другим программам, например, к браузеру Internet Explorer, программе Windows Explorer (Проводник), редактору Microsoft Word и т. д.

Все значки, отображающиеся на рабочем столе, можно временно отключить. Для этого нужно щелкнуть правой кнопкой мыши на свободном участке рабочего стола и в контекстном меню выполнить команду **View** (Вид) — в списке опций имеется флажок **Show Desktop Icons** (Отображать значки рабочего стола), состояние которого и определяет вид рабочего стола. При повторном включении значков появляются все существовавшие ранее пиктограммы, при этом их положение на рабочем столе не меняется.

Стили (темы) оформления

В системах Windows Vista (которые имеют ядро, общее с Windows Server 2008) по умолчанию предлагается новый стиль рабочего стола — *Windows Aero (см. главу 2)*. Поскольку графические "излишества" на серверной платформе могут оказаться совершенно лишними, в системах Windows Server 2008 по умолчанию предлагается более простой, менее изящный и менее требовательный к параметрам видеоподсистемы так называемый *классический стиль* оформления (Windows Classic).

При необходимости стандартные возможности интерфейса Windows Server 2008 можно расширить и получить дополнительные или все возможности оформления, имеющиеся в Windows Vista. Для этого требуется:

1. Добавить компонент Desktop Experience (Возможности рабочего стола).
2. Запустить оснастку **Services** (Службы) и включить сервис Themes (Темы), установив сначала для него автоматический режим запуска.

После этого в списке тем появится дополнительная тема — Windows Vista, позволяющая выбирать две новые цветовые схемы — Windows Aero и Windows Vista Basic *(см. далее)*.

Для изменения темы достаточно выполнить следующие операции:

1. Откройте окно **Personalization** (Персонализация) (см. рис. 3.31) и выберите задачу **Theme** (Тема).
2. В списке **Theme** (Тема) (рис. 3.36) выберите тему, которая будет использована при оформлении рабочего стола, элементов окон, значков и звуков. Если *стандартная* тема модифицировалась, то она будет отображаться в списке как **My Current Theme** (Моя текущая тема), и ее можно сохранить, нажав кнопку **Save As** (Сохранить).
3. Закройте окно, нажав кнопку **OK**.

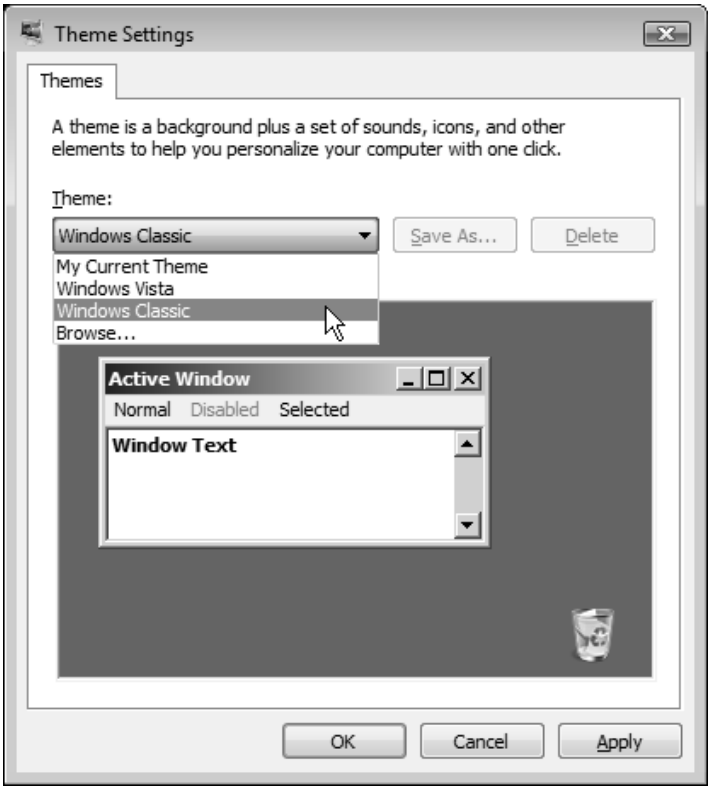


Рис. 3.36. Окно выбора темы оформления

Примечание

Темы и цветовые схемы *(см. ниже)* можно менять "на ходу", не перезагружая систему и не закрывая окон приложений.

После выбора темы можно изменить фоновый рисунок (обои) рабочего стола, выбрать заставку экрана, цветовую гамму и размер шрифтов, которые используются для надписей в окнах программ Windows Server 2008, после чего вернуться в окно **Theme** (Тема) и сохранить модифицированную тему для дальнейшего использования.

Оптимизация выбранного стиля оформления

При настройке пользовательского интерфейса всегда следует иметь в виду, что любые визуальные эффекты расходуют ресурсы системы и снижают ее производительность. Поэтому при выборе настроек интерфейса Windows Server 2008 следует руководствоваться критериями разумного компромисса. Для выбора сценария поведения базовых элементов пользовательского интерфейса (диалоговых окон, подсказок, раскрывающихся списков) выполните следующие операции:

1. На панели управления выберите задачу **System** (Система) (категория **System and Maintenance** (Система и ее обслуживание)). (Альтернативный подход — нажать клавиши <Win>+<Pause/Break>.)
2. В открывшемся окне (см. рис. 3.7) щелкните по ссылке **Advanced system settings** (Дополнительные параметры системы).
3. В традиционном для Windows окне свойств системы на вкладке **Advanced** (Дополнительно) (см. рис. 3.8) в группе параметров **Performance** (Быстродействие) нажмите кнопку **Settings** (Параметры).
4. В следующем окне (рис. 3.37) на вкладке **Visual Effects** (Визуальные эффекты) можно модифицировать параметры пользовательского интерфейса с учетом производительности компьютера. (В нашем примере видно, что для серверной платформы выбирается минимум "украшательств", даже при использовании стиля Windows Vista Classic.)

   Имеются четыре опции:

   - **Let Windows choose what's best for my computer** (Восстановить значения по умолчанию). Эта опция установлена по умолчанию, и ее не рекомендуется изменять неопытным пользователям. В этом случае система сама определяет параметры в соответствии с возможностями аппаратных средств;

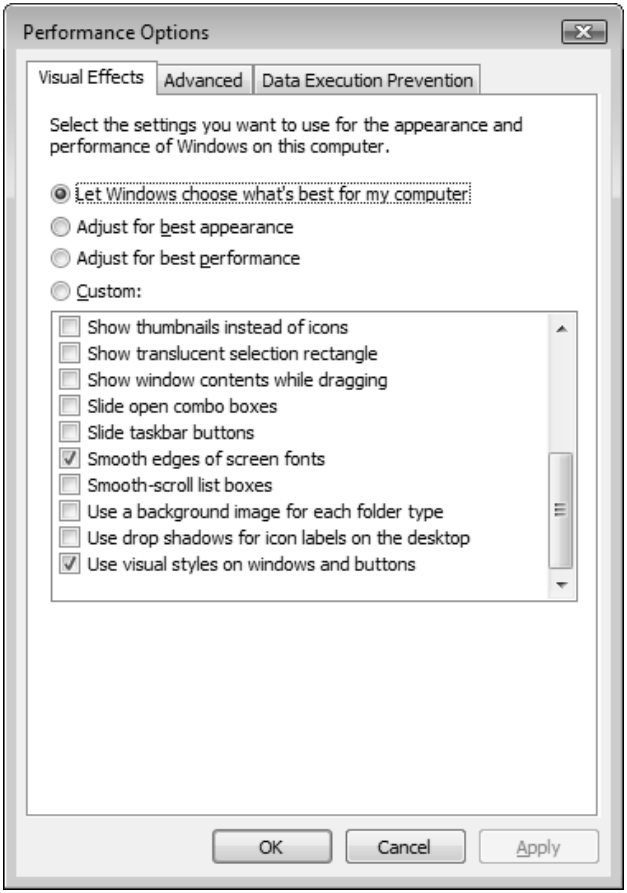


Рис. 3.37. Тонкая настройка визуальных эффектов, используемых в системе, с учетом производительности компьютера

- **Adjust for best appearance** (Обеспечить наилучший вид). Эту опцию можно выбрать при работе на мощных компьютерах при высоких требованиях к интерфейсу системы;
- **Adjust for best performance** (Обеспечить наилучшее быстродействие). Данная опция полезна для компьютеров средней мощности, когда основной акцент делается на производительности компьютера;
- **Custom** (Особые эффекты). Эту опцию рекомендуется использовать опытным пользователям, которые могут подобрать максимально сбалансированный набор параметров для своего компьютера.

5. После выбора параметров закройте окно, нажав кнопку **ОК**.

Цветовые схемы и другие параметры стиля оформления

Для выбранного стиля (схемы) оформления пользовательского интерфейса можно модифицировать цветовую гамму и другие элементы оформления (размеры и стиль окон и шрифтов и т. д.). Наибольшие возможности предоставляет схема Windows Aero, которая становится доступной после установки темы Windows Vista *(см. ранее разд. "Стили (темы) оформления")*. Сначала рассмотрим настройку параметров стиля "по максимуму" — для схемы Windows Aero.

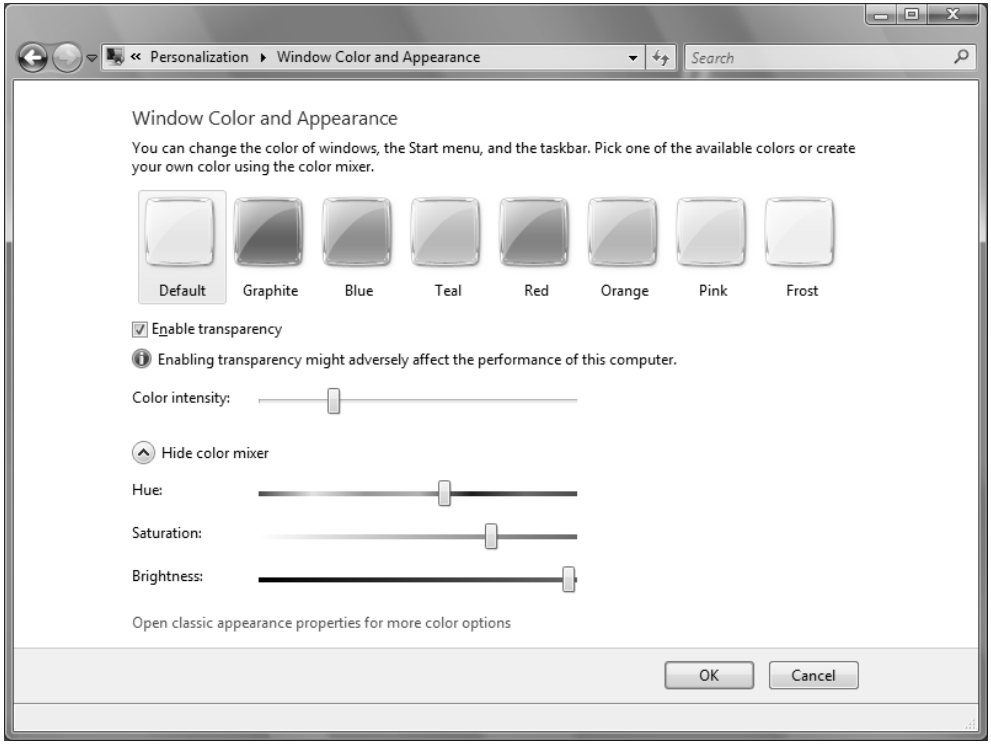


Рис. 3.38. Выбор цветовой гаммы и прозрачности окон, а также настройка дополнительных параметров пользовательского интерфейса

Для выбора цветовой схемы или изменения параметров стиля необходимы следующие действия:

1. Откройте окно **Personalization** (Персонализация) (см. рис. 3.31) и выберите задачу **Window Color and Appearence** (Цвет и внешний вид окон).

2. Цветовую гамму можно изменить, выбрав ее значок на панели (рис. 3.38). Флажок **Enable transparency** (Включить прозрачность) позволяет управлять прозрачностью окон. Ползунок **Color intensity** (Яркость цвета) позволяет подобрать предпочитаемый оттенок (если щелкнуть значок **Show color mixer** (Показать настройку цветов), то появятся три регулятора, с помощью которых можно выбирать любой цвет). Данная панель отображается только при использовании цветовой схемы Windows Aero!

   Ссылка **Open classic appearance properties…** (Открыть свойства классического внешнего вида…) позволяет получить доступ к окну выбора цветовых схем и эффектов **Appearance Settings** (Параметры оформления) (рис. 3.39). Такое окно появляется *сразу* после выбора задачи **Window Color and Appearence** (Цвет и внешний вид окон), если используется тема Windows Classic или цветовая схема Windows Vista Basic (Windows Vista – упрощенный стиль).

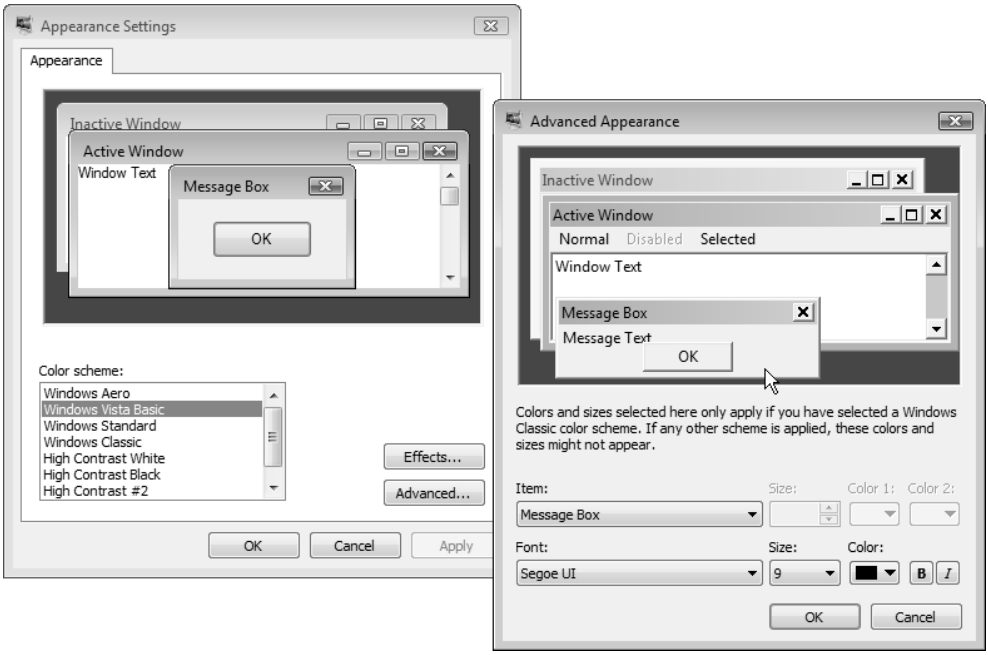


Рис. 3.39. Окно тонкой настройки элементов пользовательского интерфейса

3. Для сохранения изменений параметров нажмите кнопку **ОК**.

На рис. 3.39 обратите внимание на опцию *Windows Vista Basic* (Windows Vista – упрощенный стиль) — в этой цветовой схеме прозрачность окон не используется и многие элементы Aero Glass (например, предпросмотр окон на панели задач или Windows Flip 3D) отсутствуют. Возможно, это самый приемлемый стиль для систем Windows Server 2008, поскольку менее требователен к аппаратным ресурсам и в то же время достаточно элегантен и функционален[1].

Для тонкой настройки параметров элементов пользовательского интерфейса нужно нажать кнопку **Advanced** (Прочие) — в открывшемся после этого окне (см. рис. 3.39) можно модифицировать очень многие элементы стиля оформления, которые выбираются из списка: например, тип и размер шрифта, цвет различных окон и панелей, толщину обрамления (бордюра) окон, ширину полосы прокрутки и т. п.

Фоновый рисунок рабочего стола

В качестве фона (обоев, wallpaper) рабочего стола помимо стандартных рисунков можно использовать любое цифровое изображение. Для этого в окне программы Windows Explorer (Проводник) выберите нужное изображение, щелкните правой кнопкой мыши и в контекстном меню выполните команду **Set as Desktop Background** (Сделать фоновым рисунком рабочего стола).

Аналогичную операцию можно выполнить из окна программы Paint: нужно открыть требуемое изображение и в меню **File** (Файл) выполнить команду **Set As Background (Tiled)** (Сделать фоновым рисунком (замостить)), **Set As Background (Centered)** (Сделать фоновым рисунком (по центру)) или **Set As Background (Stretched)** (Сделать фоновым рисунком (растянуть)).

Размер и положение изображения на рабочем столе можно менять: "растянуть" его на весь рабочий стол (stretch), поместить по центру (center), сохранив оригинальный размер картинки, или "замостить" (tile) изображением весь рабочий стол.

Панель управления предоставляет специальную задачу для выбора фонового рисунка (обоев) рабочего стола. Эта операция состоит из следующих шагов:

1. Откройте окно **Personalization** (Персонализация) (см. рис. 3.31) и выберите задачу **Desktop Background** (Фоновый рисунок рабочего стола).

[1] Именно этот стиль используется практически во всех иллюстрациях данной книги.

2. Выберите тип изображений, используемых в качестве обоев, в списке **Location** (Размещение) (рис. 3.40) (помимо стандартных папок можно выбрать любую папку, содержащую картинки). В системах Windows Server 2008 по умолчанию предлагаются сплошные цвета — самый простой вариант оформления. Выберите изображение (при этом рабочий стол *сразу* меняет цвет или отображает выбранную картинку) и укажите, как располагать его на рабочем столе — для этого служит не показанный в примере переключатель **How should the picture be positioned** (Как разместить рисунок). Этот переключатель имеет три опции: **Fit to screen** (Растянуть), **Tile** (Замостить) и **Center** (По центру).

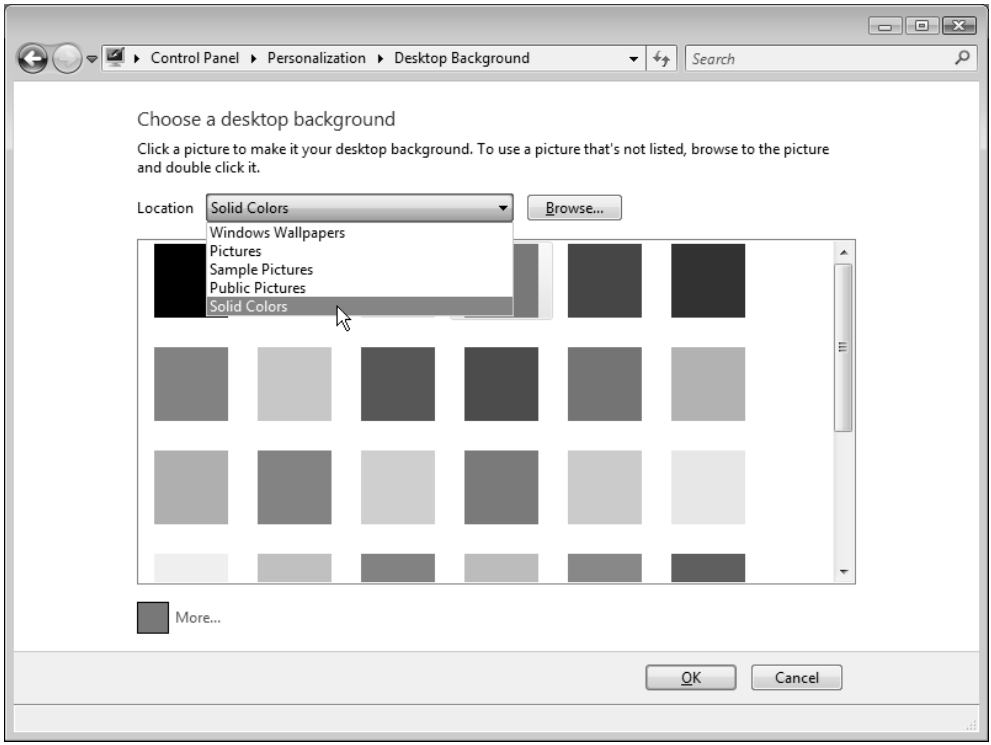


Рис. 3.40. Выбор обоев
или фонового цвета рабочего стола

3. Для сохранения изменений нажмите кнопку **ОК**.

Хранитель экрана (экранная заставка)

Заставка экрана (screen saver) появляется в периоды бездействия пользователя. В качестве заставки используются графические файлы специального формата или любые графические файлы (цифровые или отсканированные фотографии). Для выбора заставки необходимы следующие операции:

1. Откройте окно **Personalization** (Персонализация) (см. рис. 3.31) и выберите задачу **Screen Saver** (Экранная заставка).

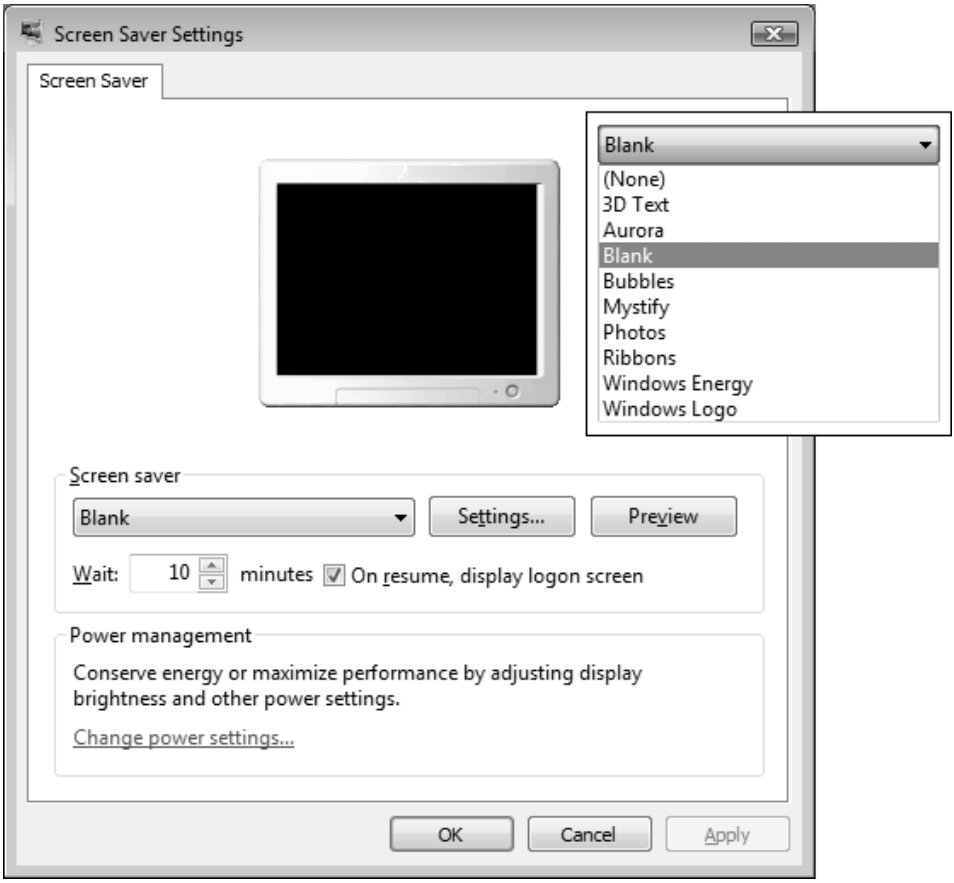


Рис. 3.41. Окно выбора заставки экрана

2. В окне **Screen Saver Settings** (Параметры экранной заставки) (рис. 3.41) выберите заставку в раскрывающемся списке (на врезке он показан пол-

ностью). Кнопка **Preview** (Просмотр) позволяет увидеть, как заставка выглядит в работе, а кнопка **Settings** (Параметры) предоставляет возможность изменения параметров заставки (местоположение картинки, частота отображения и т. д.).

3. Установите нужное время ожидания для отображения заставки (поле **Wait** (Интервал)) и выберите необходимое положение флажка **On resume, display logon screen** (Начинать с экрана входа в систему) — если он будет установлен, то при возврате из режима хранителя экрана будет появляться окно приветствия, и пользователь должен будет ввести пароль своей учетной записи.
4. После выбора параметров нажмите кнопку **ОК**.

Изначально в системах Windows Server 2008 имеются только две заставки: Blank (Пустой экран) и Windows Logo (Эмблема Windows). Выбрана заставка Windows Logo, включающаяся через 10 минут; при возобновлении работы требуется повторный вход в систему.

Дополнительные заставки (показанные на рис. 3.41) появляются после установки компонента Desktop Experience (Возможности рабочего стола).

Выбор языков и региональных стандартов

Средства многоязыковой поддержки Windows позволяют работать в системе с различными языками ввода и выбирать привычные для пользователя представления даты, времени, чисел и т. д.

Методы настройки региональных стандартов и языков в Windows Server 2008 в основном ничем не отличаются от аналогичных операций в предыдущих версиях Windows. Для изменения параметров на панели управления следует выбрать задачу **Regional and Language Options** (Язык и региональные стандарты) (категория **Clock, Language, and Region** (Часы, язык и регион)).

Дополнительные возможности можно получить при установке пакета *Multilingual User Interface (MUI) Pack*, позволяющего менять язык, используемый в интерфейсе систем Windows для отображения команд меню и текстов в служебных окнах и справочной системе. При этом язык пользовательского интерфейса можно переключать без перезагрузки компьютера (хотя пользователю необходимо заново регистрироваться в системе), а также выбирать язык интерфейса для каждого пользователя компьютера отдельно.

Помимо MUI-пакетов, имеются языковые пакеты *Language Interface Pack* (LIP), в которых локализация частичная: переведены только основные, часто используемые элементы пользовательского интерфейса и справка. LIP-пакеты для систем Windows Server 2008 легко найти на сайте Центра загрузки Microsoft (Microsoft Download Center — см. ссылку в *Приложении*), выполнив поиск по строке "Windows Server 2008 Language Packs". Скачанный файл, представляющий собой образ в формате IMG, нужно записать на CD-болванку, которая будет использоваться для установки языка в системе *(см. далее)*.

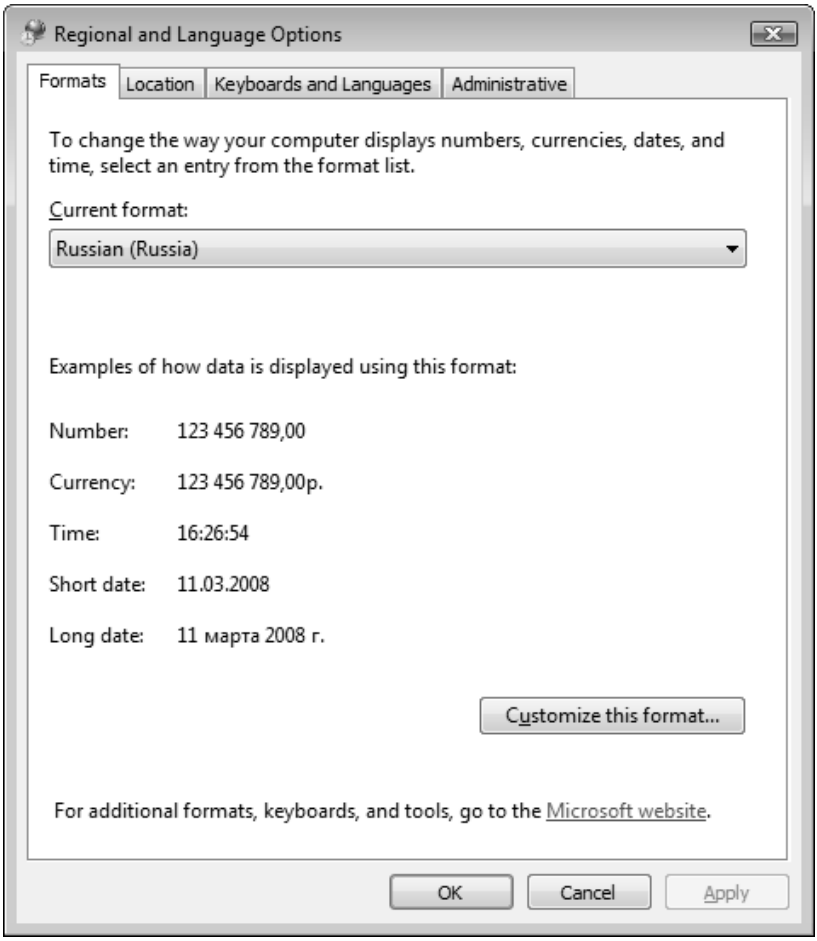


Рис. 3.42. На вкладке **Formats** задается национальный стандарт для отображения дат, чисел и валют

В окне **Regional and Language Options** (Язык и региональные стандарты) на вкладке **Formats** (Форматы) (рис. 3.42) в раскрывающемся списке **Current format** (Текущий формат) выбирается национальный стандарт, который определяет способ отображения чисел, денежных единиц, дат и времени. Для его модификации нужно нажать кнопку **Customize this format** (Изменить этот формат).

На вкладке **Location** (Местоположение) указывается страна проживания пользователя (эта настройка может использоваться веб-сайтами для отображения локальной информации, например, новостей и прогноза погоды, а также для настройки браузера Internet Explorer).

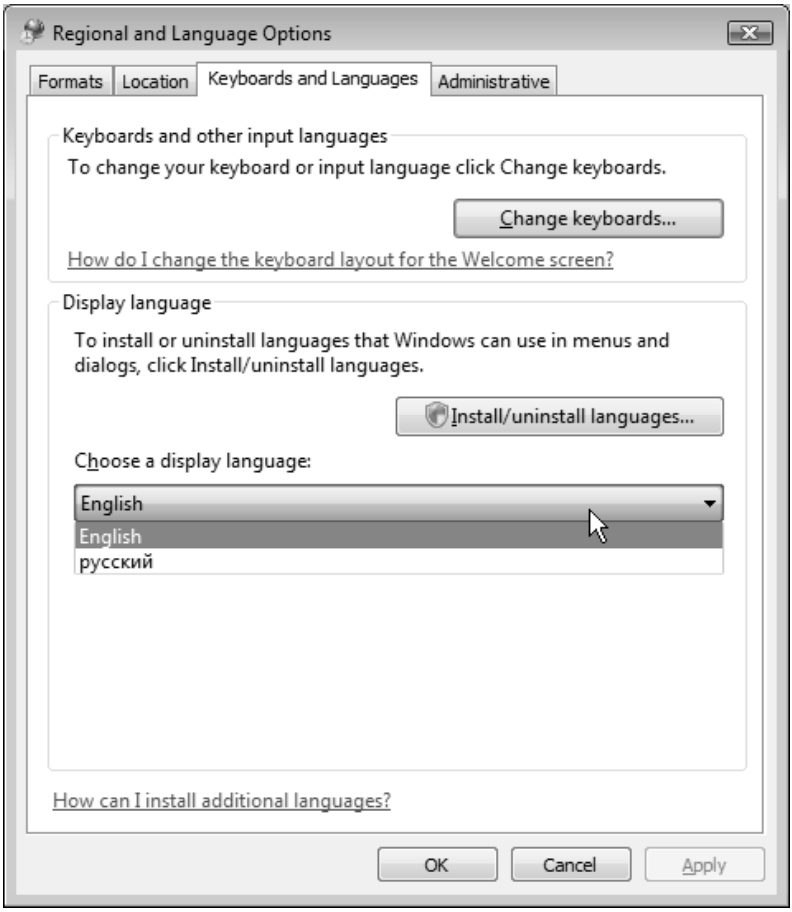


Рис. 3.43. Окно определения языков клавиатуры и интерфейса

На вкладке **Keyboards and Languages** (Языки и клавиатуры) (рис. 3.43) можно выбрать языки ввода и текстовые службы — для этого следует нажать кнопку **Change keyboards** (Изменить клавиатуру). Если в системе установлен языковый пакет (MUI или LIP), то на этой вкладке появляется меню выбора языка пользовательского интерфейса. Чтобы сменить язык, нужно выбрать соответствующую опцию в списке, закрыть все окна программ, выйти из системы и зарегистрироваться вновь.

Кнопка **Install/uninstall languages** позволяет установить или удалить дополнительные языки интерфейса. Нажав эту кнопку, необходимо установить в приводе компакт-диск с записанным LIP-пакетом, после чего следует выбрать на диске папку langpacks. В окне программы-мастера появится список языков, входящих в данный LIP-пакет (рис. 3.44). Установив флажок для нужного языка, следует нажать кнопку **Next** (Далее).

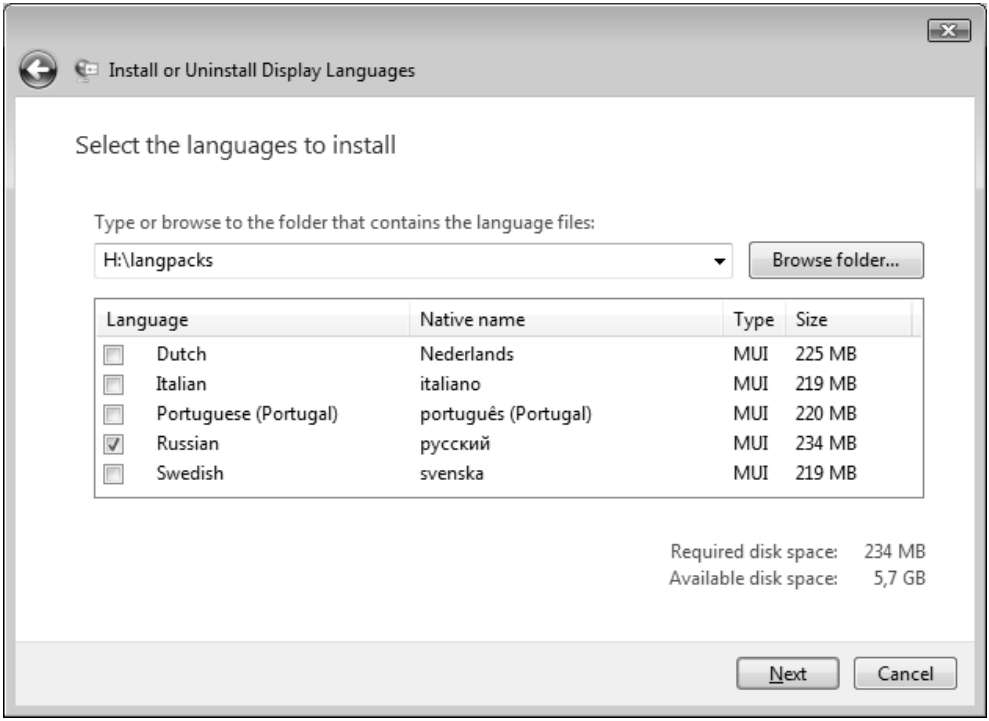


Рис. 3.44. Выбор устанавливаемого языка отображения

Затем нужно принять лицензионное соглашение и в следующем окне мастера нажать кнопку **Install** (Установить). После установки языка появится соот-

ветствующее сообщение (рис. 3.45), где будет предложено сразу же сменить текущий язык интерфейса на один из установленных — при этом нужно будет выйти (кнопка **Log off**) из системы. Теперь каждый пользователь компьютера (включая удаленных пользователей) может выбирать любой из имеющихся в системе языков.

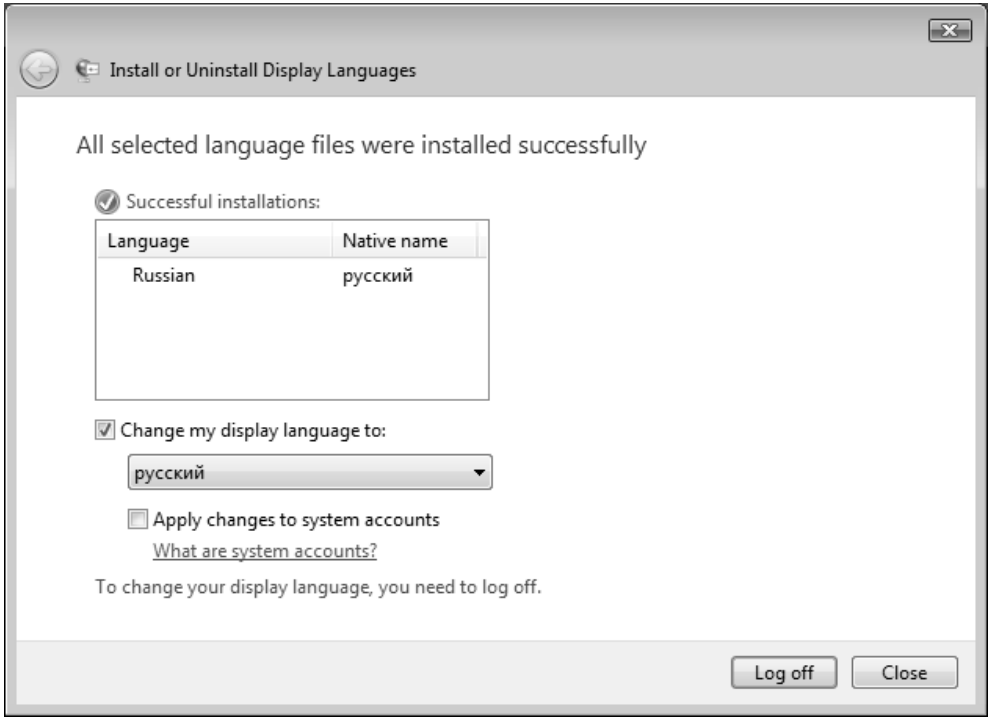


Рис. 3.45. Сообщение об установке нового языка пользовательского интерфейса

На вкладке **Keyboards and Languages** (Языки и клавиатуры) имеется кнопка **Change keyboards** (Изменить клавиатуру), нажав которую, можно в открывающемся окне на вкладке **General** (Общие) (рис. 3.46) выбрать язык ввода по умолчанию[1] (раскрывающийся список в разделе **Default input language** (Язык ввода по умолчанию)), а также установить дополнительные языки для

[1] В русских локализованных версиях по умолчанию для ввода используется русский язык, хотя системному администратору, часто работающему с командной строкой и вручную вводящему названия утилит и программ, удобнее выбрать английский.

ввода символов. Устанавливать языки нужно, если только необходимо на них *писать* в какой-нибудь программе, поскольку для *воспроизведения* текстов никаких дополнительных действий не требуется — шрифты и кодовые таблицы уже присутствуют в системе.

Рис. 3.46. В этом окне можно выбрать язык ввода, а также установить дополнительные языки и службы

Для правильного отображения меню и диалоговых окон в приложениях, которые не поддерживают стандарт Юникод (Unicode), необходимо установить соответствующие таблицы преобразования кодовых страниц.

Для этого в окне **Regional and Language Options** (Язык и региональные стандарты) нужно перейти на вкладку **Administrative** (Дополнительно) (рис. 3.47) и выбрать нужный язык, нажав кнопку **Change system locale** (Изменить язык системы) (этот выбор не повлияет на работу Юникод-совместимых при-

ложений и самой системы). Эту операцию рекомендуется выполнить, если при запуске какого-нибудь вновь установленного приложения вместо текста отображаются вопросительные знаки или другие посторонние символы.

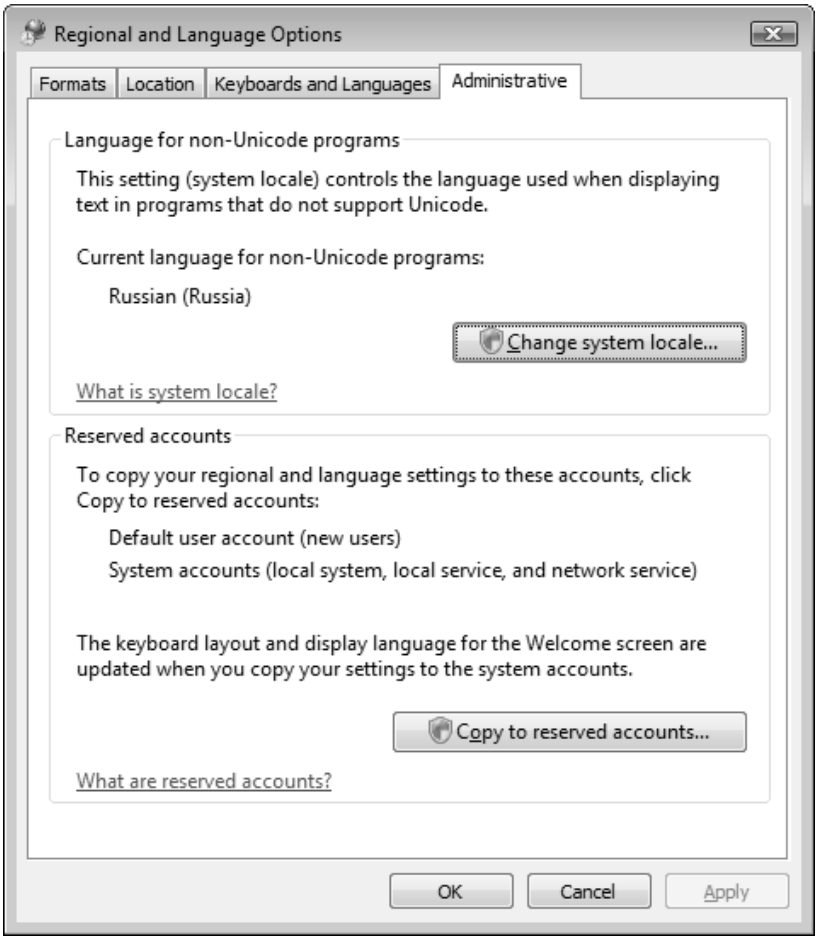


Рис. 3.47. Вкладка дополнительных текстовых настроек

Консоль управления Microsoft (MMC)

В системах Windows, начиная с Windows 2000, для управления компонентами и сервисами операционной системы используется единая среда — *Micro-*

soft Management Console, MMC (Консоль управления Microsoft), которая является общей платформой для запуска всех программных модулей администрирования, конфигурирования или мониторинга локальных компьютеров и сети в целом. Такие законченные модули называются *оснастками* (snap-in). Консоль управления сама по себе не выполняет никаких функций администрирования, но служит в качестве рабочей среды для разнообразных компонентов, на базе которых можно создавать индивидуальные управляющие инструменты.

Впервые консоль MMC появилась как стандартное средство управления в составе Windows 2000. В состав систем Windows Server 2008 включена консоль Microsoft Management Console 3.0.

Все основные административные оснастки запускаются из меню **Start** (Пуск); они располагаются в группе **All Programs** | **Administrative Tools** (Все программы | Администрирование). Оснастки можно запускать и с панели управления (задача **Administrative Tools** (Администрирование), категория **System and Maintenance** (Система и ее обслуживание)), но проще всего с ними работать, если включить группу **Administrative Tools (**Администрирование) непосредственно в меню **Start** (Пуск) *(см. главу 2)*. Кроме того, название запускаемой оснастки (включая расширение .msc — см. табл. 3.3) можно ввести непосредственно в поле поиска меню **Start** (Пуск) или в окне **Run** (Выполнить).

Типы оснасток

Нужно знать, что существуют два типа оснасток:

- *изолированная оснастка* (standalone snap-in) обеспечивает выполнение своих функций даже при отсутствии других оснасток, например, **Computer Management** (Управление компьютером);
- *оснастка-расширение* (extension snap-in) может работать только после активизации родительской оснастки. Функция оснастки-расширения заключается в увеличении числа типов узлов, поддерживаемых родительской оснасткой. Оснастка-расширение является подчиненным элементом узлов определенных типов и при каждом запуске узлов данных типов консоль автоматически запускает все связанные с ней расширения. В качестве примера можно привести расширения **Administrative Templates** (Административные шаблоны) и **Extended View** (Расширенный вид),

входящие в состав оснастки **Group Policy Object Editor** (Редактор объектов групповой политики).

Оснастки-расширения могут предоставлять различные функциональные возможности. Например, такие оснастки могут расширять пространство имен консоли, увеличивать число пунктов в меню или добавлять определенные мастера.

Пользовательский интерфейс MMC 3.0

Пользовательский интерфейс консоли Microsoft Management Console 3.0 позволяет одновременно открывать несколько документов (Multiple Document Interface, MDI). Окно консоли содержит главное меню и панель инструментов, набор которых специфичен для каждой подключенной оснастки. Главное меню обеспечивает функции управления файлами и окнами, а также доступ к справочной системе.

Рабочее окно консоли обычно содержит *панель обзора* (левое окно), *панель результатов* (центральное окно) и *панель действий* (**Actions**) (правое окно) (см. пример на рис. 3.50). Панель обзора отображает пространство имен инструментов MMC в виде дерева объектов. Это дерево содержит все видимые узлы, каждый из которых является управляемым объектом, задачей или средством просмотра. Панель результатов отображает список элементов выбранного узла. Данный список может содержать папки, оснастки, элементы управления, веб-страницы, панели задач (taskpad) и другие элементы. Панель действий содержит команды, которые можно выполнять с объектами, выбранными на панели обзора или на панели результатов (эти команды также можно выполнить в меню **Actions** (Действие)). При необходимости панели обзора и действий можно отключать.

Конфигурирование консолей MMC

Управлять системой можно с помощью стандартных автономных оснасток, поставляемых с системой. Однако в некоторых случаях требуются оснастки, которые не представлены в меню **Start** (Пуск), а иногда возникает необходимость в создании консоли со "своим" набором функций, реализуемых отдельными оснастками. В этом случае можно добавить недостающие элементы на существующую консоль или создать новую консоль MMC.

Создание новой консоли MMC

Для примера опишем процедуру создания новой консоли и добавления к ней оснасток **Services** (Службы) и **Sertificates** (Сертификаты).

1. В меню **Start** (Пуск) введите `mmc`. Можно также пользоваться командой **Run** (Выполнить) или окном командной строки (опция **Command Prompt**) — обе опции имеются по умолчанию в меню **Start** (Пуск). В любом случае после выполнения команды откроется окно пустой консоли (рис. 3.48).

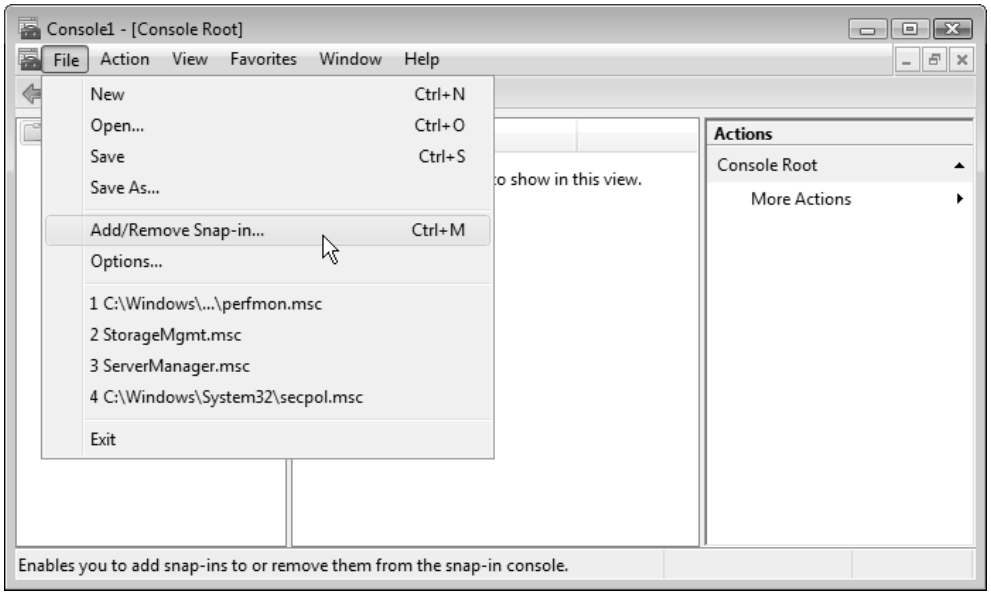


Рис. 3.48. Окно новой консоли MMC

2. В меню **File** (Консоль) выберите пункт **Add/Remove Snap-in** (Добавить или удалить оснастку) или просто нажмите клавиши <Crtl>+<M>. Откроется окно, содержащее список всех оснасток, имеющихся в системе (рис. 3.49). (Следует помнить, что набор имеющихся оснасток зависит от выбранных для сервера ролей и установленных компонентов.)
3. Список **Available snap-ins** (Доступные оснастки) содержит имеющиеся оснастки, а в списке **Selected snap-ins** (Выбранные оснастки) перечисляются уже подключенные оснастки. Если выбрать оснастку в правом списке и нажать кнопку **Edit Extensions** (Изменить расширения), то можно

перейти в окно, в котором перечислены оснастки-расширения, подключаемые вместе с изолированной оснасткой. При необходимости можно отключить ненужные оснастки-расширения.

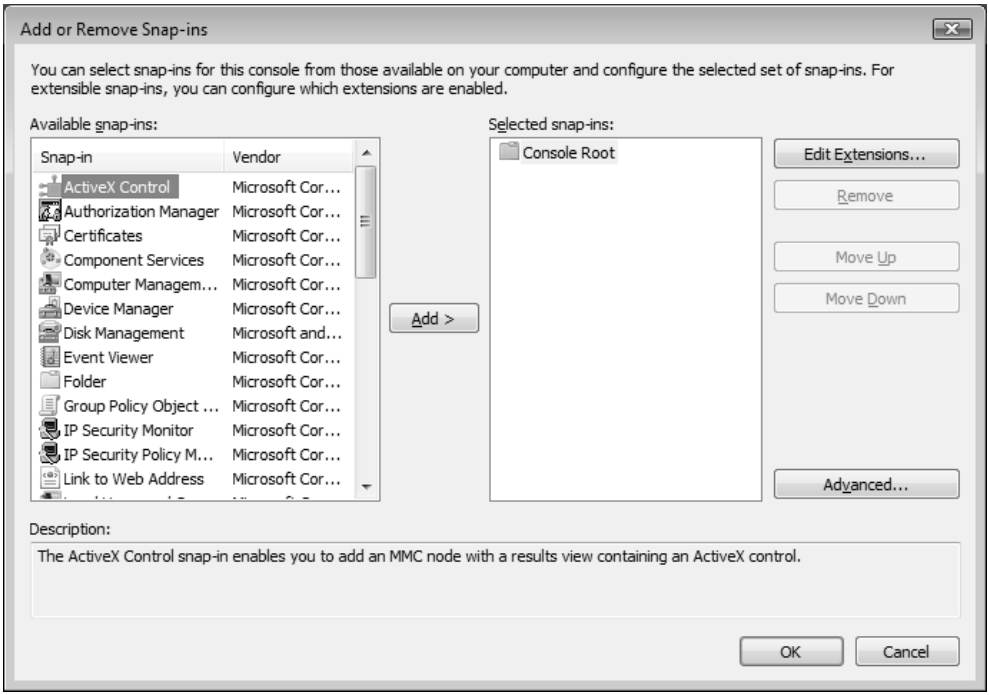


Рис. 3.49. Окно, содержащее список имеющихся оснасток

4. Выберите оснастку **Services** (Службы) и нажмите кнопку **Add** (Добавить).
5. Появится конфигурационное окно с предложением выбрать целевой компьютер, с которым будет работать данная оснастка. Оставьте опцию по умолчанию **Local computer** (Локальный компьютер) и нажмите кнопку **Finish** (Готово).
6. Теперь в списке **Available snap-ins** (Доступные оснастки) выберите оснастку **Sertificates** (Сертификаты) и аналогичным образом подключите ее к консоли, выбрав при этом опцию сертификатов для учетной записи пользователя.
7. Закройте окно выбора оснасток, нажав кнопку **OK**. Результат выполнения описанной процедуры представлен на рис. 3.50.

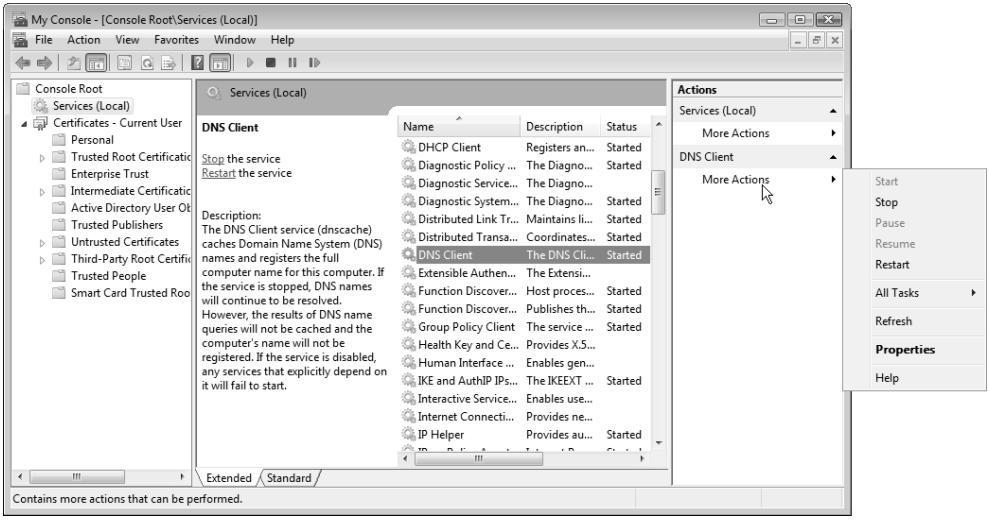


Рис. 3.50. Пример пользовательской консоли MMC

8. Для того чтобы сохранить созданный инструмент, в меню **File** (Консоль) выберите пункт **Save As** (Сохранить как) и укажите имя, с которым будет сохранен файл консоли, имеющий расширение .msc (Management Saved Console). При этом рекомендуется оставить имя папки, предлагаемой по умолчанию, — это папка **Administrative Tools** (Администрирование) в профиле пользователя (в этом случае свои консоли можно будет вызывать по имени в строке поиска меню **Start** (Пуск) или из подменю **All Programs** | **Administrative Tools** (Все программы | Администрирование).

Все пользовательские консоли MMC имеют значок с изображением красного саквояжа и ***не отображаются*** в стандартной папке **Administrative Tools** (Администрирование), входящей в состав меню **Start** (Пуск) (или вызываемой с панели управления) и являющейся общей для всех пользователей.

Установка опций консоли

Если консоль MMC создается для другого пользователя, имеющего ограниченные права, может оказаться полезным установить запрет на изменение консоли.

Для этого нужно выполнить следующие операции:

1. В меню **File** (Консоль) выберите пункт **Options** (Параметры).

2. В открывшемся окне (рис. 3.51) в списке **Console mode** (Режим консоли) выберите опцию **User mode - full access** (Пользовательский - полный доступ). В этом режиме пользователь не сможет добавлять новые оснастки в инструмент, но будет иметь возможность изменять расположение окон. (Новый режим начнет работать при следующем запуске файла консоли.)

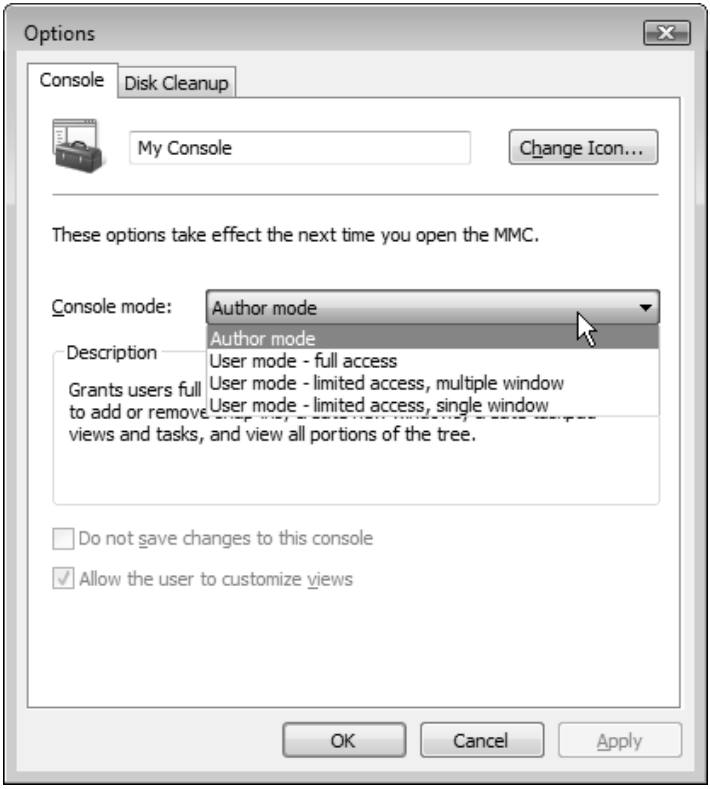


Рис. 3.51. Окно установки опций консоли MMC

3. Можно запретить другому пользователю изменение внешнего вида консоли, сняв флажок **Allow the user to customize views** (Разрешить пользователю настраивать вид консоли). Флажок **Do not save changes to this console** (Не сохранять изменения для этой консоли) позволяет запретить сохранение выполненных изменений в конфигурации, чтобы эти изменения не влияли на последующие запуски консоли.
4. Нажмите кнопку **OK** и сохраните файл консоли.

Оснастки Windows Server 2008 и их назначение

Все стандартные оснастки, имеющиеся в системах Windows Server 2008, перечислены в табл. 3.3 (некоторые оснастки могут отсутствовать в определенных редакциях Windows Server 2008). Для оснасток, включенных в пользовательский интерфейс, указаны названия соответствующих пунктов меню, для остальных оснасток даны их собственные имена, применяемые в консоли управления MMC. Звездочками отмечены оснастки, которые можно вызывать непосредственно из меню **Start** (Пуск) или из группы **Administrative Tools** (Администрирование) на панели управления. В скобках помимо названия, принятого в локализованных версиях Windows Server 2008, указано также имя автономной MMC-консоли, которое можно использовать для запуска оснастки из меню **Start** (Пуск) или окна **Run** (Выполнить)[1]; если такое имя отсутствует, то оснастку можно использовать только как *расширение* имеющейся консоли.

Таблица 3.3. *Оснастки систем Windows Server 2008*

Оснастка	Назначение
ActiveX Control (Элемент ActiveX)	Добавляет в консоль элемент ActiveX
Authorization Manager (Диспетчер авторизации, azman.msc)	Определение ролевых разрешений для приложений, которые используют диспетчер авторизации. Позволяет создать гибкую среду управления корпоративными приложениями на основе механизмов доступа, базирующихся на понятиях "роль", "задача", "операция"
Certificates (Сертификаты, certmgr.msc)	Управление сертификатами
Component Services (Службы компонентов, comexp.msc)*	Конфигурирование и администрирование COM-компонентов и COM+-приложений; предназначена для системных администраторов и разработчиков приложений
Computer Management (Управление компьютером, compmgmt.msc)*	Основной инструмент администрирования системы; содержит в своем составе ряд автономных оснасток и оснасток-расширений

[1] В обоих случаях обязательно нужно указывать расширение .msc!

Таблица 3.3 *(продолжение)*

Оснастка	Назначение
Device Manager (Диспетчер устройств, devmgmt.msc)	Содержит список всех устройств, подключенных к компьютеру, и позволяет их конфигурировать
Disk Management (Управление дисками, diskmgmt.msc)	Управление дисками и томами, разбиение дисков на логические тома, форматирование, управление совместным доступом, квотами и т. д.
Event Viewer (Просмотр событий, eventvwr.msc)*	Просмотр журналов системы, безопасности и приложений
Folder (Папка)	Служит для добавления новой папки в дерево
Group Policy Management (Управление групповой политикой, gpmc.msc)*	Управление объектами групповых политик в доменах Active Directory. Появляется при установке соответствующего компонента сервера
Group Policy Object Editor (Редактор объектов групповой политики, gpedit.msc)	Редактирование объектов групповой политики, которые могут ссылаться на сайты, домены или организационные подразделения в Active Directory или же храниться на локальном компьютере
IP Security Monitor (Монитор IP-безопасности)	Наблюдение за состоянием IP-безопасности
IP Security Policy Management (Управление политикой безопасности IP)	Управление политиками IPSec с целью обеспечения безопасных коммуникаций с другими компьютерами
Link to Web Address (Ссылка на веб-ресурс)	Позволяет добавить узел консоли, отображающий страницу в Интернете
Local Security Policy (Локальная политика безопасности, secpol.msc)*	Расширение оснастки **Group Policy Object Editor** (Редактор объектов групповой политики), позволяющее настраивать политики безопасности компьютера. Эту оснастку нельзя добавлять к консолям MMC, она может вызываться только из меню **Start** (Пуск) или из окна командной строки
Local Users and Groups (Локальные пользователи и группы, lusrmgr.msc)	Управление локальными пользователями и группами

Таблица 3.3 *(продолжение)*

Оснастка	Назначение
NAP Client Configuration (Конфигурация клиента защиты доступа к сети, NAPCLCFG.MSC)	Управление параметрами клиента защиты доступа к сети (Network Access Protection, NAP)
Print Management (Управление печатью, printmanagement.msc)	Используется для управления принтерами и очередями печати на локальных и удаленных принтерах печати. Появляется при установке соответствующей роли сервера
Reliability and Performance Monitor (Монитор производительности и стабильности, perfmon.msc)*	Определение производительности компьютера или других компьютеров в реальном времени
Reliability Monitor (Монитор стабильности системы)*	Мониторинг стабильности работы системы, регистрация ошибок программных и аппаратных средств
Remote Desktops (Удаленные рабочие столы, tsmmc.msc)*	Обеспечивает доступ к серверам терминалов и рабочим столам удаленных компьютеров
Resultant Set of Policy (Результирующая политика, rsop.msc)	Позволяет просматривать результирующую (действующую) политику для компьютера и пользователя
Routing and Remote Access (Маршрутизация и удаленный доступ, rrasmgmt.msc)	Служит для конфигурирования многопротокольных служб маршрутизации, включающих средства доступа к глобальным и виртуальным сетям (VPN), сервис преобразования адресов (NAT) и т. д.
Security Configuration and Analysis (Анализ и настройка безопасности)	Анализ и настройка параметров безопасности с помощью файлов шаблонов безопасности
Security Templates (Шаблоны безопасности)	Обеспечивает возможность редактирования файлов-шаблонов безопасности
Server Manager (Диспетчер сервера)*	Позволяет контролировать состояние сервера, выполнять общие административные задачи, добавлять или удалять роли и программные компоненты сервера

Таблица 3.3 *(продолжение)*

Оснастка	Назначение
Services (Службы, services.msc)*	Запуск, остановка и настройка служб (сервисов) Windows
Share and Storage Management (Управление общими папками и хранилищами, StorageMgmt.msc)*	Обеспечивает управление общими папками и томами
Shared Folders (Общие папки, fsmgmt.msc)	Отображает общие папки, текущие сеансы и открытые файлы
Storage Explorer (Обозреватель хранилищ, storexpl.msc)*	Служит для мониторинга и управления элементами распределенной сетевой среды SAN (System Area Network)
Task Scheduler (Планировщик заданий, taskschd.msc)*	Управление заданиями, запускающимися автоматически в соответствии с заданным расписанием
Telephony (Телефония)	Настройка и мониторинг службы телефонии
Terminal Services Configuration (Конфигурация служб терминалов, tsconfig.msc)*	Служит для настройки параметров сервера терминалов
Terminal Services Manager (Диспетчер служб терминалов, tsadmin.msc)*	Управление и мониторинг серверов терминалов
TPM Management (Управление TPM, tpm.msc)*	Управление доверенным платформенным модулем (Trusted Platform Module, TPM), на основе которого реализована функция Windows BitLocker™ Drive Encryption, обеспечивающая шифрование дисков в соответствии со спецификацией Extensible Firmware Interface (EFI)
Windows Firewall with Advanced Security (Брандмауэр Windows в режиме повышенной безопасности, WF.msc)*	Тонкая настройка брандмауэра Windows, создание правил для входящих и исходящих подключений

Таблица 3.3 *(окончание)*

Оснастка	Назначение
Windows Server Backup (Система архивации данных Windows Server, wbadmin.msc)*	Управляет функциями архивации и восстановления данных на сервере
WMI Control (Управляющий элемент WMI, WmiMgmt.msc)	Позволяет настраивать и управлять службой WMI

Примечание

Кроме оснасток, перечисленных в табл. 3.3, после установки дополнительных ролей сервера или компонентов — например, сетевых служб (DNS, DHCP и др.), служб Интернета (IIS), службы факсов, служб терминалов (Terminal Services) — в системе появляется множество других оснасток, использующихся для администрирования этих служб. Эти оснастки будут рассматриваться в соответствующих главах книги.

В табл. 3.4 перечислены важные дополнительные оснастки Windows Server 2008, устанавливаемые только на контроллерах доменов и используемые для управления службами каталога Active Directory.

Таблица 3.4. *Оснастки, устанавливаемые на контроллерах доменов Active Directory*

Оснастка	Назначение
Active Directory Domains and Trusts (Active Directory — домены и доверие, domain.msc)*	Управление доменами и доверительными отношениями между доменами
Active Directory Sites and Services (Active Directory — сайты и службы, dssite.msc)*	Конфигурирование топологии и расписаний репликации службы Active Directory. Управление службами корпоративного уровня
Active Directory Users and Computers (Active Directory — пользователи и компьютеры, dsa.msc)*	Управление пользователями, группами, организационными подразделениями (OU) и другими объектами Active Directory

Таблица 3.4 *(окончание)*

Оснастка	Назначение
ADSI Edit (Редактирование ADSI, adsiedit.msc)*	Низкоуровневый редактор объектов каталога Active Directory (раньше оснастка входила в состав пакета Windows Support Tools, а теперь является стандартным компонентом системы)

Примечание

Поскольку в системах Windows Server 2008 используется средство централизованного управления политиками в доменах Active Directory — оснастка **Group Policy Management** (Управление групповой политикой), — удалены некоторые оснастки, имеющиеся в составе Windows Server 2003: речь идет об оснастках **Domain Security Policy** (Политика безопасности домена) и **Domain Controller Security Policy** (Политика безопасности контроллера домена).

Далее будут рассмотрены некоторые программные инструменты "широкого назначения", которые часто упоминаются в других главах книги при описании тех или иных административных задач.

Традиционный инструмент администратора — оснастка *Computer Management*

Несмотря на появление новых средств (их мы рассматривали ранее), в системах Windows Server 2008, как и в предыдущих версиях Windows, оснастка **Computer Management** (Управление компьютером) (рис. 3.52) остается одним из основных средств, предназначенных для централизованного выбора параметров и конфигурирования сервисов локальных или удаленных компьютеров. Некоторые возможности этой оснастки теперь присутствуют и в оснастке **Server Manager** (Диспетчер сервера).

Оснастку можно запускать из меню **Start** (Пуск) или с панели управления. В системах Windows Vista также можно щелкнуть правой кнопкой мыши по значку **Computer** (Мой компьютер) в меню **Start** (Пуск) или на рабочем столе (если используется классический стиль интерфейса Windows) и выбрать в контекстном меню пункт **Manage** (Управление). В Windows Server 2008 в этом случае запускается оснастка **Server Manager** (Диспетчер сервера).

Примечание

Для того чтобы с помощью оснастки можно было управлять удаленным компьютером, нужно на панели обзора выбрать корневой узел дерева объ-

ектов, щелкнуть правой кнопкой мыши и выполнить команду **Connect to another computer** (Подключиться к другому компьютеру). Имя целевого компьютера можно ввести непосредственно или выбрать с помощью операции поиска в сетевом окружении (в домене).

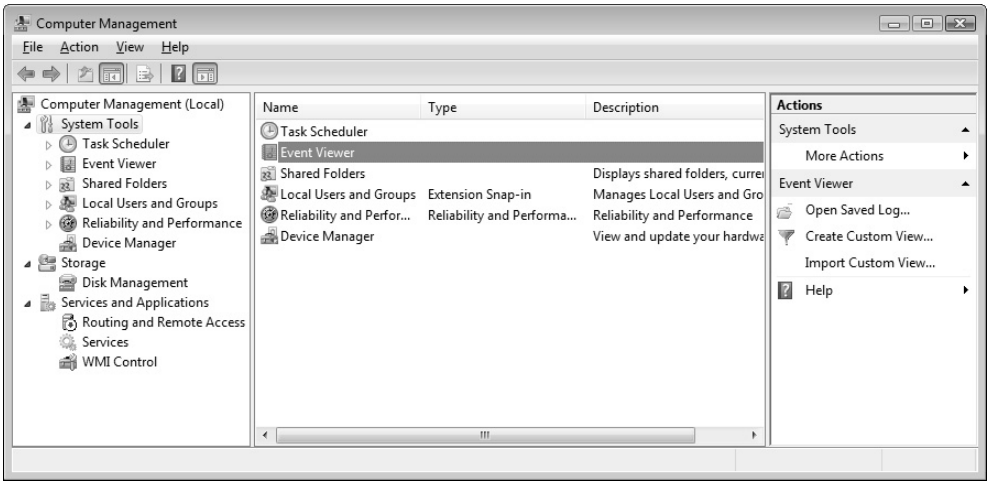


Рис. 3.52. Окно оснастки **Computer Management**

Как можно видеть на рис. 3.52, в пространстве имен оснастки имеются три узла:

- **System Tools** (Служебные программы) — узел содержит оснастки, предназначенные для администрирования системы, мониторинга событий и производительности компьютера, управления профилями пользователей и аппаратными средствами компьютера;
- **Storage** (Запоминающие устройства) — узел содержит только оснастку **Disk Management** (Управление дисками);
- **Services and Applications** (Службы и приложения) — в этом узле собраны оснастки, позволяющие управлять системными сервисами и компонентами Windows. При установке дополнительных ролей сервера — например, служб Интернета (IIS) — в составе этого узла также появляются соответствующие административные оснастки.

Использование конкретных оснасток мы будем рассматривать в разделах, посвященных определенным административным задачам: например, управлению учетными записями пользователей, мониторингу системы и т. п. При необходимости описание оснастки можно найти в предметном указателе по ее имени.

Управление системными службами

Оснастка **Services** (Службы) часто используется в различных задачах администрирования операционной системой: она позволяет просматривать статус и описание служб, запускать, останавливать и перезапускать сервисы (службы), а также с ее помощью можно конфигурировать опции запуска и восстановления сервисов. Благодаря удобному интерфейсу оснастки легко ориентироваться в назначении имеющихся служб (см. описание слева от списка служб) (рис. 3.53) и видеть их состояние.

Совет

После установки системы имеет смысл сохранить исходное состояние и тип запуска всех сервисов. Это может помочь в том случае, когда после остановки каких-то служб работа системы нарушается, но администратор не может вспомнить названия сервисов, для которых менялось состояние. Нажав кнопку **Export List** (Экспорт списка) на панели инструментов (на рис. 3.53 она отмечена кружком), можно сохранить в текстовом файле список имеющихся служб, включая описания, текущее состояние и тип запуска.

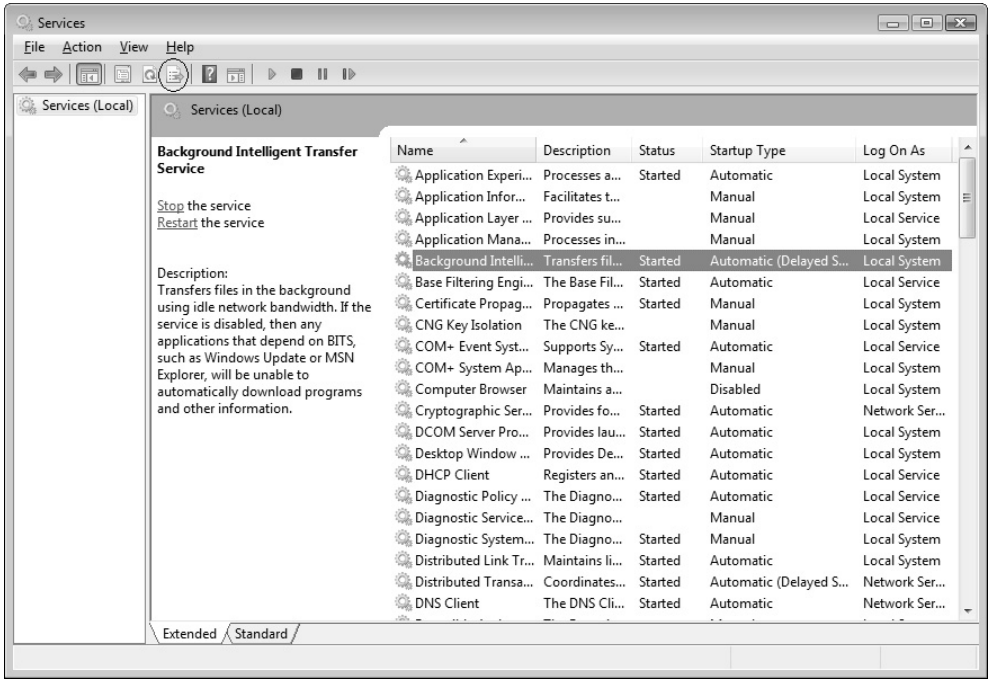


Рис. 3.53. Вид оснастки **Services**

Кнопки управления запуском службы располагаются на панели инструментов, что позволяет быстро остановить или перезапустить любой сервис. Свойства конкретной службы можно увидеть, если выполнить двойной щелчок на имени службы. В окне свойств (рис. 3.54) можно видеть имя службы (оно используется при управлении службами из командной строки) и имя исполняемого файла, связанного с этой службой (оно будет видно в списке процессов в диспетчере задач — *см. главу 5*).

В окне свойств службы (см. рис. 3.54) можно изменить тип запуска. Как можно видеть на иллюстрациях, в системах Windows Server 2008 появился новый тип запуска сервисов — отложенный старт (Delayed Start).

Оснастка **Services** (Службы) может работать и с удаленным компьютером — для этого используется команда **Connect to another computer** (Подключиться к другому компьютеру) в меню **Action** (Действие).

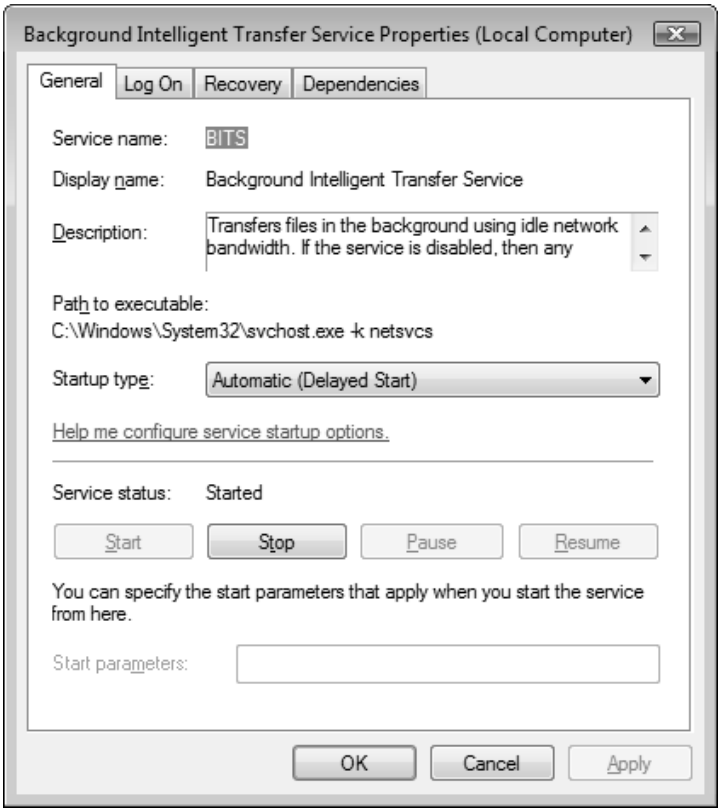


Рис. 3.54. Окно свойств службы

Для управления службами из командной строки используется утилита `sc`. Например, с помощью команды `sc query` можно получить информацию о состоянии служб локального или удаленного компьютера (работающего под управлением Windows Server 2008 или других систем, например, Windows XP или Server 2003). Последовательность команд `sc stop` *<имяСлужбы>* и `sc start` *<имяСлужбы>* позволяет перезапустить указанную службу.

Получение информации о системе

Утилита System Information (Сведения о системе) представляет исчерпывающую информацию об аппаратном обеспечении локального или удаленного компьютера, системных компонентах и программной среде. Системная информация (рис. 3.55) разделена на категории, описание которых приводится ниже.

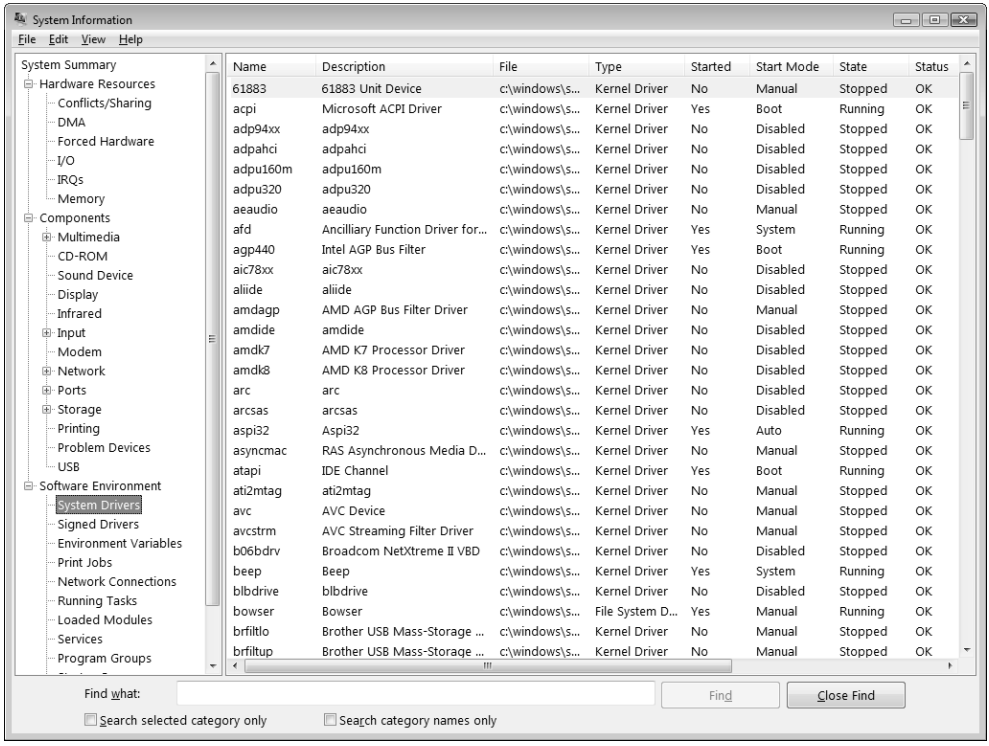


Рис. 3.55. Окно утилиты System Information

- Узел **System Summary** (Сведения о системе) отображает общую информацию о компьютере и операционной системе: версию ОС и номер сборки, тип процессора, объем ОЗУ, версию BIOS, региональные установки, а также информацию об объеме физической и виртуальной памяти на компьютере.
- Узел **Hardware Resources** (Аппаратные ресурсы) содержит информацию об используемых аппаратных параметрах, таких как каналы DMA, номера прерываний (IRQ), адреса ввода/вывода (I/O) и адреса памяти. Узел **Conflicts/Sharing** (Конфликты и совместное использование) идентифицирует устройства, которые совместно используют ресурсы или конфликтуют с другими ресурсами. Такая информация помогает выявлять проблемы, возникающие с аппаратными устройствами.
- Узел **Components** (Компоненты) отображает информацию о конфигурации аппаратных средств системы и используется для определения статуса драйверов устройств, сетевых устройств и программного обеспечения мультимедийных устройств.
- Узел **Software Environment** (Программная среда) отображает "снимок" программного обеспечения, загруженного в память компьютера. Данная информация может быть использована для просмотра статуса драйверов устройств (см. рис. 3.55), списка выполняющихся задач и т. д.

> ***Примечание***
>
> В системах Windows, начиная с Windows XP, имеется утилита командной строки SystemInfo.exe, с помощью которой можно получить общую информацию о локальной или удаленной системе. Чтобы узнать о параметрах утилиты, введите в командной строке `systeminfo /?`.

Полученную информацию можно сохранить в файле с расширением nfo (файл будет сохранен как документ MSInfo) или экспортировать в текстовый файл с помощью команды **File** | **Export** (Файл | Экспорт) для последующего анализа.

Глава 4

Типовые административные задачи

Эта глава посвящена общим вопросам администрирования систем Windows Server 2008, не относящимся к каким-то определенным ролям сервера или системным службам. Многие концепции (если не говорить об их реализации!) и инструменты, применяемые для этих целей, появились относительно давно, еще в предыдущих версиях операционных систем линейки Windows NT/2000, а некоторые — относительно "молодые" — унаследованы от Windows XP. В системе Windows Vista большинство средств администрирования были кардинально переработаны (примерами могут служить экран регистрации в системе, окно управления учетными записями или планировщик задач), появились и совершенно новые функции и утилиты. Практически все эти модифицированные и новые средства можно видеть и в системах Windows Server 2008.

Диспетчер системных ресурсов (Windows System Resource Manager)

Многие компоненты, входящие в состав оснастки **Server Manager** (Диспетчер сервера), уже рассматривались в предыдущих главах (*см. главы 1* и *3*). Эта новая оснастка является в системах Windows Server 2008 одним из основных средств администрирования. В ее окне можно видеть совершенно новое средство, появившееся в Windows Server 2008, — оснастку **Windows System Resource Manager** (Диспетчер системных ресурсов), которая используется для управления одноименным компонентом сервера (она может работать с локальным или удаленным компьютером).

Диспетчер системных ресурсов позволяет создавать политики, управляющие распределением системных ресурсов — процессоров и памяти. Это средство в первую очередь ориентировано на использование в мощных многопроцессорных системах. Главное окно оснастки **Windows System Resource Manager** (Диспетчер системных ресурсов) в составе диспетчера сервера показано на рис. 4.1.

С помощью диспетчера системных ресурсов можно реализовать следующие задачи:

- создавать политики, управляющие доступом к системным ресурсам (процессорам и памяти) на основе определенных критериев;
- использовать календарь для планирования доступа к ресурсам;
- привязывать доступ к ресурсам к определенным событиям и условиям;
- сохранять информацию об использовании ресурсов в журналах для анализа производительности системы.

Использование диспетчера требует глубокого предварительного знакомства с общими концепциями и деталями реализации этого механизма; подробную информацию можно найти во встроенной справке. В дальнейшем можно ожидать появления новых политик и возможностей диспетчера, поэтому нужно следить за появлением его обновлений.

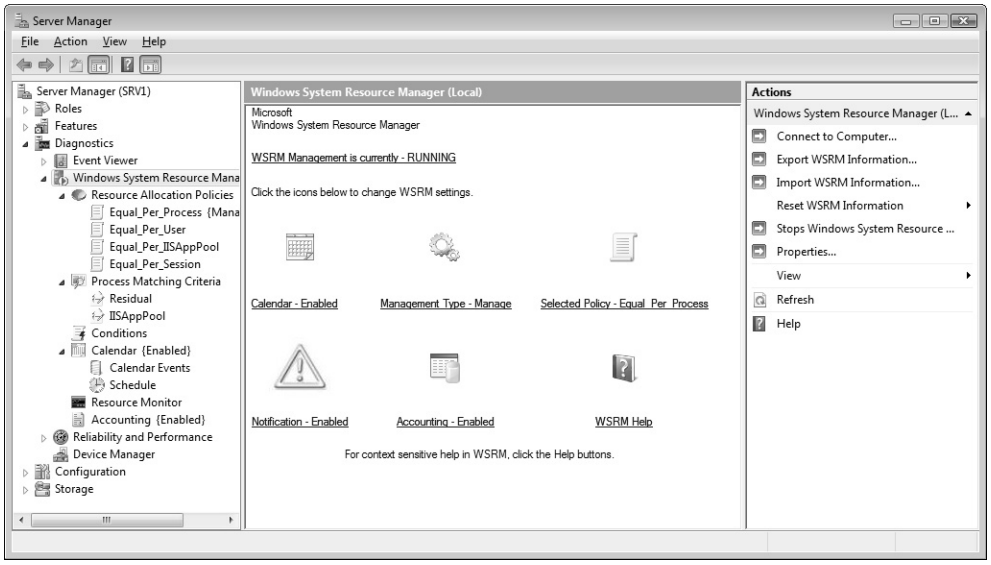


Рис. 4.1. Главное окно диспетчера системных ресурсов

Диспетчер системных ресурсов и его оснастка появляются в системе только после того, как с помощью оснастки **Server Manager** (Диспетчер сервера) устанавливается соответствующий компонент сервера — *Windows System Resource Manager* (WSRM) (Диспетчер системных ресурсов) (см. табл. 3.2). Для работы диспетчера также требуется компонент *Windows Internal Database* (Внутренняя база данных Windows), представляющий собой реляционную базу данных, которая используется только для реализации и поддержки некоторых ролей и компонентов сервера:

- UDDI Services (Службы UDDI);
- Active Directory Rights Management Services (AD RMS) (Службы управления правами Active Directory);
- Windows Server Update Services;
- Windows System Resource Manager (WSRM) (Диспетчер системных ресурсов).

Если компонент Windows Internal Database (Внутренняя база данных Windows) еще не установлен в системе при выборе одной из перечисленных ролей, то при добавлении роли или компонента появляется соответствующий запрос (рис. 4.2).

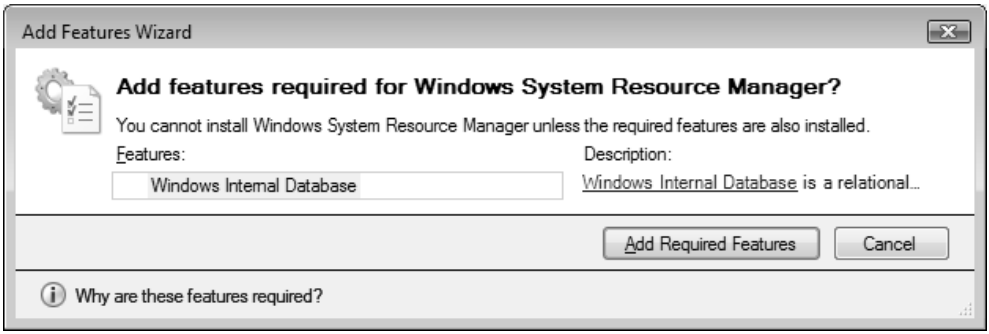


Рис. 4.2. Запрос на установку внутренней базы данных Windows

Управление учетными записями

Учетные записи пользователей (user accounts) и *групп* (group accounts) занимают важное место в обеспечении безопасности компьютера, поскольку с ними связаны разные права доступа к ресурсам, возможность выполнения на

компьютере или в сети определенного действия, например, архивации данных или выключения компьютера и т. д. В этой главе будут рассматриваться операции, выполняемые на автономных компьютерах (входящих в рабочие группы). Управление учетными записями в доменах Active Directory рассматривается позже, в *главе 12*.

Операции с учетными записями в окне панели управления

Как и в Windows Vista, на автономных компьютерах, работающих под управлением Windows Server 2008, простые операции по управлению пользователями могут выполняться с панели управления: нужно выбрать задачу **User Accounts** (Учетные записи пользователей) (категория **User Accounts** (Учетные записи пользователей)).

Рис. 4.3. Управление основными параметрами учетной записи пользователя

В окне учетной записи (рис. 4.3), помимо простых действий (изменение пароля, рисунка или типа учетной записи), можно выполнять такие важные операции, как управление сетевыми паролями и сертификатами, используемыми при шифровании файлов и папок (также *см. главу 14*); можно включать или отключать контроль учетных записей (UAC) (эта функция

также будет рассмотрена в *главе 14*). Обратите внимание на то, что многие операции требуют административных полномочий — около их названий присутствует значок системы безопасности. Операции с группами в этом окне невозможны.

Окно учетных записей пользователей на компьютере, включенном в домен, будет выглядеть немного иначе, некоторые возможности будут отсутствовать (рис. 4.4); с панели управления можно менять только основные параметры учетной записи зарегистрированного пользователя. Обычно же на доменных компьютерах для управления локальными учетными записями используется оснастка **Local Users and Groups** (Локальные пользователи и группы) *(см. далее)*.

Рис. 4.4. Окно управления параметрами учетной записи на компьютере — члене домена

Совет

В окно управления учетной записью (см. рис. 4.3) можно попасть, введя в меню **Start** (Пуск) или в окне **Run** (Выполнить) строку `control /name Microsoft.UserAccounts`. На автономных компьютерах для этого можно также использовать команду `control UserPasswords`. Однако на компьютерах — членах домена при выполнении этой команды будет запускаться оснастка **Local Users and Groups** (Локальные пользователи и группы), а на контроллерах домена — оснастка **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры).

По ссылке **Manage your network passwords** (Управление сетевыми паролями) пользователь может попасть в окно (рис. 4.5), где перечислены сохраненные имена и пароли, использованные для доступа к различным сетевым ресурсам, включая удаленные компьютеры и коммуникационную службу Windows Live (или другие ресурсы Microsoft). Здесь можно менять имеющиеся параметры, а также сохранять их (кнопка **Back up**) для переноса на другой компьютер с последующим восстановлением.

Рис. 4.5. Окно управления сохраненными сетевыми паролями

По ссылке **Manage another account** (Управление другой учетной записью) (см. рис. 4.3) можно попасть в окно, где показаны учетные записи всех пользователей, имеющихся на компьютере (рис. 4.6), при этом видны состояние каждой записи и наличие пароля. В этом окне можно выбирать записи для последующих изменений, а также создавать новые записи. Отключенную учетную запись из этого окна можно *включить*, однако для *отключения* записей используется только оснастка **Local Users and Groups** (Локальные пользователи и группы) *(см. далее)*.

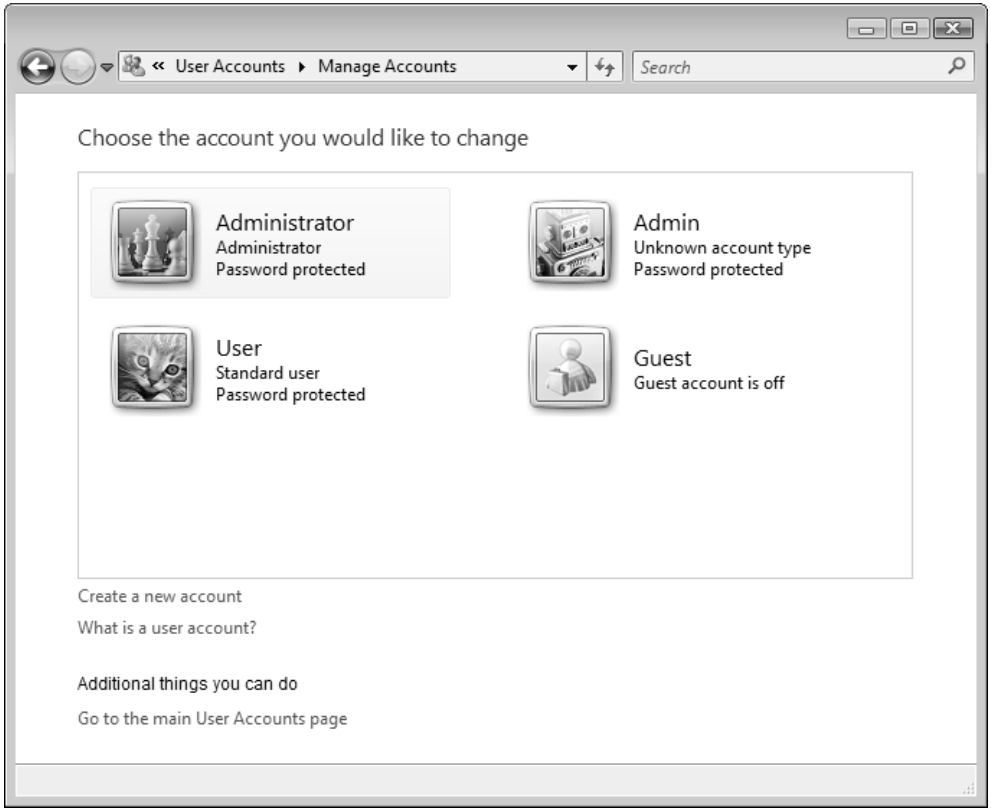


Рис. 4.6. В этом окне видны значки всех пользователей компьютера, и можно выбрать учетную запись для изменения ее параметров

Все учетные записи пользователей относятся к одному из двух типов:

- *Administrator* (Администратор) — администратор компьютера (входящий в группу Administrators (Администраторы)), имеющий все полномочия как по отношению к системе, так и по отношению ко всем файлам и папкам (кроме личных, private: разрешения на доступ к приватной информации имеют только система и владелец этой информации);
- *Standard User* (Обычный доступ) — рядовой пользователь (входящий в группу Users (Пользователи)), который имеет право только изменять свой значок и пароль, а также может читать из доступных ему папок (в свою личную папку он, конечно, может и записывать, как и в папку **Public** (Общие)).

Тип пользователя и наличие пароля (Password protected) видны в окне управления учетными записями пользователей (см. рис. 4.6). Тип обязательно ука-

зывается при создании новой учетной записи (рис. 4.7); ее пароль и другие атрибуты можно менять позже, выбрав запись в списке имеющихся.

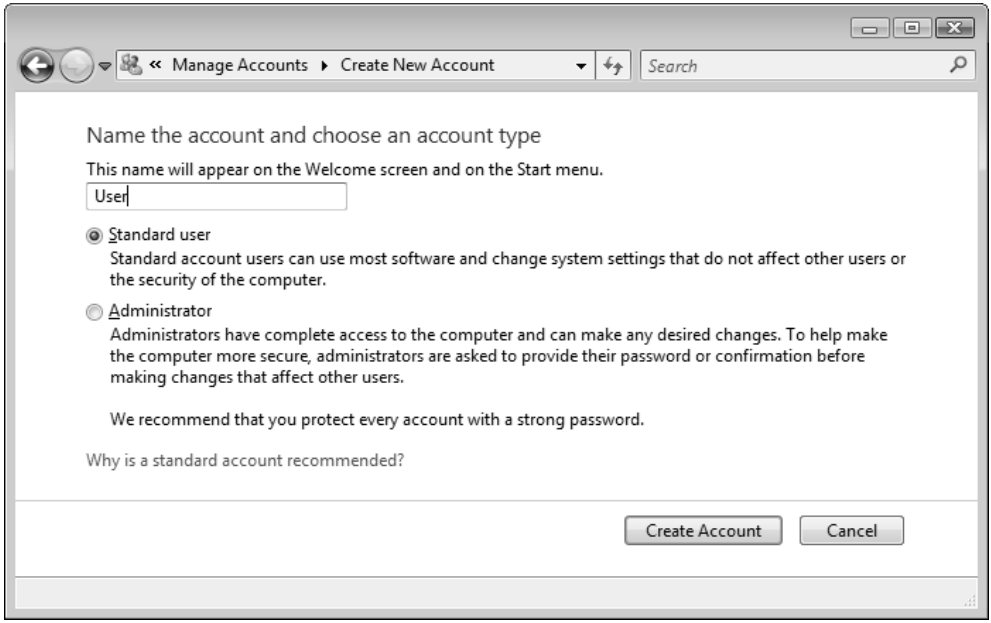


Рис. 4.7. Создание новой учетной записи и выбор ее типа

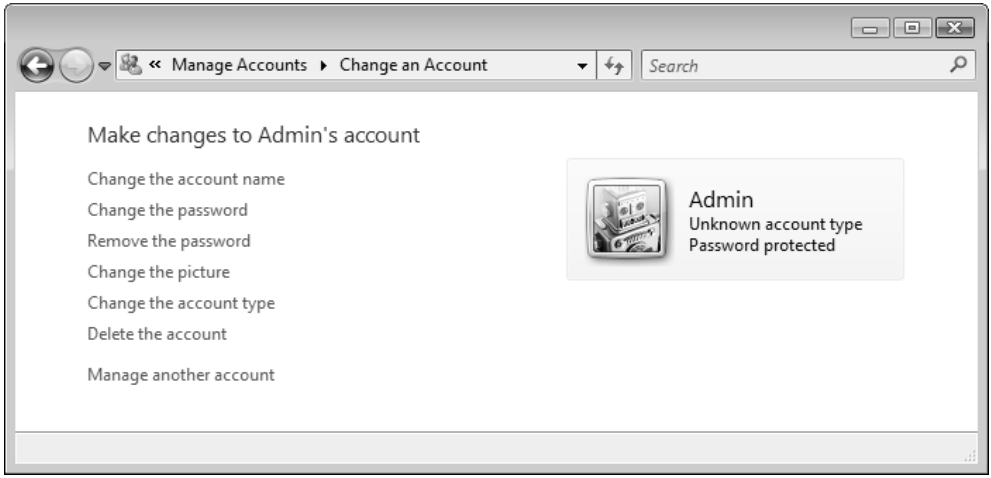


Рис. 4.8. Окно изменения атрибутов учетной записи пользователя

Как можно видеть на рис. 4.8, администратор компьютера может изменить или удалить пароль для учетной записи другого пользователя, поменять его рисунок и тип записи. При удалении учетной записи можно указать — будут ли удаляться пользовательские файлы, связанные с этой записью (содержимое личных папок), или же их следует сохранить.

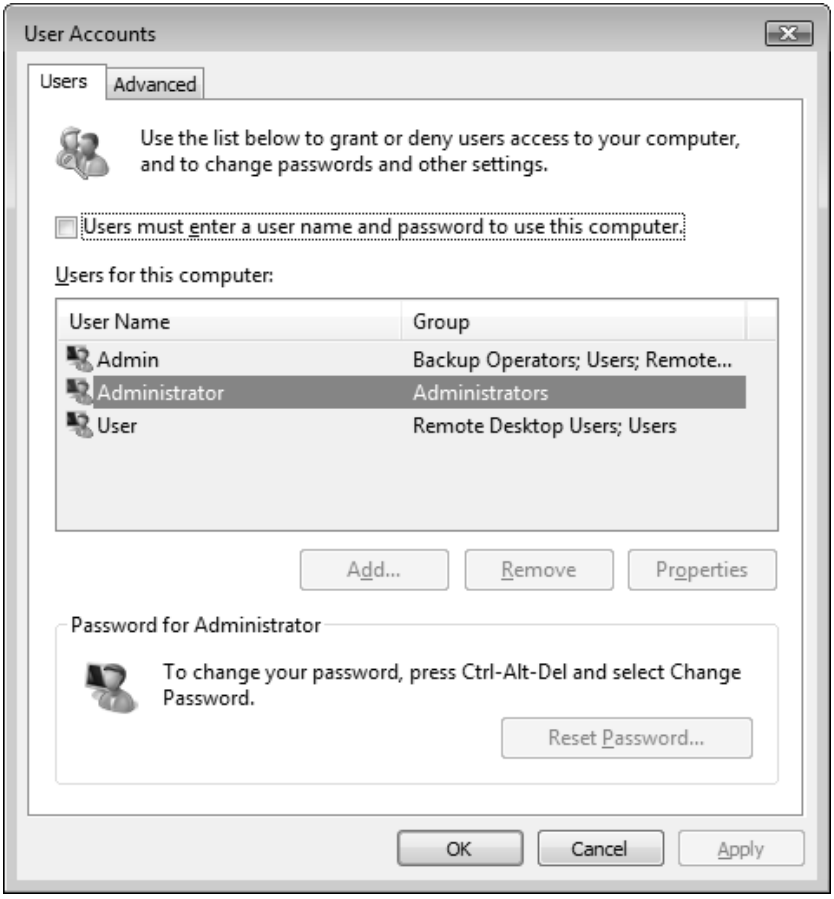


Рис. 4.9. Окно дополнительных возможностей по управлению локальными учетными записями

Имеется еще одно окно управления учетными записями, которое обычно доступно на компьютерах — членах домена — в него можно попасть из окна параметров учетной записи администратора компьютера по ссылке **Manage User**

Accounts (Управление учетными записями) (см. рис. 4.4). На автономных компьютерах в это окно можно попасть, введя строку `control userpasswords2` или `netplwiz` в меню **Start** (Пуск) или в окне **Run** (Выполнить). В окне перечислены локальные учетные записи пользователей и предлагаются некоторые дополнительные функции, касающиеся безопасности. Более интересны возможности этого окна на автономных компьютерах (рис. 4.9).

Выбрав в списке любую учетную запись, можно сменить пароль пользователя. Если флажок **Users must enter a user name and password to use this computer** (Требовать ввод имени пользователя и пароля) установлен (так задано по умолчанию), то для входа в систему каждый пользователь должен указать свой пароль. Если выбрать некоторую учетную запись и сбросить флажок (при подтверждении операции требуется также ввести пароль этой учетной записи), то вход в систему будет выполняться автоматически с использованием этой учетной записи (т. е. выполняется функция "автологон" (autologon)). Это позволяет избегать ручного редактирования реестра для включения данной функции.

Оснастка *Local Users and Groups*

Оснастка **Local Users and Groups** (Локальные пользователи и группы; lusrmgr.msc) позволяет управлять локальными учетными записями пользователей и групп — как на локальном, так и на удаленном компьютере. На компьютерах–членах домена она является основным инструментом для манипуляций с учетными записями. Запускать оснастку может любой пользователь, однако выполнять *администрирование* учетных записей могут только администраторы и члены группы Power Users (Опытные пользователи), оставленной в Windows Server 2008 для обратной совместимости.

> ***Примечание***
>
> Для работы с локальными учетными записями пользователей и групп в окне консоли применяются команды `net user` и `net localgroup` соответственно. На контроллерах доменов можно также запускать команду `net group`, позволяющую манипулировать глобальными группами.

Пример окна оснастки **Local Users and Groups** (Локальные пользователи и группы) приведен на рис. 4.10. В системах Windows Server 2008 эту оснастку

нельзя запускать из меню **Start** (Пуск); она входит в состав оснастки **Computer Management** (Управление компьютером), а также включена в состав оснастки **Server Manager** (Диспетчер сервера), имеющейся только в Windows Server 2008. Кроме того, ее можно также подключать к любой пользовательской консоли MMC. Все операции по манипулированию учетными записями пользователей и групп выполняются с помощью команд, имеющихся в контекстных меню выбранных объектов или находящихся в меню **Action** (Действие) или на панели действий (**Actions**) (на рисунке она отключена).

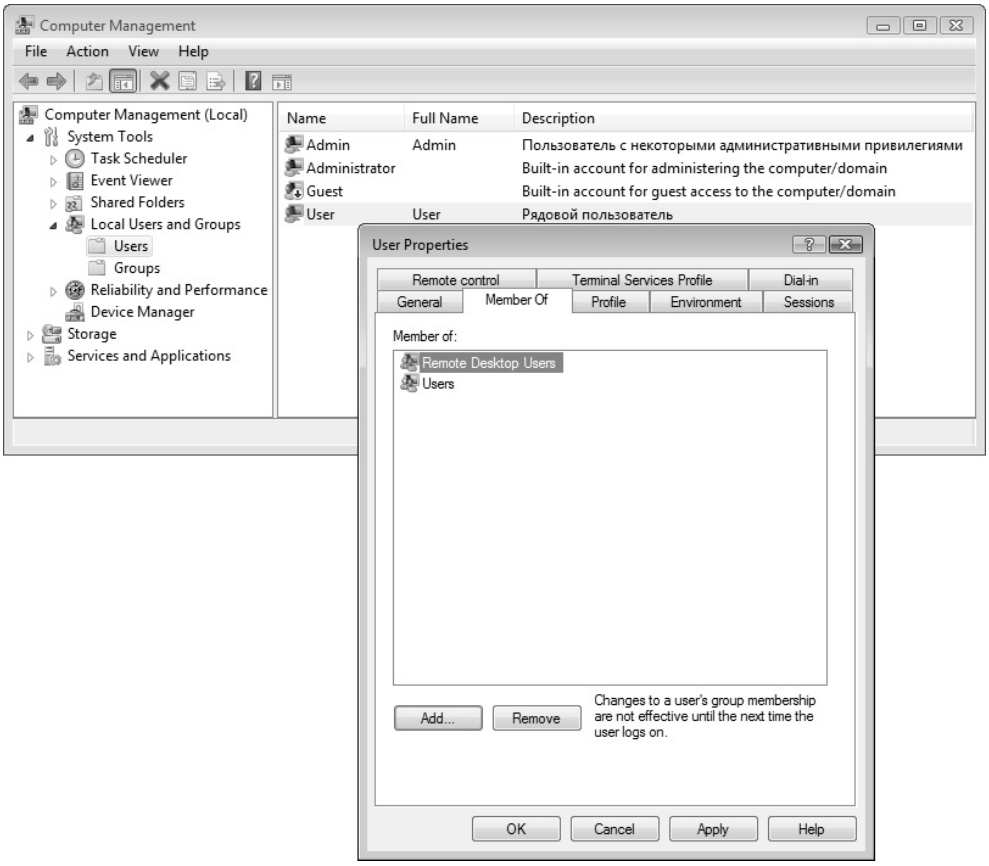


Рис. 4.10. Узел **Local Users and Groups** в составе оснастки **Computer Management** и окно свойств учетной записи пользователя

Стандартные учетные записи пользователей

Сразу после установки системы Windows Server 2008 папка **Users** (Пользователи) в окне оснастки **Local Users and Groups** (Локальные пользователи и группы) содержит всего две автоматически создаваемые встроенные учетные записи:

- **Administrator** (Администратор) — эту учетную запись используют при установке и настройке операционной системы. Она не может быть уничтожена, блокирована или удалена из группы Administrators (Администраторы), ее можно только переименовать; в системах Windows Server 2008 по умолчанию включена и используется при первом входе в систему;
- **Guest** (Гость) — эта учетная запись применяется для регистрации в компьютере без использования специально созданной учетной записи. Учетная запись **Guest** (Гость) не требует ввода пароля и по умолчанию заблокирована. (Обычно пользователь, учетная запись которого блокирована, но не удалена, при регистрации получает предупреждение и входить в систему не может.) Она является членом группы Guests (Гости), и ей можно предоставлять права доступа к ресурсам системы точно так же, как любой другой учетной записи.

Стандартные учетные записи групп

В системах Windows Server 2008 папка **Groups** (Группы) содержит шестнадцать встроенных групп. Они создаются автоматически при установке системы. Ниже описаны свойства этих групп:

- **Administrators** (Администраторы) — ее члены обладают полным доступом ко всем ресурсам системы. Это единственная встроенная группа, автоматически предоставляющая своим членам весь набор встроенных прав. По умолчанию содержит учетную запись пользователя, чье имя было введено при начальном конфигурировании системы, и встроенную учетную запись Administrator (Администратор). На компьютере, входящем в домен, в эту группу по умолчанию включается доменная группа Domain Admins (Администраторы домена);
- **Backup Operators** (Операторы архива) — члены этой группы могут архивировать и восстанавливать файлы в системе независимо от того, какими правами эти файлы защищены. Кроме того, операторы архива могут входить в систему и завершать ее работу, но они не имеют права изменять настройки безопасности. По умолчанию группа пуста;

- **Certificate Service DCOM Access** (DCOM-доступ к службе сертификатов) — членам этой группы разрешено подключаться к корпоративным Центрам сертификации (Certification Authorities). По умолчанию группа пуста;
- **Cryptographic Operators** (Криптографические операторы) — членам этой группы дано право выполнять операции, связанные с шифрованием. По умолчанию группа пуста;
- **Distributed COM Users** (Пользователи DCOM) — члены этой группы могут запускать, активизировать и использовать DCOM-объекты на данном компьютере. По умолчанию группа пуста;
- **Event Log Readers** (Читатели журнала событий) — членам этой группы разрешено чтение системных журналов локального компьютера. По умолчанию группа пуста;
- **Guests** (Гости) — эта группа позволяет выполнить регистрацию пользователя с помощью учетной записи Guest (Гость) и получить ограниченные права на доступ к ресурсам системы. По умолчанию содержит только одну учетную запись — пользователя Guest (Гость);
- **IIS_IUSRS** — группа, используемая службами Internet Information Services (IIS). Имеется, даже если эти службы ***не*** установлены; по умолчанию пуста;
- **Network Configuration Operators** (Операторы настройки сети) — группа, члены которой имеют некоторые права по настройке сетевых служб и параметров. По умолчанию пуста;
- **Performance Log Users** (Пользователи журналов производительности) — членам этой группы дано право удаленно запускать журналы регистрации системных событий на данном компьютере. По умолчанию пуста;
- **Performance Monitor Users** (Пользователи системного монитора) — этой группе дано право удаленного доступа к средствам мониторинга данного компьютера. По умолчанию пуста;
- **Power Users** (Опытные пользователи) — группа существует лишь для совместимости с предыдущими версиями Windows. Члены этой группы могут создавать учетные записи пользователей, но они имеют право модифицировать настройки безопасности только для созданных ими учетных записей. Кроме того, они могут создавать локальные группы и модифицировать состав членов созданных ими групп. То же самое они могут делать с группами Users (Пользователи), Guests (Гости) и Power

Users (Опытные пользователи). Члены группы Power Users (Опытные пользователи) не могут модифицировать членство в группах Administrators (Администраторы) и Backup Operators (Операторы архива). Они не могут быть владельцами файлов, архивировать или восстанавливать каталоги, загружать и выгружать драйверы устройств и модифицировать настройки безопасности и журнал событий. По умолчанию пуста;

- **Print Operators** (Операторы печати) — группа пользователей, которым разрешено управление принтерами домена. По умолчанию пуста;
- **Remote Desktop Users** (Пользователи удаленного рабочего стола) — эта группа содержит имена пользователей, которым явно разрешен удаленный доступ к рабочему столу. По умолчанию пуста; изначально доступ разрешен только членам группы Administrators (Администраторы);
- **Replicator** (Репликатор) — группа, используемая службой репликации файлов. Ее членами не следует делать рабочие учетные записи. По умолчанию пуста;
- **Users** (Пользователи) — члены этой группы могут выполнять большинство пользовательских функций, например, запускать приложения, пользоваться локальным или сетевым принтером, завершать работу системы или блокировать рабочую станцию. Они также могут создавать локальные группы и регулировать состав их членов. Они не могут получить доступ к общему каталогу или создать локальный принтер. По умолчанию содержит служебные записи NT AUTHORITY\INTERACTIVE (S-1-5-4) (NT AUTHORITY\ИНТЕРАКТИВНЫЕ) и NT AUTHORITY\Authenticated Users (S-1-5-11) (NT AUTHORITY\Прошедшие проверку), а также созданные на компьютере учетные записи обычных пользователей. На компьютере, входящем в домен, в эту группу по умолчанию включается доменная группа Domain Users (Пользователи домена).

Сохранение и восстановление паролей пользователей

Если локальные учетные записи системы защищаются паролями, уменьшается вероятность того, что посторонний пользователь получит несанкционированный доступ к данным. Однако в этом случае существует риск потери доступа к системе в случае забывания пароля. Если пароль обновить принудительно, то пользователь может потерять персональные настройки конфигурации

компьютера (например, сертификаты, используемые при шифровании данных). Имеется возможность сохранения пароля на дискете или флэш-устройстве, что позволит установить новый пароль в случае утраты старого. Однажды сохраненный пароль позволит войти в систему, даже если после этого текущий пароль менялся неоднократно.

Внимание!

Хранящийся на дискете или флэш-устройстве пароль фактически является ключом к компьютеру, и необходимо обеспечить сохранность этого носителя, равно как и его недоступность для посторонних. Дискеты восстановления создаются индивидуально для каждой учетной записи.

Операция сохранения пароля возможна (и имеет смысл) только на компьютерах, ***не*** входящих в домен Active Directory. На доменных компьютерах пароль может установить администратор домена.

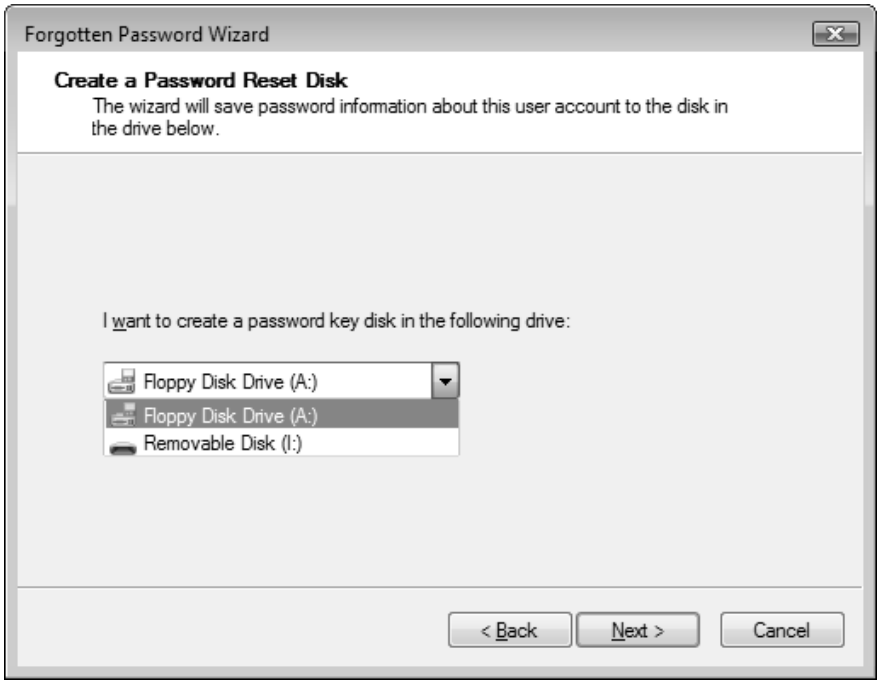


Рис. 4.11. Выбор устройства для хранения информации, необходимой для восстановления пароля учетной записи

Для сохранения пароля нужно с панели управления открыть окно задачи **User Accounts** (Учетные записи пользователей) (см. рис. 4.3) и щелкнуть по ссылке **Create a password reset disk** (Создание дискеты восстановления пароля). Пароль можно сохранять только самостоятельно, даже администратор не сможет выполнить эту операцию для *чужой* учетной записи. Мастер *Forgotten Password Wizard* (Мастер забытых паролей) попросит указать устройство, которое будет использоваться (привод флоппи-дисков или флэш-накопитель, который нужно подключить *заранее*) (рис. 4.11), а затем подтвердить текущий пароль пользователя, после чего запишет в память устройства файл userkey.psw, содержащий в зашифрованном виде пароль текущей учетной записи.

Если пароль забыт или введен неправильно, то на экране приветствия появится дополнительная ссылка **Reset password** (Сменить пароль) (рис. 4.12). Если по ней щелкнуть мышью, запустится мастер *Password Reset Wizard* (Мастер сброса пароля), который попросит установить дискету восстановления, а затем задать произвольный новый пароль (рис. 4.13). После этого пользователь возвращается в окно приветствия и может войти в систему, пользуясь *вновь созданным* паролем.

Рис. 4.12. Предложение сменить пароль в случае ошибочного ввода пароля

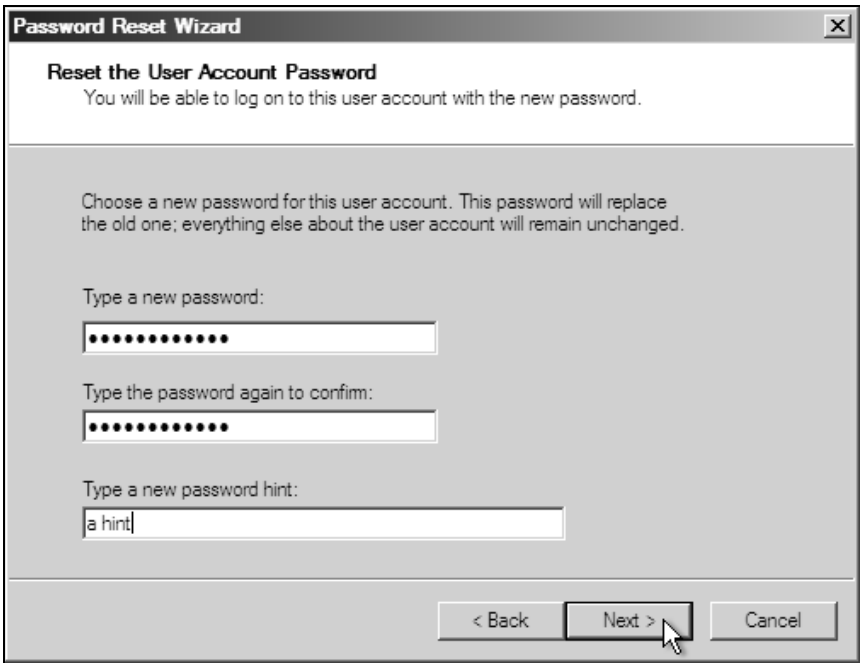


Рис. 4.13. Создание нового пароля для входа в систему

Изменение имени компьютера и подключение к домену

Чтобы получить возможность изменить описание или имя компьютера, необходимо открыть традиционное окно свойств системы (см. рис. 3.8). Для этого нужно открыть окно **System** (Система) (см. рис. 3.7), нажав клавиши <Win>+<Pause/Break>, и щелкнуть по ссылке **Advanced system settings** (Дополнительные параметры системы). Можно сразу получить доступ к нужному окну, если ввести строку `sysdm.cpl` в меню **Start** (Пуск) или в окне **Run** (Выполнить).

На вкладке **Computer Name** (Имя компьютера) указывается описание компьютера, которое будут видеть другие клиенты сети. Нажав кнопку **Change** (Изменить), мы попадем в окно (рис. 4.14), где задано имя компьютера. После изменения имени потребуется перезагрузка системы.

Рис. 4.14. Окно выбора имени компьютера и домена или локальной группы

Все компьютеры по умолчанию принадлежат к рабочей группе WORKGROUP, которая задается при установке системы. Для систем Windows Server 2008 имя группы и принадлежность к домену можно задавать только после инсталляции (если не использовать автоматическую установку). В указанном окне имя группы можно изменить, после чего требуется перезагрузить компьютер.

> ***Внимание!***
>
> Не рекомендуется одновременно менять имя компьютера и подключать его к домену — при подключении имя уже должно быть определено.

Чтобы подключить компьютер к домену Active Directory, необходимо выбрать соответствующий переключатель и ввести DNS-имя домена (см. рис. 4.14). ***До этого*** обязательно нужно изменить (или проверить) настройки протокола TCP/IP для подключения по локальной сети: предпочитаемый DNS-сервер (Preferred DNS server) должен указывать на тот же сервер, кото-

рый используют контроллеры домена (или же сетевые параметры должны автоматически получаться от корпоративного DNCP-сервера).

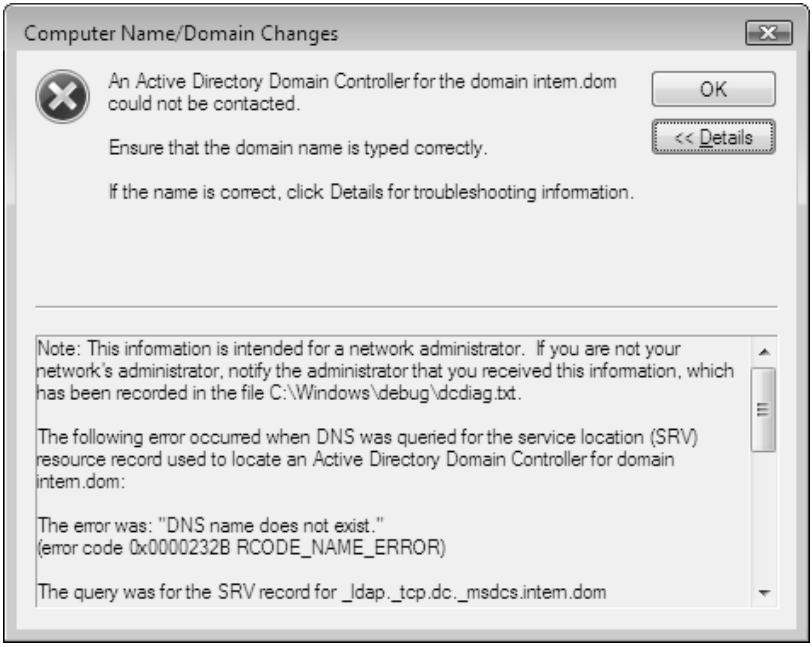


Рис. 4.15. Ошибка подключения к домену Active Directory; обычно причиной является неправильная конфигурация протокола TCP/IP

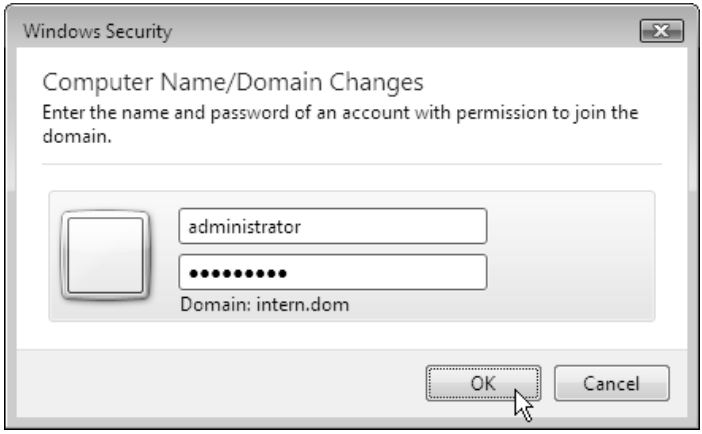


Рис. 4.16. Запрос учетных данных администратора, имеющего право добавления компьютеров в домен

После ввода DNS-имени домена и нажатия кнопки **ОК** начнется обращение к контроллерам указанного домена. Если разрешение DNS-имен настроено неверно, то дальнейшие операции невозможны — появится сообщение об ошибке (рис. 4.15) и необходимо проверять настройки протокола TCP/IP. Если подключение к контроллеру произошло, то требуется ввести имя и пароль пользователя, имеющего право на подключение компьютеров к домену (обычно указывается учетная запись администратора домена) (рис. 4.16).

Если операция подключения прошла успешно, то появляется окно приглашения в указанный домен, после чего требуется перезагрузка компьютера.

Удаленный административный доступ к компьютеру

В системах Windows, начиная с Windows XP, всегда присутствует однопользовательская версия служб терминалов (Terminal Services). С их помощью можно "войти" в систему с любого удаленного компьютера или Windows-терминала и работать в системе, как на локальной консоли. Такая функция называется *Remote Desktop* (Удаленный рабочий стол). По соображениям безопасности по умолчанию удаленный доступ выключен.

Помимо этого, имеется еще одно средство, также реализованное на основе служб терминалов и называемое *Remote Assistance* (Удаленный помощник). С его помощью пользователь компьютера может для получения помощи в работе обратиться с приглашением к удаленному пользователю (администратору, работнику службы поддержки или просто опытному специалисту) и предоставить возможность доступа к своему компьютеру. По умолчанию удаленный пользователь может только *видеть* рабочий стол компьютера, но при необходимости и обоюдном согласии можно дать право *управления* компьютером (при этом оба пользователя будут фактически одновременно работать в системе).

Далее оба названных средства и способы их применения и настройки будут по очереди рассматриваться подробно.

Удаленный рабочий стол

Для включения режима административного удаленного доступа используется вкладка **Remote** (Удаленное использование) окна **System Properties** (Свойства

системы) (рис. 4.17). (Для быстрого доступа к этому окну можно нажать клавиши <Win>+<Pause/Break>, а в открывшемся окне (см. рис. 3.7) щелкнуть по ссылке **Remote settings** (Настройка удаленного доступа).) На рисунке показаны установки, заданные по умолчанию. (Обратите внимание на то, что флажок **Remote Assistance** (Удаленный помощник) вообще недоступен.)

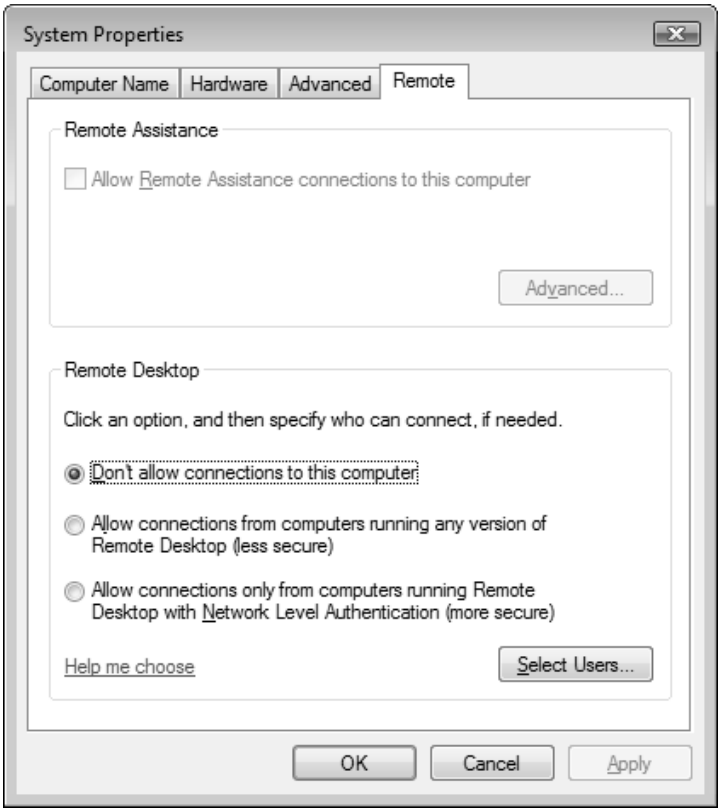


Рис. 4.17. Окно управления удаленным доступом

Для того чтобы пользователи с других компьютеров смогли обратиться к локальной системе, установите флажок **Allow connections from computers running any version of Remote Desktop** (Разрешить подключение от компьютеров с любой версией удаленного рабочего стола). Следующая опция (**Allow connections only from computers running Remote Desktop with Network Level Authentication**) разрешает подключение только от тех компьютеров, на которых используется новый метод сетевой аутентификации NLA, позво-

ляющий повысить защищенность удаленного соединения. Этот метод используется в Windows Vista и Windows Server 2008; при установке пакетов обновления его можно применять и на предыдущих версиях Windows.

Примечание

Если запустить утилиту Remote Desktop Connection (Подключение к удаленному рабочему столу), в ее окне (см. рис. 4.20) щелкнуть по значку, расположенному в верхнем левом углу, и выполнить в меню команду **About** (О программе), то в появляющемся окне по наличию строки, выделенной на рис. 4.18 ("Network Level Authentication supported" — "Поддерживается проверка подлинности на уровне сети"), можно судить о том, поддерживается ли в данной системе аутентификация NLA. Также можно видеть, что в Windows Server 2008 используется протокол RDP 6.1.

Рис. 4.18. Сообщение, указывающее на то, что данная система поддерживает NLA

После включения удаленного доступа к рабочему столу на экране появляется сообщение о том, что настройки встроенного брандмауэра Windows были автоматически изменены, и разрешены исключения для программы Remote Desktop (рис. 4.19). При необходимости можно вручную выполнить дополнительные изменения параметров брандмауэра.

Теперь, нажав кнопку **Select Users** (Выбрать пользователей), можно *явно* указать, каким пользователям разрешен удаленный доступ к компьютеру: эти пользователи автоматически будут включены в группу Remote Desktop Users (Пользователи удаленного рабочего стола). По умолчанию доступ к компьютеру имеют только администраторы. Использовать учетные записи *без* пароля для удаленного доступа нельзя.

Для инициализации сеанса удаленного доступа служит утилита *Remote Desktop Connection* (Подключение к удаленному рабочему столу) (она запускается из меню **Start** | **All Programs** | **Accessories** (Пуск | Все программы | Стандартные)). Чтобы инициировать соединение с удаленным компьютером, достаточно ввести его имя или IP-адрес и нажать кнопку **Connect** (Подключить) (рис. 4.20).

Рис. 4.19. Предупреждение об изменениях настроек встроенного брандмауэра

Рис. 4.20. Из этого окна можно инициировать сеанс работы с удаленным компьютером

Примечание

Для запуска утилиты Remote Desktop Connection (Подключение к удаленному рабочему столу) из окна командной строки используется команда `mstsc`. Ее параметры можно увидеть, запустив с ключом `/?`.

Обычно при обращении к удаленному компьютеру появляется предупреждении о том, что данное подключение не прошло полной проверки на безопасность (рис. 4.21), и это сообщение будет появляться каждый раз, пока не будет установлен флажок **Don't ask me again for remote connections to this computer** (Не выводить данное предупреждение для подключений к этому удаленному компьютеру) или не будут реализованы дополнительные средства идентификации компьютеров. Если подключение выполняется к известному компьютеру и действие инициировано самим пользователем, то можно смело нажимать кнопку **Connect** (Подключить).

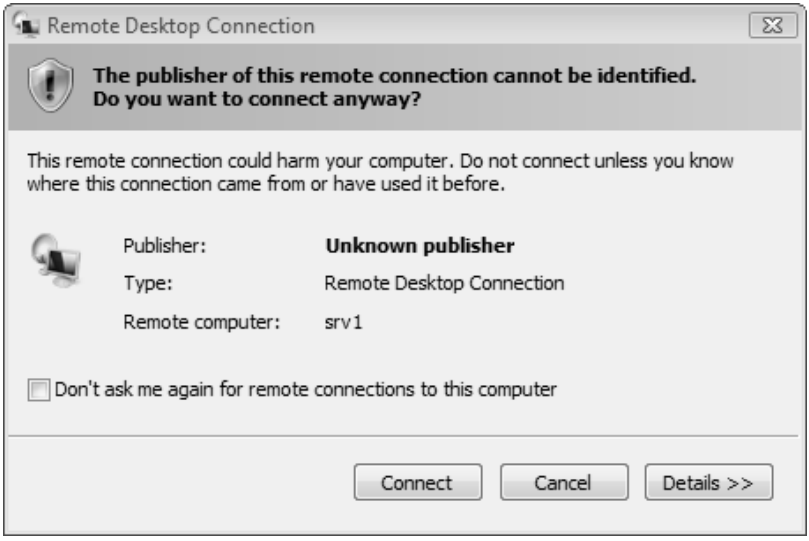


Рис. 4.21. Запрос на подтверждение легитимности выполняемого подключения

В следующем окне (рис. 4.22) потребуется указать имя и пароль учетной записи, которая будет использоваться для регистрации на удаленном компьютере. (По умолчанию предлагается имя пользователя, использовавшееся в предыдущем сеансе, но можно вводить и любое другое.) Установив флажок **Remember my credential** (Запомнить мои учетные данные), вы избавитесь от

необходимости ввода учетных данных при повторных подключениях к выбранному компьютеру. Если выполняется подключение к компьютеру, работающему под управлением операционной системы младше, чем Windows Vista, то такое окно не появляется, и параметры учетной записи вводятся в окне регистрации в удаленной системе.

Рис. 4.22. Запрос учетных данных для доступа к удаленному компьютеру

По умолчанию системы Windows Server 2008 пытаются использовать NLA-аутентификацию. Если это не удается, то может появиться сообщение, приведенное на рис. 4.23. Если текущий уровень безопасности протокола RDP приемлем для работы, то подключение можно продолжить. (Способ проверки аутентификации можно задать в окне параметров утилиты Remote Desktop Connection (Удаленное подключение к рабочему столу) — *см. ниже*.) Если все параметры заданы правильно, то появится окно регистрации в системе или сразу рабочий стол удаленного компьютера (если учетная запись и пароль были указаны заранее).

Для настройки параметров соединения в окне **Remote Desktop Connection** (Удаленное подключение к рабочему столу) (см. рис. 4.20) нажмите кнопку **Options** (Параметры). В окне параметров ознакомьтесь со всеми вкладками, на которых определяются значения. Можно, например, устанавливать размер экрана и глубину цвета (до 32 бит) (рис. 4.24); на вкладке **Experience** (Дополнительно) задается скорость подключения и т. д.

Рис. 4.23. Предупреждение о том, что запрашиваемая система поддерживает более низкий уровень аутентификации, чем Windows Vista

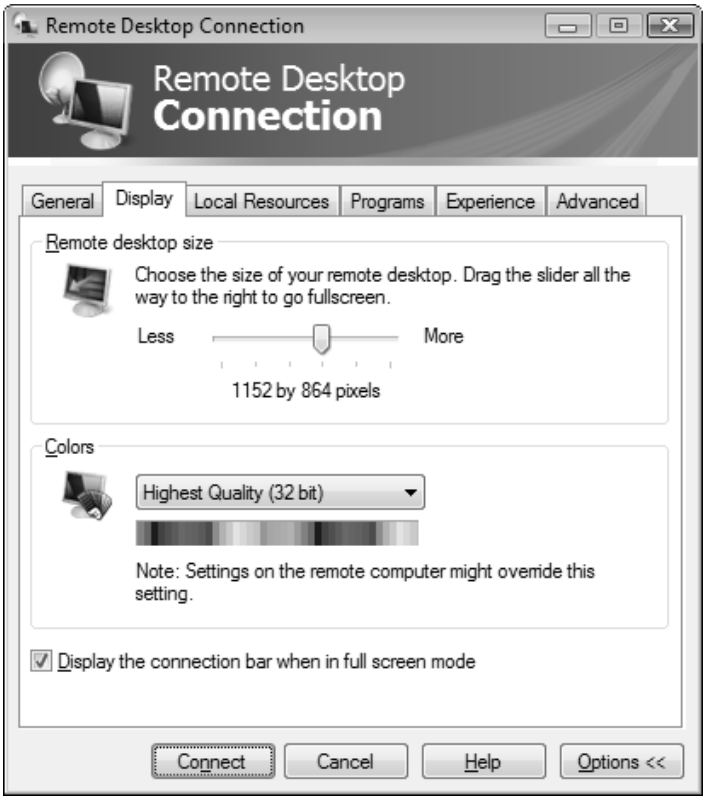


Рис. 4.24. Определение параметров окна, используемого в сеансе удаленного доступа

Следует особо обратить внимание на вкладку **Local Resources** (Локальные ресурсы) (рис. 4.25), где можно указать — какие локальные диски или другие ресурсы (например, принтеры) будут использоваться при работе на удаленном компьютере.

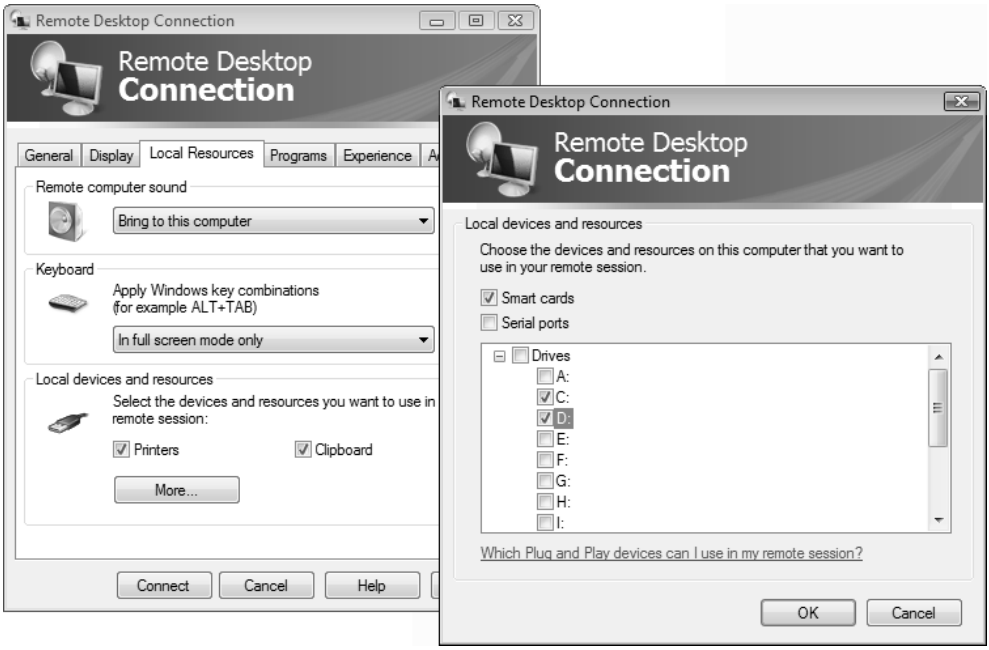


Рис. 4.25. Параметры использования локальных ресурсов в сеансе удаленного доступа

После выполнения подключения некоторые *локальные* ресурсы могут быть доступны при работе на *удаленном* компьютере — в показанном примере разрешен доступ к некоторым локальными дискам, принтеру и буферу обмена. Системные звуковые сигналы с удаленного компьютера по умолчанию переназначаются на локальный компьютер. Если разрешить подключение локальных дисков, то в окне программы Windows Explorer (Проводник) на удаленном компьютере одновременно будут отображаться диски обоих компьютеров, что очень удобно, например, для выполнения операций копирования файлов.

Сохранение и изменение параметров подключения

Параметры текущего подключения можно сохранить в файле (соответствующие команды имеются в окне параметров на вкладке **General** (Общие) — сначала нужно выполнить команду **Save As** (Сохранить как), а потом достаточно обычной команды сохранения) и использовать в дальнейшей работе для быстрой настройки подключения к конкретному компьютеру. Для редактирования сохраненных параметров подключения нужно выбрать файл или значок, щелкнуть правой кнопкой мыши и в контекстном меню выполнить команду **Edit** (Изменить) — появится окно настроек (см. рис. 4.24).

Одновременное подключение к одному компьютеру

В отличие от Windows Vista, в системах Windows Server 2008 одновременно активными могут быть не одно, а два подключения к рабочему столу, при этом считаются локальные подключения и подключения с использованием функции Remote Desktop (Удаленный рабочий стол).

Рис. 4.26. Запрос на отключение зарегистрированного пользователя в случае конфликтов

Таким образом, одновременно в системе могут работать два удаленных пользователя или один локальный и один удаленный. "Лишние" пользователи будут "выталкиваться" из системы — сеанс *удаленного* пользователя будет от-

ключаться, а *локальный* пользователь увидит экран регистрации в системе. При этом вся рабочая среда — запущенные приложения и открытые окна — будет сохраняться до последующего входа в систему. Это нужно иметь в виду как в процессе работы, так и при выключении компьютера.

Если при попытке подключения удаленного пользователя на компьютере уже зарегистрированы два других пользователя и возникает конфликт, то пользователь, входящий в систему, может выбрать учетную запись, которая должна быть отключена, — для этого нужно сделать выбор в специальном окне (рис. 4.26). Отключаемый пользователь на своем экране увидит сообщение, аналогичное показанному на рис. 4.27. В этом случае он может сразу прекратить работу (его программы и окна затрагиваться не будут и останутся в текущем состоянии до следующего подключения), либо же он может отклонить запрос на подключение, нажав кнопку **Cancel** (Отмена).

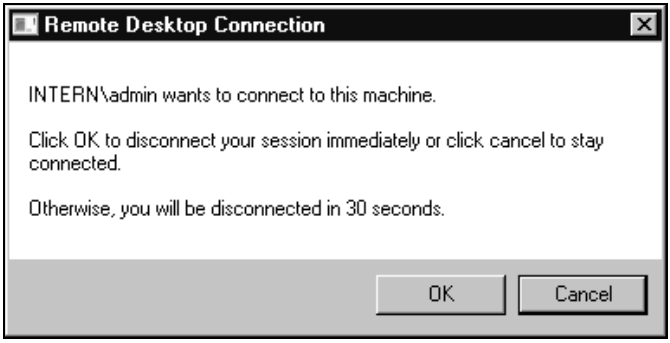


Рис. 4.27. Сообщение о попытке удаленного подключения к локальному компьютеру

Отключение от сеанса и управление удаленным компьютером

Удаленный пользователь, подключившись к компьютеру, может выйти из системы (команда **Log Off**) и закончить работу в ней, а может временно отключиться от сеанса, оставив работающие приложения и открытые окна (к которым он сможет вернуться при следующем подключении). Также, при наличии административных полномочий, пользователь может удаленно перезагрузить компьютер (**Restart**) или выключить его (**Shut Down**). Интерфейс

всех перечисленных команд зависит от удаленной операционной системы и несколько отличается для разных версий Windows.

На рис. 4.28 показано меню **Start** (Пуск) удаленной системы Windows Server 2008. Все команды, кроме отключения сеанса, присутствуют в меню; их также можно видеть в окне безопасности, в которое можно попасть, нажав кнопку **Windows Security** (Безопасность Windows). Чтобы временно отключиться от сеанса, нужно просто закрыть окно удаленного рабочего стола, щелкнув по соответствующей кнопке в его правом верхнем углу и подтвердив операцию в появляющемся окне (рис. 4.29).

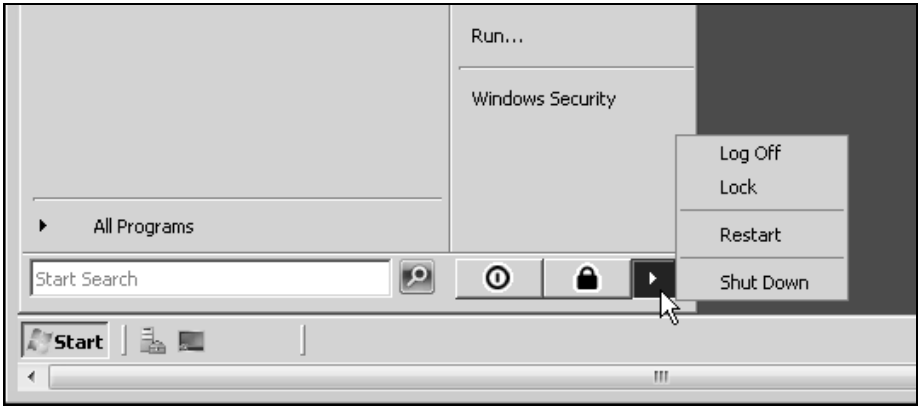


Рис. 4.28. Меню команд управления компьютером при удаленном доступе к Windows Server 2008

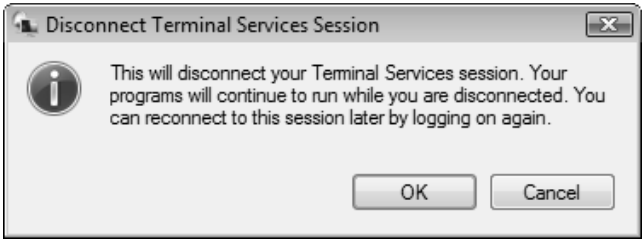


Рис. 4.29. Предупреждение об отключении сеанса удаленного доступа

Для системы Windows XP ситуация будет выглядеть иначе. Кнопки команд выхода из системы и отключения сеанса присутствуют в меню **Start** (Пуск) (рис. 4.30), а доступ к командам перезагрузки или выключения компьютера

можно получить, только нажав кнопку **Безопасность Windows** (при этом откроется окно безопасности Windows XP).

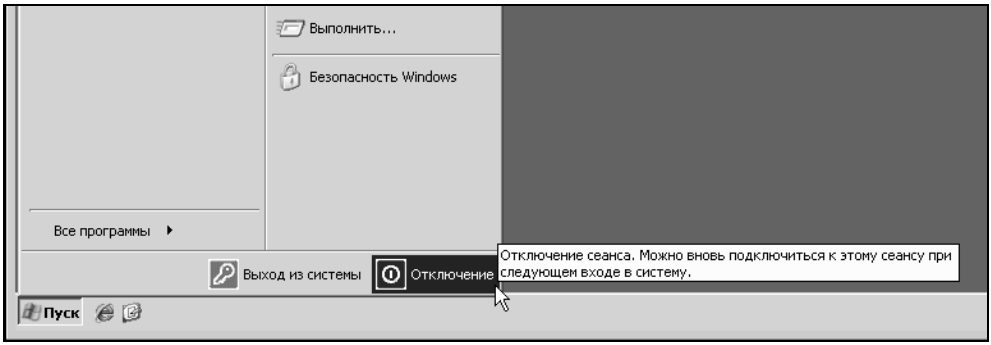


Рис. 4.30. Элементы управления сеансов удаленного доступа в Windows XP

Удаленный помощник

Для использования функции Remote Assistance (Удаленный помощник) обе взаимодействующие системы должны работать под управлением операционной системы не ниже Windows XP (следует, однако, учитывать некоторые проблемы совместимости, описанные в справочной системе Windows Server 2008).

Как видно на рис. 4.17, по умолчанию опция Remote Assistance (Удаленный помощник) на сервере недоступна, поскольку отсутствует соответствующий компонент (см. табл. 3.2). Поэтому сначала следует установить его с помощью оснастки **Server Manager** (Диспетчер сервера), после чего опция станет активной (перезагрузки не требуется).

Включать и отключать функцию Remote Assistance (Удаленный помощник) можно на вкладке **Remote** (Удаленное использование) (рис. 4.31) (сразу после установки соответствующего компонента сервера функция будет включена). Нажав на этой вкладке кнопку **Advanced** (Подробнее), можно настроить параметры удаленного помощника (рис. 4.32).

Обратите внимание на то, что по умолчанию разрешено и удаленное *управление* компьютером. Однако, несмотря на это, для получения управления компьютером во время сеанса работы удаленного помощника каждый раз требуется ***дополнительное и явное*** разрешение локального пользователя. Если не

менять срок действия запроса (по умолчанию 6 часов), то в течение этого времени приглашение будет действительным и помощник будет иметь возможность *запрашивать* доступ к локальному компьютеру, при этом всякий раз локальный пользователь должен будет дать отдельное разрешение.

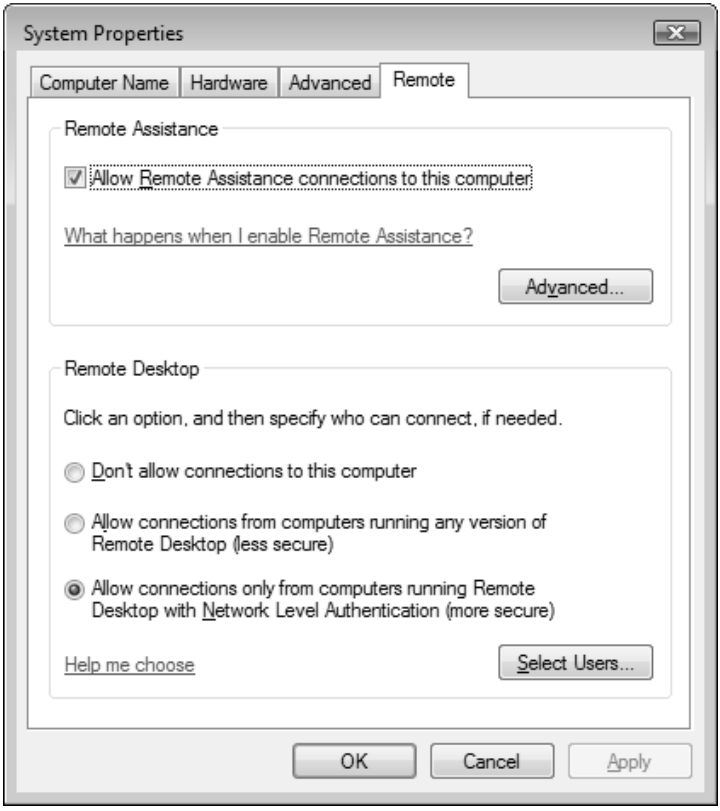


Рис. 4.31. Вкладка **Remote** после установки компонента Remote Assistance

Запрос на оказание помощи

В целом, работа с удаленным помощником не вызывает затруднений (поскольку осуществляется с помощью программы-мастера), поэтому ниже процедура инициализации сеанса совместной работы будет рассматриваться в целом.

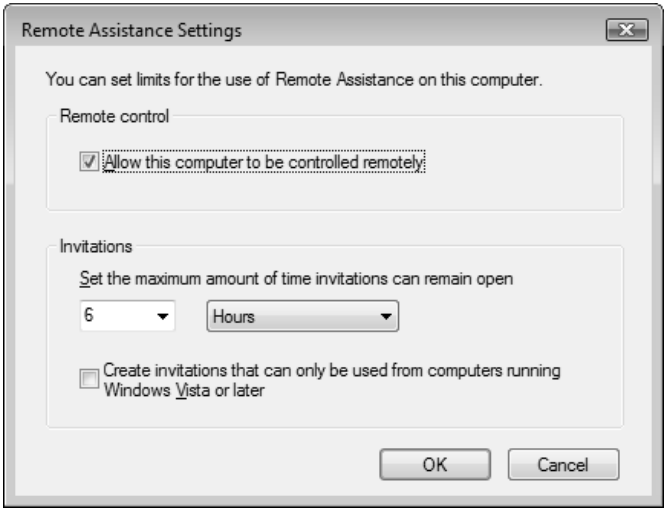


Рис. 4.32. Выбор параметров удаленного помощника

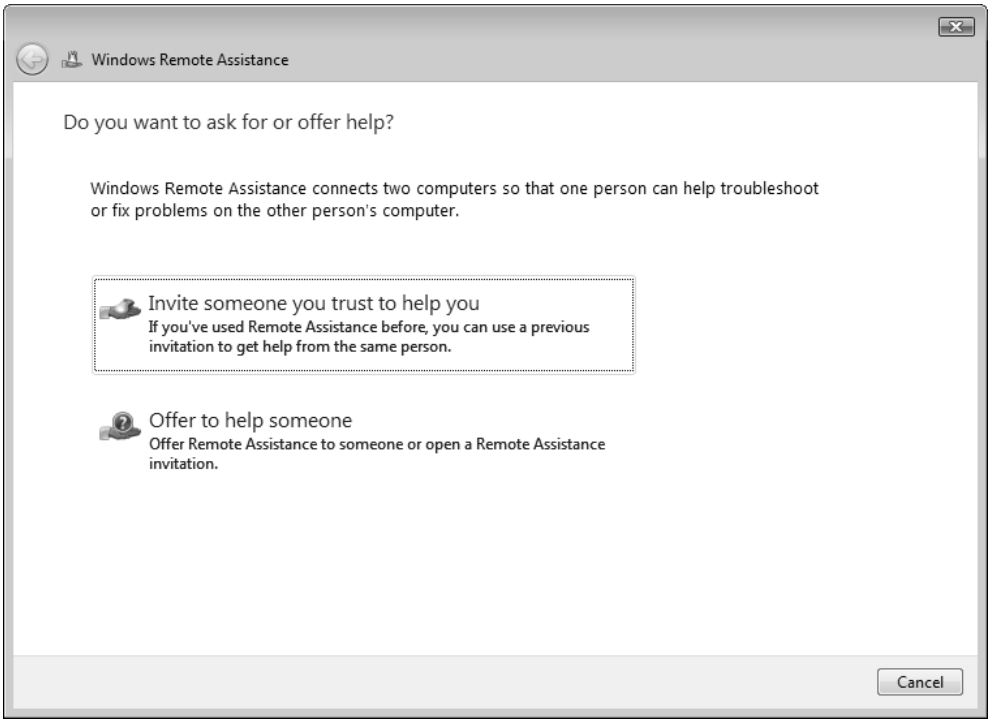


Рис. 4.33. Начальное окно запроса к удаленному помощнику

1. В меню **Start** (Пуск) выберите команду **Windows Remote Assistance** (Удаленный помощник Windows) в подменю **All Programs** | **Maintenance** (Все программы | Обслуживание) или введите в поле поиска или окне **Run** (Выполнить) команду `msra`.
2. В следующем окне (рис. 4.33) можно выбрать вариант использования удаленного помощника: первая опция (**Invite someone you trust to help you**) позволяет отправить *запрос на оказание помощи*, а вторая опция (**Offer to help someone**), наоборот, позволит вам *предложить свою помощь* другому пользователю.

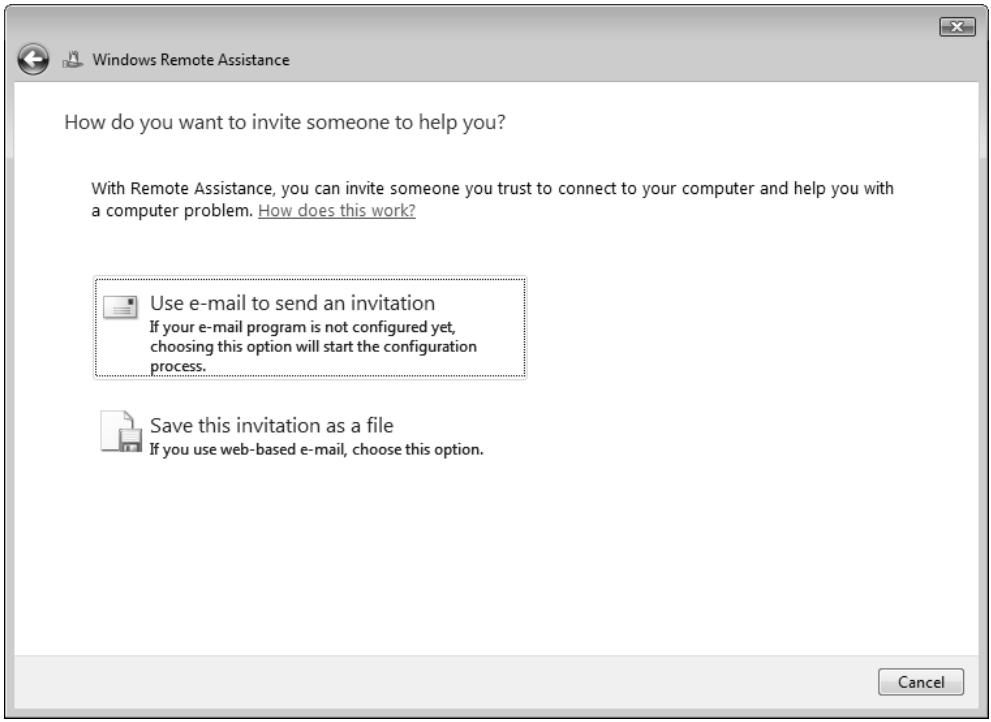


Рис. 4.34. Выбор способа передачи приглашения

3. Если предполагается запрос помощи у удаленного пользователя, то можно отправить ему запрос по электронной почте. Для этого на следующем шаге (рис. 4.34) можно выбрать подготовку стандартного письма-приглашения или же сохранить приглашение в файле, который потом будет каким-то образом переправлен удаленному пользователю. В любом случае

далее нужно будет выбрать пароль, который каким-то "безопасным" образом следует сообщить вашему коллеге (например, по телефону или другим каналам связи).

4. Если выбран вариант обычной электронной почты, мастер запустит почтовую программу и подготовит стандартный бланк запроса (рис. 4.35), в котором нужно указать адрес получателя. После отправки письма на экране появится окно программы Remote Assistance (Удаленный помощник) (рис. 4.36) и компьютер будет ожидать входящего подключения. Удаленный пользователь получит письмо с прикрепленным файлом, который он должен запустить на выполнение, а в появившемся окне подтвердить свое желание ответить на просьбу о помощи. После этого взаимодействие между пользователями (компьютерами) будет происходить в "реальном времени" — начнется подключение к компьютеру — источнику запроса.

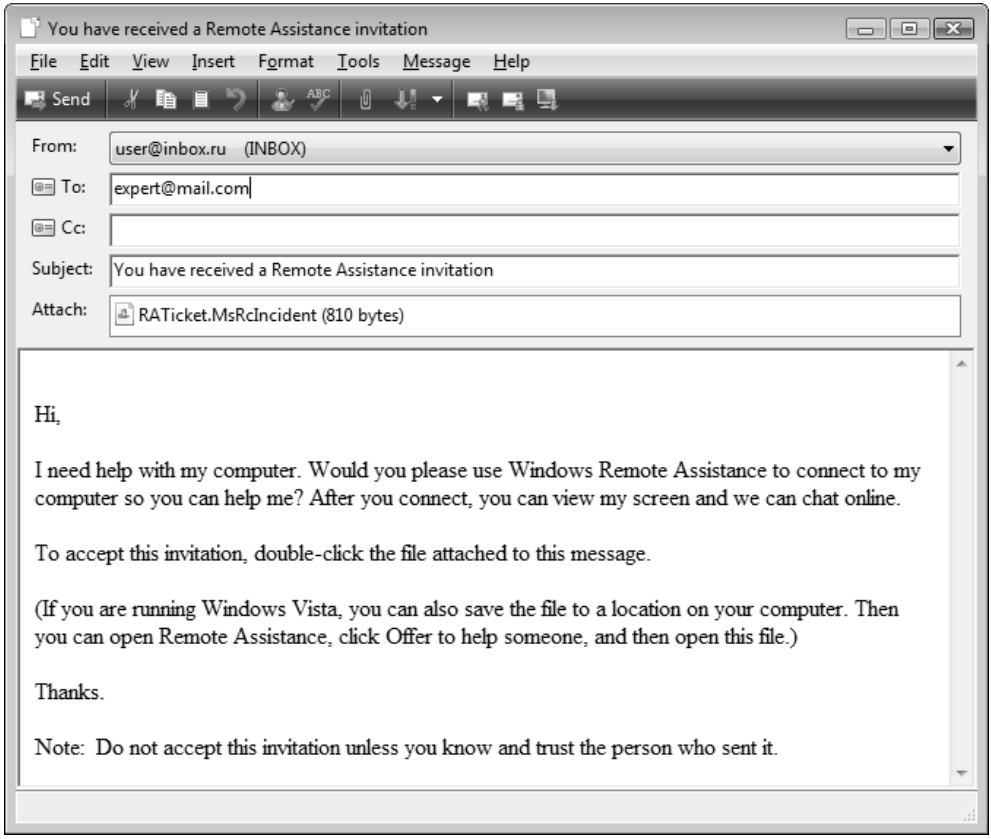


Рис. 4.35. Стандартный бланк письма с просьбой оказания помощи

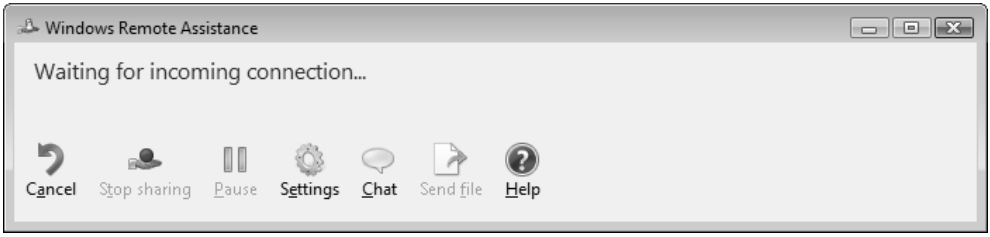


Рис. 4.36. Окно на экране компьютера, пославшего запрос, с ожиданием подключения со стороны удаленного помощника

Инициализация сеанса удаленного доступа

В момент обращения удаленного помощника к локальному компьютеру на экране появится окно запроса (рис. 4.37), где пользователь, отправивший запрос, должен подтвердить подключение к своей системе — после этого вся информация, отображаемая на экране, будет видна удаленному помощнику.

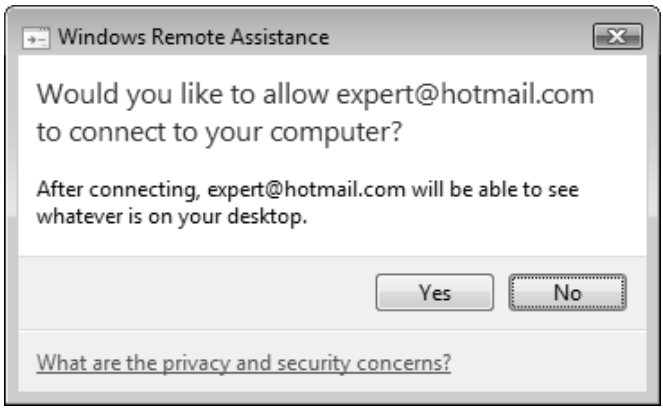


Рис. 4.37. Дополнительное разрешение на подключение к компьютеру в данный момент

После подтверждения возможности удаленного подключения в окне программы Remote Assistance (Удаленный помощник) (рис. 4.38) можно видеть состояние сеанса (строка **Connected to your helper**) и имя подключившегося пользователя (**Being helped by ...**). Из этого окна можно управлять сеансом и запускать диалог и обмен файлами (кнопки **Chat** и **Send file**).

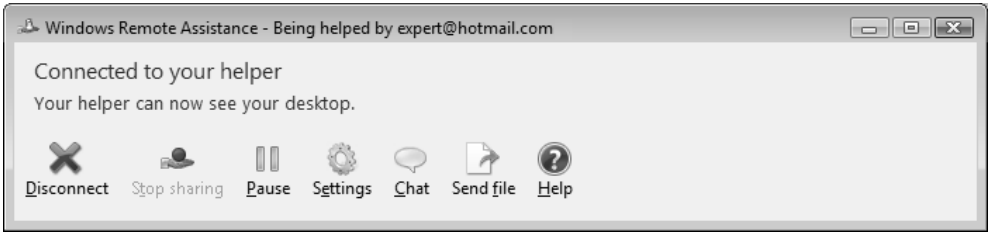


Рис. 4.38. Окно управления
активным сеансом удаленного помощника

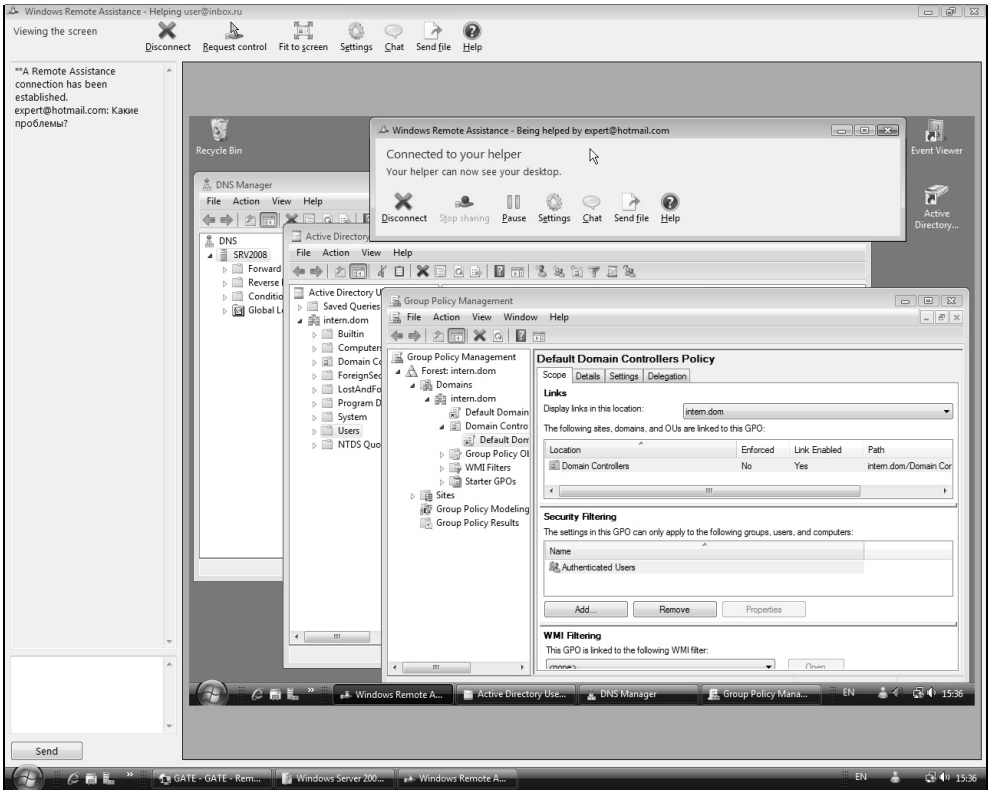


Рис. 4.39. Режим просмотра рабочего стола
на экране удаленного компьютера

На рис. 4.39 в качестве примера показано, как на экране удаленного компьютера будет выглядеть рабочий стол пользователя, запросившего помощь. В заголовке окна программы Remote Assistance (Удаленный помощник) ука-

зано, *кому* помогает удаленный эксперт (**Helping user@inbox.ru**), а в окне управления удаленным помощником на локальной системе видно, *кто* помогает (**Being helped by expert@hotmail.com**). В левой части окна видно окно диалога, в котором пользователи могут обмениваться сообщениями.

Нажав кнопку **Request control** (Запросить управление), удаленный эксперт может попросить у пользователя разрешения управлять его рабочим столом. В случае подтверждения курсор мыши активизируется, и локальной системой смогут одновременно управлять два человека. При этом пользователь, запросивший помощь, может в любой момент запретить совместную работу, нажав кнопку **Stop sharing**.

Самым удобным средством связи для запуска функции Remote Assistance (Удаленный помощник) является программа Windows Live Messenger или ее предшественники. В ее окне можно выбрать собеседника и в онлайновом режиме отправить ему запрос. После некоторого обмена сообщениями (запросов–подтверждений–передачи пароля) появится окно окончательного запроса на подключение (см. рис. 4.37) и начнется сеанс удаленного доступа.

Планирование заданий, выполняющихся по расписанию

Возможности управления запуском задач в системах Windows Vista и Windows Server 2008 значительно расширились, для чего были капитально обновлены два основных средства: автономная оснастка **Task Scheduler** (Планировщик заданий) и утилита командной строки *Schtasks.exe*. С их помощью можно составлять расписание для запуска командных файлов, прикладных программ или различных утилит для обслуживания системы. Возможны сложные расписания для запуска и останова задач, привязанные как ко времени, так и к системным событиям; одновременно могут запускаться несколько программ, и возможны различные действия по их завершению.

Существуют самые различные регламенты для запуска программ: однократно, ежедневно, еженедельно или ежемесячно в заданные дни, при загрузке системы или регистрации в ней, а также при бездействии системы (idle state). Планировщик позволяет задавать достаточно сложное расписание для выполнения заданий, в котором задаются продолжительность задания, время его окончания, количество повторов и т. п.

Совет

Утилита Schtasks, запущенная в окне командной строки без параметров, позволяет видеть список заданий, выполняющихся в системе в данный момент (в системах Windows Server 2008 даже по умолчанию этот список достаточно внушительный).

Оснастка **Task Scheduler** (Планировщик заданий; taskschd.msc) запускается из меню **Administrative Tools** (Администрирование) или — по имени — из меню **Start** (Пуск) или окна **Run** (Выполнить). Служба *Task Scheduler* (Планировщик заданий; имя Schedule) инсталлируется вместе с системой и автоматически запускается при ее загрузке.

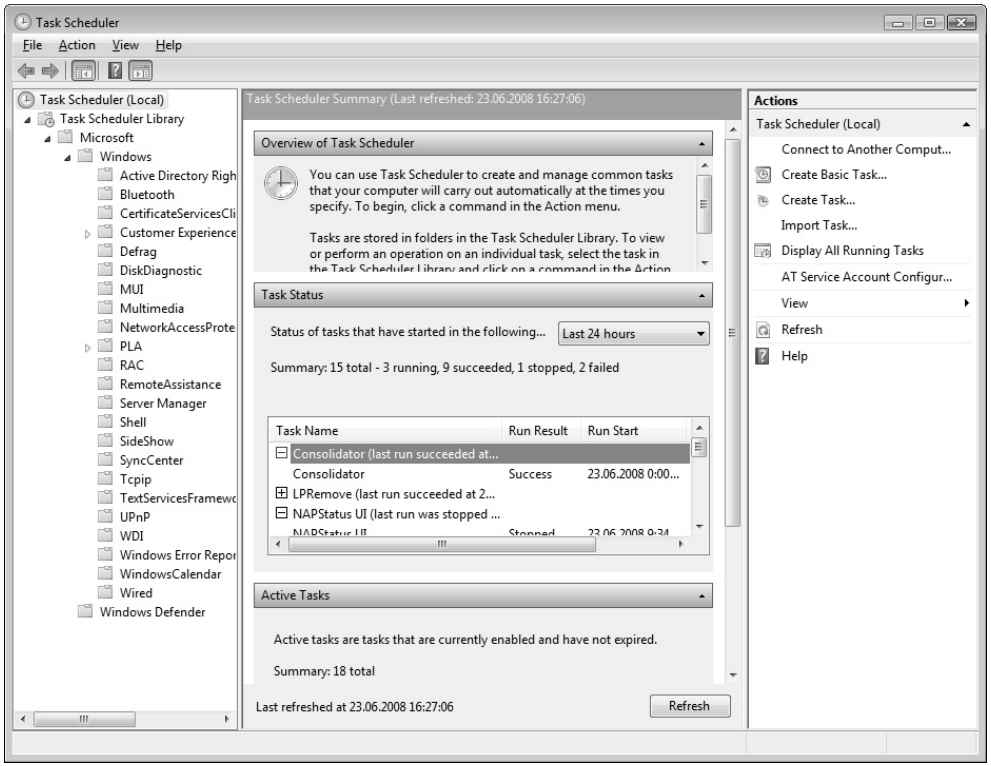


Рис. 4.40. Окно планировщика позволяет просматривать выполненные и запланированные задания

В окне планировщика заданий (рис. 4.40) легко просматривать списки запланированных заданий (что упрощает подготовку и отладку заданий), а также

общую статистику по всем заданиям. После запуска оснастки по умолчанию отображаются основные панели: на панели **Task Status** (Состояние задачи) можно быстро определить, какие задания выполняются, сколько задач завершилось успешно, а сколько потерпели неудачу (изначально показаны данные за последние 24 часа). Здесь выводится основная информация о заданиях: время запуска и окончания, состояние, результат выполнения задания. На панели **Active Tasks** (Активные задачи) указано общее количество включенных задач и дан полный их перечень с указанием времени следующего запуска, расписания и местоположения в библиотеке задач планировщика. Если в списке дважды щелкнуть по названию задачи, то откроется соответствующая папка библиотеки планировщика и можно увидеть параметры выбранного задания (см. рис. 4.41).

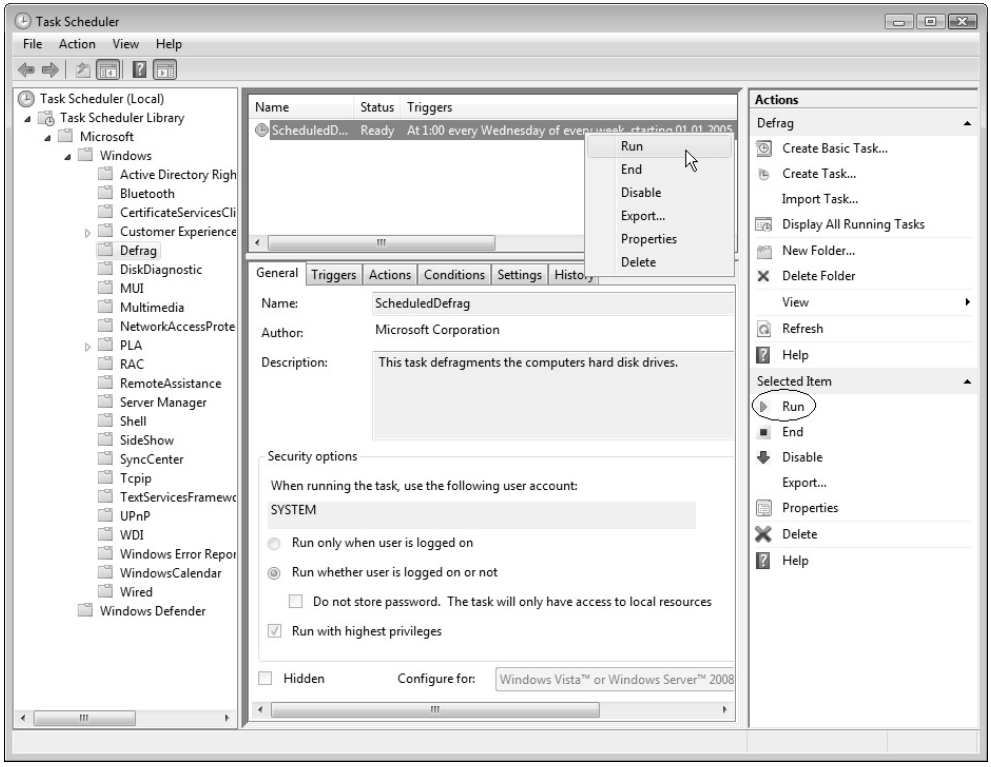


Рис. 4.41. Просмотр свойств задания и команды управления

При просмотре отдельных заданий в окне планировщика можно, не открывая дополнительных окон, сразу видеть основные параметры задания (рис. 4.41): все

параметры, включая параметры запуска и расписание, отображаются на вкладках на панели в центре главного окна оснастки. (Для изменения параметров нужно выбрать ссылку **Properties** (Свойства) права на панели **Actions** (Действия).) На вкладке **History** (Журнал) можно видеть результаты выполнения выбранной задачи. Задачу можно запустить для проверки в любой момент непосредственно из папки заданий (команда **Run** (Выполнить) в контекстном меню выбранного задания или на панели действий).

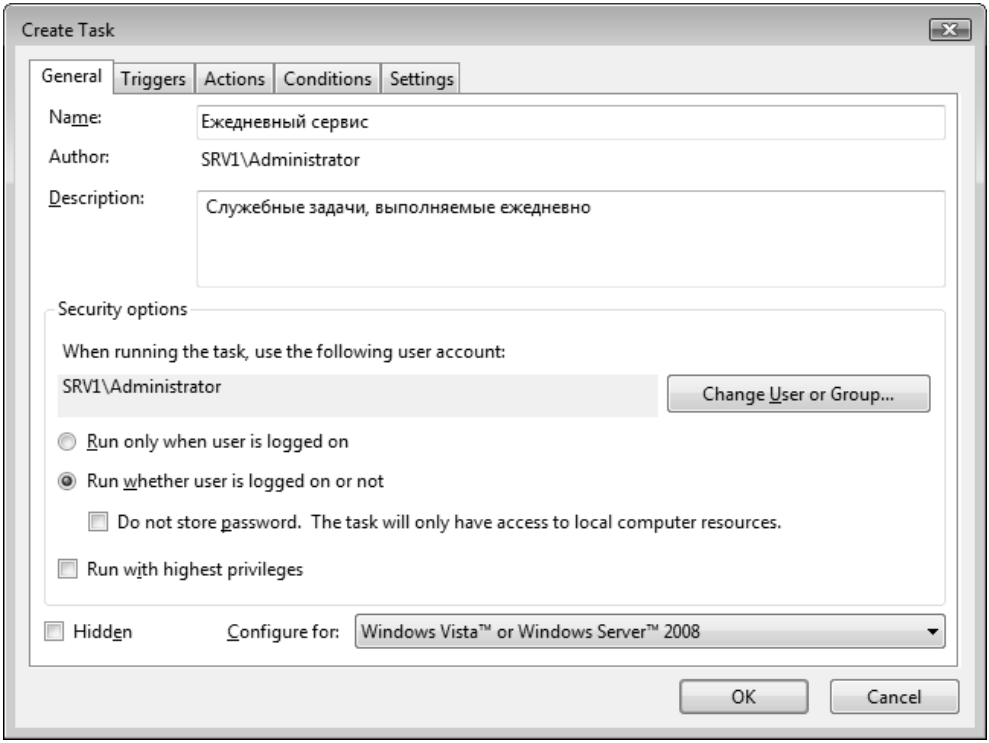


Рис. 4.42. Общие параметры новой планируемой задачи

Мастер планирования заданий (Create Basic Task Wizard), запускаемый при выборе команды **Create Basic Task** (Создать простую задачу) на панели действий, позволяет в интерактивном режиме легко и быстро указать основные параметры для запуска запланированного задания. Задания могут иметь несколько расписаний, принципиально отличающихся друг от друга. Например, некоторая программа может запускаться ежедневно в одно время, еженедельно — в другое время и однократно — в заданное время указанного дня.

Задания можно создать и вручную, нажав кнопку **Create Task** (Создать задачу) на панели **Actions** (Действия) и определив все параметры задачи на вкладках в окне свойств задания.

При создании задания необходимо сначала в библиотеке планировщика выбрать или создать папку, где будет храниться описание задания, после чего в окне ее свойств (рис. 4.42) ввести необходимую информацию: сначала, помимо имени задания, требуется указать имя и пароль пользователя, определяющие контекст безопасности, в котором выполняется задание (при этом пользователь необязательно должен быть зарегистрирован в системе). Выбрать другого пользователя можно, нажав кнопку **Change User or Group** (Изменить). Это позволяет запускать на одном компьютере несколько заданий с различными правами в отношении контекста безопасности, т. е. несколько пользователей могут одновременно иметь индивидуальные, независимые расписания запланированных заданий.

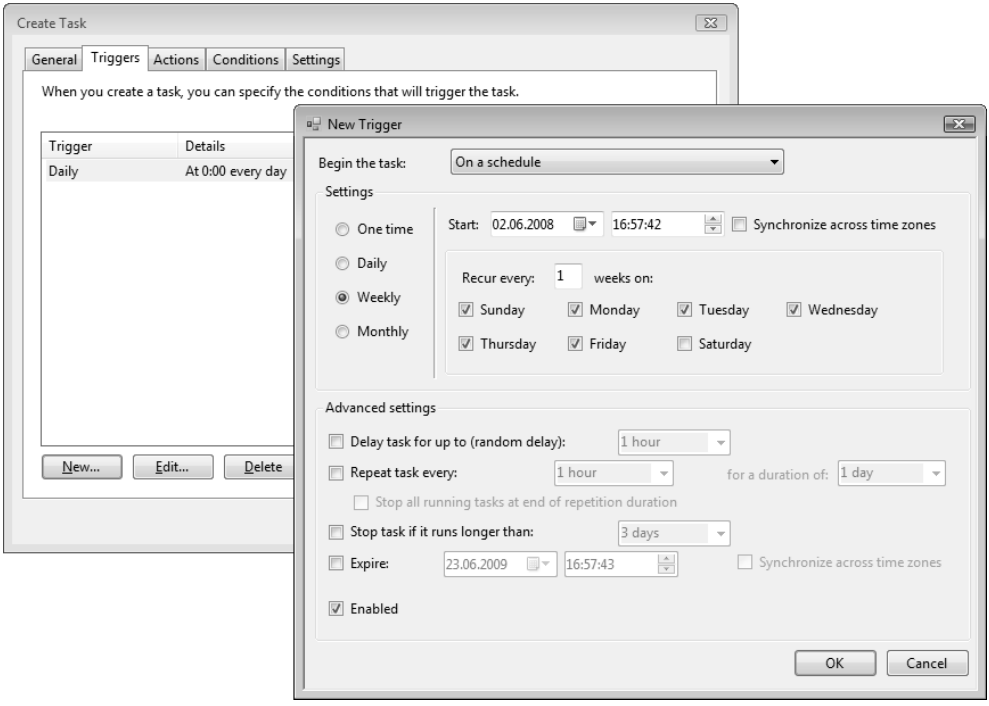


Рис. 4.43. Выбор расписания для запуска задачи

При ручном планировании заданий необходимо последовательно ввести необходимые параметры на вкладках окна **Create Task** (Создание задачи) (см. рис. 4.42), после чего можно закрыть это окно, нажав кнопку **ОК**. Если все параметры заданы правильно, новая задача появится в библиотеке планировщика заданий.

Обязательной является информация, указываемая на вкладках **Trigger** (Триггеры) и **Actions** (Действия). На первой из названных вкладок (рис. 4.43) задаются основные и дополнительные параметры расписания запуска задачи (расписаний может быть несколько одновременно). На второй вкладке перечислены действия, выполняемые в указанное время: запуск программы, отправка сообщения электронной почты или отображение сообщения.

Описания заданий можно экспортировать в виде XML-файлов — например, для сохранения или последующего импорта на других компьютерах. Соответствующие команды выполнения этих операций имеются на панели **Actions** (Действия).

Служба времени Windows (W32Time)

Служба времени Windows (Windows Time Service; имя сервиса W32Time) обеспечивает синхронизацию системных часов. В общем случае точное время можно получать от надежного источника (сервера времени), в доменах синхронизируется время на компьютерах клиентов и контроллерах домена. В доменах Active Directory точность времени особенно важна потому, что клиенты, работающие под управлением систем Windows 2000 и выше, и контроллеры домена при аутентификации используют протокол Kerberos V5, для нормальной работы которого необходимо, чтобы показания часов на компьютерах отличались не более чем на 5 минут.

В составе стека протоколов TCP/IP имеется *протокол NTP* (Network Time Protocol, RFC 1119), который служит для синхронизации системных часов компьютеров, связанных сетью TCP/IP. *Клиент* протокола NTP синхронизирует показания своих часов с показаниями часов *сервера* NTP.

Примечание

Работа службы времени определяется параметрами реестра, расположенными в разделе `HKLM\SYSTEM\CurrentControlSet\Services\W32Time`. (Все параметры, рассматриваемые далее, относятся к данному разделу реестра.)

По умолчанию служба времени Windows синхронизируется от *внешнего* сервера времени (поскольку параметр `TimeProviders\NtpClient\Enabled` равен 1), при этом параметр `Parameters\Type` имеет значение `NTP`, а параметр `Parameters\NtpServer` определяет сервер NTP, с которым происходит синхронизация. Параметр `TimeProviders\NtpServer\Enabled` изначально равен 0, и компьютер не может выполнять функции сервера времени.

В случае подключения компьютера, работающего под управлением Windows Server 2003, к домену параметр `Parameters\Type` изменяет свое значение на `NT5DS`, и синхронизация времени осуществляется только от контроллеров домена. Для систем Windows Server 2008 устанавливается значение `AllSync`, и компьютер может получать точное время как от контроллеров домена, так и от внешних серверов времени. То же самое происходит и при повышении роли рядового сервера до контроллера домена (при этом параметр `TimeProviders\NtpServer\Enabled` становится равным 1, поскольку каждый контроллер домена может выполнять функции сервера времени).

> ***Внимание!***
>
> После каждого изменения вручную параметров службы времени Windows ее следует перезапустить с помощью оснастки **Service** или в окне консоли (используя команду `net stop w32time && net start w32time`). Если использовалась утилита w32tm.exe, то параметры начинают действовать только после выполнения команды `w32tm /config /update`.

Клиенты, работающие под управлением систем Windows 2000/XP/Windows Server 2003, автоматически синхронизируют время с контроллером домена Active Directory в процессе загрузки системы. Контроллеры домена сверяют время с контроллером, выполняющим функции эмулятора PDC (PDC Emulator), или с любым контроллером *родительского* домена. Эмулятор PDC синхронизирует время с эмулятором PDC родительского домена (или корневого домена леса) или с любым сервером этого домена. Эмулятор PDC корневого домена леса должен получать время от внешнего NTP-сервера, либо возможна ситуация, когда синхронизация часов контроллера корневого домена леса не выполняется. В этом случае показания системных часов эмулятора PDC этого домена считаются эталонными.

> ***Внимание!***
>
> Служба времени немного по-разному реализована в системах Windows 2000 и Windows XP/Windows Server 2003. Поэтому отличается и синтаксис команд утилиты w32tm, используемых для выполнения одних и тех же действий.

Настройка синхронизации с источником времени

В общем случае имя или IP-адрес внешнего сервера времени можно задать с помощью команды `net time /SETSNTP:`*<имяСервераВремени>*, а команда `net time /QUERYSNTP` показывает, какой внешний сервер (серверы) времени используется в данный момент.

> ***Примечание***
>
> В качестве внешних можно использовать различные NTP-серверы времени, имеющиеся в Интернете, их примерный список имеется в статье KB262680 базы знаний Microsoft.

На компьютерах, работающих под управлением Windows XP/Windows Server 2003 и Windows Server 2008, ту же задачу можно решить с помощью следующих двух команд:

```
C:\>w32tm /config /syncfromflags:MANUAL
↳ /manualpeerlist:<имяСервераВремени>
The command completed successfully.
C:\>w32tm /config /update
The command completed successfully.
```

По умолчанию все компьютеры, работающие под управлением Windows XP и Windows Server 2003, в качестве сервера времени используют веб-узел **time.windows.com**.

Для того чтобы часы компьютера синхронизировались только в соответствии с иерархической структурой доменов (параметр `Parameters\Type` изменит значение на `NT5DS`), можно выполнить команду `w32tm /config /syncfromflags:DOMHIER /update`. Команда `w32tm /config /syncfromflags:ALL /update` позволяет разрешить получение точного времени от контроллеров домена и внешних серверов времени (при этом параметр `Parameters\Type` изменит значение на `AllSync`).

Отключение синхронизации

Для того чтобы синхронизация системных часов не осуществлялась, выполните команду `w32tm /config /syncfromflags:NO /update` (при этом параметр `Parameters\Type` изменит значение на `NoSync`). Можно вообще запре-

тить сервис NTP-клиента, установив значение параметра реестра `TimeProviders\NtpClient\Enabled` равным 0.

Чтобы компьютер перестал работать в качестве сервера времени, нужно параметру `TimeProviders\NtpServer\Enabled` задать значение 0.

После подобных изменений службу времени следует перезапустить.

Принудительная синхронизация часов

На компьютерах, работающих под управлением Windows XP/Windows Server 2003/Windows Server 2008, для выполнения синхронизации часов с заданным источником времени (внешним сервером или контроллером домена) используется команда:

```
C:\>w32tm /resync
Sending resync command to local computer...
The command completed successfully.
```

Проверка работы службы времени в домене

С помощью приведенной ниже команды можно увидеть, какие серверы времени (в листинге они показаны в строках `RefID: ...`) используются в указанном домене (если домен не задается, то проверяется текущий домен) или на компьютерах домена, перечисленных явно; также отображаются отклонения показаний часов:

```
C:\>w32tm /monitor
DC1.intern.dom *** PDC ***[192.168.0.202:123]:
    ICMP: 0ms delay
    NTP: +0.0000000s offset from DC1.intern.dom
        RefID: time-a.nist.gov [129.6.15.28]
        Stratum: 2
DC2.intern.dom [192.168.0.222:123]:
    ICMP: 0ms delay
    NTP: +0.0205003s offset from DC1.intern.dom
        RefID: DC1.intern.dom [192.168.0.202]
        Stratum: 2
```

В этом примере можно видеть, что контроллер DC1 синхронизирует время с внешним сервером **time-a.nist.gov**, а контроллер DC2 — с первым контроллером (эмулятором PDC).

Административные утилиты командной строки

Можно сказать, что количество утилит командной строки в составе систем Windows растет от версии к версии. Многие утилиты выполняют те же действия, что и различные административные оснастки, только позволяют работать в окне консоли или могут вызываться из командных файлов, автоматизирующих типовые операции. (Для Windows Server 2008 это особенно важно при использовании Windows Server 2008 Server Core.) Другие утилиты могут оказаться незаменимым вспомогательным инструментом, полезными для диагностики или выполнения специфических задач по управлению компьютерами, пользователями и сетями.

Справочная система Windows Server 2008 не содержит локальной информации по утилитам командной строки и отсылает к веб-сайтам Microsoft. Для того чтобы найти нужную веб-страницу и открыть ее в браузере, нужно в главном окне справки выбрать ссылку **Command Reference** (Справочник по командам).

Информацию о параметрах любой утилиты легко получить, запустив ее в окне командной строки с ключом `/?`.

Далее перечисляются стандартные утилиты командной строки, имеющиеся в составе Windows Server 2008, и указывается их основное назначение; эти средства могут быть особо полезны в работе администратору системы (использование некоторых утилит также рассматривается в других главах книги):

- AuditPol.exe — управление политиками аудита;
- BcdEdit.exe — редактор опций диспетчера загрузки Windows (Windows Boot Manager);
- Convert.exe — преобразование файловой системы тома из FAT в NTFS;
- Defrag.exe — дефрагментация дисковых томов;
- DiskPart.exe — управление дисками и томами;
- EventCreate.exe — позволяет администратору создавать собственные события в системных журналах;

- Fsutil.exe — управление дисковыми системами (например, позволяет управлять квотами);
- Gpupdate.exe — принудительное обновление параметров групповых политик, распространяющихся на компьютер и пользователей;
- Icacls.exe — просмотр и изменение списков управления доступом (Access Control List, ACL) для файлов и папок (модифицированная утилита Cacls.exe);
- Mklink.exe — создание жестких (hardlink) и символьных (symbolic link) связей, а также точек соединений (junction);
- Netsh.exe — управление сетевыми параметрами и подключениями;
- OpenFiles.exe — отображает открытые файлы;
- Query.exe — просмотр списков процессов, сеансов, серверов терминалов и пользователей при удаленном доступе;
- Quser.exe — просмотр списка пользователей, зарегистрированных на компьютере, при удаленном доступе;
- RegEdit.exe (RegEdt32.exe) — традиционный редактор системного реестра, имеющийся во всех системах линейки Windows NT;
- RoboCopy.exe (Robust File Copy for Windows) — мощная утилита копирования файлов;
- RunAs.exe — запуск программ с полномочиями другого пользователя;
- Sc.exe — управление системными сервисами;
- Schtasks.exe — планировщик задач, значительно более мощный, чем традиционная команда `AT`;
- ServerManagerCmd.exe (Server Manager) — просмотр, установка и удаление ролей и компонентов сервера;
- Setx.exe — просмотр, создание и изменение системных и пользовательских переменных среды (environmental variables);
- Shutdown.exe — выключение и перезагрузка локального или удаленного компьютера;
- SystemInfo.exe — полезная сводная информация, получаемая от многих компонентов системы;
- TaskKill.exe — завершение процессов (служб или прикладных программ);

- TaskList.exe — отображение списка выполняющихся на компьютере приложений, служб и процессов;
- TypePerf.exe — запись значений счетчиков производительности в окно консоли или в журнал;
- Wbadmin.exe — управление архивацией и восстановлением операционной системы, файлов, папок и томов;
- Wevtutil.exe — работа с системными журналами событий (аналог оснастки **Event Viewer** (Просмотр событий));
- Where.exe — поиск местоположения (в иерархии папок) системных утилит и программ (например, с ее помощью можно понять, относится ли конкретная программа к стандартным системным или входит в пакет Support Tools);
- Whoami.exe — получение информации об имени зарегистрированного пользователя, его принадлежности к группам, идентификаторе безопасности (SID), полномочиях (privileges) в системе и т. д.;
- Winrm.exe — управление службой Windows Remote Management (Служба удаленного управления);
- Winrs.exe — удаленная командная строка (Windows Remote Shell).

