
bhv
АЛЕКСЕЙ ЧЕКМАРЕВ
Windows Server 2008
Настольная книга администратора
Выполнение типовых операций администрирования
Базовые службы и домены
Конфигурирование ролей сервера
Управление Server Core и Hyper-V Server
СИСАДМИН
СИСТЕМНЫЙ АДМИНИСТРАТОР

Алексей Чекмарев

Windows Server 2008

Настольная книга администратора

Санкт-Петербург
«БХВ-Петербург»
2009

УДК 681.3.06
ББК 32.973.26-018.2
Ч-37

Чекмарев А. Н.

Ч-37 Windows Server 2008. Настольная книга администратора. —
СПб.: БХВ-Петербург, 2009. — 512 с.: ил. — (Системный администратор)

ISBN 978-5-9775-0374-7

Руководство может использоваться при работе с любыми редакциями операционной системы Microsoft Windows Server 2008 для 32- и 64-разрядных платформ. Помимо традиционных процедур настройки системы с помощью графического интерфейса описаны режим установки Server Core и система Hyper-V Server 2008. Подробно рассмотрены способы настройки основных ролей серверов, работающих в составе рабочих групп и доменов Active Directory. Особое внимание уделено особенностям удаленного администрирования и управлению виртуальными машинами в среде Hyper-V. Описаны файловые и сетевые службы, доменные службы Active Directory, средства архивации и восстановления, а также другие компоненты системы.

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 02.02.09.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 41,28.
Тираж 2500 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Санитарно-эпидемиологическое заключение на продукцию № 77.99.60.953.Д.002108.02.07
от 28.02.2007 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 978-5-9775-0374-7

© Чекмарев А. Н., 2009
© Оформление, издательство "БХВ-Петербург", 2009

Оглавление

Предисловие **1**

Введение.
Возможности и компоненты систем Windows Server 2008 ..... **3**

Редакции ОС Microsoft Windows Server 2008 3
Новые средства систем Windows Server 2008 5
Установка и восстановление 5
Базовые компоненты 6
Сетевые возможности 8
Серверные функции 9
Службы каталога Active Directory 10
Сравнение функциональных возможностей редакций Windows Server 2008 на различных платформах 11
Требования к аппаратным ресурсам 13
Дифференциация требований к графической подсистеме 15

Глава 1. Установка систем и виртуальных машин **17**

Подготовка к установке системы 17
Выбор режима инсталляции 18
Конфигурирование разделов на жестком диске 19
Выбор файловой системы 20
Организация систем с двойной загрузкой 20
Управление опциями загрузки 24
Особенности Windows Server 2008 Server Core 25
Интерактивная установка систем Windows Server 2008 26
Новая установка системы с загрузочного компакт-диска 27
Обновление систем Windows Server 2003 33
Выполнение процедуры обновления 34
Постинсталляционные задачи 36
Установка пароля 36
Начальное конфигурирование системы 37
Основные рабочие параметры сервера 37
Использование мастера конфигурирования 38

Установка параметров автоматического обновления Windows 41
Активация системы 46
Автоматическая инсталляция систем 46
Средства восстановления системы при сбоях 48
Опции восстановления при загрузке с инсталляционного диска 50
Службы развертывания Windows (WDS) 51
Установка служб и конфигурирование WDS-сервера 52
Добавление образов 53
Дополнительная настройка параметров WDS-сервера 56
Установка устройств в работающей системе 57
Просмотр состояния устройств 57
Установка драйверов для подключенных устройств 59
Работа с виртуальными машинами в среде Hyper-V 60
Управление сервером Microsoft Hyper-V Server 2008 61
Управление виртуальными машинами — утилита Hyper-V Manager 62
Установка новой виртуальной машины 65
Службы интеграции (Integration Services) 69
Подключение к виртуальным машинам 70

Глава 2. Конфигурирование рабочей среды и административные задачи 73

Настройка экрана регистрации в системе 73
Контроль учетных записей (UAC) 76
Виртуализация операций записи в файлы и реестр 78
Выполнение административных задач 78
Управление механизмом UAC 81
Конфигурирование системы. Панель управления 84
Непосредственный доступ к задачам панели управления 86
Свойства системы 87
Настройка монитора и элементов пользовательского интерфейса 89
Настройка параметров монитора 90
Стили (темы) оформления 91
Хранитель экрана (экранная заставка) 91
Выбор языков и региональных стандартов 92
Управление электропитанием 93
Энергосберегающие режимы Windows Server 2008 98
Установка приложений и компонентов Windows 100
Роли и компоненты сервера 100
Установка ролей и компонентов 104
Установка ролей из командной строки 107
Управление системными компонентами и учетными записями — оснастка *Computer Management* 108

Организация профилей пользователей ... 111
Профили пользователей ... 112
Структура профиля пользователя ... 112
Личные и общие папки ... 115
Поиск информации, хранящейся на сервере ... 116
Выполнение операций поиска ... 118
Конфигурирование службы Windows Search ... 120
Правила и примеры поиска ... 123
Аудит событий в локальной системе ... 124
Включение аудита ... 125
Настройка и просмотр параметров аудита для папок и файлов ... 126
Отключение аудита для выбранных объектов ... 128
Удаленный административный доступ к компьютеру ... 129
Сохранение и изменение параметров подключения ... 133
Одновременное подключение к одному компьютеру ... 133
Отключение от сеанса и управление удаленным компьютером ... 134
Включение функции Remote Desktop из командной строки ... 135
Планирование заданий, выполняющихся по расписанию ... 136
Служба времени Windows (W32Time) ... 141
Настройка синхронизации с источником времени ... 142
Синхронизация и проверка работы службы времени ... 142
Отключение синхронизации ... 143
Язык сценариев и командный процессор PowerShell ... 143
Установка и запуск PowerShell ... 144
Выполнение сценариев ... 146

Глава 3. Мониторинг системы и приложений ... 149

Средства мониторинга в Windows Server 2008 ... 149
Диспетчер задач (Task Manager) ... 151
Запуск диспетчера задач ... 151
Просмотр состояния прикладных программ ... 152
Мониторинг процессов ... 153
Слежение за работой системных служб ... 157
Анализ загрузки системы ... 159
Мониторинг сети ... 160
Просмотр списка зарегистрированных пользователей ... 161
Мониторинг программ и сервисов — программа Software Exporer ... 162
Просмотр событий, регистрируемых системой, службами и приложениями ... 164
Просмотр журналов и параметров событий ... 166
Фильтрация событий ... 168
Подписки и отправляемые события ... 170
Мониторинг параметров и стабильности работы системы ... 174
Системный монитор (Performance Monitor) ... 177

Объекты и счетчики производительности 177
Настройка счетчиков 178
Мониторинг отдельных процессов и приложений 181
Настройка способов представления информации 182
Оснастка *Reliability Monitor* (Монитор стабильности системы) 183
Компонент Data Collector Sets (Группы сборщиков данных) 185

Глава 4. Конфигурирование файловых служб 189

Установка файловых служб 189
Конфигурирование дисков и томов 192
Стили разделов 192
Разделы и тома 194
Использование оснастки *Disk Management* 195
Расширение и сжатие разделов и логических дисков 198
Дефрагментация дисков 200
Традиционные средства управления общими дисковыми ресурсами 201
Управление общим доступом из программы Windows Explorer 202
Мастер общего доступа 203
Классический подход 205
Оснастка *Shared Folders* 207
Подключение сетевых дисков и использование утилит командной строки 208
Управление разрешениями доступа к файлам и папкам 210
Правила назначения разрешений на доступ 210
Разрешения доступа на уровне файловой системы NTFS 212
Установка разрешений для файлов 213
Установка разрешений для папок 216
Определение действующих разрешений для файлов и папок 219
Передача права владения 220
Централизованное управление общими ресурсами с помощью оснастки *Share and Storage Management* 222
Квоты дискового пространства 224
Включение стандартного механизма квот 225
Использование квот 226
Управление доступом к файловом ресурсам с помощью оснастки *File Server Resource Manager* 229
Управление квотами для томов и папок 231
Блокировка копирования и создания файлов 234
Анализ использования дисковых ресурсов 236
Настройка параметров доступа к общим сетевым папкам и принтерам 237
Распределенная файловая система DFS 239
Установка компонентов DFS и начальное конфигурирование 240
Управление DFS 242
Создание пространства имен DFS 243

Добавление папок 245
Создание групп репликации 246
Управление репликацией DFS 250
Криптозащита папок и файлов, хранящихся на жестком диске 251
Обязательные требования при выполнении операций шифрования 251
Шифрование файлов и папок 252
Шифрование файлов для совместного использования 255
Копирование, перемещение, переименование и уничтожение зашифрованных файлов и папок 256
Архивация зашифрованных файлов 256

Глава 5. Архивация и восстановление информации 257

Установка системы архивации данных Windows Server 257
Способы архивации и восстановления данных и системных файлов 258
Средства управления системой архивации в Windows Server 2008 260
Архивация системы и данных 261
Настройка автоматической архивации томов 262
Использование утилиты архивации 264
Создание полного образа системы или архива отдельных томов 265
Выполнение архивации из командной строки 268
Восстановление информации 269
Восстановление данных из архива 269
Выполнение операции восстановления из командной строки 270
Прежние версии файлов и папок 271
Аварийное восстановление системы с помощью полного образа системы 274
Сохранение и восстановление состояния системы (System State) 275

Глава 6. Сетевые компоненты и службы 279

Сетевые средства, удаленные из Windows Server 2008 279
Особенности использования некоторых сетевых компонентов 280
Категории сетей (сетевое размещение) и профили встроенного брандмауэра 281
Работа на компьютере в сетевой среде 282
Централизованное управление сетевыми параметрами 284
Просмотр параметров сетевых подключений 288
Управление подключениями 292
Создание новых подключений 294
Типы сетевых подключений 295
Подключения по локальной сети 296
Телефонные (коммутируемые) подключения 297
Виртуальные частные сети (VPN) 297
Прямые подключения 298
Входящие подключения 299

Серверы DHCP 301
Основные понятия службы DHCP 303
Установка и настройка DHCP-сервера 307
Авторизация DHCP-сервера 310
Создание области действия 311
Настройка механизма динамической регистрации доменных имен 311
Сохранение и восстановление конфигурации DHCP-сервера 313
Агент ретрансляции DHCP/BOOTP 314
Серверы службы доменных имен (DNS) 315
Возможности DNS-серверов на базе Windows Server 2008 315
Возможности DNS-клиентов 317
Предварительные условия для установки DNS-сервера и способы его использования 318
Установка DNS-сервера 318
Сервер DNS на контроллере домена 319
Установка вторичных DNS-серверов 320
Администрирование DNS-серверов 321
Настройка пересылок (forwarders) 322
Управление зонами 323
Изменение типа зоны и способа хранения 324
Изменение области репликации зоны 325
Установка режима динамического обновления 327
Управление разделами приложений 327
Проверка конфигурации DNS 329
Использование утилиты DnsCmd 330
Настройка клиентов DNS 331
Служба маршрутизации и удаленного доступа (RRAS) 333
Возможности службы RRAS в Windows Server 2008 334
Начальное конфигурирование службы RRAS 336
Удаленный доступ 338
Использование сервера удаленного доступа для обслуживания VPN-подключений 338
Установка сервера удаленного доступа 339
Механизмы управления конфигурацией удаленного подключения 341
Преобразование сетевых адресов (NAT) 342
Компоненты NAT 343
Конфигурирование NAT с помощью программы-мастера 343
Настройка NAT на уже установленном сервере RRAS 345
Разрешение выделения IP-адресов локальным хостам 348
Функция разрешения DNS-имен 349
Конфигурирование преобразования специальных портов и служб 350
Конфигурирование хостов в локальной сети для работы с NAT 352
Совместное использование интернет-подключения (ICS) 352

Защита сетевых подключений с помощью встроенного брандмауэра Windows Firewall....355
Средства расширенного конфигурирования брандмауэра....361
Настройка сетевых параметров и брандмауэра из командной строки....365

Глава 7. Доменные службы Active Directory и групповые политики....369

Конфигурирование службы DNS для развертывания доменов Active Directory....369
Автоматическая настройка DNS-сервера....370
Создание дополнительных доменов....372
Проверка конфигурации DNS....372
Установка и удаление контроллеров домена....372
Особенности создания контроллеров в уже существующих доменах....374
Обновление доменов Windows Server 2003....374
Добавление контроллеров на базе Windows Server 2003 в домены Windows Server 2008....376
Добавление контроллеров на базе Windows Server 2008 в домены Windows Server 2003....376
Запуск мастера установки Active Directory....376
Завершение установки и тестирование....383
Файлы журналов....384
Использование утилиты Dcpromo из командной строки....384
Установка контроллера из архивной копии....385
Установка RODC-контроллера домена....388
Удаление контроллеров домена....391
Запуск мастера установки Active Directory....392
Принудительное понижение роли....393
Удаление с использованием утилиты командной строки....394
Особенности подключения клиентов домена....394
Основные средства администрирования доменов и каталогов Active Directory....396
Утилиты командной строки....397
Оснастка *Active Directory Users and Computers*....399
Подключение к домену или контроллеру домена....400
Управление отображением объектов каталога....401
Сохраненные запросы (Saved Queries)....401
Включение опции просмотра дополнительных компонентов....403
Режим *Users, Contacts, Groups, and Computers as containers* (Пользователи, контакты, группы и компьютеры как контейнеры)....404
Фильтрация отображаемых объектов....405
Поиск объектов в каталоге Active Directory....407
Одновременное редактирование множества объектов каталога....409
Оснастка *Active Directory Sites and Services*....410
Разделы каталога Active Directory и механизм репликации....412
Разделы приложений....414

Формирование топологии репликации 415
Служба репликации файлов (FRS) 415
Управление репликацией из командной строки 416
Просмотр списка партнеров по репликации 416
Просмотр списка соединений с партнерами по репликации 417
Принудительный запуск репликации 417
Оснастка *Active Directory Domains and Trusts* 419
Режимы работы доменов (functional levels) 419
Изменение функционального уровня домена 422
Проверка доверительных отношений 423
Оснастка *ADSI Edit* 425
Оснастка *Active Directory Schema* 427
Новые возможности групповых политик в Windows Server 2008 429
Дополнительные области контролируемых параметров 429
Улучшенное управление браузером Internet Explorer 430
Новый формат и возможности файлов административных шаблонов (ADMX) 430
Гибкость при работе в разных сетях (NLA) 431
Служба Group Policy Client 431
Системные события и журналы 432
Возможность создания нескольких локальных объектов групповой политики 432
Оснастка *Group Policy Management* 432
Начальные объекты групповой политики (Starter GPO) 435
Предпочтения (Preferences) 435
Создание ярлыка для элемента оболочки 437
Создание локальной папки и контроль за ее содержимым 438
Улучшения, касающиеся службы FRS и тома SYSVOL 438
Хранение параметров групповых политик 440
Локальные GPO-объекты 440
Доменные GPO-объекты 442
Контейнер групповых политик 442
Шаблон групповых политик 443
Подкаталоги шаблона групповых политик 443
Файл Gpt.ini 445
Средства редактирования параметров безопасности и групповых политик 445
Оснастка *Group Policy Object Editor* 446
Представление структуры GPO-объекта в окне оснастки 449
Расширения оснастки *Group Policy Object Editor* 449
Параметры безопасности (Security Settings) 451
Дополнительные инструменты настройки безопасности 452
Настройка параметров безопасности из командной строки 453
Определение действующих значений политик 455
Оснастка *Resultant Set of Policy* 455
Определение политик в домене 459
Документирование, архивация и восстановление GPO-объектов 460

ПРИЛОЖЕНИЯ 463

Приложение 1. Веб-ссылки 465

Приложение 2. Оснастки и задачи панели управления систем Windows Server 2008 468

Оснастки, их имена и назначение 468
Названия служебных утилит и задач панели управления 473

Приложение 3. Административные утилиты командной строки 475

Встроенные утилиты 475
Пакет Windows Support Tools 477

Предметный указатель 479

Предисловие

Операционные системы семейства Microsoft® Windows Server® 2008 зарекомендовали себя надежной серверной платформой и предлагают много новых решений и компонентов, выгодно отличающих их от систем предыдущей версии — Windows Server 2003. При знакомстве с новой системой всегда важно не терять время на уже знакомые вещи, при этом не пропустить и быстрее освоить важные новинки, позволяющие увеличить эффективность использования ресурсов и упростить выполнение административных задач.

Цель этой книги — помочь достаточно опытному системному администратору быстрее сориентироваться в вопросах, возникающих при использовании систем Windows Server 2008, и обратить его внимание на самые важные средства, впервые появившиеся в этой системе. На традиционные решения, знакомые по предыдущим версиям (Windows 2000 и Windows Server 2003), в книге обращается меньше внимания, как и на особенности нового пользовательского интерфейса, появившегося в Windows Vista. Такой подход позволил сделать текст конкретным и лаконичным.

Много внимания в книге уделяется особенностям нового способа конфигурирования серверов (Server Core) и технологиям виртуализации (Hyper-V) — решениям, которые совершенно не знакомы администраторам по предыдущим версиям Windows.

Автор выражает признательность издательству "БХВ-Петербург" за возможность издания этой книги и искренне благодарит всех участников творческой группы, подготовившей книгу к выходу.

Для связи с автором по электронной почте можно использовать адрес **ATchekmarev@hotmail.com** (в теме письма желательно указать название операционной системы).

Алексей Чекмарев

Введение
Возможности и компоненты систем Windows Server 2008

Этот обзорный раздел дает общее представление об основных новых возможностях операционных систем семейства Windows Server 2008, имеющихся редакциях и различиях между ними. Также рассматриваются требования к аппаратным ресурсам с учетом использования некоторых специфических компонентов (темы оформления *Windows Vista*) и ролей сервера (Hyper-V).

После выхода клиентской операционной системы Windows XP (2001 год) и "соответствующей"[1] ей серверной версии, Windows Server 2003 (2003), компания Microsoft вела разработку операционных систем нового поколения, получивших общее кодовое название *Windows Longhorn*; параллельно разрабатывались клиентская версия для рабочих станций и серверная платформа, которая была закончена на год. В конце 2005 года клиентская версия системы проекта Longhorn получила название *Microsoft® Vista™*, и официальный выпуск этой системы состоялся в январе 2007 года. В феврале 2008 года вышла в свет и серверная версия —Windows Server 2008, уже включавшая в себя пакет обновлений Service Pack 1.

На начало 2009 года Windows Server 2008 остается последней версией Windows, выпущенной компанией Microsoft, хотя уже выпущена публичная бета-версия следующей системы, названной Windows Server 2008 R2.

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

[1] Имеется в виду общность кода базовых компонентов.

редакции, за исключением Windows Server 2008 Web, могут устанавливаться в режиме *Server Core* и имеют вариант дистрибутива ***без*** компонента *Hyper-V* [1].

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 (IA64). Системы, оптимизированные для больших баз данных и ответственных приложений. Имеют высокие возможности отказоустойчивости и масштабирования, поддерживают до 64 процессоров для обеспечения критически важных задач.

Microsoft Hyper-V Server 2008. Новый самостоятельный продукт, представляющий собой бесплатную "урезанную" версию Windows Server 2008[2], предназначенную для выполнения только одной роли — Hyper-V. Таким образом, эта версия является платформой для развертывания виртуальных машин, работающих под управлением других версий операционных систем (подробности *см. в главе 1*). Для ее установки не требуется приобретение лицензии, однако соответствующие лицензии необходимы для ***каждой*** установленной виртуальной машины.

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)*. Однако для 32- и для 64-разрядных версий Windows Server 2008 дистрибутивные диски выпускаются отдельно, как и для Hyper-V Server 2008.

---

[1] Такие версии несколько дешевле "полных".

[2] Поэтому мы будет рассматривать его в книге как одну из редакций Windows Server 2008.

Новые средства систем Windows Server 2008

Далее мы рассмотрим назначение основных компонентов, впервые появившихся в Windows Server 2008 (в скобках указаны номера глав, где упомянутое средство рассматривается подробно). Именно новые функции привлекают, в первую очередь, внимание и требуют освоения при переходе на новые версии системы. В книге также рассматриваются и не упомянутые в этом разделе, традиционные компоненты и службы (например, сетевые сервисы), хотя средства управления ими тоже в немалой степени были модернизированы.

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.

Установка и восстановление

Роли сервера

Установка и удаление служб и компонентов в системах Windows Server 2008 жестко увязаны 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 2)*.

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)*.

Технология виртуализации Hyper-V™

Средства виртуализации Hyper-V позволяют запускать на компьютере другие операционные системы (x86 и x64). Эта роль сервера может устанавливаться только в 64-разрядных версиях и на процессорах, которые имеют аппаратную поддержку виртуализации Intel VT или AMD-V (список таких процессоров можно найти на сайтах производителей). Также процессор и материнская плата компьютера должны поддерживать Data Execution Protection (DEP) *(глава 1)*.

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). 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 5)*.

Базовые компоненты

Пользовательский интерфейс Windows Aero™

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

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 2)*.

Быстрое переключение пользователей (Fast User Switching)

Это средство, впервые появившееся в серверной версии Windows, позволяет нескольким пользователям быть одновременно зарегистрированными на компьютере (даже если компьютер входит в домен). Таким образом 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)*.

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 3)*.

Планировщик задач (Task Scheduler)

Планировщик задач был значительно модернизирован и превратился в мощное средство диспетчеризации задач, имеющее множество возможностей и развитый интерфейс *(глава 2)*.

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)*.

Командный процессор Windows PowerShell

Новый командный процессор, позволяющий работать в интерактивном режиме или в режиме выполнения административных сценариев. Имеет расширенные возмож-

ности доступа к компонентам системы для получения от них информации, а также для управления *(глава 2)*.

Защитник Windows (Windows Defender)

Программа Windows Defender является стандартным компонентом системы (в других версиях Windows ее можно устанавливать факультативно); она позволяет защитить компьютер от разнообразных шпионских (spyware) программ, а также нежелательных приложений, которые могут нарушить работоспособность и безопасность системы *(глава 3)*.

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.

Сетевые возможности

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.

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 6)*.

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 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 обновленной версии 7.0.

Серверные функции

Управление файловым сервером

Новые средства администрирования — такие как оснастки **Share and Storage Management** (Управление общими папками и хранилищами) и **File Server Resource Manager** (Диспетчер ресурсов файлового сервера) — позволяют эффективно распределять общие дисковые ресурсы и следить за их использованием. Также обновлены средства управления службой DFS *(глава 4)*.

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).

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.

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 доменных служб Active Directory и групповых политик целиком посвящена *глава 7*.

- Административные оснастки, используемые для управления доменами 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).
- В доменах Active Directory можно устанавливать контроллеры, доступные только для чтения (Read-Only Domain Controller) и имеющие ограниченные возможности репликации каталога. Такое решение может оказаться более безопасным для удаленных офисов, чем размещение обычных контроллеров домена.
- Для эффективной репликации каталога Active Directory возможно использование службы *DFS Replication* (Репликация DFS). Это позволяет применять более эффективный механизм синхронизации системного тома SYSVOL 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 доступа к каталогам), которые позволяют развертывать на сервере несколько экземпляров каталога Active Directory и никак не связаны с доменными службами Active Directory.

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. Каждая редакция 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 различных редакций Windows Server 2008 перечислены в табл. В1 (указаны максимальные значения параметров). Компоненты и функции, реализованные во *всех* версиях, в таблицу не включены.

Примечание

По неоднократным заявлениям компании Microsoft, в следующих серверных версиях Windows поддержка 32-разрядных платформ будет прекращена. Во всяком случае, первая бета-версия следующей системы — Windows Server 2008 R2 — предлагается только для 64-разрядных систем. Бета-версия клиентской системы — Windows 7 — доступна и для 32-, и для 64-разрядных платформ.

Таблица В1. *Основные компоненты, определяющие различия в 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	–
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

Таблица В1 *(продолжение)*

	Windows Server 2008 Web	Windows Server 2008 Standard	Windows Server 2008 Enterprise	Windows Server 2008 Datacenter	Itanium-системы
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	–
Виртуализация (Hyper-V)*	–	да	да	да	–
- Быстрая (live) миграция	–	–	да	да	–
- Кластеризация виртуальных образов	–	–	да	да	–
"Горячее" добавление/замена виртуальной памяти	–	–	да	да	–

Таблица В1 *(окончание)*

	Windows Server 2008 Web	Windows Server 2008 Standard	Windows Server 2008 Enterprise	Windows Server 2008 Datacenter	Itanium-системы
"Горячее" добавление/замена виртуальных процессоров	–	–	да	да	–
Лицензии на виртуальные машины (гостевые системы)	–	Хост+1 VM[1]	Хост+4 VM	не ограничено	не ограничено
Режим установки Server Core	да	да	да	да	–

* — в случае соответствия требований к аппаратным средствам *(см. далее)*.

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-[2] и x64-систем (предел может быть выше за 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

Перечень требований к аппаратной конфигурации, необходимой для Windows Server 2008, представлен в табл. В2. Отдельные параметры в значительной степени зависят от набора установленных ролей сервера.

---

[1] Это означает, что лицензия на установленную систему распространяется и на одну (или четыре, или неограниченное количество) систему Windows, запущенную в виртуальной среде.

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

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 При использовании роли Hyper-V или системы Hyper-V Server: 64-разрядный (x64) процессор с тактовой частотой 2 ГГц (и выше) и аппаратной поддержкой виртуализации (Intel VT или AMD-V). Аппаратная поддержка Data Execution Protection (DEP) Процессор Intel Itanium 2 для Itanium-систем (IA64)
Оперативная память	Не менее 512 Мбайт (1 Гбайт для Hyper-V Server); реально требуется 2 Гбайт и более. При использовании роли Hyper-V необходимо учитывать память, выделяемую каждой гостевой (guest) системе
Монитор	Минимально поддерживаемое разрешение экрана 800 на 600, в реальности требуется 1024 на 768 и выше[1]. Глубина цвета — 16 бит (рекомендуется 32 бита[2])
Видеоадаптер	Для базовых режимов особых требований нет. При использовании темы *Windows Vista* обязательна совместимость с DirectX 9.0; требуются поддержка Pixel Shader 2.0, драйверы, отвечающие спецификации *Windows Vista Display Driver Model* (WDDM)[3], объем видеопамяти не менее 64 Мбайт *(см. далее)*
Жесткие диски	Раздел на жестком диске с объемом свободного пространства не менее 10 Гбайт[4] 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 памяти (ОЗУ), установленной 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

[1] Минимум для комфортной работы — 1280 на 1024; при использовании стиля Aero Glass глубина цвета — 32 бита (при меньшем значении данный стиль отключается).
[2] Для лучшего отображения всех значков и окон!
[3] Не следует путать эту аббревиатуру с WDM (Win32 Driver Model).
[4] 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 некоторых встроенных приложений (например, при записи архивов на DVD-диски и т. п.).

Внимание!

При установке роли Hyper-V (в полной версии Windows Server 2008) или системы Microsoft Hyper-V Server выполняется проверка аппаратной поддержки функций виртуализации. Помимо процессора эти функции должны поддерживаться и ***быть активированы*** на материнской плате компьютера и в БИОСе (может потребоваться его обновление). Включение функции Data Execution Protection (DEP) также выполняется в БИОСе (эта опция может называться по-разному, например, Execute Disable Bit = Enabled в разделе конфигурации процессора). В полных версиях о ее наличии можно судить по сообщению "Your computer's processor supports hardware-based DEP" (Процессор вашего компьютера имеет аппаратную поддержку DEP), которое появляется в окне **Performance Options** (Параметры производительности) — кнопка **Settings** (Параметры) на панели **Performance** (Производительность) в окне дополнительных свойств системы (см. рис. 2.11).

Если названные условия не соблюдаются, то возникнет ошибка при добавлении роли или же установка системы Microsoft Hyper-V Server будет прекращена.

Дифференциация требований к графической подсистеме

Базовые (выбранные по умолчанию) режимы работы графической подсистемы Windows Server 2008 не предъявляют особых требований к аппаратным средствам — практически на любых компьютерах будут доступны стили *Windows Vista Basic* (Упрощенный стиль Windows Vista) или *Windows Classic* (Классический стиль). Однако могут возникнуть дополнительные требования при использовании всех возможностей нового визуального интерфейса *Aero Glass*, появившегося в Windows Vista и в полном объеме доступного также и в Windows Server 2008 *(см. главу 2)*.

Можно выделить три качественных уровня, определяющих возможности пользовательского графического интерфейса:

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



Глава 1

Установка систем и виртуальных машин

Эта глава посвящена различным способам установки операционных систем Windows Server 2008 и их подготовке к эксплуатации. Рассматриваются основные вопросы, возникающие с момента планирования новой инсталляции и до ее готовности к использованию в рабочих условиях. (Средства конфигурирования уже установленной системы, настройка ее компонентов и служб под конкретные задачи (роли сервера) рассматриваются отдельно в *главе 2*.)

Также описывается установка виртуальных машин при использовании роли *Hyper-V* в полных версиях Windows Server 2008 или специального продукта Microsoft Hyper-V Server 2008.

Подготовка к установке системы

В этом разделе рассматриваются небольшие, но принципиальные вопросы, с которыми нужно определиться до начала установки системы; от ответов на эти вопросы зависит выбор опций в процессе инсталляции и последовательность последующих действий. Планирование действий позволит избежать ошибок при инсталляции (что чревато необходимостью повторной установки, потерей пользовательских настроек или вынужденными ограничениями при дальнейшей работе с компьютером).

Системы 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 ознакомиться с начальными разделами *главы 4*, поскольку в них 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).

При планировании разметки дисковых томов следует предусмотреть возможности их архивации и восстановления *(см. главу 5)*. Например, если операционная система и данные будут храниться на одном диске, то это осложнит процесс архивации, поскольку стандартные средства Windows Server 2008 позволяют работать только с целыми томами (следовательно, сохранить отдельно или систему, или данные не получится).

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 неизмененном 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. далее разд. "Организация систем с двойной загрузкой")*.

Систему 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. Для сложных случаев имеется возможность использования утилиты DiskPart *(см. далее)*.

> ***ВНИМАНИЕ!***
>
> Программа установки Windows Server 2008 создает на жестком диске только *основные* разделы *(см. главу 4)*. Если необходима более сложная конфигурация логических дисков, то ее нужно готовить заранее.

- Загрузившись с дистрибутивного диска и воспользовавшись опцией восстановления системы *(см. далее разд. "Опции восстановления при загрузке с инсталляционного диска")*, 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 создаются с помощью административных средств этой операционной системы (обычно для этих целей используется оснастка **Disk Management** (Управление дисками)).

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 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 Server 2008 без особых проблем можно установить на компьютеры, на которых *уже* имеются инсталлированные 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* — появится возможность выбора операционной системы при запуске компьютера (в принципе, этих систем может быть две, три и более).

Чтобы подобная конфигурация была работоспособной, необходимо соблюдать 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 утилитами, которые доступны при загрузке с дистрибутивного диска Windows Server 2008.

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 диспетчера 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 установлены 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.

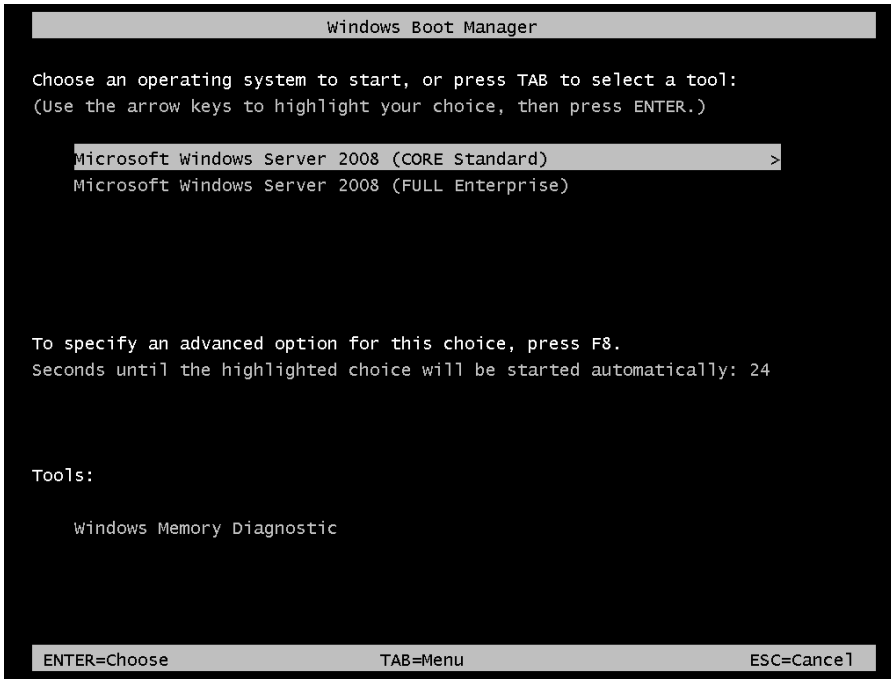


Рис. 1.1. Окно выбора загружаемой операционной системы

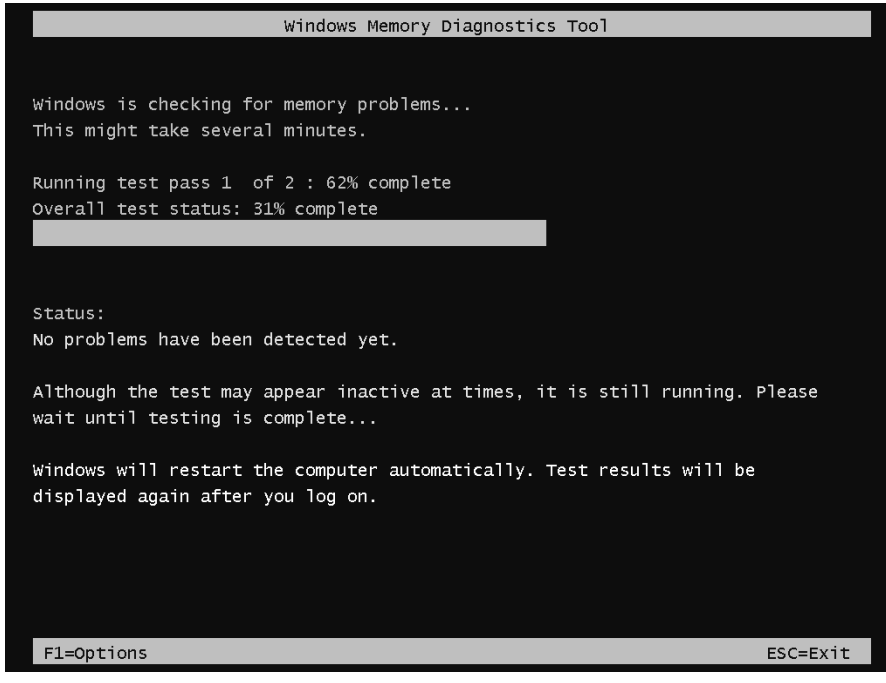


Рис. 1.2. Экран утилиты диагностики памяти

В окне параметров (рис. 1.3) выбирается подмножество тестов для диагностики (по умолчанию выполняется стандартный набор), указываются 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 о результатах выполнения теста.

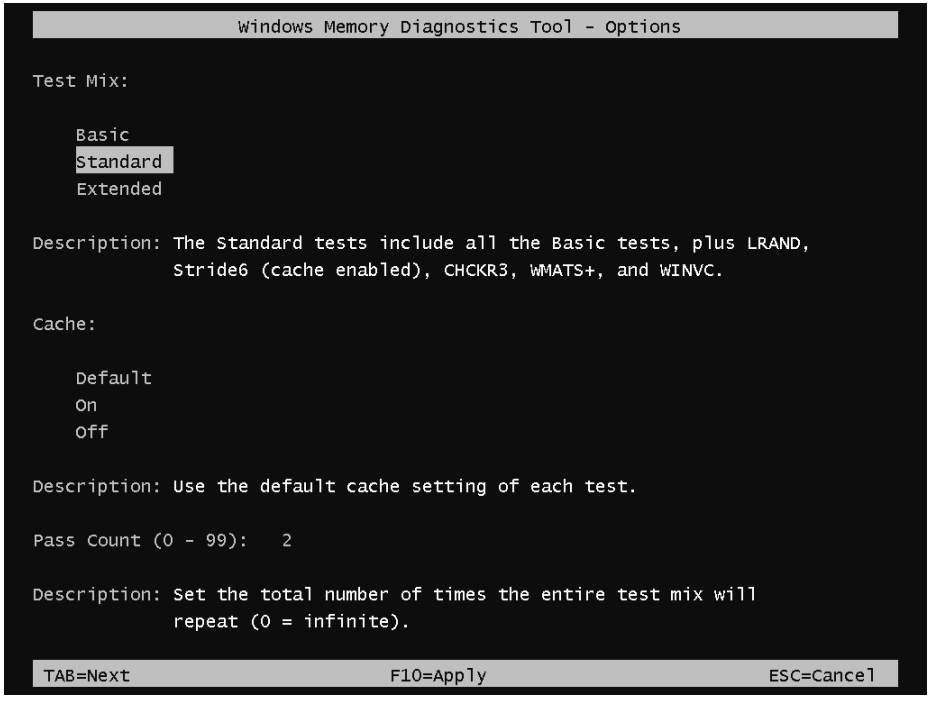


Рис. 1.3. Окно выбора параметров работы утилиты диагностики памяти

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). 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).

Управление опциями загрузки

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 получив полномочия администратора*** (т. е. окно консоли необходимо открывать от имени администратора — в заголовке окна должно присутствовать слово Administrator (Администратор)). Параметры команды можно получить, выполнив команду `bcdedit /?`.

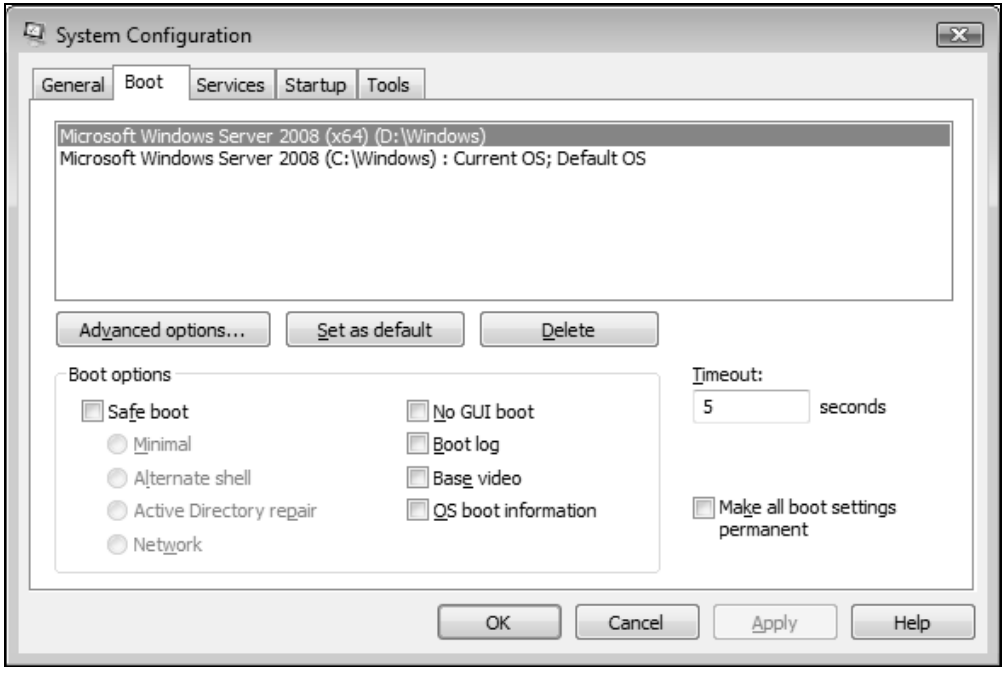


Рис. 1.4. Управление опциями диспетчера загрузки с помощью утилиты System Configuration

При запуске без параметров утилита выводит параметры имеющихся записей базы данных диспетчера загрузки. Текущую конфигурацию можно сохранить в файле с помощью следующей команды (при этом также появляются файлы вида `bcdbackup.LOG`):

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

Следующая команда позволит поменять строку, отображаемую в меню выбора систем, для *загруженной в данный момент* (имеющей идентификатор `{current}`) системы:

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

Изменить загружаемую по умолчанию систему можно с помощью команды вида (указывается идентификатор требуемой системы)

```
bcdedit /default {cbd971bf-b7b8-4885-951a-fa03044f5d71}
```

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. 1.4) перечислены опции меню выбора операционных систем и можно устанавливать особые режимы загрузки.

Наибольшими возможностями по конфигурированию опций загрузки Windows Vista/Windows Server 2008 обладают специализированные бесплатные утилиты, которые несложно найти в Интернете: например, *EasyBCD* или *VistaBootPro*. Эти утилиты могут устанавливаться и работать и в предыдущих версиях Windows.

Особенности Windows Server 2008 Server Core

Режим установки базовых служб — *Windows Server 2008 Server Core* — требует особого внимания к вопросам планирования, поскольку возможности систем в этом случае значительно ограничены. (При этом процесс установки сервера ничем не отличается от стандартной процедуры инсталляции системы.)

В режиме Server Core поддерживаются только следующие роли сервера (сравните с табл. 2.1):

- Active Directory Domain Services (AD DS)
- Active Directory Lightweight Directory Services (AD LDS)
- DHCP Server
- DNS Server
- File Services (ограничены в редакции Standard)
- Hyper-V
- Print Services
- Web Services (IIS) (с ограничениями)

При этом во всех редакциях недоступен такой важный компонент, как ASP.NET — следовательно, невозможна установка приложений, использующих эту спецификацию.

Необходимо учитывать и особенности администрирования инсталляций Windows Server 2008 Server Core. Первое, и основное, отличие этого режима — отсутствие графического интерфейса, т. е. после установки системы, загрузки и регистрации администратор увидит только пустой экран с окном консоли, а средства рабочего стола (включая меню **Start** (Пуск) и панель задач) будут отсутствовать. Полностью отсутствуют утилиты панели управления[1] (CPL-файлы) и среда консоли управления MMC, включая оснастки администрирования.

В распоряжении администратора остаются утилиты командной строки и диспетчер задач; возможно обычное переключение окон по клавишам <Alt>+<Tab> и переключение в окно безопасности при нажатии клавиш <Ctrl>+<Alt>+<Del>; для редактирования сценариев или командных файлов имеется простейший редактор Notepad.exe. Более-менее полноценное управление системой возможно только с использованием оснасток, запускаемых на рабочей станции и подключающихся удаленно к серверу.

> ***Примечание***
>
> 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*[2] посмотреть, как выглядит рабочая среда сервера. Чтобы вернуться к обычной среде, необходимо отредактировать реестр и вернуть переменной `Shell` исходное значение `explorer.exe`.

Интерактивная установка систем 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 10—20 минут (вместо 60 для предыдущих версий). (Однако процедура

---

[1] За исключением двух — *см. Приложение 2*.

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

обновления Windows Server 2003 до Windows Server 2008 по-прежнему занимает не менее часа, причем это 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[1] (2,16 Гбайт для x64). Традиционная папка \i386 на дистрибутивном диске отсутствует, 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).

Новая установка системы с загрузочного компакт-диска

Рассмотрим процедуру установки системы для самого простого случая — когда используется загрузочный дистрибутивный диск Windows Server 2008[2] и выполняется инсталляция системы на свободный раздел диска ("чистая" установка). Процесс установки системы значительно упростился по сравнению с Windows Server 2003, и теперь не требуется периодически отвечать на возникающие вопросы. Многие шаги отсутствуют, и изначально параметры (например, сетевые установки и принадлежность к определенной рабочей группе) выбираются по умолчанию; затем их можно поменять вручную, с панели управления или из окна новой специальной утилиты *Initial Configuration Tasks* (Задачи начальной настройки; oobe.exe — *см. далее*).

> ***Примечание***
>
> Установка системы Microsoft Hyper-V Server максимально проста, поскольку некоторые шаги (например, выбор версии или ввод серийного номера) там в принципе отсутствуют. Для конфигурирования системы после установки имеется специальная утилита (см. рис. 1.30).

[1] Для сравнения: дистрибутив Microsoft Hyper-V Server занимает 936 Мбайт, файл образа имеет размер 565 Мбайт.

[2] 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, загрузитесь с дистрибутивного компакт-диска. При этом устанавливается ядро системы и появляется окно выбора региональных стандартов: укажите нужный 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. 2.2) 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. 2.1.)

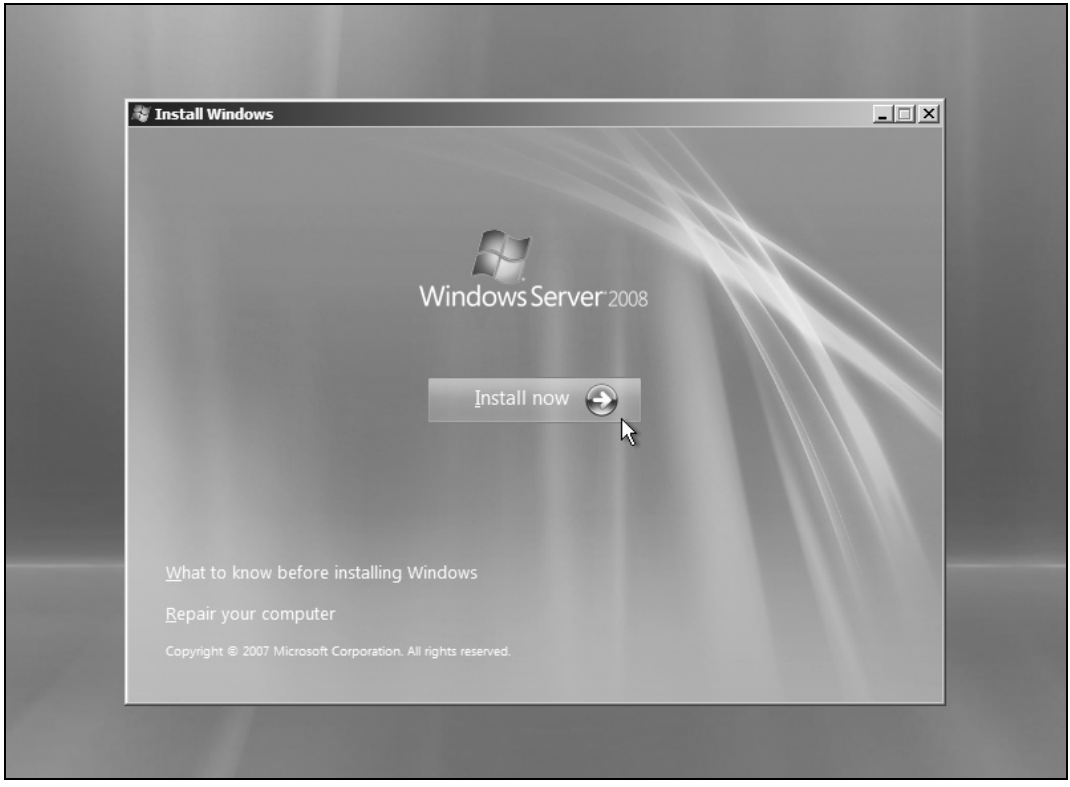


Рис. 1.5. Главное окно программы установки Windows Server 2008

2. В главном окне программы установки Windows (рис. 1.5) имеется ссылка **What to know before installing Windows** (Что следует знать перед выполнением уста-

новки Windows), позволяющая открыть 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 *далее* — см. рис. 1.23). Для запуска инсталляции нажмите кнопку **Install now** (Установить).

3. Введите серийный номер версии Windows Server 2008 (рис. 1.6). 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).

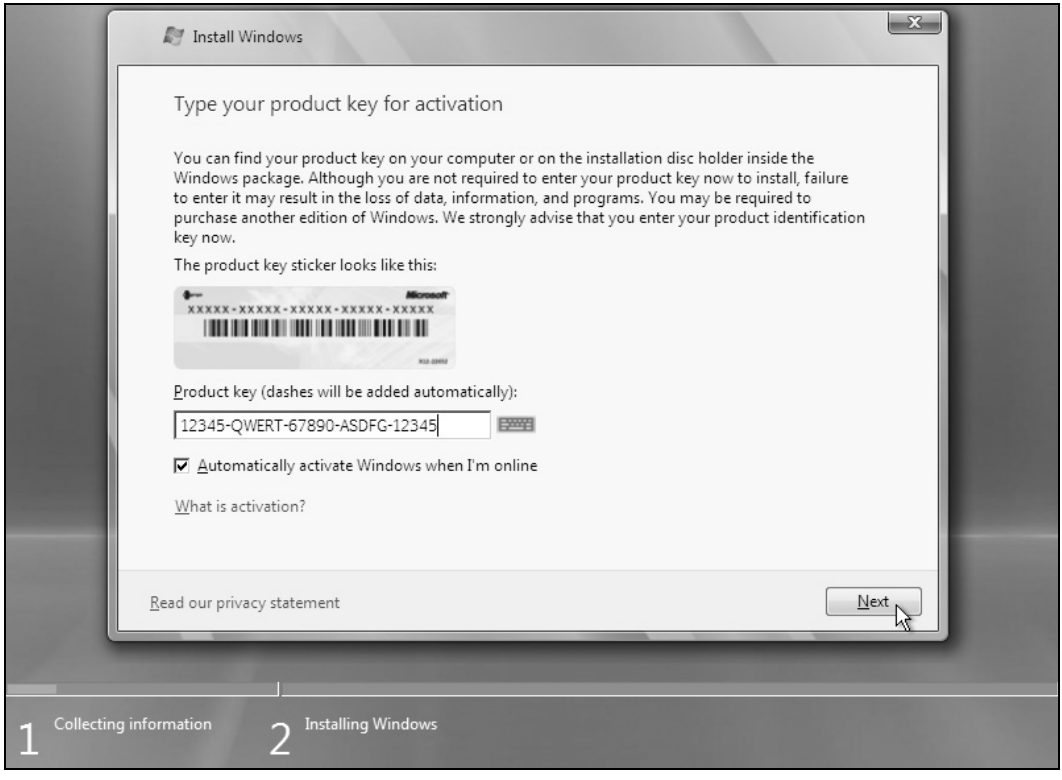


Рис. 1.6. Ввод серийного номера

При установке систем Windows Server 2008 можно не указывать сразу серийный номер и выбрать для инсталляции *любую* из редакций, имеющихся на ди-

стрибутивном диске. Этот режим удобен при работе с trial-версиями, которые можно скачать с веб-сайта Microsoft. 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)*.

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. 1.7); при этом обязательно нужно отметить флажок **I have selected the edition of Windows that I purchased** (Выбран приобретенный выпуск Windows).

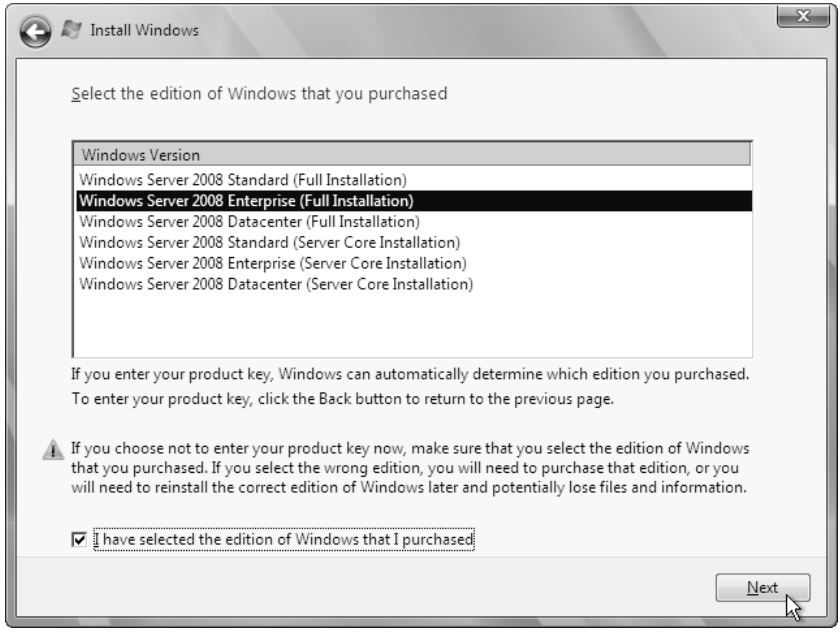


Рис. 1.7. Выбор версии устанавливаемой системы

4. На следующем этапе 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.
5. Далее предлагается выбрать способ установки системы: обновление (upgrade) или "чистая" (custom) установка (рис. 1.8). На этом шаге выбора фактически нет

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

(можно также видеть сообщение о запрете обновления), поскольку в любом случае для обновления уже инсталлированной системы программу установки нужно запускать *непосредственно из* этой системы *(см. далее)*. Для продолжения инсталляции выберите опцию **Custom (advanced)** (Полная установка (дополнительные параметры)).

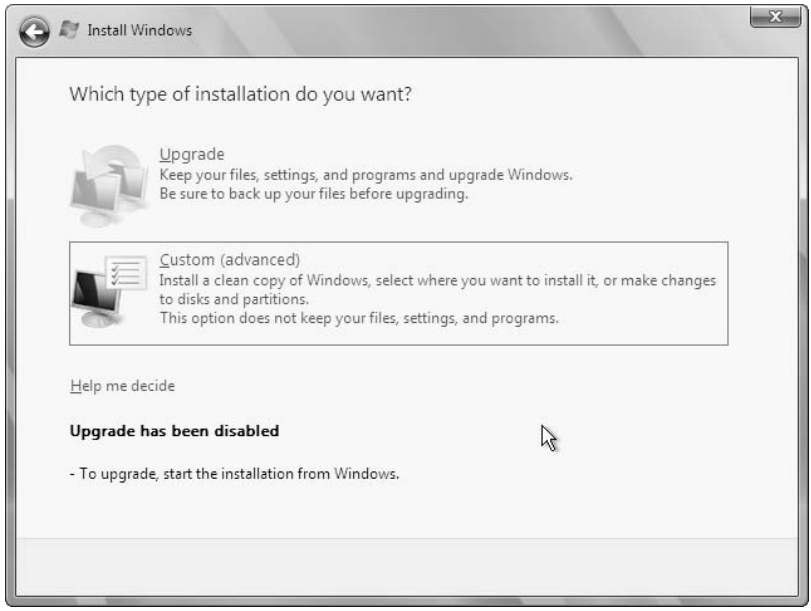


Рис. 1.8. Обновление невозможно, доступна лишь опция чистой установки системы

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. 1.9). *Вновь созданный* для установки раздел обязательно форматируется, при этом возможность выбора типа файловой системы отсутствует.