Пакет Windows Support Tools

Дополнительные административные утилиты для систем Windows XP/ Windows Server 2003 поставляются в составе пакета, который называется *Windows Support Tools* и должен устанавливаться отдельно от самой системы (этот пакет имеется на дистрибутивном диске самой системы). Теперь большинство этих утилит уже включено в Windows Server 2008; они становятся доступными в системе после установки соответствующих ролей сервера. Тем не менее, некоторые полезные утилиты (например, NetDiag.exe, Search.vbs, MoveTree.exe, ReplMon.exe, GPOTool.exe и др.) по-прежнему можно найти только в составе пакета Windows Support Tools (его можно скачать с вебсайта Центра загрузки Microsoft — см. ссылки в *Приложении*). Отдельно нужно скачивать и утилиту Active Directory Migration Tool version 3 (ADMT v3), помогающую в миграции и реорганизации доменов Active Directory. Практически все эти утилиты работают в среде Windows Server 2008.

В табл. 4.1 перечислены некоторые дополнительные утилиты Windows Server 2008, входившие ранее в состав пакета Windows Support Tools, и указаны об-

ласти их применения. Как можно видеть, большинство этих утилит используется при работе в доменах Active Directory и на контроллерах доменов.

Таблица 4.1. *Назначение дополнительных утилит для поддержки ролей сервера*

Административная задача	**Используемые инструменты**
Просмотр и редактирование объектов Active Directory	Ldp.exe, DsMod.exe, DsMove.exe, DsRm.exe
Запросы к каталогу Active Directory	DsQuery.exe, DsGet.exe, Ldp.exe
Миграция и реструктуризация; работа с объектами Active Directory	NetDom.exe, DsAdd.exe
Экспорт/импорт, пакетные операции	CSVDE.exe, LDIFDE.exe
Диагностика и обслуживание базы данных Active Directory	NTDSutil.exe
Диагностика сети	NSlookup.exe, DCdiag.exe, NLtest.exe, DNSCmd.exe, RPCPing
Репликация каталога Active Directory	RepAdmin.exe, NTFRSutl.exe
Безопасность Active Directory	DsACLs.exe, KList.exe

Глава 5

Средства мониторинга системы и приложений

В этой главе рассматриваются программы и утилиты, необходимые администратору в процессе эксплуатации отдельных систем или сетевых компьютеров. В составе систем Windows Vista/Windows Server 2008 появились новые средства мониторинга системы, ее аппаратных и программных компонентов, а также запущенных приложений. Возможности оснасток, унаследованных от предыдущих версий Windows, значительно модернизированы и расширены. С их помощью можно оценить загрузку процессора, памяти и других компонентов компьютера, обнаружить "узкие места" в работе системы, снижающие ее производительность, контролировать выполнение программ, обнаруживать сбои в работе аппаратных и программных средств.

Кроме средств мониторинга, рассматриваемых ниже, имеются разнообразные встроенные средства диагностики, позволяющие сообщать в компанию Microsoft о возникающих проблемах (например, связанных с драйверами устройств или работой приложений) и получать от нее рекомендации или решения *(см. разд. "Диагностика и устранение неполадок" в главе 3)*.

Все имеющиеся средства мониторинга упрощают работу с системой и позволяют администратору быстро обнаруживать, диагностировать и устранять неисправности, причем многие данные можно собирать дистанционно с удаленных компьютеров. Это позволяет централизованно следить за работой систем в сетевой среде.

Средства мониторинга в Windows Server 2008

В системах Windows Vista/Windows Server 2008 имеется множество средств, предназначенных для просмотра событий, происходящих в системе, а также для оптимизации и мониторинга рабочих параметров системных служб и прикладных программ. Некоторые средства традиционны для систем Windows, но кардинально переработаны по сравнению с предыдущими версиями, а некоторые инструменты — совершенно новые. Перечислим существующие программы и укажем область применения.

- Утилита *Task Manager* (Диспетчер задач) используется для просмотра рабочих параметров системы и прикладных программ (сюда входят загрузка процессора, степень использования оперативной и виртуальной памяти, коэффициент занятости сети и т. д.).
- Оснастка **Event Viewer** (Просмотр событий) позволяет анализировать события, регистрируемые приложениями, службами и самой системой.

  Журналы событий для ролей сервера и связанных с ними служб также можно просматривать с помощью оснастки **Server Manager** (Диспетчер сервера), имеющейся только в Windows Server 2008.
- Оснастка **Reliability and Performance Monitor** (Монитор производительности и стабильности) позволяет в режиме реального времени собирать и просматривать данные об использовании памяти, жесткого диска, процессора и сетевых ресурсов компьютера. В ее состав входят три компонента:
  - компонент *Performance Monitor*[1] (Системный монитор) позволяет визуально отслеживать изменения производительности системы. С его помощью можно одновременно просматривать данные с разных компьютеров в виде графиков или диаграмм, на которых отображаются показания счетчиков производительности;
  - оснастка **Reliability Monitor** (Монитор стабильности системы) позволяет оценивать надежность работы системы на протяжении некоторого интервала времени и определять "слабые места" системы;
  - компонент *Data Collector Sets* (Группы сборщиков данных) позволяет создавать наборы логически связанных счетчиков производительно-

[1] В системах Windows XP/Windows Server 2003 этот компонент называется *System Monitor*.

сти, которые затем можно использовать для ведения журналов (с последующим отображением в окне компонента Performance Monitor) или для сбора данных с других компьютеров. В них можно определять действия, которые будут выполняться при превышении счетчиками заданного максимального или минимального значения (в этом случае администратору может отправляться сообщение или может запускаться определенная им задача).

Нужно также упомянуть еще два инструмента, с помощью которых можно получить информацию о конфигурации аппаратных и программных средств, установленных драйверах и обновлениях, программных компонентах и т. п.:

- утилита командной строки *SystemInfo.exe* выводит на экран базовую информацию об операционной системе, установленной на локальном или удаленном компьютере (в том числе дату установки, основные параметры оборудования, список установленных обновлений);
- программа *System Information* (Сведения о системе) *(см. главу 3)* позволяет получить исчерпывающую информацию о каждом аппаратном и программном компоненте системы, включая описание, параметры и т. п.

Далее все перечисленные средства будут рассматриваться подробно, при этом будут упоминаться дополнительные утилиты, позволяющие решать аналогичные задачи.

Диспетчер задач (Task Manager)

Диспетчер задач (Task Manager) традиционно используется в системах Windows для мониторинга "оперативного состояния" системы (оценивать ситуацию в течение длительного времени с его помощью неудобно, для этих целей служат другие средства — *см. далее разд. "Мониторинг параметров и стабильности работы системы"*). С помощью диспетчера задач можно быстро отслеживать статус запущенных программ и завершать "зависшие" приложения, которые перестали отвечать на запросы системы. Также он позволяет отслеживать активность запущенных процессов по многим параметрам и просматривать диаграммы использования процессора и памяти; кроме того, с помощью этого монитора можно находить несанкционированно запущенные приложения, например, вредоносные программы (хотя эту задачу лучше возложить на Windows Defender (Защитник Windows)).

В системах Windows Server 2008 диспетчер задач в целом не изменился по сравнению с предыдущими версиями Windows, однако он имеет несколько

новых функций. Теперь окно диспетчера содержит шесть вкладок/индикаторов:

- **Applications** (Приложения) — показывает статус приложений, запущенных на компьютере. На этой вкладке можно завершить (снять) любую задачу, например, неотвечающую программу. В контекстном меню каждой задачи имеется команда **Go To Process** (Перейти к процессу), позволяющая переключиться на вкладку **Processes** (Процессы) и увидеть, какой процесс соответствует выбранной задаче;
- **Processes** (Процессы) — содержит информацию о процессах, запущенных на компьютере;
- **Services** (Службы) — это новая вкладка, ранее не встречавшаяся: на ней отображаются список и состояние служб с указанием идентификатора (ID) процесса, что упрощает отслеживание событий, связанных с конкретной службой;
- **Performance** (Быстродействие) — отображает динамическое состояние производительности компьютера, включая степень использования памяти и процессора;
- **Networking** (Сеть) — показывает степень загрузки сети. Индикатор отображается только при наличии на компьютере сетевой карты;
- **Users** (Пользователи) — содержит список зарегистрированных в системе пользователей. Эта вкладка имеется во всех системах, поскольку в Windows Server 2008 возможность быстрого переключения пользователей (Fast User Switching) существует на всех компьютерах, включая контроллеры и члены доменов.

Запуск диспетчера задач

Существует множество способов запуска диспетчера — все они перечислены ниже.

- Щелкнуть правой кнопкой мыши по панели задач и выбрать в контекстном меню пункт **Task Manager** (Диспетчер задач).
- Нажать комбинацию клавиш <Ctrl>+<Shift>+<Esc>.
- Нажать комбинацию клавиш <Ctrl>+<Alt>+<Del> и нажать в открывшемся окне кнопку **Start Task Manager** (Запустить диспетчер задач).
- Открыть окно **Run** (Выполнить) и ввести команду `taskmgr`; эту команду можно непосредственно ввести в поле поиска меню **Start** (Пуск).

Если диспетчер задач запущен, то в правом нижнем углу экрана на панели задач в области уведомлений (system tray) появляется индикатор загрузки процессора. Если подвести указатель мыши к этому индикатору, то будет отображена степень загруженности процессора.

Открыть окно диспетчера задач можно, дважды щелкнув по значку индикатора производительности на панели задач. Если нежелательно, чтобы свернутое окно диспетчера оставалось на панели задач, и нужно, чтобы был виден только его значок, то в окне диспетчера в меню **Options** (Параметры) выберите пункт **Hide When Minimized** (Скрывать свернутое).

По умолчание окно диспетчера задач отображается поверх всех окон; такое поведение тоже можно изменить, сбросив флажок **Always On Top** (Поверх остальных окон) в меню **Options** (Параметры).

Скорость обновления

Скорость обновления показаний диспетчера задач можно регулировать. При редком обновлении снижается нагрузка на систему, хотя при этом показания диспетчера задач могут оказаться слишком приближенными; при частом обновлении можно более точно отслеживать динамику процессов. Для выполнения принудительного обновления выполните команду **Refresh Now** (Обновить) в меню **View** (Вид) или нажмите клавишу <F5>.

В диспетчере задач можно задать следующие опции скорости обновления:

- **High** (Высокая) — обновление проводится каждые полсекунды;
- **Normal** (Обычная) — обновление выполняется каждую секунду;
- **Low** (Низкая) — показания обновляются каждые 4 секунды;
- **Paused** (Приостановить) — автоматическое обновление не производится. Для запуска обновления нажмите клавишу <F5>.

Состояние прикладных программ

На вкладке **Applications** (Приложения) (рис. 5.1) можно видеть список запущенных программ и их состояние. В том случае, если программа зависла или долго не отвечает, ее можно удалить из памяти с помощью команды **End Task** (Снять задачу). Команда **Switch To** (Переключиться) позволяет быстро перейти в окно выбранной программы.

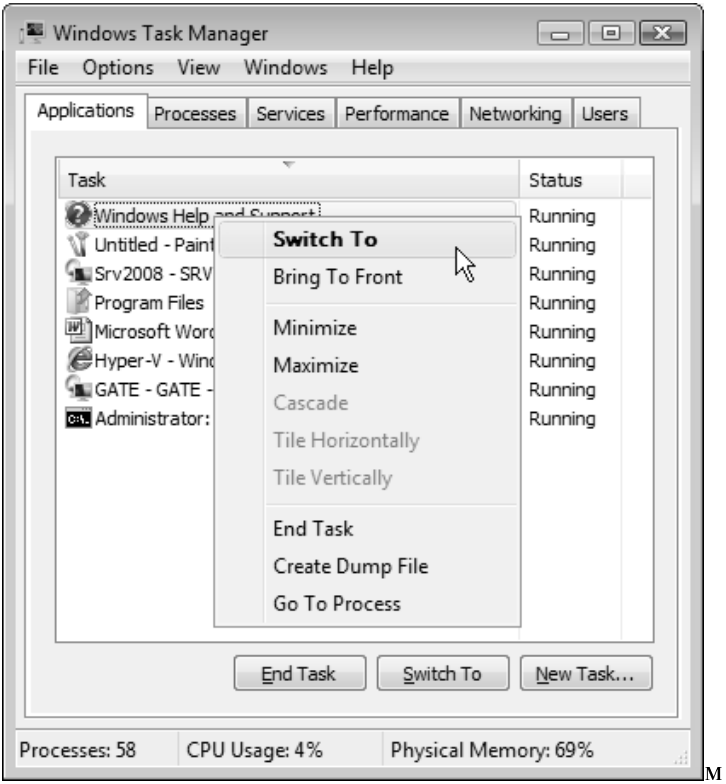


Рис. 5.1. Состояние прикладных программ, запущенных в системе

С помощью команды **Go To Process** (Перейти к процессу) можно перейти на вкладку **Processes** (Процессы), где автоматически будет выделен процесс, соответствующий выбранной изначально прикладной программе. Это особенно удобно в тех случаях, когда неизвестно имя исполняемого файла для конкретной программы.

Мониторинг процессов

Для просмотра запущенных процессов и показателей их производительности используется вкладка **Processes** (Процессы) (рис. 5.2). Таблица процессов содержит все процессы, запущенные в собственном адресном пространстве, включая все прикладные программы и системные сервисы. Обратите внимание на то, что по умолчанию для каждого процесса отображается его описание (столбец **Description**). Это значительно упрощает анализ ситуации, по-

скольку не так просто запомнить имена образов десятков процессов и названия соответствующих программ. Также на рисунке показан отсутствующий по умолчанию столбец **Command Line** (Командная строка), тесно связанный с командой **Open File Location** (Открыть место хранения файла) *(см. далее)*, — в этом столбце можно видеть параметры, использованные для запуска конкретного процесса, и полный путь к исполняемому файлу.

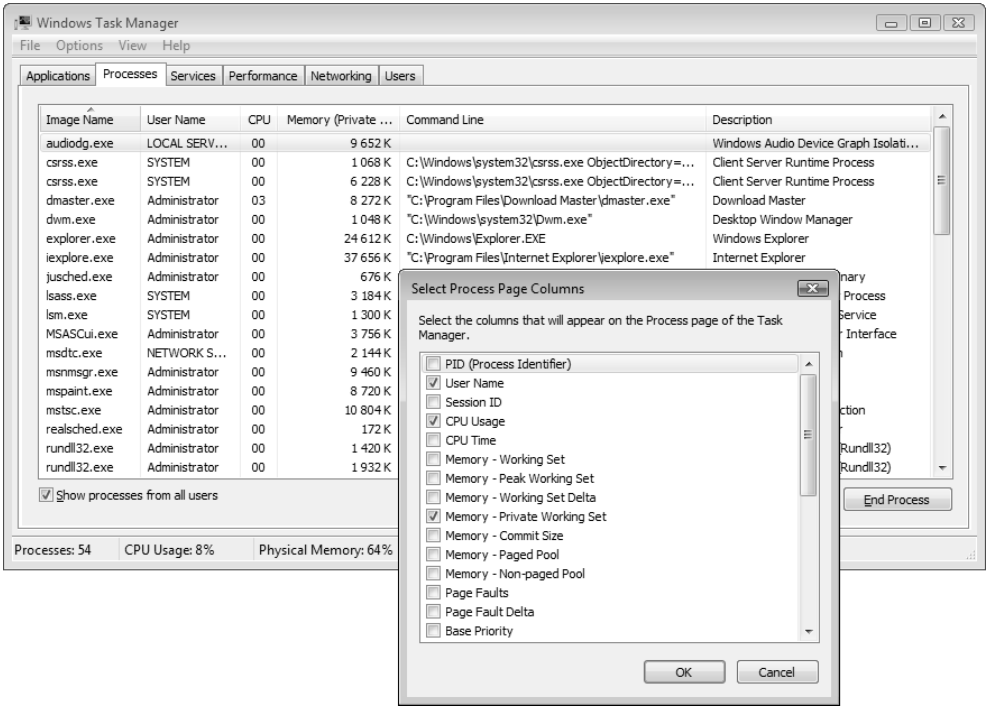


Рис. 5.2. Список процессов, запущенных в системе, и окно выбора отображаемых параметров

В контекстном меню любого процесса (рис. 5.3) присутствуют две важные команды:

- **Open File Location** (Открыть место хранения файла) — открывает новое окно Проводника, где отображается папка, содержащая исполняемый файл, связанный с данным процессом. Такая функция очень полезна в тех случаях, когда имя и "происхождение" процесса вызывают подозрение (например, если на компьютер попал вирус или "троянский конь") и нужно получить дополнительную информацию о прикладной программе.

Здесь также может помочь команда **Properties** (Свойства), с помощью которой открывается окно свойств исполняемого файла — в нем на вкладке **Details** (Подробно) обычно имеются сведения о разработчике приложения, описание программы и т. п.;

- **Go to Service(s)** (Перейти к службам) — выполняет переход на вкладку **Services** (Службы) к службе, соответствующей данному процессу (если таковая имеется).

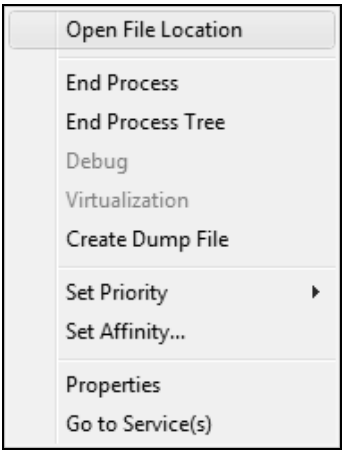


Рис. 5.3. Меню команд, имеющихся для выбранного процесса

При работе в окне командной строки можно использовать утилиты `qprocess` и `tasklist`. Информацию о параметрах можно получить во встроенной справке утилит, запустив их с ключом `/?`. *

Например, с помощью показанной ниже команды можно увидеть, с какой службой (какими службами) связан процесс или его конкретный экземпляр (например, это бывает необходимо в тех случаях, когда один двоичный образ используется для запуска различных сервисов и нужно найти определенный экземпляр процесса):

```
C:\>tasklist /SVC

Image Name                     PID Services
========================= ======== ============================
... ... ...
svchost.exe                    796 DcomLaunch, PlugPlay
```

```
svchost.exe                   856 RpcSs
svchost.exe                   896 WinDefend
svchost.exe                   988 Audiosrv, Dhcp, EventLog, lmhosts
svchost.exe                  1012 gpsvc
svchost.exe                  1028 AeLookupSvc, BITS, IKEEXT, iphlpsvc,
                                  LanmanServer, MMCSS, ProfSvc, RasMan,
                                  Schedule, seclogon, SENS, ShellHWDe-
tection,
                                  Themes, Winmgmt, wuauserv
svchost.exe                  1120 EventSystem, fdPHost, FDResPub,
                                  LanmanWorkstation, netprofm, nsi,
                                  SLUINotify, SstpSvc, W32Time
svchost.exe                  1180 AudioEndpointBuilder, Netman, TrkWks,
                                  UxSms, WdiSystemHost
svchost.exe                  1200 TabletInputService
svchost.exe                  1224 CryptSvc, Dnscache, KtmRm, NlaSvc,
                                  TermService, WinRM
```

Как можно видеть, файл svchost.exe используется для запуска множества служб (лишние строки вывода для наглядности удалены).

Утилита командной строки `taskkill` позволяет завершить нежелательный процесс, например, снять зависшую задачу.

По умолчанию в окне диспетчера задач отображаются процессы только для зарегистрированного пользователя. Администратор может установить флажок **Show processes from all users** (Отображать процессы всех пользователей) и увидеть процессы, запущенные другими пользователями (например, при удаленном доступе или при переключении пользователей) или системными учетными записями (`SYSTEM`, `NETWORK SERVICE` и т. д.).

С помощью команды **Select Columns** (Выбрать столбцы) в меню **View** (Вид) можно открыть окно выбора столбцов параметров для вкладок **Processes** (Процессы), **Networking** (Сеть) и **Users** (Пользователи). В открывающемся диалоговом окне **Select … Columns** (Выбор столбцов…) (см. пример на рис. 5.2) установите флажки рядом с теми показателями, которые должны быть отображены в таблице, и нажмите кнопку **ОК**. В нашем примере в результате такой операции на вкладке процессов появился столбец **Command Line** (Командная строка).

В табл. 5.1 приведено краткое описание показателей для вкладки **Processes** (Процессы) диспетчера задач.

Таблица 5.1. *Перечень показателей, имеющихся в диспетчере задач для списка процессов*

Столбец	Описание
Image Name (Имя образа)	Всегда отображаемое имя исполняемого файла, использованного для запуска процесса
PID (Process Identifier) (ИД процесса (PID))	Числовое значение, которое уникальным образом определяет процесс во время его работы
User Name (Пользователь)	Имя пользователя или название сервиса, запустившего процесс
Session ID (Код сеанса)	Код сеанса, связанного с данным процессом, на сервере терминалов
CPU Usage (Загрузка ЦП)	Выраженное в процентах время, в течение которого процесс использовал время процессора с момента последнего обновления
CPU Time (Время ЦП)	Суммарное время процессора, использованное процессом со времени его (процесса) запуска, выраженное в секундах
Memory – Working Set (Память – рабочий набор)	Размер *частного* рабочего набора, используемого процессом, плюс память, которую процесс может использовать совместно с другими процессами
Memory – Peak Working Set (Память – пик рабочего набора)	Максимальный размер рабочего набора, используемого процессом
Memory – Working Set Delta (Память – дельта рабочего набора)	Величина *изменения* размера рабочего набора, используемого процессом
Memory – Private Working Set (Память – частный рабочий набор)	Объем памяти, используемой процессом эксклюзивно
Memory – Commit Size (Память – выделенная память)	Объем виртуальной памяти или адресного пространства, выделенного процессу

Таблица 5.1 *(продолжение)*

Столбец	Описание
Memory – Paged Pool (Память – выгружаемый пул)	Виртуальная память, доступная для кэширования на диск, которая включает в себя всю пользовательскую память и часть системной памяти. Кэширование представляет собой перемещение редко используемых компонентов рабочей памяти из ОЗУ на другой носитель, обычно на жесткий диск
Memory – Non-paged Pool (Память – невыгружаемый пул)	Объем памяти операционной системы, используемой процессом (в килобайтах). Данная память никогда не выгружается на диск
Page Faults (Ошибки страниц)	Для процесса — количество попыток чтения данных по причине их отсутствия в памяти. Это значение накапливается с момента запуска процесса
Page Faults Delta (Дельта ошибок страниц)	Изменение количества ошибок страниц с момента последнего обновления
Base Priority (Базовый приоритет)	Базовый приоритет процесса, используемый процессором для выбора очередности выполнения процессов. Приоритет можно менять в окне диспетчера задач (см. команду **Set Priority** (Приоритет) — рис. 5.3)
Handles (Дескрипторы)	Количество дескрипторов объектов в таблице объектов процесса
Threads (Счетчик потоков)	Число потоков, запущенных процессом
USER Objects (Объекты USER)	Количество USER-объектов, используемых процессом в данный момент (эти объекты являются внутренними объектами диспетчера Window Manager и представляют собой элементы пользовательского интерфейса — окна, меню, значки и т. д.)
GDI Objects (Объекты GDI)	Количество объектов Graphics Device Interface (GDI), используемых процессом в данный момент (это объекты API-интерфейсов для устройств графического вывода)
I/O Reads (Число чтений)	Число операций ввода/вывода, сгенерированных процессом чтения, включая операции ввода/вывода для файлов, сети и устройств

Таблица 5.1 *(окончание)*

Столбец	Описание
I/O Writes (Число записей)	Число операций ввода/вывода, сгенерированных процессом записи, включая ввод/вывод файлов, сети и устройств
I/O Other (Прочий ввод-вывод)	Число операций ввода/вывода, сгенерированных процессом записи и *не являющихся* операциями чтения или записи (например, функции управления)
I/O Read Bytes (Прочитано байт)	Число байтов, прочитанных в ходе операций ввода/вывода, сгенерированных процессом чтения, включая операции ввода/вывода для файлов, сети и устройств
I/O Write Bytes (Записано байт)	Число байтов, записанных в ходе операций ввода/вывода, сгенерированных процессом записи, включая операции ввода/вывода, связанные с файлами, сетью и устройствами
I/O Other Bytes (Прочих байт при вводе-выводе)	Число байтов, переданных в ходе операций ввода/вывода, сгенерированных процессом и *не являющихся* операциями чтения или записи (например, выполнение функций управления)
Image Path Name (Путь к образу)	Полное имя образа (исполняемого файла данного процесса), например, C:\Windows\System32\svchost.exe
Command Line (Командная строка)	Команда с параметрами, используемая для запуска процесса, например, C:\Windows\System32\svchost.exe –k secsvcs
Virtualisation (Виртуализация)	Указывает — включена ли (Allowed), отключена (Disabled) или запрещена (Not Allowed) виртуализация механизма управления учетными записями (User Account Control, UAC) для данного процесса (виртуализация UAC обеспечивает перенаправление операций записи файлов и реестра в определенные места, заданные для каждого пользователя)
Description (Описание)	Название службы, программы или процесса
Data Execution Prevention (Предотвращение выполнения данных)	Указывает — включено (Enabled) или выключено (Disabled) предотвращение выполнения данных для данного процесса

СОВЕТ

Еще бóльшие возможности мониторинга процессов предоставляет программа *Process Explorer*, которую легко скачать с веб-сайта Windows Sysinternals, созданного Марком Руссиновичем (Mark Russinovich) и Брюсом Когсвелом (Bryce Cogswell) (см. ссылки в *Приложении*).

Работа системных служб

На вкладке **Services** (Службы) (рис. 5.4) перечислены все службы (сервисы), имеющиеся в системе, дано их описание и указаны текущее состояние и учетная запись безопасности, которая используется при запуске службы. Для каждой работающей службы указан идентификатор (ID) соответствующего процесса (зная этот идентификатор, проще следить за тем, какие ресурсы использует процесс). В этом окне службу можно запустить или остановить.

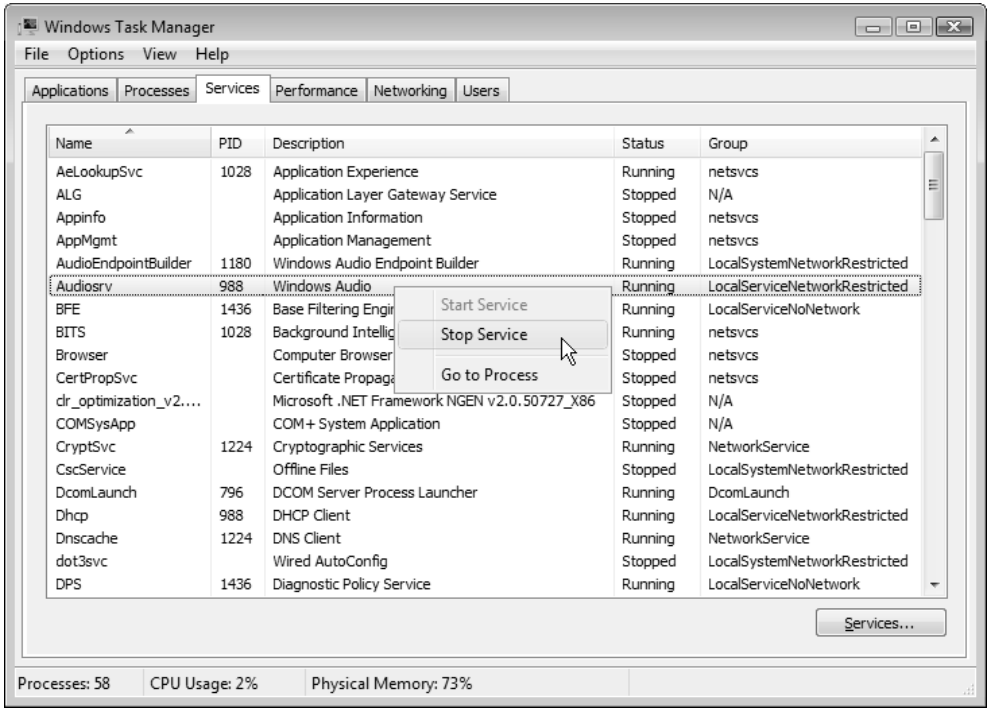


Рис. 5.4. Список системных служб и их состояние

Список многочисленных служб можно сортировать по любому столбцу. Это позволяет, например, выбирать группы по их состоянию или по принадлежности к определенной группе.

Если в контекстном меню некоторой запущенной службы выполнить команду **Go to Process** (Перейти к процессу), то откроется вкладка **Processes** (Процессы), на которой будет выбран процесс, связанный с этой службой, и, следовательно, можно увидеть, какие ресурсы использует выбранная служба. Это особенно удобно для процесса svchost.exe, который является хост-процессом для многих системных служб, и не всегда можно понять, какой его экземпляр связан с конкретной службой (или наоборот).

Таким образом, как можно видеть, вкладка **Services** (Службы) заметно расширяет функциональные возможности диспетчера задач в Windows Server 2008 (по сравнению с предыдущими версиями Windows) и повышает эффективность работы с ним.

Для получения информации о службах в окне командной строки можно использовать утилиту `sc` (команда `sc query`), с помощью которой можно также полностью управлять состоянием и параметрами службы.

Анализ загрузки системы

Для отслеживания загрузки системы (процессора и памяти) в окне диспетчера задач используется вкладка **Performance** (Быстродействие) (рис. 5.5).

Для отображения на диаграмме **CPU Usage** (Загрузка ЦП) доли процессорного времени, в течение которого процессор работал в режиме ядра (это время будет представлено линией красного цвета), выберите команду **Show Kernel Times** (Вывод времени ядра) в меню **View** (Вид).

Пользователи многопроцессорных систем могут выбрать в меню **View** (Вид) команду **CPU History** | **One Graph Per CPU** (Загрузка ЦП | По графику на каждый ЦП), с помощью которой отображается индивидуальная диаграмма занятости для каждого процессора (как показано на рис. 5.5).

На рис. 5.5 виден новый элемент диспетчера задач — кнопка **Resource Monitor** (Монитор ресурсов), нажав которую можно перейти в окно, где представлена подробная информация по загрузке процессора, диска, сети и памяти (см. рис. 5.18—21). Монитор ресурсов подробнее будет описан позже, в составе оснастки **Reliability and Performance Monitor** (Монитор производительности и стабильности).

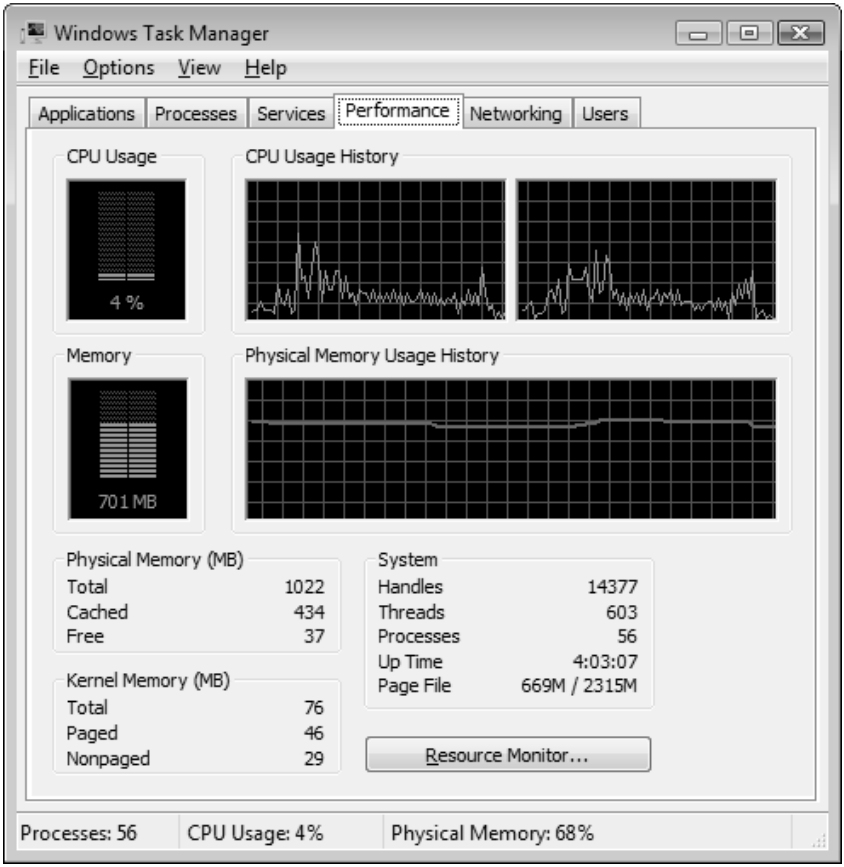


Рис. 5.5. Диаграммы занятости процессоров и памяти

Мониторинг сети

На вкладке **Networking** (Сеть) (рис. 5.6) можно в виде графика видеть объем информации, передаваемой по сети в каждый момент времени. Если на компьютере установлены несколько сетевых адаптеров (в нашем примере показаны два адаптера), то для каждого адаптера отображается отдельная панель, на которой будет представлена кривая, показывающая загрузку конкретного адаптера.

С помощью команды **View** | **Select Columns** (Вид | Выбрать столбцы) можно перейти в окно отображаемых столбцов и выбрать, к примеру, вывод в таб-

лице числа полученных (Bytes Received) и/или отправленных байтов (Bytes Sent) для каждого сетевого адаптера (см. рис. 5.6).

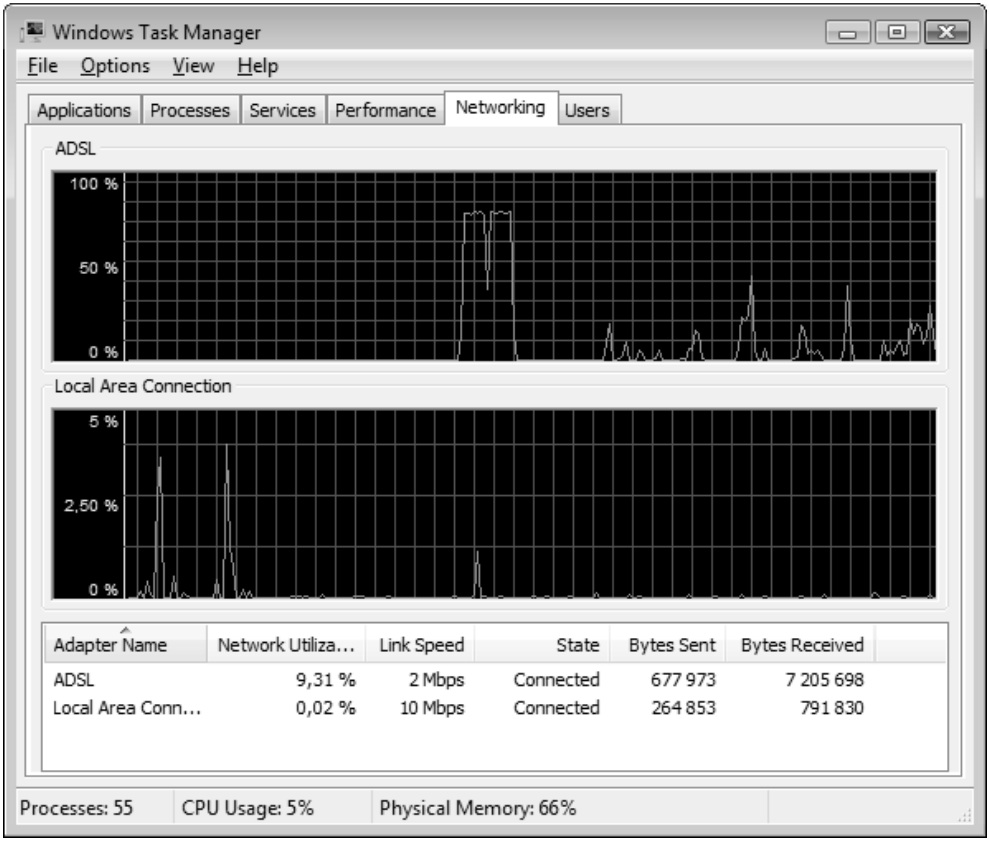


Рис. 5.6. Отображение загруженности сетевого адаптера

Команда **View** | **Network Adapter History** (Вид | Журнал сетевого адаптера) позволяет отдельно (дополнительно) отображать на графике число полученных (**Bytes Received** (Получено байт)) и/или отправленных байтов (**Bytes Sent** (Отправлено байт)); по умолчанию на графике видно *общее* количество переданных (принятых и посланных) байтов.

При необходимости в таблицу параметров можно добавить столбцы, в которых будет отображаться общее количество переданных байтов, причем если установить флажок **Options** | **Show Cumulative Data** (Параметры | Отображать накапливаемые данные), то будут учитываться не только те данные, ко-

торые были получены после запуска диспетчера задач, но и суммарные — с момента загрузки системы. Если, например, отображается окно адаптера, через который осуществляется подключение к Интернету (в нашем примере такое соединение названо "ADSL"), то на вкладке **Networking** (Сеть) можно весьма точно оценивать внешний сетевой трафик (правда, до определенного предела, поскольку после приблизительно 4 Гбайт значения счетчиков сбрасываются).

По умолчанию график загрузки сети появляется на вкладке **Networking** (Сеть) *с момента выбора этой вкладки*, и предыдущие показания видеть нельзя. Если установить новый флажок **Tab Always Active** (Вкладка всегда активна), то информация об использовании сети начинает собираться сразу же *после запуска диспетчера задач*, даже если вкладка **Networking** (Сеть) и не открывалась. В этом случае после выбора вкладки можно в виде графика видеть уже накопленные данные.

Просмотр списка зарегистрированных пользователей

На вкладке **Users** (Пользователи) отображаются имена всех пользователей, зарегистрированных в данный момент на компьютере локально (благодаря наличию опции быстрого переключения пользователей (Fast User Switching)) или удаленно (при использовании служб терминалов (Terminal Services) или функций Remote Desktop (Удаленный рабочий стол) и Remote Assistance (Удаленный помощник)). На рис. 5.7 иллюстрируется ситуация, когда в системе зарегистрированы три пользователя: один локально (Administrator), а два других удаленно.

На вкладке **Users** (Пользователи) выбранному пользователю можно послать сообщение с помощью команды контекстного меню или кнопки **Send Message** (Отправить сообщение). Кроме того, "лишних" пользователей можно отключить (кнопка **Disconnect** (Отключить); при этом все запущенные пользователем задачи сохраняются, и он сможет вернуться к ним после повторного подключения) или "разрегистрировать" их в системе (кнопка **Logoff** (Выйти из системы); в этом случае пользователь прекращает работу в системе). Для этого, разумеется, нужно иметь права администратора компьютера.

> ***Внимание!***
>
> Поскольку в системах Windows Server 2008 одновременно активными могут быть только два подключения к рабочему столу, "лишний" пользователь (в

нашем примере на рис. 5.7 — учетная запись User) отключается, хотя все его приложения остаются активными и параметры сеанса подключения сохраняются. Поэтому выключение компьютера в подобной ситуации должно выполняться с осторожностью, и следует учитывать возможность потери данных в случае принудительного прекращения работы пользователя.

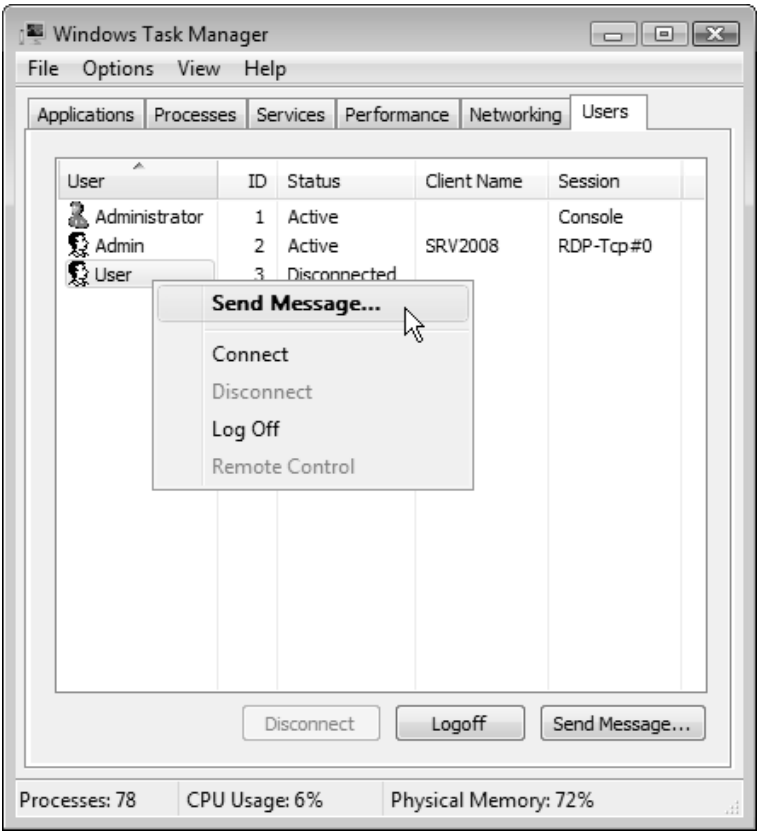


Рис. 5.7. Имена пользователей, зарегистрированных на компьютере

Просмотр событий, регистрируемых системой, службами и приложениями

Любое изменение в работе операционной системы, сервисов или приложений в системах Windows называется *событием*. В случае возникновения критических ситуаций на экране монитора появляется соответствующее сообщение.

Эти события, а также другие, которые не требуют от пользователя немедленных действий, но полезны для анализа неисправностей и мониторинга, регистрируются в *системных журналах*. Служба регистрации событий в системных журналах активизируется автоматически при каждом запуске системы.

В системах Windows Vista/Windows Server 2008 события системы, служб и приложений четко классифицированы, и их можно просматривать в индивидуальных журналах, число которых приближается к сотне.

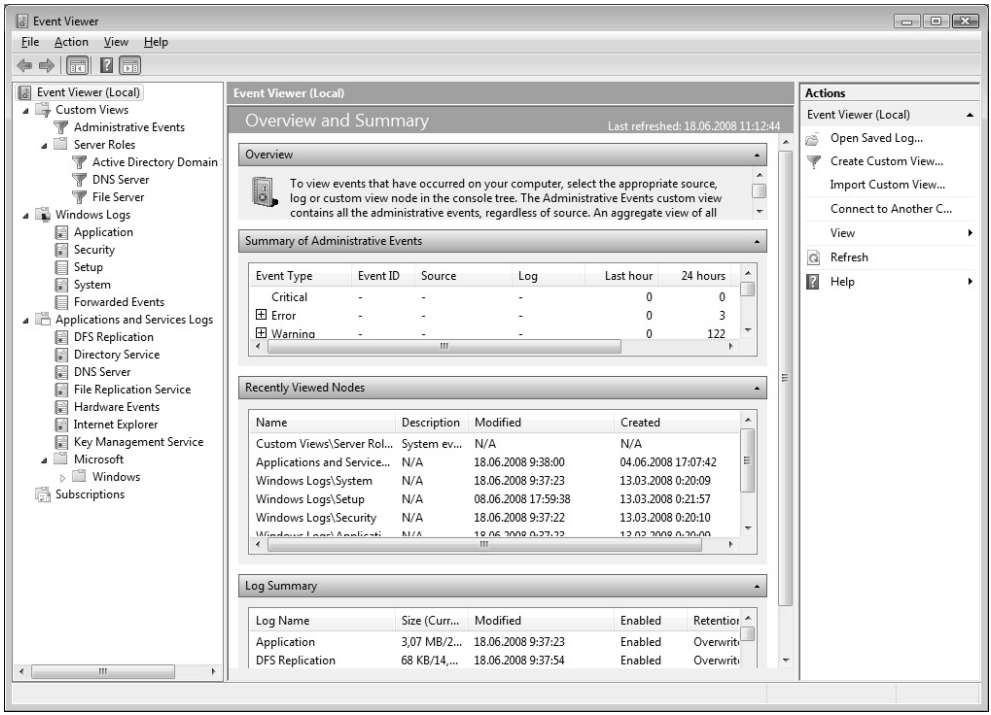


Рис. 5.8. Основное окно оснастки **Event Viewer**

Для просмотра системных журналов традиционно используется оснастка **Event Viewer** (Просмотр событий), которая в системах Windows Vista/Windows Server 2008 кардинально переработана и выглядит как информационный центр, в котором собраны все сведения о том, что происходило в системе. Несмотря на большое количество отображаемых данных и элементов управления журналами, работать с событиями стало проще, особенно при большом количестве разнообразных событий, имеющих разную степень важности. Новый дизайн оснастки позволяет видеть много обобщающей и

статистической информации, а в некоторых случаях, наоборот, сразу выбирать критически важные события.

Оснастка **Event Viewer** (Просмотр событий) входит в состав оснастки **Computer Management** (Управление компьютером) и новой для Windows Server 2008 оснастки **Server Manager** (Диспетчер сервера); ее также можно вызывать непосредственно из меню **Start** (Пуск) или с панели управления. Пример окна оснастки, запущенной автономно, показан на рис. 5.8.

После запуска оснастки в центральной части ее окна представлена статистика (сводка) по всем журналам (число ошибок, предупреждений и т. д.). Папка **Custom Views** | **Administrative Events** (Настраиваемые представления | События управления) содержит только те события, которые требуют внимания администратора — ошибки и предупреждения. Такое решение позволяет не отвлекаться на просмотр менее значительной информации. Здесь же размещаются созданные пользователем представления журналов.

В системах Windows Server 2008 в составе папки **Custom Views** (Настраиваемые представления) появился новый узел — **Server Roles** (Роли сервера), где для каждой роли сервера имеется отдельный журнал (представление), в котором отображаются только те события, которые относятся к конкретной роли (к входящим в ее состав сервисов). Это значительно упрощает контроль за работой прикладных служб.

В правой части окна оснастки находится типичная для новой консоли управления Microsoft Management Console 3.0 панель **Actions** (Действия), на которой располагаются команды, имеющиеся для объекта, выбранного с помощью курсора на других панелях оснастки. Эту панель можно быстро включать и убирать с помощью соответствующей кнопки на панели инструментов.

С помощью оснастки **Event Viewer** (Просмотр событий) можно просматривать журналы различных типов. В папке **Windows Logs** (Журналы Windows) располагаются традиционные системные журналы:

- **Application** (Приложение) — фиксирует события, зарегистрированные приложениями. События, вносимые в журнал приложений, определяются разработчиками соответствующих приложений. В системе Windows Server 2008 для подобных событий рекомендуются специальные журналы;
- **Security** (Безопасность) — содержит записи, связанные с системой безопасности, например, сообщения аудита попыток доступа в систему или обращений к ресурсам. С помощью этого журнала можно отслеживать

изменения в системе безопасности и идентифицировать бреши в защите. Типы регистрируемых в журнале событий определяются администратором. Для просмотра журнала необходимо иметь права администратора;

> ***Внимание!***
>
> В системах Windows Server 2008 по умолчанию отслеживаются многие события, связанные с безопасностью, и сведения заносятся в журнал безопасности (даже если аудит событий и не включен).

- **Setup** (Настройка) — используется для сообщений, касающихся установки и обновлений системы, ее компонентов и приложений;
- **System** (Система) — содержит записи о событиях, которые регистрируются системными компонентами. Например, в системный журнал записываются такие события, как сбой при загрузке драйвера или других системных компонентов при запуске системы. Список типов событий, которые заносятся в системный журнал, строго определен;
- **Forwarded Events** (Пересланные события) — события, полученные по запросу с других компьютеров.

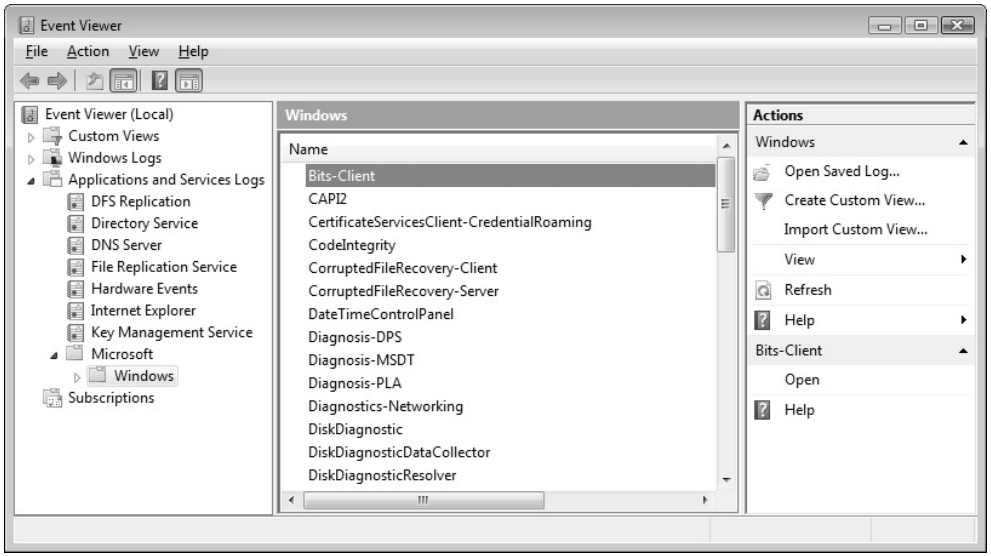


Рис. 5.9. Сообщения, поступающие от компонентов системы

В группе **Application and Services Logs** (Журналы приложений и служб) находятся специальные журналы для отдельных компонентов и системных служб (например, для DNS-сервера, службы каталогов, службы репликации файлов и т. д.). Кроме этого, в папке имеются многочисленные журналы (рис. 5.9), в которые заносятся события конкретных компонентов, служб и подсистем, в первую очередь — детальная информация об ошибках в их работе. (Например, в журнале **Bits-Client** можно найти подробную информацию о загрузке и установке различных обновлений системы.)

> ***Внимание!***
>
> Когда какой-нибудь журнал открывается, оснастка **Event Viewer** (Просмотр событий) отображает его текущее содержимое. Во время просмотра журнала информация не обновляется, если не запускать обновление. Если журнал не отображается в текущем окне, то информация автоматически обновляется при переключении журналов.

Типы событий

В журналах регистрируются перечисленные ниже типы событий.

- *Error* (Ошибка) — событие регистрируется в случае возникновения серьезного события (такого как потеря данных или функциональных возможностей). Событие данного типа будет зарегистрировано, если невозможно загрузить какой-либо из сервисов в ходе запуска системы.
- *Warning* (Предупреждение) — событие не является серьезным, но может привести к возникновению проблем в будущем. Например, если недостаточно дискового пространства, то в журнал будет занесено предупреждение.
- *Information* (Сведения) — значимое событие, которое свидетельствует об успешном завершении операции приложением, драйвером или сервисом. Такое событие может, например, зарегистрировать успешно загрузившийся сетевой драйвер.
- *Audit Success* (Аудит выполнен успешно) — событие, соответствующее успешно завершенному действию, относящемуся к безопасности системы. Примером такого события является успешная попытка входа пользователя в систему.
- *Audit Failure* (Сбой аудита) — событие, соответствующее неудачно завершенному действию, относящемуся к безопасности системы. Например, такое событие будет зарегистрировано, если попытка доступа пользователем к сетевому диску закончилась неудачей.

Просмотр журналов и параметров событий

Оснастка **Event Viewer** (Просмотр событий) в системах Windows Vista/Windows Server 2008 позволяет просматривать журналы и сразу видеть все данные о выбранном событии в окне, располагающемся ниже списка событий (рис. 5.10). Справа, на панели **Actions** (Действия), перечислены операции, которые можно выполнять с выбранным журналом и указанным событием (например, сохранять журнал, фильтровать события, создавать виды просмотра, привязывать задачу к указанному событию и т. д.).

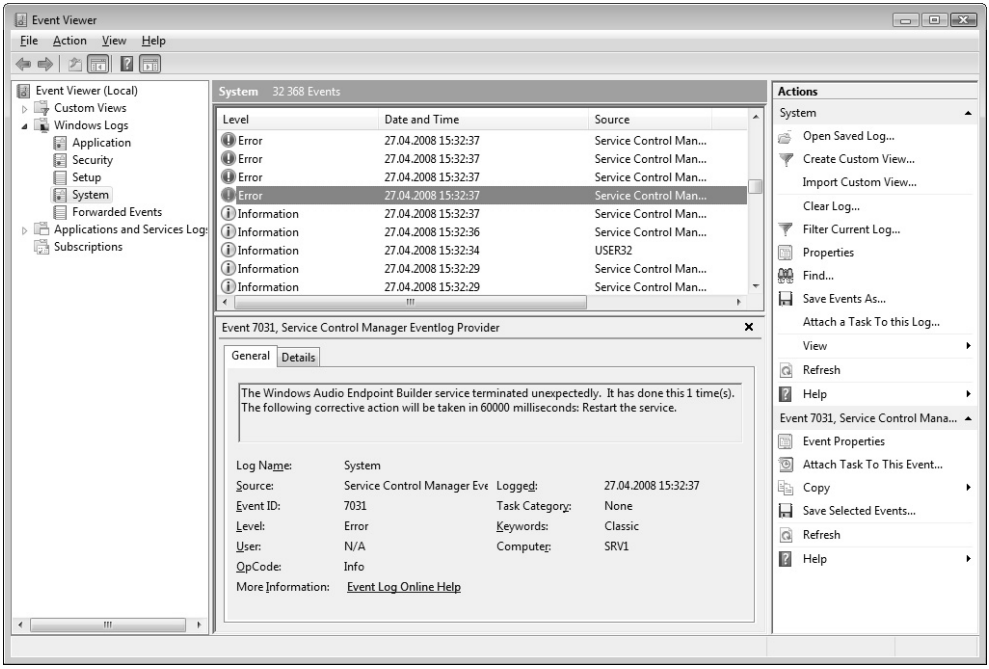


Рис. 5.10. Просмотр событий в выбранном журнале

Можно, наоборот, список событий сделать максимально видимым для удобства поиска событий, а дополнительную информацию о них просматривать в отдельном окне, по мере необходимости. Для этого в подменю **View** (Вид) на панели **Actions** (Действия) нужно сбросить флажок и отключить область просмотра (Preview Pane). Окно свойств событий в этом случае будет открываться после двойного щелчка на записи в журнале или при выборе соответствующей задачи на панели **Actions** (Действия). На вкладке **General** (Общие)

(рис. 5.11) видны все параметры события, а на панели **Details** (Подробности) приведена детальная информация о событии. Стрелки перемещения вверх и вниз позволяют просматривать записи в журнале, не закрывая окна свойств событий.

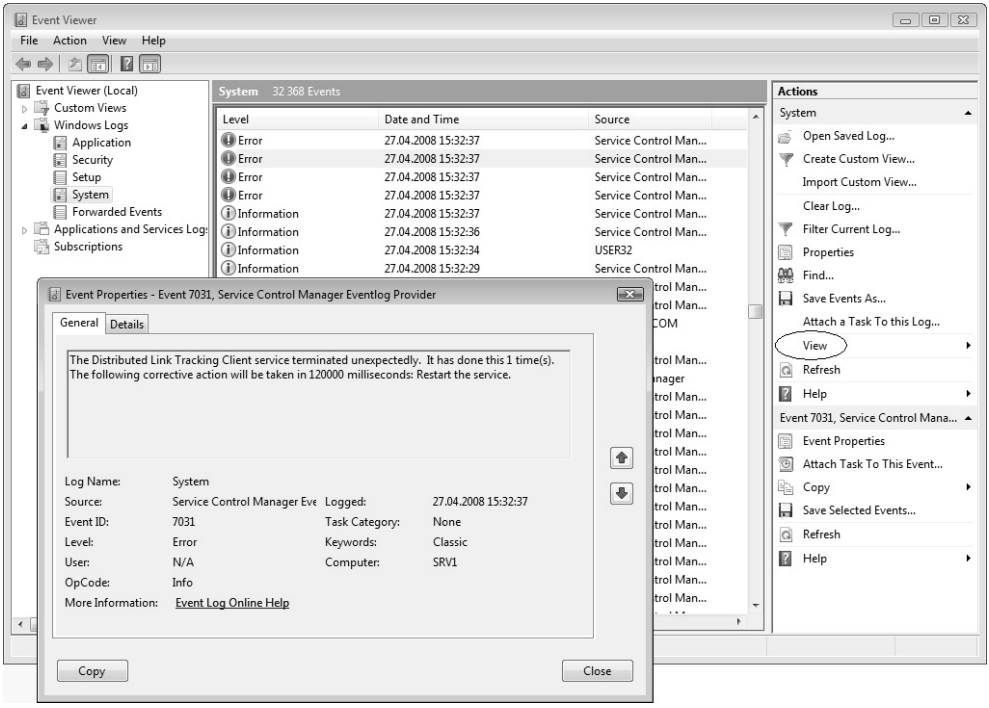


Рис. 5.11. Новый дизайн оснастки позволяет выбирать способ просмотра списка событий и информации о конкретном событии

Новая оснастка **Server Manager** (Диспетчер сервера), появившаяся в Windows Server 2008, позволяет просматривать события, относящиеся к конкретным службам, обеспечивающим выполнение той или иной роли сервера. Такая "централизация" и фильтрация событий позволяет быстро оценить, насколько сервер справляется с конкретной ролью и возникают ли при этом проблемы.

На рис. 5.12 в качестве примера показано окно оснастки для роли File Services (Файловые службы). Сразу можно видеть все события, возникшие в процессе работы, а также текущее состояние служб, относящихся к данной роли. При необходимости можно быстро вызвать другие оснастки (**Event**

Viewer (Просмотр событий) или **Services** (Службы)) и получить более детальную информацию или дополнительные возможности управления сервисами — для этого в правой части окна имеются соответствующие ссылки.

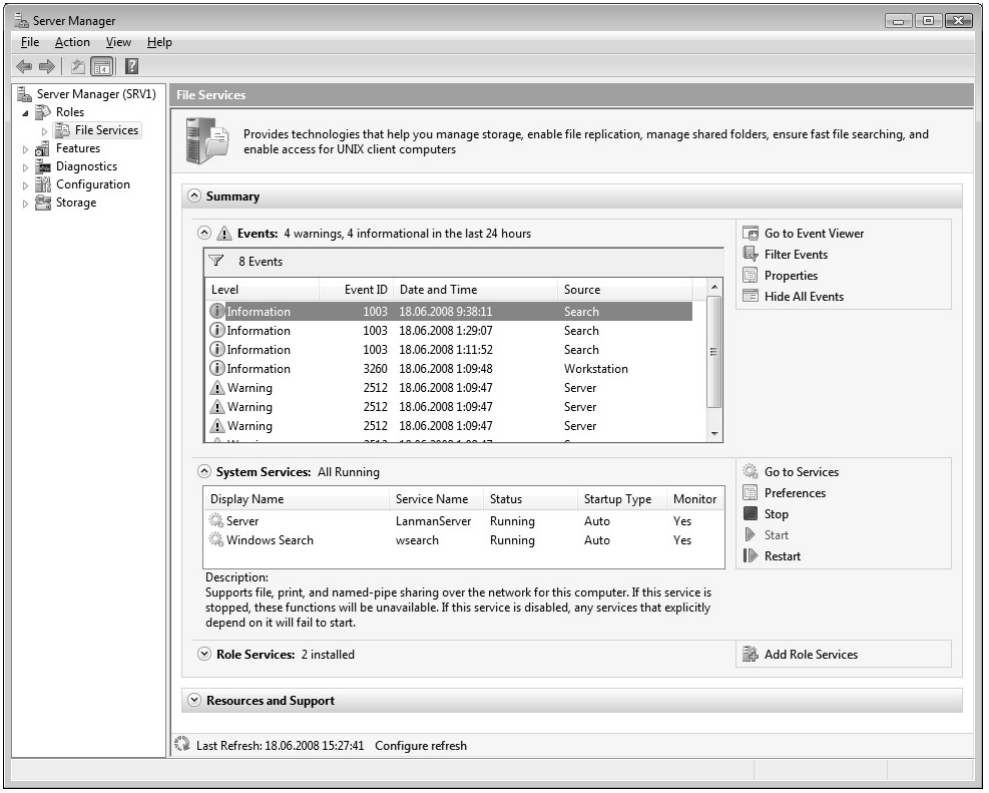


Рис. 5.12. Просмотр событий для роли сервера в окне оснастки **Server Manager**

Фильтрация событий

В системных журналах регистрируется громадное количество событий, и не все они могут быть одинаково важны для администратора. Для выбора нужных событий следует пользоваться фильтрами журналов, которые в Windows Vista/Windows Server 2008 называются *настраиваемыми представлениями* (custom view).

Для создания представления требуется выбрать нужный журнал событий и в контекстном меню выбрать команду **Create Custom View** (Создать настраиваемое представление) или **Filter Current Log** (Фильтр текущего журнала). (Эти команды похожи по сути, отличие лишь в том, что первая команда позволяет сохранить представление журнала (нескольких журналов) в виде *нового* журнала, а вторая просто ограничивает число событий, просматриваемых в конкретном журнале событий.) В окне свойств представления нужно указать характеристики событий, которые представляют интерес и будут отображаться в новом представлении или фильтре.

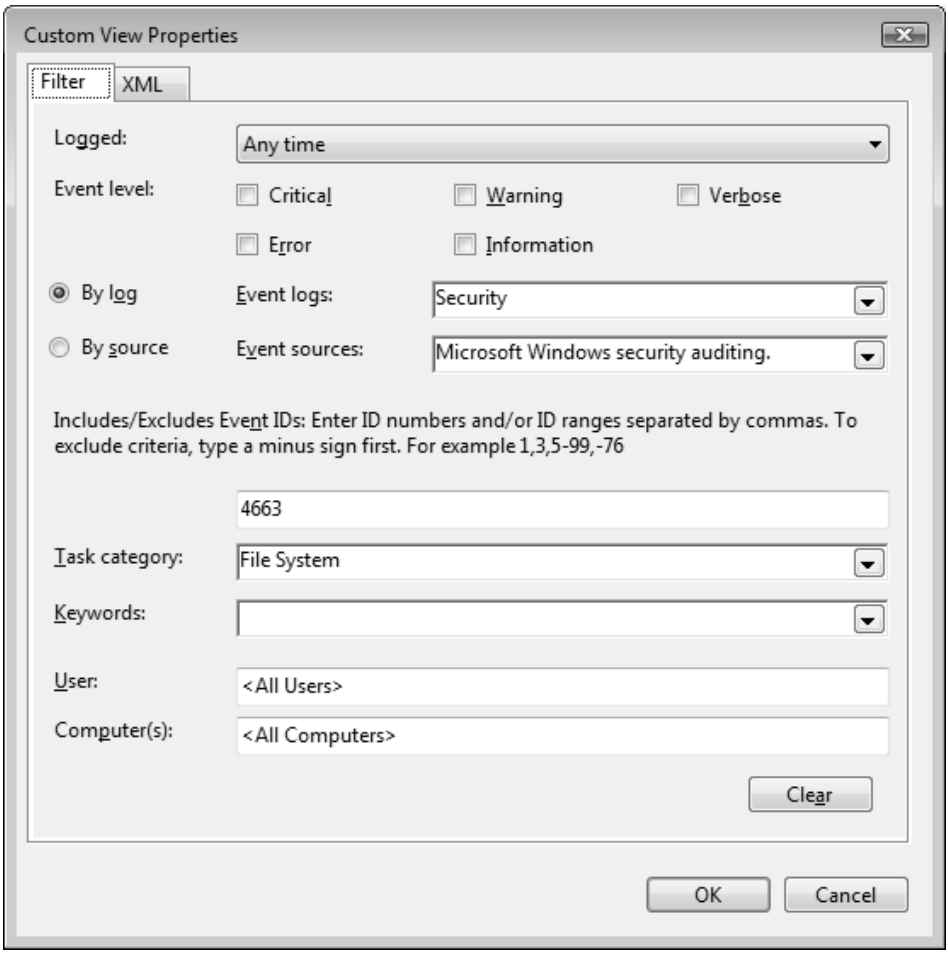


Рис. 5.13. Пример фильтра настраиваемого представления журнала

Типичной ситуацией, когда использование настраиваемого представления для журнала Security (Безопасность) просто необходимо, является задача аудита доступа к файлам и папкам жесткого диска. При включении аудита генерируется громадное количество системных событий, не представляющих непосредственного интереса для мониторинга обращений (чтения, создания, удаления и т. д.) к критически важным файлам. Поэтому следует выбирать только те события, которые отражают операции изменения файла или папки. На рис. 5.13 показан пример фильтра для решения этой задачи. Как можно видеть, из журнала Security (Безопасность) выбраны только события, связанные с аудитом (источник — Microsoft Windows security auditing). (Дату просмотра можно менять, и просматривать, к примеру, не все события, а только те, которые произошли за последний час, 12 часов и т. д.)

Из всех событий аудита выбраны только события с кодом 4663, связанные с доступом к объекту файловой системы (Task category (Категория задачи) — File System (Файловая система)). (Нужные коды событий проще всего найти опытным путем, просматривая журналы и выбирая события, представляющие интерес для мониторинга.) В результате применения фильтра количество просматриваемых событий резко уменьшается. Еще больше сузить область поиска конкретных событий можно с помощью команды **Find** (Найти), выполняющейся из контекстного меню журнала или представления, а также присутствующей на панели **Actions** (Действия). Например, можно ввести строку `WriteData` (или "Запись данных", если интерфейс русскоязычный) (или имя интересующего файла) и просматривать только операции изменения и создания файлов или папок (или события, связанные с конкретным файлом). При выполнении поиска в окне оснастки видны все свойства найденного события, поэтому нужную информацию находить очень легко.

Все созданные настраиваемые представления сохраняются в папке **Custom Views** (Настраиваемые представления) (см. рис. 5.8). Их название и другие свойства, включая параметры фильтра, можно менять в любой момент. Просмотр представлений и выполнение других операций ничем не отличаются от способов работы с обычными системными журналами Application (Приложение), Security (Безопасность) и т. д.

Подписки и отправляемые события

В системах Windows Vista/Windows Server 2008 появилась концепция *отправляемых*, или *пересылаемых событий* (forwarded event). Смысл идеи состоит в том, чтобы можно было *подписаться* на определенные события, происходящие на удаленных компьютерах (работающих под управлением

Windows Vista или Windows Server 2008). При "оформлении" подписки точно указываются тип событий и периодичность их отправки подписчику. Полученные события можно просматривать и обрабатывать так же, как и любые события в системе. Такой подход позволяет избавиться от необходимости просмотра большого количества информации, поскольку можно получать только те данные, которые требуются. В первую очередь, конечно, это будет полезно в сетевой среде со многими компьютерами.

Для активизации механизма подписок требуются действия на обоих компьютерах — на том, который будет отправлять события, и на том, который будет их получать. Реализация этого механизма возможна благодаря появлению в составе Windows Vista/Windows Server 2008 новой службы — *Windows Remote Management (WS-Management)* (Службы удаленного управления Windows (WS-Management), сервис WinRM), которая использует протокол WS-Management. Для отправления и получения сообщений имеются специальные системные сервисы: *Windows Event Collector Service* (Сборщик событий Windows, Wecsvc) и *Windows Error Reporting Service* (Служба регистрации ошибок Windows, WerSvc), запускаемые на компьютерах подписчика и отправителя соответственно.

Для управления службой WS-Management имеется системная утилита командной строки *Winrm.exe*. Ее описание и параметры можно получить, введя в окне консоли строку `winrm`.

Для того чтобы компьютер мог принимать запросы службы Windows Remote Management и передавать информацию подписчикам, необходимо его подготовить к работе с помощью команды `winrm quickconfig`. Эту команду следует ***предварительно выполнить*** на каждом компьютере, с которого необходимо получать информацию о событиях. Диалог в окне командной строки будет выглядеть следующим образом:

```
C:\>winrm quickconfig
WinRM is not set up to allow remote access to this machine for manage-
ment.
The following changes must be made:

Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP
on this machine.

Make these changes [y/n]? y

WinRM has been updated for remote management.

Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP
on this machine.

C:\>
```

По умолчанию служба сборщика событий (Windows Event Collector Service) отключена, однако при обращении к механизму подписок система может автоматически запустить службу и настроить режим начального пуска. При этом необходимо ***вручную*** разрешить в настройках встроенного брандмауэра исключения для службы Windows Remote Management.

Если в окне оснастки выбрать узел **Subscriptions** (Подписки) (см. рис. 5.8) и в контекстном меню или на панели **Actions** (Действия) выполнить команду **Create Subscription** (Создать подписку), то откроется окно свойств новой подписки (рис. 5.14). Название подписки может быть произвольным, но желательно информативным. Все полученные события по умолчанию заносятся в журнал Forwarded Events (Пересланные события).

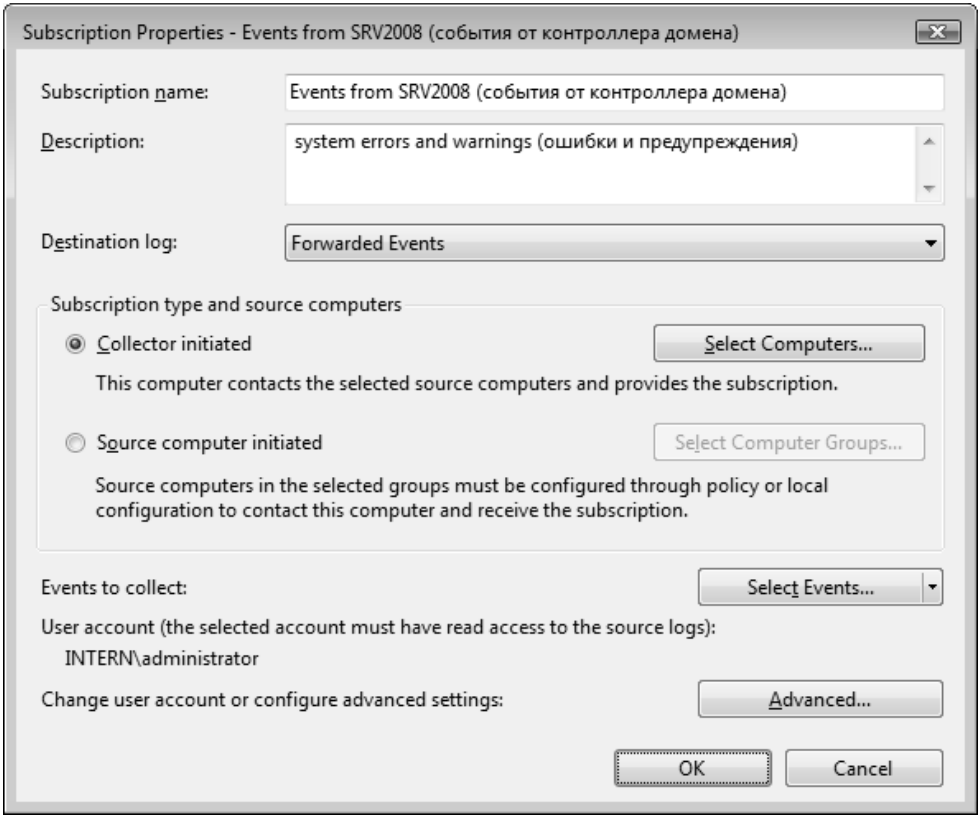


Рис. 5.14. Окно свойств подписки на события

Кнопка **Select Computers** (Выбрать компьютеры) позволяет выбрать компьютеры, с которых будут собираться события. В специальном окне (рис. 5.15) перечислены имена выбранных компьютеров; соответствующие кнопки позволяют добавлять новые имена или удалять имеющиеся. С помощью кнопки **Test** (Проверить) можно оценить работоспособность службы Windows Remote Management; это особенно важно при создании новой подписки, поскольку необходимо убедиться в том, что удаленный компьютер настроен соответствующим образом *(см. выше)*.

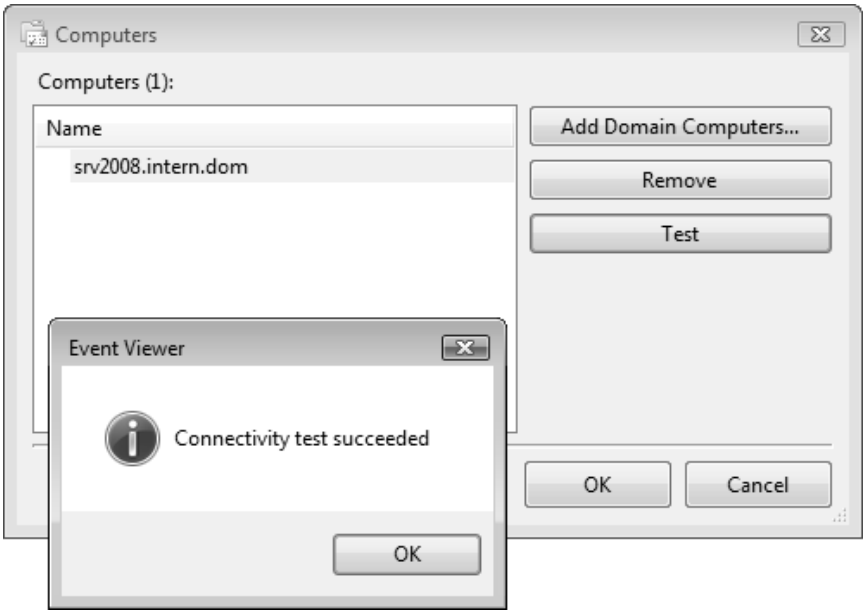


Рис. 5.15. Список компьютеров,
с которых собираются системные события

Кнопка **Select Events** (Выбрать события) в окне свойств подписки позволяет перейти к настройке фильтра событий (см. рис. 5.13) или выбрать фильтр уже существующего настраиваемого представления (для этого нужно щелкнуть по стрелке в правой части кнопки). Необходимо указать имя и пароль пользователя, имеющего возможность просмотра событий на исходном (удаленном) компьютере. Для этого и дополнительных настроек служит кнопка **Advanced** (Дополнительно). После выбора всех параметров подписки нужно нажать кнопку **OK**. После этого в папке подписок появится новая строка (рис. 5.16), и наличие зеленого флажка в левой части свидетельствует об успешном окончании опе-

рации и активности подписки. Для управления подписками используются команды в контекстном меню, показанные на рисунке.

Все подписки хранятся в папке **Subscriptions** (Подписки), и их текущее состояние легко видеть. Подписками можно также управлять и в окне свойств журнала Forwarded Events (Пересланные события) на вкладке **Subscriptions** (Подписки). События, полученные по подписке, просматриваются и анализируются так же, как и обычные журналы.

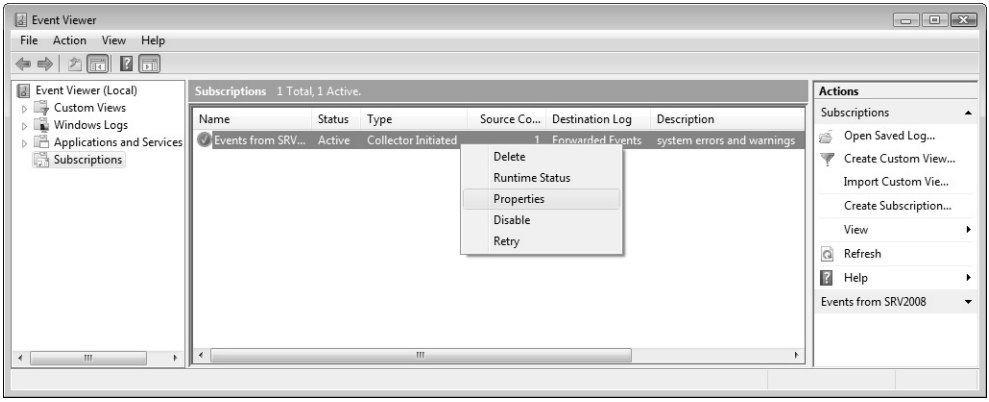


Рис. 5.16. Папка подписок и команды управления подписками

Мониторинг параметров и стабильности работы системы

Оснастка **Reliability and Performance Monitor** (Монитор производительности и стабильности) позиционируется как аналог инструмента Performance (Производительность), существующего в составе Windows XP или Windows Server 2003. Эта оснастка включает в себя следующие компоненты:

- традиционный для систем Windows компонент *Performance Monitor* (Системный монитор);
- новая оснастка **Reliability Monitor** (Монитор стабильности системы);
- компонент **Data Collector Sets** (Группы сборщиков данных), который напоминает оснастку **Performance Logs and Alerts** (Журналы и оповещения производительности), присутствующую в составе Windows XP и Windows Server 2003.

Возможности инструментов, появившихся в системах Windows Vista/ Windows Server 2008, значительно расширились, существенно изменился и их дизайн. Появились принципиально новые средства: например, оснастка **Reliability Monitor** (Монитор стабильности системы) и инструмент для оперативного мониторинга важнейших подсистем (процессора, памяти и т. д.) — компонент Resource Monitor (Монитор ресурсов).

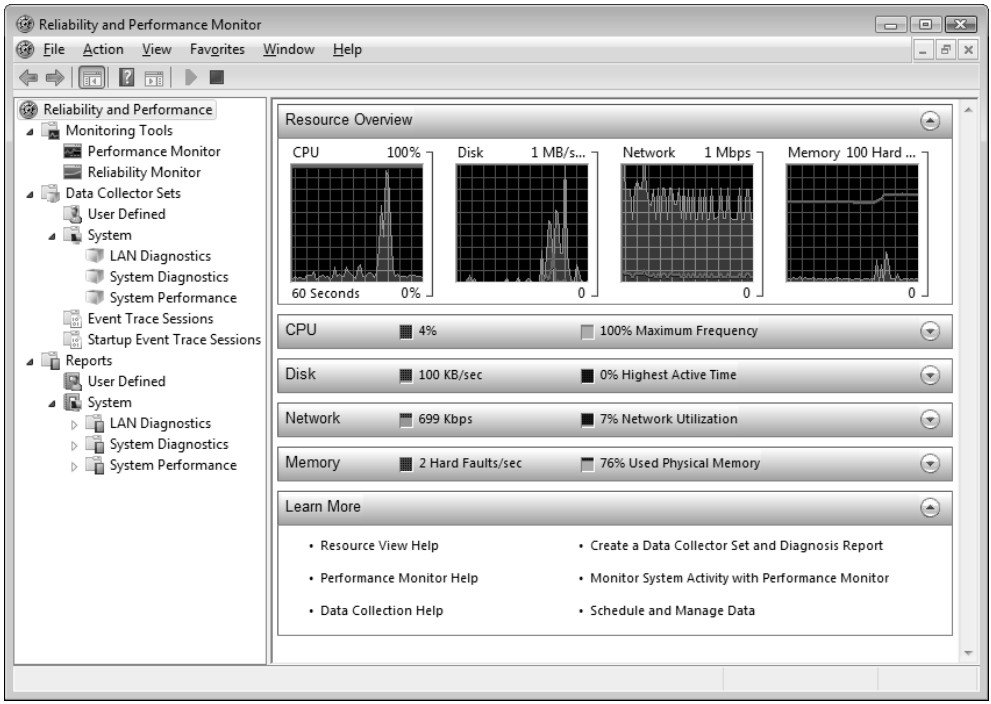


Рис. 5.17. Основной вид оснастки **Reliability and Performance Monitor**

Оснастка **Reliability and Performance Monitor** (Монитор производительности и стабильности) представляет собой мощное средство отображения количественных показателей работы системы, отображающихся в реальном времени[1] (рис. 5.17). С ее помощью администратор может собирать необходимые данные в журналы, определять пороговые значения параметров, в

[1] В русской локализованной версии имеются некоторые расхождения в названиях: везде оснастка фигурирует как "Монитор производительности и стабильности", однако в заголовке ее окна написано "Монитор надежности и производительности".

случае превышения которых будут генерироваться предупреждения или запускаться определенные задачи, создавать отчеты и анализировать работу системы на протяжении некоторого отрезка времени. Многие показания представлены в виде графиков, что облегчает их восприятие и анализ.

На рис. 5.17 центральное место в окне занимает компонент *Resource Monitor* (Монитор ресурсов), входящий в состав оснастки **Reliability and Performance Monitor** (Монитор производительности и стабильности). Он позволяет в реальном времени видеть, как используются процессор, диск, сеть и оперативная память. Для каждой из этих подсистем можно получить подробную информацию, если щелкнуть по стрелке, расположенной на соответствующей панели, находящейся ниже индикаторов производительности.

Примечание

Монитор ресурсов можно также запустить в виде автономного окна, нажав одноименную кнопку в окне диспетчера задач (см. рис. 5.5).

В окне монитора имеются панели индикаторов для четырех основных компонентов системы: центрального процессора, дисковой системы, сетевых адаптеров и памяти. Для процессора отображается список активных процессов (включая их описания) и время занятости процессора (рис. 5.18).

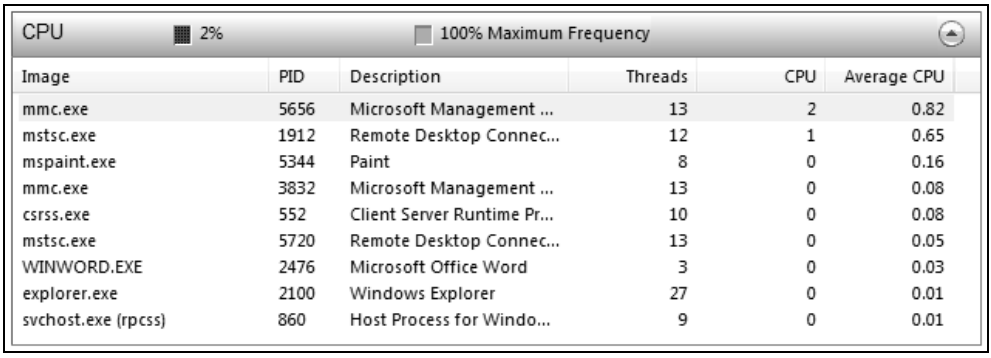
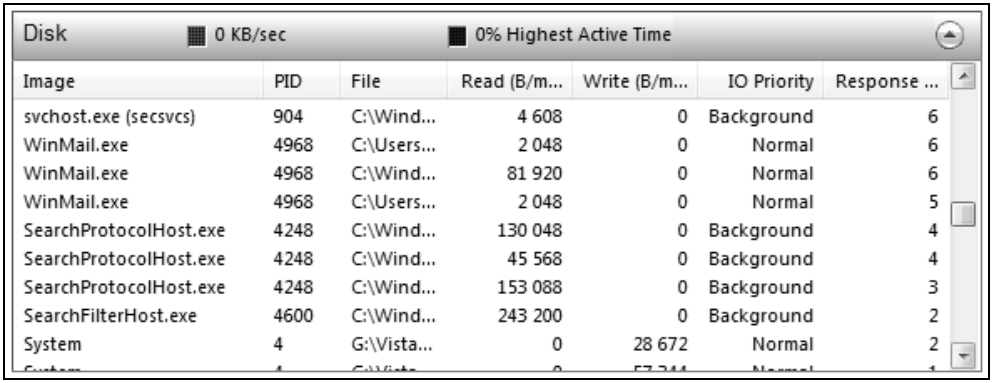


Image	PID	Description	Threads	CPU	Average CPU
mmc.exe	5656	Microsoft Management ...	13	2	0.82
mstsc.exe	1912	Remote Desktop Connec...	12	1	0.65
mspaint.exe	5344	Paint	8	0	0.16
mmc.exe	3832	Microsoft Management ...	13	0	0.08
csrss.exe	552	Client Server Runtime Pr...	10	0	0.08
mstsc.exe	5720	Remote Desktop Connec...	13	0	0.05
WINWORD.EXE	2476	Microsoft Office Word	3	0	0.03
explorer.exe	2100	Windows Explorer	27	0	0.01
svchost.exe (rpcss)	860	Host Process for Windo...	9	0	0.01

Рис. 5.18. Мониторинг загрузки центрального процессора

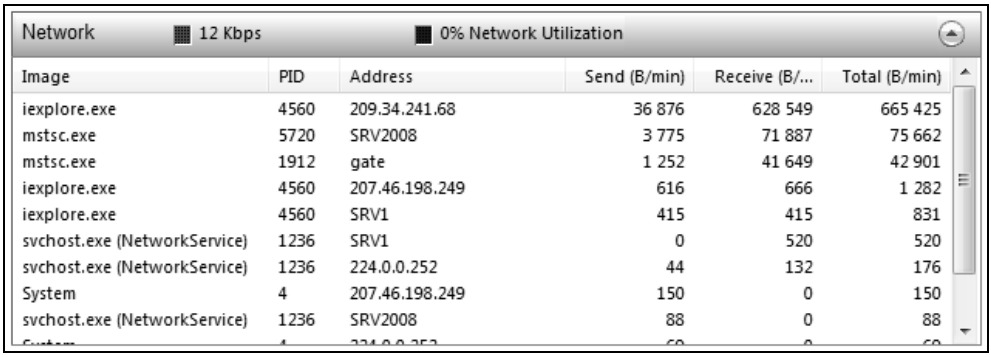
Для жесткого диска на панели можно видеть названия и идентификаторы процессов, работающих с диском; имя файла, к которому процесс обращается; количество переданной информации (рис. 5.19).



Disk 0 KB/sec 0% Highest Active Time

Image	PID	File	Read (B/m...	Write (B/m...	IO Priority	Response ...
svchost.exe (secsvcs)	904	C:\Wind...	4 608	0	Background	6
WinMail.exe	4968	C:\Users...	2 048	0	Normal	6
WinMail.exe	4968	C:\Wind...	81 920	0	Normal	6
WinMail.exe	4968	C:\Users...	2 048	0	Normal	5
SearchProtocolHost.exe	4248	C:\Wind...	130 048	0	Background	4
SearchProtocolHost.exe	4248	C:\Wind...	45 568	0	Background	4
SearchProtocolHost.exe	4248	C:\Wind...	153 088	0	Background	3
SearchFilterHost.exe	4600	C:\Wind...	243 200	0	Background	2
System	4	G:\Vista...	0	28 672	Normal	2

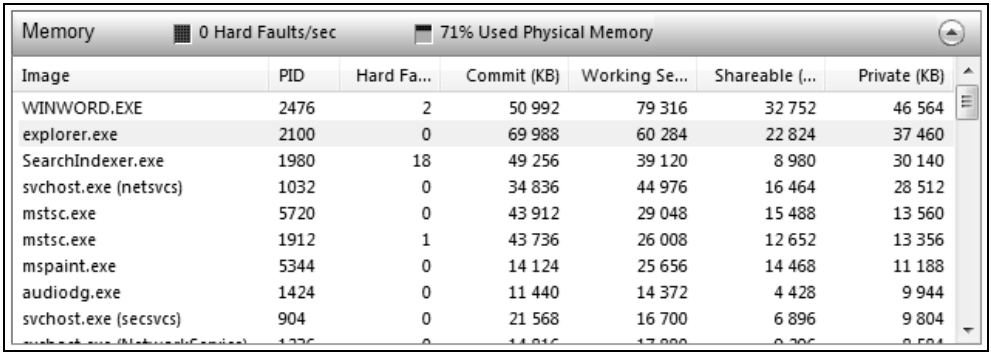
Рис. 5.19. Мониторинг дисковых операций



Network 12 Kbps 0% Network Utilization

Image	PID	Address	Send (B/min)	Receive (B/...	Total (B/min)
iexplore.exe	4560	209.34.241.68	36 876	628 549	665 425
mstsc.exe	5720	SRV2008	3 775	71 887	75 662
mstsc.exe	1912	gate	1 252	41 649	42 901
iexplore.exe	4560	207.46.198.249	616	666	1 282
iexplore.exe	4560	SRV1	415	415	831
svchost.exe (NetworkService)	1236	SRV1	0	520	520
svchost.exe (NetworkService)	1236	224.0.0.252	44	132	176
System	4	207.46.198.249	150	0	150
svchost.exe (NetworkService)	1236	SRV2008	88	0	88

Рис. 5.20. Мониторинг сетевых операций



Memory 0 Hard Faults/sec 71% Used Physical Memory

Image	PID	Hard Fa...	Commit (KB)	Working Se...	Shareable (...	Private (KB)
WINWORD.EXE	2476	2	50 992	79 316	32 752	46 564
explorer.exe	2100	0	69 988	60 284	22 824	37 460
SearchIndexer.exe	1980	18	49 256	39 120	8 980	30 140
svchost.exe (netsvcs)	1032	0	34 836	44 976	16 464	28 512
mstsc.exe	5720	0	43 912	29 048	15 488	13 560
mstsc.exe	1912	1	43 736	26 008	12 652	13 356
mspaint.exe	5344	0	14 124	25 656	14 468	11 188
audiodg.exe	1424	0	11 440	14 372	4 428	9 944
svchost.exe (secsvcs)	904	0	21 568	16 700	6 896	9 804

Рис. 5.21. Мониторинг занятости оперативной памяти

Для сети отображаются названия и идентификаторы процессов; локальные и внешние IP-адреса, по которым выполняются обращения, а также генерируемый трафик (рис. 5.20).

На панели индикаторов оперативной памяти (рис. 5.21) перечислены активные приложения и процессы, для которых указано число ошибок страниц, объем выделенной памяти и размеры рабочих наборов (общие и частные наборы показаны в отдельных столбцах).

Системный монитор (Performance Monitor)

Компонент Performance Monitor (Системный монитор) позволяет следить за параметрами, определяющими производительность локального компьютера или других компьютеров в сети. Для этого в окне монитора визуально представляются значения встроенных счетчиков производительности Windows. Могут отображаться значения, получаемые в реальном времени, или же результаты, накопленные в журналах Data Collector Sets (Групп сборщиков данных) и хранящиеся в файлах.

Объекты и счетчики производительности

Средства мониторинга получают информацию о производительности от многих компонентов операционной системы, которые в ходе своей работы генерируют данные о производительности. Такие компоненты называются *объектами производительности*. В операционной системе имеется стандартный набор объектов производительности, обычно соответствующих главным аппаратным компонентам, таким как память, процессоры и т. д. Приложения могут также инсталлировать свои объекты производительности. В Windows Server 2008 количество объектов, производительность которых можно отслеживать, исчисляется многими десятками.

Каждый объект производительности реализует так называемые *счетчики* (counter), которые собирают данные, характеризующие работу данного объекта. Например, счетчик *Pages/sec* (Обмен страниц в сек) объекта Memory (Память) отслеживает степень кэширования страниц.

В системах Windows Server 2008 значительно увеличено число объектов, производительность которых можно отслеживать (их более 80).

Чаще всего для отслеживания работы системных компонентов используются следующие объекты:

- Cache (Кэш)
- Memory (Память)
- Objects (Объекты)
- Paging File (Файл подкачки)
- PhysicalDisk (Физический диск)
- Process (Процесс)
- Processor (Процессор)
- Server (Сервер)
- System (Система)
- Thread (Поток)

Чтобы увидеть подробное описание данных, которые предоставляет конкретный счетчик, установите флажок **Show Description** (Отображать описание) в диалоговом окне добавления счетчиков **Add counters** (Добавить счетчики) (см. рис. 5.22).

Некоторые объекты (такие как Memory (Память) и Server (Сервер)) имеют только один экземпляр, в то время как другие объекты производительности могут иметь множество экземпляров. Если объект имеет множество экземпляров, то можно добавить счетчики для отслеживания статистики по каждому экземпляру отдельно или для всех экземпляров одновременно.

Например, если в системе установлено несколько процессоров, то объект Processor (Процессор) будет иметь множество экземпляров. Более того, если объект поддерживает множество экземпляров, то при объединении экземпляров в группу появятся родительский экземпляр и дочерние экземпляры, которые будут принадлежать данному родительскому экземпляру.

Настройка счетчиков

В окне компонента Performance Monitor показания счетчиков отображаются в виде графиков или диаграмм. В системах Windows Server 2008 по умолчанию отображается текущая активность процессора, и окно монитора изначально содержит только один счетчик: *% Processor Time* (% загруженности процессора) (объект Processor (Процессор)). Для добавления других счетчиков выполните следующие действия:

1. На панели результатов щелкните правой кнопкой мыши и в контекстном меню выберите команду **Add Counters** (Добавить счетчики). Другой подход — нажать кнопку **Add** (Добавить) (изображение знака "плюс" на панели инструментов) или клавиш <Ctrl>+<I>.
2. В открывшемся окне (рис. 5.22) укажите компьютер, с которого будут собираться показания счетчиков, в списке **Select counters from computer**

(Выбрать счетчики с компьютера). По умолчанию указан локальный компьютер.

3. В списке объектов выберите объект для мониторинга. Чтобы указать конкретный счетчик, нужно дважды щелкнуть по названию объекта, после чего появится перечень счетчиков, относящихся к этому объекту. Если объект имеет несколько экземпляров, выберите нужный в списке **Instances of selected object** (Экземпляры выбранного объекта).
4. Для добавления выбранного счетчика нажмите кнопку **Add** (Добавить).
5. Когда все нужные счетчики будут добавлены, закройте окно, нажав кнопку **OK**.

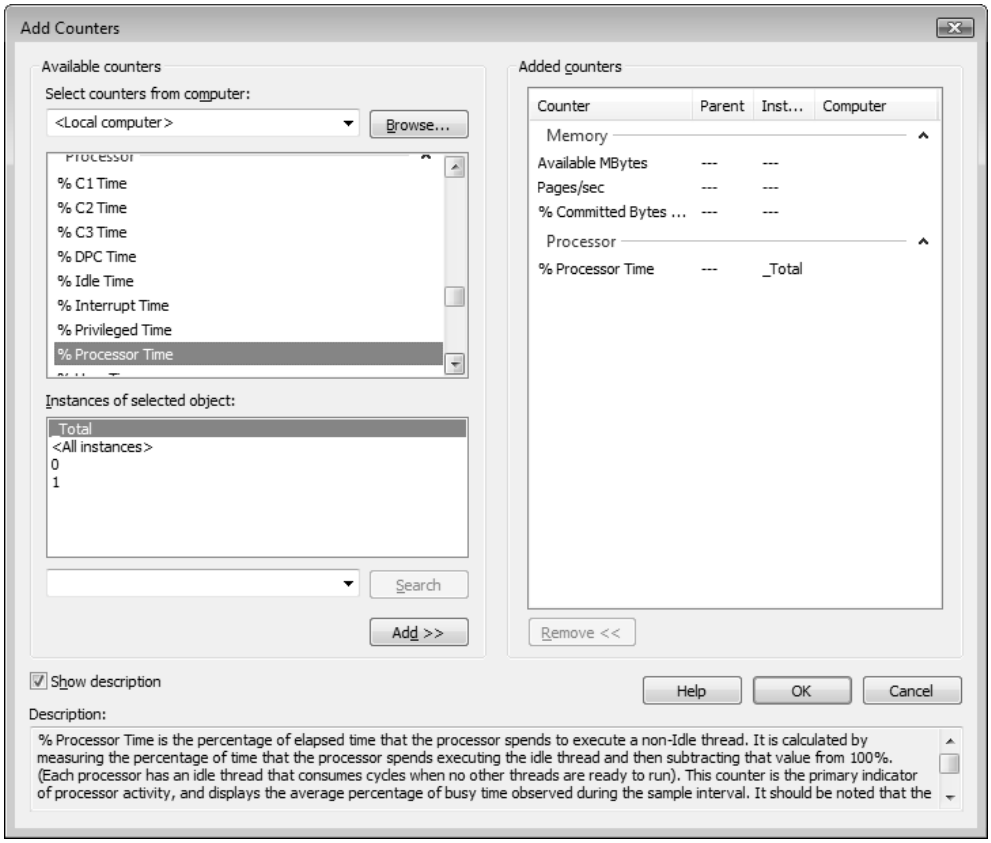


Рис. 5.22. Диалоговое окно для выбора объектов, счетчиков и экземпляров объектов для мониторинга

На рис. 5.23 показан пример окна системного монитора с диаграммами, представляющими изменение значений некоторых выбранных счетчиков. Для того чтобы график для добавленного счетчика был наглядно виден в окне и не выходил за его пределы, можно выделить название одного или нескольких счетчиков в списке и выполнить команду **Scale Selected Counters** (Масштабировать выделенные счетчики), выбрав ее в контекстном меню окна монитора. Также можно менять цвет и тип линии счетчиков *(см. далее)*.

Если навести курсор на график, отображающийся в окне монитора, то можно увидеть его название, значение и показания часов в выбранной точке. Эта информация полезна при анализе графиков, особенно если их много на экране.

Нажав на панели инструментов системного монитора кнопку **View Log Data** (Просмотр данных журнала), можно открыть для просмотра *сохраненные* файлы журналов, содержащие счетчики, выбранные ранее с помощью компонента Data Collector Sets (Групп сборщиков данных) *(см. далее)*.

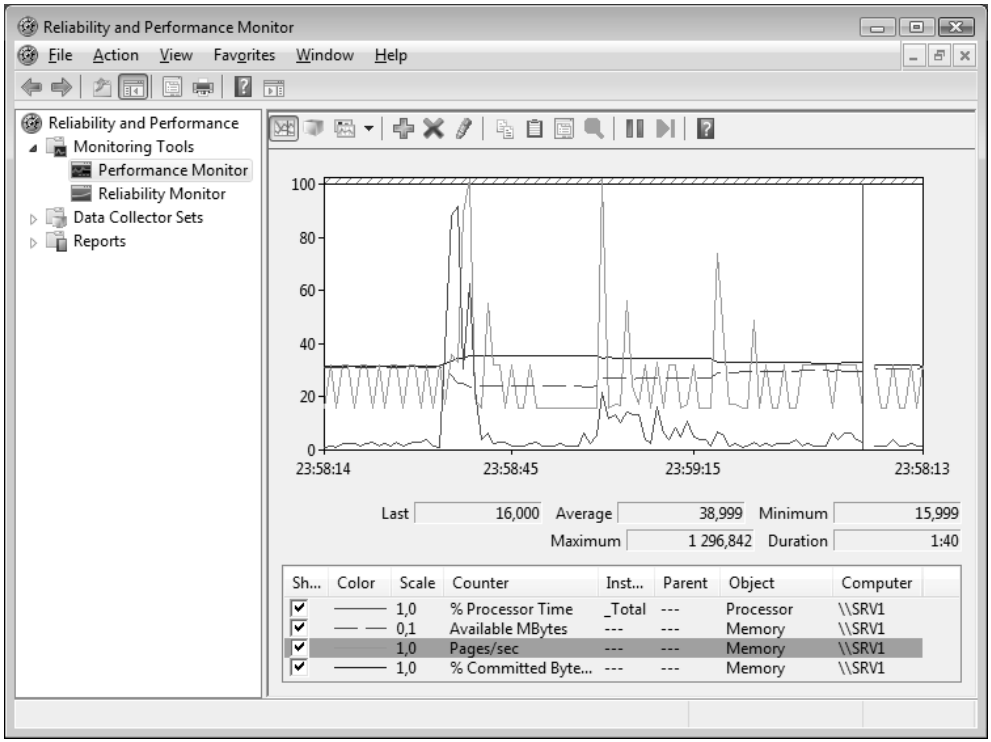


Рис. 5.23. Окно компонента Performance Monitor с активизированными счетчиками

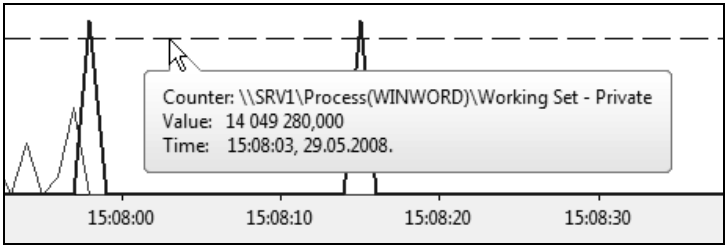


Рис. 5.24. Получение информации о графике, выбранном в окне системного монитора

Мониторинг процессов и приложений

Важной задачей мониторинга серверов является сбор информации о степени использования ресурсов для системных процессов или прикладных программ, выполняющихся на компьютере.

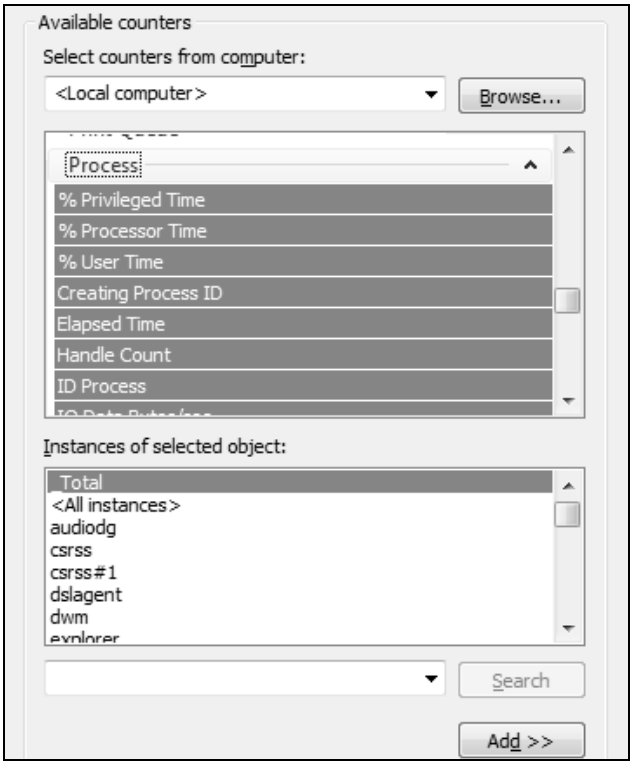


Рис. 5.25. Выбор счетчиков для системных процессов и прикладных программ

Например, проблема обнаружения "утечки памяти" при работе неправильно спроектированного приложения требует длительного слежения за объемом памяти, выделяемой данной программе. Иногда может быть важным, какую нагрузку на систему оказывают стандартные сервисы, например, служба индексирования Windows Search или другие постоянно активные приложения.

Для решения подобных задач используется объект производительности Process (Процесс). Если его выбрать в перечне имеющихся счетчиков (рис. 5.25), то можно видеть, что в списке экземпляров данного объекта присутствуют имена всех процессов (системных служб и прикладных программ), запущенных на компьютере в данный момент. Для любого из них можно выбрать нужные счетчики и добавить их в окно системного монитора.

Настройка способов представления информации

Компонент Performance Monitor (Системный монитор) предоставляет три способа просмотра информации о производительности системы: два графических (**Line** (Строка[1]) и **Histogram bar** (Линейчатая гистограмма)) и одно текстовое (**Report** (Отчет)). Выбор способа представления осуществляется с помощью раскрывающегося списка на панели инструментов (например, на рис. 5.23 выбрана опция **Line** (Строка)).

Для настройки внешнего вида окна мониторинга щелкните правой кнопкой мыши в окне диаграмм и выберите пункт **Properties** (Свойства). Можно просто дважды щелкнуть по имени счетчика в списке, расположенном в нижней части окна, — в этом случае в открывающемся окне будет выделен именно этот счетчик и можно менять параметры представления соответствующего графика.

В окне свойств системного монитора (рис. 5.26) на нескольких вкладках для графика и гистограммы можно задать ряд дополнительных параметров отображения:

- название графика или гистограммы; можно также дать название осям координат;
- диапазон и, главное, масштаб (Scale) выводимых значений (правильный масштаб необходим для того, чтобы график значений был виден или помещался в окне монитора; для автоматического выбора можно также ис-

[1] Непонятно, почему "строка", ведь line — это еще и "линия, график" (что много ближе по смыслу).

пользовать команду **Scale Selected Counters** (Масштабировать выделенные счетчики) — *см. выше*);

- характеристики графиков на диаграмме или колонок на гистограмме (например, для линий — цвет (**Color**), толщина (**Width**) и стиль (**Style**)).

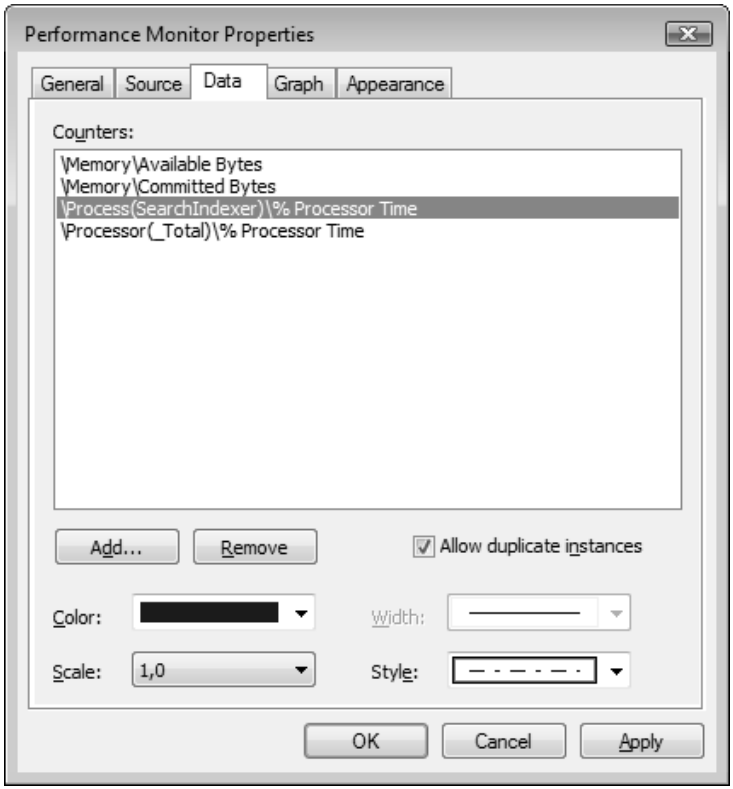


Рис. 5.26. Окно выбора вида отображаемых графиков и гистограмм

Оснастка *Reliability Monitor* (Монитор стабильности стабильности системы)

В системах Windows Vusta/Windows Server 2008 появилось совершенно новое средство, позволяющее анализировать общую стабильность работы системы и находить ее "слабые места" — это оснастка **Reliability Monitor** (Монитор стабильности системы), которая входит в состав оснастки **Reliability**

and Performance Monitor (Монитор производительности и стабильности), но может использоваться и автономно (если ее подключить к пользовательской консоли MMC).

> ***Внимание!***
>
> Данная программа требовательна к показаниям системных часов! В случае принудительной смены даты и значительной корректировки времени в процессе эксплуатации системы есть риск потерять всю ранее накопленную информацию, и проследить историю изменения стабильности системы будет невозможно.

Оснастка **Reliability Monitor** (Монитор стабильности системы) отслеживает системные события (ошибки и предупреждения), относящиеся к области надежности работы системы, и по результатам их анализа строит график стабильности системы, в котором приводится общий индекс стабильности и указывается, в какой из пяти проблемных областей были ошибки (рис. 5.27):

- *Software (Un)Installs* (Установка или удаление программ) — установка и удаление компонентов операционной системы, обновлений Windows, драйверов и приложений;
- *Application Failures* (Ошибки приложений) — "зависания" и крах приложений, принудительное завершение неотвечающих приложений;
- *Hardware Failures* (Неполадки оборудования) — отказы жесткого диска и ошибки памяти;
- *Windows Failures* (Неполадки Windows) — крах операционной системы, ошибки загрузки и выхода из спящего режима;
- *Miscellaneous Failures* (Разные неполадки) — различные ошибки и отказы, не относящиеся к уже перечисленным группам.

Если система работает идеально, то индекс равен 10 (такого практически не бывает). В зависимости от серьезности возникающих проблем или неисправностей программа снижает индекс, и его изменения в течение определенного промежутка времени видны на диаграмме.

В нижней части окна программы на раскрывающихся панелях отображается подробная информация о регистрируемом событии, например, для группы событий "Ошибки приложений" указывается имя программы, ее версия и тип отказа. Такую информацию можно получить по каждой из проблемных областей.

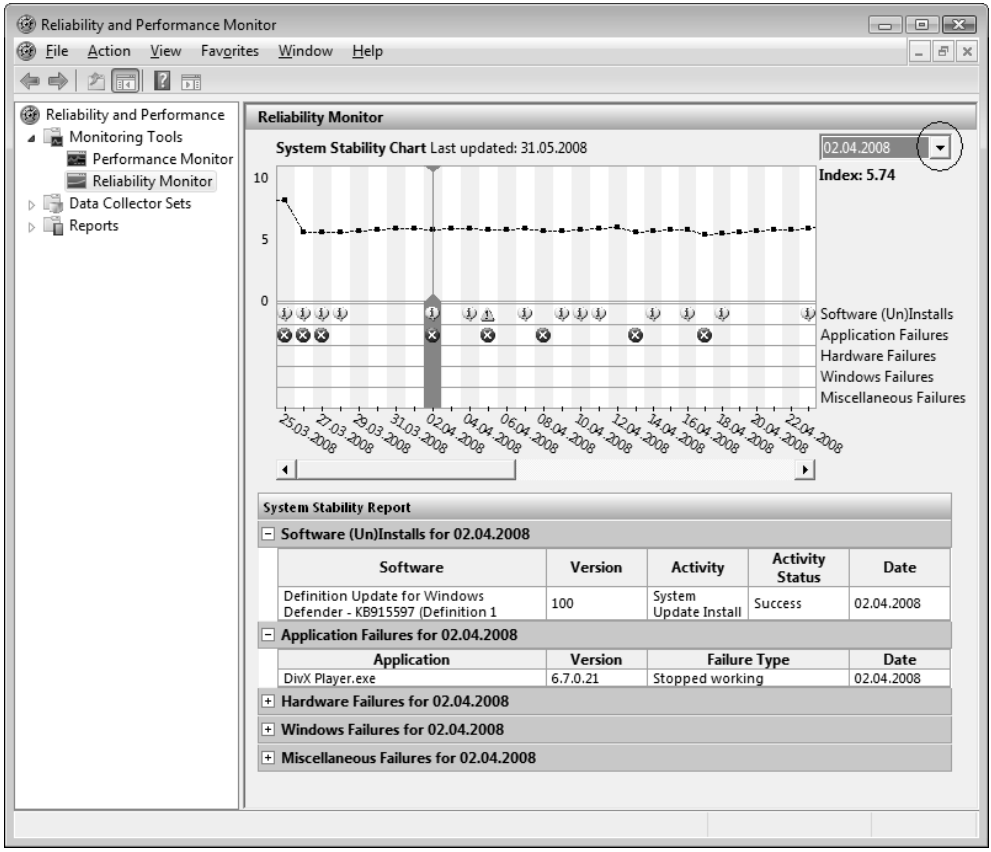


Рис. 5.27. Отображение стабильности системы на некотором временном отрезке

По умолчанию отображаются данные на текущий день. Курсором можно выбрать любую дату, отображенную на графике. Если щелкнуть по стрелке, расположенной в правом верхнем углу окна программы рядом с текущей датой, можно выбрать одну из двух команд:

- **Select All** (Выделить все) — для каждой проблемной области будут отображаться все события, произошедшие за время эксплуатации системы;
- **Select a date** (Выберите дату) — позволяет с помощью выбора в календаре быстро перейти к конкретной дате, не отображаемой на данный момент в окне.

На основании показаний монитора стабильности администратор может быстро оценить, как работает система и какие факторы влияют на ее надежность.

Например, анализируя результаты, показанные на рис. 5.27, можно сразу сказать, что все неисправности были связаны с ошибками прикладных программ (Application Failtures).

Компонент Data Collector Sets (Группы сборщиков данных)

Компонент *Data Collector Sets* (Группы сборщиков данных) можно рассматривать как аналог оснастки **Performance Logs and Alerts** (Журналы и оповещения производительности), имеющейся в системах Windows XP/Windows Server 2003. Он позволяет объединять счетчики производительности в единые логические наборы, которые можно затем использовать для создания журналов, просматриваемых в окне системного монитора или для сбора данных о производительности с удаленного компьютера. Полученные данные можно также экспортировать в электронные таблицы или базы данных для последующего анализа и создания отчетов.

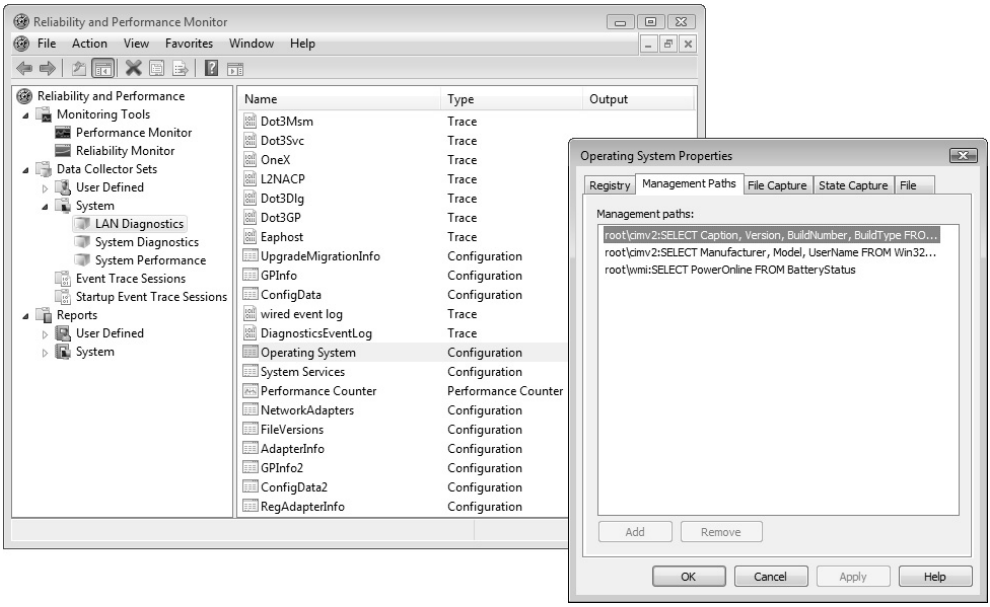
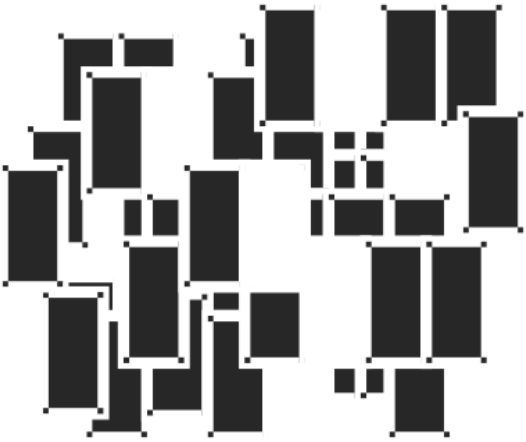


Рис. 5.28. Список стандартных системных групп сборщиков данных

Группы сборщиков данных могут создаваться вручную или с помощью специальных программ-мастеров, которые ориентированы на типовые задачи, возникающие в ходе эксплуатации системы и представляющие интерес для IP-специалистов. Имеются и уже готовые, *системные*, группы сборщиков (рис. 5.28), расположенные в папке **System** (Системный). В правой половине окна перечислены имена конкретных сборщиков данных, входящие в группу; их можно удалять и добавлять. Дважды щелкнув по названию сборщика данных, можно перейти в окно его свойств и просмотреть используемые параметры.

Группы сборщиков, создаваемые самим администратором, помещаются в папке **User Defined** (Особый) (см. рис. 5.28); при создании используется программа-мастер и различные шаблоны. В качестве группы сборщиков данных можно сохранить текущий набор счетчиков, показания которых отображаются в окне компонента Performance Monitor. Для этого нужно выбрать имя компонента в окне оснастки **Reliability and Performance Monitor** (Монитор производительности и стабильности), щелкнуть правой кнопкой мыши и в контекстном меню выполнить команду **New** | **Data Collector Set** (Создать | Группа сборщиков данных).

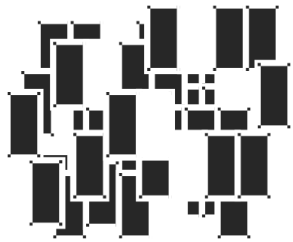
С помощью групп сборщиков данных можно также определять действия, которые будут выполняться в том случае, если некоторый счетчик производительности превысит заданное значение — в этом случае может генерироваться предупреждение или запускаться некоторая задача, предписанная администратором.



ЧАСТЬ II

Использование системных приложений и служб

Глава 6



Встроенные приложения Windows Server 2008

В этой главе рассматриваются полезные, а иногда просто необходимые, средства систем Windows Server 2008, которые могут использоваться при выполнении самых разных задач администрирования или эксплуатации компьютеров. Речь пойдет о стандартных возможностях записи оптических CD- и DVD-дисков; окне консоли, которое служит средой для выполнения всех системных утилит, и возможностях выполнения сценариев, полезных для решения объемных или рутинных задач сопровождения систем, особенно при работе с множеством компьютеров, входящих в домены Active Directory. Перечисленные средства должны быть хорошо знакомы любому администратору.

Запись данных на CD- и DVD-диски

Для записи CD- и DVD-дисков различных форматов существует множество программ от сторонних производителей, однако при выполнении повседневных задач вполне можно довольствоваться возможностями стандартных компонентов операционных систем Windows, которые уже много лет имеют встроенные средства записи CD-дисков (в том числе и аудио-CD). Системы Windows Vista/Windows Server 2008 отличаются тем, что в них реализована запись на DVD-диски (в Windows Vista также имеются стандартные программы, позволяющие создавать DVD-диски с фильмами и слайдами).

Записываемые (CD-R/DVD-R/DVD+R) и перезаписываемые (CD-RW/DVD-RW/DVD+RW) диски позволяют достаточно надежно хранить большие объемы информации, что важно при создании архивных копий пользовательских

файлов и данных прикладных программ. В составе систем Windows Server 2008 сохранен проигрыватель Windows Media Player, с помощью которого также можно записывать аудиодиски.

Возможность записи DVD-дисков имеется и у программы Windows Server Backup (Система архивации данных Windows Server) *(см. главу 15)*.

По сравнению с клиентскими версиями Windows, возможности серверных систем намного скромнее (что, впрочем, вполне естественно). В табл. 6.1 перечислены операции, которые можно выполнять с помощью встроенных средств Windows Server 2008 (прочерк в таблице означает отсутствие функции в данной программе).

Таблица 6.1. *Возможности стандартных программ записи, входящих в состав Windows Server 2008*

Программа	Запись CD /Файловая система	Запись DVD /Файловая система	Стирание дисков CD-RW/DVD-RW
Операционная система	CD с данными (возможность дозаписи) /UDF	DVD с данными* /UDF	CD и DVD; форматирование в UDF
Проигрыватель Windows Media (Windows Media Player) 11.0	Аудио-CD/CDFS и CD с данными/UDF	DVD с данными /UDF	—

*Дозапись возможна только при использовании файловой системы Live (Live File System).

В системах Windows Vista/Windows Server 2008 практически отказались от использования файловой системы CDFS на CD-болванках с мультисессионной записью — чаще используется файловая система UDF, позволяющая стирать и дозаписывать файлы. Благодаря мультисессионной записи (режим append session), можно несколько раз дозаписывать файлы на один диск (включая болванки с однократной записью). Однако при этом возникают издержки: каждая новая сессия требует дополнительно 15—17 Мбайт для записи служебной информации. Аудио-CD пишутся за одну сессию и "закрываются" (finalize), поэтому на них новые треки добавить нельзя. CDFS-диски с

данными всегда остаются с "открытой" сессией, и стандартными средствами системы их закрыть нельзя.

Системы Windows XP и Windows Server 2003 могут читать любые DVD-диски (при использовании версии UDF версий 1.5, 2.0 и 2.01), записанные в Windows Vista/Windows Server 2008.

Системы Windows Vista/Windows Server 2008 позволяют дозаписывать файлы на CD-болванки с файловой системой CDFS, однако при этом CDFS-диск преобразуется в UDF-диск, записываемый в режиме Mastered — системы предыдущих версий свободно такие диски читают, но не могут выполнять на них запись. Таким образом, совместимость CD-дисков в плане возможностей записи получается односторонняя.

Внимание!

При записи CD- и DVD-дисков могут создаваться файлы больших размеров (до нескольких гигабайт) или требуется буферная область. Поэтому нужно следить за наличием свободного места на жестком диске (дисках) и обратить внимание на все рекомендации, касающиеся выбора папок для временного хранения файлов. Некоторые программы используют при своей работе папки, определяемые значениями системных переменных `TMP` и `TEMP` (эти переменные задаются как для системы, так и для каждого пользователя).

Примечание

Для операционной системы не имеет значения технология изготовления DVD-дисков: с одинаковым успехом могут использоваться как "плюсовые" (DVD+R и DVD+RW), так и "минусовые" (DVD-R и DVD-RW) болванки. Все определяется только возможностями установленного привода.

Особенности записи файлов с длинными именами

Файловая система CDFS[1], применяемая на CD-дисках, не позволяет использовать очень длинные имена файлов (которые допустимы в файловых систе-

[1] Точнее, стандарт называется *ISO 9660*, однако для простоты и однозначности мы будем везде использовать именно аббревиатуру CDFS, поскольку она повсеместно встречается в пользовательском интерфейсе Windows.

мах на жестких дисках), и при записи таких файлов имена обрезаются до 64 символов (учитываются само имя, символ точки и расширение). Это правило относится ко всем программам. Если имя файла превышает по длине 64 символа, то сохраняется его расширение, а от имени берутся только начальные символы — столько, сколько возможно, чтобы общая длина не превысила 64 (остальные символы имени просто отбрасываются).

Все встроенные средства систем Windows Vista/Windows Server 2008 (это относится и к семейству Windows XP) допускают использование *диакритических* символов (символов, имеющих дополнительные точки и черточки над изображением буквы — á, ä, â и т. п.) в именах файлов, причем эти символы сохраняются при записи на CD- и DVD-диски (с *любыми* используемыми файловыми системами).

Предположим, что два файла имеют длинные имена, у которых 60 и более первых (расположенных слева) символов совпадают, а отличаются только символы, расположенные в самом конце. При записи на CD-диск такие имена будут "обрезаться" до какой-то позиции (это еще зависит от длины расширения файлов, которое может быть коротким или длинным), и окажется, что усеченные имена файлов будут совпадать. Подобные конфликты автоматически устраняются при записи: от имен файлов остается максимально возможное количество символов, к которым добавляется числовой суффикс (1), (2), (3), ... и т. д. Тем самым обеспечивается уникальность имен.

Для CD- и DVD-дисков, отформатированных с использованием файловой системы UDF (Universal Disk Format), ограничения не такие строгие, как для CDFS. На CD-дисках, записанных в режиме Mastered *(см. след. разд.)*, имя файла может иметь максимальную длину, равную 108 (включая символ точки и расширение). Длина имени файла, отправляемого на запись, не может превышать 200 символов, причем уже в процессе записи имена будут при необходимости обрезаны до 108 символов. В случае возникновения конфликта (если первые 108 символов имен файлов совпадают) к укороченным именам автоматически добавляются суффиксы ~1, ~2, ~3, ... и т. д.

При использовании файловой системы *Live File System* длина имен файлов может достигать 254 символа включительно — как на CD-, так и на DVD-дисках. (Сама файловая система NTFS допускает на жестких дисках максимальную длину *полного* имени файла, равную 255 символам.) Конфликты имен в этом случае невозможны, поскольку (в отличие от режима Mastered) проверяемая перед записью допустимая длина имени *точно* соответствует ограничениям файловой системы Live, а на жестком диске файлы с одинаковыми именами появиться не могут.

Новые возможности записи и форматы дисков в Windows Server 2008

Пользователи систем Windows Vista/Windows Server 2008 могут сохранять файлы любого типа не только на уже традиционных CD-R/CD-RW-дисках, но и на DVD-дисках любого типа (разумеется, при наличии соответствующего привода). В Windows Server 2008 запись информации может осуществляться непосредственно из программы Windows Explorer (Проводник), а также с помощью проигрывателя Windows Media Player 11.0, который может устанавливаться в составе компонента *Desktop Experience* (Возможности рабочего стола). (В различных версиях Windows Vista возможности записи имеют также программы Windows Movie Maker (только на CD-диски), Windows DVD Maker (DVD-студия Windows) и оболочка Windows Media Center.)

Для записи в системах Windows Vista/Windows Server 2008 преимущественно используется формат *UDF* (Universal Disk Format) — это касается и CD-, и DVD-дисков. Файловая система UDF удобна тем, что данные на диск можно записывать многократно, как на обычный жесткий диск или флэш-накопитель, а с перезаписываемых дисков файлы можно также удалять (при этом занятое место освобождается). В пользовательском интерфейсе Windows Vista/Windows Server 2008 для обозначения особого режима использования формата UDF применен новый термин — *живая файловая система* (файловая система Live, Live File System).

> ***Примечание***
>
> Любые диски (CD и DVD) записываются системами Windows Vista/Windows Server 2008 с использованием файловой системы UDF — это касается обоих возможных режимов записи *(см. след. разд.)*. Однако реализованы эти режимы по-разному, в результате чего диски с файловой системой Live могут не распознаваться на старых компьютерах или бытовых плеерах, а диски, записанные в режиме Mastered, воспринимаются нормально. Для того чтобы избежать путаницы в режимах записи, и введены разные термины для обозначения модификаций файловой системы.

Настройка режима использования пишущего привода (CD или DVD) выполняется на вкладке **Recording** (Запись) в окне свойств устройства (рис. 6.1). Убедитесь в том, что на диске, выбранном для размещения *образа* (image) записываемого диска, имеется достаточно много свободного пространства (не менее 1 Гбайт для аудиодисков и 5 Гбайт для DVD-дисков); система автоматически предлагает диск, где наибольшее незанятое пространство. Флажок **Automatically eject the disc after a Mastered burn** (Автоматически из-

влекать диск после записи ISO-диска) определяет необходимость извлечения диска из привода после записи в режиме Mastered; диски с файловой системой Live всегда остаются в приводе. Кнопка **Global Settings** (Общие параметры) открывает окно (рис. 6.2), в котором можно определить режим записи последней сессии на UDF-диске.

Рис. 6.1. Окно выбора параметров для записи компакт-дисков

Помимо образа диска, необходимо предусмотреть место для временного хранения файлов, выбранных для записи в режиме Mastered. Все файлы в этом случае сначала копируются в папку "C:\Users\<*имяПользователя*>\AppData\Local\Microsoft\Windows\Burn\ Burn" (Temporary Burn Folder (Временная папка для записи)) (проверьте, достаточно ли свободного места на диске!). После того как записан один диск, операцию можно повторить с теми же

файлами. Только после того, как пользователь полностью завершит процедуру копирования файлов на оптический диск, буфер очищается.

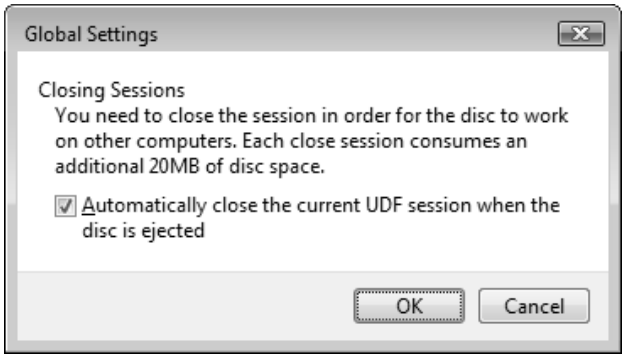


Рис. 6.2. Определение режима закрытия сеансов UDF

Выбор формата дисков и форматирование

Для записываемых и перезаписываемых CD- и DVD-дисков большое значение имеет тип файловой системы, выбранный для работы с ними (если диск новый или пустой, то встроенные программы автоматически определяют нужный им формат и дополнительные действия со стороны пользователя не требуются).

При установке в приводе пустой записываемой или перезаписываемой болванки на мониторе автоматически появляется окно (рис. 6.3), в котором нужно указать способ использования диска[1]. (В нашем примере показан DVD-диск, однако для CD-дисков окно будет аналогичным, немного изменится лишь набор опций.) Если установить флажок **Always do this for blank DVDs** (Всегда выполнять для чистых DVD) (или CD), выбранная операция будет всегда выполняться с пустыми дисками и окно запроса опций появляться не будет.

Выбор опции **Burn files to disc using Windows** (Записать файлы на диск используя Windows) означает, что запись на диск будет осуществляться с по-

[1] Если в системы установлены сторонние приложения, выполняющие запись на CD/DVD, то в этом окне могут появляться дополнительные опции, определяемые возможностями этих программ.

мощью стандартных встроенных средств системы, и на следующем шаге появится окно подготовки диска к записи (рис. 6.4). В этом окне можно ввести метку диска (по умолчанию предлагается текущая дата), а самое главное — нужно выбрать тип диска (файловую систему).

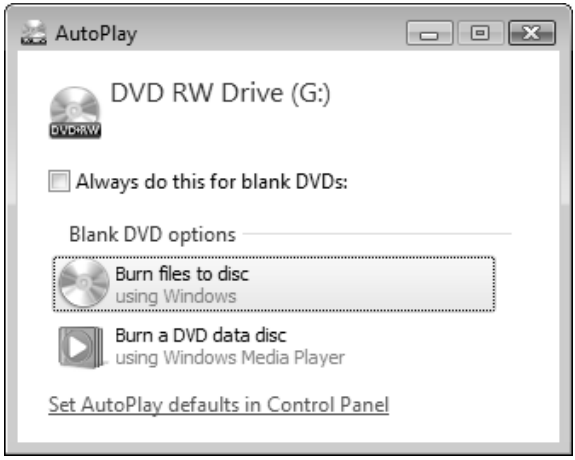


Рис. 6.3. Выбор операции, выполняющейся с пустым DVD-диском

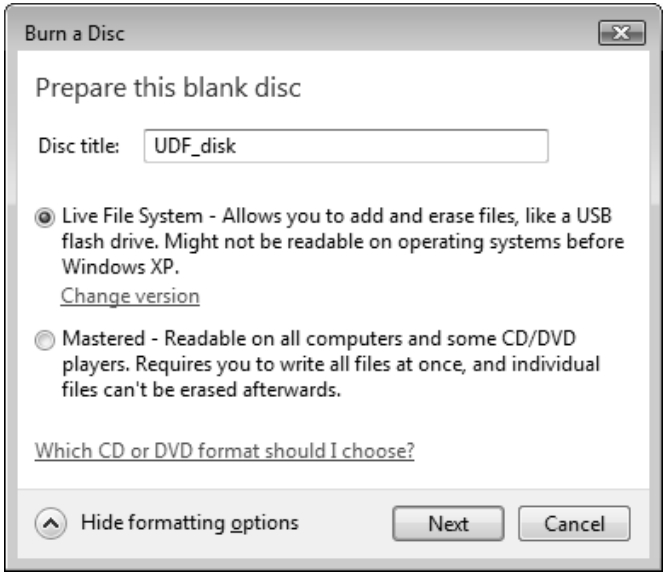


Рис. 6.4. Выбор типа файловой системы для нового CD- или DVD-диска

- *Live File System* (Живая файловая система, файловая система Live) удобна тем, что данные на диск можно записывать многократно (даже на диски CD-R/DVD-R с однократной записью), как на обычный жесткий диск или флэш-накопитель (на перезаписываемых дисках файлы можно также удалять). Кроме того, в этом случае можно использовать имена файлов максимальной допустимой длины и нет ограничений в именах файлов; файлы можно удалять или переименовывать.

  CD- и DVD-диски с использованием файловой системы Live рекомендуется применять для архивации файлов относительно небольшого объема и в тех случаях, когда информацию нужно переносить между компьютерами. Для DVD-дисков этот режим предпочтителен, поскольку он допускает дописывание файлов и на таких дисках всегда возможно быстрое форматирование. (На CD-дисках при выборе файловой системы Live всегда выполняется *полное* форматирование в UDF, что требует много времени).

- Формат *Mastered* [1] — как на CD-, так и на DVD-дисках — предпочтителен в тех случаях, когда за один раз записывается большой объем данных, и эти данные должны быть доступны на бытовых устройствах или на компьютерах с другими системами (не Windows или системами, не поддерживающими UDF). В этом случае для CD-дисков все равно используется файловая система UDF, но выполняется мультисессионная запись, в чем-то напоминающая многократную дозапись в Windows XP. DVD-диски, записанные в режиме Mastered, ***допускают только однократную запись файлов***; добавление файлов, как на CD-дисках, невозможно.

> ***Внимание!***
>
> Диски, записываемые в режиме Mastered, имеют ограничения в именах файлов (например, не допускается символ "точка с запятой"). Поэтому если при выполнении записи возникают ошибки, проверьте, не используются ли в именах какие-то нестандартные символы.

Версию UDF, используемую для форматирования диска, можно изменить, щелкнув по ссылке **Change version** (Сменить версию) и выбрав в списке любую из четырех поддерживаемых версий UDF (рис. 6.5). Версия 2.5 разработана специально для Windows Vista/Windows Server 2008 и может оказаться несовместимой с предыдущими системами Windows. Рекомендуемая версия 2.01 и версия 2.0 совместимы с Windows XP и Windows Server 2003 (они мо-

[1] В русских локализованных версиях эта опция называется *Mastered (ISO)*.

гут вызвать проблемы при использовании с более ранними версиями Windows или другими операционными системами). Версия 1.5 поддерживается системами Windows 2000, Windows XP и Windows Server 2003, но может быть несовместима со старыми версиями Windows (Windows 98) или другими системами.

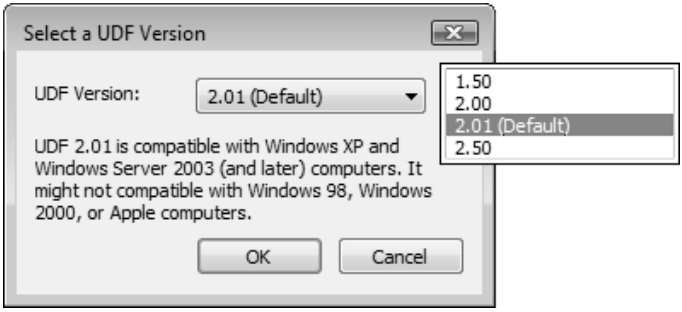


Рис. 6.5. Выбор версии UDF при форматировании новых дисков

Примечание

При форматировании с помощью утилиты format также можно выбирать версию UDF 1.02.

После нажатия кнопки **Next** (Далее) в окне подготовки нового диска (см. рис. 6.4) может появиться предупреждение о том, что операция потребует много времени, и в случае подтверждения операции система анализирует состояние диска и выполняет форматирование (рис. 6.6). Время форматирования зависит от типа болванки. Новые пустые болванки форматируются довольно быстро, как и DVD-диски, на которых *уже была* файловая система UDF. (Возможно ли для диска быстрое форматирование — это проще определить, запустив команду `format` в окне командной строки; *см. далее*.)

Форматирование (а в первую очередь — выбор используемой файловой системы) необходимо для пустых дисков *любого типа* (в том числе и с однократной записью CD-R/DVD-R); повторно форматировать можно только перезаписываемые болванки (это относится и к операции удаления файлов с диска). Необходимость подобной операции отсутствует в предыдущих версиях Windows, поскольку там запись возможна только на CD-диски с файловой системой CDFS.

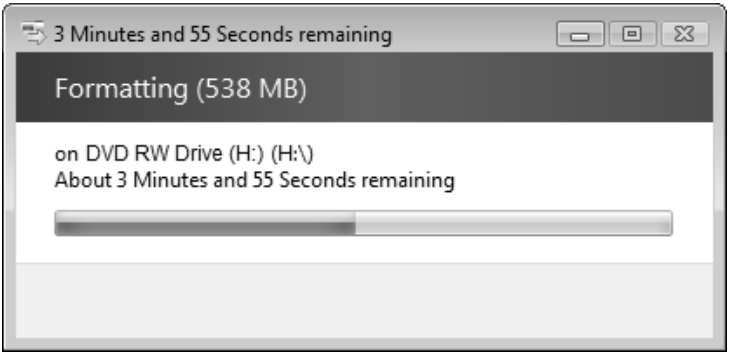


Рис. 6.6. Окно, отображающее ход процесса форматирования диска

Рис. 6.7. Окно выбора параметров форматирования перезаписываемого DVD-диска

Отформатировать диск можно в любой момент, выбрав его в окне программы Windows Explorer (Проводник) и указав в контекстном меню команду **Format** (Форматировать). Перед началом операции форматирования нужно выбрать тип файловой системы и указать метку диска (рис. 6.7). Опция быстрого форматирования (флажок **Quick Format** (Быстрое)) доступна, если только диск уже форматировался с использованием UDF. *Полное* форматирование диска, особенно DVD, может занять несколько десятков минут.

Форматировать диски можно и с помощью системной утилиты `format.exe`; в этом случае проще следить за ходом операции. Обратите внимание на то, что издержки при использовании UDF на CD-болванках довольно велики — из 650 Мбайт остаются доступными только 528084 Кбайт:

```
C:\>format F: /FS:UDF /R:1.50 /V:UDF_disk
The type of the file system is RAW.
The new file system is UDF.

WARNING, ALL DATA ON NON-REMOVABLE DISK
DRIVE F: WILL BE LOST!
Proceed with Format (Y/N)? y
Formatting 538M
A low-level format on this media may take a long time. The drive won't be
usable during this period and it is recommended not to shutdown the ma-
chine until format is complete.
Proceed with low level format (Y/N)? y

Blanking media ...
100 percent completed.
... ... ...
Performing low level format ...
100 percent completed.
... ... ...
Creating file system structures.
Format complete.
    550080 KB total disk space.
    528084 KB are available.
C:\>

(Тип файловой системы: RAW.
Новая файловая система: UDF.
ВНИМАНИЕ, ВСЕ ДАННЫЕ НА НЕСЪЕМНОМ
ДИСКЕ F: БУДУТ УНИЧТОЖЕНЫ!
Приступить к форматированию [Y(да)/N(нет)]?
...
Низкоуровневое форматирование этого носителя может занять много времени.
Диск нельзя использовать в течение этого периода; рекомендуется не выклю-
чать компьютер до завершения форматирования.
Начать низкоуровневое форматирование (Д/Н)?
Очистка носителя:
100 процентов завершено.
...
```

```
Выполнение форматирования на нижнем уровне...
Создание структур файловой системы.
Форматирование окончено.
    550080 КБ всего на диске.
    528084 КБ доступно.)
```

Полное форматирование CD-болванки на скорости 8X занимает около 10 минут вне зависимости от выбранной версии UDF.

Перенос файлов на оптические диски с использованием встроенных возможностей системы

Благодаря наличию встроенной поддержки записываемых CD- и DVD-дисков операции копирования информации на диск можно осуществлять непосредственно из окна программы Windows Explorer (Проводник). Для этого используются обычная операция переноса файлов с помощью мыши, команда **Send To** (Отправить) в контекстном меню файлов и папок, а также кнопка **Burn** (Запись на оптический диск) на панели задач программы Windows Explorer (Проводник), позволяющая быстро отправить выбранный файл или папку в очередь записи или сразу записать на UDF-диск. Размер и количество файлов не имеют значения — все возможности и рабочие операции будут одинаковыми.

Рассмотрим процедуры записи файлов на оптический диск подробно.

Запись на диск с файловой системой Live

Это самый простой и удобный вариант использования встроенных средств системы — запись выбранных файлов на диски с файловой системой Live осуществляется *сразу же* после выполнения команды **Send To** (Отправить) или нажатия кнопки **Burn** (Запись на оптический диск). Однако в случае выполнения операции записи на *пустой* диск сначала появится окно выбора файловой системы (см. рис. 6.4), в котором нужно выбрать опцию **Live File System** (Живая файловая система). В результате будет выполнено форматирование диска (для DVD-болванок эта операция выполняется довольно быстро, а для CD-болванок всегда выполняется полное форматирование; при этом система отображает время, остающееся до окончания операции — см. рис. 6.6).

При выполнении каждой операции копирования файлов система оценивает время, необходимое для завершения операции, и выдает информацию о ходе копирования (рис. 6.8). При большом объеме файлов запись на UDF-диски выполняется не очень быстро, поэтому не торопитесь извлекать диск из привода.

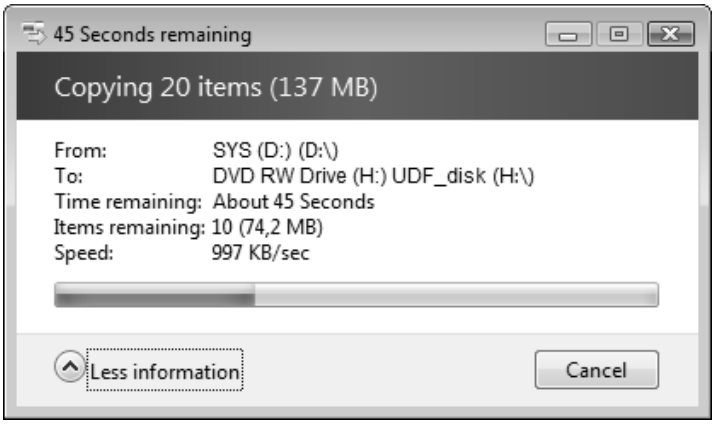


Рис. 6.8. Отображение хода процесса копирования информации на UDF-диск

Применение файловой системы Live позволяет удалять файлы с диска (при этом свободное место на диске увеличивается). Выглядит это так же, как и операция записи на такие диски (рис. 6.9). Удаление файлов происходит очень быстро.

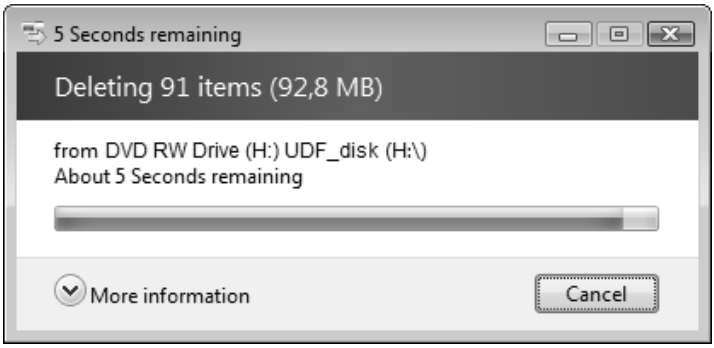


Рис. 6.9. Удаление файлов с перезаписываемого UDF-диска

После завершения операции записи UDF-диск можно извлечь из привода. Не рекомендуется это делать без необходимости, поскольку при закрытии очередной UDF-сессии записи расходуется дисковое пространство.

> ***Внимание!***
>
> Все диски с файловой системой Live будут читаться в любых системах Windows XP и Windows Server 2003. Однако запись *дополнительных* файлов на эти диски невозможна, поскольку указанные системы такого формата не поддерживают — записать информацию на диски можно будет только после их полного стирания (очистки).

Запись в режиме Mastered

Процедура записи файлов в режиме образа диска выглядит следующим образом.

1. Вставьте в пишущий привод пустую болванку или диск, на который уже выполнялась запись, но еще имеется свободное пространство.

> ***Внимание!***
>
> Системы Windows Vista/Windows Server 2008 позволяют дозаписать файлы на CDFS-диски, созданные в Windows XP/Windows Server 2003, однако при этом файловая система CDFS преобразуется в UDF и последующие операции добавления файлов в предыдущих версиях Windows будут невозможны.

2. В окне программы Windows Explorer (Проводник) выделите файлы, которые нужно копировать на компакт-диск. Щелкнув правой кнопкой мыши, откройте контекстное меню и в подменю **Send To** (Отправить) укажите привод компакт-дисков в качестве целевого устройства. Также удобно пользоваться кнопкой **Burn** (Запись на оптический диск) на панели задач программы Windows Explorer (Проводник). (Операцию выбора можно повторять несколько раз — каждый раз все файлы будут копироваться в буферную область.) При выполнении операции будет появляться системное предупреждение, показанное на рис. 6.10. Если щелкнуть мышью по всплывающему окну, то можно увидеть окно, где отображается очередь записи на диск (рис. 6.11).
3. Если диск не был подготовлен к записи, то при первом копировании файлов на устройство записи появится окно выбора типа файловой системы (см. рис. 6.4). Выберите опцию **Mastered** и нажмите кнопку **Next** (Далее).

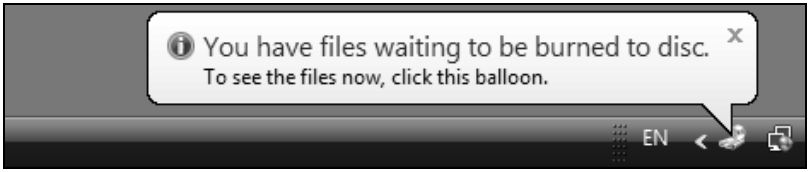


Рис. 6.10. Сообщение, указывающее на наличие файлов в очереди записи на диск

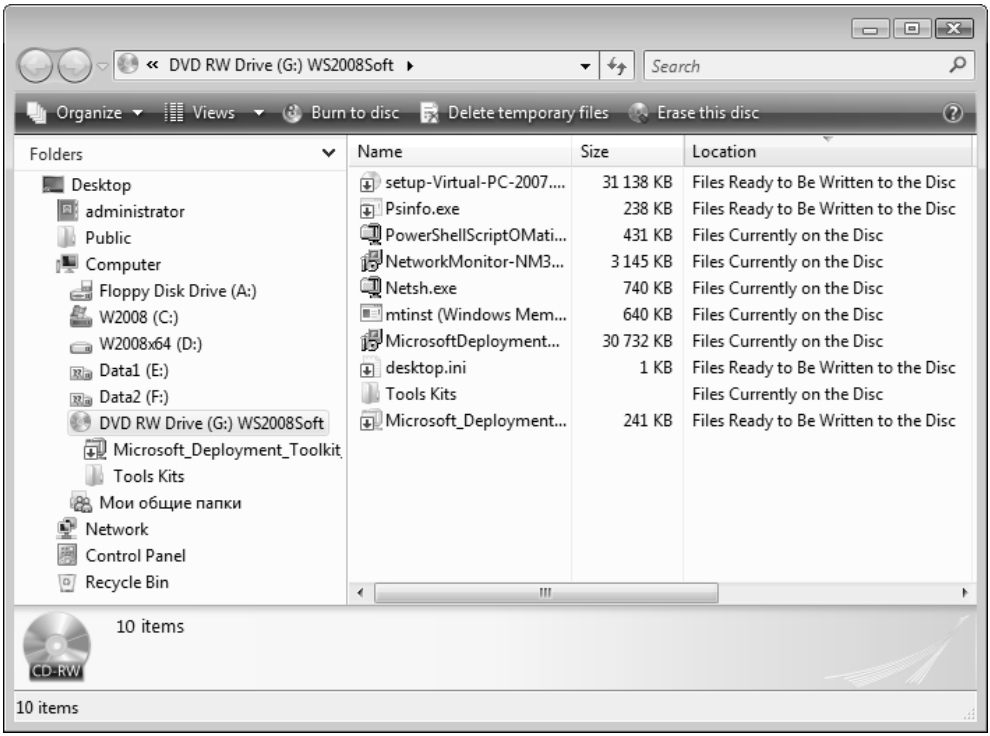


Рис. 6.11. Просмотр списка файлов, подготовленных к записи

4. В окне программы Windows Explorer (Проводник) выберите пишущий привод. В папке устройства значками ярлыков отмечены файлы, предназначенные для записи на диск; также могут отображаться имена файлов, уже находящихся на компакт-диске (поскольку мультисессионная запись позволяет несколько раз добавлять файлы на диск — это возможно только на CD-дисках). Убедитесь в том, что все файлы, которые необходимо скопировать на компакт-диск, отмечены параметром **Files Ready to be**

Written to the Disc (Подготовленные для записи на диск файлы). Это окно лучше всего просматривать в режиме Details (Таблица) (см. рис. 6.11). Прямо в окне можно переименовать файлы или удалить те из них, которые переписывать не нужно (поскольку в списке показаны ссылки на *копии* исходных файлов, хранящихся в буферной папке, операция удаления никак не скажется на самих исходных файлах).

5. Когда *все* файлы, переписываемые на диск, будут определены, выберите пишущий привод и на панели задач программы Windows Explorer (Проводник) нажмите кнопку **Burn to disk** (Запись на компакт-диск) или же выполните команду **Burn to disk** (Записать на диск) в контекстном меню привода. Появится окно (рис. 6.12), в котором можно переопределить имя диска и выбрать скорость записи (с этого момента извлечение диска из провода блокируется). После нажатия кнопки **Next** (Далее) начинается процедура записи: сначала файлы копируются в образ диска, а потом образ пишется на компакт-диск.

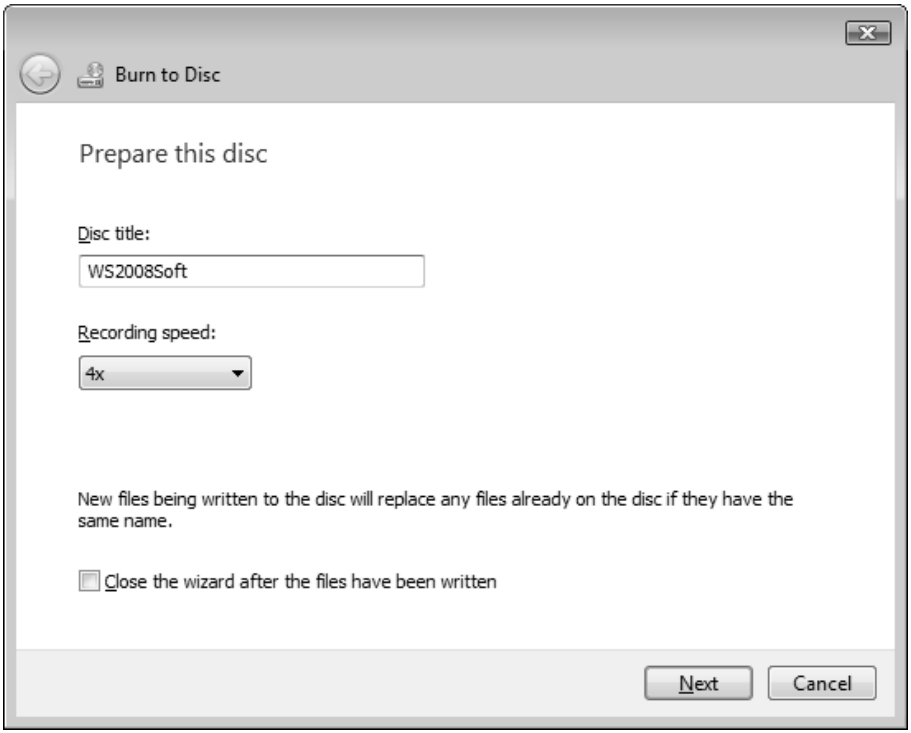


Рис. 6.12. Просмотр нового имени диска перед сеансом записи и выбор параметров

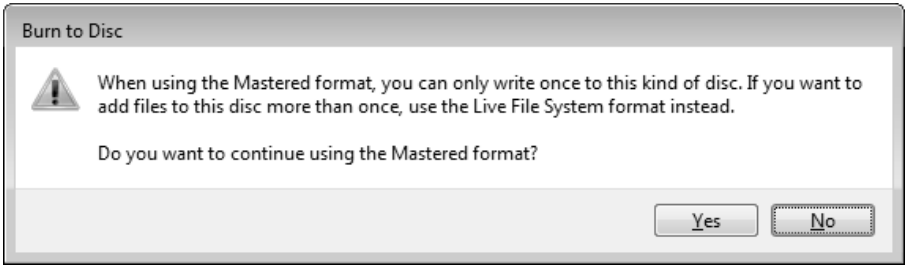


Рис. 6.13. Предупреждение о том, что запись на DVD-диск в режиме Mastered возможна только один раз

Если запись выполняется на DVD-болванку, то появится дополнительное предупреждение (рис. 6.13) о невозможности последующей дозаписи файлов на такой диск (CD-диски в режиме Mastered допускают многократное добавление файлов на уже записанный диск).

За ходом процесса записи можно наблюдать в служебном окне (рис. 6.14). Мы приводим его для того, чтобы подчеркнуть различия между способами записи Mastered-дисков и дисков с файловой системой Live (когда буфер *не* используется). Записанный Mastered-диск по умолчанию извлекается из привода (см. состояние флажка на рис. 6.1).

Появляется запрос на создание еще одной копии файлов, выбранных для копирования на диск. В случае отказа все файлы удаляются из буферной папки (не забывайте о том, что в противном случае в буфере может накопиться много ненужных данных!), и операцию записи можно считать законченной.

Примечание

При записи CD-дисков обратите внимание на то, какая файловая система используется — это всегда будет UDF.

После успешного создания образа диска может возникнуть ошибка непосредственно операции записи (рис. 6.15) (диск при этом извлекается из привода). Такая ситуация может возникнуть в случае проблем с диском — можно попробовать запись с другим диском. Можно вообще отказаться от записи, удалив все временные файлы, хранящиеся в буферной папке. Ошибка возможна из-за проблем с именами файлов, не соответствующих требованиям выбранной файловой системы на оптическом диске. В этом случае можно отложить запись, проверить, присутствуют ли недопустимые символы в именах файлов (см. рис. 6.11), при необходимости исправить имена, отображаемые в виде ссылок в папке устройства записи, и повторить операцию.

В случае ошибки при выборе файлов (папок) или при отмене операции выберите пишущий привод в окне программы Windows Explorer (Проводник) и нажмите на панели задач кнопку **Delete temporary files** (Удалить временные файлы) (после этого выбор файлов можно начать сначала). Будьте внимательны: при отказе от записи всегда нужно удалять временные файлы, поскольку система сохраняет их в буфере даже после перезагрузки компьютера или смене (извлечении) компакт-диска.

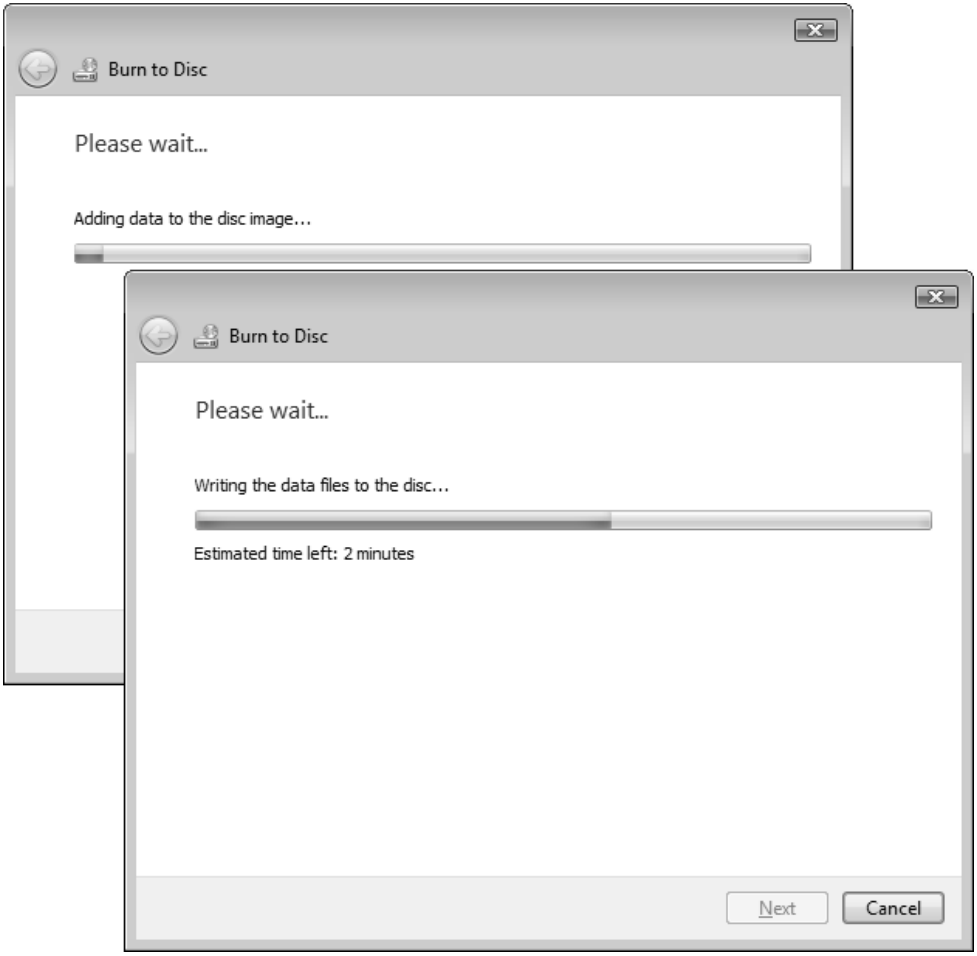


Рис. 6.14. Процесс записи Mastered-диска начинается с создания образа, после этого можно следить за ходом операции записи образа на диск

При записи дисков все необходимые команды — **Burn to disk** (Записать на диск), **Erase this disk** (Стереть этот диск) и **Delete temporary files** (Удалить временные файлы) — можно выполнять и из контекстного меню пишущего привода, выбрав его в окне программы Windows Explorer (Проводник).

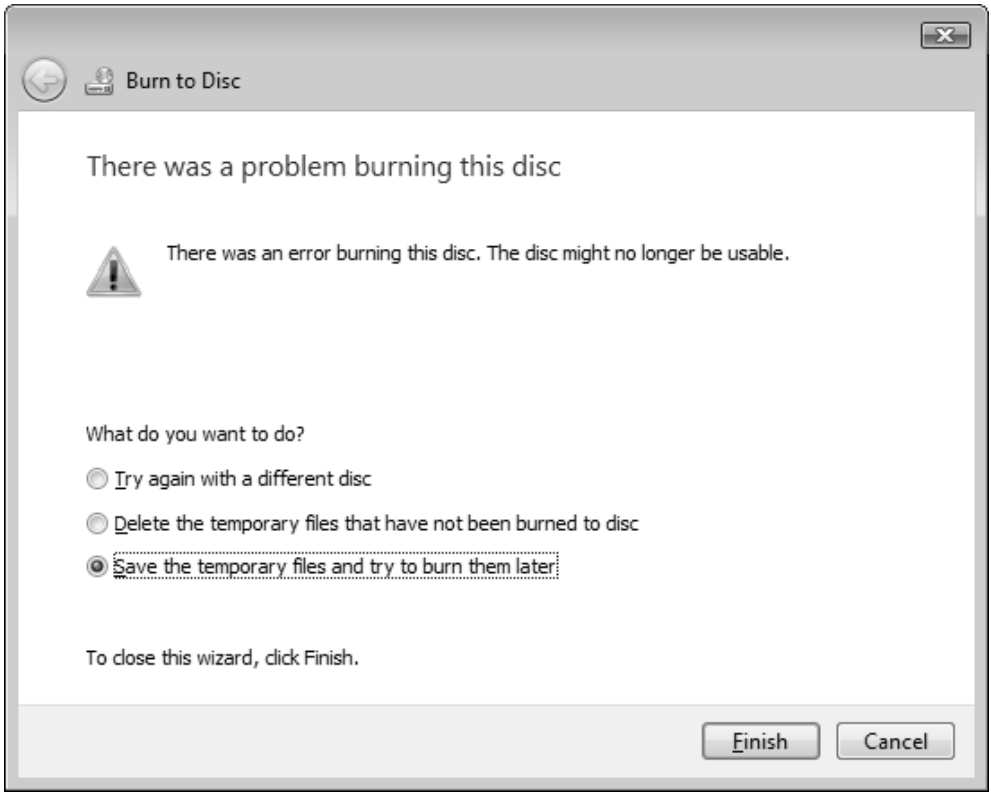


Рис. 6.15. Сообщение об ошибке записи на диск, позволяющее выбрать ответные действия

Стирание дисков

При необходимости перезаписываемый CD- или DVD-диск можно *стереть*, т. е. не просто убрать записанные файла, а удалить с него всю информацию о текущей файловой системе (после этого диск можно записать с применением файловой системы Live или режима Mastered, а также использовать любое

стороннее приложения для записи дисков). С этой целью используется команда **Erase this disk** (Стереть этот диск) в контекстном меню пишущего привода или одноименная кнопка на панели задач в окне программы Windows Explorer (Проводник).

При выполнении команды появится окно мастера стирания диска (рис. 6.16). После нажатия кнопки **Next** (Далее) начинается операция очистки диска, за ходом которой можно следить по бегущему индикатору. Если установить специальный флажок (**Close this wizard after the disc is erased**), то окно мастера автоматически закроется по окончании операции. В противном случае завершать работу мастера нужно вручную, нажав в последнем его окне кнопку **Finish** (Готово).

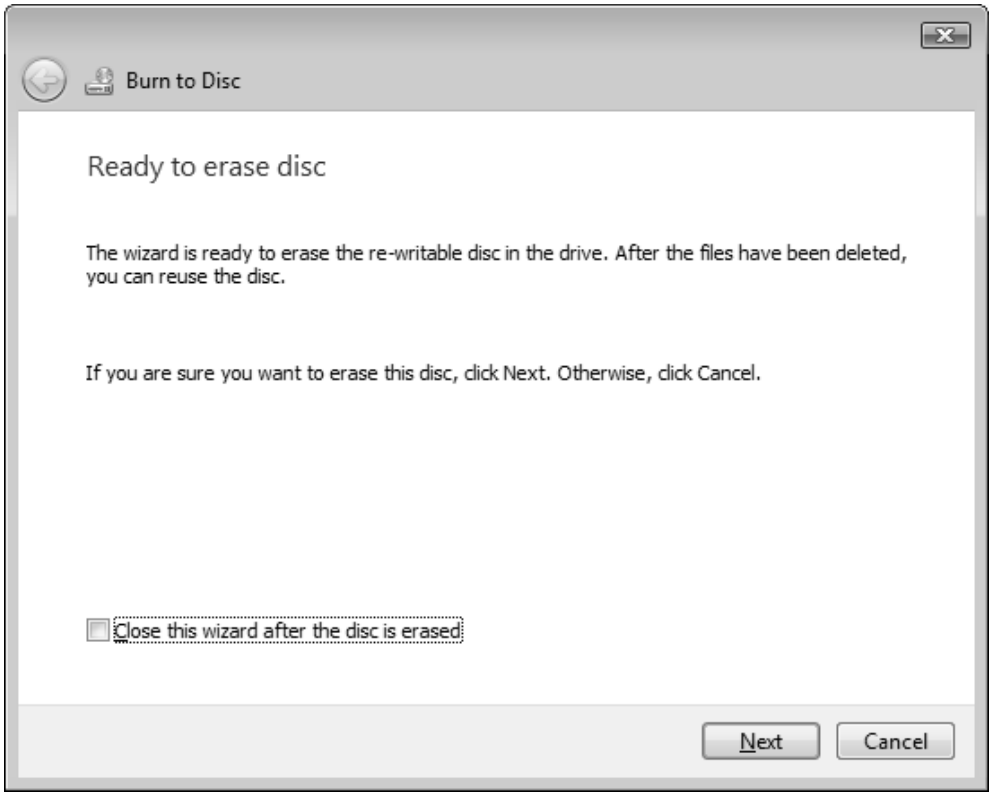


Рис. 6.16. Основное окно мастера стирания дисков

Командная строка (окно консоли)

Сложно сказать, можно ли считать *окно консоли* (окно командной строки) встроенным приложением операционной системы, но совершенно точно то, что администратору невозможно обходиться без него. Поэтому несколько слов необходимо сказать об этой программе.

Примечание

В системах Windows Vista/Windows Server 2008 имеются два командных процессора: консоль команд (процесс cmd.exe) и окно сессии MS-DOS (процесс ntvdm.exe), которое можно открыть, введя в окне **Run** (Выполнить) строку `command.com`. У этих окон разные заголовки (рис. 6.17) и разные возможности.

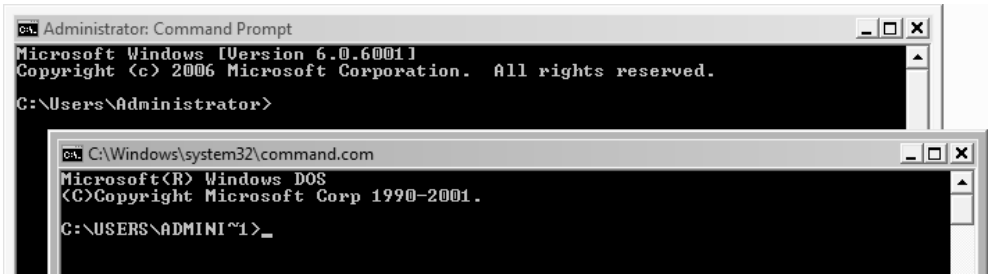


Рис. 6.17. Заголовки окна консоли и окна сессии MS-DOS

Доступ к командной строке (консоли команд) осуществляется с помощью команды **Start** | **All Programs** | **Accessories** | **Command Prompt** (Пуск | Все программы | Стандартные | Командная строка). Можно также просто ввести строку `cmd` в меню **Start** (Пуск) или в окне **Run** (Выполнить).

По заголовку окна консоли можно судить о полномочиях пользователя в данном окне. Если окно запускается с помощью команды **Run as administrator** (Запуск от имени администратора), то в заголовке окна указано **Administrator: Command Prompt** (Администратор: Командная строка) (см. рис. 6.17).

Совет

В системах Windows Vista/Windows Server 2008 в окне программы Windows Explorer (Проводник) имеется новый способ открыть окно командной строки

для любой выбранной папки *(см. разд. "Работа с объектами файловой системы в программе Windows Explorer" главы 3)*.

В окне консоли по умолчанию включен так называемый режим *автозаполнения*. В любой команде можно ввести первые символы имени папки или файла, нажать клавишу <Tab>, и система автоматически завершит имя, предлагая на выбор все имена, имеющиеся в текущей папке — при каждом повторном нажатии этой клавиши будет предложено новое имя, если подходящих имен несколько. Если вообще не ввести имени, то будут предлагаться все имеющиеся в папке имена папок и файлов по порядку.

После открытия окна консоли можно задать собственные настройки окна. Щелкните правой кнопкой мыши по заголовку окна и в контекстном меню выберите команду **Properties** (Свойства). Измените настройки окна, используя интересующие вас вкладки. При этом указанные параметры сразу будут использоваться и во всех текущих и последующих сеансах работы с командной строкой. Если в контекстном меню выбрать команду **Defaults**, то можно определить параметры (размеры, шрифт, цвет и т. д.), которые по умолчанию будут выбираться при запуске консоли другими (новыми) пользователями.

Примечания

Окно консоли и окно сессии MS-DOS настраиваются совершенно одинаково. Более того, аналогичные параметры имеет и окно оболочки Windows PowerShell *(см. далее)*.

Флажок **Quick Edit Mode** (Выделение мышью) на вкладке **Options** (Общие) разрешает *быстрое* копирование и вставку символов в командной строке при помощи мыши. Удерживая нажатой левую кнопку мыши, можно выполнять выделение части окна, а при нажатии правой кнопки выполняется запись в буфер выбранных символов или части экрана или, наоборот, вставка из буфера. Во всех последних версиях Windows эта удобная опция по умолчанию выключена.

У окна консоли имеется память команд. Если нажать клавишу <F7>, то появится окошко, где перечислены все ранее введенные команды. Можно стрелками клавиатуры выбрать любую команду и выполнить, нажав клавишу <Enter>. Эта функция очень удобна, когда часто используются "длинные" команды с большим количеством параметров. Предыдущую и последующую команды легко выбрать, просто нажимая клавиши со стрелками вверх и вниз, однако когда повторяются несколько команд, буфер команд значительно

удобнее и нагляднее. Опции буфера также можно задать на вкладке **Options** (Общие).

Обратите внимание на вкладку **Layout** (Расположение) (рис. 6.18) (показаны значения по умолчанию). Здесь задаются следующие важные параметры: размер буфера экрана (**Screen Buffer Size**), размер окна (**Window Size**) и его положение (**Window Position**).

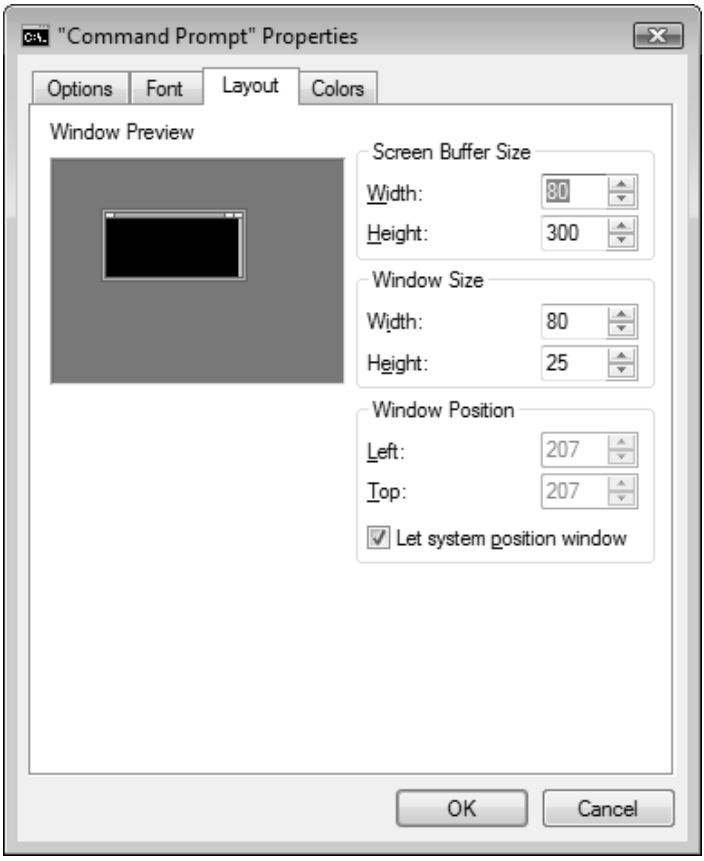


Рис. 6.18. На вкладке **Layout** задаются размеры окна командной строки и его буфера

По умолчанию количество строк буфера выставлено как 300. Это нормально при работе с системными командами и утилитами, однако при запуске некоторых устаревших полноэкранных приложений с DOS-окном окно команд-

ной строки может растянуться на все разрешенные 300 строк. Поэтому перед запуском программы лучше выбрать приемлемый размер окна консоли. В обычных условиях удобно иметь достаточно большой буфер экрана — как по высоте, так и по ширине (некоторые команды или выводимые строки бывают весьма длинными, и неудобно, когда их окончания часто переносятся на другую строку).

Чтобы подробно узнать возможности окна консоли (или окна сессии MS-DOS) и директив, используемых в командных файлах, введите следующую команду: `help cmd` или `cmd /?`. С помощью команды `help` можно получить список основных системных утилит. Информацию по системным программам также можно получить, выбрав ссылку **Command Reference** (Справочник по командам) в окне **Help and Support** (Справка и поддержка) — в этом случае выполняется обращение к веб-сайту Microsoft.

С помощью команд `help` *<имяУтилиты>* или *<имяУтилиты>* `/?` легко получить справку по любой утилите командной строки (список полезных административных утилит систем Windows Server 2008 приведен в *главе 4*). Иногда такая встроенная справка бывает точнее, чем информация из справочной системы.

Выполнение административных сценариев

Помимо командных файлов, представляющих собой текстовые файлы с расширением .cmd и содержащих директивы командного процессора и вызовы утилит командной строки с заданными параметрами, в системах Windows можно использовать *сценарии* (scripts), написанные на интерпретируемых языках программирования высокого уровня. Такими языками являются VBScript и JScript[1], а также новый язык и командный процессор — PowerShell.

Сценарии обычно используются при выполнении объемных или рутинных операций, с их помощью удобно описывать служебные задачи, связанные с объектами групповых политик, и выполняемые, например, при входе пользо-

[1] Можно, конечно, использовать и другие языки сценариев (например, Perl), при условии установки соответствующих командных процессоров. Мы говорим только о стандартных средствах, поддерживаемых в системах Windows.

вателя в систему (или домен) или при выключении компьютера. Многие операции с большим числом объектов каталога Active Directory просто невозможно выполнить вручную, а с помощью сценариев их можно осуществить за очень короткое время.

Сервер сценариев Windows (WSH)

Сервер сценариев Windows (Windows Script Host, WSH) уже давно является стандартным компонентом систем Windows (менялись только возможности и версия программы). В составе Windows Server 2008 поставляется WSH версии 5.7.

Сервер сценариев Windows позволяет запускать сценарии непосредственно с рабочего стола, из меню **Start** (Пуск), с помощью программы Windows Explorer (Проводник) или в окне командной консоли. Поддерживаются сценарии, написанные на языках VBScript и JScript. Такие сценарии позволяют использовать возможности многих технологий, имеющихся в системах Windows: например, спецификации Windows Management Instrumentation (WMI), описывающей взаимодействие с компонентами операционной системы, или интерфейсов Active Directory Service Interfaces (ADSI), обеспечивающих программный доступ к каталогу Active Directory. Кроме того, возможности управления с помощью сценариев существуют для некоторых важных системных утилит (например, для утилиты управления архивацией Wbadmin). Все это делает сценарии мощным и гибким средством управления системами.

> ***Примечание***
>
> Строго говоря, в системах Windows помимо Windows Scripting Host имеются еще две среды, позволяющие выполнять сценарии: это браузер Internet Explorer и веб-сервер, входящий в состав служб Internet Information Services.

При запуске сценария с помощью WSH можно указывать, какая оболочка будет использоваться — Cscript.Exe или Wscript.Exe. В первом случае весь вывод сообщений (например, `echo "Hello!"`) пойдет в окно консоли, во втором — сообщения будут отображаться в отдельном окне. Вариант, выбираемый по умолчанию, может устанавливаться с помощью команд `cscript //H:CScript` или `cscript //H:WScript`. Например, если задать Wscript.exe в качестве оболочки, то для всех файлов сценариев, имеющих расширение vbs, вывод сообщений будет осуществляться в специальном окне.

Запуск сервера сценариев из командной строки

При запуске сценария достаточно ввести в окне консоли его имя (расширение необязательно) или дважды щелкнуть по его имени в окне программы Windows Explorer (Проводник). Однако иногда можно или необходимо использовать дополнительные параметры WSH, и в этом случае выполнение сценариев происходит немного иначе.

Для запуска сервера сценариев из командной строки используется утилита Cscript.exe в соответствии со следующим синтаксисом:

cscript *имяСценария* [*параметрыСервераСценариев*] [*параметрыСценария*]

где:

- *имяСценария* — это имя файла сценария с расширением, например, Welcome.vbs;
- *параметрыСервераСценариев* — включают и отключают различные средства сервера сценариев. Они всегда предваряются двумя слэшами (//);
- *параметрыСценария* — передаются в сценарий. Они всегда предваряются одним слэшем (/).

Ни один из параметров не является обязательным, однако нельзя указать параметры сценария без самого сценария. Если не задать ни одного параметра, Cscript.exe выдает список параметров сервера сценариев; некоторые самые важные из них показаны в табл. 6.2.

Таблица 6.2. *Параметры сервера сценариев для Cscript.exe*

Параметр	Описание
`//B`	Пакетный режим. Не отображает на экране сообщений об ошибках и приглашения пользователей
`//E=engine`	Задает ядро, используемое для выполнения сценария
`//I`	Интерактивный режим (выбирается по умолчанию; режим, обратный задаваемому параметром `//B`)
`//Job:xxx`	Выполняет задание WSF *(см. далее)*
`//Logo`	Отображает на экране заставку (выбирается по умолчанию; режим, обратный задаваемому параметром `//NoLogo`)
`//NoLogo`	Запрещает вывод заставки

Таблица 6.2 *(окончание)*

Параметр	Описание
`//T:nn`	Время ожидания в секундах. Максимальное время, в течение которого может выполняться сценарий. (По умолчанию ограничение не устанавливается.) Этот параметр используется для предотвращения слишком длительного выполнения сценариев. Устанавливается специальный таймер, и когда время выполнения превышает установленное значение, Cscript прерывает работу ядра сценариев и завершает процесс

Запуск сценариев в среде Windows

Чтобы сценарий выполнялся в среде Windows (т. е. все сообщения будут при этом выводиться в специальное окно), нужно установить Wscript.exe в качестве оболочки по умолчанию или в окне консоли или окне **Run** (Выполнить) вводить строку `wscript` с указанием полного имени сценария и необходимых параметров сервера и сценария. Если ввести эту строку без параметров, то в окне свойств сервера сценариев можно устанавить параметры, приведенные в табл. 6.3.

Таблица 6.3. *Свойства сервера сценариев Wscript.exe*

Свойство	Применение	Эквивалент параметра команды `cscript`
Stop scripts after specified number of seconds (Останавливать сценарий после указанного числа секунд)	Максимальное количество секунд, в течение которых можно выполнять сценарий. (По умолчанию ограничение не устанавливается.)	`//T:nn`
Display logo when scripts executed in command console (Отображать на консоли сведения о программе во время выполнения сценария)	Отображать заставку. (Обратное параметру `//nologo`. Устанавливается по умолчанию.)	`//logo` или `//nologo`

Настройка индивидуальных свойств сценария. Файл с расширением wsh

С помощью страницы свойств оболочки Wscript.exe можно установить глобальные параметры, касающиеся сразу всех сценариев, выполняемых на компьютере. Однако также можно настроить индивидуальные параметры отдельно взятого сценария, позволяющие осуществлять жесткий контроль за его выполнением. Свойства конкретного сценария сохраняются в файле с расширением wsh.

Чтобы установить параметры для конкретного сценария, выберите его в окне программы **Windows Explorer** (Проводник) и откройте окно свойств. На вкладке **Script** (Сценарий) измените стандартные свойства сценария (например, максимальное время исполнения) и нажмите кнопку **OK**. В результате в папке, где находится сценарий, будет создан файл с расширением wsh, имя которого совпадает с именем сценария.

Теперь для того чтобы запустить сценарий, следует дважды щелкнуть мышью на файле *.wsh в окне программы Windows Explorer (Проводник) или использовать этот файл в качестве параметра для оболочки Wscript.exe или Cscript.exe в командной строке. Например:

```
C:\>cscript Welcome.wsh
```

Поскольку в файле с расширением wsh хранятся значения параметров, используемых сценарием при выполнении, системный администратор может создать несколько версий файла с параметрами, ориентированных на различные задачи.

Файл с расширением wsh представляет собой простой текстовый файл, формат которого сходен с форматом файла с расширением inf. Ниже приведен пример содержимого файла *.wsh.

```
[ScriptFile]
Path=D:\Welcome.vbs
[Options]
Timeout=5
DisplayLogo=0
```

Параметр `Path` в разделе `[ScriptFile]` определяет местоположение файла сценария, с которым связан данный файл *.wsh. Параметры, значения которых устанавливаются в разделе `[Options]`, соответствуют настройкам вкладки **Script** (Сценарий) окна **Properties** (Свойства). (Например, если установить

тайм-аут для сценария, выводящего сообщение в окно, то это окно не будет оставаться на экране до тех пор, пока его не закроет пользователь, а исчезнет по истечении указанного промежутка времени.)

Сервер сценариев WSH позволяет также использовать файлы *Windows script files* (*.wsf), имеющие формат Extensible Markup Language (XML). Эти файлы просты, очень эффективны и значительно расширяют возможности применения сценариев. Дополнительную информацию можно получить в статье "Using Windows Script Files (.wsf)", которую несложно найти по названию на веб-сайте MSDN (см. ссылки в *приложении*).

Командный процессор и язык PowerShell

Windows PowerShell представляет собой новую разработку Microsoft; это ориентированный на системных администраторов командный процессор, позволяющий выполнять директивы в интерактивном режиме и поддерживающий сценарии, а также язык написания этих сценариев. В процессе разработки оболочка PowerShell также называлась Windows "Monad" Shell и Microsoft Command Shell (MSH).

Директивы PowerShell называются *командлетами*[1] (cmdlet), они представляют собой простые, специализированные средства командной строки, выполняющие единственную функцию, встроенные в оболочку и предназначенные для работы с объектами. Имеется более ста стандартных командлетов, при этом можно создавать и новые, собственные командлеты.

Оболочка Windows PowerShell может работать в системах XP Service Pack 2, Windows Server 2003 Service Pack 1 и 2, Windows Server 2003 R2, Windows Vista и Windows Server 2008 на всех платформах (x86, x64 и IA64). Ее можно скачать из Центра загрузки Microsoft для всех перечисленных систем (в Windows Server 2008 оболочка PowerShell входит как стандартный компонент). Для установки и работы PowerShell требуется .NET Framework 2.0.

Windows PowerShell локализован; кроме того, имеется пакет *Multilingual User Interface Pack (MUI) Language Packs for Windows PowerShell 1.0*, который можно свободно скачать из Центра загрузки Microsoft.

---

[1] Неологизм, к которому придется привыкать (по аналогии с аплетами (applet), сервлетами (servlet)).

Этот пакет обеспечивает локализацию PowerShell для многих языков, включая русский, и может использоваться на следующих системах:

- Microsoft Windows Server 2003 R2
- Microsoft Windows Server 2003 with Service Pack 2 (SP1 и SP2)
- Microsoft Windows XP with Service Pack 2 (SP2)

Множество рабочих сценариев, которые можно использовать при изучении языка и в качестве примеров для создания собственных сценариев, можно найти на веб-сайте *TechNet Script Center* (**http://www.microsoft.com/technet/scriptcenter/default.mspx**), в разделе Windows PowerShell (см. ссылку Script Repository).

Имеется GUI-оболочка от сторонних разработчиков, с помощью которой можно построить интерактивную среду для работы с Powershell; она также имеет удобный профессиональный редактор для сценариев, написанных на языке Powershell (редактор обеспечивает форматирование, цветовое выделение команд и т. п.). Это средство бесплатное, его можно найти на веб-сайте *PowerGUI.org - Open Source Windows Powershell Community* по адресу **http://powergui.org/index.jspa**.

Установка и запуск PowerShell

В системах Windows Server 2008 оболочка PowerShell по умолчанию не активизирована; для того чтобы можно было пользоваться командлетами и выполнять сценарии, необходимо сначала с помощью оснастки **Server Manager** (Диспетчер сервера) *(см. главу 3)* установить компонент *Windows PowerShell*. После этого в меню **Start** (Пуск) появится новая программная группа — Microsoft PowerShell 1.0, содержащая команду запуска оболочки и ссылку на папку, содержащую справочные файлы GettingStarted.rtf, QuadFold.rtf, releaseNotes.rtf и UserGuide.rtf. Обязательно познакомьтесь с содержимым первого и последнего файлов. (Если на компьютере для локализации интерфейса установлен пакет Language Interface Pack (LIP), то вся информация в файлах будет на русском языке.)

Поскольку оболочка функционирует в окне консоли (ее можно запустить с помощью команды `powershell`), то она имеет соответствующий интерфейс и возможности (включая способы настройки параметров и буфер команд). Если запускать Windows PowerShell из меню **Start** (Пуск), то в заголовке окна появится характерный значок (рис. 6.19).

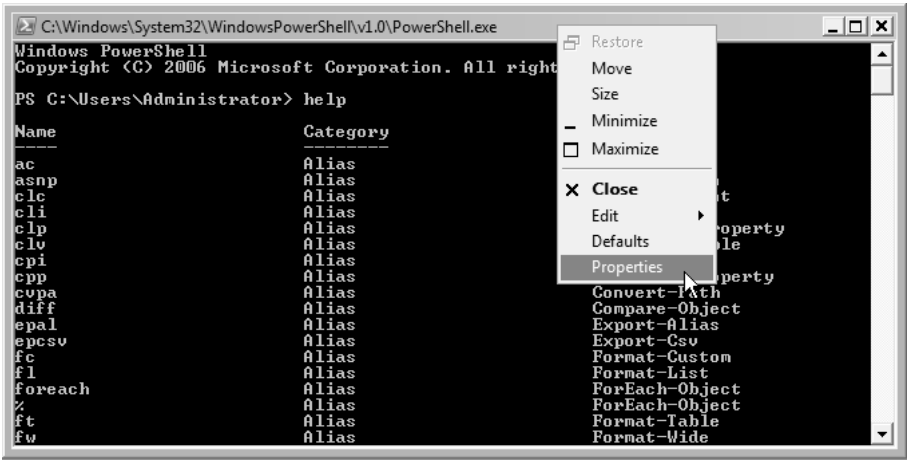


Рис. 6.19. Окно командного процессора PowerShell

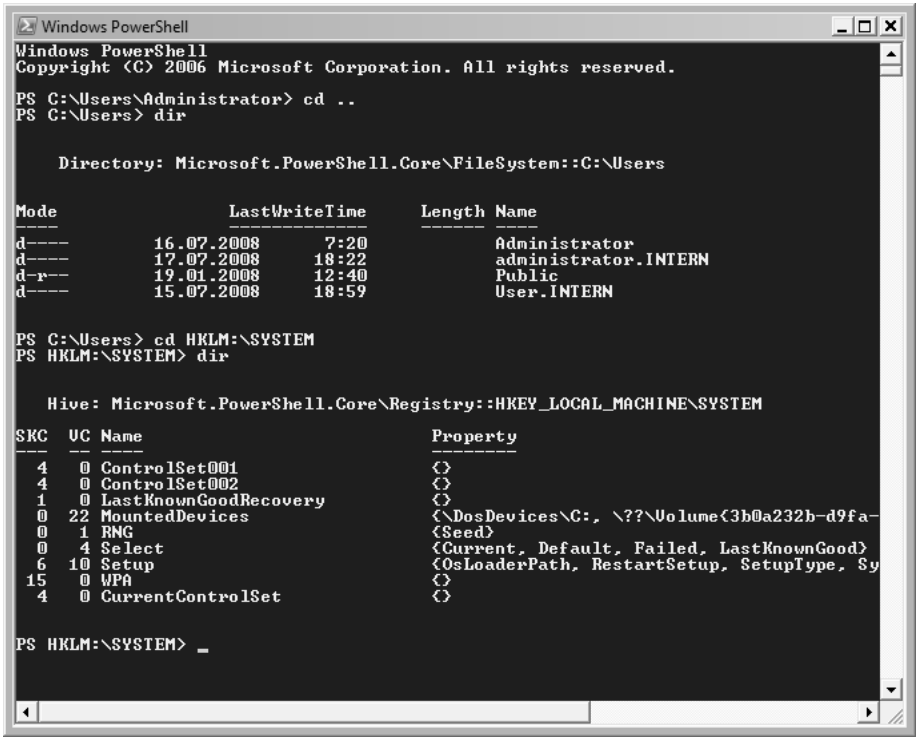


Рис. 6.20. Пример навигации по папкам файловой системы и разделам системного реестра

Список командлетов можно получить с помощью команды `get-command`; команда `help` позволяет увидеть список всех псевдонимов (альтернативных имен командлетов, используемых для краткости) и самих командлетов. Для отображения справочной информации по общим вопросам и отдельным командам используйте команду `get-help`.

С помощью оболочки PowerShell можно получить доступ ко многим разнородным ресурсам операционной системы, представленным в едином рабочем пространстве и позволяющим использовать общие команды. Концепция единого рабочего пространства иллюстрируется на рис. 6.20, где одни и те же команды `cd` и `dir` служат для навигации и просмотра совершенно разных объектов системы: сначала просматривается содержимое локальной папки файловой системы, а затем — разделы системного реестра.