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"*.

Если необходимы какие-то манипуляции с дисками непосредственно во время установки системы, то можно нажать клавиши <Shift>+<F10>, после чего "параллельно" с программой установки (ее работа не прервется) откроется окно командной строки, где можно запустить утилиту DiskPart и выполнить нужные действия. Затем установку системы можно продолжить.

На рис. 1.9 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).

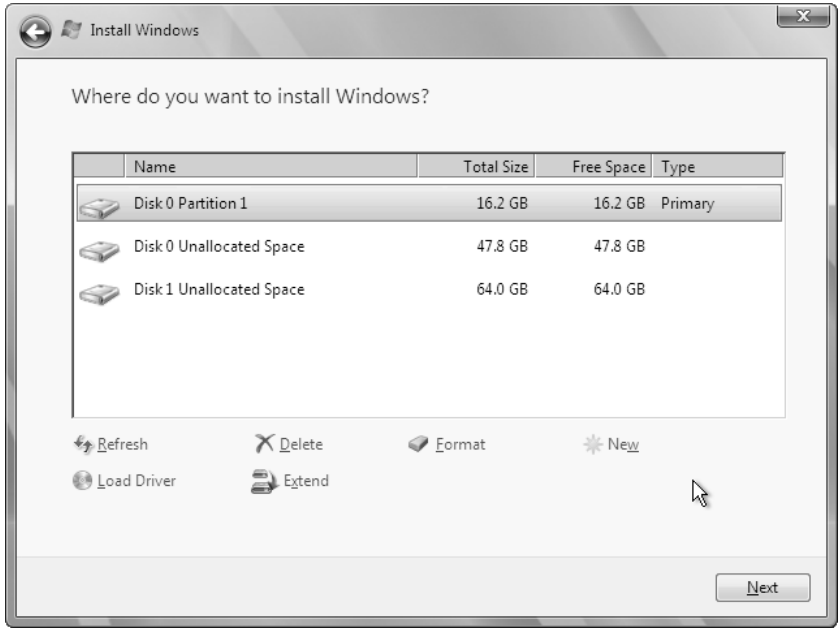


Рис. 1.9. Выбор раздела для установки

7. Теперь в течение 15—20 минут компьютер не требует никакого внимания, поскольку все дальнейшие действия выполняются в автоматическом режиме. На экране будет отображаться процесс выполнения инсталляционных процедур, во время которых компьютер может несколько раз перезагружаться. Два самых длительных по времени этапа — это извлечение файлов и установка компонентов.

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.

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 версий Windows Server 2008 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. 1.5), можно начать процедуру обновления имеющейся операционной системы. Программа предложит выполнить подключение к Интернету и загрузить последние обновления, необходимые для выполнения операции (рис. 1.10). 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 не менее часа (в зависимости от наличия дополнительных серверных служб). После загрузки обновлений программа установки будет перезапущена.

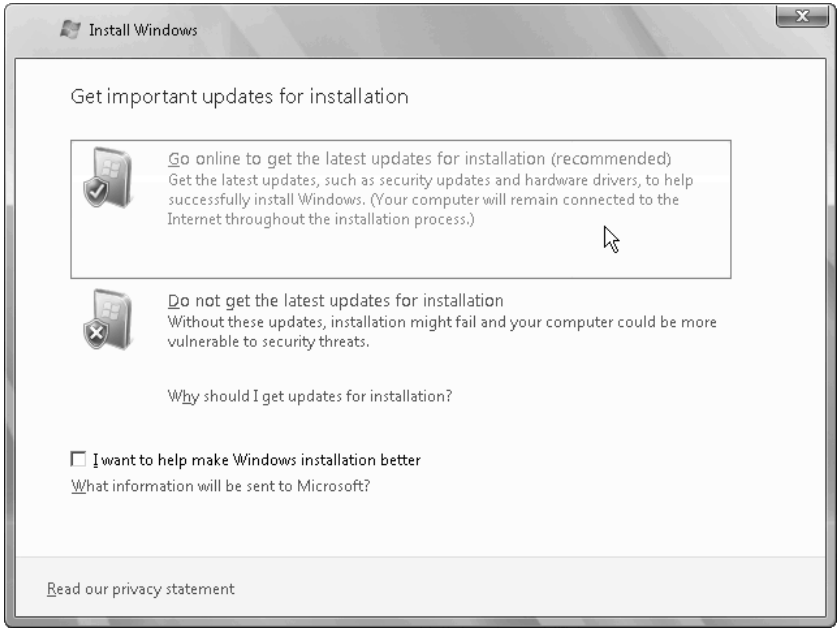


Рис. 1.10. Запрос на получение обновленных файлов для установки системы

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 ре-

дакции 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 проверки прошли нормально, то появляется окно, в котором можно выбрать тип установки (рис. 1.11): теперь помимо полной установки возможно обновление системы (сравните с рис. 1.8).

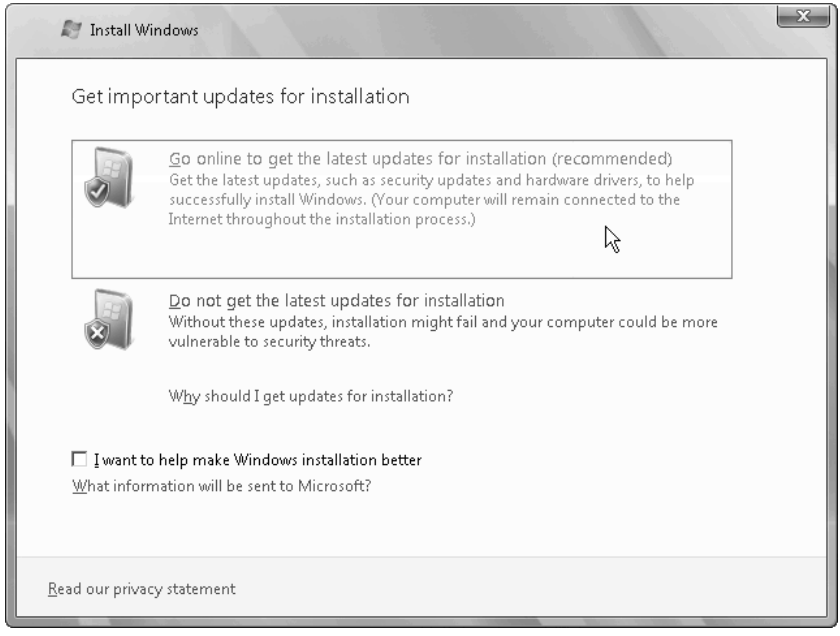


Рис. 1.11. Выбор типа установки в том случае, когда возможно обновление

При выборе обновления системы 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. Напомним, что обновление длится существенно дольше (в несколько раз), чем обычная установка новой системы.

Примечание

Особенности обновления контроллеров доменов Active Directory, связанные с изменением схемы каталога, рассматриваются в *главе 7*.

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 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. 1.12) (это верно, поскольку никакого пароля в процессе установки не задавалось). Необходимо установить и подтвердить пароль; можно сразу создать дискету восстановления пароля. После появления сообщения об успешном изменении пароля можно входить в систему.



Рис. 1.12. 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.

Для версий Windows Server Core и Hyper-V Server вход в систему после установки выполняется несколько иначе. После загрузки появляется экран регистрации, где нужно нажать клавиши <Ctrl>+<Alt>+<Del>, а затем — появляющуюся кнопку **Other User** (Другой пользователь). После этого вводится имя пользователя Administrator (других пользователей в системе еще нет!), без пароля. Только после этого появляется предупреждение о смене пароля (см. рис. 1.12).

Из командной строки пароль администратора всегда можно поменять с помощью команды `net USER administrator *`.

Начальное конфигурирование системы

Перед тем как новый сервер будет полностью готов к работе, необходимо определить рабочие параметры, которые не были заданы на этапе установки системы (некоторые из этих параметров являются обязательными). Особенно это актуально для систем Windows Server Core, где отсутствуют какие-либо вспомогательные утилиты конфигурирования. Для начала рассмотрим список параметров в целом с учетом возможностей их ручной настройки.

Основные рабочие параметры сервера

Ниже перечисляются параметры сервера с указанием способов настройки из командной строки или ссылок на главы, где компонент рассматривается подробно:

- **имя компьютера** — изначально дается произвольное, например, WIN-7E16OJGOHRP. Его можно поменять с помощью команды `netdom RENAMECOMPUTER /NewName`;
- **сетевые параметры** (IP-адрес, адрес шлюза и предпочитаемого DNS-сервера) *(глава 2)*;
- **подключение к домену** (удаление из домена) — для подключения сервера к домену используется команда `netdom JOIN`, для отключения — `netdom REMOVE`. В команде следует указывать имя и пароль доменного пользователя, имеющего право на выполнение операции;
- **активация системы** *(см. далее)*;
- параметры службы **Windows Update** *(см. далее)*;
- **разрешение монитора** *(глава 2)*;
- **время и дата** (временная зона) (утилита Timedate.cpl);
- **региональные параметры** (утилита Intl.cpl, *глава 2*);
- **подключение к удаленному рабочему столу** (Remote Desktop) *(глава 2)*;
- **пользователи и группы** *(глава 2)*;
- **брандмауэр Windows** *(глава 6)*;
- **роли и компоненты** *(глава 2)*;

После изменения некоторых из перечисленных параметров требуется *перезагрузка* компьютера, которую легко выполнить с помощью следующей команды:

```
shutdown /r /t x
```

где параметр `/r` указывает на необходимость перезагрузки, а `/t` — время ожидания до начала операции (0 — для немедленного выполнения).

Для *выключения* компьютера служит команда `shutdown /s /t 0`.

Использование мастера конфигурирования

В полных версиях Windows Server 2008 задача начальной настройки параметров сервера облегчается: при первом входе в систему администратор увидит окно программы *Initial Configuration Tasks* (Задачи начальной настройки) (рис. 1.13; на рисунке показаны исходные значения параметров, до внесения каких-либо изменений). Здесь перечислены 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.

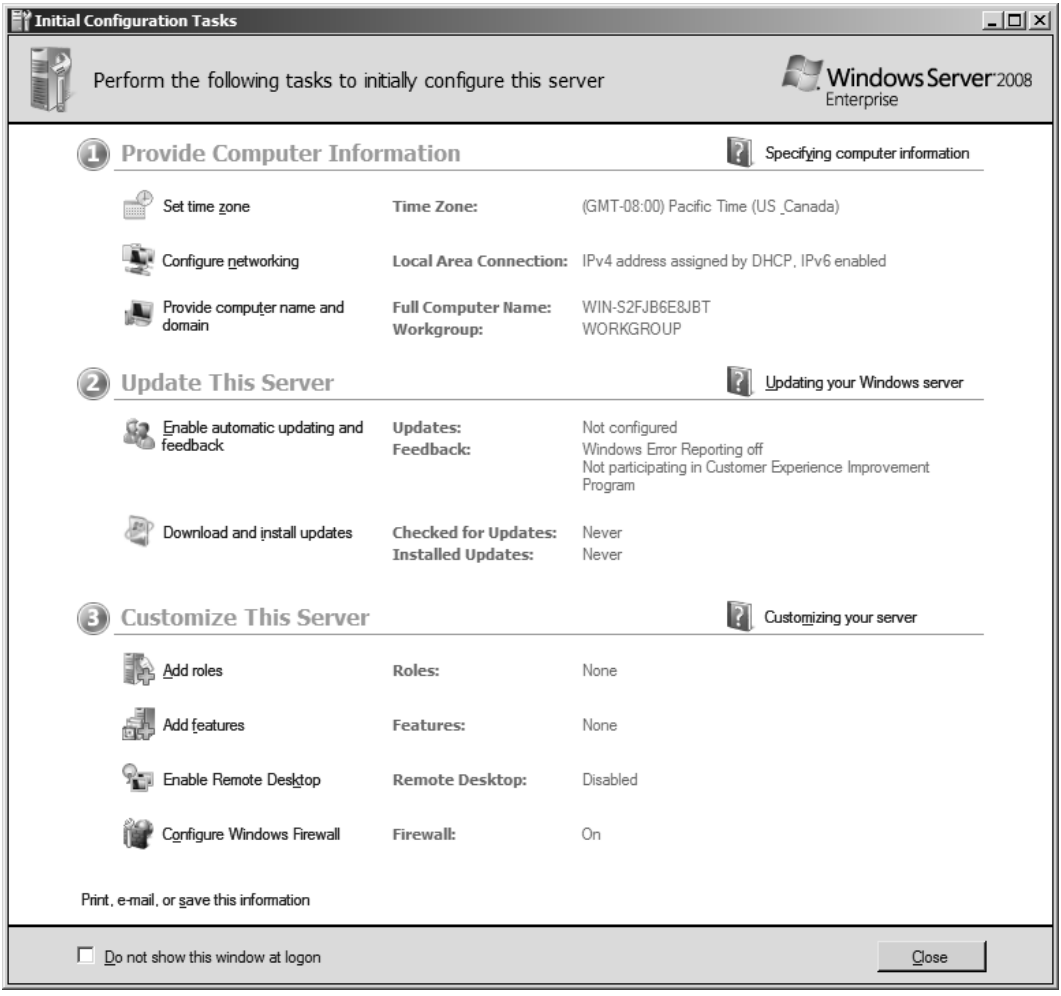


Рис. 1.13. Программа начальной настройки позволяет установить основные рабочие параметры системы

Примечание

В системе Microsoft Hyper-V Server аналогичную функцию выполняет утилита *HVConfig*, которая будет рассмотрена далее (см. рис. 1.30).

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. далее)*.

Сразу же можно добавить роли и компоненты сервера, включить удаленный доступ к рабочему столу и настроить брандмауэр.

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).

После того как при первом входе в систему окно задач начальной настройки будет закрыто, на экране появится окно основного средства администрирования сервера — окно оснастки **Server Manager** (Диспетчер сервера) (см. рис. 1.15).

Похожее средство под названием *Manage Your Server* имеется в системах Windows Server 2003 (рис. 1.14). 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. 1.15) в системах Windows Server 2008 имеет значительно бóльшие возможности, чем мастер Manage Your Server, и позволяет в своем окне управлять практически всеми ролями сервера, службами и компонентами. При первом запуске в окне диспетчера сервера можно видеть общую информацию о компьютере (включая параметры, заданные с помощью программы Initial Configuration Tasks (Задачи начальной настройки) — например, имя компьютера, рабочую группу, IP-адрес и т. д.) и параметры безопасно-

сти (состояние брандмауэра и службы обновления). (На рисунке окно программы специально показано полностью, чтобы лучше был понятен ее интерфейс.)

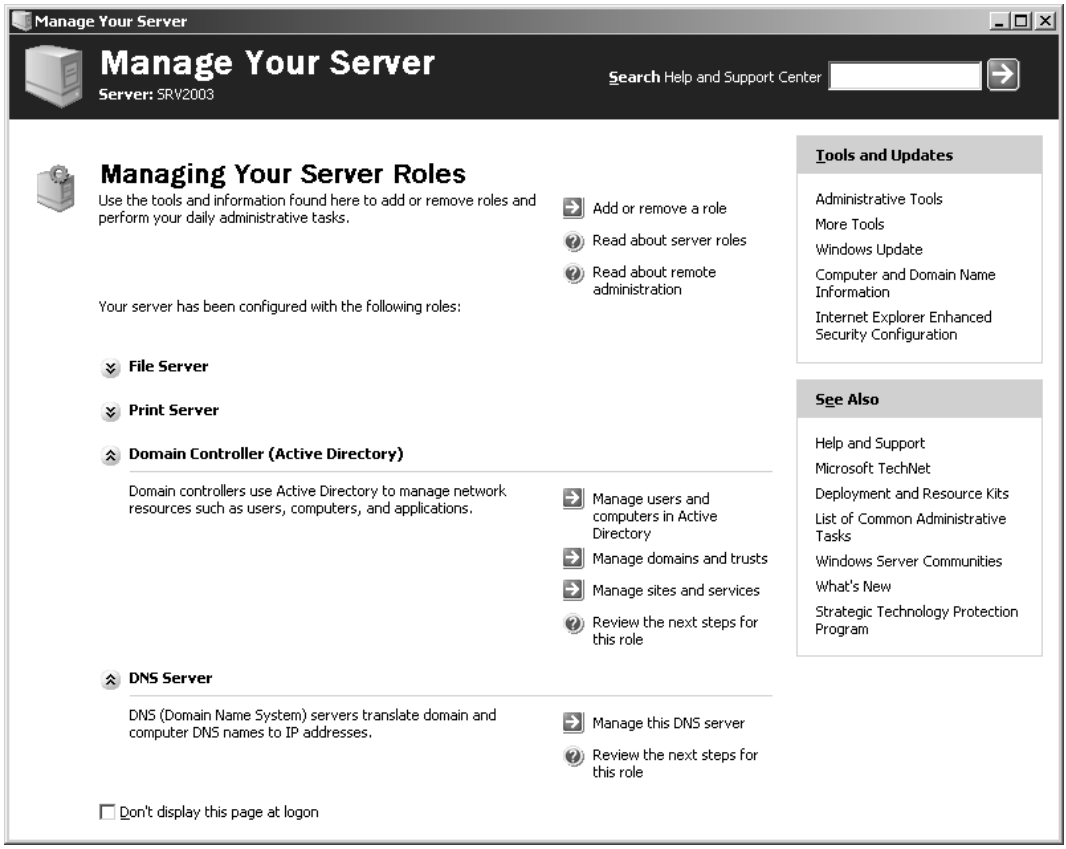


Рис. 1.14. Окно программы Manage Your Server в системах Windows Server 2003

Оснастка **Server Manager** (Диспетчер сервера) позволяет устанавливать роли сервера, службы и компоненты, более того — в Windows Server 2008 она является ***единственным средством*** (если не считать утилиты ServerManagerCmd.exe), позволяющим изменять набор функциональных возможностей сервера.

Подробно процедура установки ролей и компонентов сервера с использованием оснастки **Server Manager** (Диспетчер сервера) рассматривается в *главе 2*.

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`.



Рис. 1.15. Начальный вид оснастки **Server Manager**

Установка параметров автоматического обновления Windows

Функция автоматического обновления *Windows Update* (сервис wuauserv; исполняемый файл утилиты настройки — wuapp.exe) представляет собой системный сер-

вис, который стартует автоматически и периодически выполняет сканирование системы, чтобы определить, имеются ли на сайте Windows Update обновления, доступные для загрузки. Загрузка обновлений может осуществляться 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.

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

> ***ВНИМАНИЕ!***
>
> Особенно важно установить все обновления после инсталляции системы, поскольку имеются обновления, критически важные для работы некоторых ролей сервера (например, для Hyper-V). Проще автоматически установить все обновления, чем искать и устанавливать отдельные файлы для конкретных случаев.

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)).

Для изменения параметров службы обновления требуются следующие операции:

1. Откройте окно *Центра обновления Windows* (Windows Update), выполнив одноименную команду в меню **Start** (Пуск) или выбрав соответствующую задачу на панели управления (также можно непосредственно ввести имя программы `wuapp`). В этом окне (рис. 1.16) 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. 1.17) 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);

- 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;
- 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, поскольку одновременно 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.

Также имеются дополнительные параметры:

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

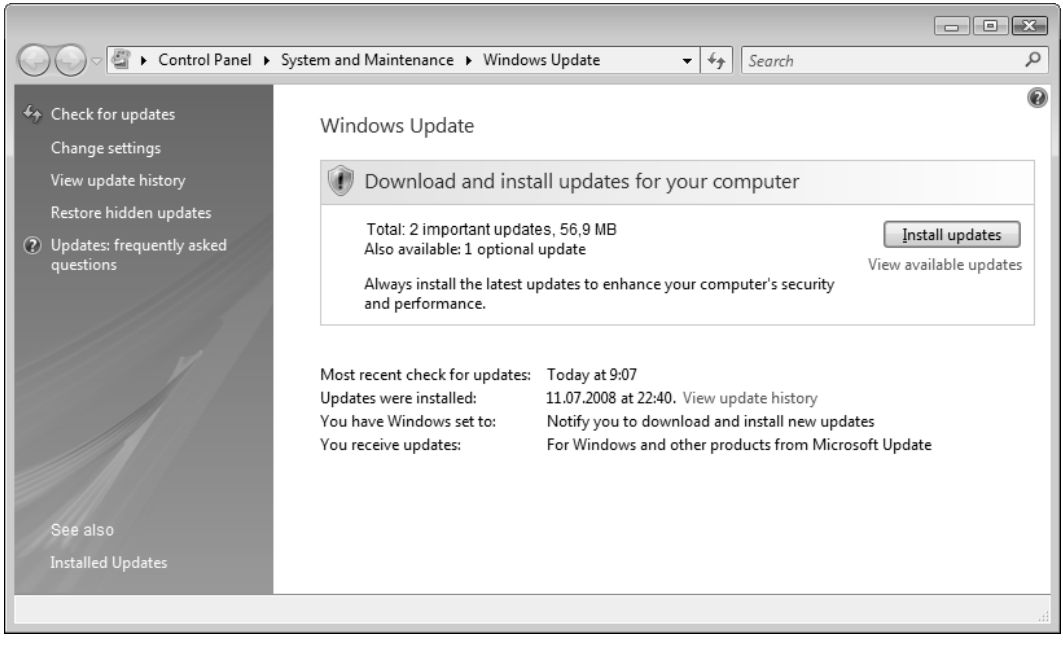


Рис. 1.16. Главное окно Центра обновлений Windows

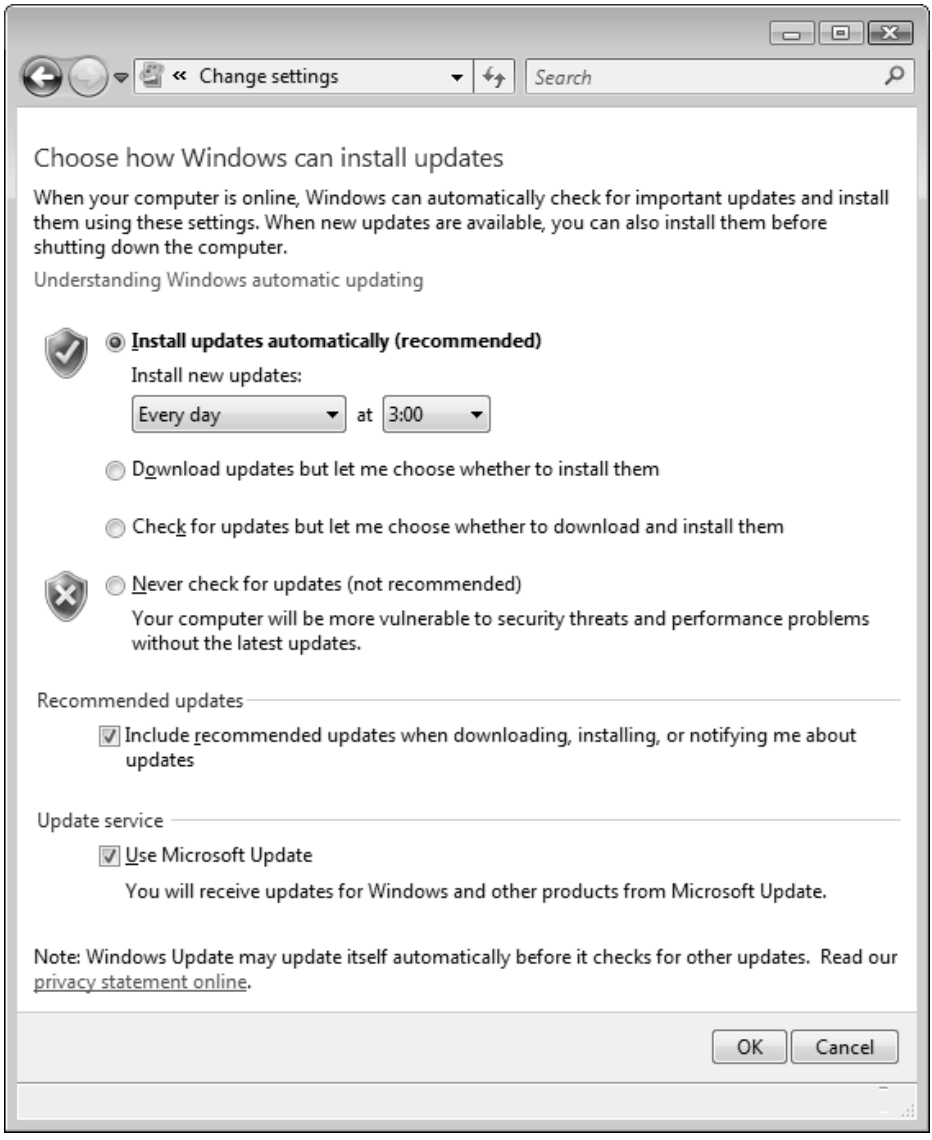


Рис. 1.17. Окно параметров автоматического обновления системы

- 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 вебстранице 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**.

Ручная настройка

Для службы автоматического обновления в системном реестре имеется раздел `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update`. Главным здесь является параметр `AUOptions` (DWORD), определяющий состояние службы. В редакциях Windows Server Core и Hyper-V Server этот параметр по умолчанию отсутствует.

Для настройки режима и выполнения поиска (и установки) обновлений в системе Hyper-V Server имеются специальные опции (пункты 5 и 6) в окне утилиты *HVConfig* (см. рис. 1.30); в редакциях Windows Server Core конфигурирование режима нужно выполнять вручную (с помощью специального сценария или непосредственно редактируя реестр в редакторе Regedit).

> ***Примечание***
>
> В системе Hyper-V Server для проверки и установки обновлений можно также применять сценарий WUA_SearchDownloadInstall.vbs, который следует искать в папке *%SystemRoot%*\System32 в подкаталоге, имя которого соответствует языку системы, например, en-US.

Для настройки некоторых параметров системы имеется служебный сценарий SCregEdit.wsf, находящийся в папке *%SystemRoot%*\System32. Возможности этого сценария можно увидеть, запустив его без параметров.

Для просмотра состояния службы обновления служит следующая команда (изначально параметр `AUOptions` отсутствует, и значения для него нет):

```
C:\Windows\System32>cscript SCregEdit.wsf /au /v
SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update AUOptions
Value not set.
```

Запретить автоматические обновления можно с помощью команды `cscript SCregEdit.wsf /au 1` — после ее выполнения появляется параметр `AUOptions`, равный 1. Для *разрешения* автоматических обновлений используется команда `cscript SCregEdit.wsf /au 4`.

После любых изменений в реестре службу обновлений необходимо перезапустить, выполнив следующую команду:

```
net stop Wuauserv && net start Wuauserv
```

Список установленных обновлений в любой версии Windows Server 2008 можно посмотреть с помощью утилиты *Systeminfo.exe*; следующая команда позволяет получить более подробную информацию о всех обновлениях:

```
wmic qfe list
```

Активация системы

Если при установке системы была разрешена автоматическая активация, то система пытается сразу же выполнить ее через Интернет. Если же флажок разрешения активации был сброшен (например, при установке пробной (trial) версии), 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. 2.10), 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. 1.18.

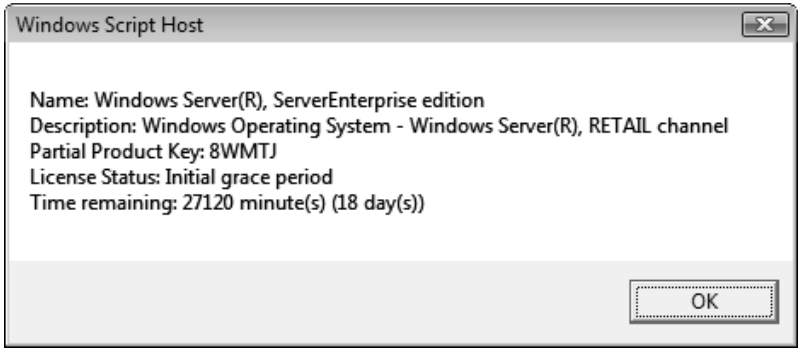


Рис. 1.18. Сообщение о лицензионном статусе системы

Вручную инициировать активацию системы можно из окна свойств системы (см. рис. 2.10) или же с помощью команды `slmgr -ato`.

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 систем

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 описывать и изучать его возможности нужно отдельно.

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 1*). Пакет хранится в виде образа (IMG) диска, его размер

для английской версии составляет 1375,9 Мбайт. После загрузки образ необходимо записать на DVD-болванку и запустить с диска программу установки.

Для установки на компьютер основных средств пакета в главном окне программы установки 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. 1.19).

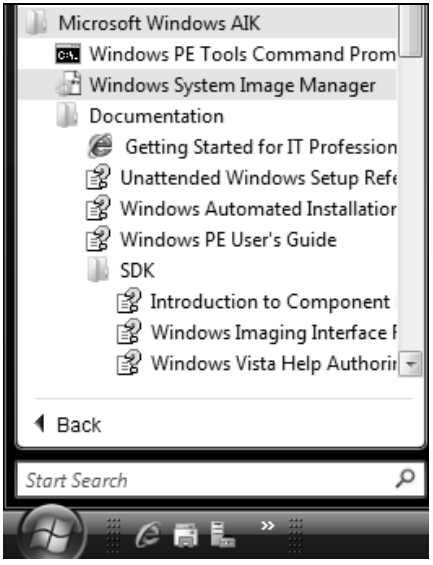


Рис. 1.19. Средства пакета Windows AIK, установленные на компьютере

Основным средством подготовки *файлов ответов* (answer files) для автоматической установки (unattended setup) является программа *Windows System Image Manager* (рис. 1.20). Файл ответов (в формате XML), обычно называемый Unattend.xml, содержит параметры и значения, необходимые для работы программы установки Windows (Windows Setup).

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.

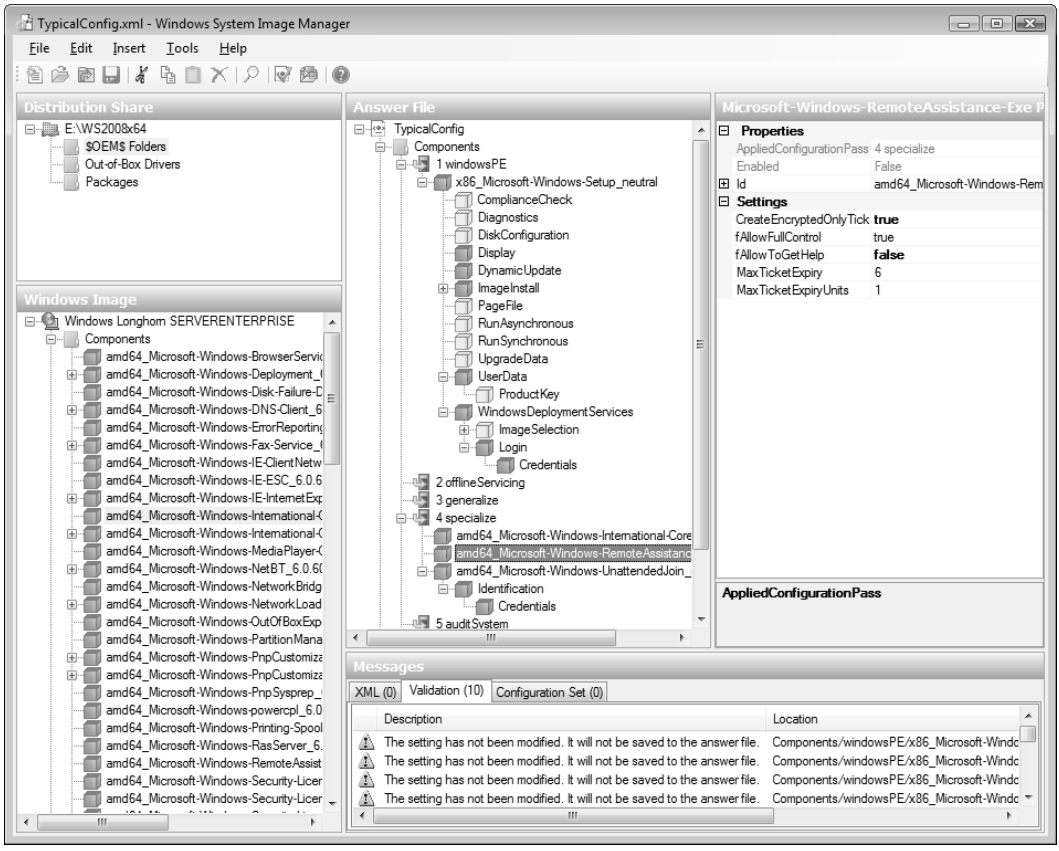


Рис. 1.20. Главное окно программы Windows System Image Manager

Средства восстановления системы при сбоях

В составе Windows Server 2008 имеется множество средств, поддерживающих целостность системы и обеспечивающих возможность восстановления поврежденной системы. Среди них можно 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. 1.28 — кнопка **Roll Back Driver** (Откатить)).

К этому следует добавить возможность восстановления полного архива системы. (В системах Windows Vista эта функция называется Windows Complete PC; помимо нее в этих системах имеются дополнительные средства, отсутствующие в серверных версиях, — возможность создания точек восстановления и функция System Restore.)

Существуют различные варианты загрузки операционной системы, список которых (рис. 1.21) 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).

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.

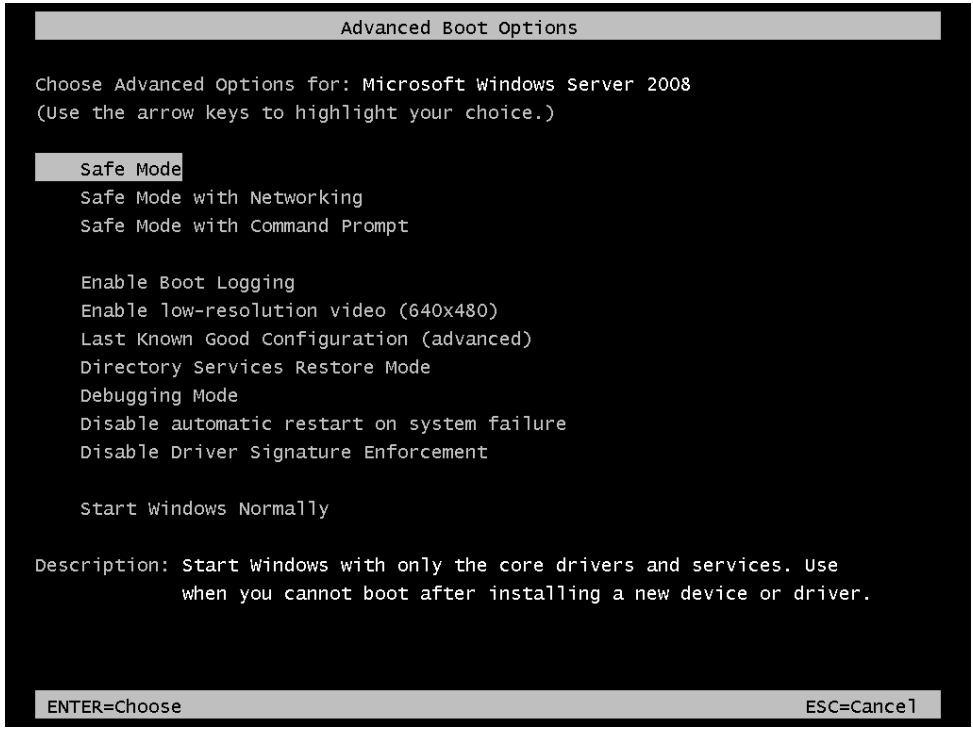


Рис. 1.21. Меню дополнительных режимов загрузки Windows Server 2008

Опции восстановления при загрузке с инсталляционного диска

После загрузки с дистрибутивного DVD-диска появляется окно программы установки Windows (см. рис. 1.5), в котором по ссылке **Repair your computer** (Восстановление системы) перейдите в меню функций восстановления системы. Сначала выберите систему, с которой нужно работать (рис. 1.22), и нажмите 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)).

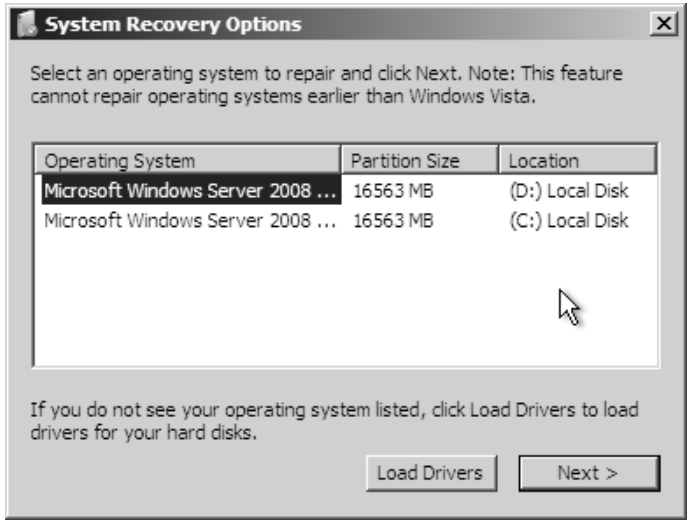


Рис. 1.22. Выбор восстанавливаемой системы

В следующем окне (рис. 1.23) выполняется выбор служебных и диагностических функций. (Для Windows Vista таких 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 *(см. главу 5)*.

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). Она позволяет протестировать память компьютера. Запуск теста памяти можно инициировать и из работающей системы, для этого имеется соответст-

вующая опция в группе **Administrative Tools** (Администрирование). При этом тест все равно будет выполняться в процессе загрузки системы.

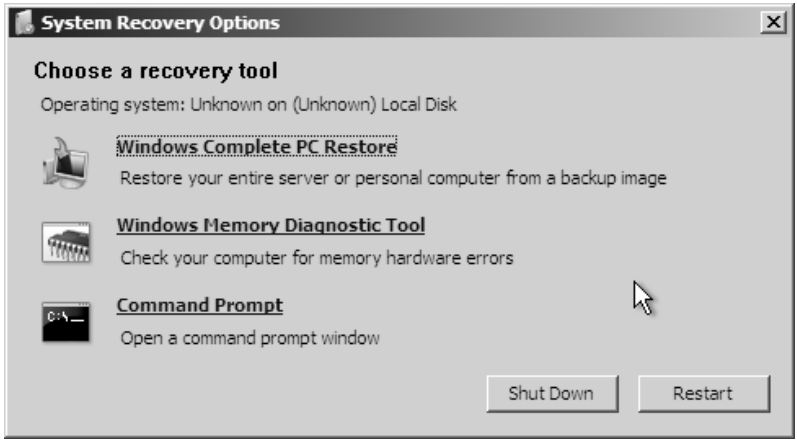


Рис. 1.23. Опции восстановления системы Windows Server 2008

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.

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 про-

цесса 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 инициализации 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. 1.26).

> ***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*.)

Процесс конфигурирования состоит из следующих этапов:

1. Укажите местоположение папки в разделе NTFS, где будут храниться образы систем, устанавливаемых с данного сервера. По умолчанию это папка C:\RemoteInstall.
2. Определите политику ответов сервера на запросы *известных* (known) и *неизвестных* (unknown) клиентов. (Для известных клиентов в каталоге Active Directory имеется заранее созданная учетная запись компьютера.) По умолчанию сервер вообще не отвечает на запросы клиентов (рис. 1.24). Выбранную политику можно потом поменять в окне свойств WDS-сервера (см. рис. 1.27) на вкладке **PXE Response Settings** (Параметры PXE-ответа).



Рис. 1.24. Определение политики ответов на запросы клиентов

Добавление образов

После нажатия кнопки **Finish** (Готово) в последнем окне мастера конфигурирования (см. рис. 1.24) выполняется настройка WDS-сервера, а затем мастер установки

предлагает сразу же добавить в хранилище образы системы. Эта процедура выглядит следующим образом:

1. Укажите путь к файлам boot.wim (*загрузочный* образ) и install.wim (*установочный* образ). В простейшем случае можно вставить в DVD-привод дистрибутивный диск и указать букву дисковода.
2. Дайте 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 укажите, какие образы будут копироваться в хранилище (рис. 1.25).

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. 1.26). 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.

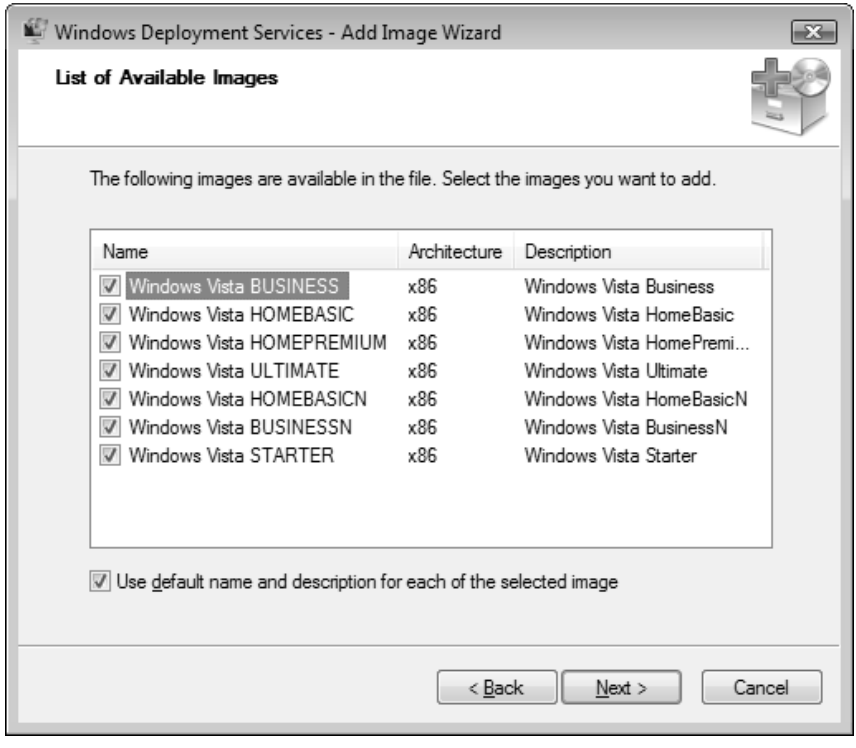


Рис. 1.25. Выбор образов, помещаемых в хранилище образов

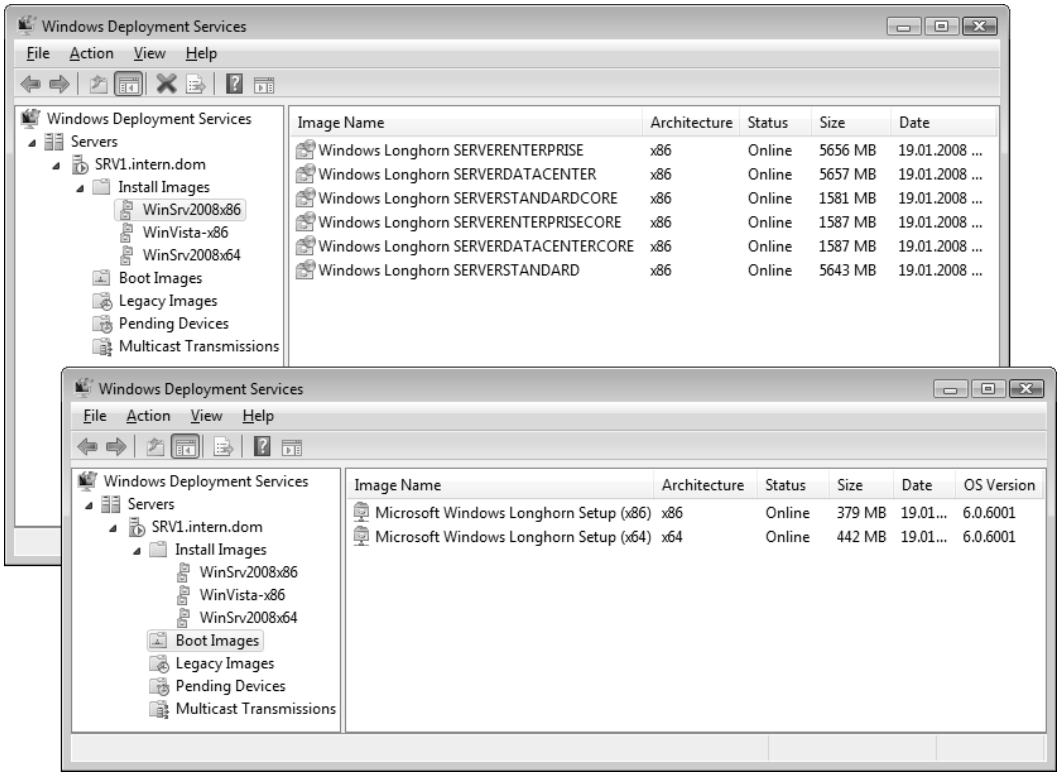


Рис. 1.26. Папки, содержащие загрузочные и установочные образы

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

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. 1.27. Окно свойств WDS-сервера

Например, на вкладке **Directory Service** (Служба каталога) (рис. 1.27) 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

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.

Просмотр состояния устройств

Основным инструментом для конфигурирования аппаратных средств систем Windows Server 2008 традиционно остается оснастка **Device Manager** (Диспетчер устройств, devmgmt.msc), которая преимущественно используется для проверки состояния аппаратных устройств (компонентов) и обновления (иногда установки) драйверов устройств компьютера (внутренних или подключаемых).

> ***Внимание!***
>
> В системах Windows Vista и Windows Server 2008 отсутствуют 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.

Для запуска диспетчера устройств (рис. 1.28) можно воспользоваться панелью управления или же ссылкой **Device Manager** (Диспетчер устройств) в окне свойств системы (см. рис. 2.10). Другой путь — ввести строку `devmgmt.msc` в окне **Run** (Выполнить) или непосредственно в меню **Start** (Пуск). Оснастку можно добавить к пользовательской консоли MMC — в этом случае ее можно подключить и к удаленному компьютеру, если так запущены все необходимые сервисы и имеются разрешения.

> ***Примечание***
>
> В меню **View** (Вид) окна диспетчера устройств имеются команды выбора способов отображения устройств и ресурсов, включая команду **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).

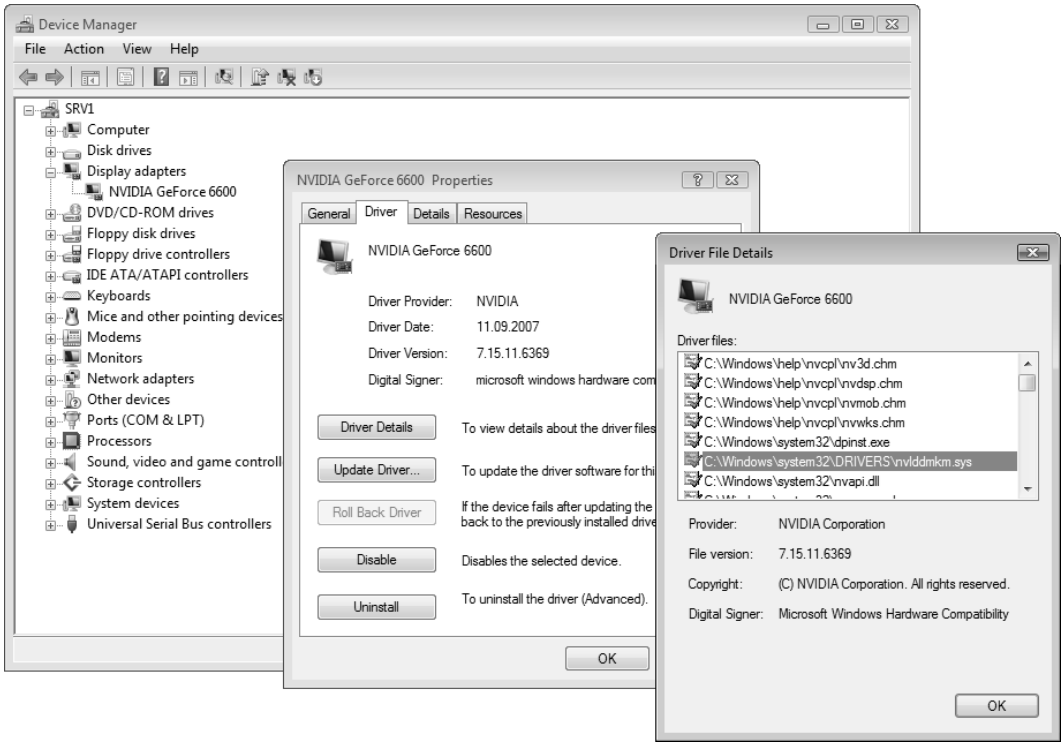


Рис. 1.28. Просмотр параметров выбранного аппаратного устройства и сведений о драйвере

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

Полезную информацию об устройствах и драйверах можно получить с помощью утилит SystemInfo.exe и System Information (Сведения о системе, Msinfo32.exe) *(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* или команды `sc query type= driver`. Для ручной установки и удаления драйверов устройств применяется утилита *Pnputil.exe*. Все эти утилиты имеются в любой версии Windows Server 2008, включая Windows Server Core и Hyper-V Server.

Установка драйверов для подключенных устройств

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, выполнится стандартная процедура распознавания устройства, и система сконфигурирует уже имеющийся у нее драйвер.

Если система обнаруживает новое устройство после загрузки, то появляется запрос, аналогичный тому, что показан на рис. 1.29 (если драйвер имеется на локальном диске, то система находит и устанавливает его сама, без всяких запросов). 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. 1.29. Запрос на установку драйвера для обнаруженного устройства

Если система успешно находит, загружает и устанавливает драйвер в автоматическом режиме, то этот процесс заканчивается появлением информационного сообщения. В противном случае драйвер нужно устанавливать вручную.

При ручной установке драйвера или необходимости его обновлении (в этом случае в окне диспетчера устройств нужно выбрать устройство и в контекстном меню вы-

полнить команду **Update Driver Software** (Обновить драйверы)) следует определить способ поиска драйвера — автоматический или ручной. 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.

При выборе опции поиска драйверов на компьютер на следующем шаге нужно определить местоположение драйверов — они могут находиться на локальном диске или на сменном носителе. 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**).

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.

Работа с виртуальными машинами в среде Hyper-V

Для установки виртуальных машин (ВМ) можно воспользоваться ролью Hyper-V, имеющейся в составе Windows Server 2008, или установить самостоятельный продукт Microsoft Hyper-V Server 2008 *(см. Введение)*. В любом случае принципы развертывания и администрирования виртуальной среды будут совершенно одинаковыми.

Для виртуальных машин, устанавливаемых в среде Hyper-V, поддерживаются следующие версии операционных систем[1] (для 32- и 64-разрядных платформ):

- все редакции Windows Server 2008;
- все редакции Windows Server 2003 с Service Pack 2;
- Windows 2000 Server и Windows 2000 Advanced Server с Service Pack 4;
- SUSE Linux Enterprise Server;
- все редакции Windows Vista с Service Pack 1;
- все редакции Windows XP Professional с Service Pack 3.

Могут устанавливаться и другие операционные системы, но их работоспособность не гарантируется.

[1] Эти системы называются *гостевыми* (guest) для хост-среды.

Примечание

Для централизованного управления виртуальными системами в корпоративной среде имеется специальный продукт — System Center Virtual Machine Manager 2008. (Пробную 180-дневную версию можно скачать с веб-сайта Microsoft — *см. Приложение 1*.) С его помощью можно контролировать работу виртуальных машин, работающих на серверах Windows Server 2008 (в среде Hyper-V) и Virtual Server 2005, выполнять миграцию ВМ между различными серверами, а также конвертировать физические диски с установленными системами в виртуальные диски образов.

Управление сервером Microsoft Hyper-V Server 2008

После регистрации администратора в системе *(см. выше разд. "Установка пароля")* на экране одновременно появляются окно консоли и окно утилиты *HVConfig.cmd* (рис. 1.30), которая является основным средством конфигурирования сервера Hyper-V. С ее помощью можно дать компьютеру рабочее имя, подключить его в домен, установить обновления и т. д. — все возможности представлены на экране.