Выполнение сценариев

В заключение скажем несколько слов о том, как выполнять сценарии, написанные на языке PowerShell. Процедура начальной проверки несложная и может выглядеть следующим образом:

1. Запустите PowerShell из окна консоли или из меню **Start** (Пуск).
2. Установите политику, разрешающую выполнять локальные сценарии, с помощью команды `set-executionpolicy remotesigned`. Без этого никакие сценарии работать не будут!
3. Откройте редактор Notepad (Блокнот) и введите оператор, содержащий сакраментальную фразу, известную всем опытным программистам:

   ```
   echo "Hello, World!"
   ```

4. Сохраните файл с любым именем и расширением ps1.
5. В окне PowerShell введите имя файла, обязательно добавляя полный путь (расширение ps1 указывать не обязательно).
6. Если сообщение появляется на экране, то проверку можно считать успешно законченной, и можно запускать другие сценарии:

   ```
   PS C:\> C:\hello
   Hello, World!
   PS C:\>
   ```

Информацию о политиках выполнения сценариев и цифровых подписях можно получить с помощью следующей команды (конвейер `more` необходим для того, чтобы просматривать справку постранично):

```
get-help about_signing | more
```

По умолчанию установлена политика *Restricted*, разрешающая выполнение команд, но полностью запрещающая сценарии. Поэтому чтобы сценарии могли выполняться, необходимо, как минимум, установить политику *RemoteSigned* — в этом случае сценарии локального компьютера будут выполняться без ограничений, а для сценариев, полученных из других источников, потребуется цифровая подпись. Самая строгая политика — *AllSigned*; в этом случае цифровые подписи должны быть абсолютно у всех сценариев.

Для установки политики и просмотра текущей политики используются, соответственно, команды `Set-ExecutionPolicy` и `Get-ExecutionPolicy`.

ГЛАВА 7

Файловые службы

В этой главе описываются средства управления локальными дисками и общими дисковыми ресурсами систем Windows Server 2008, а также дополнительные функции, связанные с использованием возможностей хранения информации. Многие из них объединены одной ролью сервера — *File Services* (Файловые службы). Некоторые функции и средства администрирования присутствовали в предыдущих версиях Windows, а некоторые появились только в Windows Server 2008. Сначала мы будем рассматривать традиционные возможности, а потом перейдем к новинкам.

> ***Примечание***
>
> Еще одна функция, относящаяся к работе с файлами — *Предыдущие версии файлов*[1] (previous versions) — описана в *главе 15*, поскольку она тесно связана с задачами архивации и восстановления данных.

Установка файловых служб

Возможности системы по выполнению функций файлового сервера определяются службами роли *File Services* (Файловые службы), которые устанавливаются с помощью оснастки **Server Manager** (Диспетчер сервера) *(см. также разд. "Роли и компоненты сервера" главы 3)* или утилиты командной строки ServerManagerCmd.

---

[1] В предыдущих версиях Windows аналогичная функция называлась *Теневые копии* (Shadow Copies).

По умолчанию в системе всегда установлена служба *File Server* (Файловый сервер), которая обеспечивает работу общих папок. Чтобы установить дополнительные средства для работы с файлами, необходимо выполнить следующие действия:

1. Запустить оснастку **Server Manager** (Диспетчер сервера), выбрать узел **Roles** (Роли) и в правой части окна оснастки найти панель **File Services** (Файловые службы).
2. Выбрать ссылку **Add Role Services** (Добавить службы ролей). В окне программы-мастера установить флажки около названия требующихся служб (рис. 7.1). Обратите внимание, что для каждой службы имеется описание.

Примечание

Все сообщения, связанные с установкой и удалением ролей, компонентов и служб ролей сервера, регистрируются в системном журнале Setup (Настройка).

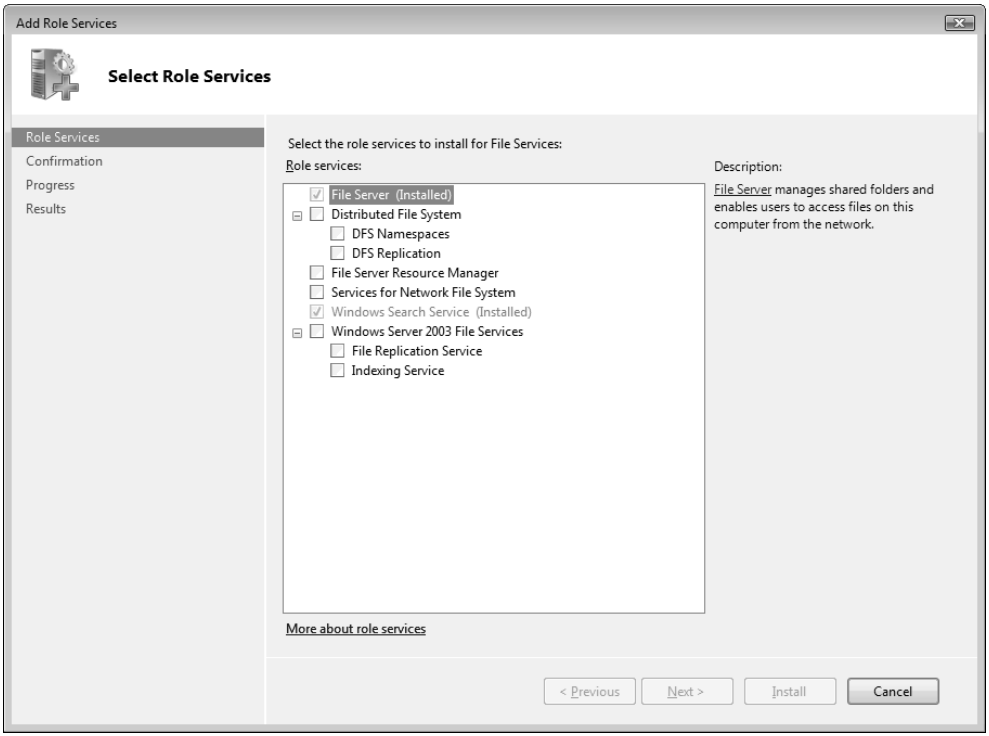


Рис. 7.1. Окно выбора устанавливаемых компонентов файловых служб

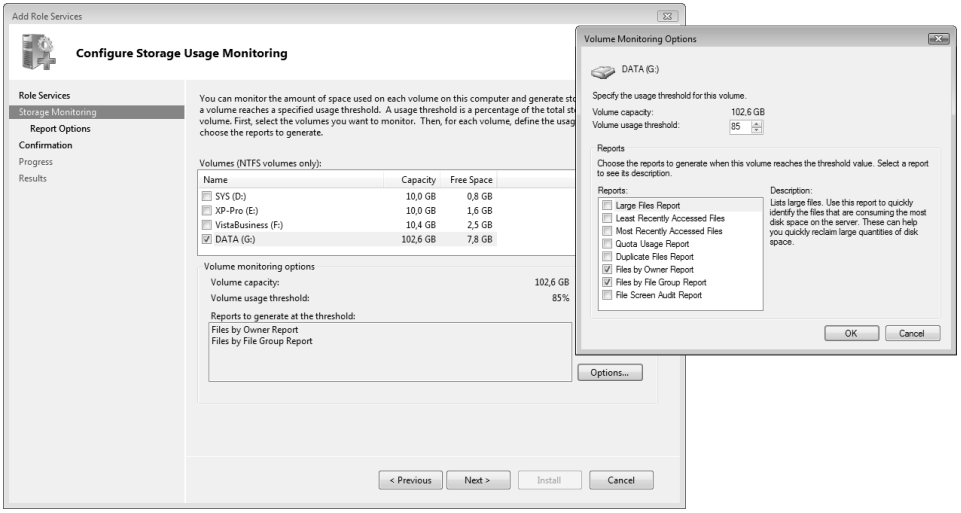


Рис. 7.2. Выбор дисковых томов для контроля за используемым пространством и других параметров для составления отчетов

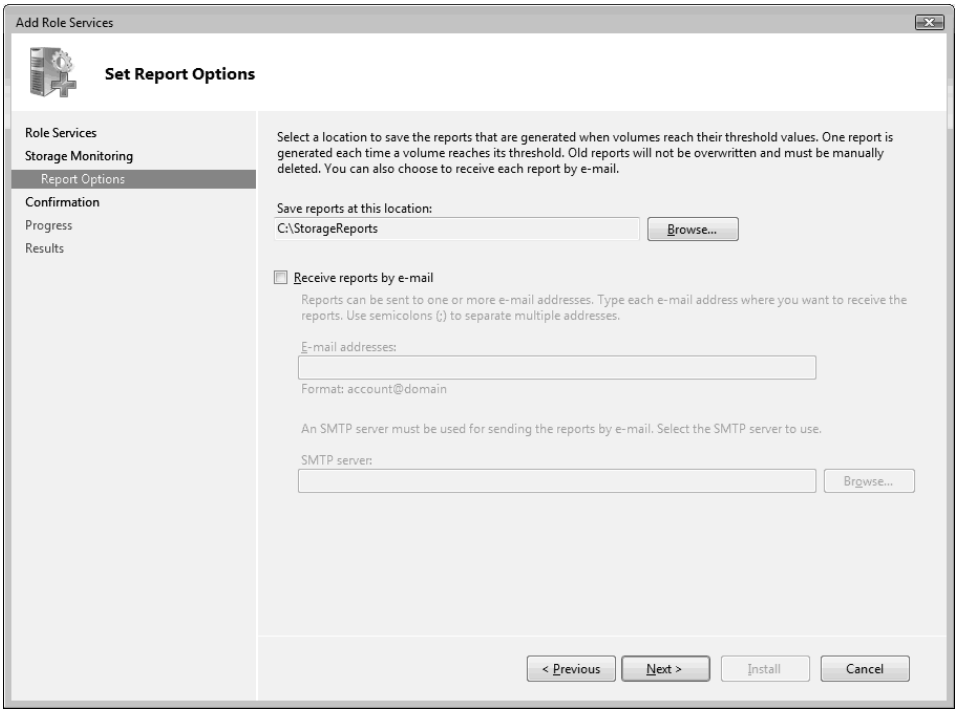


Рис. 7.3. Выбор папки для хранения отчетов и адреса электронной почты для отсылки сообщений

При установке оснастки **File Server Resource Manager** (Диспетчер ресурсов файлового сервера) можно сразу указать, для каких дисковых томов будет осуществляться мониторинг используемого пространства (рис. 7.2). Нажав кнопку **Options** (Сведения), можно определить пороговое значение для выбранного тома и виды отчетов, которые будут генерироваться. (С помощью этого средства можно, например, легко отслеживать появление на диске файлов большого размера.)

На следующем этапе нужно указать папку, где будут храниться все выбранные отчеты (рис. 7.3). Также можно определить адреса электронной почты, по которым эти отчеты будут автоматически рассылаться (в этом случае необходимо указать адрес или имя SMTP-сервера, через который почта будет отправляться).

После того как нужные службы будут установлены, в окне оснастки **Server Manager** (Диспетчер сервера) внутри папки **File Services** (Файловые службы) появятся значки для новых инструментов управления этими службами (рис. 7.4).

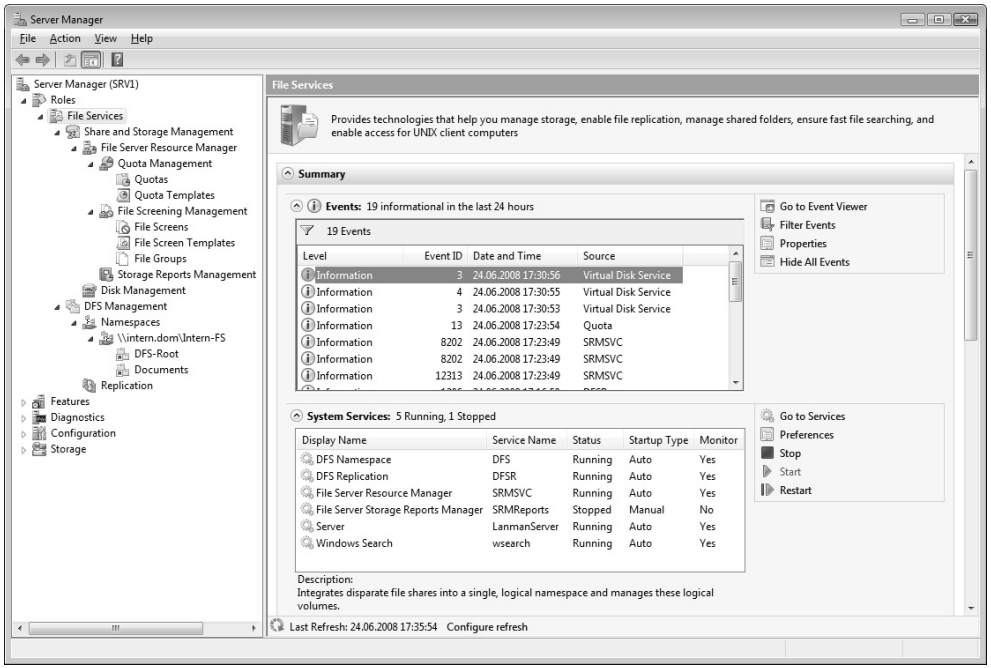


Рис. 7.4. Информационные панели для выбранной роли File Services

На панели событий можно следить за всеми информационными и критическими сообщениями, поступающими от всех файловых служб, а на панели ниже отображается текущее состояние всех сервисов. Здесь же имеются кнопки, с помощью которых сервисы можно останавливать и перезапускать.

В нижней части списка административных панелей имеется справочная панель **Resources and Support** (Ресурсы и поддержка) (рис. 7.5), где перечислены рекомендации по эффективному использованию выбранной роли и ее служб. Также здесь имеются ссылки, по которым можно обратиться к информационным и сервисным веб-ресурсам компании Microsoft.

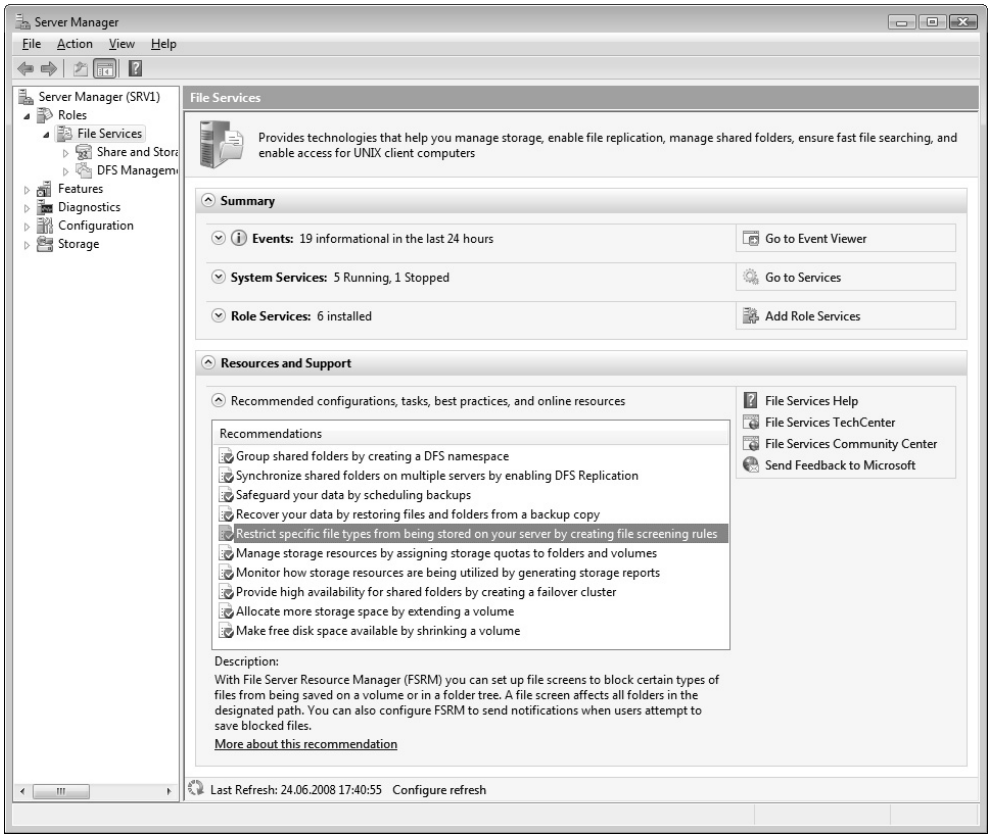


Рис. 7.5. Информационная панель — набор рекомендаций по использованию служб выбранной роли и ссылки на веб-ресурсы

Конфигурирование дисков и томов

Сначала немного общих вопросов и терминологии. При работе с дисками в системах Windows необходимо иметь представление о некоторых базовых понятиях, которые будут изложены далее. Важно понимать особенности реализации базовых концепций в системах Windows Server 2008 и отличия от предыдущей серверной версии. Без этого будут непонятны некоторые функции административных утилит, возможны и неправильные действия при выполнении операций с дисками и томами.

Стили разделов

Компьютеры, использующие x86-совместимые процессоры, для управления дисками обычно используют *главную загрузочную запись* (Master Boot Record, MBR). MBR содержит *таблицу разделов* (partition table), описывающую разбиение диска. Именно MBR-диски чаще всего используются в системах Windows. (Стиль раздела можно видеть в окне оснастки **Disk Management** (Управление дисками) — см. рис. 7.8.)

На компьютерах, работающих на базе процессоров Itanium под управлением Windows XP 64-bit Itanium Edition и соответствующих 64-разрядных серверных версий Windows, появился новый механизм распределения дискового пространства — *GUID partition table* (GPT). В настоящее время GPT-диски поддерживают и системы Windows Vista или Windows Server 2008, хотя есть определенные ограничения для разных редакций систем.

Самое существенное различие между MBR- и GPT-дисками заключается в максимально возможном размере дискового тома и в количестве разделов на диске: 18 эксабайт[1] и 128 разделов на диск — для GPT-диска и 2 терабайта и 4 основных раздела на диск — для MBR-диска (или три основных раздела и один дополнительный с неограниченным количеством логических дисков). Критически важные данные на GPT-дисках хранятся не в скрытых секторах или невыделенном пространстве, а в самих разделах; кроме того, у этих дисков имеются дополнительные основные и резервные таблицы разделов для повышения целостности. MBR-диск можно конвертировать в GPT-диск, и наоборот, если диск пуст (подобная операция возможна и для преобразования базовых и динамических дисков). (Подробную информацию о GPT-дисках сле-

[1] Эксабайт (exabyte) = 1024 петабайт = 2^{60} байт. Терабайт (terabyte) = 1024 гигабайт = = 2^{40} байт.

дует искать на веб-сайте Microsoft, воспользовавшись поиском строки `GUID partition table`.)

Хотя между MBR- и GPT-разделами и существуют некоторые различия, типы дисков (базовые и динамические), средства и методы администрирования остаются одними и теми же. Поэтому в этой книге мы не будем касаться нюансов использования GPT-разделов, тем более что их использование целесообразно на серверных платформах со сложными дисковыми конфигурациями большого объема. При инициализации пустого диска (рис. 7.6) система предлагает выбрать тип раздела и указывает на отсутствие совместимости с предыдущими версиями Windows, а также рекомендует применять GPT-разделы на дисках размером больше 2 Тбайт или для дисков, работающих в Itanium-системах.

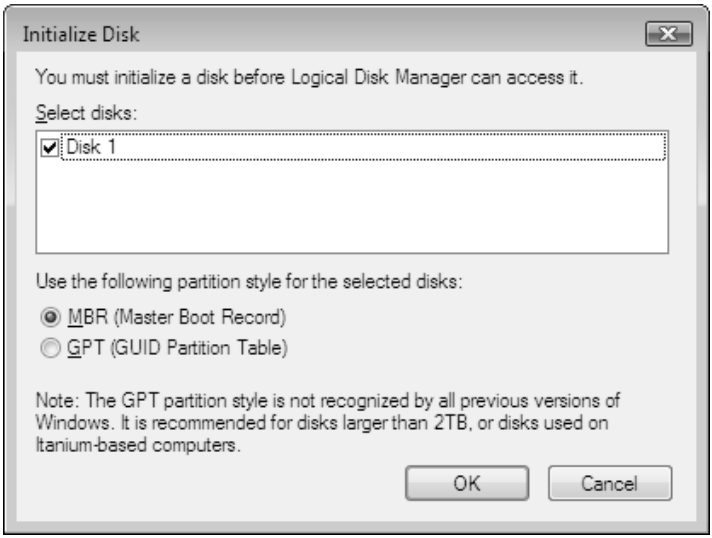


Рис. 7.6. Выбор стиля разделов при подключении к системе нового диска

Разделы и тома

Как и в предыдущих версиях Windows, в системах Windows Server 2008 можно использовать жесткие диски, работающие в *базовом* режиме хранения информации (basic storage) и в *динамическом* режиме хранения данных (dynamic storage); соответственно диски называются *базовыми* (basic) и *ди-*

намическими (dynamic). Различие между ними заключается во внутренней организации служебных разделов (файловых таблиц) на диске, что порождает разные функциональные возможности организации дискового пространства (как на одном диске, так и на массивах дисков).

Для администратора главным достоинством динамических дисков является возможность более гибкого конфигурирования дискового пространства (физических дисков и логических томов) без перезагрузки операционной системы, а также оперативного расширения или сжатия томов (хотя в системах Windows Server 2008 можно менять размер томов и на базовых дисках, но имеется больше ограничений). Чаще всего динамические диски применяются в многодисковых конфигурациях.

Базовые диски

Разделом является часть базового диска, функционирующая как логически автономная единица. *Основной раздел* (primary partition) зарезервирован для использования операционной системой, т. е. один основной раздел обязательно должен присутствовать на диске. Каждый физический диск может иметь до четырех основных разделов (или до трех, если создан дополнительный раздел). *Дополнительный раздел* (extended partition) создается с использованием оставшегося свободного пространства диска и может быть разделен на логические диски. На каждом физическом диске может быть только ***один*** дополнительный раздел.

С базовыми дисками возможны следующие операции:

- создание основных разделов и дополнительного раздела (4 основных или 3 основных и один дополнительный на каждом диске). Если при наличии четырех основных разделов попытаться создать пятый раздел, система предложит преобразовать диск в динамический;
- создание логических дисков (в дополнительном разделе);
- расширение и сжатие разделов (логических дисков) с помощью команды DiskPart.exe или оснастки **Disk Management** (Управление дисками).

> ***Внимание!***
>
> Базовый диск в любой момент можно превратить в динамический без потери информации. Обратная процедура требует предварительной архивации данных на всем диске (во всех разделах или логических дисках), т. к. вся информация на диске теряется.

Динамические диски

Динамические диски делятся не на разделы, а на тома. Том состоит из одного (или части целого) или нескольких физических дисков и может иметь одну из следующих конфигураций: *простой* том, *составной* том, *зеркальный* том, *чередующийся* том и том *RAID-5*. Базовый диск в любой момент может быть превращен в динамический диск без потери информации.

Том (volume) — это логически организованное пространство на одном или нескольких физических дисках. Оно может быть отформатировано с использованием файловой системы NTFS и иметь имя (в виде буквы).

Простой том (simple volume) использует пространство одного диска (или части диска). Это может быть один участок на диске или несколько участков, соединенных друг с другом. Простой том может быть расширен в пределах одного диска или на дополнительный диск. Если простой том распространяется на несколько физических дисков, он становится составным томом. Простой том не обеспечивает отказоустойчивости.

Составной том (spanned volume) состоит из связанного вместе пространства нескольких физических дисков (до 32 дисков). Он может распространяться на дополнительные диски и не может входить в состав зеркала *(см. ниже)*. Создавая составные тома, можно распределять нагрузку на дисковые системы. Составные тома не обеспечивают отказоустойчивости; более того, поскольку тома такого типа расположены на нескольких жестких дисках, возрастает вероятность их отказа, связанная с выходом из строя одного из дисков.

Зеркальный том (mirrored volume) (RAID-1) — это средство обеспечения отказоустойчивости, когда данные дублируются на двух физических дисках. Все данные оперативно копируются на оба диска, что обеспечивает возможность получения избыточности данных. Если один из дисков отказывает, данные могут быть доступны на уцелевшем диске зеркала. Зеркальный том не может быть расширен.

Данные на *чередующемся томе* (stripped volume) (RAID-0) разбиваются при записи и помещаются на несколько физических дисков, причем информация равномерно распределяется среди всех дисков, входящих в состав такого тома. Такой подход эффективен при необходимости быстрой записи или считывании с физических дисков большого объема информации. Скорость работы с дисковой системой увеличивается за счет распараллеливания потоков данных и одновременной записи или считывания информации с дисков тома. "Расщепление" информации также полезно при балансировке нагрузки вво-

да/вывода в многопользовательских приложениях. Тома с чередованием записываемой информации не обеспечивают отказоустойчивость. Том такого типа не может входить в зеркальный набор и его нельзя расширить.

Том RAID-5 (RAID-5 volume) является средством обеспечения высокой отказоустойчивости дисковой системы, поскольку данные тома расщепляются при записи на три (минимум) или большее количество дисков. Том RAID-5 обеспечивает избыточность информации, для чего подсчитывается контрольная сумма информации, расположенной на каждом диске. Контрольная сумма (вычисляемая величина, которая может быть использована для восстановления данных в случае их разрушения) также расщепляется и записывается на все диски массива. Если отказывает один из дисков массива, то информация, которая на нем находилась, может быть восстановлена с использованием работоспособных дисков и контрольной суммы. Том RAID-5 не может входить в зеркальный набор, и его нельзя расширить.

Общие понятия; особенности систем Windows Server 2008

Еще несколько терминов используется как с базовыми, так и с динамическими дисками.

Свободное или *нераспределенное пространство* (unallocated space) — это неиспользованная и неформатированная часть жесткого диска, которая может быть задействована при создании или расширении томов.

Системный том (system volume) содержит файлы диспетчера загрузки Windows (Windows Boot Manager) *(см. главу 1)* и другие файлы, необходимые для начальной загрузки систем.

Загрузочный том (boot volume) содержит файлы самой операционной системы, расположенные в папке *%SystemRoot%* (обычно — C:\Windows).

> **ВНИМАНИЕ!**
>
> Обычно системным и загрузочным является один и тот же том жесткого диска. Различаться эти тома могут только при установке на компьютере нескольких операционных систем (так называемые "системы с двойной загрузкой"). В этом случае нужно четко помнить о принципиальной разнице между этими понятиями.

В системах Windows Server 2008 возможности базовых дисков используются, можно сказать, минимальным образом: при установке системы и в процессе

работы стандартные средства администрирования позволяют создавать только основные разделы (primary partition), не больше 4-х. Дисковые конфигурации с дополнительным (extended) разделом полностью поддерживаются, если они унаследованы от предыдущих систем (т. е. если они были созданы с использованием других операционных систем или программ) или если они были созданы вручную с помощью утилиты DiskPart. Поэтому все разделы и логические диски на базовых дисках (так же, как и на динамических) называются томами, а точнее — *простыми томами*.

Использование оснастки *Disk Management*

Оснастка **Disk Management** (Управление дисками) остается основным инструментом администратора для выполнения "базовых" операций с дисковыми разделами (томами) или логическими дисками. Пример окна оснастки приведен на рис. 7.7.

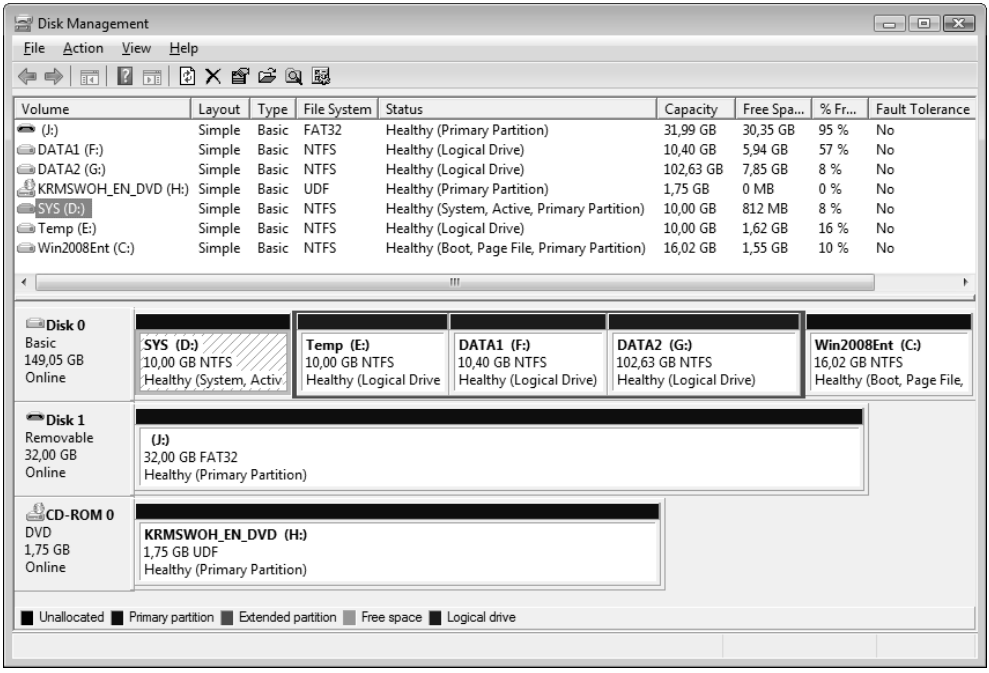


Рис. 7.7. Окно оснастки **Disk Management**

Как можно видеть, по умолчанию окно делится на две половины: в верхней перечислены логические диски (разделы или тома), а в нижней отображаются физические диски (жесткие, съемные и CD/DVD) и графически представлено деление дисков на разделы.

Оснастку **Disk Management** (Управление дисками) можно использовать как автономную оснастку или в составе основного инструмента администрирования Windows Server 2008 — оснастки **Computer Management** (Управление компьютером). В первом случае при подключении оснастки к консоли управления MMC в диалоговом окне **Select Computer** (Выбор компьютера) можно выбрать положение переключателя **This computer** (Этим компьютером), если нужно управлять локальным компьютером, либо положение **The following computer** (Компьютером, указанным ниже), если требуется управлять другим компьютером сети. В последнем случае в окне ввода следует указать имя компьютера (либо найти его, нажав кнопку **Browse** (Обзор)).

Кроме того, для локального компьютера оснастку можно запустить автономно, введя в командной строке `diskmgmt.msc`.

Внимание!

При подключении оснастки **Disk Management** (Управление дисками) (автономной или в составе других консолей MMC) к удаленному компьютеру необходимо, чтобы на этом компьютере была запущена служба Virtual Disk (Виртуальный диск; сервис vds) и в брандмауэре Windows *на обоих компьютерах* было разрешено исключение **Remote Volume Management** (Удаленное управление томами).

Примечание

При работе в окне консоли или в среде Server Core управление дисками, разделами и томами осуществляется с помощью утилиты *DiskPart.exe*, которая используется в интерактивном режиме. Утилита *Fsutil.exe* служит для управления файловыми системами, связями (link), точками повторной обработки (reparse point) и квотами.

В окне оснастки **Disk Management** (Управление дисками) большое значение имеют цветовые выделения разделов и логических дисков (особенно, если много разделов различного типа).

- **Темно-синим** помечаются основные разделы (C:, D:).
- **Синим** обозначены логические диски (E:, F:, G:).

- Свободное пространство (free space) на диске имеет **ярко-зеленый** цвет, а нераспределенное (unallocated) — **черный цвет** (в нашем примере оба типа не показаны).
- Все логические диски в этом примере располагаются в дополнительном (extended) разделе; они обведены рамкой **зеленого** цвета.

> ***Примечание***
>
> Цвета и отображение дисков в окне оснастки можно поменять, выполнив команду **Settings** (Параметры) в меню **View** (Вид) и установив новые значения.

На рис. 7.7 обратите внимание на то, что *системным* в нашем примере является первый по физическому местоположению раздел — диск D: (статус "System, Active"). На этом диске располагается диспетчер загрузки Windows, инициирующий запуск систем. *Загрузочным* является диск C: (статус "Boot, Page File"); на этом диске находятся все файлы операционной системы. Windows Server 2008 при установке в любой физический раздел всегда меняет названия дисков и себя "помещает" на диск C: (остальные диски уже именуются по порядку). Исключение составляет только вариант обновления системы: если, скажем, система загружалась с диска D:, этот диск загрузочным и останется, и название его не изменится.

Расположение панелей в окне оснастки **Disk Management** (Управление дисками) можно менять: для этого в меню **View** (Вид) имеются команды **Top** (Верх) и **Bottom** (Низ) (см. врезку на рис. 7.8). По умолчанию в верхней части окна отображается **Volume List** (Список томов), а в нижней — **Graphical View** (Графическое представление) (это расположение представлено на рис. 7.7). Если выбрать опцию **Disk List** (Список дисков), то можно видеть общие сведения о подключенных дисках[1] (рис. 7.8). Обратите внимание, что указывается стиль раздела (MBR или GPT).

Оснастка **Disk Management** (Управление дисками) позволяет выполнять следующие операции с базовыми дисками:

- создавать и удалять основные (primary) разделы (простые тома) (до 4-х);
- монтировать диски (подключать создаваемый том к *пустой* папке существующего диска);

---

[1] SATA-диски также отображаются как **IDE**.

- форматировать тома, присваивать им метки, а также помечать тома как активные;
- сжимать (shrink) и расширять (extend) тома;
- инициализировать диски;
- преобразовывать базовые диски в динамические.

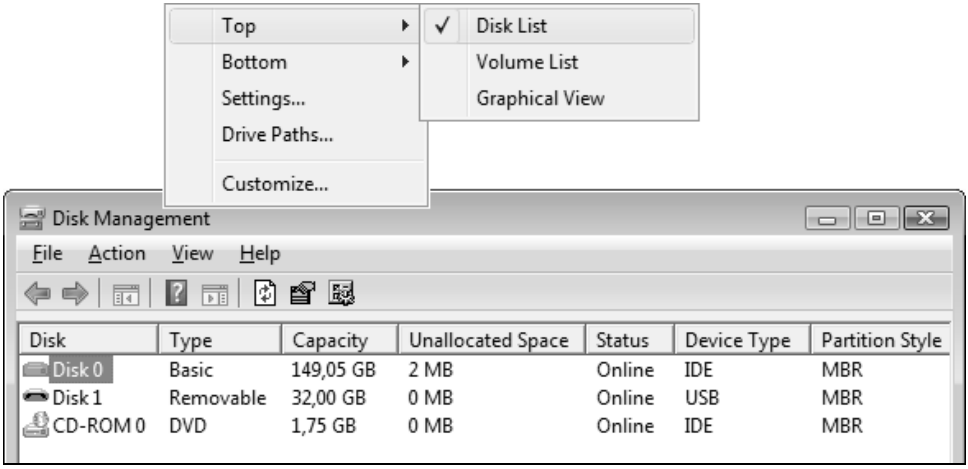


Рис. 7.8. Режим отображения подключенных дисков

Внимание!

В системе с двойной загрузкой операция преобразования базового диска вызовет неразрешимую проблему с запуском других систем, установленных на диске (система даже выдает соответствующее предупреждение при выполнении операции преобразования). Проблемы будут и с установкой второй системы Windows (любой версии) на динамический диск. Поэтому следует выбирать одно из двух: либо система с двойной загрузкой, либо динамические диски.

Оснастка ***не позволяет*** создавать наборы томов, чередующиеся и зеркальные наборы и чередующиеся наборы с четностью (такие конфигурации могут поддерживаться только как унаследованные от других систем). Нельзя создать дополнительный (extended) раздел; если по каким-то соображениям это требуется, то следует использовать утилиту командной строки DiskPart.

Внимание!

В русскоязычной терминологии систем Windows Vista/Windows Server 2008 возникла некоторая неопределенность понятия "сжать диск"[1]. Существует традиционное определение — *сжатие* (compression) средствами файловой системы всего диска или отдельных файлов и папок на томе NTFS для экономии места. В названных системах раздел или логический диск можно оперативно *сжать* (shrink) и *расширить* (extend). В первом случае размер диска уменьшается (если это возможно) и освободившееся пространство переходит в свободную (неразмеченную) область; во втором, наоборот, размер диска можно увеличить за счет свободного пространства, имеющегося на том же физическом диске.

При работе с динамическими дисками оснастка **Disk Management** (Управление дисками) позволяет осуществлять следующие действия:

- создавать и удалять простые (simple), составные (spanned), чередующиеся (stripped) и зеркальные (mirrored) тома (рис. 7.9), а также тома RAID-5 (если в системе установлено не менее 3-х жестких дисков); для базовых дисков в меню выбора типа тома доступна только первая опция;

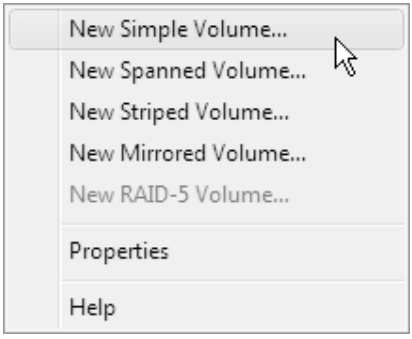


Рис. 7.9. Меню выбора типа создаваемого тома на динамическом диске

- форматировать тома и назначать им метки (имена);
- расширять тома с использованием нераспределенного пространства на том же диске или на других дисках;

[1] Сжатие томов в системах Windows Server 2003 возможно только с помощью утилиты DiskPart, где аналогичная команда называется "уменьшение размера тома" — поэтому нюансов в терминологии там нет.

- сжимать тома;
- повторно инициализировать отключенные диски;
- преобразовывать динамические диски в базовые.

> **Примечание**
>
> Для преобразования файловой системы тома из FAT в NTFS используется утилита командной строки *Convert.exe*.

Расширение и сжатие разделов и логических дисков

В системах Windows Vista/Windows Server 2008 оперативное сжатие и расширение разделов возможно не только при помощи утилиты DiskPart.exe (как в Windows XP/Windows Server 2003), но и непосредственно в окне оснастки **Disk Management**[1] (Управление дисками).

Расширить можно только такой раздел, ***непосредственно за которым*** имеется свободное (нераспределенное) пространство. Возможность сжатия раздела определяется только наличием свободного места в этом разделе.

Для *расширения* раздела используются следующие операции:

1. Выберите раздел в окне оснастки, щелкните правой кнопкой мыши и в контекстном меню выполните команду **Extend Volume** (Расширить том) — запустится мастер *Extend Volume Wizard* (Мастер расширения тома).
2. Выберите объем добавляемого дискового пространства (рис. 7.10) и нажмите кнопку **Next** (Далее). При вводе значений сразу можно видеть новый размер раздела.
3. Проверьте правильность операции и на последней странице мастера нажмите кнопку **Finish** (Готово).

Сжатие раздела выполняется аналогичным образом, только необходимо выбрать команду **Shrink Volume** (Сжать том). Выполнится опрос тома для определения доступного места для сжатия, после чего появится окно (рис. 7.11), в котором нужно указать, на сколько мегабайт будет уменьшен раздел. После нажатия кнопки **Shrink** (Сжать) операция будет выполнена. Этой операцией нужно пользоваться осторожно, чтобы на диске оставалось пространство, достаточное для работы!

---

[1] В системах Windows Server 2003 эта оснастка позволяет только расширять тома.

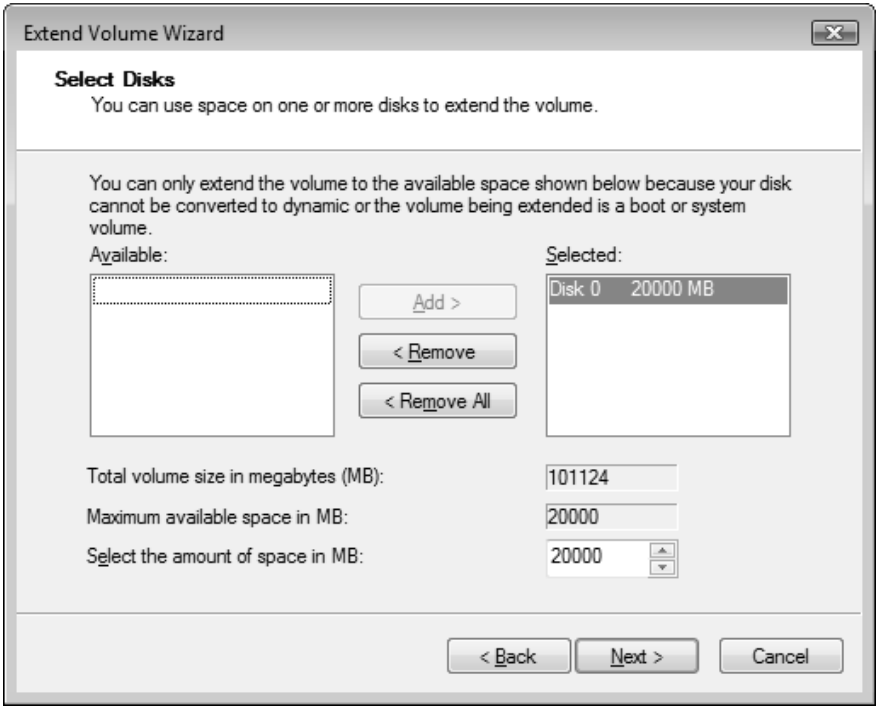


Рис. 7.10. Выбор нового размера расширяемого диска

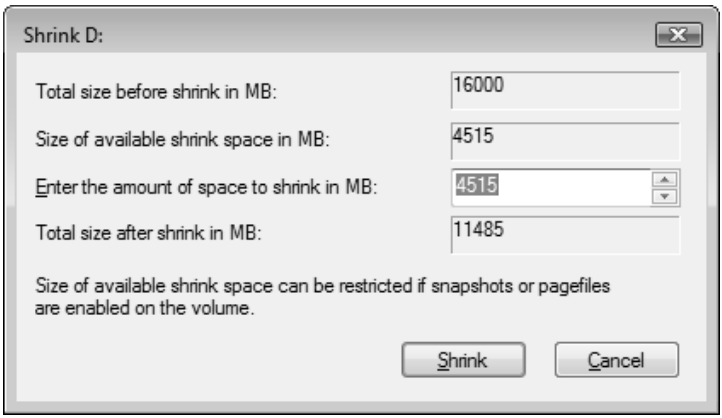


Рис. 7.11. Выбор параметров сжатия диска

Дефрагментация дисков

Операционная система не всегда располагает файлы в одном непрерывном пространстве. Фрагменты данных могут находиться в различных кластерах жесткого диска. В результате при удалении файлов освобождающееся дисковое пространство также становится фрагментированным. Чем выше степень фрагментации жесткого диска, тем ниже производительность файловой системы.

Для решения этой проблемы в состав операционных систем Windows Vista и Windows Server 2008 включена новая утилита *Disk Defragmenter* (Дефрагментация диска) (рис. 7.12).

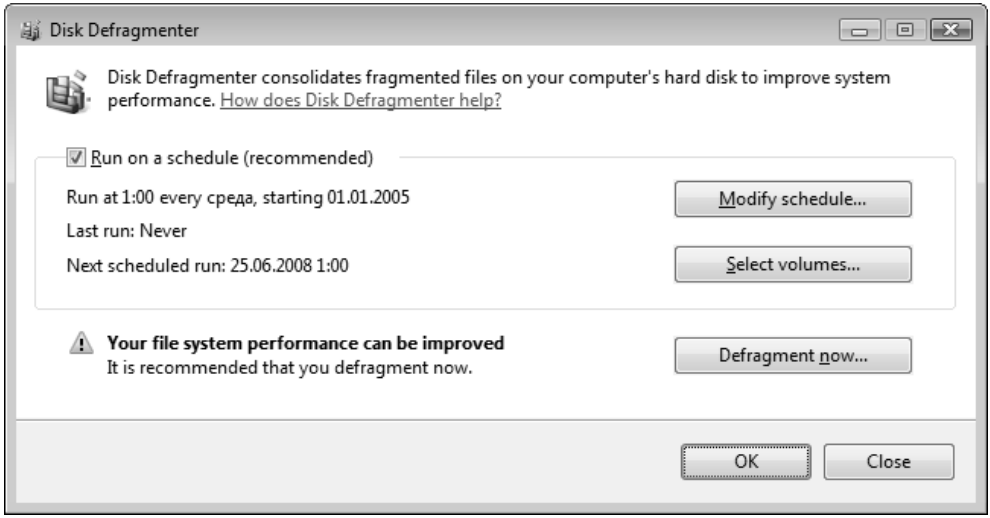


Рис. 7.12. Окно утилиты Disk Defragmenter

Примечание

Оснастка **Disk Defragmenter** (Дефрагментация диска), имеющаяся в Windows XP и Windows Server 2003, в составе систем Windows Vista и Windows Server 2008 отсутствует.

Утилиту Disk Defragmenter можно запустить из меню **Start** | **All programs** | **Accessories** | **System Tools** (Пуск | Другие программы | Стандартные | Служебные) или в окне свойств любого дискового тома на вкладке **Tools** (Сер-

вис), нажав кнопку **Defragment Now** (Выполнить дефрагментацию). Еще один вариант — выбрать задачу **Defragment your hard drive** (Дефрагментация жесткого диска) в разделе **Administrative Tools** (Администрирование), относящемся к категории **System and Maintenance** (Система и ее обслуживание) (этот вариант возможен, если только панель управления отображается с делением по категориям).

В системах Windows Server 2008 дефрагментация по умолчанию не выполняется. Если включить ее выполнение по расписанию (флажок **Run on a schedule** (Выполнять по расписанию) — см. рис. 7.12), то операция будет запускаться раз в неделю. Нажав кнопку **Modify schedule** (Изменить расписание), можно открыть окно параметров запуска задачи (рис. 7.13), в котором легко установить режим работы дефрагментатора дисков, не мешающий пользователю. Кнопка **Select Volumes** (Выбрать тома) позволяет открыть окно выбора томов (дисков), которые будут задействованы в процессе работы (по умолчанию выбраны все диски). Для принудительного и немедленного запуска утилиты следует в ее окне нажать кнопку **Defragment now** (Выполнить дефрагментацию).

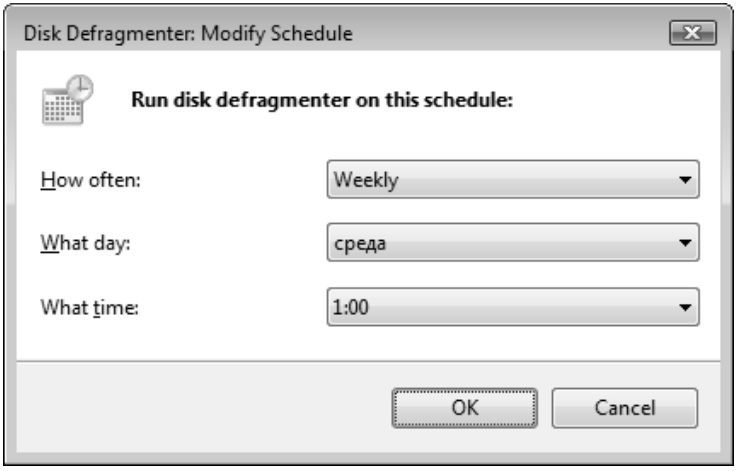


Рис. 7.13. Окно настройки расписания работы дефрагментатора дисков

Процесс работы утилиты Disk Defragmenter никак не визуализируется, лишь в окне программы отображается сообщение о выполнении операции (которую можно в любой момент отменить).

В системе имеется также утилита дефрагментации *Defrag.exe*, запускаемая из окна консоли. Параметры утилиты можно получить, введя строку `defrag /?`. (Например, с помощью команды `defrag F: -r -v` можно выполнить частичную дефрагментацию диска F:.) Для запуска операции дефрагментации по расписанию в библиотеке планировщика задач (Task Scheduler Library) (см. рис. 4.41) имеется стандартная задача Defrag, которую можно найти в папке **Microsoft** | **Windows**. По умолчанию эта задача настроена на запуск раз в неделю (что мы и видели ранее).

> ***Примечание***
>
> Для очистки дисков от ненужных файлов имеется утилита *Disk Cleanup* (Очистка диска), которую можно найти в папке **All Programs** | **Accessories** | **System Tools** (Все программы | Стандартные | Служебные) в меню **Start** (Пуск).

Традиционные средства управления общими дисковыми ресурсами

Рассмотрим способы настройки общего доступа к дискам и отдельным папкам, благодаря чему информация, хранящаяся на сервере, может быть доступна по сети для пользователей других компьютеров.

В системах Windows Server 2008 имеются различные средства управления общими ресурсами — как существовавшие в предыдущих версиях Windows, так и совершено новые, — мы будем их рассматривать в очередности "от простого к сложному".

> ***Примечание***
>
> Помимо описанных ниже средств, управлять общими ресурсами можно с помощью традиционных команд `net share`, `net use` и `net view`, запускающихся в окне консоли. Примеры их использования будут приведены далее в отдельном разделе главы.

Управление общим доступом из программы Windows Explorer

Во всех версиях Windows для создания и администрирования общих дисковых ресурсов может использоваться программа Windows Explorer (Провод-

ник) — достаточно выбрать нужную папку, в контекстном меню выполнить команду **Share** (Общий доступ и безопасность) и в окне свойств папки разрешить общий доступ. В системах Windows Vista/Windows Server 2008 порядок включения общего доступа несколько изменился.

Начальный вид вкладки **Sharing** (Доступ) в этих системах показан на рис. 7.14. Это окно будет выглядеть так для любой выбранной папки. Для разрешения/запрета на доступ к папке используются кнопка **Share** (Общий доступ) и кнопка **Advanced Sharing** (Дополнительный доступ) (использование второй кнопки требует административных привилегий). Рассмотрим по очереди эти две возможности управления общим доступом.

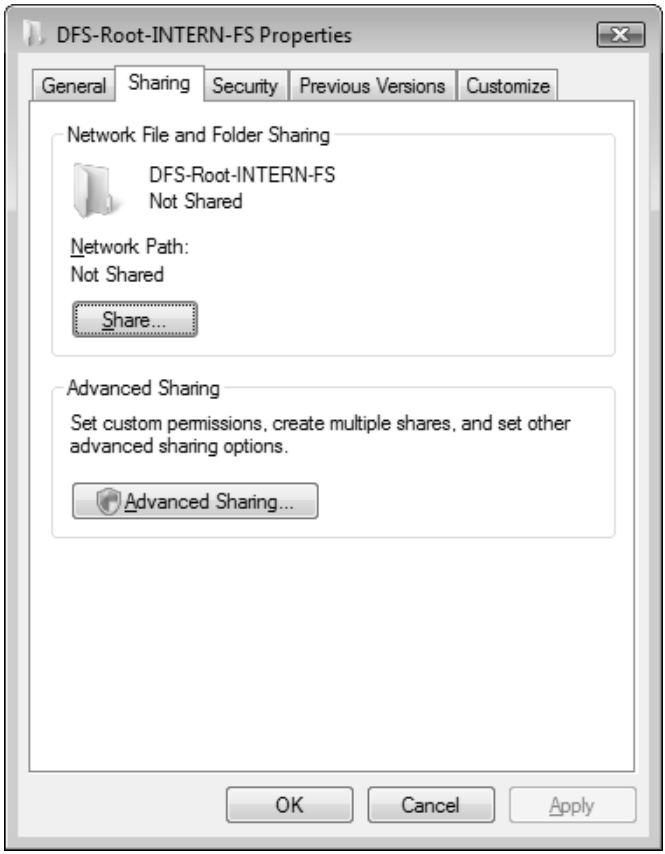


Рис. 7.14. Вкладка окна свойств папки, где можно управлять общим доступом

Примечание

Процедура управления общим доступом одинакова и для автономных систем, и для компьютеров — членов домена, хотя в доменах лучше использовать так называемый "классический" подход *(см. далее)*.

В окне программы Windows Explorer (Проводник) папки, к которым разрешен общий доступ, имеют дополнительный крошечный значок  .

Мастер общего доступа

Если на вкладке **Sharing** (Доступ) в окне свойств папки нажать кнопку **Share** (Общий доступ) (см. рис. 7.14), то запустится мастер *Sharing Wizard* (Мастер общего доступа) (рис. 7.15).

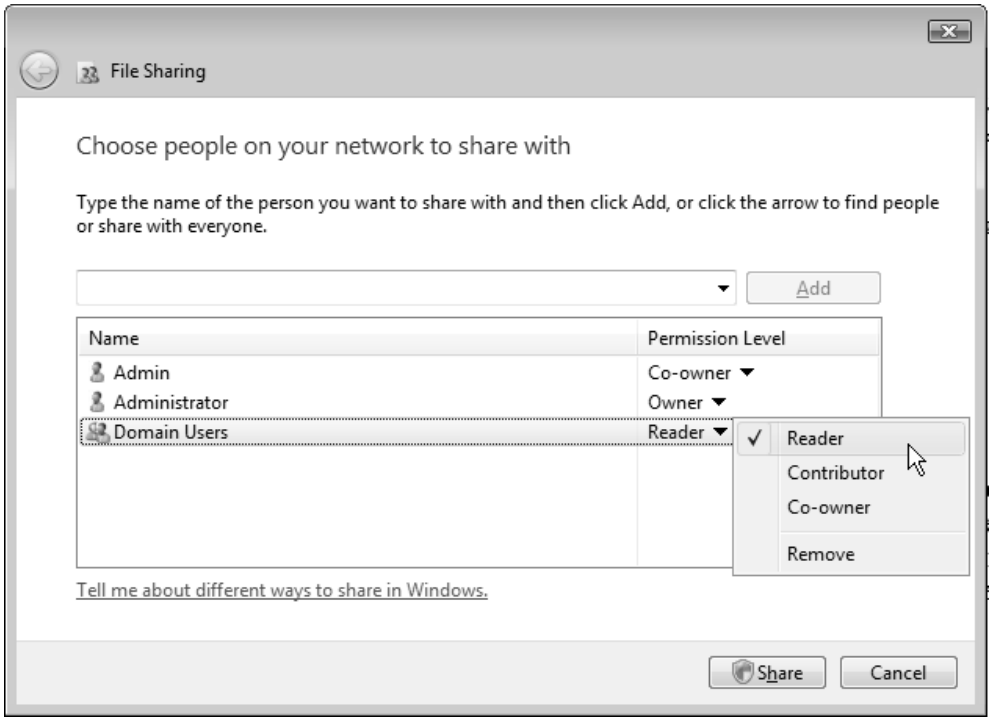


Рис. 7.15. Выбор разрешений с помощью мастера общего доступа

Он позволяет выполнять основные операции по управлению общим доступом к папке и используется, в первую очередь, в простых одноранговых сетях. Этот мастер запускается *сразу*, если в контекстном меню выбранной папки выполнить команду **Share** (Общий доступ) или нажать кнопку **Share** (Разрешить общий доступ) на панели задач.

Внимание!

Для того чтобы в программе Windows Explorer (Проводник) можно было использовать мастер общих ресурсов, необходимо, чтобы в окне свойств папок (см. рис. 2.26) (команда **Organize | Folder and Search Options** (Упорядочить | Свойства папок и поиск) на вкладке **View** (Вид) был установлен флажок **Use Sharing Wizard** (Использовать мастер общего доступа). В противном случае кнопка **Share** (Общий доступ) на вкладке **Sharing** (Доступ) окна свойств выбранной папки (см. рис. 7.14) будет недоступна.

По умолчанию в списке пользователей, которым разрешен доступ к папке (см. рис. 7.15), указан только владелец (Owner) папки. Если раскрыть список, расположенный слева от кнопки **Add** (Добавить), то в нем можно выбрать опцию **Everyone** (Все) или перейти в выбору учетной записи пользователя или группы из числа имеющихся на компьютере или в домене — после чего добавить ее в список пользователей папки.

Примечание

Вообще, следует отметить, что разрешения на доступ к папкам обычно предоставляют группам, а не пользователям. Этот момент подробно рассматривается в *разд. "Управление доступом к файлам и папкам" главы 14*.

Новому пользователю или группе по умолчанию дается разрешение **Reader** (Читатель), позволяющее только читать данные. Опция **Contributor** (Соавтор) разрешает чтение и запись, а опция **Co-owner** (Совладелец) разрешает полный (Full) доступ. После того как все пользователи и уровни разрешений выбраны, следует нажать кнопку **Share** (Общий доступ), и операция будет выполнена. Мастер сообщит о создании новой общей папки, и в результирующем окне можно выбрать ссылку просмотра всех общих ресурсов компьютера. К мастеру общих ресурсов можно обращаться и позднее — для изменения разрешений доступа или для отмены общего доступа к папке.

Примечание

В окне мастера общего доступа (см. рис. 7.15) нельзя формально отличить локального пользователя или группу от доменных. Это создает определенные неудобства, поэтому в доменах для управления разрешениями доступа лучше использовать расширенные возможности, рассматриваемые ниже.

Внимание!

Важной особенностью мастера общего доступа является то, что одновременно с предоставлением учетной записи пользователя или группы прав доступа к общему ресурсу мастер дает соответствующие разрешения ***на уровне файловой системы*** (см. подробнее в *разд. "Управление доступом к файлам и папкам" главы 14*). Соответственно изменяются (отзываются) разрешения и при удалении учетной записи из списка пользователей общего ресурса. При ручном управлении разрешениями *(см. след. разд.)* такого не происходит — права доступа и разрешения на уровне файловой системы изменяются независимо друг от друга.

Традиционный подход

Для более детальной настройки разрешений доступа к папке можно использовать традиционный для предыдущих версий Windows подход (хотя интерфейс этой операции в системах Windows Vista/Windows Server 2008 совершенно изменился). Если на вкладке **Sharing** (Доступ) в окне свойств папки нажать кнопку **Advanced Sharing** (Дополнительный доступ) (см. рис. 7.14), то откроется окно, по функциям напоминающее вкладку **Sharing** (Доступ) в системах Windows XP и Windows Server 2003. Для разрешения общего доступа в этом окне (рис. 7.16) нужно установить флажок **Share this folder** (Открыть общий доступ к этой папке).

В поле **Share name** (Имя общего ресурса) указывается произвольное название общей папки (впоследствии это поле может стать списком, поскольку имен у общей папки может быть несколько — нажав кнопку **Add** (Добавить), можно определить дополнительное имя; для каждого имени будет свой набор разрешений). Чтобы задать разрешения доступа, нужно нажать кнопку **Permissions** (Разрешения) и в открывшемся окне (рис. 7.17) выбрать требуемые параметры доступа. Кнопка **Caching** (Кэширование) позволяет перейти к настройкам режима использования папки в автономном режиме (см. рис. 7.41).

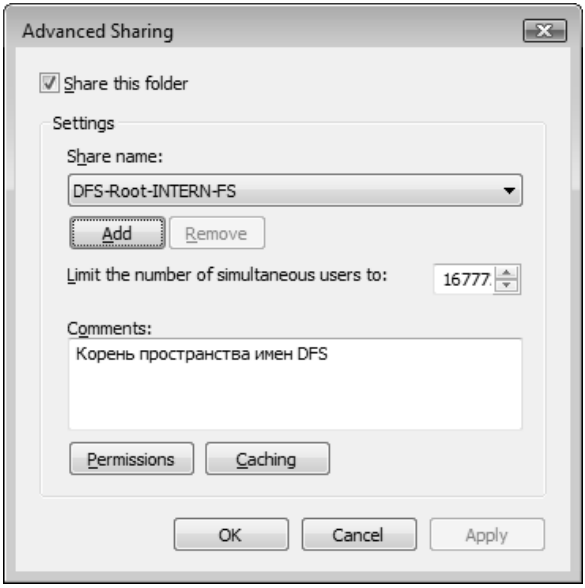


Рис. 7.16. В этом окне можно выбрать параметры общего доступа к папке

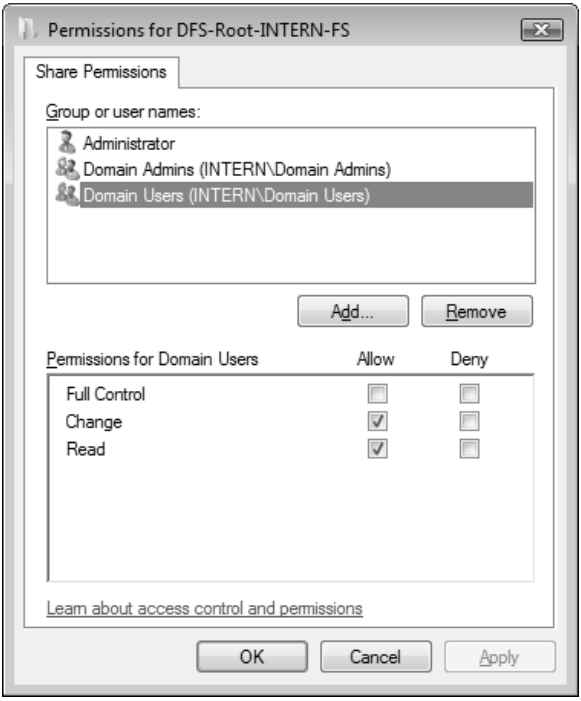


Рис. 7.17. Выбор разрешений доступа к общей папке

После того как все разрешения выбраны и окно закрыто, в окне настройки общего доступа (см. рис. 7.16) нужно нажать кнопку **ОК**, после чего общая папка будет создана. Все описанные выше окна используются и при редактировании параметров общего доступа.

> ***Внимание!***
>
> Все аспекты безопасности общих сетевых ресурсов рассматриваются в *разд. "Назначение разрешений на доступ" главы 14*, поскольку разрешения доступа нужно определять в совокупности с разрешениями, установленными на уровне файловой системы. Автоматически это делает только мастер общего доступа, описанный в предыдущем разделе.

Оснастка *Shared Folders*

Для администрирования большого количества общих папок предпочтительнее использовать традиционную автономную оснастку **Shared Folders** (Общие папки, fsmgmt.msc), которая позволяет работать как с локальными ресурсами, так и с удаленными компьютерами.

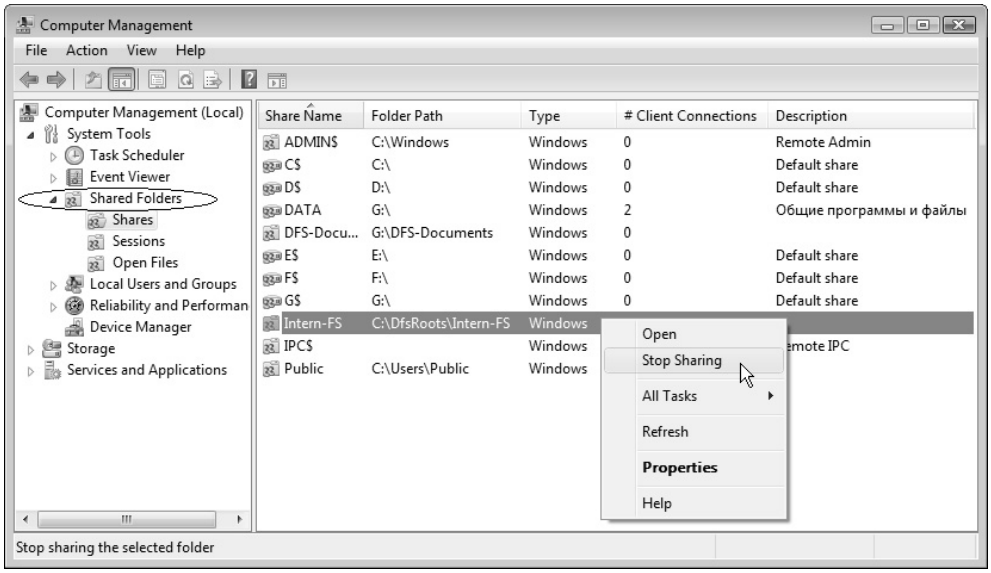


Рис. 7.18. Окно оснастки **Shared Folders** в составе инструмента **Computer Management**

С ее помощью можно также управлять сеансами и открытыми файлами. Данная оснастка используется в составе стандартного инструмента администрирования — оснастки **Computer Management** (Управление компьютером) (рис. 7.18) или запускается автономно.

С помощью узла **Shares** (Общие ресурсы) оснастки **Shared Folders** (Общие папки) можно разрешать и запрещать общий доступ к локальным папкам, а также видеть количество пользователей, подключенных к той или иной папке.

Для создания новой общей папки достаточно выбрать в окне пустое место и щелкнуть правой кнопкой мыши, после чего в контекстном меню нужно выбрать команду **New Share** (Новый общий ресурс). Запустится мастер, с помощью которого легко выполнить все действия, нужные для обеспечения общего доступа к заданной папке.

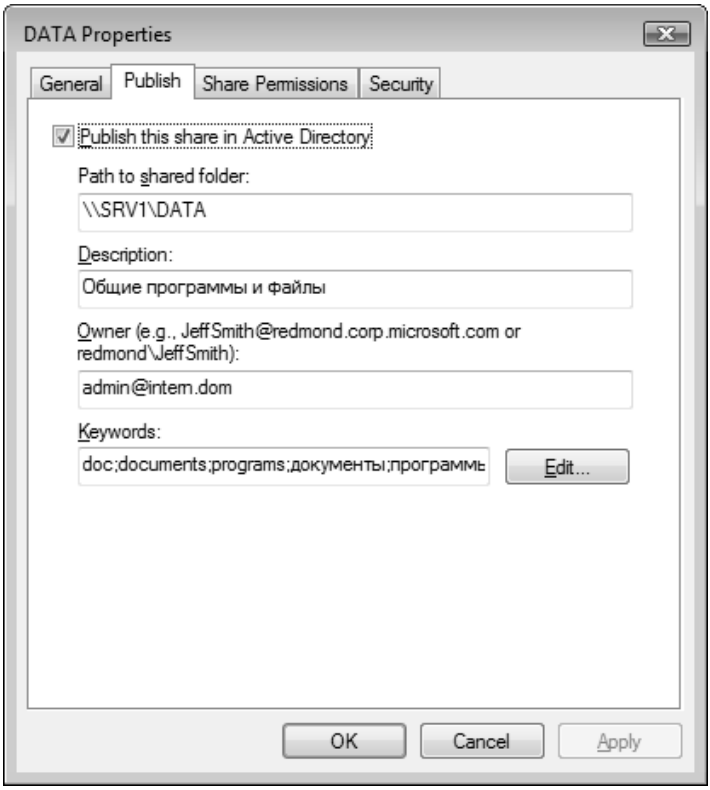


Рис. 7.19. Публикация папки в каталоге Active Directory

В окне свойств общей папки можно редактировать все ее параметры, включая имя, описание, опции кэширования, разрешения доступа и разрешения, заданные на уровне файловой системы. Кроме того, на компьютерах — членах домена можно осуществлять публикацию папки в каталоге Active Directory — для этого имеется соответствующая вкладка (рис. 7.19). Ключевые слова позволяют быстро находить любые ресурсы, опубликованные в каталоге.

Подключение сетевых дисков и использование утилит командной строки

Пользователи сети могут подключить любую постоянно необходимую общую папку в виде *сетевого диска*, который будет присутствовать в списке устройств компьютера. Иногда это необходимо для работы прикладных программ, обращающихся к данным на удаленных компьютерах. Подключения к сетевым дискам могут сохраняться и восстанавливаться при входе пользователя в систему.

Для работы с сетевыми дисками обычно используется программа Windows Explorer (Проводник). Для того чтобы общая папка на удаленном компьютере стала доступной в виде диска, достаточно в окне программы в папке **Network** (Сеть) выбрать компьютер и папку, после чего щелкнуть правой кнопкой и выполнить в контекстном меню команду **Map Network Drive** (Подключить сетевой диск). Диску можно назначить любую свободную букву устройства и указать, требуется ли повторное подключение при каждом входе в систему. Для удаления сетевого диска используется команда **Disconnect** (Отключить) в его контекстном меню.

Все операции по управлению общими папками и сетевыми дисками можно выполнять и в окне консоли. Перечислим основные команды и приведем примеры их использования. Описание параметров каждой команды и ее дополнительных опций можно получить из встроенной справки, запустив ее с ключом `/?`.

Команда `net share` может применяться для просмотра списка общих папок и принтеров, имеющихся на компьютере — для этого ее нужно запустить без параметров[1]. Если выполнить команду, указав имя общей папки, то можно

[1] Эта операция часто бывает полезной при запуске контроллеров домена, поскольку позволяет быстро проверить публикацию общих папок NETLOGON и SYSVOL, без которых нормальная работа контроллера невозможна.

увидеть параметры использования этой папки, включая описание, имена подключившихся пользователей, разрешения на доступ и т. д. — например:

```
C:\>net share DFSSpace-Folder1

Share name        DFSSpace-Folder1
Path              G:\ DFSSpace-Folder1
Remark            Папка пространства имен DFS
Maximum users     No limit
Users             Admin, User
Caching           Manual caching of documents
Permission        INTERN\administrator, FULL
                  INTERN\user, CHANGE
                  SRV1\USER, READ

The command completed successfully.
```

С помощью команды `net share` можно добавлять или изменять разрешения общего доступа, а также редактировать другие параметры общей папки.

Команда `net view` позволяет просматривать список общих папок (включая служебные) на удаленном компьютере, например:

```
C:\>net view \\srv2008

Shared resources at \\srv2008

Domain controller (PDC)

Share name                  Type  Used as  Comment

-------------------------------------------------------------
DFSSpace-Folder1            Disk
E                           Disk  Y:
F                           Disk  Z:
NETLOGON                    Disk           Logon server share
Public                      Disk
SYSVOL                      Disk           Logon server share
Users                       Disk
Windows Server 2008 Builds  Disk

The command completed successfully.
```

Также с помощью этой команды можно увидеть режим кэширования общих папок.

Команда `net use` служит для подключения и отключения сетевых дисков, она позволяет подключить общую папку на удаленном компьютере в качестве сетевого диска и назначить ему букву устройства: например, после выполнения следующей команды в системе появится сетевой диск с именем Z:, который будет представлять собой общую папку `users`, хранящуюся на компьютере `SRV2008`:

```
C:\>net use Z: \\SRV2008\users

The command completed successfully.
```

При подключении сетевых дисков можно явно указывать учетную запись безопасности, используемую для доступа к удаленному компьютеру.

> ***Примечание***
>
> Важным и уникальным достоинством команды `net use` является то, что она позволяет подключить в качестве сетевого диска папку, находящуюся *внутри* общего ресурса (программа Windows Explorer (Проводник) такой возможности не предоставляет). Например, команда `net use Z: \\SRV2008\users\docs` подключает папку `docs`, находящуюся внутри общей папки `users` как диск Z:. Таким образом, пользователь получит доступ к конкретной папке и не сможет видеть другие папки, также находящиеся в общей папке.

Настройка сетевых параметров доступа к общим папкам и принтерам

Если даже к папкам и принтерам компьютера и разрешен общий доступ, для того чтобы пользователи других компьютеров могли обращаться к общим ресурсам данного компьютера, необходимо, чтобы в брандмауэре были разрешены соответствующие порты стека протоколов TCP/IP — таким образом, имеется *набор* параметров различных подсистем, определяющий реальные возможности для клиентов сети, и эти параметры должны быть увязаны между собой. Использование ролей сервера решает эту задачу на начальном этапе (в момент добавления роли с помощью оснастки **Server Manager** (Диспетчер сервера), но в дальнейшем администратор должен сам следить за сетевыми параметрами.

Проще всего выбрать нужные для работы сетевые параметры и настройки безопасности с помощью средств Центра управления сетями и общим доступом (Network and Sharing Center), который запускается с панели управления (категория **Network and Internet** (Сеть и Интернет)) или по щелчку на значке локального подключения на панели задач *(см. главу 8)*. В его главном окне (рис. 7.20) легко выбрать положения переключателей, обеспечивающих требуемые возможности удаленного доступа к ресурсам. В нашем примере показаны параметры для компьютера, входящего в домен (доменная сеть); для публичной (общественной) сети все индикаторы будут в состоянии "выключено". Для изменения параметров нужно щелкнуть по стрелке, расположенной справа от индикатора текущего состояния.

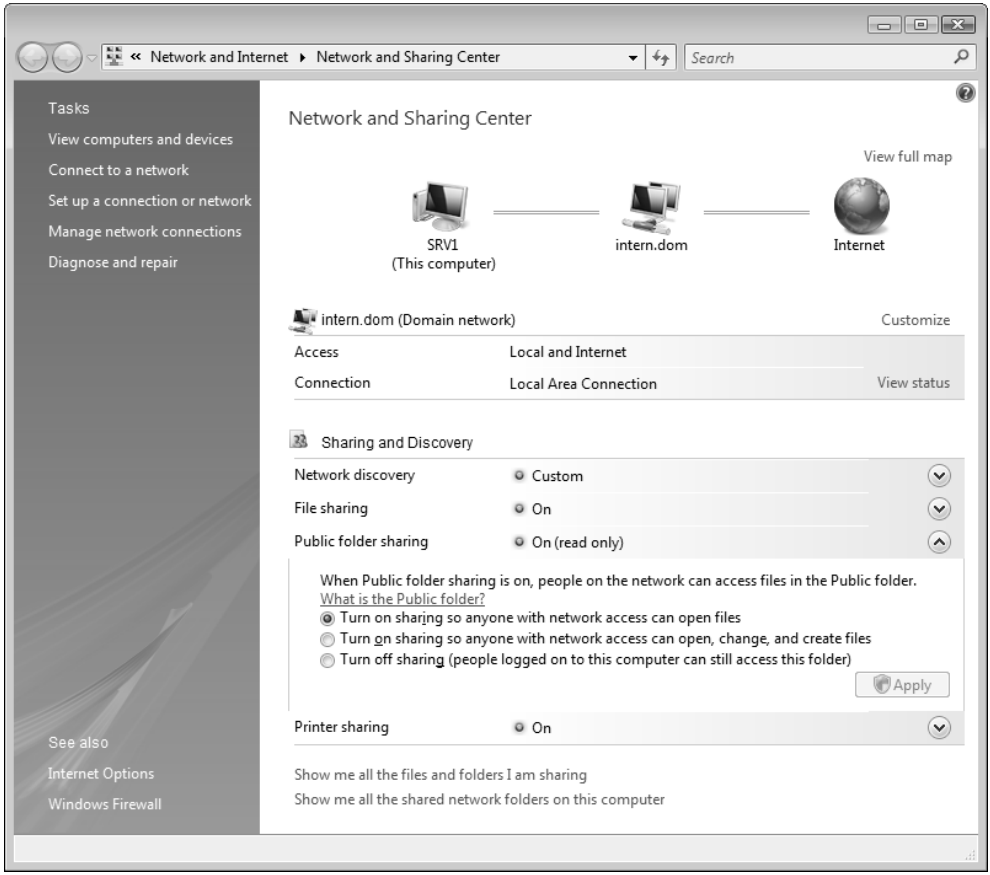


Рис. 7.20. Настройка доступа к общим ресурсам

Совокупность перечисленных ниже опций позволяет определить необходимые и безопасные параметры доступа к общим ресурсам, а также быстро менять их при подключении к другим сетям.

Только при включенном индикаторе **Network discovery** (Сетевое обнаружение) компьютер будет виден в сети; в публичных сетях обнаружение блокируется, и обращение к компьютеру вообще невозможно.

Индикатор **File sharing** (Общий доступ к файлам) позволяет на глобальном уровне разрешить или запретить доступ к общим папкам (при этом остальные индикаторы тоже выключаются). В случае запрета сбрасывается флажок **File and Printer Sharing** (Общий доступ к файлам и принтерам) на вкладке **Exceptions** (Исключения) (см. рис. 8.29) в окне параметров брандмауэра

Windows, и все ресурсы компьютера сразу же становятся невидимыми в сети, при этом имя самого компьютера остается видимым.

Индикатор **Public folder sharing** (Общий доступ к общим папкам[1]) указывает на возможность удаленного доступа к папке **Public** (Общие) локального компьютера. Возможен полный доступ, только чтение или запрет (см. рис. 7.20). Состояние запрета не означает, что пользователи не смогут обращаться к *обычным* общим папкам.

Индикатор **Printer sharing** (Использование общих принтеров) аналогичен индикатору **File sharing** (Общий доступ к файлам), только отображает дополнительное состояние общего доступа к принтерам: если индикатор выключен, то флажки общего доступа у всех принтеров снимаются (это можно проверить в окне свойств имеющихся принтеров).

На компьютерах, не входящих в домен, имеется также индикатор **Password protecting sharing** (Общий доступ с парольной защитой) (рис. 7.21). При отключении парольной защиты доступ к общим ресурсам получают *любые* пользователи (поскольку разблокируется учетная запись Guest (Гость)).

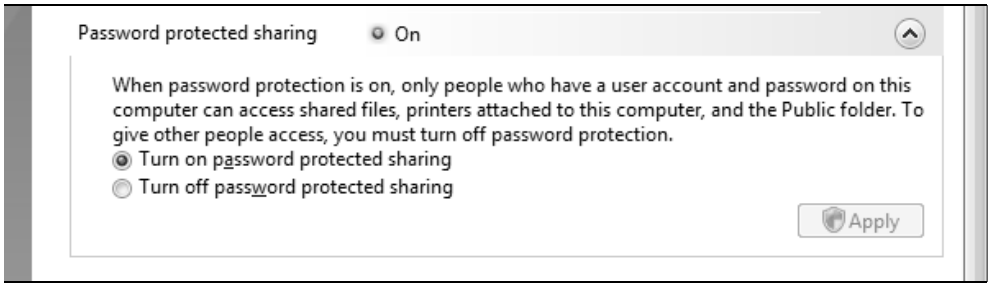


Рис. 7.21. Выбор доступа с парольной защитой

Две ссылки в нижней части окна позволяют просмотреть список общих файлов и папок, к которым будет разрешен доступ с других компьютеров. При выборе последней ссылки отображаются объекты, видимые в папке компьютера в составе узла **Network** (Сеть) (рис. 7.22). Можно сравнить список ресурсов с результатами, получаемыми при помощи команды `net share`. Мож-

[1] Неудачный перевод, сбивающий с толку: имеется в виду не доступ к общим папкам *вообще*, а доступ к папке **Public** (Общие) (см. рис. 3.71).

но также анализировать изменения в этом окне, которые будут происходить при переопределении опций доступа в окне Центра управления сетями и общим доступом.

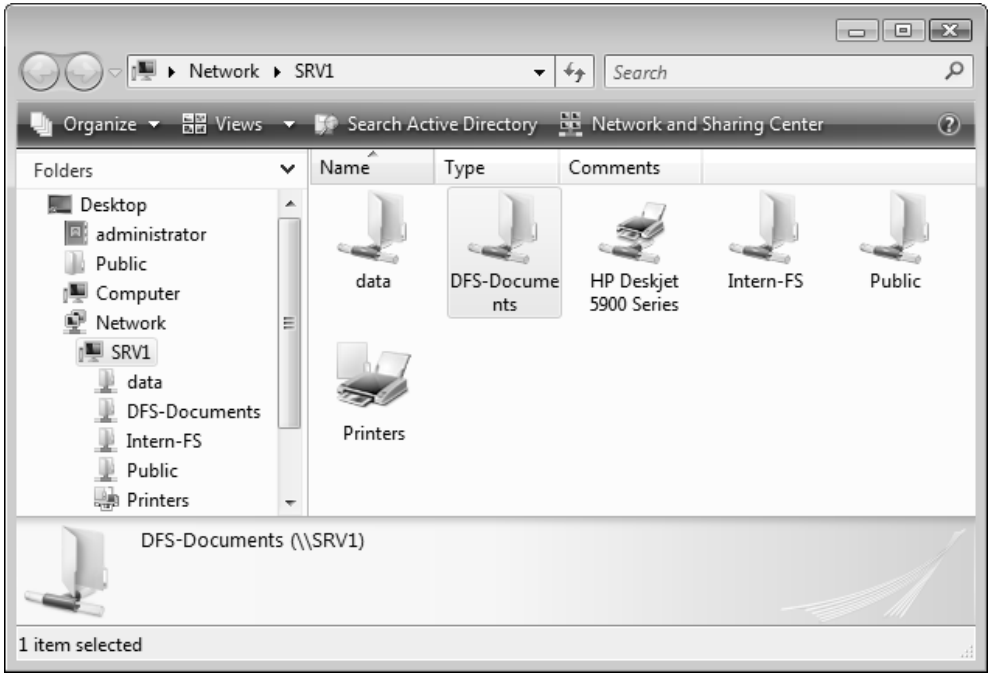


Рис. 7.22. Просмотр общих ресурсов компьютера

Квоты дискового пространства

Для файлового сервера одной из важнейших административных задач является учет дискового пространства, занимаемого файлами пользователей. При этом нужно следить за тем, чтобы один пользователь не занимал слишком много места за счет других. Подобная задача просто решается с помощью введения *квот* (quota) на дисковое пространство, доступное для работы каждому пользователю. Администратор может выделять квоты для *тома* и конкретного *пользователя*. (Из этого следует, что невозможно задать квоту для *отдельных папок* или *групп*.)

Внимание!

Квоты на отдельные папки можно устанавливать с помощью оснастки **File Server Resource Manager** (Диспетчер ресурсов файлового сервера) *(см. далее)*.

Операционная система учитывает пространство, занимаемое файлами, владельцем которых является контролируемый пользователь: если пользователь владеет файлом, размер последнего добавляется к общей сумме занимаемого пользователем дискового пространства. Важно отметить, что, поскольку квотирование выполняется по выбранному тому, не имеет значения, находится ли том на одном физическом жестком диске или на различных устройствах.

После установки квот дискового пространства пользователь сможет хранить на томе ограниченный объем данных, в то время как на этом томе может оставаться свободное пространство. При этом пользователь будет видеть не реальный размер тома, а только объем доступного ему свободного места. Если пользователь превышает установленную квоту, то в журнал событий вносится соответствующая запись. Затем, в зависимости от конфигурации системы, пользователь либо сможет записать информацию на том (более "мягкий" режим ограничений), либо ему будет отказано в записи из-за отсутствия свободного пространства ("жесткий" режим).

Внимание!

Устанавливать и просматривать квоты на диске можно только в NTFS-разделе и при наличии необходимых полномочий (задаваемых с помощью локальных или доменных групповых политик) у пользователя, устанавливающего квоты. Для работы с квотами нужно быть членом группы Administrators (Администраторы).

Примечание

Квотами можно управлять и из командной строки (следовательно, и из командных файлов). Для этого используется утилита Fsutil.exe с параметром `quota`.

Включение механизма квот

Для активизации квот на некотором томе необходимо выполнить следующие действия:

1. В окне программы Windows Explorer (Проводник) выберите конфигурируемый том и нажмите правую кнопку мыши, затем в контекстном меню

выберите команду **Properties** (Свойства). В окне свойств тома перейдите в нем на вкладку **Quota** (Квота) (рис. 7.23).

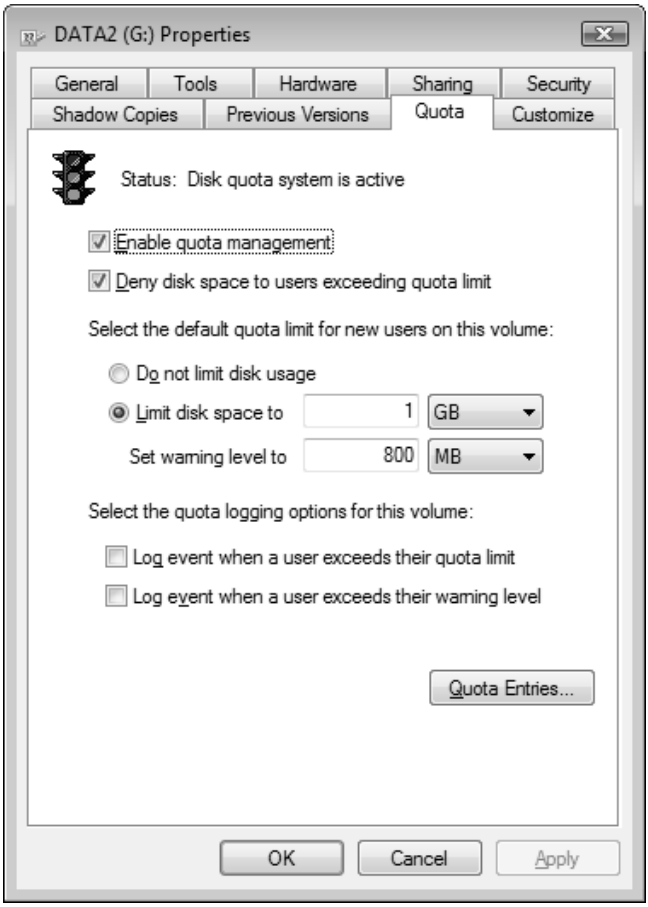


Рис. 7.23. Вкладка **Quota** окна свойств дискового тома

2. Флажок **Enable quota management** (Включить управление квотами) позволяет включить квотирование конфигурируемого тома. В этом случае будет установлен мягкий режим контроля используемого дискового пространства.
3. Если требуется задать жесткий режим ограничения, при котором пользователю в случае превышения квоты будет отказано в доступе к тому, установите флажок **Deny disk space to users exceeding quota limit** (Не выде-

лять место на диске при превышении квоты). Тогда на этой же вкладке нужно установить размер выделяемой квоты (**Limit disk space to** (Выделять на диске не более)) и порог, превышение которого вызывает запись предупреждения в журнал событий (поле **Set warning level to** (Порог выдачи предупреждений)). Эти параметры устанавливаются по умолчанию одинаковыми для всех пользователей; при необходимости можно указать индивидуальные значения для конкретных пользователей.

4. Для регистрации событий превышения квоты можно установить соответствующие флажки, находящиеся в группе **Select the quota logging options for this volume** (Протоколирование превышения квоты для этого тома).

Использование квот

Чтобы увидеть текущее состояние квот и узнать, какие пользователи превысили выделенную им квоту (в мягком режиме), нажмите кнопку **Quota Entries** (Записи квот). Появится окно (рис. 7.24), где отображается список пользователей с параметрами их квот и объемом используемого ими дискового пространства. Учетные записи пользователей, которые превысили установленную для них квоту, отмечены специальным значком в столбце **Status** (Состояние).

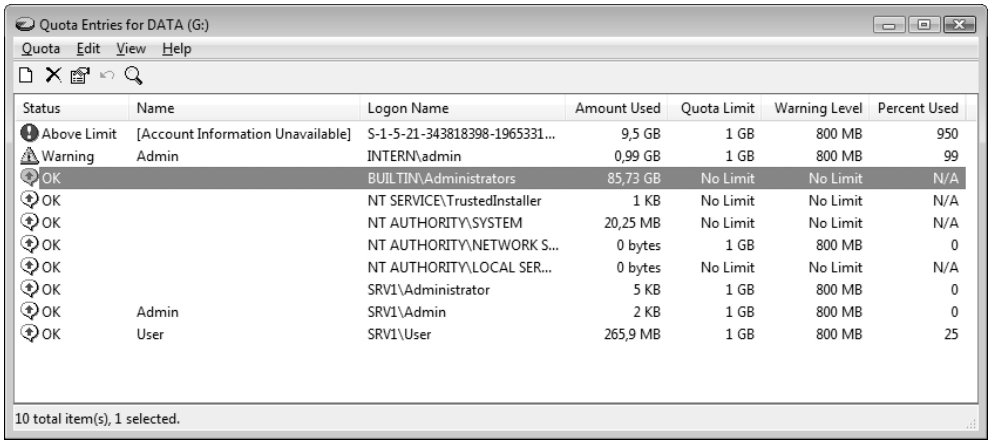


Рис. 7.24. Список пользователей, имеющих файлы на диске, и их дисковые квоты

В окне **Quota Entries** (Записи квот) можно изменить параметры квоты, задаваемой для конкретного пользователя. Для этого выберите конфигурируемую строку и дважды щелкните на ней — появится диалоговое окно **Quota Settings** (Параметры квоты) (рис. 7.25).

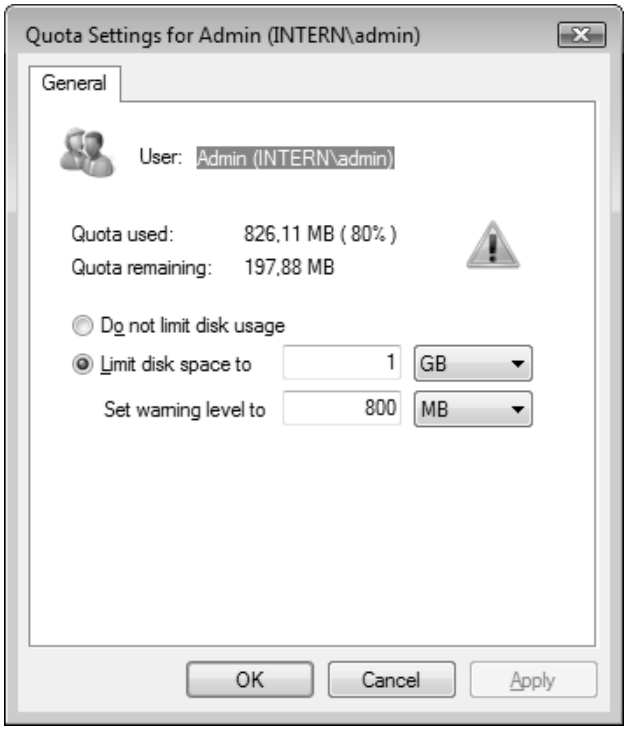


Рис. 7.25. Параметры квоты для конкретного пользователя

Если некоторый пользователь превысил свою квоту и установлен флажок **Log event when a user exceeds their quota limit** (Регистрация превышения квоты пользователем), то в системном журнале регистрируется событие, аналогичное показанному на рис. 7.26 (код события 36, его можно использовать для фильтрации журнала событий). Если при этом задан "жесткий" режим ограничений на расходуемое дисковое пространство (отказ в записи) (т. е. флажок **Deny disk space to users exceeding quota limit** (Не выделять место на диске при превышении квоты) установлен), то при выполнении любой операции записи в квотируемый том, требующей дополнительного пространства, пользователь получит предупреждение, аналогичное изображенному на рис. 7.27.

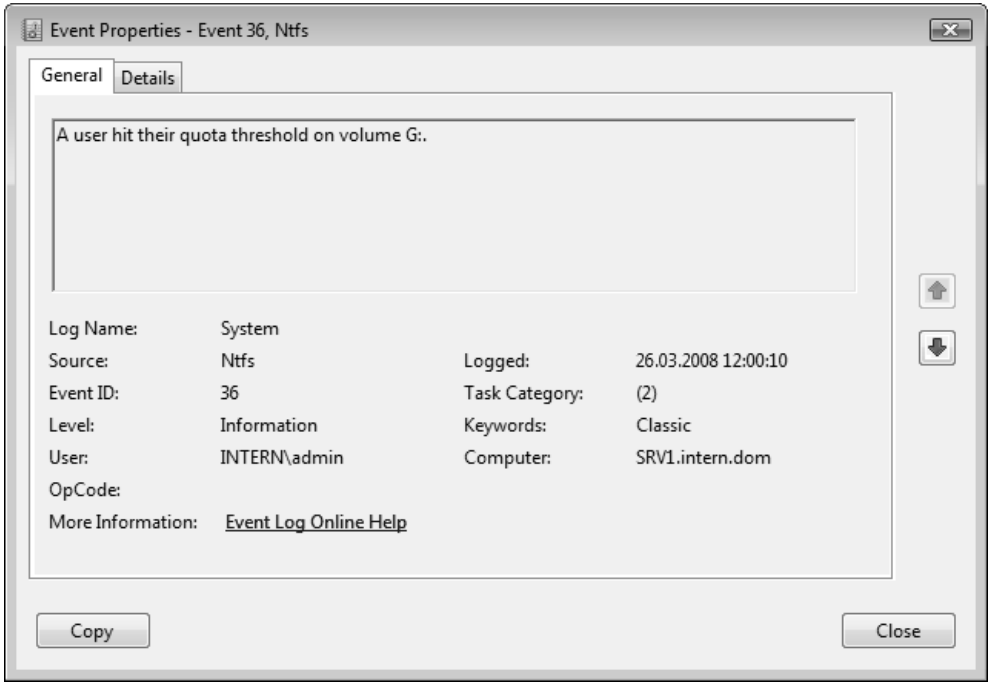


Рис. 7.26. Событие, связанное с превышением пользователем установленной квоты, может регистрироваться в журнале системы

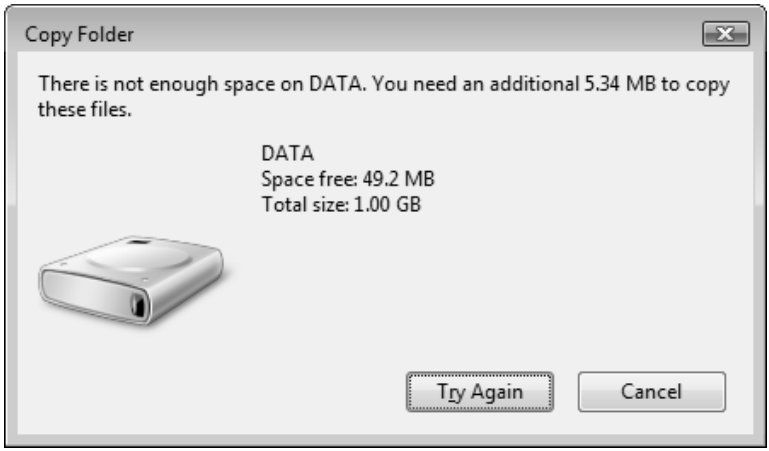


Рис. 7.27. Это сообщение указывает пользователю, что при копировании указанного файла (файлов) он превышает квоту, установленную для него на целевом томе

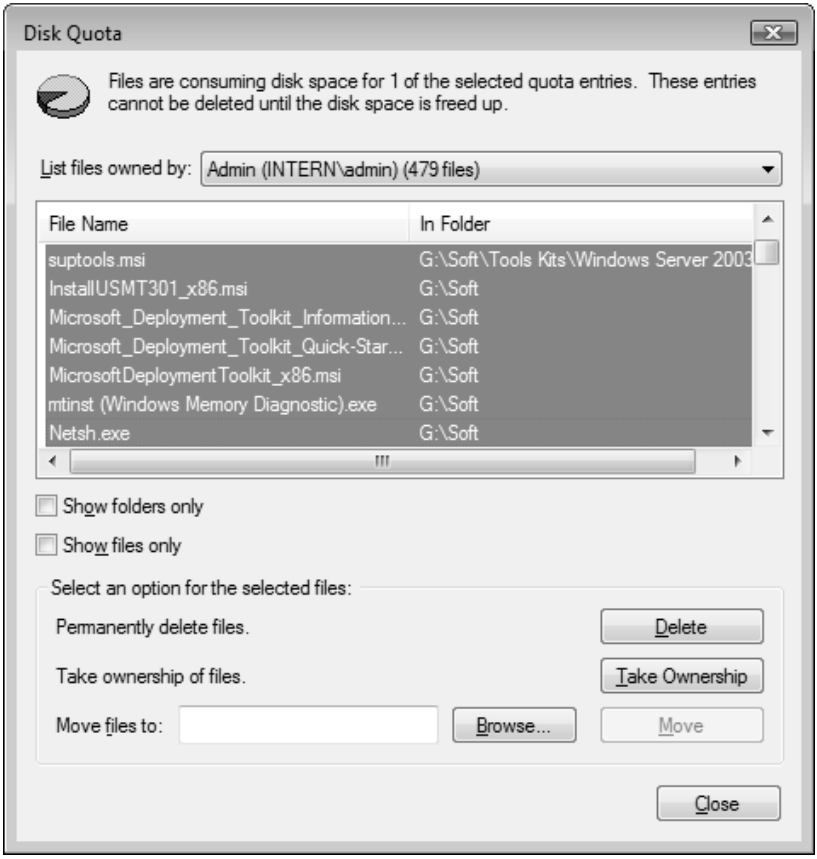


Рис. 7.28. В этом окне перечисляются все файлы (вместе с их точным местоположением), принадлежащие выбранному пользователю на указанном томе с включенным квотированием

Администратор сервера может иметь в виду одну особенность, связанную с регистрацией учетных записей пользователей в списке записей квот (см. рис. 7.24). Если пользователь записал хоть один файл на указанном томе (имеется не нулевое значение в столбце **Amount Used** (Использованный объем)), то его учетную запись нельзя так просто удалить из списка: необходимо, чтобы сначала он удалил всю "принадлежащую" ему информацию. (Или же для этого администратор может стать владельцем файла и выполнить нужные операции.) Это требование дает "побочный эффект", очень удобный для администратора: при попытке удаления имени пользователя, имеющего личные файлы на томе, легко увидеть, *какие именно* файлы принадлежат этому пользователю. (Опасаться тут нечего, поскольку учетную запись можно сразу

удалять из списка записей квот только в том случае, если пользователь ничего не записывал на данный том; в любом случае — операция удаления записей квот напрямую не связана с удалением данных.)

При попытке удаления строки из списка записей квот после подтверждения этой операции выводится список файлов, принадлежащих выбранному пользователю (рис. 7.28) (если у пользователя отсутствуют принадлежащие ему файлы, то запись просто удаляется). В этом же окне администратор может (при необходимости) выполнить операции с перечисленными файлами: стать их владельцем (выделив нужные файлы), а затем удалить или переместить в другое место. (Удалять или перемещать файлы совсем необязательно — просто при изменении "права собственности" эти файлы будут числиться за новым владельцем.)

Управление доступом к ресурсам файлового сервера — оснастка *File Server Resource Manager*

Одним из дополнительных компонентов роли File Services (Файловые службы) является оснастка **File Server Resource Manager** (Диспетчер ресурсов файлового сервера; fsrm.msc); назначение сразу понятно по названиям задач в окне программы — это управление квотами, блокировкой файлов и ресурсами хранилища (рис. 7.29). (Для установки программы используется оснастка **Server Manager** (Диспетчер сервера), в состав которой потом и будет входить эта программа — см. узел **Share and Storage Management** (Управление общими папками и хранилищами).) Каждую из перечисленных задач мы подробно рассмотрим ниже.

> ***Внимание!***
>
> При подключении оснастки **File Server Resource Manager** (Диспетчер ресурсов файлового сервера) к удаленному компьютеру необходимо, чтобы на этом компьютере в брандмауэре Windows было разрешено исключение **Remote File Server Resource Manager Management** (Управление удаленным диспетчером ресурсов файлового сервера).

Перед использованием оснастки **File Server Resource Manager** (Диспетчер ресурсов файлового сервера) важно определить некоторые важные ее параметры, в первую очередь это касается адресов электронной почты (поскольку

заданные по умолчанию значения будут давать ошибки — их нужно заменить на реальную информацию). Для выбора параметров нужно в окне оснастки щелкнуть по ссылке **Configure Options** (Настроить параметры) на панели **Actions** (Действия).

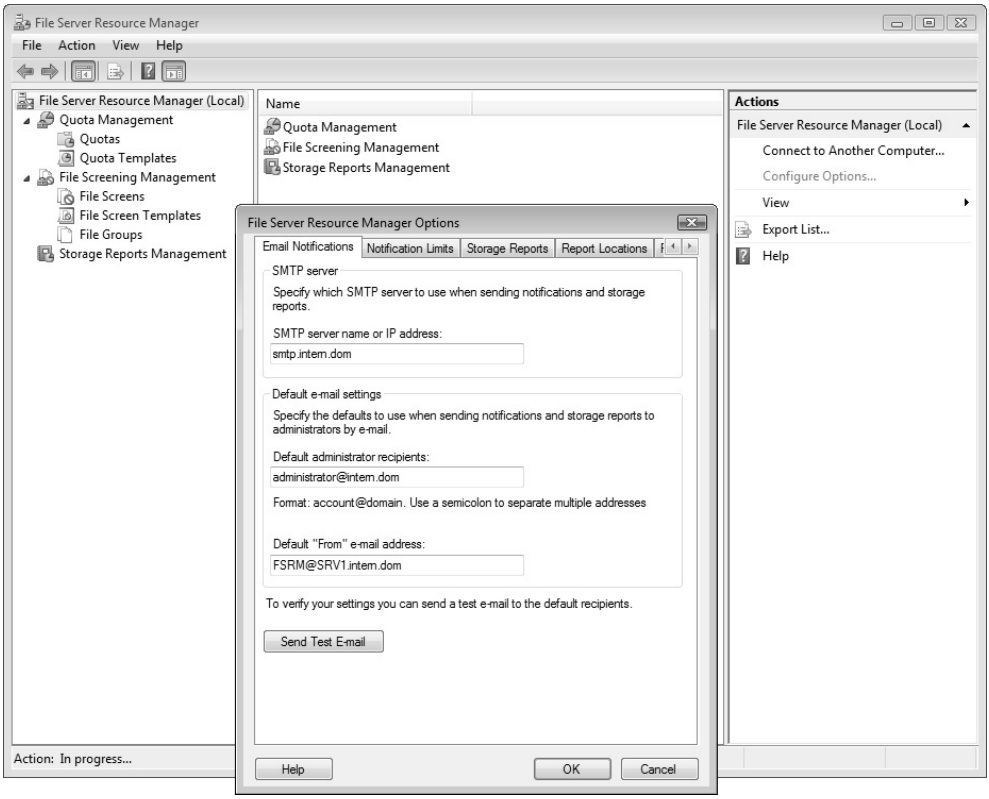


Рис. 7.29. Главное окно оснастки **File Server Resource Manager** и окно основных ее параметров

В окне параметров оснастки (см. рис. 7.29) на вкладке **Email Notifications** (Уведомления) следует указать (или, наоборот, очистить все поля):

- адрес или имя *SMTP-сервера*, через который будет отправляться почта (можно использовать серверы внешних провайдеров при условии правильной настройки);
- *адрес администратора*, который будет получать сообщения;

- *адрес отправителя*, от имени которого будут генерироваться сообщения (это имя важно для работы SMTP-сервера!).

После ввода перечисленных параметров обязательно нажмите кнопку **Send Test E-mail** (Отправить проверочное сообщение) и убедитесь в том, сообщение успешно передано и получено (указанный адресат должен получить сообщение с заголовком "Test notification message for File Server Resource Manager").

Кроме того, рекомендуется просмотреть и при необходимости скорректировать параметры на других вкладках этого окна (здесь, к примеру, определяется место хранения всех создаваемых отчетов). После всех выполненных настроек оснастку можно считать подготовленной к работе.

Управление квотами

Для управления квотами используются так называемые шаблоны квот, которые хранятся в папке **Quota Templates** (Шаблоны квоты) (рис. 7.30).

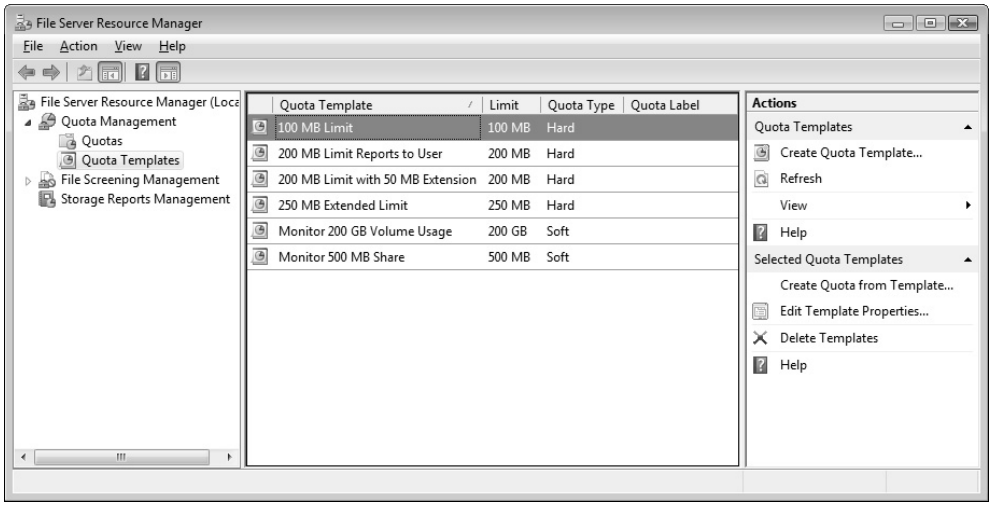


Рис. 7.30. Папка шаблонов квот

Изначально здесь представлены стандартные шаблоны, которые редактировать не рекомендуется — при необходимости следует на их основе создавать собственные шаблоны с требуемыми параметрами. Шаблон квоты определя-

ет пороговое значение для дискового пространства и реакцию на превышение квоты: для "жестких" (hard) квот это отказ в доступе, для "мягких" (soft) — предупреждение.

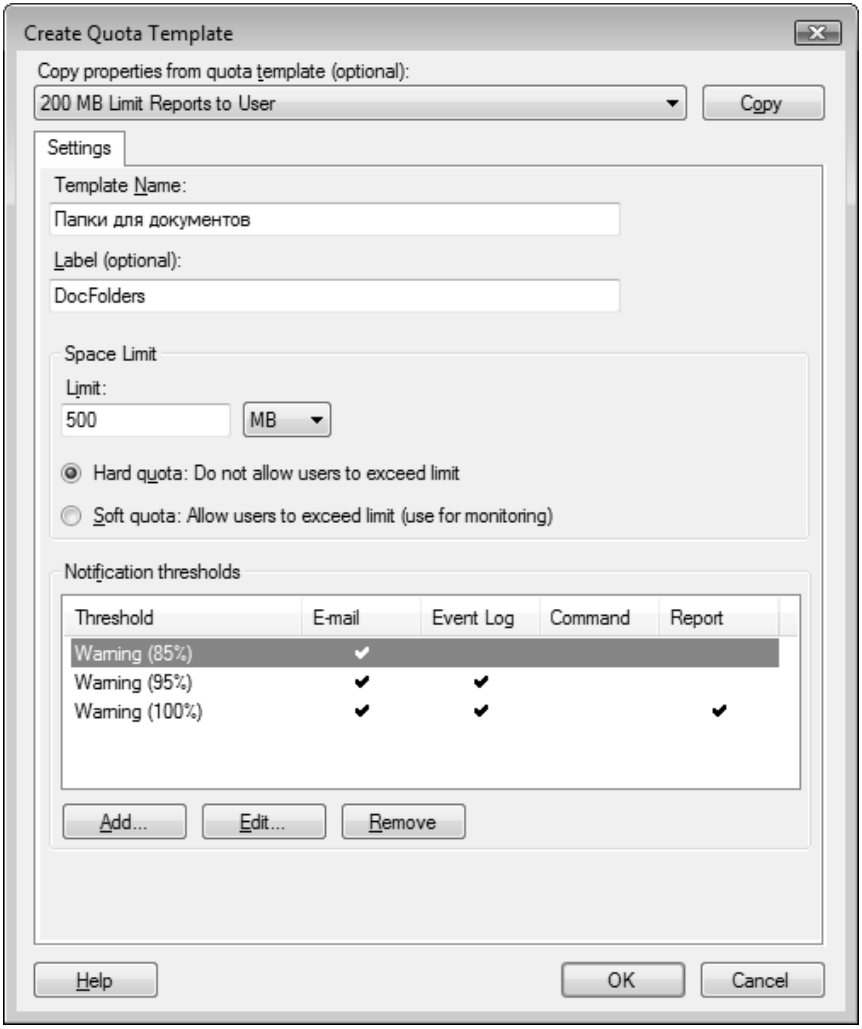


Рис. 7.31. Окно параметров нового шаблона квот

При создании своего шаблона (рис. 7.31) можно скопировать исходные параметры из имеющегося шаблона (раскрывающийся список в верхней части окна), после чего отредактировать их в соответствии со своими потребностя-

ми. Обратите внимание на то, что пороговых значений может быть несколько, и для каждого определен свой набор действий.

Активные квоты отображаются в папке **Quotas** (Квоты) (см. рис. 7.33). Новые квоты можно создавать в этой папке или в уже рассмотренной выше папке шаблонов квот. Чтобы установить квоту, достаточно лишь указать папку, на которую накладывается ограничение, и шаблон квот (рис. 7.32). Как можно видеть, с помощью оснастки **File Server Resource Manager** (Диспетчер ресурсов файлового сервера) квоты можно определять не только для целых томов, но и для отдельных дочерних папок.

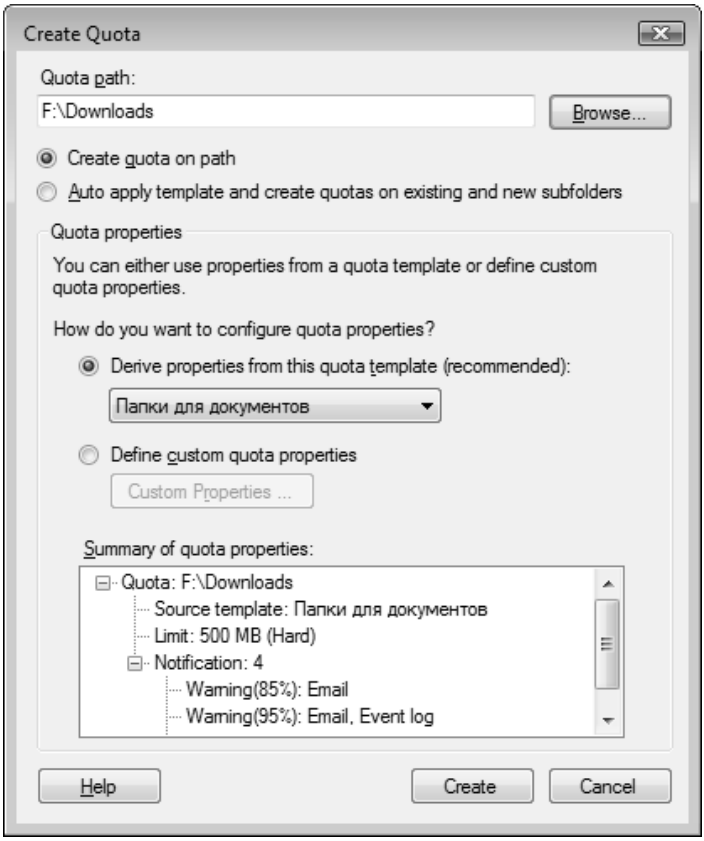


Рис. 7.32. Окно устанавливаемой квоты

В папке **Quotas** (Квоты) (рис. 7.33) видны все установленные квоты с их параметрами, а также текущее состояние папки, на которую действует выде-

ленная квота. Здесь параметры квот можно редактировать, создавать новые квоты и отключать установленные.

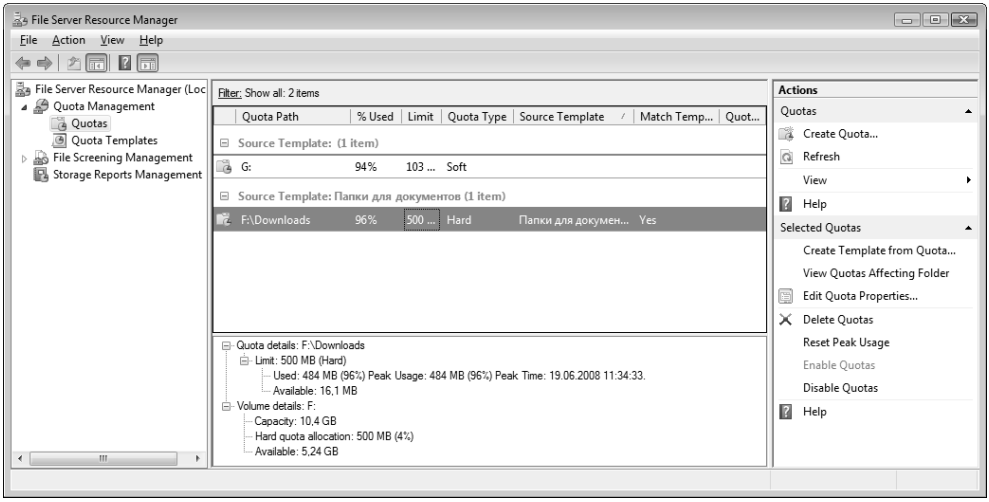


Рис. 7.33. Список активных квот

Если пользователь пытается записать данные в папку, на которую установлена квота с "жестким" ограничением, и превышает пороговое значение, то он получает сообщение об ошибке (рис. 7.34) и должен либо отказаться от операции, либо очистить целевую папку от ненужной информации.

В случае превышения пользователями пороговых значений установленных квот тот администратор, чей адрес указан в параметрах оснастки, получает по электронной почте сообщение с заголовком "Quota limit exceeded" следующего вида:

```
User SRV1\User1 has reached the quota limit for quota on F:\Downloads on
server SRV1. The quota limit is 500.00 MB and the current usage is 483.90
MB (96% of limit).
(Пользователь ... превысил предел квоты для папки... на сервере... Предел
квоты..., текущее использование ...% от предела.)
```

Таким образом, можно видеть, что с помощью средств оснастки **File Server Resource Manager** (Диспетчер ресурсов файлового сервера) можно эффективно контролировать использование дискового пространства на любых томах или отдельных папках. При этом администратор централизованно получает всю детальную информацию о загруженности ресурсов.

Рис. 7.34. Сообщение о нехватке места в папке, на которую наложена квота

Управление блокировкой файлов

Принцип настройки механизма блокировки файлов такой же, как описанная выше процедура установки квот на папки и тома: определяется правило (шаблон) фильтрации файлов и указывается папка, на которую это правило действует.

Все предопределенные (стандартные) и создаваемые шаблоны хранятся в папке **File Screen Templates** (Шаблоны фильтра блокировки файлов) (рис. 7.35), входящей в состав узла **File Screening Management** (Управление блокировкой файлов). Сразу легко понять, для каких файлов делаются ограничения. Имеющиеся шаблоны изменять не рекомендуется, следует на их основе создавать собственные. Каждый шаблон использует одну или несколько *групп*

файлов. Активные шаблоны запрещают запись файлов установленного типа, пассивные — только информируют администратора о создании таких файлов.

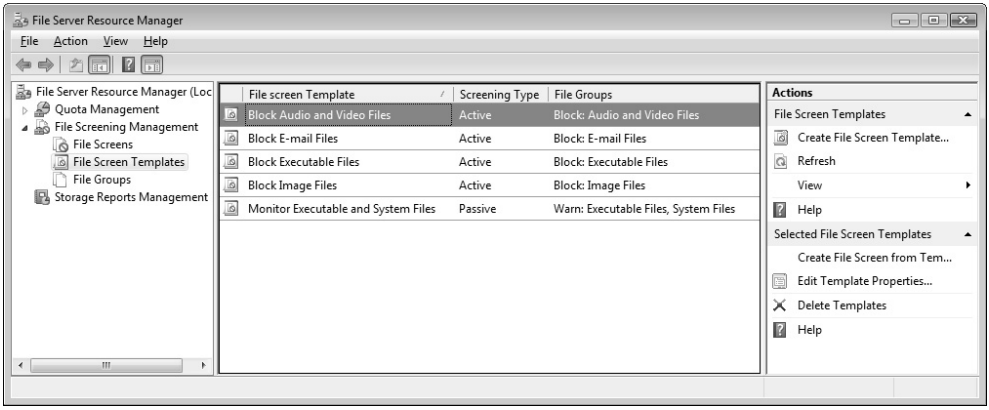


Рис. 7.35. Перечень шаблонов для блокировки файлов

Перед использованием любых шаблонов обязательно нужно просмотреть свойства шаблона и скорректировать адрес электронной почты администратора, который будет получать информацию о блокировке файлов.

В папке **File Groups** (Группы файлов) (рис. 7.36) хранятся описания файлов различных типов, представляющие собой последовательности групповых имен с определенным расширением файла. В группах файлов можно задавать исключения: на файлы этого типа блокировка действовать не будет. Например, можно запретить все файлы изображений, кроме JPG. В этом случае в целевую папку можно будет записывать только изображения указанного типа и файлы других типов (тексты, программы и т. д.), а все остальные графические файлы будут блокироваться.

Установленные правила блокировки файлов хранятся в папке **File Screens** (Фильтры блокировки файлов) (рис. 7.37). В нашем примере заблокирована запись в папку F:\Pictures всех графических файлов, за исключением JPG. Если пользователь попытается записать в папку файл запрещенного типа, он получит на мониторе сообщение о недостаточности прав на выполнение операции; при этом пользователю и администратору могут быть посланы сообщения по электронной почте.

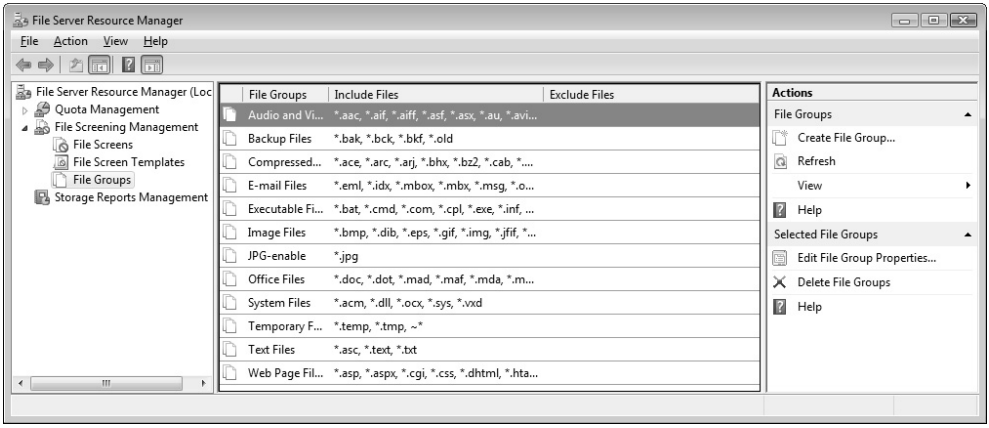


Рис. 7.36. Группы файлов различного типа

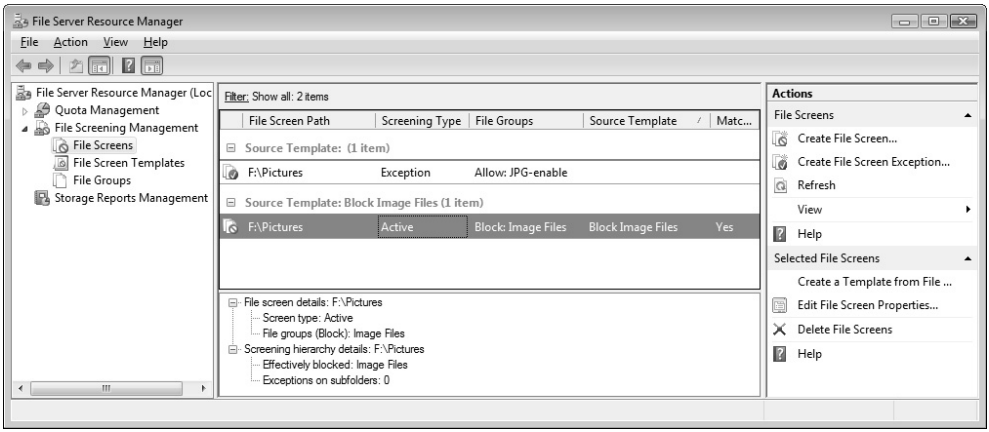


Рис. 7.37. Активные фильтры блокировки файлов

Управление ресурсами хранилища

В папке **Storage Reports Management** (Управление ресурсами хранилища) (рис. 7.38) можно создавать запросы на получение отчетов с заданными критериями для дисковых томов или папок. Эти запросы могут быть разовыми и тут же выполняться, могут храниться и выполняться планировщиком заданий по заданному расписанию. Как видно на рисунке, при создании запроса указывается целевая папка или том (один или несколько объектов), определяют-

ся типы генерируемых отчетов (вкладка **Settings**) и их параметры (**Edit Parameters**), задаются получатели отчета (вкладка **Delivery**). Для планируемых запросов также определяется расписание (вкладка **Schedule**).

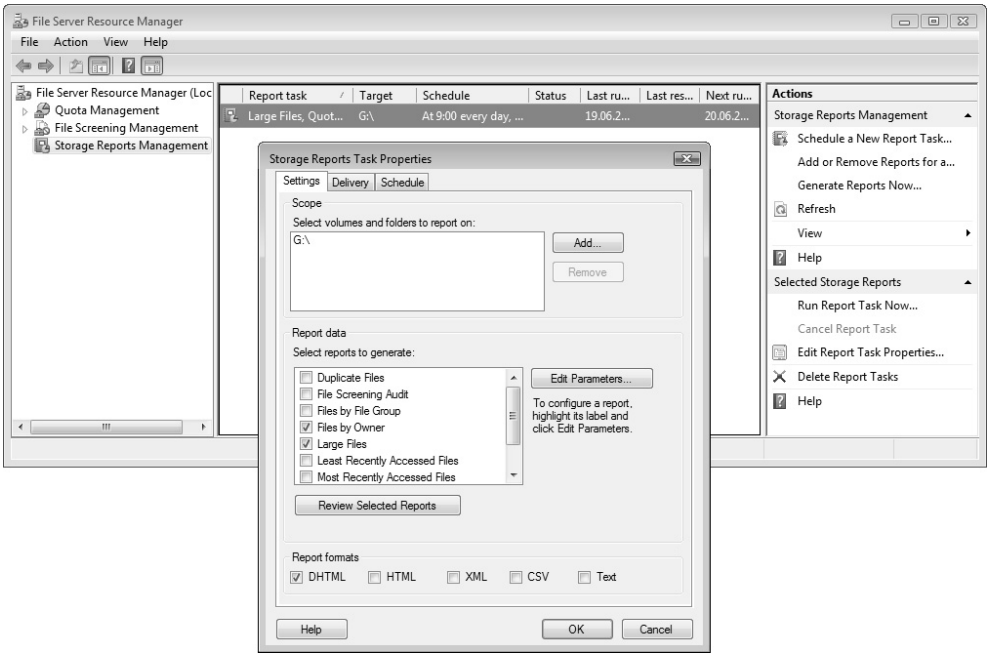


Рис. 7.38. Запланированные запросы и свойства запроса на получение отчетов

Создавать разовые или регулярные запросы можно при помощи команд на панели **Actions** (Действия). Полученные отчеты по умолчанию сохраняются в папке C:\StorageReports в соответствующих подкаталогах:

- *Incident* — автоматически генерируемые отчеты для событий превышения квот или блокировки файлов;
- *Interactive* — отчеты, созданные по запросу пользователя;
- *Scheduled* — отчеты, полученные с помощью запланированных запросов (по расписанию).

Местоположение всех папок задается в окне параметров оснастки (см. рис. 7.29).

Созданные отчеты представляют собой весьма информативные документы (обычно в формате HTML), содержащие таблицы, цветные диаграммы, ана-

литическую информацию и т. п. Их очень легко просматривать, и можно быстро принимать решения на основе собранных данных.

Средство централизованного управления общими ресурсами — оснастка *Share and Storage Management*

Оснастка **Share and Storage Management** (Управление общими папками и хранилищами; StorageMgmt.msc) присутствует в системе по умолчанию; она входит в состав оснастки **Server Manager** (Диспетчер сервера), и ее можно также запускать автономно из подменю **Administrative Tools** (Администрирование).

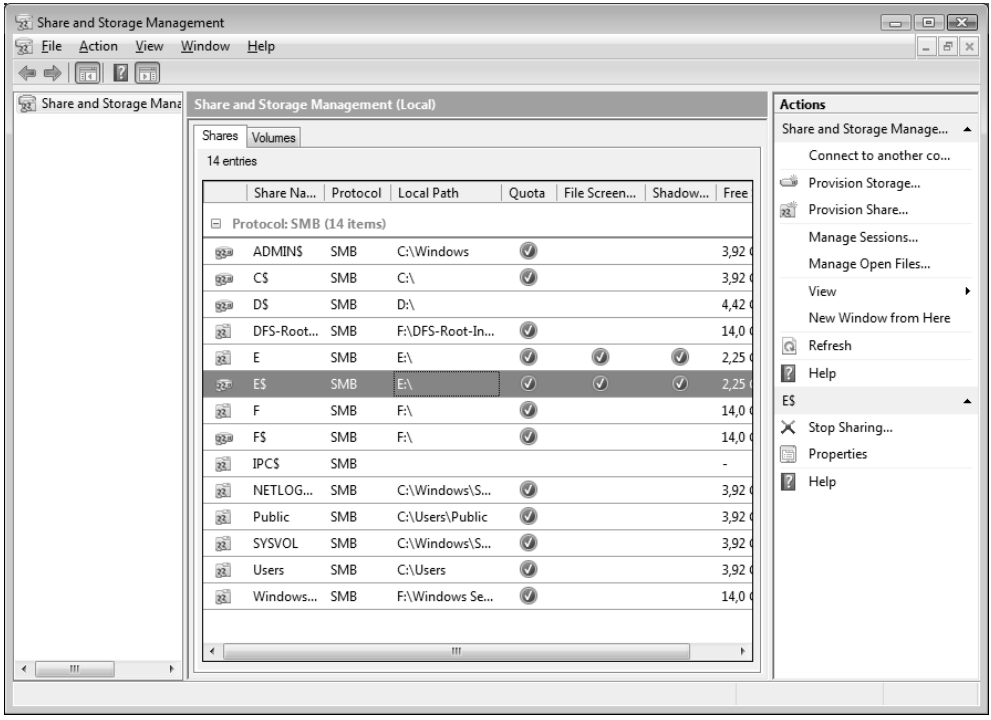


Рис. 7.39. Просмотр списка общих папок в окне оснастки **Share and Storage Management**

Эта оснастка представляет собой инструмент мониторинга и управления самого "верхнего уровня". В ее окне (рис. 7.39) можно сразу видеть общие папки, состояние квот (столбец **Quota**), наличие фильтров блокировки файлов (столбец **File Screening**) и настройки теневых копий (столбец **Shadow Copies**).

Внимание!

При подключении оснастки **Share and Storage Management** (Управление общими ресурсами и хранилищами) к удаленному компьютеру необходимо, чтобы на этом компьютере была запущена служба Virtual Disk (Виртуальный диск; сервис vds) и в брандмауэре Windows *на обоих компьютерах* было разрешено исключение **Remote Volume Management** (Удаленное управление томами).

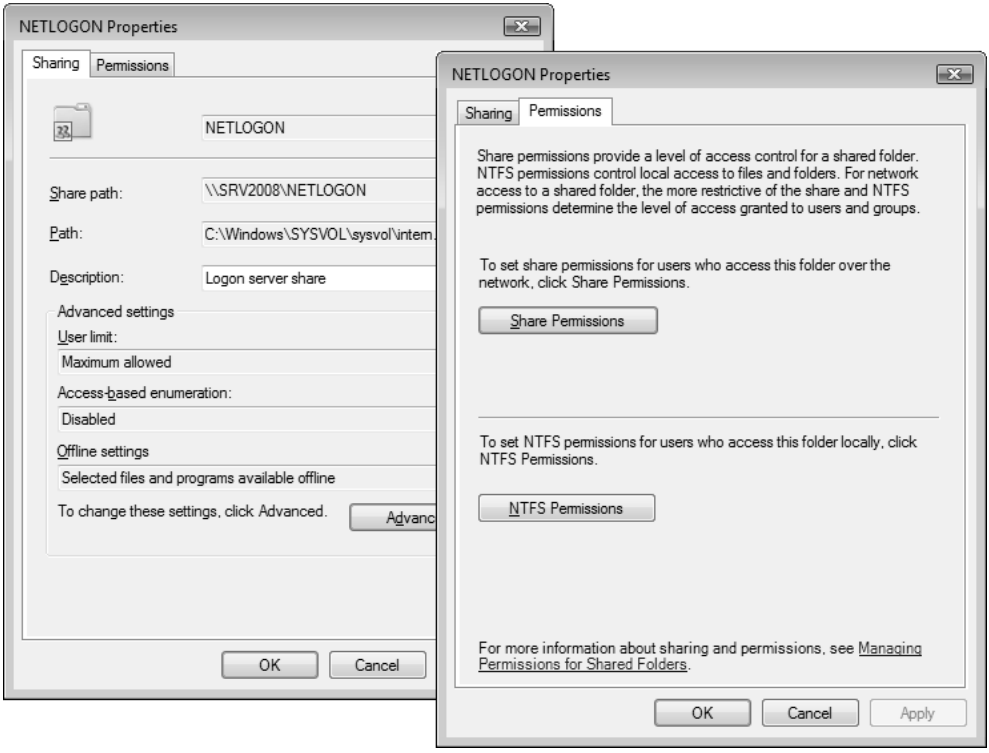


Рис. 7.40. Вкладки окна свойств общей папки

Если дважды щелкнуть по имени общей папки, то откроется окно ее свойств, где можно увидеть все параметры ресурса (рис. 7.40). С вкладки **Permissions** можно сразу получить доступ к спискам разрешений, установленных для общей папки и на уровне файловой системы. Это значительно уменьшает количество операций, необходимых для просмотра всех важных параметров.

На панели **Actions** (Действия) имеются команды, с помощью которых можно увидеть список подключений к ресурсам (ссылка **Manage Sessions**) и список открытых файлов (ссылка **Manage Open Files**). В соответствующих окнах можно просматривать параметры сеансов доступа к папкам, прекращать сеансы и закрывать файлы.

Команда **Provision Storage** (Подготовка хранилища) запускает мастер, с помощью которого можно создать и подготовить к работе новый диск, раздел или том. Такой подход упрощает работу, поскольку при этом используется один инструмент и не требуется запускать дополнительные административные оснастки. По аналогичным причинам эффективен мастер, запускаемый по команде **Provision Share** (Подготовка общего ресурса) — он позволяет в интерактивном режиме создать общую папку, определить для нее разрешения NTFS и параметры протокола доступа (SMB), установить квоту и фильтры блокировки файлов, а также выполнить публикацию ресурса в пространстве имен DFS, если таковое имеется.

Из всего сказанного выше можно сделать вывод, что большие возможности и удобство в работе делают оснастку **Share and Storage Management** (Управление общими папками и хранилищами) главным средством администрирования и мониторинга общих ресурсов для любого файлового сервера на основе Windows Server 2008.

Автономные файлы

Если пользователю необходимо работать с документами, находящимися в общей папке, в условиях отсутствия подключения к сети он может задействовать так называемые *автономные файлы* (offline files). Этот механизм позволяет пользователю при автономной работе не терять возможности просмотра общих сетевых папок и редактирования или запуска нужных файлов, которые были предварительно выбраны или открывались ранее. В этом случае на значках недоступных сетевых общих ресурсов появляется крестик, а файлы и папки, предназначенные для автономной работы, будут помечены особым значком *(см. ниже)*. После повторного подключения к сети система

автоматически переносит все изменения, сделанные пользователем в сетевых файлах в процессе автономной работы, на общий сетевой ресурс.

Права доступа к ресурсам в автономном режиме работы остаются такими же, какие они были при наличии соединения с сетью. Например, документ, доступный на сетевом общем ресурсе только для чтения, будет доступен только для чтения и при автономной работе.

Механизм автономных файлов в первую очередь ориентирован на клиентские рабочие места, однако в системах Windows Server 2008 он также реализован и доступен (хотя в серверных версиях, в отличие от Windows Vista, автономные файлы по умолчанию выключены). По сравнению с предыдущими версиями Windows все вспомогательные операции значительно упрощены (особенно это касается настройки данной функции) и их количество сведено к минимуму.

Выбор параметров кэширования общих папок

Для того чтобы файлы общих ресурсов могли быть доступными для пользователей, отключенных от сети, необходимо предварительно поместить копии этих файлов в локальный кэш компьютера. Кэш компьютера — это часть диска, доступ к которой есть всегда, вне зависимости от наличия подключения к сети. Сервер, хранящий файлы, может указать режим их использования в случае отсутствия соединения. Для автономных файлов имеются три варианта кэширования, показанные на рис. 7.41 (выбор осуществляется при разрешении общего доступа к папке после нажатия кнопки **Caching** (Кэширование)).

- В первом случае (см. рис. 7.41) предполагается, что, отключившись от сети, пользователь сможет открывать только те файлы или папки общего сетевого ресурса, которые он предварительно *явно указал*. Такой тип кэширования оптимален для работы с общим ресурсом, на котором находятся документы или рисунки. Этот вариант кэширования предлагается по умолчанию.
- Второй вариант — когда в автономном режиме будут доступны все те файлы, которые пользователь *запускал* или *открывал* из общей папки при работе в сети. В этом случае нет гарантии, что для автономной работы будут доступны *все* файлы, которые могут потребоваться.

- Кэширование файлов, т. е. их автономное использование, можно вообще *запретить* — это третий вариант.

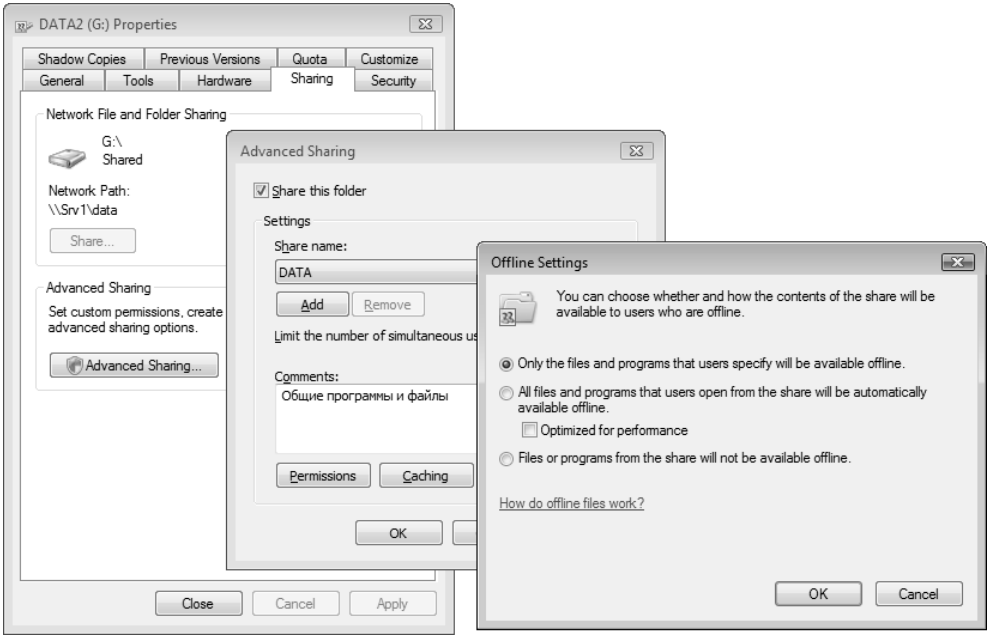


Рис. 7.41. Режимы кэширования файлов в папках с общим доступом

Подготовка компьютера к работе с автономными файлами

Для управления режимом использования автономных файлов запускается задача **Offline Files** (Автономные файлы), имеющаяся на панели управления (категория **Network and Internet** (Сеть и Интернет)). В системах Windows Server 2008 автономные файлы по умолчанию не используются, в окне их параметров (рис. 7.42) сначала требуется нажать кнопку включения. Каждый раз после отключения (кнопка **Disable Offline Files**) или повторного включения автономных файлов систему нужно перезагружать.

Кнопка **Open Sync Center** (Открыть центр синхронизации) запускает Центр синхронизации, о котором будет рассказано дальше. Окно просмотра автономных файлов, хранящихся локально (кнопка **View your offline files**), также будет показано чуть позже.

На вкладке **Disk Usage** (Использование диска) (рис. 7.43) можно регулировать объем локального дискового кэша, в котором хранятся автономные файлы, скопированные с удаленных компьютеров. (Кэш располагается на загрузочном диске, поэтому необходимо иметь на нем запас свободного места.) На вкладке **Encryption** (Шифрование) можно включать и отключать шифрование локально хранимых автономных файлов для их защиты от постороннего доступа. На вкладке **Network** (Сеть) определяется поведение функции автономных файлов при работе по медленным каналам.

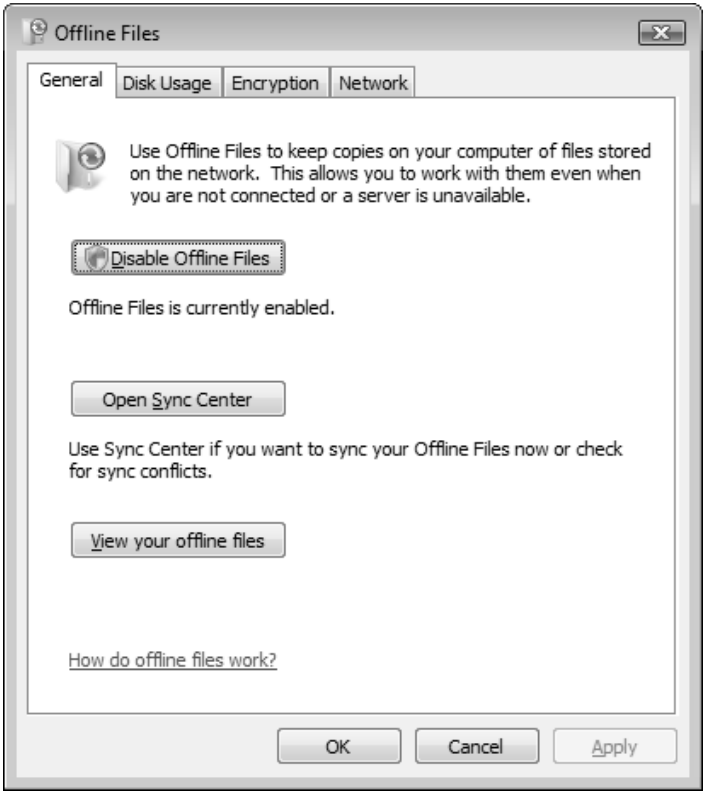


Рис. 7.42. Вкладка **General** окна параметров автономных файлов

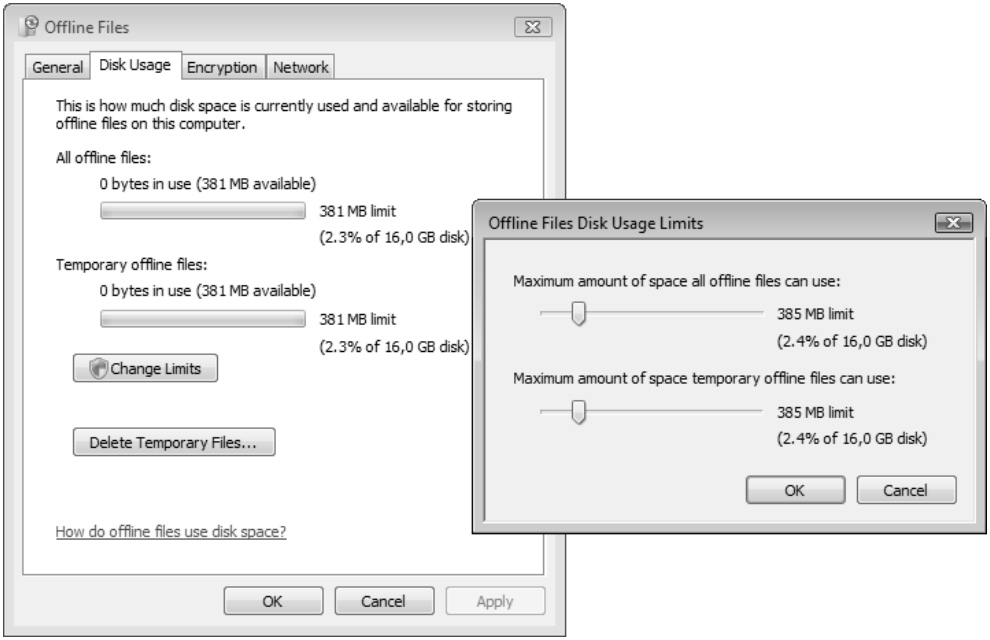


Рис. 7.43. Выбор размера буфера для хранения автономных файлов

Выбор файлов для автономной работы

После выполнения действий, описанных выше, система Windows Server 2008 готова для работы с автономными файлами. Для того чтобы указать, с какими именно файлами и папками необходимо работать автономно, нужно выполнить следующие операции (здесь подразумевается, что на удаленных папках используется режим кэширования, заданный по умолчанию — см. рис. 7.41; в противном случае — второй вариант кэширования — достаточно просто открыть нужный файл):

1. В окне программы Windows Explorer (Проводник) в папке **Network** (Сеть) найдите нужный компьютер и выберите нужные для автономного доступа файлы или папки, находящиеся на общих сетевых дисках.
2. В контекстном меню выполните команду **Always Available Offline** (Всегда доступны в автономном режиме) — сразу же начнется копирование файлов в локальный кэш и появится окно, где можно следить за ходом операции (рис. 7.44). Окно можно закрыть и продолжить работу на компьютере. (Когда необходимость в автономных файлах отпадает, флажок

Always Available Offline (Всегда доступны в автономном режиме) нужно сбросить, и соответствующие файлы будут удалены из кэша.)

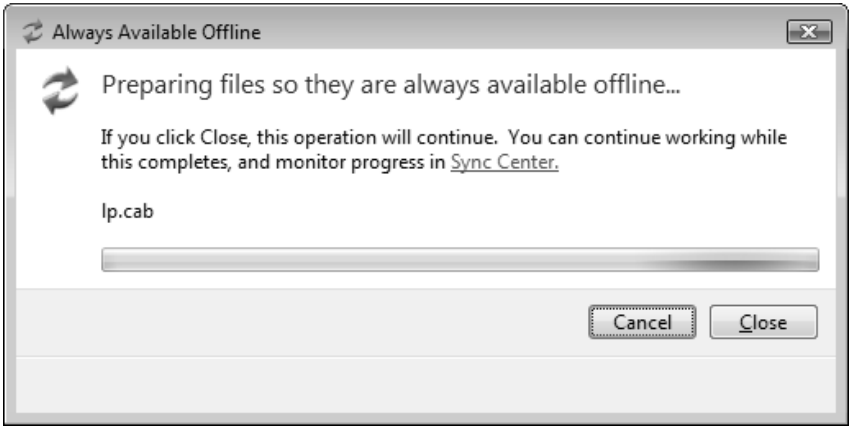


Рис. 7.44. Окно синхронизации, появляющееся при выборе автономной папки или файла

Теперь, после выбора автономных файлов, на панели задач в области уведомлений всегда будет присутствовать значок Центра синхронизации (Sync Center)  . Во время выполнения синхронизации стрелки на значке будут вращаться по кругу, по окончании появится всплывающее сообщение. Если щелкнуть по значку, то окно Центра синхронизации откроется, и в нем можно следить за ходом выполняемой операции.

Теперь выбранные для автономной работы файлы и папки можно изменять и после отключения от сети (или при выключении удаленного компьютера). Нажав кнопку **View your offline files** (Просмотреть автономные файлы) в окне настройки автономных файлов (см. рис. 7.42), можно привычным образом просматривать доступные файлы (рис. 7.45) — все они расположены в папке **Offline Files Folder**. Для большей наглядности выбрано табличное представление имен.

На папке, выбранной для автономной работы, виден значок Центра синхронизации, а также имеется указание на то, что папка доступна, несмотря на отключенное (offline) состояние (т. е. это копия папки, а не реальная папка на удаленном компьютере), и доступ к этой папке возможен всегда (Always available); при этом другие файлы, находящиеся в данной сетевой папке, недоступны.

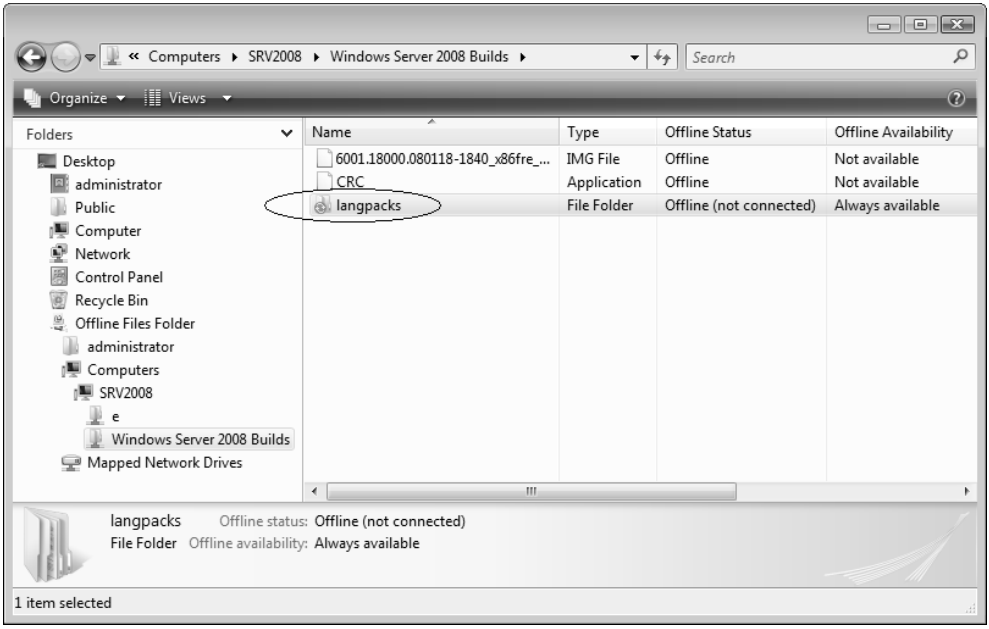


Рис. 7.45. Просмотр папки автономных файлов

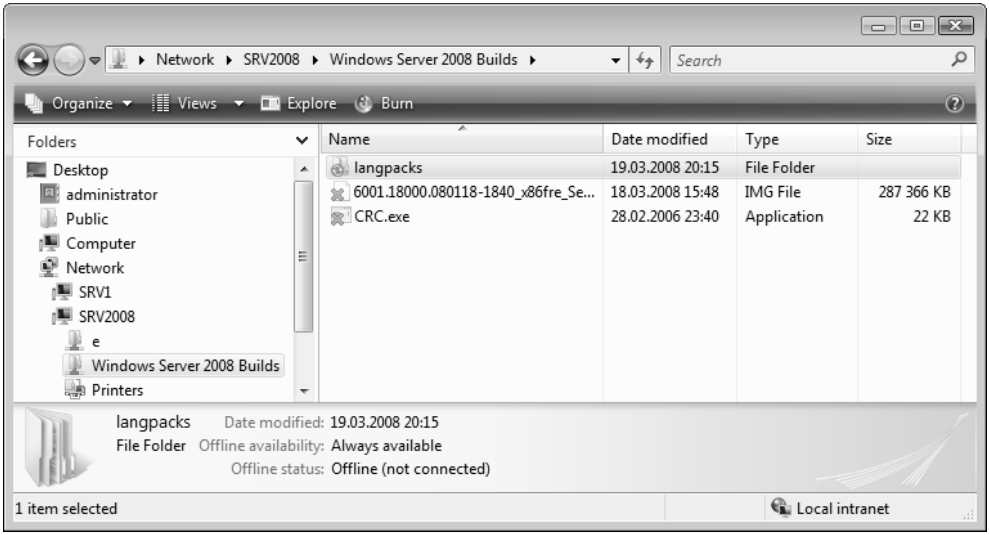


Рис. 7.46. Просмотр общих сетевых папок
на отключенном удаленном компьютере при наличии автономной папки

Еще лучше эта разница заметна, если ресурсы удаленного компьютера просматривать обычным образом — в окне программы Windows Explorer (Проводник) (рис. 7.46). На автономной папке имеется значок Центра синхронизации, и она доступна; на двух других файлах стоят крестики и они недоступны.

Синхронизация автономных файлов

В случае отключения компьютера от сети пользователь сохраняет возможность изменения автономных файлов. Однако эту возможность имеют и все пользователи, компьютеры которых не потеряли соединения с сетью (или сам пользователь удаленного компьютера). В результате этого содержимое одних и тех же файлов может стать различным, могут появиться новые файлы или файлы могут быть удалены. Поэтому после восстановления соединения с сетью необходимо выполнить синхронизацию автономных файлов локального кэша и общего сетевого ресурса.

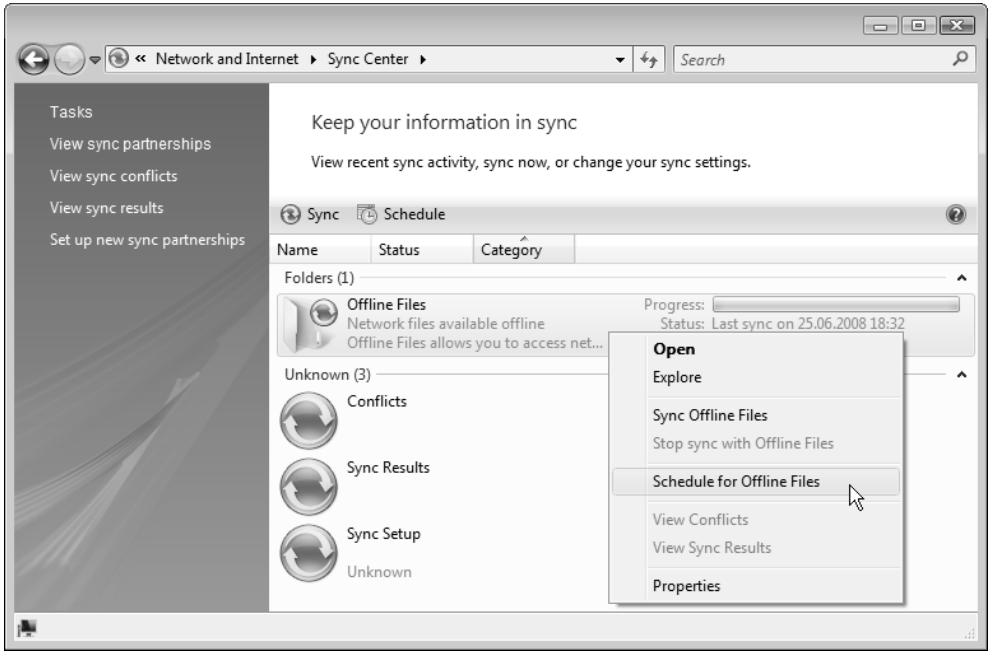


Рис. 7.47. Окно Центра синхронизации

Для выполнения этой задачи используется *Центр синхронизации* (Sync Center) (рис. 7.47), запукаемый с панели управления. Синхронизация может быть принудительной (ручной) или по расписанию. В первом случае достаточно в окне Центра синхронизации выбрать папку **Offline Files** (Автономные файлы) и нажать кнопку **Sync** (Синхронизация) на панели задач.

Для создания расписания синхронизации нужно щелкнуть по папке правой кнопкой мыши и в контекстном меню выполнить команду **Schedule for Offline Files** (Расписание для "Автономные файлы"). Можно просто нажать на кнопку **Schedule** (Расписание) на панели задач (см. рис. 7.47).

Сначала необходимо выбрать объекты для синхронизации (рис. 7.48). Расписание может быть общим для всех имеющихся автономных папок или индивидуальным (если на то есть особые причины — например, режим доступа конкретного удаленного компьютера).

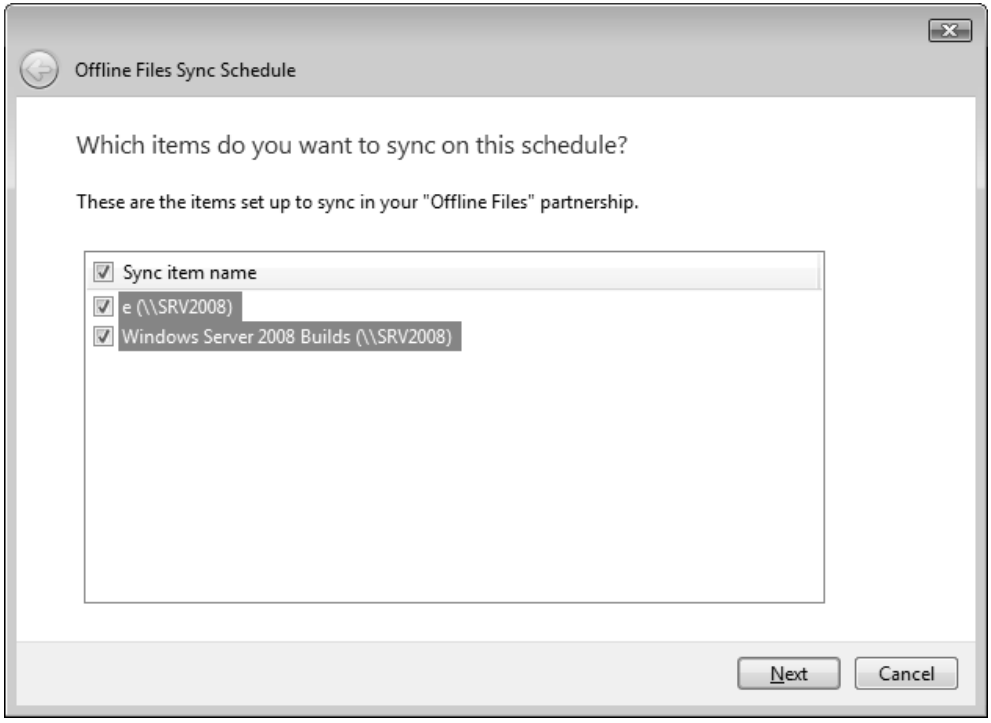


Рис. 7.48. Выбор папок
для создаваемого расписания синхронизации

Затем нужно указать режим синхронизации. Возможны два варианта (рис. 7.49):

- по расписанию;
- в определенные моменты в работе системы (например, после регистрации пользователя в системе, при бездействии или блокировке; нажав кнопку **More Options**, можно получить доступ к дополнительным возможностям выбора событий).

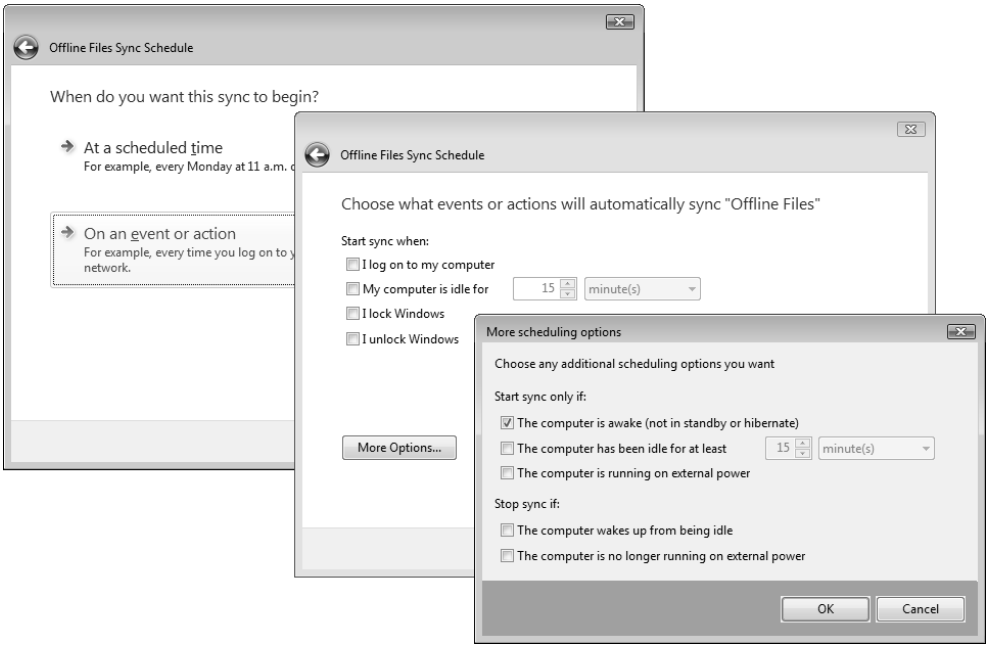


Рис. 7.49. Выбор режима синхронизации

После определения способа синхронизации и выбора параметров (расписания или событий системы) расписание нужно сохранить с понятным именем.

Теперь можно создавать другие расписания, изменять и удалять существующие — достаточно нажать кнопку **Schedule** (Расписание) на панели задач и выбрать нужное действие.

В процессе синхронизации возможны конфликты версий одноименных файлов, располагающихся на локальном компьютере и на общем ресурсе. При этом Центр синхронизации выдает количество конфликтов, и можно про-

смотреть список всех "проблемных" файлов. В таких ситуациях пользователь может выбрать одну из трех возможностей (рис. 7.50):

- оставить ту копию файла, которая хранится на локальном компьютере;
- оставить ту копию файла, которая находится на общем ресурсе;
- сохранить обе версии файла (по умолчанию — к имени одного файла добавляется имя пользователя локального компьютера).

При возникновении конфликтов пользователь может обрабатывать каждую ситуацию *отдельно*, а может указать *общее* (из числа трех указанных выше возможностей) действие для всех дублирующихся имен.

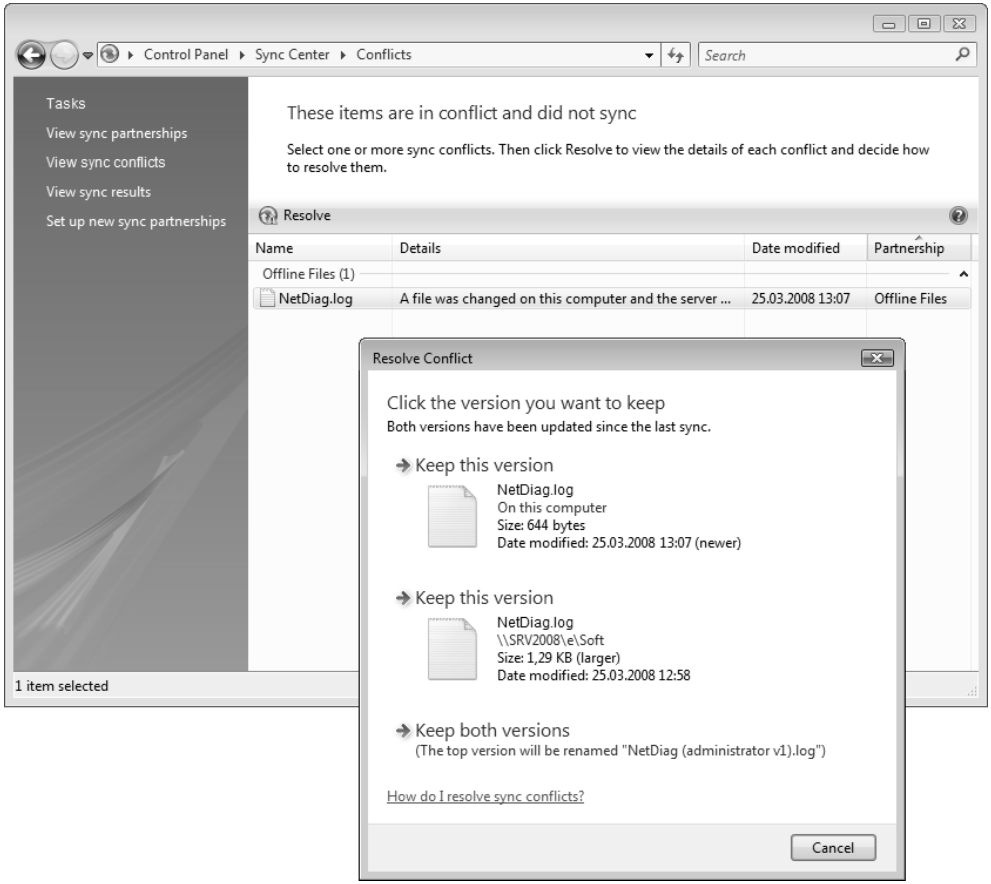


Рис. 7.50. Устранение конфликтов при синхронизации автономных файлов

Распределенная файловая система DFS

Распределенная файловая система (Distributed File System, DFS) упрощает управление данными в сети и облегчает их поиск. Она позволяет объединить файловые ресурсы, находящиеся на различных компьютерах, в единое пространство имен. С помощью DFS, вместо того чтобы работать с физической сетью, состоящей из большого количества машин с собственными именами и общими папками, пользователи могут увидеть единую структуру логических имен общих файловых ресурсов.

Достоинства DFS

Распределенная файловая система обладает целым набором преимуществ, делающих ее ценным продуктом, упрощающим организацию файловых ресурсов в корпоративной сети. Все они изложены ниже.

- **Возможность логического представления общих ресурсов, находящихся на различных серверах сети, работающих под управлением разных операционных систем.** Общее логическое пространство имен позволяет связать общие ресурсы сети и работать с ними, как будто они находятся на одном большом жестком диске. Это дает возможность создавать упрощенное представление общих ресурсов сети.
- **Удобное администрирование томов.** Общий ресурс, входящий в состав тома DFS, может быть отключен без какого-либо влияния на оставшуюся часть пространства имен тома. Это позволяет управлять физическими общими ресурсами сети независимо от их логического представления.
- **Наличие GUI-инструмента администрирования.** Администрирование распределенной файловой системы выполняется с помощью простого в работе инструмента с графическим интерфейсом. С его помощью можно выполнять просмотр, конфигурацию логических имен DFS, альтернативных общих ресурсов (реплик) и ссылок DFS, а также администрирование удаленных корней DFS.
- **Возможность организации отказоустойчивых схем хранения информации.** С одним логическим именем DFS может быть связано несколько альтернативных общих ресурсов (реплик), хранящих идентичную информацию. Между этими ресурсами можно организовать автоматическую репликацию данных. Если по каким-либо причинам один из альтернативных общих ресурсов становится недоступен, DFS автоматически

обратится к другому альтернативному общему ресурсу. Поэтому важные данные, необходимые для успешного осуществления бизнес-процессов, могут быть надежно защищены от разрушения в случае отказа файлового сервера или дискового устройства.

- **Сбалансированная нагрузка на общие ресурсы сети.** Связав одно логическое имя DFS с несколькими альтернативными общими ресурсами сети, администратор может эффективно сбалансировать нагрузку на общие ресурсы, возникающую при доступе к файлам со стороны пользователей. Запрашивая данные у логического имени DFS, пользователи фактически обращаются к одному из альтернативных общих ресурсов, связанных с данным именем. В результате происходит распределение доступа к файлам среди нескольких дисковых устройств или серверов.

- **Прозрачность соответствия логического представления данных и их физического местоположения.** Пользователи работают только с логическим представлением ресурсов сети, без учета физического расположения файловых серверов и общих ресурсов. Если данные перемещаются на другой сервер, логическое пространство DFS подвергается переконфигурированию, связанному с созданием нового соответствия между старым логическим именем DFS и новым общим ресурсом, на котором хранятся данные. Пользователь продолжает работать с логическим именем. Он может не знать, что физическое местоположение необходимой ему информации изменилось, т. е. изменение физического расположения данных полностью прозрачно для пользователей. Подобное свойство DFS позволяет администратору перемещать сетевые общие ресурсы с сервера на сервер или с одного дискового устройства на другое дисковое устройство, сохраняя при этом доступность данных.

- **Интегрирование с моделью безопасности Windows.** Распределенная файловая система не содержит самостоятельных, дополнительных средств обеспечения безопасности. Любой пользователь, который подключен к тому DFS, может беспрепятственно работать со всей информацией, к которой ему разрешен доступ с помощью разрешений файловой системы NTFS.

- **Интеллектуальное кэширование данных на стороне клиента.** Логическое дерево DFS может содержать ссылки на сотни и даже тысячи общих ресурсов. В процессе первой попытки пользователя получить доступ к информации конкретного логического имени DFS в кэш-память клиента заносится определенная информация, позволяющая в дальнейшем ускорить обращение к необходимому общему ресурсу сети при повторных

обращениях пользователя к данному логическому имени. В результате обеспечивается высокая производительность при доступе к сетевым томам через сложную иерархию ссылок.

Базовые понятия

Распределенная файловая система реализует связь между именем UNC, представляющим соответствующий объект DFS, и общим ресурсом, где фактически находятся данные. Общие ресурсы, подключенные к дереву DFS, могут находиться на любом сервере, доступном пользователю: на той же машине, где и корень, на любом сервере или рабочей станции.

Начальной точкой для логических имен дерева DFS служит *корень* распределенной файловой системы. Все остальные логические имена DFS будут находиться на следующем иерархическом уровне. Корни DFS бывают двух видов:

- *изолированный корень* (standalone DFS root) не связан с Active Directory, может иметь только одну реплику (т. е. не обеспечивает отказоустойчивость в обычных, не-кластерных системах) и не позволяет использовать службу репликации файлов (File Replication Service, FRS) для репликации данных (свойств самого корня и папок);
- *доменный корень* (domain DFS root) должен располагаться на компьютере — члене домена, может иметь несколько реплик и позволяет использовать службу FRS для репликации свойств самого корня или дочерних папок DFS.

Общие ресурсы компьютерной сети в дереве DFS представляются с помощью *папок* (folder). С корнем DFS и ссылками связаны физические общие ресурсы, называемые *конечными объектами папки* (folder target). Для каждого объекта DFS (корня или папки) должен быть указан как минимум один конечный объект. Однако к одному логическому имени DFS можно подключить и несколько общих ресурсов сети, на которых находится идентичная информация. Между такими ресурсами должна выполняться *репликация*, или синхронизация данных, и эти папки будут образовывать *группу репликации* (replication group). Они наиболее эффективны в режиме считывания данных.

Таким образом, корень и папки представляют логическую организацию DFS, а конечные объекты папки соответствуют физическому местоположению данных на сетевых компьютерах.

Доступ к любому объекту DFS, хранящемуся в общей папке, может быть получен с помощью стандартного UNC-имени, имеющего следующий вид:

```
\\<имяСервера>\<кореньDFS>\<путь>\<файл>
```

где `имяСервера` — это имя машины, где установлен корень распределенной файловой системы; `кореньDFS` — имя корня созданной распределенной файловой системы; `\<путь>\<файл>` — любое допустимое имя в структуре DFS. Как можно видеть в этом случае, используемое имя жестко "привязано" к конкретному серверу, который становится потенциальным источником отказа для всей структуры DFS.

Если распределенная файловая система работает совместно со службой каталога Active Directory (т. е. применяется доменный корень DFS), доступ к логическому имени DFS может быть получен с использованием имени домена:

```
\\<имяДомена>\<кореньDFS>\<путь>\<файл>
```

Безопасность DFS

Помимо стандартных разрешений (permissions) файловой системы NTFS и прав доступа к общим папкам, служба DFS не пользуется никакими дополнительными средствами обеспечения безопасности. При обращении пользователя к данным в пространстве логических имен DFS учитываются только права доступа к конкретным общим папкам, связанным с этими именами. При работе с доменным корнем DFS учитываются разрешения в каталоге Active Directory, установленные для соответствующих объектов.

Таким образом, права доступа на уровне файлов не зависят от структуры дерева DFS. Например, пользователи могут обращаться к одним папкам DFS и не иметь доступа к другим папкам или информации, представляющей корень пространства имен DFS.

Установка компонентов DFS

Установка служб DFS, которые входят в состав роли File Services (Файловые службы), выполняется с помощью оснастки **Server Manager** (Диспетчер сервера); они включают в себя два компонента (см. рис. 7.1):

- *DFS Namespaces* (Пространства имен DFS) — основное средство управления, позволяющее создавать логическое пространство имен, связанное с общими папками;

- *DFS Replication* (Репликация DFS) — служба, обеспечивающая синхронизацию папок на разных серверах с использованием протокола *Remote Differential Compression* (RDC; Удаленное разностное сжатие); может использоваться с пространствами имен DFS или самостоятельно.

При выборе соответствующего компонента программа установки предлагает сразу создать пространство имен DFS с помощью мастера (рис. 7.51). Администратор может отказаться и выполнить настройку позднее, с помощью оснастки **DFS Management** (Управление DFS). Если установка DFS делается впервые, то можно воспользоваться помощью мастера.

Внимание!

При использовании мастера в процессе установки компонентов DFS пространство имен создается на том сервере, на котором выполняется эта операция; т. е. этот компьютер будет сервером пространства имен и будет хранить корень DFS. При использовании оснастки **DFS Management** (Управление DFS) корень можно создавать на любом доступном сервере.

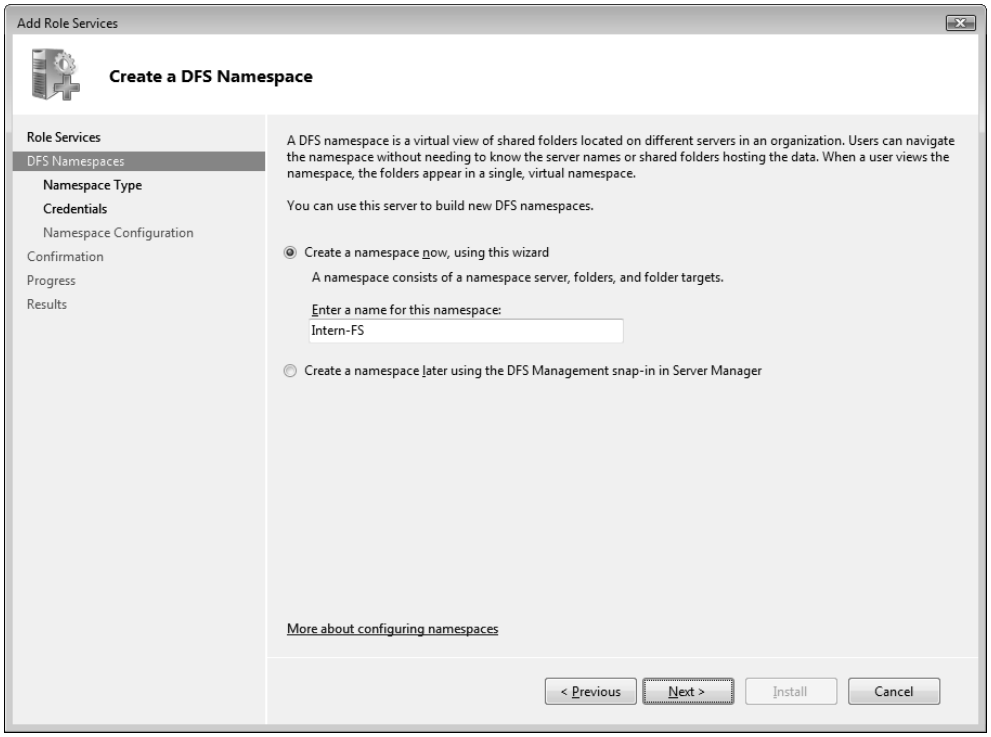


Рис. 7.51. Выбор имени для нового пространства имен DFS

На следующем шаге (рис. 7.52) указывается тип пространства имен: корень DFS может храниться в каталоге Active Directory (это повышает надежность и доступность DFS) или же на отдельном сервере (в этом случае при отказе сервера вся DFS будет недоступна). При наличии домена Active Directory лучше выбирать первую опцию.

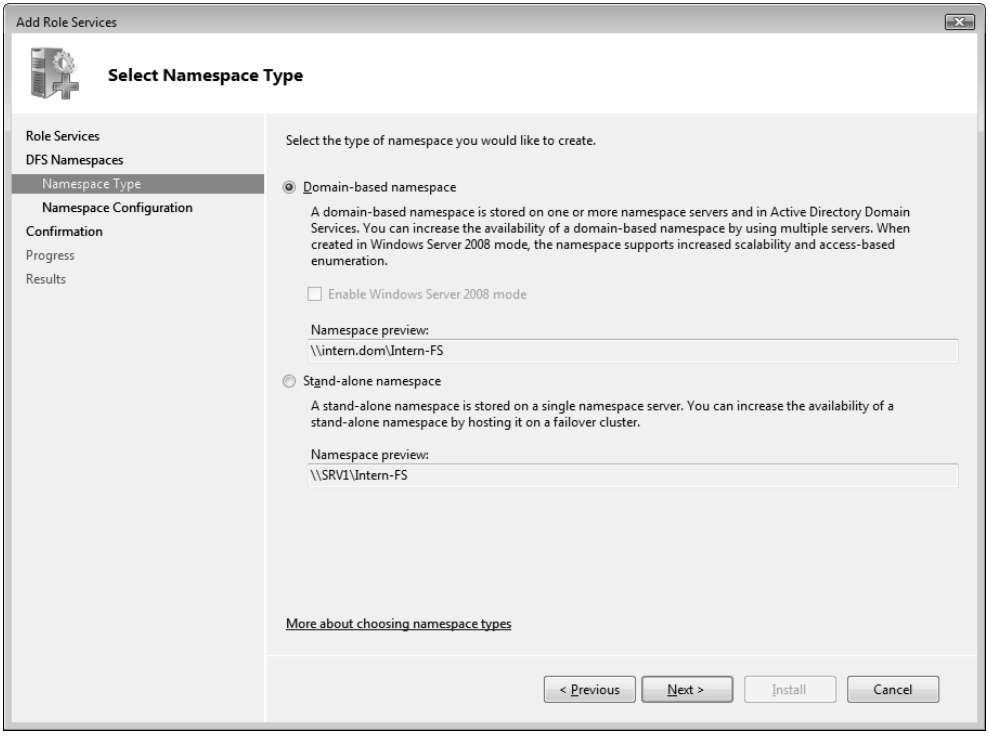


Рис. 7.52. Выбор типа пространства имен DFS

Затем мастер позволяет создать папки DFS — виртуальные каталоги, связанные с общими папками, хранящимися на различных серверах (рис. 7.53). При добавлении папок (кнопка **Add**) необходимо в формате \\<*имяСервера*>\<*имяОбщейПапки*> указывать имя реального общего ресурса и произвольное имя папки в пространстве имен DFS (рис. 7.54).

После того как пространство папок DFS будет хотя бы частично сформировано, можно нажать кнопку **Install** (Установить) и начать установку и конфигурирование служб DFS.

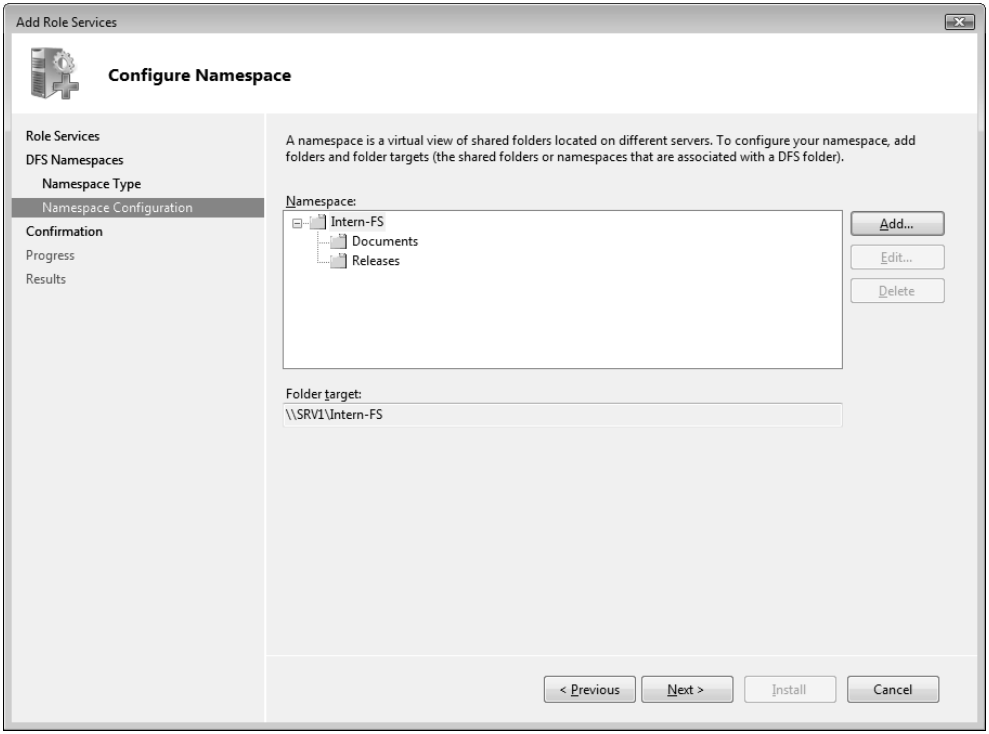


Рис. 7.53. Создание папок, входящих в новое пространство имен DFS

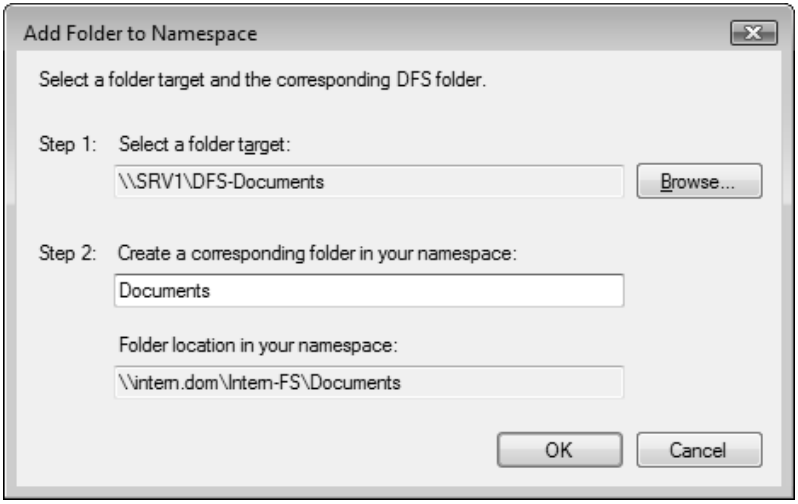


Рис. 7.54. Выбор общей папки и определение ее имени в пространстве имен DFS

Управление DFS

Управление распределенной файловой системой выполняется централизованно с помощью оснастки **DFS Management** (Управление DFS; dfsmgmt.msc) (рис. 7.55), запускаемой из подменю **Administrative Tools** (Администрирование). С ее помощью можно подключаться к любым корням DFS и управлять ими; одновременно в окне оснастки может отображаться множество корней DFS.

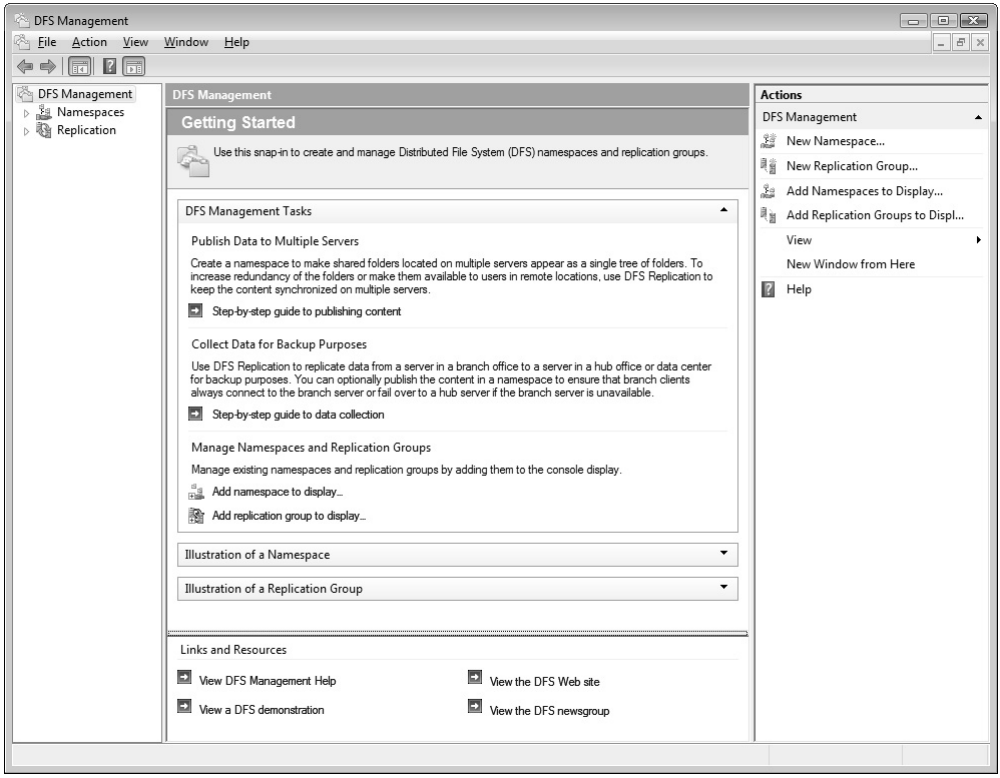


Рис. 7.55. Главная страница оснастки **DFS Management**

Для управления DFS из командной строки можно также применять утилиты *DfsUtil.exe* (создание корня и папок), *DfsCmd.exe* (создание реплик), *DfsrAdmin.exe* (общее управление) и *DfsrDiag.exe* (управление репликацией и диагностика).

При первом запуске оснастки **DFS Management** (Управление DFS) на ее главной странице (см. рис. 7.55) можно видеть ссылки на справочные ресурсы по различным аспектам использования DFS. Ссылки на панели **Actions** (Действия) позволяют выполнять основные задачи по организации DFS: создавать новые пространства имен и группы репликации. С помощью соответствующих ссылок можно выбирать объекты (пространства имен и группы репликации) для отображения в окне оснастки.

Создание пространства имен DFS

Организация дерева логических имен распределенной файловой системы начинается с создания пространства имен и связанного с ним корня DFS. Как уже было показано, создать пространство имен можно с помощью мастера при установке компонентов DFS, однако с помощью административной оснастки возможности намного шире.

Для создания нового пространства имен распределенной файловой системы:

1. Запустите оснастку **DFS Management** (Управление DFS).
2. Выберите папку **Namespaces** (Пространства имен) и на панели **Actions** (Действия) щелкните по ссылке **New Namespace** (Создать пространство имен).
3. В доменах Active Directory отказоустойчивость обеспечивается с помощью репликации данных (которую выполняет служба репликации файлов (File Replication Service, FRS)). Различные серверы в домене могут хранить параметры корня DFS, что обеспечит устойчивость корня к отказам. Сама служба Active Directory обеспечивает процесс синхронизации информации о различных репликах доменного корня DFS и относящихся к нему папках. Если компьютер, на котором создается корень DFS, не интегрирован в Active Directory, то в этом случае может быть создан только изолированный корень DFS, не обладающий средствами репликации.

   На следующей странице мастера выберите компьютер, который будет выполнять роль сервера пространства имен.
4. Укажите имя для нового пространства имен.
5. Выберите тип пространства имен: установите переключатель **Domain-based namespace** (Доменное пространство имен) или **Stand-alone namespace** (Изолированное пространство имен).
6. Проверьте правильность введенных параметров и нажмите кнопку **Create** (Создать).

На указанном сервере пространства имен на диске C: в папке \DfsRoots будет автоматически создана общая папка для хранения корня DFS; ее имя будет совпадать с именем, выбранным для пространства имен.

Теперь к новому пространству имен можно добавлять папки DFS, связанные с общими папками, хранящимися на компьютерах сети.

На рис. 7.56 изображено окно оснастки **DFS Management** (Управление DFS) с несколькими пространствами имен, хранящимися в домене intern.dom. В контекстном меню и на панели **Actions** (Действия) видны действия, которые можно выполнять для выбранного пространства имен.

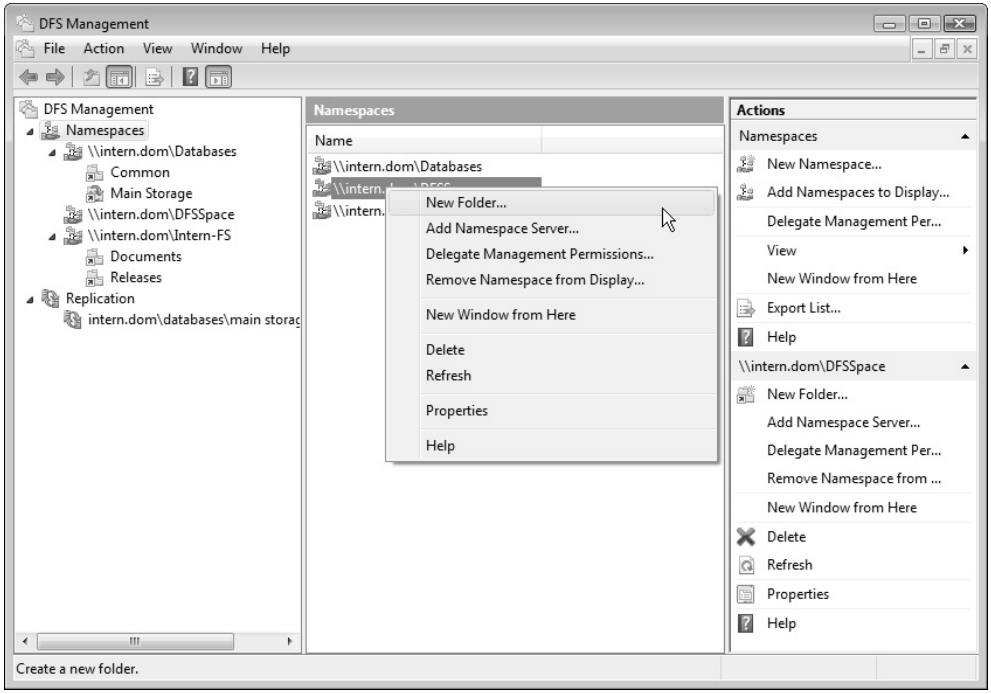


Рис. 7.56. Примеры пространств имен, открытых в окне оснастки **DFS Management**

Проверить "видимость" корня DFS можно с помощью команды `net share` — на локальном компьютере или команды `net view` *<имяКомпьютера>* — с удаленного компьютера.

С помощью следующей команды можно просматривать информацию о DFS и ее папках:

```
dfsutil /Root:\\intern.dom\Databases /View
```

Для подключения логического диска, связанного с пространством имен, можно использовать команды вида

```
net use * \\intern.dom\Databases
```

или

```
net use * \\intern.dom\Databases\<имяВложеннойПапки>
```

Добавление папок

После выполнения последовательности шагов, описанной в предыдущем разделе, появилось пространство имен DFS, с которым теперь можно связывать дочерние папки (логические имена).

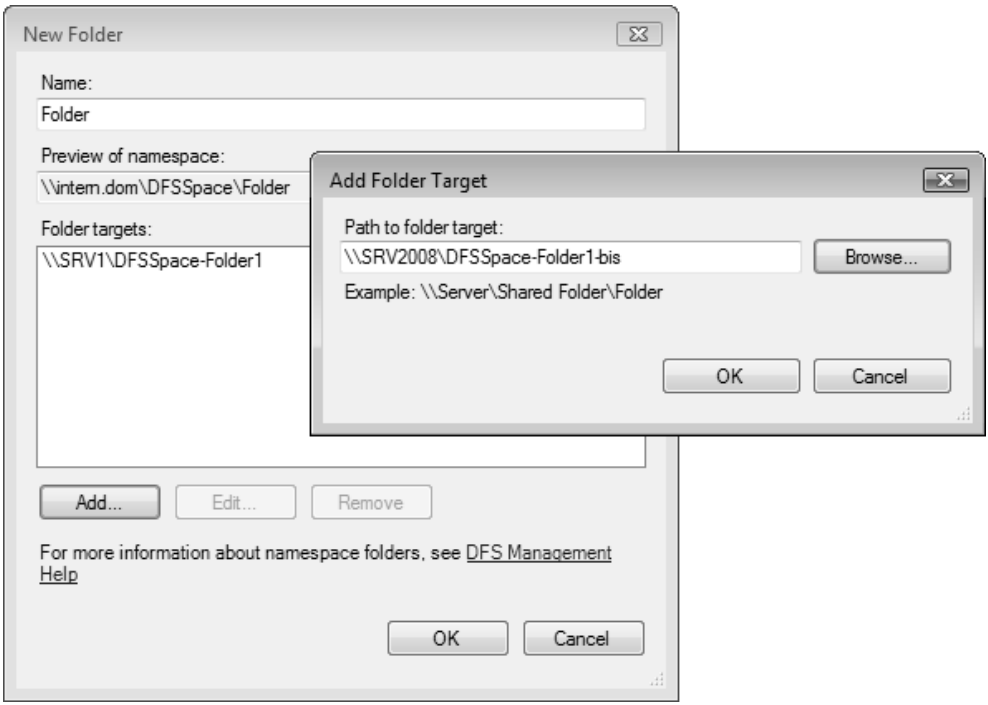


Рис. 7.57. Создание дочернего логического имени (папки) DFS

Для создания папки DFS:

1. Укажите пространство имен и в контекстном меню выберите команду **New Folder** (Создать папку) (см. рис. 7.56).
2. В окне **New Folder** (Создать папку) (рис. 7.57) укажите название папки в поле **Folder** (Папка) и, нажав кнопку **Add** (Добавить), введите UNC-имя соответствующей общей папки в поле **Path to folder target** (Путь к конечному объекту папки)). Для поиска необходимых общих ресурсов можно использовать кнопку **Browse** (Обзор). После завершения ввода информации нажмите кнопку **OK**. Если указать сразу две папки, то мастер предложит на основе этих папок создать группу репликации, т. е. содержимое этих папок будет синхронизировано между собой (эту операцию мы рассмотрим отдельно в следующем разделе). Если задана одна папка, то она просто добавляется к выбранному пространству имен DFS.