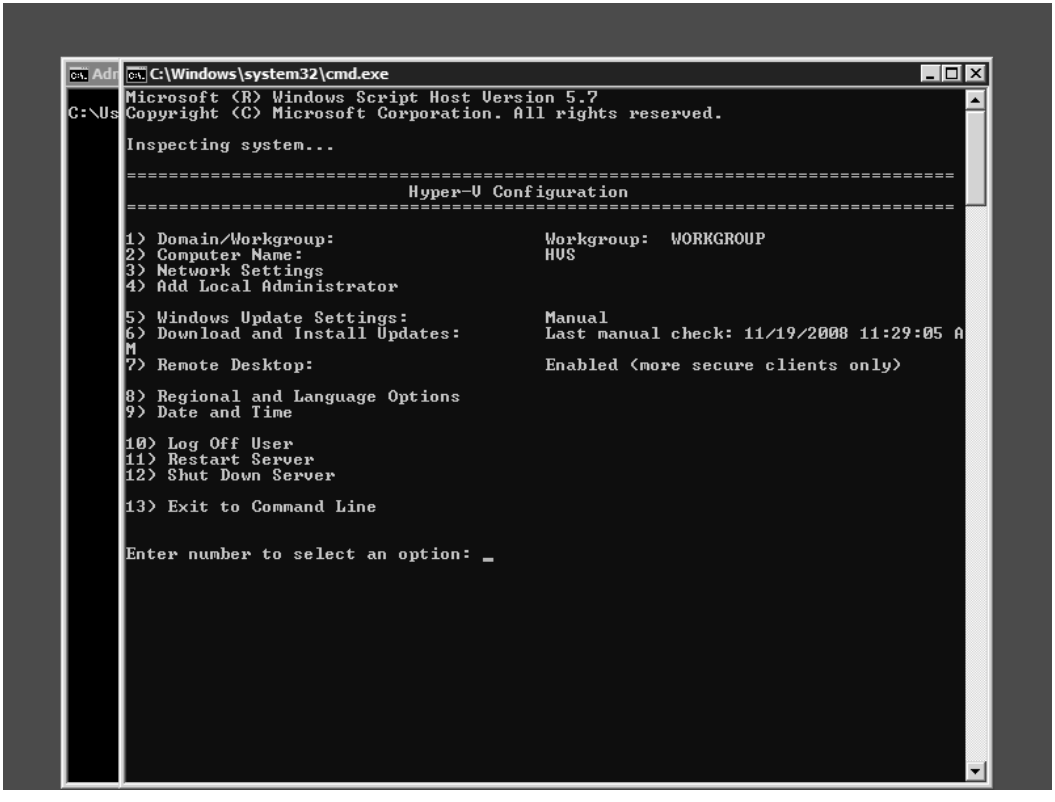


Рис. 1.30. Окно утилиты HVConfig, предназначенной для управления Hyper-V Server

Все операции по созданию и конфигурированию виртуальных машин выполняются удаленно, с помощью утилиты Hyper-V Manager[1] *(см. далее)*.

Управление виртуальными машинами — утилита Hyper-V Manager

Главным средством управления виртуальными машинами, работающими на локальном или на удаленном компьютере, является утилита *Hyper-V Manager*.

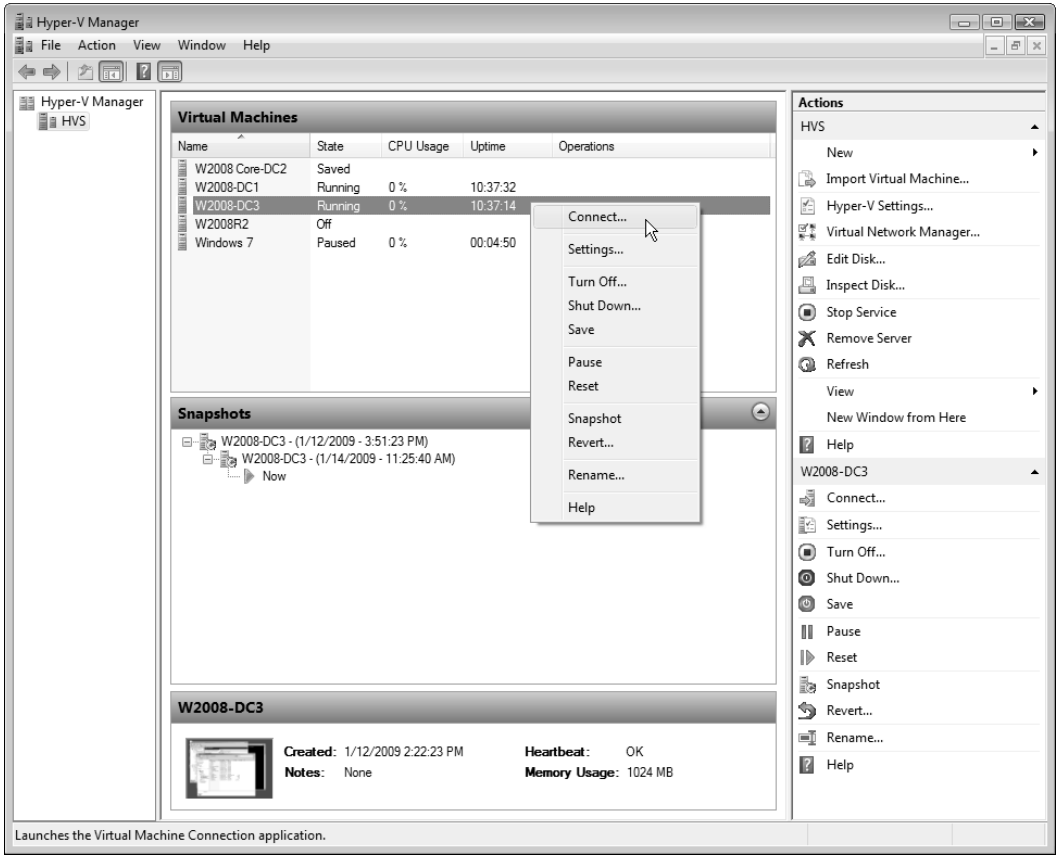


Рис. 1.31. Главное окно программы Hyper-V Manager

Для ее установки в системах Windows Server 2008 нужно добавить соответствующий компонент в группе **Remote Server Administration Tools**; при работе в систе-

[1] В Интернете можно найти сценарии, позволяющие непосредственно на сервере управлять состоянием виртуальных машин: останавливать их, запускать и т. п.

мах Windows Vista требуется скачать в Центре загрузки Microsoft *(см. Приложение 1)* и установить пакет *Hyper-V Remote Management Update for Windows Vista*[1]. Утилита запускается из меню **Administrative Tools** (Администрирование).

После запуска утилиту необходимо подключить к серверу Hyper-V (к локальному серверу она подключается автоматически) с помощью команды **Connect to Server** на панели **Actions** (Действия). После этого можно начинать работу с виртуальными машинами. На рис. 1.31 показано окно утилиты с уже установленными ВМ. На панели **Actions** (Действия) и в контекстном меню можно видеть все операции, которые можно выполнять с выбранной ВМ.

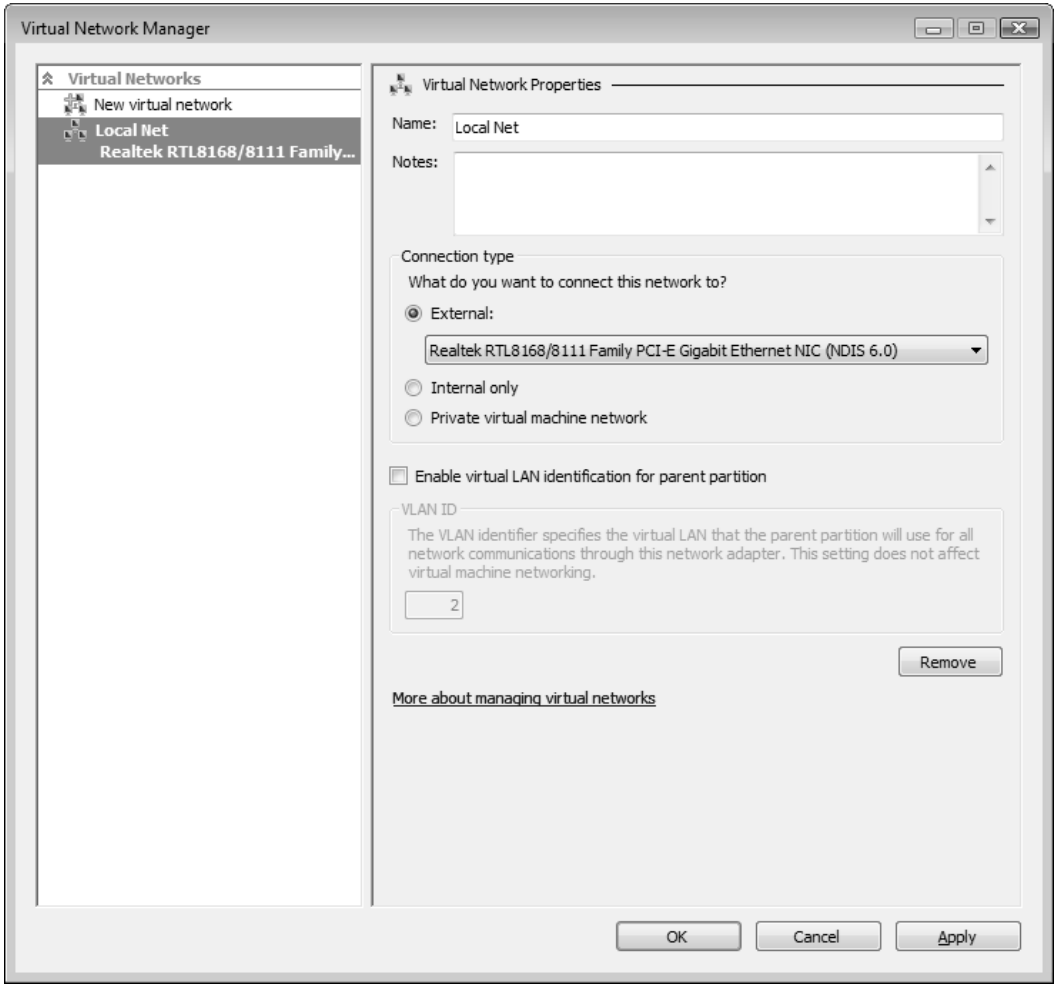


Рис. 1.32. Окно параметров виртуальной сети

[1] Имеются версии пакета для 32- и 64-разрядных систем.

Для нового сервера Hyper-V (перед началом развертывания ВМ) необходимо установить его параметры, выбрав команду **Hyper-V Settings** на панели **Actions** (Действия). Важным параметром является местоположение папок, содержащих описания ВМ и образы дисков. Также в окне параметров можно выбирать комбинацию клавиш, "освобождающих" курсор в окне ВМ (release key) *(см. далее)*.

Если создаваемые ВМ будут работать в сети, то необходимо с помощью утилиты Virtual Network Manager (Диспетчер виртуальной сети) создать соответствующие *виртуальные сети* (virtual network). Открыв окно утилиты, выберите тип сети и нажмите кнопку **Add**. В следующем окне (рис. 1.32) укажите название сети. Тип подключения (connection type) будет уже определен на основе выбранного типа сети. Для внешней сети можно также выбрать конкретный сетевой адаптер, к которому будет подключена данная сеть.

Возможны следующие типы виртуальных сетей:

- *внешняя* (external) — подключается к сетевому адаптеру сервера, в результате чего ВМ могут общаться с физической сетью (а сетевые компьютеры могут иметь доступ к ВМ);
- *внутренняя* (internal) — связывает ВМ между собой и с самим сервером. Доступ к физической сети отсутствует;
- *частная* (private) — используется только ВМ для связи между собой. Это максимально защищенная от внешнего воздействия конфигурация.

Имеющиеся виртуальные сети можно указывать при установке новых ВМ.

Для работы с виртуальными дисками (образами систем) в составе утилиты *Hyper-V Manager* имеются мастера создания, просмотра и редактирования дисков (для преобразования динамически расширяемых дисков в диски фиксированного размера и наоборот). Для их запуска на панели **Actions** (Действия) имеются соответствующие ссылки: **New | Hard Disk**, **Inspect Disk** и **Edit Disk**. При создании виртуального диска можно использовать физический диск работающей системы (подключив его к серверу), и на его основе создать виртуальную машину, полностью повторяющую конфигурацию физического сервера.

Любую ***не*** работающую (остановленную или сохраненную) виртуальную машину можно *экспортировать* (команда **Export**), а затем *импортировать* и использовать для создания другой ВМ (команда **Import Virtual Machine**). При этом могут также экспортироваться и импортироваться виртуальные диски. Такая процедура позволяет переносить ВМ между различными серверами Hyper-V, а также восстанавливать созданные ВМ на новых серверах.

Важной функцией при работе с ВМ является *создание* снимков (snapshot) системы, которые можно делать в любой момент (команда **Snapshot**). Снимок представляет собой состояние виртуальной машины (содержимое памяти и виртуального диска) на определенный момент, к которому можно вернуться в дальнейшем с помощью команды **Revert**. Например, можно сделать снимок работоспособной системы пе-

ред выполнением серьезных изменений ее конфигурации. Если эти изменения будут неудачными и система станет нестабильна, то можно просто вернуться к рабочему состоянию на какой-то момент и продолжить работу в "здоровой" системе.

Установка новой виртуальной машины

Порядок создания виртуальных машин (ВМ) следующий:

1. На панели **Actions** (Действия) щелкните по ссылке **New** и выберите опцию **Virtual Machine**.
2. В окне мастера *New Virtual Machine Wizard* (рис. 1.33) укажите имя ВМ. (Это имя произвольное и никак не связано с именем устанавливаемого компьютера. В дальнейшем его можно поменять.) Можно указать местоположение папки, хранящей описание ВМ, если она должна отличаться от каталога, заданного в параметрах сервера Hyper-V.

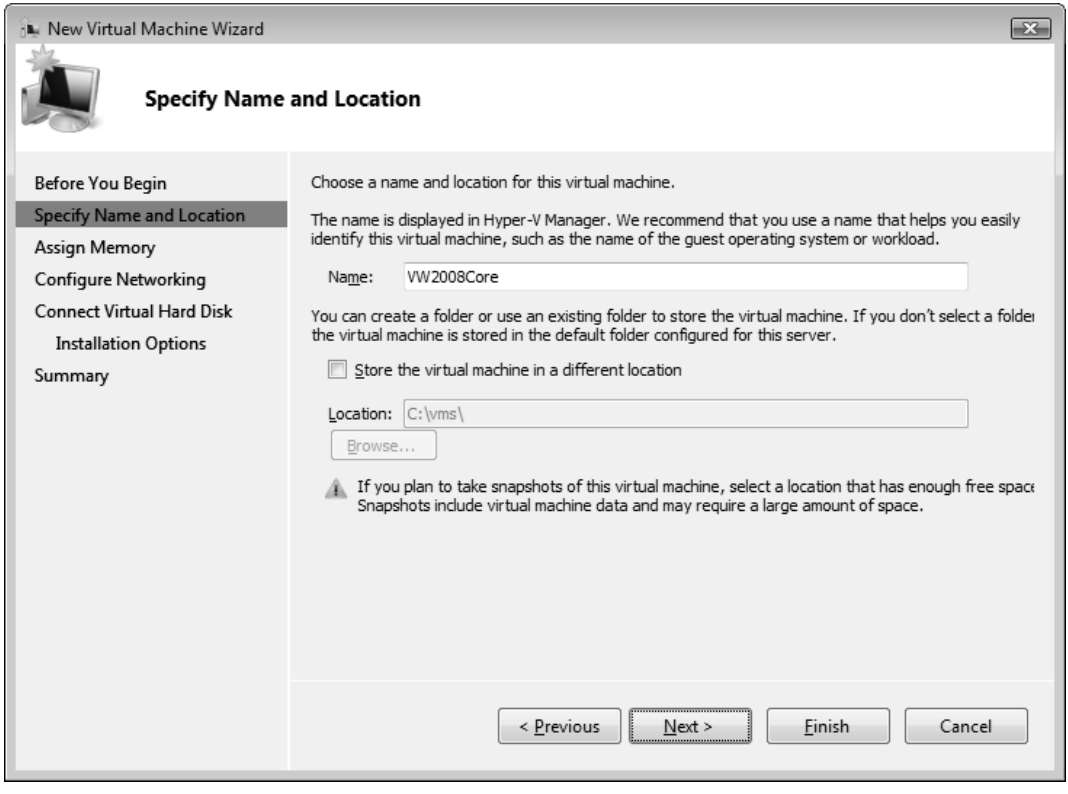


Рис. 1.33. Первый шаг в процессе установки виртуальной машины

3. На следующем шаге укажите объем памяти, выделяемый для ВМ. Сумма значений для всех *одновременно работающих* ВМ не должна превышать объема физической памяти сервера Hyper-V. В противном случае при запуске ВМ возможна ошибка, указывающая на нехватку ресурсов.
4. Выберите подключение к виртуальной сети, если новая ВМ будет работать с сетью.
5. Укажите имя, местоположение и размер создаваемого образа диска (рис. 1.34). По умолчанию создается динамически расширяемый диск размером 127 Гбайт. Реальный размер диска будет увеличиваться по мере установки дополнительных программ, добавления данных и т. п. Изначально образ диска имеет размер около 7 Гбайт для Windows Server 2008 и 2,2 Гбайт для Windows Server 2008 Server Core (без дополнительных компонентов!).

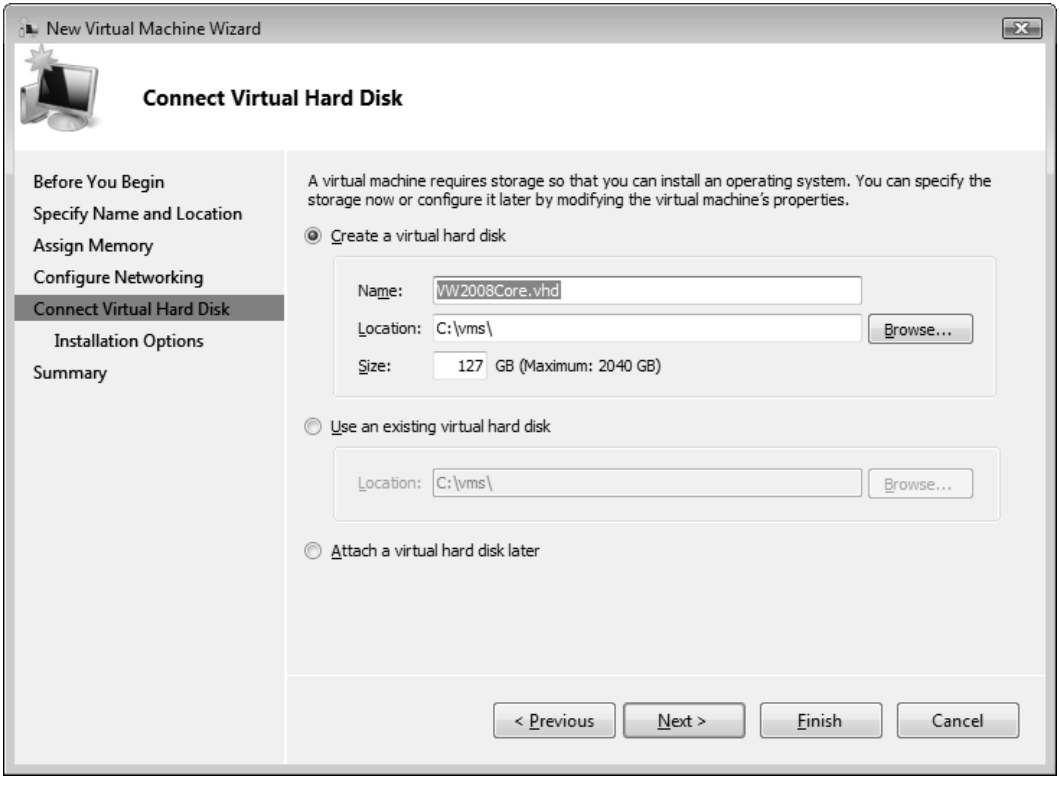


Рис. 1.34. Определение параметров образа диска

Можно указать уже существующий образ диска: созданный заранее с помощью мастера New Virtual Hard Disk Wizard или полученный при экспорте уже существующей ВМ.

6. Следующим шагом является выбор опций установки операционной системы для новой ВМ (рис. 1.35). Устанавливать систему можно с дистрибутивного диска, вставленного в CD/DVD-привод (это самый простой вариант), или из файла ISO-образа, созданного предварительно с помощью какой-нибудь утилиты и хранящегося на жестком диске сервера. Возможны и другие варианты, показанные на рисунке.

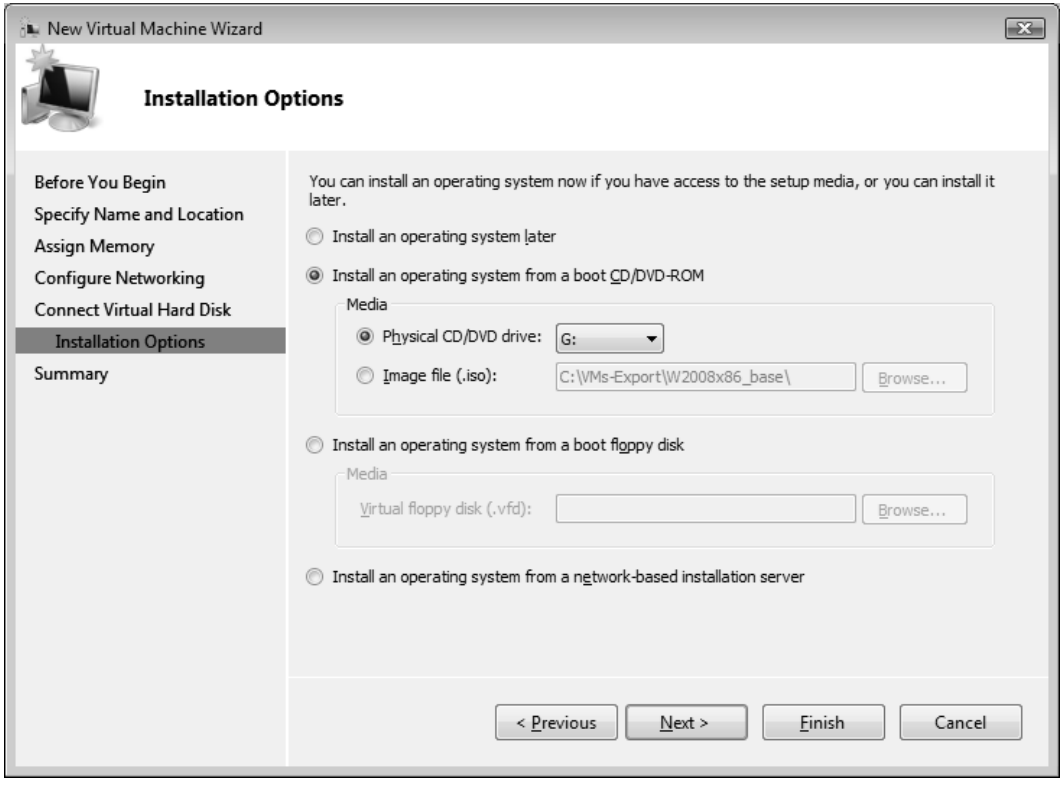


Рис. 1.35. Выбор опций установки операционной системы

7. На последней странице мастера можно установить флажок, указывающий на немедленный запуск ВМ после ее создания (обычно при этом сразу начинается установка операционной системы с указанного носителя). Проверьте введенные значения и, если ошибок нет, нажмите кнопку **Finish** (Готово) — операция начнется.

Если для создаваемой ВМ необходимо указать дополнительные параметры, то можно не начинать установку системы, а открыть окно свойств для созданной ВМ (рис. 1.36) и выбрать нужные значения. Просматривать параметры можно и для работающей ВМ, однако в этом случае их изменение невозможно (параметры меняются только для ***выключенных*** ВМ!). В показанном на рисунке окне можно за-

давать число процессоров и управлять распределением ресурсов между ВМ: указывать минимальную и максимальную степень загрузки системы, а также относительный вес данной ВМ при распределении ресурсов системы.

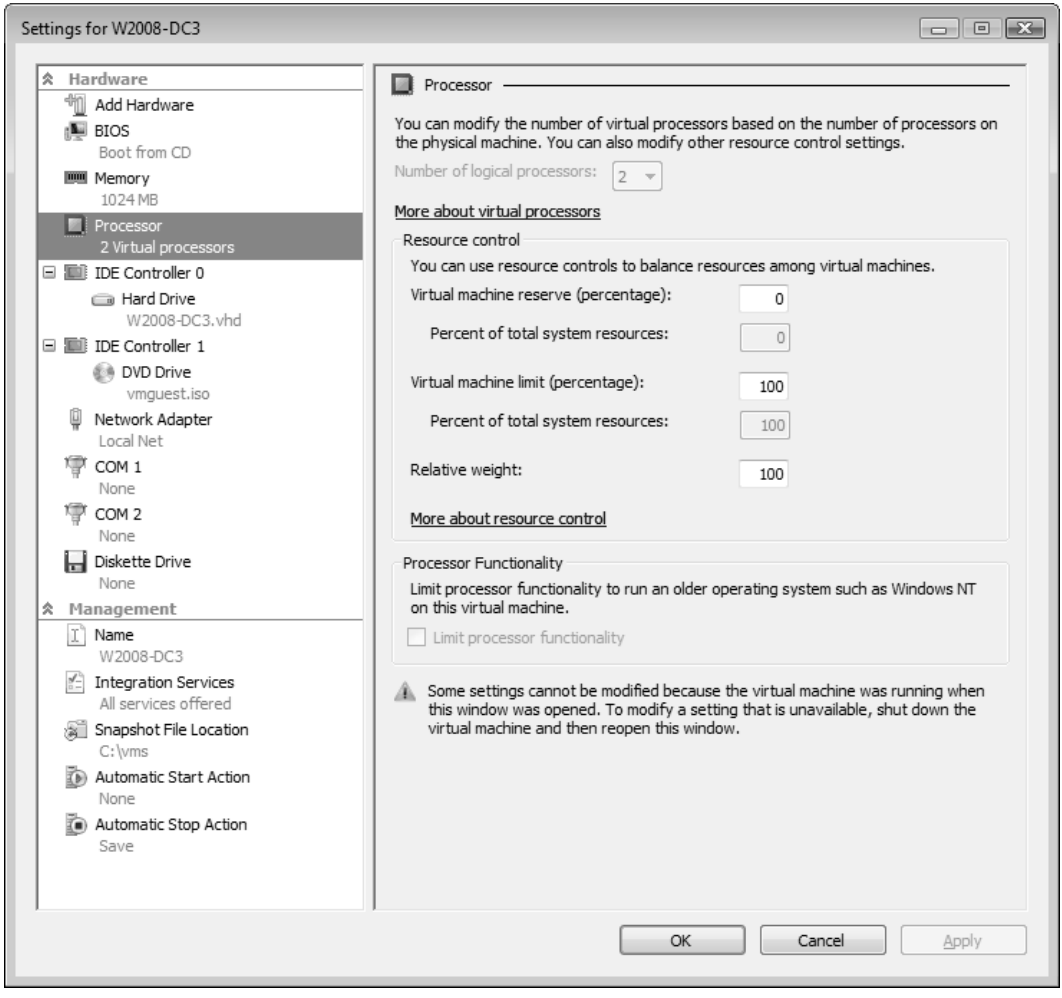


Рис. 1.36. Окно свойств виртуальной машины

Другими важными параметрами в окне свойств ВМ являются список служб интеграции (Integration Services — *см. далее*), местоположение папки для хранения снимков (snapshot) ВМ и действия, выполняемые при включении и выключении физического компьютера. По умолчанию восстанавливается состояние ВМ (рабочее или выключенное), которое было на момент выключения компьютера, а при выключении сервера происходит сохранение (save) ВМ.

Службы интеграции (Integration Services)

В каждой созданной виртуальной машине рекомендуется устанавливать так называемые *службы интеграции* (Integration Services). С их помощью обеспечивается выполнение следующих операций:

- свободное перемещение курсора между окном подключения к ВМ и другими окнами, открытыми на рабочем столе;
- корректное выключение системы (shutdown) из окна утилита Hyper-V Manager (при отсутствии служб интеграции выключение необходимо выполнять в самой ВМ);
- синхронизация времени между ВМ и сервером Hyper-V;
- обмен данными (вставка содержимого буфера обмена клиентской машины — команда **Type clipboard text** в меню **Clipboard** окна подключения к ВМ — *см. далее*);
- индикация активности ВМ (heartbeat[1]), указывающая на отсутствие зависания, краха и т. п.;
- архивация образа системы в виде снимка (snapshot).

> ***Внимание!***
>
> Перед установкой служб интеграции на виртуальные машины, работающие под управлением систем Windows XP и Windows Server 2008, необходимо установить на них последние пакеты обновления (Service Pack).

Для установки служб интеграции необходимо выполнить следующие действия:

1. Запустите виртуальную машину и подключитесь к ней.
2. В окне сеанса подключения (см. рис. 1.38) выберите команду **Insert Integration Services Setup Disk** в меню **Action**.
3. Если не выполняется автозапуск программы установки служб интеграции, то откройте окно консоли и перейдите на виртуальный диск с меткой VMGUEST, после чего запустите команду `setup` в подкаталоге \support\x86\.
4. Нажмите кнопку **ОК** в окне с сообщением о наличии предыдущей версии служб интеграции — будет выполняться их обновление.
5. После получения сообщения об успешной установке перезагрузите ВМ.

> ***Внимание!***
>
> Если службы интеграции не установлены, то в виртуальной машине может устанавливаться *совместимый* сетевой адаптер с ограниченными функциями, при этом возможны ошибки подключения к сети, если для ВМ выбран адаптер другого

[1] Буквально — "биение сердца".

типа. В этом случае в окне свойств ВМ необходимо выбирать *Legacy Network Adapter*. Возможно даже, потребуется удалить имеющийся адаптер, добавить совместимый и перезапустить ВМ. После успешной установки служб интеграции можно поменять совместимый адаптер на *Network Adapter*, который имеет значительно большее быстродействие, а также дополнительные возможности. После этого опять потребуется перезапустить ВМ.

Подключение к виртуальным машинам

Для подключения к виртуальной машине в окне утилиты Hyper-V Manager достаточно выполнить команду **Connect** в контекстном меню (см. рис. 1.31) или просто дважды щелкнуть по имени ВМ.

Для подключения к виртуальным машинам с удаленных компьютеров можно использовать специальную утилиту *VMconnect.exe*, которая появляется в папке \Program Files\Hyper-V после установки соответствующего компонента или пакета утилит для удаленного администрирования сервера Hyper-V. В окне утилиты следует выбрать имя сервера и виртуальную машину, к которой необходимо подключиться (рис. 1.37).

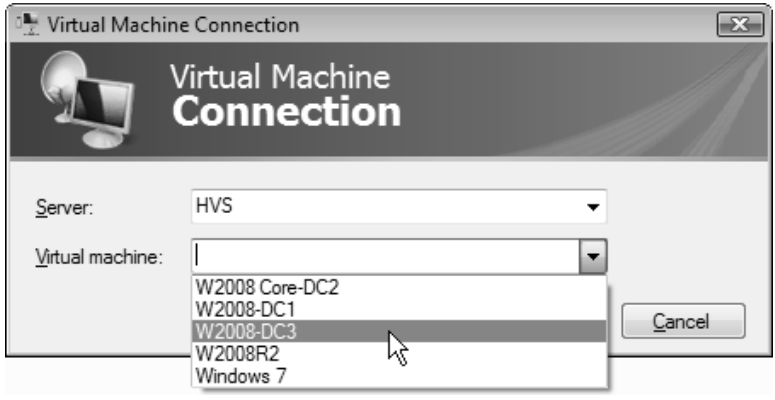


Рис. 1.37. Окно утилиты VMconnect

После подключения к работающей ВМ в специальном окне сеанса появляется окно регистрации, после чего пользователь может работать в среде виртуальной машине, как на обычном компьютере. (Подключение возможно даже к выключенной ВМ.) Окно сеанса подключения (рис. 1.38) имеет меню команд и панель управления, содержащую кнопки управления ВМ. С их помощью можно запускать и останавливать гостевую систему, делать снимки и т. д.

Если на виртуальной машине не установлены службы интеграции, то для перемещения курсора из окна сеанса подключения в другие окна, открытые на рабочем

столе, требуется каждый раз нажимать клавиши <Ctrl>+<Alt>+<Left Arror> (Стрелка влево) — так называемый *release key*, который определяется в параметрах сервера Hyper-V. После установки служб интеграции такое неудобство устраняется, и курсор можно свободно перемещать между любыми окнами, выбирая нужные объекты.

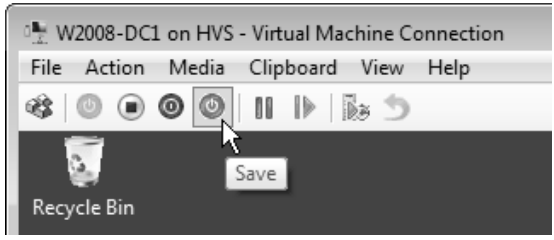


Рис. 1.38. Меню команд
и панель управления состоянием виртуальной машины

Клавиши <Ctrl>+<Alt>+<Pause/Break> позволяют переключаться между перемещаемым окном сеанса и полноэкранным режимом отображения рабочего стола виртуальной машины.

Глава 2



Конфигурирование рабочей среды и административные задачи

Эта глава охватывает самые разные вопросы, касающиеся конфигурирования рабочей среды системы: начиная с настройки параметров пользовательского интерфейса и заканчивая выбором режимов работы службы поиска. Также рассматриваются способы выполнения типовых задач, которые периодически возникают перед любым администратором (например: как запустить задачу в определенное время? как управлять удаленным компьютером? как автоматизировать типовые задачи? и т. д.). При этом в первую очередь мы будем уделять внимание тем вопросам, которые реализованы не так, как в предыдущих версиях Windows.

Настройка экрана регистрации в системе

Пользовательский интерфейс, используемый в Windows Server 2008 при входе в систему, заметно отличается от тех решений, которые применялись в предыдущих серверных 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). Он 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) был 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 (и тогда 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, причем при работе с сетевыми ресурсами.

После загрузки системы Windows Server 2008 — автономной или входящей в домен — пользователь видит экран регистрации 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)*.

После нажатия клавиш <Ctrl>+<Alt>+<Delete> появляется экран приветствия. Для входа в систему надо щелкнуть по пиктограмме имеющейся на компьютере учетной записи пользователя и ввести пароль.

По умолчанию на экране приветствия отсутствует кнопка выключения и перезагрузки компьютера, 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). (Эта кнопка также позволяет переходить в спящий режим (**Sleep**), если этот режим поддерживается компьютером.)

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`.

Порядок языков ввода (номеров кодовых таблиц) определяется значениями параметров: в примере, показанном на рис. 2.1, 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.

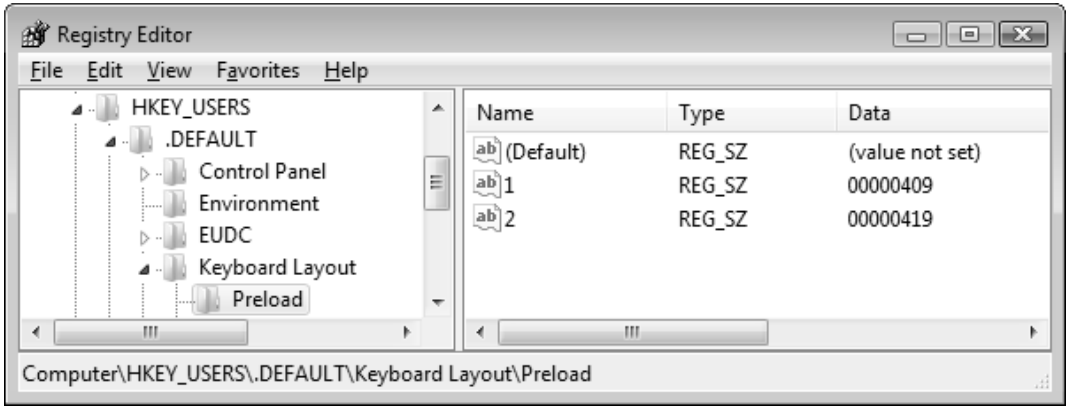


Рис. 2.1. Параметры реестра, определяющие выбор языка ввода при входе в систему

Если компьютер входит в состав домена Windows, то имя пользователя на экране задается полностью, в формате *<имяДомена>\<имяПользователя>*. Если ранее использовался локальный вход в систему, то в качестве домена указано имя самого компьютера. (Об этом нужно помнить, если необходимо на компьютере — члене домена выполнить вход с использованием локальной учетной записи.)

Если нужно войти под другим именем (или в другой домен), то следует нажать кнопку **Switch User** (Сменить пользователя) (рис. 2.2). После этого на экране помимо кнопки последнего регистрировавшегося пользователя (локального или доменного) появится кнопка **Other User** (Другой пользователь) (рис. 2.3). Нажав ее, вы попадете в окно, где можно ввести произвольное имя.

По умолчанию будет предлагаться вход в тот домен, к которому подключен компьютер (указывается NetBIOS-имя домена). (Или же может быть указано имя компьютера.) Таким образом, имя домена или локального компьютера в Windows Server 2008 задается только в составе полного имени пользователя.



Рис. 2.2. Вход в систему на компьютере, подключенном к домену



Рис. 2.3. Вход в систему под другим именем, отличным от имени текущего пользователя

Для того чтобы на экране приветствия не отображались никакие имена, необходимо 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.

Контроль учетных записей (UAC)

В системах Windows Server 2008 (как и в Windows Vista) реализован механизм разделения прав администраторов и рядовых пользователей, получивший название *User Account Control* (UAC; Контроль учетных записей[1]). Он обеспечивает различ-

[1] Иногда этот механизм также называется *Управление учетными записями пользователей*.

ный 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 текущие права не превышают прав обычного пользователя — до тех пор, пока ему не потребуются расширенные полномочия, получение которых нужно явно подтвердить. 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.

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.

Возможности рядовых пользователей (входящих в группу Users (Пользователи)) в системах 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).

Все операции, требующие *дополнительных* (административных) привилегий, отмечены в пользовательском интерфейсе систем Windows Server 2008 значками предупреждений системы безопасности — маленьким изображением щита[1] (например, их можно видеть на панели управления в режиме просмотра задач по категориям).

---

[1] Эти значки отображаются всегда, вне зависимости от того, включен или выключен механизм UAC.

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 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.

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. 3.2) и добавить столбец **Virtualisation** (Виртуализация).

Выполнение административных задач

Если рядовой пользователь пытается выполнить административную операцию, то появляется окно запроса (рис. 2.4), указывающее на необходимость ввода учетных данных администратора. После ввода пароля можно будет запустить программу с правами администратора; в противном случае операция не выполняется.

При включенном режиме Admin Approval Mode даже обычный администратор (член группы Administrators (Администраторы)) получает запросы от системы безопасности (рис. 2.5) и должен подтвердить выполнение операции с повышенными полномочиями, нажав кнопку **Allow** (Продолжить). (Такое поведение можно изменить с помощью политик — *см. далее*.)

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. 2.4, 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.



Рис. 2.4. Запрос полномочий
для выполнения административной операции

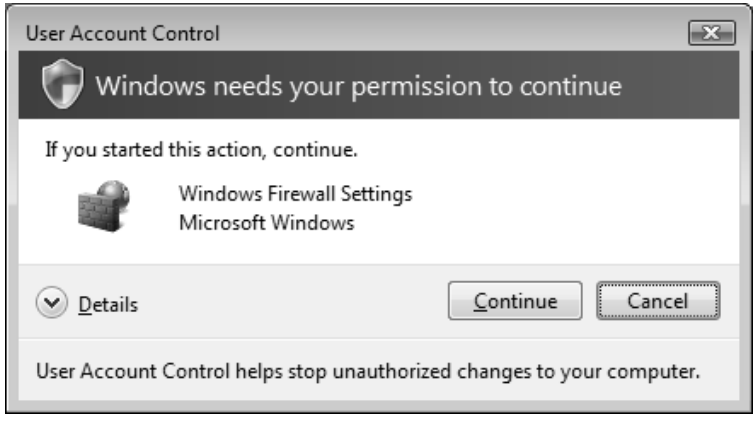


Рис. 2.5. Запрос на подтверждение выполнения административной задачи

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: кто зарегистрирован в системе — пользователь Administrator (Администратор) или любой другой пользователь? 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, хотя при этом каждый раз будет запрашиваться простое подтверждение операции (без ввода пароля). Об этом важно помнить потому, что для выполнения некоторых задач членства в группе Administrators (Администраторы) недостаточно, и даже пользователь с административными правами (но не пользователь Administrator (Администратор)) должен использовать команду **Run as administrator**[1] (Запуск от имени администратора).

Если какие-то программы или оснастки постоянно нужно запускать с повышенными правами, то вместо того чтобы каждый раз использовать команду **Run as administrator** (Запуск от имени администратора) в контекстном меню программы,

---

[1] Например, откройте окно командной строки и запустите утилиту Bcdedit — она будет работать только для пользователя Administrator (Администратор) или при запуске окна консоли с повышением полномочий.

можно задать этот режим в расширенных свойствах ярлыка программы. Для этого выберите имя программы ***в меню*** **Start** (Пуск), щелкните правой кнопкой мыши и выполните команду **Properties** (Свойства). Затем на вкладке **Shortcut** (Ярлык) (рис. 2.6) нажмите кнопку **Advanced** (Дополнительно) и в открывшемся окне установите флажок **Run as administrator** (Запуск от имени администратора).

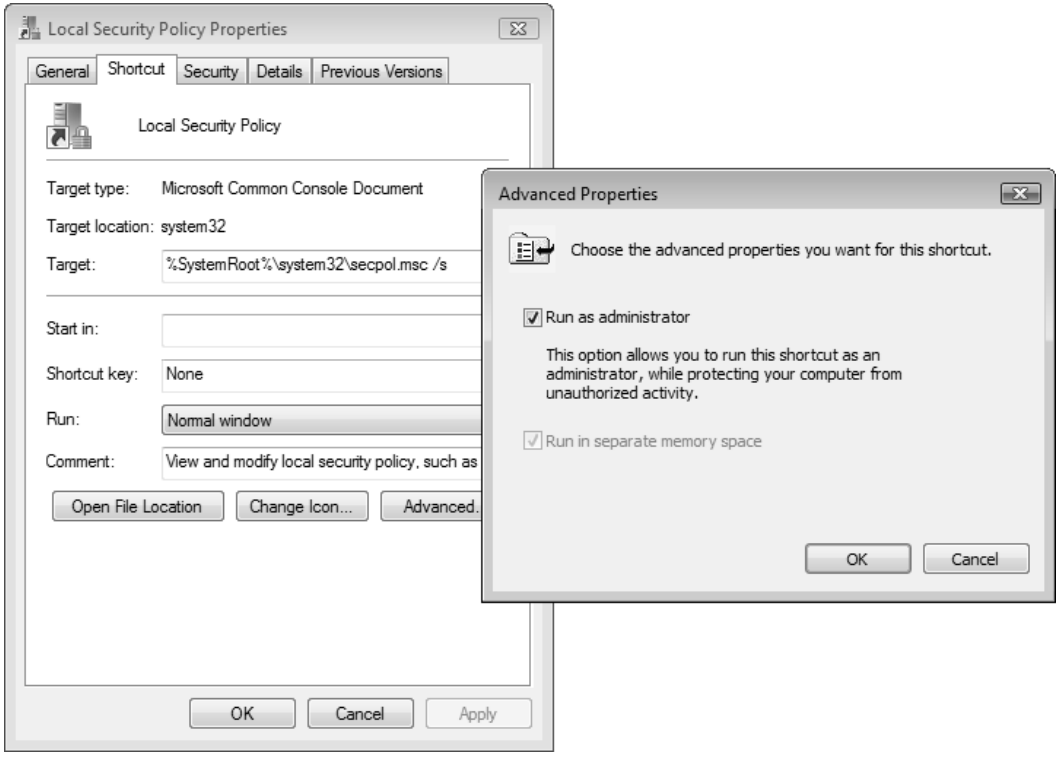


Рис. 2.6. Настройка программы или оснастки на запуск с повышенными административными полномочиями

Управление механизмом UAC

Для управления функцией контроля учетных записей (UAC) имеется несколько групповых политик (рис. 2.7). На рисунке показаны значения политик, заданные по умолчанию. По умолчанию эти политики ***определяются только локально*** (в локальных GPO), на уровне домена или контроллеров домена они не затрагиваются. Рассмотрим самые важные из перечисленных политик (не в том порядке, как они показаны на рисунке).

Обратите внимание на политику **User Account Control: Run all administrators in Admin Approval Mode** (Управление учетными записями пользователей: все адми-

нистраторы[1] работают в режиме одобрения администратором). Поскольку по умолчанию она активна, 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.

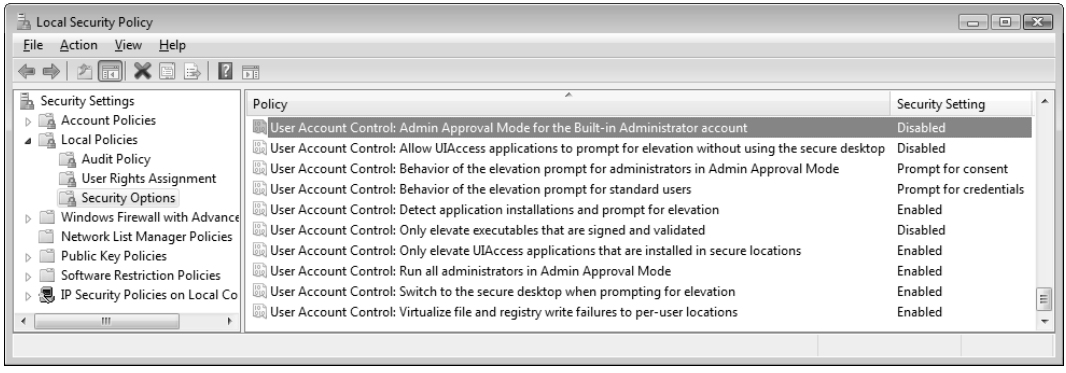


Рис. 2.7. Политики, управляющие механизмом UAC — стандартные значения

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 установки 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 выпол-

[1] Выбор названия политики кажется не совсем точным, поскольку она распространяется не только на администраторов, но и на всех *пользователей* компьютера — возможно, последнее считается само собой разумеющимся.

нении 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. 2.5. Если выбрать первую опцию, то переключение в режим повышения прав будет происходить незаметно для администраторов. 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. 2.4. 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) и выбрать опцию **Disable UAC** (Отключить контроль учетных записей (UAC)). После этого нужно нажать кнопку **Launch** (Запуск), закрыть окно утилиты и перезагрузить систему, иначе изменения не будут действовать.

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\urrentVersion\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)) и в следующем окне установить нужное положение флажка (а затем перезагрузить систему).

Конфигурирование системы. Панель управления

Практически все средства конфигурирования компонентов и сервисов систем Windows сосредоточены на *панели управления* (Control Panel), с которой также можно получить доступ и ко всем административным оснасткам. Системы Windows Server 2008 не являются исключением в этом плане. Панель управления запускается из меню **Start** (Пуск), которое можно настроить так, что она будет отображаться как подменю, где будет сразу доступна конкретная задача.

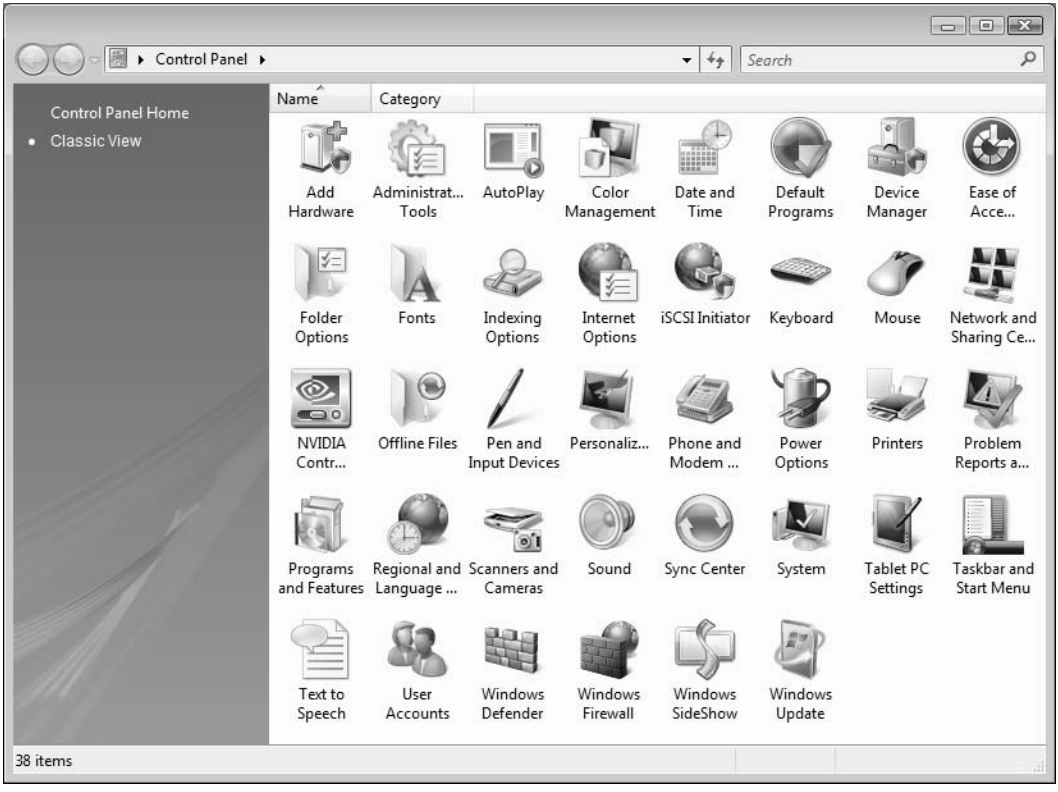


Рис. 2.8. Стандартный вид панели управления систем Windows Server 2008

Назначение задач понятно из названия, и далее мы рассмотрим только *новые* средства настройки систем Windows Server 2008 и особенности конфигурирования версий Windows Server Core и Hyper-V Server.

В Windows Server 2008 по умолчанию используется традиционный для серверных систем способ представления задач — когда одновременно отображаются значки всех утилит (рис. 2.8). В этом случае можно сразу выбрать конкретную задачу и не искать ее по тематическим категориям.

> ***Примечание***
>
> 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.

Имеется возможность просмотра задач управления с группировкой по категориям (рис. 2.9) (как принято по умолчанию в Windows Vista). Для перехода к этому виду представления задач служит ссылка **Control Panel Home** (Панель управления — домашняя страница) в левой части окна. 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.



Рис. 2.9. Вид панели управления, когда задачи сгруппированы по категориям

На рис. 2.9 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 — при этом новое окно не открывается, а все параметры отображаются в уже открытом окне панели управления. Для быстрого перехода к категориям задач можно пользоваться раскрывающимися списками в адресной строке: достаточно щелкнуть по стрелочке в виде треугольника (она выделена на рис. 2.9) — и откроется список категорий или подзадач.

> ***Внимание!***
>
> Возле названий некоторых задач, показанных на рис. 2.9, 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. выше разд. "Контроль учетных записей")*. Подобные значки отображаются всегда, вне зависимости от того, выключен контроль учетных записей (UAC) или нет.

Категории или задачи панели управления отображаются и в окне программы Windows Explorer (Проводник) — как узлы в дереве локальных папок. В зависимости от вида панели управления (классический или с делением по категориям), список отображаемых узлов будет меняться.

Непосредственный доступ к задачам панели управления

Иногда администратору 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, введя имя компонента (CPL-файла) в меню **Start** (Пуск) или в командной строке. Названия компонентов и их назначение указаны в *Приложении 2*.

Имеется команда, с помощью которой можно быстро открыть окно **Folder Options** (Свойства папки):

```
rundll32 shell32,Options_RunDLL
```

Кроме того, к *любой* задаче панели управления можно обратиться напрямую (из командной строки или из меню **Start** (Пуск), используя строку следующего вида: `control /name Microsoft.<englishNameOfTask>`[1]. Необходимо лишь удалить из имени все пробелы. Ниже перечислены примеры командных 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 (рис. 2.10) в версиях Windows Server 2008 претерпело значительную модернизацию. (Для быстрого вызова этого окна удобно использовать клавиши <Win>+<Pause/Break>; также применяется команда **System** (Система) на панели управления.) Ссылки в левой части окна свойств системы позволяют обратиться к диспетчеру устройств (Device Manager) и параметрам удаленного доступа *(см. далее)*.

> ***Примечание***
>
> *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.

Ссылка **Advanced system settings** (Дополнительные параметры системы) позволяет открыть окно свойств системы (рис. 2.11), аналогичное тому, которое обычно используется в Windows XP/Windows Server 2003 (sysdm.cpl). На вкладке **Computer Name** (Имя компьютера) можно изменить имя компьютера, добавить его в рабочую группу или домен, изменить основной DNS-суффикс (primary DNS suffix). Возможности вкладки **Advanced** (Дополнительно) позволяют, среди прочего, настроить визуальные эффекты пользовательского интерфейса, изменить местоположение файла подкачки, управлять профилями пользователей, изменять опции загрузки систем и системные переменные.

---

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

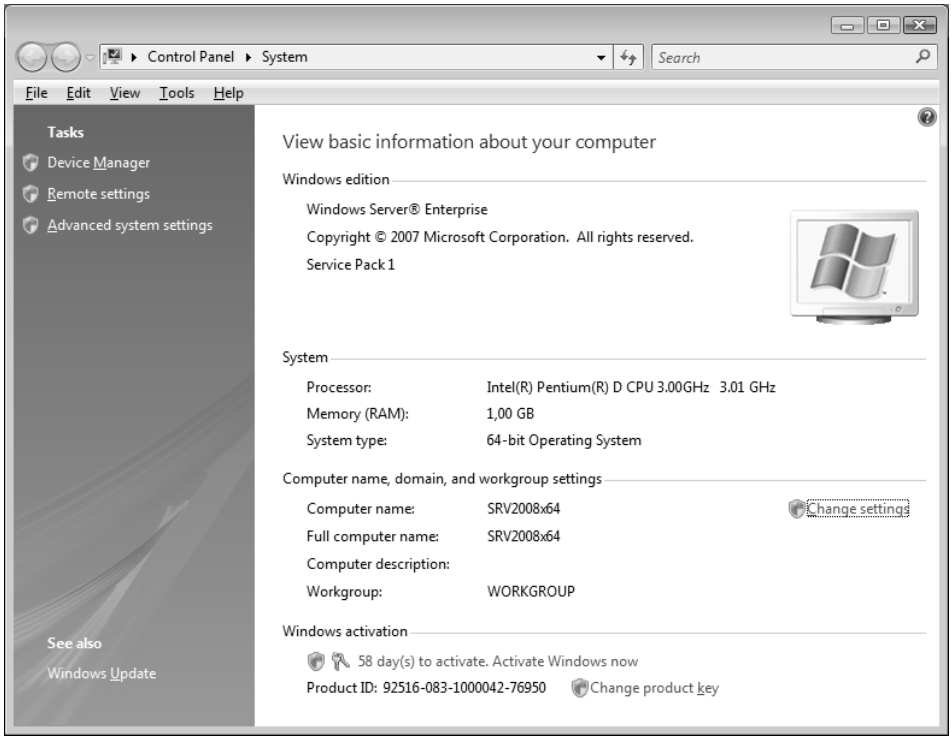


Рис. 2.10. Общие сведения о системе и компьютере

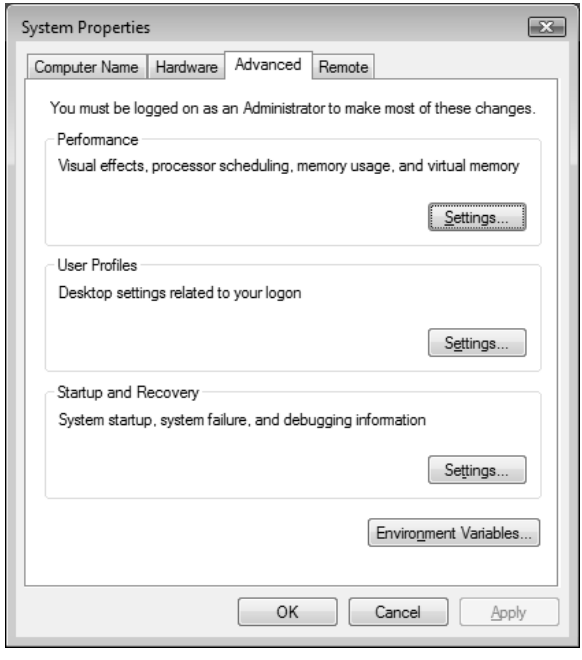


Рис. 2.11. Дополнительные возможности конфигурирования системы

Настройка монитора и элементов пользовательского интерфейса

Интерфейс утилит, используемых для настройки параметров дисплея и элементов оформления, в Windows Server 2008 заметно изменился по сравнению с Windows Server 2003, хотя основные принципы сохранились. Все группы параметров сосредоточены в специальном окне (рис. 2.12), в которое можно попасть с панели управления или же, щелкнув правой кнопкой мыши на рабочем столе и выбрав в контекстном меню команду **Personalize** (Персонализация) (категория **Appearance and Personalization** (Оформление и персонализация)). Все настройки, за исключением параметров дисплея, являются индивидуальными для каждого зарегистрированного пользователя.

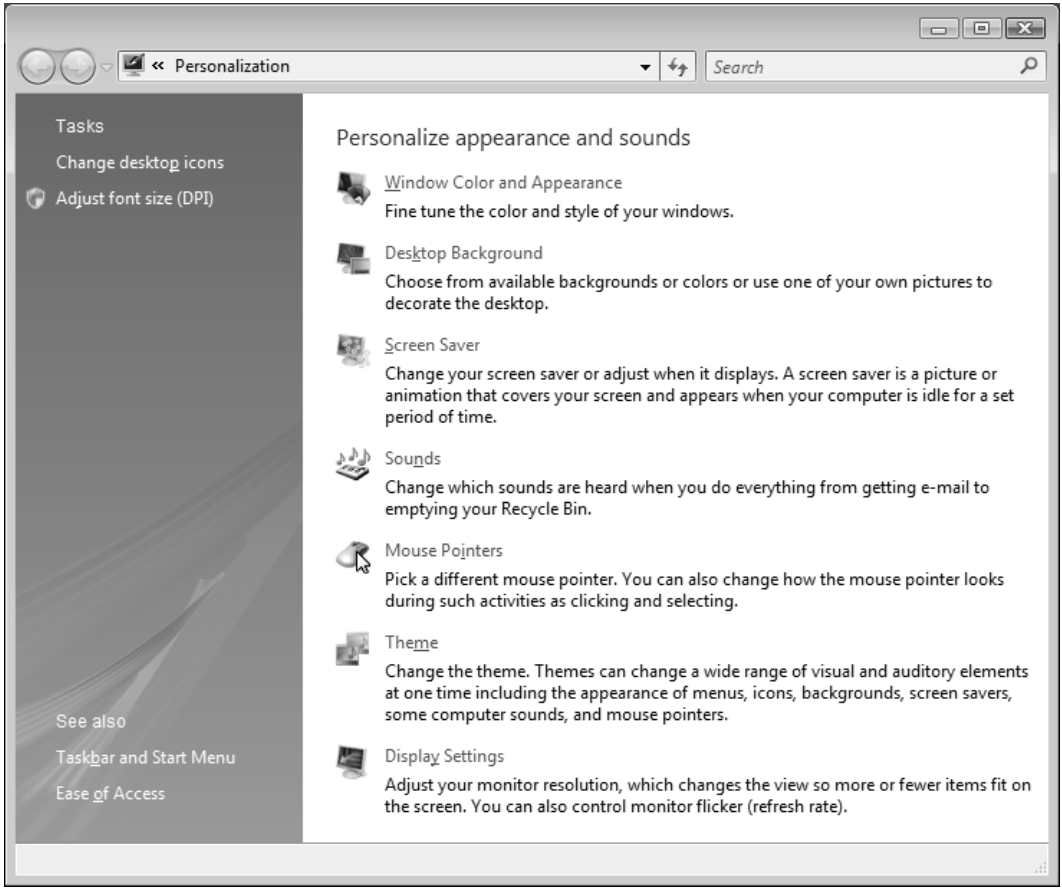


Рис. 2.12. Окно выбора личных параметров дисплея, оформления, звуковых эффектов и указателей мыши

Выбор нужных параметров не вызовет сложностей для любого пользователя Windows, поэтому мы не рассматриваем их подробно. Проблема может возникнуть для версий Windows Server Core и Hyper-V Server, где никаких GUI-средств настройки интерфейса нет, хотя необходимость в некоторых изменениях исходных значений может возникнуть. Например, стандартного разрешения 800 на 600 может оказаться недостаточно даже для работы в окне консоли. По умолчанию включен хранитель экрана с вводом пароля — это очень неудобно, если для мониторинга системы необходимо постоянно готовое к работе окно (в локальной консоли или в окне сеанса удаленного доступа): если администратор активен в нем только периодически (как часто и бывает!), то экранная заставка будет включаться и каждый раз потребуется вводить пароль. Изменение подобных параметров из командной строки — задача далеко не тривиальная, поэтому далее будут рассматриваться способы настройки, ориентированные, в первую очередь, на работу в среде Windows Server Core и Hyper-V Server.

Настройка параметров монитора

В полных версиях Windows Server 2008 для настройки видеосистемы используется задача **Display Settings** (Параметры дисплея), присутствующая в окне **Personalization** (Персонализация) (см. рис. 2.12). С ее помощью можно менять разрешение экрана, глубину цвета, а также частоту развертки и другие параметры видеоадаптера и дисплея.

В полных версиях Windows Server 2008 разрешение экрана определяется параметрами реестра, которые хранятся в разделе `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current\System\CurrentControlSet\Control\VIDEO`. Внутри него имеются разделы для графических устройств; имена разделов представляют собой идентификаторы вида `{42cf9257-1d96-4c9d-87f3-0d8e74595f78}`. В каждом из них имеется раздел `0000`, где располагаются параметры устройства, в том числе два параметра: `DefaultSettings.XResolution` (разрешение по горизонтали) и `DefaultSettings.YResolution` (разрешение по вертикали).

В системах Windows Server Core и Hyper-V Server используется устройство с именем (Device Description) `Standard VGA Graphics Adapter`; по умолчанию для него устанавливается разрешение 800 на 600 точек. Параметры устройства хранятся в разделе `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Video`. Для изменения стандартного разрешения нужно найти в разделе устройство с указанным именем (обычно оно первое в списке) и поменять для него значения параметров `DefaultSettings.XResolution` и `DefaultSettings.YResolution`. Удобнее вводить числа в десятичном формате (скажем, 1024 и 768).

После выхода из системы и повторной регистрации новые параметры начнут действовать.

Стили (темы) оформления

В системах Windows Server 2008 по умолчанию предлагается простой и нетребовательный к параметрам видеоподсистемы так называемый *классический стиль* оформления (Windows Classic). Тем не менее, сохранена возможность использования и нового, более элегантного и эффективного стиля рабочего стола, имеющегося в Windows Vista и названного *Windows Aero*. Для этого потребуется:

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, доступных задаче **Theme** (Тема) в окне **Personalization** (Персонализация) (см. рис. 2.12), появится дополнительная тема — *Windows Vista*, позволяющая выбирать две новые цветовые схемы — *Windows Aero* и *Windows Vista Basic*[1] (Windows Vista – упрощенный стиль).

> ***Примечание***
>
> Темы и цветовые схемы можно менять "на ходу", не перезагружая систему и не закрывая окон приложений.

Хранитель экрана (экранная заставка)

Заставка экрана (screen saver) появляется в периоды бездействия пользователя. Обычно в качестве заставки используются графические файлы специального формата или любые графические файлы. Для выбора параметров заставки в окне **Personalization** (Персонализация) используется задача **Screen Saver** (Экранная заставка).

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 появляются после установки компонента Desktop Experience (Возможности рабочего стола).

В системах Windows Server Core и Hyper-V Server по истечении 10 минут включается экран входа в систему и требуется ввод пароля зарегистрированного пользователя.

Работой хранителя экрана управляют параметры реестра, хранящиеся в разделе `HKEY_CURRENT_USER\Control Panel\Desktop` (первыми указаны значения, заданные по умолчанию):

- `ScreenSaverIsSecure` — 1 (требуется пароль для возобновления работы), 0 (пароль не требуется);

[1] Все иллюстрации в книге выполнены с использованием именно этой цветовой схемы.

- `ScreenSaveTimeOut` — 600 (время ожидания в секундах, если заставка активна);
- `ScreenSaverActive` — 1 (заставка активна), 0 (заставка выключена);
- `SCRNSAVE.EXE` — C:\Windows\system32\logon.scr (имя файла заставки; если заставка выключена, этот параметр можно совсем удалить).

При необходимости можно изменить эти значения и выбрать нужный режим работы заставки.

Выбор языков и региональных стандартов

Возможности настройки региональных стандартов и языков в Windows Server 2008 в основном ничем не отличаются от аналогичных операций в предыдущих версиях Windows и одинаковы во всех редакциях, включая Windows Server Core и Hyper-V Server. 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)).

При установке пакета *Multilingual User Interface (MUI) Pack* можно получить дополнительную возможность изменения языка, используемого в интерфейсе систем Windows для отображения команд меню и текстов в служебных окнах и справочной системе (это, например, может быть полезно при использовании сервера терминалов). При этом язык пользовательского интерфейса можно переключать без перезагрузки компьютера (хотя пользователю необходимо заново регистрироваться в системе) и выбирать язык 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 2*), 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. Для установки языка и переключения имеющихся языков используется вкладка **Keyboards and Languages** (Языки и клавиатуры) окна **Regional and Language Options** (Язык и региональные стандарты).

Выбор региональных параметров и имеющихся языковых возможностей осуществляется в стандартном окне **Regional and Language Options** (Язык и региональные стандарты) (рис. 2.13), которое имеется во всех версиях Windows Server 2008, включая Windows Server Core и Hyper-V Server. В полных версиях задача настройки параметров запускается с панели управления; в любых версиях — по команде `intl.cpl` из командной строки.

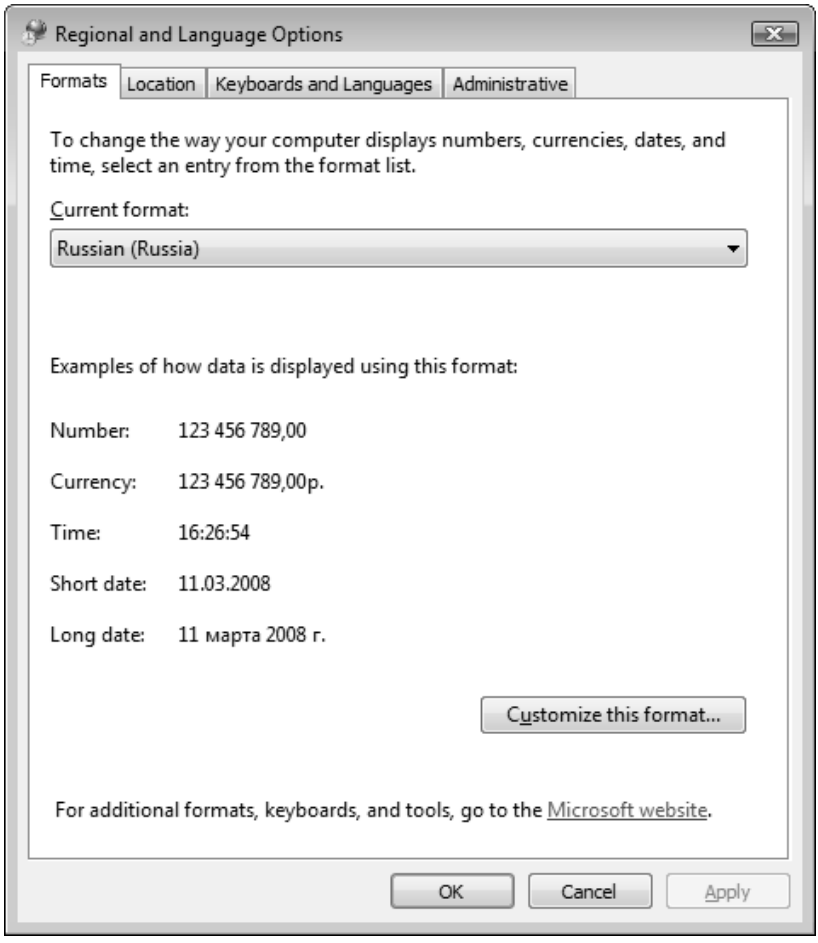


Рис. 2.13. Стандартное окно настройки региональных значений и языков

Управление электропитанием

В системах Windows Vista/Windows Server 2008 механизм управления электропитанием и интерфейс настроек параметров существенно изменились по сравнению с предыдущими версиями Windows. Вместо 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. 2.14) (можно создавать и собственные планы; обычно отображаются три плана, включая действующий, остальные скрываются).

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. 2.14), при этом указанный план сразу начинает действовать — ***никаких дополнительных подтверждений не требуется***.

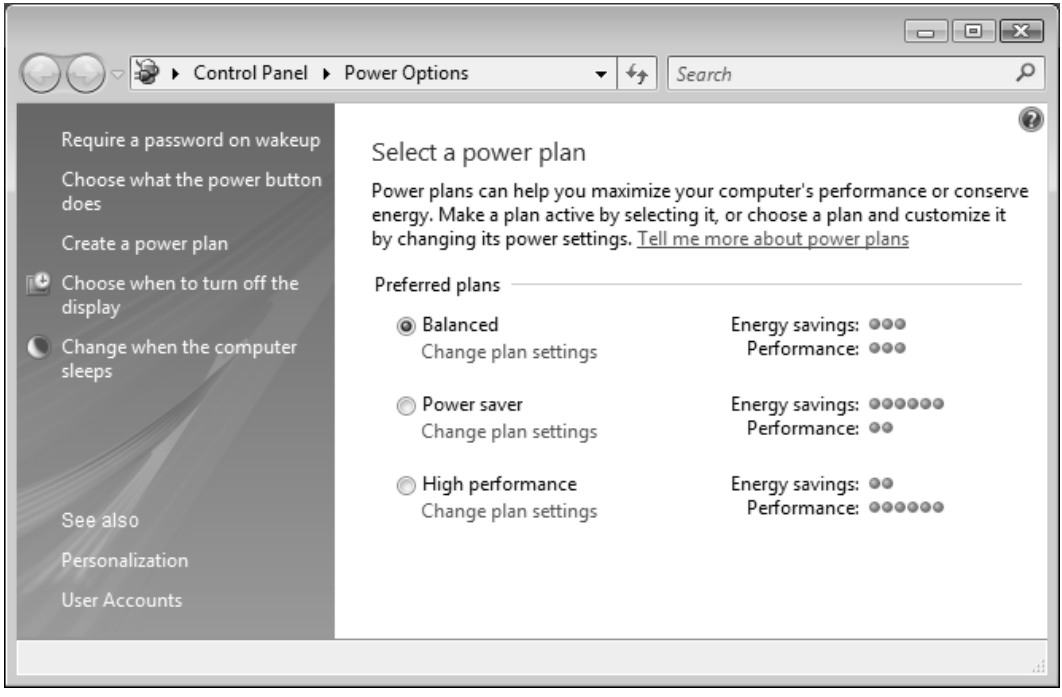


Рис. 2.14. Выбор плана электропитания

Примечание

После установки сервера рекомендуется проверить, соответствуют ли стандартные параметры электропитания (включая режимы сна) рабочим требованиям. Возможно, установленные значения будут не самыми оптимальными для конкретных условий. Например, для постоянно работающего сервера режимы сна и не требуются. Однако по умолчанию, если компьютер поддерживает соответствующие режимы, режим гибернации активизируется и файл hiberfil.sys создается.

Windows Server Core и Hyper-V Server

Для этих версий единственным средством управления электропитанием является утилита *PowerCfg.exe*. С ее помощью можно просмотреть список имеющихся планов электропитания (команда `-LIST`), выбрать другой план (команда `-SETACTIVE`) или переопределить параметры текущего плана (команда `-CHANGE`).

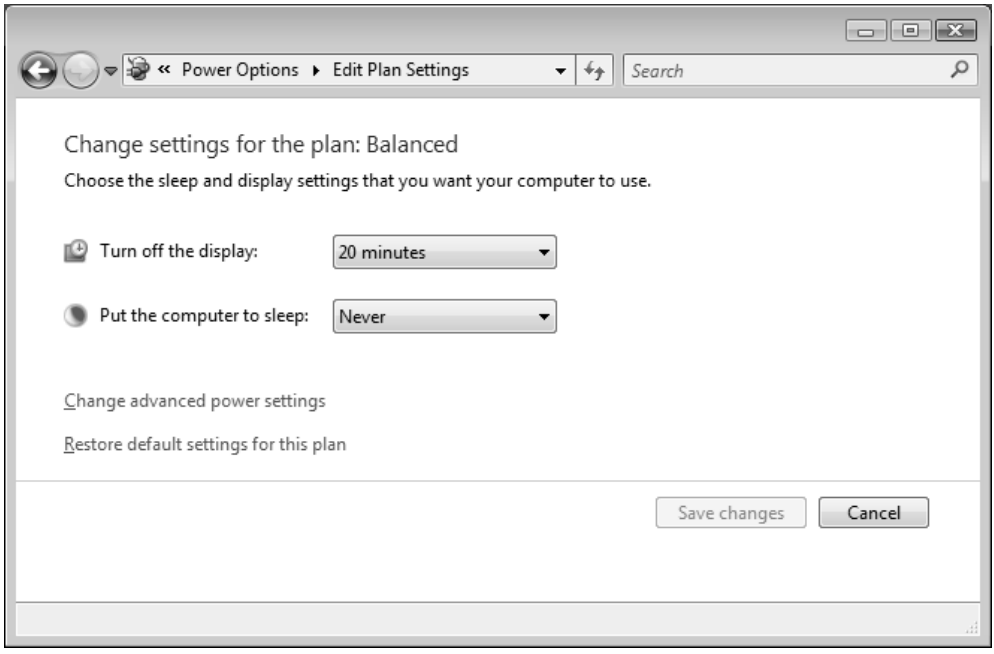


Рис. 2.15. Настройка параметров выбранного плана электропитания

Ссылка **Change plan settings** (Изменение параметров плана) позволяет открыть окно редактирования параметров выбранного плана электропитания (рис. 2.15). Здесь видны значения основных характеристик каждого стандартного плана. Для более детальной настройки режима энергосбережения щелкните по ссылке **Change advanced power settings** (Изменить дополнительные параметры питания).

В окне дополнительных параметров (рис. 2.16) определяется 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)*. Поскольку при нажатии кнопки питания в меню **Start** (Пуск) (см. рис. 2.19, вверху) могут выполняться различные действия[1] — для их выбора используется параметр **Start menu power button** (Кнопка питания меню "Пуск") (рис. 2.17). По умолчанию для систем Windows Server 2008 задано полное выключение (shutdown).

В основном окне **Power Options** (Электропитание) (см. рис. 2.14) можно также определить реакцию компьютера на нажатие кнопки питания (power button) на системном блоке — см. ссылку **Choose what the power button does** (Укажите действие кнопки питания).

---

[1] От выбранного действия зависит цвет кнопки: если будет выполняться выключение, то кнопка имеет красный оттенок; если задан режим сна, то зеленоватый.



Рис. 2.16. Настройка дополнительных параметров электропитания

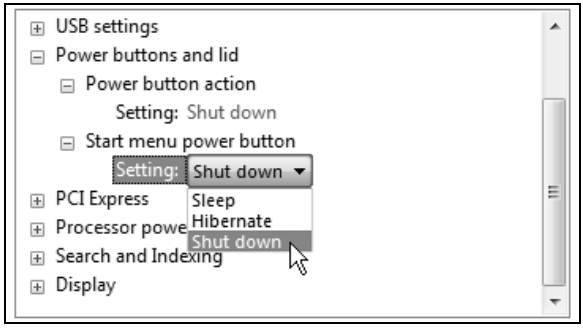


Рис. 2.17. Выбор действия, которое будет выполняться при нажатии кнопки питания в меню **Start**

В специальном окне (рис. 2.18) помимо заданной операции также указывается, нужен ли пароль при выходе из режима сна. (В системах Windows Vista возможно также индивидуально указывать действие для кнопки сна.)

В системах Windows Server 2008 при выключении компьютера с использованием меню **Start** (Пуск) выполняется то действие, которое определено для кнопки питания меню **Start** (Пуск) (рис. 2.19, вверху, левая кнопка), или выбрано в меню.



Рис. 2.18. Определение действий при нажатии кнопки питания



Рис. 2.19. Опции завершения работы (выход из системы и выключение компьютера)

Если при закрытом рабочем столе нажать клавиши <Alt>+<F4>, то появляется меню выключения (рис. 2.19, внизу), где имеются дополнительные возможности сохранения текущего рабочего состояния системы — опции **Sleep** (Сон) и **Hibernate** (Гибернация)[1]. В этих двух 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).

Энергосберегающие режимы Windows Server 2008

Уточним смысл некоторых новых терминов, связанных с энергосберегающими режимами систем Windows Vista/Windows Server 2008, и перечислим действия, выполняющиеся в разных режимах.

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**[2] (Hibernate, suspend-to-disk) — рабочие данные сохраняются *на жестком диске*. Процессор, память и диск выключаются, обычно при этом автоматически отключается и вентилятор блока питания[3] (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);

---

[1] Эта опция присутствует, если только компьютер ***не*** поддерживает *гибридный спящий режим*.
[2] Такой термин использован в локализованной русской версии.
[3] 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 (в задней части системного блока).

- **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 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. 2.19, 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 гибридный 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).)

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 предыдущих версиях Windows служит утилита Add or Remove Programs (Установка/Удаление программ).

При выборе задачи **Programs and Features** (Программы и компоненты) открывается окно, в котором перечислены все приложения, установленные в системе. 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 установленных обновлений (которые при необходимости можно и удалять).

Важное 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. 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 оснастки **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 вспомога-

тельным 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.

Начиная с Windows Server 2003, достаточно широко стало использоваться понятие *роли сервера* (server role), которое связывалось с определенными прикладными службами, работающими на сервере. Например, сервер может 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. 2.20), для которой в меню **Start** (Пуск) имеется закрепленный значок, а также соответствующий значок присутствует на панели быстрого запуска.

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[1] (Файловые службы). Список ролей приведен в табл. 2.1; он достаточно информативен сам по себе и не требует дополнительных комментариев.

---

[1] А именно — служба File Server (Файловый сервер).

Таблица 2.1. *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)
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. 2.2. Многие компоненты будут рассматриваться подробно в соответствующих главах при описании тех или иных административных задач или прикладных служб.

Таблица 2.2. *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)

Таблица 2.2 *(продолжение)*

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)
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)

Таблица 2.2 *(окончание)*

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* со всеми ее дополнительными возможностями *(см. выше)*.

Установка ролей и компонентов

Окно оснастки **Server Manager** (Диспетчер сервера, ServerManager.msc[1]) представлено на рис. 2.20. 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).

К числу этих средств относятся оснастки **Event Viewer** (Просмотр событий), **Device Manager** (Диспетчер устройств) и т. д. (сравните с рис. 2.23). 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. 2.21). Обратите внимание на ссылки, имеющиеся на панелях в правой части, — с их помощью устанавливаются и удаляются роли и компоненты, а также отдельные службы роли.

---

[1] Для запуска этой оснастки из меню **Start** (Пуск) используется специальная утилита CompMgmtLauncher.exe, хотя оснастка может запускаться непосредственно, при вводе ее имени.

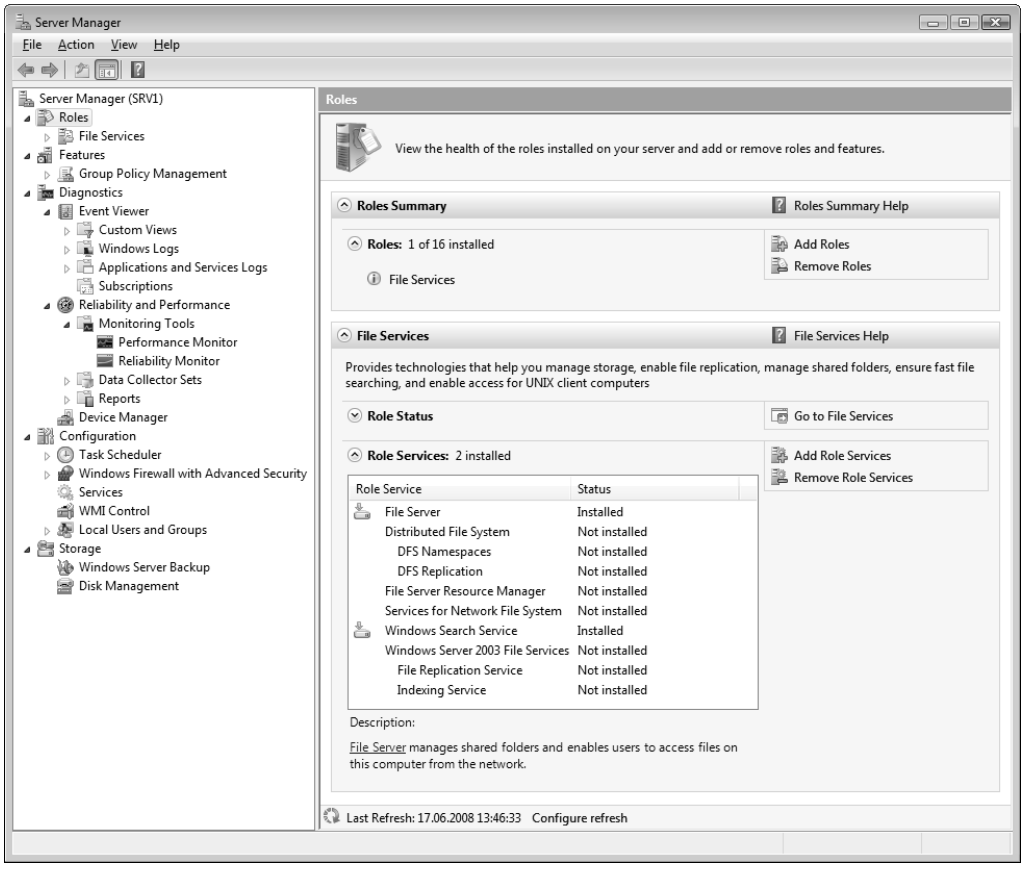


Рис. 2.20. Основное окно оснастки **Server Manager**

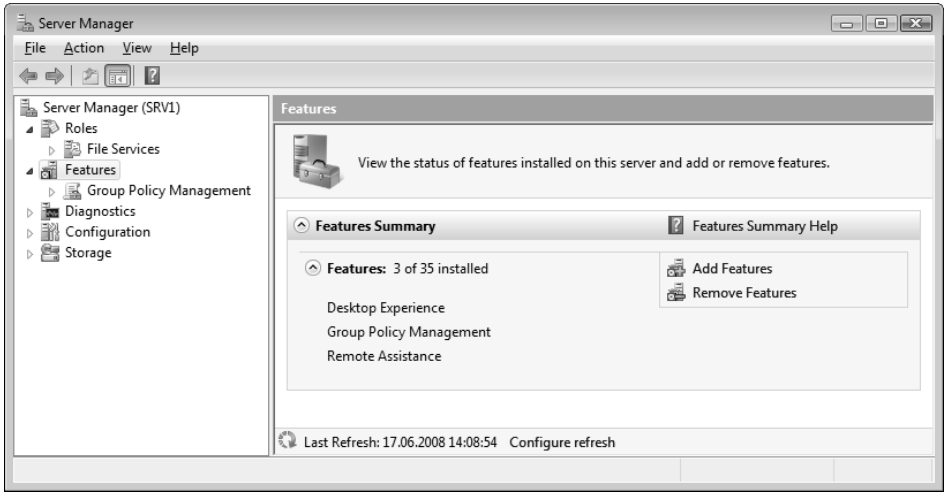


Рис. 2.21. Панель установленных компонентов

Чтобы установить роль сервера, выберите узел **Roles** (Роли) и щелкните по ссылке **Add Roles** (Добавить роли). В окне мастера добавления ролей (рис. 2.22) установите флажки около названий нужных ролей (обратите внимание на то, что для каждой роли имеется подробное описание), а затем нажмите кнопку **Install** (Установить). (Уже установленные роли отмечены галочками; для их удаления используется соответствующая ссылка на панели ролей.) После установки многих ролей требуется перезагрузка компьютера — в этом случае в окне мастера появляется предупреждение.

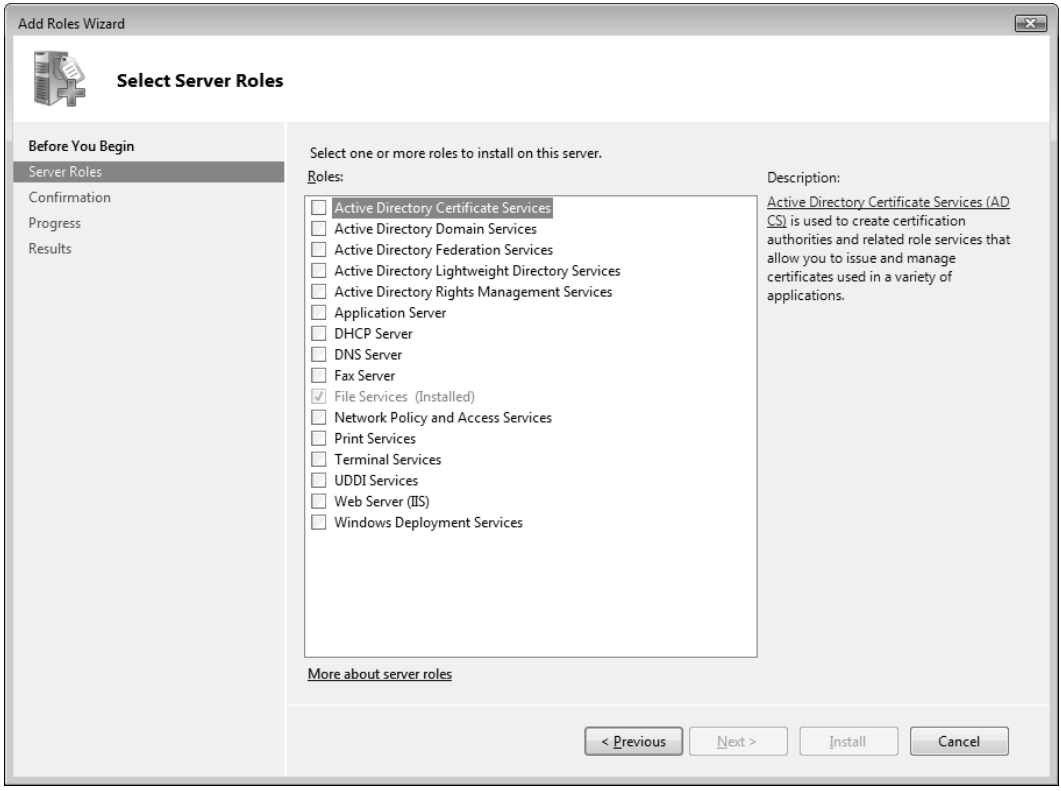


Рис. 2.22. Окно мастера добавления ролей

В процессе установки роли мастер может предложить на выбор список устанавливаемых *служб роли*. Например, в составе файловых служб имеется много разных сервисов (см. рис. 2.20), 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 следует установить галочки для нужных компонентов и нажать кнопку **Install** (Установить).

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).

Внимание!

Все сообщения, связанные с установкой и удалением ролей, компонентов и служб ролей сервера, регистрируются в системном журнале Setup (Настройка).

Установка ролей из командной строки

В полных версиях Windows Server 2008 имеется утилита *ServerManagerCmd.exe*, с помощью которой можно управлять установкой и удалением ролей и компонентов сервера. Команда `servermanagercmd -query` позволяет увидеть список всех имеющихся компонентов, где крестиком отмечены установленные роли и службы[1], например:

```
...
[X] Remote Server Administration Tools  [RSAT]
    [X] Role Administration Tools  [RSAT-Role-Tools]
        [ ] Active Directory Certificate Services Tools  [RSAT-ADCS]
            [ ] Certification Authority Tools  [RSAT-ADCS-Mgmt]
            [ ] Online Responder Tools  [RSAT-Online-Responder]
        [X] Active Directory Domain Services Tools  [RSAT-ADDS]
            [X] Active Directory Domain Controller Tools  [RSAT-ADDC]
            [ ] Server for NIS Tools  [RSAT-SNIS]
        [X] Active Directory Lightweight Directory Services Tools  [RSAT-
ADLDS]
...
```

В квадратных скобках указаны имена компонентов, которые используются для их установки и удаления. Например, для установки на сервере оснасток для администрирования доменных служб Active Directory требуется следующая команда (для удаления служит параметр `-remove`):

```
servermanagercmd -install RSAT-ADDS
```

Внимание!

Следует иметь в виду, что если при установке (удалении) указывается имя "составного" компонента, то устанавливаются все входящие в него элементы (с име-

[1] Они также выделены цветом.

нами более "низкого" уровня). Это далеко не всегда нужно, поэтому требуемые компоненты лучше указывать конкретно.

В системах Windows Server Core и Hyper-V Server утилита ServerManagerCmd.exe отсутствует; вместо нее используются две утилиты — *Oclist.exe* и *Ocsetup.exe*.

Команда `oclist` позволяет получить список компонентов в следующем виде (имена указаны после двоеточия):

```
Microsoft-Windows-ServerCore-Package
Not Installed:BitLocker
...
Not Installed:DHCPServerCore
Not Installed:DirectoryServices-ADAM-ServerCore
    Installed:DirectoryServices-DomainController-ServerFoundation
Not Installed:DNS-Server-Core-Role
...
```

Для установки и удаления компонентов служит утилита Ocsetup, которую следует запускать следующим образом (параметр `/w` необходим для того, чтобы было видно окончание операции):

```
start /w ocsetup DNS-Server-Core-Role
```

Для удаления указанного компонента к команде нужно добавить параметр `/uninstall`.

Управление системными компонентами и учетными записями — оснастка *Computer Management*

Помимо новой оснастки **Server Manager** (Диспетчер сервера) *(см. выше)*, одним из основных инструментов администрирования систем Windows Server 2008 остается традиционная оснастка **Computer Management** (Управление компьютером) (рис. 2.23). В отличие от упомянутого диспетчера сервера, эту оснастку можно подключать как к локальному компьютеру, так и к удаленным системам.

Оснастку можно запускать из меню **Start** (Пуск) или с панели управления. В предыдущих версиях Windows ее можно также вызвать, щелкнув правой кнопкой мыши по значку **Computer** (Мой компьютер) в меню **Start** (Пуск) или на рабочем столе и выбрав в контекстном меню пункт **Manage** (Управление). В системах Windows Server 2008 в этом случае запускается оснастка **Server Manager** (Диспетчер сервера).

Как можно видеть на рис. 2.23, в пространстве имен оснастки имеются три узла, содержащие оснастки определенного назначения. Практически все эти средства подробно рассматриваются в последующих главах.

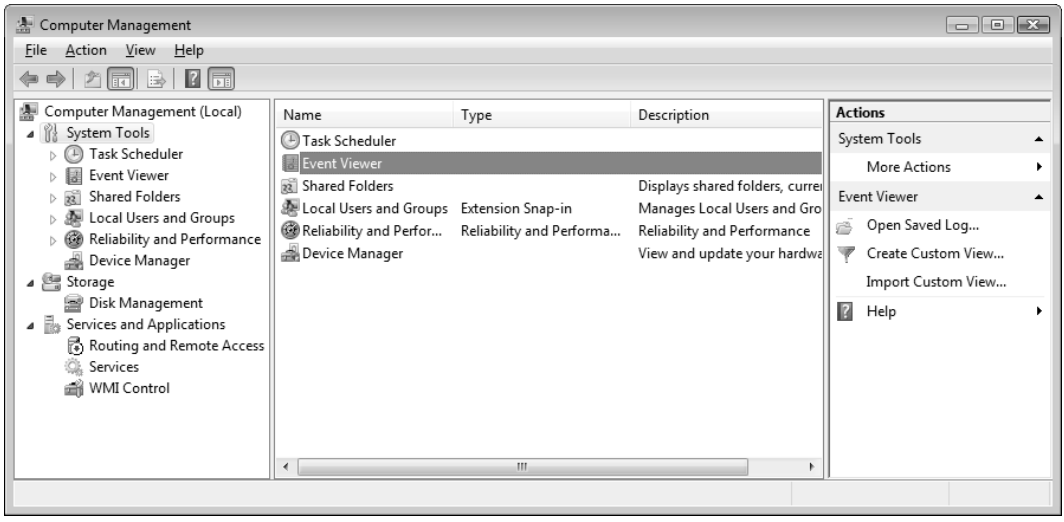


Рис. 2.23. Окно оснастки **Computer Management**

Управление учетными записями

Традиционная оснастка **Local Users and Groups** (Локальные пользователи и группы), входящая в состав оснасток **Server Manager** (Диспетчер сервера) и **Computer Management** (Управление компьютером), используется для управления локальными пользователями и группами (в доменах для управления учетными записями служит оснастка **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры). В простейших случаях для работы с локальными пользователями можно также использовать имеющуюся на панели управления задачу **User Accounts**[1] (Учетные записи пользователей) (категория **User Accounts** (Учетные записи пользователей)).

Имеется еще одно окно управления учетными записями, для доступа к которому проще всего ввести строку `control userpasswords2` или `netplwiz` в меню **Start** (Пуск) или в окне **Run** (Выполнить). В этом окне перечислены локальные учетные записи пользователей и предлагаются некоторые дополнительные функции, касающиеся безопасности. Интерес представляют возможности этого окна на автономных компьютерах (рис. 2.24).

Выбрав в списке учетную запись пользователя, можно сменить для нее пароль. 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 указывать свой пароль. Если же выбрать некоторую учетную запись и сбросить флажок (при подтверждении

[1] С ее помощью нельзя работать с учетными записями *групп*.

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.

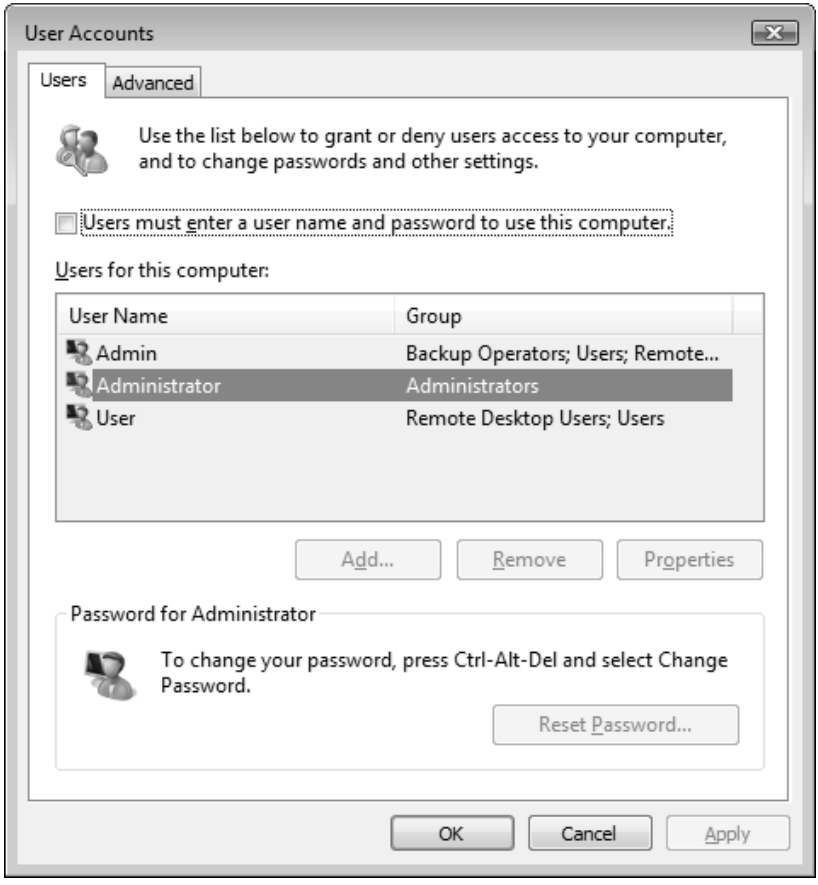


Рис. 2.24. Окно дополнительных возможностей по управлению локальными учетными записями

В окне консоли для управления учетными записями используется стандартная команда `net` с параметрами `USER`, `ACCOUNTS`, `GROUP` и `LOCALGROUP`. С ее помощью можно выполнять следующие операции:

- создавать и удалять локальные учетные записи пользователей и групп;
- просматривать списки учетных записей и членов групп;
- добавлять пользователей в группы;
- изменять политики паролей и сами пароли пользователей.

При этом есть операции, которые отсутствуют в оснастке, и их можно выполнить только с помощью утилиты `net` — например, команда `net USER /TIMES` позволяет задать время, когда пользователь сможет регистрироваться на сервере.

Кроме того, утилита `net` располагает множеством других возможностей (например, по управлению подключаемыми дисками и принтерами удаленных компьютеров — *см. главу 4)*, некоторые из которых рассматриваются в других главах.

Управление системными службами

Для различных задач администрирования часто используется оснастка **Services** (Службы), которую можно запускать самостоятельно или в составе других оснасток (см. рис. 2.20 и 2.23). С ее помощью можно просматривать статус и описание служб, запускать, останавливать и перезапускать сервисы (службы), а также конфигурировать опции запуска и восстановления сервисов. Автономная оснастка **Services** (Службы) удобна тем, что может подключаться и с удаленным компьютерам — для этого используется команда **Connect to another computer** (Подключиться к другому компьютеру) в меню **Action** (Действие).

Для управления службами из командной строки используется утилита `sc`. Например, с помощью команды `sc query` можно получить подробную и точную информацию о состоянии служб локального или удаленного компьютера[1] (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.

В версиях Windows Server Core и Hyper-V Server утилита `sc` является основным средством управления сервисами. Например, если на сервере устанавливается роль DHCP-сервера, то соответствующий сервис нужно запустить; а для того, чтобы этот сервис запускался автоматически при загрузке системы, необходимо изменить его состояние запуска. Это легко проделать с помощью следующей команды:

```
sc config DHCPServer start= auto
```

(пробел после знака "равно" обязателен!)

Организация профилей пользователей

Понимание особенностей реализации механизма пользовательских профилей в системах Windows Server 2008 важно для организации работы в среде Windows Server

[1] Для получения простого списка сервисов, запущенных на локальном компьютере, можно использовать команду `net start`. Однако это нужно делать с осторожностью, поскольку в отличие от утилиты `sc` эта команда включает в список работающих служб приостановленные (paused) сервисы!

Server 2008, поскольку администратор должен знать, где по умолчанию хранятся пользовательские файлы и как обеспечивается их защита — какая информация автоматически будет закрыта от других пользователей, а какая будет 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 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!***
>
> В системах Windows 2000/XP и Windows Server 2003 для хранения профилей пользователей используется папка *%SystemDrive%*\Documents and Settings\<*имяПользователя*>. Папка **Documents and Settings** тоже 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.

В папке **Users** (Пользователи) (помимо папки профиля администратора компьютера и скрытых системных папок) имеется папка **Public** (Общие), предназначенная для хранения информации, с которой могут работать как все локальные пользователи, так и пользователи удаленных компьютеров (если к этой папке будет разрешен общий доступ). Подробнее назначение данной папки мы рассмотрим далее.

Структура профиля пользователя

Профиль пользователя создается на основе профиля, назначаемого по умолчанию. Скрытые системные папки **Default** и **All Users**, используемые для определения на-

чальных параметров стандартного профиля, представляют собой реальные папки файловой системы. Папка **Default User** оставлена для совместимости и является ссылкой. Эти папки, как и все папки пользовательских профилей, также хранятся в папке **Users** (Пользователи) корневого каталога загрузочного диска.

На рис. 2.25 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). Обратите внимание на то, что несмотря на то что физическая папка **Public** входит в состав папки **Users**, в окне программы она отображается в виде самостоятельного объекта.

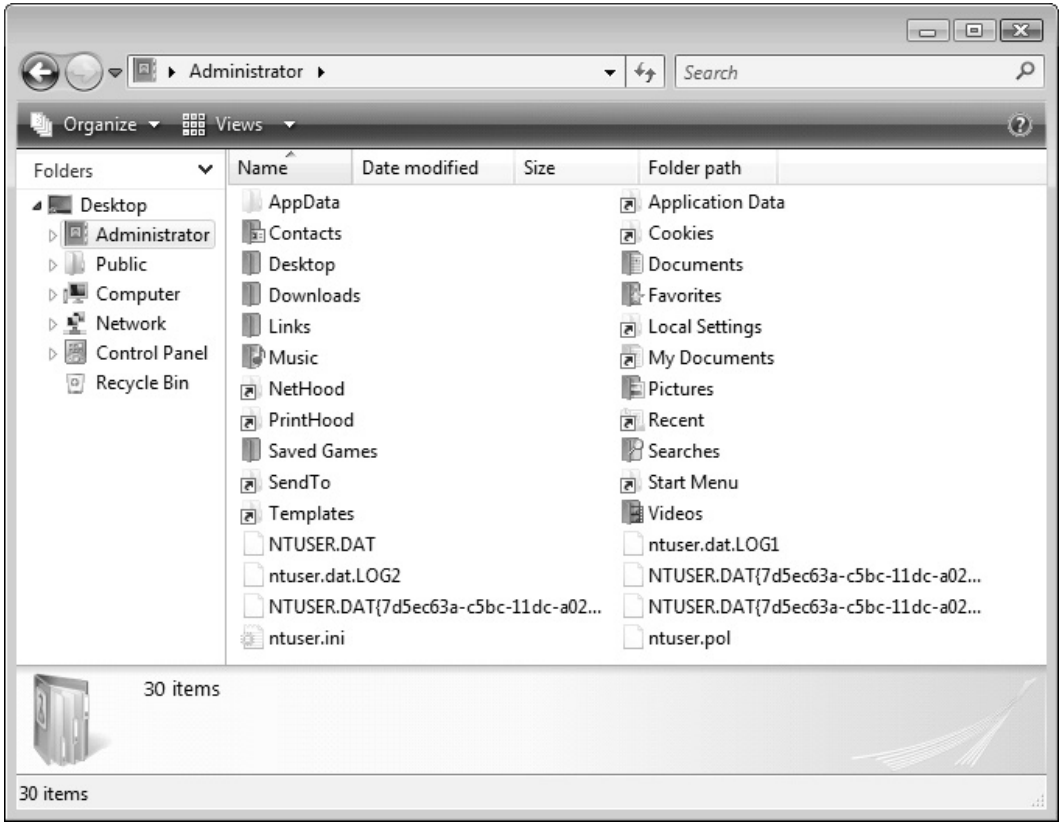


Рис. 2.25. Структура локального профиля пользователя

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`.

Некоторые папки профилей, привычных для 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. 2.3 перечислены некоторые из этих папок и указано их новое полное имя.

Таблица 2.3. *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

Таблица 2.3 *(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 (см. рис. 2.25). Назначение папок понятно из их названия. 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 требуется увидеть реальное имя папки, щелкните мышью по полю адреса — после этого будет отображаться физический путь к папке (иногда именно он нужен для работы). Это проиллюстрировано на рис. 2.26: вверху показано представление по умолчанию, внизу — реальное имя папки.

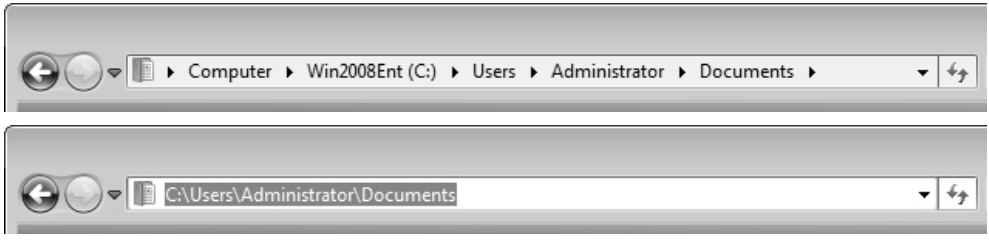


Рис. 2.26. Представление адреса папки в окне программы Windows Explorer и ее реальное физическое имя

Как уже говорилось, внутри папки **Users** (Пользователи) имеется папка **Public** (Общие), в которой пользователи могут сохранять информацию, которая будет доступна всем другим пользователям. Подкаталоги этой папки показаны на рис. 2.27. Администратор может с помощью несложной операции обеспечить доступ к подкаталогам папки **Public** (Общие), указав при этом конкретные права доступа к информации *(см. разд. " Настройка параметров доступа к общим сетевым папкам и принтерам" главы 4)*.

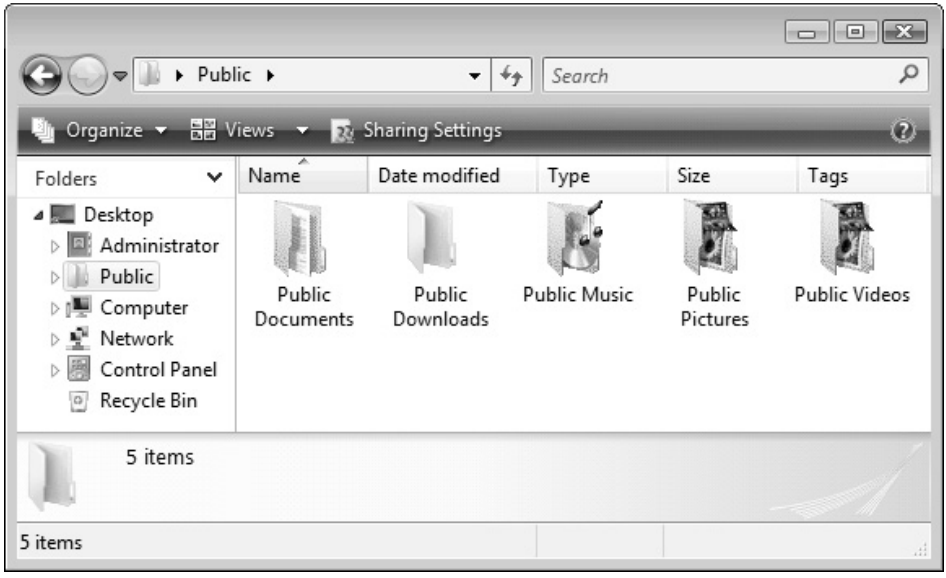


Рис. 2.27. Стандартные папки для общего доступа

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 предыдущих системах Windows: там папку **My Documents** (Мои документы) можно переместить только целиком, со всем ее содержимым.

Поиск информации, хранящейся на сервере

Средства поиска в системах 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 Indexing Service (Служба индексирования), 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, поскольку неправильные или неожиданные[1] 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 простейшего поиска, выполняющегося непосредственно из меню **Start** (Пуск), выбираются в окне свойств панели задач и меню **Start** (рис. 2.28). По умолчанию (индексированный) поиск выполняется только в личных папках пользователя, но можно указать, чтобы просматривался *весь* индекс.

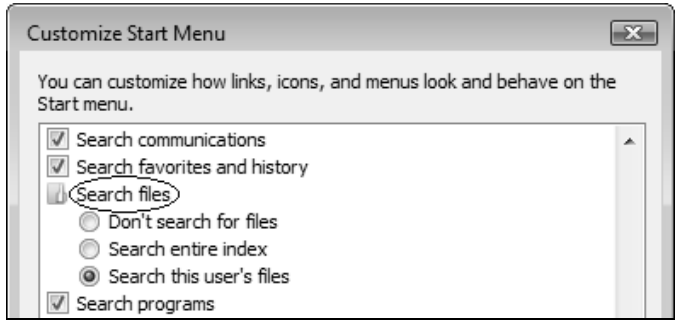


Рис. 2.28. Настройка способов поиска из меню **Start**

Отметим некоторые 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.);

[1] Если пользователь неправильно интерпретирует задаваемые параметры — т. е. он предполагает, что должна выполняться одна операция, а фактически осуществляются другие действия.