С помощью команды `dfsutil /View` можно видеть все подключенные папки, их свойства и состояние.

Создание групп репликации

Если в сети работает несколько серверов, то появляется возможность создать отказоустойчивую схему хранения важной информации с помощью реплик — альтернативных конечных объектов папки (targets), связанных с логическими папками DFS. Синхронизированные между собой общие папки образуют группу репликации.

Для создания новой группы можно открыть папку **Replication** (Репликация) и выбрать соответствующую команду. Более простой способ — выбрать папку DFS и создать для нее реплику. Для этого требуются следующие действия:

1. Выберите папку DFS и в контекстном меню выполните команду **Replicate Folder** (Реплицировать папку). Программа напомнит о том, что для репликации нужны две папки, и предложит добавить конечный объект папки (target).
2. Как и в предыдущем разделе, необходимо выбрать общую папку, после чего мастер предложит создать группу репликации для синхронизации указанных папок.
3. В случае согласия на следующем шаге выберите произвольное имя для группы репликации.

4. Далее проверьте правильность параметров для папок, выбранных в качестве участников репликации DFS (рис. 7.58). При необходимости можно вернуться назад и выбрать другие папки.

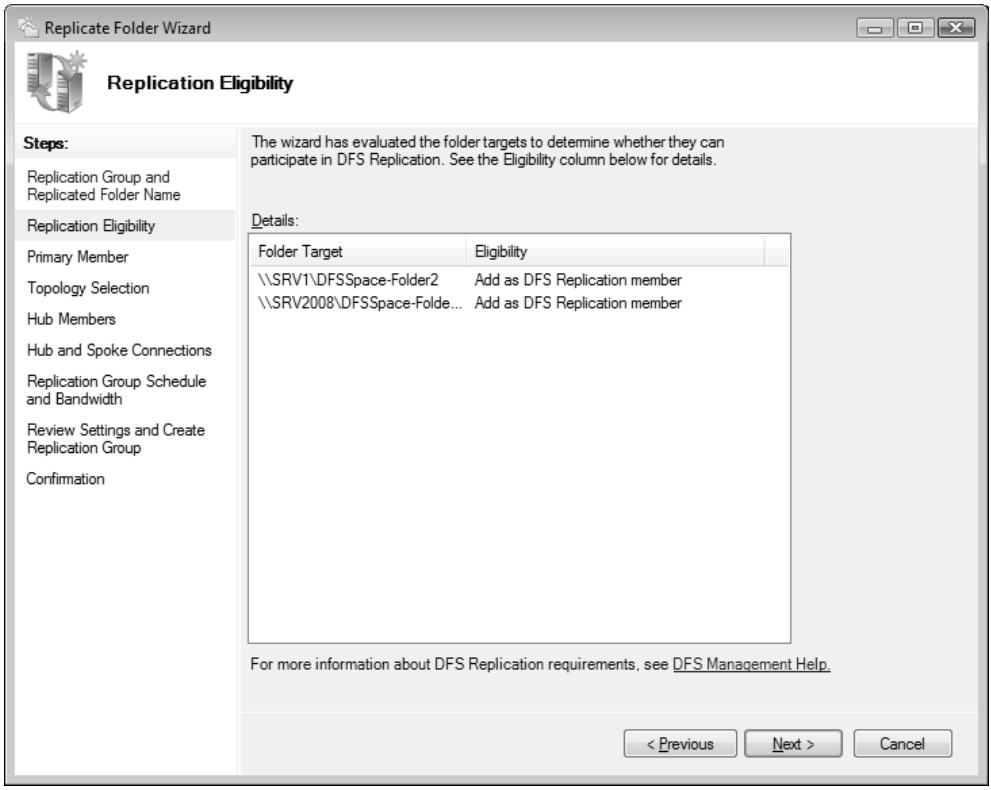


Рис. 7.58. Просмотр папок, выбранных в качестве членов группы репликации

5. Выберите сервер, на котором хранится главный член (primary member) группы репликации. Содержимое папки с этого сервера будет определяющим при выполнении начальной синхронизации.
6. Укажите топологию репликации. По умолчанию все члены группы репликации синхронизируются друг с другом (full mesh). Топологию и другие параметры репликации можно изменить в любой момент, выбрав группу репликации в папке **Replication** (Репликация).

7. На следующем шаге можно при необходимости указать скорость, с которой будет выполняться репликация, или расписание для моментов выполнения репликации.
8. На последней странице мастера проверьте правильность указанных параметров и нажмите кнопку **Create** (Создать).
9. Проверьте правильность выполнения операции (рис. 7.59). В случае возникновения ошибок на вкладке **Errors** (Ошибки) появится их подробное описание. В этом случае необходимо внести коррективы и повторить операцию.

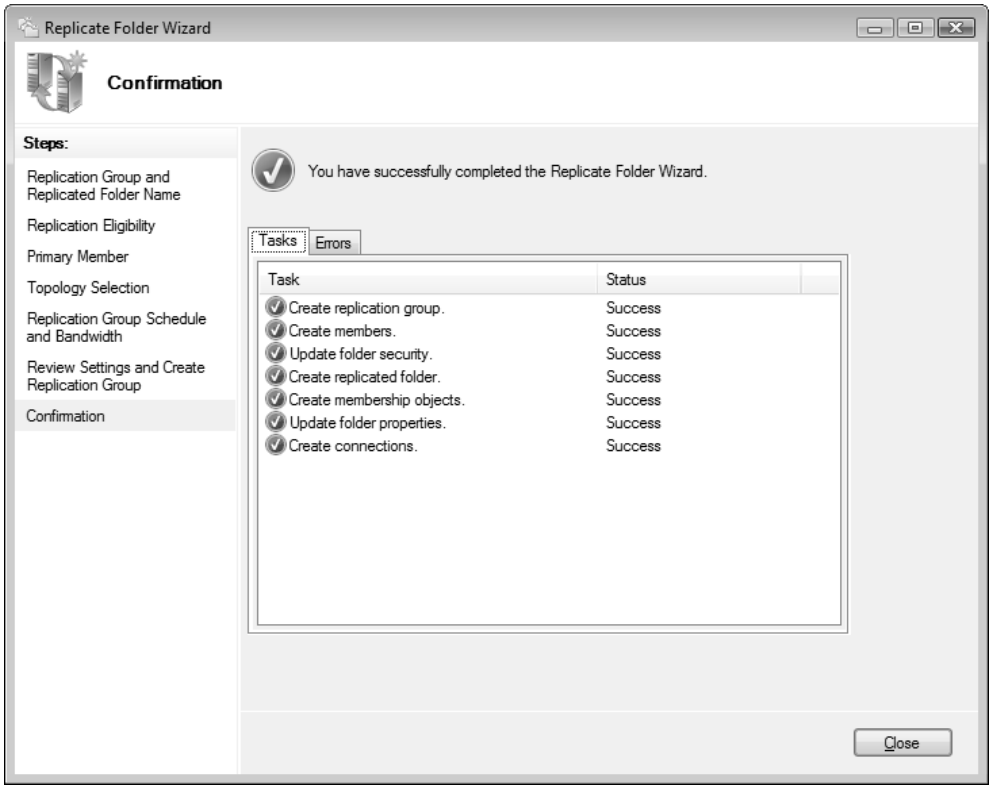


Рис. 7.59. Предупреждение о необходимости настройки репликации для альтернативного ресурса

Теперь при выборе папки DFS в окне оснастки будет видно, что для нее имеются два конечных объекта (рис. 7.60) и возможна репликация между ними. Любую конечную общую папку можно открыть в окне Проводника (команда **Open in Explorer**).

Все события, связанные с созданием групп репликации и выполнением синхронизации папок, регистрируются в системном журнале *DFS Replication* (Репликация DFS) в группе Application and Services Logs (Журналы приложений и служб).

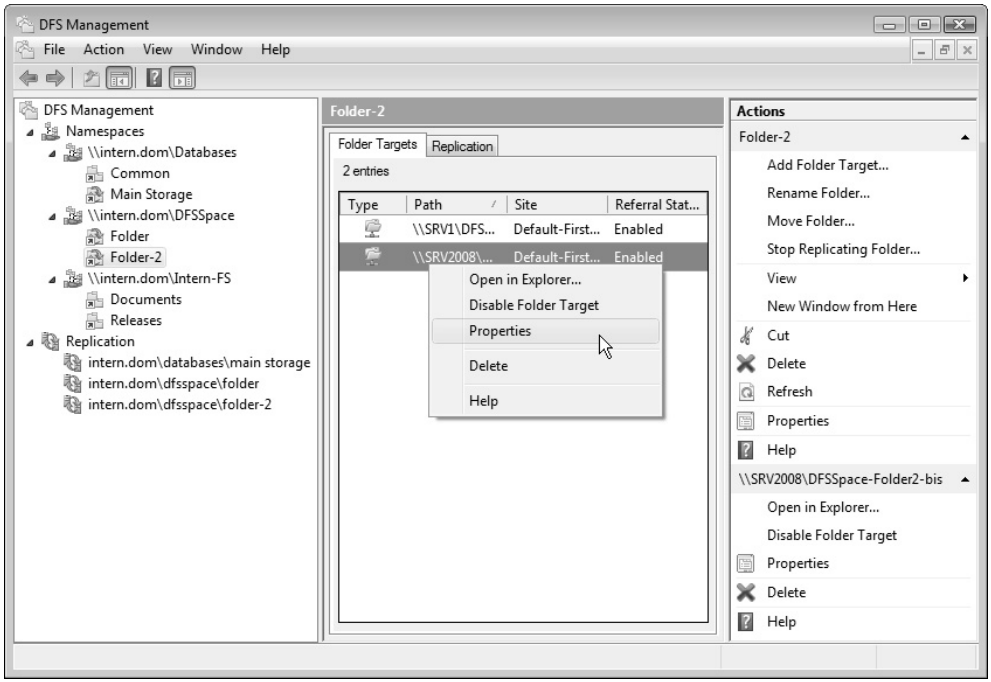


Рис. 7.60. Просмотр конечных объектов для выбранной папки DFS

Когда пользователь подключается к общему ресурсу, представленному корнем DFS или одной из папок, в окне свойств этого ресурса он увидит новую вкладку — **DFS** (рис. 7.61), на которой он может проверить состояние реплики (кнопка **Check Status** (Проверить состояние)), выбрать активную реплику (кнопка **Set Active** (Активизировать)), отмеченную галочкой в красном кружке, и узнать, с какими общими сетевыми папками связан данный объект DFS.

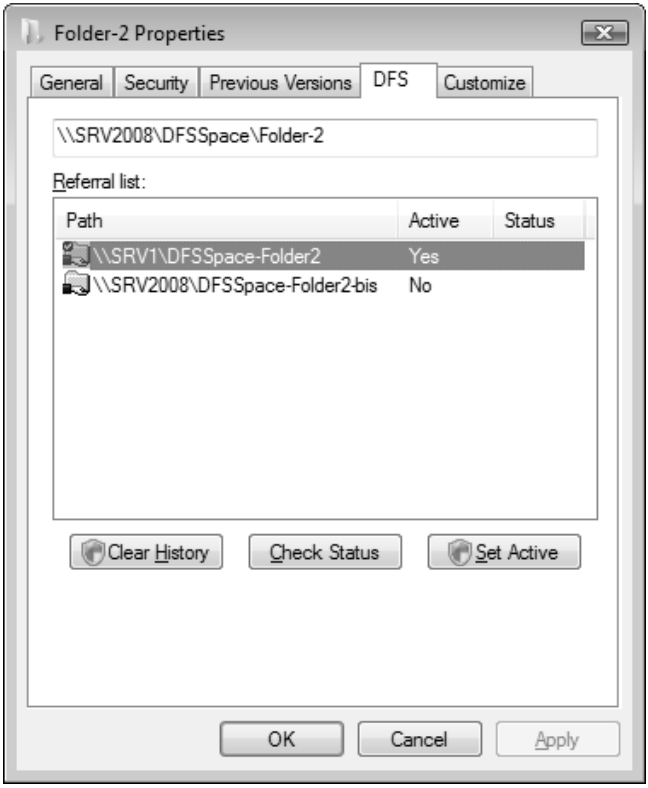


Рис. 7.61. Окно свойств файлового ресурса, представленного ссылкой DFS, имеющей две реплики

Управление репликацией DFS

Синхронизацию данных, находящихся в различных папках, входящих в группу репликации, обеспечивает сервис DFS Replication (Репликация DFS). Просмотреть параметры репликации (включая расписание, если оно установлено) можно в папке **Replication** (Репликация), где отображаются имеющиеся группы репликации (рис. 7.62). Выбрав группу и открыв вкладку **Connections** (Подключения), можно получить доступ ко всем параметрам (обратите внимание на набор команд, имеющихся на панели **Actions** (Действия)) и запустить принудительную репликацию (команда **Replicate Now**) (при этом результат операции будет зарегистрирован в системном журнале DFS Replication (Репликация DFS)).

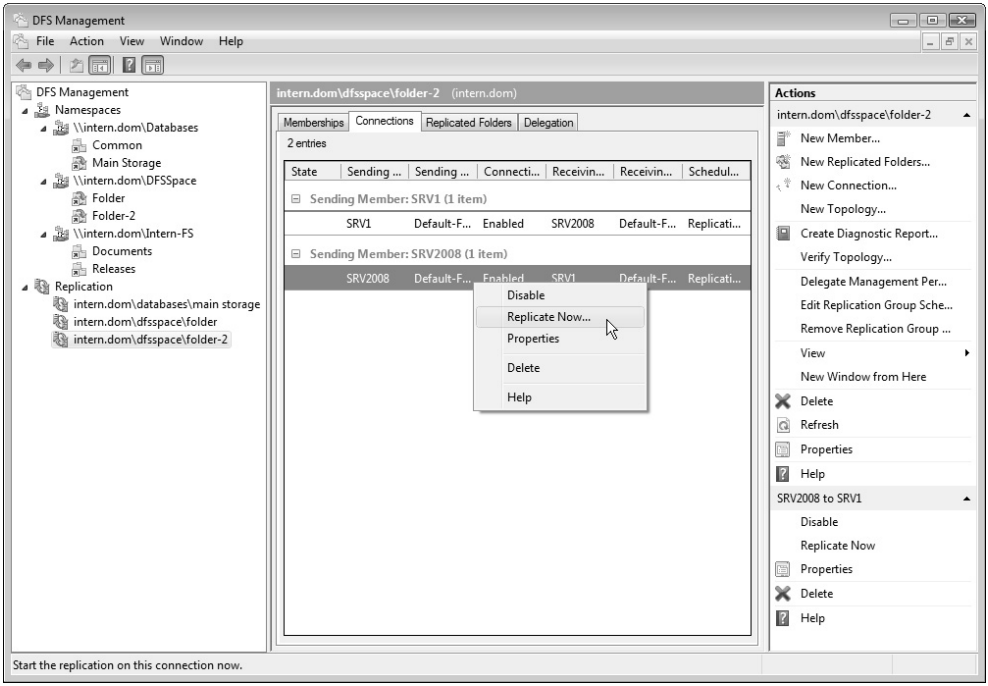
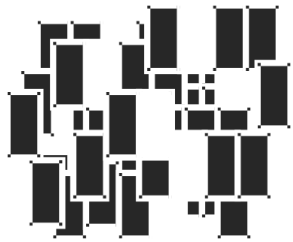


Рис. 7.62. Окно связей репликации альтернативных общих папок

Важной операцией является проверка топологии, запускаемая с панели **Actions** (Действия) с помощью соответствующей команды (ссылка **Verify Topology**).

Глава 8



Работа в сетях

В этой главе рассматривается использование компьютеров, работающих под управлением систем Windows Server 2008, в сетевой среде. В качестве *клиента* сети, предоставляющего также общие ресурсы, системы Windows Server 2008 (как и Windows Vista) по базовым функциональным возможностям практически не отличаются от предыдущих версий (хотя в деталях реализации и инструментах администрирования ресурсов имеется, конечно, много принципиально нового). (В этой главе мы не будем касаться многочисленных сетевых *служб*, таких как RRAS, DNS и т. п. — им посвящается отдельная глава.) Заметно изменился лишь пользовательский интерфейс, используемый для настройки сетевых параметров; появились новые возможности и понятия, которые важны для правильного конфигурирования систем в различных сетевых средах. В системах Windows Vista также имеются новые программы для совместной деятельности пользователей в одноранговых (peer-to-peer) сетях (в составе рабочей группы) — *People Near Me* (Соседние пользователи) и *Windows Meeting Space* (Конференц-зал Windows); в состав Windows Server 2008 эти программы не входят.

Сначала мы перечислим важнейшие сетевые новинки систем Windows Vista/Windows Server 2008, которые представляют интерес для пользователей и администраторов (очень много изменений, включая различные новые API, важны больше для программистов, и их мы касаться не будем). Затем будут рассмотрены основные понятия и операции, необходимые при работе в сетевой среде, в том числе — создание и настройка сетевых подключений. В заключение описывается встроенный брандмауэр Windows, являющийся одним из главных средств обеспечения сетевой безопасности компьютеров.

Новые сетевые возможности Windows Server 2008

В имеющих много общего системах Windows Vista и Windows Server 2008 модифицированы и улучшены многие (практически все важнейшие) сетевые протоколы (например, SMB 2.0, NDIS 6.1, драйвер Http.sys), серверные службы (DNS, DHCP и др.) и базовые компоненты, появились многочисленные новые функции, касающиеся работы в сети (особенно это касается существующих и новых API-интерфейсов). Перечислим самые важные и часто используемые средства "общего назначения", которые в первую очередь касаются всех клиентов сети (серверным службам посвящена отдельная *глава 11*).

Новая реализация стека протоколов TCP/IP

Одним из самых важных изменений является полностью переработанный стек протоколов *Next Generation TCP/IP*, который теперь одновременно поддерживает протоколы Internet Protocol version 4 (IPv4) и Internet Protocol version 6 (IPv6), позволяя лучше отвечать возрастающим потребностям глобальных сетей. По умолчанию оба протокола устанавливаются на компьютере, и их можно конфигурировать обычными средствами администрирования (в том числе и с помощью утилиты netsh). Если выполнить на компьютере обычную команду `ipconfig /all`, то можно увидеть некоторые новые параметры сетевого адаптера, например:

```
Ethernet adapter Local Area Connection:
...
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::5035:de8b:4600:2b1%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.74(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
...
```

В стеке Next Generation TCP/IP реализованы многочисленные новые стандарты и спецификации, имеется множество параметров настройки под специфические рабочие условия. Поддерживается технология Teredo, позволяющая плавно перейти на IPv6 и обеспечивающая работу в существующих IP-сетях.

Модернизированный брандмауэр Windows

Новый брандмауэр (Windows Firewall) позволяет фильтровать как входящий, так и исходящий трафик, имеет новую оснастку для администрирования, обеспечивает интеграцию с IPSec, обладает расширенными возможностями конфигурирования исключений (правил). Им можно также управлять с помощью утилиты netsh. По умолчанию брандмауэр включен (это следует учитывать в начале работы в сети, поскольку некоторые средства или службы могут быть заблокированы).

Сервис NLA и сетевые профили (категории сети)

Служба *Network Location Awareness* (NLA; Служба сведений о подключенных сетях) позволяет приложениям автоматически подстраиваться под параметры имеющихся сетей. Пользователи могут выбирать различные конфигурации для разных типов сетей.

Методы обнаружения компьютеров в сети

Предыдущие версии Windows для поиска компьютеров в сети используют протокол NetBIOS и службу Computer Browser (сервис Browser). В системах Windows Vista/Windows Server 2008 в дополнение к протоколам NetBIOS/SMB используются новые наборы протоколов: *Simple Service Discovery Protocol* (SSDP), *UPnP*, *Link-Layer Topology Discovery* (LLTD) и *Web Service-Discovery* (WS-Discovery, WSD). С помощью этих протоколов все компьютеры в сети могут отслеживать расположение имеющихся в сети служб, общих папок, принтеров и других ресурсов.

Клиент DHCP, подключения удаленного доступа и VPN-подключения

Поддерживают протокол IPv6 и компонент Network Access Protection (NAP), имеют расширенные возможности и новые средства самодиагностики.

Защита доступа к сети (Network Access Protection, NAP)

Сетевой компонент NAP, работающий вместе с новыми серверными службами *Network Policy and Access Services* (Службы политики сети и доступа) и клиентами Windows Vista и Windows XP Service Pack 3, позволяет защитить локальную сеть от подключенных компьютеров, которые не соответствуют требованиям безопасности сети. Если, к примеру, мобильный компьютер не

имеет последних обновлений безопасности и средств антивирусной защиты, он не получит доступ к сети, что позволит обезопасить ее от проникновения вирусов, червей и других подобных программ.

Новые групповые политики для управления сетевыми компонентами

Множество новых политик позволяет централизованно настраивать сетевые параметры компьютера, включая такие компоненты, как брандмауэр Windows Firewall, проводные и беспроводные сети, IP Security, DNS-клиент и т. д.

Network Policy Server

В системах Windows Server 2008 реализованы сервер и прокси-компонент службы RADIUS (Remote Authentication Dial-In User Service), получившие название *Network Policy Server* (NPS; Сервер сетевой политики). Он заменяет службу Internet Authentication Service (IAS), имеющуюся в Windows Server 2003, и выполняет ее функции для VPN- и 802.1x-подключений.

Улучшенная версия протокола IPSec

Обеспечена интеграция с брандмауэром Windows (Windows Firewall) и компонентом Network Access Protection (NAP), упрощена настройка, возможна защита связи клиента с контроллером домена, имеются новые, улучшенные средства криптографии и аутентификация, реализована поддержка протоколов IPv4 и IPv6.

Сети IEEE 802.11

Улучшена поддержка беспроводных сетей IEEE 802.11, реализована так называемая *Native Wi-Fi Architecture*, упрощен пользовательский интерфейс операций по установлению соединения, имеются новые групповые политики для управления соответствующими компонентами.

Утилита Msg для отправки сообщений

Для отправки по сети простых текстовых сообщений вместо команды `net send` теперь используется утилита Msg.exe. Сообщения могут посылаться отдельным пользователям или всем клиентам указанного сервера. Список па-

раметров утилиты легко получить, введя в командной строке имя утилиты без ключей.

Microsoft Network Monitor 3.1

Сетевой монитор, который присутствовал в составе предыдущих версий Windows, не включен в Windows Server 2008, однако его новую, совершенно переработанную версию можно свободно скачать с веб-сайта Microsoft из Центра загрузки (см. ссылки в *приложении*). Новый сетевой монитор уже адаптирован к возможностям Windows Vista и Windows Server 2008 и может использоваться для перехвата (записи) и последующего анализа сетевых пакетов, передающихся в сети.

Сетевые средства, удаленные из Windows Server 2008

В системах Windows Vista и Windows Server 2008 прекращена поддержка некоторых протоколов и служб; перечислим некоторые из них в алфавитном порядке:

- Asynchronous Transfer Mode (ATM);
- Bandwith Allocation Protocol (BAP);
- Basic Firewall в составе службы Routing and Remote Access (Маршрутизация и удаленный доступ); заменен встроенным брандмауэром Windows Firewall;
- Client Service for Netware (Клиент для сетей Netware);
- NWLink IPX/SPX/NetBIOS Compatible Transport Protocol;
- Open Shortest Path First (OSPF) (протокол маршрутизации для службы Routing and Remote Access (Маршрутизация и удаленный доступ));
- Serial Line Interface Protocol (SLIP);
- Services for Machintosh (SFM);
- SPAP, EAP-MD5-CHAP и MS-CHAP (MS-CHAP v1) (протоколы аутентификации для PPP-соединений);
- X.25.

В системах Windows Server 2008 сохранен компонент SMTP Service (Служба SMTP), позволяющий отправлять почтовые сообщения на SMTP-серверы, однако отсутствуют какие-либо встроенные средства, обеспечивающие хранение сообщений и передачу их клиентам по протоколу POP3.

Особенности конфигурирования некоторых сетевых компонентов

В составе систем Windows Server 2008 имеются следующие стандартные программные компоненты и сервисы[1], которые по умолчанию ***не*** установлены:

- SMTP Server (Сервер SMTP);
- SNMP Services (Службы SNMP);
- Subsystem for UNIX-based Applications (Подсистема для UNIX-приложений);
- Telnet Client (Клиент Telnet);
- Telnet Server (Telnet-сервер);
- TFTP Client (Клиент TFTP);
- Wireless LAN Service (Служба беспроводной локальной сети).

Для того чтобы получить доступ к перечисленным и другим сетевым средствам, необходимо установить соответствующие компоненты с помощью оснастки **Server Manager** (Диспетчер сервера) *(см. разд. "Роли и компоненты сервера" главы 3)*.

Категории сетей (сетевое размещение)

В системах Windows Vista и Windows Server 2008 появилось понятие *категории сети* (network category), которое связано с множеством параметров, определяющих уровень безопасности, предъявляемый к конкретной сети, к которой подключается компьютер. В пользовательском интерфейсе Windows Vista/Windows Server 2008 для обозначения категории сети используется термин *сетевое размещение* (Network Location).

---

[1] Этот список неполный, дополнительные модули можно увидеть при добавлении компонентов в окне оснастки **Server Manager** (Диспетчер сервера).

Выбор категории сети в первую очередь важен для пользователей мобильных компьютеров, которые могут перемещаться между разными сетями — корпоративными и общедоступными. Для таких пользователей важно, чтобы компьютер (в первую очередь встроенный брандмауэр) "помнил" для этих сетей параметры блокировки трафика для различных сетевых сервисов (например, для службы File and Printer Sharing (Служба доступа к файлам и принтерам). Для серверов, имеющих несколько сетевых подключений (особенно различного типа), также могут быть важными параметры безопасности для каждой подключаемой сети или для разных доменов.

В системах Windows Vista/Windows Server 2008 предусмотрены три категории сетей:

- *Private network* (Частная сеть (Дом)) — одноранговая закрытая сеть небольшого офиса, используемая ограниченным и известным кругом людей. По умолчанию в таких сетях разрешено распознавание компьютера и его ресурсов, что позволяет другим пользователям сети обращаться к сервисам компьютера (в том числе — к дискам и принтерам);
- *Public network* (Общественная сеть (Общественное место)) — сеть с точками доступа, располагающимися в публичных местах (интернет-кафе и т. п.), или "чужая" сеть для временного подключения. Для такой сети устанавливаются наиболее жесткие ограничения, позволяющие максимально обезопасить компьютер, например, отключено распознавание компьютера;
- *Domain network* (Доменная сеть (Работа)) — корпоративная сеть. Эта категория выбирается автоматически при подключении компьютера к домену, и ее вручную изменить нельзя.

В зависимости от выбранной категории сети встроенный брандмауэр Windows (Windows Firewall) выбирает стандартные для этой категории *исключения* (exceptions) или *правила* (rules) (если говорить о расширенной конфигурации — *см. далее*), блокируя или, наоборот, открывая те или иные порты TCP/UDP, используемые системными сервисами и приложениями. Таким образом, компьютер может быть максимально функциональным и, в то же время, защищенным в каждой конкретной сетевой среде.

Первоначальный выбор категории сети осуществляется еще при установке операционной системы. Для Windows Server 2008 по умолчанию задается категория Public network[1] (Общественная сеть). При этом компьютер не ви-

[1] Для Windows Vista категория сети указывается явно при установке и начальном конфигурировании системы.

ден сам и не видит другие компьютеры в сети; есть доступ только к Интернету.

> ***Внимание!***
>
> Перед началом работы в сети нужно проверить все параметры, включая выбранную категорию сети. Иначе из-за их несоответствия конфигурации сети могут возникнуть проблемы с доступом к общим ресурсам и т. п.

Если определить категорию Private network (Частная сеть), то параметр **Network discovery** (Сетевое обнаружение) получает значение **Custom** (Особые параметры) *(см. разд. "Настройка сетевых параметров доступа к общим папкам и принтерам" главы 7)*, в результате чего компьютер может видеть других клиентов сети и подключаться к их ресурсам; собственные общие ресурсы (если таковые имеются) другим не видны, поскольку параметр **File sharing** (Общий доступ к файлам) остается в выключенном состоянии, и администратор должен выбрать остальные параметры сетевой конфигурации.

Для настройки категорий сети в параметрах безопасности имеется группа политик в папке **Network List Manager Policies** (Политики диспетчера списка сетей). С их помощью можно определить выбор категории при подключении компьютера к новым (распознаваемым) или неопознанным сетям.

Работа в сетевой среде

При наличии сетевого адаптера (с правильно установленными драйверами) система автоматически создает *подключение по локальной сети* (Local Area Connection) — его значок отображается на панели задач в области уведомлений. Если *навести* на него курсор мыши, то появится всплывающее окно (рис. 8.1), в котором указаны подключение(-я) и название сети (сетей), с которой компьютер соединен (изначально название сети дается автоматически, но его можно и поменять). (Если компьютер подключен к домену, то в качестве названия сети по умолчанию используется DNS-имя домена.) В нашем примере компьютер имеет два активных подключения: связь с доменной сетью (указывается DNS-имя домена) и VPN-подключение (**VPN Connection**), которые обеспечивают доступ к локальной сети, Интернету[1] (тип доступа

[1] При наличии доступа к Интернету на значке подключения по локальной сети появляется изображение глобуса.

Access: Local and Internet) и внешнему VPN-серверу. Если компьютер входит в состав рабочей группы, то подключение к локальной сети обозначается значком **Network** (Сеть).

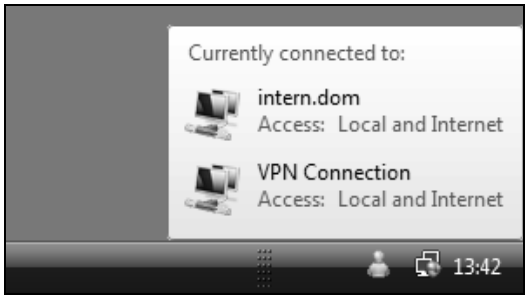


Рис. 8.1. Перечень сетей,
к которым в данный момент подключен компьютер

Примечание

Система автоматически проверяет, имеется ли подключение к Интернету, по результатам анализа сетевых параметров и пакетов.

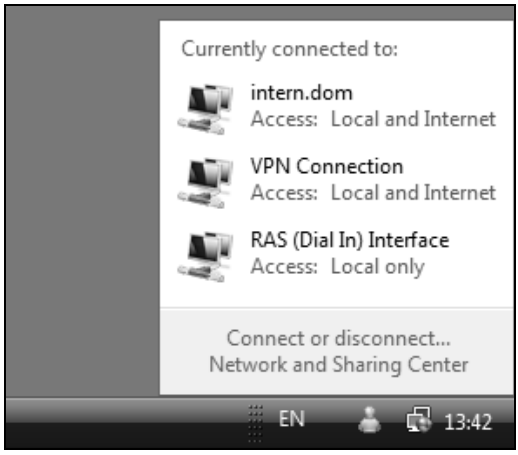


Рис. 8.2. Окно активных сетевых подключений

Если *щелкнуть* по значку подключения по локальной сети, то появится окно (рис. 8.2), в котором указаны имена подключений и сетей, к которым имеет

доступ компьютер, но также имеются две ссылки. Для подключения к другой сети достаточно щелкнуть по ссылке **Connect or disconnect** (Подключение или отключение) (если активно только подключение по локальной сети, то отображается ссылка **Connect to a network** (Подключиться к сети)). Команда **Connect To** (Подключение) может присутствовать и непосредственно в меню **Start** (Пуск) *(см. главу 2)*. Если щелкнуть по ссылке **Network and Sharing Center** (Центр управления сетями и общим доступом), то откроется главное окно всех сетевых настроек системы *(см. ниже)*.

При выполнении команды подключения к сети в специальном окне (рис. 8.3) можно выбрать любую сеть, для которой в системе ранее было создано подключение, и инициировать подключение к ней (в случае доступности в этом окне также будут указаны беспроводные сети). (Аналогичную операцию можно выполнить и в окне сетевых подключений — см. рис. 8.15.)

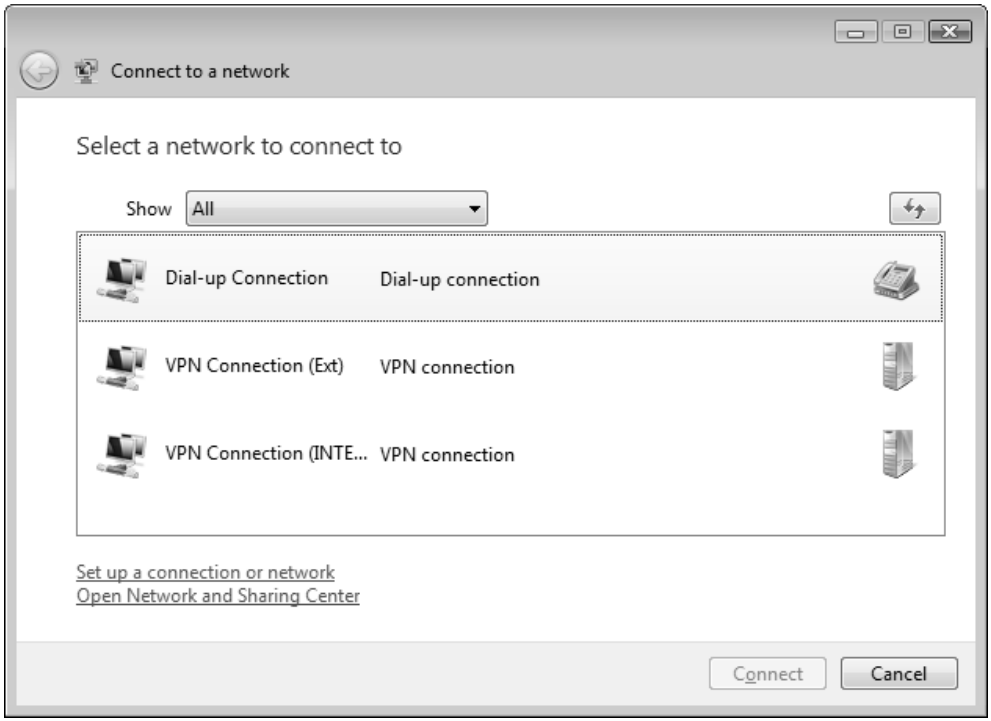


Рис. 8.3. Окно выбора подключаемой сети

Если по значку сетевых подключений щелкнуть правой кнопкой мыши, то также можно управлять подключениями и выполнять дополнительные операции — в этом случае требуемая команда выбирается в контекстном меню (рис. 8.4). Здесь следует обратить внимание на две команды:

- если необходимо следить за активностью подключения, то выполните команду **Turn on activity animation** (Включить анимацию активности). В этом случае при передаче пакетов по данному подключению на его значке будут "мигать" изображения экранов компьютеров;
- команда **Diagnose and repair** (Диагностика и восстановление) позволяет устранить неисправности при ошибках подключения. При этом проверяются и сбрасываются сетевые параметры, может обновляться IP-адрес, если он получается автоматически, и т. п.

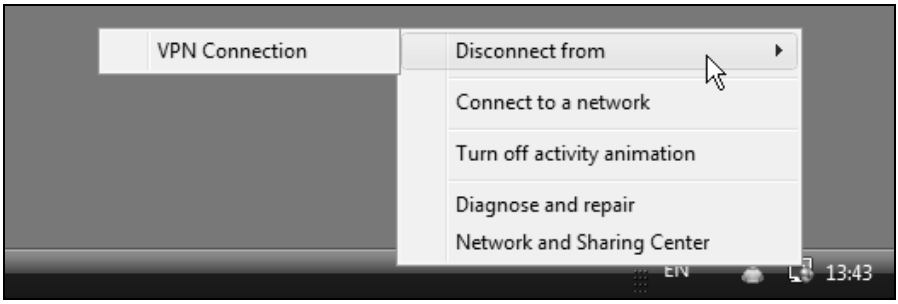


Рис. 8.4. Команды управления сетевыми подключениями и вспомогательные опции

Централизованное управление сетевыми параметрами

В системах Windows Vista и Windows Server 2008 пользовательский интерфейс всех сетевых функций заметно изменился: все операции по мониторингу и конфигурированию сетевых средств выполняются в окне **Network and Sharing Center** (Центр управления сетями и общим доступом) (рис. 8.5) — здесь можно видеть все активные подключения, менять их параметры, управлять общим доступом к файлам и принтерам, а также инициировать операции подключения к сетям, создания и конфигурирования новых подключений.

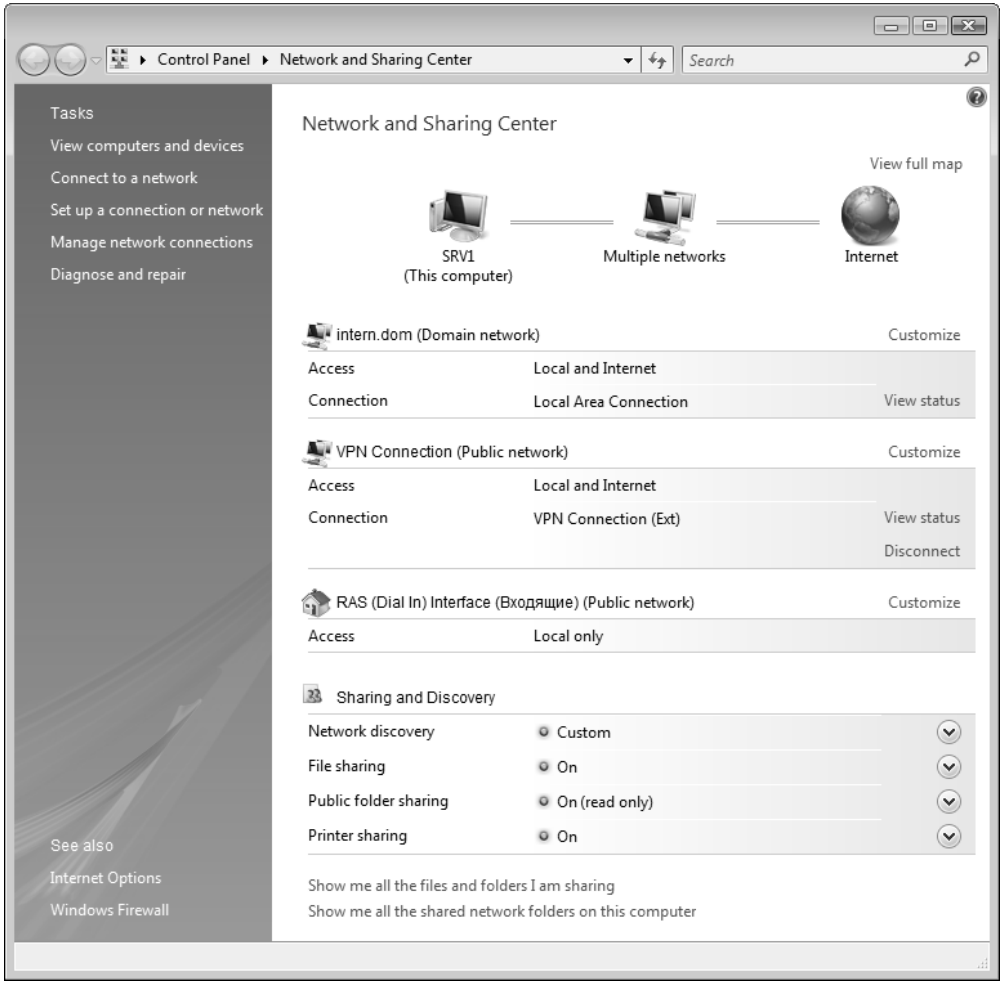


Рис. 8.5. Главное окно управления сетевыми функциями системы — **Network and Sharing Center**

Окно **Network and Sharing Center** (Центр управления сетями и общим доступом) можно открыть с панели управления, из окна активных подключений (см. рис. 8.2) или из контекстного меню подключения (см. рис. 8.4). Поначалу такой способ организации сетевых функций в системах Windows Vista и Windows Server 2008 кажется довольно непривычным, однако к новому интерфейсу управления несложно привыкнуть, поскольку суть и количество операций по настройке сети почти не изменились по сравнению с предыдущими версиями Windows.

В окне Центра управления сетями показаны режимы использования всех активных в данный момент подключений. (Для разрыва соединения используется ссылка **Disconnect** (Отключить).) Для каждого подключения указана выбранная для него категория сети (Network category): в нашем примере (см. рис. 8.5) одно подключение относится к доменной сети (Domain), а два других — к публичной (общественной) (Public). Щелкнув по ссылке **Customize** (Настройка), можно изменить категорию.

В окне настройки сетевого размещения (рис. 8.6) можно изменить имя подключения и выбрать категорию сети (размещение компьютера). Сделав выбор, нужно нажать кнопку **Next** (Далее) — система выполнит операцию и сообщит о ее результатах в следующем окне.

Для компьютера, подключенного к домену, сетевое размещение изменить нельзя — это видно на примере, приведенном на рис. 8.7. Можно только изменить сетевое имя, в качестве которого по умолчанию используется DNS-имя домена.

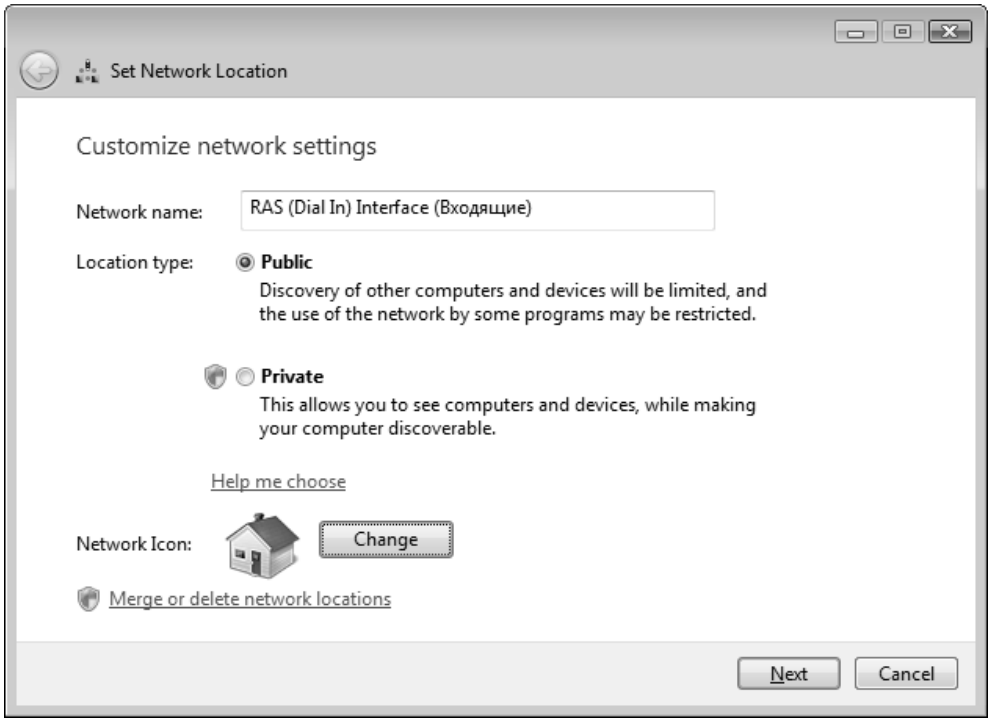


Рис. 8.6. Выбор категории сети (сетевого размещения)

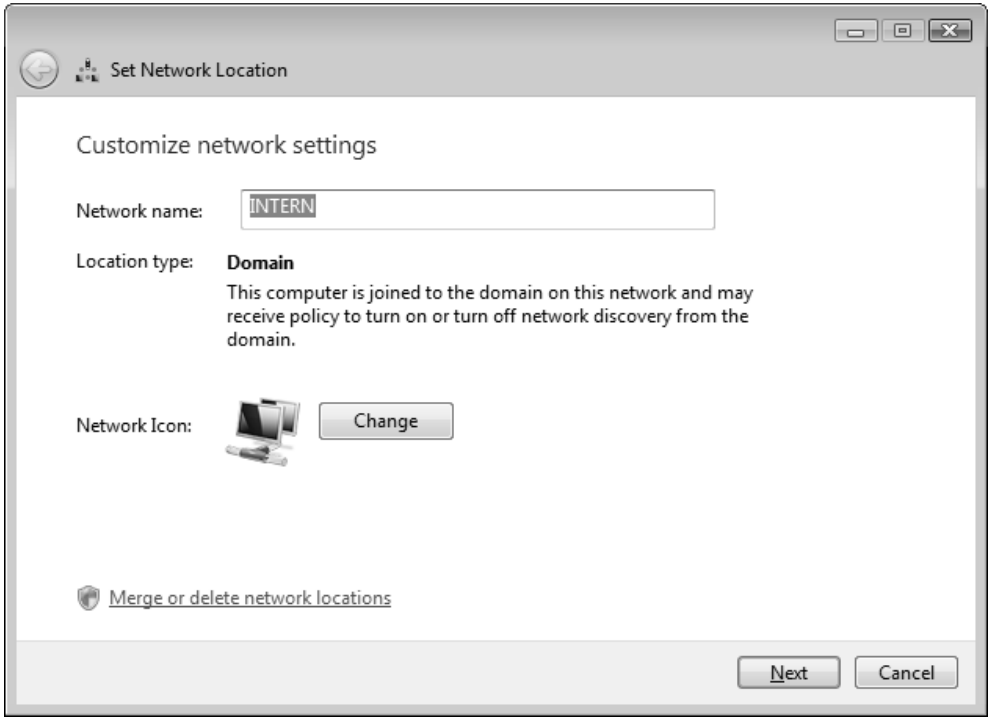


Рис. 8.7. Сетевое размещение для компьютера, входящего в состав домена

Иногда система не может проанализировать все параметры сети, к которой подключен компьютер, и в этом случае в сетевом имени (Network Name) указывается Unknown network (Неопознанная сеть). Практика показывает, что этого сообщения обычно опасаться не стоит, поскольку на работоспособности сетевого подключения это не сказывается.

Ссылка **View full map** (Просмотр полной карты) (см. рис. 8.5) позволяет увидеть так называемую *карту сети* (network map) для выбранного подключения (рис. 8.8). На этой карте представлены компьютеры, с которыми имеется связь; можно быстро увидеть основные сетевые параметры для взаимодействующих узлов (в примере показаны свойства шлюза, через который осуществляется выход в Интернет). Щелкнув по значку с изображением компьютера, можно получить доступ к списку всех имеющиеся у компьютера общих сетевых ресурсов (папок и принтеров).

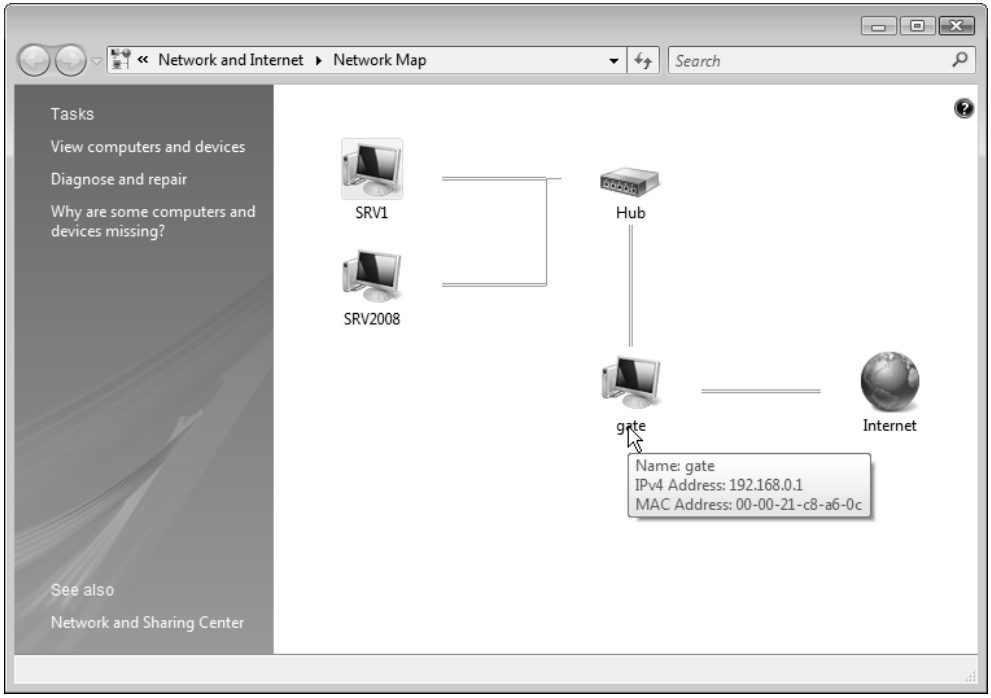


Рис. 8.8. Карта сети для выбранного подключения

Внимание!

На карте сети могут не отображаться компьютеры, работающие под управлением Windows XP. Это объясняется тем, что на них отсутствует компонент *Link Layer Topology Discovery (LLTD) responder* (Отвечающее устройство LLTD), использующийся для построения сетевой диаграммы в сетях на основе Windows Vista и Windows Server 2008. Этот компонент можно устанавливать только на Windows XP Service Pack 2; ссылку для свободного скачивания инсталляционного файла легко найти в Центре загрузки Microsoft (см. ссылку в *приложении*), выполнив поиск строки "LLTD responder".

Карту сети невозможно получить для общественной (public) сети. Сетевое сопоставление также по умолчанию отключено в доменных сетях; его можно включить с помощью групповых политик, расположенных в объектах GPO в папке **Computer Configuration** | **Administrative Templates** | **Network** | **Link-Layer Topology Discovery** (Конфигурация компьютера | Административные шаблоны | Сеть | Обнаружение топологии связи (Link-Layer)) *(см. главу 13)*.

В нижней части окна Центра управления сетями (см. рис. 8.5) показаны параметры общего доступа, определяющие настройки брандмауэра для сервисов обнаружения сети (Network Detection) и службы доступа к папкам и принтерам (File and Printer Sharing), а также параметры, связанные с некоторыми настройками системы безопасности (например, с состоянием учетной записи Guest (Гость)).

Эти параметры более подробно рассматривались в *разд. "Настройка сетевых параметров доступа к общим папкам и принтерам" главы 7*. Лучше всего понять, какие параметры используются в каждом случае, можно непосредственно в окне брандмауэра Windows (Windows Firewall), наблюдая список выбранных исключений *(см. далее)*.

Просмотр параметров сетевых подключений

По ссылке **View Status** (Просмотр состояния) в группе параметров сетевого подключения, имеющихся в окне Центра управления сетями для каждого подключения (см. рис. 8.5), можно попасть в привычное для пользователей предыдущих версий Windows окно состояния сетевого подключения, где отображаются следующие параметры: продолжительность и скорость подключения; количество байтов, отправленных (**Sent**) и принятых (**Received**) во время активности подключения, а для некоторых типов подключения еще коэффициент сжатия (**Compression**) и число ошибок (**Errors**). Обратите внимание на то, что индивидуально отображается состояние активности для протоколов IPv4 и IPv6. На рис. 8.9 для примера показано окно свойств VPN-подключения.

> ***СОВЕТ***
>
> Если в процессе работы требуется частый доступ к окну состояния (см. рис. 8.9) некоторого сетевого подключения, откройте окно сетевых подключений (см. рис. 8.15), выберите подключение и в контекстном меню выполните команду **Create Shortcut** (Создать ярлык). Ярлык может быть создан только на рабочем столе, откуда его можно переместить в любое нужное место (например, в раздел закрепленных программ меню **Start** (Пуск)).

Нажав в окне состояния подключения (см. рис. 8.9) кнопку **Details** (Сведения), можно увидеть дополнительные свойства текущего сеанса: заданные адреса стека протоколов TCP/IP (IPv4 и IPv6); способ получения адресов (DHCP или статический); наличие и тип шифрования; протокол аутентификации, а также другие параметры (они индивидуальны для каждого типа подключения). Все эти параметры особенно важны для анализа ситуации в случае неисправности подключения.

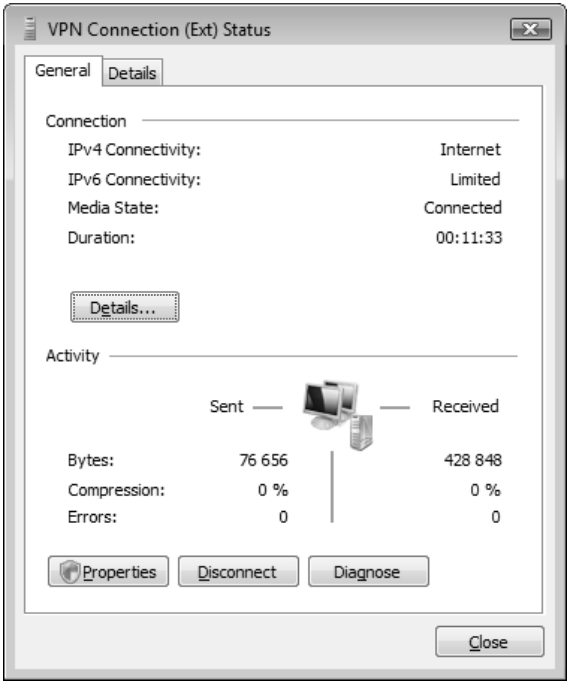


Рис. 8.9. Окно состояния сетевого подключения

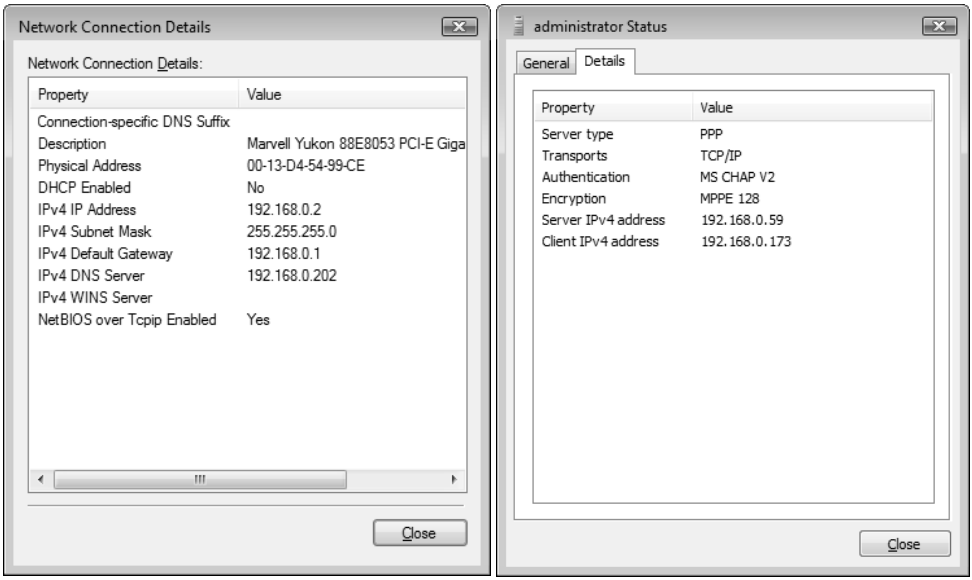


Рис. 8.10. Дополнительные свойства сеанса связи

На рис. 8.10, слева, в качестве примера показаны дополнительные параметры подключения по локальной сети, а на рис. 8.10, справа, — параметры входящего подключения, где также указаны тип сервера, методы аутентификации и шифрования.

Кнопка **Diagnose** (Диагностика) в окне состояния подключения (см. рис. 8.9) позволяет проверить правильность соединения и устранить ошибки. Мастер диагностики сети может автоматически устранить некоторые неисправности, связанные с неправильными параметрами TCP/IP протокола (например, если они не получены от DHCP-сервера), может определить отсутствие разрешения DNS-имен и обнаружить отсутствие доступа к Интернету. При наличии сетевых ошибок пользователь видит запрос на выполнение тех или иных действий, которые могут устранить неисправность (рис. 8.11).

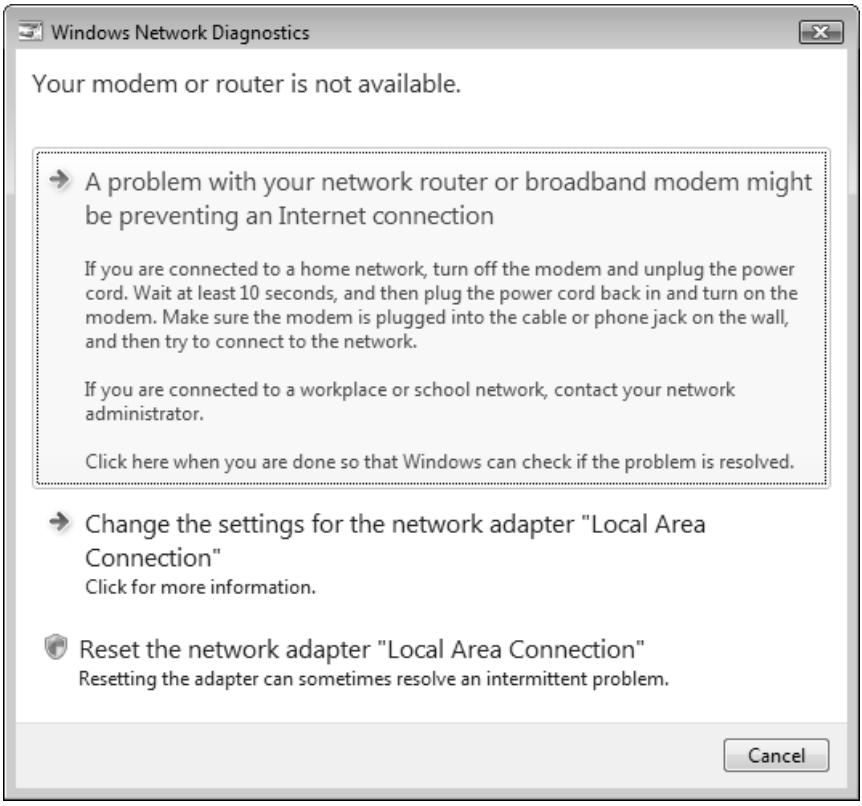


Рис. 8.11. Выбор действий
для восстановления работоспособности сетевого подключения

Если ошибка исправлена, то появляется соответствующее сообщение, и сведения об ошибке можно отправить компании Microsoft.

Совет

Иногда возникают ошибки, связанные с невозможностью получения IP-адреса и других параметров стека TCP/IP от аппаратного маршрутизатора ADSL, RRAS-сервера или компьютера, на котором включено совместное использование интернет-подключения (ICS). В этих случаях — как подсказывает мастер диагностики сети — помогает выключение и повторное включение устройства, перезапуск службы RRAS или перезагрузка компьютера с ICS-подключением.

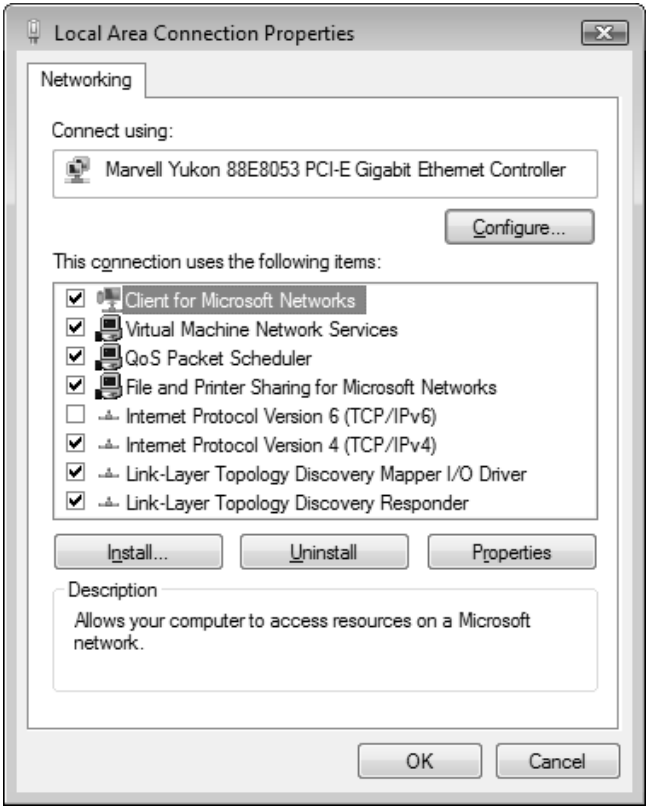


Рис. 8.12. Окно свойств подключения по локальной сети

С помощью кнопки **Properties** (Свойства) можно из окна состояния подключения попасть в окно его свойств, где для подключения по локальной сети

перечислены установленные протоколы и компоненты (рис. 8.12). Обратите внимание на то, что по умолчанию протокол TCP/IPv6 установлен, как и новые компоненты канального уровня (link-layer). При установке сетевого монитора в окне свойств также можно видеть привязку к его драйверу (Microsoft Network Monitor 3 Driver).

Для коммутируемых и VPN-подключений параметров намного больше, и они сгруппированы на нескольких вкладках. На рис. 8.13 показана вкладка **Security** (Безопасность) для VPN-подключения: здесь указываются способы идентификации клиентов и можно задавать методы шифрования сеанса (в том числе можно определять, всегда ли будут использоваться только безопасные, шифрованные, подключения).

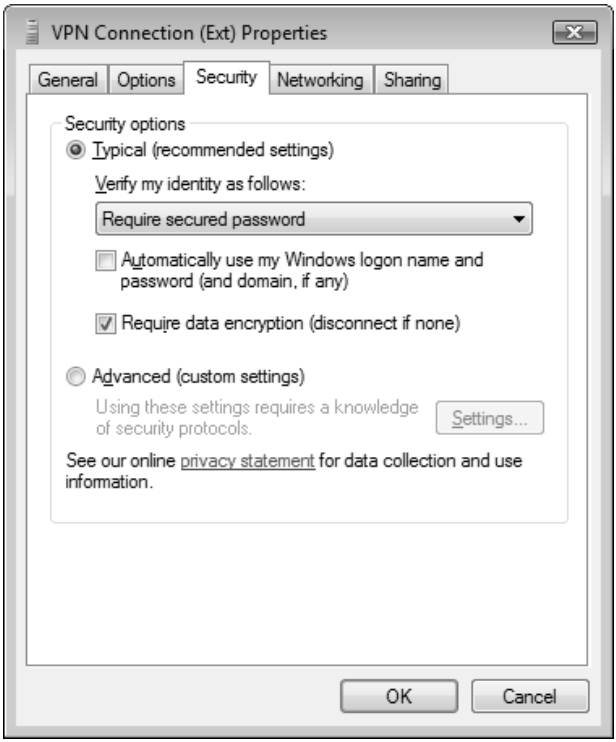


Рис. 8.13. Окно свойств VPN-подключения

В окне свойств сетевого подключения на вкладке **Networking** (Сеть) (см. рис. 8.12) можно запросить установку дополнительных клиентов, протоколов и

служб: при нажатии кнопки **Install** (Установить) появляется окно выбора типа компонентов (рис. 8.14). (Нужно, однако, отметить, что практически все стандартные сетевые компоненты, имеющиеся в составе Windows Server 2008, уже присутствуют в показанном на рис. 8.12 окне свойств подключения; можно лишь добавить *Reliable Multicast Protocol* (RMP; Надежный многоадресный протокол) или же устанавливать компоненты с дискет и других носителей.)

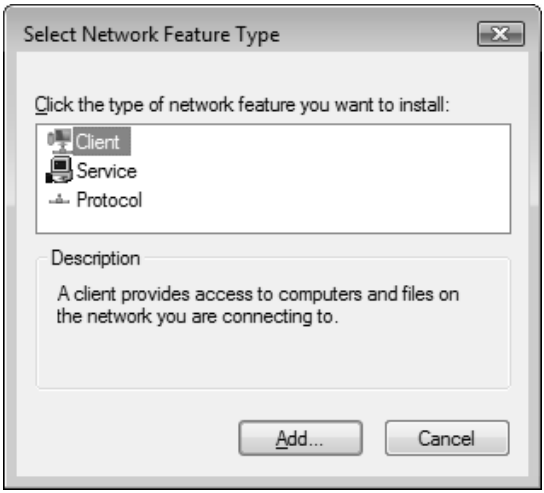


Рис. 8.14. Окно выбора устанавливаемых сетевых компонентов

Управление подключениями

Вернемся к окну Центра управления сетями (см. рис. 8.5) и рассмотрим задачи, список которых имеется в левой части окна. Для перехода в папку **Network** (Сеть) (аналог папки **My Network Places** (Сетевое окружение) в предыдущих версиях Windows; эту папку можно видеть в окне программы Windows Explorer (Проводник)) служит ссылка **View computer and devices** (Просмотр компьютеров и устройств). Если папку **Network** (Сеть) просматривать в режиме Details (Таблица), то можно включить скрытый по умолчанию столбец **Discovery Method** (Метод обнаружения) (для этого достаточно щелкнуть правой кнопкой мыши по заголовку любого столбца и установить соответствующий флажок в списке столбцов). В этом столбце для каждого

видимого компьютера указан протокол, используемый для поиска компьютеров в сети. В системах Windows Vista и Windows Server 2008 для этого обычно применяется новый протокол *Web Service-Discovery* (WS-Discovery, WSD), а для предыдущих версий Windows указывается протокол NetBIOS.

Примечание

Для просмотра сетевых параметров и управления сетевыми подключениями, протоколами и компонентами можно использовать мощную и многофункциональную утилиту командной строки *Netsh.exe*. Она запускается в интерактивном или командном режиме. В первом случае администратор выбирает нужный контекст (набор сетевых параметров, относящихся к определенному компоненту или протоколу) и пошагово выполняет имеющиеся команды. Во втором все параметры задаются утилите при запуске, и она выполняет конкретную задачу *(см. далее примеры в разд. "Просмотр параметров брандмауэра из командной строки")*. Для каждого контекста легко получить набор допустимых команд, введя слово `help` или просто символ вопроса.

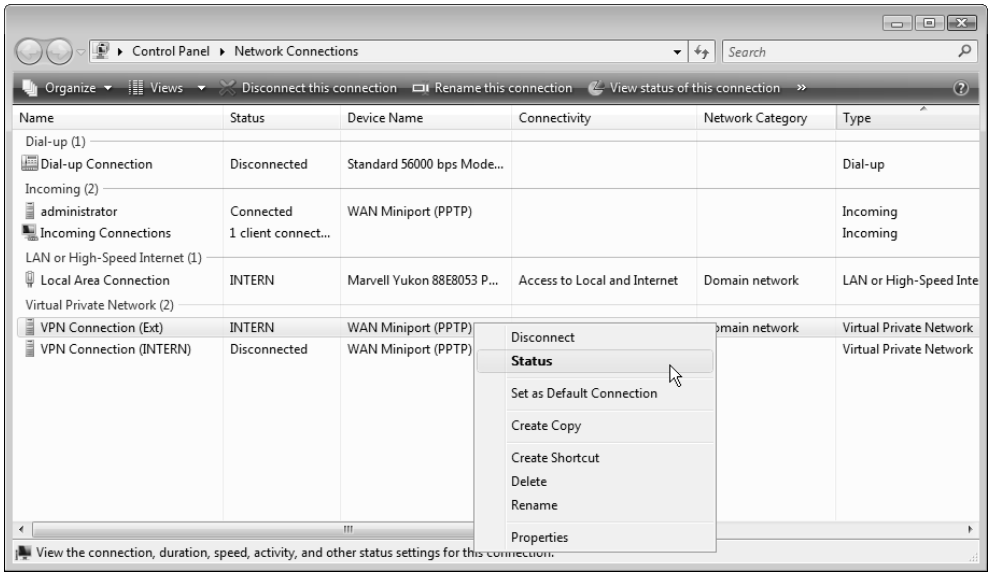


Рис. 8.15. Окно сетевых подключений

По ссылке **Connect to a network** (Подключить к сети) мы из окна Центра управления сетями попадем в окно имеющихся в системе дополнительных

подключений (см. рис. 8.3), где также можно выбирать активную беспроводную сеть (если такое подключение поддерживается и сеть имеется физически).

Для того чтобы увидеть привычную по предыдущим версиям Windows папку сетевых подключений, щелкните по ссылке **Manage network connections** (Управление сетевыми подключениями). В открывающемся при этом окне (рис. 8.15) видны *все* подключения, созданные в системе (не только активные, состояние которых отображается в окне Центра управления сетями). Здесь можно просматривать их свойства, изменять имена и выбирать наиболее удобный способ просмотра их параметров (с помощью меню **Views** (Виды)). Здесь же подключения можно активизировать (команда **Connect** (Подключить)) или, наоборот, разрывать. Нажав клавишу <Alt>, можно включить в окне отображение классического меню и задать группировку по типу (Type) подключения (как показано в нашем примере) или любую другую.

В контекстном меню телефонных и VPN-подключений имеется команда **Set as Default Connection** (Сделать подключением по умолчанию) (см. рис. 8.15). С ее помощью можно выбрать подключение, которое будет автоматически устанавливаться в том случае, если компьютер не связан с сетью, но какие-то программы (системные или, например, Internet Explorer) пытаются обратиться к сетевым ресурсам.

> ***Совет***
>
> Если приходится часто обращаться к окну сетевых подключений, то можно найти в папке C:\Windows\System32 файл ncpa.cpl, создать для него ярлык и перенести в нужное место — на рабочий стол или в меню **Start** (Пуск).

Создание новых подключений

Для создания дополнительных подключений в левой части окна Центра управления сетями (см. рис. 8.5) используется ссылка **Set up a connection or network** (Установка подключения или сети). Она позволяет запустить простой мастер создания подключений, с помощью которого в интерактивном режиме легко можно сконфигурировать подключение любого типа. Этот тип указывается сразу же, в первом окне мастера (рис. 8.16).

Чаще всего создаются коммутируемые и VPN-подключения; эти процедуры мы и рассмотрим подробнее далее, в соответствующих разделах.

Внимание!

Следует помнить о том, что по умолчанию *любое* созданное в системе сетевое подключение защищается встроенным брандмауэром Windows (Windows Firewall), который управляет трафиком по протоколам IPv4 и IPv6. Способы его конфигурирования рассматриваются далее в этой главе. Для настройки параметров брандмауэра можно также использовать утилиту Netsh.exe и групповые политики.

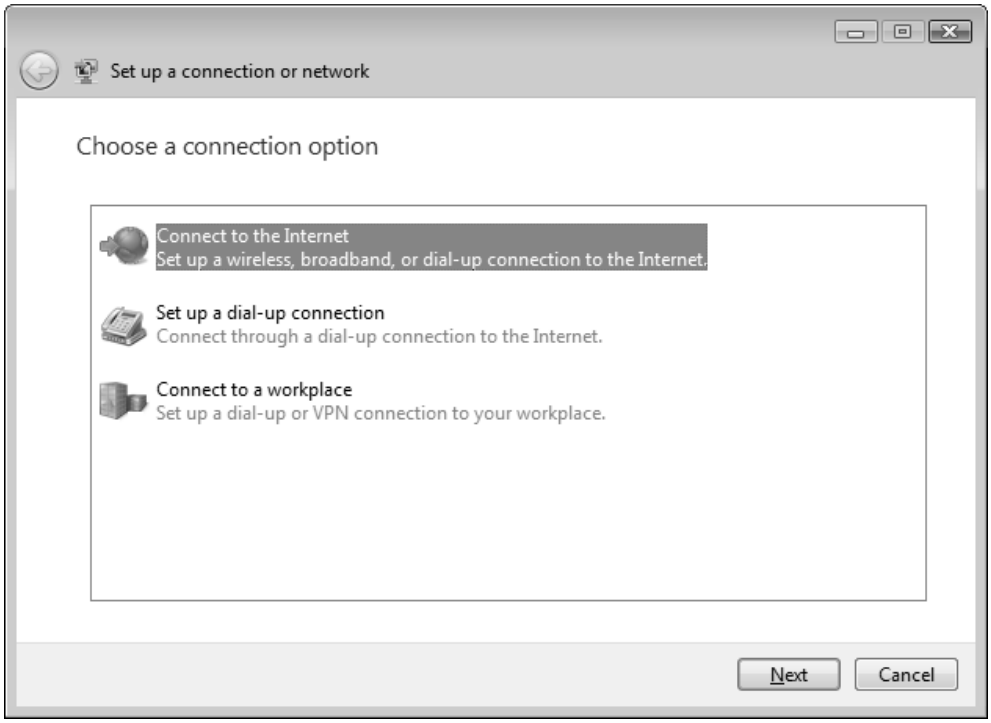


Рис. 8.16. Выбор типа создаваемого сетевого подключения

Типы сетевых подключений

Как и предшествующие версии Windows, системы Windows Server 2008 поддерживают пять типов сетевых подключений, которые перечислены в табл. 8.1.

Таблица 8.1. *Типы сетевых подключений в Windows Server 2008*

Тип подключения	Технология связи	Пример
Подключение по локальной сети (Local Area Connection)	Ethernet, Token Ring, кабельный модем, xDSL, FDDI, IP по ATM, IrDA, радиомодем, E1/T1 и т. п.	Обычный клиент высокоскоростной сети. Часто подобный тип подключений используется кабельными и ADSL-модемами
Телефонное подключение (Dial-up connection)	Модем, ISDN	Соединение с корпоративной сетью или Интернетом с использованием коммутируемого телефонного подключения и обычного модема
VPN-подключение (Virtual Private Network)	Виртуальные частные сети (VPN) по протоколам PPTP или L2TP, объединяющие или подключающие к корпоративным сетям через Интернет или другую сеть общего пользования (public network)	Безопасное соединение с корпоративной сетью через Интернет
Прямое подключение (Direct Connection)	Последовательное соединение, беспроводная сеть, параллельный кабель (DirectParallel), USB-кабель	Соединение планшетного компьютера или ноутбука с настольным компьютером; соединение двух компьютеров
Входящие подключения (Incoming connection)*	Коммутируемая (телефонная) связь, VPN- или прямое подключение	Подключение к компьютеру с использованием коммутируемой линии или VPN-канала от удаленных клиентов

* При разрешении входящих подключений в окне подключений (см. рис. 8.15) всегда имеется только *один* значок (одна запись): тип разрешенных входящих подключений — с использованием модема или VPN-каналов — указывается в свойствах этого значка. На время подключения удаленного пользователя создается свой дополнительный значок с именем этого пользователя.

Внимание!

В системах Windows Server 2008 компонент (feature) *Wireless LAN Service* (Служба беспроводной локальной сети) по умолчанию не установлен, поэтому все возможности беспроводных сетей недоступны. При необходимости нужно установить компонент с помощью оснастки **Server Manager** (Диспетчер сервера) *(см. главу 3)*.

Подключения по локальной сети

При инсталляции операционная система автоматически обнаруживает сетевой адаптер и создает для него подключение, которое так и называется — *Local Area Connection* (Подключение по локальной сети). (При наличии нескольких сетевых плат подобные подключения создаются для каждой из них.) Это подключение отображается (как и любые другие) в окне сетевых подключений (см. рис. 8.15). Если в компьютере имеется несколько сетевых адаптеров, то, соответственно, значок локального подключения появится для каждого адаптера.

По умолчанию локальное подключение всегда активно; это единственный тип подключений, который автоматически становится активным после запуска компьютера или, даже, в процессе установки ОС. Если локальное подключение разъединить, то оно после перезагрузки системы активизироваться не будет и для его работы потребуется принудительное включение.

Соединения с удаленной сетью (интернет-провайдером), осуществляемые с помощью широкополосных или ADSL-модемов и т. п. (все постоянные, автоматически устанавливаемые соединения, для которых может требоваться аутентификация на противоположной стороне), часто также конфигурируются в системе как "подключения по локальной сети" и, соответственно, активизируются сразу же после загрузки системы.

Телефонные (коммутируемые) подключения

Телефонное, или *коммутируемое*, *подключение* (dial-up connection) позволяет соединить компьютер с корпоративной сетью или с Интернетом при помощи устройств, подключаемых к обычной коммутируемой телефонной сети. Чаще всего такими устройствами являются телефонные модемы.

Прежде чем создавать коммутируемое подключение, установите и проверьте модем (для этого используется задача **Phone and Modem Options** (Телефон и модем) на панели управления). Затем в окне мастера подключений (см. рис. 8.16) нужно выбрать одну из трех опций, которые позволят создать подключение — конкретный выбор определяется лишь назначением подключения (от этого будут зависеть используемые сетевые настройки и свойства обозревателя: в одних случаях его параметры будут меняться, в других — нет). Для подключения к интернет-провайдеру можно использовать самую простую опцию — **Set up a dial-up connection** (Настройка телефонного подключения). Если нужно подключиться к корпоративному серверу удаленного доступа (RAS), выбирайте опцию **Connect to a workplace** (Подключение к рабочему месту) (в этом случае указывается только номер телефона, а имя пользователя и его пароль определяются учетной записью безопасности, которая будет использоваться при выполнении подключения).

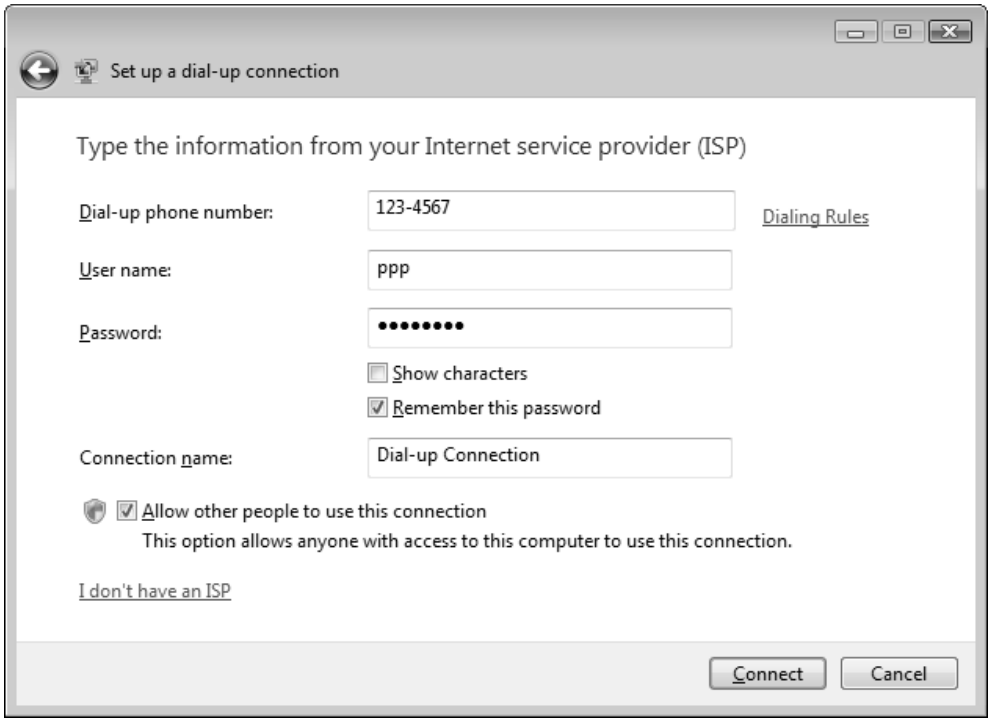


Рис. 8.17. Ввод параметров для подключения к провайдеру

После выбора нужной опции укажите модем, который будет использоваться; если модем только один, то этот шаг отсутствует. Рассмотрим далее подключение к Интернету. На следующем шаге (рис. 8.17) введите данные, полученные от интернет-провайдера: номер телефона, имя и пароль. Сразу после нажатия кнопки **Connect** (Подключить) система попытается установить созданное подключение.

В случае неудачи при создании нового подключения (*любого* типа!) пользователь имеет три возможности: он может повторить попытку, запросить диагностику или создать подключение, несмотря на ошибку подключения (в этом случае при установлении соединения пароль нужно будет вводить снова; в случае успеха он запоминается сразу) (рис. 8.18). По завершении операции новый значок или запись появляется в окне сетевых подключений (см. рис. 8.15).

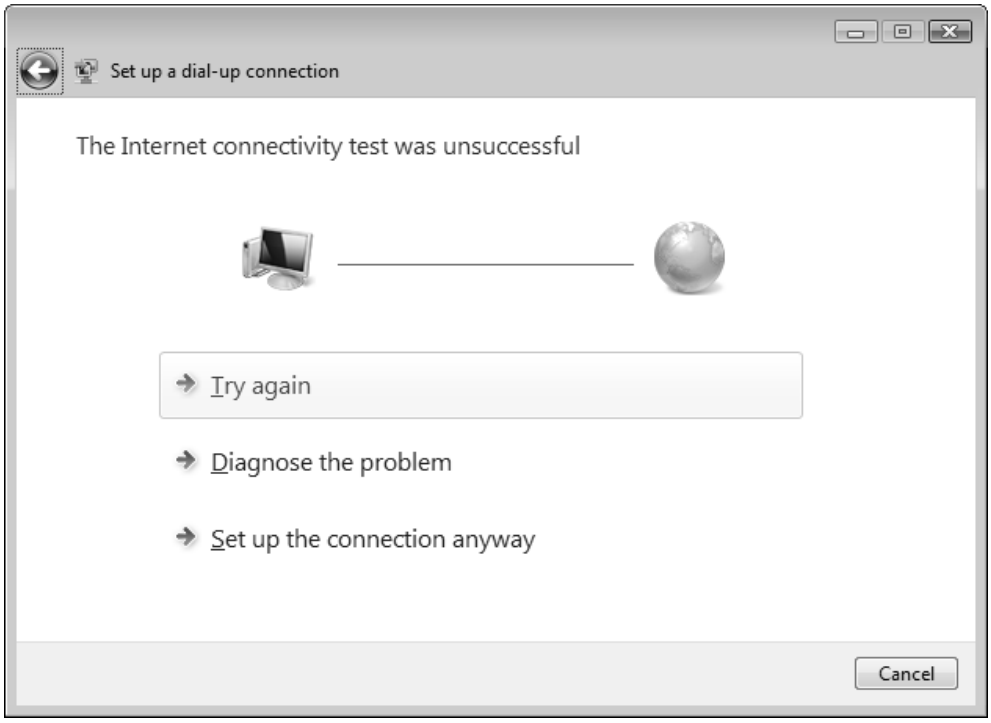


Рис. 8.18. Выбор действий
при неудачной проверке создаваемого подключения

Виртуальные частные сети (VPN)

Протоколы PPTP или L2TP, присутствующие в системе, обеспечивают надежный доступ к сетевым ресурсам при соединении с сервером удаленного доступа (RAS) через Интернет или другую сеть. Если для создания сетевого подключения к частной (private) сети используется общедоступная (public) сеть, то совокупность таких подключений называется *виртуальной частной сетью* (Virtual Private Network, VPN).

Создать VPN-канал между двумя системами достаточно просто, для этого нужно:

- на одном компьютере настроить ***входящее*** подключение *(см. далее)* и разрешить VPN (этот компьютер будет выполнять функции *VPN-сервера*);

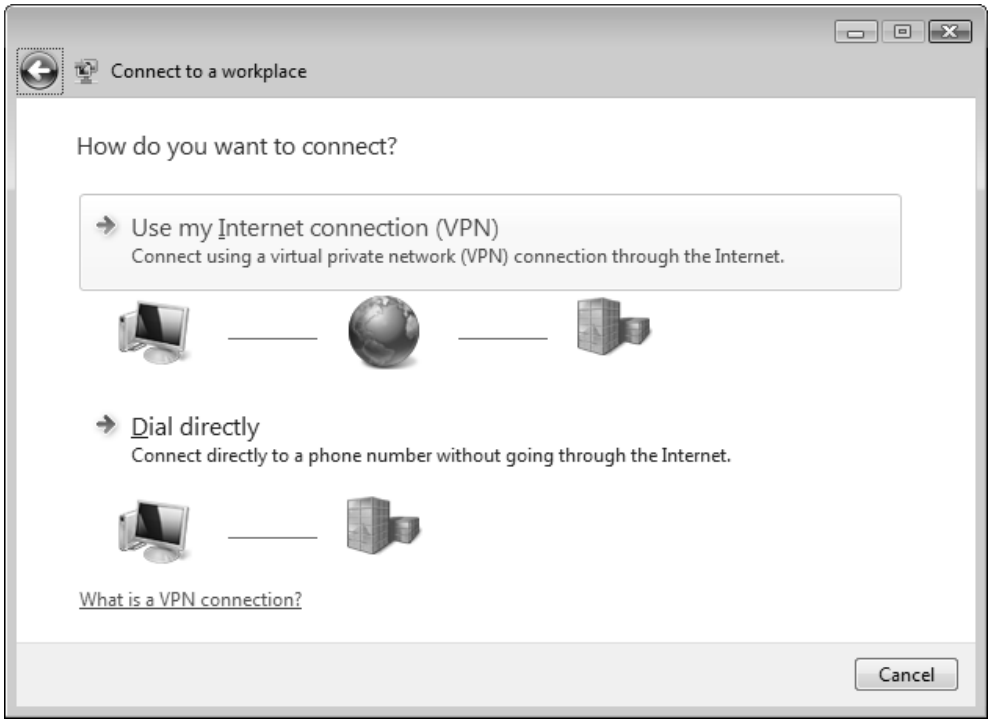


Рис. 8.19. Выбор способа подключения к удаленному рабочему месту

- а на другом — в окне мастера подключений (см. рис. 8.16) выбрать опцию **Connect to a workplace** (Подключение к рабочему месту), после чего

в окне выбора типа соединения (рис. 8.19) указать на использование VPN-подключения (**Use my Internet connection (VPN)**).

Далее следует ввести DNS-имя или IP-адрес VPN-сервера и дать VPN-подключению произвольное имя (рис. 8.20). Для регистрации на сервере нужно указать имя учетной записи и пароль, а также имя домена (сервера) (рис. 8.21). Подключение может устанавливаться сразу или в будущем — см. соответствующий флажок на рисунке. Когда подключение создано (и установлено), можно закрыть окно мастера.

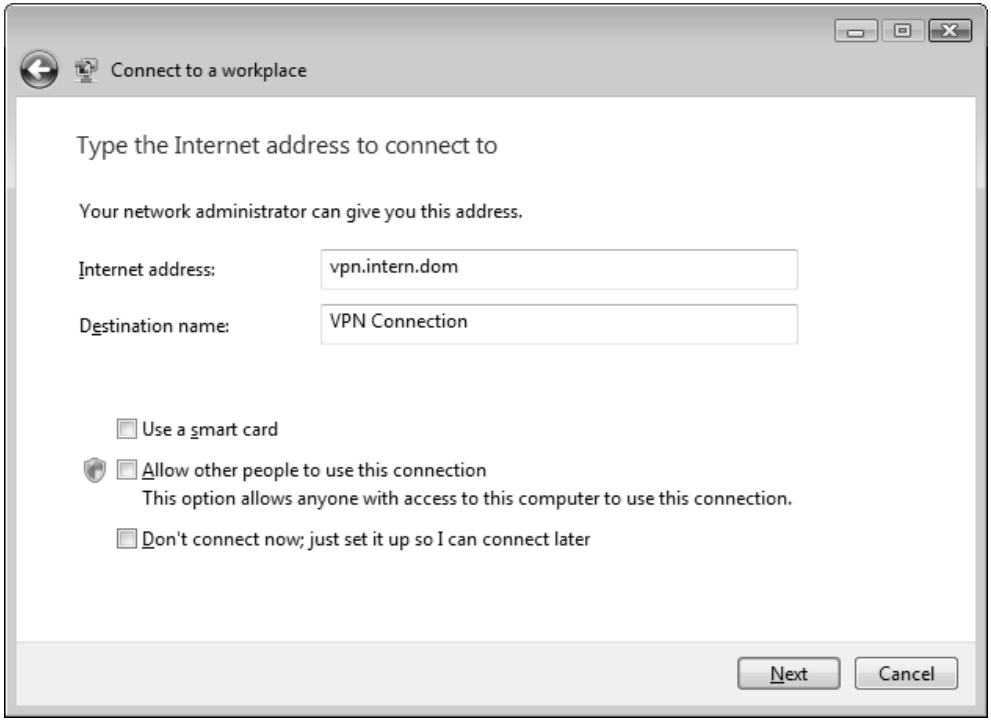


Рис. 8.20. Параметры создаваемого VPN-подключения

Передача информации по VPN-подключению по умолчанию шифруется. (Убедиться в этом можно, просматривая состояние подключения.) VPN-подключение, как и любое другое, можно сделать общим для всех компьютеров сети (т. е. разрешить опцию *Internet Connection Sharing*, ICS (Общий доступ к подключению к Интернету; *см. ниже*).

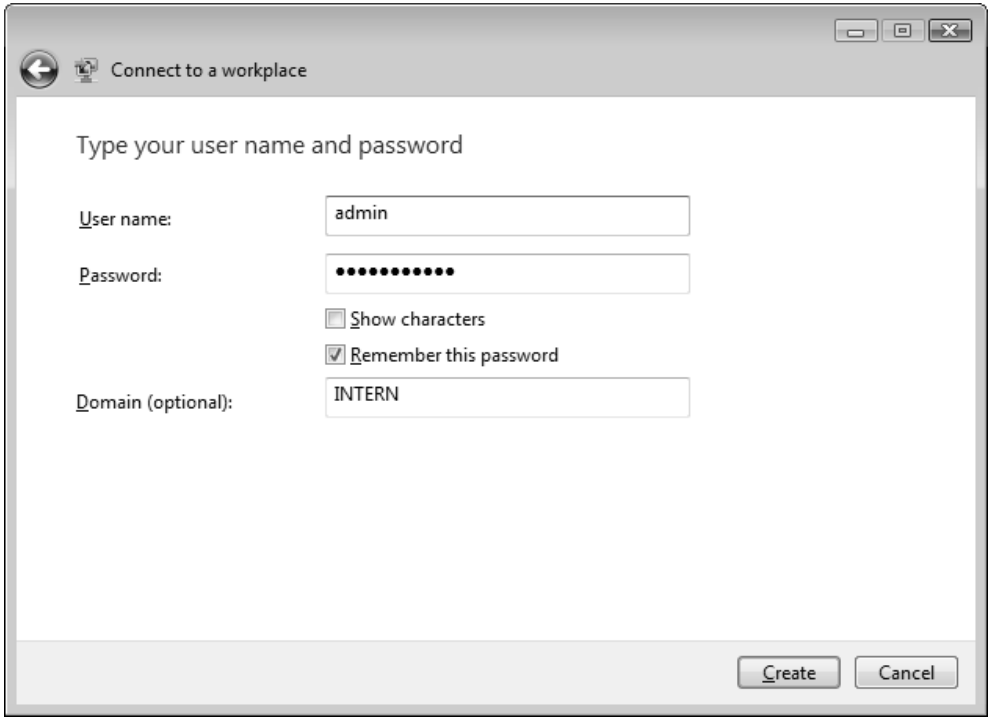


Рис. 8.21. Ввод учетных данных, используемых для подключения к VPN-серверу

Прямые подключения

Прямые подключения (Direct Connection) возможны при наличии физического соединения с другим компьютером через последовательный кабель, USB-кабель, кабель прямого параллельного подключения (DirectParallel), модем и т. д. Прямые подключения могут обходиться без аутентификации (для этого нужно настроить входящее подключение на ведомом компьютере).

Входящие подключения

При наличии *входящих подключений* компьютер под управлением Windows Server 2008 может служить сервером удаленного доступа. Можно создавать входящие подключения для приема вызовов, выполняемых с помощью телефонных подключений (модем, ISDN), VPN-подключений (PPTP, L2TP) или

прямых подключений (последовательный или параллельный кабель, беспроводная связь). В любом случае способ включения входящих подключений остается тем же самым, и его можно использовать многократно.

Процедура разрешения входящих подключений в системах Windows Vista и Windows Server 2008 инициируется не самым очевидным образом, совершенно отлично от всех остальных типов подключений. Для того чтобы включить возможность приема входящих подключений, в окне сетевых подключений (см. рис. 8.15) нажмите кнопку <Alt> — появится классическое меню (такой же метод включения меню используется в программе Windows Explorer (Проводник), браузере Internet Explorer 7.0 и т. д.) В меню выполните команду **File | New Incoming Connection** (Файл | Новое входящее подключение).

При создании подключения определяются пользователи, которые смогут удаленно подключаться к компьютеру (рис. 8.22). По умолчанию в списке представлены имеющиеся локальные или доменные учетные записи; в этом же окне можно создать и новых пользователей.

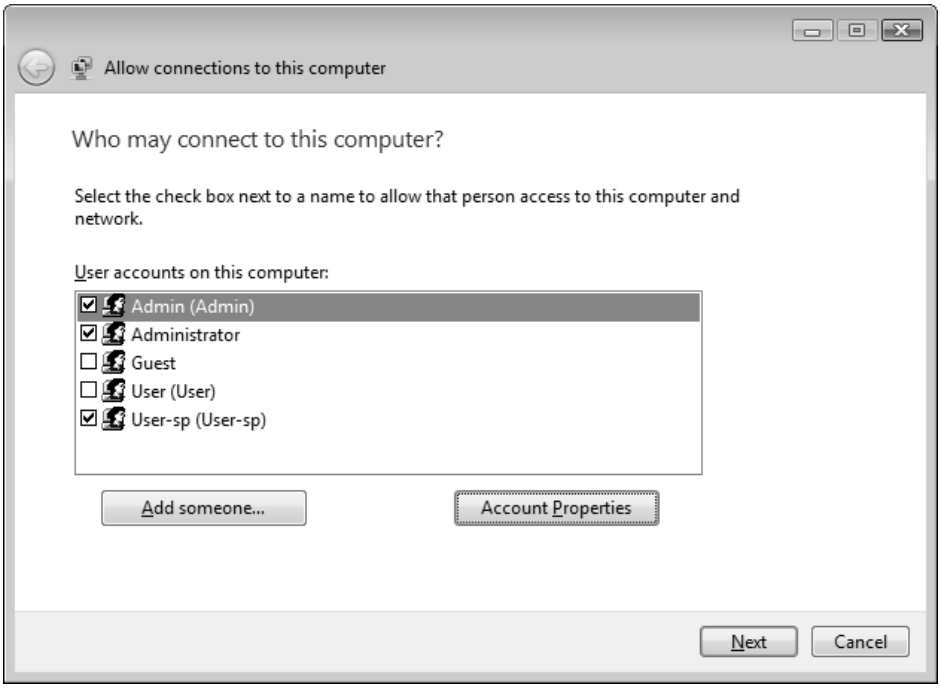


Рис. 8.22. Выбор учетных записей, которые смогут получить удаленный доступ к данному компьютеру

На следующем шаге нужно указать тип входящих подключений, которые будут использоваться (рис. 8.23). Доступ может осуществляться через сеть (Интернет) — VPN-подключения — и/или с помощью модема (модемов), подключенного к компьютеру. В первом случае компьютер будет выполнять функции *VPN-сервера*, во втором — *RAS-сервера* (Remote Access Server; сервер удаленного доступа).

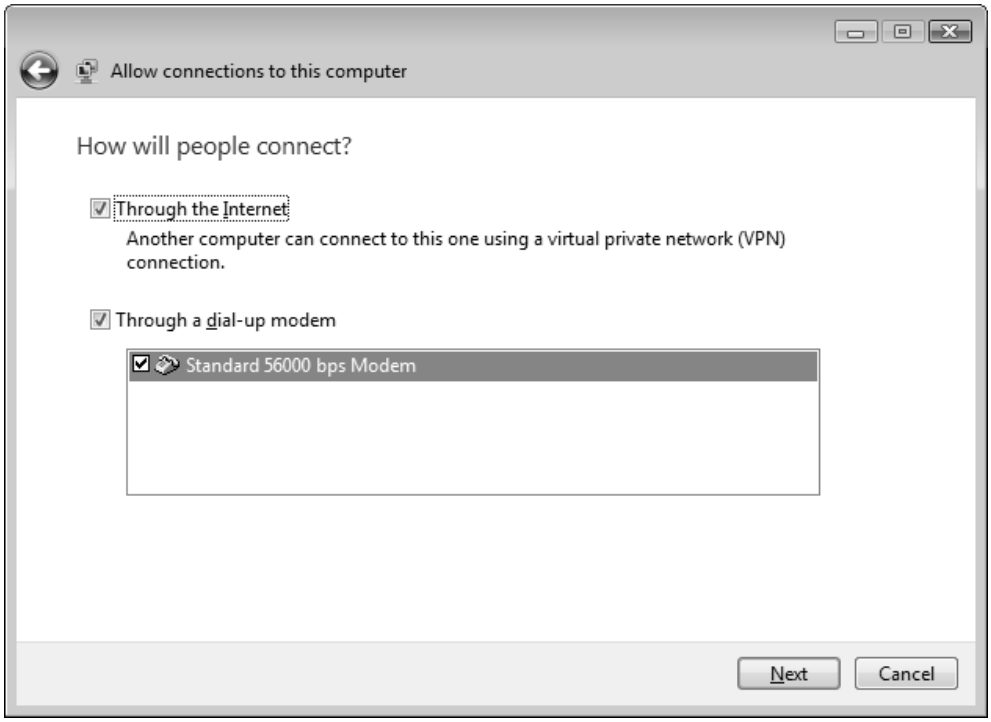


Рис. 8.23. Выбор типа разрешенных входных подключений

Затем следует выбрать службы и протоколы для входящих подключений (рис. 8.24) и, что очень важно, определить свойства протоколов (поскольку они указывают на возможность доступа к локальной сети и способ назначения IP-адресов — см. на рис. 8.24 окно свойств протокола IPv4). Когда все параметры заданы, нужно нажать кнопку **Allow access** (Разрешить доступ). Теперь удаленные клиенты смогут подключаться к локальному компьютеру.

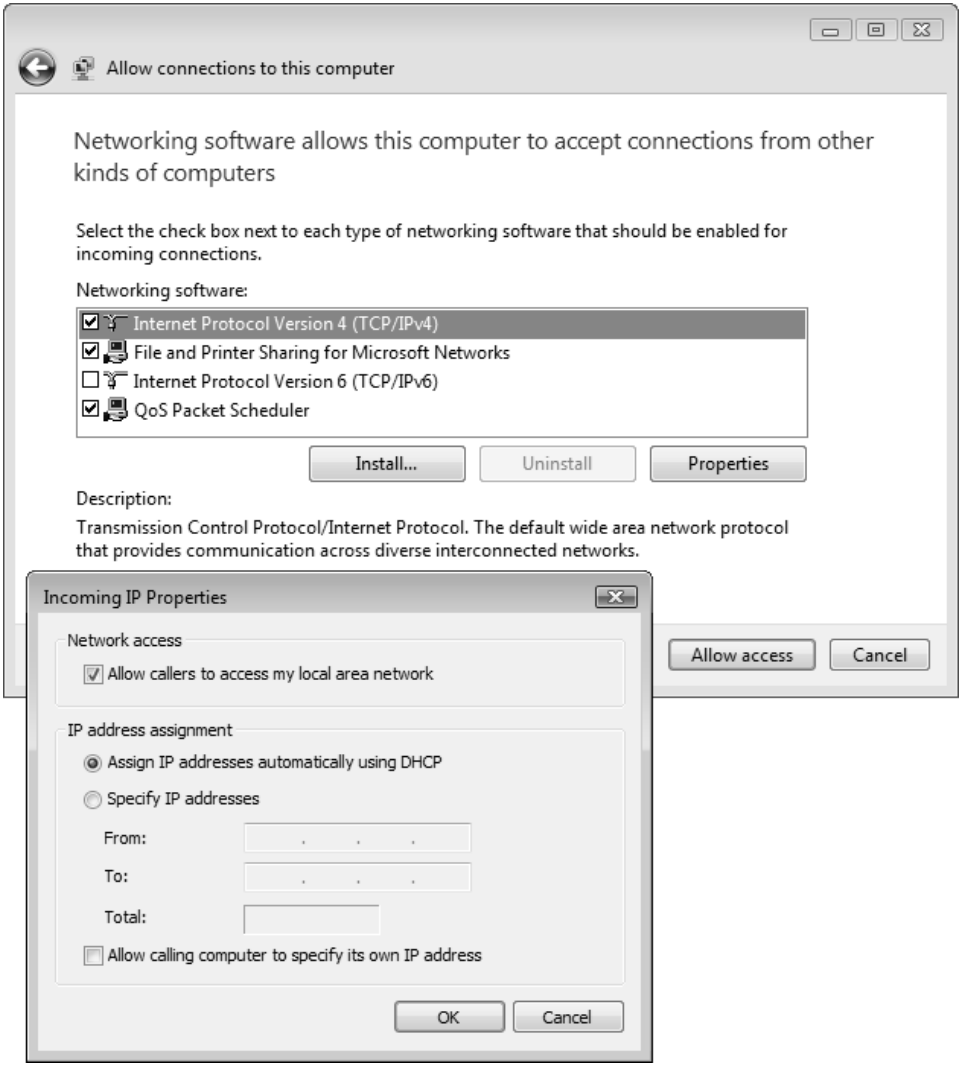


Рис. 8.24. Выбор протоколов и служб, используемых входящими подключениями

Совместное использование интернет-подключения (ICS)

Функция *Internet Connection Sharing*, ICS (Общий доступ к подключению к Интернету) позволяет одно сетевое соединение (любого типа), созданное на

компьютере, использовать для подключения небольшой одноранговой сети к Интернету или внешней сети. В этом случае данный компьютер предоставит всем остальным компьютерам локальной сети возможность использования служб преобразования сетевых адресов (Network Address Translation, NAT), выдачи адресов (DHCP) и разрешения имен (DNS).

Компьютеру, использующему ICS, требуется два сетевых подключения, например:

- подключение через обычный сетевой адаптер служит для связи между компьютерами в локальной сети;
- коммутируемое или постоянное подключение для связи компьютера с Интернетом (любой внешней сетью) или VPN-подключение к удаленному серверу.

При разрешении совместного использования внешнего подключения компьютер становится DHCP-сервером для всей локальной сети, динамически выделяя компьютерам IP-адреса при запуске систем — для этого все клиенты сети должны быть настроены на автоматическое получение параметров IP (этот режим обычно задается сразу при установке систем). Помимо этого, выбранный компьютер выполняет функции кэширующего DNS-сервера, осуществляя разрешение имен для клиентов "своей" сети (при этом используются параметры внешнего подключения и DNS-серверы интернет-провайдера).

> ***Внимание!***
>
> Операция разрешения общего доступа к подключению к Интернету довольно ответственна, поскольку влияет на существующие сетевые параметры компьютера и требует, чтобы у клиентов локальной сети была включена автоматическая настройка протокола IP. Когда разрешается совместное использование подключения, сетевой адаптер, связанный с локальной сетью, получает новый статический IP-адрес (192.168.0.1). Существующие подключения, использующие TCP/IP на этом компьютере, будут потеряны и должны быть восстановлены вручную. Поэтому данную операцию следует выполнять в самом начале работы, при развертывании сети.

Чтобы разрешить совместное использование подключения, необходимо выбрать его в окне сетевых подключений (см. рис. 8.15), открыть окно свойств и на вкладке **Sharing** (Доступ) установить флажок **Allow other network users to connect through this computer's Internet connection** (Разрешить другим

пользователям сети использовать подключение к Интернету данного компьютера) (рис. 8.25).

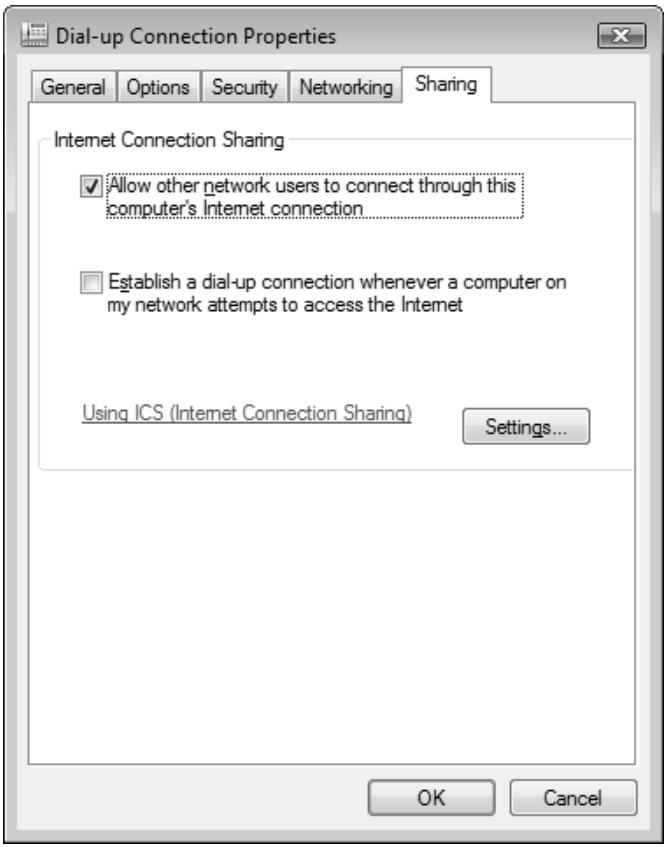


Рис. 8.25. Включение режима ICS на выбранном сетевом подключении

Если требуется, чтобы выбранное подключение автоматически активизировалось, когда другой компьютер локальной сети пытается обратиться к внешним ресурсам (а это, в первую очередь, имеет смысл для коммутируемых подключений), установите флажок **Establish a dial-up connection…** (Устанавливать телефонное подключение при попытке доступа к Интернету)[1].

[1] У постоянных подключений типа ADSL этот флажок отсутствует.

В системах Windows Server 2008 другие пользователи сети не имеют возможности управлять общим интернет-подключением.

Можно указать конкретные приложения и службы, к которым смогут обращаться пользователи Интернета или внешней сети. Например, если в локальной сети (в том числе и на других компьютерах) есть FTP-или веб-сервер, то для того, чтобы с ним могли работать извне, нужно на совместно используемом подключении разрешить соответствующую службу. Для этого на вкладке **Sharing** (Доступ) (см. рис. 8.25) следует нажать кнопку **Settings** (Настройка) и в открывшемся окне (рис. 8.26) установить флажки рядом с именами служб, которые должны быть доступны.

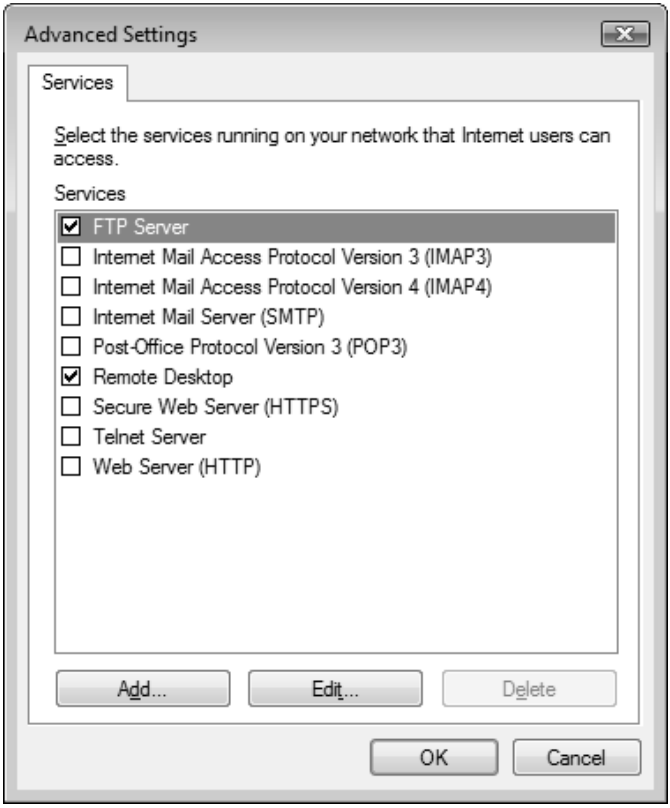


Рис. 8.26. Выбор сервисов,
к которым будет разрешен доступ для пользователей Интернета

Защита сетевых подключений с помощью встроенного брандмауэра Windows Firewall

Системы Windows Vista и Windows Server 2008 имеют в своем составе брандмауэр *Windows Firewall* (Брандмауэр Windows), который является модифицированной и значительно расширенной версией средства Internet Connection Firewall (ICF), реализованного в предыдущих версиях Windows.

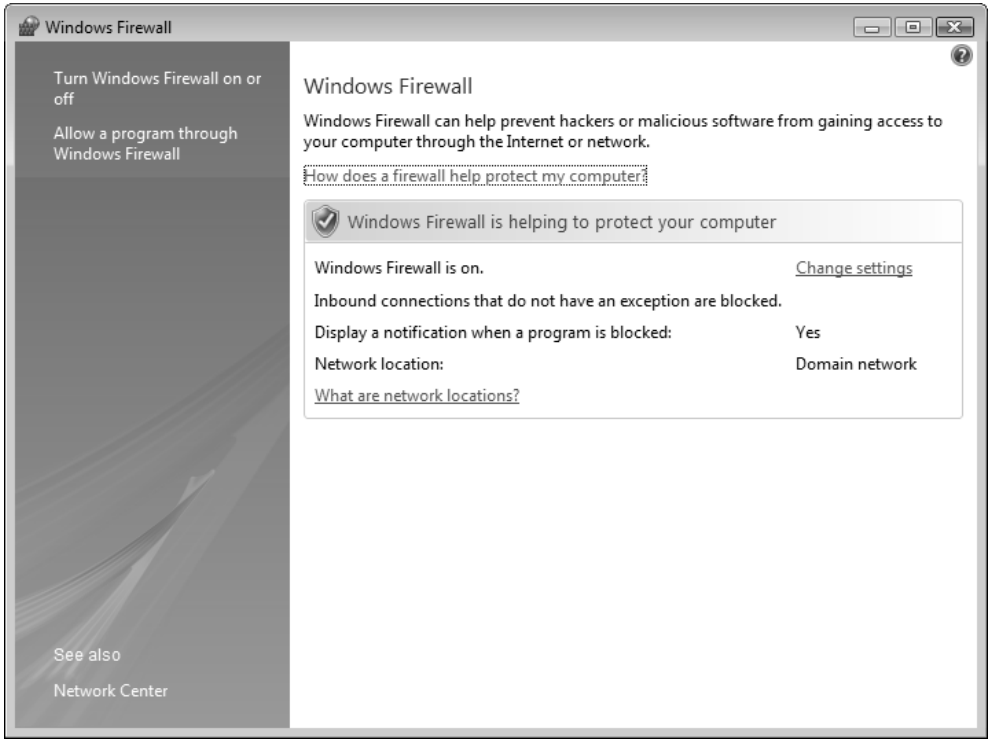


Рис. 8.27. Главное окно брандмауэра Windows

Брандмауэр Windows позволяет фильтровать всю информацию, поступающую из внешней сети (из Интернета), пропуская только разрешенные TCP/UDP-пакеты и отбрасывая все остальные. Таким образом, он ограждает компьютер от несанкционированного доступа или атак из внешней сети, сохраняя при этом возможность работы с веб-сервисами, электронной почтой,

другими компьютерами и т. д. Также возможна фильтрация *исходящих* пакетов — эта опция отсутствовала в предыдущих версиях Windows.

Брандмауэр Windows Firewall можно запустить с панели управления (категория **Security** (Безопасность)) или из окна Центра управления сетями (см. рис. 8.5). На рис. 8.27 показано главное окно брандмауэра — здесь видны его состояние (по умолчанию он включен) и основные параметры сетевой безопасности. Для настройки брандмауэра или просмотра его параметров нужно щелкнуть по ссылке **Change settings** (Изменить параметры).

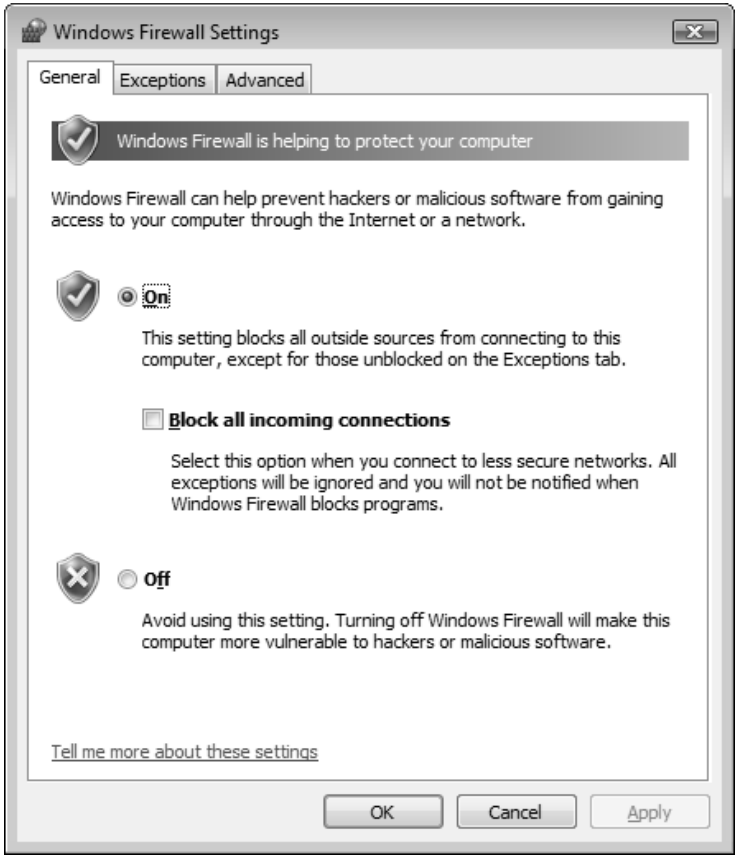


Рис. 8.28. Окно управления состоянием и параметрами брандмауэра Windows

В окне параметров (рис. 8.28), в которое можно также попасть по ссылке **Turn Windows Firewall on or off** (Включение и отключение брандмауэра

Windows), определяется состояние брандмауэра Windows. Здесь можно быстро отключать (блокировать) все входящие соединения, если работа в сети требует повышенных требований к безопасности компьютера (флажок **Block all incoming connections**).

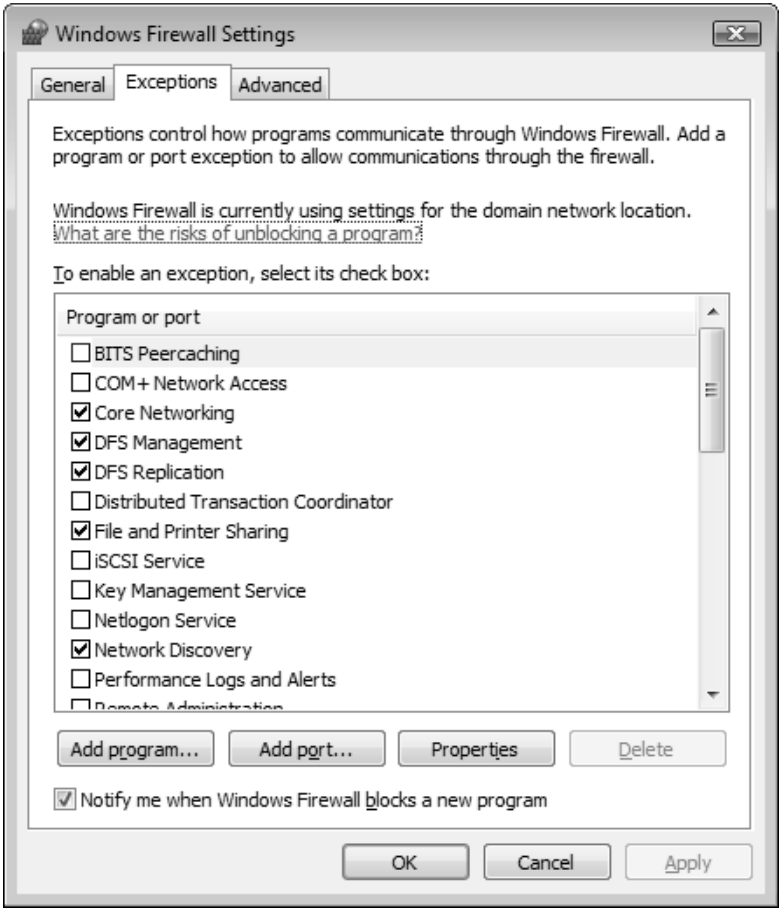


Рис. 8.29. Выбор разрешенных служб, доступных из внешней сети

На вкладке **Exceptions** (Исключения) (рис. 8.29) указываются программы и сервисы, которым *разрешен* доступ по сети. При работе с сетевыми средствами (такими как File and Printer Sharing (Общий доступ к файлам и принтерам) или Remote Desktop (Удаленный рабочий стол)), а также при подключении административных оснасток к удаленным компьютерам, нужно всегда следить за

тем, чтобы соответствующие флажки были установлены. В противном случае весь трафик к этим сервисам или программам будет заблокирован.

Поскольку флажок **Notify me when Windows Firewall blocks a new program** (Уведомлять, когда брандмауэр блокирует новую программу) (см. рис. 8.29) по умолчанию установлен, при попытке любой новой программы установить сетевое соединение брандмауэр будет сообщать об этом пользователю и ожидать от него разрешения на работу программы (рис. 8.30). Если пользователь разблокирует программу, то брандмауэр включит порты, запрашиваемые приложением, в число разрешенных. После этого программа сможет работать беспрепятственно.

Рис. 8.30. Запрос на разрешение входящих подключений для запущенной программы

Нажав кнопку **Add port** (Добавить порт) (см. рис. 8.29), можно затем вручную указать дополнительные порты TCP или UDP, работа по которым будет разрешена (рис. 8.31). Для точного определения типа сети или диапазона адресов, которым будет разрешено обращаться к указанному порту, следует нажать кнопку **Change scope** (Изменить область) и выбрать нужные параметры (рис. 8.32). Аналогичным образом можно изменить область допустимых адресов и для прикладных программ *(см. далее)*.

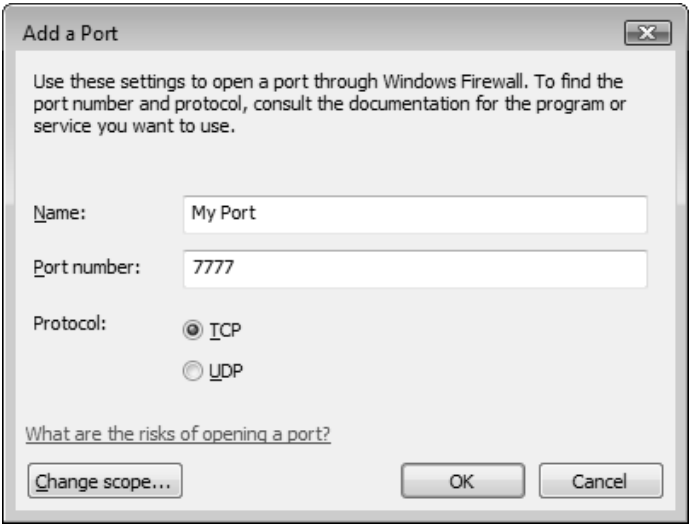


Рис. 8.31. Определение параметров порта, доступ через который будет разрешен брандмауэром Windows

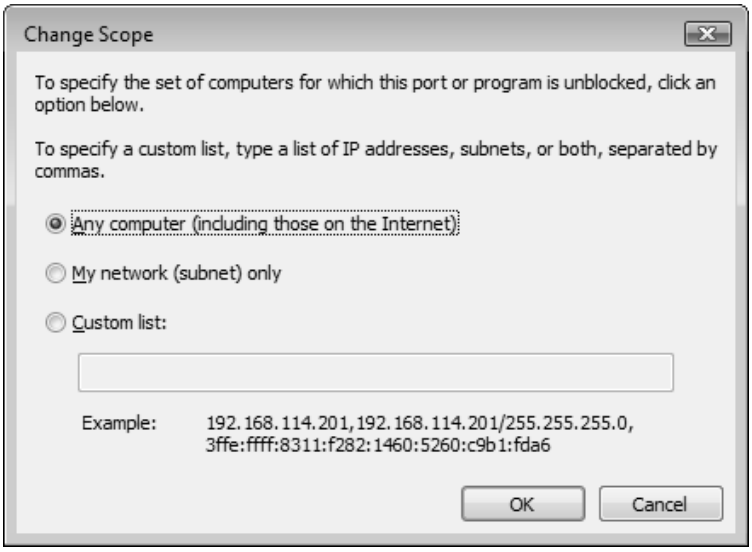


Рис. 8.32. В этом окне можно ограничить список компьютеров, получающих доступ к определенной программе или работающих с протоколом, разблокированным брандмауэром Windows

Кнопка **Add program** (Добавить программу) на вкладке исключений (см. рис. 8.29) позволяет перейти в окно выбора приложений (рис. 8.33), которые смогут взаимодействовать с другими компьютерами через сеть. Для программ, как и для дополнительных портов, можно указывать область допустимых адресов компьютеров (кнопка **Change scope**).

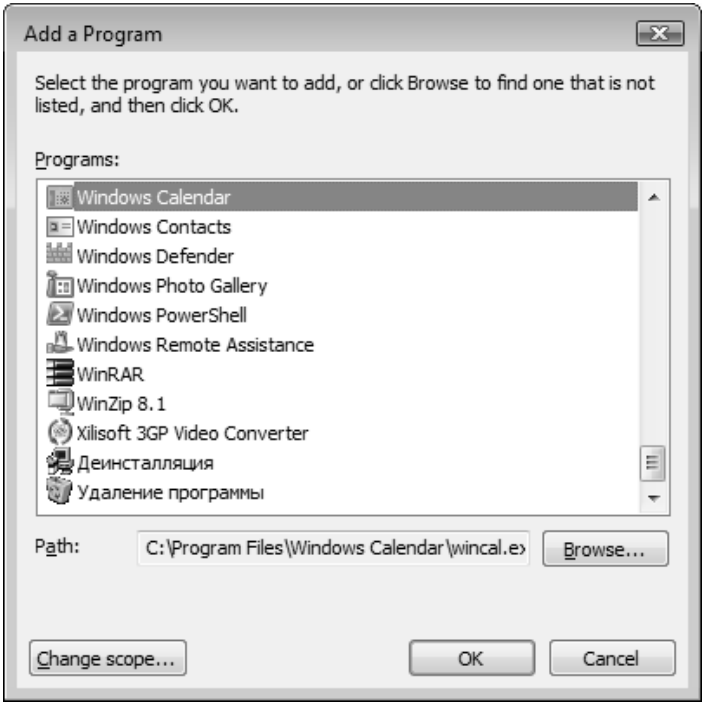


Рис. 8.33. Выбор программ, с которыми можно будет взаимодействовать через сеть

На вкладке **Advanced** (Дополнительно) (рис. 8.34) можно указать, с какими сетевыми подключениями будет работать брандмауэр (параметры будут одинаковыми для всех подключений). На нашем примере видно, что по умолчанию брандмауэр защищает все подключения, созданные в системе. Для определенных подключений, трафик по которым считается полностью безопасным, брандмауэр можно отключить.

Кнопка **Restore Defaults** (По умолчанию) (см. рис. 8.34) позволяет восстановить все стандартные значения параметров, принятые для выбранной категории сети.

Рис. 8.34. Окно выбора дополнительных параметров брандмауэра

Примечание

В брандмауэре, входящем в состав систем Windows Vista/Windows Server 2008, настройка запросов по протоколу *Internet Control Message Protocol* (ICMP), а также ведение журнала осуществляются только с помощью оснастки **Windows Firewall with Advanced Security** (Брандмауэр Windows в режиме повышенной безопасности), описываемой далее.

Просмотр параметров брандмауэра из командной строки

Поистине безграничные возможности утилиты Netsh, запускаемой в окне командной строки, можно использовать и для управления брандмауэром Windows Firewall. Иногда текущие значения сетевых параметров проще получить с ее помощью, нежели в результате просмотра многочисленных диалоговых окон или списков исключений (правил).

Для просмотра состояния брандмауэра и всех его параметров служит команда `netsh firewall show config`; с помощью команды `netsh firewall show state` можно увидеть текущее состояние (включая выбранный сетевой профиль).

Группы параметров можно просматривать индивидуально, например:

- `netsh firewall show allowedprogram` — показывает список разрешенных программ для используемых профилей;
- `netsh firewall show portopening` — перечисляет порты, вручную добавленные к списку исключений;
- `netsh firewall show icmpsetting` — показывает разрешенные ICMP-сообщения.

Для работы с брандмауэром Windows в режиме повышенной безопасности используется контекст "netsh advfirewall".

Невозможно на примерах показать все способы использования утилиты Netsh; хотелось бы, чтобы администраторы всегда помнили о ней в сложных ситуациях (например, когда нужно удаленно настроить сетевые параметры, включая конфигурацию протокола TCP/IP).

Средства расширенного конфигурирования брандмауэра

Оснастка **Windows Firewall with Advanced Security** (Брандмауэр Windows в режиме повышенной безопасности), запускаемая из меню **Administrative Tools** (Администрирование), позволяет управлять встроенным брандмауэром Windows в тех случаях, когда недостаточно стандартных опций настройки (они были рассмотрены выше). В главном окне (рис. 8.35) сразу после запус-

ка оснастки можно видеть основные параметры для каждого сетевого профиля (размещения или категории сети).

Кнопка **Windows Firewall Properties** (Свойства брандмауэра Windows) в центре начальной страницы позволяет перейти в окно настроек (рис. 8.36), где определяются общие параметры брандмауэра для каждого сетевого профиля и протокола IPSec. Таким образом, при переключении профиля (ручном или автоматическом) соответствующим образом сразу же будет меняться режим работы брандмауэра и правила для входящих и исходящих соединений.

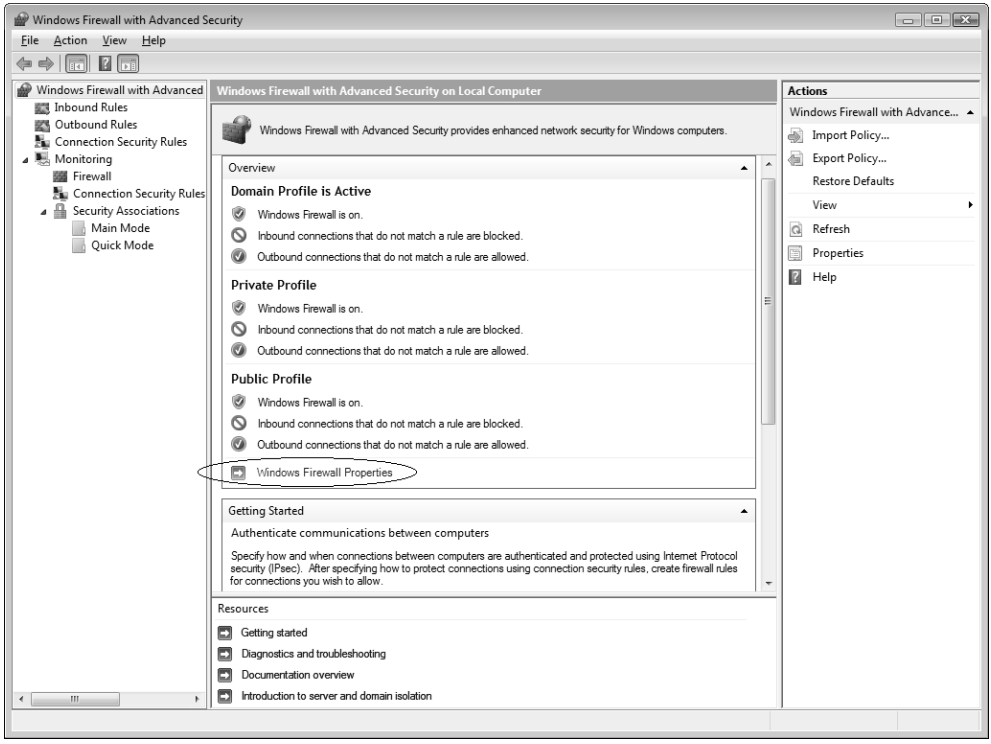


Рис. 8.35. Главное окно оснастки
Windows Firewall with Advanced Security

Брандмауэр Windows настроен на три профиля: *доменный* (Domain Profile), *частный* (Private Profile) и *общий* (Public Profile). С каждым профилем, который соответствует категории сети *(см. ранее)*, связаны определенные правила (rules), и эти правила можно индивидуально настраивать в соответ-

ствии со своими представлениями о требованиях безопасности (в данном случае речь идет о наборе разрешенных портов), предъявляемых к каждой категории сети.

Основное назначение оснастки **Windows Firewall with Advanced Security** (Брандмауэр Windows в режиме повышенной безопасности) — возможность настройки правил для входящих и исходящих пакетов "с точностью" до порта (TCP или UDP), а также управление каждым созданным правилом. В окне оснастки имеются папки, где сгруппированы правила для каждого типа соединений. Как видно на рис. 8.37, в системе имеется множество предустановленных правил, многие параметры которых менять нельзя.

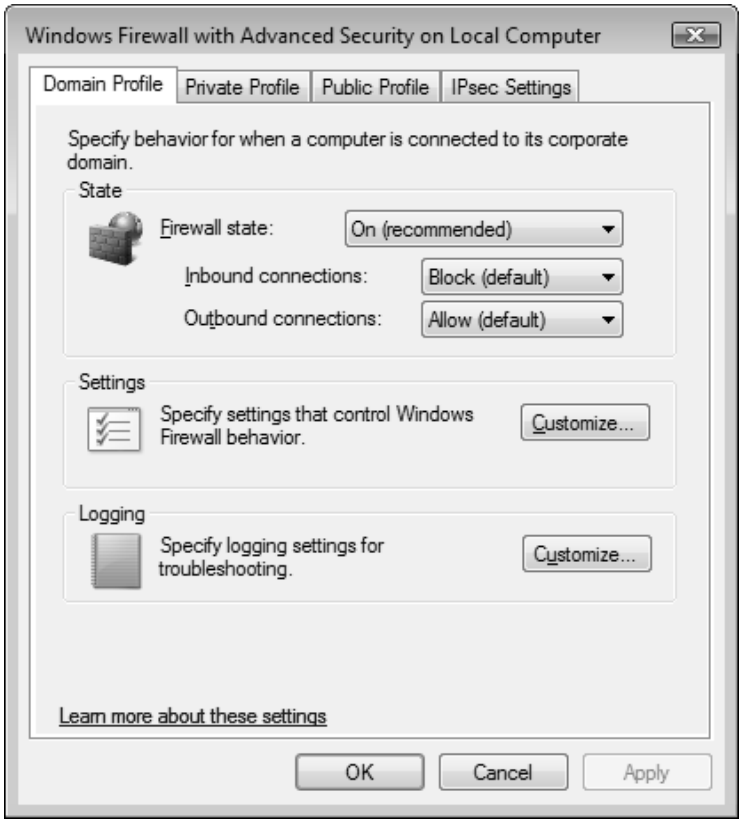


Рис. 8.36. Глобальные параметры брандмауэра для каждого типа сетевого профиля и для протокола IPSec

Помимо стандартных правил, можно создавать и конфигурировать собственные — для этого используется специальный мастер, упрощающий эту операцию. Для его запуска служит ссылка **New Rule** (Новое правило) на панели **Actions** (Действия).

В окне свойств правила можно видеть подробные сведения обо всех заданных параметрах. В первую очередь определяется, разрешены или запрещены сетевые пакеты с заданными характеристиками (на рис. 8.38 в качестве примера показано предустановленное правило, регламентирующее доступ к общим папкам и принтерам).

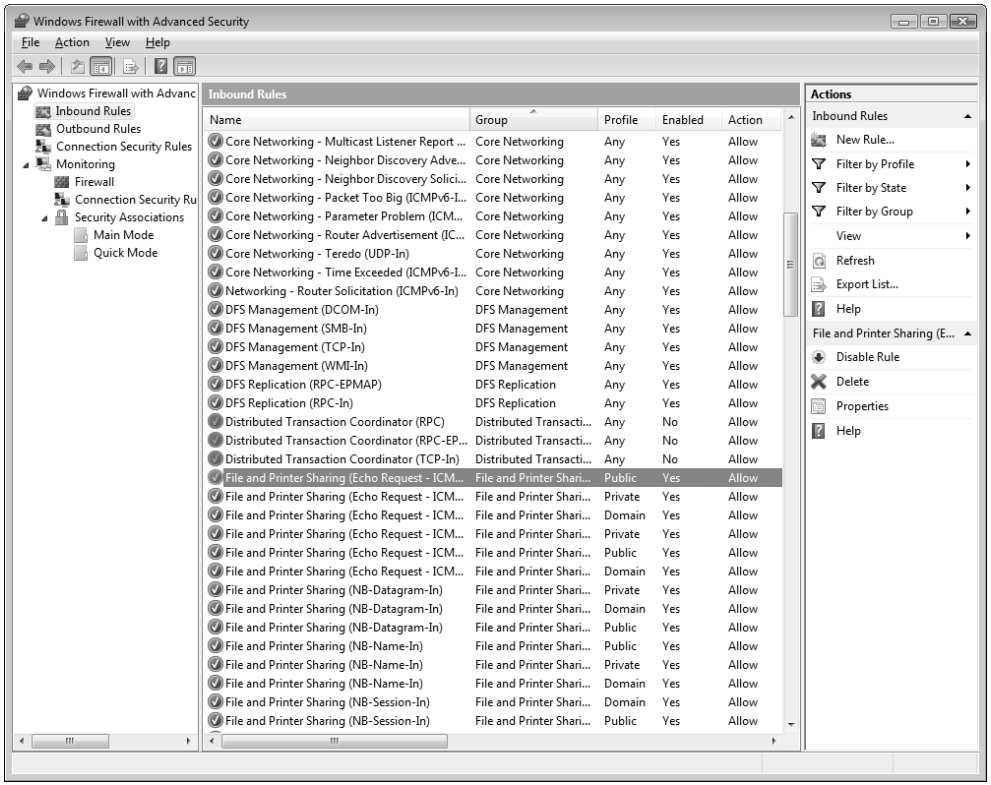


Рис. 8.37. Перечень правил, установленных для входящих соединений

На других вкладках окна свойств правила определяются параметры, описывающие все аспекты сетевого взаимодействия (протоколы, порты, диапазоны разрешенных адресов, приложения, сервисы и т. д.). Правило будет распро-

страняться только на те протоколы и порты, адреса и компьютеры, которые заданы в окне свойств (рис. 8.39).

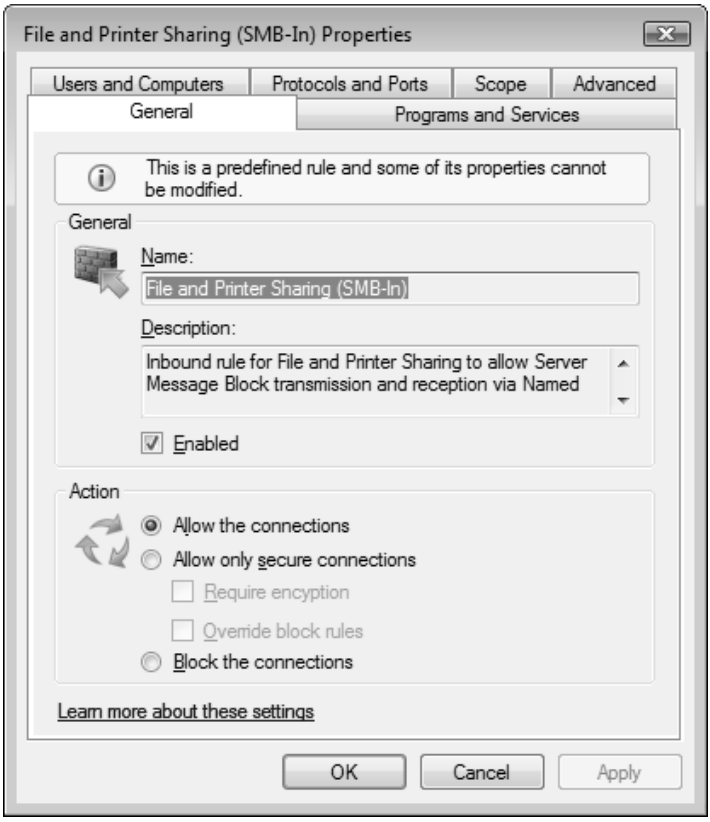
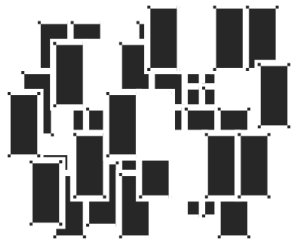


Рис. 8.38. Определение действий для данного правила

Как уже говорилось, весь трафик (сообщения) по протоколу *Internet Control Message Protocol* (ICMP регламентируется правилами, заданными в оснастке **Windows Firewall with Advanced Security** (Брандмауэр Windows в режиме повышенной безопасности). Для входящих и исходящих запросов с использованием протоколов ICMPv4 и ICMPv6 имеются стандартные правила для всех трех сетевых профилей: эти правила называются **File and Printer Sharing (Echo Request)** (Общий доступ к файлам и принтерам (эхо-запрос)). По умолчанию разрешены только эхо-запросы, остальные ICMP-сообщения блокируются.

Рис. 8.39. Протокол и порт, на которые распространяется данное правило

Глава 9



Службы печати и факсов

Эта глава содержит основные сведения по установке и совместному использованию серверов печати и факсов в сети на базе систем Windows Server 2008. Установка и использование устройств печати является несложной задачей, но при большом их количестве и при работе в сети необходимо хорошо знать способы их конфигурирования. Факс-сервер позволяет использовать модемы с возможностями факсимильной связи как обычные принтеры, при этом возможен режим совместного использования одного устройства многими сетевыми клиентами.

Службы печати

Базовые возможности служб печати в Windows Server 2008 практически не изменились по сравнению с версией Windows Server 2003. Основные отличия касаются средств администрирования и возможностей управления установкой принтеров на клиентских компьютерах, входящих в домены Active Directory.

Сначала перечислим некоторые термины, которые используются в службах печати операционных систем Windows. Это позволит лучше ориентироваться в дальнейших разделах.

Терминология

В системах Windows *устройством печати* (printing device) называется реальное физическое устройство, которое собственно и выполняет печать. *Принтер* (printer) — это программный интерфейс между операционной сис-

темой и устройством печати. Принтер определяет различные аспекты процесса печати, например, куда будет послан документ (в локальный порт, в файл или на удаленный общий ресурс печати), отправленный на печать. Когда пользователи устанавливают соединение с принтерами, они используют логическое имя принтера, которое может представлять одно или несколько устройств печати.

Драйвер принтера (printer driver) — программа, которая преобразует графические команды в специфический язык типа PostScript или PCL. В системы Windows Server 2008 включены драйверы для наиболее распространенных устройств печати. Когда принтер *создается*, устанавливается драйвер принтера и — факультативно — можно сделать принтер доступным по сети для совместного использования.

В терминологии Windows, *очередь* (queue) — группа документов, ждущих печати.

Спулер (spooler) печати, или *диспетчер очереди* печати — набор динамических библиотек (DLL), которые получают, обрабатывают, планируют и распределяют документы.

Спулинг (spooling) — процесс записи содержимого документа в файл на диске. Этот файл называется *файлом спулинга* (spool file) или *файлом очереди печати*.

Сервер печати (print server) — любой компьютер, который получает документы от клиентов и имеет подключенное локально устройство печати с разрешенным общим доступом.

Устройства печати с сетевым интерфейсом (network-interface print devices) — устройства печати, имеющие собственные сетевые платы; они не соединяются физически с сервером печати, т. к. подключены к сети непосредственно.

Возможности печати в Windows Server 2008

Рассмотрим возможности служб печати в системах Windows Server 2008. Некоторые новшества в пользовательском интерфейсе папки принтеров и факсов появились уже в Windows Vista (практически все перечисленные далее средства печати доступны и в этой системе).

Удобный пользовательский интерфейс. Изменения в пользовательском интерфейсе коснулись средств программы Windows Explorer (Проводник) и мастеров установки новых принтеров и драйверов.

- Папка **Printers** (Принтеры) (рис. 9.1) содержит значки принтеров и факсов, установленных на компьютере. Это могут быть локальные устройства печати или принтеры, установленные на других компьютерах (включая сетевые принтеры). На панели задач имеются кнопки запуска мастера установки нового принтера и просмотра свойств сервера печати *(см. далее)*.

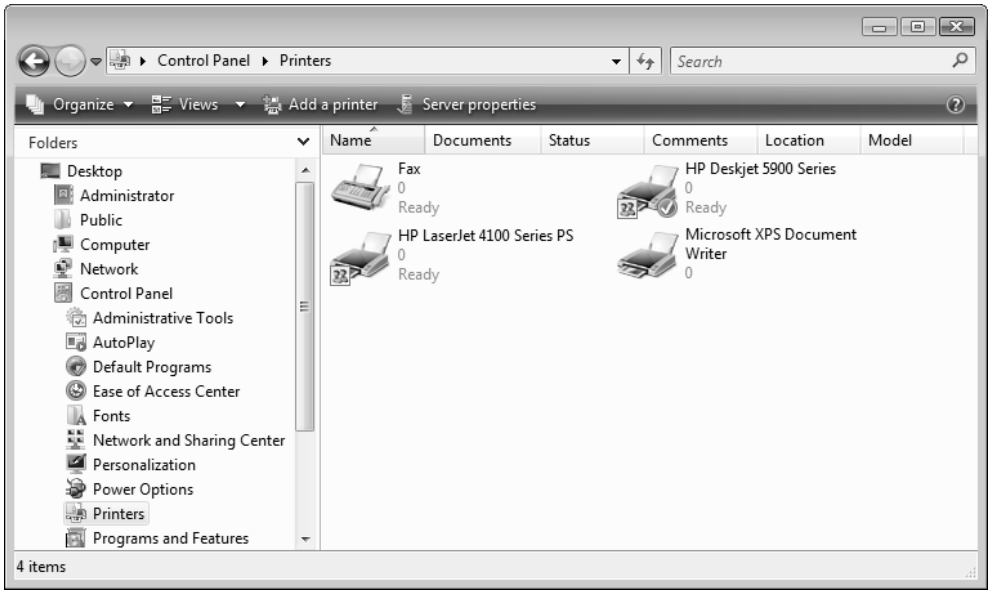


Рис. 9.1. Папка установленных принтеров и факсов

- Специальный мастер *Add Printer Wizard* (Мастер установки принтеров) позволяет пользователю подключить любой принтер, а также искать принтеры не только в сети, но и в каталоге Active Directory *(см. далее)*.
- Мастер *Add Printer Driver Wizard* (Мастер дополнительных драйверов принтера) используется при установке драйверов принтера для клиентов, работающих на других платформах (x86, x64 или Itanium) (рис. 9.2). (Имеется несколько способов для его запуска — из окна свойств принтера (см. рис. 9.10) или с соответствующей вкладки в окне свойств сервера печати).

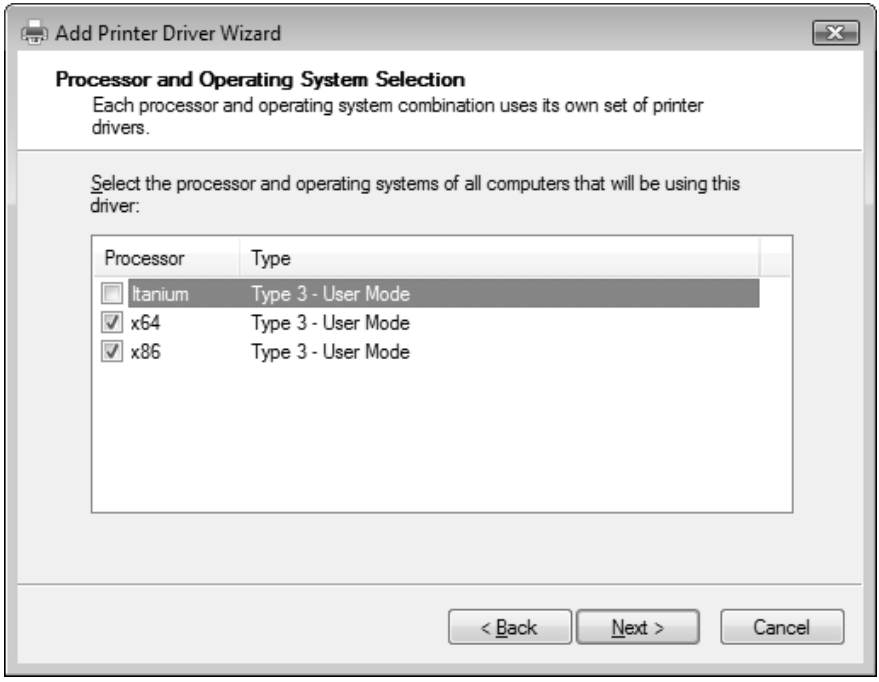


Рис. 9.2. Установка драйверов для различных компьютерных платформ

- Стандартное окно вывода на печать (рис. 9.3) позволяет устанавливать новый принтер, выполнять печать на любом имеющемся принтере (включая факс-принтеры), а также выполнять поиск принтера в каталоге Active Directory (кнопка **Find Printer** (Найти принтер)) с его последующей установкой. После установки операционной системы в этом окне сразу появляется принтер Microsoft XPS Document Writer.

Мониторинг очереди печати. Работу локальных и удаленных принтеров можно контролировать при помощи компонента Performance Monitor (Системный монитор) *(см. главу 5)*. Для объекта *Print Queue* (Очередь печати) могут быть выбраны счетчики производительности: например, *Bytes Printed/sec* (Печатаемых байт/сек), *Job Errors* (Ошибок заданий), *Total Pages Printed* (Всего напечатано страниц) и др. Кроме того, по умолчанию все сообщения о напечатанных документах и ошибках печати регистрируются в журнале системы (System) (`Event Type: Information`; `Event Source: Print`; `Event ID: 10` и `13`).

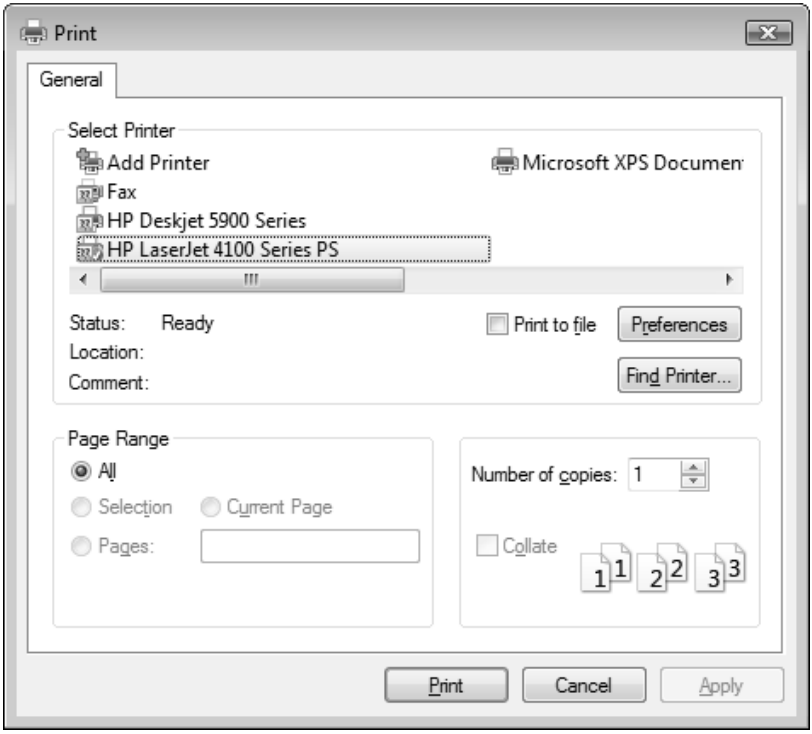


Рис. 9.3. Стандартное диалоговое окно печати

Новое устройство печати Microsoft XPS Document Writer. В системах Windows Vista и Windows Server 2008 появился стандартный принтер, который представляет собой драйвер вывода документов *в файлы* кроссплатформенного формата XPS (можно рассматривать как аналог Adobe PostScript). Эти файлы можно просматривать в браузере Internet Explorer 7.0 и печатать с помощью любой программы, поддерживающей этот формат, на самых разных компьютерных платформах.

Совместное использование факсов. Обеспечивается совместное использование не только принтеров, но и факсов: можно с любого компьютера сети отправить или получить факс, пользуясь факс-модемом, подключенным к другому компьютеру; факсы при этом рассматриваются как обычные принтеры.

Использование службы каталогов. Все общие принтеры, устанавливаемые на компьютерах в домене, могут быть представлены в виде объектов каталога Active Directory. *Публикация* (publishing) принтеров в Active Directory по-

зволяет быстро обнаружить наиболее удобные ресурсы для печати. Пользователь может проводить поиск по различным атрибутам (например, возможность цветной печати или быстродействие) или по расположению принтера (например, указать конкретный этаж в здании (location)). Как только нужный принтер найден, к нему можно сразу же подключиться и использовать, как и любой другой общий сетевой принтер.

Клиенты могут подключать принтеры, доступные в сети Windows, двумя способами: используя мастер установки принтеров или выполняя поиск в Active Directory (например, из стандартного окна **Print** (Печать) — см. рис. 9.3).

Установка принтеров с помощью групповых политик. Администраторы могут с помощью групповых политик (расширение Deployed Printers (Развернутые принтеры) — *см. главу 13*) управлять установкой на компьютеры драйверов печати.

Печать с использованием технологий Интернета. Службы печати тесно интегрированы со службами Интернета (Internet Information Services, IIS). Клиент может обращаться к сетевым принтерам через корпоративные интрасети или через Интернет. После того как принтер создан и разрешено его совместное использование, он появляется в HTML-папке принтеров.

- Печать с применением URL (Uniform Resource Locator)

  Пользователи клиентских компьютеров могут отправлять задания на серверы печати, используя формат URL: `http://<имяСервера>/<имяОбщегоПринтера>`. При этом возможна печать через брандмауэры Интернета.

- Просмотр состояния принтера

  Если на сервере печати установлены службы IIS, то автоматически генерируются HTML-страницы, отображающие состояние принтеров и очередей печати (рис. 9.4 и 9.5). Клиент может использовать любой браузер на любой платформе, чтобы приостановить, продолжить или удалить свои задания печати. Администраторы также при помощи браузера могут просматривать состояния принтеров и изменять статус заданий печати.

- Установка драйверов с веб-сервера (см. рис. 9.8)

  При отсутствии драйверов на локальном компьютере пользователь может подключиться к удаленному принтеру и загрузить драйверы с сервера печати. При этом используется имя принтера, указанное в окне его свойств при просмотре с помощью веб-браузера (см. рис. 9.5).

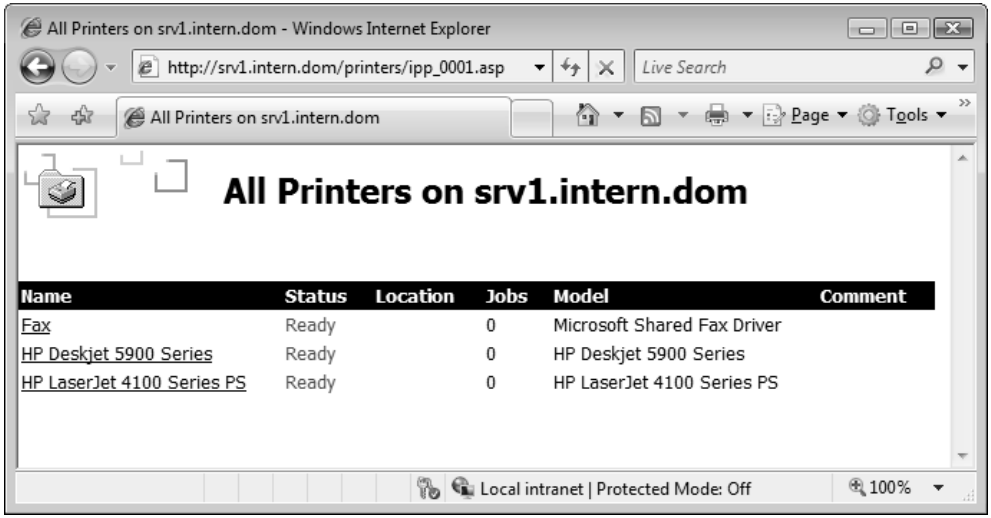


Рис. 9.4. Просмотр состояния устройств печати на сервере печати

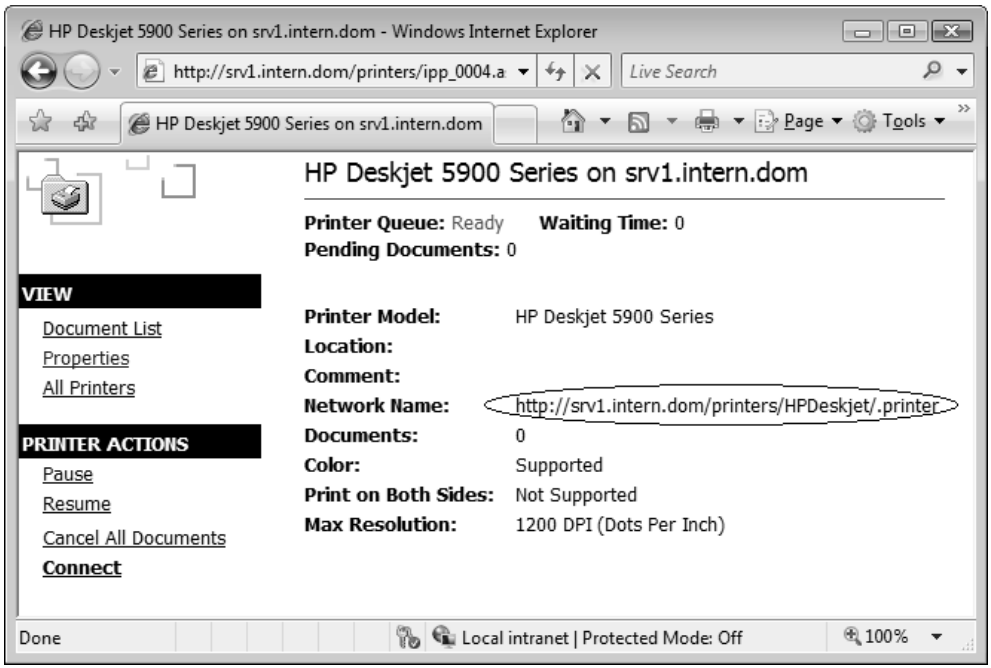


Рис. 9.5. Просмотр состояния принтера,
управление принтером и очередью печати с помощью веб-браузера

Стандартный монитор порта. Стандартный монитор порта (Standard TCP/IP Port) соединяет сервер печати и принтеры, имеющие сетевой адаптер и использующие протокол TCP/IP (см. рис. 9.7).

Средства централизованного администрирования. Администратор может с любого компьютера под управлением Windows Server 2008 дистанционно управлять серверами печати, портами, принтерами, документами и драйверами принтеров.

Администратору не нужно устанавливать драйверы принтеров на клиентских компьютерах, которым требуется доступ к серверу печати; все необходимые драйверы принтера можно установить только в одном месте — на сервере печати.

Для управления локальными или удаленными серверами и устройствами печати, а также очередями могут использоваться утилиты командной строки и административные сценарии.

Установка служб печати

Для того чтобы на компьютере под управлением Windows Server 2008 можно было в полной степени использовать возможности служб печати, необходимо с помощью оснастки **Server Manager** (Диспетчер сервера) добавить роль сервера *Print Services* (Службы печати) (рис. 9.6). (*Базовые* возможности использования общих принтеров доступны по умолчанию.)

После установки роли в меню **Administrative Tools** (Администрирование) появляется оснастка **Print Management** (Управление печатью) — главное средство управления серверами печати.

Работу служб печати обеспечивает системный сервис Print Spooler (Spooler).

Создание принтеров

Совместно используемые устройства печати могут быть подключены к параллельным или последовательным портам компьютера-сервера печати или непосредственно к сети, если они имеют встроенную плату сетевого адаптера.

При создании принтера требуется:

- выбрать порт принтера (если используется пул принтеров, выбрать несколько портов);

- указать изготовителя принтера и модель;
- задать имя принтера;
- определить имя общего ресурса принтера для доступа к нему сетевых пользователей.

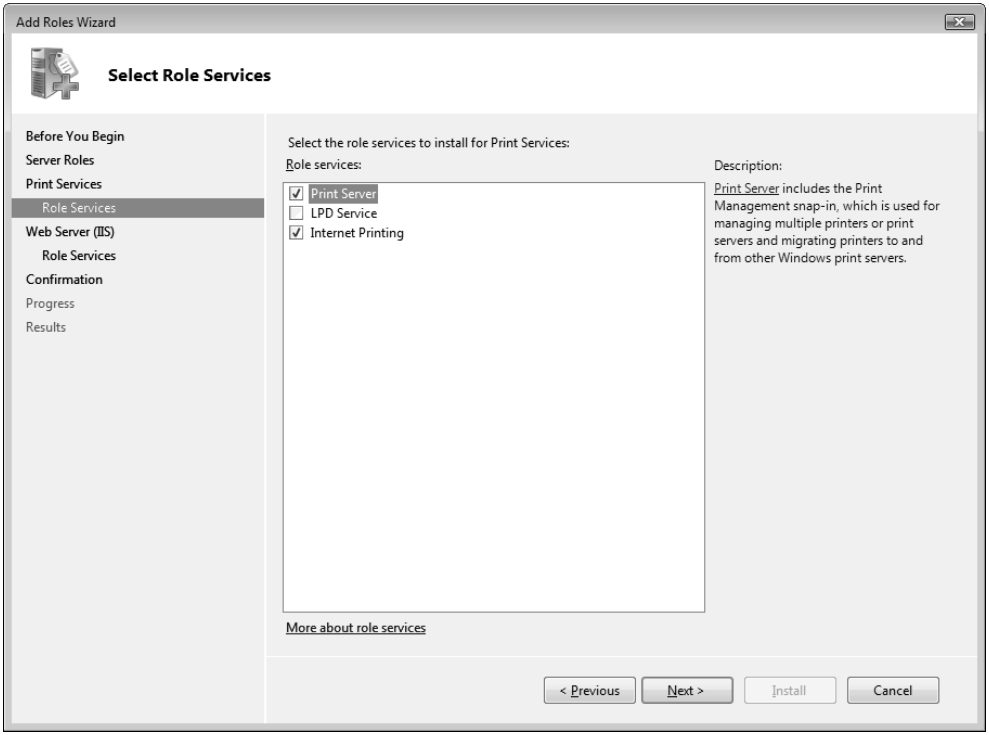


Рис. 9.6. Выбор компонентов служб печати

Внимание!

Чтобы создать принтер на сервере печати, нужно зарегистрироваться на нем в качестве члена групп Administrators (Администраторы).

В системах Windows Server 2008 мастер установки принтеров по умолчанию предлагает разрешить совместное использование принтера и в случае согласия автоматически публикует принтер в Active Directory, *если компьютер входит* в домен. В дальнейшем эти установки можно изменять в любой момент.

Если в будущем нужно совместно использовать принтер для клиентов, работающих на других платформах, нужно установить соответствующие (дополнительные) драйверы принтера для этих клиентов на сервере печати.

Установка локального или удаленного принтера

Установка локального принтера не вызывает проблем — если устройство печати соответствует стандарту Plug and Play, то система автоматически распознает новое устройство и установит нужный драйвер *(см. главу 1)*. После этого необходимо лишь проверить выбранное для принтера имя и разрешить общий доступ к нему, если это требуется. После того как драйвер принтера будет установлен, проверьте его работу, распечатав пробную страницу.

При установке принтера, найденного в каталоге Active Directory или подключенного к компьютеру, выбранному в сети с помощью программы Windows Explorer (Проводник), достаточно просто выполнить команду подключения. При необходимости с удаленного сервера печати будут установлены нужные драйверы.

Для того чтобы самому инициировать создание принтера, нужно запустить мастер *Add Printer Wizard* (Мастер установки принтеров) и указать имя удаленного принтера и некоторые дополнительные параметры. Это довольно простая процедура. Мастер установки можно вызвать из папки **Printers** (Принтеры) (см. рис. 9.1 — команда **Add a printer** (Установить принтер)).

Процедура локальной установки устройства печати, имеющего сетевой интерфейс (т. е. сетевого принтера), будет несколько отличаться. Такое устройство печати также рассматривается как локальное, и к нему также можно разрешать общий доступ. Это объясняется тем, что спулер сетевого принтера все равно работает на локальном компьютере-сервере печати.

При выборе способа установки сетевого принтера нужно указать опцию принтера TCP/IP (рис. 9.7), а затем ввести IP-адрес этого принтера (имя порта формируется автоматически; менять его нежелательно). Желательно, чтобы принтер был включен и доступен — мастер свяжется с ним и проверит наличие драйверов. Для сетевых принтеров обычно используется порт Standard TCP/IP Port. При необходимости (если устройство печати выключено) можно вручную указать тип порта и модель устройства.

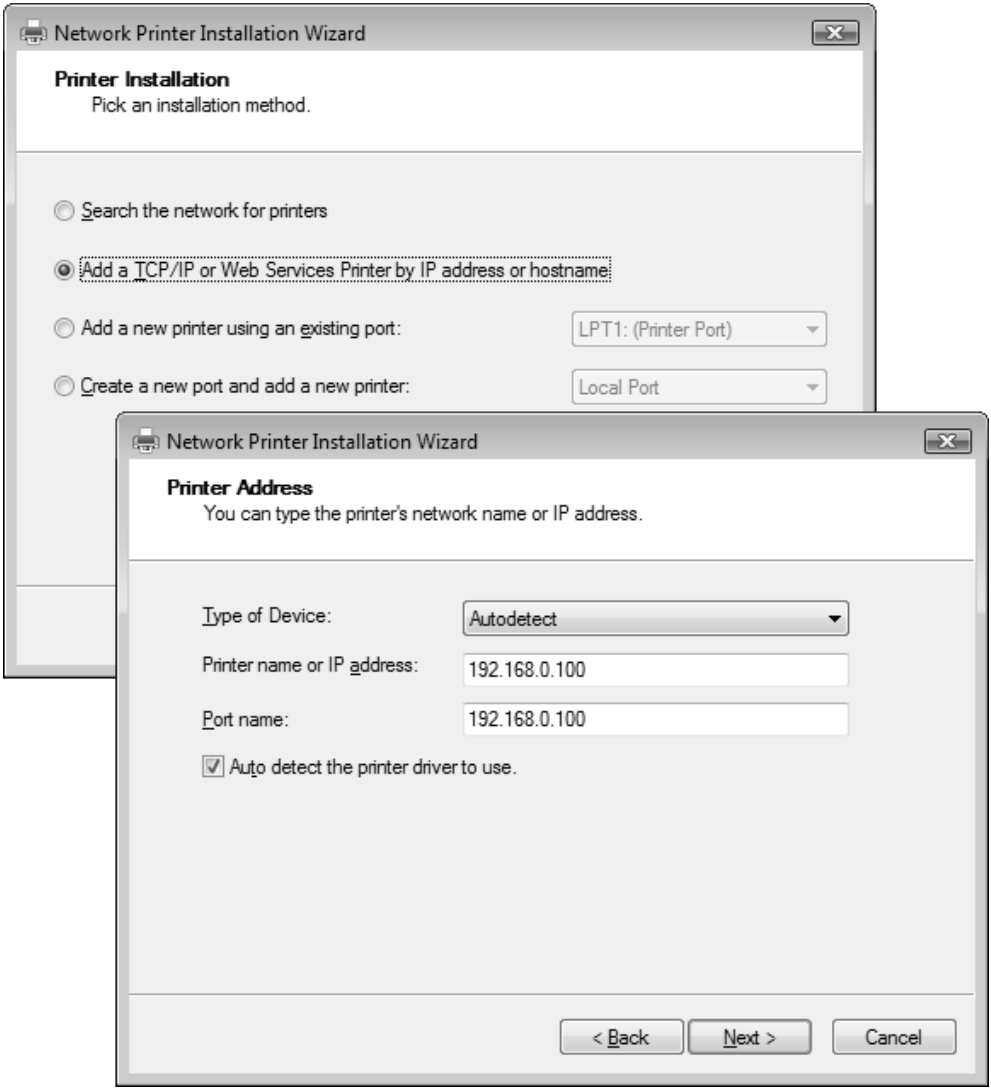


Рис. 9.7. Создание нового порта принтера TCP/IP

Печать через Интернет

Доступ к сетевым принтерам можно получать через корпоративные интрасети и через Интернет. Печать через Интернет работает так же, как и традиционная сетевая печать. Документы для печати можно отправлять непосредст-

венно на URL сетевого принтера и устанавливать драйверы принтеров из URL. Более того, сервер печати можно посетить точно так же, как и веб-узел, используя адрес типа http://<*имяСервера*>/<*имяПринтера*> или http://<*имяСервера*>/printers (см. рис. 9.4).

Для администраторов HTTP-принтер выглядит так же, как и любой другой общедоступный принтер. Дополнительные возможности печати обеспечивает служба роли *Internet Printing* (Печать через Интернет) (см. рис. 9.6), для поддержки которой автоматически устанавливаются отдельные компоненты служб Internet Information Services (IIS 7.0). У клиентов должен быть установлен компонент *Internet Printing Client* (Клиент печати через Интернет), который также использует некоторые средства служб IIS.

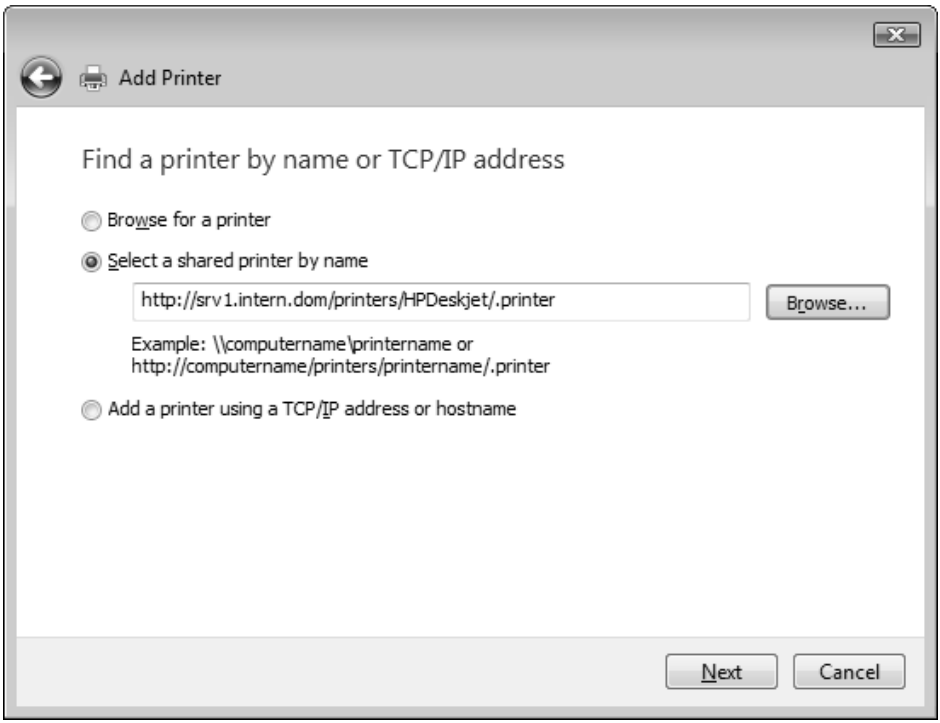


Рис. 9.8. Подключение принтера для печати через Интернет

При подключении принтера, используемого через Интернет, клиент указывает имя принтера, которое отображается на веб-странице, содержащей свойства принтера (см. рис. 9.5). Это имя вводится как имя общего принтера

(рис. 9.8), а все дальнейшие шаги по подключению принтера ничем не обличаются от стандартной процедуры создания принтера. При необходимости драйверы принтера будут загружены через Интернет и установлены на компьютере клиента. Установленный интернет-принтер появится в стандартной папке **Printers** (Принтеры) (при этом будет указано его сетевое имя).

Настройка принтера

В окне свойств принтера (рис. 9.9) можно просматривать и устанавливать следующие параметры принтера:

- общие параметры (драйвер принтера и установки страницы-разделителя); предпочтения печати для данного принтера; печать тестовой страницы;

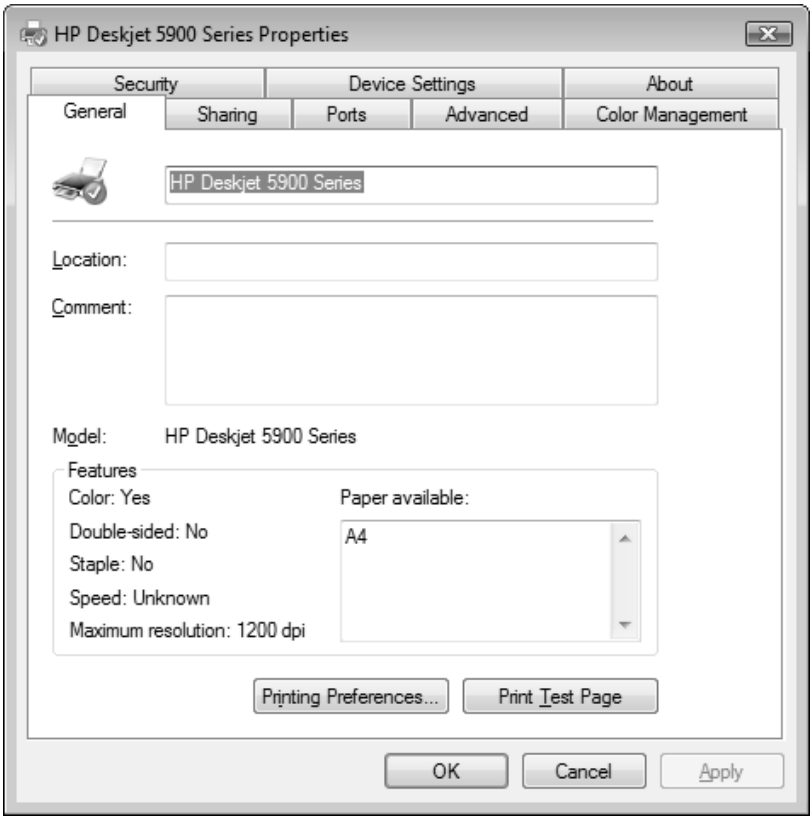


Рис. 9.9. Диалоговое окно свойств принтера

- имя общего ресурса принтера, публикация в каталоге Active Directory; установка дополнительных драйверов для других платформ (x64, Itanium);
- порт и параметры порта;
- параметры управления очередью печати; страницы-разделители;
- управление цветом для устройств цветной печати;
- параметры безопасности (разрешения);
- специфические параметры, зависящие от устройства.

Совместное использование и публикация принтеров

На вкладке **Sharing** (Доступ) окна свойств принтера (рис. 9.10) можно разрешить общий доступ к принтеру. Для этого установите флажок **Share this printer** (Общий доступ к данному принтеру), а затем введите имя общего ресурса (принтера) в поле ввода.

Хотя можно создавать принтеры с длинными именами, содержащими пробелы и специальные символы, некоторые клиенты не распознают такие имена или обрабатывают их неправильно. Если в сети есть клиенты с различными операционными системами, желательно, чтобы длина общего имени принтера не превышала 12 символов, которые не содержат пробелов или специальных символов.

По умолчанию установлен флажок **Render print jobs on client computers**, указывающий на то, что задания печати должны обрабатываться на компьютерах клиентов печати. Это позволяет снизить нагрузку на сервер печати в случае больших заданий, заданий со сложной графикой или изображений с высоким разрешением.

На вкладке **Sharing** (Доступ) можно управлять публикацией принтера в каталоге Active Directory (флажок **List in the directory** (Внести в Active Directory)). Устанавливаемое по умолчанию имя в каталоге — `\\<имяСервера>\<имяОбщегоПринтера>`.

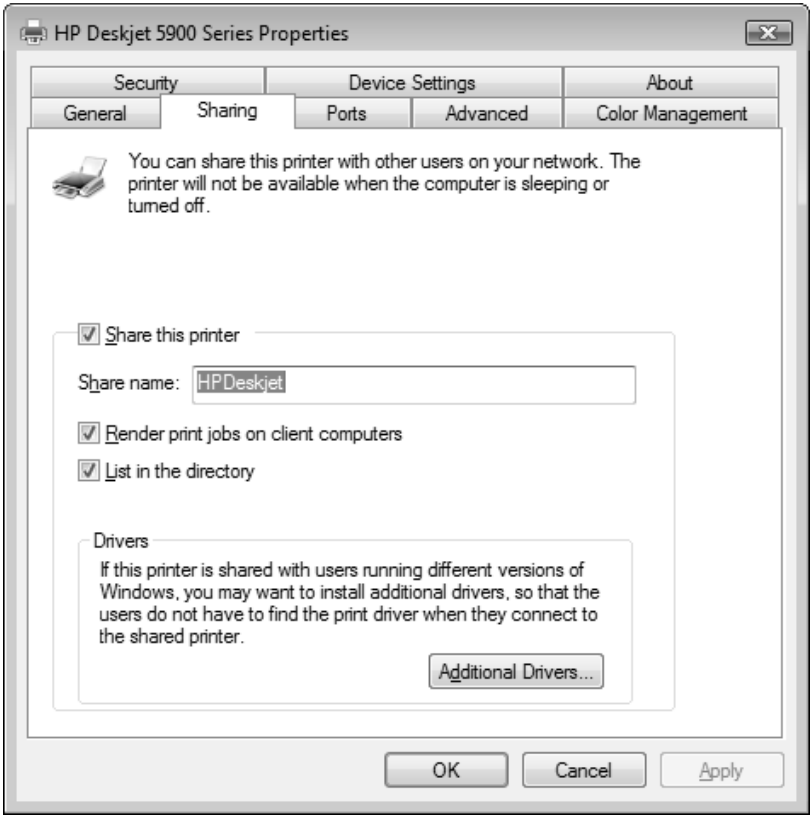


Рис. 9.10. Управление доступом и драйверами

Настройка параметров сервера печати

Сервер печати (служба спулера) обслуживает все подключенные принтеры. Он имеет свои параметры, общие для всех принтеров.

Чтобы просмотреть и установить параметры сервера печати, нужно в папке **Printers** (Принтеры) (см. рис. 9.1) нажать кнопку **Server properties** (Свойства сервера). Если вызвать классическое меню (нажав клавишу <Alt>), то команду **Server Properties** (Свойства сервера) можно также выбрать из меню **File** (Файл). В окне свойств сервера можно выполнять следующие задачи:

- создавать пользовательские формы, доступные для всех принтеров на сервере;

- изменять установки портов для всех портов на сервере (рис. 9.11) (это иногда требуется при работе с сетевыми устройствами печати);
- устанавливать драйверы принтера для различных платформ;
- выбирать расположение файла спулинга, устанавливать регистрацию ошибок диспетчера очереди печати и задавать опции уведомления для всех принтеров на сервере.

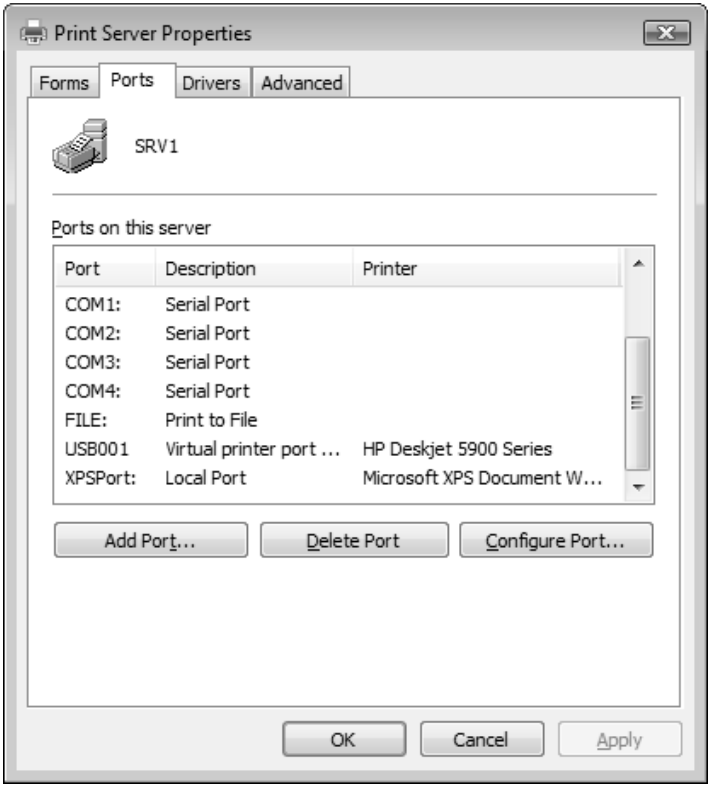


Рис. 9.11. Вкладка окна свойств сервера печати, позволяющая настраивать порты печати

Установка драйверов принтера для различных платформ

Различные аппаратные платформы и операционные системы требуют своих драйверов принтера (рис. 9.12). (Обратите внимание на наличие специально-

го драйвера для служб терминалов — *Terminal Services Easy Print*.) Например, чтобы использовать принтер, подключенный к серверу печати, клиенту, который работает под управлением 64-разрядной версии Windows, требуется соответствующий драйвер принтера. Этот драйвер может быть установлен локально или на компьютере-сервере печати (предпочтительный вариант). Сервер печати сам определяет, с каких компьютеров выполняется обращение и автоматически посылает соответствующий драйвер клиенту.

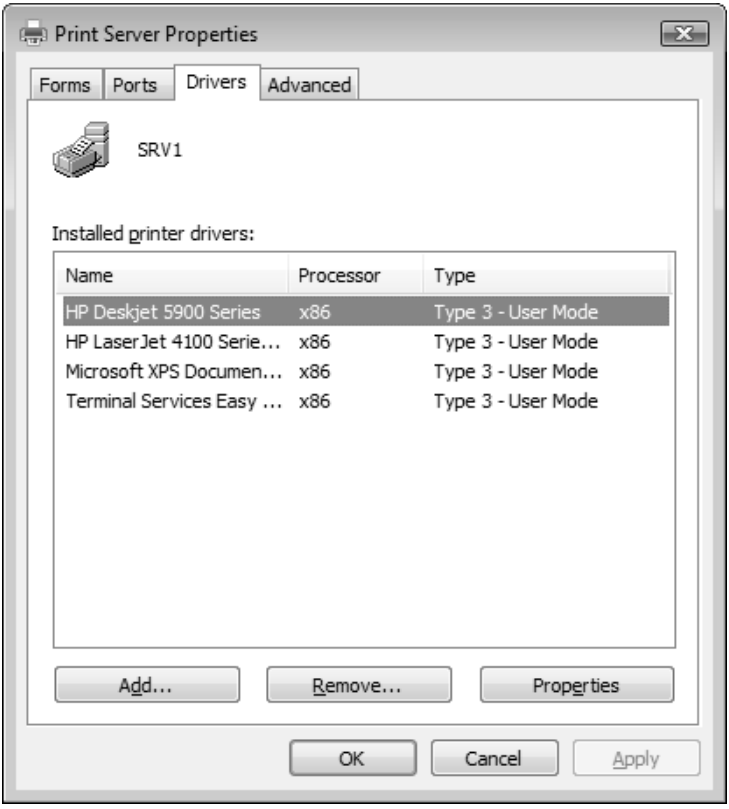


Рис. 9.12. Настройка драйверов принтера для различных платформ

Установку драйверов принтера для других платформ можно также инициировать из окна свойств принтера с вкладки **Sharing** (Доступ), кнопка **Additional Drivers** (Дополнительные драйверы) (см. рис. 9.10).

Установка дополнительных параметров сервера

На вкладке **Advanced** (Дополнительные параметры) в окне свойств сервера печати (рис. 9.13) можно определять следующие параметры:

- указывать местоположение папки очереди печати (каталога спулинга);
- разрешать регистрацию событий очереди печати;
- конфигурировать сервер печати так, чтобы он подавал звуковой сигнал в случае ошибок при посылке документов на печать;
- конфигурировать сервер печати так, чтобы он сообщал клиенту о выполнении заданий печати.

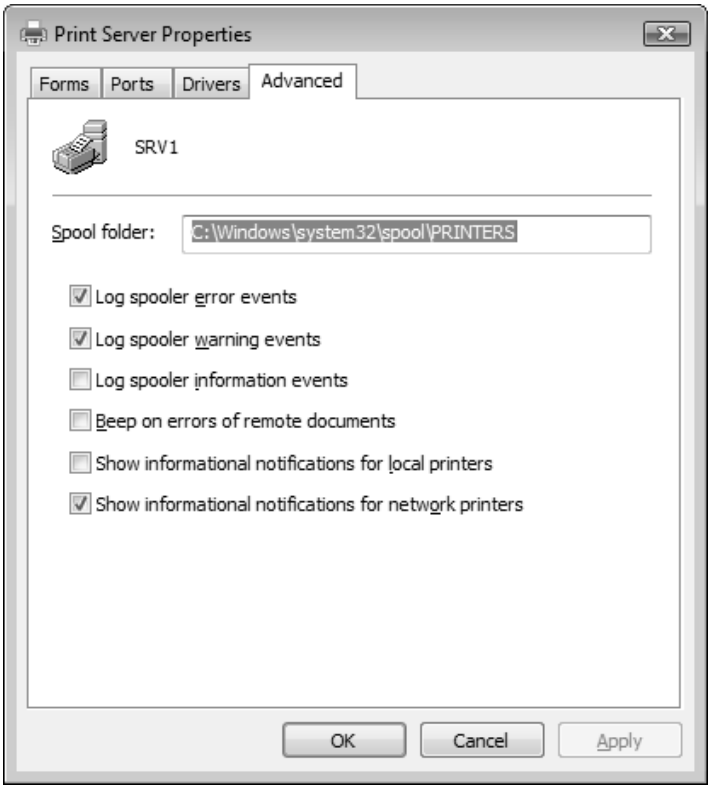


Рис. 9.13. Дополнительные настройки сервера печати

Управление серверами печати

Для централизованного управления серверами печати и подключенными к ним принтерами используется оснастка **Print Management** (Управление печатью; printmanagement.msc) (рис. 9.14). Она позволяет подключаться к разным серверам печати и просматривать состояние имеющихся принтеров и установленных драйверов, а также количество заданий. Для выбранного принтера можно видеть очередь печати и управлять ею (все команды для принтера показаны на рисунке в раскрывающемся меню).

Оснастка **Print Management** (Управление печатью) позволяет также просматривать список принтеров, устанавливаемых в домене Active Directory с помощью групповых политик (папка **Deployed Printers** (Развернутые принтеры)), и управлять этой операцией.

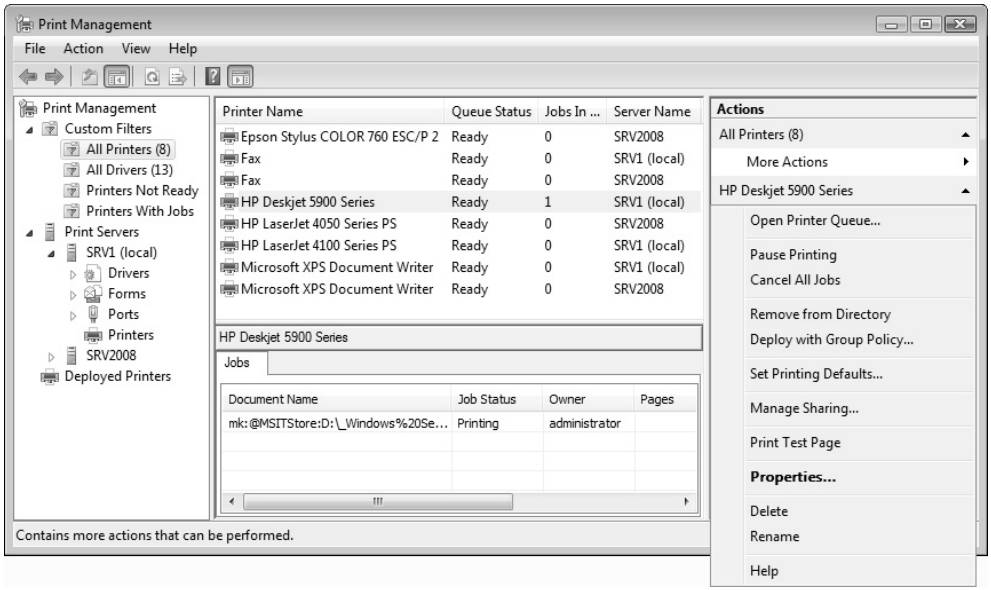


Рис. 9.14. Окно оснастки **Print Management**

Служба факс-сервера

Факс-сервер (Fax Server) позволяет организовать отправку и получение факсимильных сообщений для всех клиентов локальной сети; при этом будут

использоваться одно или несколько устройств, подключенных к одному компьютеру.

Факсы рассматриваются как принтеры, и получить информацию об установленных факсах и их состоянии можно в папке **Printers** (Принтеры) (см. рис. 9.1). При этом факсы могут выступать в качестве *устройств общего доступа* (shared devices). Вывод документов на факс осуществляется так же, как и обычная печать. Чтобы послать по факсу документ, достаточно выбрать в меню приложения, в котором данный документ открыт, команду **Print** (Печать) и указать принтер факса. При передаче понадобится добавить только информацию о получателе и замечания в мастере *Send Fax Wizard* (Мастер отправки факсов), после чего факс будет отправлен. В системах Windows Vista и Windows Server 2008 для работы с факсами имеется дополнительное средство — программа *Windows Fax and Scan* (Факсы и сканирование Windows).

Для передачи факсов используется многостраничный формат изображений TIFF (Tagged Image File Format). Можно сканировать отпечатанные документы и полученные изображения отправлять по факсу. Не требуется преобразовывать существующую графику в формат TIFF перед передачей факса — факс-сервер сделает это автоматически.

Возможности факс-сервера и программы Windows Fax and Scan

Возможности программы Windows Fax and Scan (Факсы и сканирование Windows), обеспечивающей пользовательский интерфейс для работы с факсами, и средства факс-сервера нужно рассматривать как единое целое. Перечислим основные возможности этих средств.

- **Передача сообщения на титульном листе.** Сообщения можно отправлять на титульном листе факса отдельно от текстового документа. С помощью программы *Fax Cover Page Editor* (Редактор титульных страниц факсов) пользователь может создать любой титульный лист в соответствии со своими задачами либо выбрать один из имеющихся шаблонов титульных листов. Мастер отправки факсов автоматически вносит информацию о получателе и отправителе, нужно только ввести примечание и отослать факсимильное сообщение.
- **Контроль процесса передачи факсов.** Пользователь может контролировать процесс передачи факсов (в том числе отслеживать ошибки) при по-

мощи специального средства *Fax Status Monitor* (Монитор состояния факса), которое вызывается из меню **Tools** (Сервис) программы Windows Fax and Scan (Факсы и сканирование Windows).

- **Прием факсимильных сообщений.** Службу можно настроить для автоматического приема факсов, их сохранения на диске и печати на указанном принтере или автоматической передачи получателю по электронной почте.

Установка факс-сервера

Чтобы установить факс-сервер (служба и сервис Fax), нужно с помощью оснастки **Server Manager** (Диспетчер сервера) добавить роль сервера *Fax Server* (Факс-сервер). При этом также требуется установка компонентов сервера печати.

При установке роли необходимо указать пользователей или группы безопасности, которые смогут отправлять и получать факсы на этом сервере. По умолчанию такое право всегда имеет локальная группа Administrators (Администраторы).

Затем требуется назначить *помощников маршрутизации почты* (routing assistants) — ответственных за перенаправление полученных факсов в заданные входные папки получателей документов. (По умолчанию такие полномочия имеют только локальные администраторы.) Если такие помощники назначаются (опция по умолчанию — рис. 9.15), то на следующем шаге нужно будет указать соответствующие учетные записи пользователей или групп. Можно выбрать альтернативную опцию, и тогда доступ к папке "Входящие" будут иметь все пользователи.