- после выполнения поиска непосредственно из меню **Start** (Пуск) появляется ссылка **Search Everywhere** (Искать везде), позволяющая перейти в окно поиска по всем индексированным папкам (аналогичный результат получается при нажатии клавиш <Win>+<F>);
- в окне параметров индексирования (см. рис. 2.31) имеется кнопка **Pause** (Пауза), позволяющая приостановить работу по индексированию файлов и папок на 15 минут.

> ***Примечание***
>
> Поскольку в состав систем Windows Server 2008 уже входит пакет обновлений Service Pack 1, возможности поиска в этих системах отличаются от тех, которые имеются в стандартной (release) версии Windows Vista.

Выполнение операций поиска

Для запуска функции поиска можно нажать клавиши <Win>+<F> или нажать клавишу <F3> (или <Ctrl>+<F>), выбрав папку в окне программы Windows Explorer (Проводник). 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 можно просматривать в таблице и фильтровать, выбирая типы файлов (все, почта, документы и т. п.) на панели поиска (рис. 2.29).

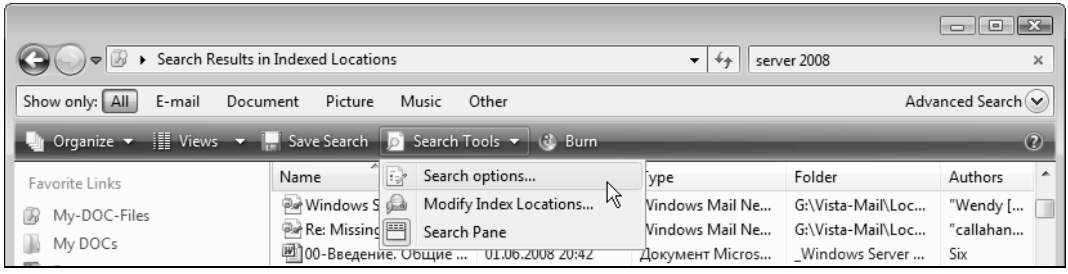


Рис. 2.29. Опции управления поиском

Совет

При выполнении поиска по сложному критерию обращайте внимание на количество найденных файлов (левый нижний угол окна результатов поиска). Это позволит следить за правильностью формирования строки поиска и понимать, влияет ли изменение параметров поиска на получаемые при этом результаты (например, если в нашем примере на рис. 2.29 в строке поиска ввести строку `server 2008` или `file:server 2008` или же строку в кавычках `"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. 2.29), создается хранимый запрос, который можно использовать в дальнейшем (в частности, для создания так называемых *виртуальных папок*).

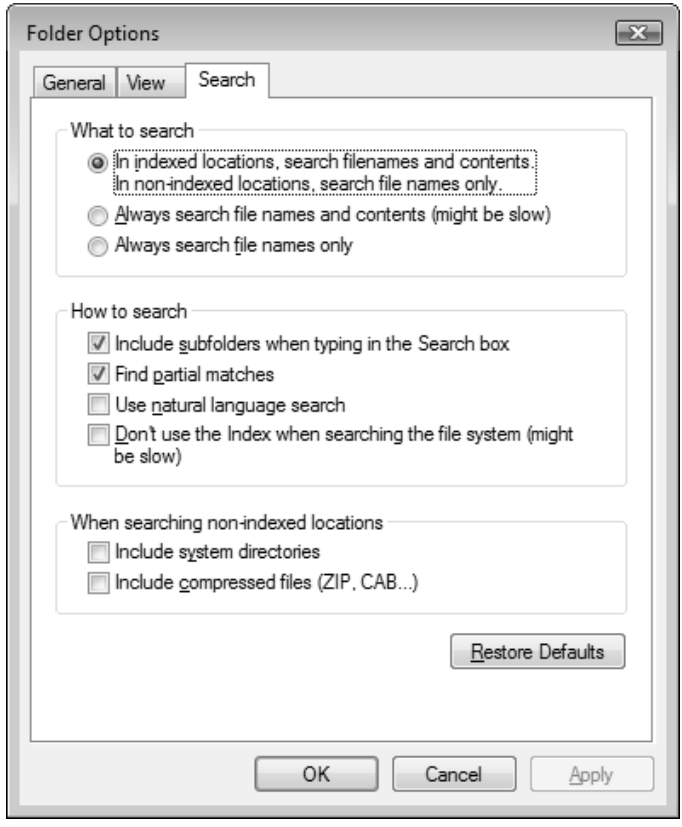


Рис. 2.30. Настройка общих параметров поиска

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. 2.30). 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. 2.29) открывается окно параметров индексирования (рис. 2.31), в котором перечислены все папки, включенные в индекс (в остальных папках поиск будет выполняться медленно, только *по именам* файлов).



Рис. 2.31. Параметры индексирования — список индексируемых папок

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 за монитором. Кнопка **Pause** (Пауза) позволяет приостановить индексирование на 15 минут.

Примечание

Окно индексируемых папок можно 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.

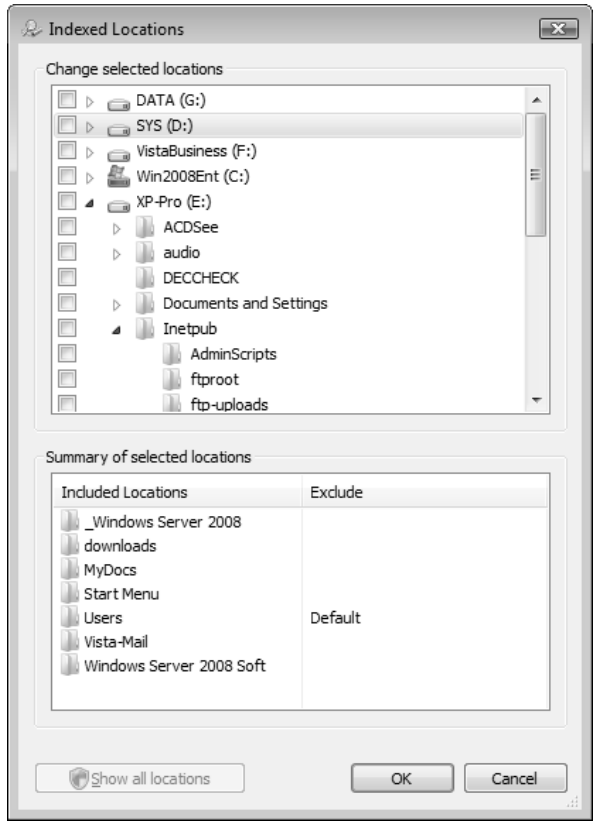


Рис. 2.32. Окно выбора индексируемых папок

Внимание!

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

[1] Нагрузку на систему в процессе индексирования несложно оценить с помощью Системного монитора (Performance Monitor) *(см. главу 3)*.

Для подготовки службы к работе нужно запустить оснастку **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)).

Рекомендуется перед началом работы сервера 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. 2.31) нажать кнопку **Modify** (Изменить) и в следующем окне (рис. 2.32) 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.

Поиск можно начинать не из специального окна, открытого с помощью клавиш <Win>+<F>, а непосредственно при просмотре папок в окне программы Windows Explorer (Проводник), когда некоторая папка выбирается на панели навигации и строка вводится в поле поиска (или если после выбора папки нажимается клавиша <F3>). В таких случаях появляется предупреждение о замедлении поиска в неиндексируемых папках. Поиск выполняется медленно, ход процесса отображается в виде зеленого столбика в поле адреса. Если щелкнуть мышью по строке предупреждения о замедлении поиска, то появится меню, в котором можно выбрать команду включения текущей папки в индекс (**Add to Index**) (это, конечно, не означает, что поиск сразу будет быстрым — на построение индекса нужно время). Поэтому рекомендуется все часто используемые папки заранее включать в индекс.

По окончании поиска в конце результирующего списка отображается панель (рис. 2.33), с которой можно запустить дополнительный поиск по *содержимому* файлов (мы помним, что в неиндекируемых папках поиск внутри файлов не выполняется!) или включить опцию расширенного поиска.

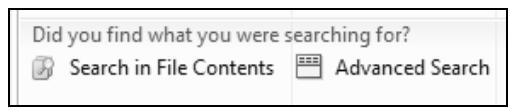


Рис. 2.33. Дополнительные возможности поиска в неиндексируемой папке

В окне расширенного поиска (рис. 2.34) 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).

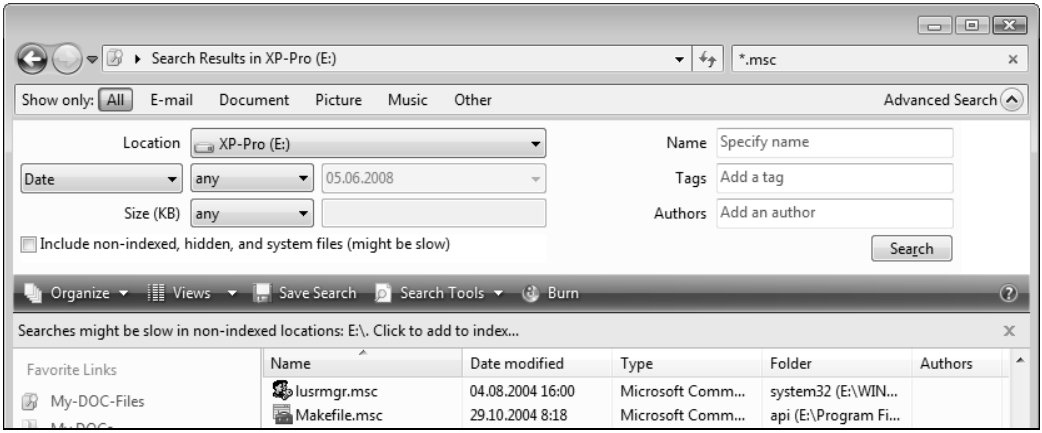


Рис. 2.34. Окно расширенного поиска

Примечание

Обратите внимание на то, что кнопка **Advanced Search** (Расширенный поиск) имеется и в стандартном окне поиска в индексированных папках, которое вызывается при нажатии клавиш <Win>+<F> (см. рис. 2.29). 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 типу документов, по тегам, по дате или размеру — реализован в окне расширенного поиска (см. рис. 2.34)).

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 про-

писные 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 обязательно 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 эквивалент для русскоязычных версий системы):

- *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, следует 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 впоследствии обращаться к ним повторно.

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.

В зависимости от поставленной задачи 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).
2. На панели структуры откройте узел **Local Policies** | **Audit Policy** (Локальные политики | Политика аудита) (рис. 2.35).
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. 2.35). В группе **Audit these attempts** (Вести аудит следующих попыток доступа) установите флажки **Success** (Успех) или **Failure** (Отказ) или оба.
4. Нажмите кнопку **OK**.

Подобную операцию следует повторить для тех политик аудита, которые требуется 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).

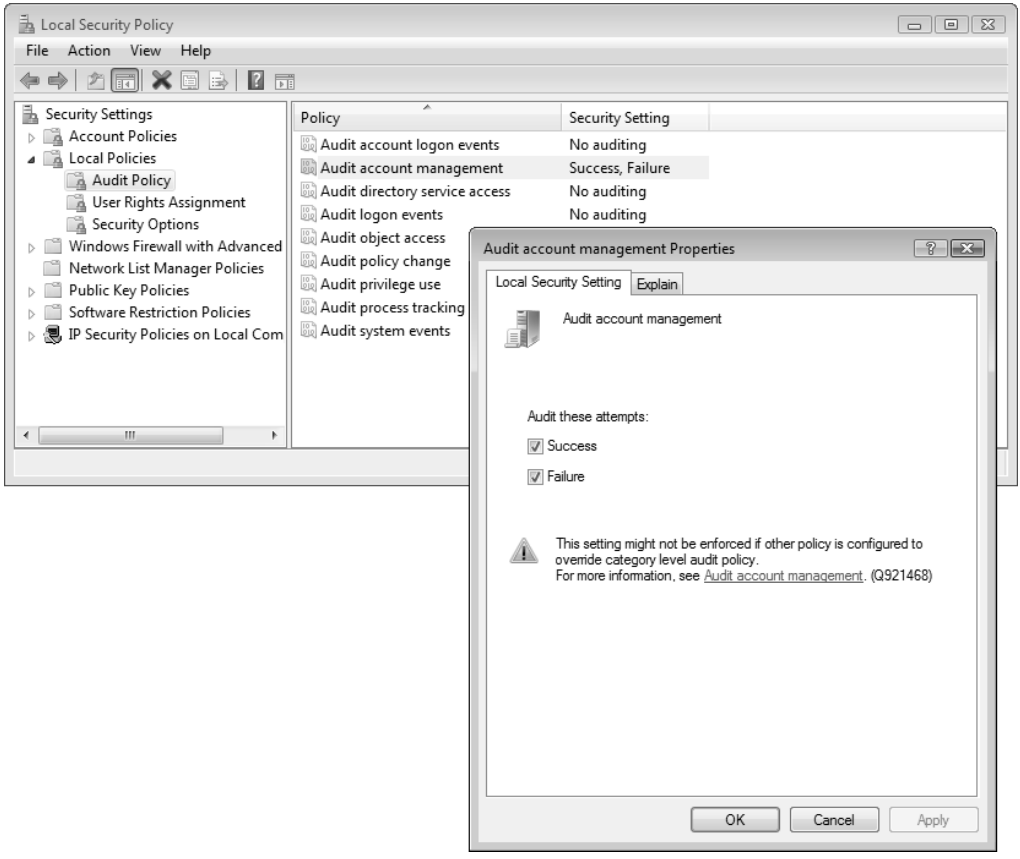


Рис. 2.35. Настройка политик аудита на локальном компьютере

Настройка и просмотр параметров аудита для папок и файлов

Для того чтобы настроить, просмотреть или изменить параметры аудита файлов и папок, требуются следующие действия:

1. В окне программы Windows Explorer (Проводник) выберите файл или папку, откройте окно свойств и перейдите на вкладку **Security** (Безопасность).

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. 2.36) — кнопку **Add** (Добавить).
3. При добавлении записей, для которых будет вестись аудит, появляется стандартное окно выбора учетных записей — выберите нужную запись и нажмите кнопку **OK**. Откроется окно **Auditing Entry** (Элемент аудита) (рис. 2.37), где нужно установить все требуемые параметры аудита для указанной записи. В списке **Apply onto** (Применять) укажите, где именно следует выполнять аудит (это поле ввода доступно только для папок). На панели **Access** (Доступ) укажите, 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).

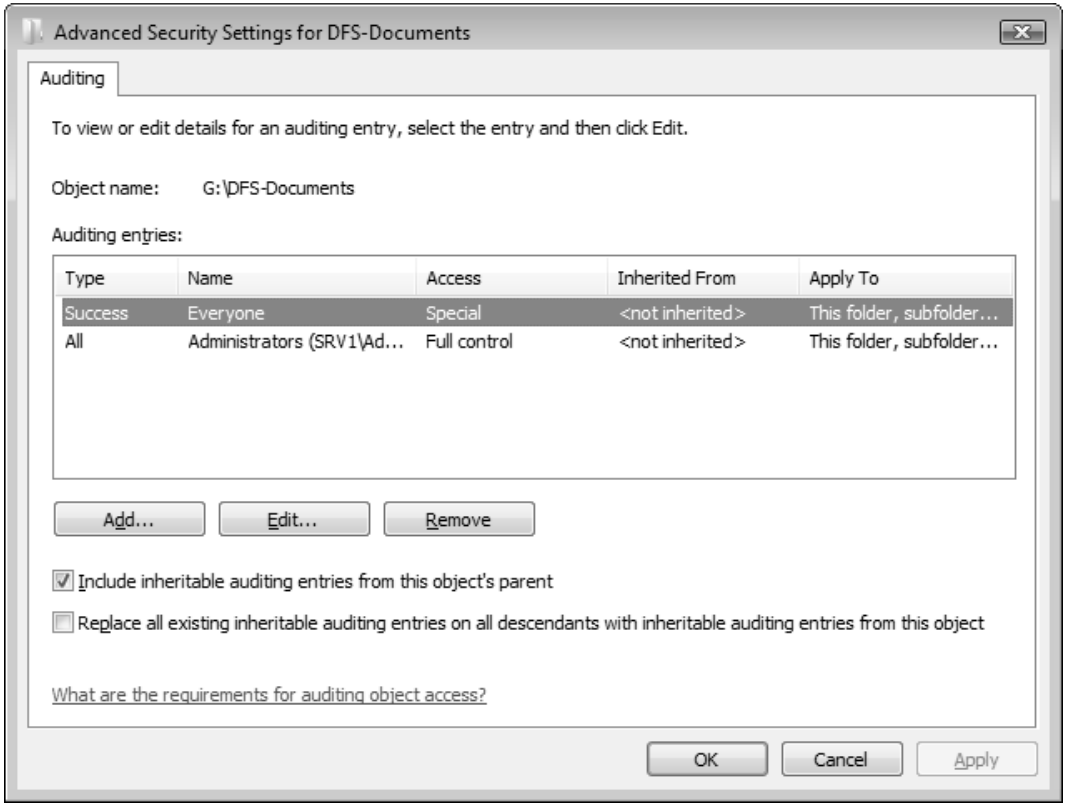


Рис. 2.36. Определение учетных записей и операций, для которых будет выполняться аудит для выбранной папки

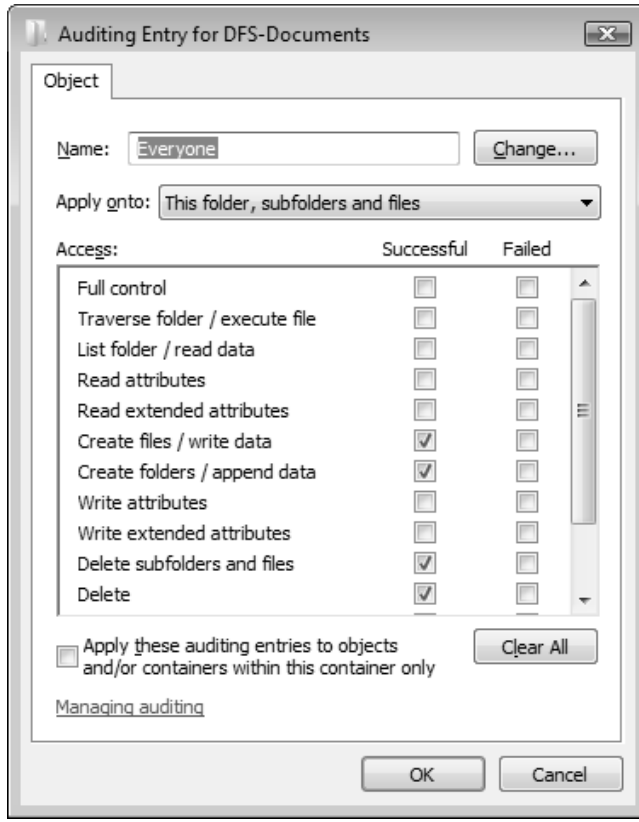


Рис. 2.37. Определение событий, аудит которых будет вестись для выбранных учетных записей (пользователей или групп)

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.

После всех выполненных действий все события доступа к выбранным объектам файловой системы будут регистрироваться в журнале безопасности, для которого лучше создать настраиваемое представление, фильтрующее нужные события *(см. разд. "Фильтрация событий" главы 3)*.

Отключение аудита для выбранных объектов

Чтобы отключить аудит для файла или папки, достаточно удалить все записи аудита в окне дополнительных параметров этого объекта (см. рис. 2.36). 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).

Удаленный административный доступ к компьютеру

Функция *Remote Desktop* (Удаленный рабочий стол) реализуется на основе служб терминалов (Terminal Services) и позволяет подключаться к системе с любого удаленного компьютера или Windows-терминала и работать, как на локальной консоли. Для версий Windows Server Core эта функция является одним из важнейших средств администрирования. По соображениям безопасности удаленный доступ по умолчанию выключен.

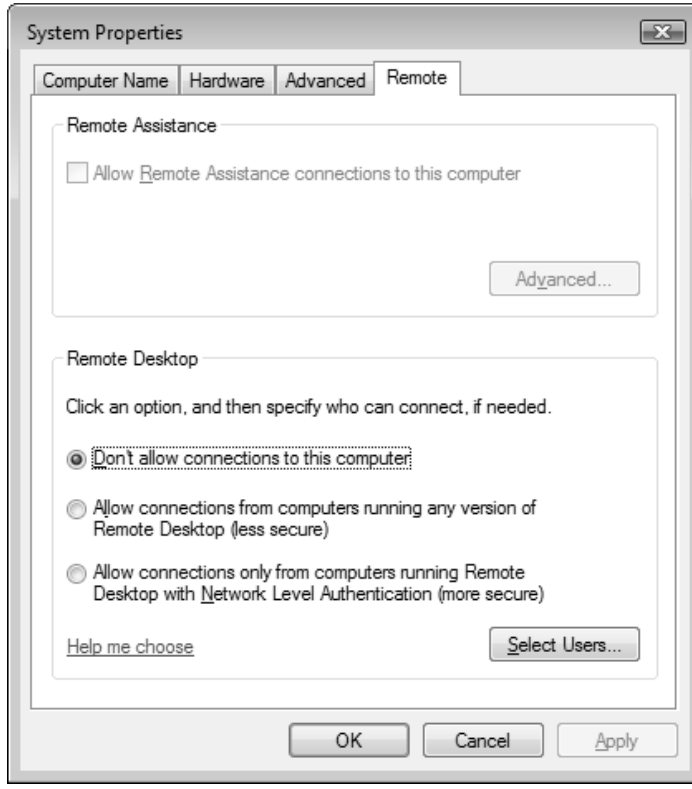


Рис. 2.38. Окно управления удаленным доступом

В системах Windows Server 2008 сохранено еще одно средство с похожими возможностями, называемое *Remote Assistance* (Удаленный помощник). С его помо-

щью пользователь компьютера может для получения консультации 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).

Для включения режима административного удаленного доступа используется вкладка **Remote** (Удаленное использование) окна **System Properties** (Свойства системы) (рис. 2.38). (Для быстрого доступа к этому окну нажмите клавиши <Win>+<Pause/Break>, а в открывшемся окне (см. рис. 2.10) щелкните 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.)

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 метод сетевой аутентификации NLA, позволяющий 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.

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.

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.

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).

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 предупреждение о том, что данное подключение не прошло полной проверки на безопасность, 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).

На следующем шаге требуется указать имя и пароль учетной записи, которая будет использоваться для регистрации на удаленном компьютере. При установке флажка **Remember my credential** (Запомнить мои учетные данные) введенные данные сохраняются и используются при повторных подключениях к выбранному компьютеру. Если выполняется подключение к компьютеру, работающему под управлением операционной системы младше, чем Windows Vista, то параметры учетной записи вводятся в окне регистрации в удаленной системе.

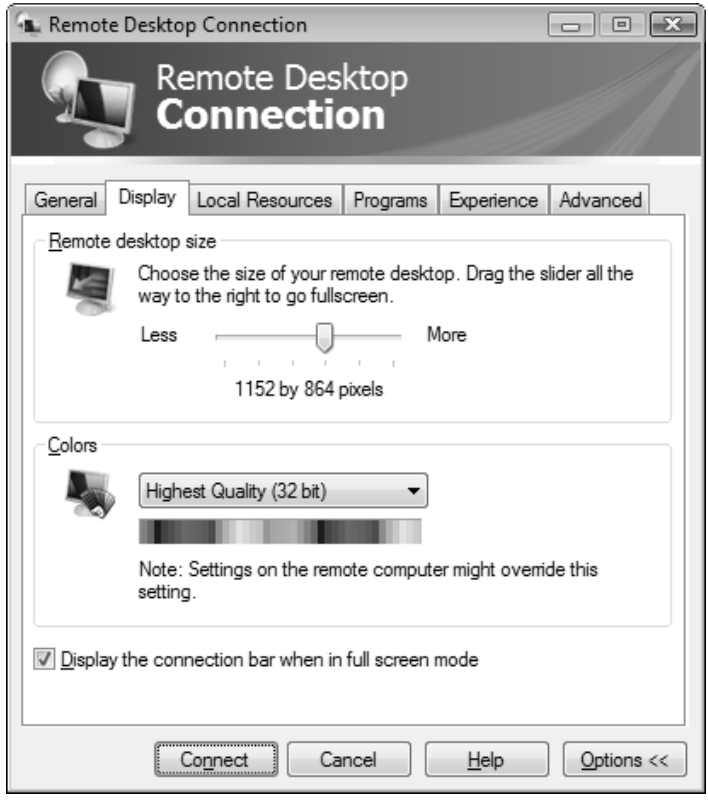


Рис. 2.39. Определение параметров окна, используемого в сеансе удаленного доступа

По умолчанию системы Windows Server 2008 пытаются использовать NLA-аутентификацию. Если это не удается, то может появиться сообщение о невозможности проверки удаленной системы. 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) нажмите кнопку **Options** (Параметры). На вкладке **General** (Общие) можно ввести имя учетной записи и сохранить параметры в файле; на вкладке **Display** (Экран) устанавливаются размер экрана и глубина цвета (до 32 бит) (рис. 2.39); на вкладке **Experience** (Дополнительно) задается скорость подключения и т. д.

Следует особо обратить внимание на вкладку **Local Resources** (Локальные ресурсы) (рис. 2.40): здесь можно указать, какие локальные диски или другие ресурсы (например, принтеры) будут использоваться при работе на удаленном компьютере.

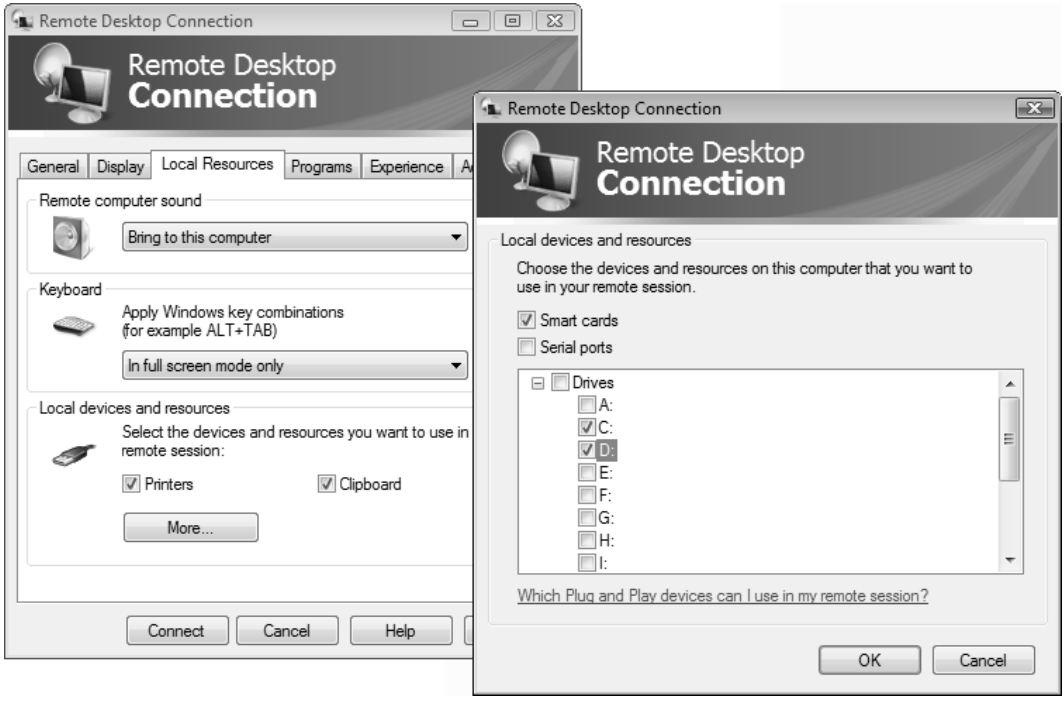


Рис. 2.40. Параметры использования локальных ресурсов в сеансе удаленного доступа

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 RDP-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 дальнейшем для быстрого подключения к конкретному компьютеру. Для редактирования сохраненных параметров подключения выберите файл или значок, щелкните правой кнопкой мыши и в контекстном меню выполните команду **Edit** (Изменить) — появится окно настроек (см. рис. 2.39).

Одновременное подключение к одному компьютеру

В системах Windows Server 2008 одновременно активными могут быть два подключения к рабочему столу, при этом считаются локальные подключения и подключения с использованием функции Remote Desktop (Удаленный рабочий стол). 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 отключаться, 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. 2.41). Отключаемый пользователь на своем экране увидит сообщение о попытке удаленного подключения к локальному компьютеру. 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).

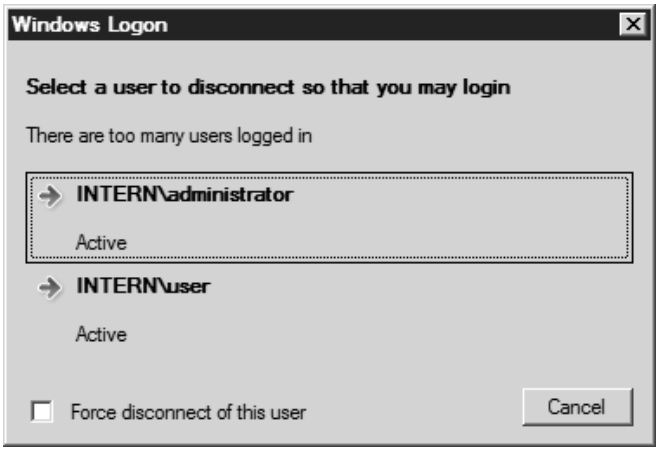


Рис. 2.41. Запрос на отключение зарегистрированного пользователя в случае конфликтов

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.

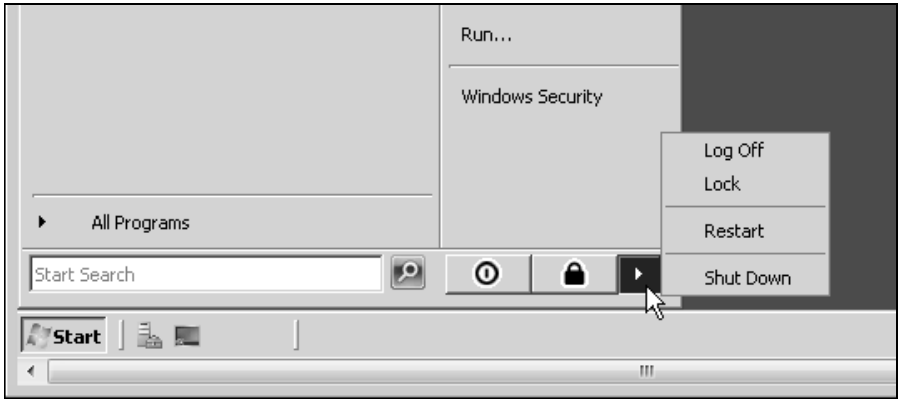


Рис. 2.42. Меню команд управления компьютером при удаленном доступе к Windows Server 2008

На рис. 2.42 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 (при этом все приложения и окна останутся в рабочем состоянии).

Для сравнения покажем подключения к удаленной системе Windows XP. Кнопки команд выхода из системы и отключения сеанса присутствуют в меню **Start** (Пуск) (рис. 2.43), а доступ к командам перезагрузки или выключения компьютера можно получить, только нажав кнопку **Безопасность Windows**.

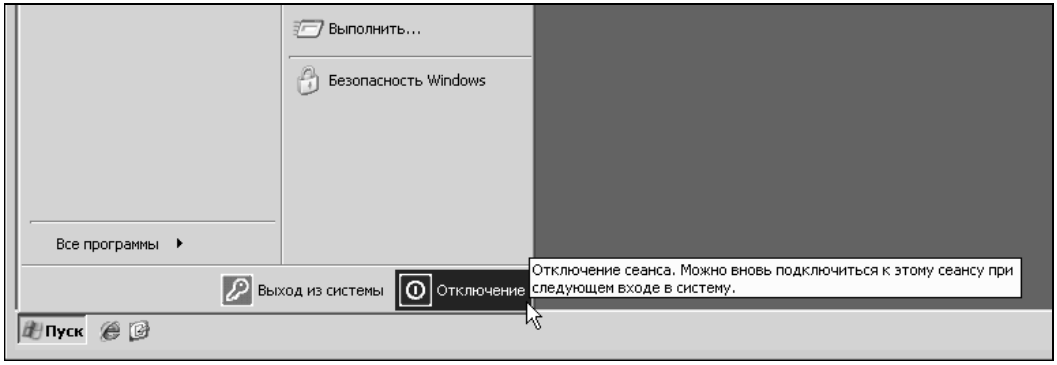


Рис. 2.43. Элементы управления сеансов удаленного доступа в Windows XP

Включение функции Remote Desktop из командной строки

Для включения удаленного доступа в версиях Windows Server Core и Hyper-V Server можно использовать утилиту RegEdit.exe и непосредственно редактировать параметры реестра или же воспользоваться имеющимися специальными сценариями.

Разрешение или запрет на работу функции Remote Desktop (Удаленный рабочий стол) определяется в системном реестре параметром `fDenyTSConnections` (DWORD), который находится в разделе `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server`.

Для изменения этого параметра в версиях Windows Server Core используется следующая команда (значение 0 разрешает удаленный доступ, 1 — запрещает[1]):

```
cscript c:\windows\system32\scregedit.wsf /ar 0
```

Уровень безопасности подключения — безопасный (more secure) или небезопасный (less secure) (см. рис. 2.38) — определяется параметром `UserAuthentication`, хранящимся в разделе `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp`. Это значение можно определить с помощью редактора реестра или посредством команды `cscript scregedit.wsf /cs` (0 соответствует небезопасным подключениям, 1 — безопасным).

В системе Hyper-V Server для выполнения описанных операций применяется стандартный сценарий управления HVConfig.cmd *(см. главу 1)*, где имеется соответствующая опция — **7) Remote Desktop**.

> ***Внимание!***
>
> При разрешении удаленных подключений к рабочему столу необходимо также разрешить соответствующие правила (группа "Remote Desktop") для встроенного брандмауэра Windows *(см. главу 6)*.

Планирование заданий, выполняющихся по расписанию

В системах Windows Server 2008 капитально обновлены два основных средства планирования задач: 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.

Для запуска программ существуют различные регламенты: 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.

---

[1] Обратите внимание на название параметра, где фигурирует слово "запрет" — поэтому именно значение 0 определяет *разрешение* операции!

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).

Служба *Task Scheduler* (Планировщик заданий; имя Schedule) инсталлируется вместе с системой и автоматически запускается при ее загрузке. Для управления задачами служит оснастка **Task Scheduler** (Планировщик заданий; taskschd.msc), запускаемая из меню **Administrative Tools** (Администрирование). В ее окне (рис. 2.44) осуществляется просмотр списков запланированных заданий (что упрощает подготовку и отладку заданий), а также общую статистику по всем заданиям. После запуска оснастки по умолчанию отображаются основные панели: панель **Task Status** (Состояние задачи) позволяет быстро определить, какие задания выполняются, сколько задач завершилось успешно и сколько потерпели неудачу (изначально показаны данные за последние 24 часа). Здесь выводится основная информация о заданиях: время запуска и окончания, состояние, результат выполнения задания.

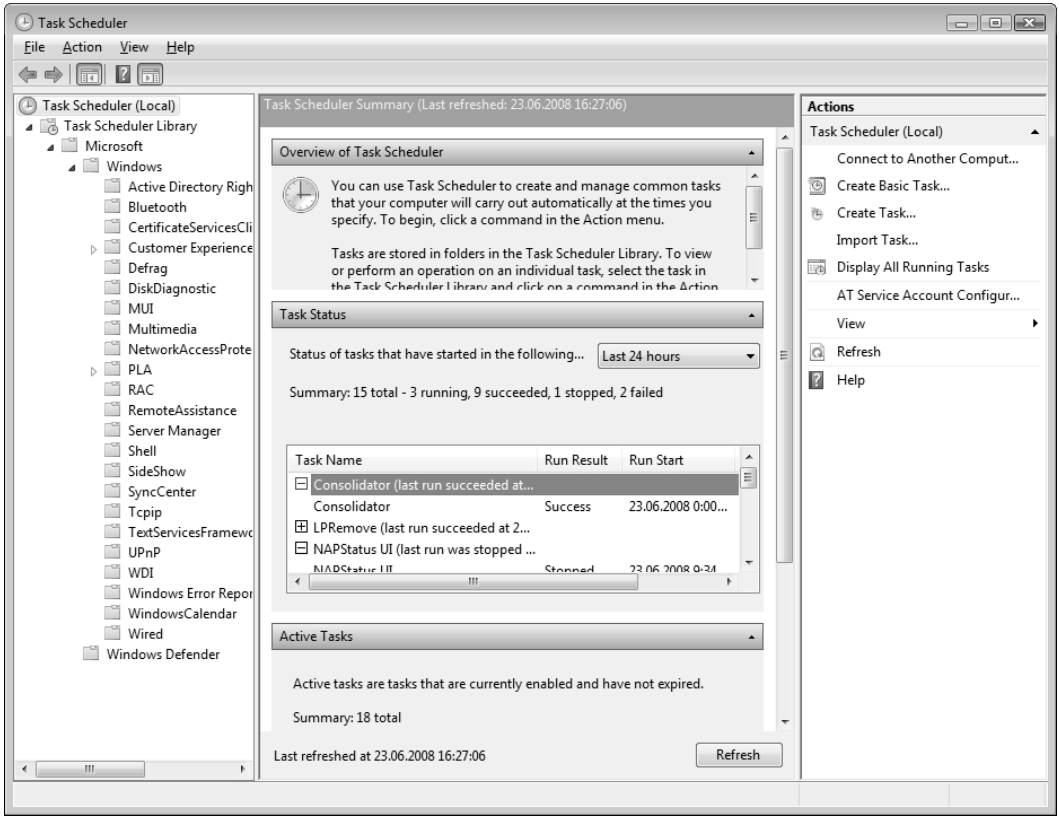


Рис. 2.44. Окно планировщика позволяет просматривать выполненные и запланированные задания

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. 2.45).

При просмотре отдельных заданий в окне планировщика можно, не открывая дополнительных окон, сразу видеть основные параметры задания[1] (рис. 2.45): все параметры, включая параметры запуска и расписание, отображаются на вкладках на панели в центре главного окна оснастки. (Для изменения параметров выберите ссылку **Properties** (Свойства) справа на панели **Actions** (Действия).) На вкладке **History** (Журнал) отображаются результаты выполнения выбранной задачи. В любой момент задачу можно запустить для проверки непосредственно из папки заданий (команда **Run** (Выполнить) в контекстном меню выбранного задания или на панели действий).

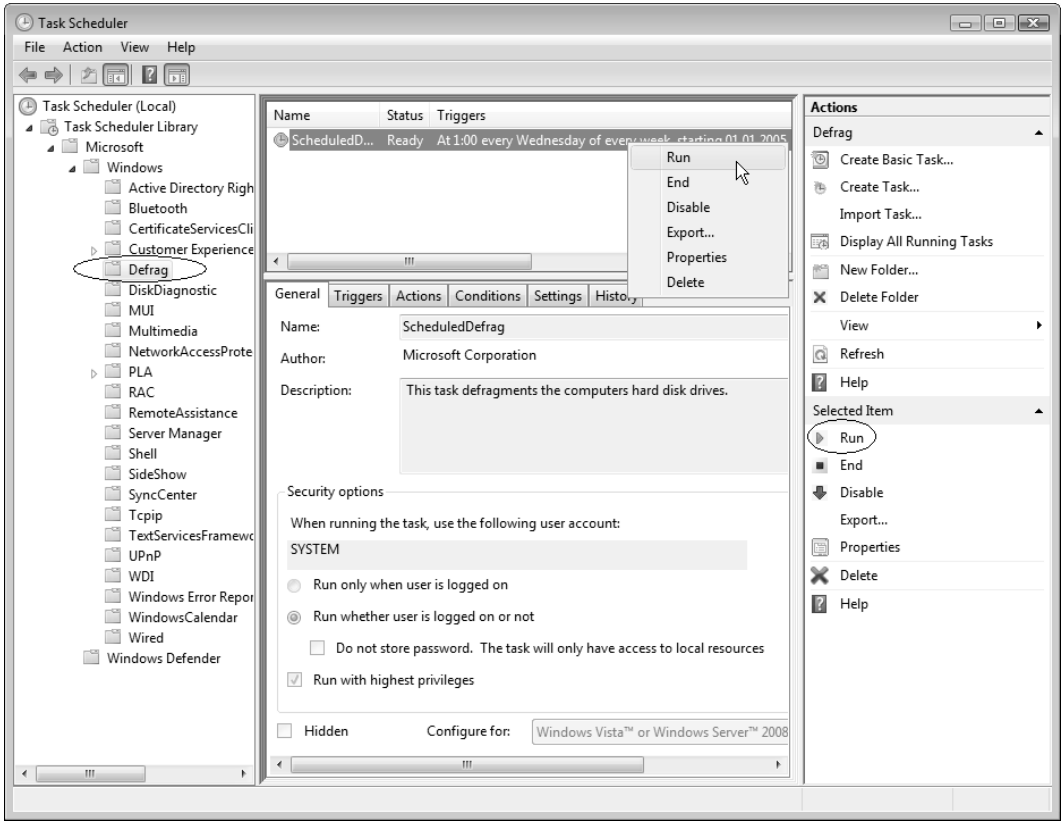


Рис. 2.45. Просмотр свойств задания и команды управления

[1] Для примера показана стандартная задача запуска утилиты дефрагментации дисков.

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.

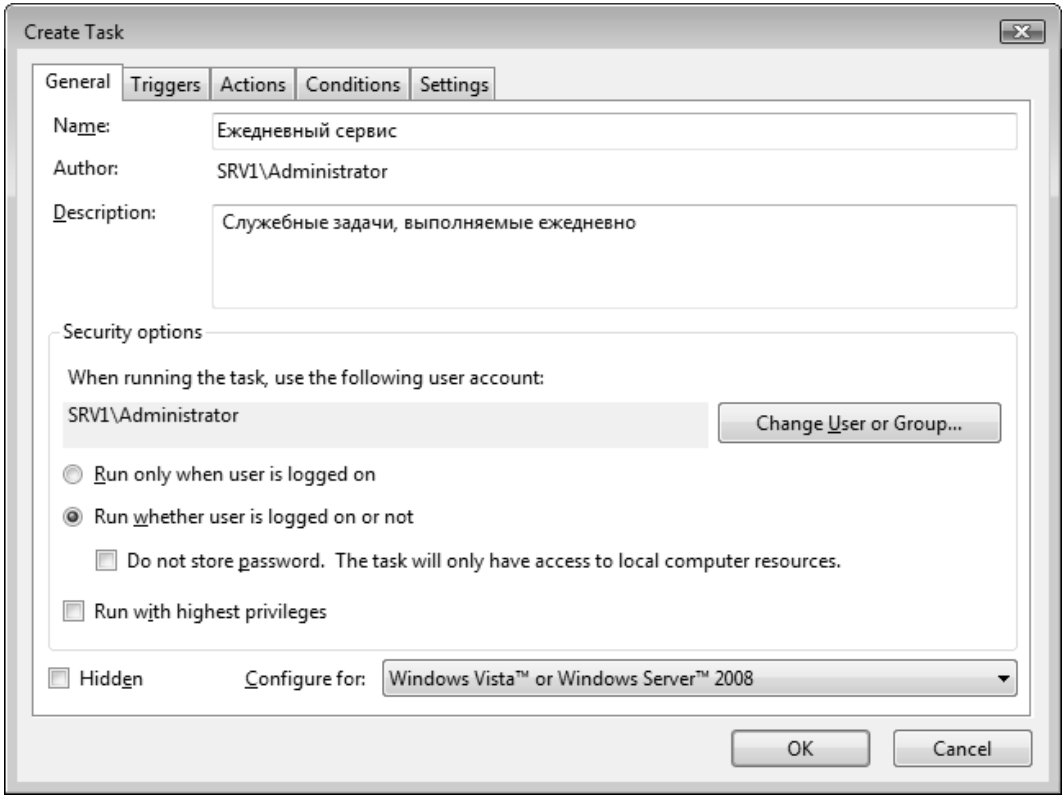


Рис. 2.46. Общие параметры новой планируемой задачи

При создании задания сначала в библиотеке планировщика выберите или создайте папку, где будет храниться описание задания, после чего в окне ее свойств (рис. 2.46) введите 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). Для выбора другого пользователя нажмите кнопку **Change User or Group** (Изменить) и найдите требуемую учетную запись. Такой подход

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.

При ручном планировании заданий последовательно введите необходимые параметры на вкладках окна **Create Task** (Создание задачи) (см. рис. 2.46), после чего закройте окно, нажав кнопку **ОК**. Если все параметры заданы правильно, новая задача появится в библиотеке планировщика заданий.

При создании задачи обязательной является информация, указываемая на вкладках **Trigger** (Триггеры) и **Actions** (Действия). На первой из названных вкладок (рис. 2.47) 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 для выполнения этих операций имеются на панели **Actions** (Действия).

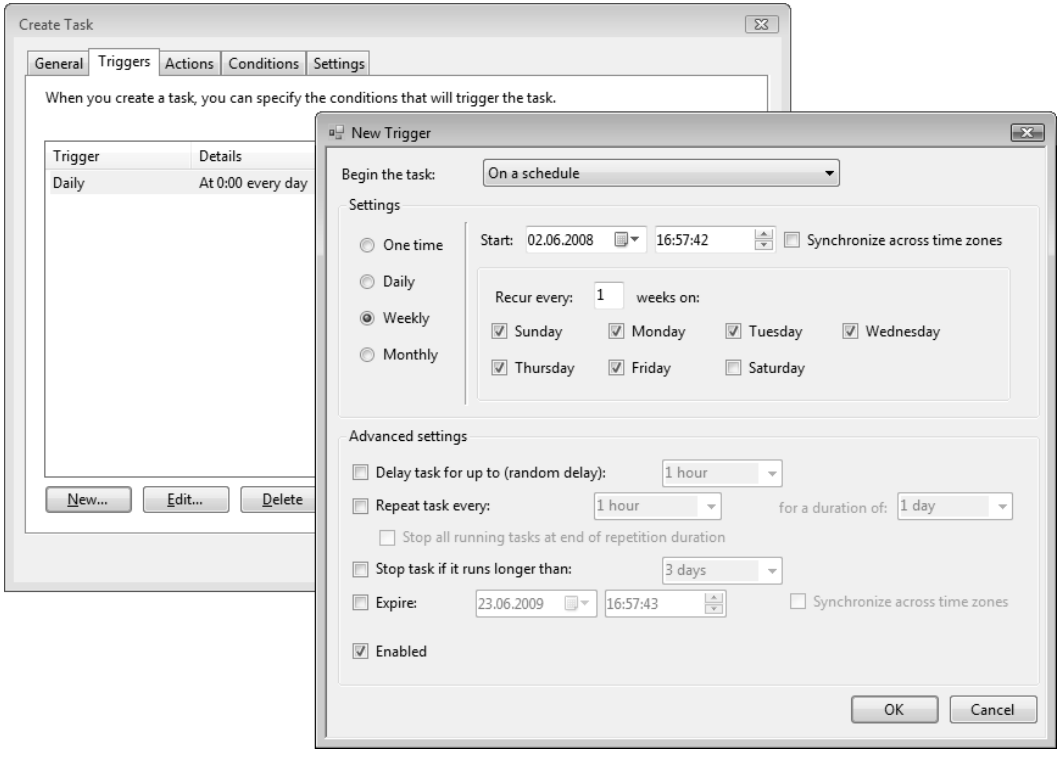


Рис. 2.47. Выбор расписания для запуска задачи

Служба времени Windows (W32Time)

Служба времени Windows (Windows Time Service; имя сервиса W32Time) обеспечивает синхронизацию системных часов. 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 к домену параметр `Parameters\Type` изменяет свое значение на `NT5DS`, и синхронизация времени осуществляется только от контроллеров домена. (Для систем Windows Server 2008 также можно использовать значение `AllSync` — тогда 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 параметров в реестре службы времени Windows ее следует перезапустить с помощью оснастки **Service** или в окне консоли (используя команду `net stop w32time && net start w32time`). Если для настройки параметров использовалась утилита w32tm.exe, то новые значения 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 кон-

троллером, 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.

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.

Эту же задачу можно выполнить 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, в качестве сервера времени используют веб-узел **time.windows.com**.

Для того чтобы часы компьютера синхронизировались только в соответствии с иерархической структурой доменов (чтобы параметр `Parameters\Type` изменил значение на `NT5DS`), выполните 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`).

Синхронизация и проверка работы службы времени

Для немедленной синхронизации часов с заданным источником времени (внешним сервером или контроллером домена) используется команда `w32tm /resync`. Если после ***нескольких*** запусков она продолжает выдавать ошибку, то следует проверить конфигурацию службы времени (особенно это важно в домене)!

Команда `w32tm /monitor` (или `w32tm /monitor /ipprotocol:4`) позволяет увидеть, какие серверы времени используются в указанном домене (если домен не задается, то проверяется текущий домен) или на компьютерах домена, перечисленных явно; также отображаются отклонения показаний часов.

Отключение синхронизации

Для того чтобы синхронизация системных часов вообще не осуществлялась, выполните команду `w32tm /config /syncfromflags:no /update` (при этом параметр `Parameters\Type` изменит значение на `NoSync`). Можно вообще запретить 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.

Язык сценариев и командный процессор 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.

> ***Примечание***
>
> Для выполнения сценариев, написанных на языках VBScript и JScript, в системах Windows Server 2008 (включая Windows Server Core и Hyper-V Server) имеется традиционный компонент — *Сервер сценариев Windows* (Windows Script Host, WSH) Текущая версия WSH — 5.7.

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

[1] Неологизм, к которому придется привыкать (по аналогии с апплетами (applet), сервлетами (servlet)).

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.

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

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) 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 по имени из меню **Run** (Выполнить), то в заголовке окна появляется специальный значок (рис. 2.48) и можно видеть полный путь к исполняемому файлу.

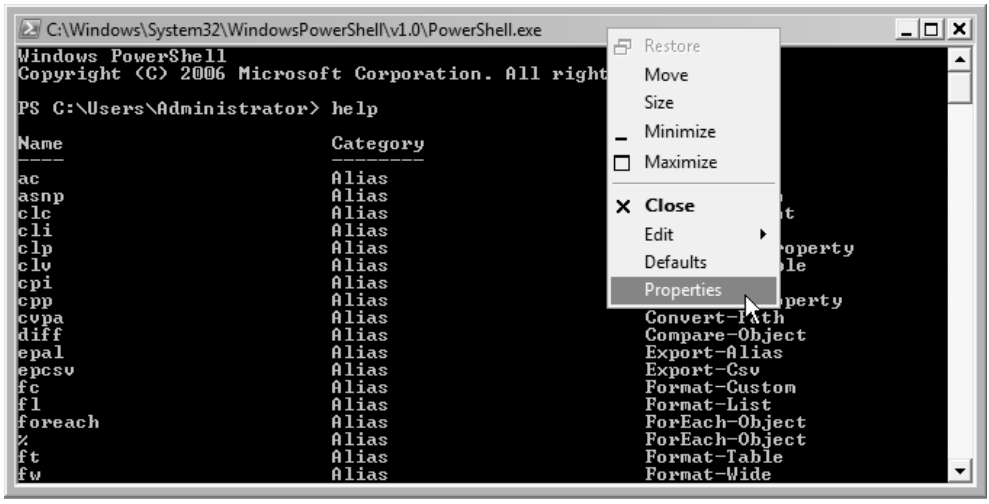


Рис. 2.48. Окно командного процессора PowerShell

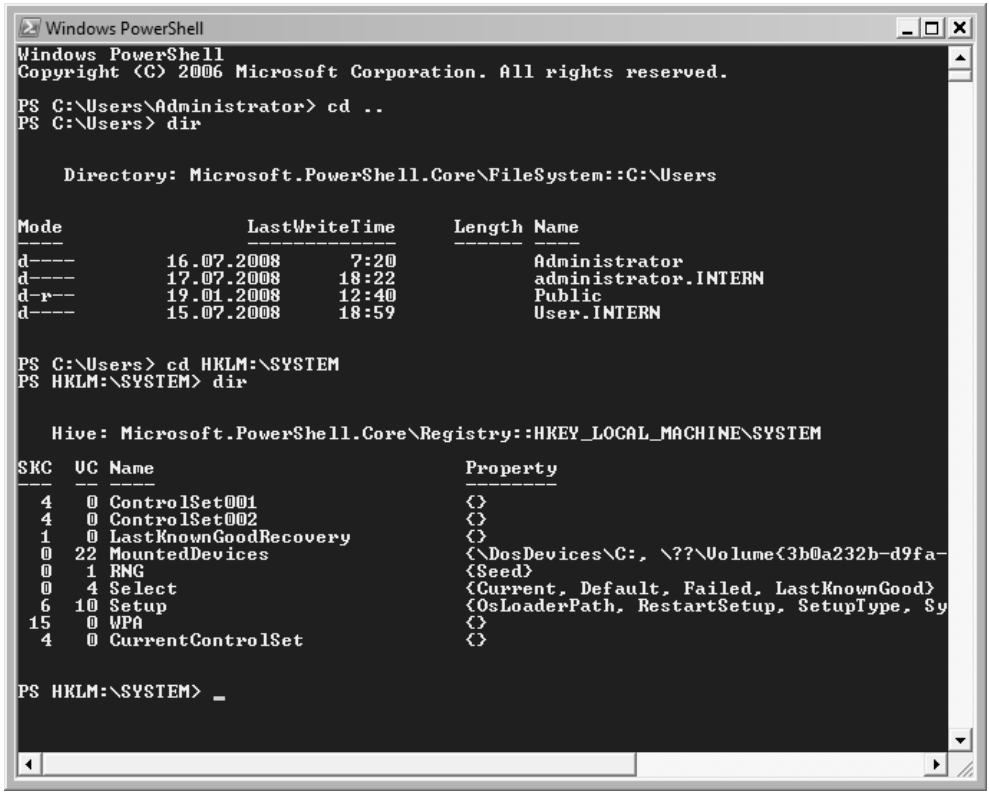


Рис. 2.49. Пример навигации по папкам файловой системы и разделам системного реестра

Если же воспользоваться возможностями меню **Start** (Пуск), то в заголовке окна будет указано название программы, а фон в окне становится синим (см. рис. 2.49).

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. 2.49, 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

Рассмотрим процедуру выполнения сценария, написанного на языке PowerShell. Она не совсем очевидная, поэтому заслуживает внимания. Процесс проверки готовности командного процессора к работе содержит несколько несложных шагов и выглядит 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 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 3

Мониторинг системы и приложений

В составе систем Windows Server 2008 появились новые средства, предназначенные для анализа событий, происходящих в системе, а также для оптимизации и мониторинга рабочих параметров системных служб и прикладных программ. 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 2)*.

Средства мониторинга в Windows Server 2008

Некоторые средства мониторинга, имеющиеся в Windows Server 2008, традиционны для систем Windows, однако кардинально переработаны по сравнению с предыдущими версиями; помимо них появились и совершенно новые инструменты. Ниже перечислены существующие программы и указаны области их применения.

- Традиционная утилита *Task Manager* (Диспетчер задач) используется для просмотра рабочих параметров системы и прикладных программ (это включает в себя загрузку процессора, степень использования оперативной и виртуальной памяти, коэффициент занятости сети и т. д.).
- С помощью привычной оснастки **Event Viewer** (Просмотр событий) можно анализировать события, регистрируемые приложениями, службами и самой

системой. Интерфейс оснастки кардинально переработан, и в ней имеется много дополнительных возможностей.

Журналы событий для ролей сервера и связанных с ними служб также можно просматривать в окне оснастки **Server Manager** (Диспетчер сервера).

- 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) обеспечивает возможность оценки надежности работы системы на протяжении некоторого интервала времени и позволяет определять "слабые места" системы;
  - компонент *Data Collector Sets* (Группы сборщиков данных) позволяет создавать наборы логически связанных счетчиков производительности, 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).
- Средство *Software Exporer* (Проводник программного обеспечения), входящее в состав программы Windows Defender (Защитник Windows), предоставляет развернутую информацию о программах и процессах, запускающихся при старте системы, активных в текущий момент и взаимодействующих с сетью.

Также следует напомнить еще о двух инструментах, 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, Msinfo32.exe) позволяет получить исчерпывающую информацию о каждом аппаратном и программном компоненте системы, включая описание, параметры и т. п.

---

[1] В системах Windows XP/Windows Server 2003 этот компонент называется *System Monitor*.

Внимание!

Из всех перечисленных выше средств в составе Windows Server Core и Hyper-V Server имеются только утилиты Task Manager (Диспетчер задач), SystemInfo.exe и System Information (Сведения о системе, Msinfo32.exe). Тем не менее, мониторинг некоторых рабочих параметров систем можно выполнять удаленно, с компьютера администратора — например, это позволяют оснастка **Event Viewer** (Просмотр событий) или компонент Performance Monitor (Системный монитор).

Диспетчер задач (Task Manager)

Диспетчер задач (Task Manager) традиционно используется в системах Windows для мониторинга "оперативного состояния" локальной 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"*). В системах Windows Server 2008 диспетчер задач в целом не изменился по сравнению с предыдущими версиями Windows, однако он имеет новые вспомогательные функции, на которые мы в первую очередь и обратим внимание. Теперь окно диспетчера содержит шесть вкладок/индикаторов, вид и назначение которых подробно описываются далее.

Запуск диспетчера задач

Существуют различные способы запуска диспетчера — первый из перечисленных ниже подходов возможен только в полных версиях Windows Server 2008, а остальные три работают во всех версиях, включая Windows Server Core и Hyper-V Server.

- 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).
- Непосредственно ввести команду `taskmgr` в окне **Run** (Выполнить), в поле поиска меню **Start** (Пуск) или в окне командной строки.

Если в полных версиях Windows Server 2008 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 зна-

чок, 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).

Просмотр состояния прикладных программ

На вкладке **Applications** (Приложения) (рис. 3.1) 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.

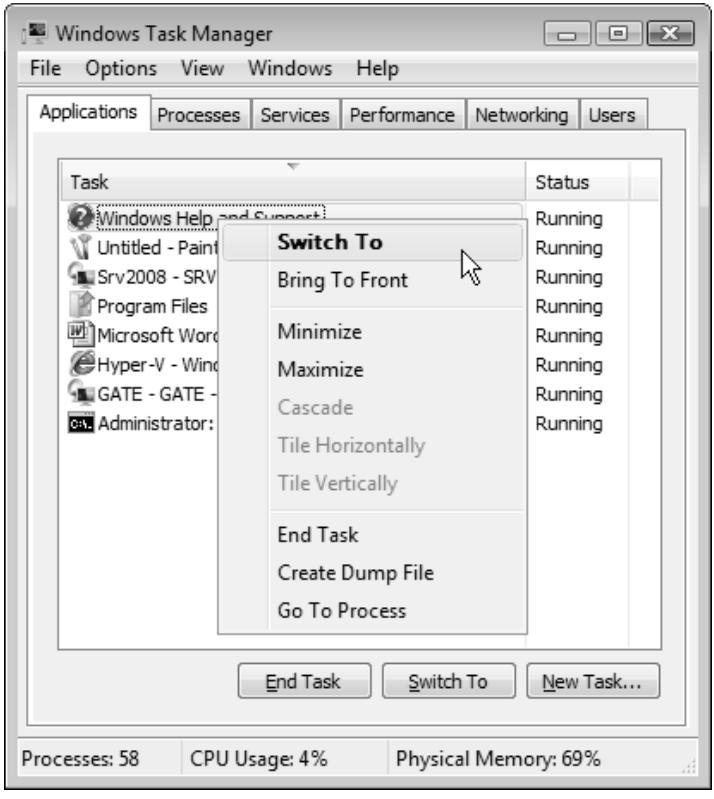


Рис. 3.1. Просмотр состояния прикладных программ, запущенных в системе

С помощью новой команды **Go To Process** (Перейти к процессу) можно перейти на вкладку **Processes** (Процессы), где автоматически будет выделен процесс, соответст-

вующий 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. 3.2). 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, поскольку 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.

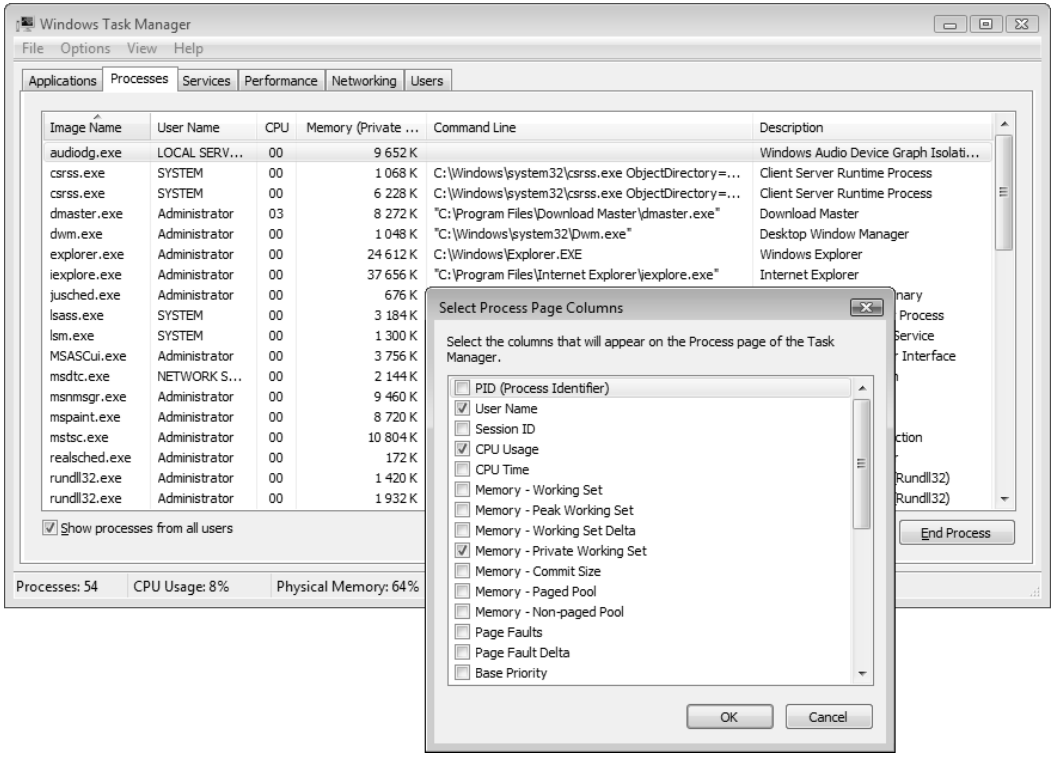


Рис. 3.2. Список процессов, запущенных в системе, и окно выбора отображаемых параметров

В контекстном меню любого процесса 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).

При работе в окне командной строки можно использовать утилиты `qprocess` и `tasklist`. (Это относится ко всем версиям, включая Windows Server Core и Hyper-V Server.) Информацию о параметрах можно получить во встроенной справке утилит, запустив их с ключом `/?`. *

Например, с помощью команды `tasklist /SVC` 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). Часто такая необходимость возникает для образов файла svchost.exe, который используется для запуска множества служб. Аналогичную информацию можно получить и с помощью программы Software Exporer (Проводник программного обеспечения) *(см. далее)*.

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. 3.2) 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. 3.1 приведено краткое описание показателей для вкладки **Processes** (Процессы) диспетчера задач.

Таблица 3.1. *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 3.1 *(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) в контекстном меню выбранного процесса)
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
I/O Writes (Число записей)	Число операций ввода/вывода, сгенерированных процессом записи, включая ввод/вывод файлов, сети и устройств

Таблица 3.1 *(окончание)*

Столбец	Описание
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

Слежение за работой системных служб

На вкладке **Services** (Службы) (рис. 3.3) 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 выбранную службу можно запустить или остановить.

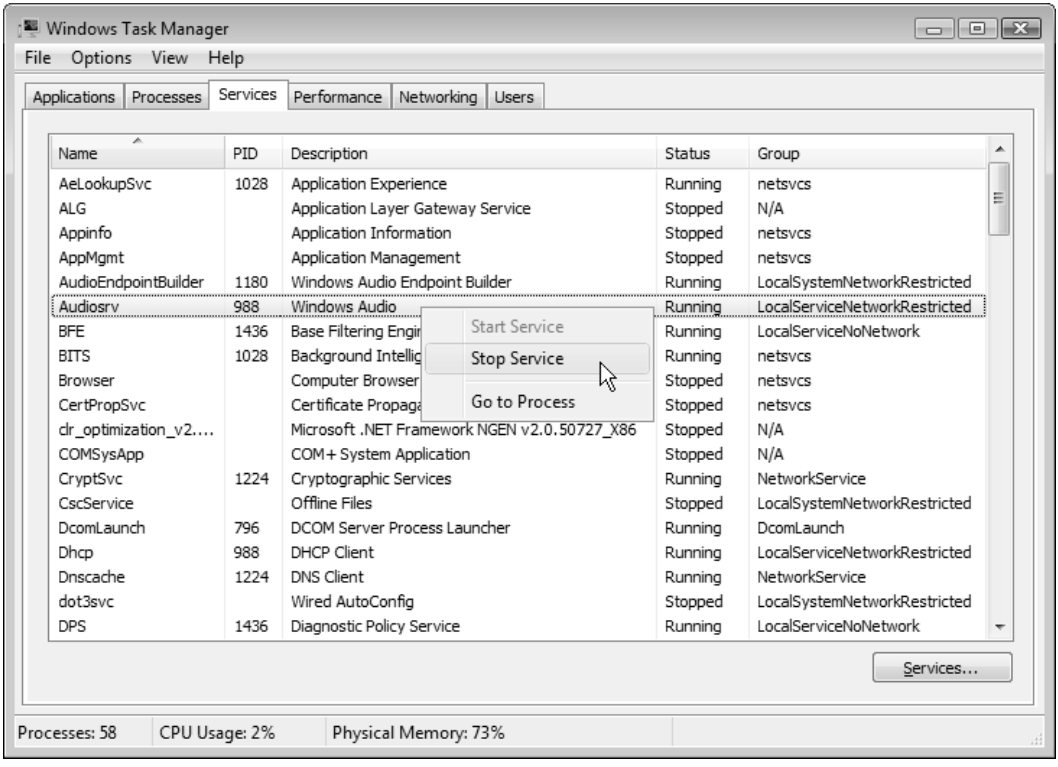


Рис. 3.3. Список системных служб и их состояние

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 (процессоров и памяти) традиционно используется вкладка **Performance** (Быстродействие) (рис. 3.4), имеющаяся в окне диспетчера задач.

На рис. 3.4 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. 3.17—3.20). Монитор ресурсов подробнее будет описан позже, в составе оснастки **Reliability and Performance Monitor** (Монитор производительности и стабильности).

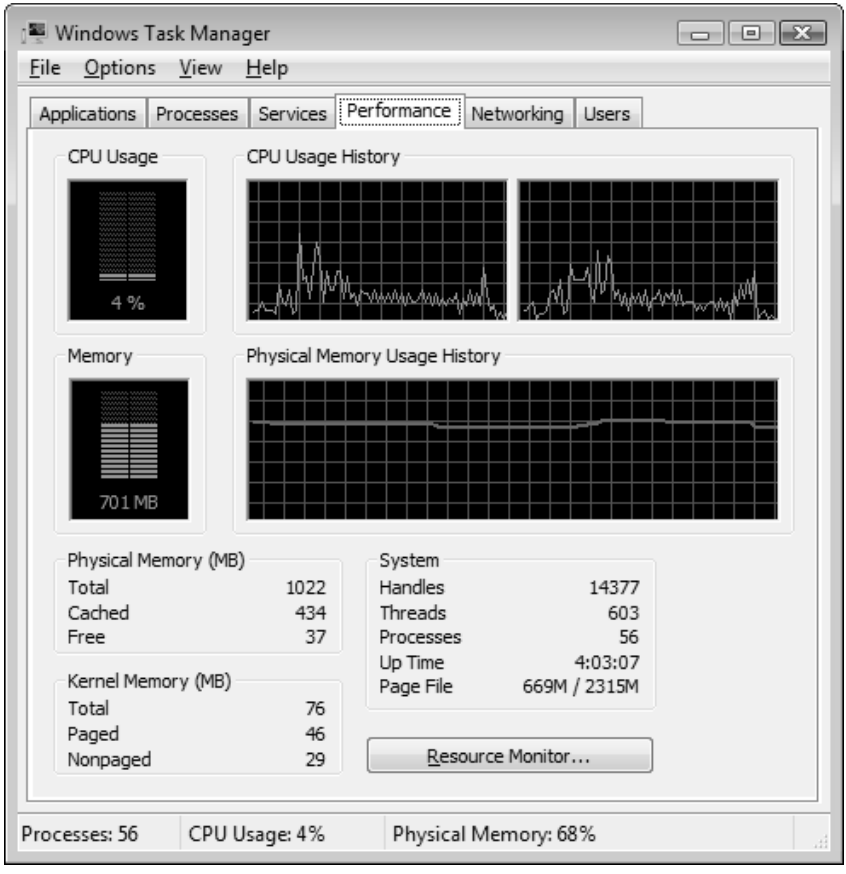


Рис. 3.4. Диаграммы занятости процессоров и памяти

Мониторинг сети

На вкладке **Networking** (Сеть) (рис. 3.5) 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.

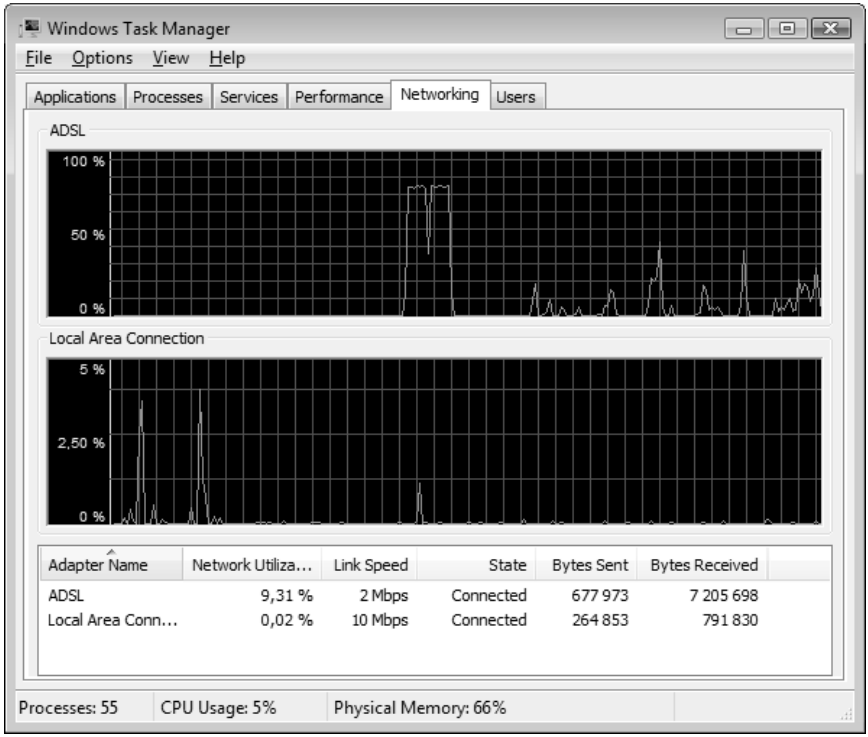


Рис. 3.5. Отображение загруженности сетевых подключений

В подменю **View** | **Network Adapter History** (Вид | Журнал сетевого адаптера) указывается тип отображаемой на графике информации: по умолчанию на графике видно только *общее* количество переданных (принятых и посланных) байтов, а кроме этого отдельно можно видеть число полученных (**Bytes Received** (Получено байт)) и/или отправленных байтов (**Bytes Sent** (Отправлено байт)).

С помощью команды **View** | **Select Columns** (Вид | Выбрать столбцы) можно перейти в окно отображаемых столбцов и выбрать, к примеру, вывод в таблице общего числа полученных (Bytes Received) и/или отправленных байтов (Bytes Sent) для каждого сетевого адаптера (см. рис. 3.5). При этом если установить флажок **Options** | **Show Cumulative Data** (Параметры | Отображать накапливаемые дан-

ные), то будут учитываться не только те данные, которые 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 и отсчет начинается с начала).

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. 3.6 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. 3.6 — 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.

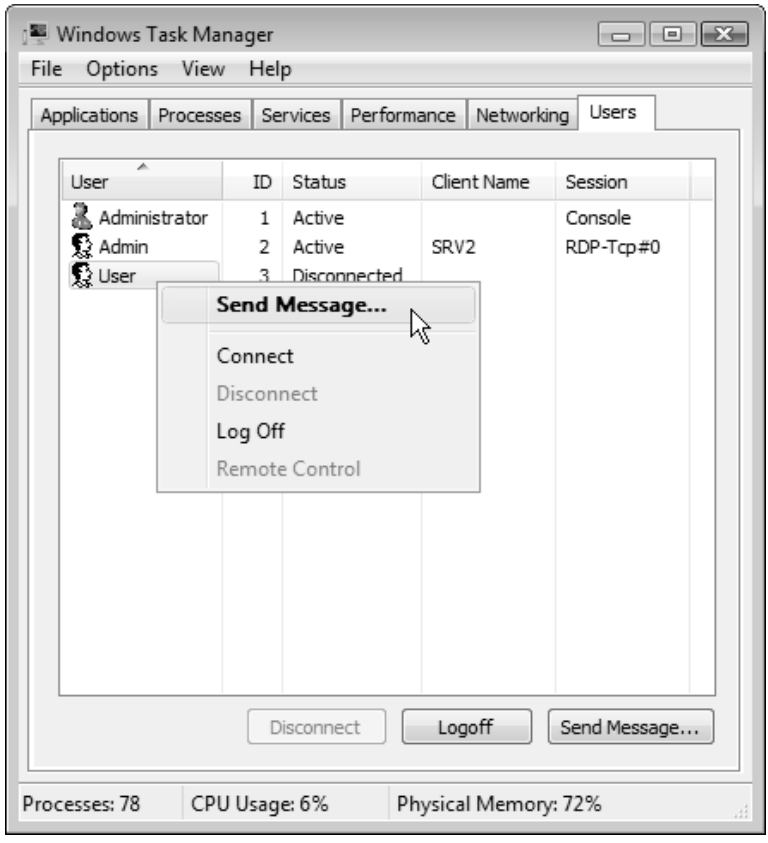


Рис. 3.6. Имена пользователей, зарегистрированных на компьютере

Мониторинг программ и сервисов — программа Software Exporer

В полных системах Windows Server 2008 имеется программа *Windows Defender* (Защитник Windows), позволяющая защитить компьютер от разнообразных шпионских (spyware) программ, а также вредоносных приложений, которые могут нарушить работоспособность и безопасность системы. Ядро программы реализовано как системный сервис (имя WinDefend), и управлять им можно с помощью оснастки **Services** (Службы).

В составе программы Windows Defender (Защитник Windows) имеется средство *Software Exporer* (Проводник программного обеспечения), которое позволяет полу-

чать 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).)

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. 3.7). Список приложений разбит по фирмам-производителям, благодаря чему ориентироваться в программах очень удобно. Непосредственно из этого окна можно сразу прекращать подозрительные задачи.

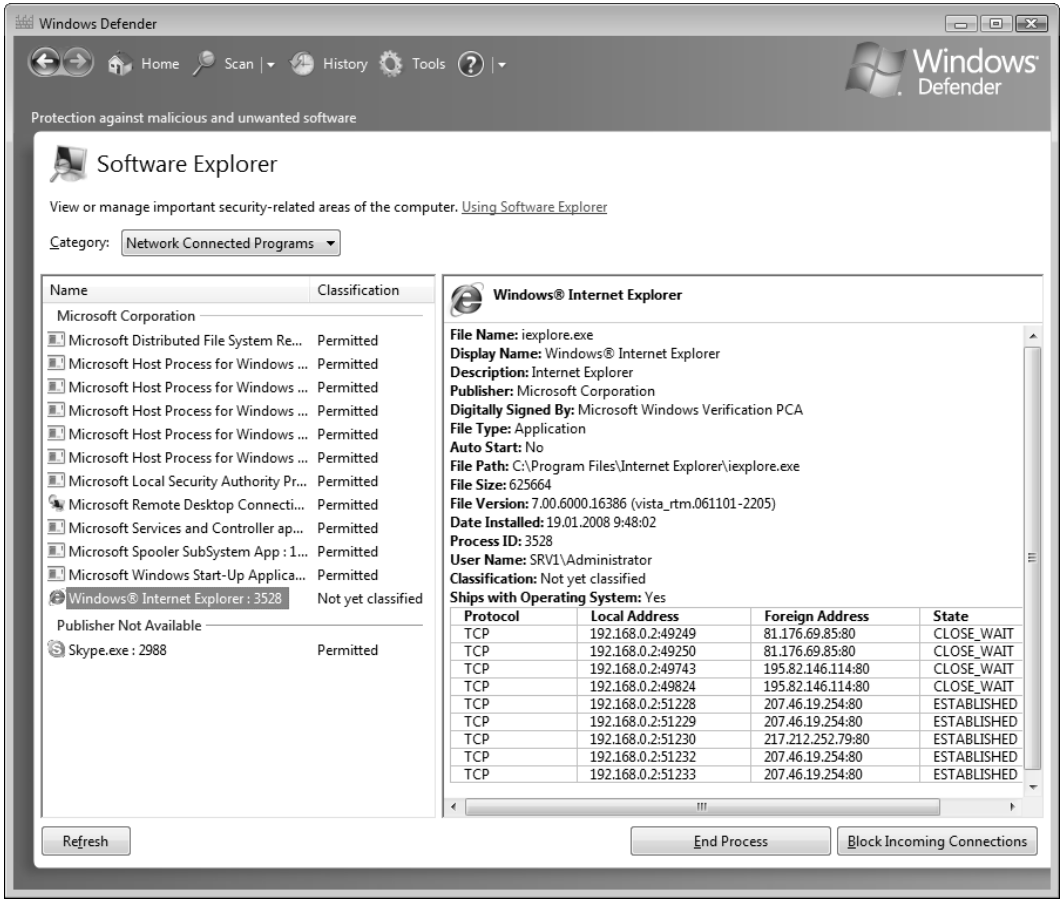


Рис. 3.7. Мониторинг процессов, обращающихся к сети

[1] В том случае, если используется новый вид панели управления с делением по категориям.

Не менее интересные режимы — просмотр программ, загружаемых при запуске системы (категория Startup Programs), и список программ, выполняющихся в данный момент (категория Currently Running Programs).

Просмотр событий, регистрируемых системой, службами и приложениями

В системах Windows Server 2008 события системы, служб и приложений четко классифицированы, и их можно просматривать в индивидуальных журналах, число которых приближается к сотне. Для просмотра системных журналов на локальном или удаленном компьютере традиционно используется оснастка **Event Viewer** (Просмотр событий), которая в системах Windows Server 2008 кардинально переработана и содержит 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.

> ***Примечание***
>
> Основной возможностью просмотра событий на компьютерах, где используется Windows Server Core или Hyper-V Server, является оснастка **Event Viewer** (Просмотр событий), подключаемая с удаленного компьютера, работающего под управлением Windows Vista или полной версии Windows Server 2008. Также можно использовать подписки на события *(см. далее)* и утилиту командной строки Wevtutil.exe. Например, команда `wevtutil qe Setup /f:text` позволяет посмотреть в текстовом режиме все события, содержащиеся в журнале Setup (Настройка).

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. 3.8.

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.

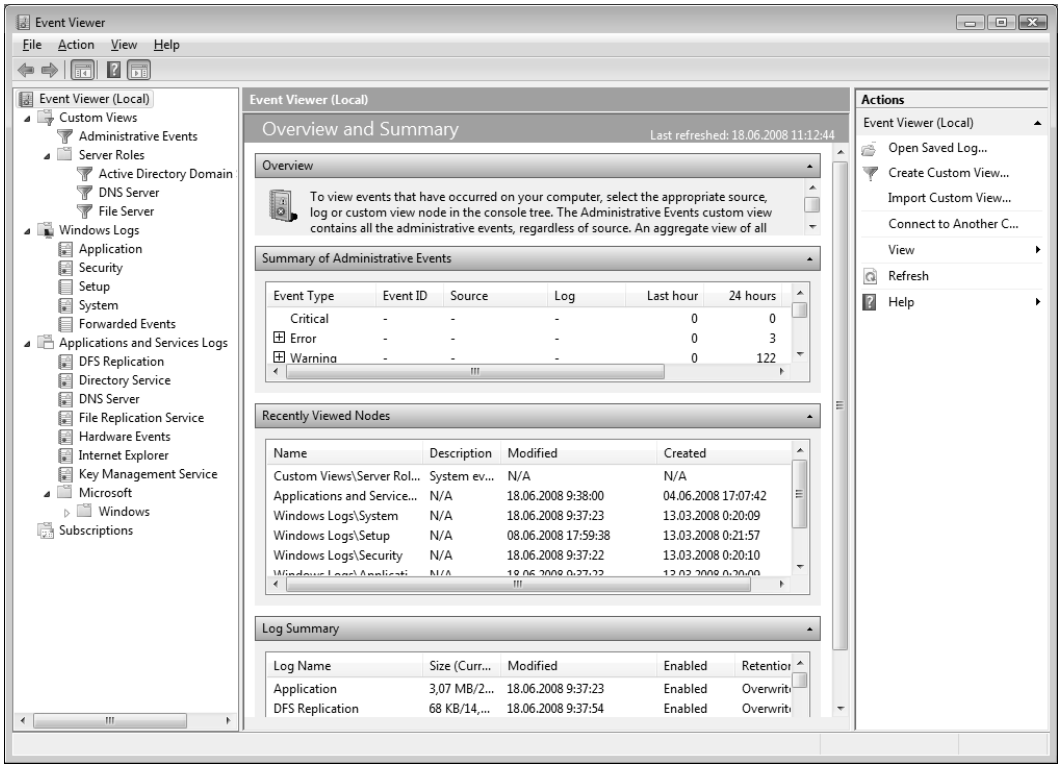


Рис. 3.8. Основное окно оснастки **Event Viewer**

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. Здесь же находится команда подключения к удаленному компьютеру (при этом можно непосредственно указать имя и пароль любой учетной записи). Данную 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. Помимо традиционных системных журналов Windows имеются два новых журнала:

- **Setup** (Настройка) — используется для сообщений, касающихся установки и обновлений системы, ее ролей, компонентов и приложений;

- **Forwarded Events** (Пересланные события) — события, полученные по запросу с других компьютеров.

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, в которые заносятся события конкретных компонентов, служб и подсистем, в первую очередь — детальная информация об ошибках в их работе.

Просмотр журналов и параметров событий

В системах Windows Server 2008 оснастка **Event Viewer** (Просмотр событий) позволяет просматривать журналы и сразу видеть все данные о выбранном событии в окне, располагающемся ниже списка событий (рис. 3.9). 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.).

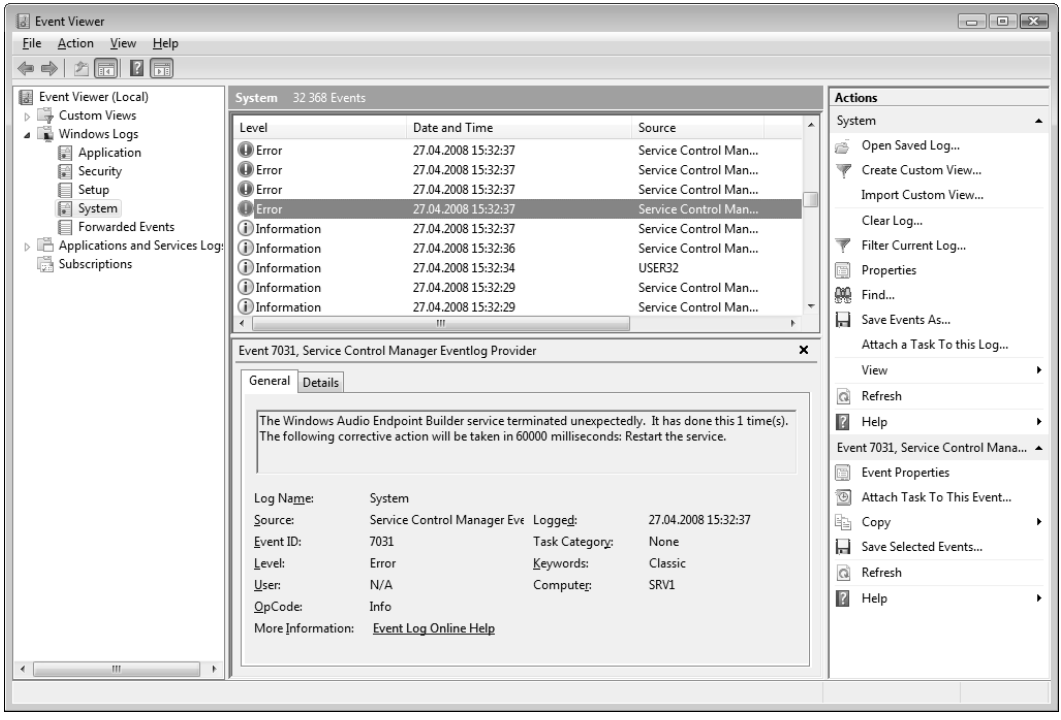


Рис. 3.9. Просмотр событий в выбранном журнале

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. 3.10) 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.

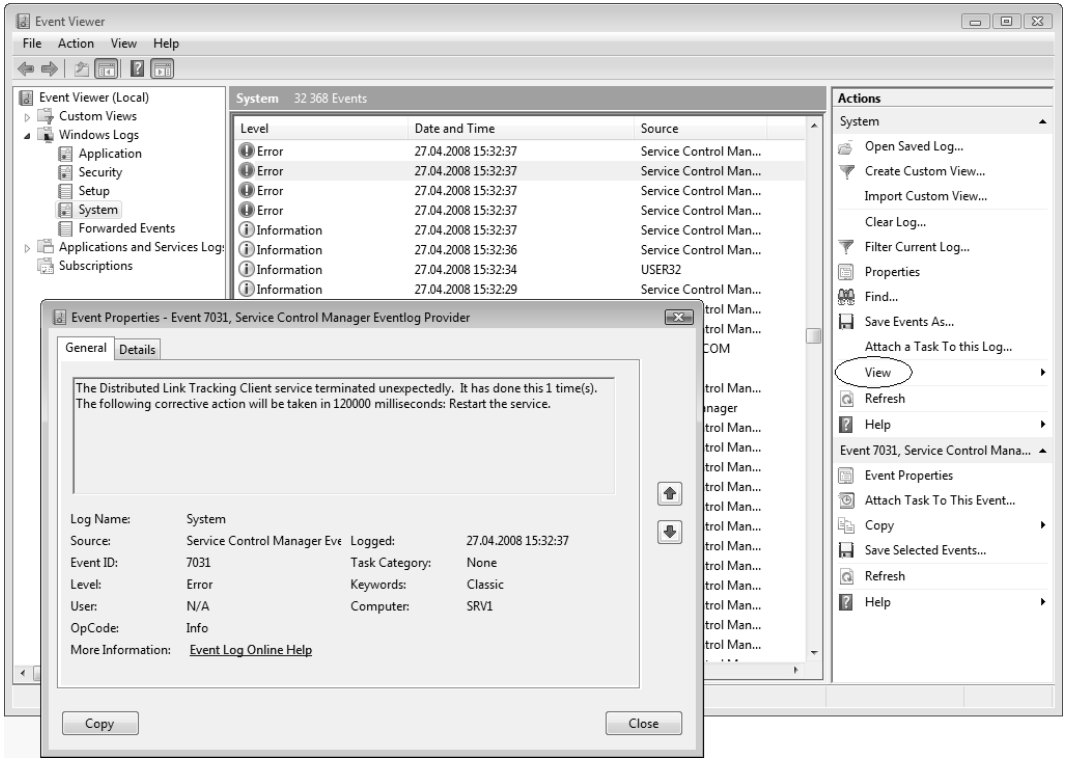


Рис. 3.10. Новый дизайн оснастки позволяет выбирать способ просмотра списка событий и информации о конкретном событии

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. 3.11 в качестве примера показано окно оснастки для роли File Services (Файловые служ-

бы). 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.

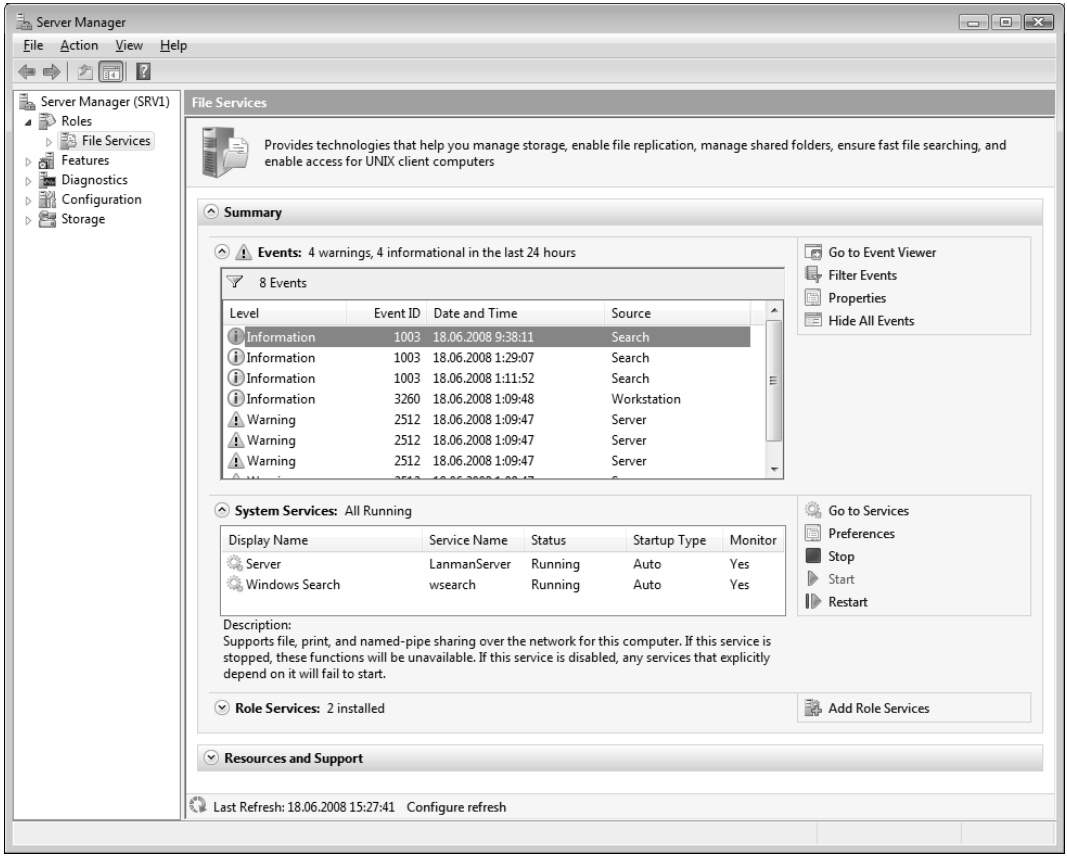


Рис. 3.11. Просмотр событий для выбранной роли сервера в окне оснастки **Server Manager**

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 по сути похожи, 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.

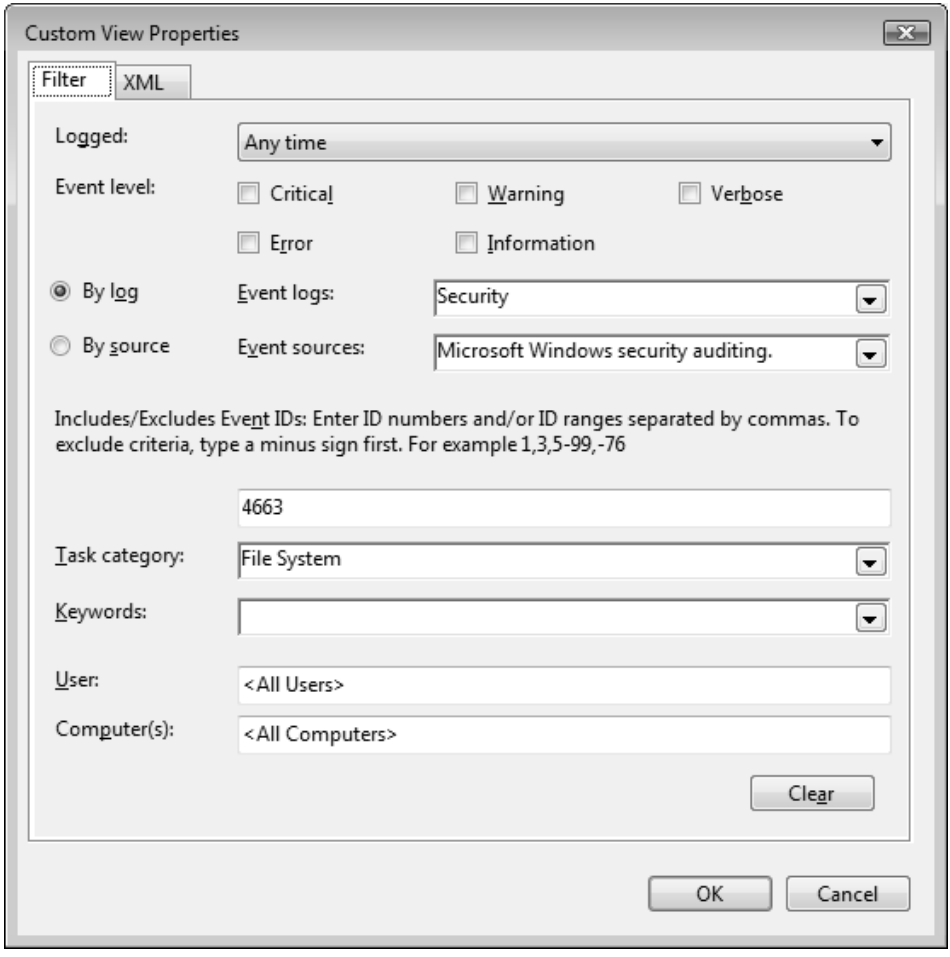


Рис. 3.12. Пример фильтра настраиваемого представления журнала

Типичной ситуацией, когда использование настраиваемого представления для журнала Security (Безопасность) просто необходимо, является задача аудита досту-

па 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. 3.12 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 по умолчанию сохраняются в папке **Custom Views** (Настраиваемые представления) (см. рис. 3.8). Их название и другие характеристики, включая параметры фильтра, можно менять в любой момент в окне свойств. 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,

это удобно в доменной среде со многими компьютерами (компьютеры, входящие в рабочую группу, настраивать сложнее).

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 management.
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. 3.8) и в контекстном меню или на панели **Actions** (Действия) выполнить команду **Create Subscription** (Создать подписку), то откроется окно свойств новой подписки (рис. 3.13). Название подписки может быть произвольным, но желательно ин-

формативным. Все полученные события по умолчанию заносятся в журнал Forwarded Events (Пересланные события).

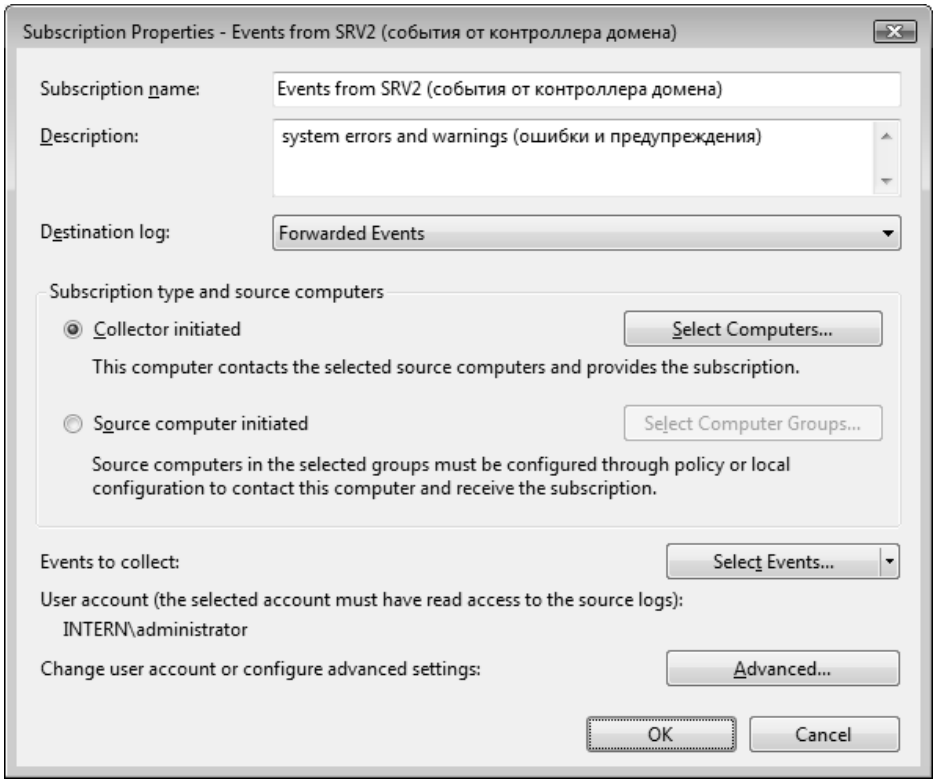


Рис. 3.13. Окно свойств подписки на события

Кнопка **Select Computers** (Выбрать компьютеры) позволяет выбрать компьютеры, с которых будут собираться события. В специальном окне (рис. 3.14) 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)*.

Кнопка **Select Events** (Выбрать события) в окне свойств подписки позволяет перейти к настройке фильтра событий (см. рис. 3.12) 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. 3.15), и наличие зеленого флажка в левой части свидетельствует об успешном окончании операции и активности подписки. Для управления подписками используются команды в контекстном меню, показанные на рисунке.

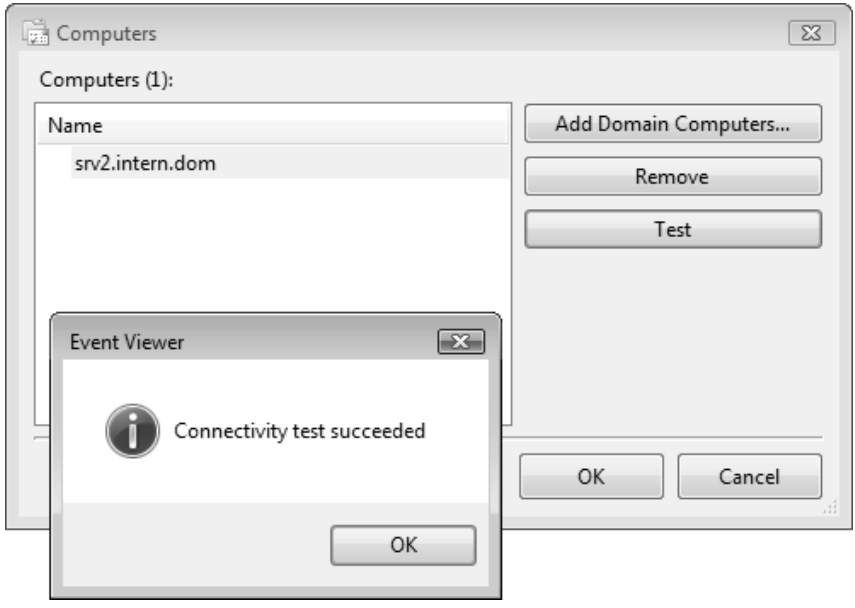


Рис. 3.14. Список компьютеров,
с которых собираются системные события

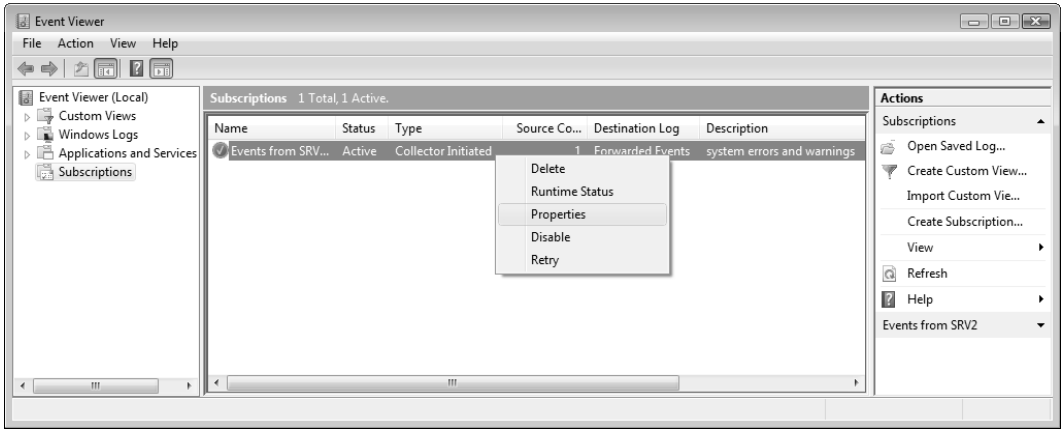


Рис. 3.15. Папка подписок и команды управления подписками

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.

Мониторинг параметров и стабильности работы системы

Оснастка **Reliability and Performance Monitor** (Монитор производительности и стабильности, perfmon.msc[1]) позиционируется как аналог инструмента Performance (Производительность), существующего в составе 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 Server 2003.

Возможности инструментов в системах 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).

> ***Внимание!***
>
> Оснастку **Reliability and Performance Monitor** (Монитор производительности и стабильности) можно подключать к удаленным компьютерам, однако не все ее компоненты будут работать даже на полных версиях Windows Server 2008. Например, компонент Resource Monitor (Монитор ресурсов) в этом случае не отображается.

Оснастка **Reliability and Performance Monitor** (Монитор производительности и стабильности) представляет собой мощное средство индикации количественных показателей работы системы, отображающихся в реальном времени (рис. 3.16). С ее помощью администратор может собирать необходимые данные в журналы и определять пороговые значения параметров, в случае превышения которых будут генерироваться предупреждения или запускаться определенные задачи, а также создавать отчеты и анализировать работу системы на протяжении некоторого от-

[1] Данную оснастку можно запускать из командной строки по имени, без расширения.

резка времени. Многие показания представлены в виде графиков, что облегчает их восприятие и анализ.

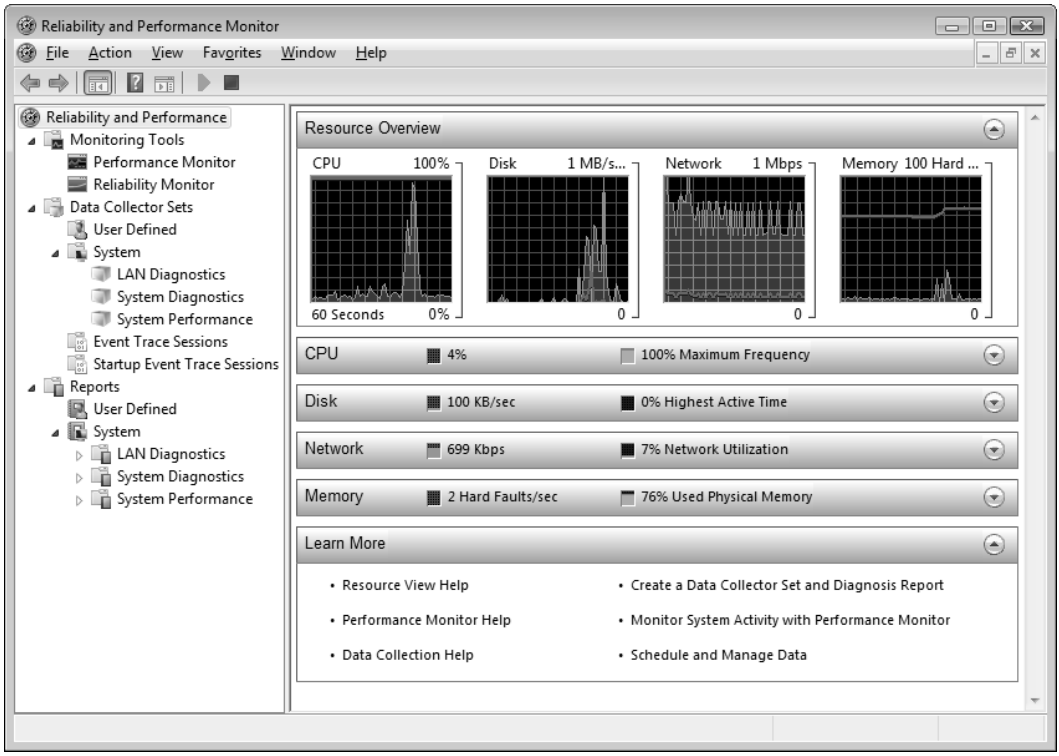


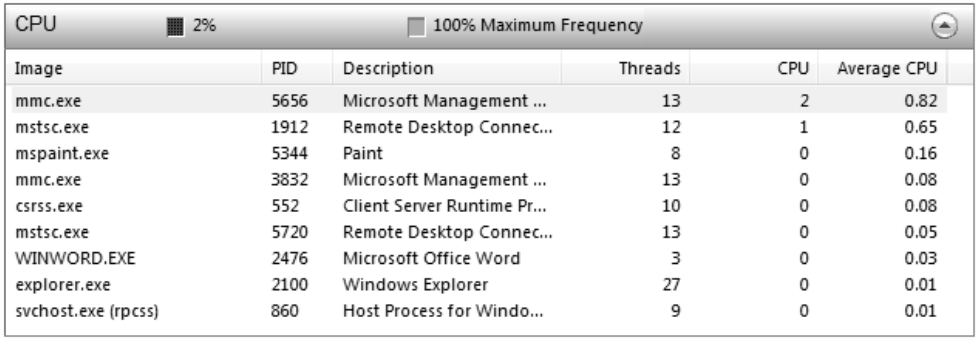
Рис. 3.16. Основной вид оснастки **Reliability and Performance Monitor**

На рис. 3.16 центральное место в окне занимает компонент Resource Monitor (Монитор ресурсов). 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 запускать автономно — для этого следует нажать одноименную кнопку в окне диспетчера задач (см. рис. 3.4) или ввести `perfmon /res` в окне командной строки или в поле поиска меню **Start** (Пуск).

В окне монитора имеются панели графических индикаторов для четырех основных компонентов системы: центрального процессора, дисковой системы, сетевых адаптеров и памяти. Для процессора отображаются список активных процессов (включая их описания) и время занятости процессора (рис. 3.17).