После установки роли в папке **Administrative Tools** (Администрирование) появляется оснастка **Fax Service Manager** (Диспетчер службы факсов), позволяющая управлять работой факс-сервера.

Для непосредственного создания и просмотра факсов используется "клиентская" программа Windows Fax and Scan (Факсы и сканирование Windows), которая появляется в системе Windows Server 2008 после установки компонента *Desktop Experience* (Возможности рабочего стола) *(см. главу 3)*. (Эта программа имеется и в Windows Vista.)

Примечание

После установки факс-сервера на компьютере появляется общая папка faxclient, по умолчанию она связана с подкаталогом

%SystemRoot%\system32\clients\faxclient. В этой папке находятся установочные файлы для пользователей тех операционных систем, где клиент службы факсов отсутствует. Установка выполняется с применением стандартных средств инсталляции программ, имеющихся на панели управления; после этого запускается мастер установки принтеров для подключения к удаленному факс-серверу.

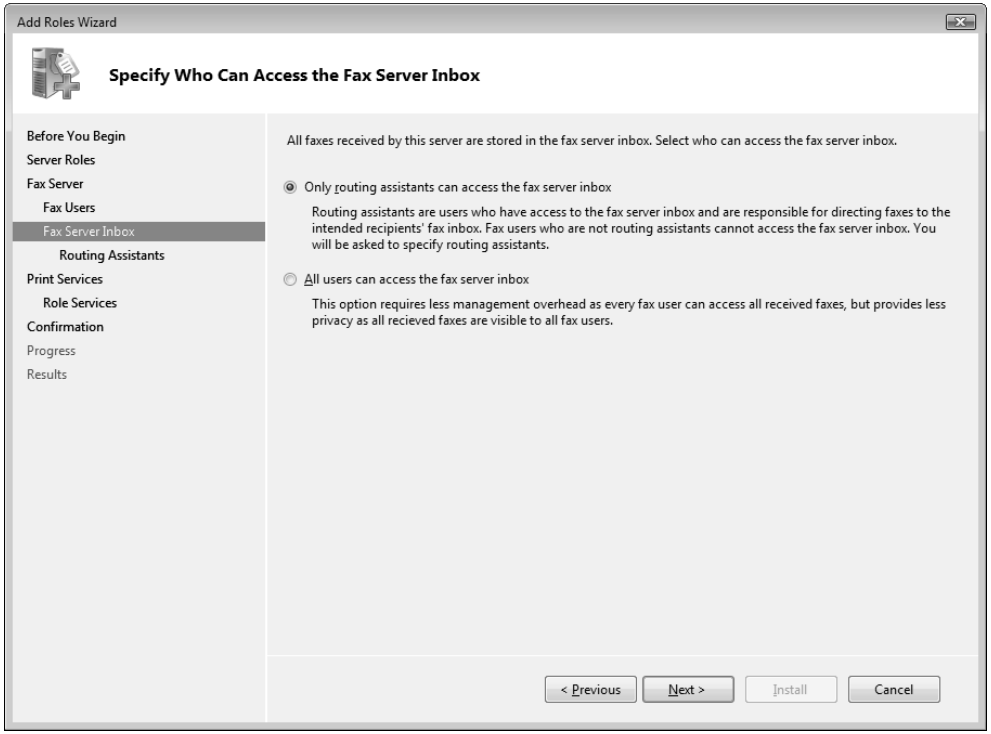


Рис. 9.15. Выбор помощников маршрутизации почты

Редактор титульных страниц факсов

Редактор титульных страниц факсов (Fax Cover Page Editor) (рис. 9.16) позволяет осуществлять редактирование шаблонов титульных листов, которые используются в процессе передачи факсов. Можно создавать общие титульные страницы, чтобы совместно использовать их из нескольких профилей. По умолчанию служба факсов включает четыре шаблона таких страниц (см. рис. 9.17). При передаче факса шаблон получает информацию, предоставленную пользователем в окне **Sender Information** (Сведения об отправителе),

вызываемом из меню **Tools** (Сервис) программы Windows Fax and Scan (Факсы и сканирование Windows), и автоматически добавляет ее к передаваемой титульной странице.

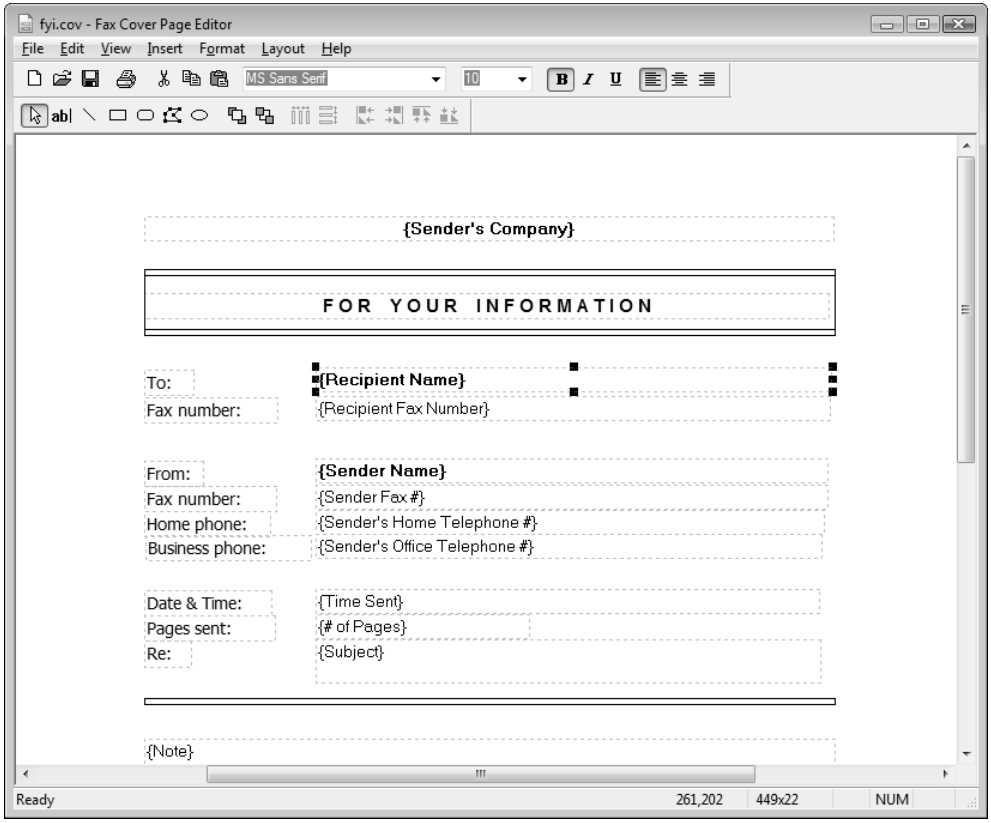


Рис. 9.16. Редактор титульных страниц позволяет быстро создать фирменные бланки на основе имеющихся шаблонов

Имеются стандартные титульные страницы (файлы с расширением cov). Их список можно видеть в окне оснастки **Fax Service Manager** (Диспетчер службы факсов) (папка **Cover Pages** (Титульные страницы)). Пользователь программы Windows Fax and Scan (Факсы и сканирование Windows) может в меню **Tools** (Сервис) выбрать команду **Cover Pages** (Титульные страницы) и получить доступ к личным титульным страницам (рис. 9.17). Здесь можно создавать новые страницы или выбирать для редактирования существующие.

Нажав кнопку **Copy** (Копировать), пользователь может открыть окно общих (стандартных) титульных страниц и скопировать в свою папку для дальнейшего использования или редактирования (оригиналы при этом не изменяются). Все личные титульные страницы хранятся в папке **Fax | Personal Coverpages**, появляющейся в папке **Documents** (Документы) после установки программы.

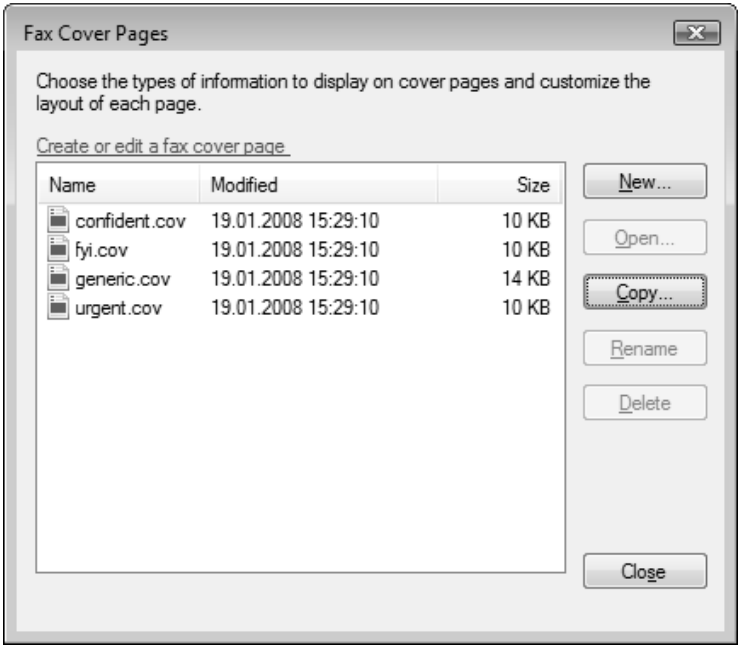


Рис. 9.17. Перечень персональных титульных страниц

Программа Windows Fax and Scan (Факсы и сканирование Windows)

В составе систем Windows Vista и Windows Server 2008 имеется новая программа *Windows Fax and Scan* (Факсы и сканирование Windows; WFS.exe), объединяющая в себе средства сканирования, а также подготовки, отправки и приема факсов. Также из этой программы можно вызывать Fax Status Monitor (Монитор состояния факса).

Программа Windows Fax and Scan (Факсы и сканирование Windows) (рис. 9.18) имеет два достаточно независимых режима работы, ориентированных на факсы и на сканированные изображения (для переключения режимов служат кнопки в левом нижнем углу окна программы). Любой выбранный в окне программы файл можно распечатать, сохранить в локальной папке, отправить как факс или как сообщение электронной почты (в виде прикрепленного файла).

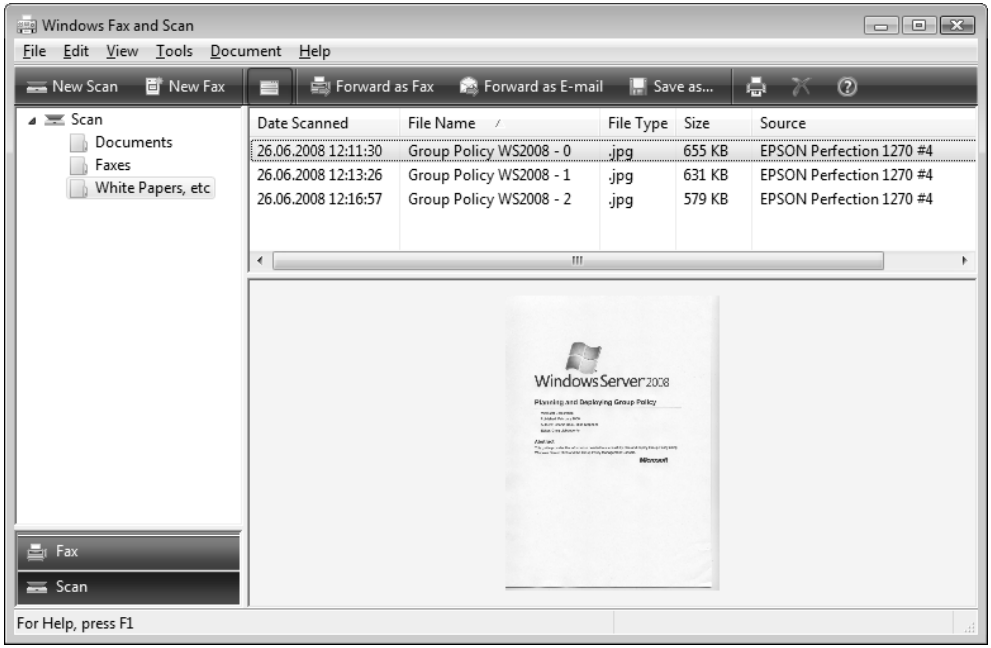


Рис. 9.18. Универсальная программа для работы с факсами и сканером

Подготовка к работе

Программу Windows Fax and Scan (Факсы и сканирование Windows) сначала следует подготовить к работе и создать учетную запись для работы с факс-сервером. (Эта операция инициируется автоматически при первой отправке факса.)

Необходимо в меню **Tools** (Сервис) выбрать команду **Fax Accounts** (Учетные записи факса) и в открывшемся окне нажать кнопку **Add** (Добавить). Далее следует указать, как будут передаваться факсы — с помощью локального

факс-сервера или через сервер факсов, установленный на другом компьютере (рис. 9.19).

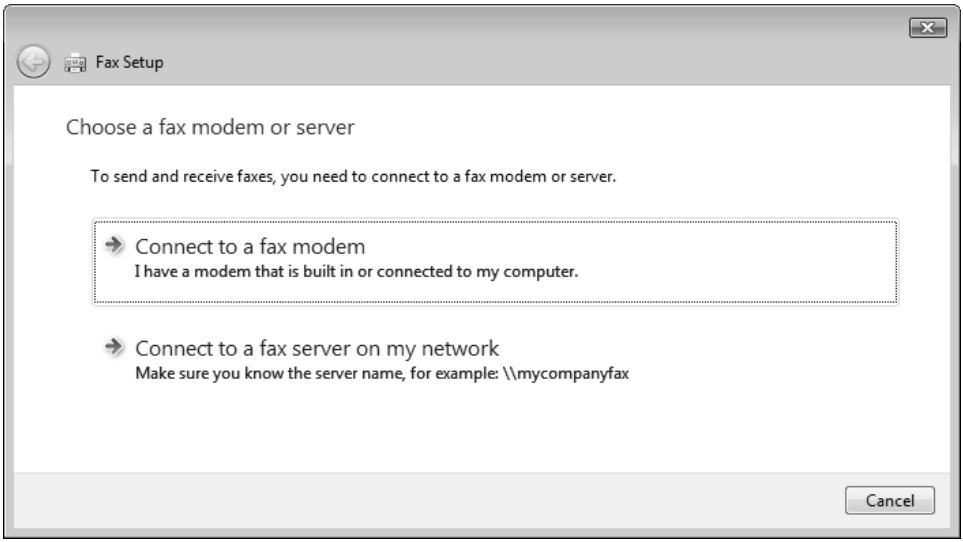


Рис. 9.19. Конфигурирование программы при первом запуске создания факса

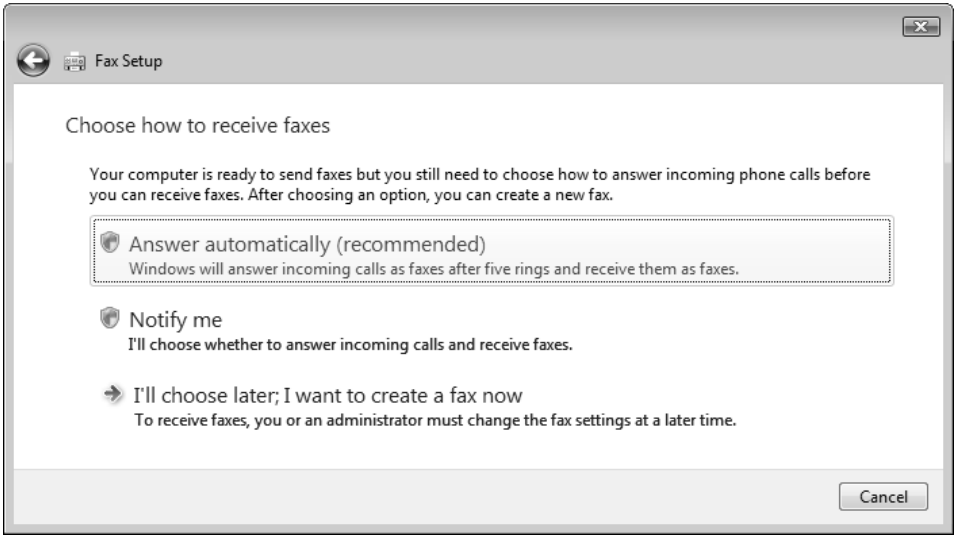


Рис. 9.20. Выбор способа ответа при приеме факсов

Затем следует ввести произвольное понятное имя модема, выбранного для передачи факсов, — это имя будет использоваться как имя учетной записи, которая будет по умолчанию выбираться для отправки факсов. Учетные записи можно удалять, менять и создавать заново.

Затем нужно выбрать способ получения факсов (рис. 9.20); при этом можно вообще отказаться от выбора (последняя опция). После этого учетная запись будет создана, и программа будет готова к отправке факсов через указанный факс-сервер.

После настройки программы факсов можно в любой прикладной программе использовать факс как устройство печати: при отправке документа на факс автоматически формируется графическое изображение, которое вставляется в новый факс. После этого в окне редактора факсов необходимо только указать получателя и тему.

Сканирование изображений

Для запуска сканера достаточно нажать кнопку **New Scan** (Новое сканирование) на панели задач в окне программы. В окне настройки (рис. 9.21) осуществляется выбор параметров сканирования и предварительный просмотр изображения. Непосредственно в этом окне можно отрегулировать яркость и контрастность изображения. Для быстрой смены групп параметров служат наборы заранее определенных параметров, выбираемые в списке **Profile** (Профиль). Профиль определяет цветовой формат (цвет, полутоновой серый или черно-белый), тип сохраняемого файла и разрешение сканера.

После выбора профиля или собственных параметров нужно нажать кнопку **Preview** (Просмотр), получить изображение и определить рамки сканирования. При нажатии кнопки **Scan** (Сканировать) операция начинает выполняться, после чего созданный файл копируется в пользовательскую папку, а имя нового документа появляется в окне программы в списке сканированных документов. Здесь документу можно дать другое имя, отправить как факс или в качестве вложения в сообщение электронной почты, сохранить под другим именем или в другом формате и распечатать.

Изображения, полученные с помощью программы Windows Fax and Scan (Факсы и сканирование Windows), не попадают автоматически в программу просмотра изображений *Windows Photo Gallery* (Фотоальбом Windows), поскольку папка сканированных документов по умолчанию не просматривается фотоальбомом. Однако если сканирование запустить из программы Windows Photo Gallery (Фотоальбом Windows) при помощи команды **File** | **Import**

from Camera or Scanner (Файл | Импортировать с камеры или сканера), то полученное изображение будет импортироваться непосредственно в фотоальбом, и при этом ему можно задать ключевые слова.

Для группировки изображений можно использовать собственные папки (см. рис. 9.18), которые физически будут размещаться в профиле пользователя в папке **Documents** (Документы) (специальный подкаталог **Scanned Documents** (Отсканированные документы)).

Примечание

Изображения можно также сканировать с помощью программы Paint. В этом случае также запускается мастер работы со сканером. В окне программы полученное изображение можно отредактировать, а потом сохранить в файле нужного формата (BMP, JPEG, TIFF или PNG).

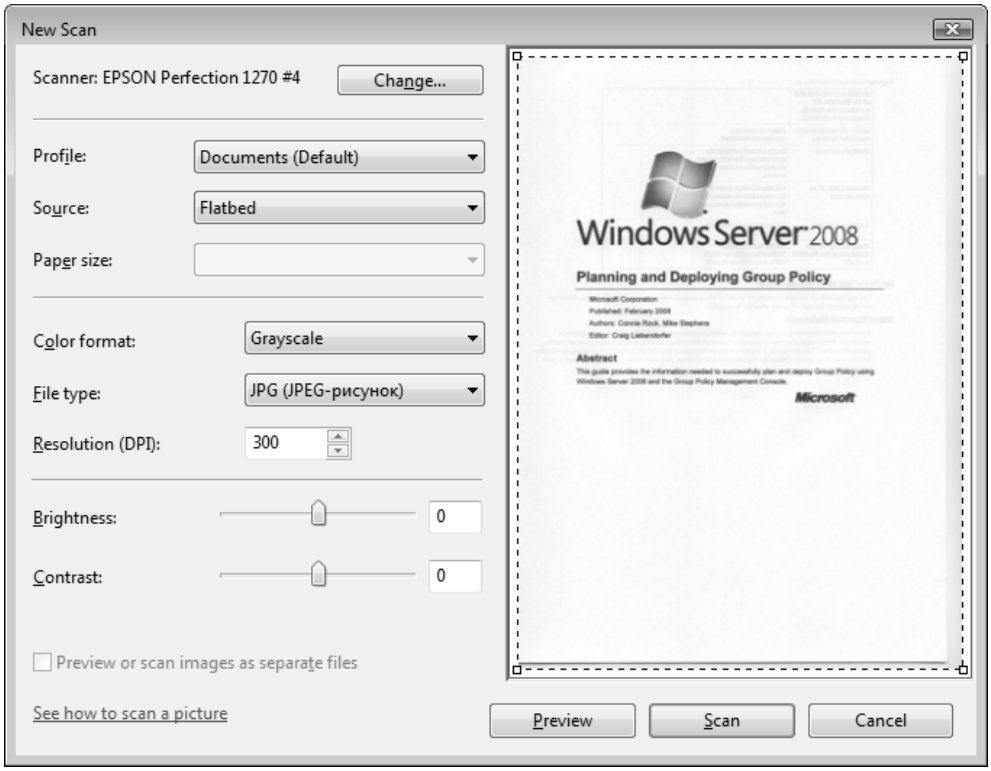


Рис. 9.21. Настройка режима сканирования и предварительный просмотр изображения

Использование стандартного мастера для работы со сканером удобно тем, что не нужны никакие специальные программы, можно обойтись минимумом операций, и эти операции будут одинаковыми для сканеров любых моделей.

Создание факса

Перед созданием факсов можно (хотя и не строго обязательно) выполнить команду **Sender Information** (Сведения об отправителе) в меню **Tools** (Сервис) и ввести нужную информацию (имя, номер своего факса, адрес электронной почты и т. п.). Затем с помощью команды **Cover Pages** (Титульные страницы) в том же меню можно перейти в окно, где перечислены личные титульные страницы, в которые затем будет (при необходимости) заноситься содержимое отправляемых факсов.

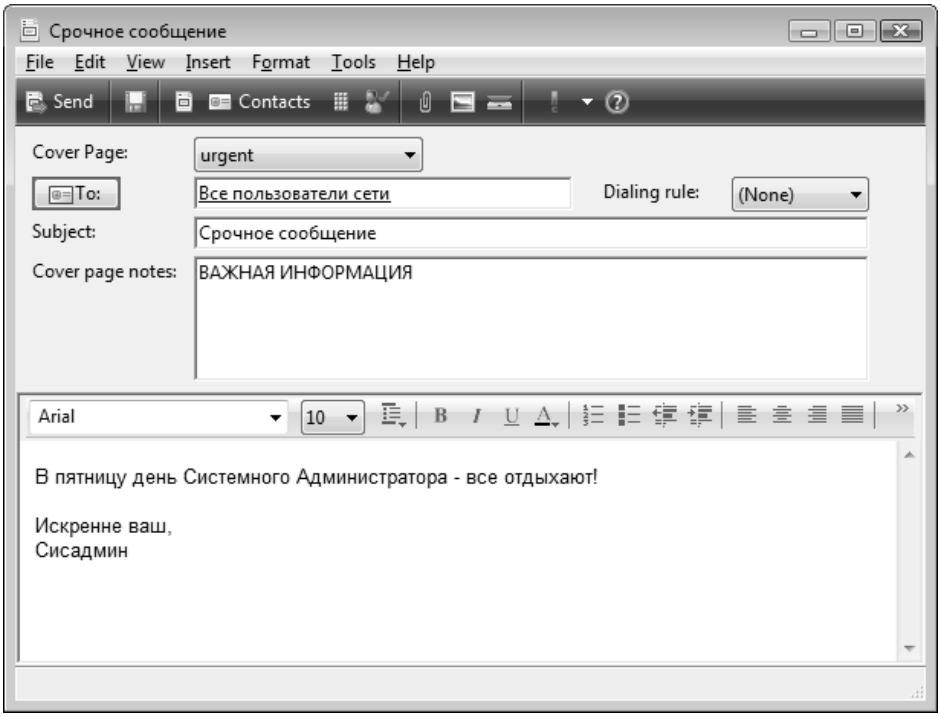


Рис. 9.22. Окно редактора создаваемых факсов

Теперь можно нажать кнопку **New Fax** (Создать факс) на панели инструментов. В окне редактора факсов (рис. 9.22; в заголовке его окна автоматически

отображается выбранная тема факса) можно выбрать титульную страницу и ввести нужную информацию (при этом доступны стандартные средства форматирования текста). В поле **To** (Кому) обязательно указывается получатель факса из списка контактов (его телефон будет автоматически использоваться при отправке факса; при отсутствии телефона факса дальнейшие операции будут невозможны).

Когда факс готов, следует нажать кнопку **Send** (Отправка). Отправленные факсы помещаются в очередь и обрабатываются в соответствии с заданными параметрами пересылки. За прохождением факсов можно следить в окне *монитора состояния факса* (Fax Status Monitor) (рис. 9.23), которое в любой момент открывается с помощью соответствующей команды из меню **Tools** (Сервис). Здесь отслеживается выполнение всех операций по передаче факсов и возникающие ошибки — все события регистрируются в списке сообщений.

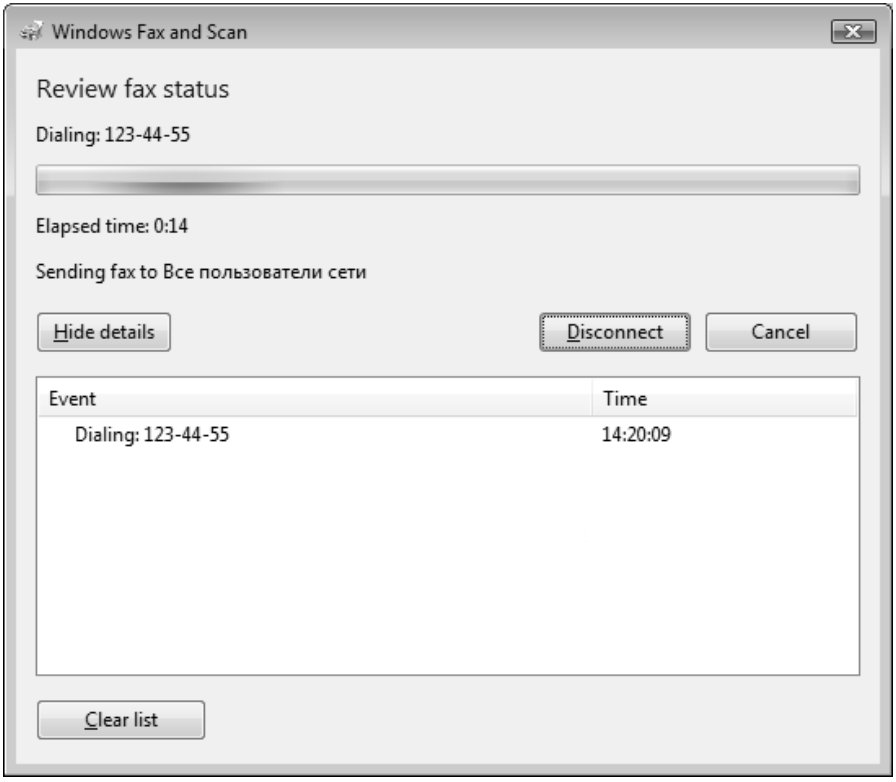


Рис. 9.23. Окно монитора позволяет следить за ходом операций по отправке и приему факсов

Все факсы группируются в окне программы по папкам, где их можно просматривать и выбирать для печати. Отправляемые факсы помещаются в папку **Outbox** (Исходящие). Любой факс можно переслать как вложение в сообщение электронной почты (см. кнопку на панели инструментов). Для ручного приема факсов служит кнопка **Receive a Fax Now** (Принять факс сейчас).

Диспетчер службы факсов

Для общего управления факс-сервером используется оснастка **Fax Service Manager** (Диспетчер службы факсов; fxsadmin.msc) (рис. 9.24).

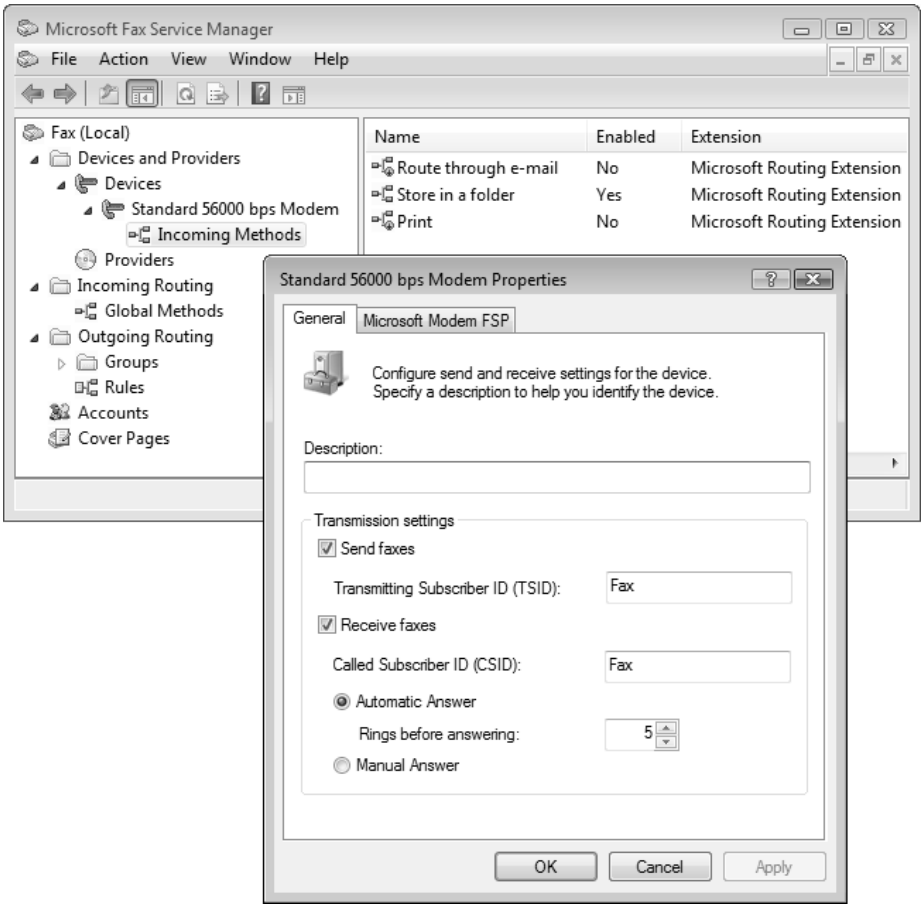


Рис. 9.24. Оснастка **Fax Service Manager**

Она предназначена для централизованного управления серверами, на которых установлены службы факсов. (По умолчанию она используется только для локального факс-сервера; при добавлении к консоли MMC ее можно подключить к удаленному компьютеру.) Ниже перечислены задачи, решаемые с помощью команд в окне этой оснастки:

- управление сервисом факса (запуск и остановка);
- конфигурирование факс-модемов на передачу и прием факсов;
- управление входящими и исходящими правилами (Incoming Methods), а также маршрутизацией факсов (Outgoing Routing);
- управление учетными записями администраторов факс-сервера;
- просмотр и редактирование общих титульных страниц.

Общие параметры работы факс-сервера определяются в окне свойств (рис. 9.25) (чтобы его открыть, нужно в окне оснастки выбрать корневой узел в дереве объектов и в контекстном меню выполнить команду **Properties** (Свойства)). Здесь можно следить за состоянием очередей факсов, включать протоколирование всех событий, задавать местоположение папки для хранения полученных и исходящих факсов, назначать разрешения доступа к факс-серверу и т. д.

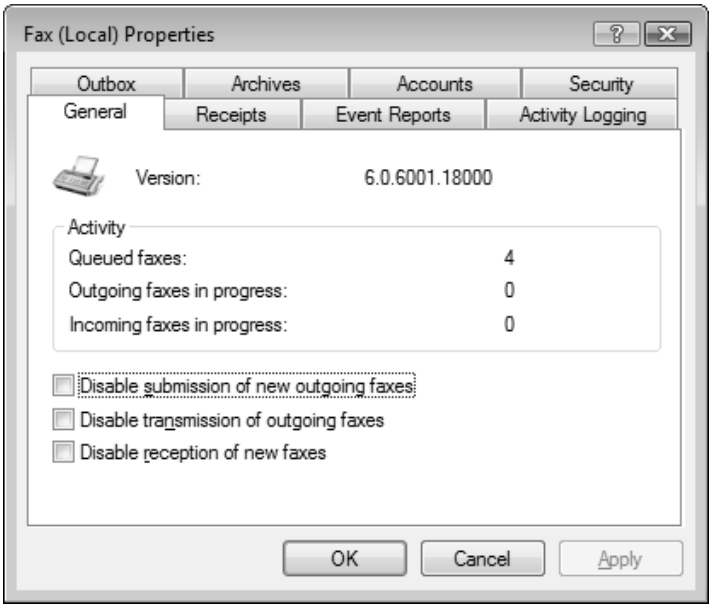


Рис. 9.25. Окно свойств факс-сервера

Глава 10

Службы терминалов

Эта глава посвящена службам *Terminal Services* (Службы терминалов), которые, возможно, являются одним из самых интересных и обновленных компонентов систем Windows Server 2008. Возможности сервера терминалов очень широки, как многочисленны и параметры, необходимые для настройки различных вариантов использования служб TS. Поэтому мы ограничимся демонстрацией самых интересных режимов, а также рассмотрим способы развертывания и средства администрирования служб терминалов.

Службы терминалов (Terminal Services) представляют собой совокупность сетевых служб, обеспечивающих удаленный доступ к серверу при помощи программного обеспечения "тонкого" клиента, выступающего в качестве эмулятора терминала. Все приложения и команды пользователя выполняются непосредственно на сервере, на котором функционируют службы терминалов. Удаленному пользователю передаются только образы экрана приложения, запущенного на сервере. Со стороны клиента серверу передается информация о нажатых на клавиатуре клавишах и о перемещении мыши. Эта информация обрабатывается службами терминалов сервера в рамках сеанса конкретного пользователя. Хотя служба терминалов может одновременно работать с множеством сеансов, пользователь, входя в систему, видит процессы только своего сеанса связи, не зависящие от других клиентских сеансов.

Службы терминалов позволяют получить доступ к приложениям с тех компьютеров, ресурсов которых недостаточно для выполнения подобных программ. Работая со службами терминалов, пользователи могут запускать программы, работать с документами и сетевыми ресурсами так же, как и на локальном компьютере.

Функциональные возможности служб терминалов на базе Windows Server 2008 будут понятны в ходе дальнейшего обсуждения средств администрирования серверов терминалов, клиентских программ и основных режимов работы данных служб.

Серверные средства администрирования

При использовании служб терминалов необходимо контролировать дополнительные параметры учетных записей пользователей, определяющие саму возможность доступа к этим службам, а также настройки сеансов удаленного доступа. Администратор должен устанавливать требуемые параметры, пользуясь оснасткой **Active Directory Users and Computers** (Active Directory – пользователи и компьютеры) для клиентов домена или оснасткой **Local Users and Groups** (Локальные пользователи и группы), если сервер терминалов автономный.

Рассмотрим административные оснастки, используемые для управления службами терминалов.

> ***Примечание***
>
> Помимо оснасток, которые будут описаны далее, имеются утилиты командной строки, с помощью которых можно осуществлять администрирование служб терминалов, управление сеансами и просмотр запущенных процессов.

Оснастка *Terminal Services Configuration* (Настройка служб терминалов)

Во время установки служб терминалов автоматически настраивается подключение по протоколу RDP (Remote Desktop Protocol) для работы с серверами терминалов и их удаленного администрирования. Это подключение обеспечивает клиентам вход в систему на сервер и установление сеанса. По завершении установки служб можно изменить свойства этого подключения с помощью оснастки **Terminal Services Configuration** (Настройка служб терминалов; tsconfig.msc) (рис. 10.1).

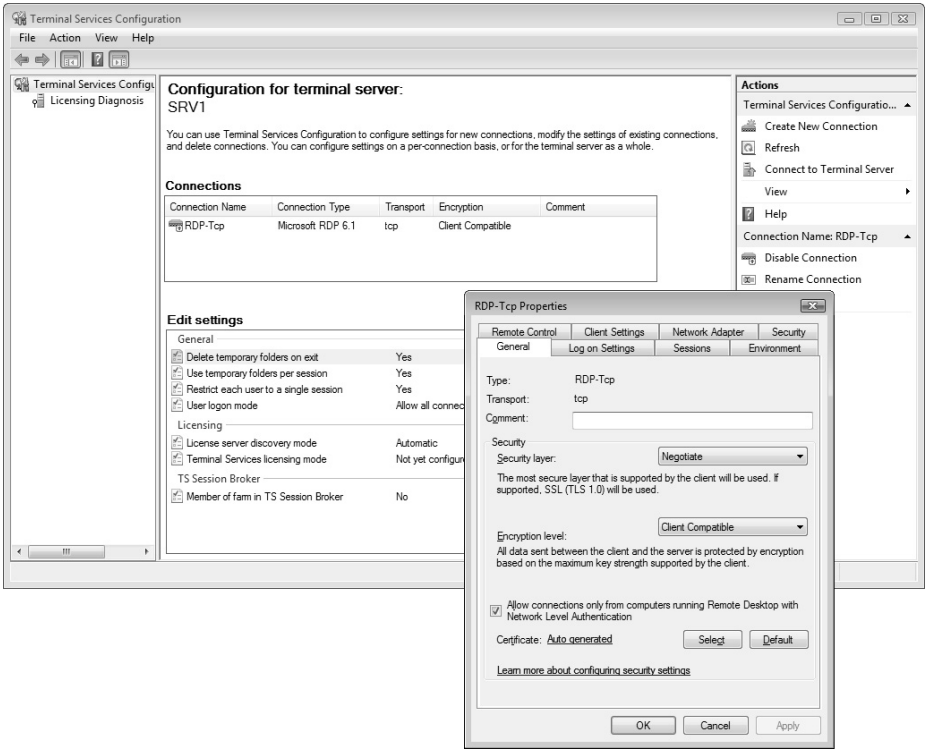


Рис. 10.1. Оснастка **Terminal Services Configuration**

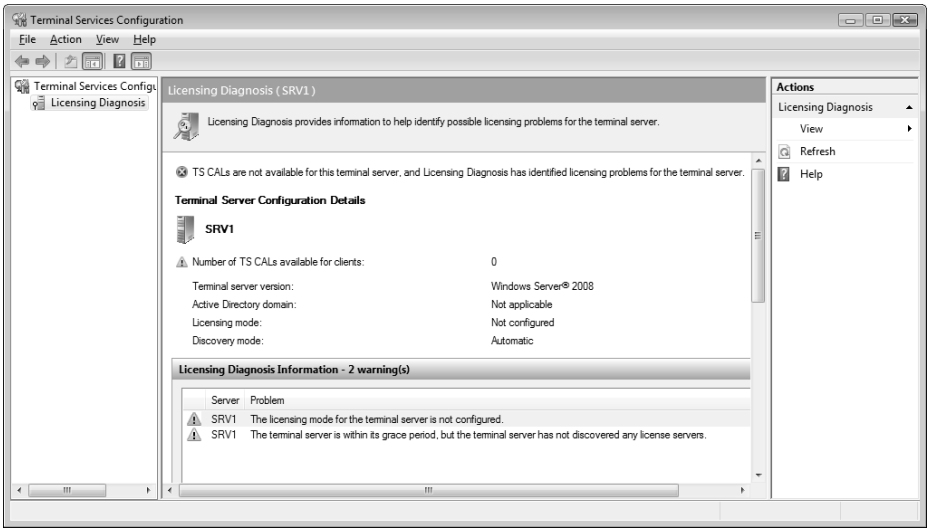


Рис. 10.2. Информация службы лицензирования для выбранного сервера терминалов

Также оснастка **Terminal Services Configuration** (Настройка служб терминалов) позволяет подключаться к службам лицензирования и получать от них информацию о типе лицензирования для выбранного сервера терминалов и количестве лицензий (рис. 10.2).

Оснастка *Terminal Services Manager* (Диспетчер служб терминалов)

Оснастка **Terminal Services Manager** (Диспетчер служб терминалов; tsadmin.msc) (рис. 10.3) является основным средством управления серверами терминалов, развернутых в корпоративной сети. Она используется для управления сеансами связи и позволяет контролировать запущенные процессы.

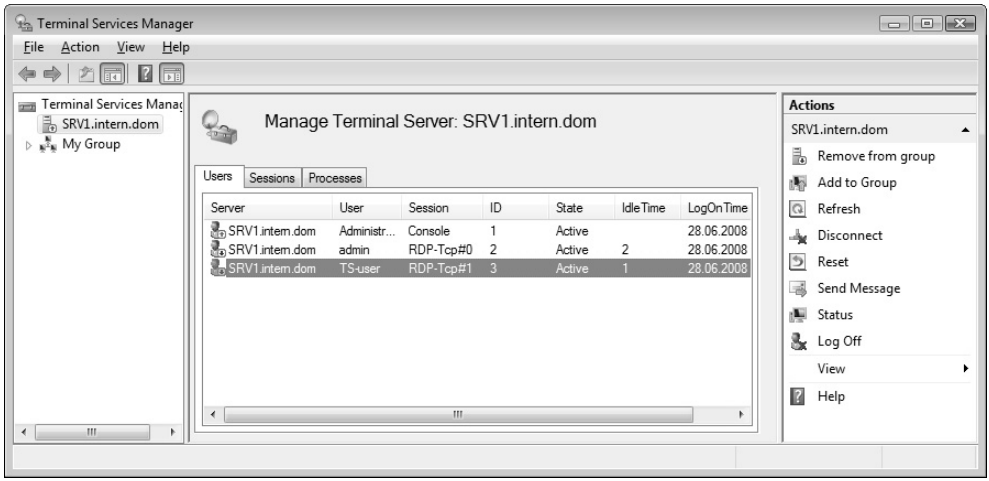


Рис. 10.3. Оснастка **Terminal Services Manager**

Когда пользователь устанавливает подключение, подключаясь к терминальному серверу с клиентского компьютера, то этот сеанс (session) появляется в списке сеансов в рабочем поле диспетчера служб терминалов. Все сеансы связи отображаются на вкладке **Sessions** (Сеансы), где можно также видеть имя компьютера, с которого выполнено подключение (рис. 10.4). (Как можно видеть на рисунке, с одного компьютера может быть сделано несколько подключений.) Любые приложения, работающие в сеансе связи пользователя, отражаются в списке процессов на вкладке **Processes** (Процессы) (эту информацию можно видеть и в окне диспетчера задач). Таким образом, можно

наблюдать за всеми пользователями, сеансами связи и процессами на терминальном сервере при помощи одной утилиты. Все доступные команды представлены на панели **Actions** (Действия).

Когда оснастка **Terminal Services Manager** (Диспетчер служб терминалов) запускается на самом сервере терминалов из меню **Start** (Пуск), то появляется сообщение о том, что некоторые возможности оснастки будут недоступны, и для того чтобы их можно было использовать, необходимо запускать оснастку в сеансе клиентского подключения к серверу терминалов (рис. 10.5).

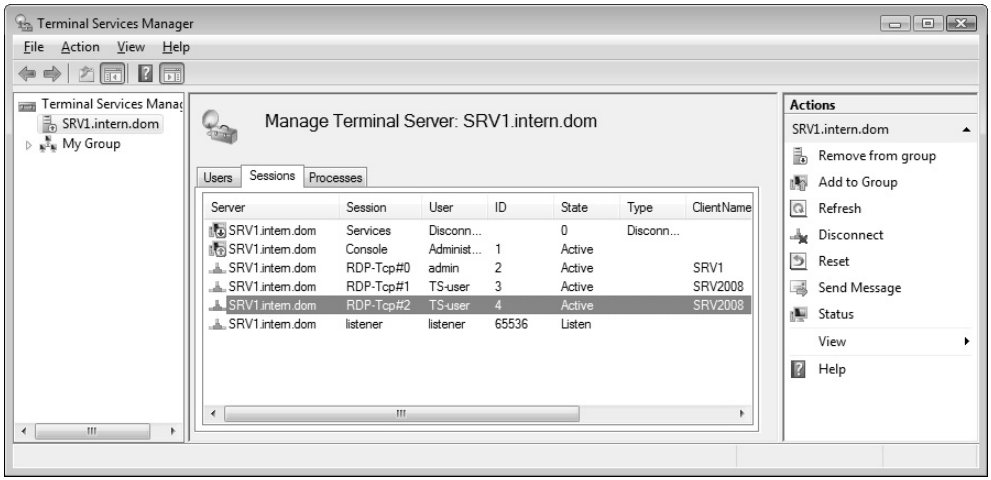


Рис. 10.4. Просмотр сеансов удаленного доступа и команды управления сеансами

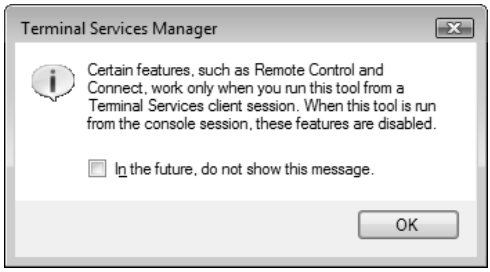


Рис. 10.5. Предупреждение об ограничении возможностей оснастки при запуске с консоли

В папке **Terminal Services** (Службы терминалов), входящей в меню **Administrative Tools** (Администрирование), имеется веб-ссылка **TS Web**

Access Administration, автоматически запускающая веб-браузер и создающая сеанс удаленного подключения к оснастке **Terminal Services Manager** (Диспетчер служб терминалов) — в этом случае становятся доступными все ее возможности.

Оснастка *TS RemoteApp Manager* (Диспетчер RemoteApp служб терминалов)

Оснастка **TS RemoteApp Manager** (Диспетчер RemoteApp служб терминалов; remoteprograms.msc) (рис. 10.6) является ключевой для управления доступом к приложениям, развернутым на сервере терминалов.

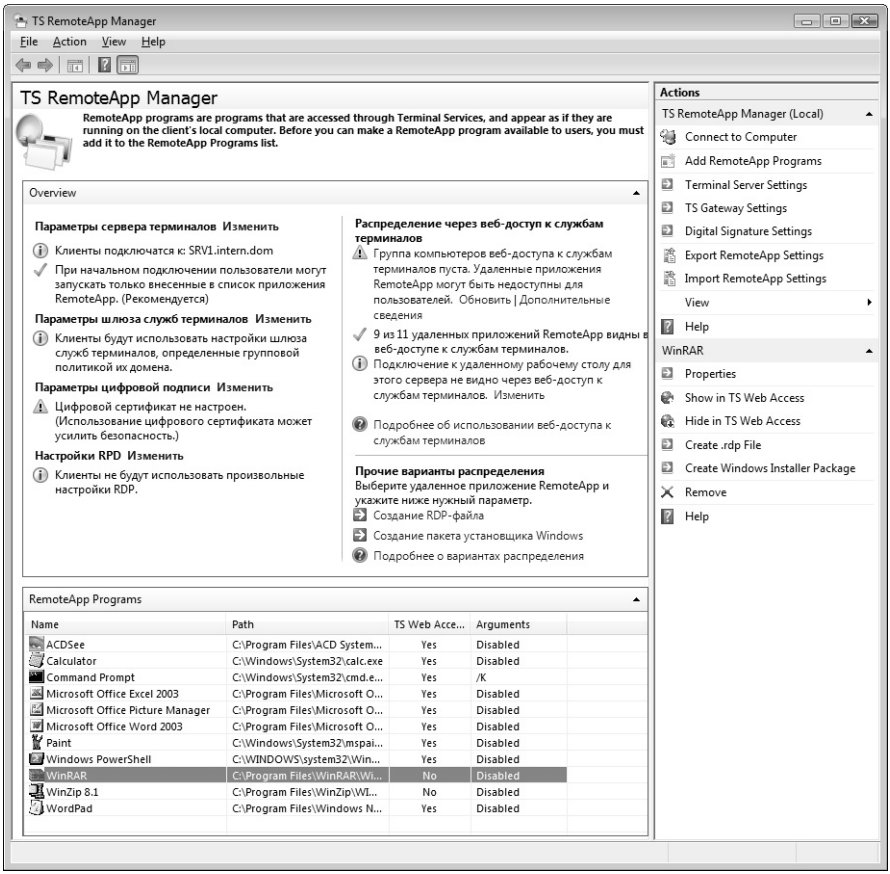


Рис. 10.6. Управление приложениями, развернутыми на сервере терминалов

Следует внимательно изучить все ее возможности, которых очень много. Для этого, в первую очередь, в окне оснастки нужно просмотреть все ссылки, имеющиеся на центральной панели. Это позволит сразу получить представление об основных способах удаленного использования установленных приложений. Описание разделов параметров в окне оснастки отображается на том языке, который соответствует региональным установкам, имеющимся на компьютере. Поэтому в нашем примере оно на русском языке.

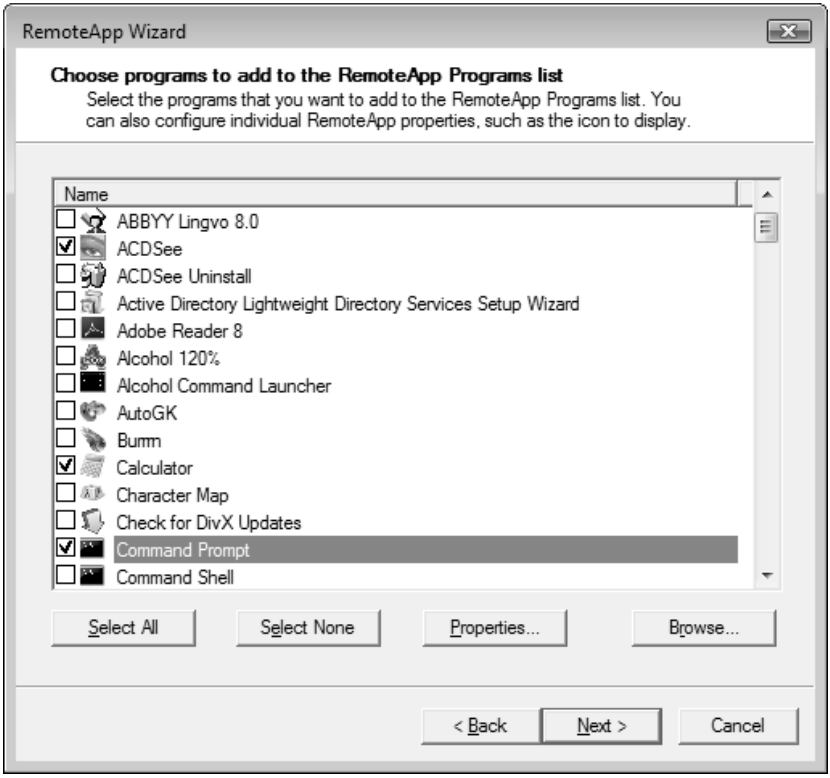


Рис. 10.7. Список программ, предлагаемых для удаленного использования

Чтобы сделать некоторую программу доступной для клиентов сервера терминалов, воспользуетесь ссылкой **Add RemoteApp Programs** (Добавить программы RemoteApp) на панели **Actions** (Действия). Программа-мастер поможет сделать необходимые для этого настройки. В окне предлагаемых программ (рис. 10.7) нужно выбрать программу (понятно, что этот список зависит от набора программ, установленных на сервере терминалов!), а если

требуемая программа отсутствует, то можно нажать кнопку **Browse** (Обзор) и найти ее файл на локальном диске.

Нажав кнопку **Properties** (Свойства), можно установить дополнительные параметры, необходимые для запуска приложения (рис. 10.8). Флажок **RemoteApp program is available through TS Web Access** по умолчанию установлен — следовательно, программа будет доступна для веб-подключений и появится в окне, которое удаленный пользователь видит при подключении к серверу терминалов с помощью веб-браузера (см. рис. 10.10). Если это не требуется, то флажок можно снять.

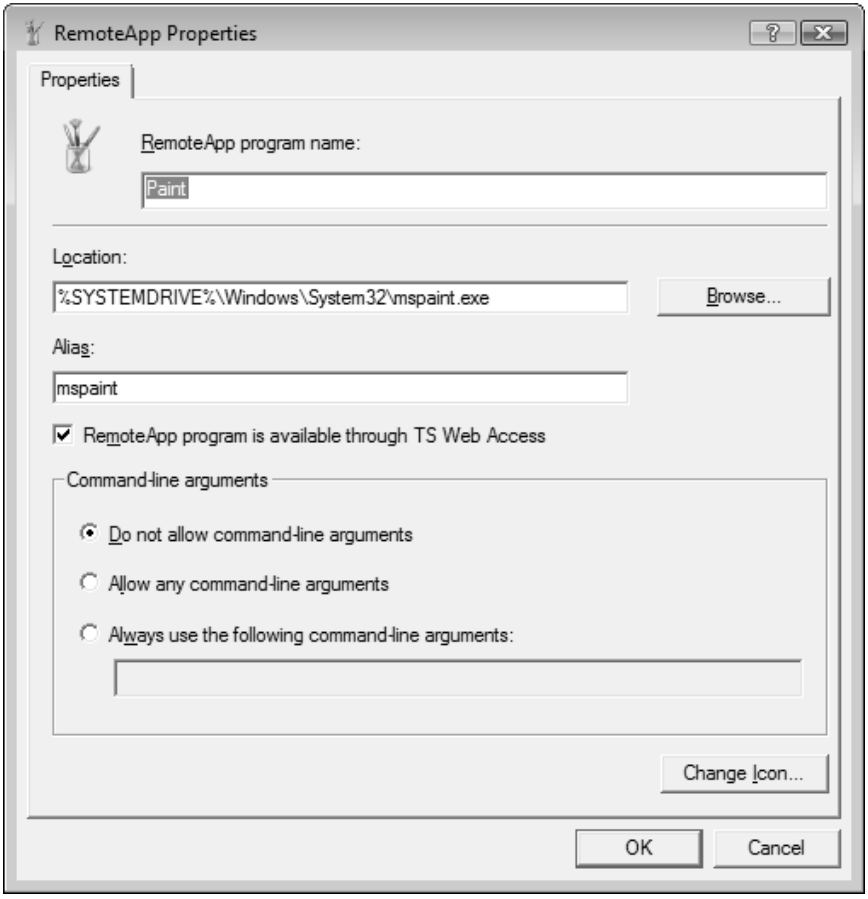


Рис. 10.8. Выбор списка параметров для запуска приложения и управление его видимостью для веб-подключений

Затем необходимо проверить список программ и параметров, после чего нажать кнопку **Finish** (Готово). Выбранная программа появится в списке доступных приложений (см. рис. 10.6).

Ссылка **Create .rdp File** на панели **Actions** (Действия) (см. рис. 10.6) позволяет создать RDP-файл с параметрами, необходимыми для подключения к серверу терминалов и запуска указанного удаленного приложения. Если пользователь запускает у себя на компьютере такой файл *(см. далее разд. "Утилита Remote Desktop Connection (Подключение к удаленному рабочему столу)")*, то после ввода параметров учетной записи он сразу увидит у себя на экране окно приложения, запущенного на сервере терминалов.

Рис. 10.9. Выбор ресурсов, доступных в сеансе удаленного доступа

Удаленный пользователь, подключающийся к серверу терминалов при помощи веб-браузера, должен ввести в поле адреса строку вида `http://<имяСервера>/ts`. Он увидит начальную веб-страницу сервера терминалов, содержащую пиктограммы опубликованных приложений (см. рис. 10.10). При выборе приложения пользователь может в специальном окне

(рис. 10.9) выбрать ресурсы своего компьютера, которые будут доступны в сеансе удаленного доступа (например, при выборе дисков (опция **Drives**) он будет иметь доступ и к дискам сервера терминалов, и к своим локальным дискам). Однако администратор может отключить все эти возможности (см. рис. 10.12).

После этого пользователь увидит у *себя* на экране окно приложения, работающего на *удаленном* сервере терминалов (рис. 10.10). В нашем примере видно, что в окне консоли, отображаемой на компьютере пользователя, видно содержимое диска сервера терминалов.

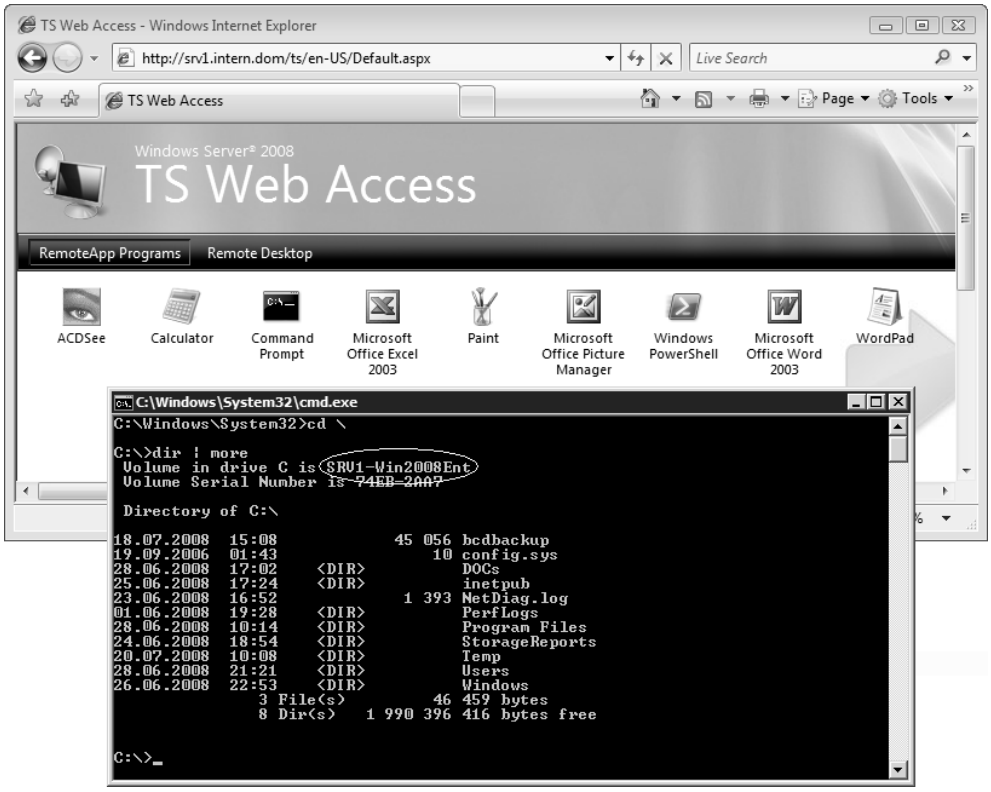


Рис. 10.10. Работа с программой, запущенной на сервере терминалов

Если в главном окне оснастки **TS RemoteApp Manager** (Диспетчер RemoteApp служб терминалов) выбрать ссылку **Изменить** в разделе **Параметры сервера терминалов**, то откроется окно параметров, где указывается

имя сервера и используемый RDP порт (что может быть важно для настройки брандмауэра) (рис. 10.11). Если установить флажок **Show a remote desktop connection to this terminal server in TS Web Access**, то в списке программе доступных через веб-подключение (см. рис. 10.10), появится также значок удаленного доступа к рабочему столу.

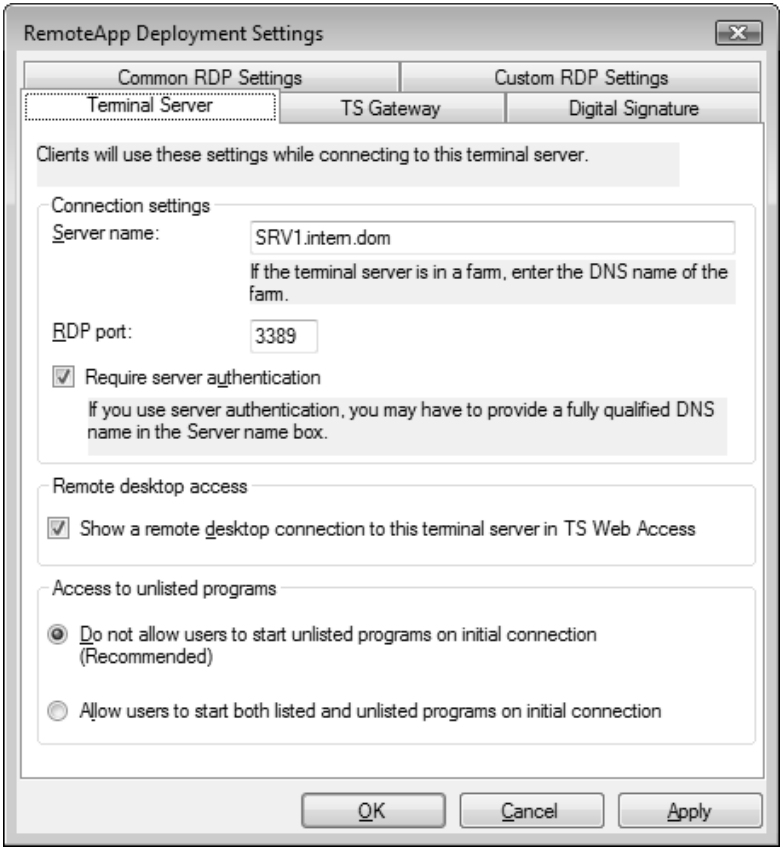


Рис. 10.11. Основные параметры сервера терминалов при работе с удаленными приложениями

Важные для работы удаленных пользователей параметры сервера перечислены на вкладке **Common RDP Settings** (Общие параметры RDP) (рис. 10.12). В зависимости от установленных опций, пользователи в сеансе удаленного подключения будут иметь полный или ограниченный доступ к своим локаль-

ным ресурсам (см. рис. 10.9). Администратор может запретить любые перечисленные на этой вкладке возможности.

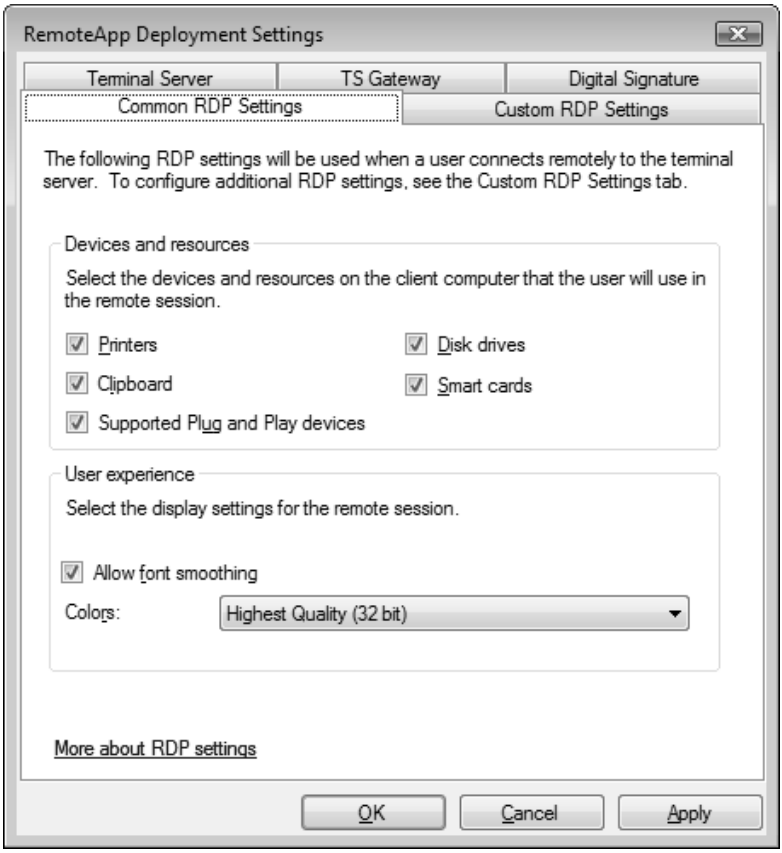


Рис. 10.12. Выбор ресурсов, доступных пользователю в сеансе удаленного подключения

Клиентские средства подключения к серверам терминалов

Имеется несколько программ, которые могут быть использованы для подключения к службам терминалов, в том числе и для удаленного администрирования системы.

Утилита Remote Desktop Connection (Подключение к удаленному рабочему столу)

Утилита *Remote Desktop Connection* (Подключение к удаленному рабочему столу; mstsc.exe) является основным клиентом для работы со службами терминалов и выполнения удаленного администрирования *(см. главу 4)*. Утилита позволяет сохранять выбранные пользователем параметры подключения к удаленному компьютеру или серверу терминалов. RDP-файлы позволяют автоматизировать процесс установки соединения со службами терминалов и входа на сервер, а при использовании файлов, подготовленных с помощью оснастки **TS RemoteApp Manager** (Диспетчер RemoteApp служб терминалов), может сразу запускаться программа, установленная на сервере терминалов.

В отличие от обычного режима подключения к удаленному рабочему столу *(см. главу 4)*, когда число сеансов не может быть больше двух, при использовании сервера терминалов количество сеансов ограничено только наличием клиентских лицензий.

Подключение через Интернет

Удаленный клиент может подключиться к серверу терминалов (при условии, что на нем также установлены службы IIS — компонент TS Web Access) через Интернет или другую сеть, используя обычный веб-браузер и введя в поле адреса строку вида `http://<имяСервера>/ts`.

После подключения к серверу терминалов появится главная страница сервера (используемый язык зависит от региональных установок на компьютере клиента), на которой пользователь может выбирать опубликованные приложения (см. рис. 10.10) или опцию подключения к удаленному рабочему столу (рис. 10.13) (для переключения служат соответствующие кнопки). В этом случае дополнительные параметры указываются непосредственно на веб-странице.

Оснастка *Remote Desktops* (Удаленные рабочие столы)

Для работы со службами терминалов, как и для удаленного подключения к рабочим столам, может использоваться оснастка **Remote Desktops** (Удален-

ные рабочие столы; tsmmc.msc /s), запускаемая из папки **Terminal Services** (Службы терминалов), входящей в меню **Administrative Tools** (Администрирование).

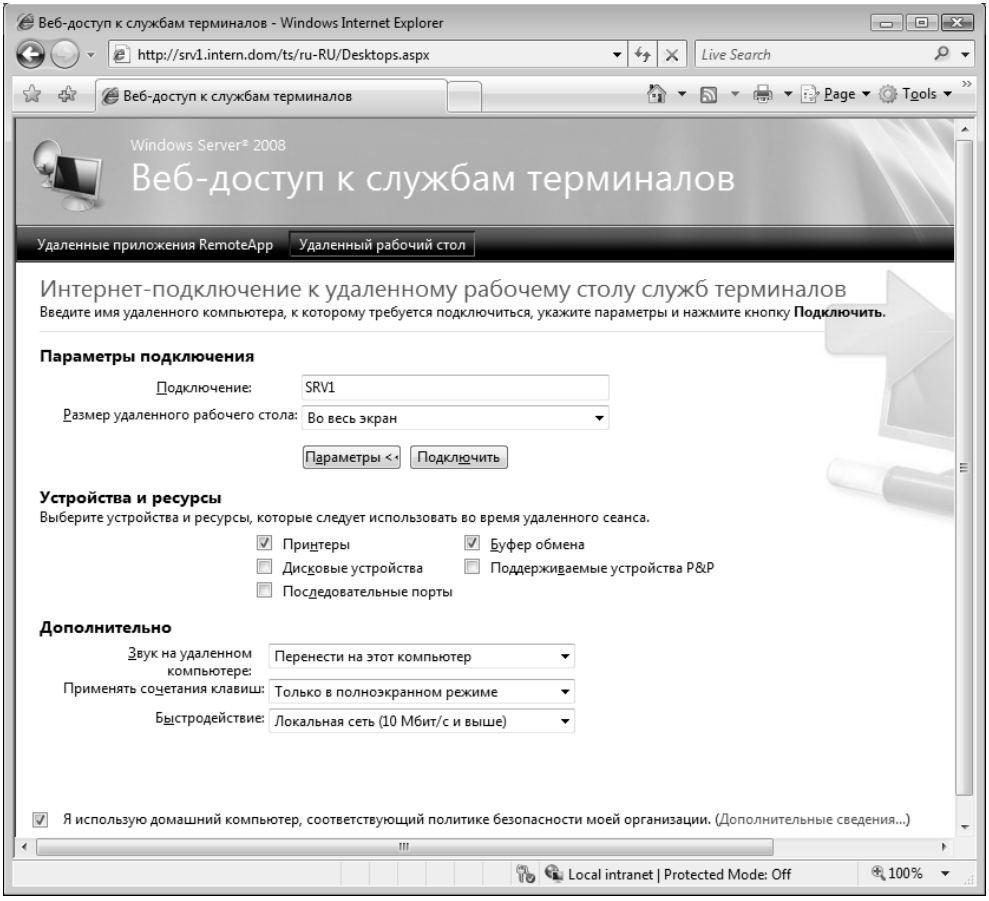


Рис. 10.13. Подключение к службам терминалов через Интернет

На рис. 10.14 для примера показано одновременное подключение к серверу терминалов srv1.intern.dom и рабочему столу компьютера gate. Каждый сеанс предварительно создается и конфигурируется, после чего любой сеанс можно легко инициировать с помощью команды **Connect** (Подключить) в контекстном меню выбранного компьютера. После подключения легко можно переключаться между различными сеансами.

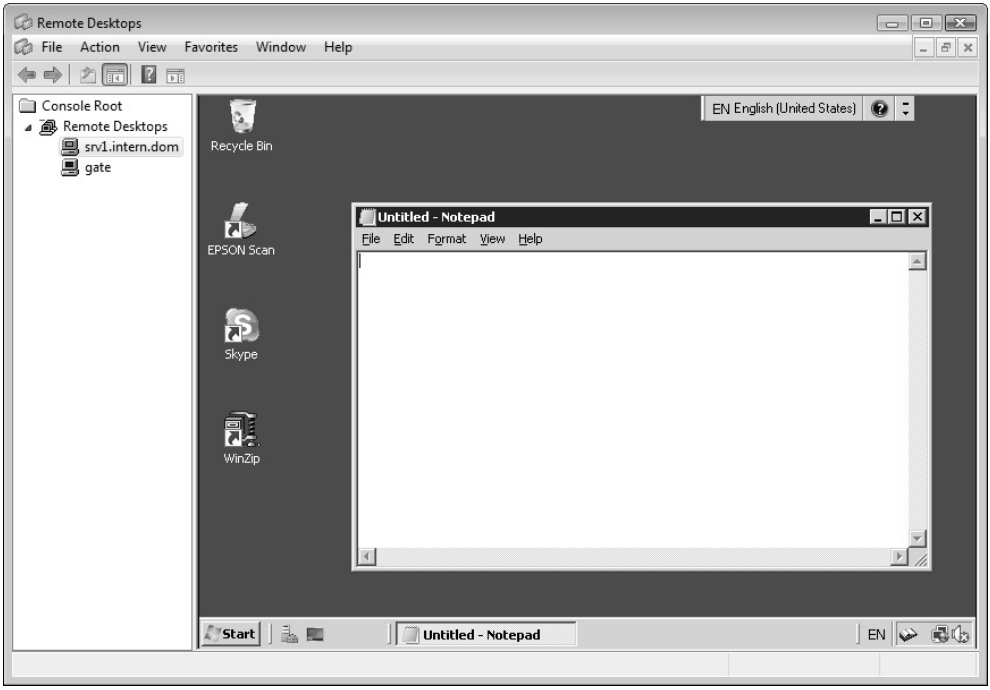


Рис. 10.14. Окно оснастки **Remote Desktops** с подключениями к удаленным компьютерам

Установка служб терминалов

Для использования служб терминалов на компьютере, работающем под управлением Windows Server 2008, необходимо с помощью оснастки **Server Manager** (Диспетчер сервера) добавить роль сервера *Terminal Services* (Службы терминалов). При установке можно выбрать отдельные компоненты служб (рис. 10.15). В "минимальном" варианте достаточно только первой службы. Без установки лицензий службы терминалов могут в пробном (trial) режиме проработать 120 дней. (При этом никаких функциональных ограничений не будет!)

На следующем шаге мастер добавления роли попросит выбрать опцию сетевой аутентификации (рис. 10.16) *(см. примечание к рис. 4.18)*. Этот выбор должен быть согласован с версиями клиентских программ, используемых для подключения к устанавливаемому серверу терминалов.

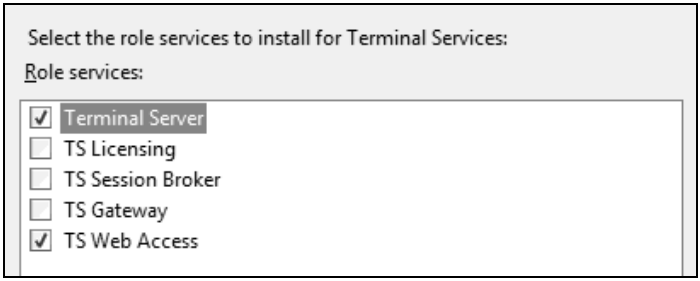


Рис. 10.15. Набор компонентов при установке служб терминалов

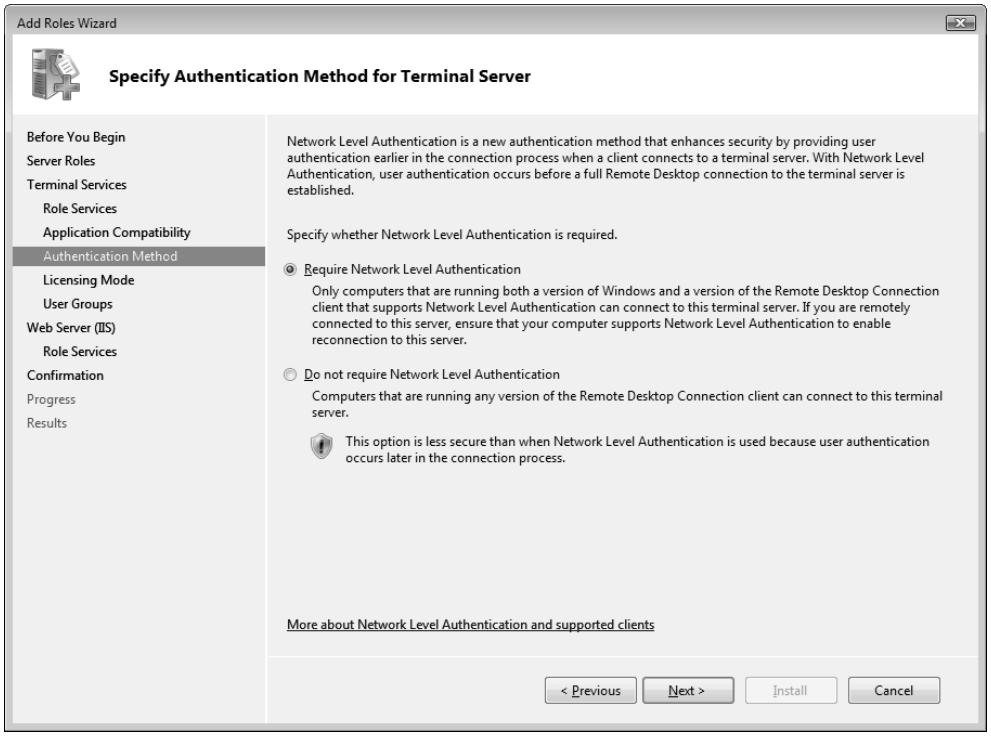


Рис. 10.16. Выбор уровня сетевой аутентификации

Далее следует указать схему лицензирования служб терминалов (рис. 10.17). Выбор опции зависит от имеющихся лицензий, но можно начать работу и без их наличия. Тем не менее, вопрос с лицензиями нужно решить в течение 120 дней, иначе использование служб терминалов будет невозможным.

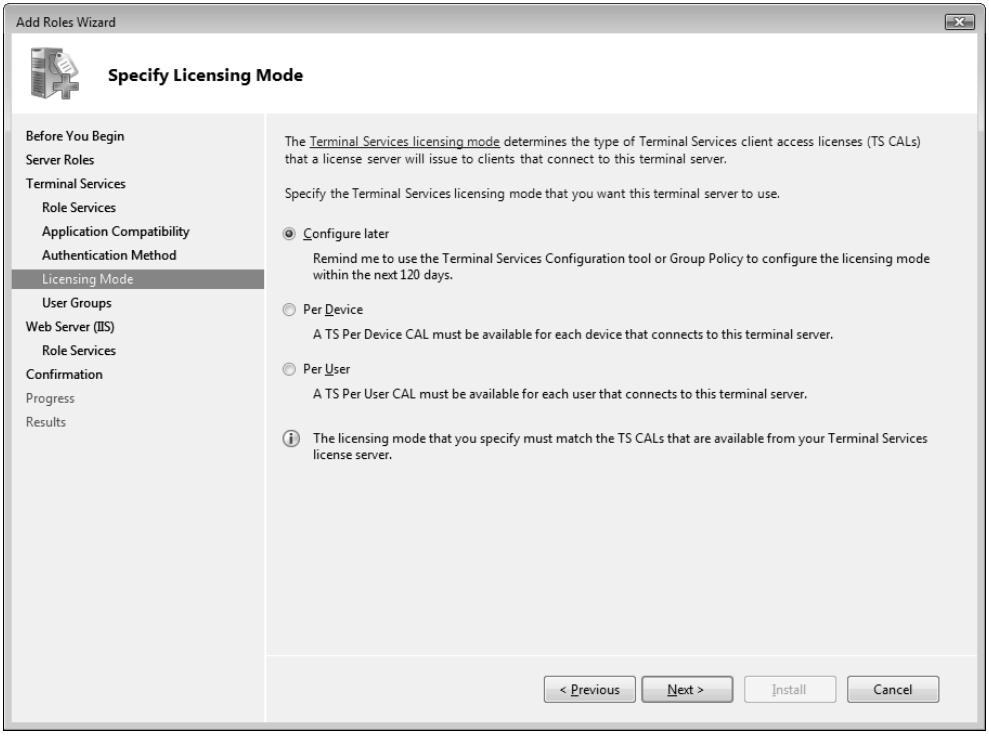


Рис. 10.17. Выбор схемы лицензирования служб

По умолчанию доступ к установленному серверу терминалов имеют члены локальных групп Administrators (Администраторы) и Remote Desktop Users (Пользователи удаленного рабочего стола). При необходимости следует добавить другие учетные записи.

Если при добавлении роли Terminal Services (Службы терминалов) выбирается компонент TS Web Access, то на следующем шаге происходит автоматический выбор и установка нужных элементов служб IIS 7.0.

По завершении работы мастера добавления роли сервер терминалов будет готов к работе.

Глава 11

Сетевые службы

Данная глава посвящена ключевым сетевым службам, которые используются в сетях, построенных на базе стека протоколов TCP/IP. Рассмотрены все основные вопросы, необходимые для развертывания каждой службы в локальной сети. В системах Windows Server 2008 этим службам соответствуют следующие роли сервера, добавляемые с помощью оснастки **Server Manager** (Диспетчер сервера):

- DNS Server (DNS-сервер)
- DHCP Server (DHCP-сервер)
- Network Policy and Access Services (Службы политики сети и доступа)
- Web Server (IIS) (Веб-сервер (IIS))

В этой последовательности мы и будем рассматривать службы более подробно.

Серверы службы доменных имен (DNS)

Служба доменных имен (Domain Name System, DNS) является важным компонентом любой крупной сетевой инфраструктуры. Служба доменных имен осуществляет *разрешение*, или преобразование, символьных имен в IP-адреса. Символьные имена используются для доступа к ресурсам Интернета и веб-узлам корпоративной сети.

Служба DNS является обязательной для доменов Active Directory, и для развертывания доменов нужен хотя бы один DNS-сервер. Это требование нельзя игнорировать. Иерархия доменов Active Directory "отображается" на пространство имен DNS. Клиенты доменов на базе Active Directory используют

службу DNS для обнаружения контроллеров домена, а контроллеры обращаются к ней для поиска адресов партнеров по репликации. Поэтому процессы создания доменной структуры и формирования DNS-имен являются взаимосвязанными. Ошибки, допущенные при проектировании пространства имен DNS (например, неудачный выбор имен доменов), могут серьезно осложнить внедрение и развитие сети, а в некоторых случаях может даже потребоваться повторное развертывание всего леса доменов.

Планирование структуры DNS-имен

Перед использованием серверов DNS в сети — особенно при развертывании доменов Active Directory — необходимо тщательно спланировать пространство используемых имен DNS. Перечислим основные задачи и вопросы, которые необходимо решить до установки службы:

- выбор и предварительная регистрация имени корневого домена (если это имя будет доступно для общего доступа из Интернета);
- определение местоположения серверов DNS — внутри частной сети или у провайдера служб Интернета;
- будет ли устанавливаемый DNS-сервер использоваться для обеспечения работы доменов Active Directory;
- выбор типа DNS-сервера (кэширующий, основной, вторичный);
- выбор зон DNS, определение способов их хранения и областей репликации;
- определение требований к доменным именам компьютеров.

Возможности DNS-серверов на базе Windows Server 2008

Ниже перечислены основные функциональные возможности серверов DNS в системах Windows Server 2008.

- **Соответствие стандартам RFC.** Служба DNS базируется на открытых протоколах и полностью соответствует промышленным стандартам (RFC).
- **Возможность взаимодействия с другими реализациями DNS-серверов.** Поскольку служба DNS построена на основе существующих стан-

дартов, она успешно взаимодействует совместно с большинством других реализаций DNS (например, BIND).

- **Поддержка протокола динамического обновления в соответствии с RFC.** Служба DNS позволяет клиентам динамически обновлять ресурсные записи при помощи динамического протокола обновления DNS (стандарт RFC 2136). Это облегчает администрирование DNS, избавляя от необходимости вносить эти записи вручную. Компьютеры под управлением Windows, начиная с Windows 2000, могут динамически регистрировать свои доменные имена. Возможны безопасные обновления (secure updates), которые разрешены только клиентам, прошедшим аутентификацию в домене.

- **Поддержка инкрементных передач зоны между серверами.** Передача зоны осуществляется между DNS-серверами в качестве средства синхронизации отдельных экземпляров базы данных зоны (это необходимо только для зон, не интегрированных в Active Directory). Стандартная процедура передачи зоны предполагает копирование всей базы данных зоны с одного сервера на другой. Инкрементная передача зоны позволяет копировать только сведения об изменениях.

- **Поддержка множества типов ресурсных записей.** Служба DNS обеспечивает поддержку различных типов ресурсных записей (RR), включая записи SRV (расположение службы) и ATMA (адрес ATM), что значительно расширяет возможности использования DNS в глобальных сетях.

- **Зоны-заглушки** (stub zones). Зона-заглушка представляет собой фрагмент зоны, содержащий только те ресурсные записи (типов SOA, NS и A), что необходимы для нахождения DNS-серверов, являющихся носителями полной версии зоны. Поэтому зоны-заглушки попросту перенаправляют клиентские запросы тем DNS-серверам, которые хранят авторитетные зоны и могут выполнить разрешение доменных имен, принадлежащих к этим зонам.

- **Условные пересылки запросов** (conditional forwarding). Данный механизм позволяет перенаправлять запросы клиентов на другие DNS-серверы в соответствии с доменным именем, содержащимся в запросе. Обычный режим пересылки (forwarding) предполагает перенаправление *всех* запросов на определенный DNS-сервер или группу серверов. Механизм условных пересылок фактически позволяет выполнять на DNS-сервере сортировку запросов: некоторую часть запросов сервер способен разрешить сам, другая часть будет перенаправлена различным серверам имен.

Условные пересылки могут быть, к примеру, использованы как средство организации взаимодействия двух лесов доменов, имеющих собственные, совершенно независимые пространства имен DNS. В этом случае для разрешения имен на DNS-серверах одного леса указываются адреса DNS-серверов другого леса, которые будут обрабатывать запросы, обращенные к "чужому" пространству имен.

- **Интеграция со службой Active Directory.** Как уже говорилось, наличие службы DNS является обязательным условием развертывания Active Directory, поскольку она используется как основной механизм обнаружения ресурсов и адресное пространство DNS-имен является основой для именования объектов в Active Directory. В свою очередь, DNS-серверы могут использовать каталог Active Directory для хранения зон в том случае, если эти серверы установлены на контроллерах домена. При этом процесс репликации зон (в режиме со многими мастерами) осуществляется непосредственно средствами Active Directory.

  Область репликации зоны зависит от того, в каком разделе каталога она хранится. На серверах Windows 2000 Server зоны могут располагаться только в разделе доменных имен, который реплицируется между контроллерами одного домена. Для DNS-серверов на базе Windows Server 2003/Windows Server 2008 ситуация проще, поскольку они могут хранить зоны в разделах приложений (application partition).

  В том случае, когда DNS-сервер установлен на контроллере домена, для размещения содержимого зоны могут использоваться два специальных стандартных *раздела приложений* (application partitions) с именами ForestDnsZones.<*DNSимяЛеса*> и DomainDnsZones.<*DNSимяДомена*>. Эти разделы по умолчанию реплицируются на все DNS-серверы леса и домена соответственно (а не на *все* контроллеры домена). Кроме того, зоны могут храниться и в разделах приложений, созданных администратором и имеющих свои собственные области репликации. В этом случае именно администратор определяет контроллеры домена, на которых будут храниться реплики этих разделов.

- **Групповые политики** (group policy) для управления параметрами DNS-клиентов на компьютерах, работающих под управлением систем Windows XP и выше (см. в объектах групповых политик узел **Computer Configuration** | **Administrative Templates** | **Network** | **DNS Client**), а также политики, управляющие обновлением ресурсных SRV-записей, которые контроллеры домена на базе Windows Server 2003/Windows Server 2008 регистрируют в DNS (узел **System** | **Net Logon** | **DC Locator DNS Records**).

- **Интеграция с другими сетевыми службами Microsoft.** Служба DNS взаимодействует с другими сетевыми службами Windows и содержит функции, не описанные в RFC. Это касается интеграции со службами WINS и DHCP (например, клиенты нижнего уровня не могут непосредственно регистрировать или обновлять свои DNS-имена; однако это возможно с помощью службы WINS, которая будет выполнять нужные действия в DNS).
- **Эффективные административные инструменты.** Для управления DNS-серверами используется специальная оснастка; кроме того, имеются программы-мастера, позволяющие выполнять повседневные задачи по администрированию сервера, а также дополнительные утилиты командной строки для управления серверами DNS.
- **Возможности ведения журнала и отладочные режимы.**

Возможности DNS-клиентов

В составе систем Windows 2000 и выше имеется служба DNS-клиента (DNS Client; имя сервиса Dnscache). DNS-клиент выполняет обращения к DNS-серверам и позволяет разрешать доменные имена в IP-адреса. DNS-клиент имеет следующие возможности:

- **кэширование ответов.** Ресурсные записи (RR), полученные в ответ на запросы, добавляются в клиентский кэш. Эта информация хранится в течение определенного времени (определяется временем жизни записи, time-to-live, TTL) и может использоваться при последующих запросах;
- **кэширование отрицательных ответов.** Помимо положительных ответов от серверов DNS, DNS-клиент также кэширует отрицательные ответы на запросы. Отрицательный ответ приходит, если ресурсная запись с запрошенным именем не существует. Кэширование отрицательных ответов предотвращает повторные запросы для несуществующих имен, снижающие производительность клиентской службы;
- **блокировка неотвечающих серверов DNS.** DNS-клиент при поиске использует список серверов, упорядоченных по предпочтению. Этот список включает все серверы DNS, настроенные для каждого сетевого подключения. Система способна перестраивать этот список, основываясь на следующих критериях: предпочтитаемые серверы DNS имеют высший приоритет, а остальные серверы DNS чередуются. Неответившие серверы временно удаляются из списка.

Предварительные условия для установки DNS-сервера и способы его использования

Сервер, на котором функционирует служба DNS, должен иметь статический IP-адрес. Нельзя использовать адрес, выделяемый сервером DHCP.

Рассмотрим три основных режима работы серверов DNS и особенности их реализации в системах Windows.

- **Кэширующий** (caching). Автономный сервер DNS, который сразу после установки не хранит авторитетных зон и, следовательно, может только хранить ответы на запросы клиентов, полученные от других DNS-серверов (*серверов пересылки*, forwarders) (см. рис. 11.2). Если серверы пересылки для такого сервера не заданы, то он может использовать *корневые ссылки* (root hints), что, в принципе, нежелательно. Таким образом, чтобы обеспечить функционирование кэширующего сервера, необходимо его установить и сконфигурировать серверы пересылки (если сервер имеет выход в Интернет, часто в этом качестве выступают DNS-серверы провайдера Интернета). После этого сервер сможет разрешать запросы тех клиентов сети, для которых он будет указан в качестве предпочитаемого (preferred).
- **Основной** (primary). Сервер, который поддерживает обновляемую, авторитетную зону (или несколько зон) для некоторого домена (или нескольких доменов, если зон несколько). Эта зона содержит ресурсные записи для компьютеров данного домена. Зона может копироваться с основного сервера на вторичные серверы (если не используются зоны, интегрированные в Active Directory).
- **Вторичный** (secondary). Сервер, хранящий доступную для чтения (read-only) копию зоны, копируемой с некоторого основного (авторитетного) сервера. (Зон может быть множество. При этом сервер может быть вторичным для одной зоны и основным для другой зоны.) Если же и основной, и вторичный серверы DNS поддерживают зоны, интегрированные в Active Directory, то такие серверы рассматриваются как равноправные (т. е. понятия "первичный/вторичный" для них отсутствуют), и обновления могут выполняться на любом сервере. Для интегрированных зон требуются серверы DNS, работающие на контроллерах домена Active Directory. В системах Windows 2000 содержимое таких зон реплицируется только в пределах одного домена, в системах Windows Server 2008 зоны могут также храниться в разделах приложений, область репликации которых определяет администратор.

Установка DNS-сервера

Для установки DNS-сервера на базе Windows Server 2008 необходимо с помощью оснастки **Server Manager** (Диспетчер сервера) добавить роль *DNS Server* (DNS-сервер). Потом из меню **Administrative Tools** (Администрирование) запускается оснастка **DNS** (dnsmgmt.msc), и все дальнейшие манипуляции с сервером и зонами осуществляются с ее помощью.

Вновь установленный DNS-сервер работает в режиме кэширования запросов (поскольку по умолчанию на нем настроены корневые ссылки (root hints), которые могут разрешать запросы клиентов), и не поддерживает авторитетных зон. Сервер может обслуживать запросы, поступающие по всем имеющимся интерфейсам, или только по указанным явно на вкладке **Interfaces** (Интерфейсы) в окне свойств сервера (см. рис. 11.2).

Установка и настройка DNS-сервера на автономном компьютере или рядовом сервере в составе домена не вызывает проблем, поэтому мы, в первую очередь, будем обсуждать те случаи, когда DNS-серверы используются на контроллерах домена.

Сервер DNS на контроллере домена

Когда службы Active Directory и DNS устанавливаются на сервере одновременно (на первом контроллере домена в сети — *см. главу 12*), мастер установки Active Directory (утилита Dcpromo.exe) автоматически создает на DNS-сервере авторитетную зону для указанного домена (леса). Если сервер DNS уже имелся в сети (пусть даже и на том компьютере, который станет контроллером домена), необходимо вручную создать зону для нового леса и разрешить динамическое обновление этой зоны.

По умолчанию мастер установки Active Directory создает две авторитетных зоны — для корневого домена леса и служебную зону _msdcs (см. рис. 12.1). Обе зоны интегрированы в Active Directory и допускают только безопасные обновления. Зона для домена хранится в разделе приложений DomainDnsZones.<*DNSимяДомена*>, который реплицируется на все DNS-серверы *корневого домена*. Служебная зона хранится в разделе приложений ForestDnsZones.<*DNSимяЛеса*>, который реплицируется на все DNS-серверы *всего* леса доменов.

Когда в существующем лесе создается *дочерний домен*, используется зона корневого домена леса и мастер автоматически создает в ней субдомен DNS

для дочернего домена. Однако если к лесу добавляется *новое дерево*, необходимо вручную создать авторитетную зону для нового пространства имен DNS. То есть необходимо вручную создавать авторитетную зону для каждого нового доменного дерева, за исключением случая одновременной установки Active Directory и службы DNS на одном сервере.

> **ВНИМАНИЕ!**
>
> Утилита Dcpromo не создает на сервере DNS зон обратного просмотра (reverse zones). Поэтому для того чтобы сервер DNS был полностью сконфигурированным (без зоны обратного просмотра некоторые утилиты не могут отображать полную информацию), можно вручную создать соответствующую зону обратного просмотра (поскольку она используется многими утилитами и приложениями), разрешить ее динамическое обновление и перерегистрировать адрес контроллера с помощью команды `ipconfig /registerdns`.

Безопасные обновления (secure updates) и настройка разрешений (на вкладке **Security** (Безопасность) в окне свойств зоны — см. рис. 11.3) разрешены только для DNS-зон, интегрированных в Active Directory. Такие зоны возможны только на DNS-серверах, установленных на контроллерах домена.

Когда обычная зона, хранящаяся в текстовом файле, преобразуется в интегрированную в Active Directory, соответствующий файл этой зоны перемещается из папки *%SystemRoot%*\system32\dns во вложенную папку backup. Одновременно в каталоге Active Directory для хранения зоны создаются объекты (типов *dnsZone* и *dnsNode*): если зона хранится на всех контроллерах домена, то объекты размещаются в контейнере CN=MicrosoftDNS,CN=System раздела доменных имен, а на серверах Windows Server 2003 и Windows Server 2008 зоны могут располагаться в соответствующих разделах приложений. Также можно легко выполнить обратное преобразование — из интегрированной зоны в обычную.

> **ВНИМАНИЕ!**
>
> Следует помнить о том, что контроллеры на базе Windows 2000 не поддерживают разделов приложений. Поэтому для того, чтобы DNS-серверы, работающие на контроллерах под управлением Windows 2000 Server и Windows Server 2003/Windows Server 2008, могли совместно использовать интегрированные зоны, нужно выбирать соответствующую область репликации зоны (на все контроллеры домена — *см. далее*).

Установка вторичных DNS-серверов

Для увеличения отказоустойчивости сети можно устанавливать дополнительные (резервные) серверы DNS. Эта задача очень проста, если DNS-сервер устанавливается на каком-нибудь контроллере домена и зоны DNS являются интегрированными в Active Directory — после запуска новый сервер DNS *автоматически* загружает доступную зону (зоны) из каталога Active Directory. В этом случае все DNS-серверы будут равноправными, и понятие *вторичного сервера* будет лишено смысла, поскольку авторитетную зону можно будет обновлять на любом сервере.

Если DNS-сервер устанавливается на рядовом сервере или если интегрированные в Active Directory зоны не используются, то нужные зоны необходимо создавать вручную, обеспечивая *передачу зоны* (zone transfer) (управление этой функцией осуществляется в окне свойств зоны на вкладке **Zone Transfers** (Передачи зон)). В этом случае сервер будет функционировать как вторичный, поэтому и зоны должны создаваться *вторичными*, или *дополнительными* (secondary zones) — с указанием *основных* (master) DNS-серверов.

После установки нового DNS-сервера необходимо указать IP-адрес этого сервера в списке предпочитаемых серверов в окне свойств протокола TCP/IP на клиентах или контроллерах домена.

Администрирование DNS-серверов

Для настройки локального или удаленных DNS-серверов используется оснастка **DNS** (рис. 11.1), запускаемая из меню **Administrative Tools** (Администрирование). После установки сервера можно выбрать его имя в окне оснастки и из контекстного меню вызвать мастер *Configure a DNS Server Wizard* (Мастер настройки сервера DNS), который помогает создавать зоны и ресурсные записи; им можно пользоваться и в дальнейшей работе.

Непосредственно в окне оснастки **DNS** можно просматривать условные пересылки запросов (папка **Conditional Forwarders**) и журнал событий DNS сервера (папка **DNS Events**).

Для администрирования DNS-серверов также можно использовать обновленную утилиту командной строки *DnsCmd.exe*. Эта утилита имеет множество новых команд, поскольку она также позволяет работать с разделами приложений. (Однако для полноценного управления разделами приложений следует использовать утилиту NTDSutil.exe.)

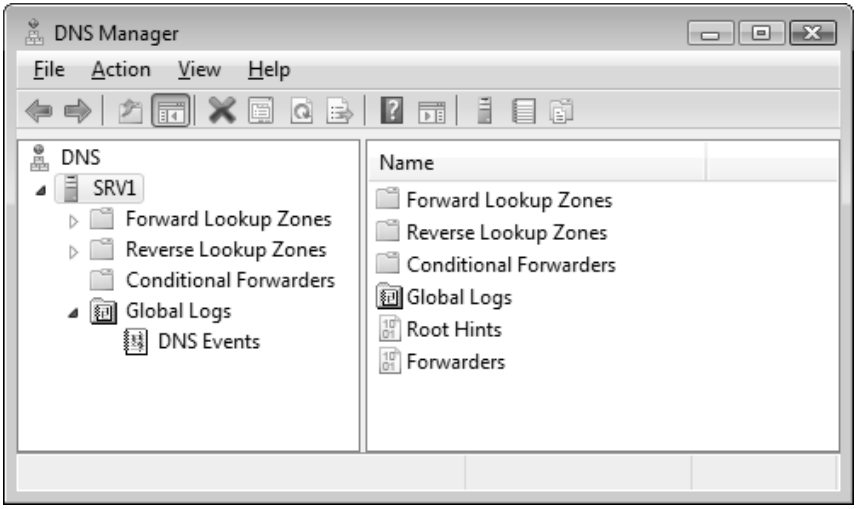


Рис. 11.1. Окно оснастки **DNS** на серверах Windows Server 2008

Внимание!

По умолчанию администрировать DNS-сервер имеют право члены группы DnsAdmins. Однако они не могут останавливать и перезапускать сервер (сервис DNS), а также имеют ограниченные права по управлению зонами, хранящимися в разделах приложений. (Полные права на DNS-сервер имеет локальный администратор компьютера, а также администраторы домена и предприятия.) Поэтому для "тонкой настройки" административных возможностей следует использовать разрешения на конкретные зоны и разделы приложений каталога Active Directory.

Настройка пересылок (forwarders)

DNS-серверы на базе Windows Server 2008 могут сразу же после установки разрешать DNS-запросы ко внешним именам (например, к именам Интернета) (разумеется, если на сервере указан шлюз (default gateway) и имеется интернет-подключение)). В этом случае для пересылки указывается адрес шлюза, заданного для компьютера (предполагается, что он может также выполнять разрешение имен) или используются *корневые ссылки* (root hints) — серверы сети Интернет, разрешающие DNS-имена первого уровня. Для большей эффективности обработки запросов и для того, чтобы не перегружать корневые серверы Интернета, рекомендуется явно указывать *серверы пересылки* (например, адреса DNS-серверов провайдера Интернета). Это делается с помо-

щью оснастки **DNS**, на вкладке **Forwarders** (Пересылка) в окне свойств DNS-сервера (рис. 11.2).

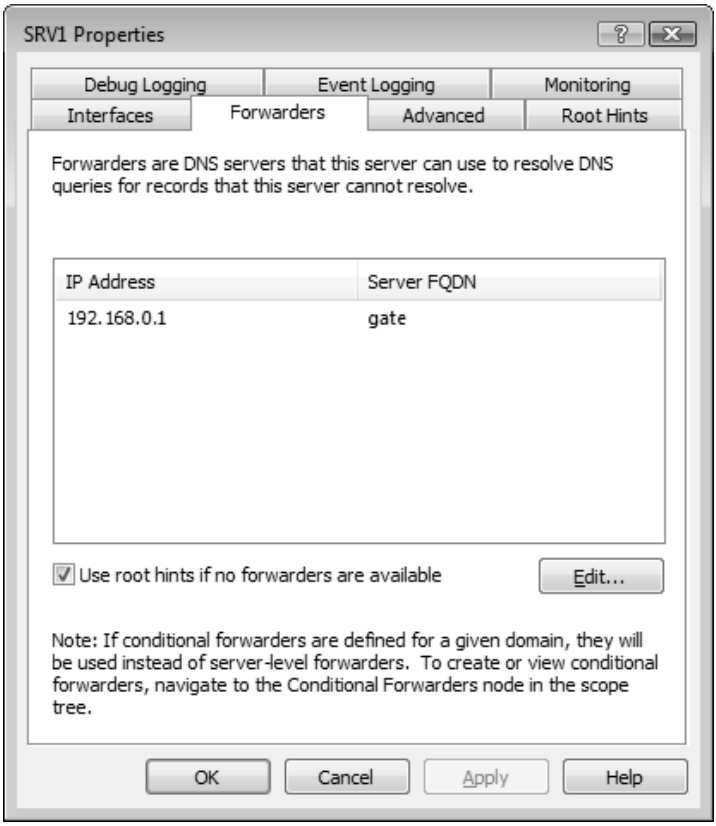


Рис. 11.2. Настройка серверов пересылки для разрешения внешних имен

Управление зонами

Фактически процедура начальной настройки DNS-сервера сводится к созданию необходимых зон, которые будут использоваться для хранения ресурсных записей. Администратор может в любой момент менять параметры зоны, причем обслуживание клиентских запросов при этом никак не нарушается. Для этого нужно открыть окно свойств зоны, выполнив в ее контекстном меню команду **Properties** (Свойства). Основные параметры зоны (которые мы

подробно рассмотрим в последующих разделах) задаются при ее создании с помощью мастера конфигурирования сервера или команды **New Zone** (Создать новую зону) в контекстном меню папок зон прямого (forward) и обратного (reverse) просмотра.

После того как зона создана, администратор может менять следующие общие свойства зоны:

- приостанавливать или разрешать использование зоны;
- изменять способ хранения (тип) зоны;
- управлять репликацией зоны, хранящейся в каталоге Active Directory;
- разрешать динамическое обновление зоны.

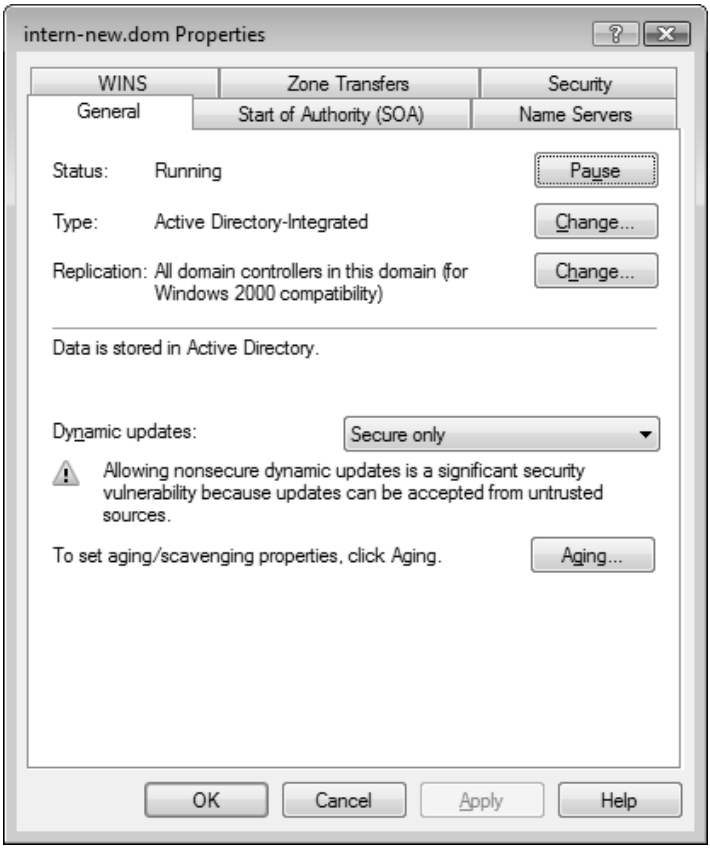


Рис. 11.3. Окно свойств зоны DNS, интегрированной в каталог Active Directory

Последующее изменение конфигурации DNS-сервера может понадобиться по разным причинам, например:

- при изменении имени сервера;
- при изменении имени домена для сервера;
- при изменении IP-адреса сервера;
- при удалении DNS-сервера из сети;
- при изменении основного сервера (primary server) зоны.

Окно свойств (рис. 11.3) обычной зоны состоит из пяти вкладок. Для зоны, интегрированной в Active Directory, появляется шестая вкладка — **Security** (Безопасность), на которой администратор может ограничить доступ к зоне и ее содержимому.

> ***СОВЕТ***
>
> Для того чтобы можно было быстрее просматривать свойства зон, пользуйтесь кнопкой **Properties** (Свойства). При ее нажатии сразу открывается окно свойств объекта, выбранного в окне оснастки, и контекстными меню пользоваться не нужно.

Изменение типа зоны и способа хранения

На вкладке **General** (Общие) в поле **Type** (Тип) отображается тип зоны (см. рис. 11.3). При необходимости его изменения нужно нажать кнопку **Change** (Изменить). В открывшемся окне (рис. 11.4) администратор должен выбрать новый тип зоны. Обратите внимание, что установленный флажок **Store the zone in Active Directory** (Хранить зону в Active Directory) свидетельствует о том, что зона *интегрирована* в каталог Active Directory. Поскольку этот способ хранения не допускает использование дополнительных носителей зон (вторичных DNS-серверов), выбор переключателя **Secondary zone** (Дополнительная зона) в качестве типа зоны приводит к тому, что данный флажок автоматически снимается и становится недоступным для изменения.

Если зона хранится в Active Directory, администратор может регламентировать доступ к объектам пространства имен DNS на вкладке **Security** (Безопасность). Такую вкладку имеет каждый объект пространства имен DNS (домены, зоны, ресурсные записи).

DNS-серверы поддерживают *зоны-заглушки* (stub zone). Такие зоны позволяют корневому DNS-серверу (хранящему авторитетную зону леса, например,

intern.dom) иметь сведения о серверах, являющихся авторитетными для некоторой дочерней зоны (например, sub.intern.dom).

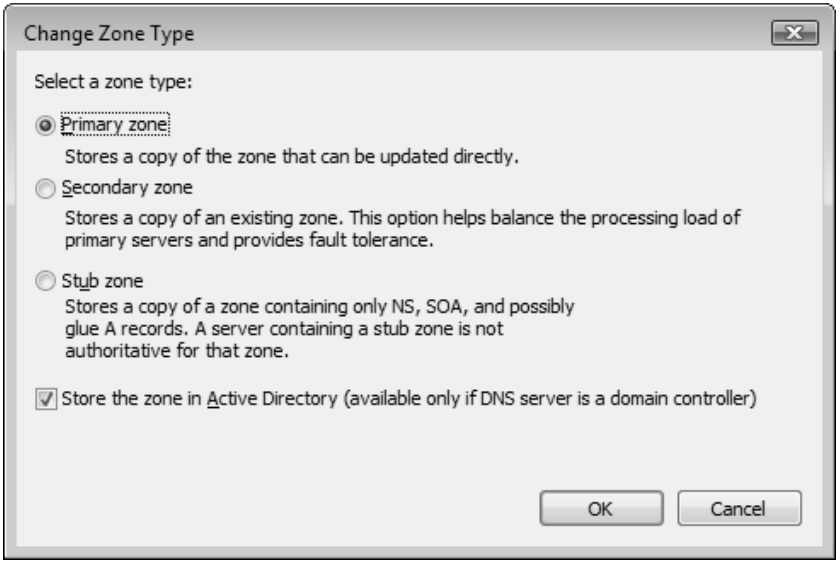


Рис. 11.4. Выбор типа (способа хранения) зоны

Поскольку условные пересылки способны решать те же задачи, что и зоны-заглушки, очень трудно увидеть различия между ними — в обоих случаях запросы пользователей по разрешению определенного доменного имени перенаправляются на конкретный(ые) DNS-сервер(ы). Использование зон-заглушек обеспечивает бóльшую гибкость в конфигурировании структуры DNS. Изменение списка DNS-серверов, выступающих в качестве носителей полноценной копии зоны (а соответственно, способных выполнить разрешение определенного множества доменных имен), приводит к автоматическому обновлению зоны-заглушки на всех ее носителях. В случае же использования механизма условных пересылок администратору придется вручную изменить конфигурацию всех вовлеченных DNS-серверов.

Изменение области репликации зоны

Для DNS-серверов на базе серверов Windows Server 2003 и Windows Server 2008 в поле **Replication** (Репликация) вкладки **General** (Общие) окна свойств зоны указывается область распространения изменений зоны (для систем

Windows 2000 интегрированные зоны могут храниться только в разделе доменных имен, и выбора тут нет). Это поле отображается только для зон, интегрированных в Active Directory. Фактически значение данного поля определяет раздел каталога, в котором хранится содержимое зоны. Соответственно, выбор раздела влияет на область репликации изменений. Нажав кнопку **Change** (Изменить), администратор может в открывшемся окне определить новое место хранения зоны (рис. 11.5). Перечень значений, предлагаемых администратору в этом окне, приведен в табл. 11.1.

Таблица 11.1. *Области репликации зон, интегрированных в Active Directory*

Область репликации	Описание
To all DNS servers in this forest (На все DNS-серверы в лесу)	Зона размещается в разделе приложений, доступном в пределах *всего леса*
To all DNS servers in this domain (На все DNS-серверы в домене)	Зона размещается в разделе приложений, доступном в пределах *конкретного домена*
To all domain controllers in this domain (На все контроллеры домена в домене)	Зона размещается в доменном разделе каталога. Этот способ размещения зоны необходимо выбирать, если в качестве носителей зоны также используется Windows 2000 DNS Server
To all domain controllers in the scope of this directory partition (На все контроллеры домена в области видимости следующего раздела приложений)	Зона размещается в некотором разделе приложений, реплика которого имеется на данном контроллере домена. Этот раздел создается администратором. Администратор также определяет и контроллеры домена, которые будут хранить реплики этого раздела приложений

Область репликации зоны можно также изменить с помощью утилиты DnsCmd. (Для просмотра содержимого раздела приложений используйте оснастку **ADSI Edit** (Редактирование ADSI) — *см. главу 12*.) Следующая команда позволит быстро найти имена всех контроллеров — хранителей реплики указанного раздела приложений (ForestDnsZones.intern.dom):

```
C:\>dnscmd /DirectoryPartitionInfo ForestDnsZones.intern.dom
Directory partition info:
```

```
  DNS root:    ForestDnsZones.intern.dom
  Flags:       0x19 Enlisted Auto Forest
  State:       0
  Zone count: 5
  DP head:     DC=ForestDnsZones,DC=intern,DC=dom
  Crossref:    CN=38b7d5d7-a386-4de7-a646-
85c358b758d0,CN=Partitions,CN=Con...
  Replicas:    2
    CN=NTDS Settings,CN=SRV1,CN=Servers,CN=INTERN-
Site,CN=Sites,CN=Configu...
    CN=NTDS Settings,CN=SRV2,CN=Servers,CN=INTERN-
Site,CN=Sites,CN=Configu...
Command completed successfully.
```

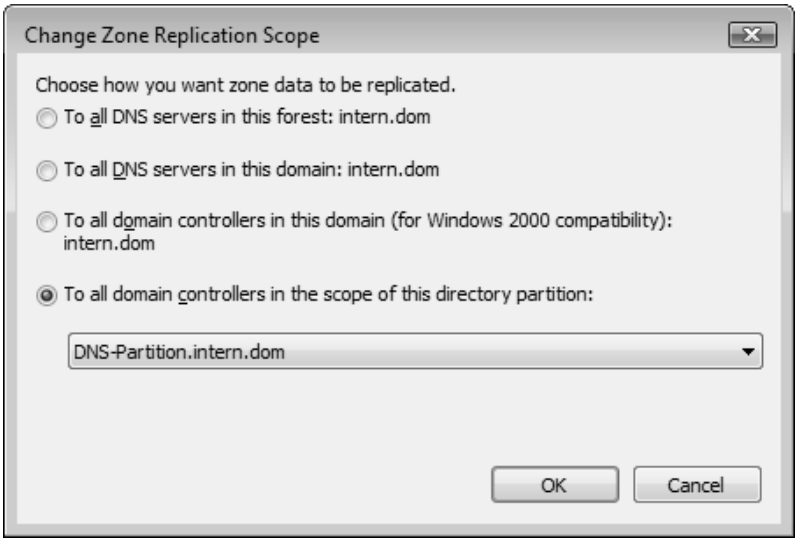


Рис. 11.5. Выбор области репликации зоны

Имя DNS-сервера можно не указывать, если команда выполняется непосредственно на этом сервере.)

Для перемещения зон в другой раздел каталога используется команда `dnscmd /ZoneChangeDirectoryPartition`. Зоны можно перемещать только *целиком*.

Установка режима динамического обновления

Режим динамической регистрации ресурсных записей в зоне задается параметром **Dynamic updates** (Динамическое обновление) на вкладке **General** (Общие) окна свойств зоны (см. рис. 11.3). Динамическое обновление выполняется при выборе опции **Nonsecure and secure** (Небезопасные и безопасные), однако в этом случае регистрация и обновление записей будут разрешены для любых клиентов, в том числе и неаутентифицированных в домене. Для активизации более строгого режима безопасного обновления необходимо выбрать значение **Secure only** (Только безопасные).

Управление разделами приложений

Связь между разделами приложений каталога Active Directory и службой DNS (и утилитой DnsCmd.exe) становится вполне понятной, если помнить о том, что в доменах на базе Windows Server 2003/Windows Server 2008 специальные разделы приложений могут использоваться для хранения DNS-зон, интегрированных в Active Directory.

Утилита DnsCmd помимо возможностей управления DNS-серверами предоставляет администратору возможность создания и удаления разделов приложений, а также позволяет назначать контроллеры домена хранителями реплик разделов приложений и удалять реплики (другим инструментом для выполнения этих операций является утилита NTDSutil.exe).

Работа с репликами разделов приложений

С помощью следующей команды раздел приложений можно создать на любом DNS-сервере, расположенном на контроллере домена, работающего под управлением Windows Server 2003/Windows Server 2008:

```
C:\>dnscmd /CreateDirectoryPartition DNS-Partition.intern.dom
DNS Server . created directory partition: DNS-Partition.intern.dom
Command completed successfully.
```

Имя раздела приложений произвольное, однако на DNS-сервере должна быть создана авторитетная зона, соответствующая родительскому домену (в нашем примере — intern.dom), иначе доступ к разделу будет невозможен. Если команда выполняется непосредственно на контроллере домена, где установлен DNS-сервер, то имя сервера указывать необязательно. Этот контроллер сразу же становится хранителем нового раздела приложений.

Увидеть, какие разделы приложений имеются на DNS-сервере, можно с помощью команды[1]:

```
C:\>dnscmd /EnumDirectoryPartitions
Enumerated directory partition list:

        Directory partition count = 3

 DNS-Partition.intern.dom                    Enlisted
 DomainDnsZones.intern.dom                   Enlisted Auto Domain
 ForestDnsZones.intern.dom                   Enlisted Auto Forest

Command completed successfully.
```

(В данном примере два последних раздела — стандартные разделы, используемые службой DNS. Они имеют соответствующие области репликации: в пределах домена и в рамках всего леса доменов.)

Для того чтобы сделать другой контроллер домена хранителем реплики раздела приложений, используется следующая команда:

```
C:\>dnscmd srv2.intern.dom /EnlistDirectoryPartition DNS-
Partition.intern.dom
DNS Server srv2.intern.dom enlisted directory partition: DNS-
Partition.intern.dom
Command completed successfully.
```

> ***Внимание!***
>
> В отличие от "универсальной" утилиты NTDSutil, с помощью утилиты DnsCmd можно работать только с теми контроллерами домена, где работает служба DNS.

После того как изменения области репликации раздела отобразятся в топологии репликации (между носителями реплик должны быть установлены или модифицированы соединения репликации — это автоматически делает сервис Knowledge Consistency Checker, KCC) на указанном контроллере домена появится реплика раздела. Это можно проверить с помощью команды `dnscmd`

[1] Также можно использовать утилиты Ldp.exe и NTDSutil.exe.

`/DirectoryPartitionInfo`, которую можно выполнять на любом DNS-сервере.

Следующая команда позволяет удалить реплику раздела приложений с некоторого контроллера домена:

```
C:\>dnscmd srv2.intern.dom /UnenlistDirectoryPartition DNS-
Partition.intern.dom

DNS Server srv2.intern.dom unenlisted directory partition: DNS-
Partition.intern.dom

Command completed successfully.
```

И, опять-таки, на фактическое удаление копии раздела с указанного контроллера потребуется некоторое время — пока сервис KCC не отследит изменения топологии репликации (или если не будет выполнена принудительная репликация).

Для удаления разделов используется команда `dnscmd /DeleteDirectoryPartition`. При этом нужно следить за тем, чтобы в разделе не хранились бы интегрированные зоны (т. е. сначала нужно удалить зоны в оснастке **DNS** или изменить тип хранения зон на обычный, в файле) — в противном случае содержимое зон будет утеряно.

Создание специальных разделов приложений для службы DNS

Если роль DNS Server (Сервер DNS) была добавлена на сервере раньше, чем этот сервер был повышен до контроллера домена, то стандартные разделы приложений ForestDnsZones.<*DNSимяЛеса*> и DomainDnsZones.<*DNSимяДомена*>, которые могут использоваться сервером DNS, на этом контроллере домена не создаются. В результате два этих раздела вообще могут отсутствовать в лесу доменов. Если принимается решение использовать зоны, интегрированные в Active Directory, и для них требуются соответствующие разделы приложений, то для их создания проще всего выполнить команду `dnscmd /CreateBuiltinDirectoryPartitions` с параметром `/Domain`, `/Forest` или `/AllDomains` — в зависимости от того, какая область репликации требуется. Например, для создания раздела ForestDnsZones.<*DNSимяЛеса*> необходима следующая команда:

```
C:\>dnscmd /CreateBuiltinDirectoryPartitions /Forest

DNS Server . completed operation successfully

Command completed successfully.
```

После репликации изменений каталога Active Directory и обновления топологии репликации все контроллеры в лесу доменов, на которых установлены DNS-серверы, станут хранителями реплики раздела ForestDnsZones.<*DNSимяЛеса*>. Аналогичную операцию можно выполнить и для разделов DomainDnsZones.<*DNSимяДомена*>. Можно создать раздел в конкретном домене, а с помощью параметра `/AllDomains` можно создать разделы для *всех* доменов леса, где установлены DNS-серверы.

Проверка конфигурации DNS

По окончании процесса установки службы DNS необходимо проверить работоспособность сервера. Следует убедиться в том, что DNS-сервер может обслуживать запросы к именам, относящимся к зонам прямого и обратного просмотра. Если сервер обеспечивает разрешение имен в домене, нужно также проверить возможность динамического обновления зон. Такие проверки могут потребоваться и в процессе эксплуатации службы DNS — в случае возникновения ошибок при разрешении имен.

Тестирование особенно важно, если "внешний" DNS-сервер (находящийся на удаленной площадке или, даже, в другой организации) используется для хранения авторитетных зон доменов. Гарантировать работоспособность службы DNS можно лишь после выполнения определенных *тестов*, поскольку иногда их результаты могут разойтись с мнением администратора о правильности сетевой конфигурации — в этом случае информация, полученная с помощью системных утилит, будет более достоверной.

Использование утилиты Nslookup

В первую очередь необходимо проверить способность сервера DNS обрабатывать запросы — т. е. осуществлять разрешение имен, относящихся к хранящимся на нем зонам. Такая проверка не будет лишней перед созданием нового домена или перед подключением клиента к домену.

Для проверки самого сервера используется следующая команда (введите ее на проверяемом компьютере-клиенте или сервере — создаваемом контроллере домена):

```
C:\>nslookup 192.168.0.2
```

`192.168.0.2` — IP-адрес сервера DNS, который указан как предпочитаемый сервер в свойствах TCP/IP на проверяемом компьютере.

Примерный результат выполнения команды показан ниже:

```
Server:  srv1.intern.dom
Address:  127.0.0.1

Name:    srv1.intern.dom
Address:  192.168.0.2
```

Здесь строка `Server` содержит имя сервера DNS, а строка `Name` показывает имя, полученное в результате разрешения, заданного в команде IP-адреса. В приведенном примере эти имена совпадают (поскольку мы запросили у сервера DNS его собственное имя), однако можно проверить разрешение любых IP-адресов, для которых на сервере DNS зарегистрированы соответствующие имена.

Нужно также проверить, как DNS-имена компьютеров разрешаются в IP-адреса. При подключении клиента к домену можно проверить имя домена (например, с помощью команды `nslookup intern.dom`), а также имя контроллера домена (для этих целей можно также использовать утилиту *NLtest.exe*).

Если полученный результат будет отличаться от ожидаемого или появятся сообщения об ошибках, подобные " can't find … : Non-existent domain" (не найдено… несуществующий домен), необходимо проверить все настройки протокола TCP/IP, наличие связи и зон прямого и обратного просмотра. Если, например, в ответе сервера DNS содержатся приведенные выше сообщения, сервер может функционировать нормально, однако зона обратного просмотра может отсутствовать или быть поврежденной.

> ***Примечание***
>
> В отличие от рассматриваемой далее утилиты DnsCmd.exe, команда Nslookup может использоваться вместе с DNS-серверами любых типов (и на любых платформах).

Использование утилиты DnsCmd

После проверки разрешения имен можно проверить свойства зон прямого и обратного просмотра, в том числе возможность динамического обновления. Для этих целей (помимо оснастки **DNS**) удобно использовать утилиту командной строки DnsCmd.exe. Утилиту можно запускать на любом компьюте-

ре, который имеет доступ к проверяемому серверу, где функционирует служба DNS. Эта утилита может выполнять все операции, необходимые для удаленного управления DNS на базе серверов Windows 2000 Server и выше.

> ***Примечание***
>
> Также для проверки конфигурации DNS можно использовать специализированные утилиты DCdiag.exe и NetDiag.exe.

Для перечисления зон используется команда `/enumzones`. (Если утилита запускается непосредственно на DNS-сервере, то его имя можно не указывать.) Пример выполнения этой команды приводится ниже:

```
C:\>dnscmd srv1.intern.dom /EnumZones

Enumerated zone list:

        Zone count = 6

 Zone name                      Type       Storage         Properties

 .                              Cache      AD-Domain
 _msdcs.intern.dom              Primary    AD-Forest       Secure
 0.168.192.in-addr.arpa         Primary    AD-Domain       Secure Rev
 intern.dom                     Primary    AD-Domain       Secure
 intern-new.dom                 Primary    AD-Legacy       Secure
 sub.intern.dom                 Primary    File


Command completed successfully.
```

В приведенном примере `srv1.intern.dom` — имя DNS-сервера под управлением Windows Server 2003 или Windows Server 2008 (в системах Windows 2000 перечисленные режимы хранения зон невозможны), зона `"."` соответствует кэшированным запросам, `intern.dom` — имя зоны и DNS-имя домена (`_msdcs.intern.dom` — служебная зона этого домена), а `0.168.192.in-addr.arpa` — зона обратного просмотра (об этом говорит параметр `Rev`) для частной сети 192.168.0.0 (маска 255.255.255.0; имена, адрес и маска зависят от конфигурации конкретной сети).

Обычные зоны (хранящиеся в файлах) помечаются как `File`, а зоны, реплицирующиеся на все контроллеры домена (хранящиеся в разделе доменных имен), отмечены как `AD-Legacy`. Зоны, хранящиеся в разделе приложений ForestDnsZones.<*DNSимяЛеса*>, помечаются как `AD-Forest`; а для раздела приложений DomainDnsZones.<*DNSимяДомена*> указывается `AD-Domain`. Если зона отмечена как `AD-Custom`, то она хранится в разделе приложений, созданном администратором.

Параметр `Update` (или `Secure` — для безопасных обновлений) указывает на то, что зона может обновляться динамически. Это свойство зоны можно также проверить с помощью следующей команды:

```
C:\>dnscmd srv1.intern.dom /ZoneInfo intern.dom AllowUpdate
Zone query result:
Dword:  1 (00000001)
Command completed successfully.
```

Значение `1` указывает на то, что зона динамическая, а значение `2` указывает на безопасное обновление зоны.

После создания контроллера домена (в особенности это касается первого контроллера в лесу или в новом дереве) обязательно проверьте регистрацию всех необходимых SRV-записей. SRV-записи можно проверять и с помощью утилиты DnsCmd, но все же самым лучшим средством для проверки контроллеров домена является утилита DCdiag.exe, которая — в том числе — эффективно обнаруживает ошибки в конфигурации DNS для указанного или локального компьютера. Например, если следующая команда не выводит никакой информации, то можно считать, что указанный контроллер работает без ошибок:

```
C:\>dcdiag /s:srv1.intern.dom /q
C:\>
```

Не следует пренебрегать проверкой DNS, особенно при работе в домене, поскольку многие проблемы клиентов и контроллеров домена могут быть вызваны неправильным разрешением DNS-имен.

Настройка клиентов DNS

В системах Windows 2000 и выше конфигурация клиентов DNS включает следующие параметры (два первых из них являются обязательными, значения остальных можно оставить стандартными или изменять только в случае необходимости):

- DNS-имя хоста, или компьютера (например, `srv1`) (см. рис. 4.14);
- IP-адреса предпочитаемого (preferred) и дополнительных (alternate) DNS-серверов, которые будут использоваться клиентом для разрешения DNS-имен;

- *основной DNS-суффикс* (primary DNS suffix), используемый для формирования полного (fully qualified) имени хоста (например, в полном имени `srv1.intern.com` суффиксом является "окончание" `intern.com`); DNS-суффикс можно также задавать индивидуально для каждого сетевого подключения. DNS-суффикс обязателен только при работе компьютеров в составе домена, он изменяется автоматически и вмешательство администратора обычно не требуется;
- разрешения на регистрацию в службе DNS полного имени клиента с учетом суффиксов DNS (основного суффикса и суффиксов подключений, если таковые имеются);
- очередность имен доменов, используемых при запросах в случае неполностью заданного имени компьютера (без суффиксов DNS).

> ***Внимание!***
>
> Не рекомендуется в качестве DNS-суффиксов (а также имен доменов Active Directory) использовать DNS-имена доменов первого уровня — имена, состоящие только из одной метки (например, `internal` или `local`). В этом случае возможны проблемы с динамическим обновлением записей на DNS-серверах. (Как правило, применяют имена доменов не ниже второго уровня.)

Имя хоста DNS (а также описание компьютера) задается при установке на компьютер операционной системы. (Это имя обычно соответствует NetBIOS-имени компьютера, длина которого не превышает 15 символов.) Впоследствии изменять имя хоста можно в окне **Computer Name/Domain Changes** (Изменение имени компьютера или домена) (см. рис. 4.14); там же можно задать основной DNS-суффикс компьютера, нажав кнопку **More** (Дополнительно). В специальном окне (рис. 11.6) отображается основной DNS-суффикс — обычно это имя того домена, в который входит данный компьютер (например, `intern.dom`). (По умолчанию (после установки системы) суффикс отсутствует.) После смены суффикса требуется перезагрузка системы.

Если компьютер подключается к домену Active Directory, основной DNS-суффикс формируется автоматически из имени домена после подключения и перезагрузки клиента. Смена суффикса автоматически происходит и при перемещении клиента из одного домена в другой.

> ***Внимание!***
>
> Обратите внимание на то, что флажок **Change primary DNS suffix when domain membership changes** (Сменить основной DNS-суффикс при смене

членства в домене) обычно (по умолчанию) установлен. Это особенно важно для серверов, роль которых повышается до контроллеров домена, и для компьютеров, подключаемых к домену. В противном случае контроллеры и члены домена не получат правильное полное имя и не смогут зарегистрировать его на предпочитаемом DNS-сервере.

Для управления основным DNS-суффиксом на компьютерах, работающих под управлением систем Windows 2000 и выше, можно также использовать групповую политику **Primary DNS Suffix** (узел **Computer Configuration** | **Administrative Templates** | **Network** | **DNS Client** (Конфигурация компьютера | Административные шаблоны | Сеть | Клиент DNS)). Если политика определяет некоторый суффикс, то локально заданное значение игнорируется.

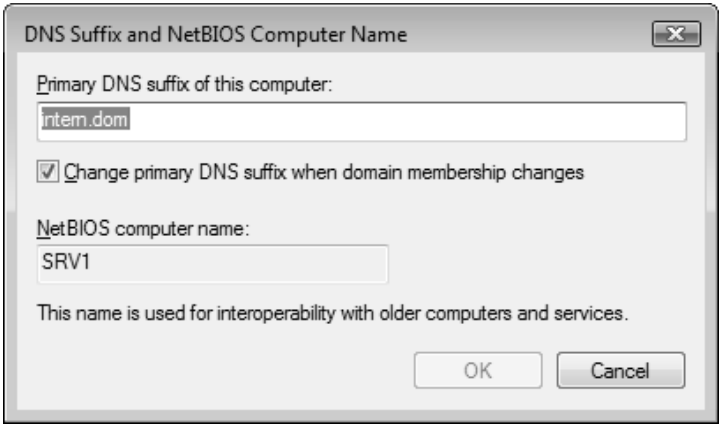


Рис. 11.6. Установка основного DNS-суффикса для компьютера

Если компьютер входит в состав домена Active Directory, то в качестве DNS-серверов следует указывать ***те же*** серверы, которые используются контроллерами домена. Ни в коем случае нельзя указывать адреса серверов провайдера Интернета. Для разрешения имен Интернета необходимо на предпочитаемых DNS-серверах настроить пересылку запросов (forwarding) на внешние DNS-серверы.

Все настройки клиентов значительно упрощаются, если все параметры TCP/IP получаются от сервера DHCP. Однако в случае каких-то проблем подключения к домену или разрешения имен следует внимательно проверять конфигурацию DNS непосредственно на компьютере клиента.

Сервер DHCP

Протокол *DHCP* (Dynamic Host Configuration Protocol, протокол динамической конфигурации хоста) предназначен для динамического выделения клиентам сети (хостам) различных параметров, используемых стеком TCP/IP. Этот протокол удобен при централизованном управлении сетевыми настройками на клиентских машинах.

В спецификации протокола DHCP определяются два участника обмена данными:

- *служба клиента DHCP*, используя широковещательные пакеты, находит DHCP-сервер и запрашивает у него параметры для настройки стека протоколов TCP/IP. DHCP-клиент так или иначе реализован во всех системах Windows;
- *служба сервера DHCP* обрабатывает клиентские запросы, осуществляя выдачу в аренду IP-адреса из некоторого диапазона. Каждый адрес выделяется на определенный срок, по окончании которого хост должен либо продлить срок аренды, либо освободить адрес. Все удовлетворенные запросы пользователя фиксируются службой сервера DHCP в собственной базе данных.

Подобное решение позволяет предотвратить выделение одного IP-адреса двум хостам. Одновременно с выдачей IP-адреса DHCP-сервер может также предоставить клиенту дополнительную информацию о настройках стека протоколов TCP/IP, такую как маска подсети, адрес шлюза по умолчанию и адреса серверов DNS и WINS и т. д.

Ниже перечислены основные возможности службы DHCP (серверов и клиентов) на базе серверов Windows Server 2008.

- **Интеграция с DNS.** DHCP-серверы и DHCP-клиенты могут осуществлять динамическую регистрацию выдаваемых IP-адресов базе данных DNS-сервера. При этом в базе данных DNS-сервера создаются ресурсные записи типа PTR (указатель) и A (адрес). Если клиент не может сам зарегистрировать свой адрес на DNS-сервере, то DHCP-сервер может выполнить регистрацию при выделении адреса.
- **Защита от подмены серверов.** Если используется компьютер — член домена, то одним из обязательных условий функционирования DHCP-сервера является требование его авторизации в каталоге Active Directory. При каждом запуске служба DHCP-сервера пытается обнаружить в ката-

логе запись, подтверждающую авторизацию службы. Если подобная запись не найдена, служба сервера не запускается.

- **Автоматическая настройка клиентов.** Служба DHCP-клиента в случае отсутствия в сети DHCP-сервера может выполнить необходимую настройку самостоятельно. Используя для работы временную конфигурацию стека протоколов TCP/IP, клиент продолжает попытки связаться с DHCP-сервером в фоновом режиме каждые 5 минут. При этом автоматическое назначение адреса всегда прозрачно для пользователей. Адреса для такого рода клиентов выбираются из диапазона частных сетевых адресов TCP/IP, которые не используются в Интернете *(см. далее)*.

- **Возможность задания альтернативной конфигурации DHCP-клиента.** Для DHCP-клиента можно задать альтернативную конфигурацию TCP/IP (используемую при отсутствии DHCP-сервера), что позволяет перемещать компьютер между различными подсетями.

- **Возможность резервного копирования базы данных DHCP.** В базе данных DHCP-сервера хранится информация о выданных клиентам IP-адресах, включая информацию о времени окончания аренды. Регистрация этой информации позволяет избежать повторного выделения уже выданных адресов. Повреждение этой базы данных может привести к тому, что работоспособность сети окажется под угрозой. Администратор может выполнять резервное копирование базы данных DHCP-сервера. Созданная резервная копия может использоваться впоследствии для восстановления работоспособности DHCP-сервера.

- **Выделение групповых адресов.** DHCP-сервер может выдавать клиентам *групповые* (multicast) адреса, которые используются приложениями, передающими данные множеству клиентов (например, программами для проведения видео- или аудиоконференций).

- **Специализированные опции и поддержка классов опций.** Администратор может создавать собственные классы DHCP (используемые для конфигурации клиентов) в соответствии с необходимостью. Механизм *пользовательских классов* позволяет применять DHCP в заказных приложениях для сетей масштаба предприятия. *Классы поставщиков* (vendor classes) могут использоваться для настройки различных функций сетевого аппаратного обеспечения.

Основные понятия службы DHCP

Протокол DHCP представляет собой развитие протокола BOOTP (RFC 951 и 1084), позволявшего динамически назначать IP-адреса (в дополнение к удаленной загрузке бездисковых станций). Служба DHCP предоставляет клиентам все параметры для настройки стека протоколов TCP/IP и дополнительную информацию для функционирования определенных сервисов. Перечислим основные понятия протокола DHCP.

- **Область действия** (scope). Под *областью действия* в DHCP понимается диапазон последовательных IP-адресов, выдаваемых по запросу DHCP-клиентам. Все клиенты одной области получают одинаковые параметры. Область должна быть определена прежде, чем DHCP-клиенты смогут использовать DHCP-сервер для получения IP-адресов и других параметров.

  На рис. 11.7 показан пример конфигурации DHCP-сервера, на котором созданы несколько областей действия для разных подсетей. Если область не активна, то она помечается соответствующим значком (стрелка вниз).

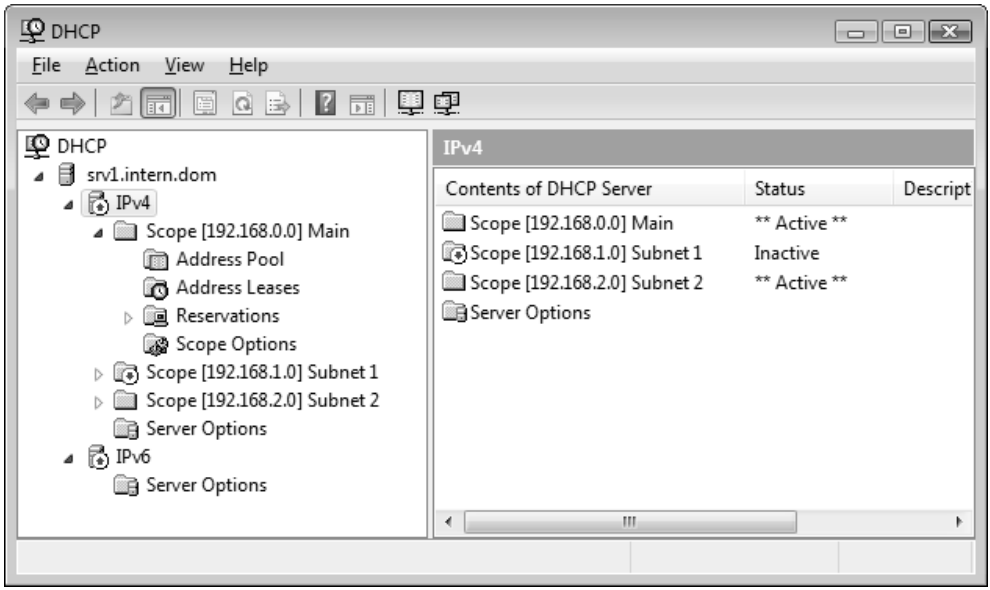


Рис. 11.7. Пример областей действия, созданных на DHCP-сервере

Если в сети для обеспечения отказоустойчивости имеется несколько DHCP-серверов, необходимо распределить имеющиеся диапазоны адресов между ними. Как правило, для каждой подсети должны быть доступны как минимум два DHCP-сервера, способных выдать необходимый IP-адрес. При этом рекомендуется создавать на этих серверах области с *одинаковыми* пулами адресов (например, 192.168.1.1–192.168.1.254), но с *разными* диапазонами исключения (к примеру, 192.168.1.1–192.168.1.127 для одного сервера и 192.168.1.128–192.168.1.254 — для другого).

Если DHCP-серверы находятся в одной подсети, то пул адресов можно делить пополам (как показано выше). Запросы от клиентов будут случайным образом распределяться между серверами.

- **Суперобласть** (superscope). Множество областей действия, объединенных в отдельный административный объект, представляет собой *суперобласть*. Суперобласти позволяют упростить развертывание службы DHCP в *мультисетях* (multinets). (Мультисеть — это сеть, в которой в пределах одного физического сегмента существуют две и более логических подсетей: например, одни клиенты сети могут относиться к подсети 192.168.1.0 (255.255.255.0), а другие — к подсети 192.168.2.0 (255.255.255.0).)

- **Пул адресов** (address pool). Диапазон разрешенных к сдаче в аренду адресов некоторой области DHCP называется *пулом адресов* (для этой области) (см. рис. 11.8).

- **Диапазон исключения** (exclusion range). *Диапазон исключения* — это последовательность IP-адресов в пределах области действия, которые должны быть исключены из предоставления службой DHCP (т. е. зарезервированы для каких-то целей).

  На рис. 11.8 показан пул адресов, заданных для некоторой области (Subnet 2): определен диапазон адресов от 192.168.2.1 до 192.168.2.254. При этом поддиапазон 192.168.2.204–192.168.2.254 исключен из пула адресов (он будет выделяться резервным DHCP-сервером), а поддиапазон 192.168.2.1–192.168.2.10 зарезервирован под адреса, которые будут задаваться статически.

- **Резервирование** (reservation). *Резервирование* позволяет на основе MAC-адреса (физического адреса сетевого адаптера) назначить клиенту постоянный IP-адрес и гарантировать, что указанное устройство в подсети будет всегда использовать один и тот же IP-адрес.

  Как видно на рис. 11.9, адрес 192.168.2.1 зарезервирован для конкретного компьютера (он будет выдаваться только компьютеру с заданным MAC-

адресом, например, 0013D45499CE[1]). Для резервирования можно определить собственные параметры DHCP: в этом примере компьютеру указывается адрес DNS-сервера.

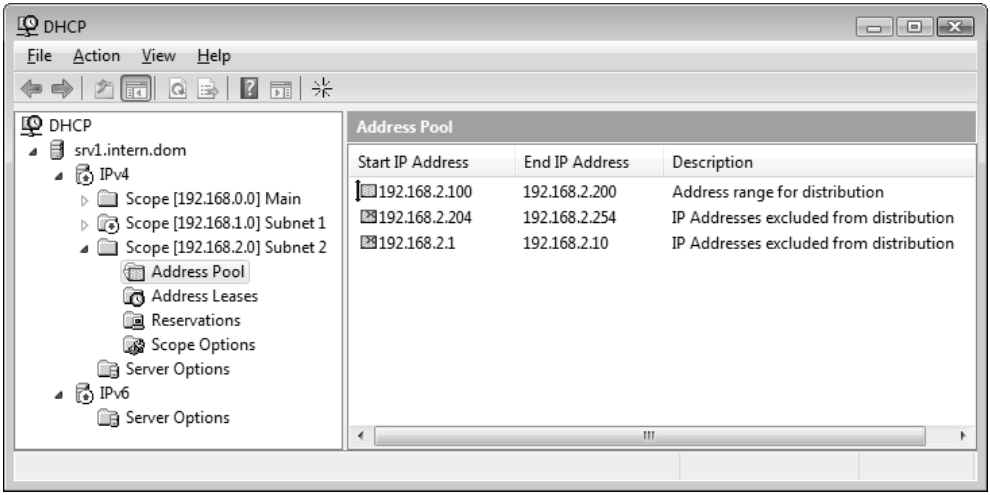


Рис. 11.8. Пример адресного пула для области действия

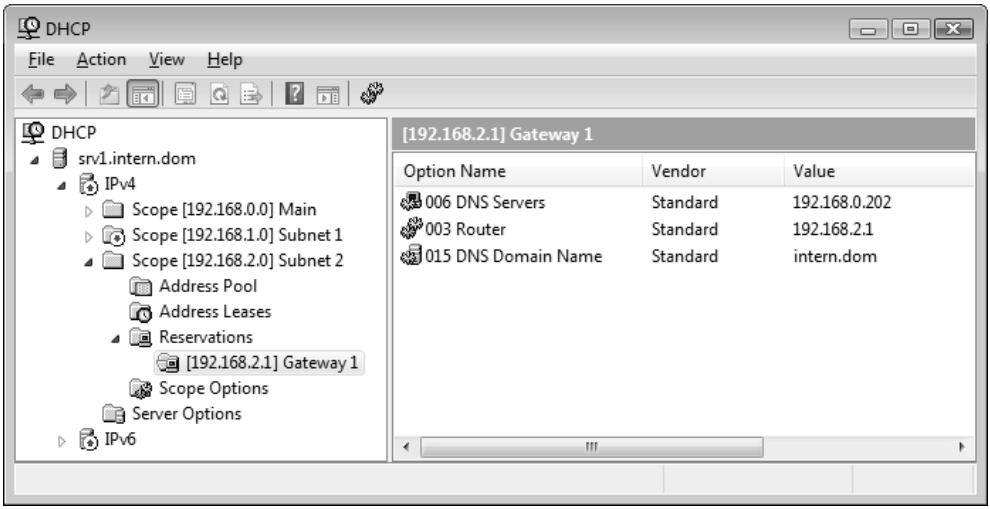


Рис. 11.9. Пример зарезервированного адреса

[1] MAC-адрес состоит из двенадцати символов в шестнадцатеричной нотации.

(Значки около названия параметра позволяют понять, на каком "уровне" эти значения были определены: в данном примере имя DNS-домена задано в параметрах DNCH-сервера, адрес шлюза в параметрах области действия, а адрес DNS-сервера — для конкретного объекта.)

- **Период аренды** (lease). Под *периодом аренды* понимается отрезок времени, в течение которого клиент может использовать выделенный IP-адрес. По истечении половины срока действия аренды клиент должен возобновить аренду, обратившись к серверу с повторным запросом. Следует помнить о том, что продолжительность периода аренды влияет на частоту обновления аренды (другими словами, на интенсивность обращений к серверу). Период аренды можно устанавливать индивидуально для каждой области действия (по умолчанию — 8 дней).

  На рис. 11.10 показан список адресов, выданных клиентам DHCP-сервера. Для каждого адреса указывается DNS- или NetBIOS-имя компьютера (для резервирования указывается его имя) и время окончания аренды. Если срок аренды истек и клиент не возобновил аренду, то около соответствующего адреса появляется значок  . Для зарезервированного адреса 192.168.0.10 срок аренды не указан (поскольку аренда бессрочная), однако видно, что этот клиент свой адрес получил (статус `active`).

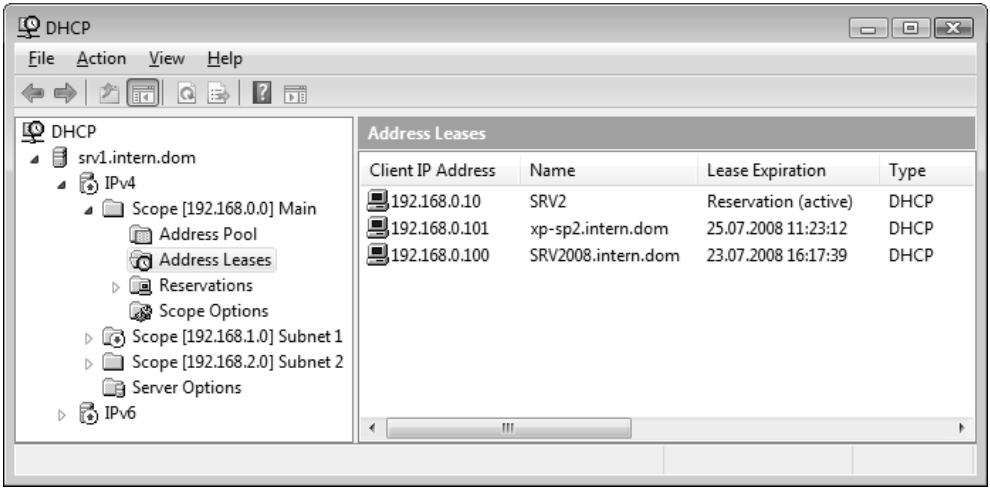


Рис. 11.10. Список выданных адресов со сроками истечения аренды

- **Параметр DHCP** (DHCP option). *Параметры DHCP* представляют собой сетевые настройки (в первую очередь параметры стека TCP/IP), которые DHCP-сервер может назначать клиентам одновременно с выделением IP-адреса. Сервер DHCP поддерживает более 60 параметров. В качестве примера можно привести следующие параметры: IP-адреса шлюза по умолчанию, адрес WINS-сервера или адрес DNS-сервера. Проверить полученные клиентом параметры можно с помощью утилиты *Ipconfig.exe*.

  Параметры DHCP могут быть определены индивидуально (для каждой области и резервирования) или глобально — для всех областей, заданных на DHCP-сервере. У каждой области действия имеется папка **Scope Options**, в которой задаются параметры для конкретной области (такие параметры имеют значок). На рис. 11.9 показан пример параметров DHCP для резервирования (конкретного клиента), где параметры определены на различных уровнях. Имеется папка **Server Options**, где определены параметры, используемые всеми областями (эти параметры отмечены значком), созданными на сервере[1]. Если некоторый параметр задан и для сервера, и для области, то действующим является значение, указанное в папке **Scope Options** для области.

- **Класс параметров DHCP** (DHCP option class). Клиентов DHCP-серверов можно объединять в так называемые *классы*. Класс рассматривается в данном случае, как некая логическая группа компьютеров, объединенных по некоторому признаку: например, к одному классу можно отнести компьютеры, имеющие доступ к Интернету, поскольку сетевые компоненты таких компьютеров могут потребовать дополнительной настройки. Параметры DHCP задаются индивидуально для каждого класса, и применяются, соответственно, только к тем клиентам, которые относятся к данному классу (производителей или пользователей). Классы могут определяться как для всего DHCP-сервера, так и на уровне отдельных областей или индивидуальных клиентов (резервирований). Для работы с классами нужно открыть окно параметров сервера или области действия и перейти на вкладку **Advanced** (Дополнительно).

Агент ретрансляции DHCP/BOOTP

Работа протоколов BOOTP и DHCP основана на механизмах широковещания. Обычно маршрутизаторы по умолчанию не ретранслируют широковещатель-

[1] Поэтому не нужно удивляться тому, что в папке **Scope Options** могут отображаться параметры, которые там и не определялись.

ные пакеты, что может создать трудности для получения IP-адресов клиентами, находящимися в другой подсети. Передача широковещательных рассылок DHCP/BOOTP может выполняться *агентом ретрансляции* (DHCP relay), который прослушивает подсети на наличие широковещательных сообщений DHCP/BOOTP и переадресовывает их на некоторый заданный DHCP-сервер.

Использование агентов ретрансляции избавляет от необходимости устанавливать сервер DHCP в каждом физическом сегменте сети. Агент не только обслуживает прямые локальные запросы клиента DHCP и перенаправляет их на удаленные DHCP-серверы, но также и возвращает ответы удаленных DHCP-серверов клиентам.

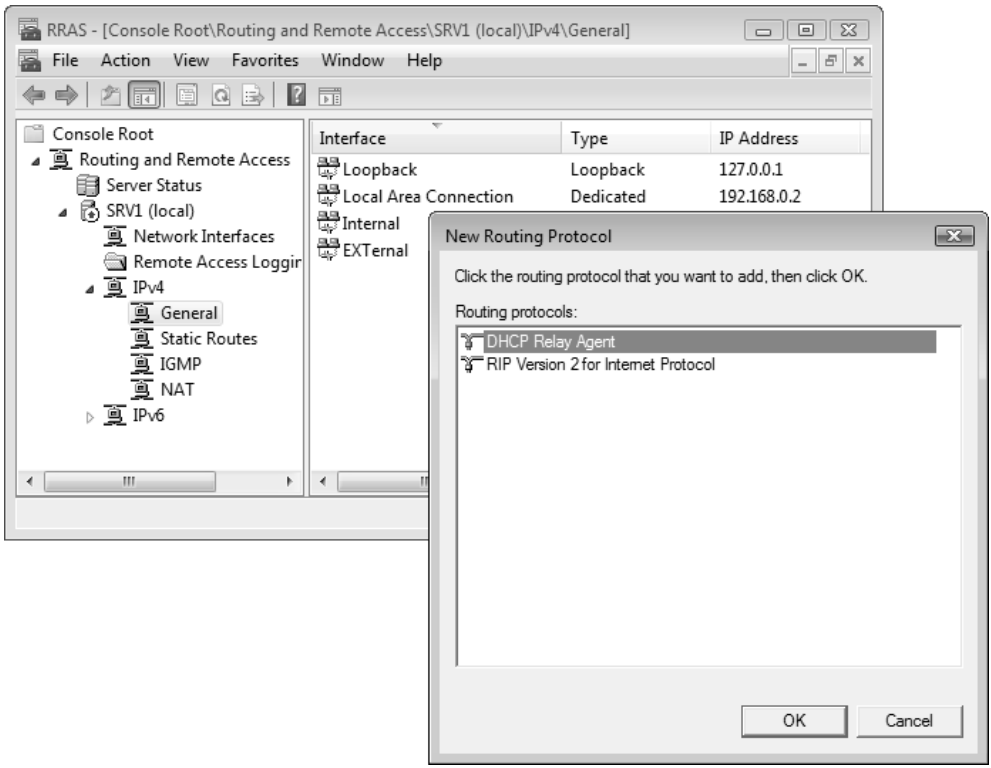


Рис. 11.11. Включение агента ретрансляции DHCP в окне оснастки **Routing and Remote Access**

Для установки агента ретрансляции необходимо использовать (предварительно включив и настроив) службу Routing and Remote Access (Маршрути-

зация и удаленный доступ). RRAS-сервер, выбранный для установки агента, должен быть настроен как маршрутизатор; на нем не должно быть службы DHCP. Для включения агента ретрансляции необходимо выполнить следующие действия:

1. В окне оснастки **Routing and Remote Access** (Маршрутизация и удаленный доступ) выбрать папку **IPv4** | **General** (IPv4 | Общие).
2. В контекстном меню папки выполнить команду **New Routing Protocol** (Новый протокол маршрутизации).
3. Выбрать в списке опцию **DHCP Relay Agent** (рис. 11.11).
4. Открыть контекстное меню появившегося узла **DHCP Relay Agent** и, выполнив команду **New Interface** (Новый интерфейс), выбрать сетевые интерфейсы, с которых агент ретрансляции будет принимать клиентские запросы.
5. Открыть контекстное меню узла **DHCP Relay Agent** и, выполнив команду **Properties** (Свойства), указать адрес (адреса) DHCP-серверов, которым будут переадресовываться запросы клиентов.

Установка и настройка DHCP-сервера

Для развертывания в сети службы DHCP необходимо, как минимум, выполнить следующие действия:

1. Установить DHCP-сервер.
2. Если DHCP-сервер установлен на компьютере — члене домена или на контроллере домена, то необходимо авторизовать его в каталоге Active Directory.
3. При установке DHCP-сервера на компьютере, имеющем несколько сетевых адаптеров, необходимо проверить привязку сервера к сетевым подключениям: должны быть включены только те сегменты, которым требуется поддержка DHCP.
4. Можно определить параметры DHCP для всего сервера — в этом случае они будут применяться и ко всем областям действия (если параметры не переопределяются на уровне области). Для этого в контекстном меню папки **Server Options** (Параметры сервера) необходимо выполнить команду **Configure Options** (Настроить параметры) и задать требуемые параметры.

5. Создать область действия и определить ее свойства (параметры DHCP).
6. Разрешить использование DHCP на клиентах в окне свойств протокола TCP/IP.

> ***Внимание!***
>
> Компьютер, выбранный на роль DHCP-сервера, должен иметь статический IP-адрес.

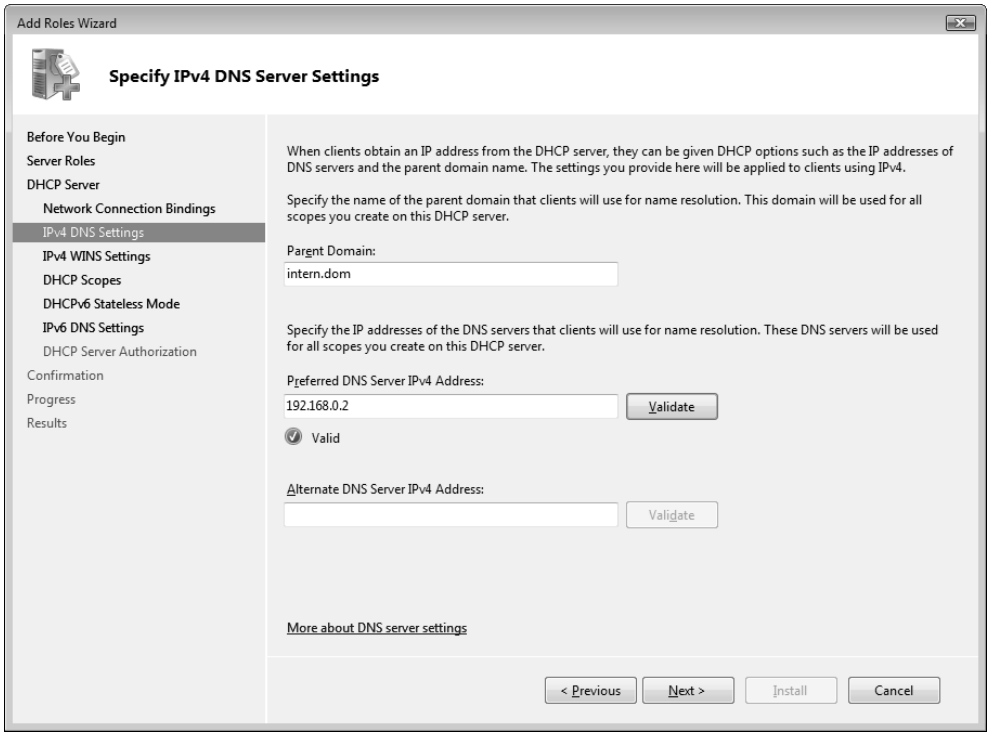


Рис. 11.12. Ввод имени обслуживаемого домена и адреса предпочитаемого DNS-сервера

Для установки DHCP-сервера нужно запустить оснастку **Server Manager** (Диспетчер сервера) и добавить серверу роль *DHCP Server* (DHCP-сервер). В процессе установки DHCP-сервера можно сразу указать, какие сетевые адаптеры, имеющие статические адреса, новый сервер будет обслуживать.

Дальнейшие шаги в работе мастера добавления роли будут следующими:

1. Предлагается ввести имя домена, в котором сервер будет работать, и адрес предпочитаемого DNS-сервера, используемого клиентами домена (рис. 11.12). С помощью кнопки **Validate** можно сразу проверить доступность и работоспособность указанного DNS-сервера. (На следующем шаге аналогичным образом можно задать имя WINS-сервера, если он используется в сети для совместимости со старыми клиентами.)
2. Далее мастер добавления роли предложит сразу создать область (области) действия для нового сервера (рис. 11.13). В окне параметров области (scope) необходимо указать ее имя и диапазон адресов. По необходимости можно задать адрес шлюза по умолчанию, типа подсети (он определяет длительность аренды адресов для проводных и беспроводных сетей) и необходимость немедленной активации области действия.

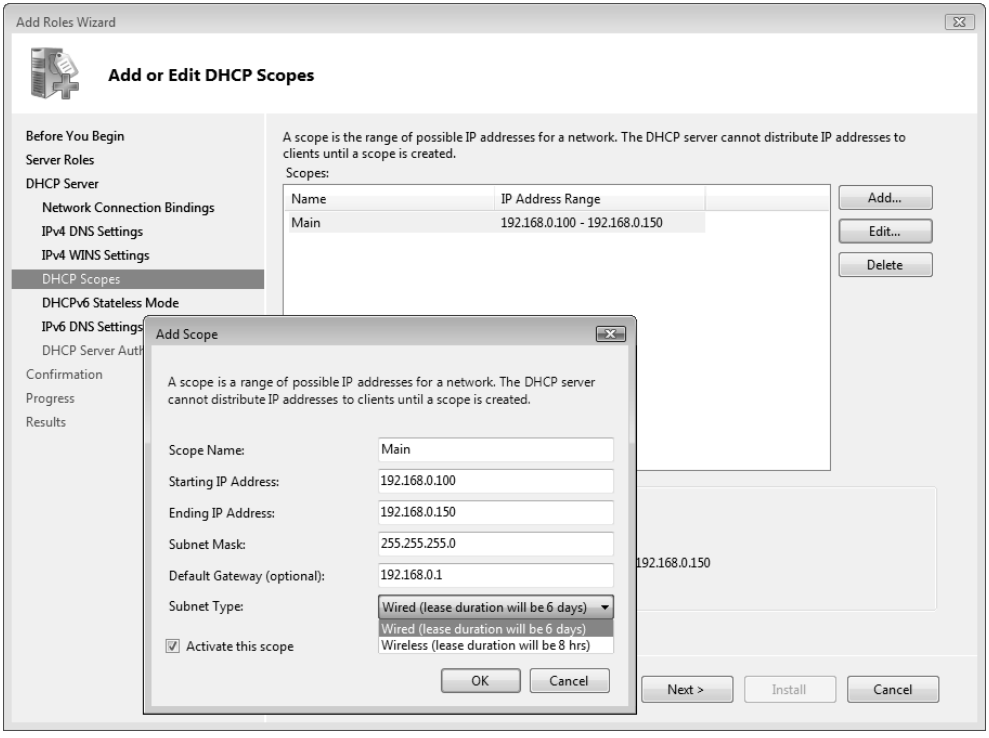


Рис. 11.13. Создание новых областей действия (scopes)

3. Если в сети отсутствуют клиенты с адресами IPv6, то на следующем шаге можно запретить режим *DHCPv6 stateless mode*.
4. Затем нужно указать учетную запись, которая будет использоваться для авторизации DHCP-сервера в службе доменов Active Directory, или отказаться от авторизации (в этом случае ее обязательно нужно будет выполнить потом, иначе сервер не будет обслуживать клиентов). Для автономного DHCP-сервера, работающего в сети без доменов, авторизация, в принципе, не требуется.
5. После проверки всех введенных параметров можно нажать кнопку **Install** (Установить) и начать установку DHCP-сервера.

После добавления роли проверить запуск DHCP-сервера можно при помощи оснастки **Services** (Службы) (имя сервиса — DHCPServer).

Если DHCP-клиент, посылающий широковещательные запросы на обнаружение DHCP-серверов, не получает никакого ответа (по причине недоступности или неработоспособности службы DHCP), то он может самостоятельно выбрать IP-адрес из служебного диапазона адресов (подсеть 169.254.0.0, маска 255.255.0.0), поскольку опция *автоконфигурирования* по умолчанию включена на всех клиентах, которым разрешено получение параметров от службы DHCP. После этого клиент будет каждые пять минут повторять попытки обнаружения DHCP-сервера и получения от него IP-адреса.

Для принудительного запуска процедуры получения адреса и обновления параметров можно использовать команду `ipconfig /renew`. В системах Windows XP и выше можно воспользоваться командой проверки и устранения сетевых неисправностей, которая имеется в контекстном меню значка сетевого подключения локальной сети (если этот значок отображается на панели задач).

Авторизация DHCP-сервера

Если DHCP-сервер установлен на компьютере, входящем в домен (это может быть рядовой сервер или контроллер домена), то, прежде чем сервер сможет приступить к работе, он обязательно должен быть авторизован в каталоге Active Directory. Только после этого клиенты смогут работать с данным сервером. При авторизации в контейнере CN=NetServices,CN=Services,CN=Configuration,DC=<*DNSИмяЛеса*> создается объект типа *dHCPClass*, соответствующий DHCP-серверу (имя объекта содержит IP-адрес DHCP-сервера).

Все обязанности по обнаружению неавторизованных DHCP-серверов возложены непосредственно на сами DHCP-серверы. Осуществляется это следующим образом. DHCP-сервер при запуске обращается к Active Directory, чтобы просмотреть список IP-адресов авторизованных серверов. Если сервер не обнаруживает свой адрес в этом списке, он останавливает свою работу. Если DHCP-сервер на базе Windows 2000 Server или Windows Server 2003 входит в домен Windows NT 4.0, то авторизация не выполняется.

Внимание!

Если DHCP-сервер установлен на автономном компьютере (не входящем в домен), то он сможет работать ***только*** в подсети, в которой отсутствуют авторизованные DHCP-серверы. В противном случае DHCP-сервер не запускается (хотя сервис DHCPServer и остается в рабочем состоянии и на сервере можно создавать и активизировать области действия).

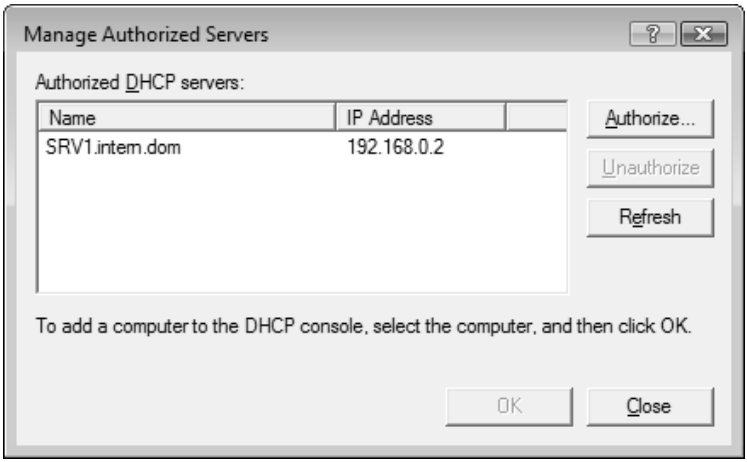


Рис. 11.14. Список авторизованных DHCP-серверов

Для авторизации DHCP-сервера (если это не было сделано при его установке) необходимо запустить оснастку **DHCP**, выбрать корневой объект DHCP и в контекстном меню выполнить команду **Manage authorized servers** (Управление авторизованными серверами). Система покажет список уже авторизованных DHCP-серверов (рис. 11.14). Для авторизации других серверов нужно нажать кнопку **Authorize** (Авторизовать) и указать IP-адрес DHCP-сервера. Команда **Authorize** (Авторизовать) имеется также в контекстном меню объ-

ектов, представляющих серверы в окне оснастки **DHCP**. Подключившись к конкретному серверу, можно его авторизовать при помощи этой команды.

Каждый работоспособный DHCP-сервер в окне оснастки **DHCP** должен быть отмечен значком  . Если отображается другой значок, то по какой-то причине DHCP-сервер не смог запуститься — либо он не авторизован, либо не работает сервис DHCPServer. В любом случае такая ситуация требует вмешательства администратора.

Создание области действия

Для создания области действия (scope) в окне оснастки **DHCP** используется мастер *New Scope Wizard* (Мастер создания области), который запускается из контекстного меню DHCP-сервера по команде **New Scope** (Создать область).

При создании области следует указать следующие ее характеристики:

1. Имя (обязательно) и описание (необязательно).
2. Начальный и конечный IP-адреса (пул адресов), а также маску подсети.
3. Диапазоны адресов исключений (необязательно).
4. Длительность аренды (по умолчанию — 8 часов).

Затем мастер предлагает сразу определить параметры DHCP для новой области (это можно сделать и позднее, однако в этом случае область сразу не активизируется):

1. Адрес (адреса) маршрутизатора (шлюза по умолчанию, опция "003 Router"). Шлюз по умолчанию (основной шлюз) используется для маршрутизации пакетов, адресованных хостам в других подсетях. Если хост не знает IP-адреса маршрутизатора, он не сможет взаимодействовать с подобными хостами.
2. Имя родительского домена (см. примечание ниже) (опция "015 DNS Domain Name") и адрес предпочитаемого DNS-сервера (опция "006 DNS Servers"). Можно указывать несколько DNS-серверов, что обеспечит разрешение имен в случае, если один из серверов выйдет из строя.
3. Адрес WINS-сервера для разрешения NetBIOS-имен (опция "044 WINS/NBNS Servers"). При указании WINS-сервера также автоматически задается опция "046 WINS/NBT Node Type" со значением 0x8 (гибридный узел, H-node).

Формально, ни один из перечисленных выше параметров не является обязательным для области (в этом случае будут действовать параметры, определенные для всего сервера). После создания область действия можно активизировать сразу или же отложить эту операцию на более позднее время. Активизация области действия приводит к тому, что IP-адреса, заданные пулом адресов, могут быть по требованию сданы в аренду клиентам.

Мастер создания области позволяет определить только стандартные параметры DHCP (DHCP Standard Options). Для определения дополнительных параметров необходимо в меню папки **Scope Options** (Параметры области), имеющейся у каждой области, выполнить команду **Configure Options** (Настроить параметры) и выбрать нужную вкладку параметров (основных или расширенных).

Настройка механизма динамической регистрации доменных имен

Если в сети используется служба DNS и в ней разрешена динамическая регистрация ресурсных записей, то необходимо правильно организовать взаимодействие служб DNS и DHCP. На рис. 11.15 показаны заданные по умолчанию параметры, определяющие действия DHCP-сервера в отношении службы DNS. Установленный флажок **Enable DNS dynamic updates according to the settings below** (Включить динамическое обновление DNS в соответствии с настройкой) разрешает DHCP-серверу регистрировать DNS-имена "от имени" клиентов.

Приведенные на рис. 11.15 установки подразумевают, что клиенты работают под управлением систем выше Windows 2000: эти клиенты по умолчанию самостоятельно регистрируют свою запись типа A, а запись типа PTR для них регистрирует DHCP-сервер (в соответствии со специальным запросом, формируемым клиентом). Если установить переключатель **Always dynamically update DNS A and PTR records** (Всегда динамически обновлять DNS A- и PTR-записи), то сервер будет регистрировать записи обоих типов, независимо от того, был ли соответствующий запрос от DHCP-клиента или не было.

Флажок **Discard A and PTR records when lease is deleted** (Удалять A- и PTR-записи при удалении аренды) должен быть установлен — в этом случае ресурсные записи будут удалены с DNS-сервера, если клиент не продлил аренду или если соответствующая строка была вручную удалена из списка выданных адресов (из папки **Address Leases**).

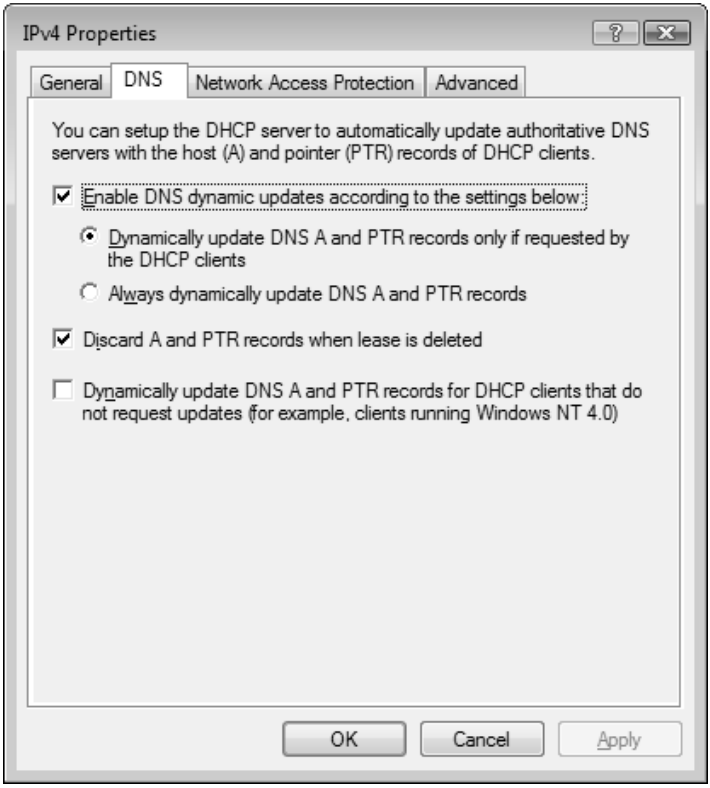


Рис. 11.15. Активизация режима автоматической регистрации доменных имен в базе данных DNS

Если какие-то клиенты сети не могут сами регистрировать и обновлять ресурсные записи в DNS, а также не могут посылать DHCP-серверу соответствующий запрос на выполнение этой операции, то для того, чтобы DHCP-сервер мог после выдачи адреса клиенту обновить записи в DNS, необходимо установить флажок **Dynamically update DNS A and PTR records for DHCP clients that do not request updates** (Динамически обновлять DNS A- и PTR-записи для DHCP-клиентов, не требующих обновления).

Сохранение конфигурации DHCP-сервера

Для сохранения всех параметров DHCP-сервера достаточно в окне оснастки DHCP открыть контекстное меню сервера и выполнить команду **Backup** (команда **Restore** служит, соответственно, для восстановления). По умолчанию данные

сохраняются в локальной папке, но можно указать и произвольное место для хранения конфигурации. Эту операцию можно выполнять на серверах, работающих под управлением Windows Server 2003, и рекомендуется ее делать при обновлении операционной системы до Windows Server 2008 — это позволит обезопасить информацию DHCP-сервера на случай неудачного обновления.

Утилита Netsh.exe позволяет сохранить конфигурацию DHCP-сервера в текстовом файле. Этот файл можно использовать для архивации или переноса данных на другой сервер (после редактирования параметров и изменения IP-адреса сервера) или для восстановления информации после переустановки системы.

Для сохранения данных DHCP-сервера используется следующая команда (в данном случае выходные сообщения утилиты Netsh переназначаются в файл):

```
netsh -f dhcp-show.txt > dhcp-config.txt
```

`dhcp-show.txt` — текстовый командный файл, содержащий директивы для утилиты Netsh:

```
interface
dhcp
server 192.168.0.2
dump
```

`192.168.0.2` — IP-адрес DHCP-сервера.

Для восстановления данных сервера полученный файл конфигурации нужно использовать в качестве командного файла:

```
netsh exec dhcp-config.txt
```

После выполнения указанной команды DHCP-сервер ***необходимо перезапустить*** (с помощью команды `net stop DHCPServer && net start DHCPServer` или оснасток **DHCP** или **Services** (Службы)).

Служба маршрутизации и удаленного доступа (RRAS)

Служба *Routing and Remote Access Service* (RRAS — Служба маршрутизации и удаленного доступа) обеспечивает две основные функции:

- **удаленный доступ** — связь удаленных клиентов с компьютером или локальной сетью при помощи коммутируемых или VPN-подключений (Virtual Private Network);

- **маршрутизацию** сетевых пакетов между локальными сетями или локальной сетью и внешней (например, Интернетом), включая преобразование сетевых адресов (NAT).

Пользователи устанавливают соединение с *сервером удаленного доступа*, реализованного на базе службы RRAS, при помощи клиентского программного обеспечения удаленного доступа, которое имеется в составе любой версии Windows. Сервер удаленного доступа (под которым мы в дальнейшем подразумеваем любой компьютер под управлением Windows Server 2008, на котором установлена служба маршрутизации и удаленного доступа) аутентифицирует как пользователей, так и сеансы связи удаленных маршрутизаторов. Все службы, доступные пользователям, работающим в локальной сети (включая доступ к совместно используемым файлам и принтерам, доступ к веб-серверам и серверам электронной почты), доступны также и пользователям, подключающимся удаленно (через сервер удаленного доступа).

Соединение с виртуальной частной сетью (или VPN-подключение) представляет собой защищенное соединение типа "точка-точка" через сеть общего пользования (например, Интернет) или большую корпоративную сеть. Поддержка сервером удаленного доступа механизма виртуальных частных сетей позволяет устанавливать безопасное соединение с корпоративной сетью через различные открытые сети (такие, например, как Интернет). Для эмуляции прямого соединения данные инкапсулируются специальным способом, т. е. снабжаются специальным заголовком, который предоставляет информацию, необходимую для маршрутизации, чтобы пакет мог достигнуть адресата. Получателем пакета является VPN-клиент либо VPN-сервер. Часть пути, по которому данные следуют в инкапсулированном виде, называется *туннелем*.

Для организации безопасной виртуальной частной сети (VPN) перед инкапсуляцией данные шифруются. Перехваченные по пути следования пакеты невозможно прочитать без ключей шифрования. Участок VPN-соединения, на котором данные передаются в зашифрованном виде, и называется, собственно, виртуальной частной сетью. Сервер удаленного доступа в случае использования механизма VPN выступает в качестве посредника, осуществляя обмен данными между клиентом VPN и корпоративной сетью. При этом сервер удаленного доступа осуществляет все необходимые преобразования данных (шифрование/дешифрование). Для этого используются специальные *протоколы туннелирования* (tunneling protocols). VPN-клиент и VPN-сервер должны использовать один и тот же протокол туннелирования, чтобы создать VPN-соединение. В службе удаленного доступа в Windows Server 2008 реализована поддержка протоколов туннелирования PPTP и L2TP.

Возможности службы RRAS в Windows Server 2008

Перечислим основные возможности службы маршрутизации и удаленного доступа, реализованные в Windows Server 2008.

- **Поддержка IPv6**. Включает в себя PPPv6 (передача трафика IPv6 через PPP-подключения или подключение на базе PPPoE (PPP over Ethernet)), VPN-туннели, L2TP поверх IPv6, агента ретрансляции DHCPv6 и RADIUS поверх транспорта IPv6.
- **Протокол туннелирования SSTP** (Secure Socket Tunneling Protocol). Новый вид туннеля виртуальной частной сети (VPN), обеспечивающий прохождение трафика через брандмауэры, блокирующие трафик PPTP и L2TP/IPsec. В этом случае применяется инкапсуляция трафика PPP поверх канала SSL или протокола HTTPS (TCP-порт 443) и поддерживаются надежные методы шифрования, такие как EAP-TLS.
- **Поддержка 128-разрядного алгоритма шифрования RC4 для протокола PPTP**.
- **Использование механизма Network Access Protection (NAP — Защита доступа к сети) для VPN-подключений**, выполняемых клиентами на базе Windows Vista и Windows Server 2008. Доступ к сети клиентов, не отвечающих требованиям установленной политики, может быть ограничен.
- **Интеграция механизма преобразования сетевых адресов (NAT) со встроенным брандмауэром Windows.** Реализованный в Windows Server 2008 встроенный брандмауэр может быть использован для фильтрации пакетов, обрабатываемых транслятором сетевых адресов.
- **Поддержка механизма предварительных ключей для аутентификации в случае использования протоколов L2TP/IPSec.** *Предварительным ключом* (pre-shared key) называется последовательность символов, известная заранее клиенту и серверу удаленного доступа. Этот ключ используется для аутентификации участников соединения удаленного доступа в ситуации, когда применяются защищенные протоколы L2TP/IPSec. Использование механизма предварительных ключей позволяет администратору отказаться от развертывания инфраструктуры открытых ключей (Public Key Infrastructure, PKI).
- **Поддержка механизмом преобразования сетевых адресов (NAT) защищенных соединений, осуществляемых с применением протоколов L2TP/IPSec.** Можно использовать механизм преобразования сетевых ад-

ресов для организации виртуальных частных сетей. Фактически речь идет о том, что соединение с виртуальной частной сетью может быть создано через интерфейс NAT.

- **Интеграция с Active Directory.** Сервер удаленного доступа на базе Windows Server 2008, являющийся частью домена Windows и зарегистрированный в каталоге, может обращаться к параметрам настройки удаленного доступа пользователя (например, к разрешениям удаленного доступа и параметрам ответного вызова), которые хранятся в Active Directory. После регистрации сервера удаленного доступа в Active Directory им можно управлять и отслеживать его состояние при помощи стандартных инструментов.
- **Поддержка протокола аутентификации MS-CHAP версии 2.** Протокол проверки подлинности запроса-подтверждения (Microsoft Challenge Handshake Authentication Protocol, MS-CHAP v2) предназначен для аутентификации участников соединения и создания ключей шифрования непосредственно во время установления соединения удаленного доступа. Протокол MS-CHAP v2 может быть также использован для аутентификации участников соединения при построении виртуальных частных сетей.
- **Поддержка протокола аутентификации EAP.** Расширяемый протокол аутентификации EAP (Extensible Authentication Protocol) позволяет использовать новые методы проверки подлинности участников подключения удаленного доступа, включая реализацию защиты, основанную на смарт-картах. Интерфейс EAP позволяет подключать модули проверки подлинности сторонних производителей.
- **Механизм политик удаленного доступа.** Под политикой удаленного доступа понимается набор условий и параметров настройки соединения, предоставляющих сетевым администраторам большую гибкость по установке и настройке разрешений удаленного доступа и атрибутов соединений.
- **Поддержка широковещательных адресов IP** (IP multicast). Используя механизм IGMP router and proxy версии 2 (маршрутизатор и посредник IGMP), сервер удаленного доступа может поддерживать обмен групповым IP-трафиком между клиентами удаленного доступа и Интернетом или корпоративной сетью.

Примечание

Рекомендуем также обратиться к *разд. "Сетевые средства, удаленные из Windows Server 2008" главы 8.* Протокол распределения полосы пропуска-

ния BAP (Bandwidth Allocation Protocol), а также протокол управления распределением полосы пропускания BACP (Bandwidth Allocation Control Protocol) исключены из состава Windows Vista, а в Windows Server 2008 присутствуют, но в выключенном состоянии.

Начальное конфигурирование службы RRAS

Служба RRAS по умолчанию устанавливается на каждый компьютер, работающий под управлением Windows Server 2008, но находится в отключенном состоянии (сервис RemoteAccess). Перед началом ее конфигурирования (для использования в ***любом режиме***) необходимо на сервере) с помощью оснастки **Server Manager** (Диспетчер сервера) добавить роль *Network Policy and Access Services* (Службы политики сети и доступа. Можно выбрать и отдельные службы роли сервера (рис. 11.16). После установки роли службу RRAS обязательно нужно настроить.

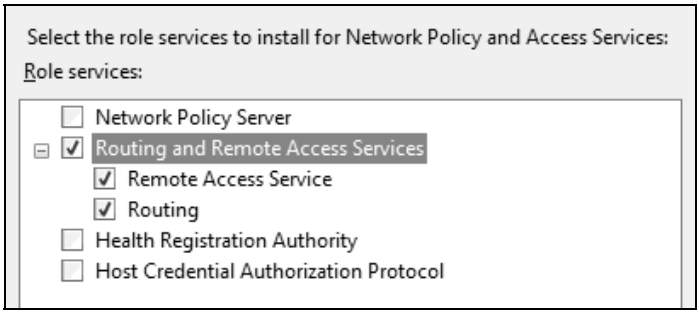


Рис. 11.16. Выбор компонентов службы RRAS

Основное средство управления службой RRAS — оснастка **Routing and Remote Access** (Маршрутизация и удаленный доступ, rrasmgmt.msc) — может запускаться автономно, из меню **Administrative Tools** (Администрирование). Также она входит в состав оснастки **Computer Management** (Управление компьютером).

Начальная настройка службы маршрутизации и удаленного доступа осуществляется при помощи мастера *Routing and Remote Access Server Setup Wizard* (Мастер настройки сервера маршрутизации и удаленного доступа). Для запуска этого мастера необходимо в окне административной оснастки выбрать имя конфигурируемого сервера и в контекстном меню выбрать опцию

Configure and Enable Routing and Remote Access (Настроить и включить маршрутизацию и удаленный доступ). При помощи указанного мастера администратор может сконфигурировать сервер в качестве маршрутизатора и/или сервера удаленного доступа, а также активизировать на нем механизм преобразования сетевых адресов.

Первым шагом будет выбор основной роли, которую будет выполнять сервер с установленной службой RRAS (рис. 11.17).

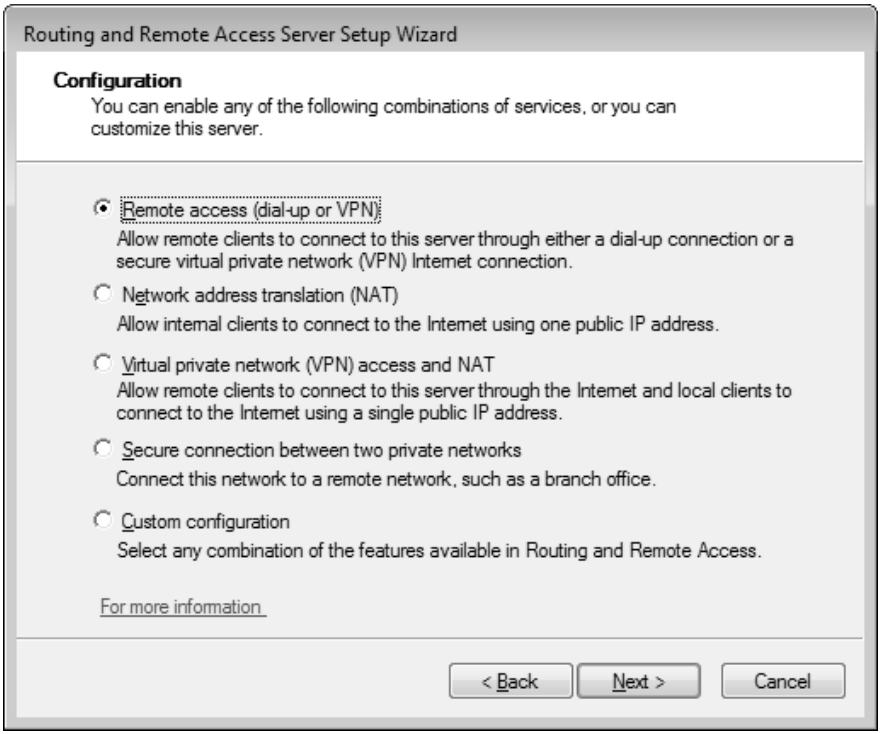


Рис. 11.17. Выбор начальной конфигурации сервера

Имеются следующие варианты начальной настройки сервера RRAS:

- **Remote access (dial-up or VPN)** (Удаленный доступ (VPN или модем)) — установка сервера удаленного доступа, позволяющего удаленным клиентам подключаться к серверу через коммутируемые и VPN-подключения;
- **Network address translation (NAT)** (Преобразование сетевых адресов NAT) — преобразование внутренних адресов во внешние; стандартный

вариант для подключения пользователей локальной сети к Интернету через одно подключение;

- **Virtual private network (VPN) access and NAT** (Доступ к виртуальной частной сети (VPN) и NAT) — совмещение двух указанных выше возможностей;
- **Secure connection between two private networks** (Безопасное соединение между двумя частными сетями) — использование сервера в качестве маршрутизатора;
- **Custom configuration** (Особая конфигурация) — любая комбинация перечисленных возможностей; можно вручную выбирать устанавливаемые службы.

После того как выполнено начальное конфигурирование, при дальнейшей работе параметры настройки можно изменять в окне свойств сервера — добавлять или удалять режимы работы сервера RRAS.

> ***Примечание***
>
> Для выключения RRAS-сервера и удаления конфигурации служит опция **Disable Routing and Remote Access** (Отключить маршрутизацию и удаленный доступ).

Удаленный доступ

Под удаленным доступом понимается решение, основанное на маршрутизации обращений подключающегося удаленного клиента в локальную сеть корпорации. Все приложения, посредством которых происходит доступ к ресурсам корпоративной сети, функционируют непосредственно на стороне клиента.

Следует также упомянуть про другую возможность организации доступа к ресурсам корпоративной сети — *дистанционное управление* (remote control). Под дистанционным управлением понимается решение, основанное на использовании удаленными пользователями программных и вычислительных ресурсов сервера. При этом также возможен доступ к ресурсам корпоративной сети. Однако все приложения, посредством которых этот доступ осуществляется, выполняются не на клиенте, а на сервере. Клиенту передаются только образы экрана. Данное решение реализуется при помощи служб терминалов (terminal services) *(см. главу 10)* или удаленного доступа к рабочему столу *(см. главу 4)*.

Использование сервера удаленного доступа для обслуживания VPN-подключений

Сервер удаленного доступа под управлением Windows Server 2008 может обслуживать VPN-подключения, выступая в качестве VPN-сервера. Необходимо понимать, что фактически речь идет о все том же удаленном доступе к ресурсам корпоративной сети. Однако, в отличие от обычного удаленного доступа, взаимодействие клиента и сервера осуществляется по защищенному каналу, который реализуется за счет использования специальных *протоколов туннелирования*. Применение механизма виртуальных частных сетей (VPN) оправдано в ситуации, когда нельзя исключать риск перехвата конфиденциальных данных (например, если взаимодействие с удаленным клиентом реализуется через открытые общественные сети).

Если администратор планирует использовать сервер удаленного доступа для обслуживания VPN-подключений, он должен определить, какой из протоколов туннелирования будет применяться для создания защищенного канала. Администратор должен выбрать между протоколом PPTP и протоколом L2TP. Протокол PPTP поддерживается всеми клиентами Microsoft (в том числе старыми версиями Windows). Минусом этого протокола является отсутствие механизмов, гарантирующих целостность передаваемых данных и подлинность участников соединения. Протокол L2TP свободен от этих недостатков. В целом он является более предпочтительным вариантом, нежели протокол PPTP. Протокол L2TP базируется на механизмах протокола IPSec, поддержка которого реализована в операционных системах Windows 2000 и выше.

Если администратором в качестве средства создания защищенного канала был выбран протокол туннелирования L2TP, он должен определить, как именно будет осуществляться взаимная аутентификация участников VPN-соединения. Протокол IPSec, поверх которого функционирует протокол туннелирования L2TP, поддерживает два способа аутентификации участников соединения: *цифровые сертификаты* (речь идет о цифровых сертификатах, назначаемых компьютерам) и *предварительный ключ* (pre-shared key). С точки зрения безопасности более надежным способом является использование цифровых сертификатов.