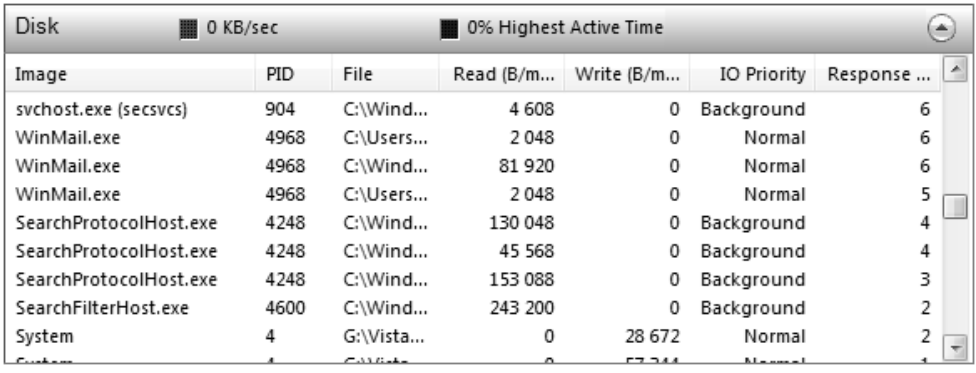


CPU 2% 100% Maximum Frequency

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. 3.17. Мониторинг загрузки центрального процессора

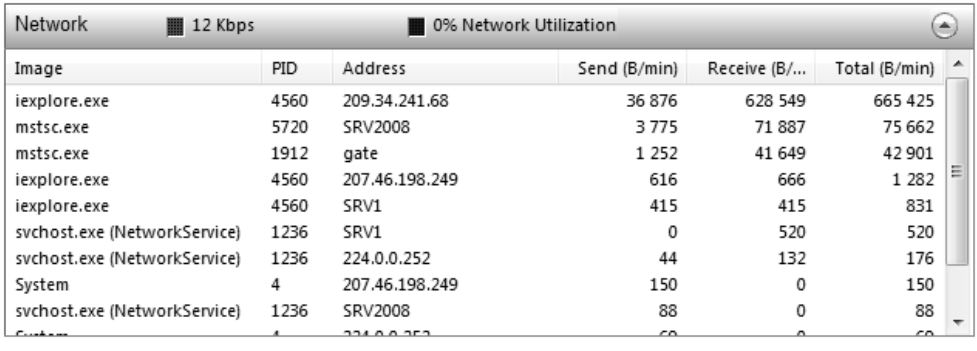
Для жесткого диска на панели можно видеть названия и идентификаторы процессов, работающих с диском; имя файла, к которому процесс обращается; количество переданной информации (рис. 3.18).



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. 3.18. 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. 3.19. Мониторинг сетевых операций

Для сети отображаются названия и идентификаторы процессов; локальные и внешние IP-адреса, по которым выполняются обращения, а также генерируемый трафик (рис. 3.19).

На панели индикаторов оперативной памяти (рис. 3.20) 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).

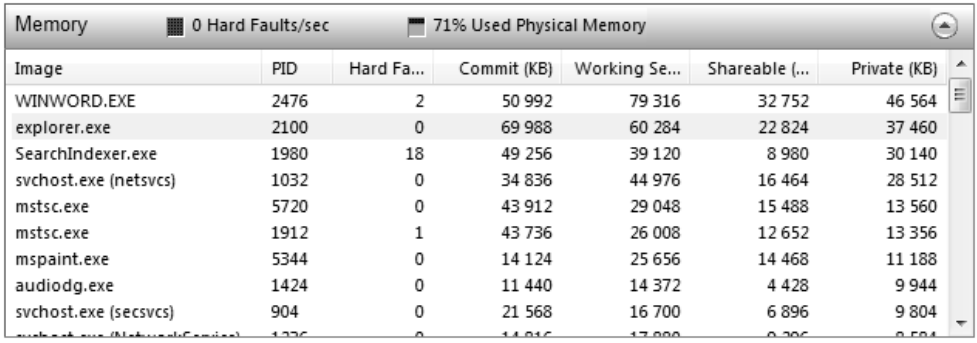


Image	PID	Hard Fa...	Commit (KB)	Working Se...	Shareable (...	Private (KB)
WINWORD.EXE	2476	2	50 992	79 316	32 752	46 564
explorer.exe	2100	0	69 988	60 284	22 824	37 460
SearchIndexer.exe	1980	18	49 256	39 120	8 980	30 140
svchost.exe (netsvcs)	1032	0	34 836	44 976	16 464	28 512
mstsc.exe	5720	0	43 912	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. 3.20. Мониторинг занятости оперативной памяти

Системный монитор (Performance Monitor)

Компонент Performance Monitor (Системный монитор) позволяет следить за параметрами, определяющими производительность локального компьютера или удаленных компьютеров, работающих 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 (Группы 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 десятками (их более 80).

Каждый объект производительности имеет 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. 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. 3.21).

Чаще всего для оценки производительности сервера используются следующие объекты:

- Memory (Память)
- Network Interface (Сетевой интерфейс)
- Paging File (Файл подкачки)
- PhysicalDisk (Физический диск)
- Process (Процесс)
- Processor (Процессор)
- Server (Сервер)
- System (Система)

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.

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 клавиши <Ctrl>+<I>.
2. В открывшемся окне (рис. 3.21) 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**.

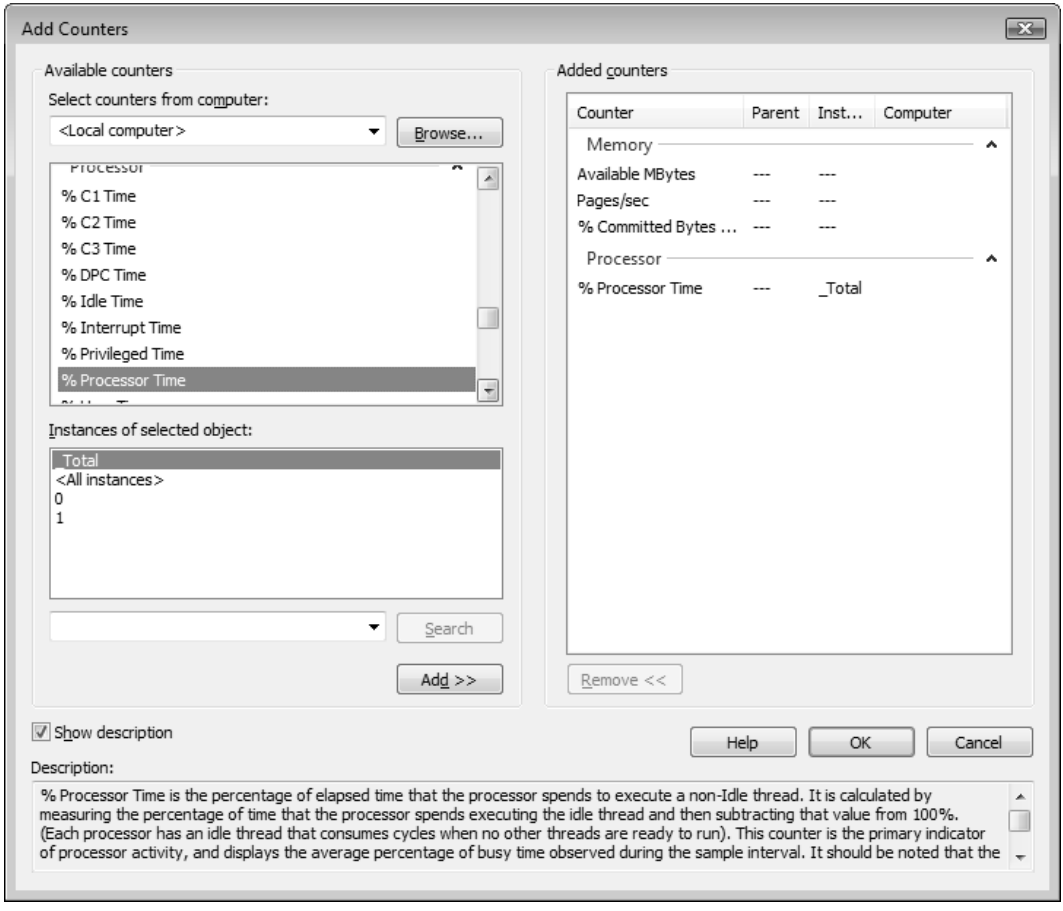


Рис. 3.21. Диалоговое окно для выбора объектов, счетчиков и экземпляров объектов для мониторинга

На рис. 3.22 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 название счетчика, значение и показания часов в выбранной точке

(рис. 3.23). Эта информация полезна при анализе графиков, особенно если их много на экране.

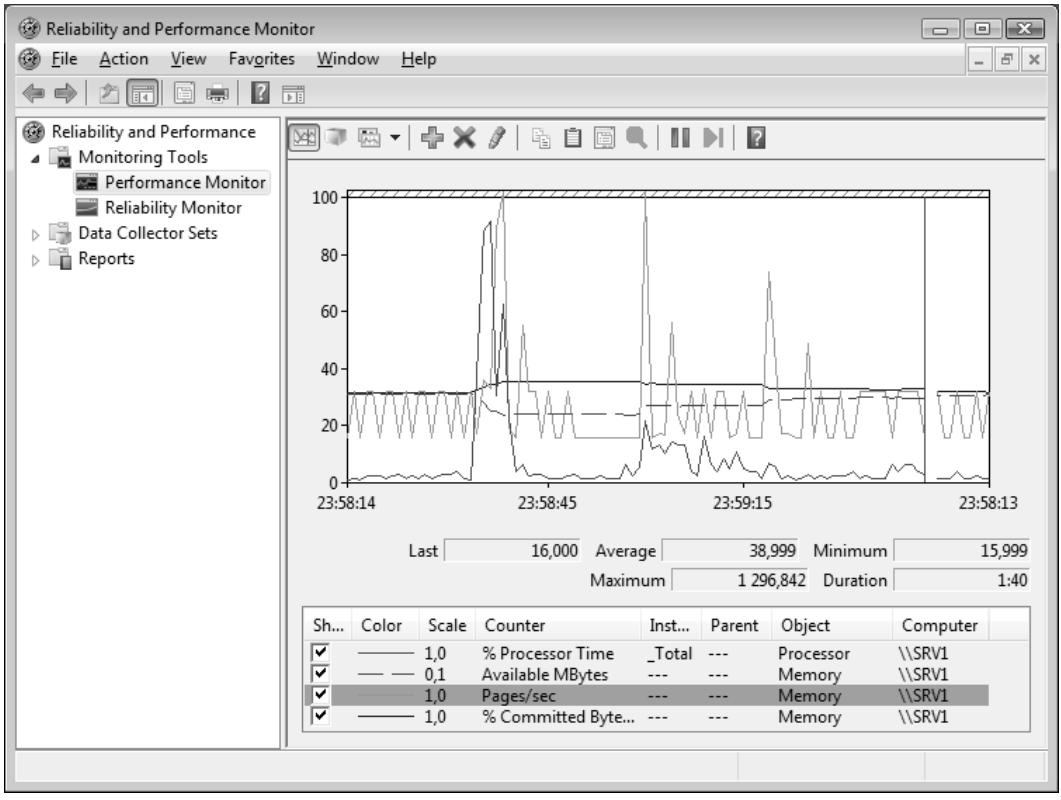


Рис. 3.22. Окно компонента Performance Monitor с активизированными счетчиками

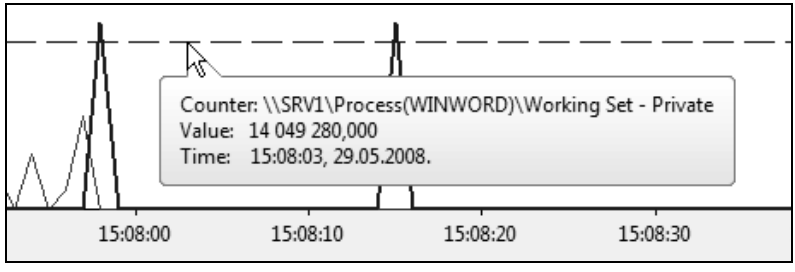


Рис. 3.23. Получение информации о графике, выбранном в окне системного монитора

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 (Группы сборщиков данных) *(см. далее)*.

Мониторинг отдельных процессов и приложений

Важной задачей мониторинга серверов является сбор информации о степени использования ресурсов для системных процессов или прикладных программ, выполняющихся на компьютере.

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.

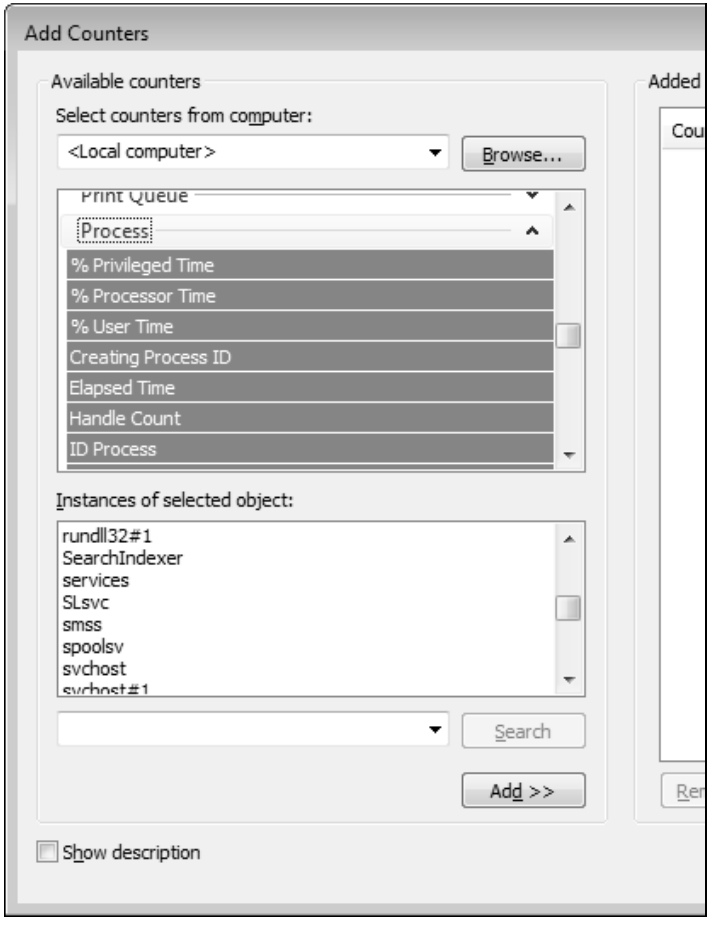


Рис. 3.24. Выбор счетчиков для системных процессов и прикладных программ

Для решения подобных задач используется объект производительности Process (Процесс). Если его выбрать в перечне имеющихся счетчиков (рис. 3.24), то можно видеть, что в списке экземпляров данного объекта присутствуют имена всех про-

цессов (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. 3.22 выбрана опция **Line** (Строка)).

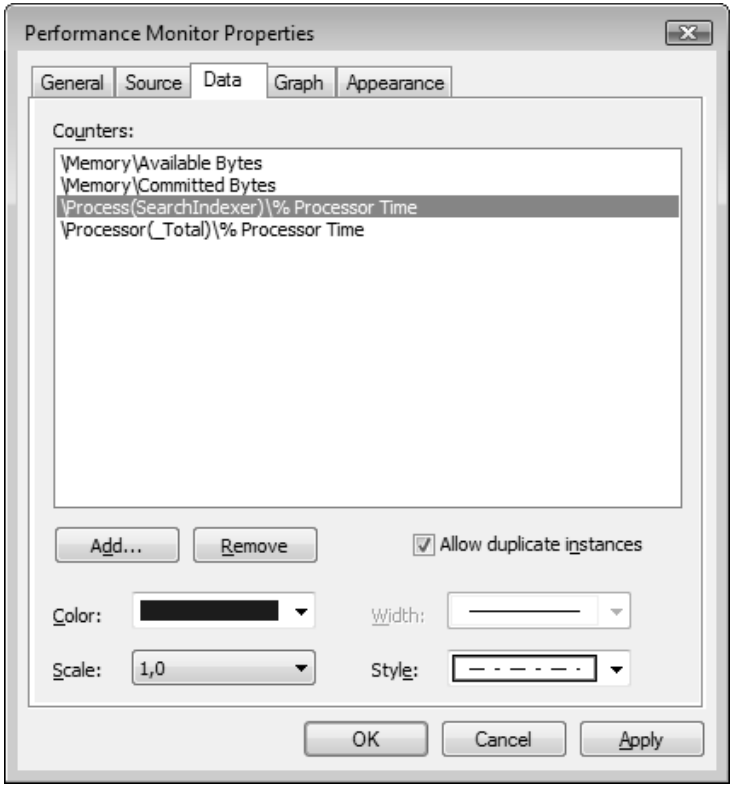


Рис. 3.25. Окно выбора вида отображаемых графиков и гистограмм

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, —

[1] Вернее было бы сказать — линия, график (что много ближе по смыслу).

в этом случае в открывающемся окне будет выделен именно этот счетчик и можно менять параметры представления соответствующего графика для лучшей наглядности при одновременном отображении нескольких графиков.

В окне свойств системного монитора (рис. 3.25) 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 использовать 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**)).

Оснастка *Reliability Monitor* (Монитор стабильности системы)

В системах Windows Vista/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 может работать и с удаленными компьютерами, если на них установлены полные версии Windows Server 2008.

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. 3.26):

- *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.

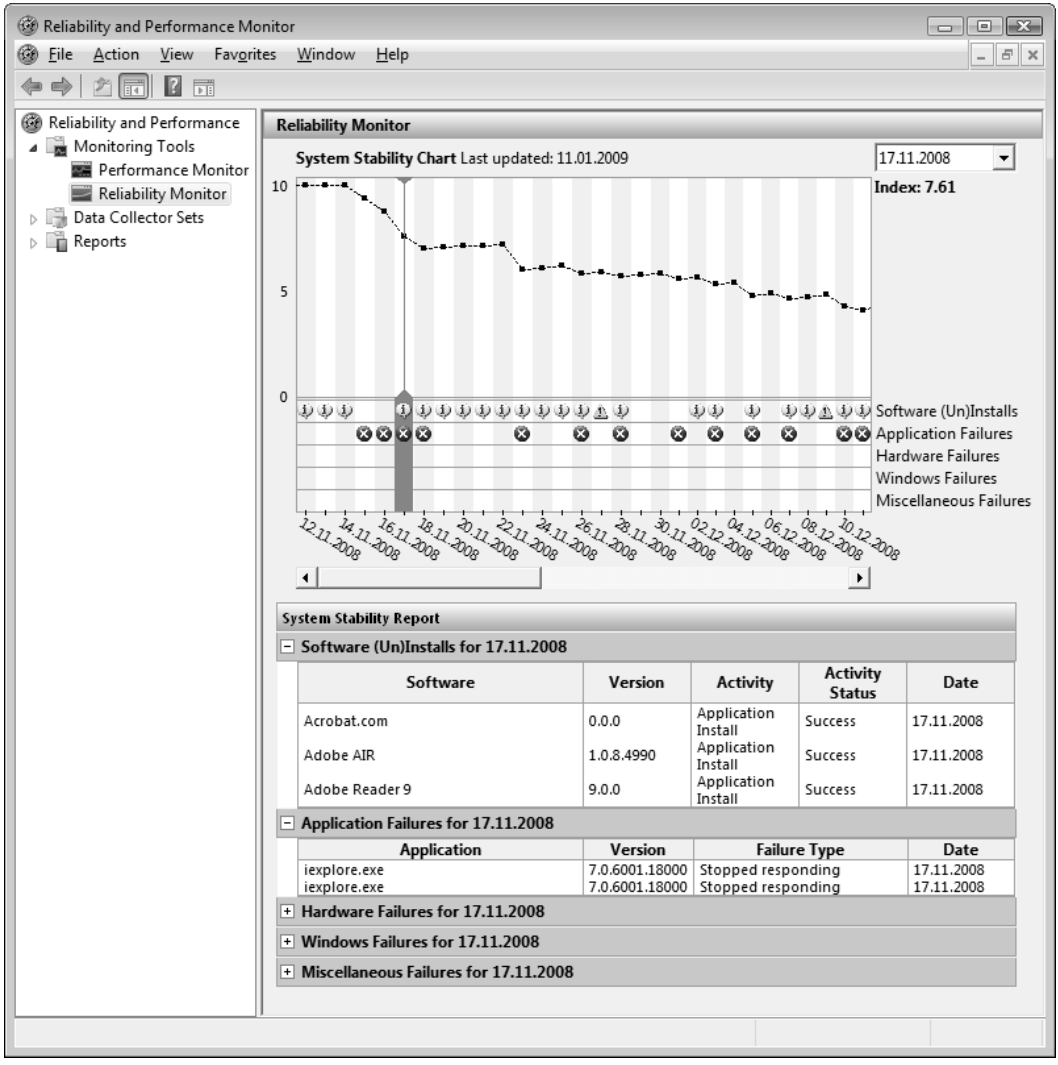


Рис. 3.26. Отображение стабильности системы на некотором временно́м отрезке

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.

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.

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 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.

> ***Внимание!***
>
> Группы сборщиков данных можно запускать и на удаленном компьютере, подключив к нему оснастку **Reliability and Performance Monitor** (Монитор производительности и стабильности). Однако для этого на компьютере должна быть установлена полная версия Windows Server 2008.

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. 3.27), расположенные в папке **System** (Системный). В правой половине окна перечислены имена конкретных сборщиков данных, входящих в группу; их можно удалять и добавлять. Дважды щелкнув по названию сборщика данных, можно перейти в окно его свойств и просмотреть используемые параметры.

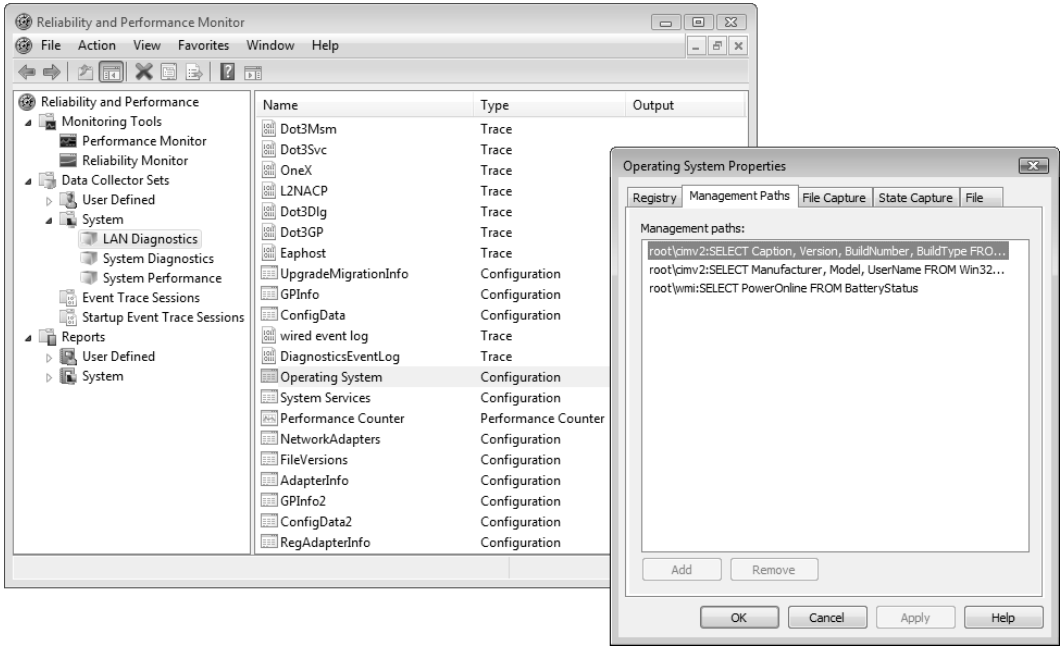


Рис. 3.27. Список стандартных системных групп сборщиков данных

Совет

Запустив группу System Performance, можно получить отчет о производительности системы, степени использования компонентов, "узких местах" и т. п. Группа System Diagnostics позволяет получить подробнейшую информацию о системе. Сборщики данных в течение минуты анализируют работу системы, и на основе полученных результатов генерируются отчеты в виде таблиц и многочисленных графиков, которые можно посмотреть в окне оснастки в папке **Reports** (Отчеты) (на диске они хранятся в папке C:\PerfLogs\System). В частности, это позволяет определить, достаточно ли в системе оперативной памяти, хватает ли быстродействия процессора для запущенных процессов, все ли устройства работают правильно и т. п. Рекомендуется периодически выполнять эти проверки для всех серверов.

Группы сборщиков, создаваемые самим администратором, помещаются в папке **User Defined** (Особый) (см. рис. 3.27); при их 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 (Системный монитор). 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.



Глава 4

Конфигурирование файловых служб

В этой главе описываются средства управления локальными дисками и общими дисковыми ресурсами систем Windows Server 2008, а также дополнительные функции, связанные с хранением информации (например, управление доступом к файлам и папкам или защита от несанкционированного доступа). Многие из них объединены одной ролью сервера — *File Services* (Файловые службы). Некоторые функции и средства администрирования присутствовали и в предыдущих версиях Windows, а многие появились только в Windows Server 2008[1].

> ***Примечание***
>
> Еще одна функция, относящаяся к работе с файлами — *Предыдущие версии файлов*[2] (previous versions), — описывается в *главе 5*, поскольку она тесно связана с задачами архивации и восстановления данных.

Установка файловых служб

Для систем Windows Server 2008 возможности компьютера как файлового сервера определяются службами роли *File Services* (Файловые службы). 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. Запустите оснастку **Server Manager** (Диспетчер сервера), выберите узел **Roles** (Роли) и в правой части окна оснастки найдите панель **File Services** (Файловые службы).

---

[1] Следует заметить, что многие новинки систем Windows Server 2008 касаются именно роли файлового сервера.

[2] В предыдущих версиях Windows аналогичная функция называлась *Теневые копии* (Shadow Copies).

2. Выберите ссылку **Add Role Services** (Добавить службы ролей). В окне программы-мастера установите флажки около названий требующихся служб и компонентов (рис. 4.1).

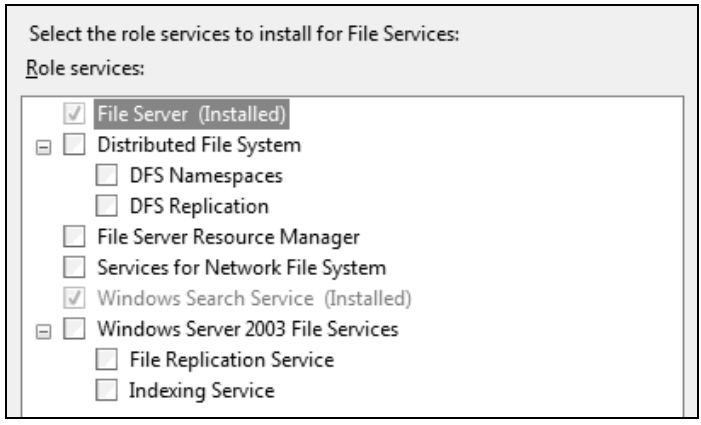


Рис. 4.1. Окно выбора устанавливаемых компонентов файловых служб

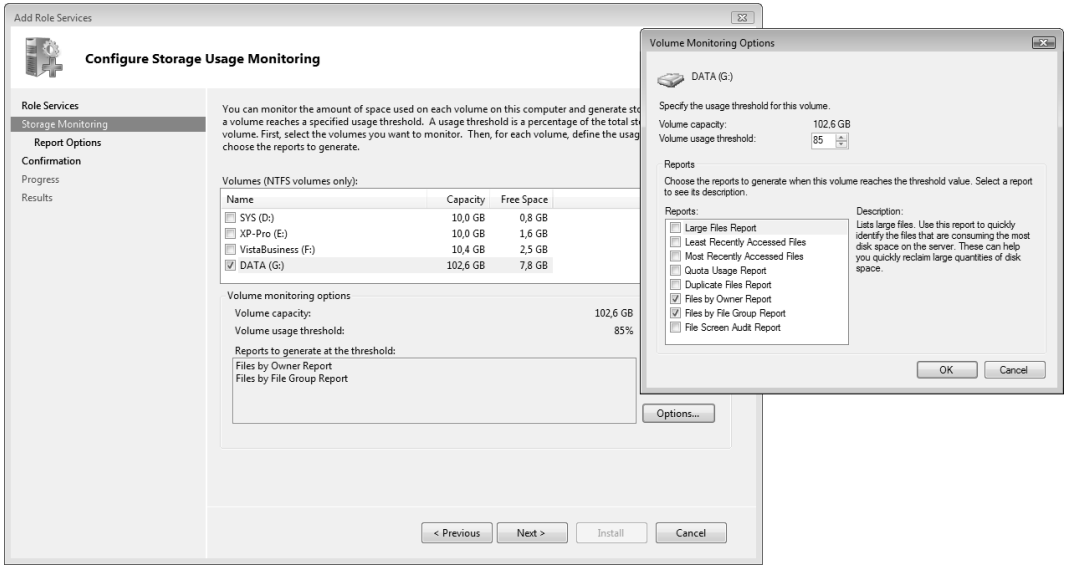


Рис. 4.2. Выбор дисковых томов для контроля за используемым пространством и других параметров для составления отчетов

При установке оснастки **File Server Resource Manager** (Диспетчер ресурсов файлового сервера) можно сразу указать, для каких дисковых томов будет осуществляться мониторинг используемого пространства (рис. 4.2). При нажатии кнопки **Options** (Сведения) открывается окно, где задаются пороговое значение для вы-

бранного 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. Также можно задать 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. 4.3). На панели событий легко 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.

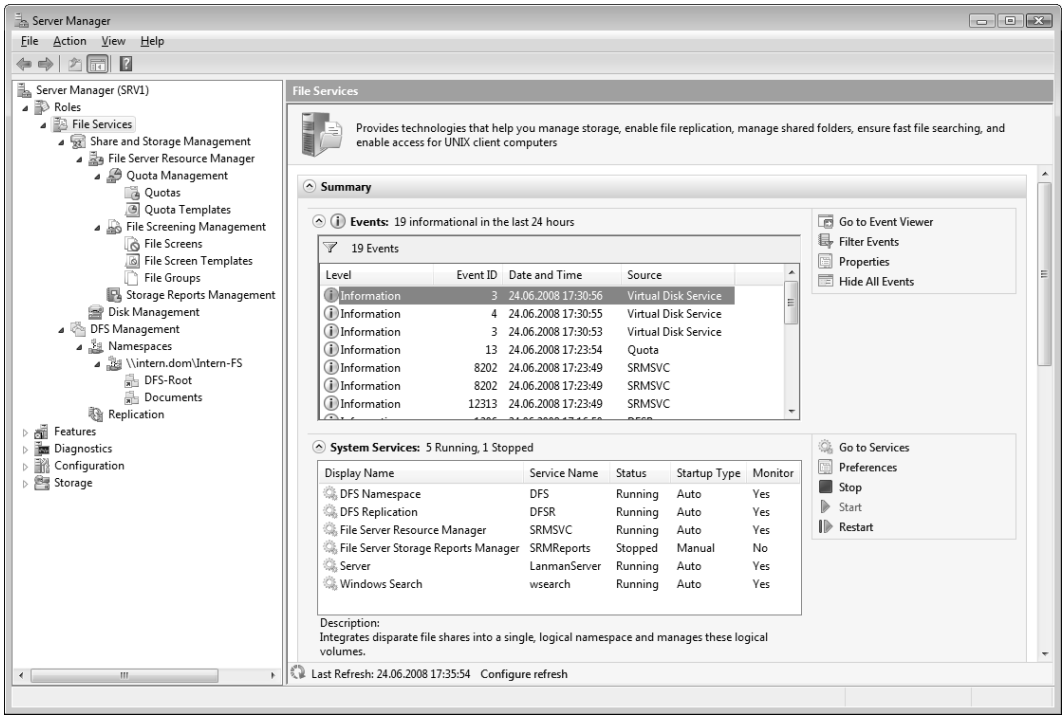


Рис. 4.3. Информационные панели для роли File Services

В нижней части списка административных панелей имеется справочная панель **Resources and Support** (Ресурсы и поддержка) (рис. 4.4), где перечислены рекомендации по эффективному использованию выбранной роли и ее служб (в начале работы с ролью или службами полезно ознакомиться к предлагаемой информаци-

ей!). Также здесь имеются ссылки, по которым можно обратиться к информационным и сервисным веб-ресурсам компании Microsoft.

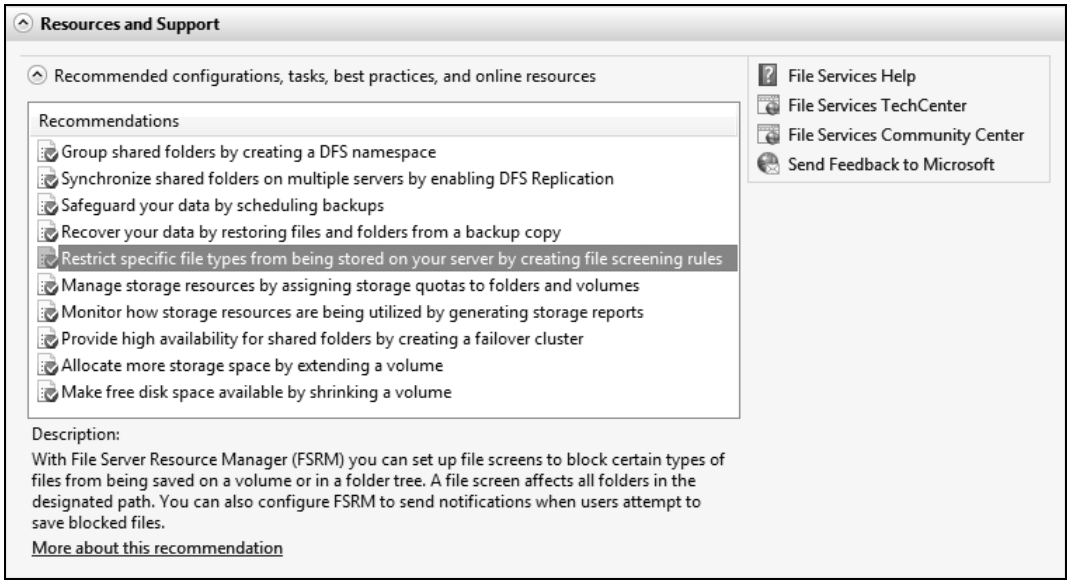


Рис. 4.4. Информационная панель — набор рекомендаций по использованию служб выбранной роли и ссылки на веб-ресурсы

Конфигурирование дисков и томов

Рассмотрим сначала некоторые общие вопросы, необходимые для понимания способов организации дисковых ресурсов в системах Windows Server 2008. Нужно сразу отметить, что все подходы, реализованные в предыдущей серверной версии, сохраняются и в этих системах.

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).)

На компьютерах, работающих на базе процессоров Itanium под управлением Windows XP 64-bit Itanium Edition и соответствующих 64-разрядных серверных версий Windows, впервые появился другой 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 следует искать на веб-сайте Microsoft, воспользовавшись поиском строки `GUID partition table`.)

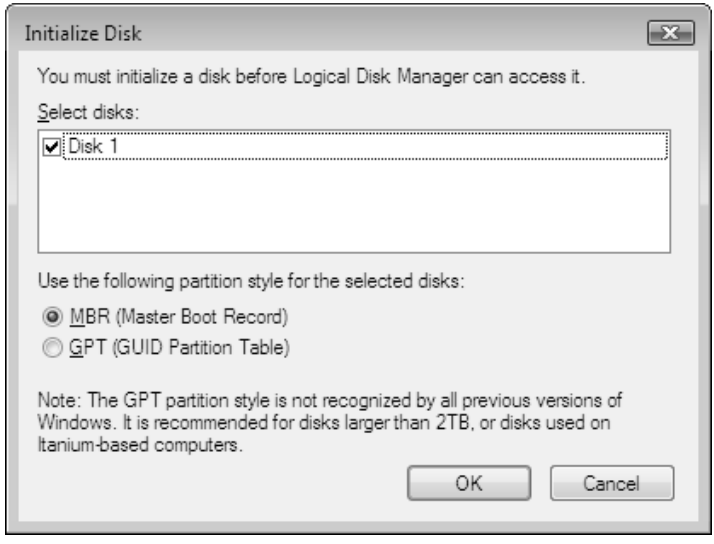


Рис. 4.5. Выбор стиля разделов при подключении к системе нового диска

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. 4.5) система предлагает выбрать тип раздела и

[1] Эксабайт (exabyte) = 1024 петабайт = 2^{60} байт. Терабайт (terabyte) = 1024 гигабайт = 2^{40} байт.

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.

Разделы и тома

Как и в предыдущих версиях Windows, в системах Windows Server 2008 используются жесткие диски, работающие в *базовом* режиме хранения информации (basic storage) и в *динамическом* режиме хранения данных (dynamic storage); соответственно диски называются *базовыми* (basic) и *динамическими* (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 для них имеется больше ограничений). Чаще всего динамические диски применяются в многодисковых конфигурациях.

Базовые диски

Базовые диски могут делиться на *разделы* — так называется часть 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, он может занимать все свободное пространство диска). 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.

> ***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.
>
> 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.

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) числом 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.

Динамические диски

Динамические диски делятся не на разделы, а на *тома* (volume). Том — это логически организованное пространство на одном или нескольких физических дисках. Как и предыдущие версии Windows, системы Windows Server 2008 поддерживают следующие типы томов:

- *простой том* (simple volume);
- *составной том* (spanned volume);
- *зеркальный том* (mirrored volume);
- *чередующийся том* (stripped volume) (RAID-0);
- *том RAID-5* (RAID-5 volume).

Использование оснастки *Disk Management*

Оснастка **Disk Management** (Управление дисками, diskmgmt.msc) (рис. 4.6) традиционно остается основным инструментом администратора для выполнения операций с дисковыми разделами (томами) или логическими дисками. Ее можно использовать как автономную оснастку или в составе оснастки **Computer Management** (Управление компьютером) — в этом случае можно динамически подключаться к любым компьютерам сети. При добавлении автономной оснастки к консоли управления MMC подключение к локальному или удаленному компьютеру выбирается "статически" и меняться не может.

> ***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 версиях Windows Server Core и Hyper-V Server 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.

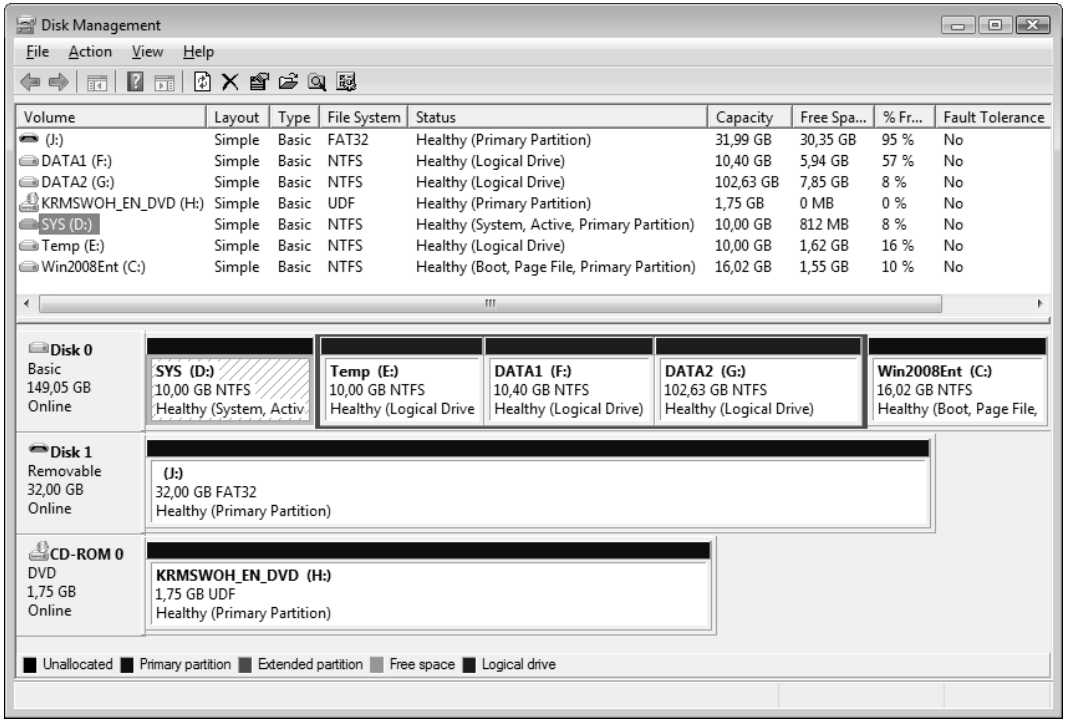


Рис. 4.6. Окно оснастки **Disk Management**

На рис. 4.6 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 "помещает" себя 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. 4.7). По умолчанию в верхней части окна отображается **Volume List** (Список томов), а в нижней — **Graphical View** (Графическое представление) (это расположение представлено на рис. 4.6). Если выбрать опцию **Disk List** (Список дисков), то можно видеть общие сведения о подклю-

ченных дисках[1] (рис. 4.7). Обратите внимание, что здесь указывается стиль раздела (MBR или GPT).

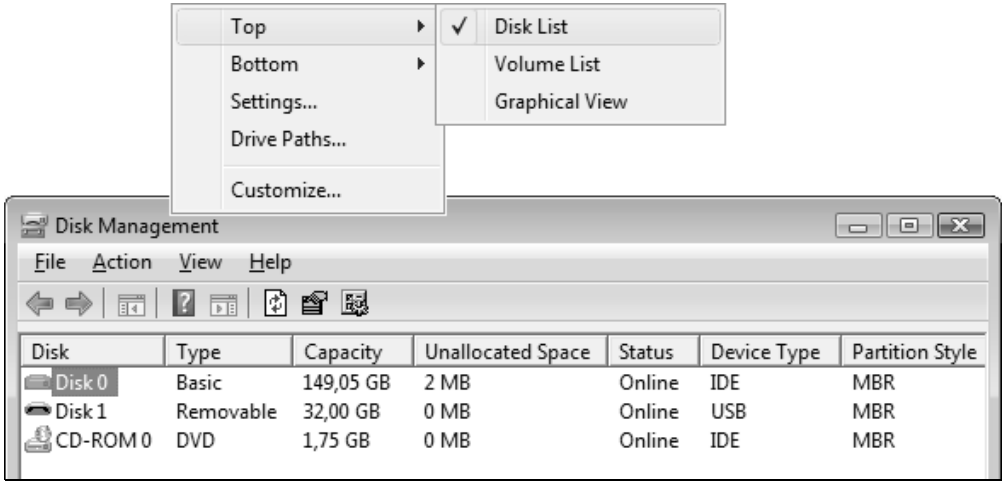


Рис. 4.7. Режим отображения подключенных дисков

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);
- форматировать тома, присваивать им метки, а также помечать тома как активные;
- сжимать (shrink) и расширять (extend) тома;
- инициализировать диски;
- преобразовывать базовые диски в динамические.

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 "сжимать диск". Существует тради-

[1] SATA-диски также могут отображаться как **IDE**.

ционное 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, 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;
- форматировать тома и назначать им метки (имена);
- расширять тома с использованием нераспределенного пространства на том же диске или на других дисках;
- сжимать тома;
- повторно инициализировать отключенные диски;
- преобразовывать динамические диски в базовые.

Расширение и сжатие разделов и логических дисков

В системах Windows Server 2008 оперативное сжатие и расширение разделов возможно не только при помощи утилиты DiskPart.exe (как в 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. 4.8) 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).

[1] В системах Windows Server 2003 эта оснастка позволяет только *расширять* тома.

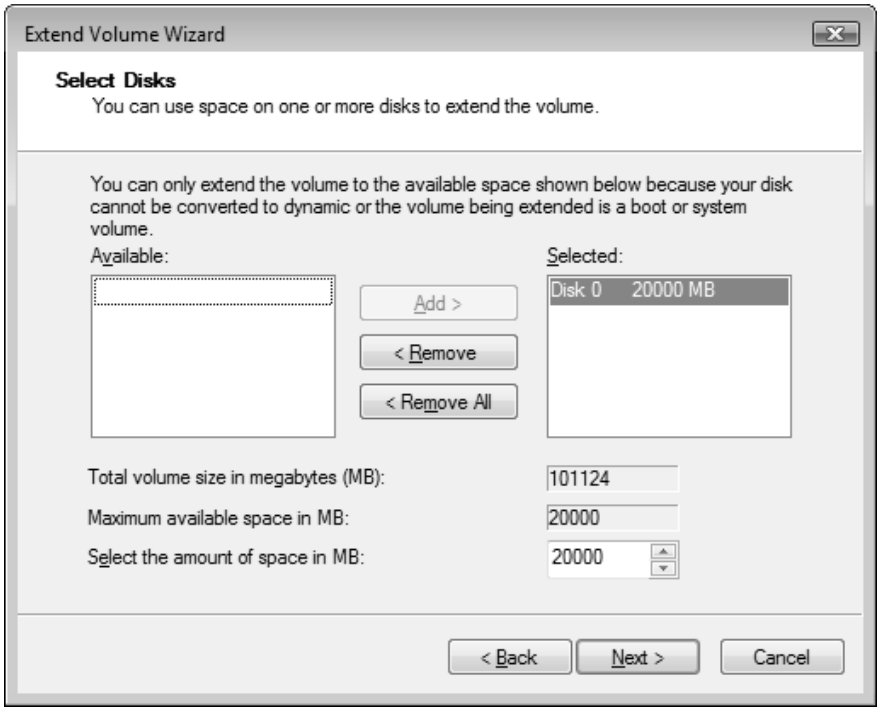


Рис. 4.8. Выбор нового размера расширяемого диска

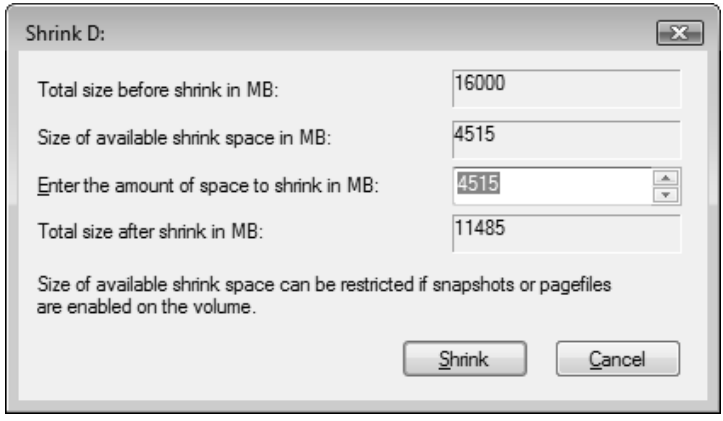


Рис. 4.9. Выбор параметров сжатия диска

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. 4.9), 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!

Дефрагментация дисков

Для уменьшения фрагментации дисковых томов в состав операционных систем Windows Vista и Windows Server 2008 включена утилита *Disk Defragmenter* (Дефрагментация диска) (рис. 4.10). Оснастка **Disk Defragmenter** (Дефрагментация диска), имеющаяся в Windows XP и Windows Server 2003, теперь отсутствует.

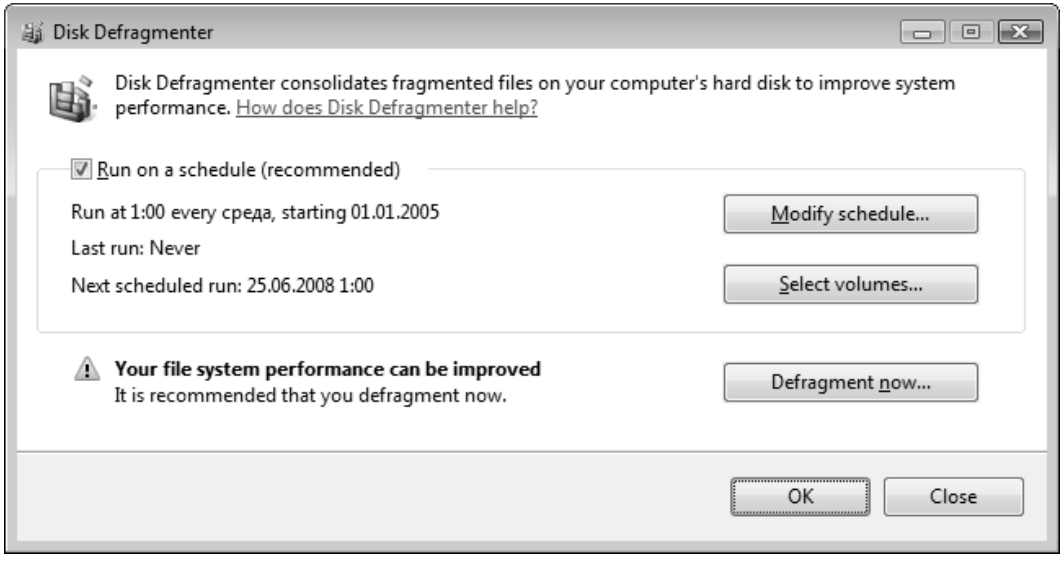


Рис. 4.10. Окно утилиты Disk Defragmenter

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** (Сервис), 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). После запуска утилита автоматически анализирует диски и указывает — следует ли провести дефрагментацию.

В системах Windows Server 2008 по умолчанию дефрагментация ***не*** выполняется. Если включить ее выполнение по расписанию (флажок **Run on a schedule** (Выполнять по расписанию) — см. рис. 4.10), то операция будет запускаться раз в неделю. Нажав кнопку **Modify schedule** (Изменить расписание), можно открыть окно параметров запуска задачи (рис. 4.11) и установить режим работы дефрагментатора, не мешающий работе сервера. 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 за-

пуска утилиты следует в ее окне нажать кнопку **Defragment now** (Выполнить дефрагментацию).

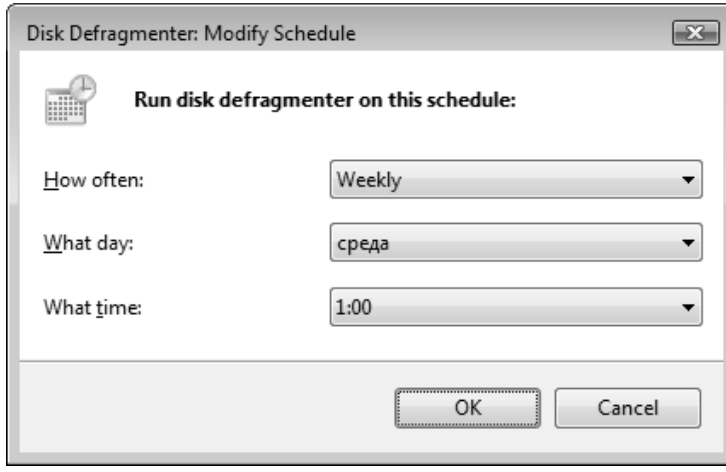


Рис. 4.11. Окно настройки расписания работы дефрагментатора дисков

Процесс работы утилиты Disk Defragmenter никак не визуализируется, лишь в окне программы отображается сообщение о выполнении операции (которую можно в любой момент отменить).

Во всех версиях Windows Server 2008 (включая Windows Server Core и Hyper-V Server) имеется 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) 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 выше).

Традиционные средства управления общими дисковыми ресурсами

Рассмотрим способы настройки *общего доступа* к дискам и отдельным папкам. В системах Windows Server 2008 имеются различные средства управления общими ресурсами — как существовавшие в предыдущих версиях Windows, так и совершенно новые. Сначала будут описаны традиционные средства и особенности их реализации в Windows Server 2008.

Управление общим доступом из программы Windows Explorer

Зачастую для создания и администрирования общих дисковых ресурсов достаточно возможностей программы Windows Explorer (Проводник): нужно выбрать требуемую 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 реализация такого подхода несколько изменилась[1].

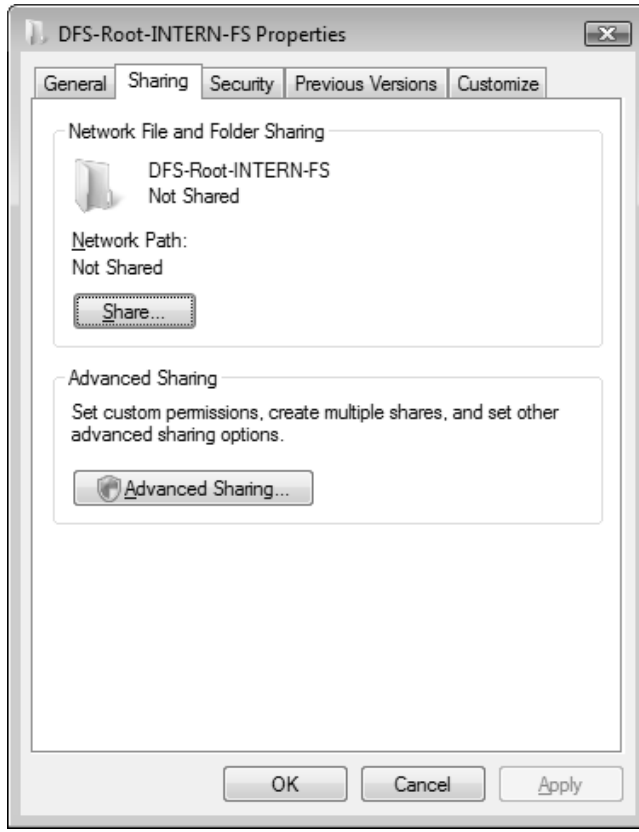


Рис. 4.12. Вкладка окна свойств папки, откуда можно управлять общим доступом к выбранной папке

Примечание

Все аспекты безопасности общих сетевых ресурсов рассматриваются далее в *разд. "Управление разрешениями доступа к файлам и папкам"*, поскольку разре-

[1] Нужно отметить, что для настройки параметров доступа теперь требуется чуть больше нажатий клавиш или щелчков мыши.

шения доступа нужно определять в совокупности с разрешениями, установленными на уровне файловой системы. Автоматически это делает только мастер общего доступа, описанный в следующем разделе.

Начальный вид вкладки **Sharing** (Доступ) в этих системах показан на рис. 4.12. 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.

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 небольшой дополнительный значок  .

Мастер общего доступа

Если на вкладке **Sharing** (Доступ) в окне свойств папки нажать кнопку **Share** (Общий доступ) (см. рис. 4.12), то запустится мастер *Sharing Wizard* (Мастер общего доступа) (рис. 4.13). 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 (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. 4.12) будет недоступна.