Установка сервера удаленного доступа

Перед выполнением процедуры конфигурирования сервера удаленного доступа необходимо определиться со следующими вопросами:

- **распределение IP-адресов между клиентами удаленного доступа.** Существуют два варианта: использование в сети DHCP-сервера и получение

IP-адреса непосредственно от сервера удаленного доступа из некоторого статического пула, определенного администратором;

- **максимальное количество входящих подключений.** От этого зависит то, сколько модемов, ориентированных на подключение удаленных пользователей, потребуется подключить к серверу удаленного доступа;
- **модель конфигурирования параметров удаленного подключения будет использоваться.** Параметры удаленного подключения могут задаваться на уровне учетных записей отдельных пользователей или определяться политикой удаленного доступа. На этапе развертывания сервера удаленного доступа должны быть произведены все необходимые настройки учетных записей пользователей, а также определены параметры политик удаленного доступа;

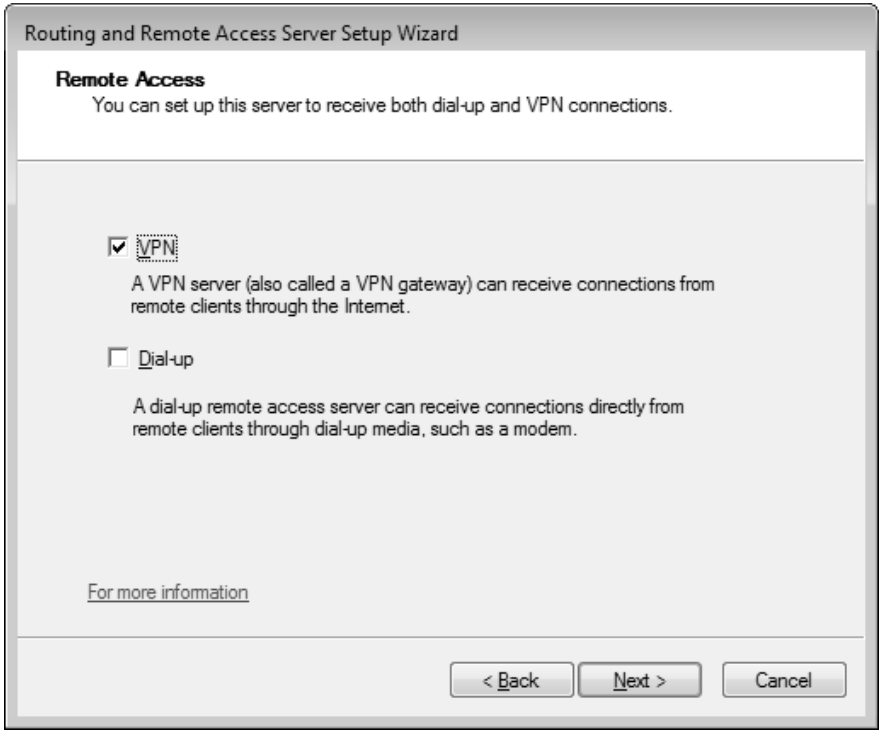


Рис. 11.18. Определение типов подключений, которые будут разрешены на конфигурируемом сервере удаленного доступа

- **схема аутентификации.** Имеются два варианта — либо аутентификация выполняется непосредственно сервером удаленного доступа, либо используются средства протокола RADIUS. Использование протокола RADIUS оправдано в ситуации, когда в сети имеется несколько серверов удаленного доступа. В этом случае администратор имеет возможность реализовать централизованное управление процессом аутентификации пользователей.

Рассмотрим процедуру настройки сервера удаленного доступа на примере установки VPN-сервера (настройка сервера, обслуживающего коммутируемые подключения, выполняется аналогичным образом). После запуска мастера начального конфигурирования необходимо выбрать опцию **Remote access (dial-up or VPN)** (Удаленный доступ (VPN или модем)).

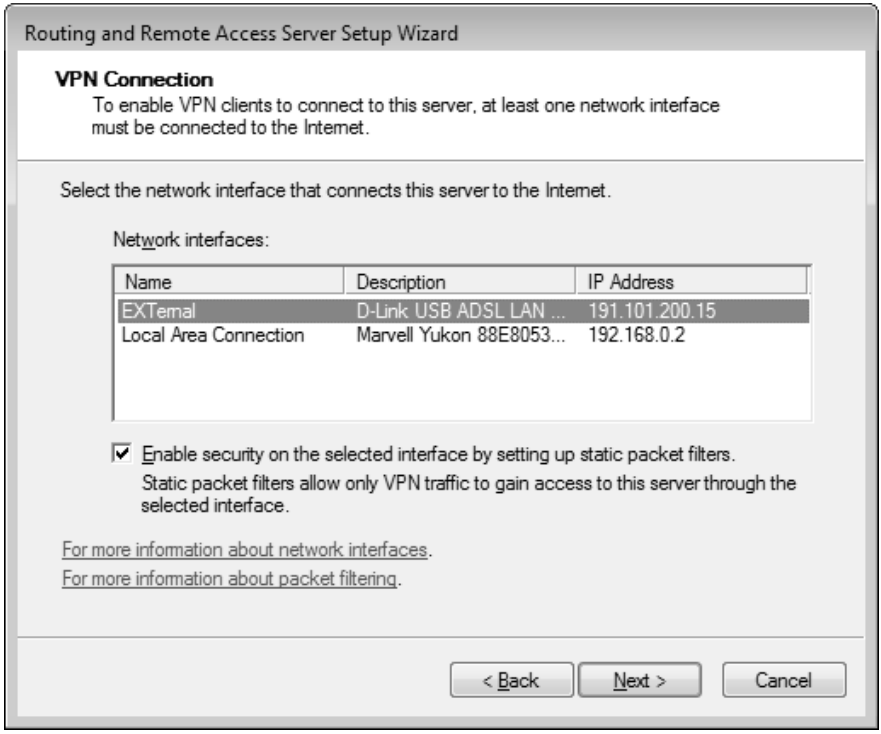


Рис. 11.19. Выбор внешнего интерфейса и разрешение включения статических фильтров

На странице *Remote Access* (Удаленный доступ) (рис. 11.18) необходимо уточнить функции, которые будет выполнять конфигурируемый сервер. Если сервер должен обслуживать обычные коммутируемые подключения удаленных пользователей, следует установить флажок **Dial-up** (Удаленный доступ). Флажок **VPN** (Доступ к виртуальной частной сети (VPN)) нужно устанавливать только в том случае, если сервер должен обслуживать VPN-подключения внешних пользователей (подключающихся, например, через Интернет).

Затем следует выбрать интерфейс, подключенный к внешней сети (Интернету) (рис. 11.19), и разрешить фильтрацию пакетов. По умолчанию устанавливаются статические фильтры, пропускающие через выбранный интерфейс только трафик VPN-подключений.

Рис. 11.20. Указание способа предоставления клиентам IP-адреса

Далее требуется определить способ предоставления подключающимся клиентам IP-адресов, необходимых для работы в корпоративной сети (рис. 11.20). По умолчанию адреса выдаются автоматически сервером уда-

ленного доступа или DHCP-сервером. Выбор опции **Automatically** (Автоматически) означает использование DHCP-сервера. Если требуется выделять адреса из статического пула, следует выбрать опцию **From a specified range of addresses** (Из заданного диапазона адресов). В последнем случае администратор должен будет задать этот диапазон на следующей странице мастера.

И наконец, на последней странице мастера (рис. 11.21) необходимо ответить на запрос об использовании сервера RADIUS — т. е. выбрать схему аутентификации пользователей. Если аутентификация будет выполняться непосредственно сервером удаленного доступа, необходимо выбрать опцию **No, use Routing and Remote Access to authenticate connection requests** (Нет, использовать маршрутизацию и удаленный доступ для проверки подлинности запросов на подключение). В случае использования для аутентификации сервера RADIUS необходимо выбрать переключатель **Yes, set up this server to work with a RADIUS server** (Да, настроить данный сервер для работы с RADIUS-сервером).

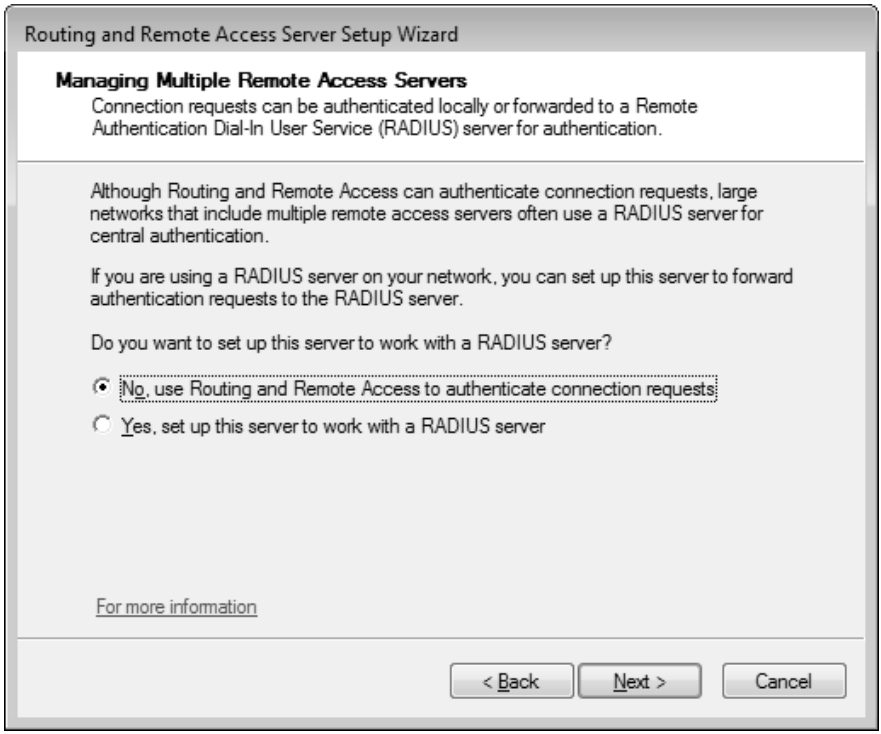


Рис. 11.21. Выбор способа аутентификации клиентов удаленного доступа

По окончании своей работы мастер запустит службу маршрутизации и удаленного доступа. Начиная с этого момента, сервер удаленного доступа готов обслуживать подключения удаленных пользователей.

В простейшем случае используется обычная аутентификация на сервере с указанием локальных учетных записей, которые клиенты указывают при подключении к данному серверу.

Информацию о сеансах удаленного доступа к серверу можно просматривать в папке **Remote Access Clients** (Клиенты удаленного доступа) (рис. 11.22). Один и тот же пользователь может создавать несколько подключений и при этом входить на сервер под одним именем. В этом окне сеансы можно принудительно отключать.

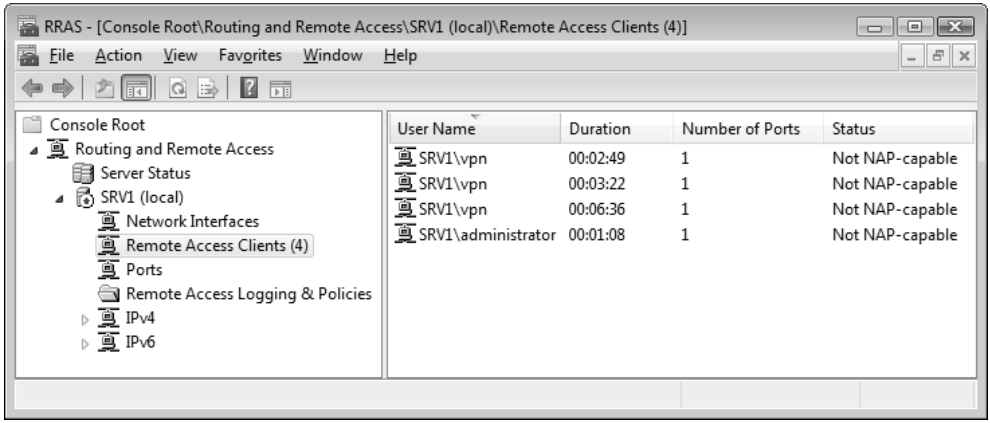


Рис. 11.22. Просмотр сеансов подключения к серверу удаленного доступа

Механизмы управления конфигурацией удаленного подключения

Настройка параметров удаленного доступа для конкретного пользователя может выполняться двумя способами: либо при помощи специальных атрибутов учетной записи пользователя, либо посредством политик удаленного доступа.

Специальные параметры учетной записи пользователя

Вся информация о пользователях размещается в каталоге Active Directory в виде объектов, ассоциированных с учетными записями, или в локальной базе

учетных записей. При этом с каждым подобным объектом связан определенный набор атрибутов. В том числе имеются специальные атрибуты, позволяющие задать конфигурацию удаленного доступа для конкретного пользователя.

Настройка параметров учетной записи пользователя, используемых для конфигурирования удаленного доступа, выполняется на вкладке **Dial-in** (Входящие звонки) в окне свойств объекта, ассоциированного с учетной записью пользователя, в оснастке **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры). В случае автономного сервера удаленного доступа для конфигурирования аналогичных параметров учетной записи используется оснастка **Local Users and Groups** (Локальные пользователи и группы).

Политики удаленного доступа

Для управления удаленным доступом могут использоваться *политики удаленного доступа* (remote access policy). Под политикой удаленного доступа понимается набор условий и параметров соединения, которые предоставляют сетевому администратору больше возможностей в настройке разрешений удаленного доступа и атрибутов соединения. Фактически политика удаленного доступа представляет собой совокупность параметров, определяющих конфигурацию сетевого подключения.

При помощи политики удаленного доступа можно предоставлять разрешения удаленного доступа в зависимости от времени дня, дня недели, группы объектов, к которой принадлежит объект, ассоциированный с учетной записью звонящего пользователя, типа требуемого подключения (коммутируемое или VPN-подключение). Можно определить параметры настройки подключения, которые ограничивают максимальное время сеанса связи, тип аутентификации и шифрования, а также фильтрацию IP-пакетов.

Важно помнить, что при использовании политик удаленного доступа соединение разрешается, только если параметры настройки соединения соответствуют по крайней мере одной из политик удаленного доступа (в соответствии со свойствами учетной записи пользователя и конфигурацией политики удаленного доступа). Если параметры настройки при попытке соединения не соответствуют ни одной из политик удаленного доступа, попытка соединения отклоняется независимо от свойств учетной записи пользователя. На серверах удаленного доступа эти политики конфигурируются с помощью оснастки **Routing and Remote Access** (Маршрутизация и удаленный доступ).

Преобразование сетевых адресов (NAT)

Механизм *преобразования сетевых адресов* (Network Address Translation, NAT) реализует преобразование IP-адресов и номеров портов пакетов TCP и датаграмм UDP, которыми обмениваются локальная и внешняя (такая как Интернет) сети. Наличие этого механизма позволяет организовать взаимодействие локальной сети с Интернетом простыми средствами, без привлечения специализированного программного обеспечения.

> ***Примечание***
>
> Преобразователь адресов в первую очередь разработан для подключения к открытым сетям (таким как Интернет) небольших локальных сетей. Этот механизм не предназначен для соединения воедино нескольких разрозненных локальных сетей или подключения нескольких локальных сетей филиалов к общекорпоративной сети.
>
> В качестве альтернативы механизму преобразования сетевых адресов в небольших сетях можно использовать функцию Internet Connection Sharing, ICS (Общий доступ к подключению к Интернету) — *см. главу 8*.

Компоненты NAT

Механизм преобразования сетевых адресов включает в себя следующие элементы:

- **компонент преобразования.** В этом качестве рассматривается сервер, выступающий в качестве *транслятора сетевых адресов* (NAT). Именно транслятор сетевых адресов является тем компонентом, который собственно и выполняет преобразование IP-адресов и номера портов пакетов TCP и датаграмм UDP, передаваемых между локальной сетью и внешней сетью;
- **компонент адресации.** RRAS-сервер с установленным NAT, предоставляющий информацию о конфигурации IP-адреса другим компьютерам домашней сети. Компонент адресации представляет собой упрощенный DHCP-сервер, передающий клиентам сведения об IP-адресе, маске подсети, IP-адресе шлюза по умолчанию, DNS-сервере (в качестве последних двух адресов используется IP-адрес непосредственно самого транслятора сетевых адресов). Все компьютеры в локальной сети (являющиеся клиентами NAT) могут быть сконфигурированы как клиенты DHCP, чтобы автоматически получать конфигурацию IP;

- **компонент разрешения имен.** Сервер с преобразователем адресов становится DNS-сервером для других компьютеров локальной сети. Когда он получает от клиента запросы о разрешении имен, то пересылает их серверам DNS в межсетевой среде, на которые он настроен, и возвращает ответы на компьютер в локальную сеть.

Конфигурирование NAT с помощью программы-мастера

Механизм NAT может быть активизирован на любом компьютере под управлением Windows Server 2008. Для этого необходимо соответствующим образом сконфигурировать службу Routing and Remote Access (Маршрутизация и удаленный доступ). Для начальной настройки службы используется программа-мастер *(см. выше)*, в окне которой необходимо указать опцию **Network address translation (NAT)** (Преобразование сетевых адресов NAT) (см. рис. 11.17).

Рис. 11.23. Выбор сетевого интерфейса для работы механизма NAT

Примечание

По сравнению с Windows Server 2003, настройка NAT с помощью мастера стала значительно проще.

На странице *NAT Internet Connection* (Подключение к Интернету на основе NAT) мастера (рис. 11.23) следует выбрать подключение, которое будет использоваться механизмом преобразования имен. Предполагается, что это подключение к Интернету (или другой внешней сети). Администратор может выбрать одно из существующих подключений, выбрав переключатель **Use this public interface to connect to the Internet** (Использовать общедоступный интерфейс для подключения к Интернету). В качестве альтернативы администратор может создать подключение по требованию, выбрав опцию **Create a new demand-dial interface to the Internet** (Создать интерфейс для нового подключения по требованию к Интернету).

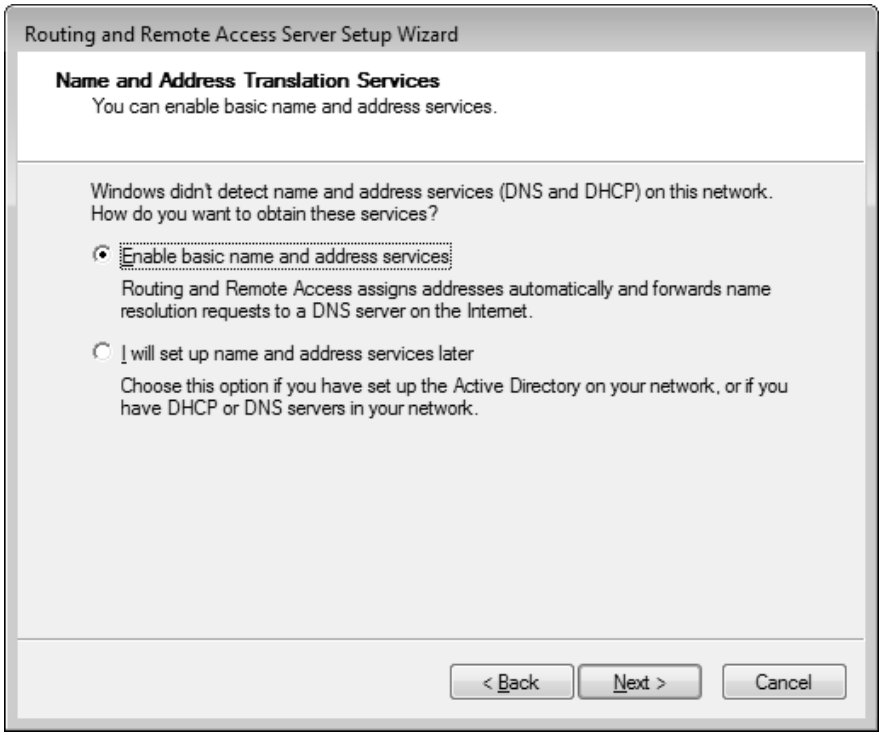


Рис. 11.24. Выбор механизма разрешения DNS-имен и выделения IP-адресов

Подключение по требованию (demand-dial interface) используется, как правило, в случае коммутируемого доступа к внешней сети. Оно устанавливается только в том случае, когда один из пользователей запрашивает доступ к ресурсам Интернета и по окончании работы пользователя разрывается. Если для работы механизма NAT был выбран интерфейс соединения по требованию, система запустит мастер создания соединения по требованию.

На следующем шаге нужно указать, должен ли сервер с устанавливаемым NAT обслуживать DHCP- и DNS-запросы клиентов сети (рис. 11.24). Если эти службы в сети отсутствуют, то можно выбрать опцию, предлагаемую по умолчанию. В этом случае сервер будет выдавать IP-адреса из диапазона адресов той подсети, с которой связан локальный сетевой интерфейс.

В последнем окне мастера нужно нажать кнопку **Finish** (Готово) — мастер запустит службу RRAS и выполнит заданное конфигурирование. При этом в параметрах встроенного брандмауэра Windows автоматически активизируется исключение **Routing and Remote Access** (Маршрутизация и удаленный доступ).

Настройка NAT на уже установленном сервере RRAS

Если в сети уже имеется функционирующий сервер, на котором сконфигурирована служба RRAS, можно выполнить активизацию механизма NAT без использования специального мастера конфигурирования. Если интерфейс, обеспечивающий подключение к Интернету (например, подключение по требованию), уже имеется, то необходимо выполнить следующую последовательность действий:

1. Запустить оснастку **Routing and Remote Access** (Маршрутизация и удаленный доступ).
2. Если в списке активных протоколов (узел **IPv4**) отсутствует объект **NAT**, нужно добавить к списку протокол преобразования сетевых адресов (NAT). Для этого нужно выбрать папку **IPv4** | **General** (IPv4 | Общие), вызвать контекстное меню и выбрать в нем команду **New Routing Protocol** (Новый протокол маршрутизации). В открывшемся окне (рис. 11.25) следует выбрать строку **NAT** и подтвердить свой выбор, нажав кнопку **OK**.
3. На следующем этапе требуется выбрать сетевые интерфейсы, которые будут работать с механизмом преобразования сетевых адресов. Вызовите контекстное меню папки **NAT** и выберите в нем команду **New Interface** (Новый интерфейс).

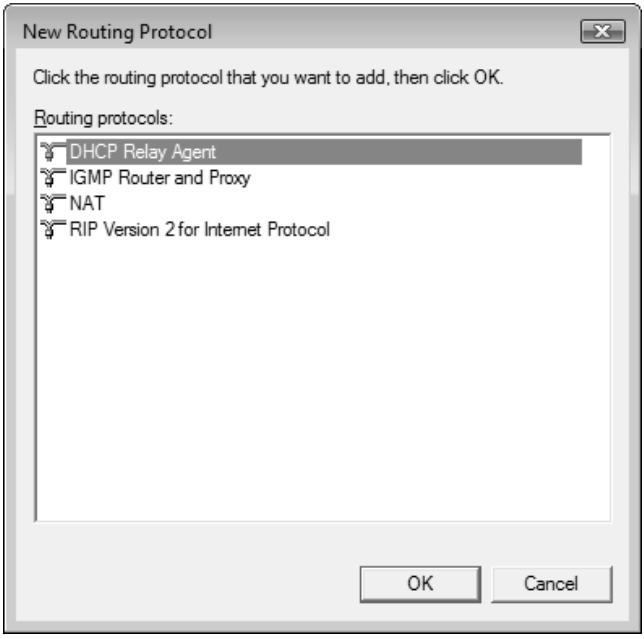


Рис. 11.25. Установка протокола преобразования сетевых имен

Из списка установленных интерфейсов необходимо выбрать требуемый и нажать кнопку **OK**. Далее, в открывшемся окне на вкладке **NAT** (рис. 11.26), в зависимости от типа выбранного интерфейса, надо выполнить следующие действия:

- для сетевого интерфейса, подключенного к Интернету, необходимо установить переключатель **Public interface connected to the Internet** (Общий интерфейс подключен к Интернету) и установить флажок **Enable NAT on this interface** (Включить NAT на данном интерфейсе);
- для сетевого интерфейса, подключенного к локальной сети, необходимо установить переключатель **Private interface connected to the private network** (Частный интерфейс подключен к частной сети).

4. Закрыть окно, нажав кнопку **OK**. Теперь NAT включен и может обслуживать подсеть, подключенную к локальному интерфейсу. С помощью команд в контекстном меню папки **NAT** можно просматривать статистику по полученным и отправленным пакетам, количеству операций преобразования (mapping), а также по запросам на получение адресов (DHCP) и на разрешение имен (DNS) (рис. 11.27).

Рис. 11.26. Активизация механизма NAT для выбранного сетевого интерфейса

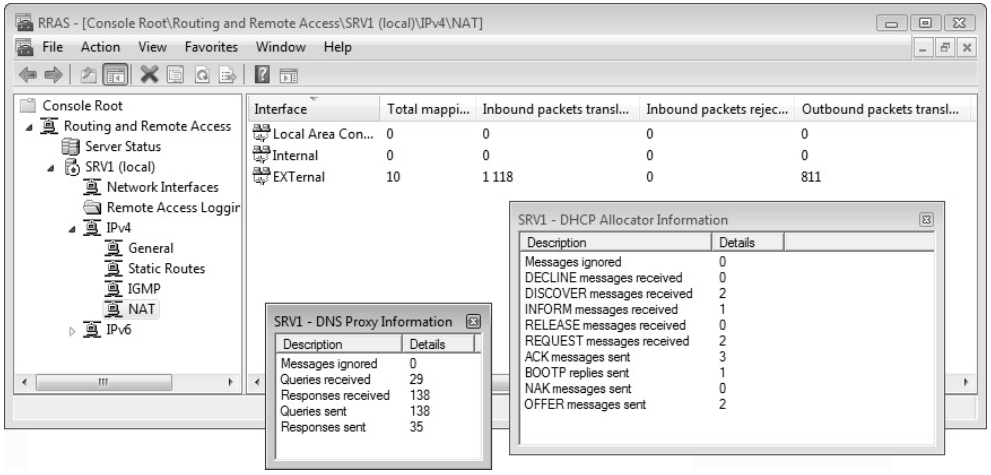


Рис. 11.27. Просмотр статистики по работе NAT

Разрешение выделения IP-адресов локальным хостам

Сервер, на котором активизирован механизм NAT, может обслуживать клиентские DHCP-запросы на получение IP-адресов. Чтобы разрешить эту функцию, необходимо открыть окно свойств папки **NAT**, перейти на вкладку **Address Assignment** (Назначение адресов) (рис. 14.28) и установить флажок **Automatically assign IP addresses by using the DHCP allocator** (Назначать IP-адреса с помощью DHCP-распределителя). Поля **IP address** (IP-адрес) и **Mask** (Маска) позволяют задать номер подсети, к которой будут относиться конфигурируемые клиенты DHCP в локальной сети. По умолчанию предлагается весь диапазон адресов (вся подсеть), обслуживаемых локальным интерфейсом. При необходимости, нажав кнопку **Exclude** (Исключить), администратор может исключить некоторые адреса из этого диапазона.

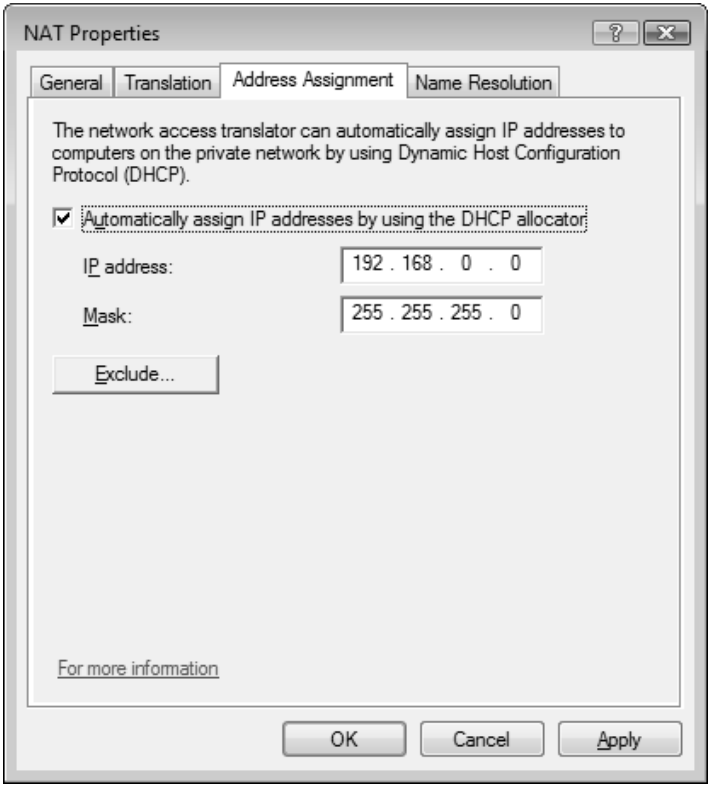


Рис. 14.28. Разрешение использования протокола DHCP для выделения адресов локальным хостам

Функция разрешение DNS-имен

Помимо динамического выделения адресов хостам локальной сети, сервер с установленным NAT может выполнять разрешение доменных имен в локальной сети. Чтобы включить подобный механизм, нужно открыть окно свойств папки **NAT**, перейти на вкладку **Name Resolution** (Разрешение имен в адреса) (рис. 14.29) и установить флажок **Clients using Domain Name System (DNS)** (Для клиентов, использующих службу DNS).

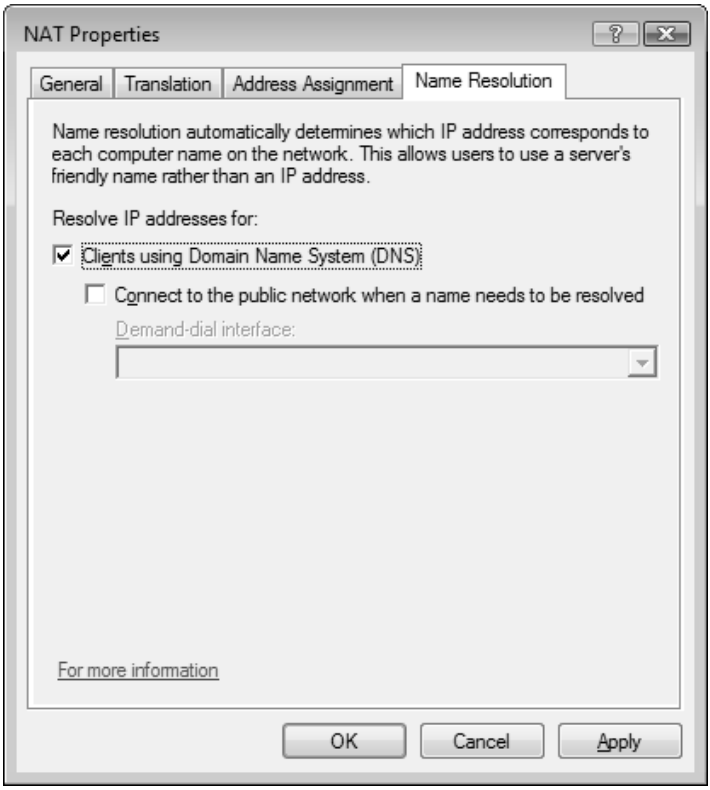


Рис. 14.29. Включение разрешения доменных имен через механизм NAT

Если требуется, чтобы соединение с Интернетом устанавливалось в тот момент, когда один из расположенных в частной сети хостов отправляет запрос на разрешение имени компьютеру с NAT, то следует установить флажок **Connect to the public network when a name needs to be resolved** (Подклю-

чаться при этом к публичной сети) и выбрать в списке **Demand-dial interface** (Интерфейс вызова по требованию) требуемый интерфейс.

Конфигурирование преобразования специальных портов и служб

Администратор может выполнить более точную настройку механизма NAT, выполнив конфигурирование специальных портов. Фактически администратор задает специфические правила преобразования пакетов, приходящих на определенные порты.

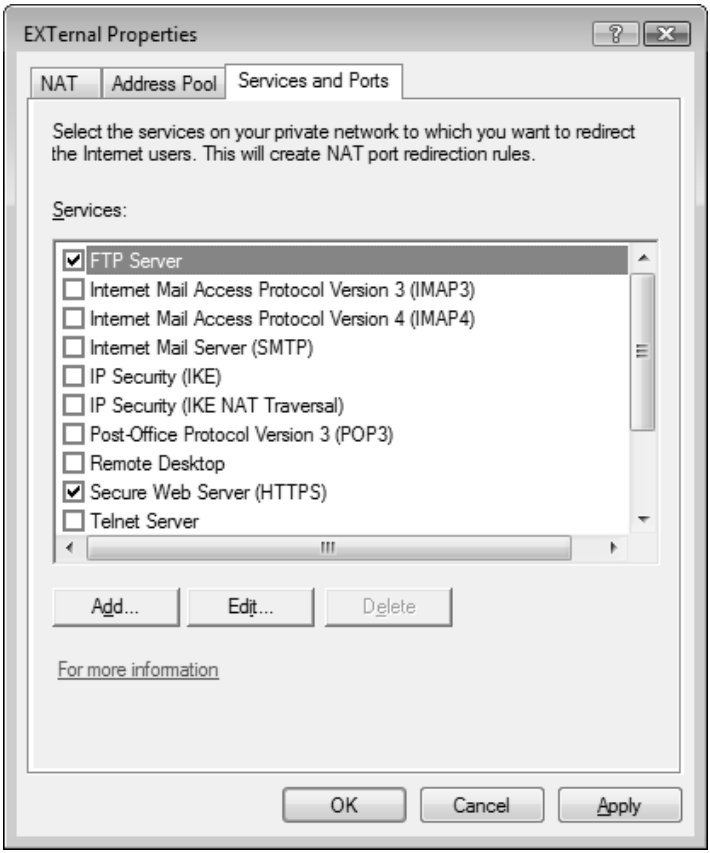


Рис. 11.30. Расширенная настройка преобразователя адресов

Подобное решение позволяет обеспечить прозрачное функционирование корпоративных приложений поверх механизма NAT. Например, администратор может определить порядок преобразования пакетов, приходящих на порт 25 (протокол SMTP).

Расширенная настройка механизма преобразования портов осуществляется на вкладке **Services and Ports** (Службы и порты) в окне свойств внешнего сетевого интерфейса (см. рис. 11.26). Администратору предлагается выбор из 13 предопределенных сетевых служб (рис. 11.30). При необходимости можно создать новые описания служб.

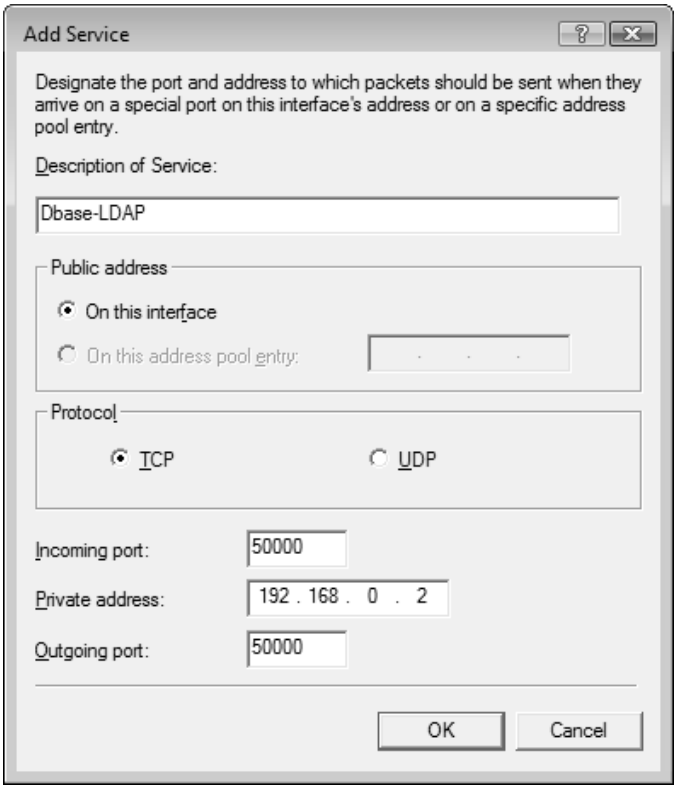


Рис. 11.31. Создание нового правила преобразования портов

Для предопределенных служб администратор может определить только частный адрес хоста (адрес в частной сети), на котором запущена указанная служба. Все остальные параметры изменены быть не могут. В процессе соз-

дания нового описания службы (правила преобразования) администратору необходимо помимо имени определить следующие параметры (рис. 11.31):

- действительный адрес, для которого создается правило. По умолчанию предполагается адрес, используемый конфигурируемым интерфейсом. Если для интерфейса сконфигурирован пул адресов, в поле у переключателя **On this address pool entry** (на этом элементе пула адресов) необходимо указать один из адресов этого пула;
- протокол (TCP или UDP) в группе переключателей **Protocol** (Протокол);
- номер внешнего порта в поле **Incoming port** (Входящий порт). Это порт, на который будут приходить пакеты;
- адрес хоста в корпоративной сети, на который будет выполняться перенаправление всех транслируемых пакетов подобного типа, в поле **Private address** (Адрес в частной сети);
- номер внутреннего порта в поле **Outgoing port** (Исходящий порт). Это порт, который будет использоваться для преобразования заголовка пакета.

Конфигурирование хостов в локальной сети для работы с NAT

Каждый клиент сети, который будет использовать механизм NAT, должен иметь соответствующую (согласованную с конфигурацией NAT) настройку стека протоколов TCP/IP:

- IP-адрес, принадлежащий к разрешенному диапазону частных адресов. В рассматриваемом нами примере он должен относиться к сети с идентификатором 192.168.0.0 и маской 255.255.255.0;
- маска подсети (255.255.255.0);
- в качестве шлюза по умолчанию должен быть указан IP-адрес локального интерфейса RRAS-сервера с NAT;
- в качестве DNS-сервера должен быть указан IP-адрес локального интерфейса RRAS-сервера с NAT.

Информационные службы Интернета (IIS 7.0)

В состав Windows Server 2008 входят интернет-службы *Internet Information Services (IIS) 7.0*, которые содержат *Web Server (IIS)* (Веб-сервер (IIS)), служ-

бу *FTP Publishing Service* (Служба FTP-публикации), компоненты *ASP.NET* и множество дополнительных служб. Все службы IIS 7.0 объединены единым стандартным интерфейсом администрирования и общими методами управления и связаны с ролью сервера *Web Server (IIS)* (Веб-сервер (IIS)).

> ***Внимание!***
>
> Служба POP3 Service, позволяющая использовать компьютер в качестве почтового сервера, исключена из состава служб IIS 7.0 на платформе Windows Server 2008.

Далее будут рассмотрены вопросы установки служб на компьютере и подготовка к работе веб-сервера и FTP-сервера. Этого достаточно для развертывания этих служб, наполнения статическим содержимым и обеспечения доступа к ним со стороны клиентов локальной сети или Интернета (при наличии постоянного внешнего, public, IP-адреса).

В простейшем случае запуск серверов, входящих в состав служб IIS 7.0, сводится к следующим простым этапам:

1. Установка служб IIS 7.0.
2. Разрешение доступа к серверам через брандмауэр Windows.
3. Запуск сервиса FTP-сервера, если он устанавливался.
4. Наполнение серверов содержимым. Этот этап постоянный, поскольку информационное наполнение обычно изменяется в течение всего срока службы серверов.

Установка служб IIS 7.0

Для установки или удаления компонентов с помощью оснастки **Server Manager** (Диспетчер сервера) необходимо выбирать роль *Web Server (IIS)* (Веб-сервер (IIS)) (рис. 11.32). Для установки веб-сервера также требуется компонент Windows Process Activation Service — Process Model.

По умолчанию устанавливаются не все компоненты (при установке роли мастер сам выбирает нужные службы роли), поэтому многие названия служб будут отмечены серым квадратом (в этом случае можно раскрыть соответствующий узел и увидеть, какие составляющие модули включены, а какие нет).

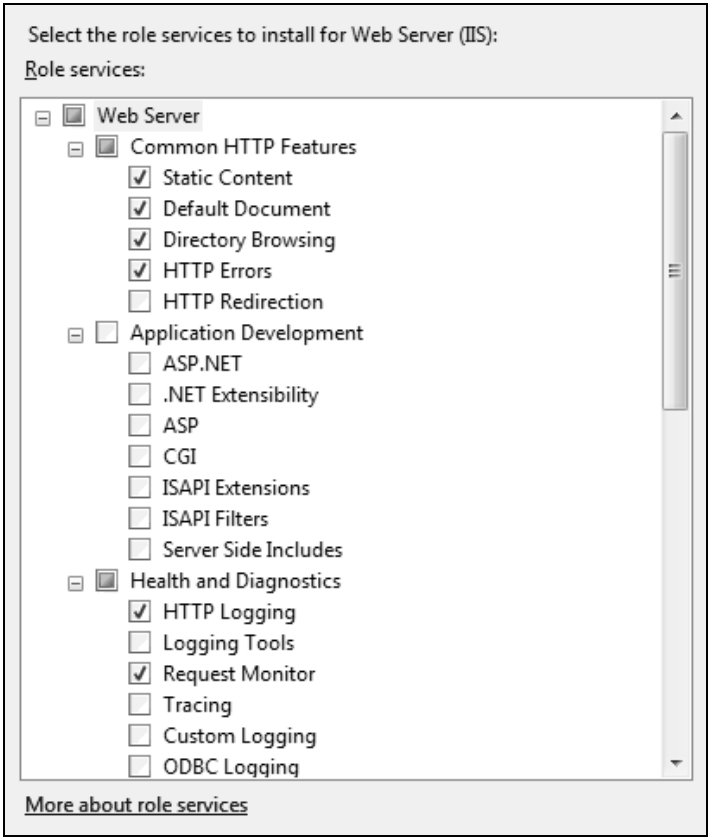


Рис. 11.32. Выбор устанавливаемых компонентов служб IIS

Служба *FTP Publishing Service* (Служба FTP-публикации) (входящие в нее компоненты — FTP Server (FTP-сервер) и FTP Management Console (Консоль управления FTP)) по умолчанию не выбирается в составе служб роли, поэтому при необходимости соответствующие флажки следует установить дополнительно.

Компоненты служб IIS 7.0 иногда требуются при установке других сетевых служб или средств (например, при использовании средств печати через Интернет) — в этом случае дополнительные компоненты выбираются автоматически.

После установки роли Web Server (IIS) (Веб-сервер (IIS)) оснастки **Internet Information Services (IIS) Manager** (Диспетчер служб IIS) и **Internet Infor-**

mation Services (IIS) 6.0 Manager (Диспетчер служб IIS 6.0) добавляются к оснастке **Computer Management** (Управление компьютером) и включаются в меню **Administrative Tools** (Администрирование). При первом запуске диспетчер служб IIS можно видеть имя сервера, список задач и ссылки на полезные онлайновые ресурсы, посвященные службам IIS 7.0 и приложениям ASP.NET (рис. 11.33).

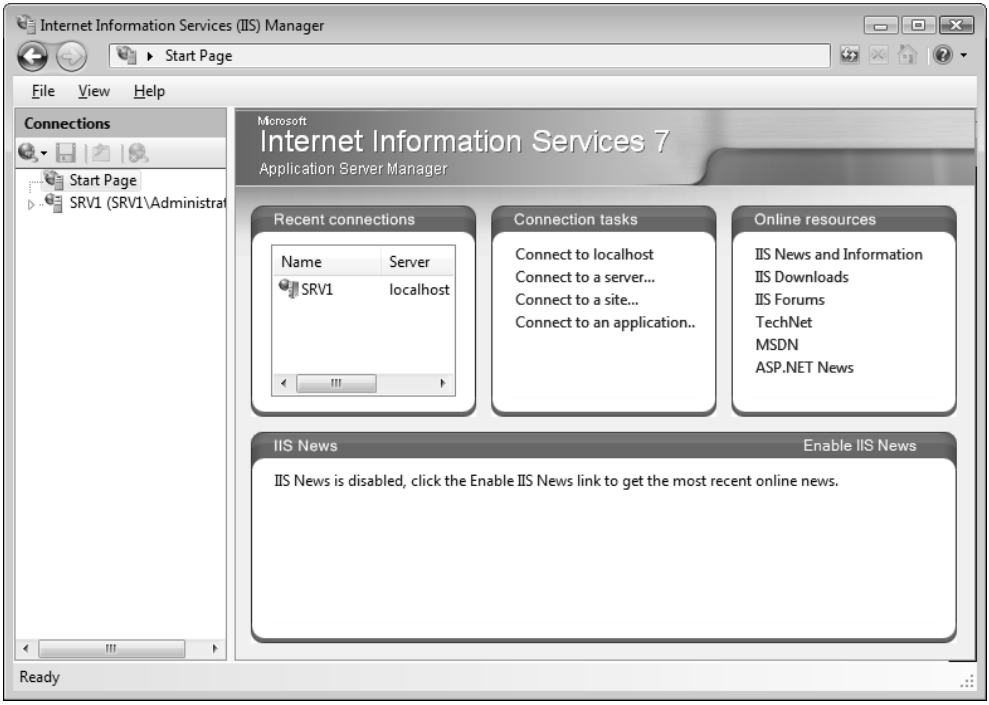


Рис. 11.33. Начальная страница оснастки управления службами IIS 7.0

На компьютере, где установлены службы IIS, имеется встроенная группа IIS_IUSRS, а также создается учетная запись IUSR_*<имяКомпьютера>* — эти записи используются для обеспечения безопасности при работе служб.

После установки служб IIS в корне дискового тома, где находятся системные файлы (*%SystemDrive%*\), создается каталог \inetpub, содержащий корневые папки для веб-сервера и FTP-сервера — \wwwroot и \ftproot (эта папка пустая) соответственно. Оба сервера могут работать сразу после установки, поскольку-

ку для служб WWW и FTP разрешен анонимный доступ (только нужно *запустить* службу FTP, поскольку по умолчанию ее пуск не выполняется).

> ***Примечание***
>
> По умолчанию для службы FTP Publishing Service (Службы FTP-публикации; сервис MSFTPSVC), обеспечивающей работу FTP-сервера, задан ручной режим запуска. Поэтому нужно либо каждый раз запускать ее после перезагрузки компьютера, либо установить для нее с помощью оснастки **Services** (Службы) режим автоматического запуска.

Если после установки служб IIS 7.0 в окне веб-браузера на любом компьютере локальной сети в поле адреса ввести строку `http://<имяСервераIIS>` (на локальном компьютере можно использовать строку `http://localhost`) или `ftp://  <имяСервераIIS>`, то можно увидеть, соответственно, страницу-заставку веб-сервера, имеющуюся в каталоге \inetpub\wwwroot, или содержимое папки \inetpub\ftproot. Поэтому практически сразу же после установки можно заниматься информационным наполнением серверов.

> ***Внимание!***
>
> Настройки служб IIS должны быть скоординированы с параметрами встроенного брандмауэра Windows (Windows Firewall), если он включен. Необходимо разрешить все используемые службы и порты и проверить их доступность. В окне параметров брандмауэра (см. рис. 8.29) на вкладке **Exceptions** (Исключения) необходимо установить флажки **FTP Server** (FTP-сервер) и **World Wide Web Services (HTTP)** (Службы Интернета (HTTP)).

Средства администрирования служб IIS и приложений ASP.NET

Средства управления службами IIS 7.0 объединены с подсистемой конфигурирования ASP.NET-приложений — это хорошо видно по интерфейсу диспетчера служб IIS, где в окне оснастки все группы параметров сгруппированы в две так называемых *области* — ASP.NET и IIS (рис. 11.34). Такой задачно-ориентированный подход позволяет быстро находить нужные группы параметров для каждой практической ситуации.

Базовая настройка служб IIS 7.0 достаточно проста, если говорить о подготовке их к работе и конфигурировании структуры папок, определяющих статическое информационное наполнение серверов WWW и FTP. Как уже гово-

рилось, общим инструментом управления службами IIS 7.0 и приложениями ASP.NET является оснастка **Internet Information Services (IIS) Manager**[1] (Диспетчер служб IIS) (InetMgr.exe) (рис. 11.35), с помощью которой можно работать со службами IIS, находящимися на любом компьютере в локальной сети.

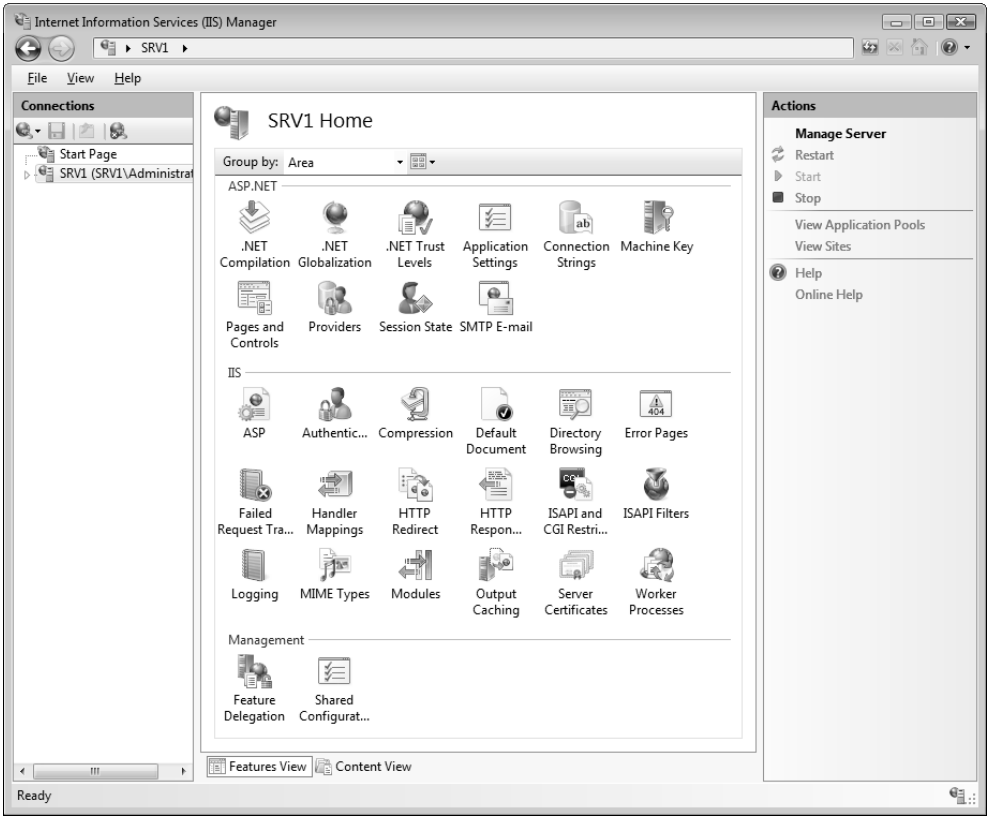


Рис. 11.34. Основные задачи для выбранного сервера с установленными службами IIS 7.0

Как можно видеть на рисунке, интерфейс оснастки весьма насыщенный, это позволяет быстро выбирать нужные параметры, относящиеся к определенной задаче (которая определяется *областью* управления (список **Areas**) или *ка-*

[1] Для краткости мы будем ее называть просто **IIS Manager** (Диспетчер служб IIS).

тегорией (список **Categories**)). Некоторые параметры и действия, показанные в данном окне, будут описаны ниже.

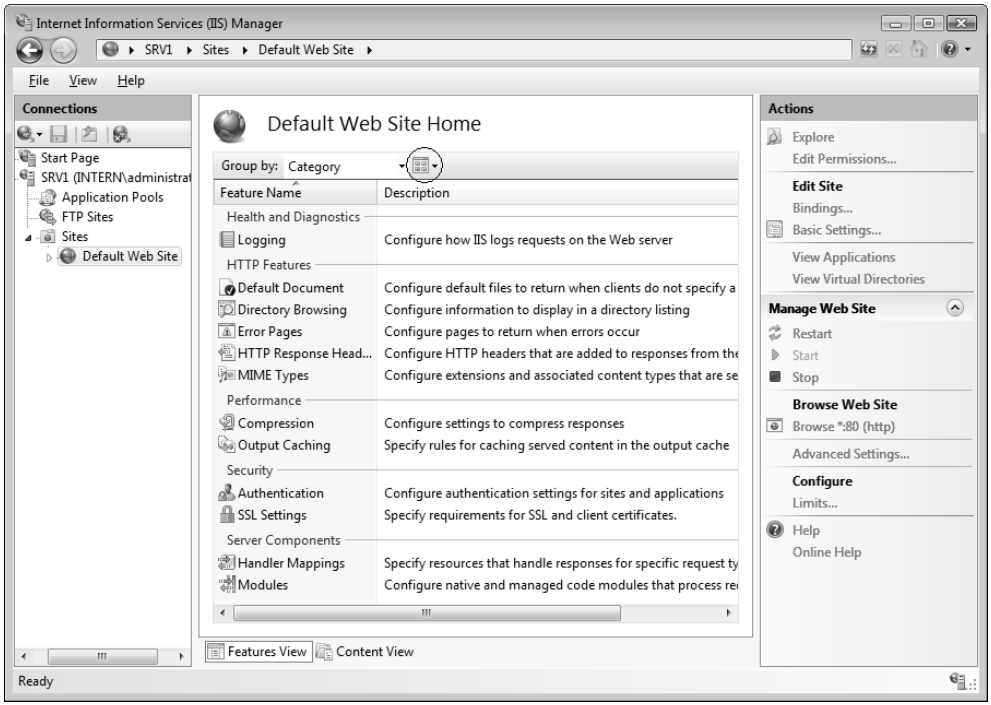


Рис. 11.35. Оснастка **Internet Information Services (IIS) Manager**

Кнопка **Views** (Режимы) (отмечена кружком на рис. 11.35) позволяет переключать вид представления групп параметров (по умолчанию выбран режим **Icons** (Значки), в нашем примере — **Details** (Сведения)). Все относящиеся к выбранному объекту задачи отображаются справа на панели **Actions** (Действия). Например, с этой панели легко запустить или остановить веб-сайт, просмотреть список работающих на нем приложений или список его виртуальных каталогов.

Обратите внимание на кнопки **Features View** (Просмотр возможностей) и **Content View** (Просмотр содержимого) в нижней части окна оснастки — с их помощью можно быстро переключаться между режимами выбора задач и просмотра содержимого контейнера (папки) выбранной в окне структуры объектов.

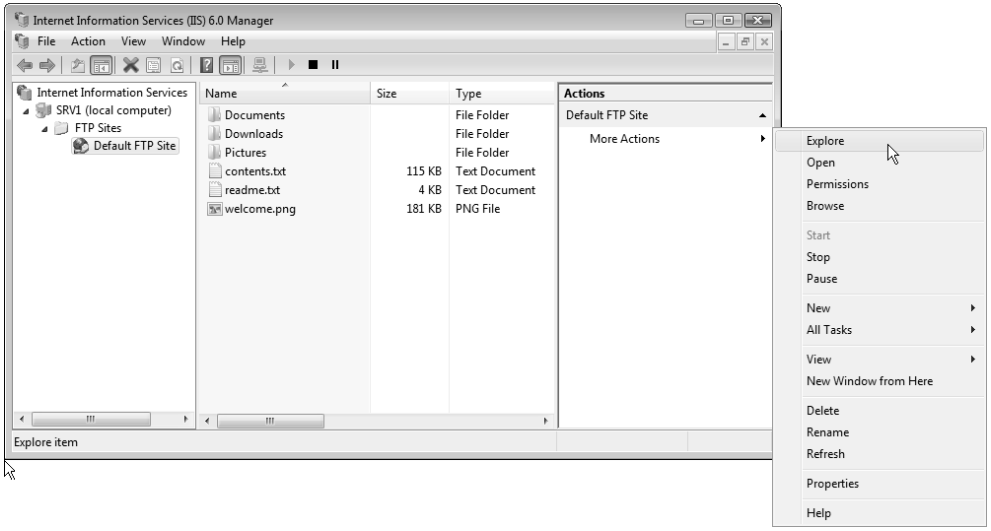


Рис. 11.36. Окно оснастки **IIS 6 Manager**, используемой для управления FTP-сервером

Для управления FTP-сервером используется административная оснастка от предыдущей версии служб IIS — оснастка **IIS 6 Manager** (Диспетчер служб IIS 6.0) (рис. 11.36). Как несложно заметить, ее интерфейс значительно отличается от версии 7.0.

По умолчанию в окне оснастки виден только FTP-сайт, созданный по умолчанию, и виртуальные каталоги, если таковые имеются на сервере. Если в правой половине окна щелкнуть правой кнопкой мыши или нажать кнопку **Actions** (Действие) в меню оснастки, то появится меню операций, которые можно выполнять с узлом, указанным слева в окне структуры папок. Например, команды **Explore** (Проводник) и **Browse** (Обзор) позволяют увидеть содержимое корневого каталога FTP-сервера (см. пример на рис. 11.36) или выбранного виртуального каталога, а команда **Permissions** (Разрешения) открывать окно списка управления доступом (ACL) для указанного каталога — в этом окне задаются разрешения на уровне файловой системы NTFS.

Свойства веб- и FTP-узлов

Если при обращении к веб-сайту пользователь указывает только имя сайта (или имя компьютера), то должна открываться определенная страница —

обычно это домашняя страница сайта. Если в окне оснастки **IIS Manager** (Диспетчер служб IIS) дважды щелкнуть по папке **Default Document** (Документ по умолчанию) (см. рис. 11.35), то появится панель, на которой задан список имен файлов, которые будут использоваться в этом случае (рис. 11.37). Имя, находящееся выше других, имеет более высокий приоритет, т. е. при наличии файла с таким именем будет отображаться только его содержимое. По умолчанию в папке \wwwroot имеется только файл iisstart.htm — он и выполняется при первом обращении к сайту, если нет других страниц. Можно удалить ненужные файлы, оставив в нем только одно имя.

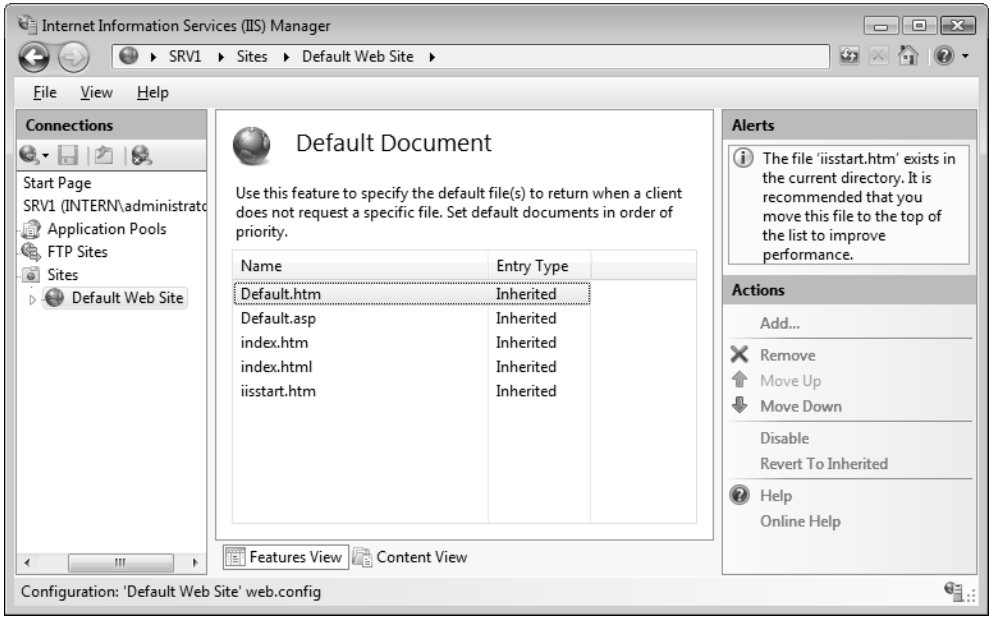


Рис. 11.37. На этой панели задаются файлы, открываемые при обращении к веб-сайту

Папка \ftproot сразу после установки служб IIS 7.0 пустая — поэтому при обращении по адресу `ftp://<имяСервераIIS>` или `ftp://localhost` пользователь увидит пустое окно браузера или пустой список в окне FTP-клиента.

В окне свойств FTP-сайта определяются все параметры работы сервера (рис. 11.38). В частности, здесь задается отображаемое имя сайта, номер порта TCP, по которому выполняется доступ, число возможных подключений, время тайм-аута (при бездействии клиента) и параметры журнала регистрации

событий. Нажав кнопку **Current Sessions**, можно увидеть параметры текущих подключений: имя пользователя, его IP-адрес и время подключения.

По умолчанию для служб WWW и FTP разрешается анонимный доступ (без аутентификации). По умолчанию при анонимном доступе используется учетная запись IUSR_*<имяКомпьютера>*. При необходимости можно установить более жесткие параметры доступа к узлам, в первую очередь это относится к FTP-узлам. Обычно информация, публикуемая на веб-сервере, выставляется "на всеобщее обозрение", и нет необходимости как-то ограничивать доступ к ней (и так вся информация доступна только для чтения). Доступ же к FTP-серверу нередко предлагается только для определенного круга лиц, поэтому анонимный доступ может быть неприемлемым.

Права доступа к FTP-узлу задаются в окне его свойств на вкладке **Security Accounts** (Безопасные учетные записи) (рис. 11.39). Как можно видеть, по умолчанию разрешены анонимные подключения.

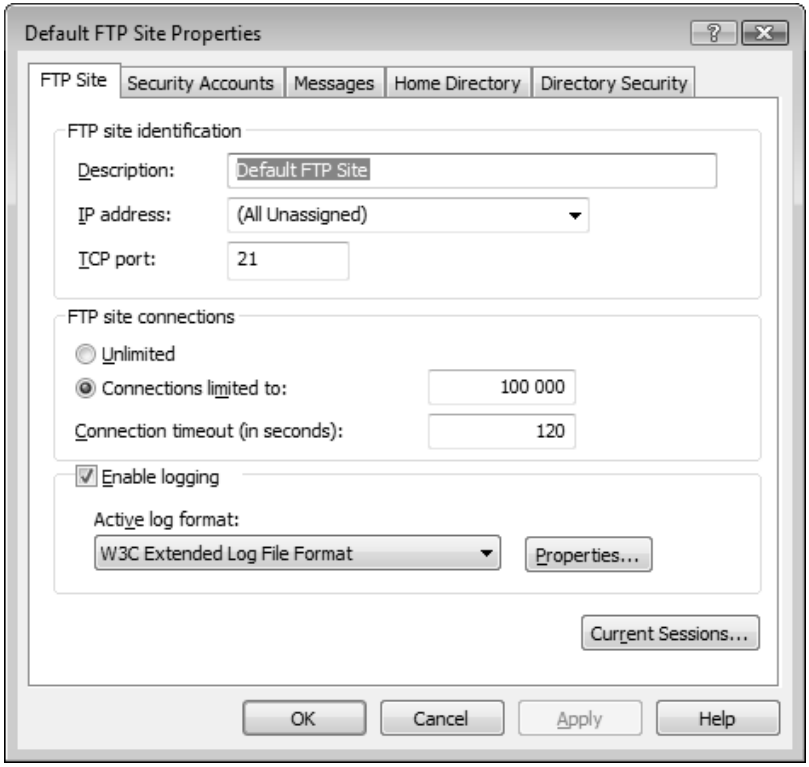


Рис. 11.38. Основные параметры FTP-сервера

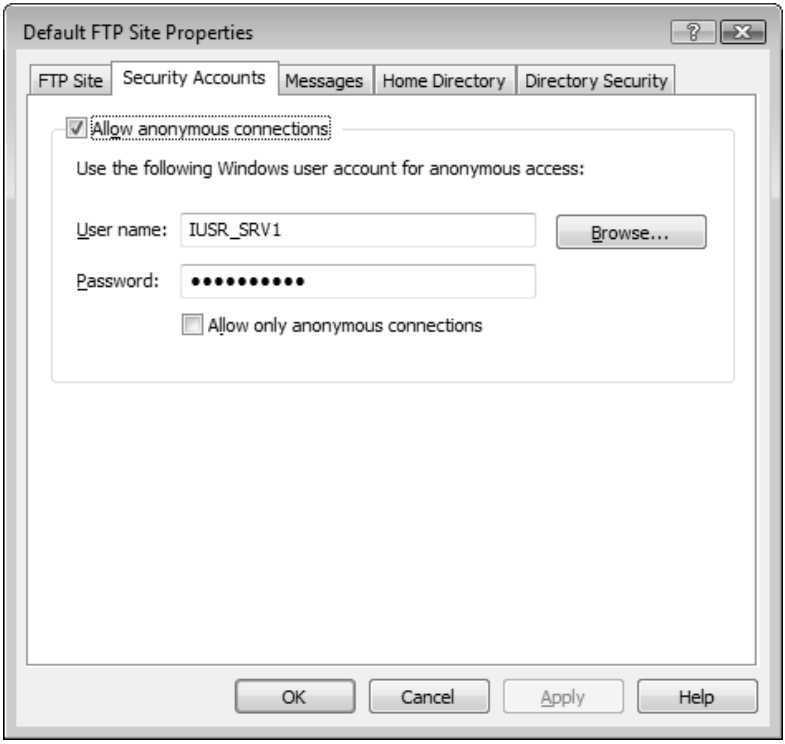


Рис. 11.39. Окно настройки прав доступа к FTP-серверу

Выбранное для доступа имя пользователя можно, в принципе, применять для установки разрешений на уровне файловой системы, например, для детализации прав пользователей, обращающихся к FTP-узлу, например, если разрешена запись файлов. По умолчанию доступ к узлу имеют и те клиенты, которые могут указывать параметры учетных записей безопасности. Запись, если она разрешена, возможна для всех клиентов FTP-узла, и только на уровне файловой системы можно, например, разрешить запись клиентам, указывающим параметры учетных записей безопасности, и запретить для анонимного доступа (т. е. пользователю IUSR_*<имяКомпьютера>*).

Если анонимный доступ запретить, то доступ к FTP-узлу будут иметь только те клиенты, которые укажут имя локальной учетной записи и ее пароль.

Внимание!

По умолчанию все операции доступа к FTP-серверу регистрируются в журнале, который располагается в папке *%SystemRoot%*\System32\LogFiles.

Управление информационным наполнением

Службы IIS в Windows Server 2008 по умолчанию настроены так, чтобы клиенты могли практически сразу работать с веб-сервером или FTP-сервером. Очевидно, что серверы должны предоставлять клиентам какую-то полезную информацию, и эта информация должна быть предварительно подготовлена или *опубликована* (т. е. должен быть разрешен доступ к локальным папкам из Интернета или интрасети).

Начальные действия. Первым шагом в развертывании веб-узла является определение структуры веб-страниц. Необходимо указать, в каких папках хранятся документы, публикуемые на веб-сервере, — он не может отображать документы, которые находятся вне пределов указанных каталогов, т. е. следует связать логическую структуру веб-страниц с физическим расположением документов на жестком диске.

К установленному по умолчанию веб-серверу можно даже обратиться сразу же, до публикации какой-либо пользовательской информации. Достаточно в окне браузера, запущенного на каком-нибудь компьютере в сети или на том же самом компьютере, где находятся службы IIS, ввести адрес `http://<имяСервераIIS>`. Вместо имени сервера можно использовать его IP-адрес или строку `localhost` (на локальном компьютере). Изначально отображается страница приветствия служб IIS, где на множестве языков написана фраза "Добро пожаловать". Если эта картинка видна, то веб-сервер работоспособен, и можно заниматься его информационным наполнением. Вид страницы определен тем файлом, который задан для отображения по умолчанию — см. рис. 11.37 (более приоритетным является файл, помещенный в списке выше других). В исходном состоянии в домашнем каталоге ничего нет, кроме файла iisstart.htm.

Если необходимо опубликовать информацию немедленно, не тратя время на создание структуры каталогов узла, можно просто скопировать публикуемые файлы в основной каталог по умолчанию. Пользователи сети смогут обращаться к этим файлам, вводя URL-адрес `http://<имяСервераIIS>/<имяФайла>`. Можно также создать HTML-файл с именем Default.htm и поместить его в домашний (корневой) каталог. В этом случае сервер будет также "откликаться" на адрес `http://<имяСервераIIS>`, но теперь вместо страницы приветствия вы должны увидеть свой HTML-документ.

Для FTP-сервера начальные шаги тоже очень простые: нужные файлы и папки следует скопировать в папку \ftproot. При обращении к серверу пользователь

увидит их имена в окне браузера или в командной строке (если используется FTP-клиент, работающий в окне консоли).

> ***Внимание!***
>
> Если доступ к FTP-серверу отсутствует, отключите режим Passive FTP в браузере или FTP-клиентах, с помощью которых выполняется обращение к серверу.

Задание домашних каталогов. Каждый веб-узел или FTP-узел имеет корневой, или *домашний каталог* (home directory). Домашний каталог — отправная точка для организации информационной структуры публикуемых веб-страниц. Он содержит домашнюю страницу (см. рис. 11.37) или индексный файл, который является стартовой страницей узла и содержит ссылки на другие страницы на узле. Домашний каталог привязывается к имени веб-узла (которое в свою очередь должно быть связано с внешним IP-адресом) или к имени сервера. Например, если имя узла — **www.mysite.com** и корневой каталог — \Webserver\MySite, то браузер, обращаясь по URL **http://www.mysite.com**, получит файлы из корневого каталога. В локальной сети, если имя сервера — Infoserver, то браузер, обращаясь по URL **http://Infoserver**, также получит доступ к файлам в домашнем каталоге.

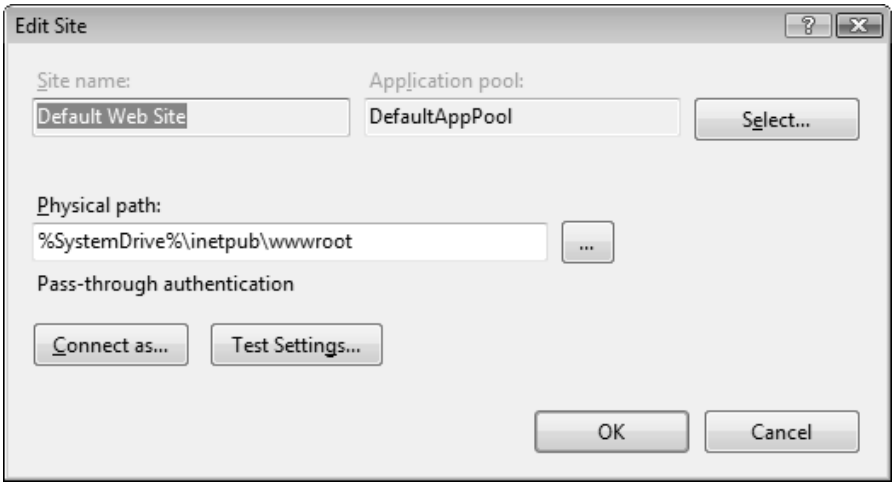


Рис. 11.40. Задание домашнего каталога веб-сервера

Корневые каталоги по умолчанию (\wwwroot и \ftproot в папке *%SystemRoot%*\inetpub) создаются при установке служб IIS 7.0. Чтобы изменить домашний каталог для веб-сервера, на главной странице оснастки **IIS Manager** (Диспетчер служб IIS) выберите задачу **Basic Settings** (Основные настройки) (см. рис. 11.35). В появившемся окне (рис. 11.40) можно переопределить физический путь к каталогу, выбрав любую локальную папку.

Для FTP-узла корневой каталог указывается в окне свойств сервера на вкладке **Home Directory** (Корневой каталог) (рис. 11.41). Здесь же определяется возможность записи файлов на FTP-сервер. Нужно также следить за тем, какие разрешения на запись в корневой каталог (а также и в виртуальные каталоги, если таковые имеются) установлены на уровне файловой системы.

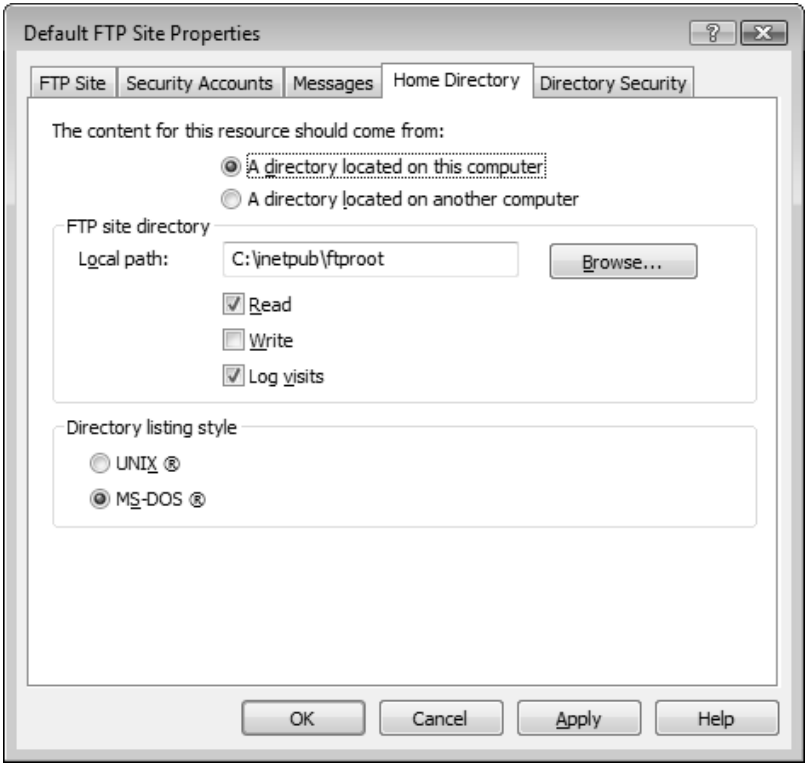


Рис. 11.41. Корневой каталог FTP-сервера

Виртуальные каталоги. Чтобы публиковать информацию из *любой* папки, расположенной в произвольном месте файловой системы вне корневого ка-

талога WWW- или FTP-сервера, можно создавать *виртуальные каталоги*. Виртуальный каталог — это каталог, который для клиента выглядит так, как если бы он был частью домашнего каталога сервера. На рис. 11.35 на панели действий можно видеть ссылку **View Virtual Directories** (Просмотреть виртуальные каталоги), позволяющую перейти на панель, где перечислены и создаются каталоги, образующие логическую структуру веб-страниц на сервере. Достаточно выбрать задачу **Add Virtual Directory** (Добавить виртуальный каталог) и заполнить окно свойств нового каталога.

Каждый виртуальный каталог имеет *псевдоним* (alias), т. е. имя, которое веб-браузеры используют для обращения к этому каталогу. Поскольку псевдоним обычно короче полного пути каталога, пользователям его удобнее вводить. Псевдоним безопаснее; пользователи не знают, где файлы физически расположены на сервере, и не могут использовать данную информацию для изменения этих файлов. Псевдонимы упрощают организацию структуры папок, используемых для хранения содержимого веб-сайта, и перемещение подкаталогов. Не изменяя URL-адрес каталога, можно изменить отображение между псевдонимом и физическим местоположением каталога.

Предположим, что для публикации информации в сети установлен узел INTERN-Site. В табл. 11.2 показано соответствие между физическим местоположением файлов и URL, по которому файлы доступны.

Таблица 11.2. *Примеры соответствия между физическим местоположением, псевдонимом и URL-адресом*

Физическое местоположение	**Псевдоним**	**URL**
C:\inetpub\wwwroot	Домашний каталог (нет псевдонима)	http://intern-site
d:\samples\Text	Documents	http://intern-site/Documents
C:\inetpub\wwwroot\Downloads	Нет	http://intern-site/Downloads
\\Srv2\info\Pics	Pictures	http://intern-site/Pictures
C:\inetpub\wwwroot\Schedule	Нет	http://intern-site/Schedule

Как виртуальные, так и физические каталоги (каталоги без псевдонима) видны в окне оснастки **IIS Manager** (Диспетчер служб IIS) (рис. 11.42). Значки, представляющие виртуальные каталоги, имеют изображение стрелки в ниж-

нем левом углу. (В нашем примере еще можно видеть виртуальный каталог Printers, который появляется при установке компонента печати через Интернет — *см. главу 9.*)

Рис. 11.42. Просмотр физических и виртуальных каталогов для веб-сервера

Для простого веб-узла виртуальные каталоги не требуются. Можно просто разместить все файлы в основном каталоге узла. Однако если нужно построить сложный узел или задать различные URL для разных частей узла, можно добавлять виртуальные каталоги по необходимости.

ГЛАВА 12

Домены Active Directory

Вопросы планирования и администрирования доменов Active Directory не охватить даже в целой книге, поэтому в этой главе будут рассмотрены только основные понятия, базовые задачи, возникающие при развертывании леса доменов, средства администрирования и их главные возможности.

Также будет описана процедура установки экземпляров служб *Active Directory Lightweight Directory Services* (Службы Active Directory облегченного доступа к каталогам (AD LDS)), которые позволяют использовать возможности "автономного" каталога Active Directory, не зависящего от наличия службы доменов.

Основные концепции доменов Active Directory

Рассмотрим сначала базовые понятия доменов Active Directory, чтобы были понятны термины, используемые в этой главе. Читатель, работавший с доменами на базе Windows 2000 Server или Windows Server 2003, может спокойно пропустить этот раздел. Однако в случае возникновения неясностей можно вернуться к определениям терминов.

Службы доменов Active Directory базируются на нескольких открытых стандартах:

- протокол *Lightweight Directory Access Protocol* (LDAP v3, Упрощенный протокол доступа к каталогам);
- система доменных имен *DNS* (Domain Name System);
- протокол аутентификации *Kerberos v5*.

Эти стандарты (особенно LDAP) во многом определили терминологию, используемую в архитектуре каталога Active Directory.

Протокол LDAP — основа информационной модели Active Directory

Спецификация *Lightweight Directory Access Protocol* (LDAP) определяет принципы построения сетевых каталогов и способы доступа к каталогу со стороны сетевых клиентов и приложений. Служба каталога Active Directory поддерживает протокол LDAP версий 2 и 3. Протокол LDAP является частью стека протоколов TCP/IP, что и послужило одной из причин его популярности.

Основы протокола LDAP (в частности, способы именования объектов и фильтры запросов) необходимо хорошо понимать при работе со многими системными утилитами и программами, а также для написания сценариев. Из-за ограниченности места мы не можем изложить эти вопросы, поэтому при необходимости читатель может обратиться к другим источникам.

Спецификация LDAP определяет многие понятия, касающиеся логической организации объектов каталога Active Directory. Эти термины часто используются при работе с доменами и административными оснастками, поэтому мы кратко опишем их.

Схема каталога

Определения всех классов объектов, а также совокупность правил, позволяющих управлять структурой каталога и его содержимым, хранятся в специальной иерархической структуре, которая называется *схемой каталога* (schema). Чтобы создать в каталоге объект нового типа, необходимо, прежде всего, добавить в схему определение нового класса объектов. При этом принято говорить о *расширении* (extending) схемы.

Способы именования объектов каталога

Для успешной работы с объектами каталога необходимо однозначно идентифицировать каждый объект. Для именования и идентификации объектов в каталоге протокол LDAP использует *отличительные имена*. Наряду с именами DNS — это два самых часто встречающихся способа именования объек-

тов в Active Directory. Однако имеются и дополнительные форматы имен, применяемые в определенных ситуациях.

Относительное отличительное имя (relative distinguished name, RDN) уникальным образом идентифицирует объект внутри *некоторого контейнера* (при этом само по себе, в масштабах всего леса доменов, это имя может повторяться). RDN-имя состоит из *спецификатора* (specifier) имени атрибута и некоторого символьного значения, например:

- CN=Domain Controllers
- OU=Staff
- DC=dom

Полное отличительное имя, или, просто, *отличительное имя* (distinguished name, DN), является уникальным в пределах леса (forest) или информационного дерева каталога и служит первичным ключом для определенного объекта каталога. Отличительное имя состоит из *относительных* отличительных имен, представляющих собой ветви информационного дерева.

Ниже приведен пример отличительного имени объекта. Аббревиатура (используемая как спецификатор имени) CN означает Common Name (общее имя), OU соответствует Organizational Unit (организационная единица), а DC означает Domain Component (доменный компонент):

- CN=User,OU=Staff,DC=intern,DC=dom

Полное доменное имя (Fully Qualified Domain Name, FQDN) также называется *полным именем компьютера* (full computer name) и представляет собой имя компьютера (хоста) (NetBIOS-имя) плюс *основной суффикс DNS* (primary DNS suffix; т. е. имя домена, в котором находится компьютер). Например, полное DNS-имя компьютера SRV1, входящего в домен sub.intern.dom, будет таким:

- srv1.sub.intern.dom

Порты LDAP

Соединения по протоколу LDAP между клиентом и агентом сервера каталога (DSA) осуществляются с использованием протокола Transmission Control Protocol (TCP) или User Datagram Protocol (UDP). Это справедливо и для взаимодействий между клиентом и контроллером домена Active Directory. В следующей таблице перечислены порты протокола, применяемые при различных способах доступа. Полужирным курсивом отмечены порты, которые

используются по умолчанию административными оснастками Active Directory и многими утилитами, в частности, утилитой Ldp.exe и оснасткой **ADSI Edit** (Редактирование ADSI).

Функция	Порт
LDAP	***389*** (TCP и UDP)
LDAP Secure Sockets Layer (SSL)	636 (TCP)
Global Catalog (GC)	***3268*** (TCP)
Global Catalog Secure Sockets Layer (SSL)	3269 (TCP)

Служба DNS и Active Directory

Для того чтобы клиент смог подключиться к контроллеру домена, он должен точно знать его расположение в сети. В качестве средства определения местонахождения различных сетевых служб компания Microsoft выбрала службу DNS (Domain Name System), которая традиционно используется в TCP/IP-сетях для разрешения символических имен в IP-адреса. Для описания местоположения сетевых служб (сервисов) DNS использует специальный тип ресурсных записей — SRV-записи.

Соглашение о доменных именах, лежащее в основе DNS, используется как основной способ именования доменов Active Directory. Благодаря этому пространство имен доменов Active Directory полностью соответствует иерархии имен DNS.

Требования к DNS со стороны доменов Active Directory

В доменах Active Directory служба DNS требует особого внимания. Нужно выделить два важнейших момента:

- домены Active Directory требуют *обязательного* развертывания или использования службы DNS;
- служба Active Directory может работать с *любой* службой DNS, которая соответствует перечисленным ниже условиям:
  - поддерживает SRV-записи;

- разрешает использование в именах символа подчеркивания ("_"), поскольку он встречается в зарезервированных системных именах (например, _gc._tcp.*domain.com*);
- и, желательно (хотя и не строго обязательно), обеспечивает динамическое обновление ресурсных записей.

По умолчанию все контроллеры доменов Active Directory автоматически регистрируют и обновляют все соответствующие ресурсные DNS-записи типа SRV, CNAME и A. Если динамическое обновление невозможно, то администратор обязан вручную выполнять эту операцию.

Механизм динамической регистрации доменных имен обеспечивает тесную интеграцию служб DNS и DHCP. Динамическая регистрация имен может быть осуществлена либо DHCP-клиентом, либо службой сервера DHCP. Такое решение легко объяснимо, учитывая, что в большинстве случаев изменение IP-адреса клиента связано со службой DHCP.

Если клиентский компьютер работает под управлением операционных систем Windows 2000 и выше, он может самостоятельно зарегистрировать свое имя в базе данных DNS-сервера. В этом случае регистрация осуществляется службой DHCP-клиента. Служба сервера DHCP может зарегистрировать доменное имя одновременно с выделением в аренду IP-адреса.

Примечание

Для нормальной работы Active Directory не требуются зоны обратного просмотра (reverse zones), и мастер установки Active Directory не создает их. Однако рекомендуется все же создавать такие зоны самостоятельно, чтобы обеспечить нормальную работу различных утилит DNS (например, Nslookup).

Как правило, и клиенты, и контроллеры домена Active Directory используют один и тот же предпочитаемый (preferred) DNS-сервер (или несколько серверов), хранящий авторитетную зону (authoritative zone) для домена. IP-адрес этого сервера указывается в свойствах протокола TCP/IP на вкладке **DNS** в окне **Advanced TCP/IP Settings** (Дополнительные параметры TCP/IP).

В качестве адреса предпочитаемого DNS-сервера нельзя указывать адрес DNS-сервера провайдера услуг Интернета. При необходимости внутрисетевой DNS-сервер должен *переадресовать* запросы к внешним доменам на DNS-серверы провайдера *(см. главу 11)*.

Ресурсные записи DNS, регистрируемые контроллерами домена Active Directory

Для определения местонахождения серверов, предоставляющих услуги определенных служб (например, LDAP-сервера или сервера Kerberos), используются SRV-записи службы DNS.

Все ресурсные записи типа SRV и A, которые каждый контроллер домена Active Directory должен зарегистрировать на предпочитаемом сервере DNS в процессе своей загрузки, хранятся в файле *%SystemRoot%*\system32\config\netlogon.dns. (Если используемый DNS-сервер не обеспечивает динамическое обновление записей, необходимо зарегистрировать эти записи вручную.)

Если контроллер домена хранит реплики разделов приложений (application directory partitions), то он для каждого раздела регистрирует в DNS две SRV-записи и A-запись. Эти записи позволяют различным приложениям находить сервер для конкретного раздела, выполняя операцию просмотра DNS.

Для тестирования параметров DNS на контроллерах домена удобно использовать утилиту DCdiag.exe, которая проверяет все параметры DNS на контроллерах домена, являющихся партнерами по репликации, а также доступность этих контроллеров. Кроме того, на любых компьютерах можно применять утилиту Netdiag.exe.

Доменная структура Active Directory

Операционные системы Windows (начиная с Windows NT) традиционно использовали понятие "домена" для логического объединения компьютеров, совместно использующих единую политику безопасности. Перечислим основные задачи, которые решаются путем формирования доменной структуры.

- **Создание областей административной ответственности.** Используя доменную структуру, администратор может поделить корпоративную сеть на области (домены), управляемые отдельно друг от друга. Каждый домен управляется своей группой администраторов. Однако существуют и другие способы формирования административной иерархии (организация подразделений), речь о которых пойдет дальше.
- **Создание областей действия политики учетных записей.** Политика учетных записей определяет правила применения пользователями учетных записей и сопоставленных им паролей. В частности, задается длина пароля, количество неудачных попыток ввода пароля до блокировки

учетной записи, а также продолжительность подобной блокировки. Поскольку эти вопросы решаются организационно на уровне всего домена, данный комплекс мер принято называть *политикой учетных записей*. (Эти политики нельзя определять на уровне подразделений!)

- **Разграничение доступа к объектам.** Каждый домен реализует собственные настройки безопасности (включая идентификаторы безопасности и списки контроля доступа). Разнесение пользователей в различные домены позволяет эффективно управлять доступом к важным ресурсам. С другой стороны, применение *доверительных отношений* (trust relationships) позволяет обеспечить пользователям одного домена доступ к ресурсам других доменов.
- **Изоляция трафика репликации.** Для размещения информации об объектах корпоративной сети используются доменные разделы каталога. Каждому домену соответствует свой раздел каталога, называемый *доменным*. Все объекты, относящиеся к некоторому домену, помещаются в соответствующий раздел каталога. Изменения, произведенные в доменном разделе, реплицируются исключительно в пределах домена. Соответственно, выделение удаленных филиалов в отдельные домены может позволить существенно сократить трафик, вызванный репликацией изменений содержимого каталога. Необходимо отметить, однако, что домены являются не единственным (и даже не основным) способом формирования физической структуры каталога. Того же самого результата администратор может добиться за счет использования механизма сайтов.

> ***Примечание***
>
> Для работы доменов, точнее для аутентификации по протоколу Kerberos, важна синхронизация системных часов на всех клиентах и контроллерах домена. Поэтому важное место в работе доменов занимает *Служба времени Windows* (W32Time), настройка которой рассматривалась в *главе 4*.

Иерархия доменов

Имя домена Active Directory записывается в форме *полного доменного имени* (Fully Qualified Domain Name, FQDN), которое определяет положение домена относительно корня пространства имен. Полное доменное имя образуется из имени домена, к которому добавляется имя родительского домена. Так, например, для домена sub, являющегося дочерним по отношению к домену intern.dom, полное доменное имя будет записано в форме sub.intern.dom.

Выбор подобной схемы именования позволил формировать доменное пространство имен по аналогии с иерархией имен службы DNS. Нужно также заметить, что каждому домену Active Directory помимо DNS-имени сопоставлено уникальное NetBIOS-имя.

Совокупность доменов, использующих единую схему каталога и общую конфигурацию, называется *лесом доменов* (forest). Имена входящих в лес доменов необязательно являются смежными, но так же как и в случае пространства имен DNS, домены Active Directory могут образовывать непрерывное иерархическое пространство имен. В этом случае они связываются между собой отношениями "родитель-потомок". При этом имя дочернего домена обязательно включает в себя имя родительского домена. Совокупность доменов, образующих непрерывное пространство смежных имен, называют *деревом доменов* (domain tree). Лес может состоять из произвольного количества деревьев домена.

Первое созданное в лесу доменов дерево является *корневым деревом*. Первый созданный в дереве домен называется *корневым доменом* дерева (tree root domain), он используется для ссылки на данное дерево.

Соответственно, первый домен, созданный в лесу доменов, называется *корневым доменом леса* (forest root domain). Он играет очень важную роль, связывая деревья, образующие лес доменов, воедино и поэтому не может быть удален. В частности, в нем располагаются важнейшие административные группы, которые не могут быть удалены или перемещены. При потере корневого домена лес, фактически, перестает быть работоспособным!

Особое внимание необходимо уделить вопросу именования доменов и, в частности, корневого домена. Для корневого домена лучше всего использовать доменное имя второго уровня (состоящего из двух компонентов, например, intern.dom).

Контроллеры домена

Серверы, обеспечивающие централизованные административные функции, включающие в себя аутентификацию и авторизацию пользователей, конфигурирование безопасности клиентов, настройку пользовательской среды и т. д., называются *контроллерами домена* (domain controller, DC). На каждом контроллере домена, работающем под управлением серверных операционных систем Windows 2000 Server и выше, функционирует служба каталога Active Directory, и контроллеры являются носителями полнофункциональных копий каталога.

Особенно следует отметить тот факт, что все контроллеры домена Active Directory обладают возможностью внесения изменений в собственную копию каталога. Это позволяет рассматривать любой контроллер домена как потенциальную точку административного воздействия на корпоративную сеть, поскольку администратор может осуществлять конфигурирование всех контроллеров и клиентов домена Active Directory, подключившись к определенному контроллеру. Именно из этих соображений в доменах на базе Windows Server 2008 была реализована возможность установки контроллеров домена, где возможности изменения объектов каталога ограничены, и что самое главное — эти изменения не реплицируются в другие домены. Такие контроллеры получили название *Read-Only Domain Controllers* (RODC).

Специализированные роли контроллеров домена

Служба каталога Active Directory использует модель *репликации с множеством равноправных участников* (multimaster replication). (Это касается и доменных служб Active Directory, и служб Active Directory Lightweight Directory Services (AD LDS) (Службы Active Directory облегченного доступа к каталогам).) С точки зрения подсистемы репликации не имеет значения, какой из носителей осуществляет изменения в каталоге. Изменения могут быть произведены в любой из копий каталога.

Однако существует определенный класс операций, которые должны выполняться только одним контроллером домена. Этот класс операций называется *операциями с одним исполнителем* (Flexible Single-Master Operations, FSMO). Если привлечь к выполнению подобных операций несколько контроллеров домена, нельзя исключать возможность конфликтов. В определенных случаях подобные конфликты могут привести к нарушению целостности каталога.

Имеются два типа операций с одним исполнителем, которые принято называть *ролями контроллеров домена*. От первого типа ролей требуется уникальность исполнителя в пределах всего леса доменов. Роль данного типа может быть возложена только на один контроллер в лесу доменов. К другому типу ролей предъявляется требование уникальности исполнителя только в пределах домена. В каждом домене может быть только один исполнитель (хозяин) FSMO-роли. Таким образом, в рамках леса доменов исполнителей каждой из подобных ролей будет столько же, сколько и доменов, образующих лес.

Рассмотрим пять имеющихся специализированных FSMO-ролей.

- **Хозяин схемы** (Schema Master). Контроллер домена, осуществляющий изменения в схеме каталога. Существование только одного владельца

(хозяина) схемы в пределах леса доменов исключает возможность конфликтов, связанных с ее изменением. Отказ владельца схемы приводит к тому, что выполнение операции расширения схемы станет невозможным.

- **Хозяин именования доменов** (Domain Naming Master). Контроллер домена, отслеживающий изменения в структуре леса доменов. Любое изменение пространства имен доменов Active Directory (добавление, удаление, а также переименование доменов) осуществляется исполнителем данной роли. Тем самым гарантируется целостность пространства имен и уникальность его компонентов. Отказ исполнителя этой роли приводит к тому, что любое изменение пространства имен каталога станет невозможным.
- **Хозяин идентификаторов RID** (Relative ID Master). Контроллер домена, осуществляющий генерацию идентификаторов (глобальные идентификаторы, идентификаторы безопасности и т. п.). От идентификатора в первую очередь требуется уникальность. Самый простой способ гарантировать уникальность генерируемых идентификаторов возложить обязанность исполнителя данной роли на один контроллер в домене. Отказ исполнителя данной роли приводит к тому, что создание объектов в домене станет невозможным.
- **Эмулятор основного контроллера домена** (PDC Emulator). Эта роль унаследована от доменов Windows 2000. Если домен находится на функциональном уровне *Windows 2000 mixed*, то эмулятор основного контроллера домена (PDC) используется для обеспечения репликации изменений между контроллерами домена Windows NT 4.0 и домена Active Directory. Исполнитель роли фактически эмулирует домен Windows NT. Поскольку в домене Windows NT допустимо наличие только одного основного контроллера (PDC), его эмулятор в домене Active Directory также может быть только один. На других функциональных уровнях эмулятор основного домена используется для изменения паролей учетных записей, а также играет ведущую роль в процессе синхронизации системных часов всех контроллеров домена. Эмулятор PDC по умолчанию выбирается оснасткой **Group Policy Object Editor** (Редактор объектов групповой политики). Поэтому, если исполнитель данной роли недоступен, администратор может столкнуться с проблемами при редактировании доменных объектов групповой политики.
- **Хозяин инфраструктуры** (Infrastructure Master). Контроллер домена, отвечающий за структуру каталога. В процессе удаления или перемещения объектов один из контроллеров домена должен взять на себя обязан-

ности по сохранению ссылки на данные объекты до тех пор, пока эти изменения не будут реплицированы на все остальные контроллеры домена. Если в домене имеются несколько контроллеров домена, желательно не совмещать функции исполнителя данной роли и сервера глобального каталога. Лучше разнести эти функции на разные контроллеры домена, которые обязательно должны быть соединены высокоскоростным каналом. Если в домене имеется только один контроллер, этим требованием можно пренебречь.

По умолчанию все специализированные роли назначаются первому контроллеру домена, установленному в новом лесе доменов. Аналогичным образом, в процессе создания нового домена первый установленный в нем контроллер будет выбран в качестве исполнителя ролей, уникальных в пределах этого домена. Понижение контроллера домена, выбранного в качестве исполнителя специализированной роли, до рядового сервера приводит к тому, что роли передаются другому контроллеру домена.

При необходимости администратор может в любой момент передать любую FSMO-роль другому контроллеру домена. Это может потребоваться, например, в ситуации, когда планируется обновление аппаратного обеспечения контроллера. В процессе нормальной передачи роли текущий исполнитель роли освобождается от исполнения специфических обязанностей и становится обычным контроллером домена.

Если администратор не может обеспечить доступность сервера, являющегося исполнителем специализированной роли, либо восстановление его работоспособности не представляется возможным, он должен возложить обязанности исполнения данной роли на другой контроллер домена. Процесс принудительной передачи функций исполнителя специализированной роли другому контроллеру домена называется *захватом,* или *присвоением*, *роли* (seizing).

Доверительные отношения

Доверительные отношения (trusts) представляют собой связь, устанавливаемую между доменами, которая позволяет пользователям одного домена аутентифицироваться на контроллерах другого домена и, как следствие, получать доступ к ресурсам этих доменов. Именно механизм доверительных отношений позволяет организовывать домены в некоторую структуру, называемую лесом доменов.

Суть доверительных отношений между двумя доменами сводится к тому, что *доверяющий домен* (trusting domain) доверяет процесс аутентификации (проверки подлинности учетных данных — имени и пароля) *доверенному домену* (trusted domain). Пользователь, аутентифицированный доверенным доменом, может получить доступ к ресурсам в доверяющем домене.

Домены Active Directory допускают создание как односторонних, так и двусторонних доверительных отношений. Двусторонние доверительные отношения строятся на основе протокола аутентификации Kerberos v5 и обладают свойством транзитивности.

Можно использовать доверительные транзитивные отношения как для соединения доменов в пределах одного леса, так и для соединения разных лесов доменов (если оба леса работают на функциональном уровне *Windows Server 2003* — т. е. в них используются контроллеры домена не ниже Windows Server 2003).

Обратите внимание, что доверительные отношения внутри леса и внутри дерева доменов устанавливаются системой автоматически, в процессе создания домена или дерева доменов. Администратор не может как-либо отозвать их или удалить. Все остальные типы доверительных отношений создаются администратором вручную.

Подразделения (организационные единицы)

Подразделения, или *организационные единицы* (organizational unit), представляют собой объекты каталога контейнерного типа, посредством которых администратор может организовать некоторую логическую структуру объектов сети с целью наиболее эффективного управления ими, а также для разграничения административных полномочий.

Каждый домен реализует собственную иерархию подразделений. Подразделения, принадлежащие к различным доменам, никак не связаны между собой.

Группы

Подразделения являются не единственным механизмом, который администратор может использовать для группировки объектов по некоторому признаку. Объекты, ассоциированные с пользователями, компьютерами и контактами, могут быть объединены в *группы* (groups). Это позволяет упростить процесс управления, поскольку администратор может в процессе управления сослаться на всю группу, а не указывать отдельные объекты. Наиболее часто группы упоминаются в контексте объединения пользователей. Тем не менее,

необходимо всегда помнить, что группа может включать в себя объекты следующих типов:

- пользователи (users);
- компьютеры (computers);
- контакты (contacts).

Домены Active Directory позволяют объединять объекты в группы двух типов: *группы безопасности* (security groups) и *группы рассылки* (distribution groups).

С каждой группой связано понятие *области действия* (group scope). Область действия определяет, в какой части леса доменов на данную группу можно ссылаться. Существуют три области действия групп:

- *доменная* область действия (domain local scope);
- *глобальная* область действия (global scope);
- *универсальная* область действия (universal scope).

Допускается преобразование группы из одного типа в другой. Возможно использование *вложенных групп* (nested groups), т. е. разрешается одни группы включать в состав других.

Охарактеризуем группы со всеми возможными областями действия.

- **Группы с доменной областью действия.** Этим группам могут назначаться разрешения *только в пределах того домена*, в котором они определены. Членами группы с доменной областью действия могут являться объекты, а также другие группы с любыми областями действия. Объекты, а также группы с глобальной и универсальной областью действия могут принадлежать к любому домену леса. В состав группы могут также входить группы с доменной областью действия, принадлежащие к тому же домену. Эти группы называются *доменными группами* (domain local group).
- **Группы с глобальной областью действия.** Группы с данной областью действия доступны (им могут назначаться разрешения) в рамках всего леса доменов. Членами группы могут являться объекты и группы с глобальной областью действия, принадлежащие к тому же домену, что и сама группа. Такие группы носят название *глобальных групп* (global group).
- **Группа с универсальной областью действия.** Эти группы также доступны в рамках всего леса доменов. В состав группы могут входить объекты, а также группы с универсальной или глобальной областью действия, принадлежащие к любому домену леса. Эти группы называются *универсальными группами* (universal group).

С каждой группой в момент создания ассоциируется объект каталога, значения атрибутов которого определяют ее характеристику. Один из атрибутов содержит список всех членов группы. В случае изменения состава группы будут реплицироваться не все значения атрибута (в случае, если группа насчитывает тысячи объектов, подобная репликация может вызвать заметный трафик), а только произведенные изменения. В данном случае речь идет о механизме *репликации связанных значений* (linked value replication). Этот механизм будет работать только в случае, когда лес доменов находится на функциональном уровне *Windows Server 2003*.

> **ПРИМЕЧАНИЕ**
>
> В данном разделе речь велась о группах доменов Active Directory. Однако на каждом компьютере имеются так называемые *локальные группы* (local group). Эти группы доступны только в пределах того компьютера, к которому они принадлежат, и разрешения им могут быть предоставлены только на локальном компьютере.

Режимы работы доменов (functional levels)

Домены Active Directory могут иметь разные *уровни функциональности* (functional levels), или *режимы работы*, что определяется версиями операционных систем, используемых на контроллерах доменов. От уровня работы домена зависит возможность выполнения некоторых функций, которые не реализуются на контроллерах предыдущих версий (Windows 2000 Server или Windows Server 2003).

Говоря о режимах или функциональных уровнях доменов (и леса), нужно сразу отметить некоторые важные моменты:

- невозможно понизить функциональный уровень домена (или леса) без переустановки Active Directory в этом домене (или полной реорганизации леса);
- после повышения уровня домена в домене нельзя создавать контроллеры на базе серверов более младших версий;
- необязательно, чтобы все домены в дереве работали на одном функциональном уровне (нужно только понимать, что невозможно, например, в лесу доменов, работающем в режиме *Windows Server 2008*, иметь домен уровня *Windows Server 2003*; это объясняется тем, что раздел Schema является общим для всего леса);

- функциональный уровень домена никак не влияет на работу клиентов — это касается аутентификации, доступа к ресурсам и т. д.

В следующей таблице перечислены возможные *функциональные уровни домена* и типы контроллеров домена, которые могут присутствовать или создаваться на этих уровнях.

Функциональный уровень домена	**Поддерживаемые контроллеры домена**
Windows 2000 native (основной режим)	Windows 2000, Windows Server 2003 и Windows Server 2008
Windows Server 2003	Windows Server 2003 и Windows Server 2008
Windows Server 2008	Только Windows Server 2008

Ниже описаны основные возможности, имеющиеся для различных режимов работы ***доменов*** Active Directory.

Режим работы домена	**Функциональные возможности**
Windows 2000 native (основной режим)	Создание вложенных групп безопасности Поддержка универсальных групп (членами которых могут быть учетные записи любого домена) История идентификаторов SID (SID history), которая необходима при миграции учетных записей Преобразование типов групп (групп безопасности и групп рассылки (distribution groups))
Windows Server 2003	Все возможности предыдущего режима Переименование контроллеров домена Регистрация времени входа пользователя в домен Создание новых учетных записей компьютеров и пользователей в произвольных контейнерах каталога (по умолчанию они создаются в контейнерах Users и Computers) Выборочная аутентификация (фильтрация полномочий пользователей и групп одного домена по отношению к ресурсам другого домена

(окончание)

Режим работы домена	Функциональные возможности
Windows Server 2008	Все возможности предыдущего режима Использование службы DFS Replication для репликации тома SYSVOL Регистрация всей информации о времени входа пользователя в домен, включая имя его рабочей станции и количество неудачных попыток Назначение политик паролей пользователям и глобальным группам безопасности

Полностью отсутствует режим работы Windows 2000 mixed (смешанный), это означает, что ***контроллеры на базе Windows NT Server 4.0 не могут находиться в доменах*** вместе с контроллерами Windows Server 2008.

Функциональные уровни леса определяют возможности, имеющиеся для всех доменов леса. Ниже перечислены имеющиеся функциональные уровни леса и поддерживаемые в них контроллеры домена.

Функциональный уровень леса	Поддерживаемые контроллеры домена	Функциональные уровни для существующих или новых доменов
Windows 2000	Windows 2000, Windows Server 2003 и Windows Server 2008	Любые из перечисленных выше
Windows Server 2003	Windows Server 2003 и Windows Server 2008	Windows Server 2003 и Windows Server 2008
Windows Server 2008	Только Windows Server 2008	Только Windows Server 2008

В следующей таблице указаны возможности для каждого режима работы ***леса*** доменов Active Directory.

Режим работы леса	Функциональные возможности
Windows 2000	Все стандартные опции
Windows Server 2003	Все возможности предыдущего режима Доверительные отношения на уровне лесов Переименование доменов Репликация каталога на уровне свойств элементов каталога Возможность установки контроллеров только для чтения (RODC) на базе Windows Server 2008 Улучшенные алгоритмы механизмов репликации (Knowledge Consistency Checker (KCC) и Intersite Topology Generator (ISTG)) Возможность создания специальных групп для авторизации на основе ролей Деактивация и переопределение атрибутов и классов в схеме каталога
Windows Server 2008	Все возможности предыдущего режима. Пока новые возможности отсутствуют; все новые домены по умолчанию будут функционировать в режиме Windows Server 2008

Физическая структура каталога

Крупные сети представляют собой совокупность подсетей, соединенных между собой коммуникационными линиями с различной пропускной способностью. В этом случае возникает задача оптимизации трафика по каналам связи. Недостаточная пропускная способность отдельных линий может стать причиной возникновения проблем с поиском объектов, аутентификацией пользователей, а также репликацией изменения каталога.

Сайты и подсети

Физическая структура каталога определяется физической структурой сети. В зависимости от пропускной способности коммуникационных линий сеть

делится на области, получившие название сайтов. *Сайт* (site) представляет собой совокупность *подсетей*, соединенных между собой высокоскоростными линиями связи. Предполагается, что сайты соединяются друг с другом каналами с небольшой пропускной способностью.

> ***Примечание***
>
> Под термином "подсеть" в данном случае понимается подсеть IP. Администратор может создать в каталоге объекты, ассоциируемые с подсетями. Границы сайта описываются именно этими объектами.

Физическая структура сети не связана с *логической* структурой доменов Active Directory. Сайты представляют собой самостоятельные образования, не зависящие от пространства имен доменов. Это означает, что принадлежность объекта к тому или иному сайту не влияет на его положение в каталоге. Выбор того или иного сайта определяется, прежде всего, тем, в какой подсети физически находится данный объект. Например, в зависимости от того, на каком компьютере пользователь входит в сеть, он может рассматриваться как находящийся то в одном, то в другом сайте.

Поскольку структура сайтов реализуется независимо от структуры доменов, один домен может быть разделен на несколько сайтов и, напротив, один сайт может быть образован фрагментами нескольких доменов.

Структура сайтов является основным механизмом, посредством которого администратор может влиять на формирование топологии репликации (не создавая при этом новых доменов). Поскольку считается, что сайты соединяются друг с другом медленными линиями связи, репликация изменений внутри сайта и между сайтами имеет несколько различий. Внутри сайта контроллеры домена соединены линиями с высокой пропускной способностью. Соответственно, произведенные изменения могут сразу же реплицироваться между контроллерами домена. Для репликации между сайтами обычно применяется передача изменений по определенному расписанию.

При входе пользователя в сеть его аутентификация осуществляется ближайшим контроллером домена. В процессе обнаружения ближайшего контроллера домена в первую очередь используется информация о сайте, к которому принадлежит компьютер, запрашивающий аутентификацию. Ближайшим считается контроллер домена, расположенный в том же сайте, что и аутентифицируемый пользователь.

Важное место в процессе аутентификации занимает также *сервер Глобального каталога*. Поэтому рекомендуется в каждом сайте размещать как мини-

мум один сервер Глобального каталога, хотя это требование можно обойти, используя кэширование универсальных групп (или вообще отключив обращение к Глобальному каталогу при аутентификации). Многие компоненты доменов Active Directory (а также пользователи) используют серверы Глобального каталога для поиска объектов. В случае если доступ к серверу Глобального каталога осуществляется через линии связи с низкой пропускной способностью, многие операции службы каталога будут выполняться медленно.

В ходе создания леса доменов мастером установки Active Directory автоматически создается сайт по умолчанию с именем Default-First-Site-Name (это имя можно свободно изменить). Формируя физическую структуру сети, администратор должен самостоятельно создать новые сайты и задать для них границы, создав объекты, ассоциированные с имеющимися подсетями IP. В процессе создания нового контроллера на основании выделенного ему IP-адреса служба каталога автоматически отнесет его к соответствующему сайту. При этом в разделе конфигурации каталога в рамках данного сайта будет создан объект класса *Server*, связанный с контроллером домена.

Соединения и связи сайтов

Топология репликации формируется при помощи специального класса объектов — *соединений*, или *подключений* (connections). Соединение представляет собой однонаправленное соглашение между двумя контроллерами домена о передаче изменений. С каждым соединением связан объект в разделе конфигурации каталога. Атрибуты объекта, ассоциированного с соединением, определяют передающего партнера по репликации, а также расписание репликации и используемый при этом транспорт. Все соединения автоматически генерируются системным сервисом *Knowledge Consistency Checker*[1], KCC, который проверяет существующую топологию и доступность имеющихся соединений и при необходимости вносит соответствующие коррективы.

Контроллеры домена, расположенные в различных сайтах и взаимодействующие между собой в процессе репликации, называются *серверами-плацдармами*, или *серверами-форпостами* (bridgehead server). В каждом сайте один из контроллеров домена берет на себя обязанности по управлению входящими соединениями для всех серверов-плацдармов сайта. Этот контроллер домена называется *генератором топологии между сайтами* (Inter-

[1] В справочной системе этот сервис называется "Проверка согласованности знаний (KCC)".

Site Topology Generator, ISTG). Если контроллер домена, выполняющий функции ISTG, становится недоступен (например, выходит из строя), эта функция автоматически возлагается на другой контроллер домена.

В случае репликации между сайтами используется термин *связь сайтов* (site link), который описывает соединения двух и более узлов, способных обмениваться информацией при помощи единого транспорта. Связь узлов используется для задания стоимости соединения (cost), расписания репликации и транспорта. Механизм стоимостей позволяет оценить связь сайтов с точки зрения доступности коммуникационных линий и их пропускной способности. Если имеется несколько связей сайтов, для репликации будет выбрана та, что обладает меньшим значением стоимости.

Несколько связей сайтов, использующих единый транспорт, образуют *мост связей сайтов* (site link bridge). Использование мостов связей сайтов полезно в больших сетях, поскольку избавляет от необходимости описывать все возможные комбинации соединений между каждым из сайтов.

Серверы глобального каталога

Глобальный каталог (Global Catalog, GC) представляет собой базу данных, содержащую фрагменты всех доменных контекстов имен, образующих пространство имен каталога. Глобальный каталог является важной и неотъемлемой частью Active Directory, в нем содержатся сведения обо *всех* объектах, принадлежащих ко *всем* доменным контекстам имен. Однако в Глобальном каталоге хранятся не все объекты целиком, а только подмножество их атрибутов. Выбираются те атрибуты, которые чаще всего присутствуют в запросах пользователей.

Атрибуты, размещаемые в Глобальном каталоге, определяются схемой каталога. Администратор может определить для размещения в Глобальном каталоге дополнительные атрибуты. Однако необходимо помнить, что расширение числа атрибутов, заносимых в Глобальный каталог, приводит к росту его объема.

Процесс добавления нового атрибута для размещения в Глобальном каталоге влечет за собой синхронизацию всех его реплик. Если лес находится на функциональном уровне *Windows Server 2003* и выше, добавление нового атрибута приведет к репликации только этого атрибута на все носители Глобального каталога. Если же лес находится на функциональном уровне *Windows 2000*, добавление нового атрибута приводит к полной синхронизации всех реплик Глобального каталога.

Контроллеры домена, выполняющие функции носителя Глобального каталога, принято называть *серверами Глобального каталога* (Global Catalog server). При этом на контроллере домена создается дополнительный раздел, который используется для размещения Глобального каталога. Глобальный каталог хранится в том же файле (ntds.dit; по умолчанию в папке *%SystemRoot%*\NTDS), что и реплика самого каталога Active Directory. Для его тиражирования на другие серверы Глобального каталога используется стандартная топология репликации, генерируемая для каталога Active Directory.

Сервер Глобального каталога выполняет две основных функции.

- **Поиск объектов.** Клиенты могут обращаться к Глобальному каталогу с запросами на поиск объектов, основываясь на известных значениях атрибутов. Глобальный каталог хранит в себе информацию обо всех доменных разделах леса, поэтому он позволяет осуществлять поиск объектов по *всему* лесу доменов.
- **Аутентификация пользователей.** Сервер Глобального каталога предоставляет информацию о членстве пользователя в различных группах с универсальной областью действия (universal group). Эта информация требуется в процессе аутентификации пользователя. Именно на основании членства пользователя в тех или иных группах происходит назначение прав доступа. Более того, сервер Глобального каталога необходим в том случае, если для регистрации в системе пользователь использует свое основное имя (UPN). Если сервер Глобального каталога оказывается недоступным, то контроллер домена, осуществляющий аутентификацию, не будет располагать данными, необходимыми для авторизации пользователя. В результате пользователю будет отказано в регистрации. Исключение составляют члены группы Domain Admins (Администраторы домена), аутентификация которых осуществляется даже в том случае, когда сервер Глобального каталога недоступен.

В лесу доменов должен быть как минимум один сервер Глобального каталога. Поэтому по умолчанию его обязанности возлагаются на первый контроллер домена, установленный в лесу доменов. Тем не менее, любой контроллер домена может быть сконфигурирован в качестве сервера Глобального каталога. Это может быть сделано в силу различных причин. Например, чтобы снизить нагрузку на медленные линии связи, обычно принято устанавливать как минимум по одному серверу Глобального каталога для каждого сайта.

Механизмы репликации каталога

Каталог Active Directory является распределенной сетевой базой данных. Каждый контроллер домена является носителем копии каталога. При этом каждая из копий является полнофункциональной. Это означает, что каждый контроллер домена может вносить изменения в собственную копию каталога. Все произведенные изменения должны быть автоматически распространены на другие копии. Служба каталога должна располагать механизмом, который бы обеспечил поддержание отдельных копий каталога в согласованном состоянии. В подобных случаях традиционно используют механизм синхронизации, основанный на обмене между носителями копии каталога информацией об изменениях. Поскольку на каждый носитель каталога передается копия (реплика) изменений, этот процесс получил название *репликации* (replication) изменений.

Разделы каталога

С точки зрения механизма репликации каталог Active Directory представляет собой не цельную иерархическую структуру, а отдельные фрагменты, которые, являясь частью каталога, образуют самостоятельное дерево. В терминологии службы Active Directory подобная совокупность ветвей называется *прилегающим поддеревом* (contiguous subtree) или *контекстом имен* (naming context).

Разделение пространства имен каталога на фрагменты позволяет оптимизировать процесс синхронизации копий каталога между множеством его носителей. Это достигается за счет того, что в каждом контексте имен хранится информация определенного вида. По умолчанию каталог Active Directory поделен на три контекста имен, которые называются *разделами каталога* (directory partition):

- **доменный раздел каталога**, или *раздел доменных имен* (domain partition), используется для размещения информации о сетевых ресурсах, принадлежащих к определенному домену. Реплики доменного раздела располагаются на всех контроллерах указанного домена. Соответственно изменения, происходящие в этом разделе, реплицируются только на эти реплики;
- **раздел схемы** (Schema partition). Понятие схемы каталога было дано в начале главе. Для ее хранения используется специальный объект каталога. Поскольку схема является общей для всех доменов леса, изменения в ней распространяются на все контроллеры всех доменов;

- **раздел конфигурации** (Configuration partition) содержит информацию, используемую различными системными службами, в том числе и самой службой каталога. В частности, в разделе конфигурации хранится информация, описывающая топологию репликации между контроллерами домена. Эта информация необходима для успешного функционирования службы каталога в целом, поэтому изменения в данном разделе реплицируются на все контроллеры в лесу доменов.

Реплики трех указанных разделов каталога присутствуют в обязательном порядке на *всех* контроллерах домена. Доменный раздел каталога индивидуален для каждого домена. Реплики раздела схемы и раздела конфигурации одинаковы для всех контроллеров домена в лесу.

Разделы схемы и конфигурации существуют также во всех экземплярах служб Active Directory Lightweight Directory Services (Службы Active Directory облегченного доступа к каталогам (AD LDS). Контекст имен, или контекст именования по умолчанию (default naming context), необязателен в момент создания экземпляра служб, но без него использование каталога невозможно (поскольку в этом случае каталог не сможет выполнять свою главную задачу информационного хранилища).

> ***Примечание***
>
> На серверах глобального каталога присутствует еще один раздел — содержащий подмножество атрибутов объектов всех доменных разделов каталога. При этом со стороны клиентов данный раздел доступен только для чтения информации.

Любой контроллер домена Active Directory может производить изменения в собственных репликах каталога в любой момент времени. При этом все произведенные изменения будут синхронизированы с другими репликами. Подобная модель репликации получила название *репликации с множеством равноправных участников* (multimaster replication). Вышесказанное не относится к RODC-контроллерам, изменения на которых не реплицируются на другие контроллеры.

Разделы приложений

Дополнительно к перечисленным выше разделам, в доменах Active Directory на базе серверов Windows Server 2003 и Windows Server 2008 могут быть созданы особые разделы, которые получили название *разделов приложений* (application directory partitions). Разделы приложений могут быть созданы при

необходимости администратором, либо непосредственно самими приложениями. В разделе приложений могут быть размещены любые объекты, определения которых содержатся в схеме, за исключением субъектов подсистемы безопасности (таких, например, как учетные записи пользователей или компьютеров).

Служба каталога Active Directory, реализованная на базе Windows 2000 Server, использовала для размещения информации приложений доменные разделы и раздел Configuration. Это приводило к тому, что прикладные данные реплицировались на все контроллеры домена (даже когда этого и не требовалось). Изменение этой информации приводило к синхронизации всех копий каталога и могло стать причиной интенсивного трафика репликации.

Использование разделов приложений позволяет сократить накладные расходы, вызванные репликацией. В отличие от трех основных разделов каталога, реплицируемых на все контроллеры домена, разделы приложений могут располагаться на строго оговоренных контроллерах. Администратор может перечислить контроллеры домена, на которые необходимо разместить копии определенного раздела каталога. Приложениям зачастую не требуется, чтобы размещенная ими в каталоге информация была доступна повсеместно в сети. Существуют приложения, применение которых ограничено отдельным доменом или деревом доменов. Если приложение, для которого создается раздел, используется только в двух доменах леса, то копии раздела приложения должны быть размещены только на контроллерах домена двух указанных доменов. Контроллеры других доменов не будут содержать данный раздел.

Имеются два встроенных раздела приложений, которые используются службой DNS для размещения содержимого зон, интегрированных с Active Directory. Это разделы ForestDnsZones.*forestName* и DomainDnsZones.*forestName*. При этом вместо суффикса *forestName* в имени раздела указывается DNS-имя корневого домена леса.

Формирование топологии репликации

Процесс репликации предполагает обмен изменениями в разделах каталога между отдельными участниками. Для обозначения односторонней передачи данных от одного партнера по репликации к другому используется термин *соединение* (connection). Соединение, или *подключение*, представляет собой однонаправленное соглашение о репликации, заключенное между двумя контроллерами домена.

Одним из наиболее ответственных моментов в работе подсистемы репликации является формирование инфраструктуры соединений между имеющимися контроллерами домена. Подобная инфраструктура называется *топологией репликации* (replication topology). Каждый раздел каталога строит свою собственную топологию репликации, используя при этом общие с другими разделами соединения или создавая собственные.

За формирование топологии репликации отвечает специальный системный процесс *Knowledge Consistency Checker*, KCC. Этот процесс выполняется на всех контроллерах домена. При этом KCC основывается на информации о физической структуре каталога (совокупности сайтов и связанных с ними подсетей). Периодически активизируясь, KCC проверяет доступность существующих соединений. Основываясь на полученных данных, KCC может переформировать топологию репликации для некоторого раздела каталога. Именно KCC отвечает за установление соединения с партнером по репликации. Соединения генерируются автоматически, хотя служба каталога допускает определение соединений непосредственно администратором.

Отдельно следует сказать про формирование топологии репликации для разделов приложений. Хотя администратор вручную определяет контроллеры, хранящие реплики этих разделов, генерация и поддержание топологии репликации для этих разделов осуществляются сервисом KCC автоматически.

Служба репликации файлов (FRS)

Каталог рассматривается как централизованное место хранения информации о сетевых ресурсах. Однако в силу определенных причин некоторая часть информации не может быть размещена в каталоге. Например, специальная сетевая папка NETLOGON (Logon server share) используется для хранения информации, необходимой для регистрации в сети. Эта папка предназначена для размещения перемещаемых или обязательных профилей пользователей, сценариев регистрации, групповых политик и т. п. Данная информация жизненно необходима для корректного функционирования сети. При этом требуется, чтобы эта папка присутствовала на всех контроллерах домена.

Служба репликации файлов (File Replication Service, FRS) представляет собой стандартный механизм репликации с множеством равноправных участников. На контроллерах домена служба FRS выполняет синхронизацию содержимого системного тома SYSVOL (Logon server share). Том SYSVOL создается на каждом сервере непосредственно в ходе повышения его до контроллера домена и используется для размещения системных файлов общего

доступа. В частности, именно внутри него располагается уже упоминавшаяся папка NETLOGON. Помимо этого, в томе SYSVOL размещаются все шаблоны доменных объектов групповой политики *(см. главу 13)*. В доменах, работающих в режиме *Windows Server 2008*, появилась новая возможность — для репликации тома SYSVOL можно использовать службу DFS Replication, что позволяет значительно уменьшить трафик репликации.

Создание системного тома SYSVOL

Том SYSVOL создается непосредственно в ходе повышения сервера до контроллера домена. Когда устанавливается первый контроллер домена в сети, в этой папке на основе имеющихся административных шаблонов создаются стандартные объекты групповых политик. Служба FRS извещает службу NETLOGON о том, что системная папка доступна для общего доступа. Только после этого сервер может использоваться как контроллер домена.

В случае установки последующих контроллеров домена после создания тома SYSVOL служба репликации файлов осуществляет его наполнение. Содержимое тома копируется с уже существующего контроллера домена. Только после этого сервер сможет объявить себя новым контроллером домена.

> ***Внимание!***
>
> По умолчанию том SYSVOL размещается непосредственно внутри системной папки *%SystemRoot%*. Однако в процессе повышения роли сервера до контроллера домена администратор может указать любое другое место расположения этого тома. Единственное условие — том должен находиться на NTFS-разделе.

Топология каталога и служба FRS

Для своей работы служба FRS запрашивает информацию о физической структуре службы каталога, серверах каталога и соединениях между ними. Другими словами, служба репликации файлов не создает своей инфраструктуры, а использует топологию репликации каталога для собственных целей. В частности, служба репликации файлов задействует объекты, ассоциированные с соединением (connection objects), для передачи файлов. При этом учитывается расписание репликации, определенное в рамках этих объектов.

Внимание!

Необходимо понимать, что фактически механизм репликации службы каталога и служба репликации файлов представляют собой две различных службы, действующие независимо друг от друга. Об этом особенно важно помнить при работе с объектами групповых политик (GPO), поскольку они имеют две части: "доменную", хранящуюся в каталоге Active Directory, и "файловую", хранящуюся на диске в томе SYSVOL. Если изменения в одной части не синхронизированы с изменениями в другой (скажем, из-за ошибок репликации в одной из служб), целостность объекта GPO нарушается.

Конфигурирование службы DNS для развертывания доменов Active Directory

Рассмотрим некоторые особенности настройки службы DNS, обеспечивающей работу доменов Active Directory. В силу того, что существует множество сетевых конфигураций и требований к корпоративной сети, сложно дать однозначные рекомендации по настройке DNS. Поэтому мы рассмотрим основные соображения, которые администратор должен учитывать при конфигурировании сети.

Автоматическая настройка DNS-сервера

Простейшая ситуация — когда при создании первого контроллера в лесу доменов разрешается установка DNS-сервера. В этом случае мастер установки Active Directory после установки служб каталога сам устанавливает и конфигурирует DNS-сервер на этом контроллере (см. рис. 12.9), используя DNS-имя корневого домена.

Помимо трех стандартных разделов каталога, создаются два специализированных раздела приложений, используемых службой DNS. Для хранения SVR-записей, необходимых для работы всего леса, создается дополнительная зона, имя которой частично совпадает с именем основной авторитетной зоны (с именем корневого домена леса) — _msdcs.<*DNSимяДомена*>. После перезагрузки контроллера домена все ресурсные записи регистрируются на DNS-сервере. Полученный результат для домена intern.dom представлен на рис. 12.1.

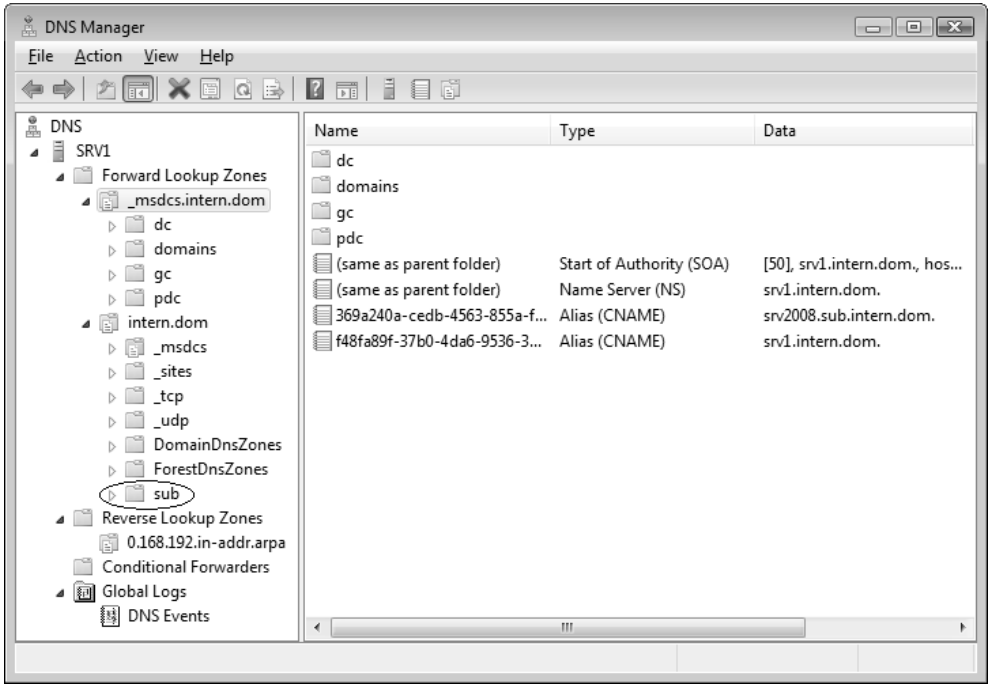


Рис. 12.1. Зоны DNS для корневого домена леса intern.dom, созданные и сконфигурированные мастером установки Active Directory

Важно понимать, что хотя в пространстве DNS-имен *поддомен* _msdcs в составе корневой зоны выполнял бы те же функции, что и *зона* _msdcs.intern.dom, с точки зрения способов хранения зон разница принципиальная. Все поддомены зоны intern.dom (они имеют значок обычной папки) хранятся внутри этой зоны (в файле или в Active Directory). Самостоятельная зона _msdcs.intern.dom, хоть и представлена внутри зоны intern.dom специальным значком , хранится совершенно независимо от нее.

Зона intern.dom по умолчанию находится в разделе приложений DC=DomainDnsZones,DC= intern,DC=dom, а зона _msdcs.intern.dom хранится в разделе DC=ForestDnsZones,DC= intern,DC=dom[1]. (Это несложно проверить, подключившись к каждому разделу с помощью оснастки **ADSI Edit** (Редактирование ADSI).)

[1] Имена этих разделов являются зарезервированными (поскольку используются особым образом), и не следует создавать собственные разделы с такими именами.

Обе зоны являются интегрированными в Active Directory, для них разрешены только безопасные обновления (Secure only). Зона _msdcs.intern.dom реплицируется на все DNS-серверы *леса* intern.dom (опция **All DNS servers in this forest**), а зона intern.dom реплицируется на все DNS-серверы *домена* intern.dom (опция **All DNS servers in this domain**).

Это означает, что при установке DNS-сервера на контроллере домена intern.dom этот контроллер автоматически станет хранителем реплики раздела приложений DC=DomainDnsZones,DC= intern,DC=dom, и — как следствие — этот сервер получит копию зоны intern.dom (и, разумеется, всех других зон, хранящихся в этом разделе приложений).

Аналогично, при установке DNS-сервера на контроллере любого домена леса intern.dom (кроме корневого домена леса) этот контроллер автоматически станет хранителем реплики раздела приложений DC=ForestDnsZones, DC= intern,DC=dom, и этот сервер получит копию зоны _msdcs.intern.dom (и других имеющихся зон).

Внимание!

Дополнительные DNS-серверы загружают интегрированные в Active Directory зоны при своей перезагрузке. Поэтому после установки DNS-сервера может потребоваться его перезапуск.

В принципе для хранения DNS-зон можно использовать и собственные, специально созданные разделы приложений. В этом случае реплики разделов нужно создавать вручную.

Примечание

Обратите внимание на то, что хотя зона обратного просмотра и имеется в папке Reverse Lookup Zones — как рекомендуемый вариант — она была создана вручную, а мастер установки Active Directory не создает обратных зон на сервере DNS.

Службу DNS можно установить заранее и создать авторитетную зону для корневого домена нового леса Active Directory. При этом неважно, на каком компьютере установлен DNS-сервер — на отдельном компьютере или на будущем контроллере домена — конфигурация DNS-зон будет отличаться от той, которая была описана в предыдущем разделе.

Создание дополнительных доменов

Если после создания корневого домена в лесу появляются новые домены, то настройка службы DNS зависит от имен этих доменов:

- для нового дерева с *несмежным именем* авторитетную зону на DNS-сервере следует предварительно создать вручную, учитывая способ хранения и область репликации. Пример такой зоны показан на рис. 12.2;

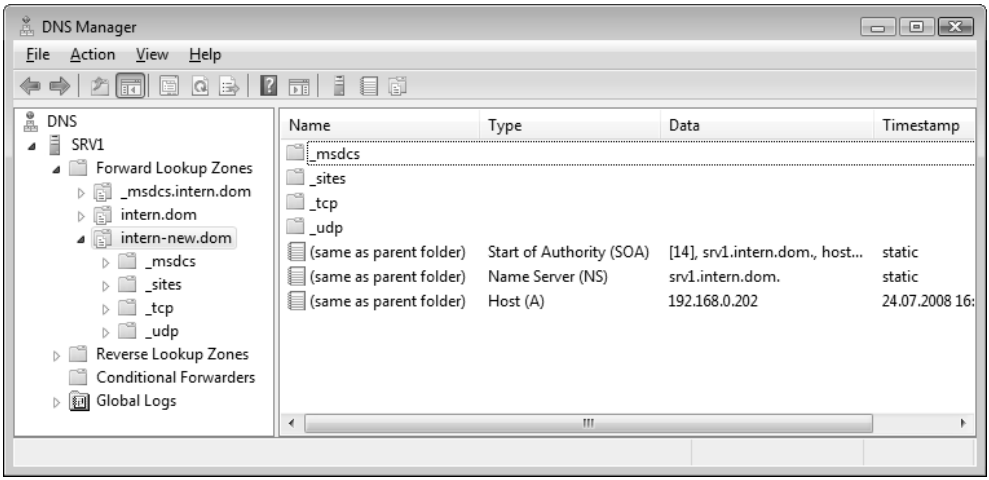


Рис. 12.2. Авторитетная зона для нового дерева доменов

- DNS-поддомены в авторитетной зоне дерева доменов Active Directory создаются на DNS-сервере автоматически при создании первого контроллера *дочернего домена*. На рис. 12.1 отмечена зона домена sub.intern.dom (входящего в лес intern.dom). Поскольку на контроллере этого домена установлен DNS-сервер, то будет создан специальный раздел приложений DomainDnsZones.sub.intern.dom, содержимое которого будет реплицироваться только на DNS-серверы, работающие на контроллерах этого дочернего домена.

Для дочерних доменов можно заранее (до развертывания самих доменов) вручную создавать и независимые, авторитетные зоны. В этом случае их можно будет конфигурировать независимо от родительских зон.

Таким образом, можно видеть, что вариантов конфигурирования DNS для развертывания доменов Active Directory может быть очень много, и админи-

стратор легко может создать набор зон для различных доменных топологий и для разных конфигураций сетевой среды.

Проверка конфигурации DNS

Это один из самых важных этапов при подготовке сервера к операции повышения роли. Из-за скрытых ошибок в DNS созданный контроллер домена может работать неправильно, хотя причин для этого не так много. Возможны следующие ошибки:

- на компьютере не указан предпочитаемый сервер DNS;
- на предпочитаемом сервере DNS отсутствует нужная авторитетная зона (имя домена);
- авторитетная зона существует, но не является динамически обновляемой.

Мастер установки Active Directory проверяет конфигурацию DNS и может сообщать о найденных ошибках. В этом случае лучше прекратить процедуру создания контроллера и разобраться в причинах появления диагностических сообщений.

Не забывайте о том, что конфигурацию DNS (регистрацию SRV-записей) необходимо проверять и *по окончании* процесса повышения роли сервера. Поэтому тестирование контроллеров (например, с помощью утилит DCdiag и NetDiag) лишним не будет.

Установка и удаление контроллеров домена

Термины "создание контроллера домена", "установка доменных служб Active Directory" и "повышение роли сервера" (promotion) в некотором смысле являются синонимами, поскольку описывают один и тот же процесс (аналогично можно говорить об "удалении контроллера", "удалении Active Directory" или о "понижении роли контроллера"). Нельзя создать контроллер домена, не установив доменные службы Active Directory.

Контроллер домена можно понизить (demote) (или деинсталлировать доменные службы Active Directory) до рядового сервера домена (или автономного сервера) (а затем, при необходимости, снова повысить роль сервера). В обоих случаях используется мастер *Active Directory Installation Wizard* (Мастер установки Active Directory) (утилита DCpromo.exe).

Внимание!

Важным отличием реализации доменных служб Active Directory на базе серверов Windows Server 2008 является то, что служба каталога функционирует как самостоятельный системный сервис NTDS, и, следовательно, его можно останавливать и запускать независимо от других служб. Это позволяет выполнять обслуживание базы данных каталога без необходимости загрузки в режиме Directory Services Restore Mode.

Для анализа содержимого каталога (например, для определения, какие объекты были удалены) "снимки" базы данных Active Directory, полученные с помощью утилиты Ntdsutil.exe (директива Snapshot), можно "монтировать" (т. е. обеспечивать к ним доступ как к LDAP-серверу), используя утилиту *Dsamain.exe*, а затем просматривать при помощи утилиты Ldp.exe. Такая возможность появилась только в Windows Server 2008.

Итак, для создания контроллера домена Active Directory можно использовать следующие способы:

- запустить мастер установки Active Directory на уже установленной системе (на автономном или рядовом сервере — члене домена); с этим мастером можно работать в диалоговом режиме или же в режиме автоматической установки (unattended mode; *см. разд. 7.7*). В результате будет создан контроллер нового домена или дополнительный контроллер в уже существующем домене;
- обновить контроллер домена на базе Windows Server 2003. Утилита DCpromo.exe запускается автоматически после того, как закончится обновление системы до Windows Server 2008 и компьютер будет перезагружен.

Создание контроллеров в уже существующих доменах

Создание новых доменов Active Directory на базе Windows Server 2008 или установка дополнительных контроллеров в таких доменах сложностей не вызывает, эту процедуру мы подробно рассмотрим позже. Сначала рассмотрим такие случаи установки дополнительных контроллеров, которые имеют специфику или требуют дополнительных действий. Сюда включена и процедура обновления доменов Windows Server 2003, поскольку, как правило, в этом случае образуется "смешанная" среда контроллеров, имеющая свои особенности.

Обновление доменов Windows Server 2003

При обновлении имеющихся доменов Windows Server 2008 используется уже созданная топология доменов и существующая структура DNS, которая практически никак не меняется. Задача сводится к обновлению операционных систем на контроллерах домена до более старшей версии.

При обновлении домена Windows Server 2003 до Windows Server 2008 или при установке контроллера домена на базе Windows Server 2008 в лесу Windows Server 2003 сначала ***необходимо обновить схему***, другими словами — *подготовить* лес и домены. Без этого установка контроллеров Windows Server 2008 невозможна.

Процедура обновления схемы включает в себя такие операции:

- создание новых объектных классов и атрибутов;
- добавление новых атрибутов к уже существующим классам;
- модификация дескрипторов безопасности, назначаемых классам по умолчанию;
- изменение членов групп безопасности.

Этап 1. Сначала с помощью команды `adprep /forestprep` следует подготовить *лес*. Утилита командной строки Adprep.exe располагается на дистрибутивном диске Windows Server 2008 и в папке \sources\adprep. При этом команда должна выполняться на контроллере домена, являющемся владельцем FSMO-роли Schema Master. Все изменения должны быть реплицированы во всем лесу! ***Только после этого***, если указанная операция пройдет без ошибок, можно перейти к подготовке доменов. Ниже приведены сообщения, отображаемые в окне консоли при обновлении леса доменов[1] (утилита запускается с компакт-диска):

```
D:\sources\adprep>adprep /forestprep

ADPREP WARNING:

Before running adprep, all Windows 2000 Active Directory Domain Control-
lers in t he forest should be upgraded to Windows 2000 Service Pack 4
(SP4) or later.

[User Action]

If ALL your existing Windows 2000 Active Directory Domain Controllers
meet this requirement, type C and then press ENTER to continue. Other-
wise, type any other key and press ENTER to quit.
```

[1] Обратите внимание на имена LDF-файлов, совпадающие с номером схемы. Последняя версия — 44.

```
C

Opened Connection to SRV2003
SSPI Bind succeeded
Current Schema Version is 30
Upgrading schema to version 44
Connecting to "SRV2003"
Logging in as current user using SSPI
Importing directory from file "C:\WINDOWS\system32\sch31.ldf"
Loading entries.....................................
139 entries modified successfully.
... ... ...

The command has completed successfully
Connecting to "SRV2003"
Logging in as current user using SSPI
Importing directory from file "C:\WINDOWS\system32\sch44.ldf"
Loading entries............
11 entries modified successfully.

The command has completed successfully

................................................

Adprep successfully updated the forest-wide information.

D:\sources\adprep>
```

Все действия, выполняемые утилитой Adprep, регистрируются в журналах (папка *%SystemRoot%*\System32\Debug\Adprep\Logs), которые следует просмотреть в случае возникновения ошибок.

Этап 2. На втором этапе необходимо подготовить ***каждый*** домен: для этого на всех контроллерах, являющихся владельцами FSMO-роли Infrastructure Masters, нужно выполнить следующую команду:

```
D:\sources\adprep>adprep /domainprep /gpprep

Running domainprep ...

Adprep successfully updated the domain-wide information.

Adprep successfully updated the Group Policy Object (GPO) information.

D:\sources\adprep>
```

Внимание!

Нужно помнить о том, что домены Windows Server 2003 можно обновлять только тогда, когда они работают в режиме *Windows 2000 native*.

Добавление контроллеров на базе Windows Server 2003 в домены Windows Server 2008

Сервер Windows Server 2003 можно сделать контроллером существующего домена Windows Server 2008, ***если только*** домен имеет функциональный уровень *Windows 2000 native* и не выше. При создании нового домена на базе серверов Windows Server 2003 необходимо, чтобы функциональный уровень леса бы не выше *Windows 2000*. В других случаях при установке службы Active Directory будет возникать фатальная ошибка.

Добавление контроллеров на базе Windows Server 2008 в домены Windows Server 2003

Сервер Windows Server 2008 можно сделать контроллером существующего леса доменов Windows Server 2003 (в составе имеющегося домена или в качестве контроллера нового домена), ***если только*** этот лес подготовлен. То есть фактически операция создания нового контроллера является обновлением доменов до более высокой версии. Поэтому, как говорилось ранее, сначала нужно обновить схему и подготовить домены с помощью команд `adprep /forest` и `adprep /domain`. Только после этого можно создавать контроллеры на базе Windows Server 2008.

Требования и ограничения

Установка доменных служб Active Directory возможна только при выполнении некоторых важных условий. Мастер установки Active Directory проверяет различные параметры, зависящие от типа создаваемого контроллера домена. Основные условия для развертывания и эксплуатации доменов Active Directory перечислены ниже.

- Только член локальной группы Administrators (Администраторы) может запускать утилиту DCpromo на автономном сервере. На рядовом сервере — члене домена это право также имеют члены групп Domain Admins (Администраторы домена) и Enterprise Admins (Администраторы предприятия).
- Только члены группы Enterprise Admins (Администраторы предприятия) могут создавать новые домены (дочерние домены или новые деревья). Новый домен в лесу можно заранее создать с помощью утилиты NTDSutil

- Члены групп Domain Admins (Администраторы домена) и Enterprise Admins (Администраторы предприятия) могут добавлять контроллеры в существующий домен. Эту операцию можно разрешить и для отдельных пользовательских учетных записей, если дать им право подключать компьютеры к домену и создавать соответствующие объекты репликации.
- Необходимо иметь развернутую службу DNS. Если используется ранее существовавшая служба DNS, она должна отвечать требованиям Active Directory и быть сконфигурирована соответствующим образом. Если "повышаемый" сервер будет первым контроллером домена в сети, в которой отсутствуют серверы DNS, ***необходимо*** разрешить мастеру установки Active Directory установить роль DNS-сервера.

> ***Примечание***
>
> DNS-зоны обратного просмотра для работы Active Directory не требуются. Тем не менее, рекомендуется конфигурировать их, т. к. они используются многими утилитами и приложениями.

- NetBIOS-имя сервера должно быть уникальным в домене. NetBIOS имя нового домена должно быть уникальным в лесу.
- Если создается дочерний домен (или новое дерево), родительский домен и корневой домен леса должны уже существовать и быть доступны.

Запуск мастера установки Active Directory

Существуют два способа запуска мастера Active Directory Installation Wizard (Мастер установки Active Directory) в интерактивном режиме:

- запустить оснастку **Server Manager** (Диспетчер сервера) и установить роль Active Directory Domain Services (AD DS) (Доменные службы Active Directory);
- ввести команду `dcpromo` в меню **Start** (Пуск) в окне **Run** (Выполнить).

В любом случае на первом этапе только копируются двоичные файлы, а также устанавливаются некоторые службы (их запуск при этом запрещен), в том числе:

- *Active Directory Domain Services* (сервис NTDS);
- *Intersite Messaging* (сервис IsmServ);
- *Kerberos Key Distribution Center* (сервис kdc).

Эти файлы и службы останутся на сервере, даже если отказаться от установки контроллера. Чтобы убрать их полностью, следует удалить роль с помощью диспетчера сервера или посредством команды `dcpromo /uninstallBinaries`.

Примечание

Создавать и удалять контроллер домена можно и в автоматическом режиме, используя команду `dcpromo /answer:<файлОтветов>`. Пример файла ответов будет приведен ниже.

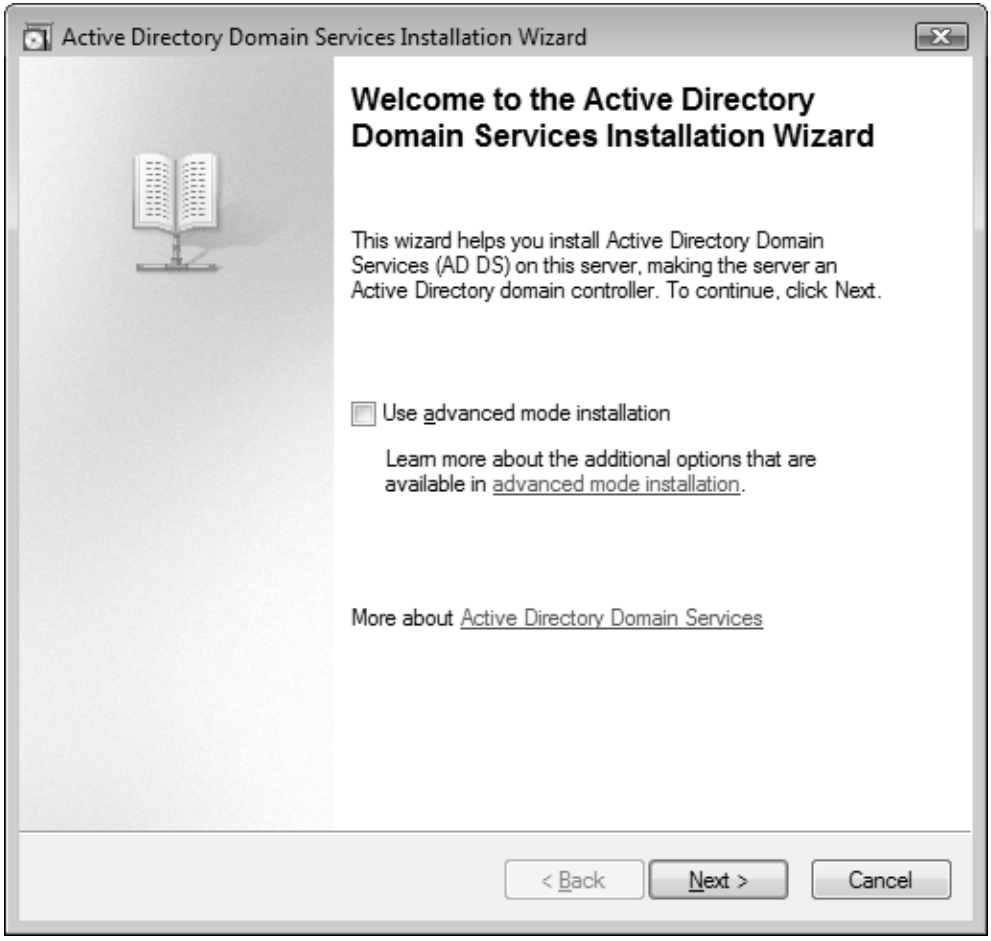


Рис. 12.3. Начальное окно мастера установки Active Directory

При добавлении роли из окна оснастки **Server Manager** (Диспетчер сервера) мастер установки Active Directory нужно запустить вручную (для этого на панели ролей имеется специальная ссылка). Если используется второй способ запуска, то после копирования двоичных файлов (при этом всегда отображается специальное информационное окно) появится первое окно мастера (рис. 12.3).

Флажок **Use advanced mode installation** (см. рис. 12.3) позволяет выключить дополнительные возможности при работе мастера установки Active Directory (это соответствует выполнению команды `dcpromo` с параметром `/adv`). Эти возможности перечислены в табл. 12.1.

Таблица 12.1. *Дополнительные возможности мастера установки Active Directory*

Этап установки	Дополнительные опции выбора параметров
Новый лес	**Domain NetBIOS name** (NetBIOS-имя домена)
Новый домен в существующем лесу	Новое дерево доменов с несмежными именами **Domain NetBIOS name** (NetBIOS-имя домена) **Source Domain Controller** (Исходный контроллер домена) (см. рис. 12.14)
Дополнительный контроллер домена в существующем домене	**Install from Media** (Установка из архива) (см. рис. 12.13) **Source Domain Controller** (Исходный контроллер домена) **Specify Password Replication Policy** (Указать политику репликации паролей) (только при установке RODC-контроллера) (см. рис. 12.15)
Создание учетной записи для RODC-контроллера	**Specify Password Replication Policy** (Указать политику репликации паролей)
Связывание сервера с учетной записью RODC-контроллера	**Install from Media** (Установка из архива) **Source Domain Controller** (Исходный контроллер домена)

Мы рассмотрим работу мастера в "полном" режиме; если установка контроллера домена осуществляется в обычном режиме, то нужно помнить о том, что некоторые параметры будут устанавливаться по умолчанию и определенные возможности (перечисленные в табл. 12.1) будут недоступны.

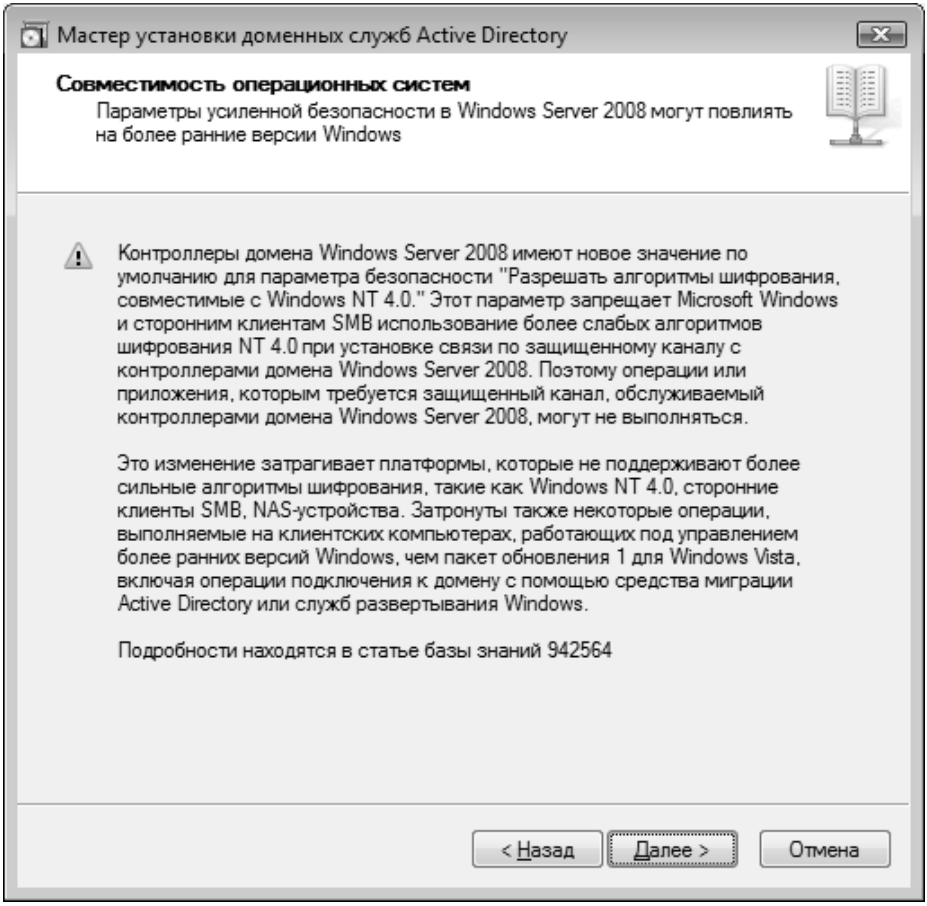


Рис. 12.4. Предупреждение о возможных проблемах совместимости систем

Первое, что делает мастер установки Active Directory — предупреждает о новых значениях параметров безопасности, которые могут помешать клиен-

там подключаться к доменам (рис. 12.4[1]). Нужно учесть все соображения, изложенные в указанной статье базы знаний.

В общем случае при установке Active Directory существуют четыре возможности (рис. 12.5); от выбора опции зависят дальнейшие шаги установки и параметры, которые потребуется ввести на этих этапах.

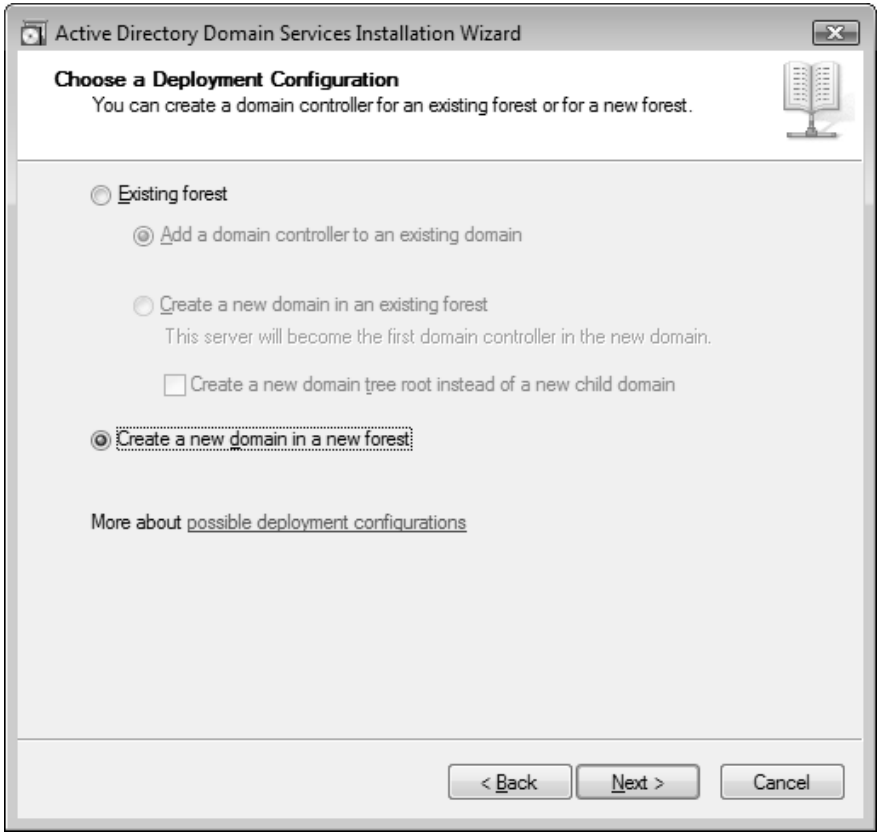


Рис. 12.5. Выбор местоположения нового контроллера в топологии доменов Active Directory

Каждый вариант интуитивно понятен, и требуется лишь ответить на вопросы мастера. Мы рассмотрим начальное развертывание доменов Active Directory,

[1] Чтобы не было недопонимания, и читатели смогли лучше осознать важность данного момента, специально показано окно из *локализованной* версии сервера.

поскольку это самый ответственный этап и некоторые критически важные операции в других случаях будут уже отсутствовать.

Итак, имеются следующие варианты создания доменов и установки нового контроллера домена[1]:

- новый лес доменов:
  - **Create a new domain in a new forest** (Создать новый домен в новом лесу) — корневой домен леса (intern.dom);
- уже существующий лес доменов (опция **Existing forest**):
  - **Add a domain controller to existing domain** (Создать контроллер домена в существующем домене) — дополнительный контроллер в любом имеющемся домене;
  - **Create a new domain in an existing forest** (Создать новый домен в существующем лесе) — дочерний домен любого имеющегося домена (sub.intern.dom);
  - **Create a new domain tree root instead of a new child domain** (Создать новое корневое дерево доменов вместо нового дочернего домена) — новое дерево несмежных имен, т. е. отличающихся от имени корневого домена существующего леса (intern-new.dom).

Примечание

Создание нового леса — это единственная опция, которая не требует связи с уже существующим доменом. Во всех других случаях разделы Schema и Configuration реплицируются с некоторого контроллера — источника существующего домена (при создании дополнительного контроллера) или родительского домена (при создании дочернего домена), либо в корневом домене (при создании нового дерева). Даже если контроллер на базе устанавливается из архивной копии, некоторые из существующих контроллеров домена должны быть доступны (те контроллеры, которые выполняют специфические FSMO-роли).

Далее процедура установки контроллера домена будет выглядеть следующим образом (рассматривается создание нового леса):

1. Необходимо ввести имя корневого домена леса (рис. 12.6). В зависимости от сделанного ранее выбора это имя будет использоваться для создания

[1] Имена доменов условные, выбраны для примера.

нового леса или нового дерева доменов или же в качестве родительского имени для других случаев. К этому моменту необходимо точно определиться в выборе DNS-имен, а также понимать, какое полное DNS-имя получит новый контроллер домена. Мастер проверит существование в сети указанных DNS- и NetBIOS-имен, и в случае отсутствия конфликтов позволит продолжить работу.

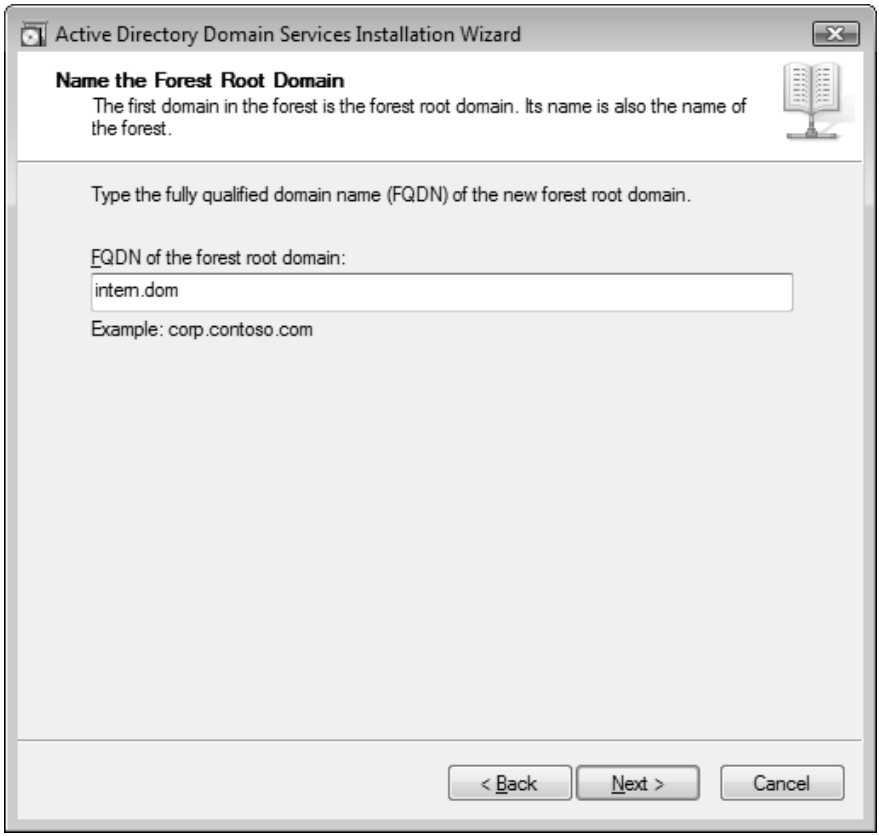


Рис. 12.6. Выбор имени корневого домена леса

2. На следующем шаге можно (в случае необходимости!) скорректировать NetBIOS-имя создаваемого домена. По умолчанию оно генерируется из DNS-имени (например, для домена intern.dom будет выбрано имя INTERN). (Этот шаг отсутствует в обычном режиме работы мастера установки.)

3. Можно сразу установить функциональный уровень (режим работы) нового *леса*, отличный от "минимального" (рис. 12.7). Соответственно все домены, создаваемые в этом лесу, должны (и будут) иметь уровень не ниже указанного на этом этапе.

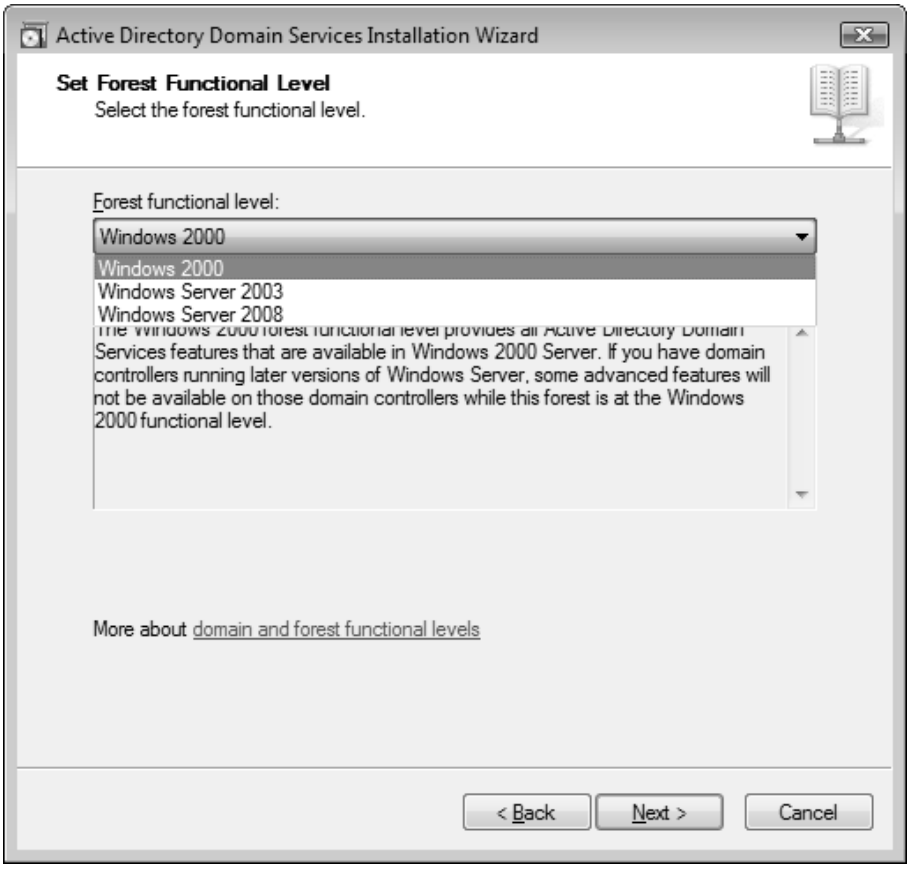


Рис. 12.7. Выбор функционального уровня нового леса

4. Функциональный уровень нового *домена* также можно задать сразу при установке контроллера (рис. 12.8). В принципе, он может отличаться от режима работы всего леса (но не быть выше). Требуемый уровень выбирается в раскрывающемся списке; в поле, расположенном под ним, перечисляются возможности, доступные для каждого режима работы домена.

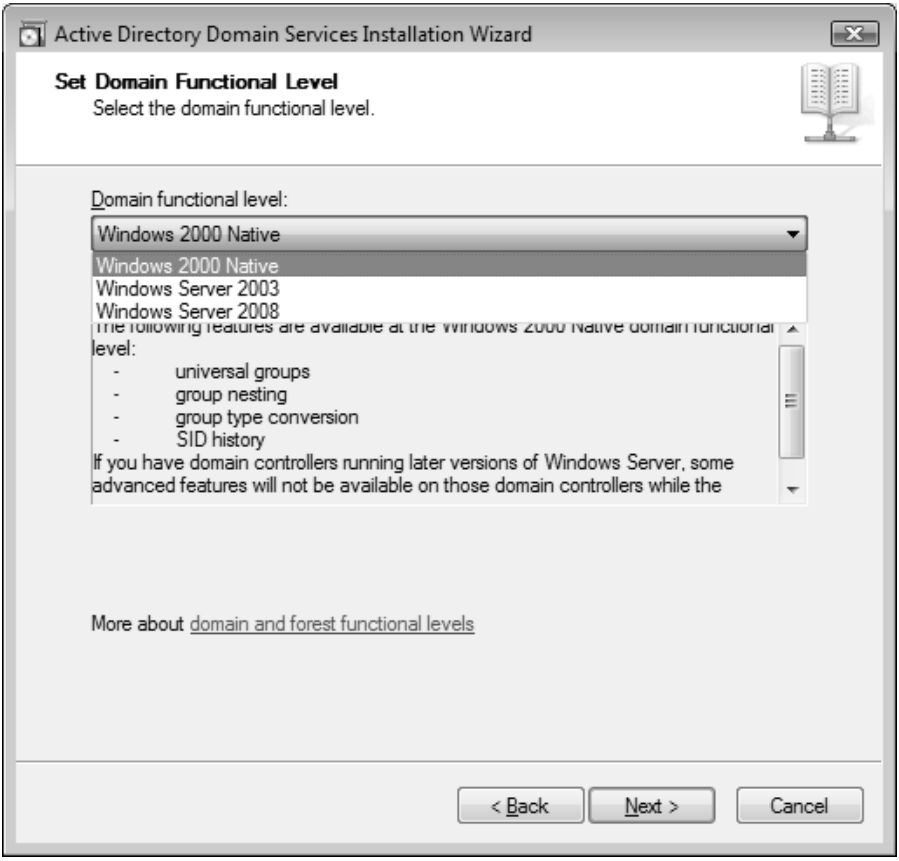


Рис. 12.8. Определение функционального уровня нового домена

5. Затем мастер проверяет конфигурацию DNS, и если сервер DNS не установлен или в развернутой службе DNS отсутствуют записи для создаваемого леса, то предлагает установить роль *DNS Server* и сконфигурировать DNS-сервер на данном компьютере (рис. 12.9).

   Если служба DNS в сети имеется и не планируются ее изменения, то опцию установки DNS-сервера следует отключить. Также на этом этапе можно указать, будет ли контроллер домена сервером Глобального каталога, и должен ли он быть RODC-контроллером (доступным только для чтения) (эта опция доступна только при запуске мастера установки с дополнительными возможностями и если домен работает в режиме Windows Server 2003 и выше). При создании RODC-контроллеров рекомендуется

устанавливать DNS-сервер, чтобы в домене сохранялась возможность разрешения имен при потере связи с другими доменами.

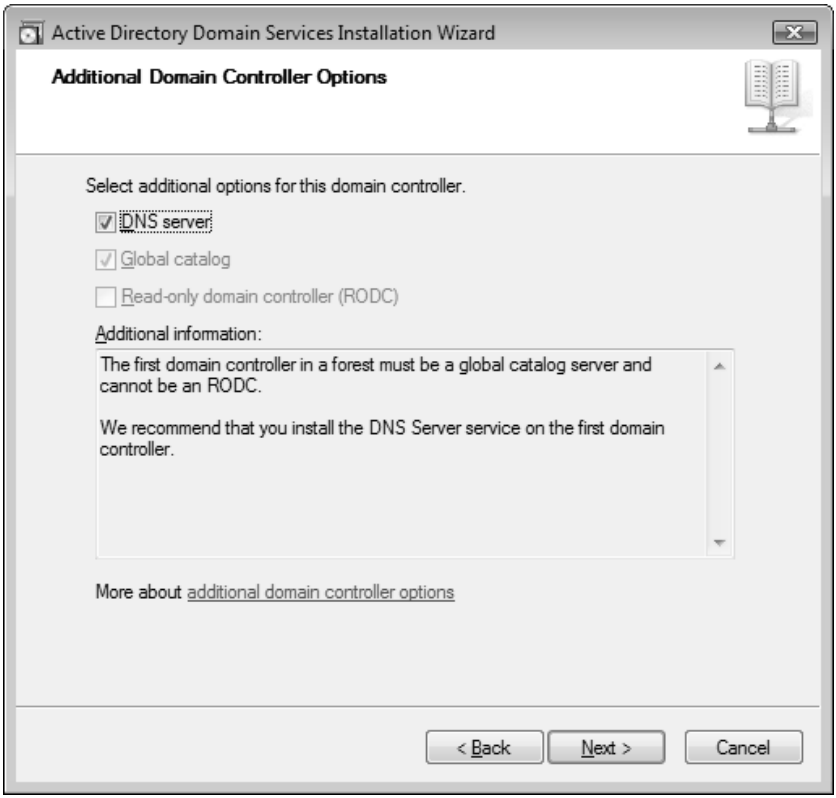


Рис. 12.9. Выбор дополнительных свойств нового контроллера домена

6. На следующем этапе мастер проверяет конфигурацию службы DNS. Если появляется сообщение о невозможности регистрации имени нового контроллера домена (рис. 12.10), то необходимо понять причину подобного сообщения, поскольку в противном случае установка контроллера может оказаться неудачной. Например, такая ошибка может возникнуть, если на предпочитаемом DNS-сервере отсутствует авторитетная зона для нового дерева доменов (мастер установки Active Directory такие зоны автоматически не создает). Возможно, нужно проверить разрешение DNS-имен для данного сервера. Продолжить создание контроллера домена без установки DNS-сервера можно, но только в случае полного понимания ситуации, и

если нормальная регистрация всех служебных записей в системе DNS будет обеспечена в дальнейшем.

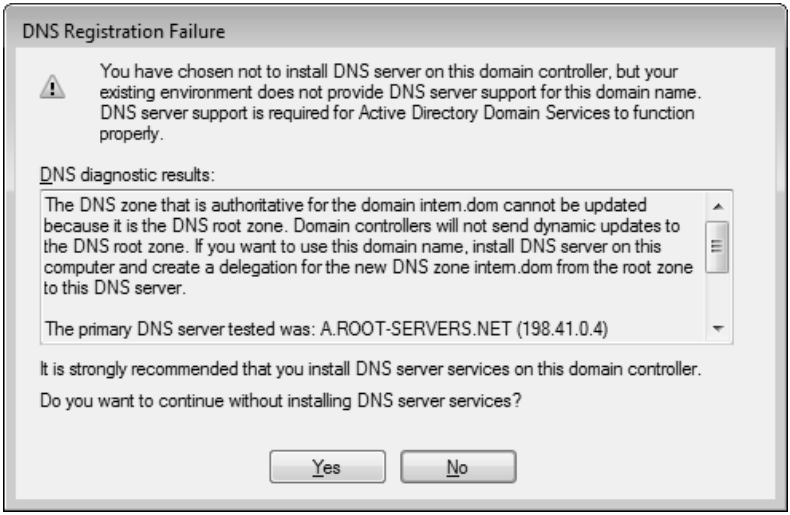


Рис. 12.10. Ошибка регистрации имени контроллера в службе DNS

7. Необходимо указать местоположение файлов базы данных Active Directory, журналов и тома SYSVOL (рис. 12.11). На контроллерах с очень большой нагрузкой (десятки тысяч пользователей) эти файлы могут находиться на разных физических дисках. Лучше сразу определиться с выбором местоположения файлов, поскольку *после* создания контроллера это можно будет сделать не так просто (только с помощью утилиты Ntdsutil).
8. Далее мастер попросит установить пароль *администратора для режима восстановления каталога* (Directory Services Restore Mode Administrator). Эта учетная запись ***отличается от стандартной встроенной записи Administrator*** (Администратор) и используется при загрузке системы в режиме Directory Services Restore Mode (см. рис. 15.17).
9. В следующем окне мастера (рис. 12.12) нужно проверить правильность выбранных параметров. В случае ошибок можно вернуться на любой описанный выше этап и изменить выбранные опции. Набор параметров можно экспортировать в файл ответов (кнопка **Export settings**) и использовать для установки других контроллеров домена (с соответствующей корректировкой значений).

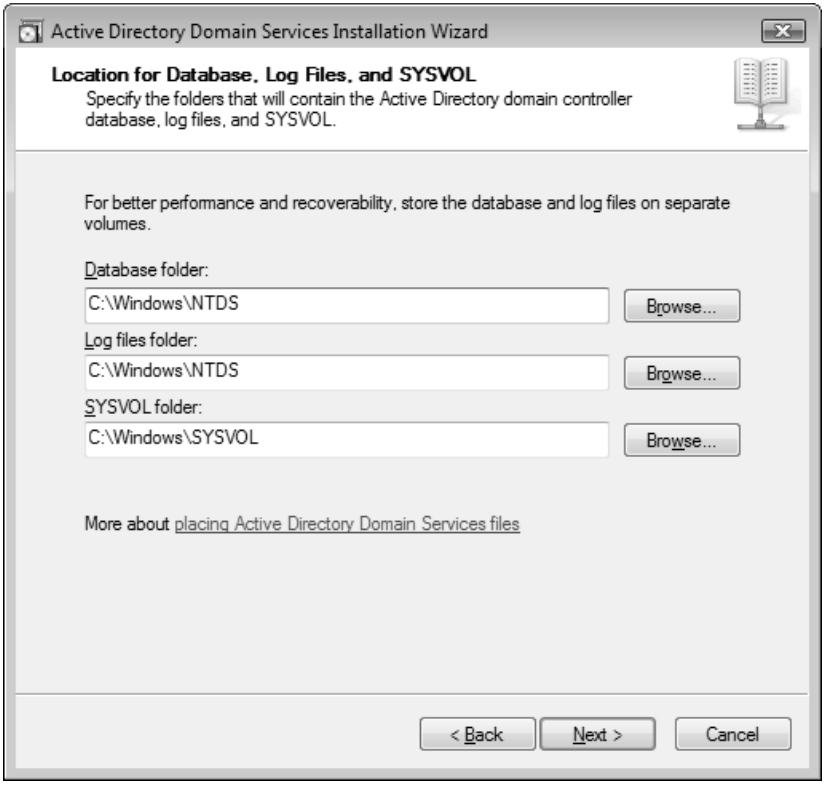


Рис. 12.11. Выбор местоположения файлов каталога Active Directory

Ниже приведен пример файла ответов для конфигурации нового контроллера домена, рассмотренной выше (это обычный текстовой файл в формате txt):

```
; DCPROMO unattend file (automatically generated by dcpromo)
; Usage:
;   dcpromo.exe /unattend:C:\AD-Install-SRV1.txt
;
[DCInstall]
; New forest promotion
ReplicaOrNewDomain=Domain
NewDomain=Forest
NewDomainDNSName=intern.dom
ForestLevel=0
```

```
DomainNetbiosName=INTERN
DomainLevel=0
InstallDNS=Yes
ConfirmGc=Yes
CreateDNSDelegation=No
DatabasePath="C:\Windows\NTDS"
LogPath="C:\Windows\NTDS"
SYSVOLPath="C:\Windows\SYSVOL"
; Set SafeModeAdminPassword to the correct value prior to using
; the unattend file
SafeModeAdminPassword=
; Run-time flags (optional)
; RebootOnCompletion=Yes
```

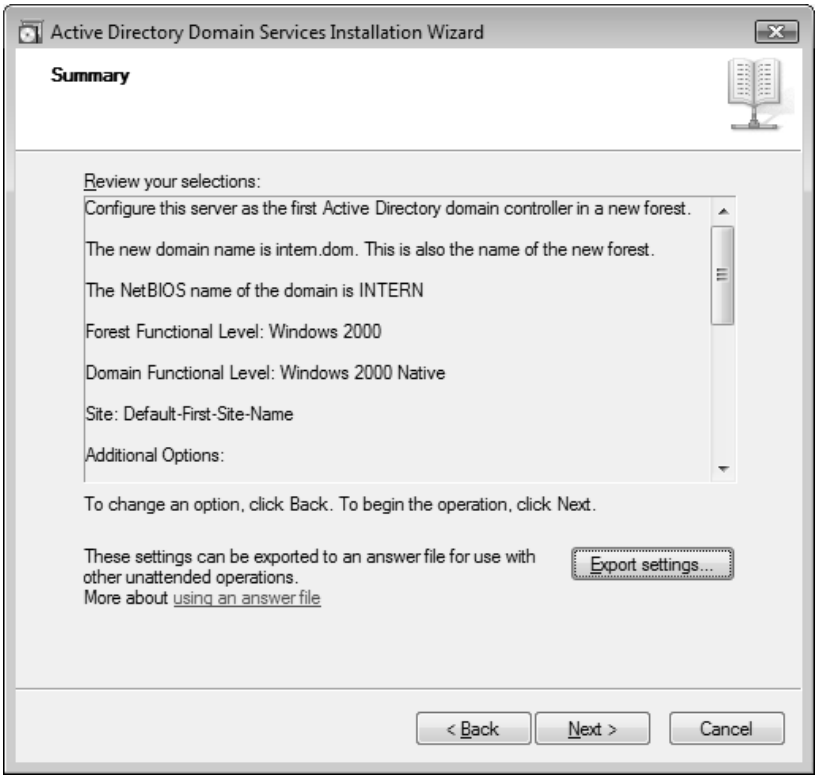


Рис. 12.12. Итоговая информация по параметрам создаваемого контроллера домена

10. После нажатия кнопки **Next** (Далее) в окне просмотра выбранных параметров (см. рис. 12.12) ***начнется конфигурирование*** служб Active Directory (вернуться назад уже будет нельзя). За ходом процесса и названием выполняемых операций можно следить в специальном окне. Если была задана установка DNS-сервера, то затем будет также добавлена эта роль сервера.
11. В последнем окне мастера сообщаются результаты выполнения операции установки Active Directory. Завершите его работу, нажав кнопку **Finish** (Готово). После этого потребуется перезагрузка системы.

Завершение установки и тестирование

После перезагрузки системы можно зарегистрироваться в созданном домене, используя имя и пароль локального администратора. Локальный администратор сервера, на котором был создан самый первый контроллер домена в новом лесе, становится членом следующих групп:

- Administrators (Администраторы) (встроенная локальная группа);
- Domain Admins (Администраторы домена) (входит в группу Administrators);
- Domain Users (Пользователи домена) (входит во встроенную локальную группу Users);
- Enterprise Admins (Администраторы предприятия) (входит в группу Administrators);
- Group Policy Creator Owners (Владельцы-создатели групповой политики);
- Schema Admins (Администраторы схемы).

Внимание!

Рекомендуется просмотреть все сообщения в журналах событий и протестировать новый контроллер домена с помощью утилит DCdiag и NetDiag. Для проверки репликации между контроллерами домена используйте оснастку **Active Directory Sites and Services** (Active Directory – сайты и службы).

Примечание

Объекты контроллеров домена всегда создаются в подразделении Domain Controllers в разделе доменных имен.

Файлы журналов

Все события, возникающие в процессе установки Active Directory, регистрируются в журналах, которые могут быть весьма полезными для анализа причин неудачной установки; эти журналы находятся в папке *%SystemRoot%*\debug:

- DCPROMO.LOG (процесс установки Active Directory в целом, создание разделов каталога, настройка безопасности сервисов и т. д.);
- dcpromoui.log (действия мастера установки);
- NetSetup.LOG (проверка сетевых имен);
- NtFrs_xxxx.log (журналы службы репликации файлов FRS);
- NtFrsApi.log (подготовка службы FRS).

Установка контроллера из архивной копии

Дополнительный контроллер можно создать, используя копию базы данных Active Directory, полученную с имеющегося контроллера домена. Такой подход позволяет значительно уменьшить время на начальную репликацию разделов в том случае, если контроллеры связаны медленным коммутируемым каналом, или если база данных Active Directory имеет значительные размеры. При этом, однако, в процессе повышения роли сервера все равно необходима связь между создаваемым контроллером и существующим доменом (или указываемым при установке контроллером домена).

> ***Внимание!***
>
> Архив состояния системы можно использовать только для создания дополнительного контроллера *существующего* домена. Новые домены и/или деревья можно создавать только обычным способом.
>
> В доменах на базе серверов Windows Server 2003 для установки контроллера домена с носителя используется архив состояния системы (System State), создаваемый с помощью программы архивации. В серверах Windows Server 2008 используется совсем другой подход.

Сначала нужно подготовить копию базы данных Active Directory. Для этого используются утилита *Ntdsutil.exe*, имеющаяся на всех контроллерах домена, и новая ее директива `ifm` (аббревиатура от Install From Media — установка с носителя). При установке обычного контроллера домена требуется копия базы данных с обычного контроллера; при создании RODC-

контроллера необходимо снимать и использовать копию с уже существующего RODC-контроллера.

Ниже приведена последовательность команд, которые следует выполнить на контроллере домена, который будет "эталоном" для новых серверов каталога Active Directory (вводимые команды выделены полужирным шрифтом) — база данных с этого контроллера будет скопирована в указанную папку:

```
C:\>ntdsutil
ntdsutil: Activate Instance ntds
Active instance set to "ntds".
ntdsutil: ifm
ifm: Create Full F:\InstallationMedia-SRV2008
Creating snapshot...
Snapshot set {2f19a2a6-b3fd-4103-ba28-692ab4ecc668} generated success-
fully.
Snapshot {c81a37c3-75d1-4531-a029-b1544dbc2c27} mounted as
C:\$SNAP_200807231330
_VOLUMEC$\
Snapshot {c81a37c3-75d1-4531-a029-b1544dbc2c27} is already mounted.
Initiating DEFRAGMENTATION mode...
     Source Database:
C:\$SNAP_200807231330_VOLUMEC$\Windows\NTDS\ntds.dit
     Target Database: F:\InstallationMedia-SRV2008\Active Direc-
tory\ntds.dit
                 Defragmentation  Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................


Copying registry files...
Copying F:\InstallationMedia-SRV2008\registry\SYSTEM
Copying F:\InstallationMedia-SRV2008\registry\SECURITY
Snapshot {c81a37c3-75d1-4531-a029-b1544dbc2c27} unmounted.
IFM media created successfully in F:\InstallationMedia-SRV2008
ifm: quit
ntdsutil: quit
C:\>
```

Теперь все файлы в указанной папке можно записать на любой носитель, который будет использоваться при создании контроллера домена.

Необходимо будет использовать расширенный режим работы мастера установки Active Directory (см. рис. 12.3). Можно также запустить мастер с помощью команды `dcpromo /adv`. Дальнейшие шаги следующие:

1. После выбора домена, для которого создается контроллер, и дополнительных параметров контроллера (см. рис. 12.9) появится окно **Install from Media** (Установка с носителя) (рис. 12.13). Здесь можно указать имя папки с архивом. Если оставить опцию **Replicate data over the network from an existing domain controller**, то установка контроллера будет выполняться в обычном режиме, и данные будут реплицироваться по сети с имеющегося контроллера домена.

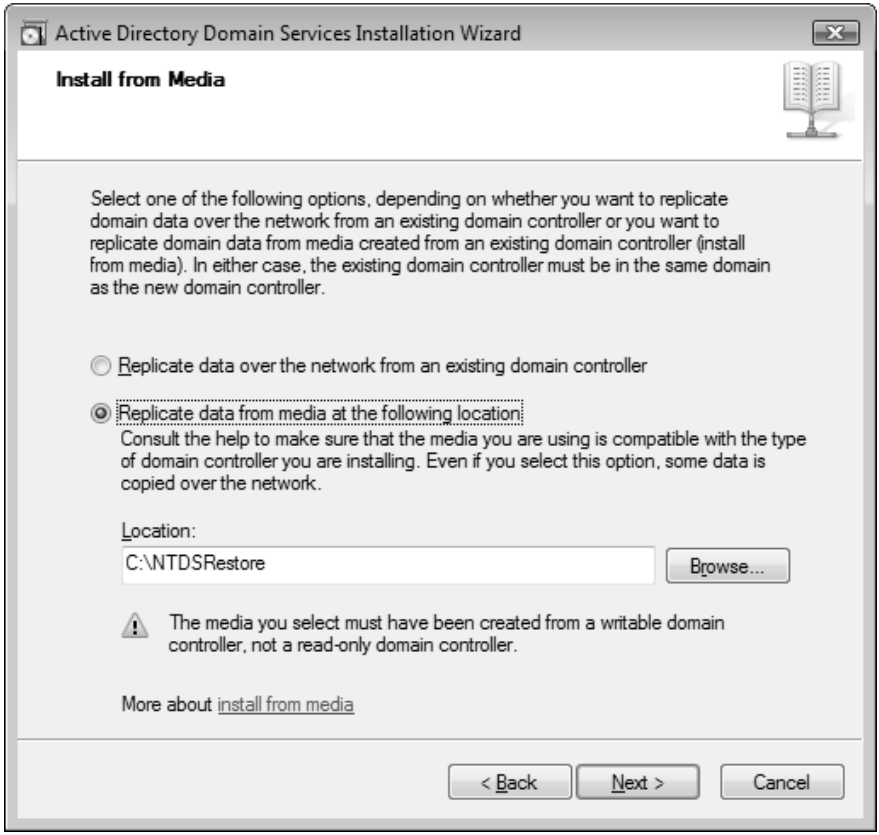


Рис. 12.13. Выбор установки контроллера из архивной копии

2. На следующем шаге можно указать, с какого именно контроллера домена будет осуществляться репликация данных каталога (рис. 12.14) (эта опция появляется только в расширенном режиме работы мастера установки Active Directory). По умолчанию контроллер выбирается автоматически, но если имеются какие-то особенности топологии репликации, то это можно сделать и принудительно. В списке перечисляются все доступные контроллеры, и можно выбрать любой.

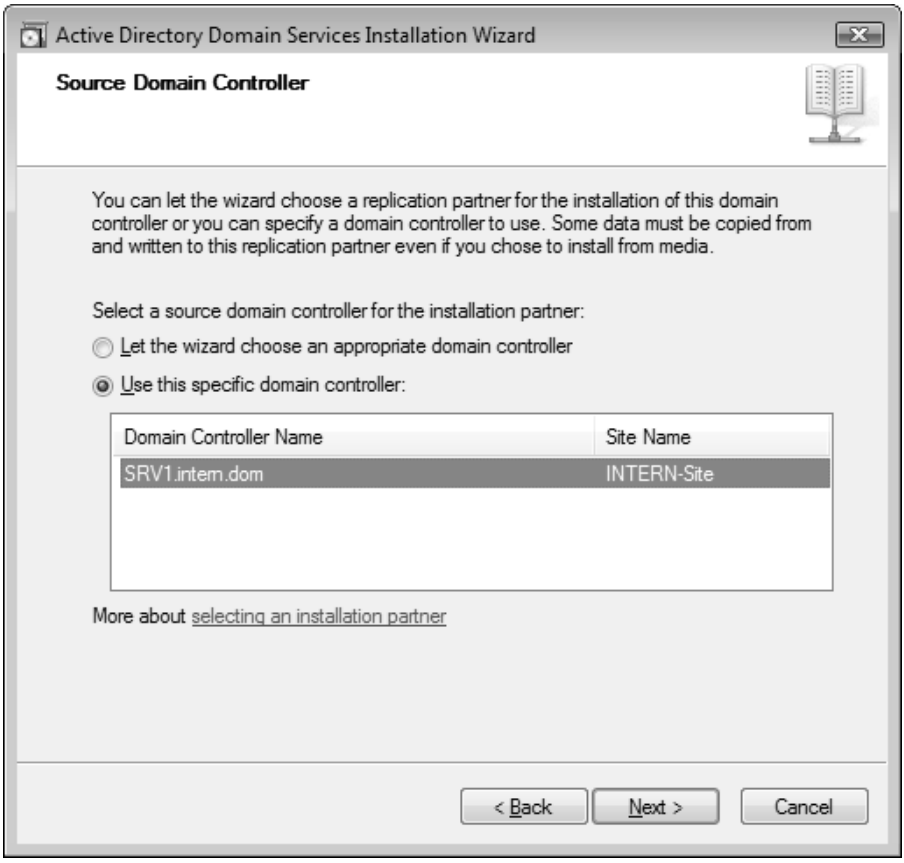


Рис. 12.14. Выбор исходного контроллера домена для выполнения репликации

После всех выполненных действий процедура создания контроллера домена выполняется как обычно, все дальнейшие шаги уже были описаны ранее.

Установка RODC-контроллера домена

Установка контроллеров "только для чтения" (Read-only Domain Controller, RODC) имеет некоторые особенности, связанные с характером использования таких контроллеров.

Внимание!

Для установки RODC-контроллера функциональный уровень леса должен быть Windows Server 2003 и выше. При этом мастер установки Active Directory должен запускаться в расширенном режиме.

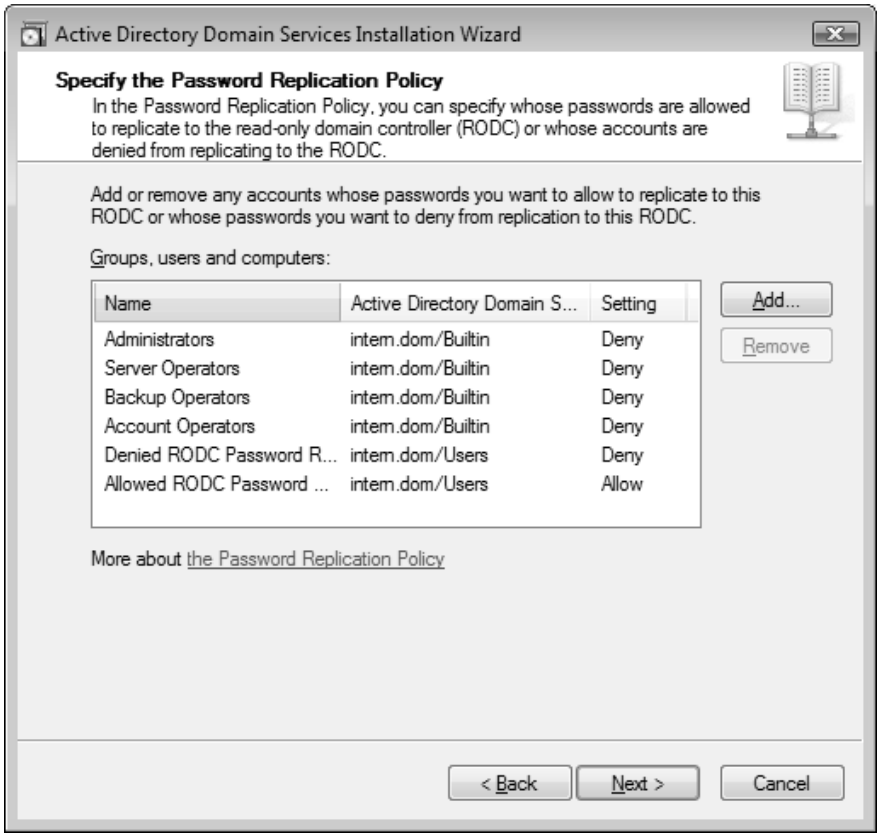


Рис. 12.15. Определение политики репликации паролей

При установке RODC-необходимо задать политику репликации паролей (рис. 12.15), т. е. определить, пароли каких пользовательских учетных записей бу-

дут реплицироваться на данный контроллер. Если какой-то пароль будет отсутствовать на контроллере домена, то невозможно зарегистрироваться в домене с помощью учетной записи, для которой этот пароль задан. Таким образом, повышается защищенность доменной среды. По умолчанию политика репликации паролей определяет группы, для членов которых пароли не копируются. Как можно видеть на рисунке, разрешена только одна доменная группа — Allowed RODC Password Replication Group. Для членов этой группы будет возможна регистрация на создаваемом RODC-контроллере. Можно добавить другие учетные записи или удалить имеющиеся (тогда на них политика действовать не будет).

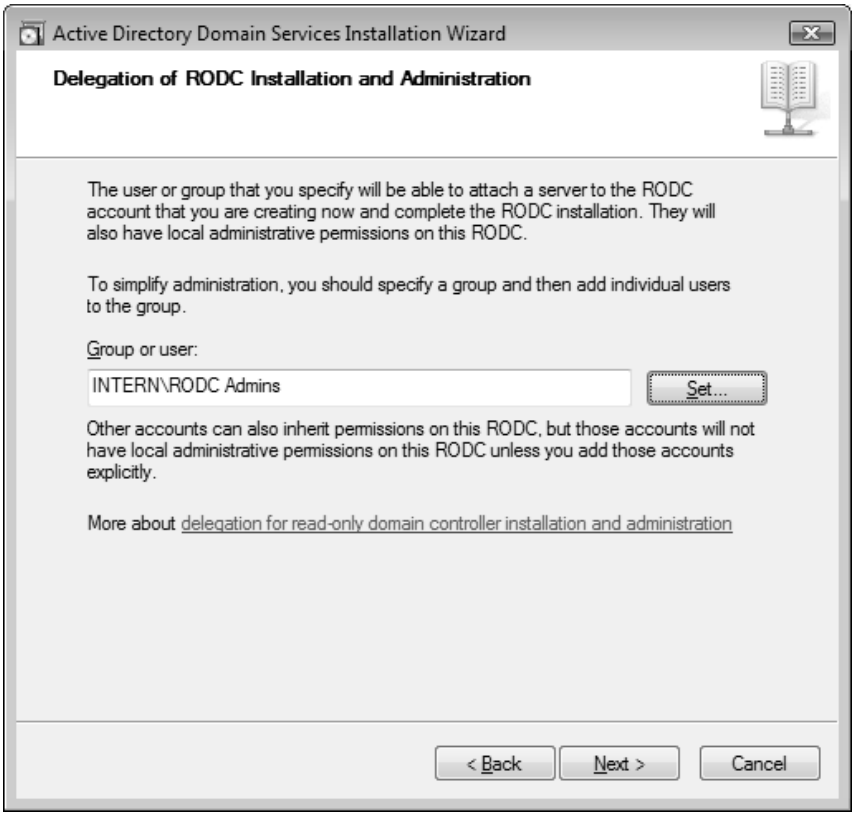


Рис. 12.16. Выбор локальных администраторов для RODC-контроллера

Для RODC-контроллера можно создать специальную группу администраторов или пользовательскую учетную запись и указать ее при создании кон-

троллера (рис. 12.16). Данная учетная запись получит право закончить установку контроллера (например, после физического перемещения компьютера на площадку удаленного подразделения). Также указанная учетная запись будет иметь локальные полномочия на данном контроллере.

В остальном установка RODC-контроллера не отличается от процедуры создания обычных контроллеров домена. Мастер установки будет рекомендовать установить на сервере роль DNS-сервера для того, чтобы в удаленном подразделении сохранялась возможность разрешения имен при разрыве связи с главным офисом.

Удаление контроллера домена

Контроллер домена нельзя *просто* удалить как объект из существующей доменной структуры, т. к. информация о нем хранится во многих контейнерах каталога Active Directory и, главное, нужно сообщить партнерам по репликации о том, что данный контроллер прекращает работу. С помощью процедуры, называемой *понижением роли* (demotion), можно корректно удалить Active Directory с компьютера, лишить сервер функций контроллера домена и автоматически обновить связанную с ним информацию в каталоге Active Directory (если этот контроллер не последний в сети). Если же контроллер домена поврежден или полностью неисправен, то необходимо вручную "чистить" каталог Active Directory.

Операция понижения контроллера домена выполняется мастером установки Active Directory (утилита Dcpromo). Если попытаться удалить с сервера роль Active Directory Domain Services (AD DS) (Доменные службы Active Directory) с помощью оснастки **Server Manager** (Диспетчер сервера), то это сделать не получится и появится сообщение о необходимости запуска мастера установки.

После удаления контроллера домена с помощью мастера установки Active Directory на сервере останутся двоичные файлы *(см. выше разд. "Запуск мастера установки Active Directory")*, которые следует убрать с помощью оснастки **Server Manager** (Диспетчер сервера) или посредством команды `dcpromo /uninstallBinaries`.

Требования и ограничения

Как и при установке контроллера домена, должны быть доступны другие домены Active Directory (родительский или корневой), иначе процесс понише-

ния роли не начнется (если только этот контроллер не последний в лесу доменов). Контроллер домена нельзя удалить, если репликация обновлений разделов каталога с "понижаемого" сервера закончилась неудачей, поэтому проверьте отсутствие ошибок репликации перед его удалением.

> ***Внимание!***
>
> Перед выполнением операции понижения роли контроллера домена следует убедиться в том, что контроллер не является сервером Глобального каталога или исполнителем специализированных FSMO-ролей. Необходимо, чтобы после удаления контроллера в домене оставался хотя бы один сервер Глобального каталога. Обычно FSMO-роли автоматически передаются какому-нибудь другому контроллеру домена, однако администратор может предпочесть самостоятельно управлять этим процессом, предварительно передав роли в соответствии с требованиями конкретной конфигурации сети.

Если удаляется последний контроллер в домене, это означает удаление всего домена.

Удалить можно только тот домен, который не имеет дочерних доменов и не является корневым доменом леса (который может удаляться только самым последним).

Запрещается удалять контроллеры домена, являющиеся последними носителями реплик разделов приложений (application directory partition). Администратор должен сначала вручную удалить разделы приложений с помощью утилиты NTDSutil или разрешить эту операцию мастеру.

> ***Внимание!***
>
> Удаление последней реплики раздела приложений приводит к потере всех хранящихся в ней данных. Как следствие, это может привести к отказу или неверной работе прикладной программы, использующей этот раздел.

Запуск мастера установки Active Directory

Для удаления контроллера домена Active Directory запустите на нем мастер установки Active Directory — утилиту Dcpromo.exe.

Может появиться сообщение, показанное на рис. 12.17. Убедитесь в том, что в лесу имеется другой сервер Глобального каталога (GC).

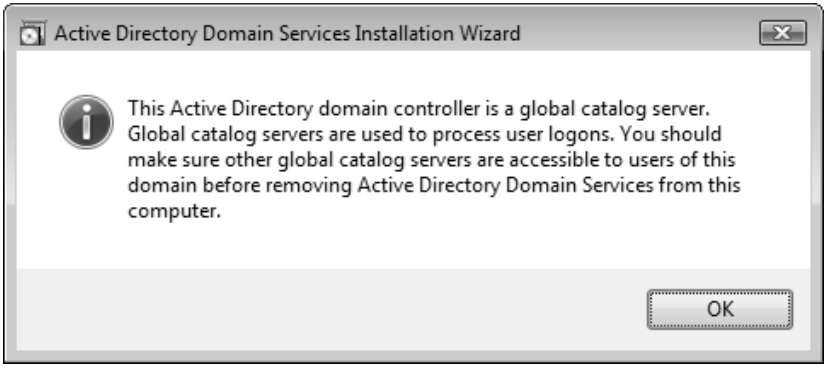


Рис. 12.17. Следует следить за тем, чтобы в сети оставалось нужное количество серверов Глобального каталога

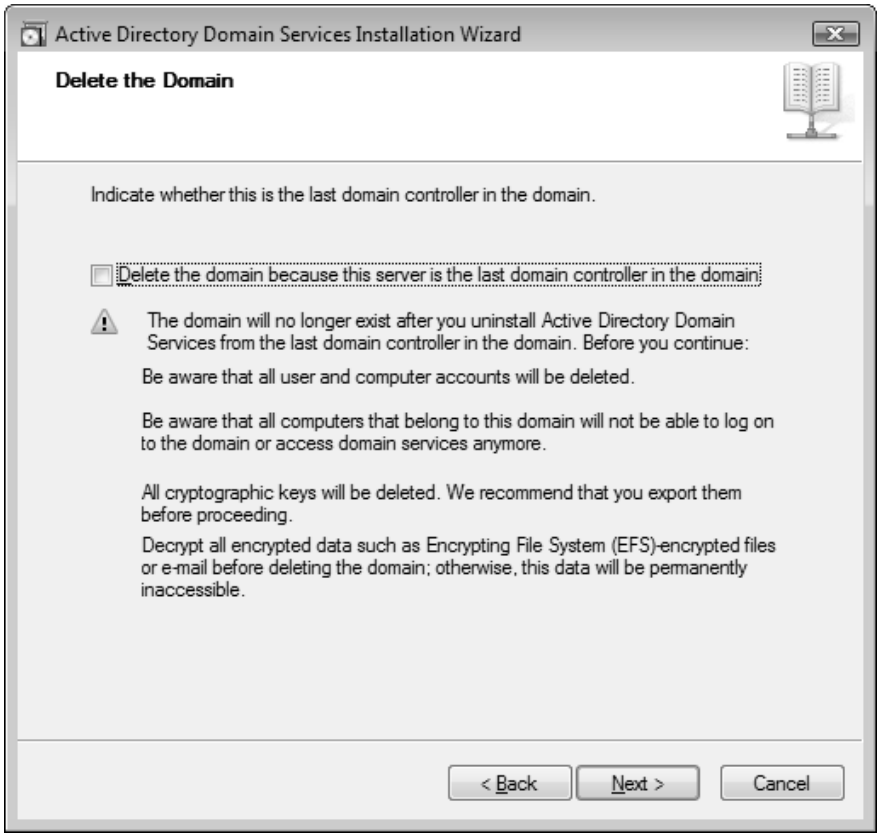


Рис. 12.18. Подтверждение удаления домена

При необходимости создайте новой сервер GC, дождитесь момента, когда он будет объявлен, и только тогда продолжайте процесс удаления контроллера домена.

На следующем шаге мастер установки потребует определить статус флажка **Delete the domain because this server is the last domain controller in the domain** (Удалить этот домен, поскольку данный сервер является в нем последним контроллером домена) (рис. 12.18). Для удаления последнего контроллера в некотором дочернем домене (т. е. при удалении этого дочернего домена) или в корневом домене дерева (т. е. при удалении всего этого дерева) нужно будет ввести имя и пароль пользователя, входящего в группу Enterprise Admin (Администраторы предприятия).

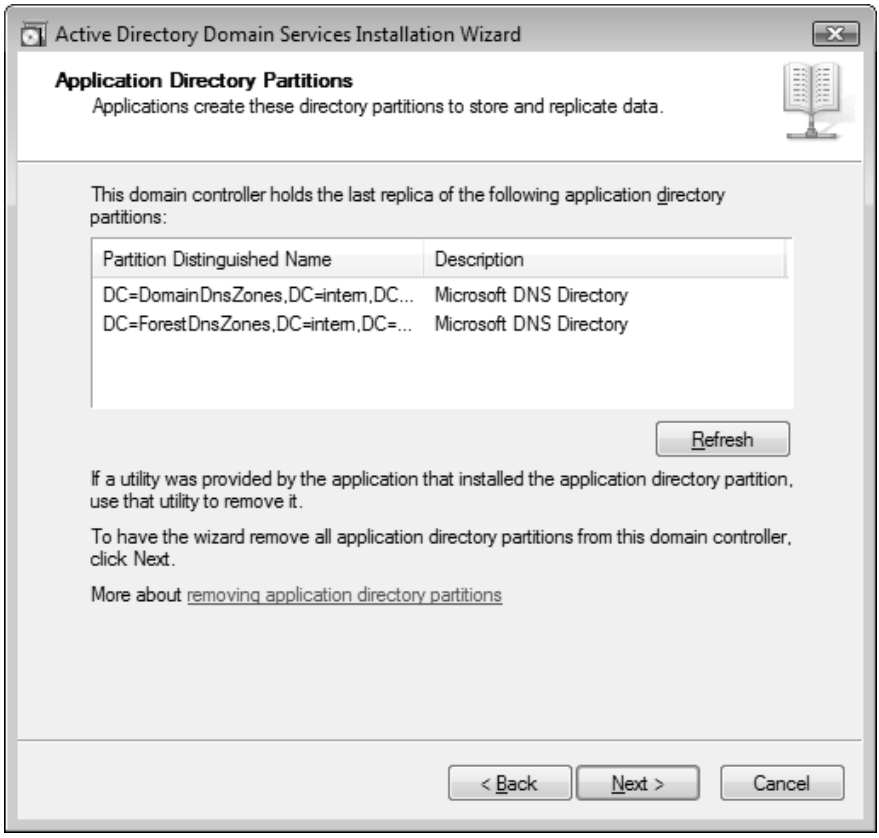


Рис. 12.19. Список разделов приложений на данном контроллере домена

Для удаления дополнительного контроллера домена достаточно иметь полномочия пользователя, входящего в группу Domain Admins (Администраторы домена).

Если удаляемый контроллер работает и хранит *последние* реплики одного или нескольких разделов приложений, то появится предупреждение, аналогичное тому, что показано на рис. 12.19. В этом случае разделы приложений можно удалить вручную (например, с помощью утилит NTDSutil или DnsCmd) или разрешить системе удалить разделы приложений на этом контроллере — для этого на следующей странице мастера (рис. 12.20) следует подтвердить операцию, установив флажок **Delete all application directory partitions on this domain controller**. Если не сделать ни того, ни другого, то процедура понижения роли будет прервана.

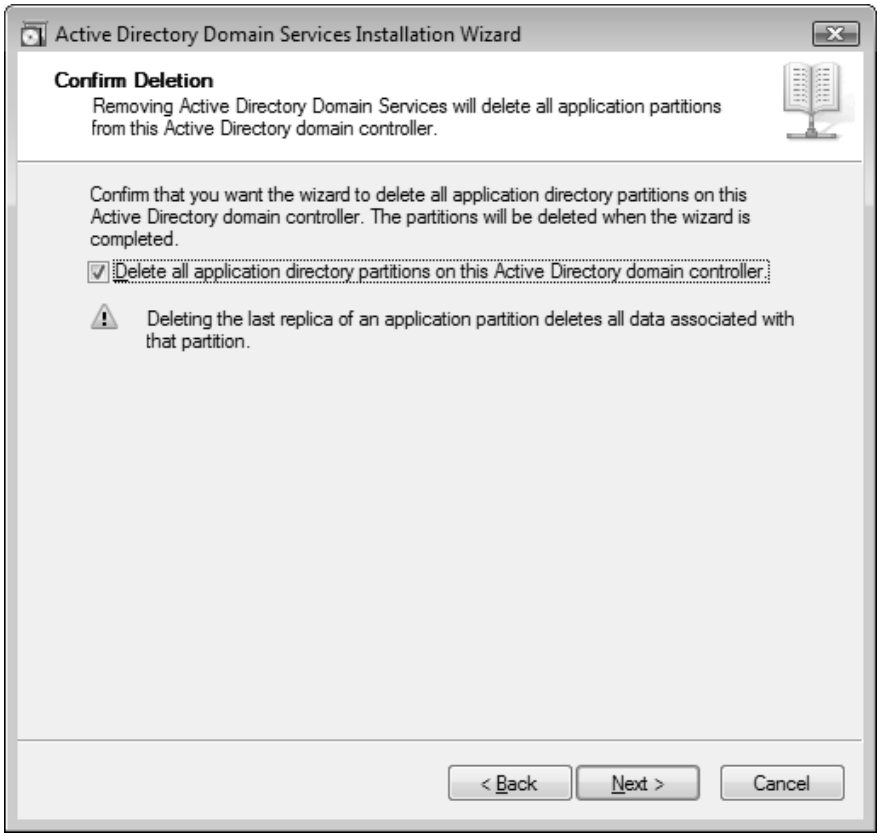


Рис. 12.20. Подтверждение удаления разделов приложений

После установки нового пароля для локальной учетной записи Administrator (Администратор) и проверки параметров можно нажать кнопку **Next** (Далее) — начнется удаление контроллера. Установив в информационном окне флажок **Reboot on completion**, можно разрешить автоматическую перезагрузку сервера по завершении операции.

Когда Active Directory удаляется с некоторого контроллера домена и процесс понижения роли завершается (после перезагрузки сервера), все соответствующие ресурсные записи удаляются с предпочитаемого сервера DNS (если, конечно, этот сервер поддерживает динамическое обновление записей) и записи в файле *%SystemRoot%*\System32\config\netlogon.dns деактивируются.

После удаления Active Directory последний контроллер *любого* домена становится автономным сервером, принадлежащим к рабочей группе WORKGROUP. При этом основной суффикс DNS на компьютере не меняется. Если контроллер не последний в домене, то после понижения роли он становится рядовым сервером (member server) этого домена.

После выполнения операции понижения роли контроллера домена можно удалить двоичные файлы служб Active Directory, удалив роль с помощью оснастки **Server Manager** (Диспетчер сервера).

Принудительное понижение роли

Иногда может возникнуть ситуация, когда по разным причинам корректное удаление контроллера домена невозможно, при этом операционную систему на сервере переустанавливать нежелательно (если, например, на нем имеются различные прикладные программы). Для контроллера на базе Windows Server 2008 имеется возможность принудительного удаления, при котором ***не выполняется репликация с другими контроллерами и не корректируется содержимое каталога*** Active Directory.

Чтобы удалить службу Active Directory с контроллера домена и превратить его в обычный сервер, выполните в окне консоли команду `dcpromo /forceRemoval` (справку по многочисленным возможностям этой директивы можно получить с помощью команды `dcpromo /?:Demotion`[1]). Запустится мастер установки Active Directory, который позволит выполнить требуемую операцию. При этом в отличие от нормальной операции понижения роли, затем потребуются дополнительные ручные операции: проследите, удалены ли ресурсные записи на предпочитаемом DNS-сервере, и уберите все ссылки

[1] Двоеточие обязательно!

на контроллер домена в оставшейся структуре каталога Active Directory (например, с помощью оснастки **Active Directory Sites and Services** (Active Directory – сайты и службы)).

Не забудьте удалить двоичные файлы Active Directory с помощью оснастки **Server Manager** (Диспетчер сервера) или посредством команды `dcpromo /uninstallBinaries`.

Особенности подключения клиентов домена

Когда клиентский компьютер включается в домен Active Directory, соответствующая учетная запись компьютера *всегда* создается в контейнере Computers. Затем, при необходимости, эту учетную запись можно переместить в любой контейнер (подразделение).

Однако возможен и другой подход. Учетную запись можно создать *до того* как компьютер подключается к домену: подготовьте эту запись (с помощью оснастки **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры) или команды `netdom ADD`) в любом контейнере, а затем используйте ее при добавлении компьютера.

> ***Примечание***
>
> В доменах, имеющих функциональный уровень *Windows Server 2003*, с помощью утилиты RedirCmp.exe можно назначить любой контейнер (подразделение) для новых учетных записей компьютеров. В этом случае можно, например, назначить этому контейнеру специальную политику (привязав к контейнеру заранее сконфигурированный GPO-объект), которая *сразу же* будет действовать на все новые учетные записи.

Для подключения к домену клиентских компьютеров необходимо выполнение всего двух требований:

- в домене должно быть обеспечено разрешение имен;
- политики безопасности (опции шифрации и подписывания сетевого трафика) на клиентах и на контроллерах домена должны совпадать.

Проблемы с подключением компьютеров в домены Active Directory возникают, в первую очередь, из-за несогласования протоколов для каналов связи между клиентом и контроллером домена.

Примечание

В случае возникновения ошибок при добавлении клиентского компьютера в домен Active Directory проверьте сначала на этом компьютере параметры протокола TCP/IP (в частности, адрес предпочитаемого DNS-сервера) и доступность контроллеров этого домена. Для этой цели лучше всего использовать утилиту NetDiag.

По умолчанию контроллеры на базе Windows Server 2008 требуют цифровых подписей для всех обменов информацией по протоколу SMB (Server Message Block — Блок серверных сообщений) и используют аутентификацию LAN Manager NTLMv2. Кроме того, требуется, чтобы все безопасные каналы (secure channel) подписывались и шифровались.

Рассмотрим политики безопасности, влияющие на порядок взаимодействия между клиентами и контроллерами домена — эти политики должны быть согласованы между ними. Выбор политик должен осуществляться администратором домена на основе реальной ситуации в сети.

- Подписывание SMB-трафика определяется политикой **Microsoft network server: Digitally sign communications (always)** (ей соответствует параметр реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\requiresecuritysignature`).
- Требование подписи или шифрации для безопасных каналов задается политикой **Domain member: Digitally encrypt or sign secure channel data (always)** (соответствующий параметр реестра — `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\requiresignorseal`).
- Протокол аутентификации клиентов определяется политикой **Network security: LAN Manager authentication level** (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\lmcompatibilitylevel). Политика, установленная локально на клиенте, должна соответствовать требованиям, предъявляемым политиками контроллеров домена.

Нужно помнить о том, что сразу после загрузки системы действуют *локальные* политики безопасности, и только после аутентификации клиентского компьютера на контроллере домена к клиенту применяются доменные политики, которые могут переопределить локальные значения. Однако если локальные параметры безопасности не позволят клиенту "договориться" с контроллером о порядке обмена данными, то и аутентификации клиента (и подключения к домену) не произойдет.

Основные оснастки для администрирования доменов и каталогов Active Directory

Оснастки, необходимые для администрирования доменов Active Directory, устанавливаются на серверах при создании на их базе контроллеров домена. Эти оснастки перечислены в табл. 3.4 и будут подробно рассматриваться далее. В системах Windows Server 2008 имеется возможность установки средств удаленного администрирования каталогов на любом сервере. Для этого нужно лишь с помощью оснастки **Server Manager** (Диспетчер сервера) установить соответствующие компоненты удаленного управления (рис. 12.21).

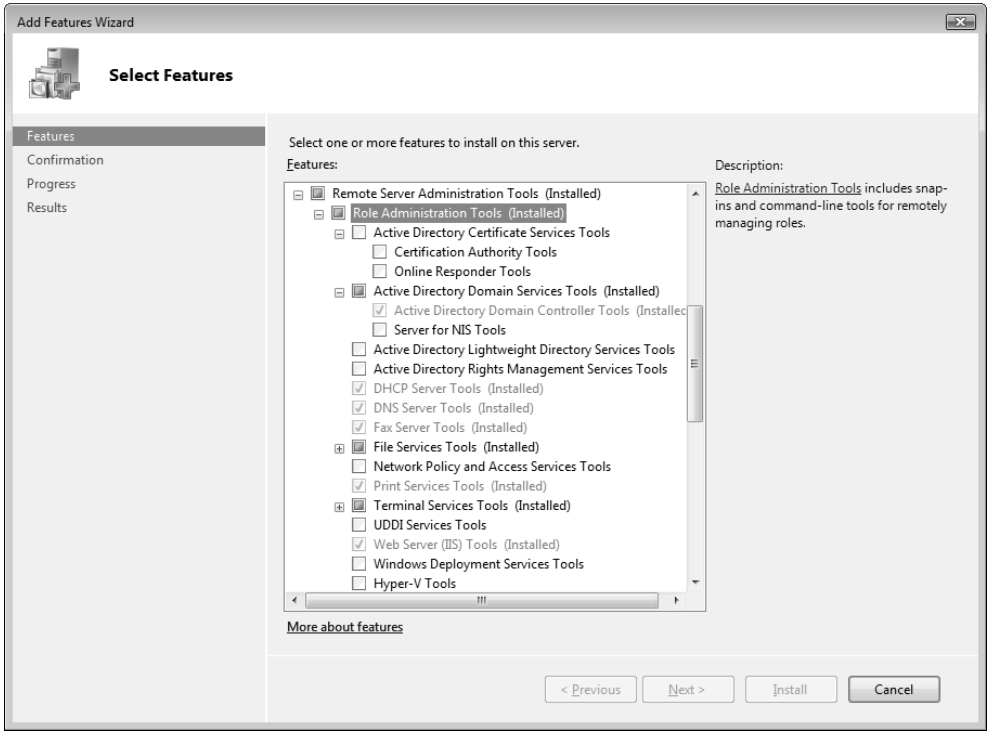


Рис. 12.21. Компоненты для удаленного управления ролями

Некоторые инструменты для администрирования каталогов Active Directory ранее входили в состав пакета Windows Support Tools; сейчас они являются стандартными программами серверов Windows Server 2008. Помимо упомя-

нутой в табл. 3.4 оснастки **ADSI Edit** (Редактирование ADSI), можно также назвать еще утилиту *Active Directory Administration Tool* (Ldp.exe), с помощью которой можно выполнять поиск и модификацию объектов Active Directory при помощи запросов LDAP (включена новая версия 3.0). В составе пакета Windows Support Tools остается очень удобная утилита *Active Directory Replication Monitor* (Replmon.exe), позволяющая следить за состоянием и топологией репликации доменов Active Directory, инициировать репликацию различных разделов каталога и выполнять мониторинг ролей FSMO и состояния контроллеров домена.

Совет

Для того чтобы запускать административные оснастки для управления удаленными серверами, не регистрируясь на них с учетными записями администраторов (что не приветствуется требованиями безопасности), используйте команду `runas`; например, следующая команда позволяет запустить оснастку управления групповыми политиками и указать альтернативную учетную запись:

```
runas /noprofile /env /user:DOMAIN\administrator "mmc gpmc.msc"
```

Оснастка *Active Directory Users and Computers*

При работе с доменами оснастка **Active Directory Users and Computers** (Active Directory – пользователи и компьютеры) используется, наверное, чаще других административных инструментов. Основное назначение оснастки — создание и модификация в доменном разделе каталога различных объектов, необходимых как для работы домена (например, учетных записей пользователей, компьютеров и групп, подразделений, общих папок и т. д.), так и для приложений, хранящих свои данные в каталоге Active Directory. Оснастка позволяет управлять правами доступа к объектам каталога и делегировать пользователям и группам определенные административные полномочия на управление контейнерами (доменами, подразделениями, сайтами и т. д.).

Внимание!

В контроллерах домена на базе Windows Server 2008 с помощью оснастки **Active Directory Users and Computers** (Active Directory – пользователи и компьютеры) нельзя инициировать какие-либо операции с GPO-объекта-

ми — просмотр, редактирование, управление наследованием, определение результирующих политик (запуск оснастки **Resultant Set of Policy**, RSoP, для выбранных контейнеров и объектов) и т. п. Вся работа с GPO-объектами осуществляется только с помощью оснастки **Group Policy Management** (Управление групповой политикой).

Подключение к домену или контроллеру домена

В каждый момент времени оснастка **Active Directory Users and Computers** (Active Directory – пользователи и компьютеры) может работать только с одним контроллером и, следовательно, с одним доменом. По умолчанию выбираются домен и контроллер домена, где в настоящий момент зарегистрировался пользователь (если имя домена не было изменено и сохранено при установке флажка **Save this domain setting for the current console box** (Сохранить этот параметр домена для этой консоли) — рис. 12.22).

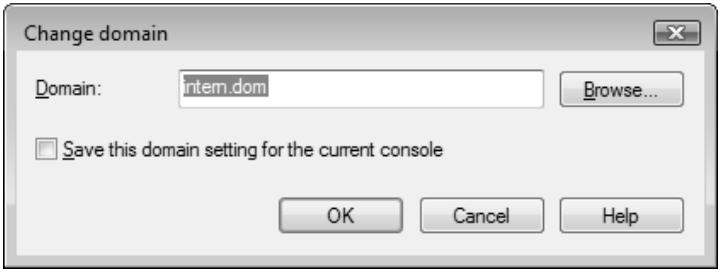


Рис. 12.22. Можно выбрать для администрирования любой домен, входящий в состав леса

Для выбора домена поместите курсор в корень оснастки или на доменный объект в окне структуры и выберите команду **Change Domain** (Сменить домен) в меню **Action** (Действие). В окне **Change domain** (Смена домена) введите имя домена в поле **Domain** (см. рис. 12.22) или нажмите кнопку **Browse** (Обзор) и выберите домен в раскрывающемся доменном дереве. Обратите внимание на флажок **Save this domain setting for the current console** (Сохранить этот параметр домена для этой консоли), с помощью которого можно сохранить в консоли несколько оснасток, настроенных на разные домены.

Аналогичным образом вы можете выбрать любой контроллер в текущем домене: для этого используйте команду **Change Domain Controller** (Сменить контроллер домена) в меню **Action** (Действие). Это бывает нужным, когда по каким-то причинам (например, при выявлении проблем с репликацией) вам необходимо администрировать какой-нибудь сервер Глобального каталога или контроллер домена, владеющий определенной FSMO-ролью, например, PDC Emulator. В окне **Change Directory Server** (Смена сервера каталогов) (рис. 12.23) можно видеть имя текущего контроллера домена и список имеющихся контроллеров (или же можно ввести имя и порт для сервера AD LDS).

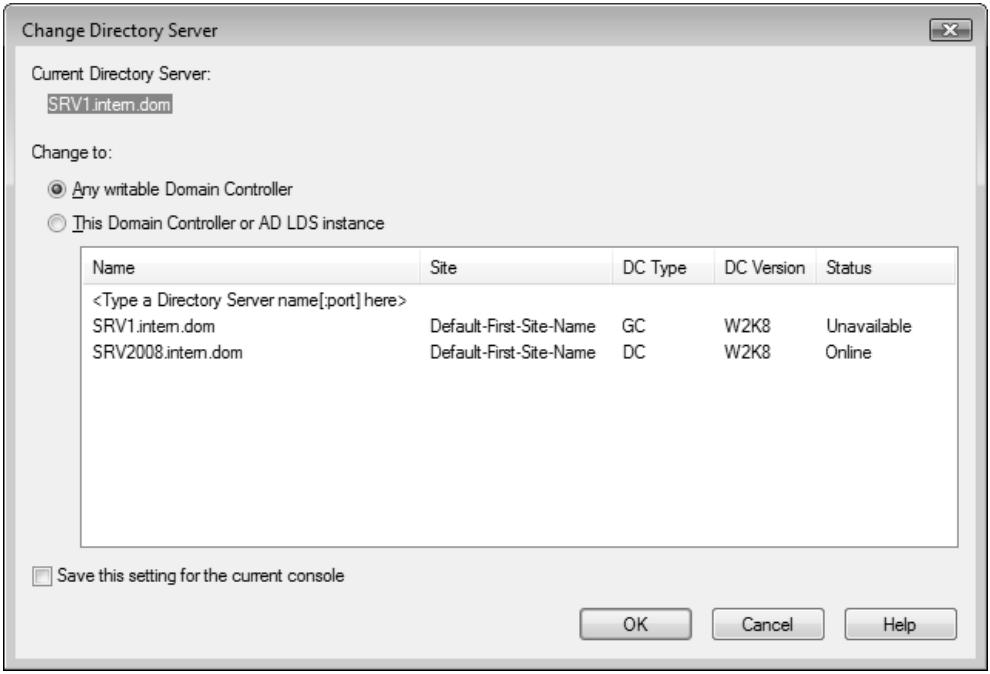


Рис. 12.23. Выбор контроллера домена

Управление отображением объектов каталога

Оснастка **Active Directory Users and Computers** (Active Directory – пользователи и компьютеры) имеет некоторые специфические опции, которые

практически не влияют на суть операций по администрированию, однако существенно влияют на количество отображаемых объектов. Все эти опции рассматриваются ниже.

Сохраненные запросы (Saved Queries)

Администратор может создать один или несколько запросов на основе LDAP-фильтров и сохранить их в среде оснастки для последующего использования. Такие запросы позволяют быстро отбирать только нужные объекты, что упрощает работу при наличии большого числа объектов одного типа (пользователей, групп, компьютеров и т. д.). Очень важно и то, что в отличие от основного окна оснастки, в котором набор выбранных для отображения полей одинаков для всех просматриваемых контейнеров, для каждого запроса можно установить индивидуальный набор полей.

Все имена запросов хранятся в папке **Saved Queries** (Сохраненные запросы) в окне дерева объектов, и их можно помещать в папки, создавая некоторую организационную структуру (рис. 12.24).

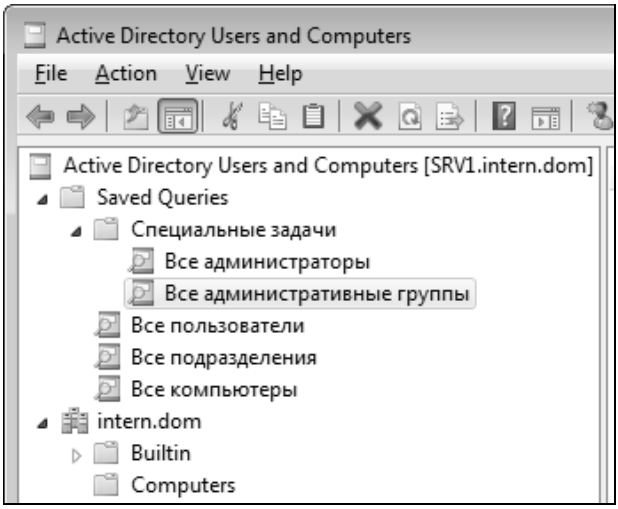


Рис. 12.24. Пример дерева сохраненных запросов

Новый запрос можно создавать непосредственно в окне оснастки или можно импортировать описание уже существующих запросов (в формате XML).

Для создания запроса воспользуйтесь следующей процедурой:

1. Выберите папку **Saved Queries** (Сохраненные запросы) или другую уже существующую внутри ее папку и щелкните правой кнопкой мыши.
2. Выберите в контекстном меню команду **New** | **Query** (Создать | Запрос).
3. В окне **New Query** (Новый запрос) (рис. 12.25) заполните поля **Name** (Имя) и **Description** (описание необязательно).

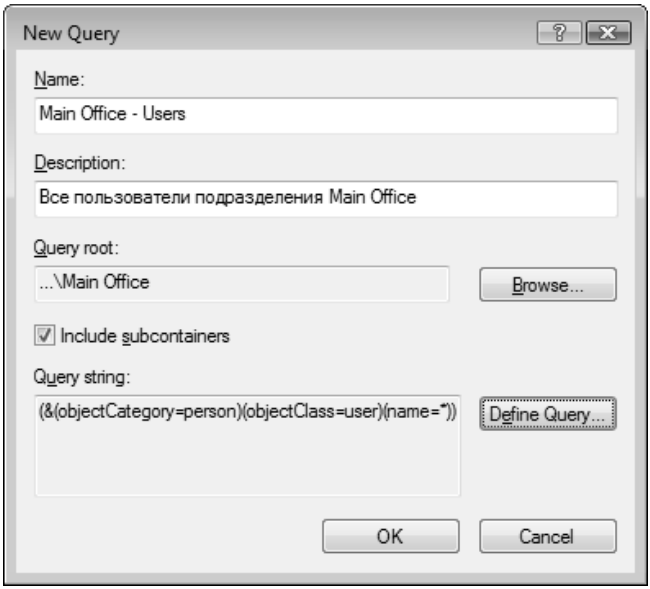


Рис. 12.25. Пример нового сохраненного запроса

4. Нажмите кнопку **Browse** (Обзор) и выберите корень запроса — некоторый контейнер в структуре домена (по умолчанию просматривается весь домен). Проверьте, правильно ли выбрано состояние флажка **Include subdirectories** (Включая подконтейнеры).
5. Нажмите кнопку **Define Query** (Запрос) и определите нужную строку запроса.
6. Нажмите кнопку **OK**. Запрос готов.

Сохраненные запросы не сортируются, а запоминаются в структуре запросов в порядке их создания. Сортировать имена запросов можно только в окне результатов (правое подокно оснастки).

Для распространения сохраненных запросов имеется вполне законный и проверенный путь: достаточно просто экспортировать (сохранить) *описание запроса* (query definition) (в формате XML) и импортировать его на тех компьютерах, где оно требуется. Для этого выберите запрос и в контекстном меню выполните команду **Export Query Definition** (Экспорт определения запроса). Сохраните описание в файле, скопируйте этот файл на другой компьютер, запустите на нем оснастку **Active Directory Users and Computers** (Active Directory – пользователи и компьютеры), вызовите контекстное меню для папки **Saved Queries** (Сохраненные запросы) (или для любой вложенной папки) и выполните команду **Import Query Definition** (Импорт определения запроса).

Включение опции просмотра дополнительных компонентов

По умолчанию в основном режиме окна оснастки **Active Directory Users and Computers** (Active Directory – пользователи и компьютеры) отображается только пять узлов (если не считать подразделений, созданных администратором). Этого недостаточно для выполнения некоторых задач, и в этом случае необходимо включать режим *Advanced Features*, в котором также отображаются некоторые важные "невидимые" контейнеры и появляются дополнительные возможности. Для этого используется команда **Advanced Features** (Дополнительные компоненты) в меню **View** (Вид).

Одним из важнейших узлов, отображаемых в расширенном режиме, является контейнер System (рис. 12.26), который обеспечивает доступ ко многим системным объектам.

Что еще важнее, только в режиме Advanced Features (Дополнительные компоненты) в окне **Properties** (Свойства) для каждого объекта Active Directory появляются вкладки **Object** (Объект), **Security** (Безопасность) и новая вкладка — **Attribute Editor** (Редактор атрибутов) (см. рис. 12.27). На вкладке **Security** отображаются, в частности, все изменения, связанные с делегированием прав на управление объектами каталога. Если, например, вам нужно отозвать административные права, данные пользователю или группе в отношении некоторого объекта, то следует открыть эту вкладку в свойствах объекта и удалить соответствующие разрешения.

Внимание!

В окне свойств контейнеров теперь отсутствует вкладка **Group Policy** (Групповая политика), на которой в системах Windows 2000/Windows Server

2003 можно просматривать список GPO-объектов, связанных с данным контейнером, и выполнять различные настройки, связанные с применением групповых политик.

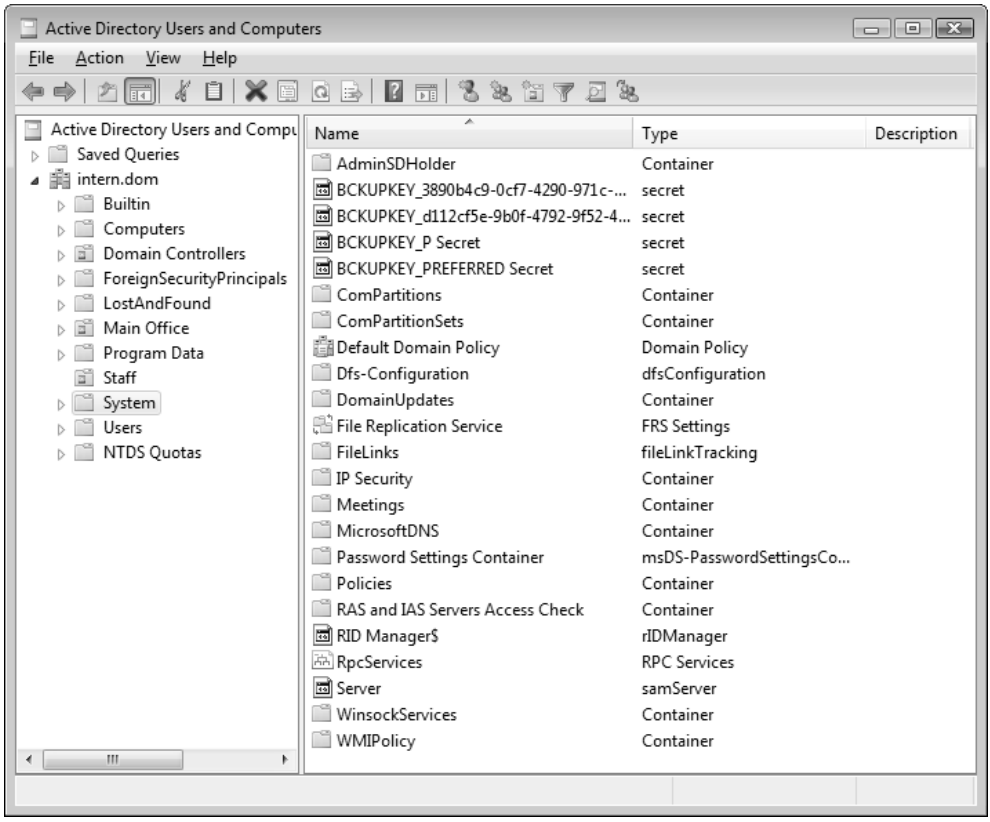


Рис. 12.26. Просмотр дерева доменных объектов в режиме Advanced Features

У всех объектов каталога на вкладке **Object** (Объект) появился флажок **Protect object from accidental deletion** (Защитить объект от случайного удаления). Этот флажок по умолчанию установлен для всех операций создания новых контейнеров; вручную его можно установить и для любых других объектов каталога. Когда флажок установлен, при попытке удаления объекта будет возникать ошибка, указывающая на отсутствие прав на выполнение операции. Поэтому для удаления таких защищенных объектов нужно сначала открыть окно свойств объекта и сбросить данный флажок.

Вкладка **Attribute Editor** (Редактор атрибутов) (рис. 12.27) обеспечивает доступ к свойствам выбранного объекта каталога, которые не отображаются на панелях свойств оснастки, и позволяет редактировать их значения (если это допустимо правилами доступа к объектам каталога).

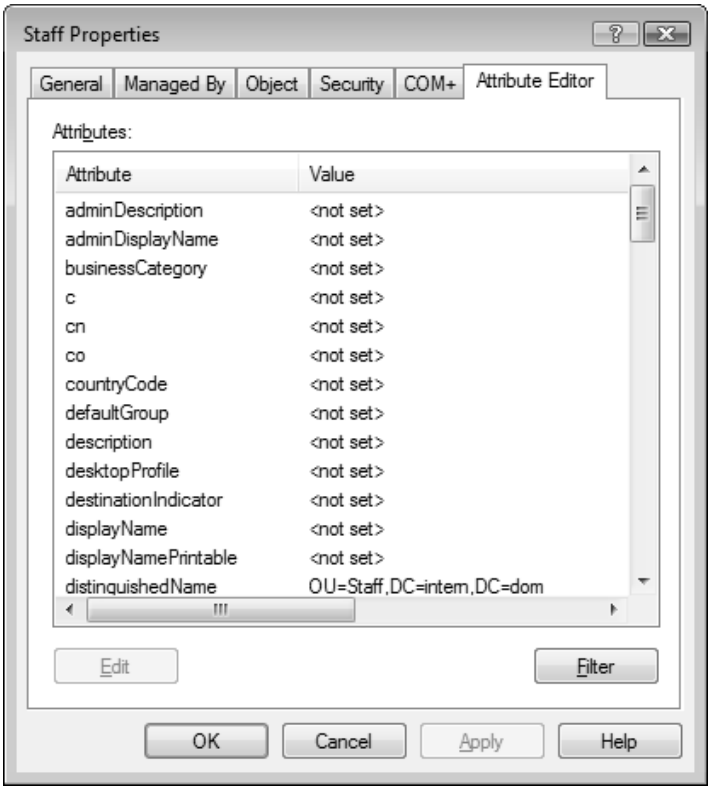


Рис. 12.27. Вкладка редактора атрибутов выбранного объекта каталога

Режим *Users, Contacts, Groups, and Computers as containers* (Пользователи, контакты, группы и компьютеры как контейнеры)

Некоторые объекты Active Directory являются контейнерами, которые могут содержать другие объекты. По умолчанию это отношение визуально не представлено в окне оснастки **Active Directory Users and Computers** (Active

Directory – пользователи и компьютеры). Тем не менее, в некоторых ситуациях необходимо видеть отношения между объектами. Сравните, например, два экрана, показанных на рис. 12.28 и рис. 12.29.

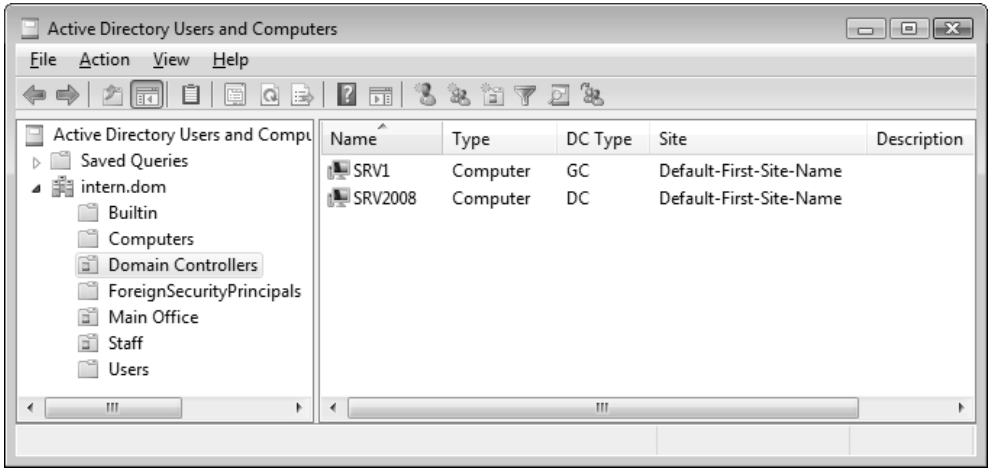


Рис. 12.28. Контроллеры домена — вид по умолчанию

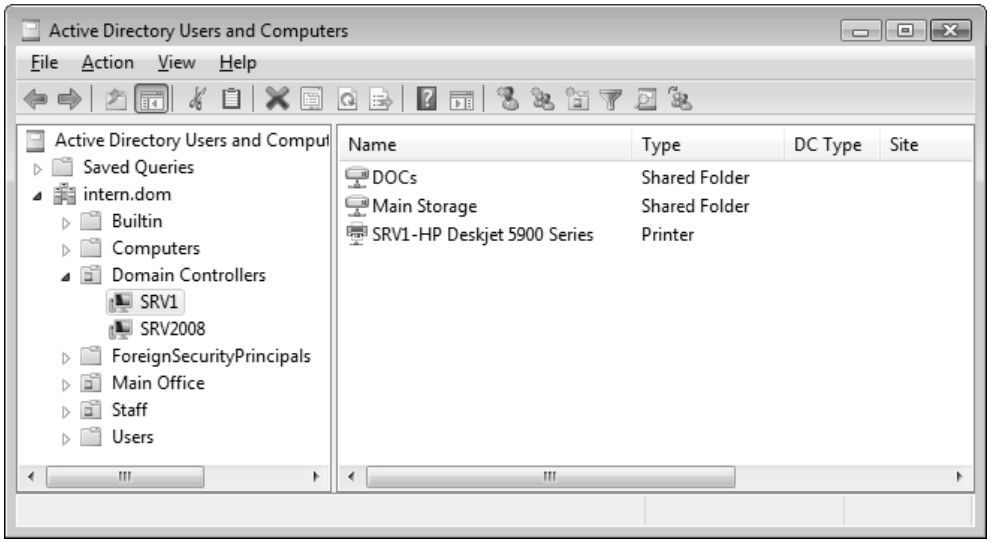


Рис. 12.29. В режиме Users, Contacts, Groups, and Computers as containers можно увидеть опубликованные объекты, связанные к выбранным контроллером домена

На первом представлено стандартное изображение подразделения Domain Controllers и контроллера домена SRV1; на втором этот же контроллер домена показан как контейнер.

Как видно на рис. 12.29, контроллер домена на самом деле имеет дочерние объекты, в частности, с ним связаны имена опубликованных объектов: принтера и общих папок.

Примечание

Изначально все принтеры публикуются в Active Directory в виде дочерних объектов соответствующих компьютеров. Для удобства пользователей или администраторов эти объекты можно затем переместить в одно подразделение; однако команда **Search** (Поиск) является более удобным и корректным средством работы с принтерами.

Фильтрация отображаемых объектов

При большом количестве объектов в Active Directory на поиск отдельных объектов может уходить много времени. Однако можно установить *фильтр* и просматривать только нужные объекты. Выберите команду **Filter Options** (Параметры фильтра) в меню **View** (Вид) или нажмите кнопку **Set Filtering Options** (Установка параметров фильтрации)  на стандартной панели инструментов. Тип отображаемых объектов можно выбрать из предлагаемого списка (рис. 12.30) или же можно создать собственный пользовательский фильтр (процесс создания фильтра интуитивно понятен и достаточно прост — сначала выбирается тип объектов и имя атрибута, а затем условие).

Внимание!

При использовании фильтров возникает потенциальная опасность при работе с контейнерами (подразделениями). Предположим, что установлен фильтр, который отображает только учетные записи компьютеров. Может показаться, что в подразделении нет объектов или оно содержит только ненужные учетные записи компьютеров. Легко забыть о том, что это подразделение может содержать объекты других типов, и нечаянно удалить подразделение *целиком*, а не только отображаемые учетные записи. Поэтому не забывайте выключать все фильтры перед выполнением операций удаления или перемещения контейнерных объектов!

Поэтому при использовании фильтров рекомендуется обязательно включать область описания (Description Bar) и обращать внимание на строку **[Filter Activated]** (Фильтр включен), которая напоминает о работе фильтра

(рис. 12.31). Эта панель включается в окне **Customize View** (Настройка), открывающемся по команде **View** | **Customize** (Вид | Настройка).

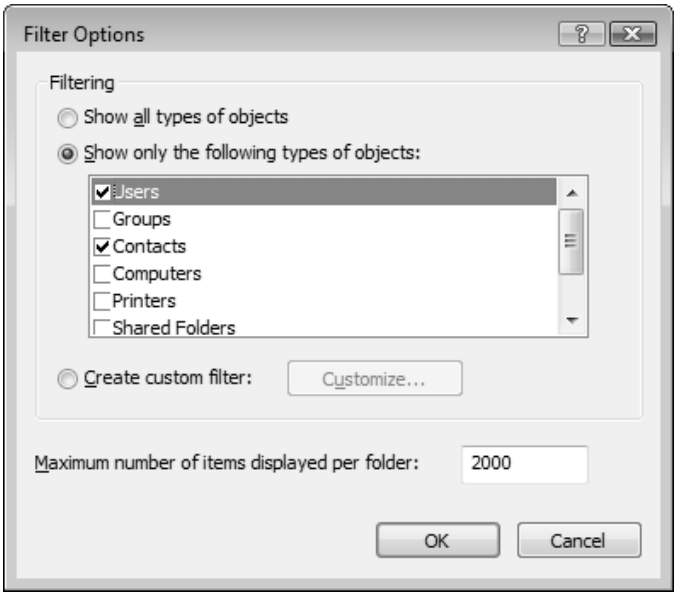


Рис. 12.30. Пример фильтра отображаемых объектов

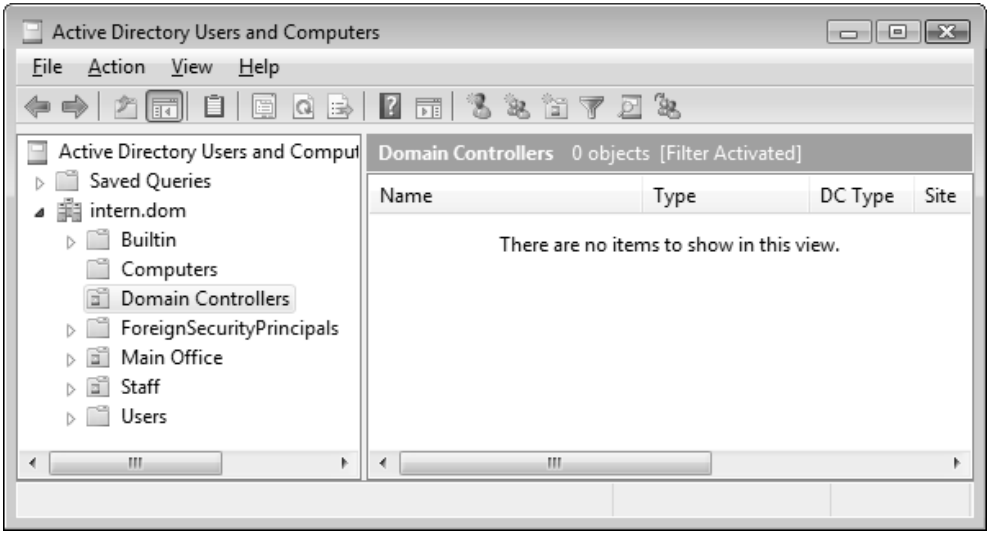


Рис. 12.31. Количество отображаемых объектов и указание на включенный фильтр

Поиск объектов в каталоге Active Directory

Другим средством, облегчающим работу с большим числом объектов Active Directory и позволяющим находить объекты определенного типа (или с заданными свойствами), является опция **Find** (Поиск). В некотором смысле она работает как и фильтр, только имеет более широкую область действия: объекты можно находить во всем каталоге (в лесу), в любом домене или в указанном контейнере. Для поиска объектов можно использовать команду **Find** (Найти), имеющуюся в контекстном меню каждого контейнера, или же можно выбрать контейнер и нажать кнопку **Find objects in Active Directory Domain Service** (Поиск объектов в доменных службах Active Directory)  на панели инструментов.

Набор полей поиска (и расширенного поиска) меняется в зависимости от типа объекта каталога (можно искать пользователей, компьютеры, принтеры и т. д.). Условия поиска для расширенных операций задаются так же, как и для фильтров, и имеют те же ограничения. Опция **Custom Search** (Пользовательский поиск) в списке **Find** (Найти) предоставляет наибольшую гибкость в работе: можно указать в запросе практически любой атрибут любого объектного типа каталога. Также имеется опция **Common Queries** (Общие запросы), с помощью которой можно находить только пользователей, компьютеры и группы. Например, с ее помощью можно найти заблокированные пользовательские и машинные учетные записи или пользовательские записи, не использованные в течение указанного интервала времени (в днях). В окне найденных объектов в контекстных меню можно выбирать те же команды, которые имеются для этих объектов в главном окне оснастки (см. рис. 12.32).

Примечания

Когда выполняется поиск пользователей при выборе опции **Find Users, Contacts, and Groups** (Пользователи, контакты и группы), наличие строки, введенной в поле **Name**, проверяется во *всех* атрибутах, определяющих имена — *cn*, *First name*, *Last name* и *Display name*.

Обратите внимание на то, что список **In** (Где) содержит список (history) контейнеров (подразделений), которые выбирались при обзоре доменного дерева (кнопка **Browse**).

Пример окна **Find** (Найти) и результаты поиска показаны на рис. 12.32. С помощью указанного запроса во всем каталоге найдены все группы, имена которых начинаются с буквы "s". Этот пример иллюстрирует тот факт, что

поиск можно выполнять во всем лесу доменов (в данном случае имеются два домена — intern.dom и sub.intern.dom), а не только в домене или контейнере. Обратите также внимание на то, что группа Server Operators (Операторы сервера) имеется в обоих доменах, однако только в одном домене (корневом домене леса) есть группа Schema Admins (Администраторы схемы).

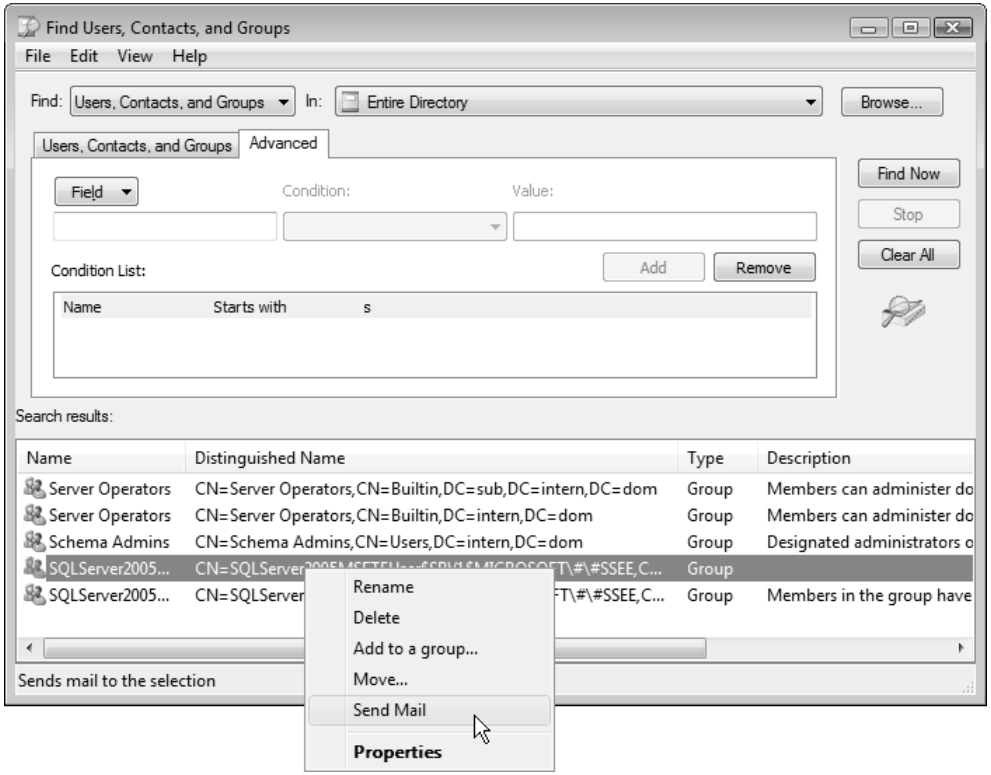


Рис. 12.32. Поиск объектов в каталоге Active Directory

Режим отображения в окне, показанном на рис. 12.32, не является стандартным. Например, чтобы увидеть полные отличительные имена найденных объектов (содержащие имена родительских контейнеров), выберите команду **Choose Columns** (Выбрать столбцы) в меню **View** (Вид), найдите столбец с именем **Distinguished Name** (Различающееся имя) и добавьте его в список **Columns shown** (Отображаемые столбцы).

Одновременное редактирование множества объектов каталога

Оснастка **Active Directory Users and Computers** (Active Directory – пользователи и компьютеры) позволяет одновременно редактировать свойства нескольких объектов каталога, в первую очередь — пользовательских учетных записей. Для большинства объектов каталога (компьютеров, групп, подразделений и т. д.) одновременно можно поменять только описание (description).

Рис. 12.33. Изменение UPN-суффикса, времени входа в систему и запрос на смену пароля

Однако для пользовательских учетных записей можно изменять свыше 30 атрибутов. Объекты для редактирования выбираются как обычно — при помощи курсора и клавиш <Shift> и <Ctrl>. Затем в контекстном меню или в

меню **Action** (Действие) нужно выполнить команду **Properties** (Свойства). Если выделено несколько учетных записей, что появляется *модифицированное* окно **Properties** (Свойства). Примеры различных вкладок этого окна показаны на рис. 12.33 и рис. 12.34.

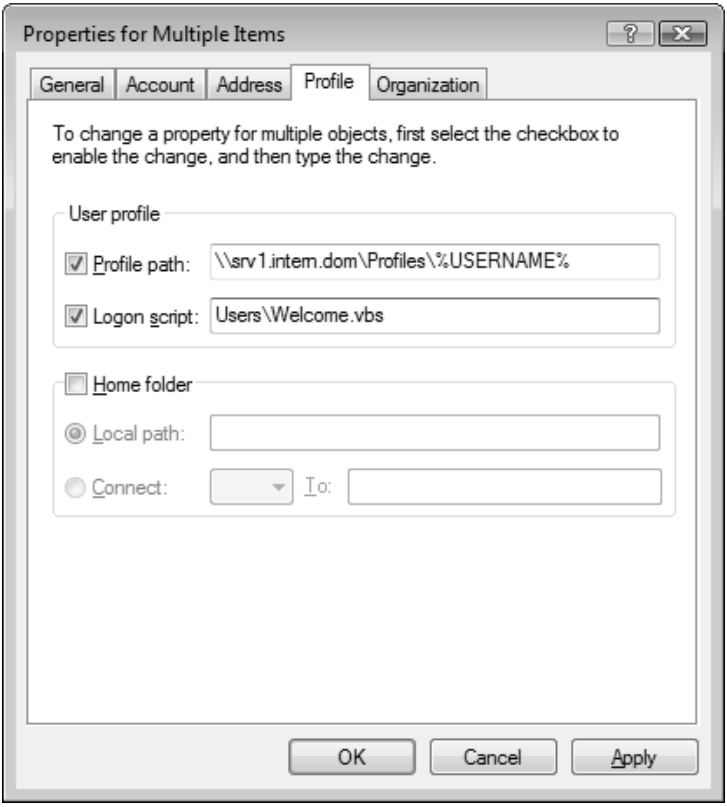


Рис. 12.34. Назначение перемещаемого профиля и сценария входа (справа) для нескольких пользовательских учетных записей

На вкладке **Profile** (Профиль) можно задавать все те свойства, которые доступны в обычном окне свойств учетной записи пользователя. Если какой-нибудь флажок установлен, то значение соответствующего поля будет переопределено. Если это поле пусто, то имеющееся значение очищается (удаляется). Если флажок не установлен (соответствующее поле недоступно), то имеющиеся значения поля остаются без изменений.

Оснастка *Active Directory Sites and Services*

Оснастка **Active Directory Sites and Services** (Active Directory – сайты и службы) является основным инструментом с графическим интерфейсом, с помощью которого администратор может конфигурировать Active Directory как *распределенную сетевую службу*. (Другие административные оснастки представляют Active Directory на логическом уровне, как единое информационное хранилище.) Эта оснастка редко используется в небольших сетях с единственным сайтом и несколькими контроллерами домена. Однако в больших сетях, состоящих из многих сайтов, эта оснастка становится одним из важнейших средств администрирования топологии каталога Active Directory.

Кроме контроллеров доменов Active Directory, оснастку можно использовать для управления топологией репликации экземпляров каталога AD LDS. Набор административных средств, включая данную оснастку, можно устанавливать на серверах независимо от доменной службы Active Directory (см. перечень компонентов на рис. 12.21).

Ниже перечислены операции, которые можно выполнять с помощью оснастки **Active Directory Sites and Services** (Active Directory – сайты и службы):

- назначение контроллерам домена роли сервера Глобального каталога;
- изменение топологии репликации в лесу (создание/удаление сайтов, подсетей, связей (links) и соединений);
- разрешение кэширования универсальных (universal) групп;
- создание схемы расположения (location scheme), используемой объектами принтеров, компьютеров, сайтов и подсетей;
- ручной запуск репликации внутри сайта и между сайтами;

> ***Примечание***
>
> В контроллерах на базе Windows Server 2008 имеется новая возможность запуска репликации с помощью данной оснастки. Можно выбрать любой другой контроллер и инициировать входящую или исходящую репликацию между указанным сервером и локальным контроллером. Раньше такую операцию можно было делать только при помощи специальных утилит (например, Active Directory Replication Monitor (Replmon.exe)).

- запуск процесса Knowledge Consistency Checker (KCC) для регенерации топологии репликации;
- изменение расписаний и интервалов для репликации внутри сайта и между сайтами;
- назначение связям стоимости пути (cost);
- назначение серверов-форпостов (серверов-плацдармов, bridgehead);
- делегирование пользователям или группам прав на управление сайтами, подсетями, серверами и другими контейнерами;
- настройка параметров безопасности и аудита для различных объектов, определяющих топологию репликации;
- назначение политик запросов LDAP.

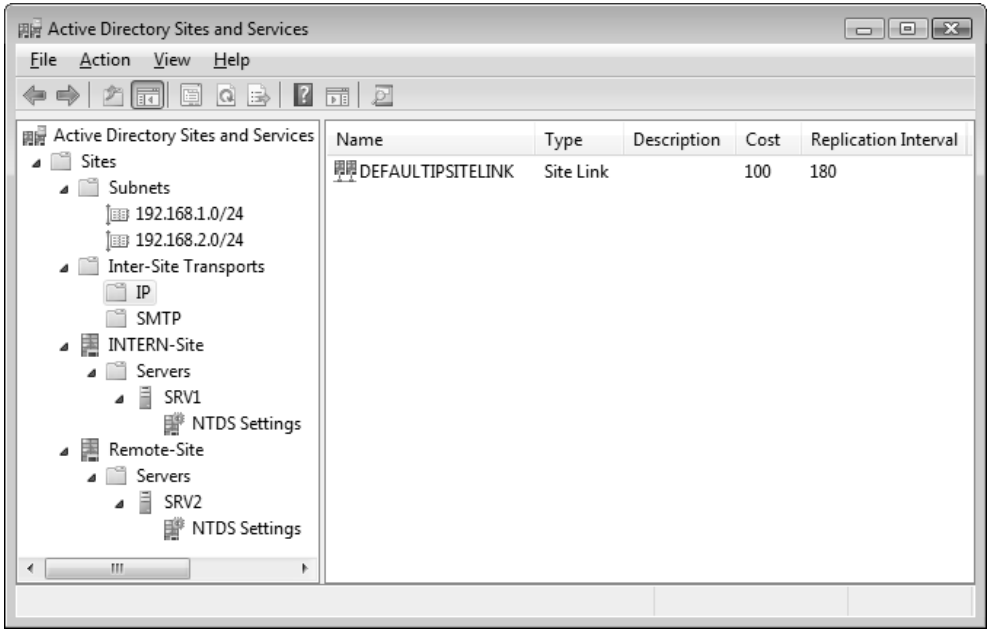


Рис. 12.35. Пример простой сети с двумя сайтами

Внимание!

В отличие от контроллеров домена на базе Windows Server 2003, оснастку **Active Directory Sites and Services** (Active Directory – сайты и службы) нельзя использоваться для выбора GPO-объектов, привязанных к сайтам;

для работы со всеми GPO-объектами можно использовать только оснастку **Group Policy Management** (Управление групповой политикой).

На рис. 12.35 показано главное окно оснастки **Active Directory Sites and Services** (Active Directory – сайты и службы), в котором представлены практически все основные элементы сетевой топологии: сайты, подсети, межсайтовые связи, соединения и серверы (контроллеры домена).

Оснастка *Active Directory Domains and Trusts*

Оснастка **Active Directory Domains and Trusts** (Active Directory – домены и доверие) в первую очередь ориентирована на администратора предприятия и, в частности, предоставляет ему возможность быстрого просмотра леса доменов и выбора администрируемого домена.

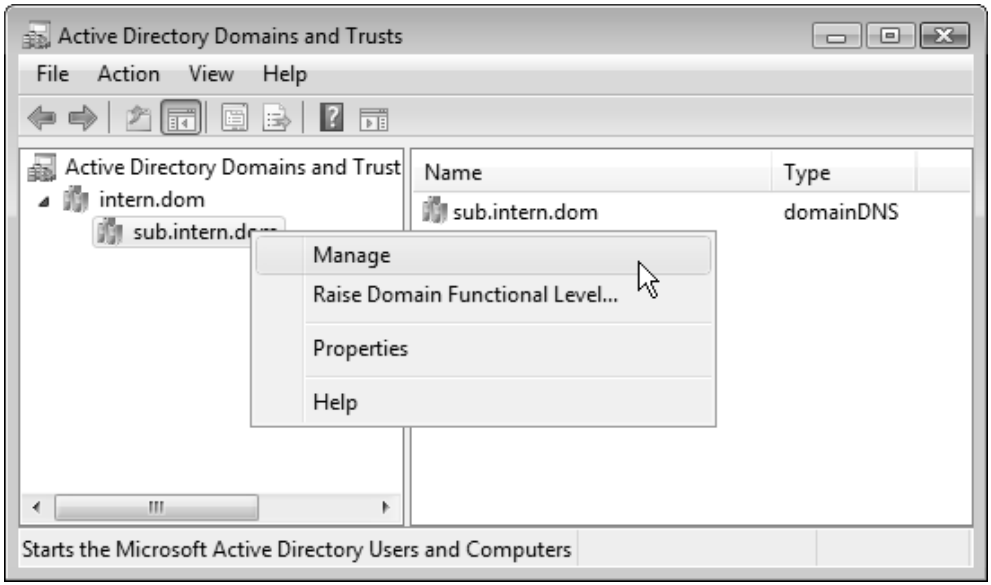


Рис. 12.36. Выбор администрируемого домена в лесу доменов

На рис. 12.36 в качестве примера показано главное окно этой оснастки, в котором отображается структура простого леса, состоящего из двух доменов

(с корневым доменом intern.dom). Если выбрать домен в окне структуры и выполнить команду **Manage** (Управление), присутствующую в контекстном меню или в меню **Action** (Действие), то для администрирования этого домена будет запущена оснастка **Active Directory Users and Computers** (Active Directory – пользователи и компьютеры).

Изменение функционального уровня (режима работы) домена

С помощью оснастки **Active Directory Domains and Trusts** (Active Directory – домены и доверие) осуществляется повышение функционального уровня (functional level) отдельного домена или всего леса. При этом всегда следует помнить, этот ***уровень потом понизить нельзя***!

> ***Примечание***
>
> Изменить режим работы или функциональный уровень *домена* можно и при помощи оснастки **Active Directory Users and Computers** (Active Directory – пользователи и компьютеры).

Чтобы повысить функциональный уровень *домена*, выберите его имя в дереве доменов и в контекстном меню выполните команду **Raise Domain Functional Level** (Изменение режима работы домена) (см. рис. 12.36). В появившемся окне (рис. 12.37) будут указаны текущий уровень домена и новые возможные уровни (если таковые имеются).

Если в выбранном домене все контроллеры работают под управлением Windows Server 2008, можно сразу перейти на функциональный уровень *Windows Server 2008*. Для этого нужно выбрать его из списка и нажать кнопку **Raise** (Изменить). Если в домене присутствуют контроллеры на базе младших систем (Windows 2000 или Windows Server 2003), возникнет ошибку. Система сообщит о контроллерах, препятствующих повышению функционального уровня; эту информацию можно будет сохранить в файле.

В случае выполнения условий повышения уровня операция выполняется, и ее результат реплицируется на все контроллеры выбранного домена. Необходимо дождаться окончания репликации, после чего можно проверить текущий функциональный уровень домена.

Чтобы повысить уровень *леса*, выберите в окне оснастки корень дерева объектов и выполните в контекстном меню команду **Raise Forest Functional**

Level (Изменение режима работы леса). Опять-таки, все возможные ошибки будут обнаружены, и их можно будет сохранить.

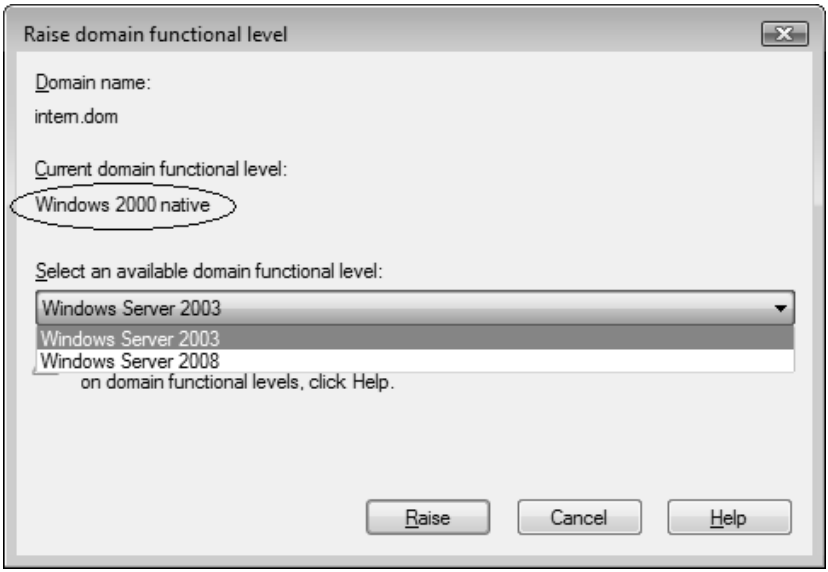


Рис. 12.37. Выбор функционального уровня домена

Если два леса доменов функционируют на уровне *Windows Server 2003* и выше, то при помощи оснастки **Active Directory Domains and Trusts** (Active Directory – домены и доверие) между корневыми доменами этих лесов можно установить *доверительные отношения на уровне лесов* (forest trusts).

Проверка доверительных отношений

С помощью оснастки **Active Directory Domains and Trusts** (Active Directory – домены и доверие) администратор может проверять доверительные отношения между доменами и создавать новые отношения. В первую очередь это касается доверительных отношений с другими лесами, поскольку такие отношения должны создаваться вручную. Иногда также возникает необходимость создания явных, односторонних доверительных отношений между доменами Active Directory, относящихся к разным доменным деревьям (или лесам — при наличии доверительных отношений на уровне лесов, forest trusts) или, даже, к одному дереву.

Для проверки доверительного отношения между доменами пользуйтесь следующей процедурой:

1. Откройте окно свойств домена.
2. Выберите отношение на вкладке **Trusts** (Доверия) (рис. 12.38) и нажмите кнопку **Properties** (Свойства).

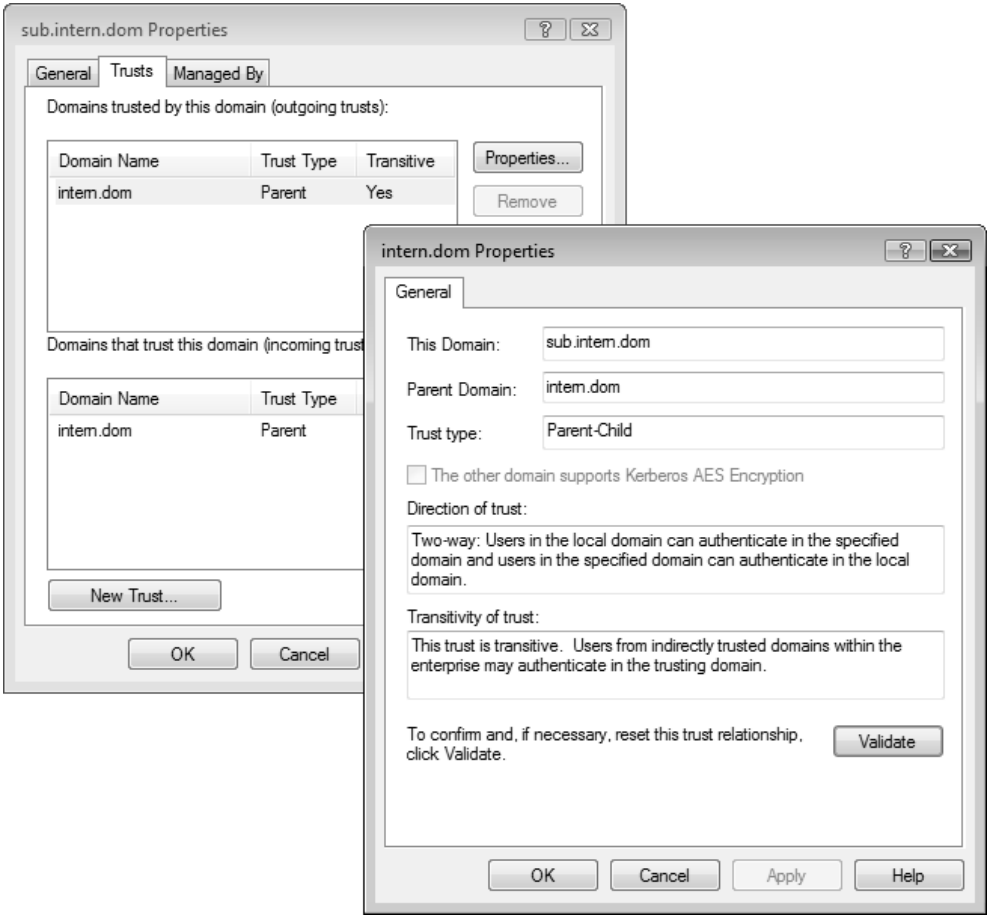


Рис. 12.38. Просмотр свойств доверительных отношений между доменами

3. В открывшемся окне нажмите кнопку **Validate** (Проверка). При наличии двусторонних отношений всегда проверяется исходящее (outgoing) отношение и предлагается ввести учетные данные администратора другого

домена для проверки входящего (incoming) отношения. Если оба отношения находятся в рабочем состоянии, появляется сообщение: "The trust has been verified. It is in place and active." (Доверие проверено. Оно работоспособно и активно.)

Если система сообщает об ошибке и предлагает заново инициализировать (reset) отношение, ответьте утвердительно. Обычно в этом случае отношения успешно восстанавливаются. Для проверки и обновления доверительных отношений можно также пользоваться утилитой NetDom.exe.

Оснастка *ADSI Edit* (Редактирование ADSI)

Можно сказать, что оснастка **ADSI Edit** (Редактирование ADSI) для Active Directory играет такую же роль, что и утилита Regedit.exe для системного реестра. С помощью этой оснастки можно получить "низкоуровневый" доступ к каталогам Active Directory. Она позволяет выполнять следующие операции:

- подключаться к любому разделу каталога, включая разделы приложений;
- непосредственно подключаться к любому объекту Active Directory с использованием отличительного имени объекта;
- просматривать, перемещать и переименовывать объекты Active Directory, а также модифицировать любые их атрибуты (если эта операция допустима);
- настраивать параметры безопасности "с точностью" до одного атрибута;
- выполнять запросы по всему каталогу и сохранять их для последующего использования;
- создавать и удалять объекты любых типов (если эта операция допустима);
- обращаться к Глобальному каталогу.

Ранее оснастка **ADSI Edit** (Редактирование ADSI) входила в состав пакета Windows Support Tools, а в системах Windows Server 2008 она является стандартным компонентом сервера и устанавливается при добавлении ролей *Active Directory Domain Services (AD DS)* (Доменные службы Active Directory) и/или *Active Directory Lightweight Directory Services* (Службы Active Directory облегченного доступа к каталогам (AD LDS)). Также она входит в состав средств удаленного администрирования (см. рис. 12.21).

Оснастку можно запускать автономно, из меню **Administrative Tools** (Администрирование), или добавлять к любым консолям MMC.

Подключение к разделам каталога

Оснастка **ADSI Edit** (Редактирование ADSI) работает с пространствами имен каталога Active Directory, также называемыми *контекстами* или *разделами каталога*. Для доменной службы Active Directory имеются три стандартных раздела, перечисленных ниже (для примера в скобках приведены отличительные имена контекстов для домена с DNS-именем domain.com):

- контекст именования по умолчанию (Default naming context), или доменный раздел (DC=*domain*, DC=*com*);
- раздел Configuration (CN=Configuration, DC=*domain*, DC=*com*);
- раздел Schema (CN=Schema, CN=Configuration, DC=*domain*, DC=*com*).

Первый раздел реплицируется между всеми контроллерами, входящими в конкретный домен. Два других раздела реплицируются между всеми контроллерами, входящими в доменное дерево.

Кроме того, все LDAP-каталоги (к которым относится и Active Directory) имеют еще один специальный объект, к которому может подключаться оснастка:

- *RootDSE*

Этот объект хранит информацию об основных свойствах каталога, включая перечень имеющихся имен разделов; он описывает конфигурацию и возможности данного сервера каталога.

В доменах на базе серверов Windows Server 2003/Windows Server 2008 оснастка **ADSI Edit** (Редактирование ADSI) позволяет также подключаться к любым *разделам приложений*. Например, если на контроллере домена устанавливается DNS-сервер, то по умолчанию создаются два встроенных раздела приложений (см. рис. 12.1):

- ForestDnsZones (DC=ForestDnsZones, DC=*domain*, DC=*com*)
- DomainDnsZones (DC=DomainDnsZones, DC= *domain*, DC= *com*)

На рис. 12.39 в качестве примера показано окно оснастки, где выполнены подключения к двум службам каталогов Active Directory: службе домена intern.dom и экземпляру службы AD LDS, имеющему раздел DC=Dbase.

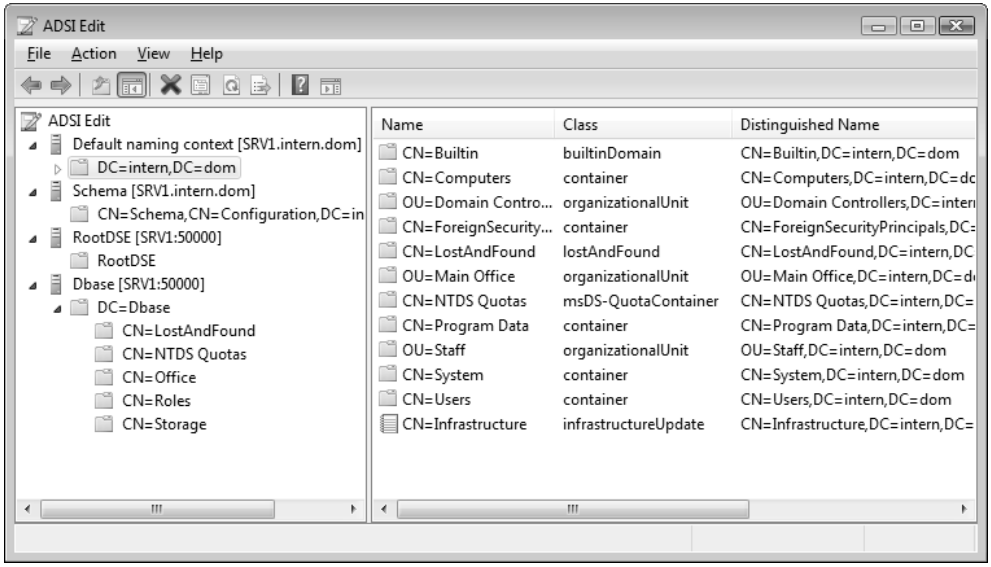


Рис. 12.39. Окно оснастки **ADSI Edit**
с примерами подключений к различным разделам каталогов Active Directory

Рис. 12.40. Подключение к некоторому пространству имен

Просмотр и редактирование атрибутов объектов каталога выполняются в окне свойств этого объекта; команда создания новых объектов вызывается из контекстного меню выбранного контейнера.

Для создания нового соединения (подключения к разделу каталога или объекту RootDSE) выберите корень дерева в окне структуры и выполните команду **Connect to** (Подключение к) в контекстном меню. Дайте соединению имя в поле **Name** и введите отличительное имя объекта или выберите одно из предопределенных пространств имен в списке **Select a well known Naming Context** (Выберите известный контекст именования) (рис. 12.40). Для работы можно выбирать любые домены или серверы каталога. При подключении к доменной службе Active Directory обычно используется контроллер, на котором выполнена регистрация.

При подключении к экземплярам каталога AD LDS необходимо указывать имя сервера и номер порта (рис. 12.41). Для них существуют только два стандартных пространства имен: Schema и Configuration. Произвольное отличительное имя каталога может задаваться при его создании (см. рис. 12.47).

Рис. 12.41. Подключение к разделу каталога AD LDS

В окне **Advanced** (Дополнительные параметры) (для его вызова нажмите кнопку **Advanced** в окне **Connection Settings**) можно указать альтернативное имя пользователя и его пароль, номер порта и протокол: переключатель **LDAP** или **Global Catalog** (рис. 12.42). Для просмотра или изменения свойств соединения выполните команду **Settings** в его контекстном меню. Любое соединение можно удалить при помощи команды **Remove**.

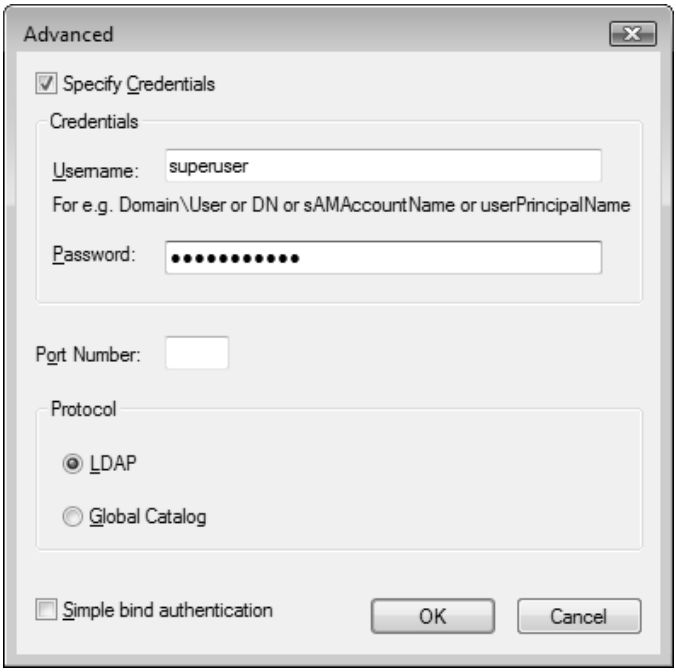


Рис. 12.42. Окно дополнительных свойств соединения

Оснастка *Active Directory Schema*

Оснастка **Active Directory Schema** (Схема Active Directory) является основным GUI-инструментом, позволяющим просматривать и модифицировать классы и атрибуты каталогов Active Directory и AD LDS. Эта оснастка позволяет просматривать идентификаторы (X.500 OID) классов и атрибутов, диапазоны допустимых значений атрибутов, обязательные и необязательные атрибуты классов, а также другую метаинформацию об атрибутах и классах.

Примечание

Другой инструмент, позволяющий работать со схемой, — оснастка **ADSI Edit** (Редактирование ADSI); работа с ней требует значительно более глубокого знакомства с внутренним устройством Active Directory. Два других пути модификации схемы — использование сценариев или утилит для пакетной обработки, таких как LDIFDE и CSVDE.)

Установка оснастки

Оснастка **Active Directory Schema** (Схема Active Directory) по умолчанию присутствует на контроллерах домена. При этом оснастка не появляется ни в меню **Start** (Пуск), ни на панели управления, и ее нужно вручную добавлять к какой-нибудь консоли MMC. Перед этим необходимо зарегистрировать библиотеку DLL с помощью следующей команды:

```
regsvr32 schmmgmt.dll
```

Обязательно должно появиться сообщение, показанное на рис. 12.43.

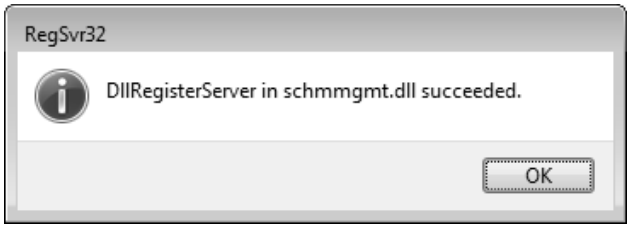


Рис. 12.43. При успешной регистрации DLL-файла должно появиться такое сообщение

После того как файл schmmgmt.dll зарегистрирован на компьютере, можно создать новый документ MMC (представляющий собой консоль, сохраненную с произвольным именем), содержащий оснастку **Active Directory Schema** (Схема Active Directory) (рис. 12.44), или добавить оснастку к уже существующей пользовательской консоли.

Примечание

Оснастка **Active Directory Schema** (Схема Active Directory) может устанавливаться на любом сервере Windows Server 2008 в составе набора инструментов удаленного администрирования каталогов Active Directory (см. рис. 12.21).

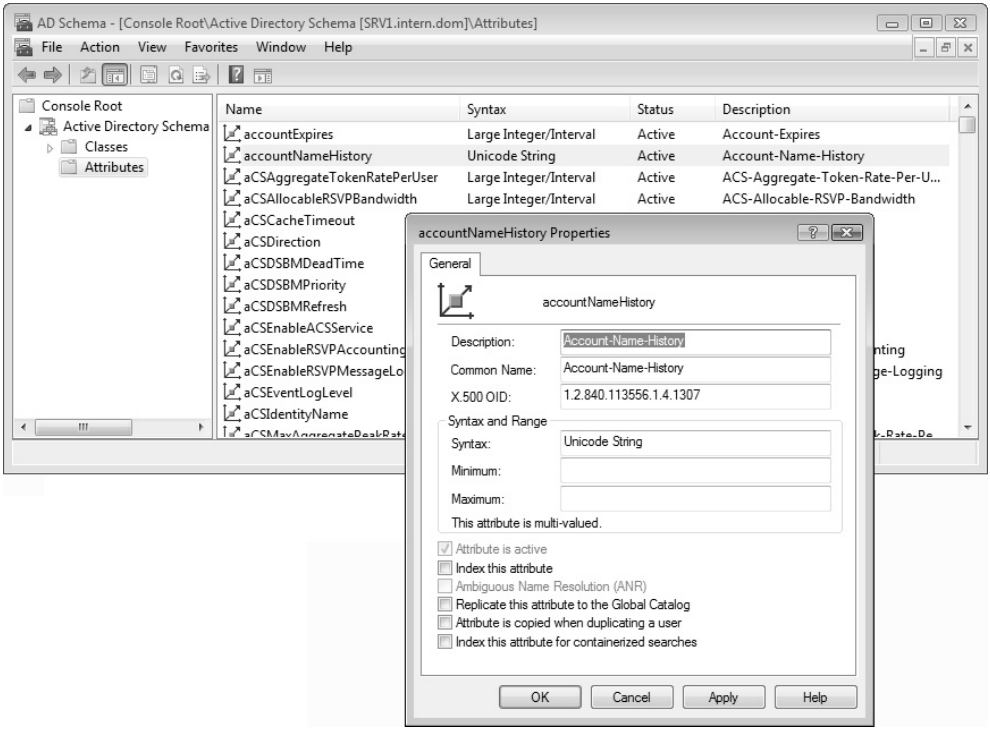


Рис. 12.44. Окно оснастки **Active Directory Schema**

Внесение изменений в схему

В лесу доменов Active Directory изменения схемы разрешены только на том контроллере домена, который владеет FSMO-ролью Schema Master. (Для поиска хозяина схемы в лесу доменов можно воспользоваться командой `dsquery server -hasfsmo schema`). По умолчанию схему могут модифицировать только члены группы Schema Admins (Администраторы схемы). Для каталогов AD LDS требуются права, заданные при установке экземпляра каталога.

Чтобы модифицировать и, в особенности, расширять схему, нужно глубоко понимать концепции LDAP-каталогов и доменов Active Directory, а также структуру классов каталога. Эти вопросы требуют отдельной книги. Однако даже при обычной эксплуатации службы каталога у администратора может возникнуть необходимость выполнить некоторые операции, например, пере-

численные ниже (даны имена флажков на вкладке **General** в окне свойств атрибутов; см. рис. 12.44):

- **Attribute (class) is active**. Если некоторый вновь созданный (например, тестовый) атрибут или класс еще не используется в Active Directory (т. е. не создавались объекты этого класса, или атрибут не добавлялся к имеющимся классам), можно "запретить" его. (Атрибуты и классы Active Directory нельзя *удалить*.) Такой атрибут или класс рассматривается как *несуществующий* (defunct). В доменах, имеющих функциональный уровень *Windows Server 2003*, такой объект можно *переопределить* (redefine — т. е. переопределить его свойства) и снова *активизировать* (reactivate);
- **Index this attribute** (Индексировать этот атрибут). Индексирование атрибута ускоряет выполнение часто используемых запросов, в которых указан данный атрибут;
- **Replicate this attribute to the Global Catalog** (Репликация этого атрибута в Глобальный каталог). Если некоторый атрибут включен в Глобальный каталог, его значения можно получать, выполняя запросы в рамках всего леса;
- для классов имеется флажок **Show objects of this class while browsing** (Отображать объекты этого класса при просмотре). Он управляет значением атрибута *showInAdvancedViewOnly*. Если этот флажок установлен, то значение атрибута будет равно `FALSE` и новый объект будет всегда виден в административных оснастках. Состояние флажка имеет значение только для пользовательских (вновь созданных) классов.

Чтобы выполнить перечисленные операции, в окне структуры раскройте узел **Attributes** или **Classes** и найдите нужный атрибут или класс. Откройте окно **Properties** и установите соответствующий флаг на вкладке **General**.

> ***Внимание!***
>
> После того как новый атрибут добавляется в Глобальный каталог, изменения будут реплицироваться по всему лесу доменов. (Это относится ко многим операциям по модификации схемы.) Например, вы включили в Глобальный каталог атрибут *department*. В результате все значения этого атрибута для пользовательских объектов должны будут реплицироваться на серверы Глобального каталога. Этот процесс может создавать заметный трафик в сети. Поэтому подобные операции не следует выполнять часто, и их нужно хорошо планировать.

Установка служб каталогов AD LDS

Служба каталога Active Directory впервые появилась в операционных системах Windows 2000 и была неразрывно связана со службой доменов Windows. Позже появилась "автономная" версия службы каталогов, названная Active Directory Application Mode, ADAM[1] (Прикладной режим Active Directory). Ее можно свободно загружать и устанавливать в различных системах, начиная с Windows XP. В серверах Windows Server 2008 службы *Active Directory Lightweight Directory Services (AD LDS)* (Службы Active Directory облегченного доступа к каталогам) являются частью системы и связаны с одноименной ролью сервера.

Службы AD LDS могут устанавливаться на любом сервере Windows Server 2008 и никак не связаны с ролью сервера *Active Directory Domain Services (AD DS)* (Доменные службы Active Directory). Таким образом, сервер может являться контроллером домена и при этом на нем могут быть установлены службы AD LDS.

Службы AD LDS устанавливаются как системный сервис с уникальным именем, поэтому на сервере могут быть развернуты несколько экземпляров (instance) этих служб, которые будут функционировать независимо друг от друга. (Состоянием этих сервисов — как и обычных системных служб — можно управлять с помощью оснастки **Services** (Службы).) Для репликации содержимого каталога между различными серверами службы AD LDS используются RPC-вызовы (т. е. службы FRS или DFS Replication не задействуются).

После установки роли AD LDS файлы, необходимые для работы служб, появляются в папке *%SystemRoot%*\ADAM. В папке *%SystemRoot%*\Help можно найти файл справки adam.CHM, где достаточно подробно описаны все способы развертывания и использования служб AD LDS.

Для установки роли Active Directory Lightweight Directory Services (AD LDS) (Службы Active Directory облегченного доступа к каталогам) используется оснастка **Server Manager** (Диспетчер сервера). После установки роли нужно создать экземпляр служб с помощью специального мастера *Active Directory Lightweight Directory Services Setup Wizard* (Мастер установки служб Active Directory облегченного доступа к каталогам (AD LDS)), который запускается из меню **Administrative Tools** (Администрирование).

---

[1] Эта аббревиатура встречается до сих пор.

Примечание

Для управления каталогами AD LDS имеется утилита *Dsdbutil.exe*, по многим возможностям напоминающая утилиту Ntdsutil.exe, используемую вместе с доменными службами Active Directory.

Экземпляр служб AD LDS можно также устанавливать с носителя (их архива). Все необходимые операции аналогичны тем, которые рассматривались для случая установки контроллера домена.

Для управления службами AD LDS и изменения объектов каталога используются стандартные оснастки, рассмотренные ранее:

- оснастка **Active Directory Sites and Services** (Active Directory – сайты и службы);
- оснастка **ADSI Edit** (Редактирование ADSI);
- оснастка **Active Directory Schema** (Схема Active Directory).

Создание и удаление экземпляра служб AD LDS

После установки роли AD LDS необходимо создать хотя бы один экземпляр служб. Для этого нужно запустить мастер — из меню **Administrative Tools** (Администрирование) или с помощью команды `%windir%\adam\adaminstall` (возможно также добавление параметра `/adv`).

Дальнейшие шаги по созданию экземпляра служб AD LDS выглядят следующим образом:

1. Необходимо указать, создается новый экземпляр или реплика уже существующего. (Рассмотрим создание нового экземпляра.)
2. Новому экземпляру служб нужно дать имя (рис. 12.45). В соответствии с этим именем будет назван и сервис, связанный с данным каталогом Active Directory.
3. Следующий очень важный шаг — выбор номеров портов LDAP для нового экземпляра служб (рис. 12.46). По умолчанию предлагаются номера, которые обычно используют контроллеры доменов Active Directory. Поэтому лучше выбирать другие номера в предложенном диапазоне (например, если сервер *является* контроллером домена, то предлагаться будут порты 50000 и 50001). Номер порта является "ключом" для доступа к этому экземпляру служб AD LDS, и если его не запомнить, то потом определить будет достаточно сложно. Обратите внимание на то, как номер порта отображается в окне оснастки **ADSI Edit** (Редактирование ADSI) (см. рис. 12.41).

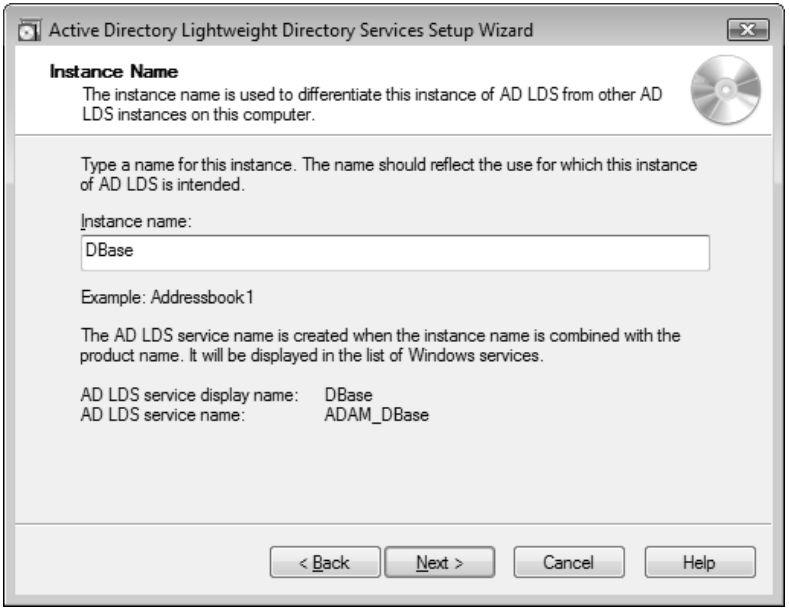


Рис. 12.45. Выбор имени экземпляра каталога Active Directory

Рис. 12.46. Выбор LDAP портов для доступа к каталогу

4. Затем указывается необходимость создания раздела приложений и имя раздела, если такой раздел будет создаваться сразу (рис. 12.47) (потом создавать разделы можно с помощью утилиты *Ldp.exe*). Если раздел не создать, то для нового каталога будет доступен только объект RootDSE.

Рис. 12.47. Определение имени раздела приложений

5. По умолчанию все данные нового каталога хранятся в папке C:\Program Files\Microsoft ADAM\<*имяЭкземпляра*>\data. На следующем шаге это местоположение можно изменить.

6. Нужно указать учетную запись, которую экземпляр каталога будет использовать при своей работе. По умолчанию это учетная запись Network Service.

7. По умолчанию административные права по отношению к новому каталогу получает зарегистрированный пользователь; можно выбрать учетную запись, которая будет использоваться для управления данным каталогом.

8. Следует указать, какие объекты по умолчанию будут созданы в каталоге — для этого используются стандартные файлы описаний (в формате LDIF) (рис. 12.48). Если содержимое каталога будет реплицироваться ме-

жду несколькими серверами, то необходимо, как минимум, выбрать файл MS-AdamSyncMetadata.LDF.

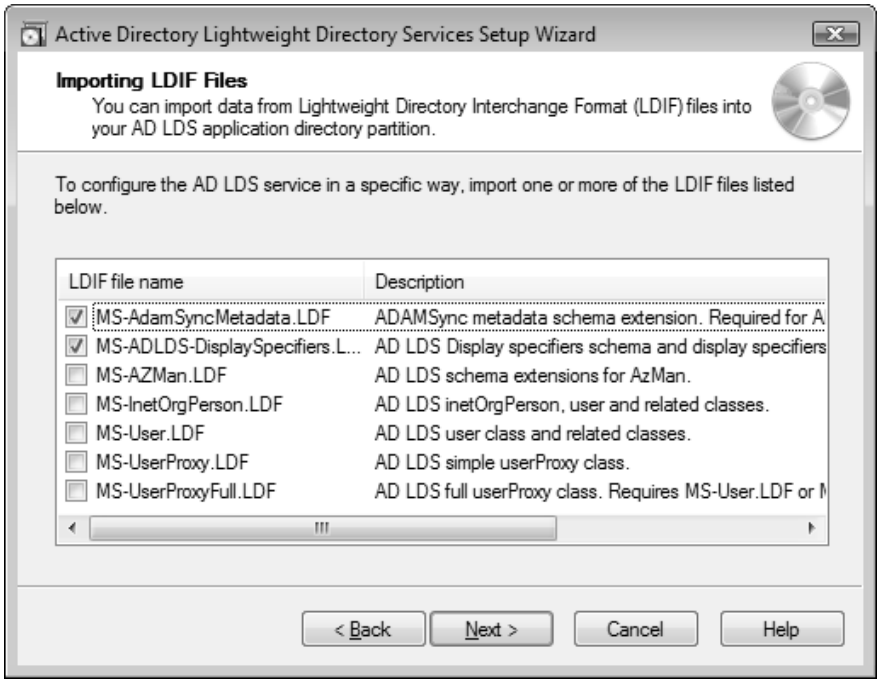


Рис. 12.48. Выбор объектов, создаваемых в каталоге по умолчанию

9. В следующем окне мастера после проверки введенных параметров можно нажать кнопку **Next** (Далее) — начнется установка нового экземпляра каталога служб AD LDS.

За работой установленных экземпляров служб AD LDS очень удобно наблюдать в окне оснастки **Server Manager** (Диспетчер сервера), выбрав соответствующую роль (рис. 12.49). В нашем примере можно видеть, что на сервере работают два экземпляра служб, имеющие имена DBase и Store. Из этого окна (см. ссылки в правом нижнем углу) можно запускать мастер создания экземпляров каталога и административные утилиты для работы с каталогом.

Для проверки работоспособности нового экземпляра каталога AD LDS можно с помощью оснастки **ADSI Edit** (Редактирование ADSI) подключиться к объекту RootDSE или созданному разделу приложений.

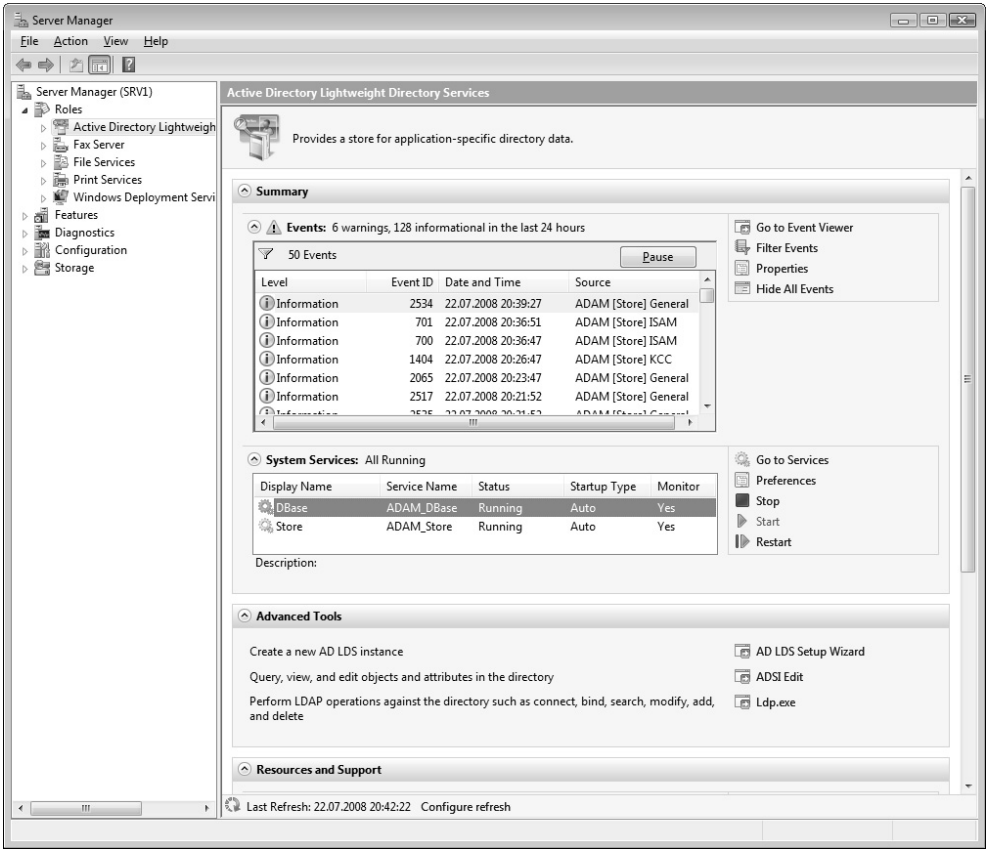


Рис. 12.49. Управление работой экземпляров служб AD LDS и мониторинг событий

Для этого чтобы удалить экземпляр служб AD LDS необходимо на панели управления выбрать опцию **Program and Features** (Программы и компоненты) и найти строку с именем вида AD LDS Instance *<имяЭкземпляра>*. Далее этот экземпляр удаляется как обычная программа (при этом удаляется сервис с именем ADAM_*<имяЭкземпляра>*).

Глава 13

Групповые политики

Механизм *групповых политик* (group policy) является важнейшим средством для конфигурирования параметров безопасности системы, управления пользовательской средой и приложениями. В первую очередь их эффективность проявляется в доменах Active Directory, где групповые политики позволяют реализовать концепцию централизованного администрирования систем и пользователей.

В этой главе рассматриваются особенности реализации и принципы работы с групповыми политиками в системах Windows Server 2008, использующихся автономно (в составе рабочих групп) или входящих в домены Active Directory.

Новые возможности групповых политик в Windows Server 2008

В плане реализации механизма групповых политик системы Windows Server 2008 имеют много общего с Windows Vista, поскольку ядро систем разрабатывалось в рамках одного проекта. Усилия разработчиков были направлены на расширение возможностей групповых политик по управлению системными компонентами и приложениями, а также на упрощение использования политик в многоязыковой среде.

В системах Windows Server 2008 свыше 3000 групповых политик (почти в два раза больше, чем в предыдущих серверных версиях Windows). Бóльшая часть новых политик (около 80%) относится к области безопасности.

Перечислим далее основные принципиально новые возможности групповых политик в Windows Vista/Windows Server 2008 и в первую очередь те, которые интересны при использовании компьютеров в доменной среде. Некото-

рые средства групповых политик были реализованы уже в предыдущих версиях Windows, однако в Windows Vista/Windows Server 2008 они заметно модернизированы и расширены.

Новый формат и возможности файлов административных шаблонов (ADMX)

В системах Windows более ранних версий, чем Windows Vista/Windows Server 2008, описания регистровых групповых политик хранятся в текстовых файлах административных шаблонов, которые называются ADM-файлами. В системах Windows Vista/Windows Server 2008 для хранения описаний политик используется новый формат шаблонов — *Administrative Template Files*, ADMX, который базируется на спецификации XML.

ADMX-файлы делятся на две группы: не зависящие от языка, используемого в системе, и зависимые от языка. Этот подход позволяет администраторам легко выбирать язык, используемый в работе, и одни и те же параметры групповых политик могут без проблем редактироваться на различных языках.

В доменах ADMX-файлы не хранятся на томе SYSVOL. Это позволяет уменьшить трафик репликации содержимого тома за счет уменьшения размера объектов групповой политики (GPO).

Средства администрирования групповых политик позволяют работать как со старыми ADM-файлами, так и с новым форматом ADMX. Это обеспечивает гибкость при работе администратора в разных версиях Windows. Однако для администрирования политик, использующих ADMX, необходим компьютер с операционной системой не ниже Windows Vista.

Дополнительные области контролируемых параметров

Помимо предпочтений (preferences), появились новые группы параметров, которыми можно управлять с помощью "традиционных" групповых политик. Среди них отметим следующие функции и средства (управление некоторыми из них было возможно и в предыдущих версиях Windows, но в Windows Vista/Windows Server 2008 появились дополнительные политики):

- антивирусная защита;
- управление электропитанием;

- установка устройств (таких как USB-накопители, CD- и DVD-приводы и другие сменные носители);
- встроенный брандмауэр Windows (Windows Firewall);
- новые возможности браузера Internet Explorer 7.0;
- назначение принтеров с учетом местоположения;
- установка драйверов устройств (делегирование рядовым пользователям возможности установки драйверов для принтеров);
- средства защиты доступа к сети (Network Access Control (NAP) и др.);
- беспроводные сети;
- доступ к панелям инструментов, панели задач, меню **Start** (Пуск) и т. д.;
- службы терминалов (Terminal Services);

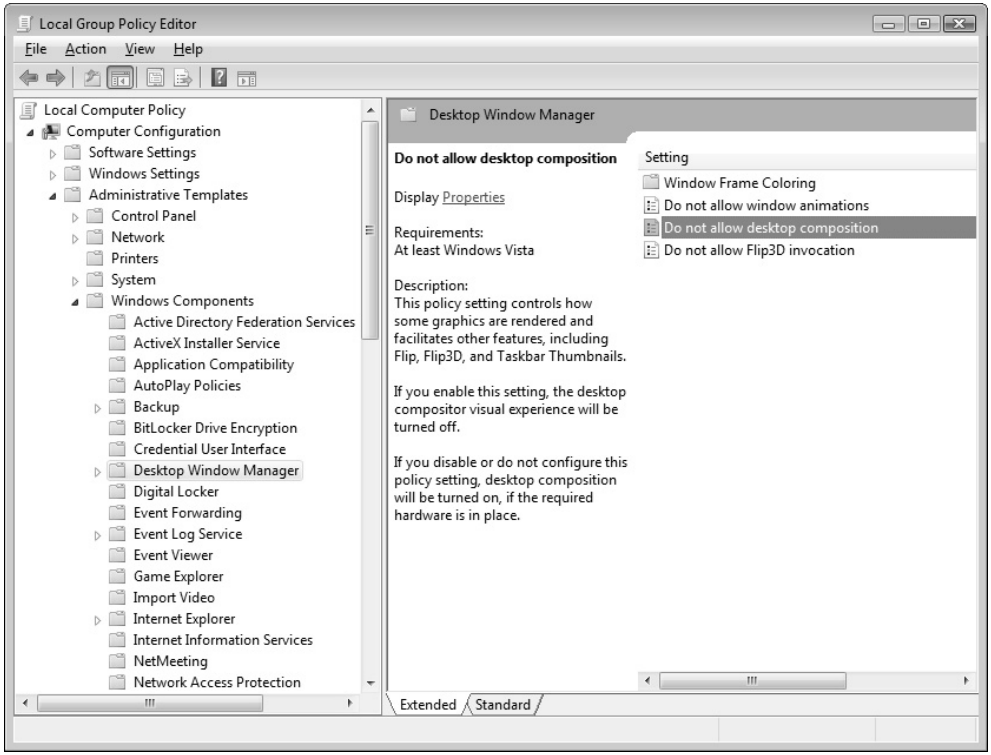


Рис. 13.1. Новые области действия групповых политик систем Windows Vista и Windows Server 2008

- планшетные компьютеры (Tablet PC);
- управление учетными записями (User Account Control, UAC);
- средства диагностики и решения проблем.

Некоторые новые области групповых политик можно видеть на рис. 13.1.

Гибкость при работе в разных сетях (NLA)

Механизм *Network Location Awareness* (NLA) позволяет групповым политикам гибко реагировать на изменение сетевой конфигурации компьютера и доступности ресурсов, что особенно важно для мобильных пользователей. Благодаря механизму NLA групповые политики могут точно определить момент готовности сети или сетевого адаптера и изменять свое поведение. Это касается и наличия или отсутствия связи с контроллерами домена. Применение групповых политик возможно даже при блокировке протокола ICMP брандмауэром или корпоративным сетевым экраном.

Служба Group Policy Client

В системах Windows Vista и Windows Server 2008 механизм групповых политик полностью изолирован от службы Winlogon, что обеспечивает более надежную работу и самой системы, и групповых политик. Для этого появилась новая служба — *Group Policy Client* (Клиент групповой политики, сервис gpsvc). Новый подход дает некоторые дополнительные преимущества:

- в системе могут устанавливаться новые файлы групповых политик, при этом не требуется перезагрузка операционной системы;
- работа групповых политик более эффективна, поскольку расходуется меньше ресурсов, используемых в фоновом режиме;
- уменьшается размер занятой памяти и повышается общая производительность.

Системные события и журналы

Благодаря наличию новой самостоятельной службы Group Policy Client (Клиент групповой политики) упрощается регистрация событий, связанных с применением групповых политик. Это позволяет упростить локализацию ошибок и повысить информационную ценность записей в журнале событий.

Возможность создания нескольких локальных объектов групповой политики

В системах Windows Vista/Windows Server 2008 может существовать *несколько* локальных объектов групповых политик — это уникальная для систем Windows возможность, которая упрощает управление средой в тех случаях, когда компьютер используется несколькими пользователями. Отдельные политики могут назначаться разным локальным пользователям или встроенным группам. Например, для рядовых пользователей компьютеров и для администраторов можно установить различные групповые политики. Администраторы систем могут вообще отключить применение параметров локальных групповых политик для своих учетных записей. Использование этой возможности будет описано далее.

Улучшенное управление браузером Internet Explorer

Новая версия браузера Internet Explorer 7.0, включенная в состав Windows Vista/Windows Server 2008 и устанавливаемая в предыдущих версиях Windows, полностью управляется с помощью групповых политик (в особенности это касается всех новых возможностей браузера) (рис. 13.2). Теперь параметрами браузера можно управлять централизованно, без необходимости установки расширения Internet Explorer Maintenance (IEM) или пакета Internet Explorer Administration Kit (IEAK).

Оснастка *Group Policy Management*

Оснастка **Group Policy Management**[1] (Управление групповой политикой, gpmc.msc) (рис. 13.3) позволяет централизованно управлять объектами групповых политик в многодоменных лесах Active Directory, упрощая многие рутинные операции, а также сохранять, восстанавливать и переносить GPO-объекты. Ранее эту оснастку можно было скачать дополнительно с веб-сайта Microsoft, теперь она является штатным компонентом систем Windows Server 2008. Ее возможности можно использовать из административных сценариев. Новая версия оснастки позволяет работать с новым форматом описания политик — ADMX-файлами.

---

[1] Она также называлась *Group Policy Management Console*.

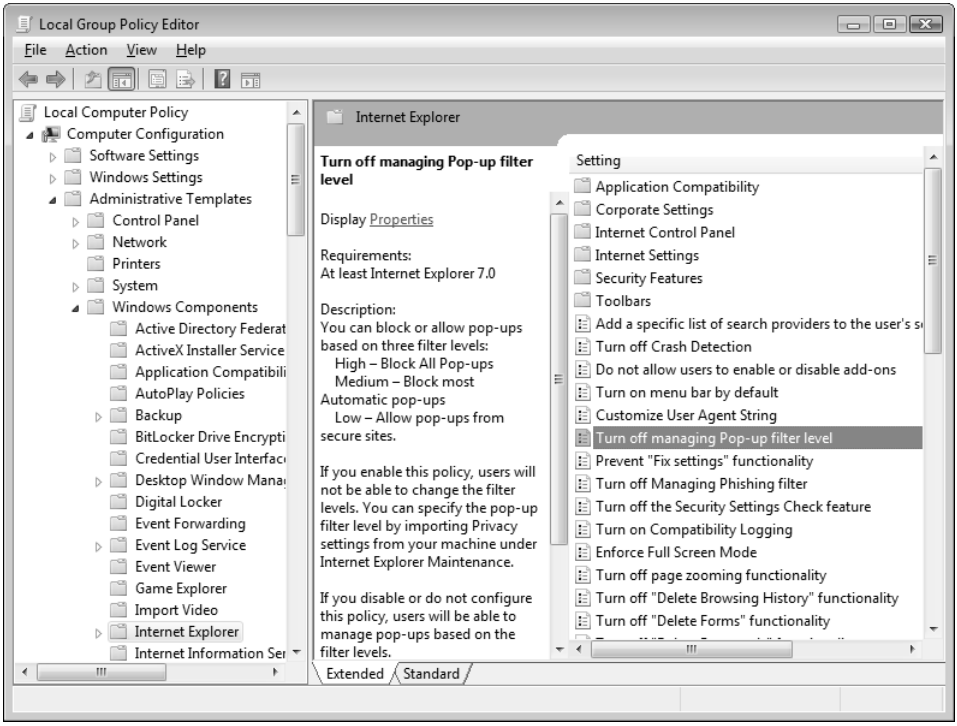


Рис. 13.2. Политики, управляющие работой браузера Internet Explorer

Среди самых важных операций, которые можно выполнять с помощью оснастки **Group Policy Management** (Управление групповой политикой), отметим следующие:

- создание, привязка (управление связями, links) и удаление GPO-объектов, а также выбор объекта для редактирования;
- просмотр значений параметров GPO-объектов;
- управление наследованием, блокировкой и запретом переопределения GPO-объектов;
- определение результирующей политики (RSoP-данных) в *режиме ведения журнала* (logging mode) и в *режиме планирования* (planning mode);
- документирование свойств GPO-объектов и значений заданных в них политик;
- создание архивных копий GPO-объектов, восстановление объектов из архивов, а также их копирование;

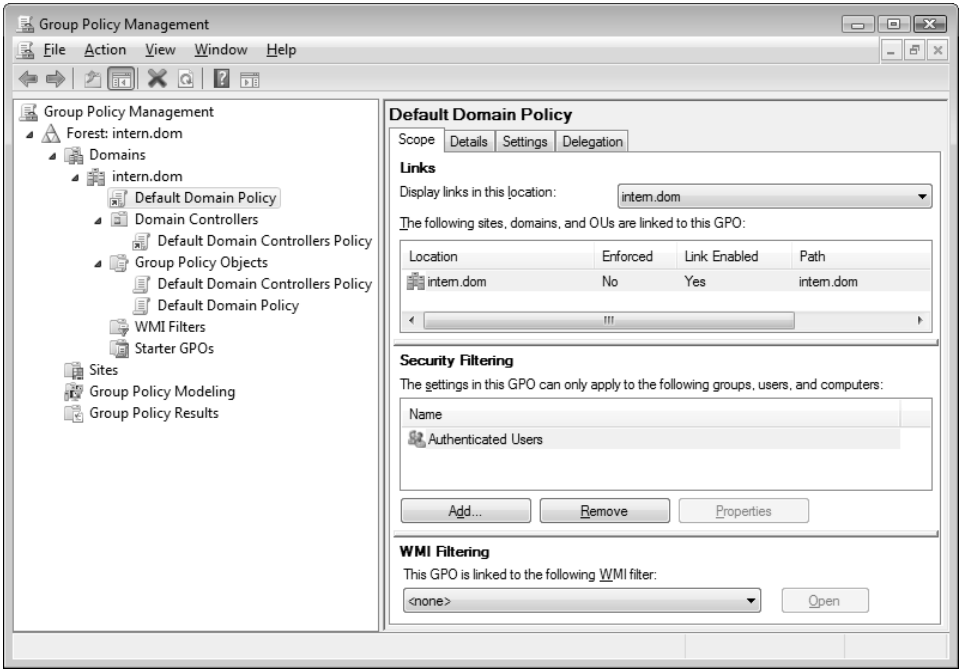


Рис. 13.3. Окно оснастки **Group Policy Management**

- импорт групповых политик в указанный GPO-объект;
- управление разрешениями на GPO-объекты и определение групп безопасности, к которым применяется GPO-объект (фильтрация групп);
- управление WMI-фильтрами;
- создание сценариев, позволяющих управлять GPO-объектами.

В системах Windows Server 2008 оснастка **Group Policy Management** (Управление групповой политикой) является *единственным* инструментом для манипулирования доменными объектами групповой политики (если не считать оснастки **Group Policy Object Editor** (Редактор объектов групповой политики), позволяющей редактировать параметры конкретного выбранного GPO-объекта). Отсутствует возможность, как в Windows Server 2003, работать с политиками в окне оснастки **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры) — вызывать редактор групповых политик, управлять блокировкой, наследованием и т. п. — теперь соответствующая вкладка в свойствах объектов доменов и подразделений отсутствует.

Оснастка **Group Policy Management** (Управление групповой политикой) может устанавливаться как компонент на любом сервере (для этого нужно воспользоваться оснасткой **Server Manager** (Диспетчер сервера) — *см. главу 3*); она запускается из меню **Administrative Tools** (Администрирование), а также появляется в списке компонентов в окне оснастки **Server Manager** (Диспетчер сервера). На контроллерах домена оснастка устанавливается автоматически, при повышении роли сервера.

В окне оснастки **Group Policy Management** (Управление групповой политикой) представлены все контейнеры (домены, подразделения, сайты), существующие в лесу доменов, и имеются следующие папки:

- **Domains** (Домены). Здесь содержатся имена всех доменов (видимостью которых можно управлять с помощью команды **Show Domains** (Показать домены)) и всех подразделений, входящих в домен (непосредственно в этой папке можно создавать и новые подразделения). (В качестве дочерних объектов каждое подразделение имеет список привязанных к нему GPO-объектов.) Кроме того, имеется папка **Group Policy Objects** (Объекты групповой политики), в которой перечислены *все* GPO-объекты, созданные в конкретном домене, а также папка **WMI Filters** (Фильтры WMI), где можно видеть описания всех имеющихся в домене фильтров;
- **Sites** (Сайты). Вполне очевидно, что здесь находится список сайтов и привязанных к ним GPO-объектов (если таковые имеются);
- **Group Policy Modeling** (Моделирование групповой политики). В эту папку помещаются все результаты запросов RSoP-данных, полученные в *режиме планирования* (planning mode);
- **Group Policy Results** (Результаты групповой политики). В эту папку помещаются результаты запросов RSoP-данных, полученные в *режиме ведения журнала* (logging mode).

Все команды, имеющиеся для некоторой выбранной папки или для GPO-объекта, можно видеть в контекстном меню или в меню **Action** (Действие).

Если выбрать некоторое подразделение, то в правой половине окна оснастки на вкладке **Linked Group Policy Objects** (Связанные объекты групповой политики) указаны GPO-объекты, *непосредственно* привязанные к этому подразделению, а на вкладке **Group Policy Inheritance** (Наследование групповой политики) хорошо видна *иерархия* GPO-объектов: т. е. список всех объектов, действие которых — согласно принципу наследования — распространяется на выбранное подразделение. GPO-объект с наименьшим номером будет са-

мым приоритетным (т. е. его параметры могут переопределить параметры политик, заданные во всех других GPO-объектах).

Начальные объекты групповой политики (Starter GPO)

Начальные, или стартовые, объекты групповой политики (Starter GPO) являются "шаблонами", которые можно использовать впоследствии при создании новых GPO-объектов. Они содержат только политики для компьютера и пользователей, входящие в состав узла **Administrative Templates** (Административные шаблоны) *(см. далее)*. Если в окне оснастки выбрать узел **Starter GPOs** (Начальные объекты групповой политики), то вначале содержимое узла отсутствует, и отображается кнопка **Create Starter GPOs Folder**, нажав которую, можно создать папку для хранения начальных GPO-объектов (рис. 13.4).

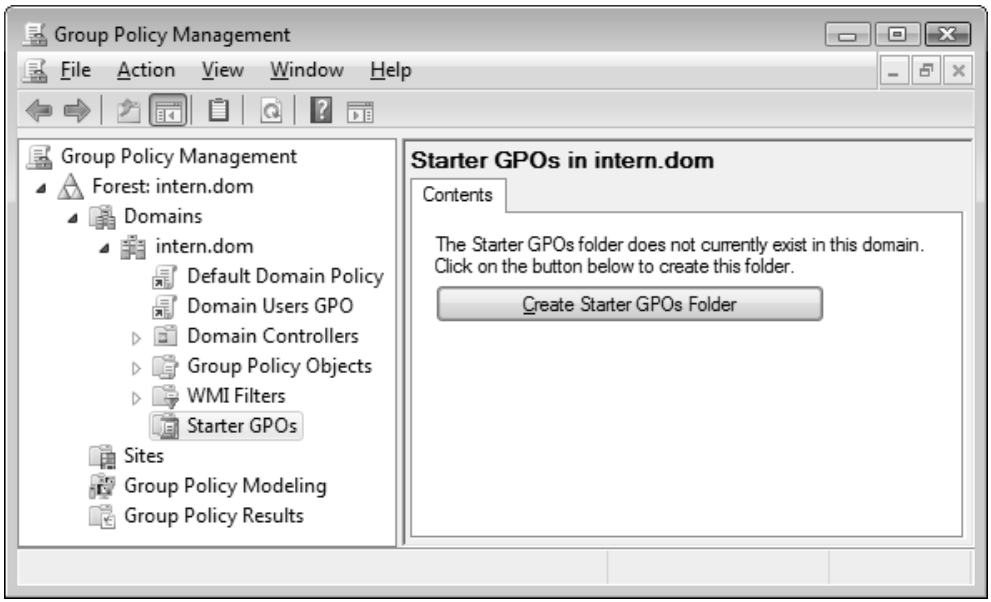


Рис. 13.4. Панель запуска операции по созданию начального GPO

Все операции по работе с начальными GPO-объектами — редактирование, архивация и восстановление — не отличаются от обычных манипуляций с

GPO-объектами (невозможна лишь привязка GPO-объекта к контейнерам каталога Active Directory). При создании нового GPO-объекта можно указать, какой начальный объект берется за основу (рис. 13.5) — все заданные в нем параметры сразу будут перенесены в новый GPO-объект.

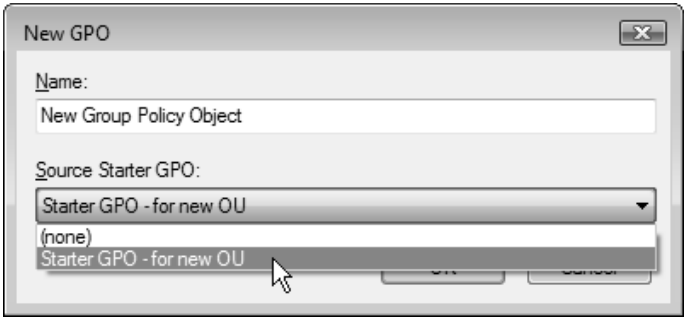


Рис. 13.5. Выбор начального GPO-объекта при создании нового объекта групповой политики

Предпочтения (Preferences)

В доменах Active Directory на базе серверов Windows Server 2008 имеются расширения обычных групповых политик, названные *предпочтениями* (preferences) (рис. 13.6). (Предпочтения имеются только в доменных GPO-объектах!) С помощью предпочтений можно конфигурировать рабочую среду клиентских компьютеров, причем имеются механизмы фильтрации, позволяющие точно указывать, на какие системы будут распространяться действия политик (в Windows Server 2003 аналогичные действия могут выполнять WMI-фильтры).

Предпочтения (а их около двух десятков — см. примеры на рис. 13.6) могут действовать по отношению к компьютерам и/или пользователям и распространяются на клиентские компьютеры, работающие под управлением систем Windows XP Service Pack 2, Windows Server 2003 Service Pack 1 и более поздних.

Примечание

Действия, выполняемые с помощью предпочтений, можно реализовать с помощью административных сценариев, подключаемых к GPO-объектам.

Однако предпочтения использовать намного удобнее, а также проще контролировать набор заданных действий.

Назначение и способы использования предпочтений проще всего понять на примерах. Рассмотрим два случая.

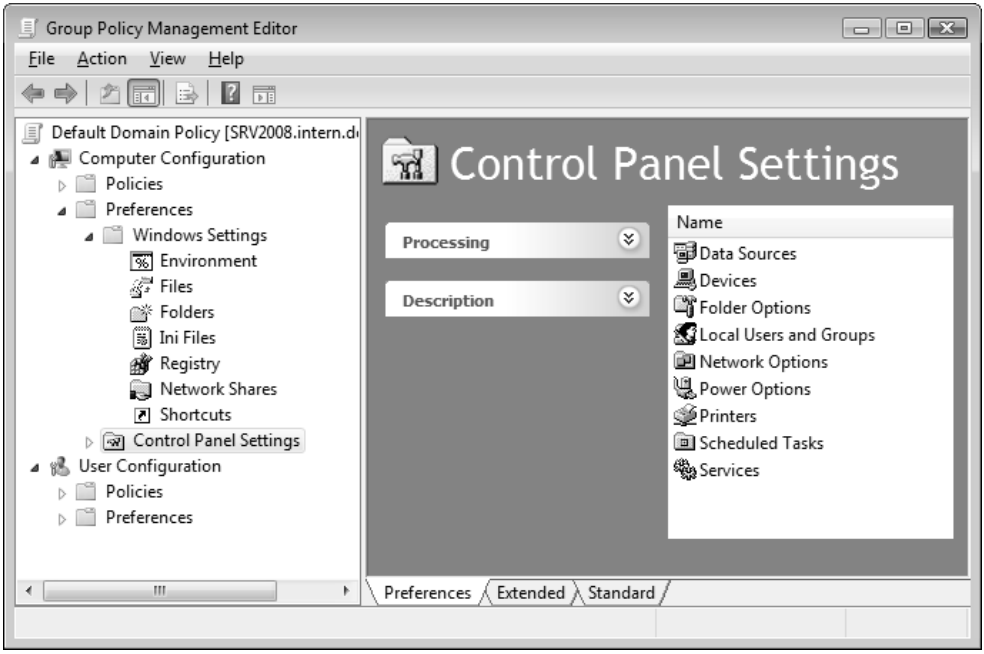


Рис. 13.6. Папки предпочтений в доменном GPO-объекте

Создание ярлыка для элемента оболочки

Мы хотим, чтобы у всех пользователей, подпадающих под действие некоторого доменного GPO-объекта (в нашем примере выбрана политика всего домена), на рабочем столе отображался ярлык для программы Windows Defender.

Для этого нужно выполнить следующие действия:

1. Открыть GPO-объект для редактирования.
2. В конфигурации пользователя открыть папку **Preferences** | **Windows Settings** | **Shortcuts** (Настройка | Конфигурация Windows | Ярлыки) (см. рис. 13.7).

3. В правом окне щелкнуть правой кнопкой мыши и выполнить команду **New** | **Shortcut** (Создать | Ярлык).
4. В окне параметров предпочтения задать нужные параметры (рис. 13.7). Как минимум, необходимо указать имя предпочтения (поле **Name**), тип объекта (раскрывающийся список **Target type**), местоположение ярлыка (список Location; в нашем примере выбран рабочий стол) и целевой объект (поле **Target object**; для выбора объекта[1] нужно нажать кнопку справа от поля). Также можно указать значок для ярлыка (поле **Icon file path**).

Рис. 13.7. Параметры предпочтения для отображения ярлыка на рабочем столе

На вкладке **Common** (Общие параметры) можно дать описание предпочтения, а также задать фильтр для выбора характеристик клиентских систем, на которые будет распространяться действие данного предпочтения — для этого нужно установить флажок **Item-level targeting** (Нацеливание на уровень элемента).

[1] Выбирать всегда можно только те объекты, которые имеются на компьютере, где запущена оснастка.

Теперь после применения политик у пользователей появится ярлык, и это будет происходить каждый раз при обновлении политик (даже если ярлык будет вручную удален с рабочего стола).

Создание локальной папки и контроль за ее содержимым

Необходимо, чтобы у пользователей на локальном диске C: присутствовала папка с именем DOCs. (Подвариант задачи: необходимо, чтобы в указанном каталоге — например, в папке для временных файлов — отсутствовали какие-либо файлы.)

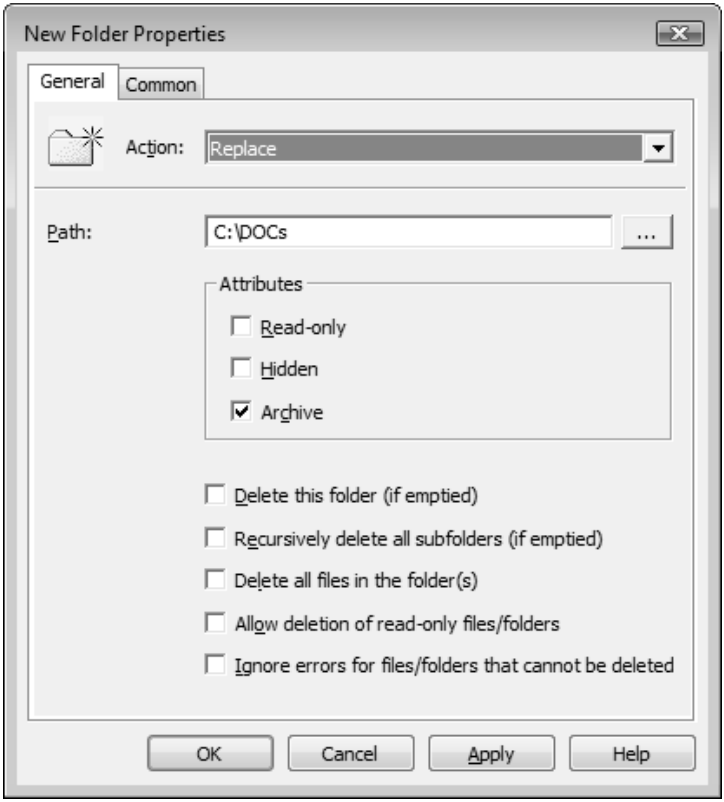


Рис. 13.8. Предпочтение для управления локальной папкой и ее содержимым

Эта задача решается с помощью предпочтений, создаваемых в папке **Folders** (Папки). Начальные шаги те же, что и в предыдущем разделе, мы рассмотрим только параметры предпочтения.

По умолчанию для предпочтения задается действие **Update** (Обновить). В этом случае папка будет создана, если она отсутствует. Если установить действие **Replace** (Заменить), то предпочтение будет применяться к имеющемуся объекту, и возможны дополнительные действия — в этом случае будут доступны флажки, расположенные в нижней половине окна свойств (рис. 13.8). С их помощью можно удалить саму папку, вложенные папки и файлы внутри папки (папок) (флажок **Delete all files in the folder (s)**). Задайте нужные действия и нажмите кнопку **OK**.

Теперь, после применения политик, у клиентов домена появится указанная папка.

Улучшения, касающиеся службы FRS и тома SYSVOL

На работе групповых политик сказываются улучшения, обусловленные возможностью использования службы DFS Replication[1] (Репликация DFS, сервис DFSR) для репликации тома SYSVOL и применение нового формата административных шаблонов (ADMX files). Это позволяет уменьшить трафик в сети, связанный с репликацией тома SYSVOL между контроллерами доменов, поскольку служба DFS Replication, выполняющая репликацию файлов по расписанию с учетом загрузки сети, использует новый алгоритм сжатия, известный как *Remote Differential Compression* (RDC). Он позволяет реплицировать между компьютерами только изменения данных, что значительно сокращает трафик. Данная возможность доступна только в доменах, имеющих функциональный уровень *Windows Server 2008*.

Поскольку, благодаря новому формату ADMX, каждый объект групповой политики, созданный в Windows Server 2008, не обязательно содержит в себе все файлы административных шаблонов (в отличие от предыдущих версий Windows), общий объем данных, хранящихся в томе SYSVOL, уменьшается, а, следовательно, становится более эффективной репликация.

---

[1] Эта служба обычно применяется для синхронизации папок DFS.

В составе Windows Server 2008 имеется специальное средство, позволяющее передать репликацию тома SYSVOL от традиционной службы File Replication Service (FRS; Служба репликации файлов) к службе DFS Replication.

Для серверов Windows Server 2008 результат выполнения утилиты Dcpromo, служащей для создания контроллера домена, зависит от функционального уровня домена:

- если домен имеет функциональный уровень *Windows Server 2008*, то для репликации тома SYSVOL сервер будет использовать службу DFS Replication;
- если домен имеет функциональный уровень *Windows Server 2003*, то для репликации тома SYSVOL будет использоваться служба FRS.

Хранение параметров групповых политик

Все параметры групповых политик, заданных для локальной системы или для компьютеров и пользователей домена, хранятся в структурах, называемых *объектами групповой политики* (group policy object, GPO).

Различают два вида объектов групповой политики — *локальные* объекты групповой политики (local GPO) и *хранимые в каталоге Active Directory* объекты групповой политики, которые используются контроллерами и членами домена (эти объекты GPO мы будем называть *доменными*).

Локальные объекты GPO

Локальный объект групповой политики (Local Group Policy Object, LGPO) имеется на каждом компьютере, работающем под управлением Windows, начиная с Windows 2000; этот объект создается в процессе установки операционной системы. Его параметры *всегда* влияют на локальную систему и каждого зарегистрированного пользователя, однако если компьютер подключается к домену, то сам компьютер и пользователь, работающий на нем, подпадают также под действие GPO-объектов, определенных в контексте данного домена. Поэтому параметры, заданные локальным объектом GPO, могут быть переопределены на более высоком уровне (на уровне сайта, домена или подразделения).

Локальный объект групповой политики представляет собой усеченный вариант шаблона групповых политик *(см. далее)* и располагается в скрытой папке

%SystemRoot%\System32\GroupPolicy (см. рис. 13.9). Администраторы и операционная система обладают полным доступом к этой папке. Пользователи имеют доступ только на чтение.

Внимание!

Значения некоторых групповых политик (например, политик безопасности — узел **Security Settings** (Параметры безопасности) в конфигурации компьютера или пользователя) хранятся не в шаблоне групповых политик, а непосредственно в реестре или в базе данных локальных политик безопасности *%SystemRoot%*\security\database\secedit.sdb. Эти значения задаются при установке операционной системы и изменяются сразу же при переопределении групповых политик в окне оснастки **Group Policy Object Editor**, запущенной для локального GPO. В доменных объектах GPO значения подобных групповых политик хранятся в файле GptTmpl.inf *(см. далее)*.

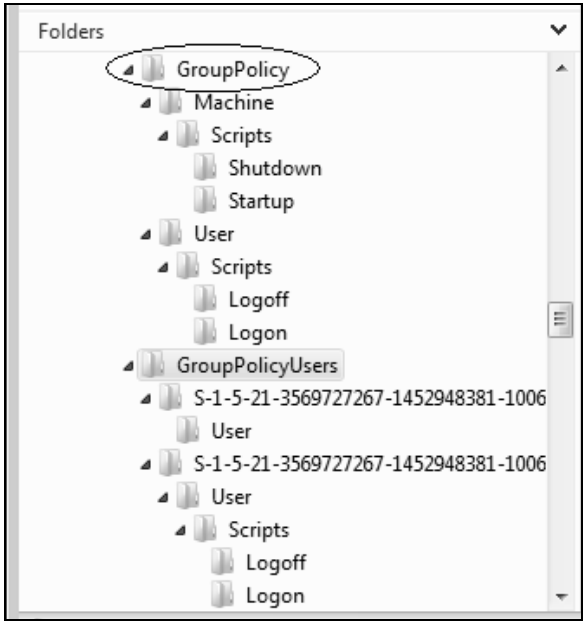


Рис. 13.9. Структура папок локальных объектов групповой политики в Windows Vista/Windows Server 2008

Для просмотра параметров безопасности (которые обрабатываются расширением **Security Settings**) может использоваться оснастка **Local Security Policy** (Secpol.msc). Для редактирования *всего* локального GPO нужно из

командной строки запустить оснастку **Group Policy Object Editor** (Редактор объектов групповой политики) (GPEdit.msc). Обе эти оснастки будут рассмотрены позже.

В системах Windows 2000/XP и Windows Server 2003 локальный GPO применяется ко ***всем*** локальным учетным записям пользователей, включая администратора. В системах Windows Vista/Windows Server 2008 реализована возможность назначения индивидуальных политик каждому пользователю или всем пользователям, не являющимся администраторами (или, наоборот, только администраторам). Локальный GPO, назначенный *конкретному* пользователю, хранится внутри папки *%SystemRoot%*\System32\GroupPolicyUsers — в папке, имя которой представляет собой идентификатор безопасности SID пользователя. Структура папок "общего" локального GPO и "индивидуальных" GPO (для двух пользователей, которым были назначены дополнительные политики) показана на рис. 13.9.

Доменные объекты GPO

Доменные объекты GPO хранят значения параметров групповых политик в двух структурах — *контейнере групповых политик* (Group Policy Container, GPC) и *шаблоне групповых политик* (Group Policy Template, GPT).

Контейнер групповых политик

Контейнер групповых политик представляет собой объект Active Directory, в котором хранятся следующие важные свойства GPO:

- номер версии, с помощью которого синхронизируются изменения в контейнере и в шаблоне;
- список расширений (их идентификаторы), хранящих свои настройки в объекте групповой политики;
- состояние GPO (разрешенные и запрещенные части);
- местоположение (имя шаблона групповых политик) в томе SYSVOL (например, \\intern.dom\sysvol\intern.dom\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}).

Пример отличительных имен контейнеров групповых политик — два стандартных объекта, создаваемых по умолчанию в любом домене Active Directory (их GUID-идентификаторы неизменны): объект *Default Domain Policy* с именем

CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System, DC=<*имяДомена*> и объект *Default Domain Controllers Policy* с именем CN={6AC1786C-016F-11D2-945F-00C04fB984F9},CN=Policies,CN=System, DC=<*имяДомена*> (рис. 13.10).

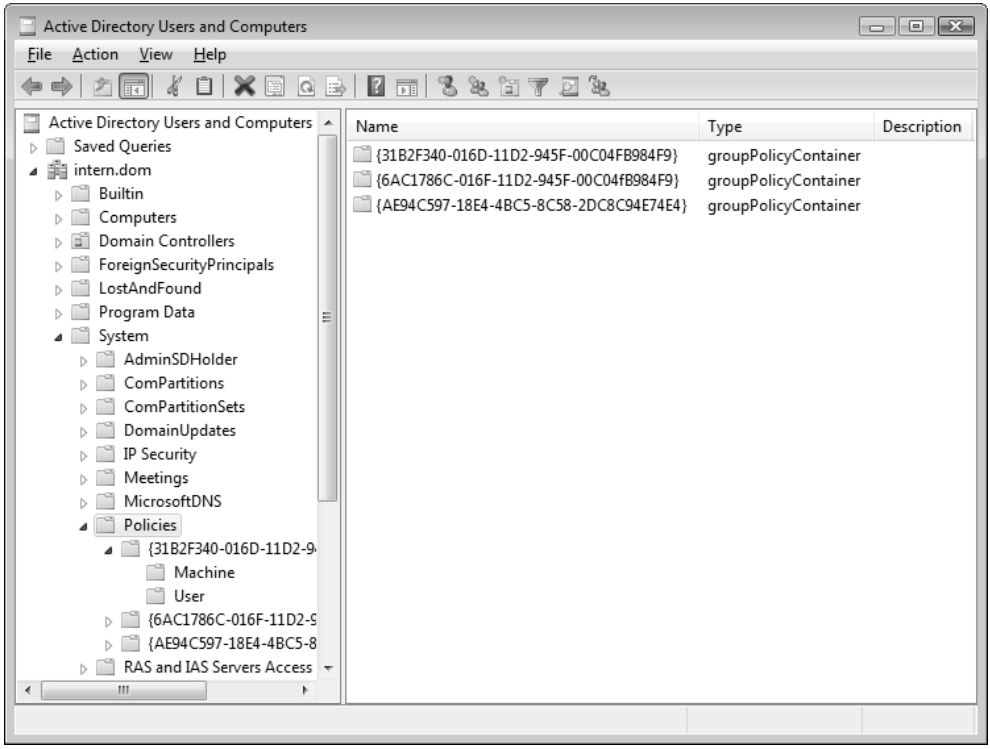


Рис. 13.10. Хранение контейнеров групповых политик в каталоге Active Directory

Шаблон групповых политик

Шаблон групповых политик — это структура подкаталогов и файлов на жестком диске, где, собственно, и хранятся значения объектов групповых политик. Папки шаблонов доменных групповых политик находятся на системном томе (SYSVOL) контроллеров доменов в папке **Policies**. Имя папки шаблона объекта GPO выступает в качестве *глобального уникального идентификатора* (Global Unique Identifier, GUID), однозначно характеризующего данный объект групповой политики (рис. 13.11).

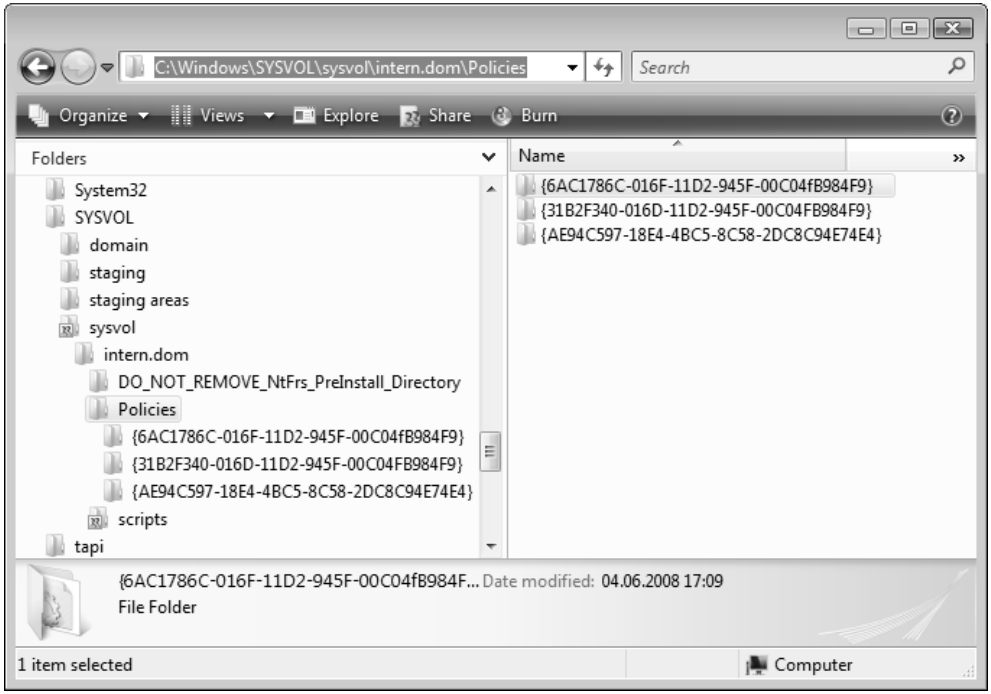


Рис. 13.11. Хранение шаблонов групповых политик на томе SYSVOL

Подкаталоги шаблона групповых политик

Ниже перечислены подкаталоги, содержащиеся по умолчанию внутри папки шаблона групповых политик (рис. 13.12). В локальных GPO некоторые из указанных папок отсутствуют.

- **Machine**. Здесь хранится имеющий специальный формат файл Registry.pol со значениями параметров реестра, устанавливаемых для *компьютера* с помощью расширения Administrative Templates. При загрузке операционной системы файл Registry.pol анализируется, и его данные записываются в реестр в раздел `HKEY_LOCAL_MACHINE`. Подкаталог **Scripts** содержит папки **Shutdown** и **Startup** для хранения сценариев выключения и запуска системы (соответственно). В папке **Microsoft\Windows NT\SecEdit** находится файл GptTmpl.inf, где хранятся параметры безопасности для компьютеров, на которые распространяется область действия доменного объекта GPO. Содержимое папки **Applications** зависит от того, какие приложения назначены компьютеру с помощью данного объекта GPO.

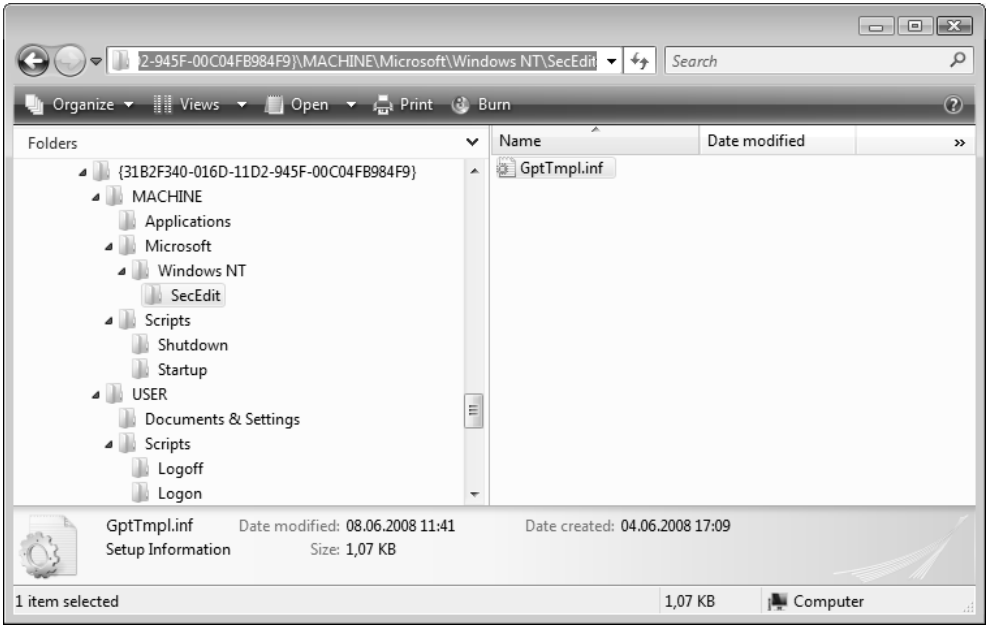


Рис. 13.12. Структура шаблона групповой политики

Примечание

В составе пакета Windows Resource Kit имеется утилита *Regview.exe*, с помощью которой легко увидеть параметры, хранящиеся в файле Registry.pol. Например, для просмотра машинных параметров в локальном GPO-объекте используется следующая команда:

```
regview Windows\System32\GroupPolicy\machine\Registry.pol
```

- **User**. Здесь хранится файл Registry.pol со значениями параметров реестра, устанавливаемых для *пользователей* с помощью расширения Administrative Templates. Когда пользователь регистрируется в системе, файл Registry.pol анализируется, и его данные записываются в реестр в раздел `HKEY_CURRENT_USER`. Папка **User** содержит подкаталог **Scripts**, где по умолчанию находятся все сценарии и связанные с ними файлы, а также подкаталоги **Logoff** и **Logon** (для сценариев выхода из системы и регистрации в системе). При использовании перенаправления папок (Folder Redirection) подкаталог **Documents & Settings** содержит файл Fdeploy.ini, в котором хранится информация о состоянии специальных пользовательских папок.

Папки **Machine** и **User** появляются сразу же при создании объекта GPO. Другие подкаталоги создаются при определении соответствующих политик.

> ***Внимание!***
>
> В системах Windows Vista/Windows Server 2008 административные шаблоны, определяющие регистровые политики, ***не входят*** в состав GPO-объектов. Поэтому в этих системах в шаблоне групповых политик отсутствует папка **Adm**, где в предыдущих версиях Windows хранятся все файлы *.adm, подключенные к некоторому объекту GPO.

Файл Gpt.ini

Непосредственно в корне папки шаблона групповых политик находится файл *Gpt.ini*. Для локального объекта GPO этот файл содержит следующую информацию:

- номер версии объекта GPO;
- список идентификаторов (GUID) клиентских расширений оснастки **Group Policy Object Editor** (Редактор объектов групповой политики);
- состояние объекта GPO (какие его части разрешены или запрещены).

Для доменных GPO-объектов файл Gpt.ini хранит:

- номер версии объекта;
- отображаемое имя объекта GPO (если он не относится к стандартным).

Средства редактирования групповых политик

Для настройки параметров безопасности в Windows Server 2008 используются две[1] основные оснастки:

- **Group Policy Object Editor** (Редактор объектов групповой политики). При работе в доменах эта оснастка вызывается при необходимости из ос-

[1] В доменах оснастка **Group Policy Object Editor** (Редактор объектов групповой политики) может использоваться для редактирования различных доменных GPO-объектов и фигурировать под разными именами, однако по сути это одна и та же программа.

настки **Group Policy Management** (Управление групповой политикой) для выбранного объекта групповых политик *(см. далее)*;

- **Local Security Settings** (Локальная политика безопасности).

Эти оснастки служат для просмотра и редактирования так называемых *объектов групповой политики*, или GPO-объектов (Group Policy Object, GPO).

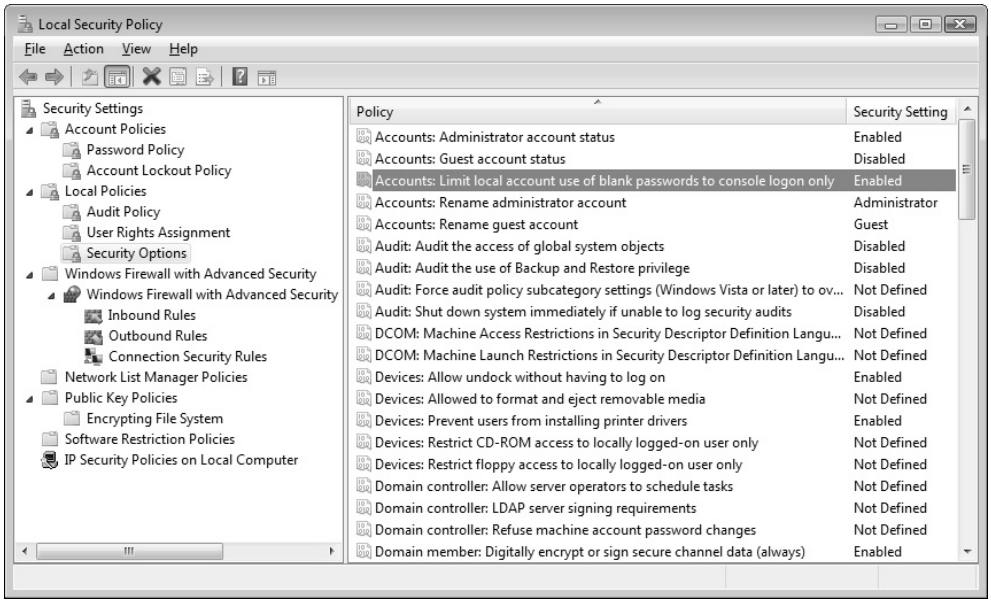


Рис. 13.13. Окно оснастки **Local Security Settings**

Примечание

Оснастка **Local Security Settings** (Локальная политика безопасности, secpol.msc) (рис. 13.13[1]) входит как расширение в состав оснастки **Group Policy Object Editor** (Редактор объектов групповой политики), но ее можно использовать и автономно, вызывая из меню **Administration Tools (**Администрирование) (в системах Windows Server 2008 *нельзя* подключать ее к пользовательским консолям MMC). Эта оснастка обеспечивает доступ только к ограниченному подмножеству параметров групповой политики, располо-

[1] Обратите внимание на политику, выбранную для примера в окне оснастки: по умолчанию для удаленного доступа к компьютеру нельзя использовать учетные записи, не имеющие пароля.

женных в контейнере **Security Settings** (Параметры безопасности) локального объекта групповой политики. Данную оснастку мы не будем описывать отдельно, поскольку оснастка **Group Policy Object Editor** (Редактор объектов групповой политики) перекрывает все ее возможности.

Оснастка *Group Policy Object Editor*

Оснастку **Group Policy Object Editor** (Редактор объектов групповой политики) можно запускать как для локального компьютера, так и для удаленного:

- для локального нужно в окне командной строки или в окне **Start** | **Run** (Пуск | Выполнить) ввести `gpedit.msc`;
- для удаленного компьютера необходимо открыть пустую консоль MMC и при добавлении в нее оснастки выбрать удаленный компьютер.

Также она используется для редактирования всех доменных GPO-объектов, привязанных или непривязанных к контейнерам домена (домену, подразделениям и сайтам).

В любом случае нельзя *динамически* "переключать" оснастку на другой компьютер после ее запуска (это можно делать только из командной строки, если при запуске указывать конкретный объект GPO).

При добавлении редактора политик к консоли MMC могут присутствовать дополнительные варианты использования стандартной оснастки (рис. 13.14). Оснастка **Group Policy Management Edition** (Редактор управления групповыми политиками) служит для редактирования GPO-объектов, хранящихся в домене; при подключении этой оснастки можно выбрать конкретный GPO-объект в структуре леса доменов (рис. 13.15). Оснастка **Group Policy Starter GPO Editor** (Редактор GPO инициирующей программы групповой политики) используется только вместе с начальными GPO-объектами, если таковые имеются в домене.

Поскольку в системах Windows Vista/Windows Server 2008 параметры групповых политик можно назначать отдельному локальному пользователю, при подключении оснастки **Group Policy Object Editor** (Редактор объектов групповой политики) к консоли MMC после выбора компьютера можно нажать кнопку **Browse** (Обзор) и в открывшемся окне на вкладке **Users** (Пользователи) указать пользователя, к которому будет применяться данный объект GPO (рис. 13.16). Настройка параметров любых объектов политик осуществляется одинаково.

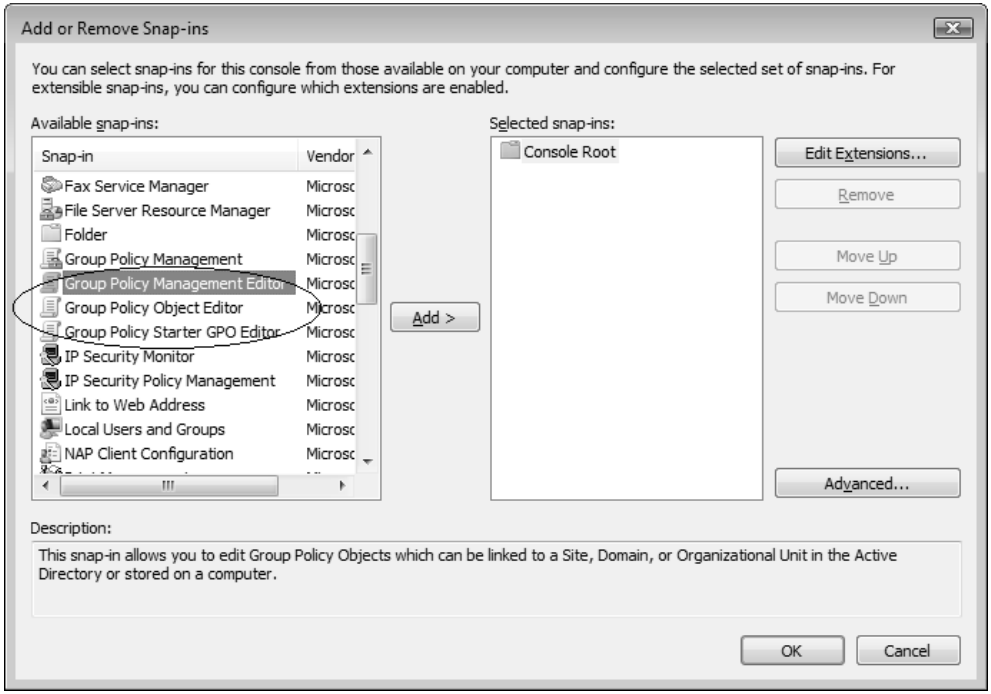


Рис. 13.14. Выбор редактора групповых политик

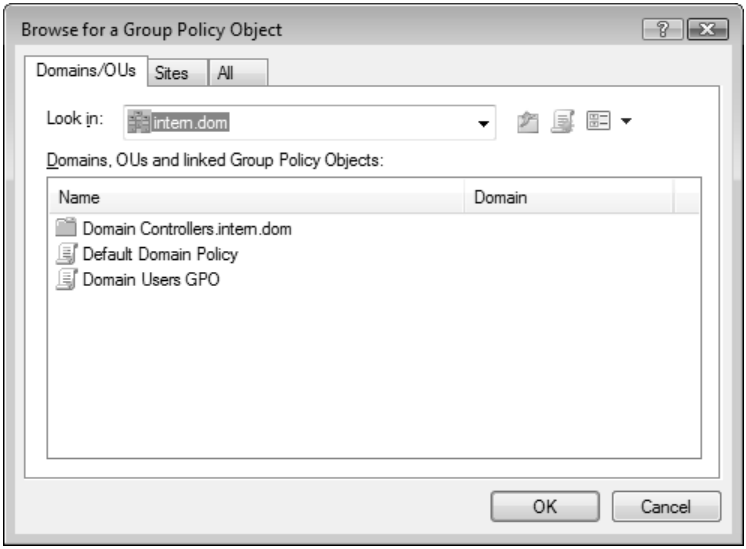


Рис. 13.15. Выбор доменного GPO-объекта при подключении оснастки

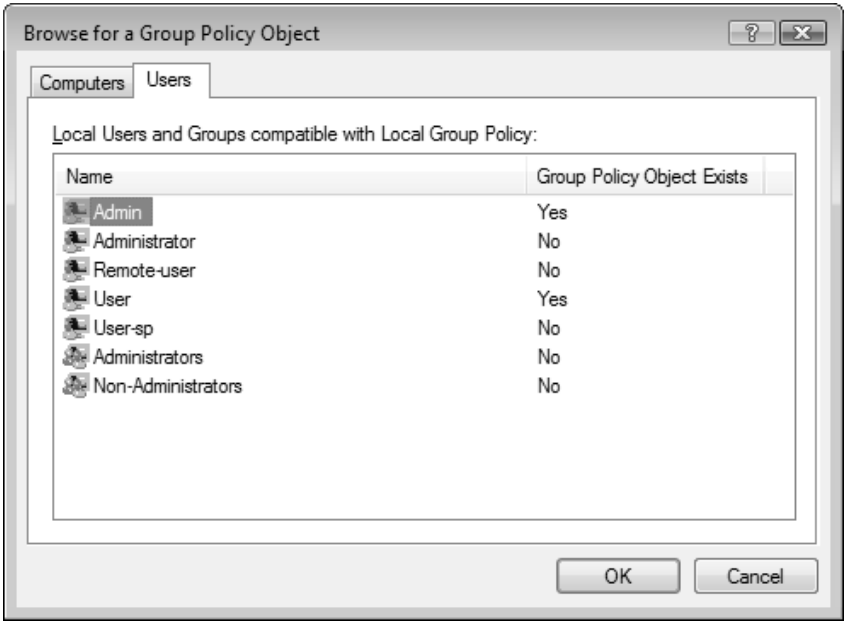


Рис. 13.16. Выбор пользователя, на которого будут распространяться параметры объекта GPO

Как можно видеть на рис. 13.16, политики локального объекта GPO могут также создаваться индивидуально для двух локальных *групп*: стандартной локальной группы Administrators (Администраторы) и служебной группы, которая определяет всех остальных пользователей, не относящихся к администраторам (Non-Administrators).

Представление структуры GPO-объекта в окне оснастки

Оснастка **Group Policy Object Editor** (Редактор объектов групповой политики) позволяет конфигурировать параметры групповой политики, касающиеся как компьютера, так и пользователя. В панели пространства имен оснастки соответствующие группы параметров представлены контейнерами **Computer Configuration** (Конфигурация компьютера) и **User Configuration** (Конфигурация пользователя) (рис. 13.17).

- Узел **Computer Configuration** (Конфигурация компьютера) содержит параметры всех политик, определяющих работу *компьютера*. Эти поли-

тики регулируют функционирование операционной системы, определяют права пользователей в системе, работу системных служб и средств безопасности и т. д. Групповая политика, заданная внутри этого узла, применяется к компьютеру на этапе загрузки системы и в дальнейшем — при выполнении циклов обновления.

- Узел **User Configuration** (Конфигурация пользователя) содержит параметры всех политик, определяющих работу *пользователей* (или отдельного пользователя). Данные политики регулируют вид рабочего стола и конфигурацию рабочей среды, управляют пользовательскими сценариями входа и выхода и т. д.; они применяются к пользователю при его входе в систему и в дальнейшем — при выполнении циклов обновления.

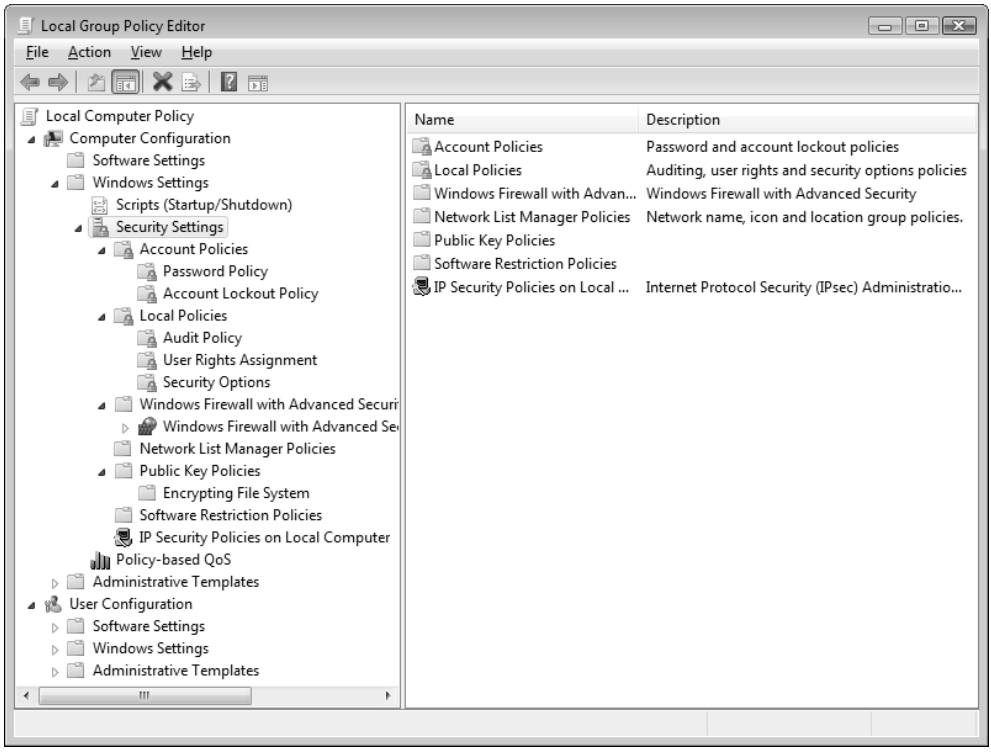


Рис. 13.17. Развернутое дерево объектов оснастки **Group Policy Object Editor**, в котором можно видеть основные ее расширения для локального объекта GPO

Расширения оснастки *Group Policy Object Editor*

В состав родительских узлов **Computer Configuration** (Конфигурация компьютера) и **User Configuration** (Конфигурация пользователя) входят дочерние узлы, каждый из которых является полноценным расширением оснастки **Group Policy Object Editor** (Редактор объектов групповой политики). Эти узлы могут присутствовать в обоих родительских узлах (как, например, **Scripts** (Сценарии) или **Security Settings** (Параметры безопасности)) — хотя и с различными политиками — или в одном из них. Имеются следующие расширения:

- *Software Installation* (Установка программ) и *Remote Installation Services* (Службы удаленной установки). Служат для централизованного управления программным обеспечением корпоративной сети. С их помощью можно задавать различные режимы установки новых программ для компьютеров и/или для пользователей;
- *Scripts* (Сценарии). Сценарии используются для автоматического выполнения набора команд при загрузке операционной системы и в процессе завершения ее работы, а также при регистрации и отключении пользователя от сети. Для выполнения сценариев, написанных на JScript и Visual Basic Scripting Edition, можно применять сервер сценариев (Windows Scripting Host);
- *Deployed Printers* (Развернутые принтеры) (другое название — *Pushed Printer Connection Extension* (Расширение перемещенных подключений принтеров)). Новое расширение, позволяющее управлять назначением принтеров, подключаемых в зависимости от местоположения компьютера в сети. Появляется, если на компьютере и в сети имеется роль сервера печати;
- *Security Settings* (Параметры безопасности). Служит для настройки параметров системы безопасности компьютеров: политик аудита и блокировки учетных записей, права пользователей и т. п. *(см. далее)*;
- *Folder Redirection Editor** (Редактор перенаправления папок). Позволяет перенаправлять обращение к пользовательским папкам (**Documents** (Документы), **Pictures** (Изображения) и т. д.) на сетевой ресурс;
- *Policy-based QoS* (QoS на основе политики). Новое расширение, позволяющее управлять работой службы управления качеством (Quality of Service);

- *Internet Explorer Maintenance* (Настройка Internet Explorer). Политики, управляющие работой и конфигурацией браузера Internet Explorer;
- *Administrative Templates* (Административные шаблоны). Здесь находятся групповые политики, управляющие параметрами реестра, которые определяют поведение и внешний вид рабочего стола и других элементов пользовательского интерфейса, управляют работой компонентов операционной системы и приложений. Файлы административных шаблонов (*.amdx) в Windows Vista/Windows Server 2008 хранятся в папке *%SystemRoot%*\PolicyDefinitions.

Параметры безопасности (Security Settings)

Рассмотрим подробнее расширение Security Settings (Параметры безопасности), с помощью которого задаются параметры системы безопасности систем Windows. Политики, определяемые этим расширением, действуют на компьютеры и частично на пользователей. В системах Windows Vista/Windows Server 2008 в составе этого расширения появились новые политики. Перечислим группы политик, отвечающих за безопасность, и укажем области их применения (звездочкой отмечены политики, использующиеся только в доменных объектах GPO и отсутствующие в локальных GPO).

- *Account Policies* (Политики учетных записей). Настройка политик безопасности учетных записей в масштабах домена или локальных учетных записей. Здесь определяются политика паролей, политика блокировки паролей и политика Kerberos, распространяющаяся на весь домен.
- *Local Policies* (Локальные политики). Настройка политики аудита, назначение прав пользователей и определение различных параметров безопасности.
- *Event Log** (Журнал событий). Настройка политик безопасности, определяющих работу журналов событий приложений, системы и безопасности.
- *Restricted Groups** (Группы с ограниченным доступом). Управление членством пользователей в заданных группах. Сюда обычно включают встроенные группы, такие как Administrators (Администраторы), Backup Operators (Операторы архива) и другие, имеющие по умолчанию права администратора. В эту категорию могут быть включены и иные группы, безопасность которых требует особого внимания и членство в которых должно регулироваться на уровне политики.
- *System Services** (Системные службы). Настройка безопасности и параметров загрузки для работающих на компьютере служб.

- *Registry** (Реестр). Настройка прав доступа к различным разделам реестра.
- *File System** (Файловая система). Настройка прав доступа к определенным файлам.
- *Wired Network (IEEE 802.3) Policies** (Политики проводной сети (IEEE 802.3[1])). Настройка параметров клиентов, подключающихся к проводным сетям, принадлежащим разным доменам.
- *Windows Firewall with Advanced Security* (Брандмауэр Windows в режиме повышенной безопасности). Настройка правил и других параметров встроенного брандмауэра Windows (Windows Firewall).
- *Network List Manager Policies* (Политики диспетчера списка сетей). Настройка сетевых параметров компьютера и определение возможностей пользователей для разных категорий сети (сетевого размещения) *(см. главу 8)*.
- *Wireless Network (IEEE 802.11) Policies** (Политики беспроводной сети (IEEE 802.11)). Централизованная настройка параметров (включая методы проверки подлинности) клиентов беспроводной сети в доменах Active Directory.
- *Public Key Policies* (Политики открытого ключа). Настройка политик безопасности в отношении шифрования информации с помощью EFS, авторизации корневого сертификата в масштабах домена, авторизации доверенного сертификата и т. д. Политика EFS существует и для локального GPO, остальные политики применяются только в доменах.
- *Software Restriction Policies* (Политики ограниченного использования программ). Политики, указывающие на то, какие приложения могут, а какие программы не могут выполняться на локальном компьютере.
- *Network Access Protection**. Настройка политик, определяющих требования к клиенту, подключающемуся к сети, и предоставляющих полный или ограниченный доступ к сети в зависимости от того, насколько клиент соответствует этим требованиям[2]. В процессе проверки могут анализироваться различные аспекты безопасности: наличие обновлений программных средств и антивирусной защиты, параметры конфигурации и брандмауэра, список открытых и закрытых портов TCP/IP и т. д.

---

[1] Стандарт IEEE 802.3 описывает проводные сети Ethernet.

[2] Компонент NAP Client for Windows XP включен в пакет обновлений Windows XP Service Pack 3.

- *IP Security Policies* (Политики IP-безопасности). Настройка политик безопасности IP для компьютеров, находящихся в определенной области действия.

Дополнительные инструменты настройки безопасности

В составе Windows Server 2008 имеется целый набор административных средств, позволяющих анализировать текущие параметры безопасности системы, создавать шаблоны с заданными параметрами и применять их на рабочих системах.

К средствам настройки безопасности относятся следующие компоненты:

- *оснастка* ***Security Templates*** (Шаблоны безопасности) — этот инструмент позволяет создавать описания (шаблоны) различных конфигураций безопасности, которые хранятся в виде текстовых файлов. Данные конфигурации могут соответствовать разным задачам или уровням требований к безопасности систем. Затем эти конфигурации можно импортировать в расширение Security Settings (Параметры безопасности) оснастки **Group Policy Object Editor** (Редактор объектов групповой политики) и использовать на конкретных компьютерах;
- *оснастка* ***Security Configuration and Analisys*** (Анализ и настройка безопасности) — данный инструмент позволяет импортировать один или несколько шаблонов в базу данных безопасности (это может быть база данных локальной политики компьютера или любая другая личная база). В результате создается специфическая для конкретного компьютера база данных безопасности, которая хранит композитную настройку. Затем ее можно активизировать на компьютере и проанализировать состояние текущей конфигурации безопасности по отношению к композитной настройке. Такая операция позволяет сравнивать различные конфигурации параметров и проверять их действие на практике, после чего проверенную конфигурацию можно экспортировать в новый шаблон и распространять на другие компьютеры;
- *Secedit.exe* — утилита командной строки, позволяющая автоматизировать задачи настройки безопасности (анализировать текущие значения, конфигурировать их и экспортировать в шаблоны безопасности);

- *мастер Security Configuration Wizard* (Мастер настройки безопасности) — программа-мастер, позволяющая настроить конфигурацию параметров безопасности на "эталонном" компьютере и применять ее на других компьютерах.

Определение действующих политик

При работе с групповыми политиками часто используются две утилиты командной строки, которые в первую очередь полезны в доменах, особенно при большом количестве GPO-объектов:

- *GPUpdate.exe* — утилита позволяет принудительно обновить параметры политик, задаваемых объектами GPO, на локальном или удаленном компьютере. Это бывает необходимо после изменения групповых политик, когда нужно, чтобы они немедленно стали активными (возможна также принудительная перезагрузка системы). Политики можно обновлять все вместе или для пользователя и компьютера по отдельности (для просмотра списка параметров можно утилиту запустить с ключом `/?`);
- *GPResult.exe* — эта утилита позволяет определить, какие настройки групповых политик фактически применяются по отношению к указанному компьютеру и/или пользователю. Может выполняться и для удаленного компьютера. Запускать команду лучше всего с ключом `/v` — в этом случае сразу становятся видны ее возможности. Аналогичную задачу выполняет описываемая ниже оснастка **Resultant set of Policy** (Результирующая политика).

Оснастка *Resultant Set of Policy*

В составе систем Windows Server 2008 уже традиционно имеется удобный инструмент для работы с групповыми политиками, который особенно полезен в крупных доменах с многоуровневой иерархией GPO-объектов, — это оснастка **Resultant Set of Policy** (Результирующая политика). Но даже и на отдельном компьютере с его помощью можно быстро увидеть, какие групповые политики назначены конкретному пользователю, не перебирая все узлы структуры локального объекта GPO.

Примечание

В доменах удобнее использовать новую оснастку **Group Policy Management** (Управление групповой политикой), которая имеет множество возможностей по манипулированию объектами GPO. Эта оснастка также позволяет запрашивать RSoP-данные *(см. далее)*.

В простейшем случае оснастка **Resultant Set of Policy** (Результирующая политика) просто регистрирует все применяемые политики и показывает, какой GPO-объект "отвечает" за конкретные политики.

Продемонстрируем это на примере.

1. Откройте пустую консоль MMC и добавьте в нее оснастку **Resultant Set of Policy** (Результирующая политика). (В *главе 3* работа с консолями MMC обсуждалась подробно.)

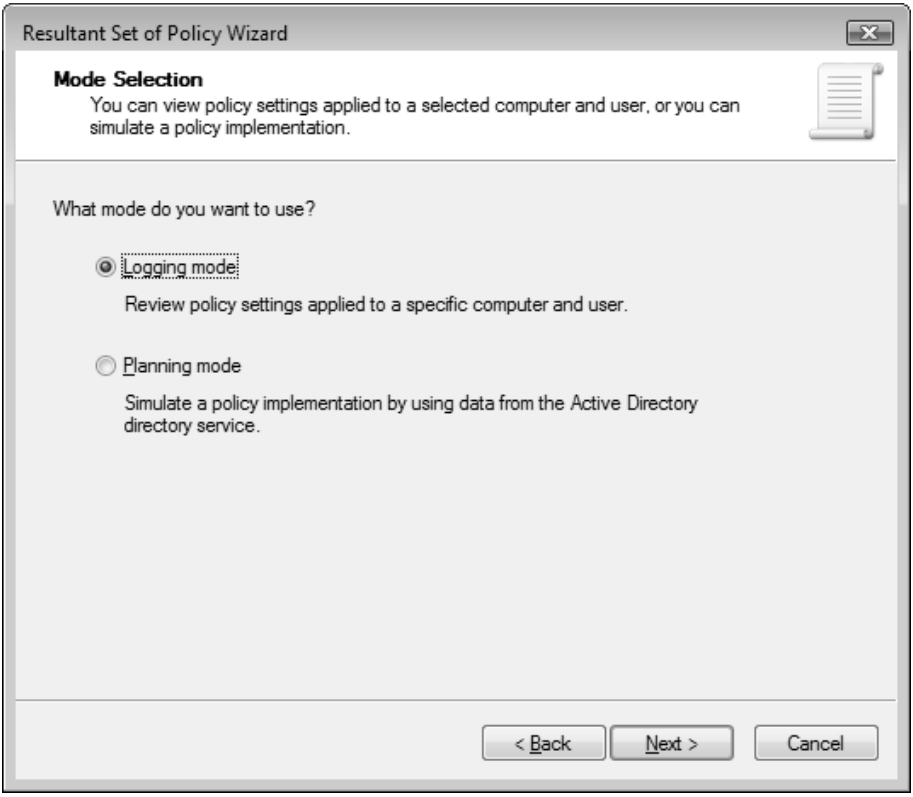


Рис. 13.18. Выбор режима сбора RSoP-данных

2. На левой панели окна оснастки выберите корневой узел с именем оснастки и в контекстном меню или в меню **Action** (Действие) выполните команду **Generate RSoP Data** (Создать данные RSoP). Запустится мастер *Resultant Set of Policy Wizard* (Мастер результирующей политики).

3. Для автономного компьютера доступен только *режим ведения журнала* (режим входа, logging mode), для компьютеров — членов домена имеется также *режим планирования* (planning mode) (рис. 13.18). В режиме входа можно получить данные только для пользователей, ***уже регистрировавшихся хотя бы раз на выбранном компьютере***; в режиме планирования работа групповых политик эмулируется на основе данных, получаемых от службы каталога Active Directory. Выберите нужный режим.

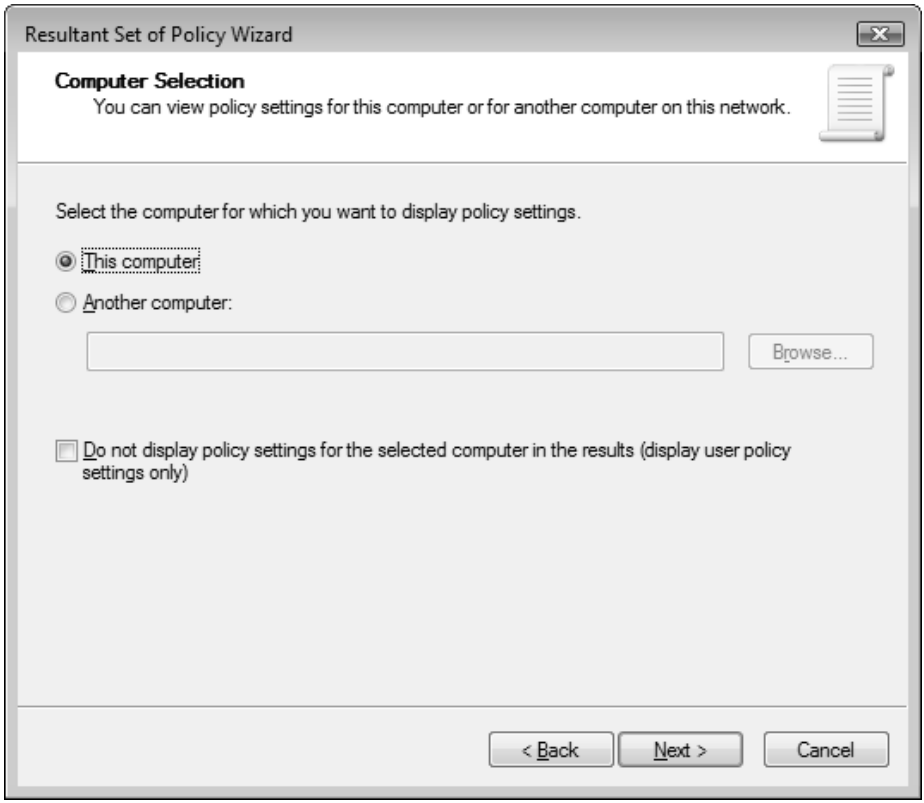


Рис. 13.19. Выбор компьютера,
для которого генерируются RDoP-данные

4. Укажите компьютер, для которого проверяются параметры групповых политик (рис. 13.19). Если политики компьютера не представляют интереса и их не нужно генерировать, то можно для ускорения работы установить флажок **Do not display policy settings for the selected computer in the results**.
5. Выберите пользователя, для которого проверяются установки групповых политик (рис. 13.20). В этом окне видны все учетные записи пользователей, регистрировавшихся на компьютере и, следовательно, имеющих на нем RSoP-данные. Если же требуются только значения параметров для компьютера и пользовательские данные получать не нужно, то выберите переключатель **Do not display user policy settings in the results**.

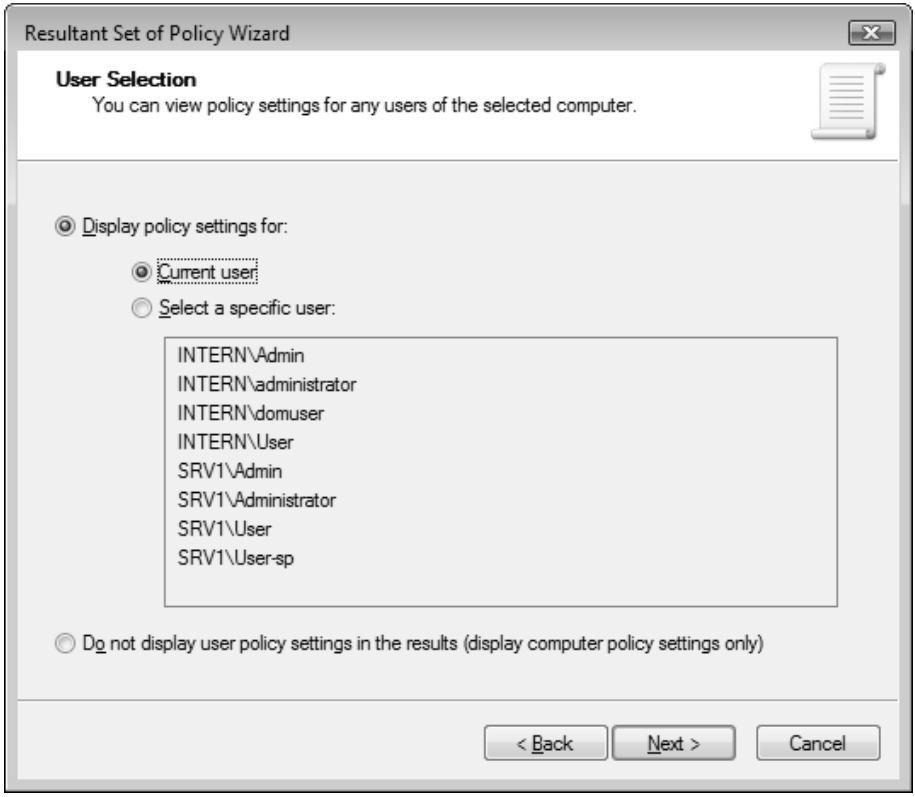


Рис. 13.20. Выбор учетной записи пользователя, для которого будут определяться значения групповых политик

6. Когда все параметры запроса выбраны, на странице сводки нажмите кнопку **Next** (Далее). Система некоторое время будет анализировать параметры политик, после чего процесс добавления оснастки к консоли MMC будет завершен — можно анализировать результаты.

В окне (рис. 13.21), напоминающем окно оснастки **Group Policy Object Editor** (Редактор объектов групповой политики), будут отображаться только те папки (ниже второго уровня), в которых имеются измененные политики. Например, в нашем примере показано, что для выбранного пользователя установлены три политики, влияющие на внешний вид меню **Start** (Пуск). Две политики определены в специально созданном объекте GPO, действие которого распространяется на обычных пользователей домена, а одна задается стандартной политикой домена (Default Domain Policy). Соответствующие имена GPO-объектов можно видеть в столбце **GPO Name** (Имя GPO).

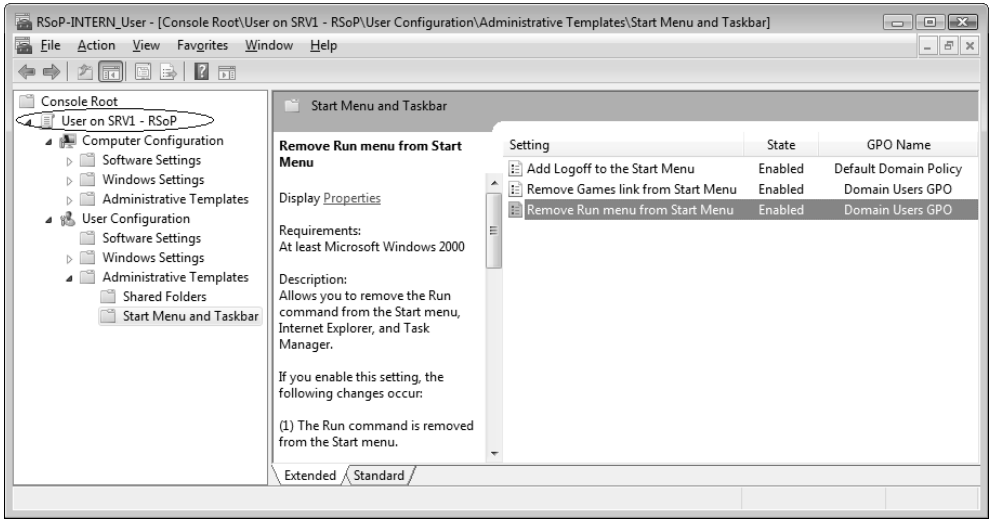


Рис. 13.21. Оснастка **Resultant Set of Policy** позволяет быстро определить, какие политики установлены для компьютера или пользователя

Полученные сведения можно проверить с помощью утилиты GRResult и сравнить результаты. Подобная информация очень полезна в сложных ситуациях, когда компьютер подключен к домену и имеется множество наследуемых групповых политик, заданных разными объектами GPO.

Обновить результаты для уже сконфигурированной оснастки можно при помощи команды **Refresh Query** (Обновление запросов), которая имеется в контекстном меню папки *<имяПользователя><имяКомпьютера> - RSoP* (см. рис. 13.21). Эта команда также имеется в меню **Action** (Действие). Команда **Change Query** (Изменить запрос) позволяет модифицировать текущие параметры консоли (после этого запрос можно повторить с новыми параметрами).

Созданную консоль MMC можно сохранить; при повторных запусках оснастка каждый раз будет обновлять все значения и выведет актуальные данные. В процессе сбора информации отображается окно (рис. 13.22), в котором можно следить за ходом операции. (Такое же окно появляется и при первом добавлении оснастки к консоли MMC.) ***Обратите внимание*** на сообщение в этом окне: для систем, начиная с Windows Vista SP1, для получения параметров *всех* групповых политик необходимо использовать утилиту GPResult.

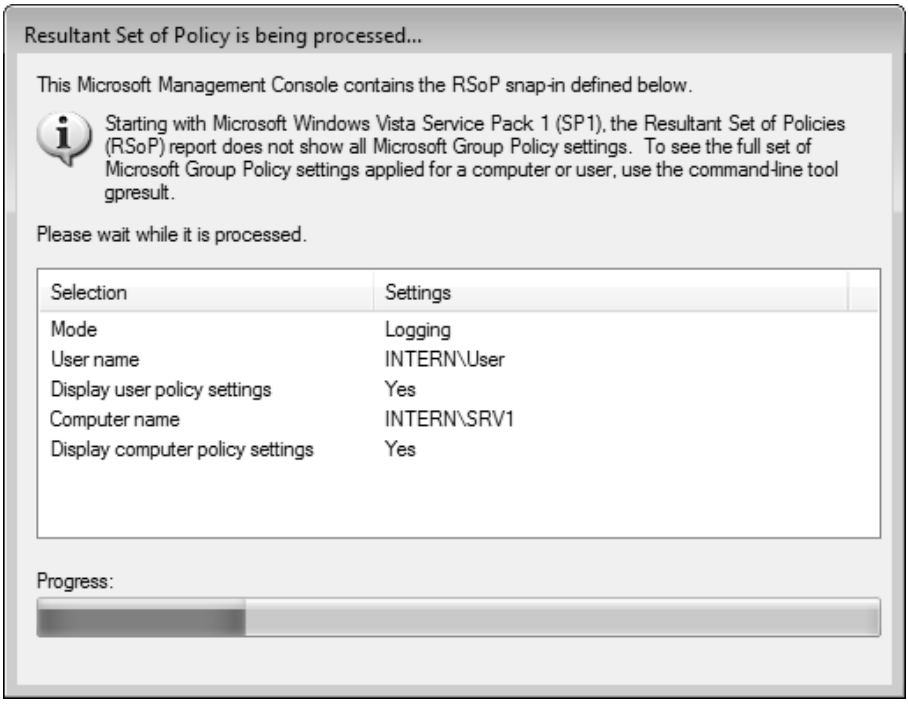


Рис. 13.22. Отображение процесса сбора RSoP-данных для указанного компьютера и пользователя

Определение политик в домене

Действующие политики в доменах определяются в окне оснастки **Group Policy Management** (Управление групповой политикой). Для хранения и просмотра полученных отчетов по действующим политикам имеются две папки: **Group Policy Modelling** (Моделирование групповой политики) и **Group Policy Results** (Результаты групповой политики) (рис. 13.23).

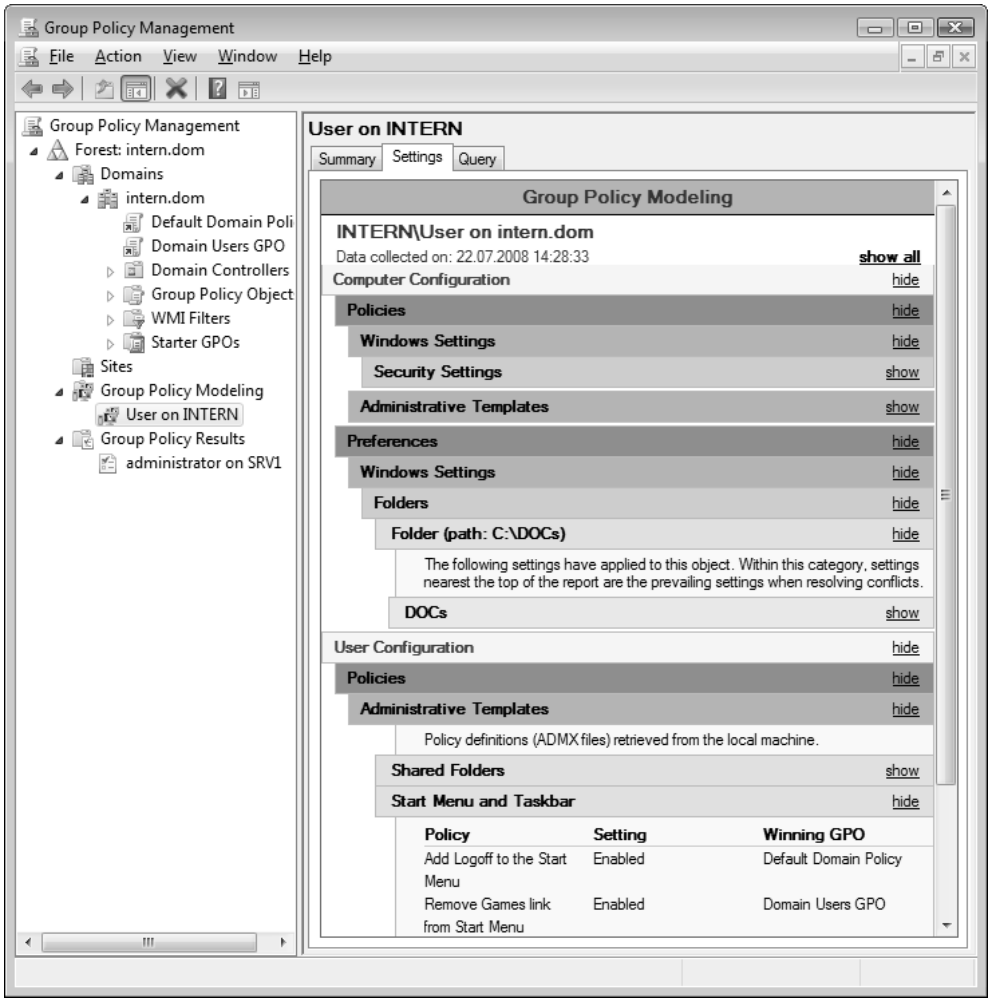


Рис. 13.23. Просмотр RSoP-данных, смоделированных для выбранного пользователя домена

В первой папке хранятся результаты, полученные в режиме планирования; в этом случае можно определять, какие политики будут действовать на компьютер или пользователя при размещении учетной записи в некотором контейнере каталога Active Directory. Во второй папке можно увидеть результаты политик, примененных к пользователю на конкретном компьютере домена (пользователь должен хотя бы раз там зарегистрироваться) — это соответствует режиму входа для оснастки **Resultant Set of Policy** (Результирующая политика).

Для определения действующих политик нужно выбрать режим получения RSoP-данных и из контекстного меню соответствующей папки запустить либо мастер *Group Policy Modelling Wizard* (Мастер моделирования групповой политики), либо мастер Group Policy Results Wizard (Мастер результатов групповой политики). Параметры запроса выбираются в интерактивном режиме, эта процедура аналогична той, что была рассмотрена в предыдущем разделе при использовании оснастки **Resultant Set of Policy** (Результирующая политика). Отличаться будет лишь способ представления результатов. На рис. 13.23 можно видеть, как выглядят RSoP-данные, полученные для конкретного пользователя указанного домена.

Документирование, архивация и восстановление GPO-объектов

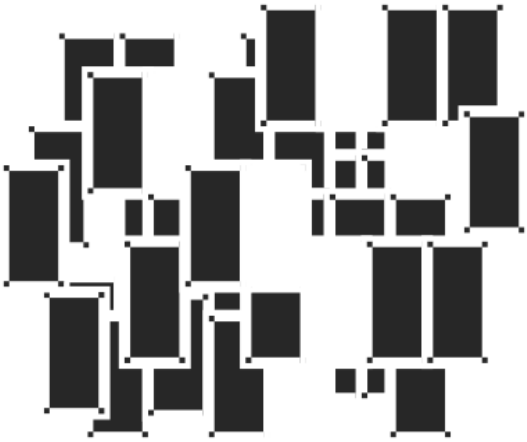
Оснастка **Group Policy Management** (Управление групповой политикой) компенсирует весьма существенный пробел в функциональных возможностях стандартных административных средств систем Windows 2000/XP/Windows Server 2003: эти средства не позволяют сохранять и восстанавливать значения параметров *всех* групповых политик, определенных в локальных и доменных GPO-объектах, а также переносить GPO-объекты из одного домена в другой.

Если выбрать объект GPO в любой папке окна оснастки (см. пример на рис. 13.3) и выполнить в контекстном меню команду **Save Report** (Сохранить отчет), то будет создан HTML-файл, в котором содержатся все характеристики объекта: имя, номер версии, состояние, привязки, параметры фильтрации групп и безопасности, а также все значения установленных политик. Этот файл очень информативен и удобен для просмотра и печати.

Если выбрать GPO-объект в папке **Group Policy Objects** (Объекты групповой политики), то в контекстном меню объекта можно увидеть команды **Back Up**

(Архивировать) и **Restore from Backup** (Восстановить из архива), позволяющие создать архивные копии объекта и восстанавливать объект из определенной копии. С помощью команды **Import Settings** (Импорт параметров) можно загрузить в выбранный GPO-объект параметры политик любого ранее сохраненного объекта, при этом текущие значения параметров можно сохранить в архиве. Команда **Copy** позволяет скопировать выбранный объект в буфер.

В контекстном меню самой папки **Group Policy Objects** (Объекты групповой политики) имеются команды **Back Up All** (Архивировать все) и **Manage Backups** (Управление архивацией). С их помощью можно эффективно создавать архивы, следить за разными версиями объектов GPO и восстанавливать нужные комбинации параметров групповых политик. Команда **Paste** позволяет создать из буфера копию существующего объекта GPO, причем исходный и новый объекты могут находиться в разных доменах или лесах.



ЧАСТЬ III

Обеспечение безопасности системы и данных

Глава 14

Защита системы и пользовательских данных

Проблема защиты системы и хранящейся на компьютере информации имеет множество аспектов, и для обеспечения безопасности в системах Windows Server 2008 имеются совершенно разные механизмы и технологии. Некоторые функции и программы уже описывались в предыдущих главах книги (например, средства диагностики, автоматические обновления, встроенный брандмауэр и т. д.). В этой главе рассматриваются общие решения, позволяющие обезопасить систему от несанкционированных вмешательств и регламентирующие доступ к данным, хранящимся на компьютере. Некоторые средства используются в системах Windows уже достаточно давно (например, управление доступом к объектам файловой системы или шифрование данных с помощью EFS), другие — такие как контроль учетных записей (UAC) или программа Windows Defender — появились только в версиях Windows Vista/Windows Server 2008.

В системах Windows Vista доступ ко многим средствам безопасности можно получить из окна *Security Center* (Центр обеспечения безопасности Windows), и для мониторинга различных параметров безопасности (состояния брандмауэра, антивируса и других программ) имеется специальная служба (сервис). В системах Windows Server 2008 таких возможностей нет, и администратор сам должен следить за состоянием всех средств защиты и контролировать их параметры.

Контроль учетных записей (UAC)

Одной из самых важных и заметных новинок в системах Windows Vista и Windows Server 2008 явился простой, но эффективный механизм разделения

прав администраторов и рядовых пользователей, получивший название *User Account Control* (UAC; Контроль учетных записей[1]). Он обеспечивает различный уровень доступа к важным, защищенным частям системы и отделяет истинно административные задачи от стандартных задач, выполняемых обычными пользователями.

Кроме того, уменьшается риск при работе на компьютере с применением учетной записи администратора системы, поскольку его права не превышают права обычного пользователя — до тех пор, пока ему не потребуются расширенные полномочия, получение которых нужно подтвердить явно. Даже если злоумышленник или шпионская программа получат доступ к компьютеру, то текущие права зарегистрированного пользователя не предоставят им возможности нарушить работу системы и произвести критически важные изменения.

Примечание

Для управления параметрами механизма контроля учетных записей на компьютерах используются групповые политики.

Администратор имеет в системе два маркера доступа: *полный* (full access token) и так называемый *фильтрованный* (filtered access token), причем при регистрации в системе ему дается фильтрованный маркер, а полный маркер применяется только при выполнении административных задач, при подтверждении перехода в режим *Admin Approval Mode* (Режим одобрения администратором). Обычные процессы и приложения запускаются с использованием фильтрованного маркера доступа и, следовательно, имеют ограниченные полномочия.

Рядовые пользователи получают при регистрации в системе обычный *пользовательский* маркер доступа (user access token), и полные права доступа для обычного пользователя не превышают те, которые предоставляет администратору фильтрованный маркер доступа.

Примечание

В системах Windows Server 2008 режим Admin Approval Mode по умолчанию выключен для встроенной учетной записи Administrator (Администратор), но включен для других членов локальной группы Administrators (Администраторы). Таким образом, только встроенный администратор имеет сразу после входа в систему полные права.

---

[1] Иногда этот механизм также называется *Управление учетными записями пользователей.*

Возможности рядовых пользователей (входящих в группу Users (Пользователи)) в системах WindowsVista и Windows Server 2008 несколько расширены: им предоставлены дополнительные полномочия, необходимые для выполнения типовых задач, не представляющих угрозы для безопасности системы (поскольку эти полномочия "ниже" прав администратора системы). Например, обычные пользователи могут выполнять служебные задачи, перечисленные ниже (для систем Windows Vista список таких задач шире):

- изменение параметров монитора;
- установка шрифтов;
- подключение принтеров и устройств, требующих дополнительных драйверов;
- подключение к безопасным беспроводным сетям;
- создание и настройка VPN-подключений;
- проверка обновлений.

Все операции, требующие *дополнительных* (административных) привилегий, отмечены в пользовательском интерфейсе систем WindowsVista/Windows Server 2008 значками предупреждений системы безопасности — маленьким изображением щита[1] (например, их можно видеть на панели управления в режиме просмотра задач по категориям — см. рис. 3.4). По их наличию рядовой пользователь легко может определять, какие действия ему будут разрешены, а какие нет.

Виртуализация операций записи в файлы и реестр

С реализацией механизма контроля учетных записей (UAC) тесно связана функция *виртуализации* (virtualization), обеспечивающая перенаправление данных, которые устаревшие прикладные программы не имеют возможности записать информацию в защищенные области файловой системы или реестра (такие как папки *%ProgramFiles%*, *%Windir%*, *%Windir%\system32* или раздел реестра `HKLM\Software\...`). Виртуализация облегчает запуск тех программ, которые не могли работать с полномочиями рядового пользователя и требовали административных прав.

---

[1] Эти значки отображаются всегда, вне зависимости от того, включен или выключен механизм UAC.

По умолчанию виртуализация включена и обеспечивает для приложений перенаправление операций записи файлов в папку *%LocalAppData%*\VirtualStore, входящую в состав локального профиля пользователя. Обычно имя этой папки имеет вид C:\Users\<*имяПользователя*>\AppData\Local\VirtualStore. Для виртуализации операций записи в реестр используется корневой раздел `HKEY_ CURRENT_USER\Software\Classes\VirtualStore`.

Функцией виртуализации также можно управлять с помощью групповых политик. Диспетчер задач позволяет увидеть, используется ли виртуализация для некоторого процесса: для этого нужно открыть вкладку **Processes** (Процессы) (см. рис. 5.2) и добавить столбец **Virtualisation** (Виртуализация).

Выполнение административных задач

Если рядовой пользователь попытается выполнить административную операцию, то появится окно запроса (рис. 14.1), указывающее на необходимость ввода учетных данных администратора. Пользователь может ввести пароль администратора и, нажав кнопку **ОК**, запустить программу с правами администратора.

Рис. 14.1. Запрос полномочий для выполнения административной операции

При включенном режиме Admin Approval Mode даже обычный администратор (член группы Administrators (Администраторы)) также получает запрос от системы безопасности (рис. 14.2) и должен подтвердить выполнение операции с повышенными полномочиями, нажав кнопку **Allow** (Продолжить).

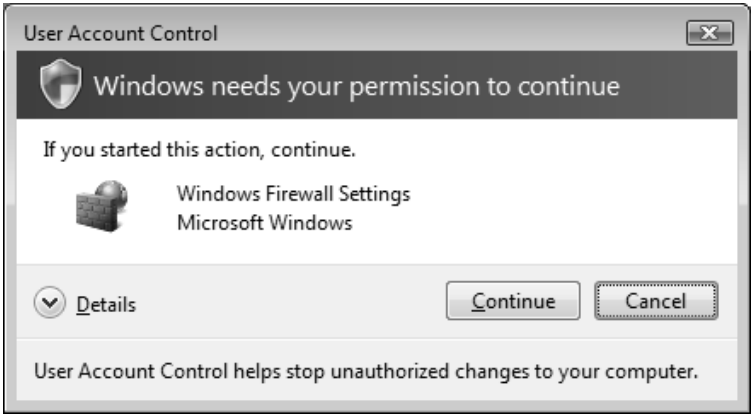


Рис. 14.2. Запрос на подтверждение выполнения административной задачи

В контекстном меню каждого исполняемого файла в окне программы Windows Explorer (Проводник) или опции меню **Start** (Пуск) имеется команда **Run as administrator** (Запуск от имени администратора). С ее помощью любой пользователь может запустить приложение с правами администратора. При этом появится сообщение, аналогичное показанному на рис. 14.1, и потребуется ввод административного пароля.

То, что права пользователя различаются при обычной работе и при "повышении" его полномочий до административных, легко проверить на следующем примере.

Если рядовой пользователь откроет окно командной строки и выполнит указанную ниже команду, то среди списка групп, в которые он входит (а именно принадлежность к этим группам и определяет полномочия пользователя!), будет присутствовать учетная запись новой встроенной группы безопасности (обратите внимание на идентификатор SID группы):

```
C:\>whoami /groups
...
Mandatory Label\Medium Mandatory Level Unknown SID type S-1-16-8192
Mandatory group, Enabled by default, Enabled group
```

```
(Обязательная метка\Средний обязательный уровень Неизвестный тип SID
 S-1-16-8192  Обязательная группа, Включены по умолчанию, Включенная группа)
```

Эта группа определяет уровень полномочий пользователя как Medium (Средний).

Если пользователь запустит окно командной строки при помощи команды **Run as administrator** (Запуск от имени администратора) и введет административный пароль, то идентификатор группы безопасности будет другим:

```
C:\>whoami /groups

...

Mandatory Label\High Mandatory Level Unknown SID type S-1-16-12288
Mandatory group, Enabled by default, Enabled group

(Обязательная метка\Высокий обязательный уровень Неизвестный тип SID
 S-1-16-12288 Обязательная группа, Включены по умолчанию, Включенная
группа)
```

В этом случае уровень полномочий определен как High (Высокий), и пользователь в окне командной строки будет работать с правами администратора.

Совет

Можно очень быстро определить права текущего пользователя в системе. Для этого из меню **Start** (Пуск) нужно открыть окно командной строки (Command Prompt). Если в заголовке окна присутствует слово Administrator (Администратор), то используется учетная запись встроенного администратора. Для всех других пользователей, включая членов группы Administrators (Администратор), заголовок будет обычным. Если из меню **Start** (Пуск) запустить какую-нибудь системную утилиту, требующую административных прав (например, оснастку **Local Security Policy** (Локальная политика безопасности)), то рядовой пользователь увидит сообщение о недостаточности прав, а член группы Administrators (Администраторы) сможет без ограничений работать с этой программой. Это важно помнить потому, что для выполнения некоторых задач членства в группе Administrators (Администраторы) недостаточно, и даже администратор (не встроенная учетная запись Administrator (Администратор)) должен использовать команду **Run as administrator** (Запуск от имени администратора).

Если какие-то программы или оснастки нужно постоянно запускать с повышенными правами, то вместо того чтобы каждый раз использовать команду **Run as administrator** (Запуск от имени администратора) в контекстном меню программы, можно задать этот режим в расширенных свойствах ярлыка про-

граммы. Для этого нужно выбрать программу в меню, щелкнуть правой кнопкой мыши и выполнить команду **Properties** (Свойства). Затем на вкладке **Shortcut** (Ярлык) (рис. 14.3) нужно нажать кнопку **Advanced** (Дополнительно) и в открывшемся окне установить флажок **Run as administrator** (Запуск от имени администратора).

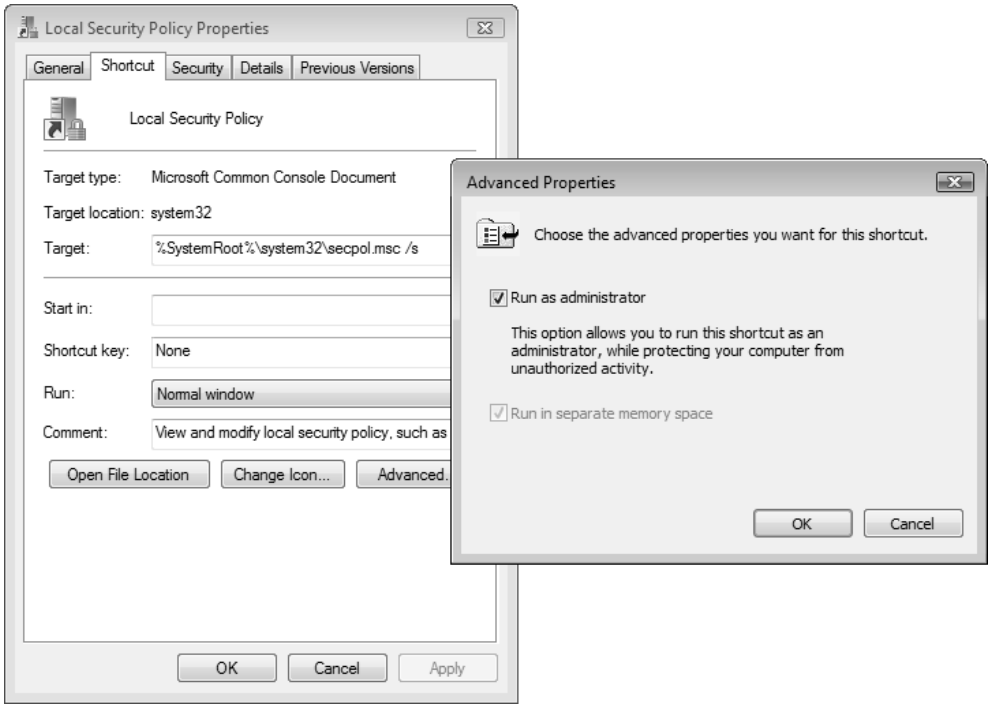


Рис. 14.3. Настройка программы или оснастки на запуск с повышенными административными полномочиями

Управление механизмом UAC

Для управления функцией контроля учетных записей (UAC) имеется несколько групповых политик (рис. 14.4). На рисунке показаны значения политик, заданные по умолчанию. По умолчанию эти политики ***определяются только локально*** (в локальных GPO — *см. главу 13*), для каждого отдельного компьютера (с установленными системами Windows Vista и Windows

Server 2008); на уровне домена или контроллеров домена они не затрагиваются. Рассмотрим самые важные из перечисленных политик.

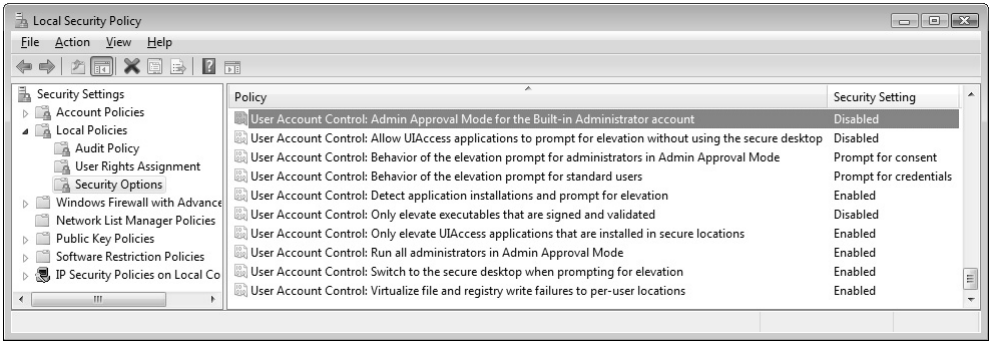


Рис. 14.4. Политики, управляющие механизмом UAC — стандартные значения

Обратите внимание на политику **User Account Control: Run all administrators in Admin Approval Mode** (Управление учетными записями пользователей: все администраторы[1] работают в режиме одобрения администратором). Поскольку по умолчанию она включена, все пользователи, включая администраторов, при обычной работе (т. е. без повышения полномочий) должны подтверждать выполнение операций, требующих полные полномочия. Система получается более защищенной, поскольку злоумышленник, даже получив доступ к текущему сеансу работы на компьютере, не сможет выполнить операции, критически важные для системы. Эта политика, собственно говоря, и управляет в системе включением/выключением механизма UAC.

Политика **User Account Control: Admin Approval Mode for the Built-in Administrator account** (Управление учетными записями пользователей: режим одобрения администратором для встроенной учетной записи администратора) по умолчанию выключена и в Windows Vista, и в Windows Server 2008. Однако в Windows Vista вход в систему осуществляется с использованием учетной записи пользователя, созданного при установке системы и входящего в группу Administrators (Администраторы) — следовательно, режим одобрения на него распространяется. В системах Windows Server 2008 после уста-

[1] Выбор названия политики не совсем понятен, поскольку она распространяется не только на администраторов, но и на всех *пользователей* компьютера — возможно, последнее считается само собой разумеющимся.

новки для входа в систему используется встроенная учетная запись Administrator (Администратор), и в работе постоянно используются повышенные полномочия.

При запросе на повышение прав происходит переключение к безопасному рабочему столу, где доступ к другим программам запрещен и никакие другие действия, кроме ввода учетных данных, невозможны. Если политику **User Account Control: Switch to the secure desktop when prompting for elevation** (Управление учетными записями пользователей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав) отключить, то запрос будет отображаться в обычном диалоговом окне Windows.

Политика **User Account Control: Virtualizes file and registry write failures to per-user locations** (Управление учетными записями пользователей: виртуализация сбоев записи в файл или реестр в расположения пользователей) позволяет управлять виртуализацией. Если в системе используются только приложения, разработанные для Windows Vista и следующих версий, то эту политику можно и отключать (если на то есть какие-то причины). Однако при отключенной политике могут не работать приложения, совместимые с предыдущими версиями Windows и записывающие данные в защищенные области.

Политика **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode** (Управление учетными записями пользователей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором) может иметь одно их трех значений: **Elevate without prompting** (Повышение без запроса), **Prompt for credentials** (Запрос учетных данных) и **Prompt for consent** (Запрос согласия). Окно запроса согласия — эта опция стоит по умолчанию — и показано на рис. 14.2. Если выбрать первую опцию, то переключение в режим повышения прав будет происходить незаметно для пользователя. Однако такой режим работы рекомендуется выбирать только в проверенных, защищенных системах.

Политика **User Account Control: Behavior of the elevation prompt for standard users** (Управление учетными записями пользователей: поведение запроса на повышение прав для обычных пользователей) имеет два значения: **Automatically deny elevation requests** (Автоматически отклонять запросы на повышение прав) и **Prompt for credentials** (Запрос учетных данных). Окно запроса на повышение прав — эта опция задана по умолчанию — показано на рис. 14.1. При выборе первой опции пользователи не будут видеть никаких изменений в своей работе, но и не получат доступ к административным средствам.

В тех случаях, когда по каким-то соображениям нужно отключить механизм UAC, то это можно сделать либо с помощью описанных выше политик, либо при помощи утилиты System Configuration (Конфигурация системы) (Msconfig.exe), которая имеется в меню **Administrative Tools** (Администрирование). В окне утилиты необходимо перейти на вкладку **Tools** (Сервис) (рис. 14.5) и выбрать опцию **Disable UAC** (Отключить контроль учетных записей (UAC)). После этого нужно нажать кнопку **Launch** (Запуск), закрыть окно утилиты и перезагрузить систему.

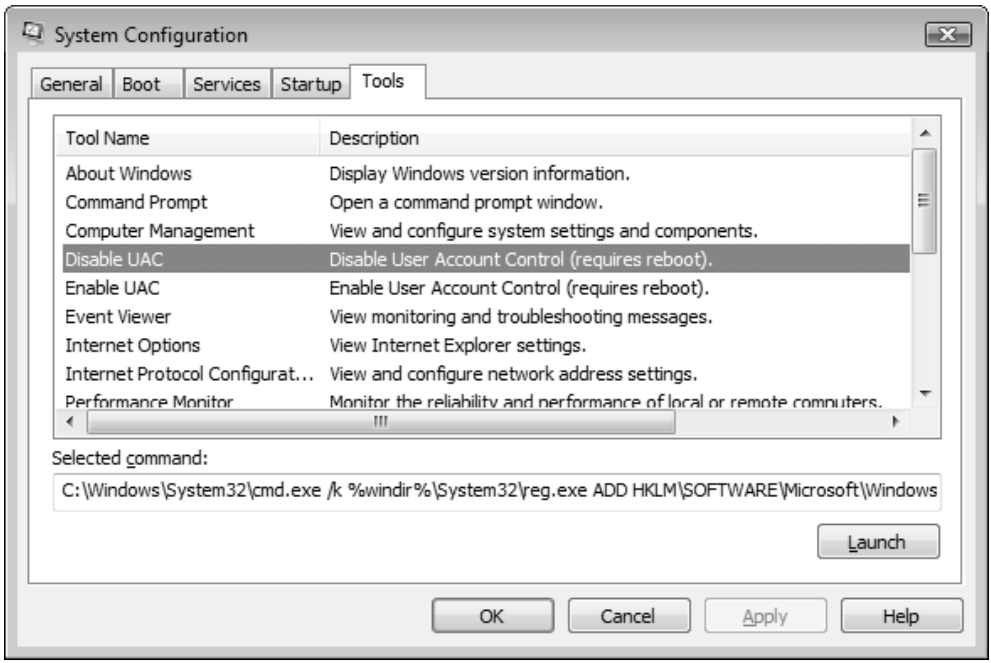


Рис. 14.5. Управление UAC с помощью утилиты System Configuration

При использовании утилиты System Configuration (Конфигурация системы) становится понятным, что за включение/выключение механизма UAC отвечает параметр `EnableLUA`, входящий в раздел `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System` системного реестра.

Проще всего включать/отключать контроль учетных записей (UAC) с панели управления — нужно лишь выбрать задачу **User Accounts** (Учетные записи пользователей) (категория **User Accounts** (Учетные записи пользователей)),

щелкнуть по ссылке **Turn User Account Control on or off** (Включение или отключение контроля учетных записей (UAC)) (см. рис. 4.3) и в следующем окне установить нужное положение флажка. После этого нужно не забыть перезагрузить систему.

Защита компьютера от шпионских программ

В состав систем Windows Vista/Windows Server 2008 включена программа *Windows Defender* (Защитник Windows), ранее известная под именем Windows AntiSpyware и свободно скачиваемая с веб-сайта Microsoft. Эта программа позволяет защитить компьютер от разнообразных шпионских (spyware) программ, а также вредоносных приложений, которые могут нарушить работоспособность и безопасность системы. В системах Windows Vista/Windows Server 2008 ядро программы реализовано как системный сервис (имя WinDefend) и управлять им можно с помощью оснастки **Services** (Службы).

Защитник Windows можно запустить из меню **Start** | **All Programs** (Пуск | Все программы), также он доступен на панели управления (категория **Security** (Безопасность). Значок программы  может постоянно отображаться в области уведомлений на панели задач (это определяется в параметрах), в этом случае программа запускается после двойного щелчка по этому значку. Обычно значок программы появляется только тогда, когда программа обнаруживает активность, требующую от нее определенных действий, или если проверка системы давно не выполнялась.

На рис. 14.6 показано главное окно программы. В нем отображаются информация о состоянии компьютера, время последнего сканирования, расписание запуска, статус онлайновой защиты и версия описаний программ (файлы описаний могут загружаться из Интернета автоматически, по мере регулярного обновления на веб-сайте Microsoft). В меню **Scan** (Проверить) можно выбрать операции быстрого и полного сканирования, а также определить свои параметры сканирования компьютера.

Защитник Windows работает в двух режимах:

- сканирование системы (памяти и жесткого диска) по запросу пользователя или по расписанию;

- постоянное присутствие в памяти и слежение за появлением опасных процессов с выдачей оперативного предупреждения пользователю (это стандартное состояние программы).

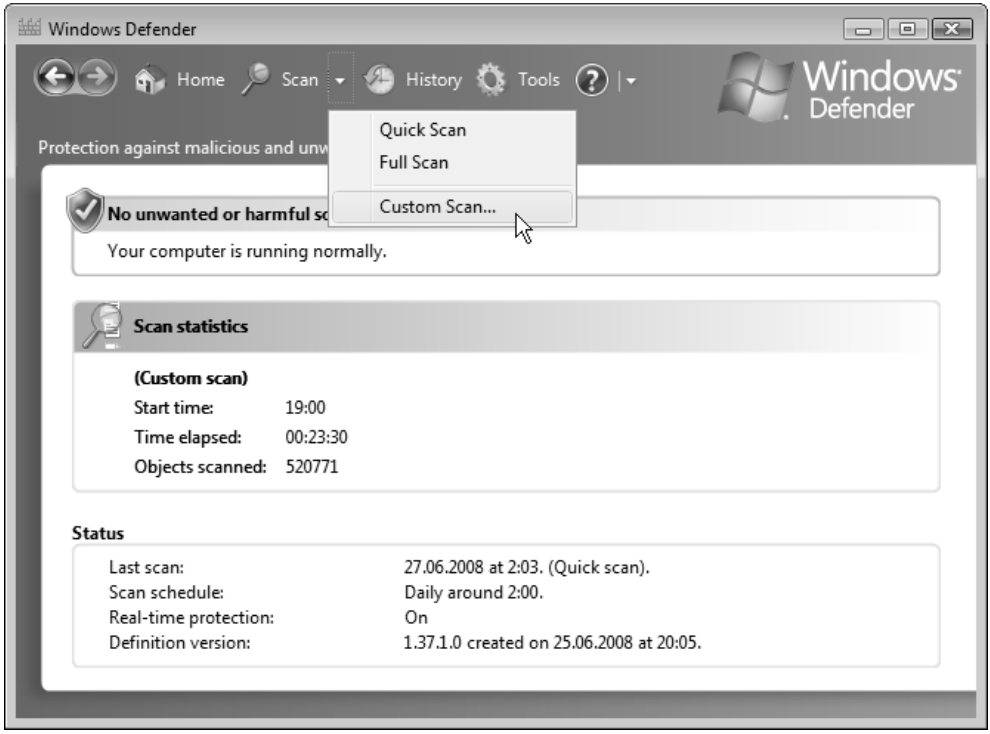


Рис. 14.6. Главное окно программы Windows Defender

Нажав кнопку **Tools** (Программы), можно попасть в окно параметров программы и дополнительных средств (рис. 14.7). Ссылка **Quarantined items** (Объекты в карантине) позволяет увидеть список приложений, которые были заблокированы по той причине, что представляли угрозу безопасности компьютера.

Если удаление было ошибочным, то программу можно восстановить и разрешить ее работу. Если Защитник Windows не смог принять решение о блокировке программы, то он запрашивает подтверждение на работу приложения и разрешенные программы помещает в раздел **Allowed items** (Разрешен-

ные объекты). Средство Software Exporer (Проводник программного обеспечения) мы рассмотрим в следующем разделе.

Рис. 14.7. Окно параметров и программ

По ссылке **Options** (Параметры) можно попасть в окно многочисленных параметров программы Windows Defender (рис. 14.8). В нем определяется расписание запуска программы, разрешается загрузка обновленных описаний сигнатур, выбираются параметры онлайновой (real-time) проверки и т. д. В конце длинного списка параметров находятся два флажка, первый из которых включает и выключает саму программу Windows Defender (при этом будет остановлен и сервис WinDefend; однако после перезагрузки системы он автоматически стартует снова), а второй — разрешает рядовым пользователям сканировать компьютер.

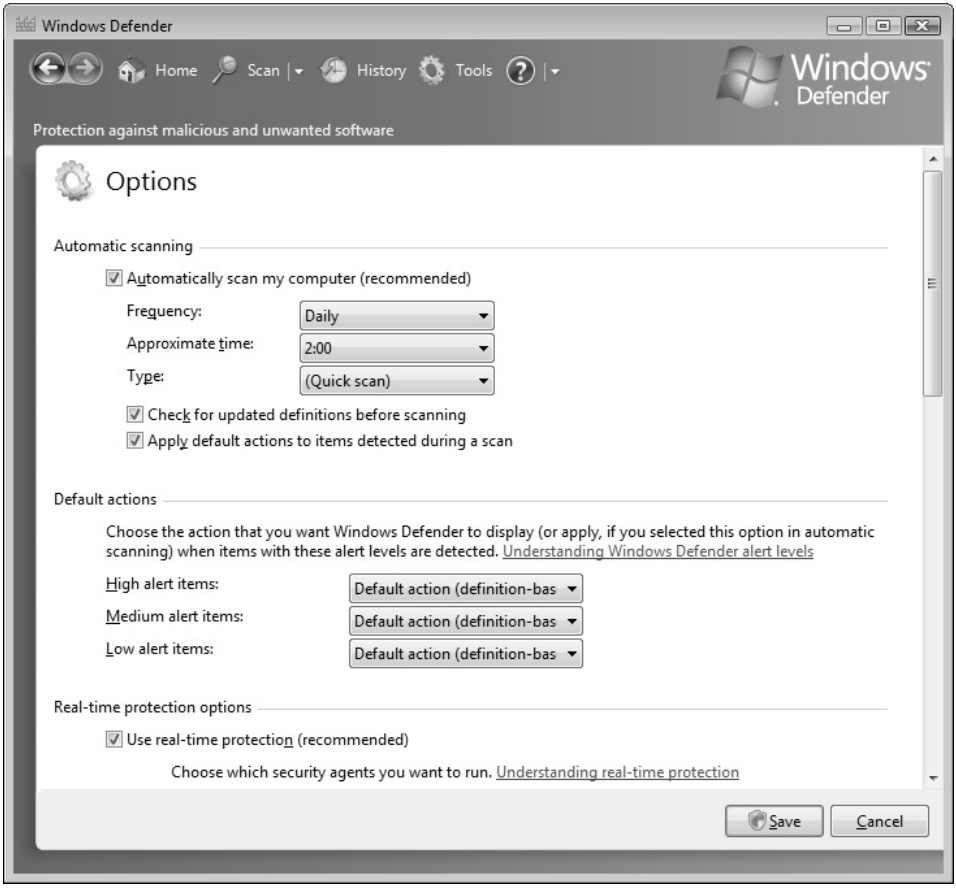


Рис. 14.8. Окно параметров программы Windows Defender

Мониторинг программ и сервисов — программа Software Exporer

Средство Software Exporer (Проводник программного обеспечения) позволяет получать подробную информацию обо всех программах, работающих в системе. (Ссылка на Software Exporer также имеется непосредственно на панели управления[1] — см. категорию **Programs** (Программы), ссылка **View currently running programs** (Просмотр выполняющихся программ).)

[1] В том случае, если используется новый вид панели управления с делением по категориям.

В окне программы вместо списка не всегда понятных имен процессов можно видеть названия и параметры соответствующих приложений, включая другие важные сведения, например, номера портов и внешние IP-адреса, к которым обращается программа (рис. 14.9). Список приложений разбит по фирмам-производителям, благодаря чему ориентироваться в программах очень удобно. Непосредственно из этого окна можно сразу прекращать подозрительные задачи.

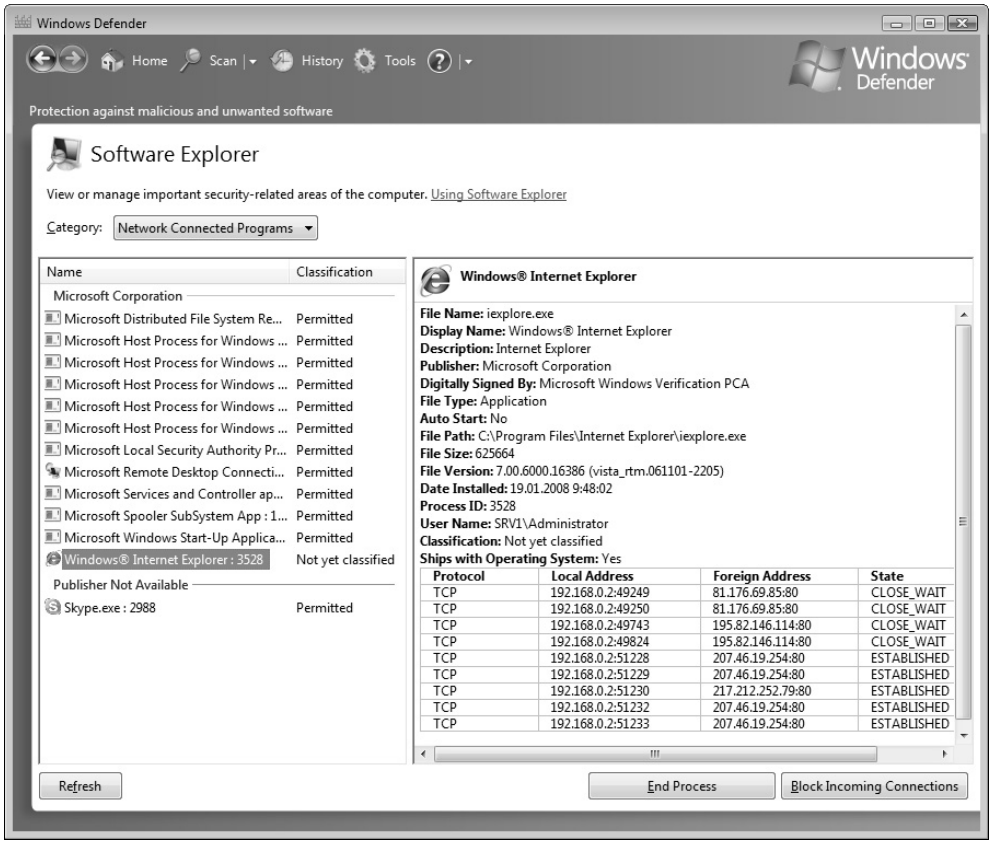


Рис. 14.9. Мониторинг процессов, обращающихся к сети

Не менее интересные режимы — просмотр программ, загружаемых при запуске системы (категория Startup Programs), и список программ, выполняющихся в данный момент (категория Currently Running Programs).

Управление доступом к файлам и папкам

Если компьютер выполняет роль файлового сервера, то одной из важнейших задач администратора является распределение прав доступа к хранящейся информации. Это касается и отдельных файлов, и папок. Задача управления доступом к дисковым ресурсам, как правило, возникает при доступе по локальной сети, но также может быть актуальной, когда на компьютере работают несколько пользователей.

Мы рассмотрим назначение прав доступа *в совокупности* — для локального доступа и для сетевого, поскольку методы выбора этих прав тесно взаимосвязаны, и важно понимать, какие же разрешения будет иметь, в конце концов, каждый пользователь. Если сетевой доступ отсутствует, то можно пропустить следующий раздел и перейти сразу к разрешениям доступа на уровне файловой системы.

Правила назначения разрешений на доступ

Для общих папок разрешения на доступ к ресурсу определяются на двух уровнях:

- *на уровне общей папки*; эти разрешения распространяются на ***все*** вложенные папки и файлы, содержащиеся в общей папке, и действуют только при доступе к папке через сеть;
- *на уровне файловой системы NTFS* (если общая папка расположена на FAT-томе, то такие разрешения для нее невозможны); эти разрешения можно назначать как всей папке, так и ***конкретным*** вложенным папкам и файлам внутри общей папки; они действуют всегда, независимо от способа доступа к папке.

При выборе разрешений доступа обычно руководствуются следующими правилами:

- на уровне общего ресурса рекомендуется задавать наиболее "широкие" права (если позволяют требования безопасности — полный доступ для всех);
- на уровне файловой системы NTFS определяются более "узкие" разрешения на конкретные папки и файлы для отдельных групп или пользователей.

Такой подход упрощает администрирование полномочий пользователей. Результирующие права доступа ***определяются наиболее "строгими" разрешениями, установленными либо на уровне общего ресурса, либо на уровне файловой системы*** (при этом самыми приоритетными являются *запреты* каких-либо разрешений — когда установлен флажок **Deny** (Запретить)).

Предположим, на уровне общей папки установлено разрешение Read (Чтение) для группы Everyone (Все). Если вдруг нужно какой-то группе или пользователю дать более широкие права, например, разрешение на запись в какую-то папку, то это сделать невозможно, поскольку права доступа ограничены на уровне общей папки более "узким" разрешением Read (Чтение). Кроме того, разрешения на уровне общей папки не позволяют детализировать права доступа, поскольку они распространяются на весь общий ресурс и представляют собой достаточно обобщенные возможности (чтение, изменение или полный доступ). Разрешения, заданные на уровне файловой системы, более "универсальны": они не зависят от того, зарегистрирован ли пользователь на компьютере локально или обращается к нему через сеть.

> ***Внимание!***
>
> Разрешения принято предоставлять не отдельным пользователям, а группам (в соответствии с функциональными задачами, возлагаемыми на эти группы). Пользователи же получают права опосредованно, через членство в определенной группе. Главным образом это связано с тем, что членство пользователя в группе поменять значительно легче, чем все разрешения, если бы они были назначены *непосредственно* этому пользователю. Кроме того, групп обычно значительно меньше, чем пользователей. В первую очередь это правило актуально при работе в больших сетях, имеющих множество компьютеров и пользователей.

Разрешения, заданные "внутри" каждого уровня (т. е. на уровне общей папки или на уровне файловой системы), являются *аддитивными*, т. е. результирующие права будут складываться из всех разрешений, явно или косвенно распространяющихся на пользователя (в первую очередь это правило применимо к разрешениям, задаваемым на уровне файловой системы, поскольку различных разрешений там больше). Если, например, пользователь имеет разрешение на чтение, а группе, в которую он входит, дано разрешение на запись, то в результате этот пользователь будет иметь возможность *и* читать, *и* записывать.

> ***Внимание!***
>
> Пользователи клиентских компьютеров, имеющие учетные записи без пароля, не могут обращаться по сети к общим папкам систем Windows Server

2008, поскольку в этих системах по умолчанию действует политика безопасности **Accounts: Limit local account use of blank passwords to console logon only** (Учетные записи: разрешить использование пустых паролей только при консольном входе) (см. рис. 13.13) — т. е. пустые пароли допускаются только при локальном входе в систему, а при обращении по сети аутентификация пользователя не производится. Поэтому для обеспечения доступа к общим папкам нужно либо дать пользователям пароли, либо отключить эту политику.

Способы настройки разрешений на уровне общих ресурсов рассмотрены в *разд. "Управление общими дисковыми ресурсами" главы 7*. Если мастер *Sharing Wizard* (Мастер общего доступа) не используется, то изначально при разрешении общего доступа к папке предоставляется разрешение Read (Чтение) для группы Everyone (Все). В случае его применения учетные записи и их права выбираются индивидуально, при этом ***автоматически устанавливаются аналогичные разрешения и на уровне файловой системы***.

Ниже мы рассмотрим, как установить разрешения доступа к объектам файловой системы.

Разрешения доступа на уровне файловой системы

Устанавливая пользователям определенные *разрешения* (permissions) на доступ к файлам и папкам, администраторы системы могут защищать информацию от несанкционированного доступа. Каждый пользователь должен иметь определенный набор разрешений на доступ к конкретному объекту файловой системы.

Кроме того, пользователь автоматически становится *владельцем* создаваемого файла или папки. Администратор может назначить себя владельцем любого объекта файловой системы (файла или папки). В системах Windows Server 2008 возможна и обратная передача владения от администратора к пользователю (или от одного пользователя — другому).

Как уже говорилось, разрешения пользователя на доступ к объектам файловой системы работают по принципу *дополнения* (аддитивности). Это значит, что *действующие* разрешения, т. е. те разрешения, которые пользователь реально имеет в отношении конкретной папки или файла, образуются из всех *прямых* (заданных явно) и *косвенных* (полученных через членство в группах) разрешений, которые объединяются с помощью логической функции ИЛИ.

Следует однако заметить, что правило сложения разрешений с помощью логического ИЛИ не выполняется, когда пользователь имеет определенное *разрешение*, а группе, в которую он входит, *отказано* в этом разрешении (или наоборот). В этом случае отказ в разрешении (Deny) имеет более высокий приоритет над предоставлением разрешения, т. е. в результате пользователь не будет иметь данного разрешения. При установке отказа всегда появляется окно с напоминанием о серьезности такого действия (поскольку очень легко вообще лишить пользователя доступа к файлу или папке).

Наличие возможности отказа пользователю или группе в разрешении для файлов и папок сделало ненужным разрешение *No Access* (Нет доступа), применявшееся в системах Windows ранее. Теперь для отказа пользователю в разрешении на доступ к какому-либо файлу или папке достаточно включить пользователя в группу, которой отказано в разрешении Full control (Полный доступ) для данного объекта файловой системы. При этом запреты можно устанавливать и более детально — на выполнение только определенных операций.

Установка разрешений для файлов

Все операции с разрешениями доступа к файлам и папкам выполняются в окне программы Windows Explorer (Проводник). В системах Windows Vista и Windows Server 2008 несколько изменился интерфейс, используемый при работе с разрешениями (при выполнении *изменений* всегда требуются дополнительные шаги), хотя общая логика операций осталась прежней.

Рассмотрим подробно порядок выполнения операций с файлами — аналогичные шаги требуются и при выборе папок, поэтому их мы не будем описывать так подробно.

Для назначения пользователю или группе разрешения на доступ к определенному файлу:

1. Выберите файл и нажмите правую кнопку мыши. Выполните команду **Properties** (Свойства) контекстного меню. В появившемся окне свойств файла перейдите на вкладку **Security** (Безопасность) (рис. 14.10). Обратите внимание: в системах Windows XP/Windows Server 2003 на этой вкладке можно *сразу* изменять разрешения для имеющихся в списке групп и пользователей, а в Windows Vista/Windows Server 2008 их можно только просматривать без возможности модификации.

На панели **Group or user names** (Группы или пользователи) показан список пользователей и групп, которым уже предоставлены разрешения для данного файла. Для того чтобы добавить или удалить пользователей или группы, следует нажать кнопку **Edit** (Изменить). Кнопка **Advanced** (Дополнительно) позволяет получить доступ к тонкой настройке на уровне специальных разрешений.

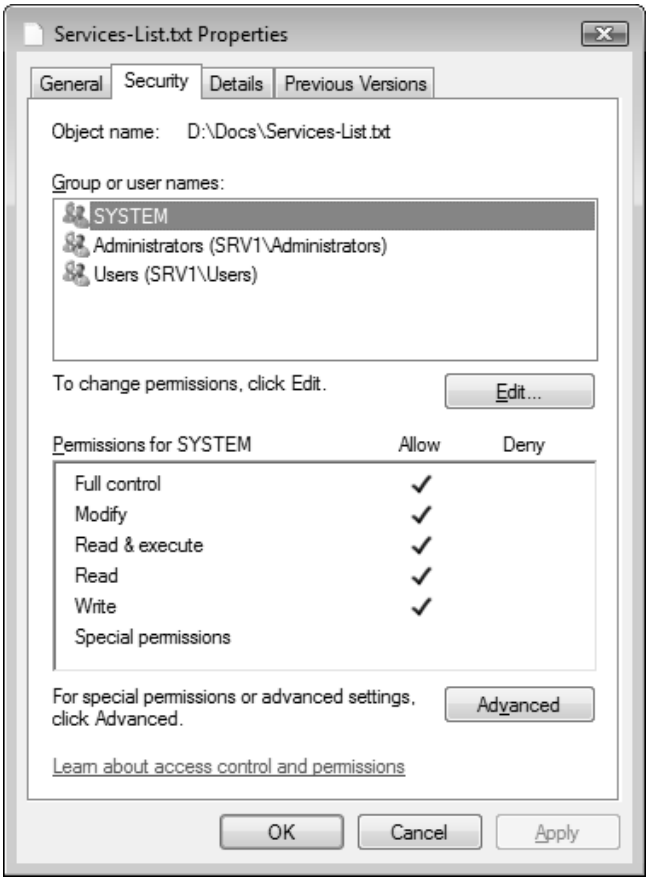


Рис. 14.10. Вкладка **Security** окна свойств файла

2. После нажатия кнопки **Edit** (Изменить) появляется окно (рис. 14.11), вид которого привычен пользователям Windows XP/Windows Server 2003: здесь можно изменять разрешения для указанных групп и пользователей (разрешения представлены не просто галочками, как в предыдущем окне,

а флажками, которые можно устанавливать и сбрасывать). Для изменения этого списка служат кнопки **Add** (Добавить) или **Remove** (Удалить).

Рис. 14.11. Окно редактирования разрешений доступа

3. При добавлении учетных записей появится диалоговое окно (рис. 14.12), где нужно указать имена пользователей или групп, которые получат права доступа к файлу. (В доменах также можно указывать учетные записи *компьютеров*.)

   Здесь имеются две возможности: можно *сразу* ввести имя в окне **Enter the object names to select** (Введите имена выбираемых объектов) и нажать кнопку **Check Names** (Проверить имена) для проверки введенного имени (такая проверка не обязательна, но желательна); если имя правильное, нажмите кнопку **OK**. Для *поиска* нужных имен можно нажать кнопку **Advanced** (Дополнительно). При этом откроется модифицированное окно

выбора учетных записей (рис. 14.13), в котором можно указать местоположение (location) учетной записи (домен или локальный компьютер) и выполнить поиск, нажав кнопку **Find Now** (Поиск). В нижней половине окна появится список всех групп и пользователей, имеющихся для данного размещения — локального компьютера, домена или конкретного подразделения. Выбрав все нужные имена (возможен множественный выбор), закройте окно, нажав кнопку **OK**. Указанное имя (или несколько имен) появится в списке (см. рис. 14.12). При необходимости выбор имен можно повторить. Когда выбор закончен, нажмите кнопку **OK**.

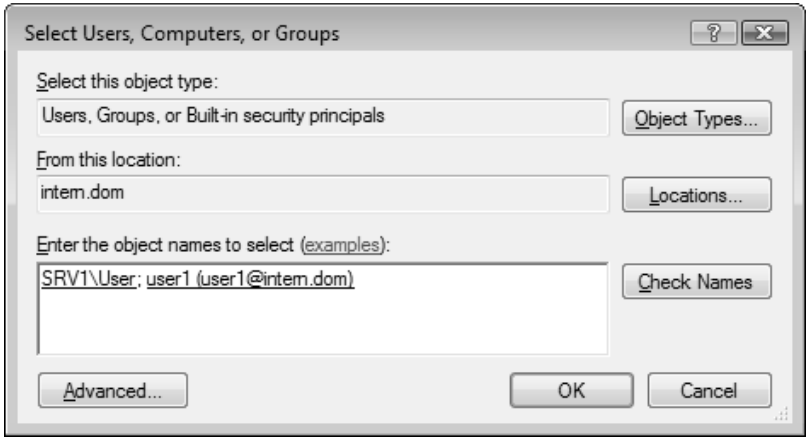


Рис. 14.12. Диалоговое окно выбора учетных записей пользователей, компьютеров и групп

4. Теперь в окне разрешений для выбранного объекта файловой системы (см. рис. 14.11) пользователю или группе можно назначить *стандартные разрешения* для файлов — **Full control** (Полный доступ), **Modify** (Изменение), **Read & execute** (Чтение и выполнение), **Read** (Чтение) и **Write** (Запись). Для установки разрешения или отказа в разрешении служат флажки **Allow** (Разрешить) и **Deny** (Запретить).

Каждое из перечисленных выше стандартных разрешений состоит из набора *специальных* (особых) разрешений, задающих возможность выполнения того или иного более частного действия с файлами или папками. В табл. 14.1 показано соответствие между стандартными и специальными разрешениями для файлов. Более подробно специальные разрешения рассмотрены далее.

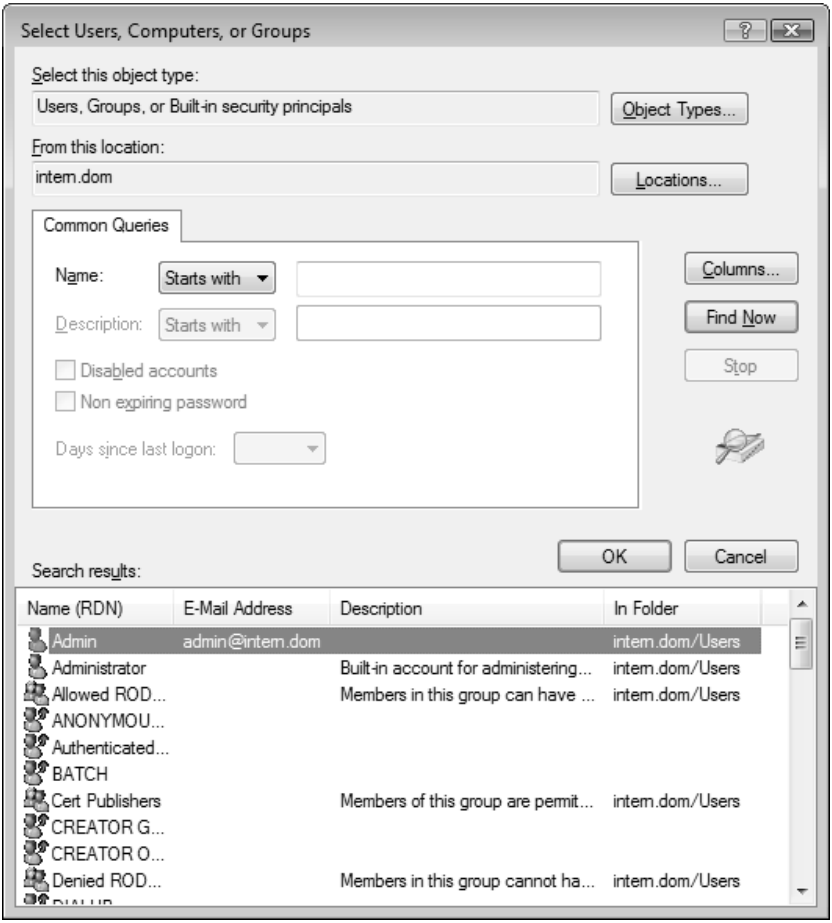


Рис. 14.13. Поиск и выбор пользователей и группы для назначения им разрешений доступа

Таблица 14.1. *Соответствие стандартных и специальных разрешений для файлов*

Специальные разрешения	**Стандартные разрешения**				
	Full control	**Modify**	**Read & execute**	**Read**	**Write**
Traverse folder/ execute file (Траверс папок/ выполнение файлов)	○	○	○		

Таблица 14.1 *(продолжение)*

Специальные разрешения	Стандартные разрешения				
	Full control	**Modify**	**Read & execute**	**Read**	**Write**
List folder/read data (Содержание папки/чтение данных)	○	○	○	○	
Read attributes (Чтение атрибутов)	○	○	○	○	
Read extended attributes (Чтение дополнительных атрибутов)	○	○	○	○	
Create files/ write data (Создание файлов/запись данных)	○	○			○
Create folder/ append data (Создание папок/дозапись данных)	○	○			○
Write attributes (Запись атрибутов)	○	○			○
Write extended attributes (Запись дополнительных атрибутов)	○	○			○
Delete (Удаление)	○	○			
Read permissions (Чтение разрешений)	○	○	○	○	○
Change permissions (Смена разрешений)	○				

Таблица 14.1 *(окончание)*

Специальные разрешения	Стандартные разрешения				
	Full control	**Modify**	**Read & execute**	**Read**	**Write**
Take ownership (Смена владельца)	○				

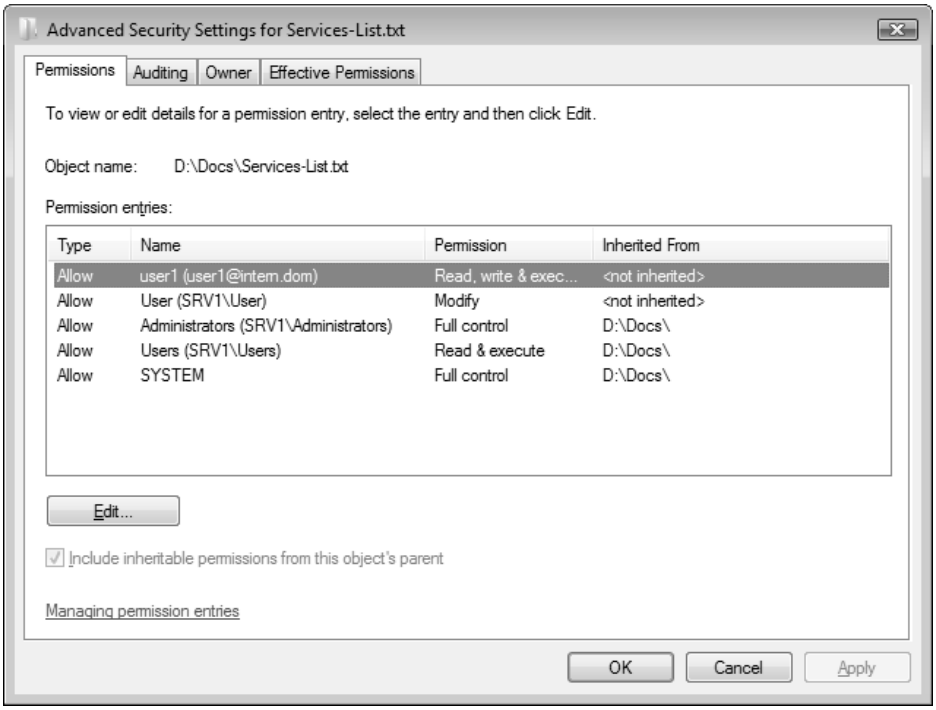


Рис. 14.14. Окно просмотра дополнительных параметров безопасности для файла

Чтобы получить доступ к специальным разрешениям, нужно в окне свойств файла на вкладке **Security** (Безопасность) (см. рис. 14.10) нажать кнопку **Advanced** (Дополнительно). В окне дополнительных параметров безопасности (рис. 14.14) можно видеть, от какой папки унаследованы разрешения, действующие на выбранный файл, а также можно определить (и изменить) владельца файла. Кнопка **Edit** (Изменить) позволяет получить доступ к окну редактирования специальных разрешений, назначение которых указано в табл. 14.2.

Таблица 14.2. *Специальные разрешения для файлов и папок*

Специальное разрешение	Описание
Traverse folder/execute file (Траверс папок/ выполнение файлов)	Определяет возможность перемещения по папкам файловой системы вне зависимости от того, имеет или не имеет пользователь разрешения доступа к пересекаемым в процессе перемещения папкам. На работу этого разрешения влияет локальная политика **Bypass traverse checking** (Обход перекрестной проверки). Разрешение **Execute file** (Выполнение файлов) определяет возможность исполнения программ
List folder/read data (Содержание папки/чтение данных)	Определяет возможность просмотра имен файлов или подкаталогов данной папки (относится только к папкам). Разрешение **Read data** (Чтение данных) определяет возможность просмотра данных файла
Read attributes (Чтение атрибутов)	Определяет возможность просмотра атрибутов файла или папки. Сами атрибуты определяются операционной системой
Read extended attributes (Чтение дополнительных атрибутов)	Определяет возможность просмотра дополнительных атрибутов файла или папки. Сами дополнительные атрибуты определяются операционной системой
Create files/ write data (Создание файлов/запись данных)	Определяет возможность создания файлов внутри папки (относится только к папкам). Разрешение **Write data** (Запись данных) определяет возможность изменения содержимого файлов или перезаписи существующих данных файла новой информацией (относится только к файлам)
Create folder/ append data (Создание папок/ дозапись данных)	Определяет возможность создавать подкаталоги внутри данной папки (относится только к папкам). Разрешение **Append data** (Дозапись данных) определяет возможность присоединения новых данных к существующему файлу без изменения, уничтожения или перезаписи существующей информации (относится только к файлам)
Write attributes (Запись атрибутов)	Определяет возможность изменения атрибутов файла или папки. Атрибуты определяются операционной системой

Таблица 14.2 *(окончание)*

Специальное разрешение	Описание
Write extended attributes (Запись дополнительных атрибутов)	Определяет возможность изменения дополнительных атрибутов файла или папки. Дополнительные атрибуты определяются программой и могут быть ею изменены
Delete subfolders and files (Удаление подпапок и файлов)	Определяет возможность удаления подкаталогов и файлов, находящихся в данной папке, даже если для этих подкаталогов и файлов нет разрешения **Delete** (Удаление). Это разрешение имеется ***только у папок***
Delete (Удаление)	Определяет возможность удаления файла или папки. Если установлен отказ в разрешении **Delete** (Удаление) для некоторой папки или файла, их все же можно удалить, получив разрешение **Delete subfolders and files** (Удаление подпапок и файлов) на *родительскую* папку
Read permissions (Чтение разрешений)	Определяет возможность чтения таких разрешений для файлов и папок, как *Полный доступ*, *Чтение* и т. д.
Change permissions (Смена разрешений)	Определяет возможность изменения таких разрешений для файлов и папок, как **Full control** (Полный доступ), **Read** (Чтение) и т. д.
Take ownership (Смена владельца)	Определяет возможность вступления во владение данным файлом или папкой. Владелец файла или папки может всегда изменить разрешения к этому объекту, независимо от других разрешений

Использование утилит командной строки

Имеются утилиты, позволяющие в окне консоли управлять разрешениями доступа на уровне файловой системы. Стандартная утилита *Icacls.exe* используется для просмотра, установки и изменения разрешений для файлов и папок. На веб-сайте Microsoft можно также найти полезную утилиту *Perms.exe*, с помощью которой легко определить, какие права доступа имеет определенный пользователь в отношении указанных файлов и папок. Утилита *Fileacl.exe* является аналогом Icacls.exe, но имеет более широкие возможности.

Установка разрешений для папок

Процедура установки разрешений для папок совершенно не отличается от описанной выше процедуры назначения разрешений для файлов, немного отличается лишь список стандартных разрешений: для папок еще имеется разрешение **List folder contents** (Список содержимого папки), определяющее возможность просмотра ее содержимого. Соответствие между стандартными и специальными разрешениями для папок показано в табл. 14.3.

Таблица 14.3. *Соответствие стандартных и специальных разрешений для папок*

Специальные разрешения	Стандартные разрешения					
	Full control	**Modify**	**Read & execute**	**List folder contents**	**Read**	**Write**
Traverse folder/execute file (Траверс папок/ выполнение файлов)	○	○	○	○		
List folder/read data (Содержание папки/чтение данных)	○	○	○	○	○	
Read attributes (Чтение атрибутов)	○	○	○	○	○	
Read extended attributes (Чтение дополнительных атрибутов)	○	○	○	○	○	
Create files/write data (Создание файлов/запись данных)	○	○				○
Create folder/ append data (Создание папок/дозапись данных)	○	○				○
Write attributes (Запись атрибутов)	○	○				○

Таблица 14.3 *(окончание)*

Специальные разрешения	Стандартные разрешения					
	Full control	**Modify**	**Read & execute**	**List folder contents**	**Read**	**Write**
Write extended attributes (Запись дополнительных атрибутов)	○	○				○
Delete subfolders and files (Удаление подпапок и файлов)	○					
Delete (Удаление)	○	○				
Read permissions (Чтение разрешений)	○	○	○	○	○	○
Change permissions (Смена разрешений)	○					
Take ownership (Смена владельца)	○					

Внимание!

Пользователь или группа, имеющие право **Full control** (Полный доступ) на папку, могут удалить любой файл, находящийся в этой папке, вне зависимости от разрешений, заданных для данного файла.

При редактировании дополнительных параметров безопасности (рис. 14.15) для папок имеются дополнительные возможности, касающиеся изменения иерархии наследуемых разрешений.

Флажок **Include inheritable permissions from the object's parent** (Добавить разрешения, наследуемые от родительских объектов) (он имеется в окне дополнительных параметров и для файлов) по умолчанию установлен, и выбранный объект автоматически получает все разрешения, заданные на более высоких уровнях. Если этот флажок сбросить, всякое наследование прекратится и все разрешения будут явно заданы только на уровне данного объекта.

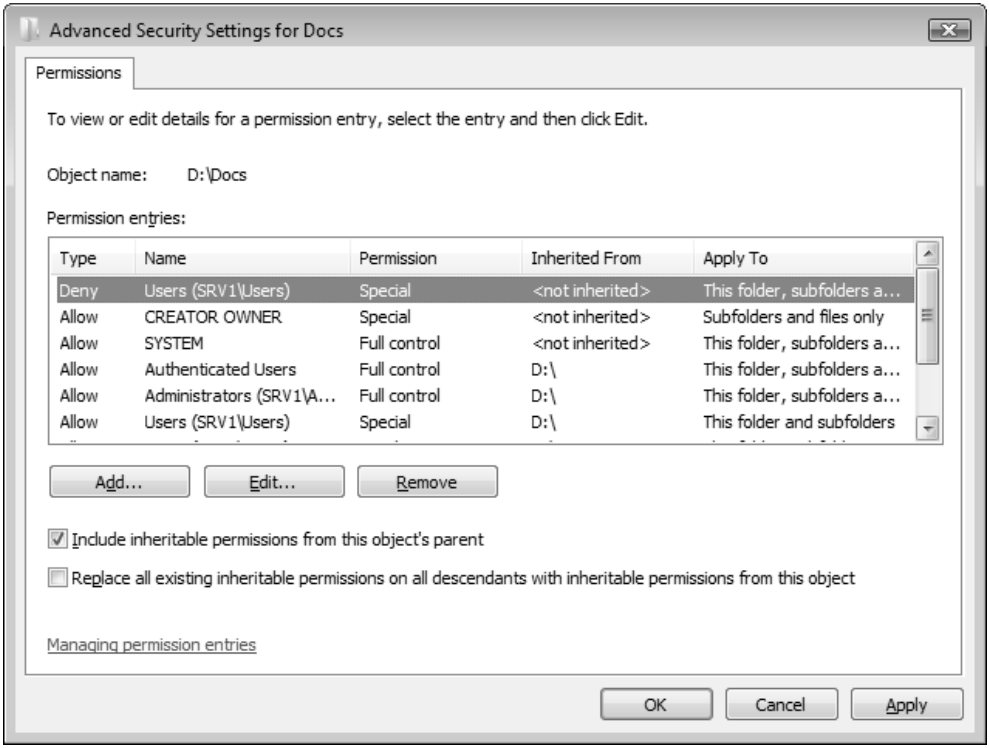


Рис. 14.15. Окно редактирования дополнительных параметров безопасности для папки

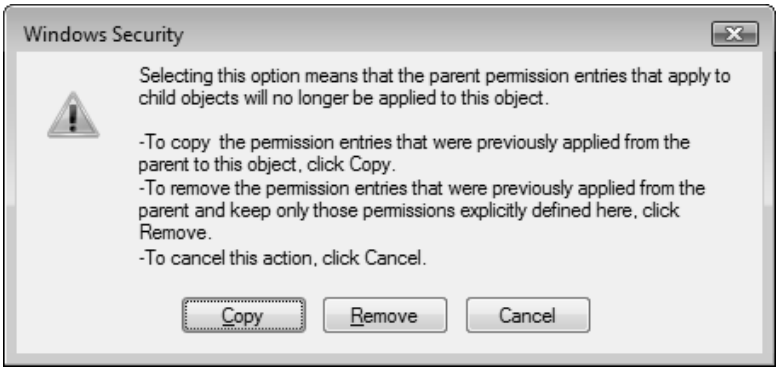


Рис. 14.16. Выбор действий при отказе от наследования разрешений от родительских объектов

При изменении порядка наследования возможны два варианта действий (рис. 14.16): можно *скопировать* разрешения (и затем изменять их, как требуется) или *удалить* (и задать новые).

Если установить флажок **Replace all existing inheritable permissions on all descendants with inheritable permissions from this object** (Заменить все наследуемые разрешения для всех потомков на новые наследуемые разрешения от этого объекта) (см. рис. 14.15), то все разрешения, заданные явно или неявно для дочерних объектов (файлов и папок), будут удалены и заменены на те разрешения, которые определены для выбранной папки.

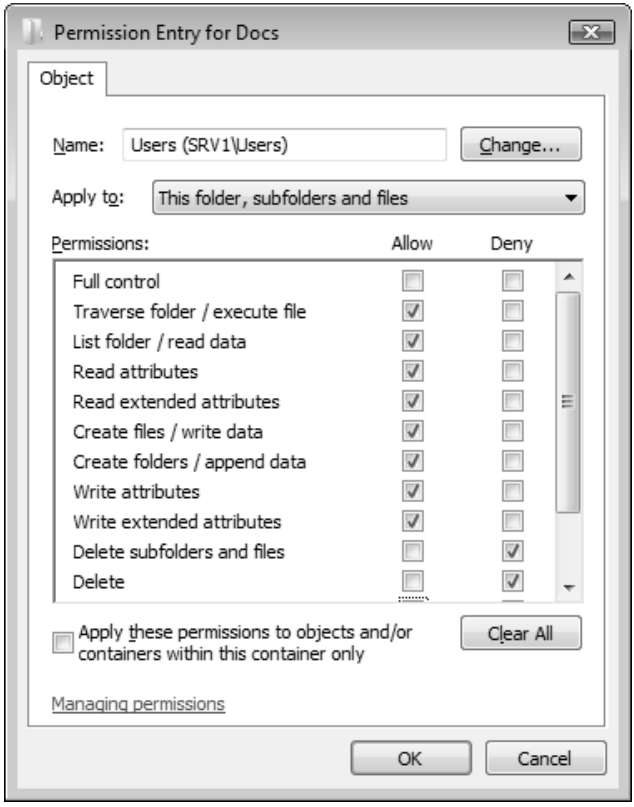


Рис. 14.17. Специальные разрешения для папки

Если для папки необходимо задать специальные разрешения, то в окне дополнительных параметров (см. рис. 14.15) нужно нажать кнопку **Edit** (Изменить). Появится окно **Permissions Entry** (Элемент разрешения) (рис. 14.17),

где можно установить специальные разрешения для папки, а также в списке **Apply onto** (Применять) выбрать область их действия.

Возможны следующие области действия установленных разрешений:

- **This folder only** (Только для этой папки);
- **This folder, subfolders and files** (Для этой папки, ее подпапок и файлов);
- **This folder and subfolders** (Для этой папки и ее подпапок);
- **This folder and files** (Для этой папки и ее файлов);
- **Subfolders and files only** (Только для подпапок и файлов);
- **Subfolders only** (Только для подпапок);
- **Files only** (Только для файлов).

Когда флажок **Apply these permissions to object and/or containers within this container only** (Применять эти разрешения к объектам и контейнерам только внутри этого контейнера) не установлен (по умолчанию), выбранные разрешения будут распространяться не только на объекты, определенные полем **Apply onto** (Применять), но и на все объекты, находящиеся ниже по дереву.

Определение действующих разрешений для файлов и папок

Как уже говорилось, пользователь или группа получают разрешения на доступ к файлам или папкам *непосредственно* и через *членство в группах* (следует также помнить о том, что в доменах Active Directory группы могут быть членами других групп). Поэтому не всегда просто и быстро узнать, какие же разрешения имеет пользователь для конкретного объекта. Для решения этой задачи имеется функция определения *действующих разрешений* (effective permissions).

1. Выберите нужный файл или папку и перейдите на вкладку **Security** (Безопасность).
2. Нажмите кнопку **Advanced** (Дополнительно) и в окне **Advanced Security Settings** (Дополнительные параметры безопасности) перейдите на вкладку **Effective Permissions** (Действующие разрешения).
3. Нажмите кнопку **Select** (Выбрать). Откроется окно выбора учетных записей, аналогичное тому, какое появляется при добавлении разрешений (см. рис. 14.12).

4. Выберите требуемую учетную запись локального или доменного пользователя или группы и нажмите кнопку **OK**.

Теперь на вкладке **Effective Permissions** (Действующие разрешения) будут отображены все разрешения, которые выбранный пользователь или группа имеют по отношению к данному объекту (рис. 14.18).

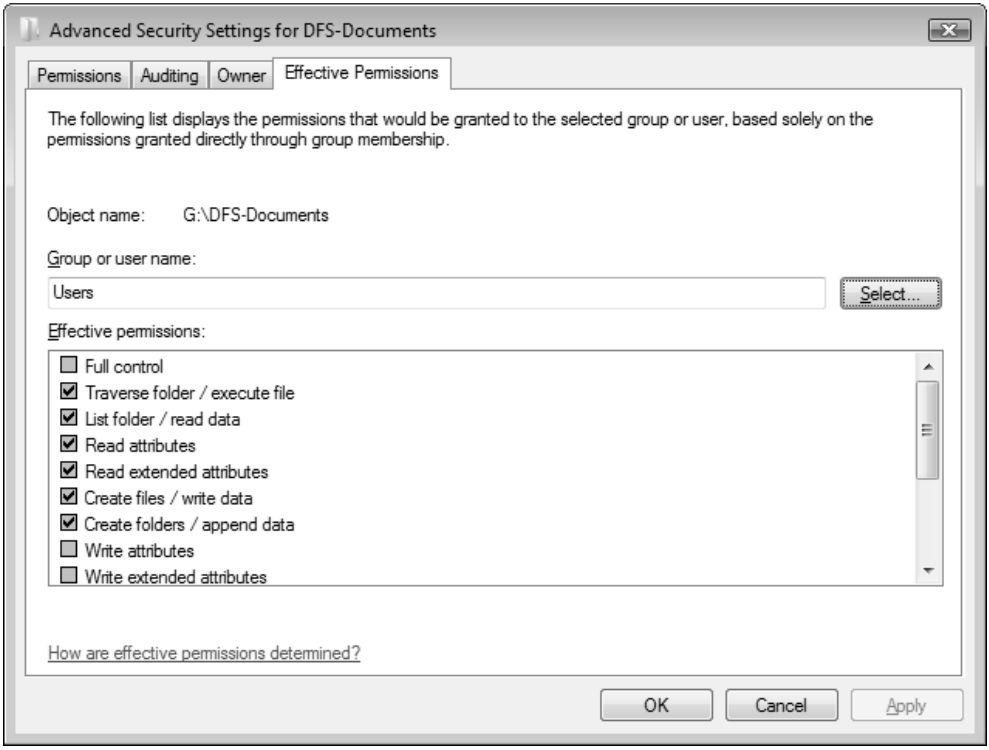


Рис. 14.18. На вкладке **Effective Permissions** отображаются все разрешения для выбранного пользователя или группы

Передача права владения

В системах Windows Server 2008 право владения файлом или папкой не является характеристикой, жестко привязанной к создателю данного объекта. Пользователь, создавший файл или папку, становится *владельцем* этого объекта. Однако при необходимости владельцем файла может стать администратор или пользователь с аналогичными правами, и, кроме того, право владе-

ния может быть передано другому пользователю — это может сделать пользователь, имеющий разрешение на смену владельца (право Take Ownership (Смена владельца)).

Кроме того, с помощью локальных или доменных групповых политик можно указывать, какие пользователи *всегда* могут становиться владельцами файлов или других объектов (по умолчанию такое право имеют только администраторы), при этом они могут даже не иметь никаких других разрешений для этого объекта.

Совет

Из вышесказанного следует административное правило получения разрешений на любой недоступный объект (в том числе для объектов, у которых ошибочно удалены *все* разрешения): нужно стать его владельцем, а затем установить нужные разрешения для себя или других пользователей и групп.

Рис. 14.19. Вкладка **Owner** диалогового окна **Advanced Security Settings**

Для передачи владения объектом файловой системы или для просмотра текущего владельца файла или папки откройте соответствующее окно свойств, перейдите на вкладку **Security** (Безопасность) и нажмите кнопку **Advanced** (Дополнительно). В окне **Advanced Security Settings** (Дополнительные параметры безопасности) (см. рис. 14.14 или 14.18) перейдите на вкладку **Owner** (Владелец). Текущий владелец объекта виден в поле **Current owner** (Текущий владелец). После нажатия кнопки **Edit** (Изменить) откроется окно, где владельца можно поменять (см. рис. 14.19).

В этом окне видны учетные записи, по умолчанию имеющие право получения во владение данного объекта файловой системы. Для смены владельца выделите учетную запись пользователя, которому вы хотите передать право владения, и нажмите кнопки **Apply** (Применить) и **OK**. Если право владения нужно передать какому-то другому, то нужно нажать кнопку **Other users or groups** (Другие пользователи или группы) и воспользоваться стандартной процедурой поиска учетных записей (см. рис. 14.12) — имя найденного пользователя или группы появится в окне потенциальных владельцев (рис. 14.19), где его следует выбрать и закончить операцию, нажав кнопку **ОК**.

Аудит событий в локальной системе

Аудит (audit) — это процесс, позволяющий фиксировать некритические события, происходящие в операционной системе и имеющие отношение к ее поведению, в первую очередь — к безопасности: например, регистрация в системе или попытки создания объекта файловой системы, получения к нему доступа или удаления. Мониторинг таких событий (помимо "стандартных" событий, регистрирующихся в системных журналах) может быть важен для анализа изменений в состоянии системы в процессе ее эксплуатации.

При настройке аудита администратор сам выбирает, какие события должны отслеживаться. Информация о таких событиях будет заноситься в обычный *журнал событий* операционной системы. Каждая запись журнала хранит данные о типе выполненного действия, пользователе, выполнившем его, а также о дате и моменте времени выполнения данного действия. Полученную в результате информацию (журнал Security (Безопасность)) можно просматривать с помощью традиционной оснастки **Event Viewer** (Просмотр событий).

Аудит позволяет отслеживать как успешные, так и неудачные попытки выполнения определенного действия, поэтому при просмотре журнала событий

можно выяснить, кто предпринял попытку выполнения неразрешенного ему действия.

Настройка аудита может выполняться как в один, так и в два приема:

1. Сначала аудит следует активизировать с помощью оснасток **Local Security Settings** (Локальная политика безопасности) или **Group Policy Object Editor** (Редактор объектов групповой политики). (Хотя в системах Windows Server 2008 аудит по умолчанию выключен, в журнале безопасности все равно регистрируется много событий.) При этом необходимо определить набор (тип) отслеживаемых событий. Это могут быть, например, вход и выход из системы, попытки получить доступ к объектам файловой системы и т. д. Для многих *системных* событий достаточно одной этой операции активизации аудита, и их регистрация в журнале начинается немедленно.
2. На втором шаге следует указать, какие конкретно объекты необходимо подвергнуть аудиту, и для каких групп или пользователей он будет осуществляться. Эта операция выполняется в окне свойств этих объектов, где задаются разрешения на доступ (для этого редактируются так называемые *списки управления доступом* (Access Control List, ACL) — *см. далее*). Для разных объектов — файлов, реестра или объектов каталога Active Directory — используемый при этом пользовательский интерфейс будет различаться, но несущественно.

Включение аудита

Для активизации аудита на автономном компьютере (или компьютере — члене рабочей группы) выполните следующие действия:

1. Запустите оснастку **Local Security Settings (**Локальная политика безопасности). Можно также воспользоваться оснасткой **Group Policy Object Editor** (Редактор объектов групповой политики) (введите в командной строке gpedit.msc).
2. На панели структуры откройте узел **Local Policies** | **Audit Policy** (Локальные политики | Политика аудита) (рис. 14.20).
3. На правой панели отображается список имеющихся политик аудита. Выполните двойной щелчок на имени изменяемой политики аудита — появится диалоговое окно, с помощью которого можно разрешить или запретить аудит (см. рис. 14.20). В группе **Audit these attempts** (Вести аудит

следующих попыток доступа) установите флажки **Success** (Успех) или **Failure** (Отказ) или оба.

4. Нажмите кнопку **OK**.

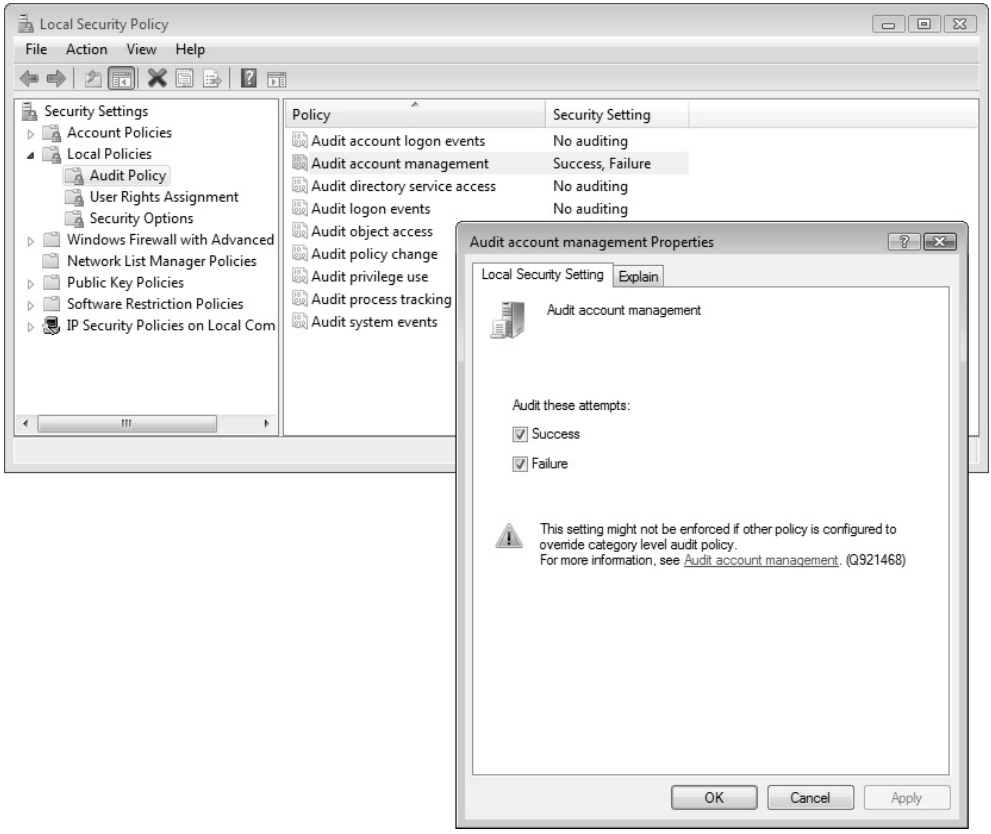


Рис. 14.20. Настройка политик аудита на локальном компьютере

Подобную операцию следует повторить для тех политик аудита, которые вы хотите активизировать. Для того чтобы отключить аудит, флажки **Success** (Успех) и **Failure** (Отказ) следует снять.

Операция включения аудита для компьютеров, входящих в домен, будет аналогичной — только нужно будет сначала выбрать объект групповых политик (GPO), связанный с доменом или организационным подразделением (OU) *(см. главу 13)*.

Настройка и просмотр параметров аудита для папок и файлов

Для того чтобы настроить, просмотреть или изменить параметры аудита файлов и папок, нужны следующие действия:

1. В окне программы Windows Explorer (Проводник) выберите файл или папку, откройте окно свойств и перейдите на вкладку **Security** (Безопасность).

   Внимание!

   Нужно помнить, что аудит доступа к файлам и папкам возможен только на томах NTFS.

2. На вкладке **Security** (Безопасность) нажмите кнопку **Advanced** (Дополнительно), а затем откройте вкладку **Auditing (**Аудит). Обычно эта вкладка пуста. Если нужно проводить (включить) аудит для пользователя или группы, нажмите кнопку **Edit** (Изменить), а в открывшемся окне (рис. 14.21) — кнопку **Add** (Добавить).

3. При добавлении записей, для которых будет вестись аудит, появляется диалоговое окно **Select Users, Computers or Groups** (Выбор: "Пользователи", "Компьютеры" или "Группы") (см. рис. 14.12). Выберите нужную учетную запись и нажмите кнопку **OK**. Откроется окно **Auditing Entry** (Элемент аудита) (рис. 14.22), где нужно установить все требуемые параметры аудита. В списке **Apply onto** (Применять) укажите, где следует выполнять аудит (это поле ввода доступно только для папок). На панели **Access** (Доступ) необходимо указать, какие события нужно отслеживать: окончившиеся успешно (**Successful** (Успех)), неудачно (**Failed** (Отказ)) или оба типа событий. Флажок **Apply these auditing entries to objects and/or containers within this container only** (Применять этот аудит к объектам и контейнерам только внутри этого контейнера) определяет, нужно ли распространять введенные настройки аудита на файлы и папки, находящиеся только в выбранной папке (не глубже).

   По умолчанию аудит будет распространяться на все вложенные объекты. В противном случае установите этот флажок (или выберите в списке **Apply onto** (Применять) опцию **This folder only** (Только для этой папки)). Это позволит не выполнять аудит для тех вложенных объектов файловой системы, которые не представляют интереса. После завершения настройки

аудита для папки или файла нажмите несколько раз кнопку **OK**, чтобы закрыть все диалоговые окна.

4. Если требуется просмотреть или изменить настройки аудита для уже существующего пользователя или группы, нажмите кнопку **Edit** (Изменить) (см. рис. 14.21). Появится окно **Auditing Entry** (Элемент аудита), где можно редактировать параметры аудита для выбранной учетной записи. По окончании внесения изменений закройте все окна свойств.

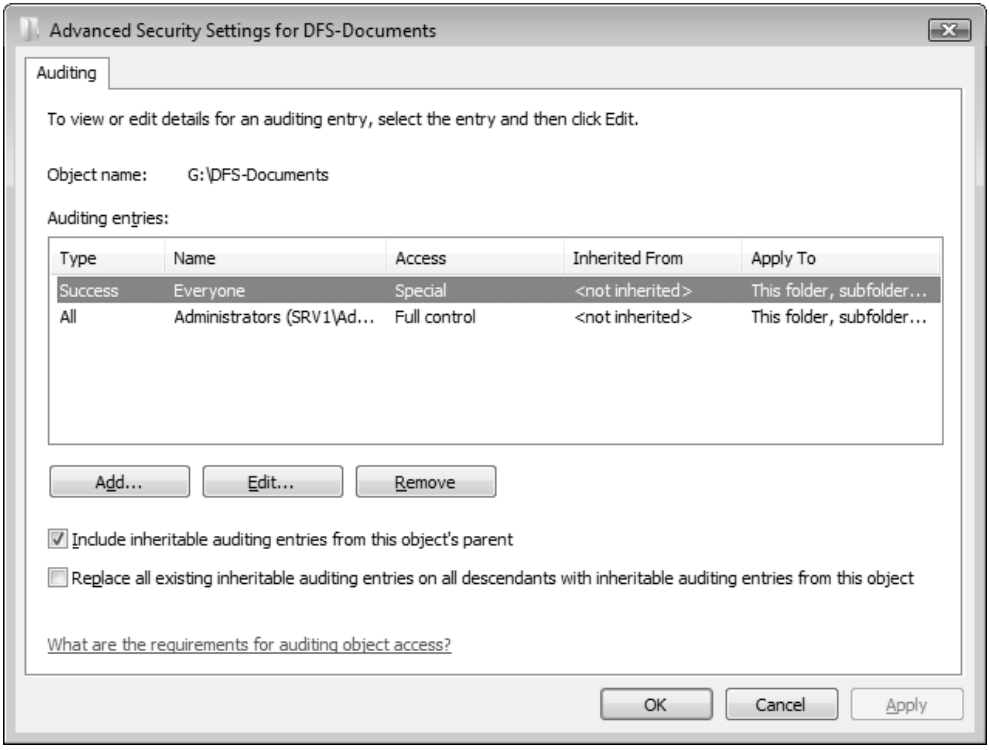


Рис. 14.21. Определение учетных записей и операций, для которых будет выполняться аудит для выбранной папки

После всех выполненных действий все события доступа к выбранным объектам файловой системы будут регистрироваться в журнале безопасности, для которого лучше создать настраиваемое представление, фильтрующие нужные события *(см. разд. "Фильтрация событий" главы 5)*.

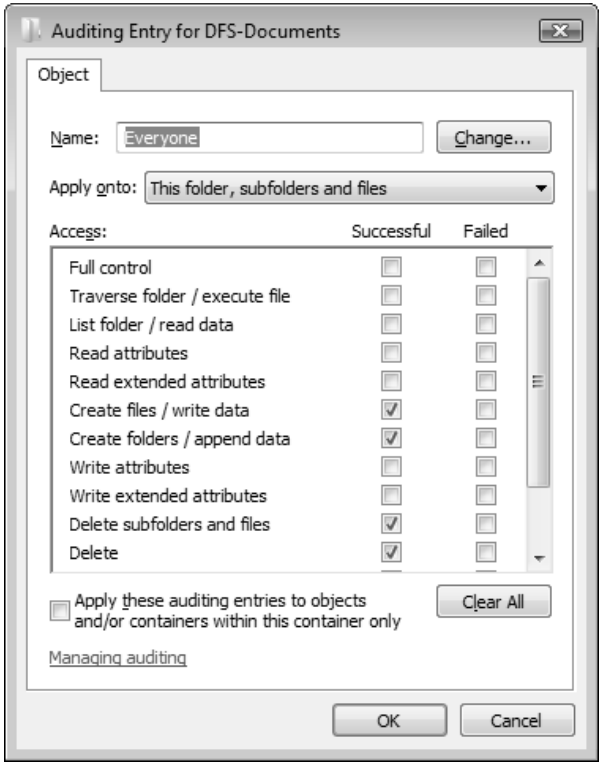


Рис. 14.22. Определение событий, аудит которых будет вестись для выбранных учетных записей (пользователей или групп)

Отключение аудита

Чтобы отключить аудит для файла или папки, достаточно удалить все записи аудита в окне дополнительных параметров (см. рис. 14.21). Если кнопка **Remove** (Удалить) недоступна, это значит, что настройки аудита наследуются от родительской папки, и нужно менять иерархию наследования (т. е. изменять параметры аудита *родительских* объектов).

Криптозащита папок и файлов, хранящихся на жестком диске

Для обеспечения конфиденциальности информации, хранящейся на жестком диске, в системах Windows, начиная с Windows 2000, используется *Encrypting*

File System (EFS) (Шифрованная файловая система), работающая только на томах NTFS.

> ***Примечание***
>
> Для шифрования целых дисков в системах Windows Vista и Windows Server 2008 также можно использовать компонент BitLocker Drive Encryption (Шифрование диска BitLocker), для работы которого требуется аппаратный Trusted Platform Module (TPM; Доверенный платформенный модуль).

Система EFS позволяет пользователю шифровать свои файлы без всякого вмешательства со стороны администратора: она автоматически генерирует для пользователя пару ключей (открытый и личный), применяемых для криптозащиты данных, и создает сертификат для операций шифрования. Исключается необходимость предварительного расшифровывания данных при доступе к ним. Операции шифрования и дешифрования выполняются автоматически, "на лету", при записи или считывании информации. Шифрование и дешифрование файлов может быть выполнено как для определенных файлов, так и для всей папки. Таким образом, криптозащита данных прозрачна для пользователя.

> ***Внимание!***
>
> Нельзя шифровать сжатые файлы и папки (и наоборот — нельзя сжимать зашифрованные данные). Выбор одной операции приведет к автоматической отмене другой.
>
> Шифрование папок или файлов не защищает их от удаления или просмотра содержимого папок. Поэтому при необходимости нужно сочетать шифрование с установкой соответствующих разрешений доступа на уровне файловой системы NTFS.

Если зашифрованные файлы будут использоваться совместно с другими пользователями, то владелец файлов должен сам добавить сертификаты тех пользователей, которым он разрешает доступ к этим данным. Впоследствии каждый полномочный пользователь может при необходимости независимо расшифровать файл при помощи своего личного ключа.

Обязательные требования при выполнении операций шифрования

Самая серьезная ошибка при работе с EFS возникает после переустановки операционной системы на компьютере, где пользователи шифровали данные,

но не выполнили дополнительных операций по сохранению сертификатов. В этом случае ***данные будут безвозвратно утеряны***, поскольку ранее доступ к ним имели только два пользователя той системы, в которой данные были зашифрованы: пользователь, выполнивший эту операцию, и так называемый *агент восстановления* (Data Recovery Agent) — пользователь, имеющий право расшифровать информацию. Ошибка состоит в том, что для расшифровки данных необходимо предъявить сертификаты одного из названных пользователей, а для этого эти сертификаты нужно было заранее экспортировать и сохранить.

Примечание

Создать сертификат и ключ для агента восстановления EFS можно в окне командной строки при помощи команды `cipher /R`. Администратор может использовать созданные файлы для определения политики восстановления *(см. разд. "Параметры безопасности (Security Settings)" главы 13)*.

Для того чтобы избежать ошибок, связанных с отсутствием экспортированного сертификата пользователя, зашифровавшего информацию, в системах Windows Vista/Windows Server 2008 предусмотрены дополнительные меры по защите от подобных ситуаций. Рассмотрим их работу на конкретном примере.

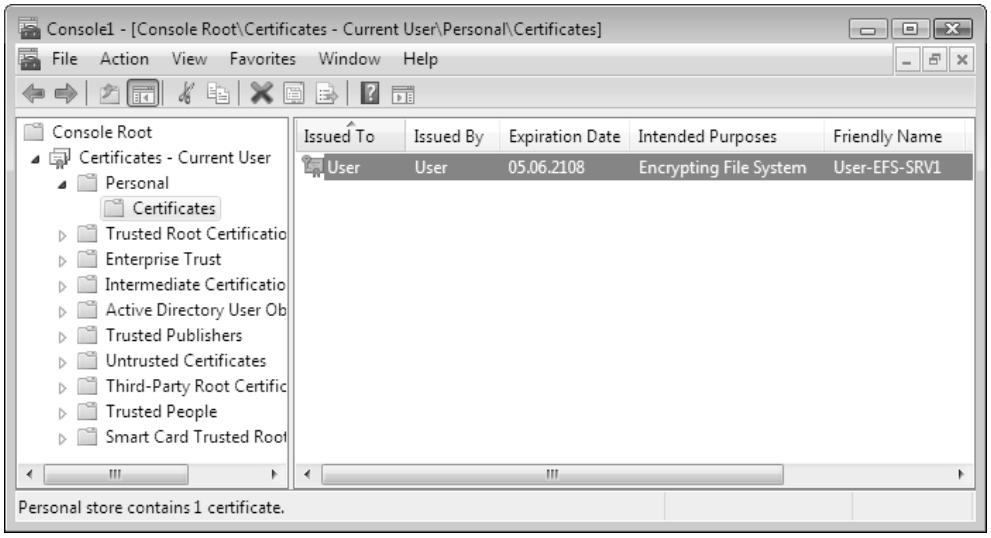


Рис. 14.23. Сертификат, выданный пользователю для выполнения операции шифрования данных

Примечание

Управление сертификатами, их импорт и экспорт осуществляются с помощью оснастки **Certificates** (Сертификаты) (эту оснастку можно добавить к любой консоли MMC — *см. главу 3*). Пользователи могут управлять только своими собственными сертификатами. На рис. 14.23 приведен пример окна оснастки, в котором можно видеть личные сертификаты пользователя — в частности, сертификат, который система автоматически выдала пользователю (от его имени) при первом выполнении операции шифрования файла или папки (см. рис. 14.25). Назначение сертификата отображается в соответствующем столбце (Intended Purposes).

Шифрование файлов и папок

Поскольку операция шифрования выполняется автоматически и "прозрачно" для пользователя, работа с файлом может продолжаться так же, как и до включения криптозащиты. Например, можно, как и прежде, открыть текстовый документ и отредактировать его. Все остальные пользователи, которые попытаются получить доступ к зашифрованному файлу, получат сообщение об ошибке доступа, поскольку они не владеют необходимым личным ключом, позволяющим им расшифровать файл.

Внимание!

Рекомендуется шифровать папки (со всем их содержимым), а не отдельные файлы. В этом случае уменьшается риск того, что окажется доступным расшифрованное содержимое файла (например, при его копировании в незашифрованную папку).

Операция шифрования/дешифрования информации выполняется в окне программы Windows Explorer (Проводник) и выглядит следующим образом:

1. Выберите файл или папку, которую требуется зашифровать, нажмите правую кнопку мыши и выберите в контекстном меню команду **Properties** (Свойства).
2. В появившемся окне свойств на вкладке **General** (Общие) нажмите кнопку **Advanced** (Другие). Откроется диалоговое окно **Advanced Attributes** (Дополнительные атрибуты) (рис. 14.24).
3. В группе **Compress or Encrypt attributes** (Атрибуты сжатия и шифрования) установите флажок **Encrypt contents to secure data** (Шифровать со-

держимое для защиты данных) и нажмите кнопку **OK**. (Соответственно, для дешифрования необходимо снять этот флажок.)

4. Нажмите кнопку **OK** в окне свойств зашифровываемого файла или папки. В появившемся диалоговом окне подтвердите режим выполнения операции.

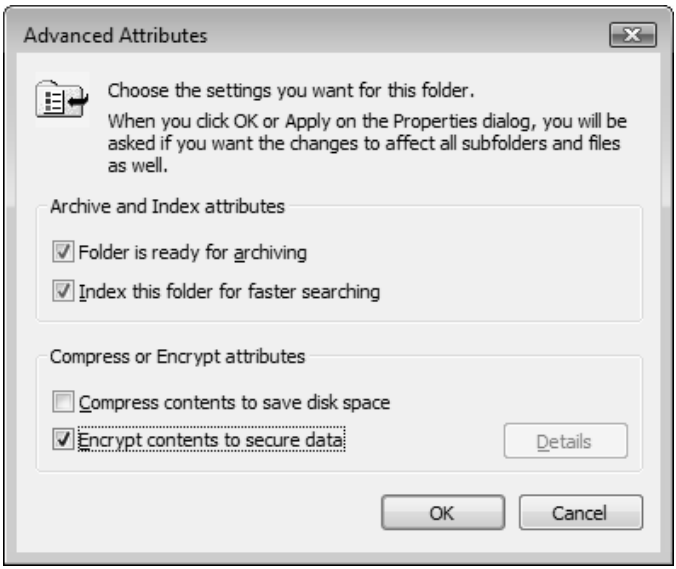


Рис. 14.24. Окно дополнительных атрибутов файла или папки

При шифровании папки можно указать следующие режимы:

- **Apply changes to this folder** (Применение изменений только к этой папке).
- **Apply changes to this folder, subfolders and files** (К этой папке и всем вложенным папкам и файлам).

> ***Примечание***
>
> Если выбрать для шифрования отдельный файл, система предложит зашифровать также папку, в которой тот находится. Это делать необязательно, однако при копировании файл может "потерять" атрибут "шифрованный". Имена зашифрованных файлов и папок в окне Проводника отображаются зеленым цветом.

Если операция шифрования выполнялась на компьютере, не являющемся членом домена, то после того как окно свойств шифруемого объекта будет

закрыто, на панели задач в области уведомлений появится значок и всплывающее окно предупреждения о необходимости сохранения ключа шифрования EFS (рис. 14.25). (Это предупреждение появляется только при первом выполнении операции шифрования данных, и значок не исчезнет с панели до тех пор, пока не будет выполнено требование.) Сохранить ключ можно при помощи специальной программы-мастера или вручную, экспортировав свой сертификат с помощью оснастки **Certificates** (Сертификаты) *(см. далее)*.

Рис. 14.25. Предупреждение шифрованной файловой системы EFS

Рис. 14.26. Запрос на экспорт ключа EFS

Если щелкнуть по значку EFS на панели задач, то появится окно, в котором нужно выбрать опцию **Back up now** (Архивировать сейчас) (рис. 14.26). В этом случае запустится мастер *Certificate Export Wizard* (Мастер экспорта сертификатов), с помощью которого легко выполнить требуемую операцию сохранения личного ключа.

Мастер экспорта попросит указать параметры экспортируемой информации (рис. 14.27), пароль для защиты личного ключа и имя файла, в котором будет записан сертификат. Нужно понимать, что этот файл будет ключом к любой информации, шифруемой пользователем, поэтому его нужно соответствующим образом хранить и запоминать на дискете или съемном носителе. После подтверждения правильности выбранных характеристик операция экспорта будет выполнена. Теперь значок на панели задач и предупреждение о необходимости сохранения ключа больше появляться не будут.

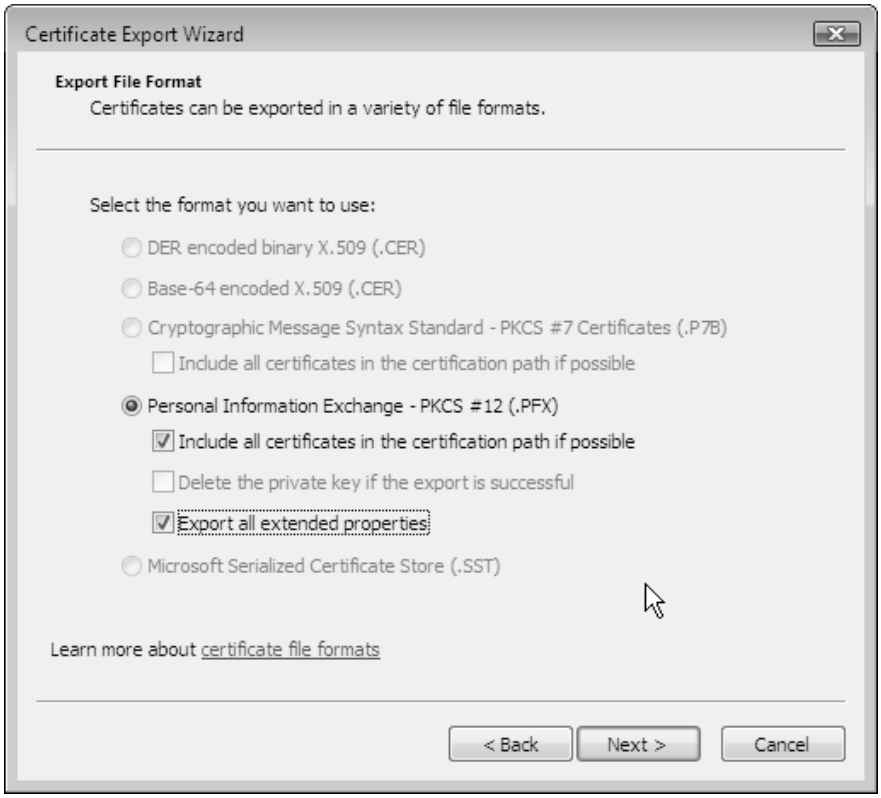


Рис. 14.27. Параметры экспортируемого ключа EFS

Теперь при необходимости сохраненный сертификат можно при помощи оснастки **Certificates** (Сертификаты) и операции импорта установить в любой системе и использовать для дешифрования данных.

> ***Примечание***
>
> Для шифрования/дешифрования файлов и папок можно использовать утилиту командной строки *cipher.exe*. Запущенная без параметров, эта утилита покажет состояние для всех файлов в текущей папке — какие из них зашифрованы, а какие нет, и будут ли шифроваться файлы, помещенные в эту папку.

Шифрование файлов для совместного использования

Системы Windows Server 2008 (как и Windows XP) поддерживают совместный доступ к зашифрованным *файлам*[1], расположенным на общих сетевых ресурсах или на локальных дисках. Дополнительные разрешения можно давать только для каждого отдельного файла.

> ***Внимание!***
>
> Перед тем как разрешать совместный доступ к зашифрованным файлам, необходимо предварительно импортировать сертификат нового пользователя *(см. далее разд. "Экспорт сертификата и восстановление зашифрованных файлов на другом компьютере")*.

После того как владелец-создатель зашифровал папку со вложенными файлами или отдельный файл, он может снова открыть окно **Advanced Attributes** (Дополнительные атрибуты) (см. рис. 14.24) и нажать кнопку **Details** (Подробно). Появится окно, аналогичное изображенному на рис. 14.28. Здесь перечислены все пользователи (включая владельца файла), которым разрешен доступ к файлу. (Можно указывать учетные записи локального компьютера или доменных пользователей.)

Чтобы расширить круг полномочных лиц, нужно нажать кнопку **Add** (Добавить) и в открывшемся окне (рис. 14.29) указать, какие пользователи смогут также работать с зашифрованным файлом.

---

[1] Подчеркнем — совместный доступ к зашифрованным *папкам* разрешать нельзя.

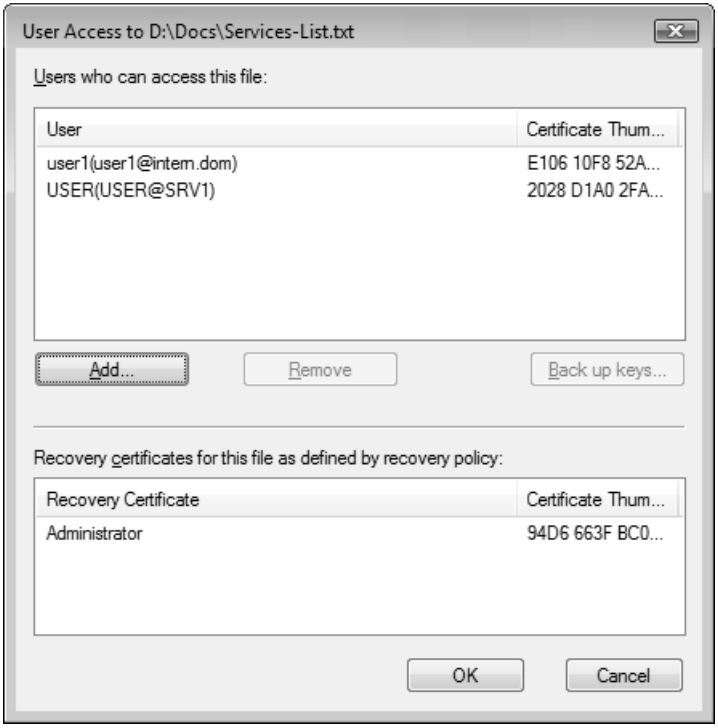


Рис. 14.28. Список пользователей, имеющих доступ к зашифрованному файлу

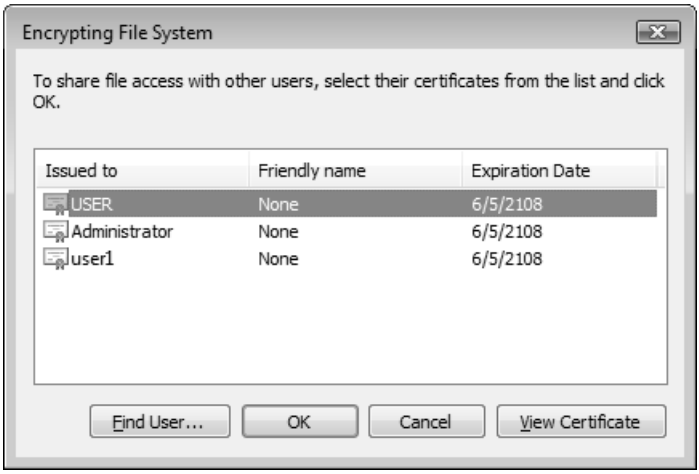


Рис. 14.29. Данное окно позволяет выбрать пользователя и просмотреть его сертификат

В этом окне можно запросить просмотр имеющихся сертификатов пользователей, а также найти сертификаты пользователей в каталоге Active Directory (если компьютер подключен к домену и сертификаты опубликованы в каталоге).

Копирование, перемещение, переименование и уничтожение зашифрованных файлов и папок

Операции копирования, перемещения, переименования и уничтожения зашифрованных файлов и папок выполняются точно так же, как и с незашифрованными объектами. Однако следует помнить, что пункт назначения зашифрованной информации (целевая папка или том) должен поддерживать шифрование (т. е. должен иметь файловую систему NTFS). В противном случае при копировании данные будут расшифрованы, и копия будет содержать открытую информацию.

Архивация зашифрованных файлов

Резервную копию зашифрованного файла можно создать путем его обычного копирования на другой жесткий диск или с использованием утилиты архивации. Однако, как сказано выше, простое копирование, например, на дискету, на раздел FAT или оптический диск может привести к тому, что резервная копия будет содержать открытые данные, доступные для чтения любому пользователю.

Специализированная операция архивации не требует для ее выполнения доступа к открытым ключам пользователя — только к архивируемой информации. Поэтому для обеспечения безопасности конфиденциальных данных при создании резервных копий рекомендуется применять стандартные средства архивации, описанные в *главе 15*. В процессе архивации зашифрованные данные будут скопированы на указанный носитель без дешифрования.

Экспорт сертификата и восстановление зашифрованных файлов на другом компьютере

Если система не предложила автоматически экспортировать сертификат, выдаваемый пользователю при выполнении первой операции шифрования

файла или папки *(см. ранее разд. "Шифрование файлов и папок")*, то эту операцию следует выполнить вручную, чтобы не подвергнуть риску утраты зашифрованные данные (например, в случае краха и переустановки системы).

Кроме того, иногда возникает необходимость восстановить зашифрованную информацию *не на том* компьютере, на котором она была заархивирована. Это можно выполнить с помощью утилиты архивации, которая сохраняет информацию в зашифрованном виде вместе с атрибутом шифрования. Однако нужно позаботиться о переносе на новый компьютер соответствующего сертификата и личного ключа пользователя либо с помощью перемещаемого профиля, либо вручную.

На любом компьютере, где зарегистрировался пользователь, обладающий *перемещаемым* профилем, будут применяться одни и те же ключи шифрования.

Ручной перенос личного ключа и сертификата выполняется в два этапа: сначала следует создать резервную копию сертификата и личного ключа, а затем восстановить созданную копию на другом компьютере.

Примечание

Для экспорта сертификатов, использованных для шифрования файлов, можно также использовать простую программу-мастер (рис. 14.30), которая запускается из окна управления параметрами учетной записи пользователя (см. рис. 4.3).

Создание резервной копии любого сертификата (*экспорт* сертификата) состоит из следующих шагов:

1. Запустите оснастку **Certificates** (Сертификаты) (см. рис. 14.23).
2. В левом подокне оснастки откройте папку **Personal** (Личные), а затем папку **Certificates** (Сертификаты). В правом подокне появится список сертификатов, выданных пользователю.
3. Укажите переносимый сертификат и щелкните правой кнопкой мыши. (Для шифрования файлов нас интересует сертификат с назначением (Intended Purposes) Encrypting File System (Шифрующая файловая система (EFS)).) В появившемся контекстном меню выберите команду **All Tasks** (Все задачи). В ее подменю выберите команду **Export** (Экспорт). Запустится мастер *Certificate Export Wizard* (Мастер экспорта сертификатов).

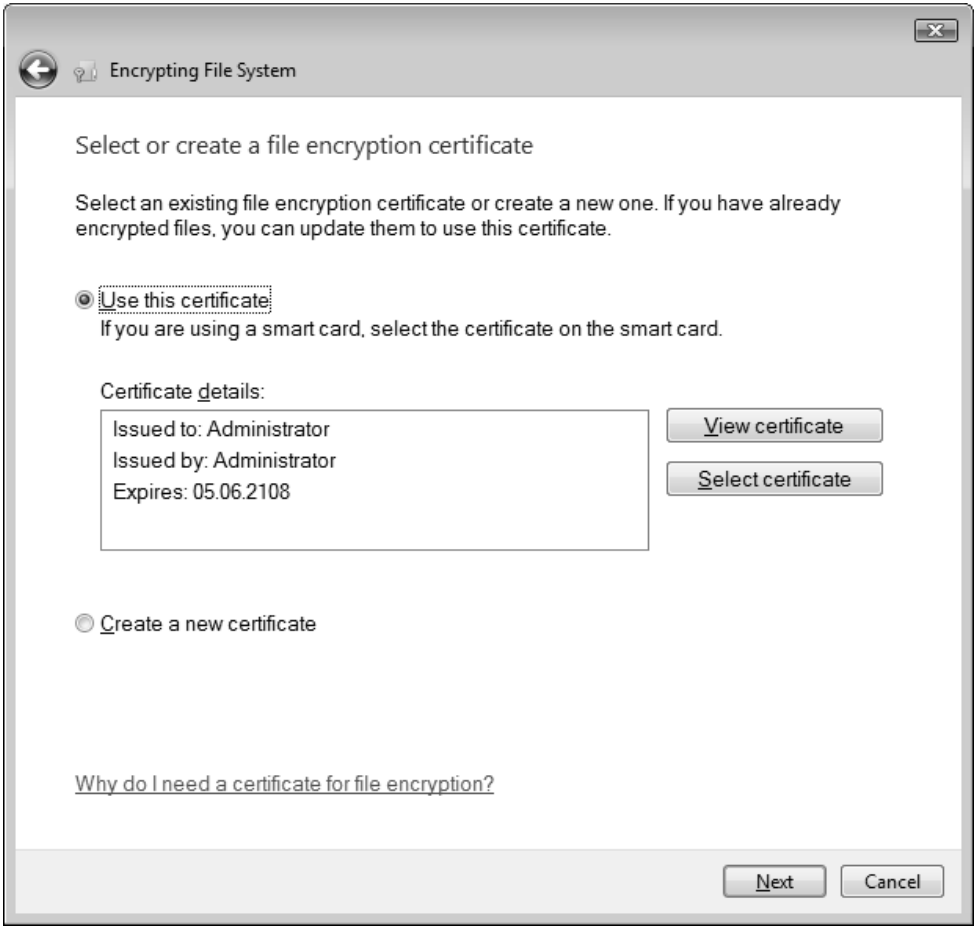


Рис. 14.30. Мастер управления сертификатами для текущей учетной записи пользователя

4. В окне мастера (обязательно!) выберите опцию **Yes, export the private key** (Да, экспортировать закрытый ключ) и нажмите кнопку **Next** (Далее).
5. На следующей странице мастера доступен только один формат (PFX), предназначенный для персонального обмена информацией. Нажмите кнопку **Next** (Далее).
6. Введите произвольный пароль, защищающий данные файла *.pfx, а также путь для сохранения файла; затем нажмите кнопку **Next** (Далее).

7. Проверьте список экспортируемых сертификатов и ключей — для выполнения операции нажмите кнопку **Finish** (Готово).
8. Завершите работу мастера экспорта нажатием кнопки **OK** в окне, сообщающем об успешном выполнении процедуры экспорта.

Внимание!

Операцию экспорта может выполнить только сам пользователь. Даже администратор не может экспортировать личный ключ другого пользователя (хотя он и может экспортировать все сертификаты, хранящиеся на компьютере — но без личных ключей).

Совет

Перед тем как экспортировать сертификат, выберите его в окне оснастки **Сертификаты** (Certificates), откройте окно свойств и дайте сертификату *понятное имя* (Friendly name), включающее имя пользователя и компьютера, а также назначение сертификата (EFS). Это позволит в дальнейшем (например, при импорте) не путаться в экспортированных сертификатах.

В результате сертификат и секретный ключ будут экспортированы в файл с расширением .pfx, который может быть скопирован на съемный носитель и перенесен на другой компьютер.

Для восстановления (*импорта*) сертификата из резервной копии:

1. Перенесите созданный на предыдущем этапе файл с расширением .pfx на компьютер, где вы планируете восстанавливать зашифрованные данные, и дважды щелкните по его имени — автоматически запустится мастер *Certificate Import Wizard* (Мастер импорта сертификатов).
2. Следуйте указаниям мастера — подтвердите имя и местоположение файла с расширением .pfx, а на следующей странице введите пароль защиты данного файла.
3. Подтвердите выбор хранилища на основе типа сертификата — восстановление данных из резервной копии будет выполняться в папку **Personal** (Личные). (Для импорта *личных* сертификатов всегда используется данная опция!)
4. Проверьте правильность параметров и для начала операции импорта нажмите кнопку **Finish** (Готово). После завершения процедуры импорта нажмите кнопку **OK** и закройте окно мастера импорта.

Импорт сертификатов на другом компьютере

Если вы передаете свой сертификат другому пользователю — например, для того, чтобы тот разрешил вам работать с зашифрованными файлами, — то процедура импорта будет немного отличаться от той, что описана выше.

При выборе хранилища (п. 3) необходимо выбрать опцию **Place all certificates in the following store** (Поместить все сертификаты в следующее хранилище) и, нажав кнопку **Browse** (Обзор), выбрать в списке хранилищ опцию **Trusted People** (Доверенные лица) (соответствующая папка видна на рис. 14.23). Затем импорт выполняется стандартным образом, как было описано выше.

Глава 15

Восстановление системы и данных

Для файловых серверов, да и для любых систем, всегда важна задача архивации пользовательских данных и файлов самой системы — на случай ее выхода из строя по каким-то причинам. Если отдельные файлы и папки можно просто скопировать на съемный носитель (особенно при помощи встроенных средств записи на DVD-диски), то с системными файлами это сделать гораздо сложнее (например, если необходимо сохранить реестр системы или базу данных каталога Active Directory). Поэтому необходимо пользоваться специальными средствами архивации и восстановления данных, которые имеются в системе.

Средства резервного копирования и восстановления информации в системах Windows Vista/Windows Server 2008 претерпели капитальное обновление по сравнению с предыдущими версиями Windows. Интерфейс программ архивации сильно изменился, некоторые возможности стали недоступны (нельзя, например, просто сохранить в архив отдельную папку или файл; выполняется только архивация дисков целиком, при этом файлы выбираются по типу). Эти программы, входящие в состав систем Windows Server 2008, существенно отличаются даже от Windows Vista по возможностям и внешнему виду.

Помимо средств архивации, в этой главе также описаны возможности восстановления системы при сбоях или в случае полного отказа жесткого диска.

Примечание

Для *восстановления ранее созданных архивов* на компьютерах, работающих под управлением Windows Server 2008, имеется утилита Windows NT Backup Restore Utility, которую можно свободно скачать из Центра загрузки Microsoft (см. ссылки в *приложении*). Для других целей ее использовать нельзя.

Установка системы архивации данных Windows Server

В системах Windows Server 2008 средства архивации и восстановления по умолчанию отсутствуют; для того чтобы ими можно было пользоваться, необходимо с помощью оснастки **Server Manager** (Диспетчер сервера) *(см. главу 3)* установить компонент *Windows Server Backup Features* (Возможности системы архивации данных Windows Server). Этот компонент содержит две опции:

- *Windows Server Backup* (Система архивации данных Windows Server) — включает управляющую оснастку MMC, утилиту командной строки Wbadmin.exe и сами службы архивации и восстановления;
- *Command-line Tools* (Программы командной строки) — утилиты, позволяющие создавать резервные копии по расписанию и управлять ими с помощью сценариев Windows PowerShell; этот компонент устанавливать необязательно.

С работой средств архивации и восстановления тесно связана функция, называемая *Previous Versions* (Предыдущие, или прежние, версии), — она будет рассматриваться далее в отдельном разделе. Ранее аналогичная возможность называлась *Shadow Copies* (Теневые копии).

При использовании программ архивации и восстановления с удаленными компьютерами нужно помнить о том, что для нормальной работы в брандмауэре Windows должно быть установлено исключение *Windows Backup* (Архивация Windows) (при установке компонента это делается автоматически, но иногда требуется контролировать этот момент).

Для использования средств архивации Windows Server нужно быть членом локальной группы Administrators (Администраторы) или группы Backup Operators (Операторы архива), при этом оснастку или утилиту Wbadmin нужно запускать с повышением полномочий (от имени администратора).

Система архивации Windows Server Backup использует для своей работы службу *Volume Shadow Copy Service* (VSS). После того как вначале создается полный архив (full backup), можно указать режим добавочной архивации (incremental backup, инкрементное резервное копирование). В этом случае будут сохраняться только те данные, которые изменялись после момента предыдущей архивации. Даже при использовании полных архивов система Windows Server Backup работает быстрее, чем службы архивации предыдущих версий.

Способы архивации и восстановления данных и системных файлов

Необходимость в восстановлении информации может возникнуть в результате разных причин — из-за ошибок в конфигурации системы, при запуске плохо написанной прикладной программы или при установке непроверенного драйвера. Также случаются ошибки при удалении информации (как пользователями сервера, так и администраторами). В случае полного выхода из строя жесткого диска теряются все данные, хранящиеся на нем. На каждый случай должны быть предусмотрены меры по восстановлению системы или информации.

В системах Windows Server 2008 набор средств, обеспечивающих архивацию и восстановление данных и системных файлов, минимален. Доступ ко всем возможностям обеспечивает оснастка **Windows Server Backup** (Система архивации данных Windows Server wbadmin.msc) и утилита командной строки Wbadmin.exe. Функции системы архивации Windows Server перечислены в табл. 15.1.

Таблица 15.1. *Возможности системы архивации данных в Windows Server 2008*

Сохраняемая информация	Используемое средство	Способ применения
Персональные файлы пользователей и данные прикладных программ	Архив тома	Необходимо периодическое сохранение всех созданных и измененных файлов. В частности, это рекомендуется делать перед модернизацией компьютера или установкой пакета обновлений (service pack)
Состояние системы (файлы системы и системных приложений, реестр, база данных Active Directory)	Архив состояния системы	Рабочее состояние системы нужно сохранять на случай серьезных отказов или ошибок при изменении конфигурации. Архив базы данных Active Directory может потребоваться при ошибочном удалении разделов или объектов каталога
Все содержимое физического диска (дисков)	Полный архивный образ системы (в Windows Vista он называется *Windows Complete PC*)	Имеет смысл сохранить состояние всех данных на компьютере на момент его полностью работоспособного состояния. Такая копия окажется полезной на случай полного выхода из строя компьютера или жесткого диска

Таблица 15.1 *(окончание)*

Сохраняемая информация	Используемое средство	Способ применения
Текущее содержимое файлов	Теневые копии (Shadow Copies)	Система может периодически делать "снимки" томов и сохранять их в служебной области диска. Пользователь может вернуться к версии файла, существовавшей ранее, на момент создания очередного снимка. По мере заполнения буферной области файлы удаляются, поэтому эта возможность не может гарантировать существование старых версий данных

В системах Windows Vista и Windows Server 2008 любую информацию можно архивировать на следующие носители:

- жесткие диски (внутренние и общие сетевые);
- съемные диски;
- записываемые и перезаписываемые DVD-диски.

Нельзя копировать архивы на ленту. Архивируются только тома, имеющие файловую систему NTFS.

Важной особенностью систем Windows Server 2008 является то, что для хранения резервных копий, создаваемых по расписанию, а также полного образа системы ***требуется отдельный выделенный диск*** (внутренний или съемный).

Примечание

В системах Windows Vista для автоматического или ручного сохранения состояния системы используются так называемые *точки восстановления* и функция *System Restore* (Восстановление системы). С их помощью периодически или перед выполнением важных обновлений сохраняется состояние всех важных системных файлов и параметров (включая реестр), и это состояние легко восстановить в случае ошибок в загрузке системы или при появлении нестабильности в работе (например, после неудачного редактирования реестра, установки непроверенных драйверов и т. п.). В серверных версиях Windows такая возможность не реализована.

Средства управления системой архивации в Windows Server 2008

Как уже говорилось, административные средства для управления программами архивации и восстановления в системах Windows Server 2008 кардинально отличаются от тех, которые имеются во всех предыдущих версиях Windows (включая Windows Vista[1]). Основным инструментом является оснастка **Windows Server Backup** (Система архивации данных Windows Server; wbadmin.msc) (ее аналог при работе в окне консоли или Windows Server Core — утилита Wbadmin.exe). Запуск оснастки осуществляется из подменю **Administrative Tools** (Администрирование).

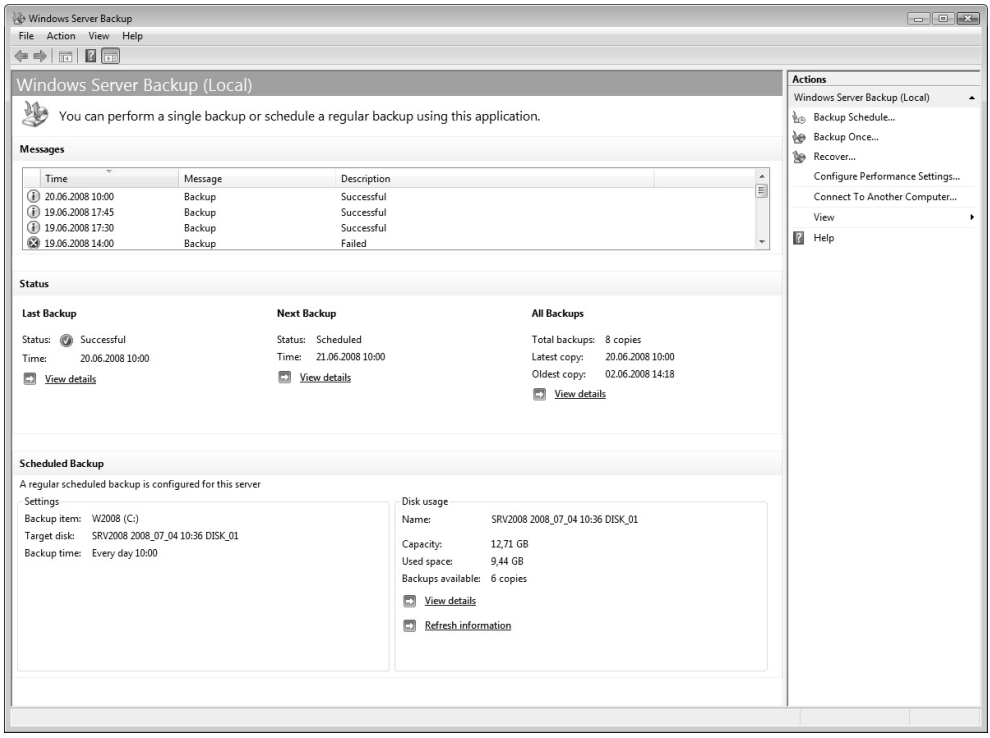


Рис. 15.1. Окно оснастки **Windows Server Backup**

[1] Нужно отметить, что по сравнению с Windows Vista, интерфейс средств управления стал более лаконичным, продуманным и интуитивно понятным.

Окно оснастки **Windows Server Backup** (Система архивации данных Windows Server) показано на рис. 15.1. В нем легко видеть текущее состояние служб — на панели **Status** (Состояние) отображается время последней и следующей операции архивации, количество выполненных операций и их результат (в поле **Messages**). Наличие запланированных архиваций и параметры используемого для этого физического диска показаны на панели **Scheduled Backup** (Архивация по расписанию).

Ссылки на панели **Actions** (Действия) позволяют запустить операции архивации и восстановления (они будут рассмотрены позже). Оснастку можно подключать к удаленному компьютеру.

Щелкнув по ссылке **Configure Performance Settings** (Настройка параметров производительности), можно перейти в окно, где указывается тип архивирования для каждого тома (рис. 15.2). При необходимости можно выбрать индивидуальные параметры в зависимости от нагрузки на конкретный диск.

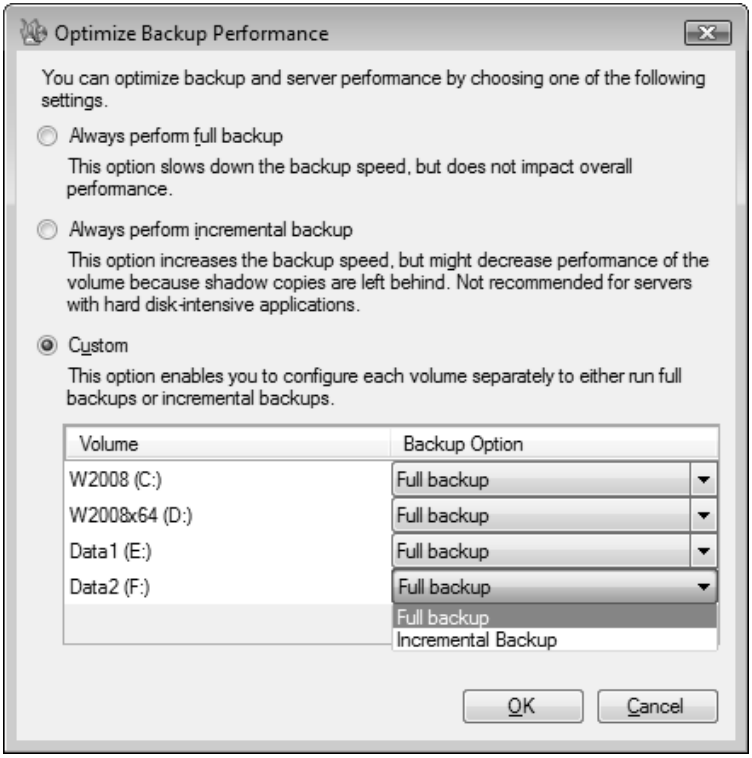


Рис. 15.2. Выбор типов архивации для конкретных томов

Выполнение операций архивации системы и данных

Сначала рассмотрим способы создания архивов, содержащих критические тома (которые содержат файлы, необходимые для загрузки системы, и компоненты самой системы) и некритические тома (данные пользователей и прикладных программ).

Создание полного образа системы или архива отдельных томов

Если система находится в рабочем состоянии и в ней установлены все необходимые прикладные программы, то имеет смысл сохранить полный образ системы со всей информацией, хранящейся на локальных дисках. При выходе компьютера из строя образ системы легко можно восстановить на компьютере с аналогичной аппаратной конфигурацией. Разумеется, для сохранения полного архива потребуется жесткий диск большого объема.

> ***Примечание***
>
> В системах Windows Server 2008 нет отдельной операции по сохранению полного образа системы (как функция Windows Complete PC в Windows Vista). Необходимо просто при создании архива указать опцию **Full server** (Весь сервер). При восстановлении системы программа-мастер сама поймет, можно ли из имеющихся архивов выполнить полное восстановление сервера.

Чтобы создать образ системы или архив отдельных томов, выполните следующие операции:

1. В окне оснастки **Windows Server Backup** (Система архивации данных Windows Server) (см. рис. 15.1) выберите ссылку **Backup Once** (Однократная архивация). Запустится мастер *Backup Once Wizard* (Мастер однократной архивации), который поможет выбрать все нужные параметры.
2. Мастер может использовать параметры, определенные для архивации по расписанию (в этом случае можно соглашаться с установленными параметрами или корректировать их), или другие, заданные для конкретной операции — необходимо сделать соответствующий выбор. (Далее будет рассматриваться ситуация, когда планируемых операций нет.)

3. На следующем этапе указывается, какой архив будет создаваться — полный образ системы (опция **Full Server**) или архив отдельных томов (опция **Custom**) (рис. 15.3). Образ всей системы будет занимать значительный объем, и это нужно учитывать при выборе целевой папки или носителя.

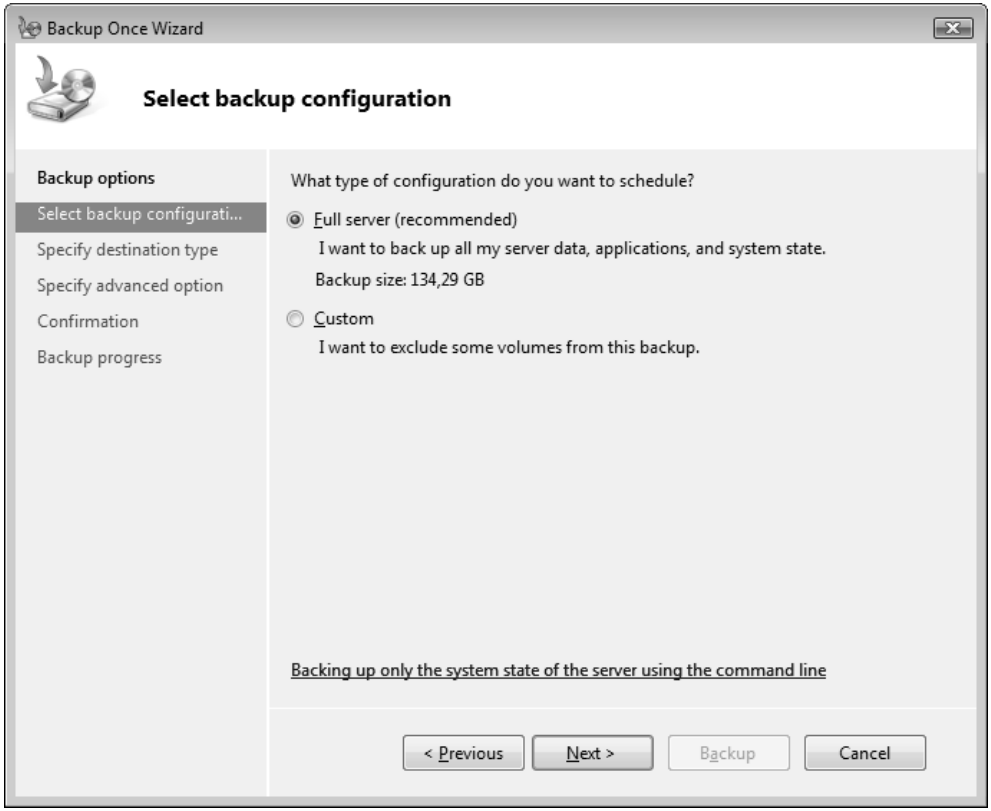


Рис. 15.3. Выбор типа архива — полный образ системы или архив отдельных томов

4. При выборе опции **Custom** (Настраиваемый) можно указать, какие именно диски войдут в состав архива (рис. 15.4). По умолчанию установлен флажок **Enable system recovery** (Включить восстановление системы) — в этом случае в архив войдут все компоненты операционной системы и файлы, необходимые для загрузки. Если флажок снять, то можно архивировать только некритические тома.

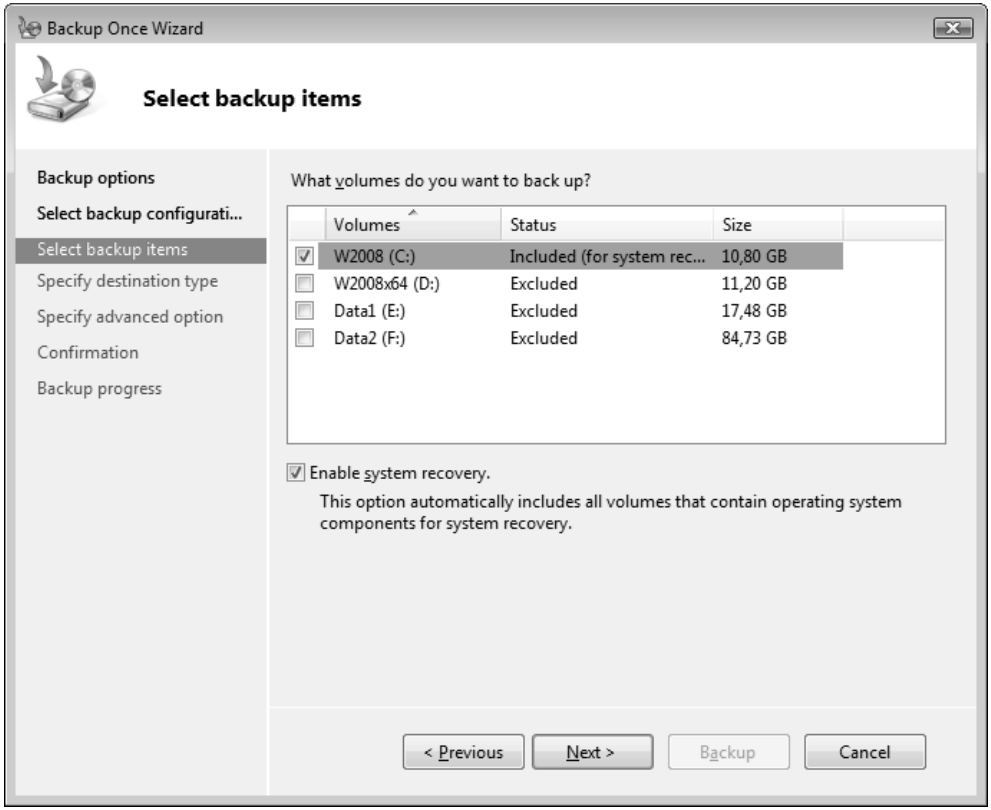


Рис. 15.4. Список дисков, которые будут включены в образ системы

5. Затем программа предложит выбрать для записи образа один из локальных дисков (жесткий диск или DVD-привод) или удаленную общую сетевую папку — выберите нужный вариант. (Архив нельзя сохранять на том же диске, который будет включен в его состав; следовательно, при наличии единственного раздела (логического диска) или тома создание архива возможно только на DVD-дисках или в сети.)

6. На следующем шаге нужно указать тип архива службы Volume Shadow Copy Service (VSS). Если в системе нет других программ для архивации данных, то можно выбрать опцию **VSS full backup** (Полная архивация VSS).

7. На завершающем шаге проверьте правильность выбора параметров архивации и нажмите кнопку **Backup** (Архивировать). После этого начнется

теневое копирование выбранных дисков в указанное место. За ходом процесса можно следить в окне мастера (рис. 15.5). Это окно можно закрыть, и тогда за выполнением операции можно следить в окне оснастки на панели **Messages** (Сообщения).

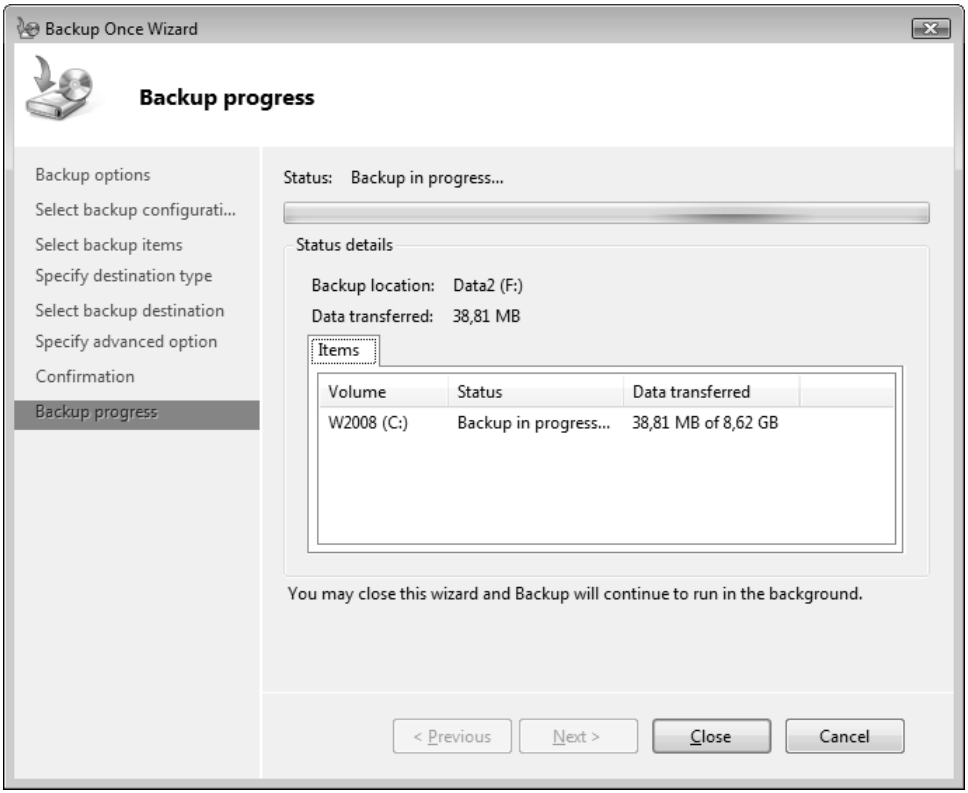


Рис. 15.5. Отображение процесса архивации

После выполнения операции на целевом диске создается папка WindowsImageBackup, содержащая подкаталог, имя которого соответствует имени архивируемого компьютера, а внутри него — папка с файлами архива. В имени этой папки фигурируют дата создания архива и служебный код.

Примечание

Поскольку теперь в системах Windows Vista/Windows Server 2008 отсутствуют стандартные средства архивации *отдельных* файлов и папок, то

для создания копий важных данных остаются два средства: встроенные возможности записи DVD-дисков и утилита *Robocopy.exe*, обладающая очень эффективными и развитыми возможностями по копированию файлов. С ее помощью легко копировать файлы из одной папки в другую (при этом можно копировать только измененные файлы или файлы с заданными свойствами), а также можно обеспечивать "синхронизацию" содержимого двух папок.

Автоматическая архивация томов

Автоматическое резервное копирование критических и некритических томов выполняется программой архивации в соответствии с заданным расписанием. Особенностью систем Windows Server 2008 является то, что в этом режиме для хранения архивов должен использоваться ***отдельный*** внутренний или внешний жесткий диск (DVD-диски или общие сетевые папки выбирать нельзя). Этот диск не виден в окне программы Windows Explorer (Проводник) и применяется только в целях архивации и восстановления данных.

Для настройки режима архивации по расписанию выполните следующие действия:

1. В окне оснастки **Windows Server Backup** (Система архивации данных Windows Server) (см. рис. 15.1) выберите ссылку **Backup Schedule** (Расписание архивации). Дальнейшие действия будет направлять мастер *Backup Schedule Wizard* (Мастер расписания архивации).
2. Как и при однократной архивации, необходимо указать — весь сервер будет копироваться или только отдельные тома.
3. В случае архивации отдельных томов нужно выбрать те тома, которые будут включены в архив.
4. Выберите расписание для выполнения процедуры автоматической архивации (рис. 15.6) (это расписание впоследствии можно менять в любой момент); в течение одного дня операция может выполняться многократно. В первый раз, когда будет создаваться полная копия данных, процедура потребует много времени. При последующих запусках копируются только новые или измененные файлы. При выборе расписания нужно исходить из критерия оптимальности: частое выполнение операции будет мешать работе, а при редком запуске "возраст" каждой версии архива будет слишком большим — данные в архиве окажутся слишком старыми.

5. Теперь необходимо указать физический диск для хранения архива. В начальный момент мастер сообщает, что не найдены внешние диски или диски, подключенные к портам USE или FireWire. Нужно нажать кнопку **Show All Available Disks** (Показать все доступные диски) и в появляющемся окне выбрать диск, подходящий для работы. Его имя появится в окне **Available disks** (Доступные диски), где его следует отметить флажком (рис. 15.7). После нажатия кнопки **Next** (Далее) появится предупреждение о том, что все тома и данные на диске будут уничтожены — необходимо подтвердить правильность использования выбранного диска.

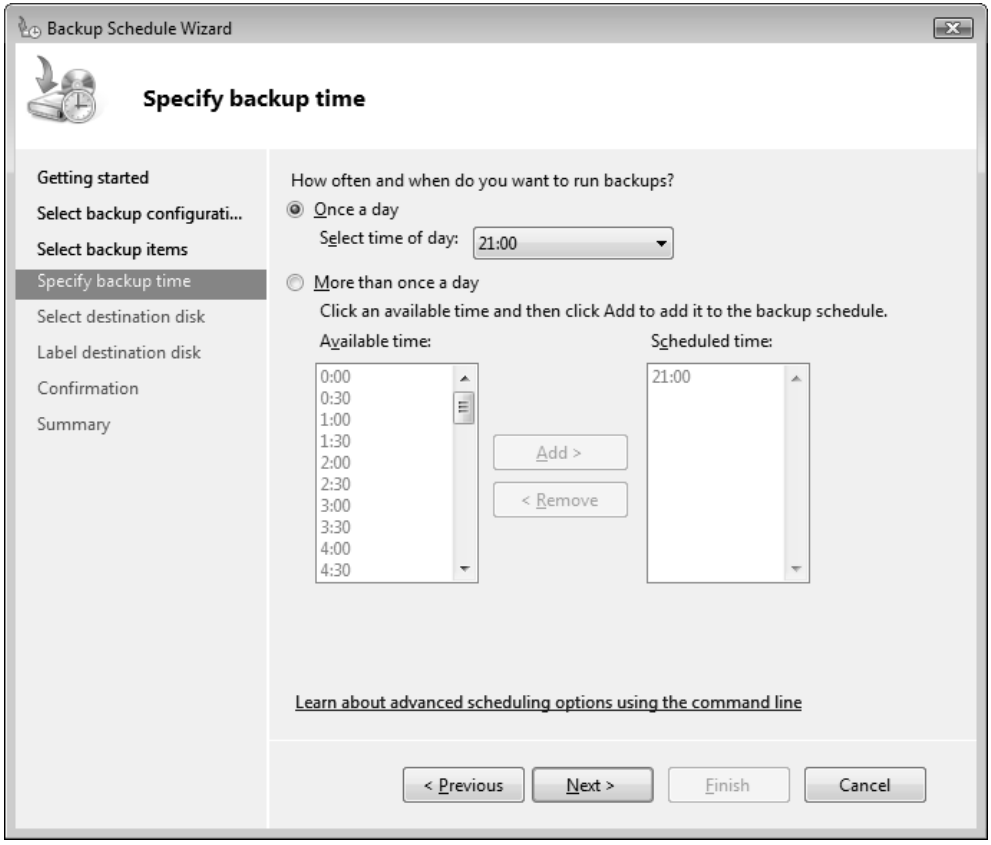


Рис. 15.6. Расписание автоматической архивации данных

6. В следующем окне мастер укажет название метки диска (оно включает дату и время создания архива) — эту информацию следует сохранить и

использовать для маркировки диска, поскольку она может потребоваться при восстановлении данных из архива.

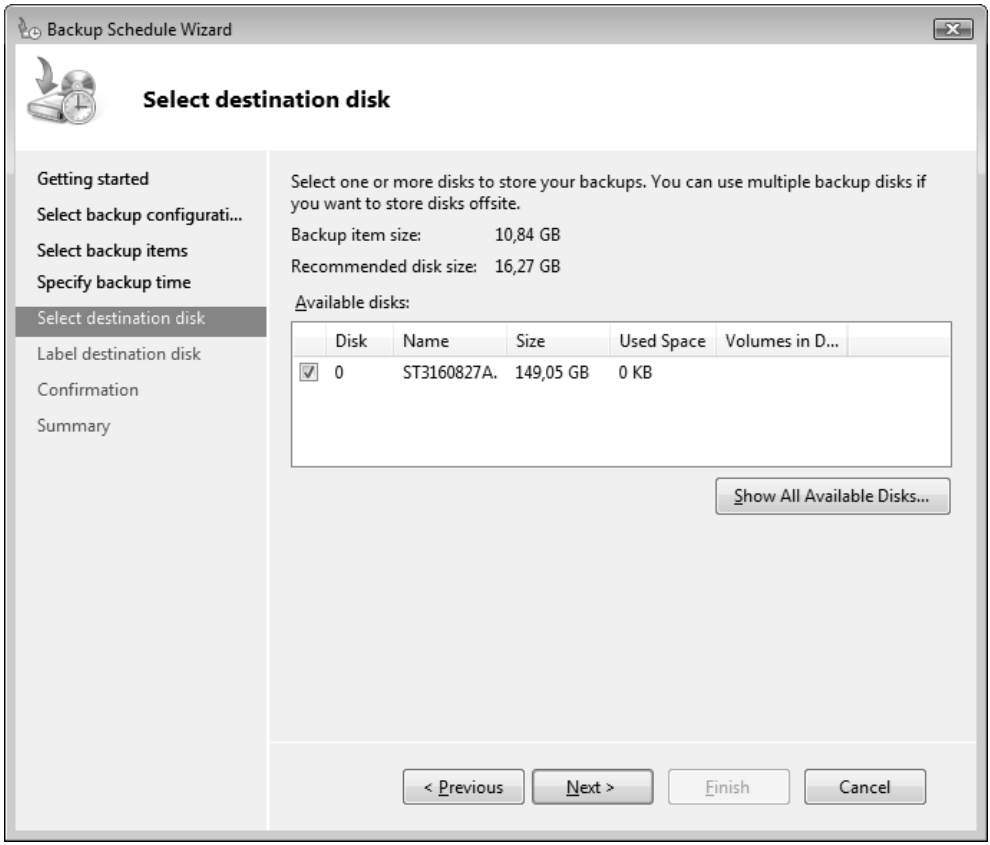


Рис. 15.7. Выбор целевого диска для хранения архивов, создаваемых по расписанию

7. На последнем этапе необходимо проверить правильность параметров и нажать кнопку **Backup** (Архивировать). Целевой диск будет отформатирован и появится сообщение об успешном окончании подготовки операции плановой архивации. После этого окно мастера можно закрыть.

Параметры архивации по расписанию, а также имя и свойства целевого диска, будут отображаться в окне оснастки **Windows Server Backup** (Система архивации данных Windows Server) на панели **Scheduled Backup** (Архивация по расписанию). Щелкнув по ссылке **View Details** (Показать подробности),

можно увидеть сведения о всех архивах, записанных на данный диск, включая размер начального архива и обновлений, записанных при выполнении повторных операций архивации.

Если теперь выбрать ссылку **Backup Once** (Однократная архивация) и согласиться с выбором параметров, заданных для архивации по расписанию, то можно тут же начать запланированную операцию.

Сохранение и восстановление состояния системы (System State)

Для сохранения состояния системы в системах Windows Server 2008 требуется особая процедура, поскольку с помощью оснастки **Windows Server Backup** (Система архивации данных Windows Server) эту операцию выполнить нельзя.

Состояние системы включает в себя следующую информацию:

- Системный реестр
- Регистрационная база классов COM+
- Файлы, необходимые для загрузки системы, включая файлы самой системы
- Системные файлы, защищенные функцией Windows File Protection

Кроме того, могут присутствовать дополнительные компоненты, если они установлены в системе:

- База данных служб сертификатов (Certificate Services)
- Служба каталога Active Directory
- Том SYSVOL
- Информация службы кластеров
- Метакаталог служб IIS

Состояние системы можно сохранить только на внутренний или внешний диск компьютера; DVD-диск или сетевую общую папку использовать нельзя. Из архива состояния системы восстанавливаются только само состояние системы и системные приложения, для восстановления тома или файлов следует применять обычные архивные копии.

Для сохранения состояния системы используется утилита командной строки Wbadmin. Ниже приведен пример выполнения операции с использованием локального тома (E:):

```
C:\>wbadmin start systemstatebackup -backupTarget:E:
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Starting System State Backup [02.06.2008 17:02]
Retrieving volume information...

This would backup the system state from volume(s) SYS(D:),Win2008Ent(C:)
to E:.
Do you want to start the backup operation?
[Y] Yes [N] No y

Creating the shadow copy of volumes requested for backup.
Creating the shadow copy of volumes requested for backup.
Identifying system state files to backup (This may take a few minutes)...
Found (779) files
... ... ...

Found (57585) files
Search for system state files complete
Starting backup of files
Overall progress - 0% (Currently backing up files reported by 'System
Writer')
... ... ...

Overall progress - 98% (Currently backing up files reported by 'System
Writer')
Backup of files reported by 'System Writer' completed
Backup of files reported by 'FSRM Writer' completed
Backup of files reported by 'COM+ REGDB Writer' completed
Backup of files reported by 'WMI Writer' completed
Overall progress - 99% (Currently backing up files reported by 'Registry
Writer')

Summary of backup:
------------------

Backup of system state completed successfully [02.06.2008 17:31]

Log of files successfully backed up
'C:\Windows\Logs\WindowsServerBackup\SystemStateBackup 02-06-2008 17-07-
40.log'

C:\>
```

После выполнения операции на целевом диске создается папка WindowsImageBackup, содержащая подкаталог, имя которого соответствует имени компьютера, а внутри него — папка SystemStateBackup. Внутри нее будут храниться конкретные версии состояния системы.

Для восстановления состояния системы используется команда `wbadmin start systemstaterecovery`. Если ее запустить без дополнительных ключей, то выводится список необходимых параметров.

Восстановление информации

Теперь можно рассмотреть операции, связанные с использованием созданных архивов. Помимо простого извлечения данных из архивов, в системах Windows Vista/Windows Server 2008 имеется функция получения прежних версий файлов, которая для пользователя выглядит одинаково в обоих версиях систем (хотя способы подготовки архивов, используемых для реализации этой функции, отличаются).

Восстановление данных из архива

Если имеются вручную или автоматически (по расписанию) созданные архивы, то можно пользоваться операцией восстановления данных. При этом можно восстанавливать информацию из архивов, подготовленных на других компьютерах.

Процедура восстановления случайно удаленных или испорченных данных выглядит следующим образом:

1. В окне оснастки **Windows Server Backup** (Система архивации данных Windows Server) (см. рис. 15.1) выберите ссылку **Recover** (Восстановление). Запустится мастер *Recovery Wizard* (Мастер восстановления).
2. Сначала нужно указать, с какого сервера нужно восстанавливать данные: с локального компьютера или с другого (опция **Another server**). При выборе первой опции будут просматриваться *все* архивы, имеющиеся на компьютере: как созданные по расписанию и хранящиеся на отдельных дисках, так и архивы, созданные по запросу. В случае выбора "другого" компьютера можно указывать только вручную созданные архивы, задавая их точное местоположение — это может быть раздел локального жесткого диска, DVD-привод или общая сетевая папка. В остальном эти две опции не различаются.
3. Для указанного на предыдущем шаге местоположения мастер ищет созданные архивы и указывает, какие из них доступны. При этом отображается календарь, по которому можно выбрать дату создания архива. Если

на некоторый день приходится несколько архивов, то их можно выбирать по дате создания. Следует указать архив, который будет использоваться для восстановления данных.

4. Далее укажите, какая информация будет копироваться из архива: это могут быть файлы и папки; приложения, зарегистрированные в системе Windows Server Backup, или целые тома.

5. При выборе опции восстановления файлов и папок можно указать конкретные объекты, которые требуется выбрать из архива (рис. 15.8). Необходимо просмотреть дерево папок и выделить в окне справа нужные файлы или папки (операция выделения осуществляется так же, как в окне программы Windows Explorer (Проводник)).

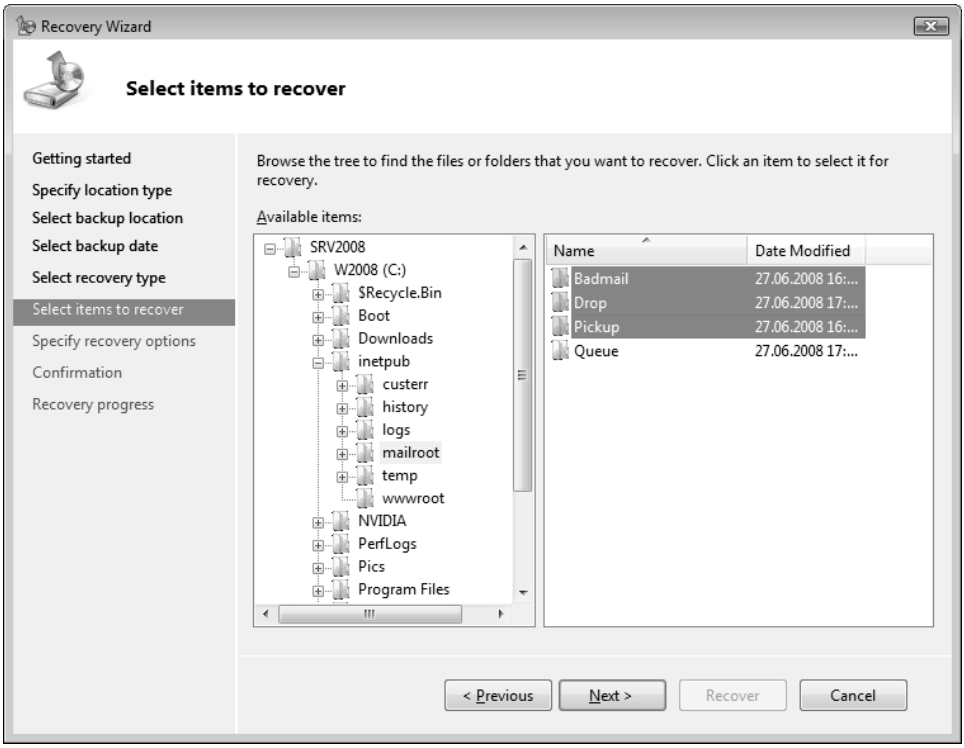


Рис. 15.8. Выбор отдельных файлов и папок для восстановления

6. Укажите местоположение для восстанавливаемых данных: файлы могут записываться в исходное место или в произвольно выбранную папку

(рис. 15.9). Можно выбрать действие, которое будет выполняться в случае конфликтов: при совпадении имен файлы могут восстанавливаться с другими именами, старые файлы могут перезаписываться или же конфликтующие файлы будут пропущены (т. е. останутся версии, существующие на момент выполнения операции). По умолчанию для файлов и папок восстанавливаются параметры безопасности NTFS.

7. На завершающем этапе нужно проверить список восстанавливаемых файлов или папок и запустить операцию, нажав кнопку **Restore** (Восстановить).

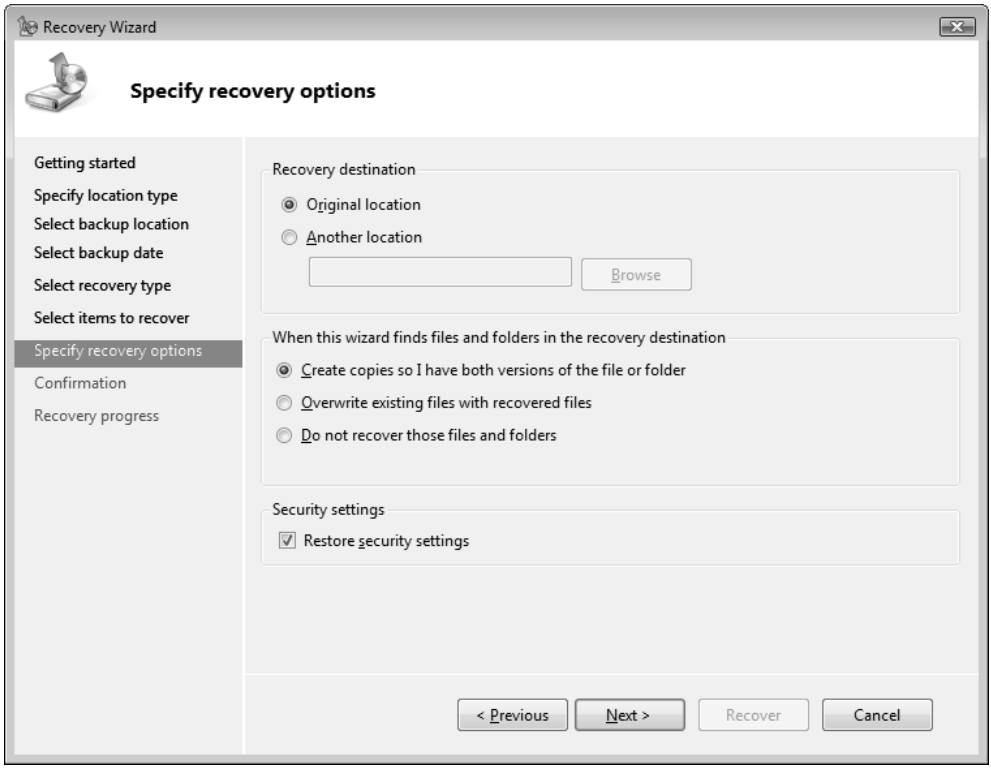


Рис. 15.9. Выбор местоположения восстанавливаемых файлов

Прежние версии файлов и папок

В системах Windows Server 2008 имеется возможность восстановления *предыдущих версий* (previous versions) файлов и папок. Это может потребоваться

при случайном удалении информации или при необходимости вернуться к более ранней версии файла. Функция прежних версий доступна локальным пользователями сервера и сетевым клиентам, которые обращаются к общим папкам.

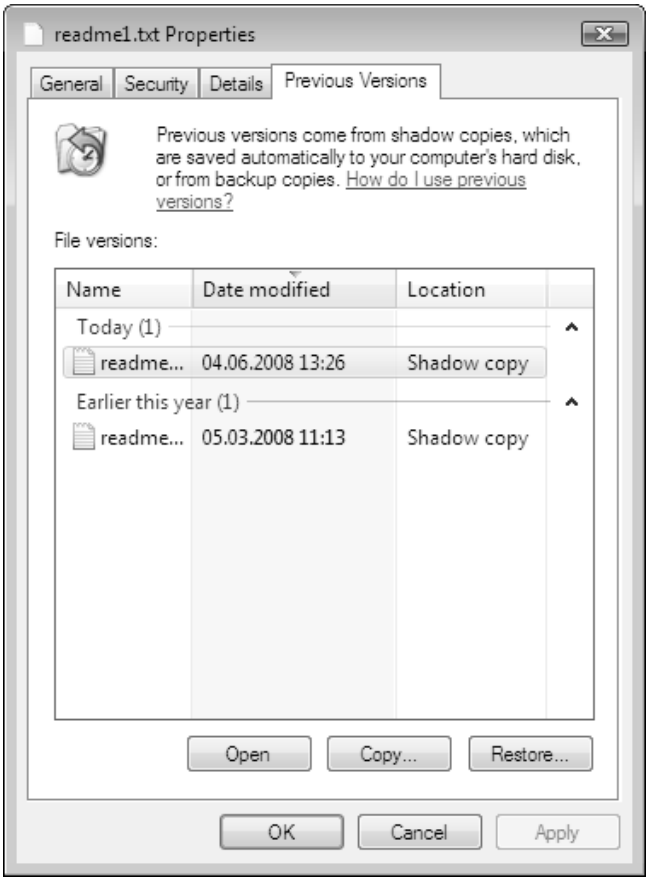


Рис. 15.10. Выбор предыдущей версии файла для восстановления или копирования

Если открыть окно программы Windows Explorer (Проводник), то можно видеть, что в контекстном меню любого файла или папки имеется команда **Restore previous versions** (Восстановить прежнюю версию). Если для выбранного файла или папки создавались архивные копии, то в окне свойств на вкладке **Previous Versions** (Предыдущие версии) (рис. 15.10) можно увидеть

сохраненные варианты содержимого файла или папки, просмотреть их и восстановить на исходное место (кнопка **Restore** (Восстановить)) или в альтернативную папку (кнопка **Copy** (Копировать)).

Для того чтобы функция предыдущих версий файлов работала, необходимо сначала включить теневые копии на конкретном томе. Для этого нужно выполнить следующую процедуру:

1. В окне программы Windows Explorer (Проводник) выберите любой диск, щелкните правой кнопкой мыши и в контекстном меню выполните команду **Configure Shadow Copies** (Настроить теневые копии).
2. В списке томов, имеющихся на сервере (рис. 15.11), укажите нужный том и нажмите кнопку **Enable** (Включить).

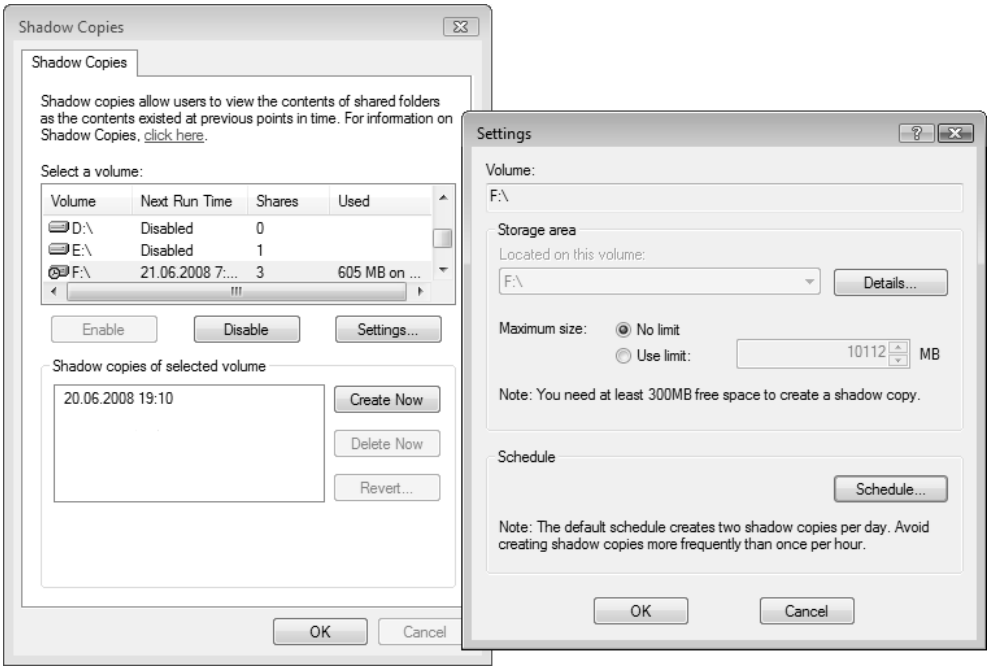


Рис. 15.11. Окно просмотра теневых копий, имеющихся на сервере, и окно параметров выбранной теневой копии

3. При включении теневой копии появляется сообщение о том, что для ее создания будет использоваться расписание, установленное по умолчанию,

и что параметры, выбранные по умолчанию, могут быть не пригодны для серверов с большой нагрузкой (рис. 15.12). Поэтому стандартные параметры нужно проверить и при необходимости скорректировать.

Рис. 15.12. Предупреждение о включении теневых копий для выбранного тома

4. После подтверждения операции теневая копия будет создана и время ее создания появится в окне **Shadow copies of selected volume** (Теневые копии выбранного тома). (С помощью кнопки **Create Now** (Создать) теневую копию можно создать в любой момент.)
5. Кнопка **Settings** (Параметры) (см. рис. 15.11) позволяет просмотреть параметры выбранной теневой копии. В окне параметров задается размер буферной области и определяется расписание для создания теневой копии (по умолчанию это делается по рабочим дням, два раза в день, в 7-00 и 12-00).
6. После выбора параметров окно можно закрыть, нажав кнопку **ОК**.

Если в окне теневых копий выбрать по дате создания определенную версию копии, то с помощью кнопки **Revert** (Восстановить) можно восстановить содержимое всех файлов, существовавшее на момент создания этой теневой копии. При этом все изменения, выполненные позднее этого времени, будут утеряны.

Аварийное восстановление системы с помощью полного образа системы

В случае краха системы можно восстановить ее состояние и все пользовательские данные из образа системы — разумеется, если этот образ был предварительно создан на отдельном физическом диске.

Для восстановления системы с помощью ее образа требуются следующие операции:

1. Запустите программу установки Windows, загрузившись с дистрибутивного диска.
2. В первом окне программы установки щелкните по ссылке **Repair your computer** (Восстановление системы) (см. рис. 1.7).
3. В окне **System Recovery Options** (Параметры восстановления системы) (см. рис. 15.19) выберите опцию **Windows Complete PC Restore** (Восстановление архива Windows Complete PC).

Рис. 15.13. Выбор архива для полного восстановления компьютера

4. Запустится мастер восстановления, который попытается найти подходящий образ системы или попросит установить жесткий диск, на котором был сохранен полный архив. Если мастер может самостоятельно найти образ на жестком диске, то необходимо уточнить, какой из архивов будет использоваться (рис. 15.13). (Автоматически выбирается самый "свежий" архив.)
5. После выбора архива нужно убедиться в правильности информации и определить состояние флажка, указывающего, будет ли выполняться форматирование дисков (рис. 15.14). По умолчанию флажок сброшен, и форматируются только восстанавливаемые диски (использованные при создании образа) — вся информация на них удаляется и будет скопирована из архива. Другие диски, если они имеются на компьютере, не затрагиваются при восстановлении. Нажав кнопку **Advanced** (Дополнительно), можно определить параметры перезагрузки системы и необходимость проверки дисков (рис. 15.15; указаны значения по умолчанию).

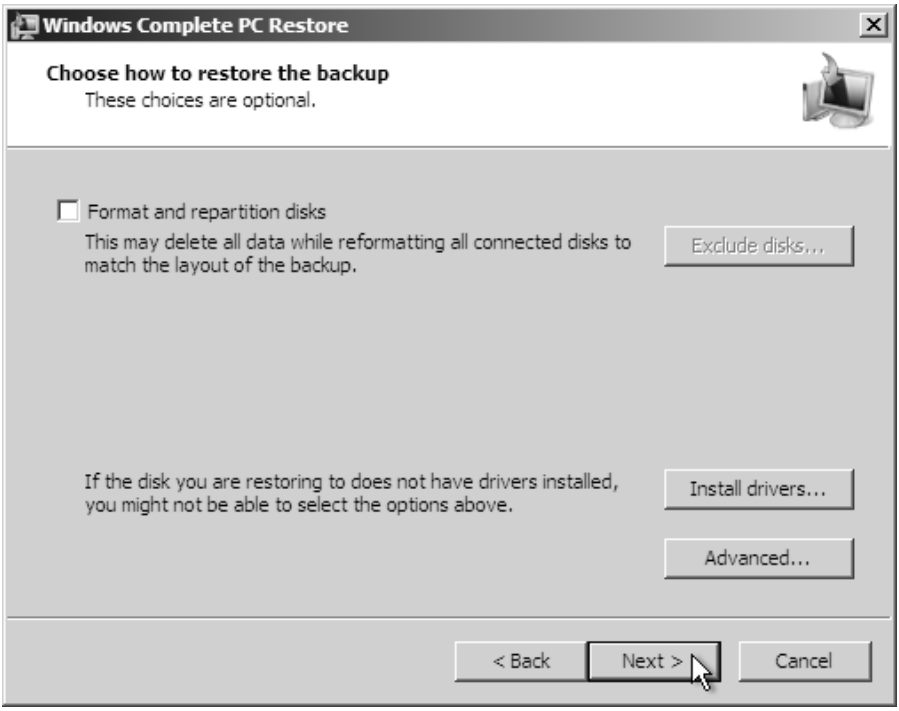


Рис. 15.14. Опция выполнения форматирования

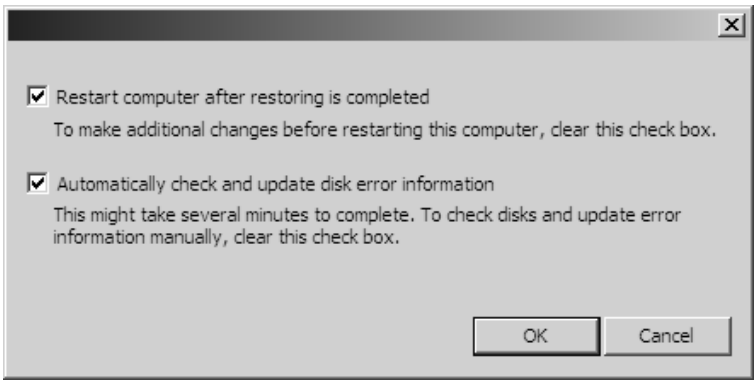


Рис. 15.15. Дополнительные параметры операции восстановления из полного архива системы

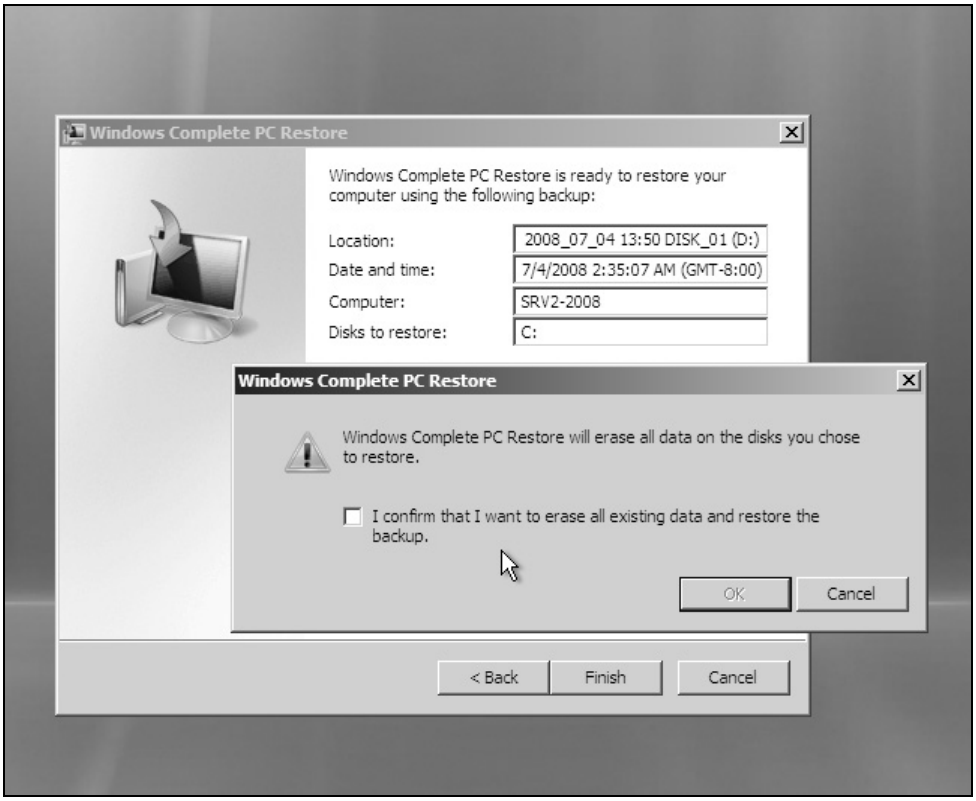


Рис. 15.16. Предупреждение о форматировании восстанавливаемых дисков

6. После нажатия кнопки **Finish** (Готово) (рис. 15.16) нужно подтвердить согласие на удаление информации с восстанавливаемых дисков, и только затем начнется восстановление архива, после чего компьютер автоматически перезагрузится.

Восстановление образа происходит заметно быстрее, чем его создание.

Средства восстановления системы при сбоях

В составе Windows Server 2008 имеются различные средства, поддерживающие целостность системы и обеспечивающие возможность восстановления поврежденной системы. Необходимо упомянуть некоторые традиционные для систем Windows возможности:

- защита системных файлов от просмотра и замены, осуществляемая на уровне разрешений доступа к файловой системе NTFS, а также с помощью средства Windows File Protection;
- проверка системных файлов с помощью утилиты Sfc.exe;
- верификация цифровой подписи файлов с использованием утилиты Sigverif.exe;
- возможность отката драйверов (Driver Rollback; см. рис. 1.29 — кнопка **Roll Back Driver** (Откатить)).

К этому следует добавить возможность восстановления полного архива системы. (В системах Windows Vista эта функция называется Windows Complete PC; еще в них имеются точки восстановления и функция System Restore.)

Существуют различные варианты загрузки операционной системы, список которых (рис. 15.17) вызывается в момент загрузки системы (в этом случае нужно успеть нажать клавишу до появления заставки) или из меню выбора систем по нажатию клавиши <F8>.

При использовании *безопасного режима* (Safe mode) система загружается с минимальным набором драйверов устройств и сервисов. Этот режим позволяет устранить сбои, вызванные некорректной установкой нового программного обеспечения или драйверов устройств. Ошибки, связанные с некорректной работой новых драйверов, весьма успешно устраняет режим *последней удачной конфигурации* (Last Known Good).

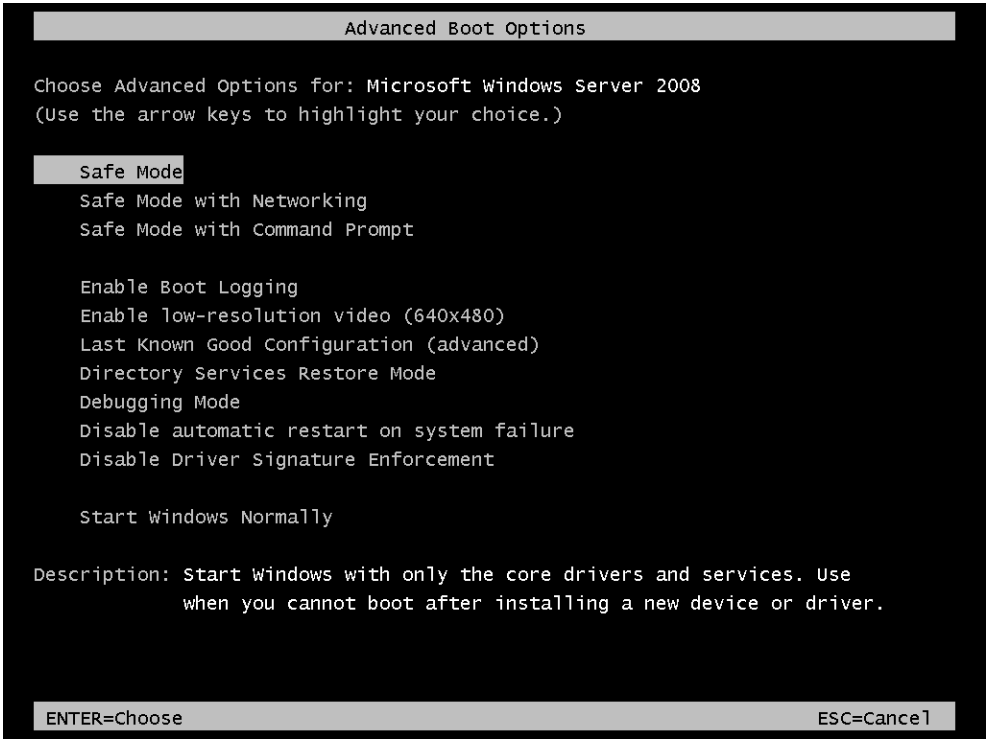


Рис. 15.17. Меню дополнительных режимов загрузки Windows Server 2008

В тех случаях, когда повреждения системы серьезны, требуется ее восстановление с помощью ранее сохраненного полного архивного образа всей дисковой конфигурации (Windows Complete PC). Для этого нужно загрузиться с дистрибутивного DVD-диска.

Опции восстановления при загрузке с инсталляционного диска

После загрузки с дистрибутивного DVD-диска появляется окно программы установки Windows (см. рис. 1.7), в котором по ссылке **Repair your computer** (Восстановление системы) можно перейти в меню функций восстановления системы. Сначала необходимо выбрать систему, с которой вы будете работать (рис. 15.18), и нажать кнопку **Next** (Далее). В некоторых случаях, для того чтобы появился список установленных систем (пусть даже одна строка),

необходимы дополнительные драйверы (кнопка **Load Drivers** (Загрузить драйверы)).

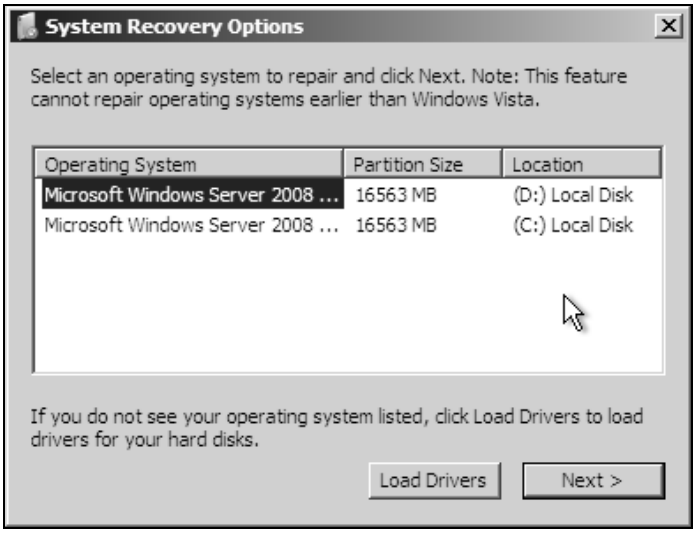


Рис. 15.18. Выбор восстанавливаемой системы

В следующем окне (рис. 15.19) можно выбрать средство, которое будет использоваться для восстановления системы. (Для Windows Vista этих возможностей немного больше, поскольку там имеются механизм точек восстановления и возможность автоматического исправления загрузочного сектора диска.) Для систем Windows Server 2008 главным средством восстановления является опция **Windows Complete PC Restore** (Восстановление архива Windows Complete PC), позволяющая восстановить всю дисковую конфигурацию (включая пользовательские данные и приложения) из полного архивного образа системы.

Опция **Windows Memory Diagnostic Tool** (Средство диагностики памяти Windows) присутствует также в меню выбора систем в случае систем с двойной загрузкой (см. рис. 1.1—1.4). Она позволяет протестировать память компьютера. Запуск теста памяти можно инициировать и из работающей системы, для этого имеется соответствующая опция в группе **Administrative Tools** (Администрирование). При этом тест все равно будет выполняться в процессе загрузки системы.

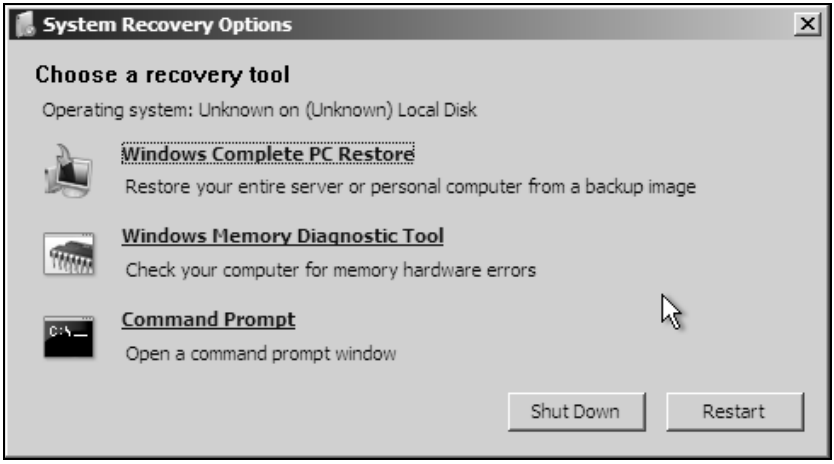


Рис. 15.19. Опции восстановления системы Windows Server 2008

Третья опция, **Command Prompt** (Командная строка), аналогична *консоли восстановления* (Recovery Console), которая имеется в системах Windows предыдущих версий. Окно командной строки предоставляет администраторам необходимый минимум средств, позволяющих выполнить восстановительные процедуры в системе (но набор этих средств заметно шире, чем в консоли восстановления). С помощью утилит, запускаемых в этом окне, можно размечать и форматировать диски, выполнять чтение и запись данных на локальные жесткие диски. Особенно полезной опция **Command Prompt** (Командная строка) может оказаться в том случае, если для восстановления системы требуется скопировать на жесткий диск один или несколько системных файлов (с дискеты или дистрибутивного диска) или же сконфигурировать дисковые разделы. Функции консоли управления, устанавливаемой с дистрибутивного диска на жесткий диск и запускаемой из меню загрузки, в системах Windows Server 2008 отсутствуют.

Приложение

Веб-ссылки

Практически все предлагаемые далее ссылки указывают на веб-сайты компании Microsoft (и вряд ли это вызовет удивление). При необходимости более глубокого знакомства с тем или иным продуктом или технологией, включенной в состав операционной системы Windows, основным источником информации являются сайты TechNet и MSDN. При поиске решений возникших проблем лучше всего обращаться к базе знаний Microsoft Knowledge Base. Все основные и развернутые материалы размещаются на главном (англоязычном) сайте; русскоязычное зеркало сравнительно небольшое по объему и содержит, в первую очередь, общую информацию. На многих веб-страницах (сайтах) язык отображения зависит от языковых настроек, установленных в браузере.

Начнем с сайта, который администратор сети посещает, возможно, чаще других сайтов Microsoft. Разнообразные утилиты, упоминаемые в книге, а также различные обновления и полезные программы нужно искать по ключевым словам, названию программы или имени дистрибутивного файла на главной странице *Центра загрузки Microsoft* (Microsoft Download Center) (имеется русскоязычное зеркало):

www.microsoft.com/downloads/

На этом сайте можно, например, найти два ценных справочных файла в CHM-формате:

- Windows Command Reference (файл WinCmdRef.exe) — справочник по командам консоли (удобно иметь его под рукой, а не искать каждую команду по веб-ссылкам);
- Windows Server® 2008 Network Shell (Netsh) Technical Reference (файл Netsh.exe) — справочник по параметрам утилиты Netsh.exe, которая полезна при работе с сетевыми интерфейсами и многими сетевыми компонентами. Без такого руководства разобраться со всеми возможностями утилиты довольно сложно.

- *Домашняя страница Windows Server 2008* (главная страница продукта):

  www.microsoft.com/rus/windowsserver2008/ (РУС)

  www.microsoft.com/windowsserver2008/

  На этом сайте или в Центре загрузки Microsoft несложно найти ссылку для скачивания пробной (trial) версии Windows Server 2008.

- *Microsoft TechNet Home Page* (домашняя страница веб-сайта "Microsoft TechNet", являющегося крупнейшей библиотекой статей для IT-специалистов по всем продуктам Microsoft. Здесь имеются ссылки на блоги, где можно найти самую свежую информацию о новых продуктах или решения возникающих проблем):

  technet.microsoft.com/ru-ru/default.aspx (РУС)

  technet.microsoft.com/en-us/default.aspx

- *Windows Server TechCenter* (прямые ссылка на раздел TechNet, посвященный серверным продуктам):

  technet.microsoft.com/ru-ru/windowsserver/ (РУС)

  technet.microsoft.com/en-us/windowsserver/

- *MSDN Home Page* (главная страница библиотеки для разработчиков Microsoft Developer Network):

  msdn.microsoft.com

  (перенаправляет на **http://msdn.microsoft.com/en-us/default.aspx** или **http://msdn.microsoft.com/ru-ru/default.aspx** — в зависимости от языка, используемого по умолчанию в браузере; аналогичные ссылки на английском и русском сайте могут направлять на совершенно разные по содержанию веб-страницы).

- Веб-страница, посвященная технологии виртуализации:

  www.microsoft.com/rus/virtualization/ (РУС)

- *Microsoft TechNet: Windows Sysinternals* (системные утилиты от известных разработчиков и специалистов по Windows Марка Руссиновича (Mark Russinovich) и Брюса Когсвела (Bryce Cogswell)):

  www.microsoft.com/technet/sysinternals/

- *Scripting with Windows PowerShell* (специальный сайт, посвященный новому языку сценариев и среде исполнения):

  www.microsoft.com/technet/scriptcenter/hubs/msh.mspx

  По ссылке **Windows PowerShell Script Repository** можно перейти в библиотеку готовых сценариев, которые могут оказаться полезными в работе или при изучении языка PowerShell.

- Две ссылки на русскоязычном сайте Intel помогут выбрать модель процессора, поддерживающего Hyper-V и Intel® VT:

  www.intel.com/cd/products/services/emea/rus/server/processors/344493.htm

  www.intel.com/cd/products/services/emea/rus/desktop/processors/327655.htm

Предметный указатель

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

А

Б

В

Г

Д

Ж

З

И

К

Л

М

Н

О

П

P

C

Т

У

Ф

Х

Ц

Ч

Ш

Э

Ю, Я