По умолчанию в списке пользователей, которым разрешен доступ к папке (см. рис. 4.13), 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.

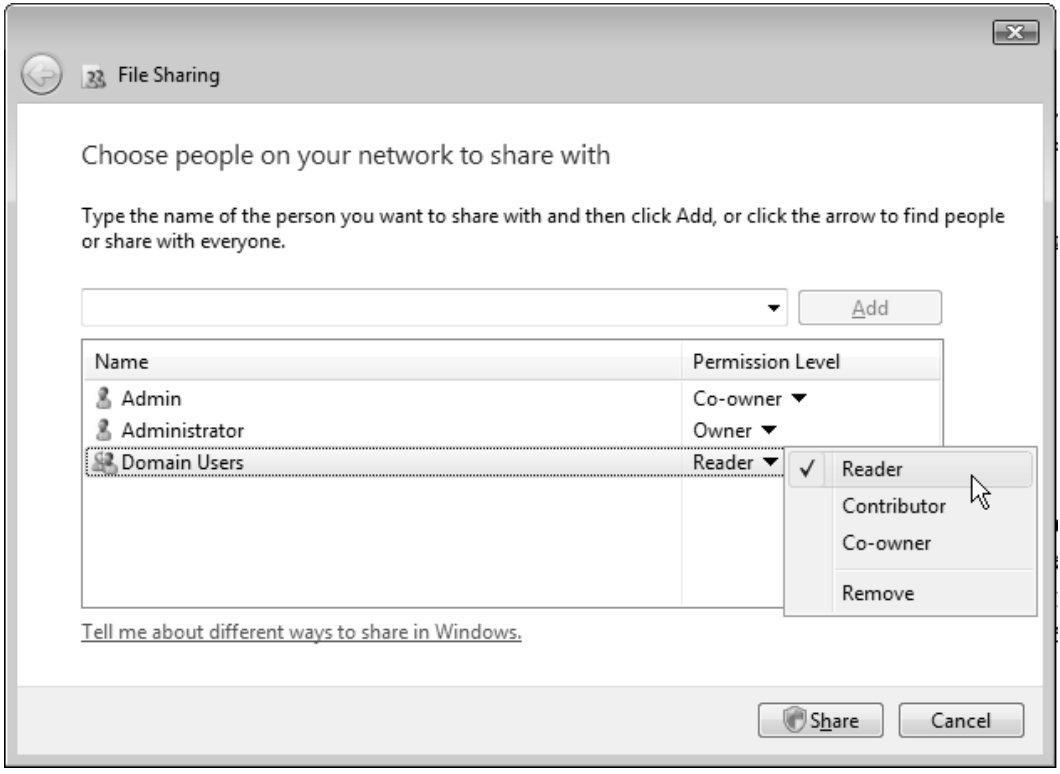


Рис. 4.13. Выбор разрешений с помощью мастера общего доступа

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. 4.13) нельзя формально отличить локального пользователя или группу от доменных. Это создает определенные неудобства, поэтому в доменах для управления разрешениями доступа лучше использовать классический подход, рассматриваемый ниже.

Вообще, следует отметить, что в сетях со множеством клиентов разрешения на доступ к папкам обычно предоставляют группам, а не пользователям. Этот момент подробно рассматривается далее в *разд. "Управление разрешениями доступа к файлам и папкам"*.

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. далее)*. Соответственно изменяются (отзываются) разрешения и при удалении учетной записи из списка пользователей общего ресурса. При ручном управлении разрешениями такого не происходит — права доступа и разрешения на уровне файловой системы изменяются независимо друг от друга.

Классический подход

Для более детальной настройки разрешений доступа к папке можно использовать традиционный для предыдущих версий Windows подход (хотя интерфейс этой операции в системах Windows Server 2008 совершенно изменился). Если на вкладке **Sharing** (Доступ) в окне свойств папки нажать кнопку **Advanced Sharing** (Дополнительный доступ) (см. рис. 4.12), то откроется окно, по функциям напоминающее вкладку **Sharing** (Доступ) предыдущих версий Windows.

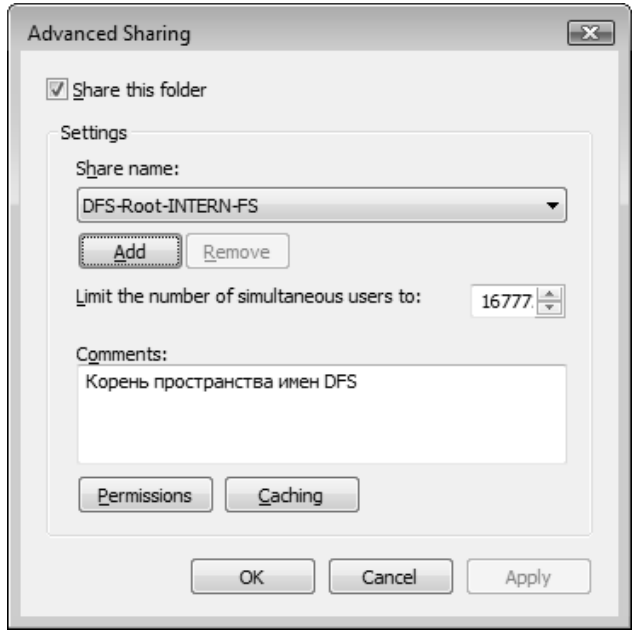


Рис. 4.14. В этом окне определяются параметры общего доступа к папке

Для разрешения общего доступа в этом окне (рис. 4.14) установите 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). Кнопка **Caching** (Кэширование) позволяет перейти к настройкам режима использования папки в автономном режиме. Чтобы задать разрешения доступа, нажмите кнопку **Permissions** (Разрешения) и в открывшемся окне (рис. 4.15) выберите требуемые параметры доступа.

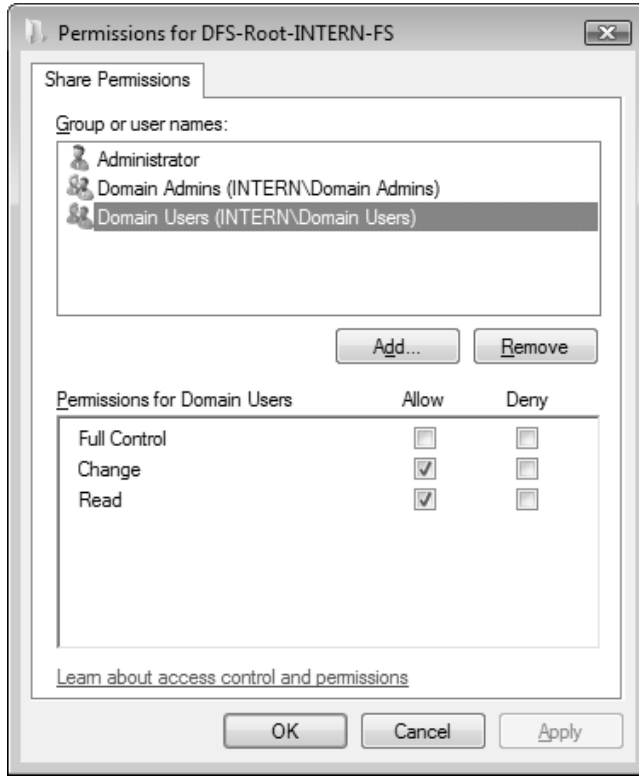


Рис. 4.15. Выбор разрешений доступа к общей папке

Внимание!

По умолчанию всем новым общим папкам дается разрешение Read (Чтение) для группы Everyone (Все). Не забудьте изменить настройки, если для работы требуются другие, более широкие (узкие) разрешения!

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 (что удобно для управления общими ресурсами систем Windows Server Core и Hyper-V Server). С ее помощью можно также управлять сеансами и открытыми файлами. Данная оснастка используется в составе стандартного инструмента администрирования — оснастки **Computer Management** (Управление компьютером) (рис. 4.16) или запускается автономно.

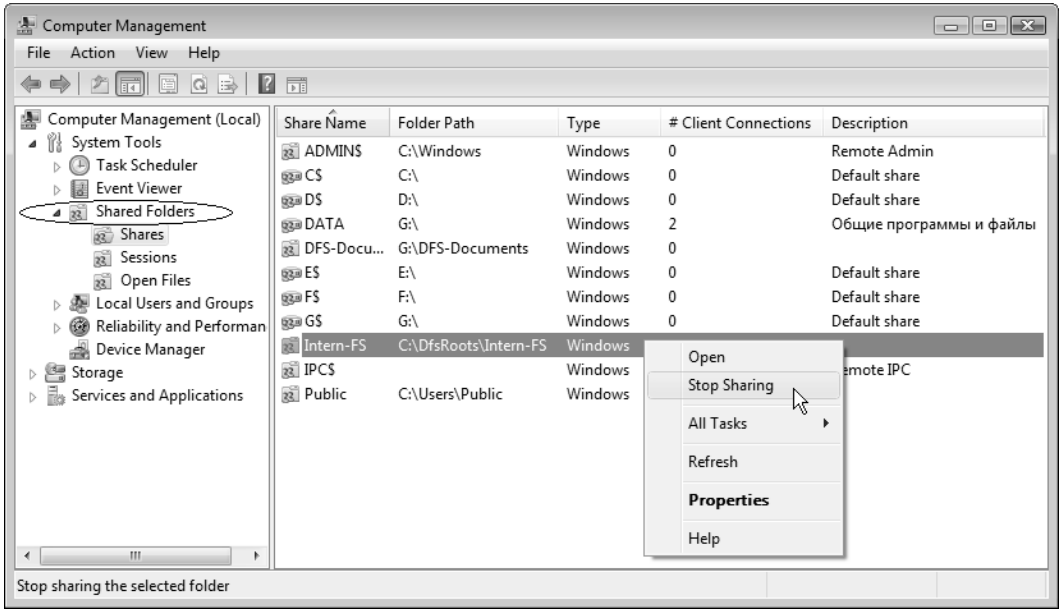


Рис. 4.16. Окно оснастки **Shared Folders** в составе инструмента **Computer Management**

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.

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. 4.17). Ключевые слова позволяют быстро находить любые ресурсы, опубликованные в каталоге.

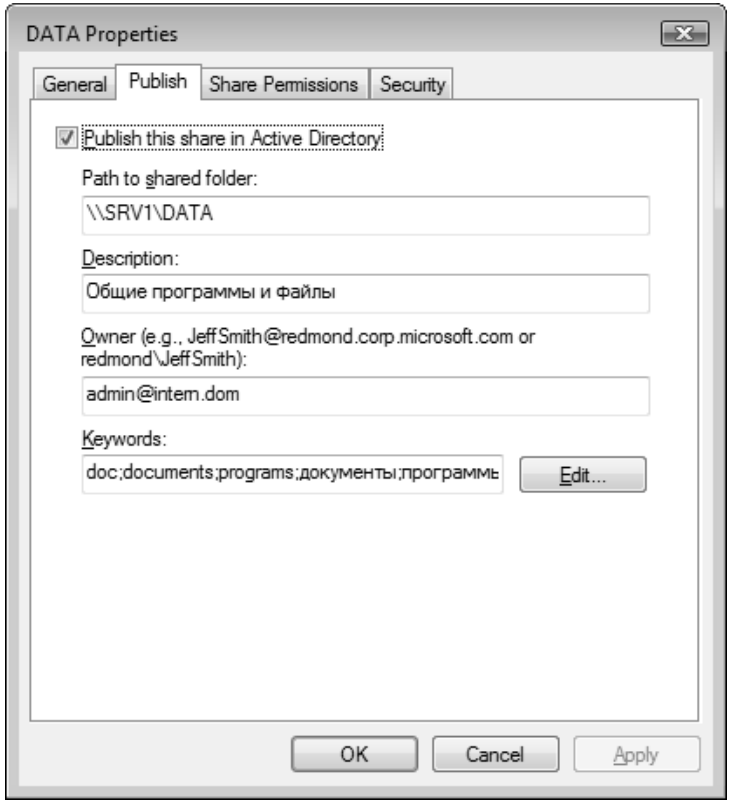


Рис. 4.17. Публикация папки в каталоге Active Directory

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. 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 контекст-

ном 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` применяется 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 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 ресурсов (включая служебные — параметр `/all`) на удаленном компьютере, например:

```
C:\>net view \\dc2

Shared resources at \\dc2

Domain controller (PDC)

Share name                  Type  Used as  Comment

-------------------------------------------------------------
F                           Disk  Z:
NETLOGON                    Disk           Logon server share
SYSVOL                      Disk           Logon server share
Users                       Disk

The command completed successfully.
```

[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.

Также с помощью этой команды можно увидеть режим кэширования общих папок (параметр `/cache`).

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 Y:, который будет представлять собой общую папку `users`, хранящуюся на компьютере `DC2`:

```
C:\>net use Y: \\DC2\users
The command completed successfully.
```

При подключении сетевых дисков можно явно указывать учетную запись безопасности, используемую для доступа к удаленному компьютеру.

Важным 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 X: \\DC2\users\docs` подключает папку `docs`, находящуюся внутри общей папки `users` как диск X:. Таким образом, пользователь получит доступ к конкретной папке и не сможет видеть другие папки, также находящиеся в общей папке.

Еще одно достоинство команды `net use` заключается в возможности подключения к так называемым *административным общим папкам*, которые по умолчанию имеются в ***любой*** системе Windows (см. рис. 4.16). Имя административной папки образуется из буквы диска и знака доллара ($). Например, команда `net use * \\DC1\C$` позволяет подключиться к диску C: на указанном компьютере. Такой подход упрощает работу с удаленными системами, особенно в тех случаях, когда обычные общие папки на них отсутствуют.

Управление разрешениями доступа к файлам и папкам

Одной из важнейших задач администратора файлового сервера является распределение прав доступа к хранящейся информации. Это касается и отдельных файлов, и папок. Имеются разные механизмы управления доступом к информации, но мы рассмотрим назначение прав доступа *в совокупности*, поскольку методы выбора этих прав тесно взаимосвязаны, и важно понимать, какие же разрешения будет иметь, в конце концов, каждый пользователь.

Правила назначения разрешений на доступ

Для того чтобы не нарушалась целостность изложения темы, повторим некоторые "хрестоматийные" правила настройки доступа к общим ресурсам.

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.

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. 7.34) — 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 были рассмотрены выше. 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 применения мастера учетные записи и их права выбираются индивидуально, при этом ***автоматически устанавливаются аналогичные разрешения и на уровне файловой системы***.

Разрешения доступа на уровне файловой системы NTFS

Устанавливая пользователям определенные *разрешения* (permissions) на доступ к файлам и папкам, администраторы системы могут защищать информацию от несанкционированного доступа.

Кроме того, каждый пользователь автоматически становится *владельцем* создаваемых файлов или папок. Это также обуславливает его права доступа к данным. 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.

Однако следует заметить, что правило сложения разрешений может нарушиться, если пользователю дано 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, и в результате пользователь фактически не будет иметь данного разрешения. Поэтому при установке отказа всегда появляется окно с напоминанием о серьезности такого действия (поскольку очень легко вообще лишить пользователя доступа к файлу или папке).

Установка разрешений для файлов

Все операции с разрешениями доступа к файлам и папкам инициируются 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 вся логика операций осталась прежней.

Рассмотрим порядок выполнения операций с файлами; аналогичные шаги потребуются и при работе с папками, поэтому для папок будут указаны только отличия.

Использование утилит командной строки

Имеются утилиты, позволяющие в окне консоли управлять разрешениями доступа на уровне файловой системы. Стандартная утилита *Icacls.exe*[1] используется для просмотра, установки и изменения разрешений для файлов и папок. Она имеется во всех версиях Windows Server 2008, включая Windows Server Core и Hyper-V Server.

Для назначения пользователю или группе разрешения на доступ к определенному файлу:

1. Выберите файл, нажмите правую кнопку мыши и выполните команду **Properties** (Свойства) контекстного меню. В окне свойств файла перейдите на вкладку **Security** (Безопасность) (рис. 4.18). 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.

[1] Эта утилита является обновленной и расширенной версией утилиты *Cacls.exe*, которая сохранена во всех системах.

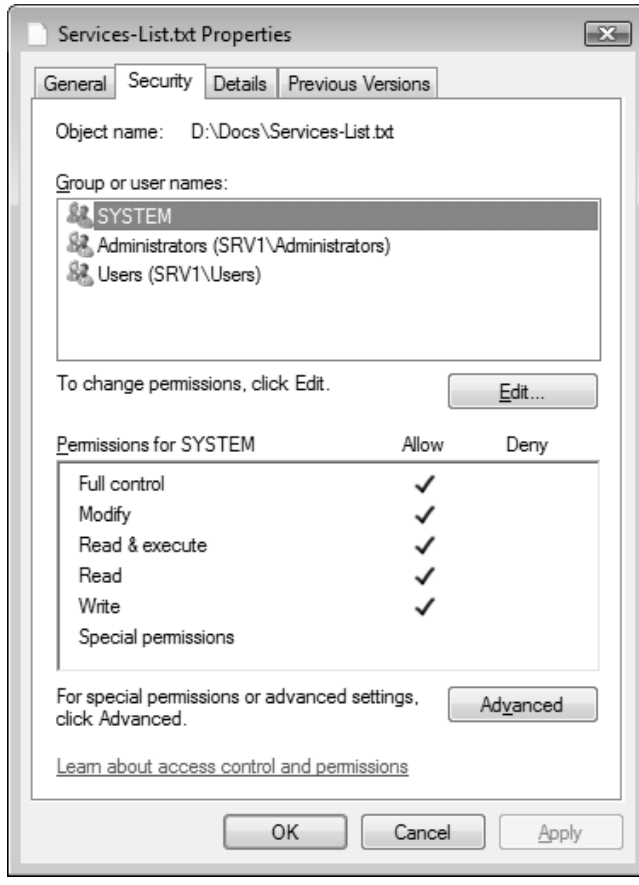


Рис. 4.18. Вкладка **Security** окна свойств файла

2. После нажатия кнопки **Edit** (Изменить) появляется окно (рис. 4.19), вид которого привычен пользователям предыдущих версий Windows: 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).

3. При добавлении учетных записей появится диалоговое окно, 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). Для *поиска* нужных имен можно нажать кнопку **Advanced** (Дополнительно). При этом откроется модифицированное окно выбора учетных записей (рис. 4.20), в котором можно указать местоположе-

ние (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.

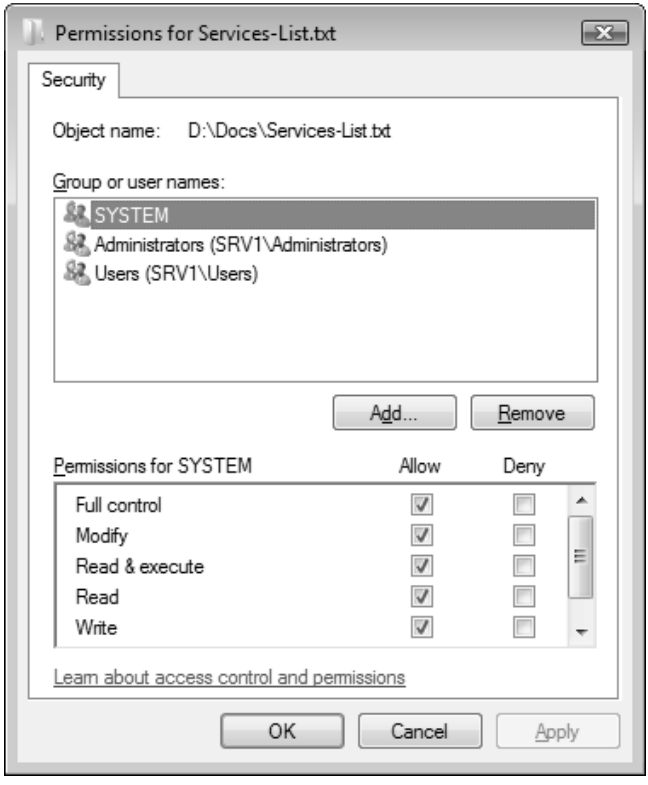


Рис. 4.19. Окно редактирования разрешений доступа

4. После выбора нужных учетных записей можно вернуться в окно редактирования разрешений (см. рис. 4.19) и назначить пользователю или группе *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.

Чтобы получить доступ к специальным разрешениям, в окне свойств файла на вкладке **Security** (Безопасность) (см. рис. 4.18) нажмите кнопку **Advanced** (Дополнительно). В окне дополнительных параметров безопасности (рис. 4.21) показано,

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.

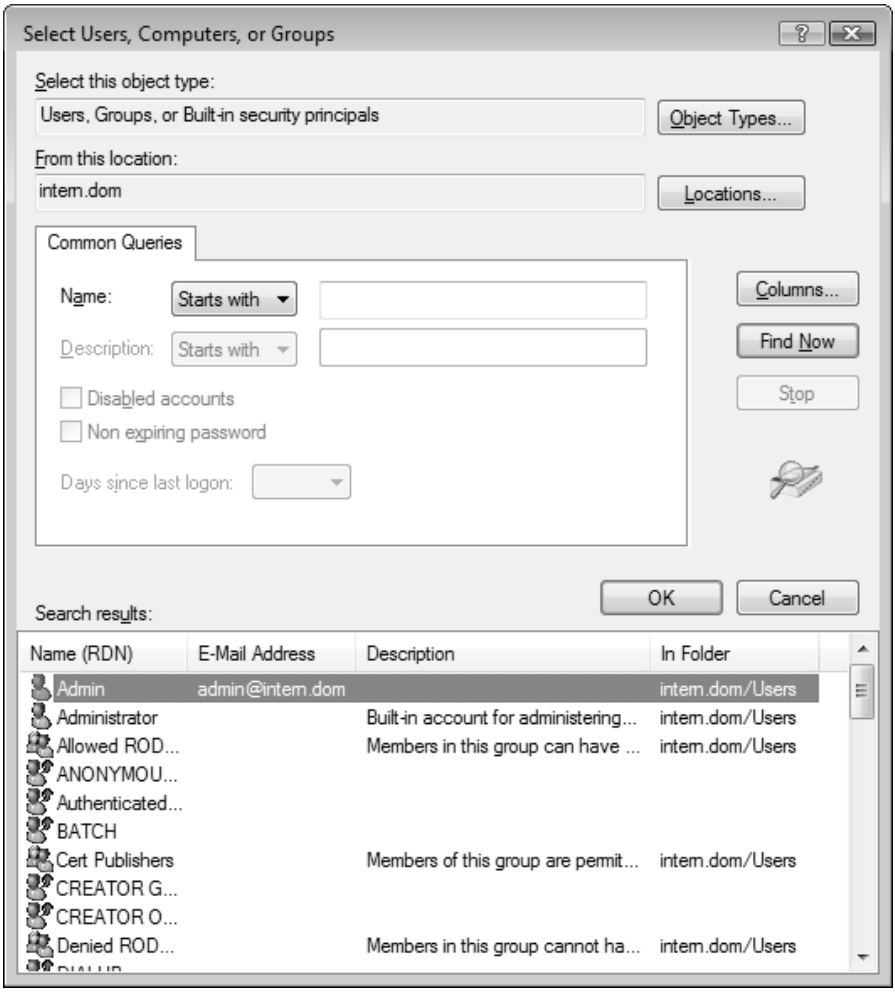


Рис. 4.20. Стандартное окно поиска и выбора учетных записей

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.

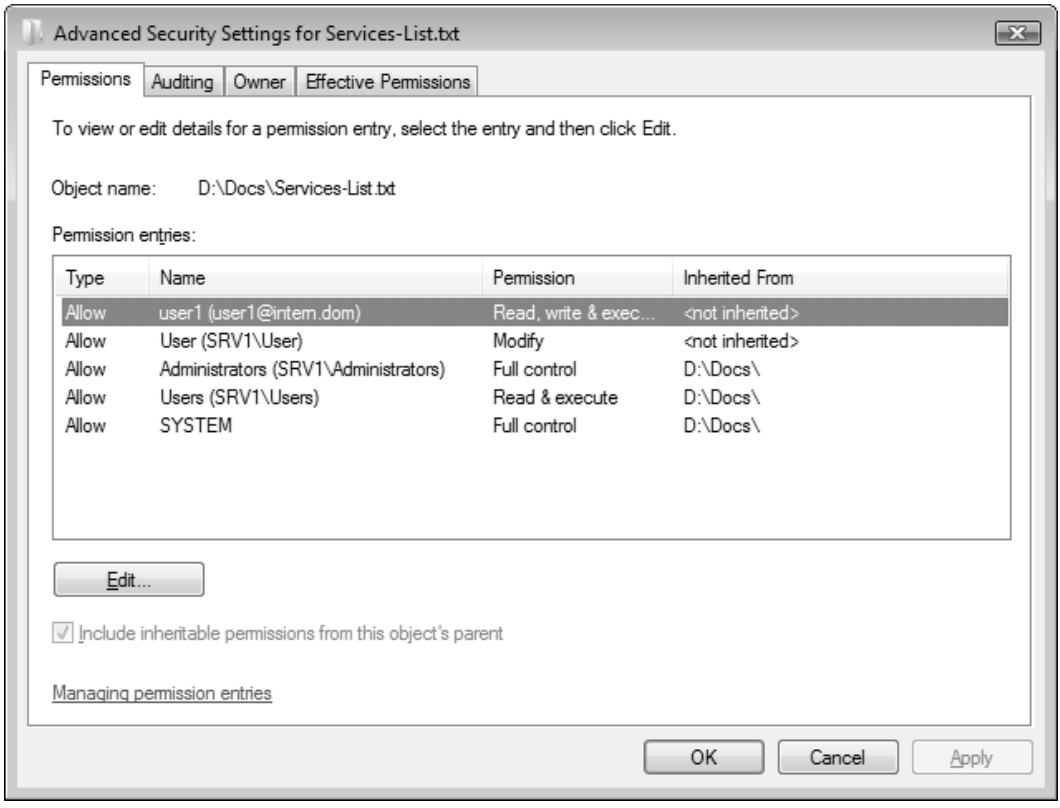


Рис. 4.21. Окно просмотра дополнительных параметров безопасности для файла

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 для папок (рис. 4.22) имеются дополнительные возможности, касающиеся изменения иерархии наследуемых разрешений (обратите внимание на отсутствующий для файлов столбец **Apply To** (Применять к), где указана область действия каждого разрешения).

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, то всякое наследование прекратится и все разрешения будут явно заданы только на уровне данного объекта. В этом случае возможны два варианта действий: можно *скопировать* разрешения (а затем изменять их, как требуется) или *удалить* (и задать новые).

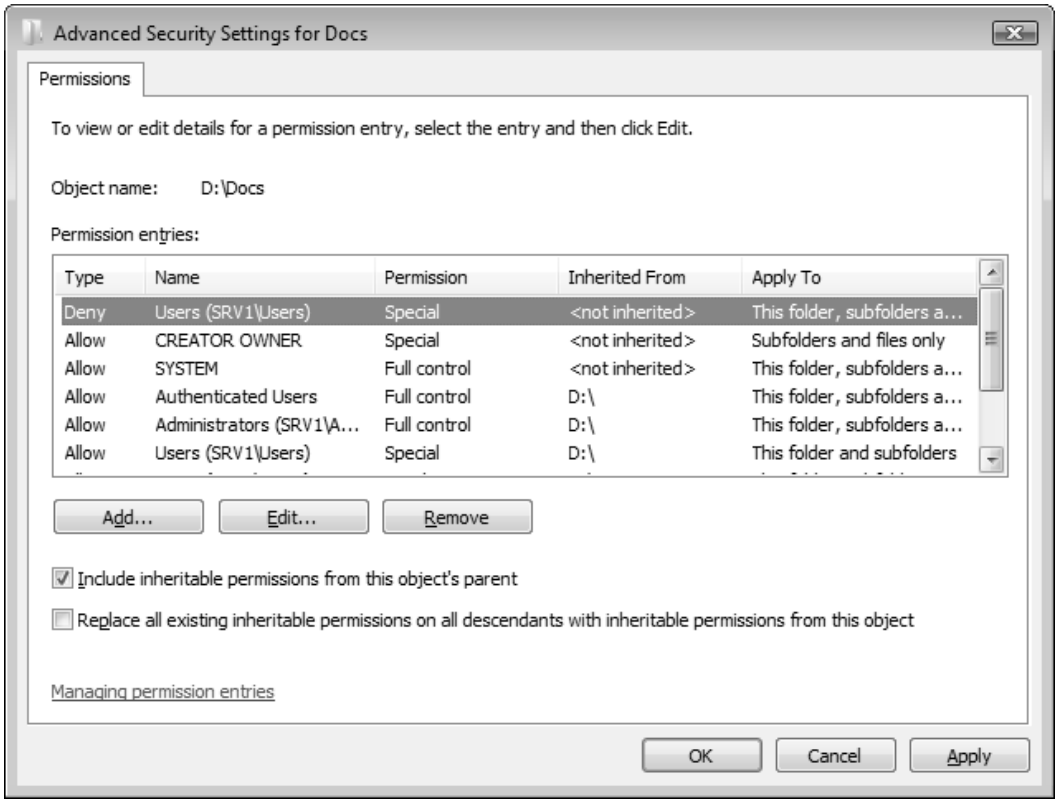


Рис. 4.22. Окно редактирования дополнительных параметров безопасности для папки

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. 4.22), 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.

Чтобы задать для папки *специальные* разрешения, в окне дополнительных параметров (см. рис. 4.22) нажмите кнопку **Edit** (Изменить). Появится окно **Permissions Entry** (Элемент разрешения) (рис. 4.23), где устанавливаются специальные разрешения для папки; в списке **Apply onto** (Применять) можно также выбрать область их действия.

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.

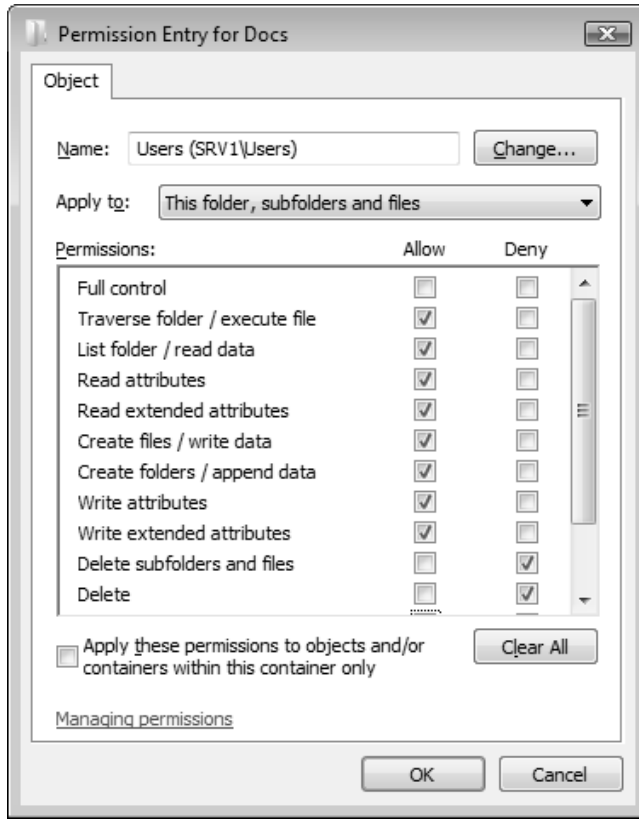


Рис. 4.23. Специальные разрешения для папки

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 легко узнать, какие же разрешения имеет пользователь для конкретного объекта. Для решения этой задачи имеется функция определения *действующих разрешений* (effective permissions), которую можно использовать следующим образом:

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) и выберите требуемую учетную запись локального или доменного пользователя или группы, после чего 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. 4.24).

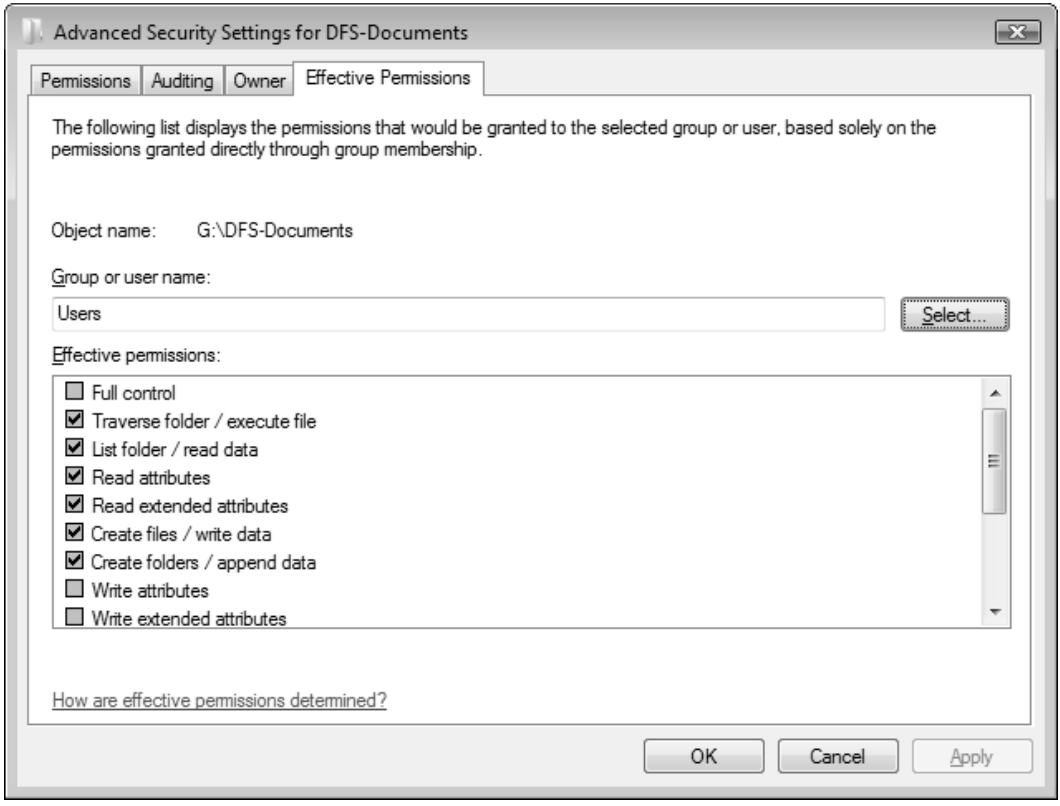


Рис. 4.24. На вкладке **Effective Permissions** отображаются все разрешения для выбранного пользователя или группы

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 полномочиями, и, кроме того, право владения может быть передано

другому пользователю — это может сделать пользователь, имеющий разрешение на смену владельца (право Take Ownership (Смена владельца)).

С помощью локальных или доменных групповых политик можно указать, 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.

Для передачи владения объектом файловой системы или для просмотра текущего владельца файла или папки требуются следующие действия:

1. Откройте соответствующее окно свойств, перейдите на вкладку **Security** (Безопасность) и нажмите кнопку **Advanced** (Дополнительно).

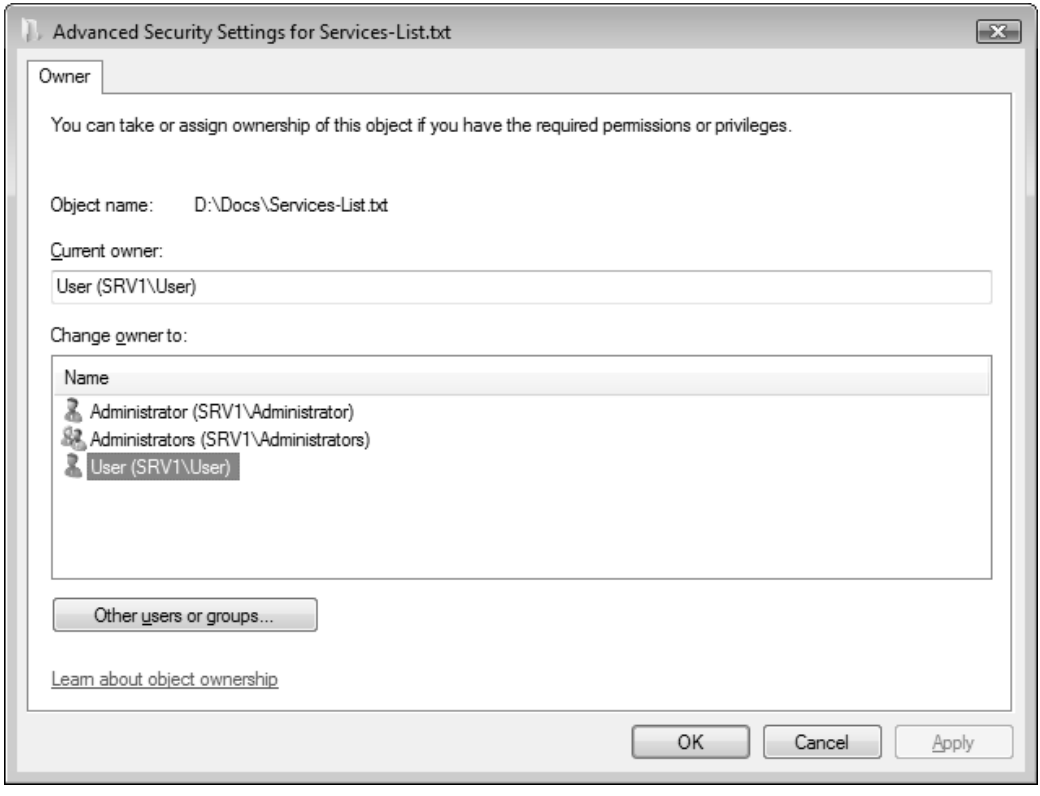


Рис. 4.25. Вкладка **Owner** диалогового окна **Advanced Security Settings**

2. В окне **Advanced Security Settings** (Дополнительные параметры безопасности) (см. рис. 4.21) перейдите на вкладку **Owner** (Владелец). Текущий владелец объекта виден в поле **Current owner** (Текущий владелец).
3. После нажатия кнопки **Edit** (Изменить) откроется окно, где владельца можно поменять (см. рис. 4.25). В этом окне видны учетные записи, по умолчанию имеющие право получения во владение данного объекта файловой системы. Для смены владельца выделите нужную учетную запись и нажмите кнопки **Apply** (Применить) и **OK**.
4. Если право владения нужно передать какому-то другому, то нажмите кнопку **Other users or groups** (Другие пользователи или группы) и воспользоваться стандартной процедурой выбора учетных записей — после этого имя найденного пользователя или группы появится в окне потенциальных владельцев (рис. 4.25), где его следует выделить и закончить операцию, нажав кнопку **OK**.

Централизованное управление общими ресурсами с помощью оснастки *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).

Эта оснастка представляет собой инструмент мониторинга и управления "верхнего уровня". В ее окне (рис. 4.26) 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).

Если дважды щелкнуть по имени общей папки, то откроется окно ее свойств, где отображаются все параметры ресурса (рис. 4.27). 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) (см. рис. 4.26) имеются команды, с помощью которых отображаются 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.

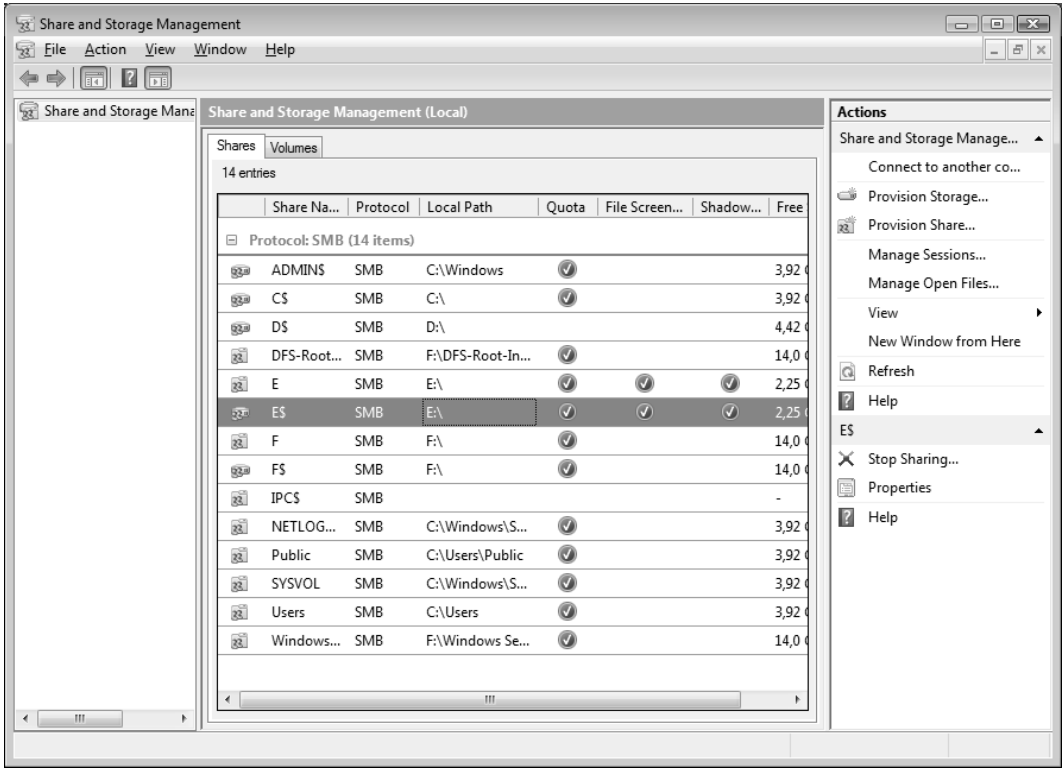


Рис. 4.26. Просмотр списка общих папок в окне оснастки **Share and Storage Management**

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.

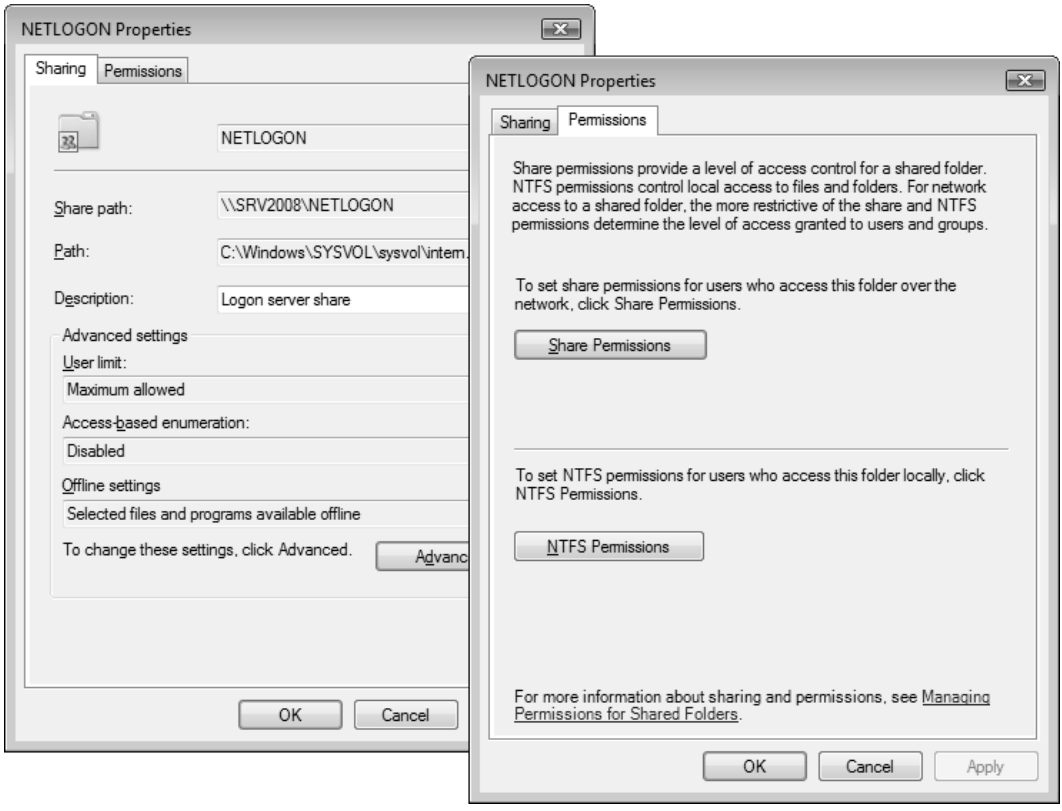


Рис. 4.27. Вкладки окна свойств общей папки

Квоты дискового пространства

Для файлового сервера важной административной задачей 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*; невозможно задать квоту для *групп*. В системах Windows Server 2008 появилась возможность устанавливать квоты на отдельные *папки* — для этого используется оснастка **File Server Resource Manager** (Диспетчер ресурсов файлового сервера). Поскольку использование этой оснастки требует дополнительных операций, назначение квот с ее помощью мы рассмотрим в отдельном разделе *(см. далее)*.

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`. Эту утилиту можно использовать и в редакциях Windows Server Core. Для включения квот служит команда `fsutil quota enforce`, а для назначения квоты конкретному пользователю — команда `fsutil quota modify`.

Включение стандартного 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 выполните команду **Properties** (Свойства). В окне свойств тома перейдите в нем на вкладку **Quota** (Квота) (рис. 4.28).
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 выделять 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.

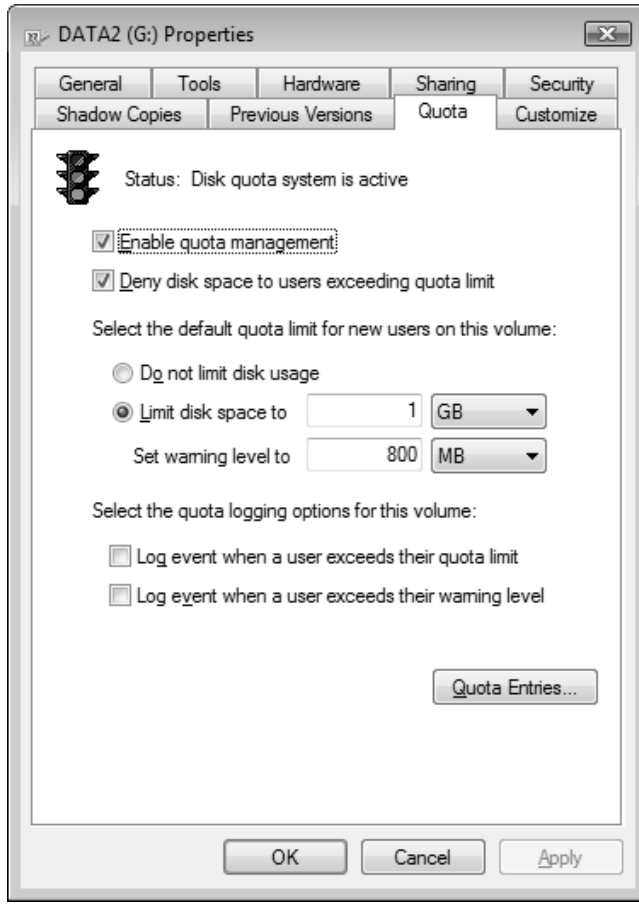


Рис. 4.28. Вкладка **Quota**
окна свойств дискового тома

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) (или в окне консоли используйте команду `fsutil quota query`). Появится окно (рис. 4.29), 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).

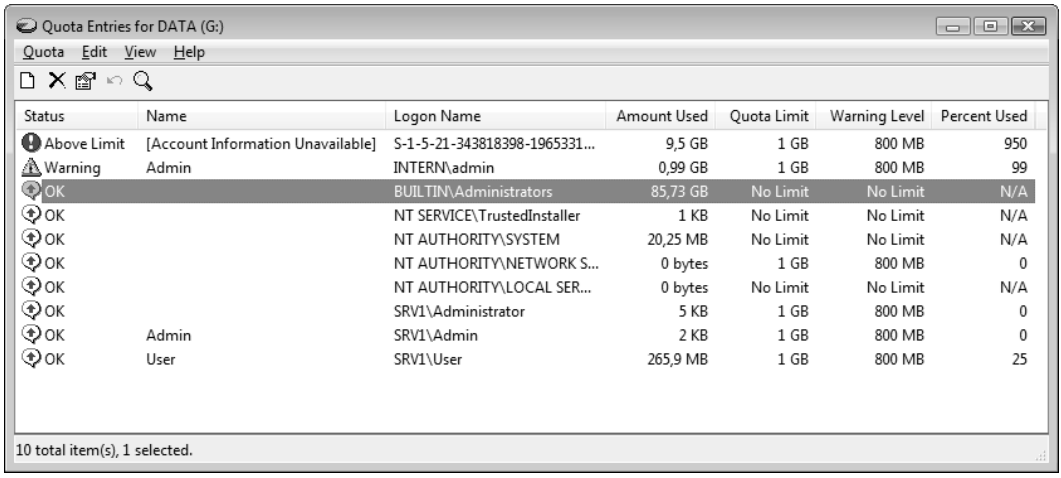


Рис. 4.29. Список пользователей, имеющих файлы на диске, и их дисковые квоты

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. 4.30).

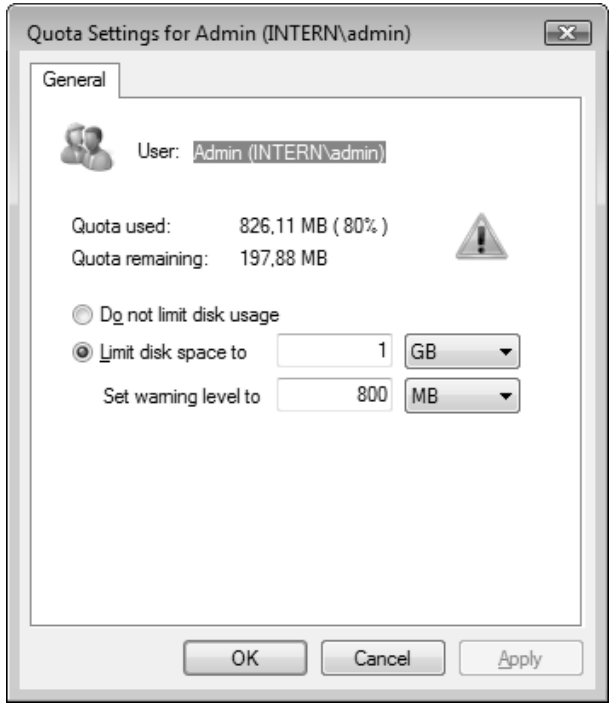


Рис. 4.30. Параметры квоты для конкретного пользователя

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 информационное событие с кодом 36 от источника "Ntfs" (данный код 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 ошибку, указывающую на недостаток свободного места.

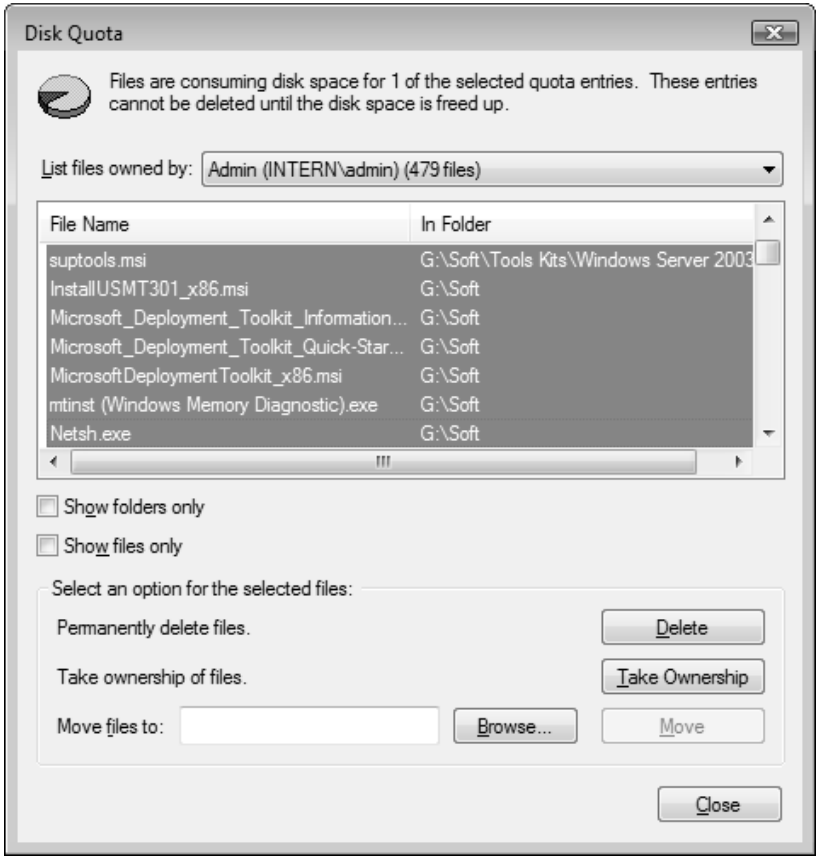


Рис. 4.31. В этом окне перечисляются все файлы (вместе с их точным местоположением), принадлежащие выбранному пользователю на указанном томе с включенным квотированием

Следует иметь в виду одну особенность, связанную с регистрацией учетных записей пользователей в списке записей квот (см. рис. 4.29). 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.) Такое 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.

При попытке удаления строки из списка записей квот после подтверждения этой операции выводится список файлов, принадлежащих выбранному пользователю (рис. 4.31) (если же у пользователя отсутствуют принадлежащие ему файлы, то запись просто удаляется). В этом окне администратор может выполнить операции с перечисленными файлами: стать их владельцем (выделив нужные файлы), а затем удалить или переместить в другое место. (Причем удалять или перемещать файлы совсем необязательно — просто при изменении "права собственности" эти файлы будут числиться за новым владельцем.)

Управление доступом к файловым ресурсам с помощью оснастки *File Server Resource Manager*

Одним из дополнительных компонентов роли *File Services* (Файловые службы) (см. рис. 4.1) 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. 4.32). (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).

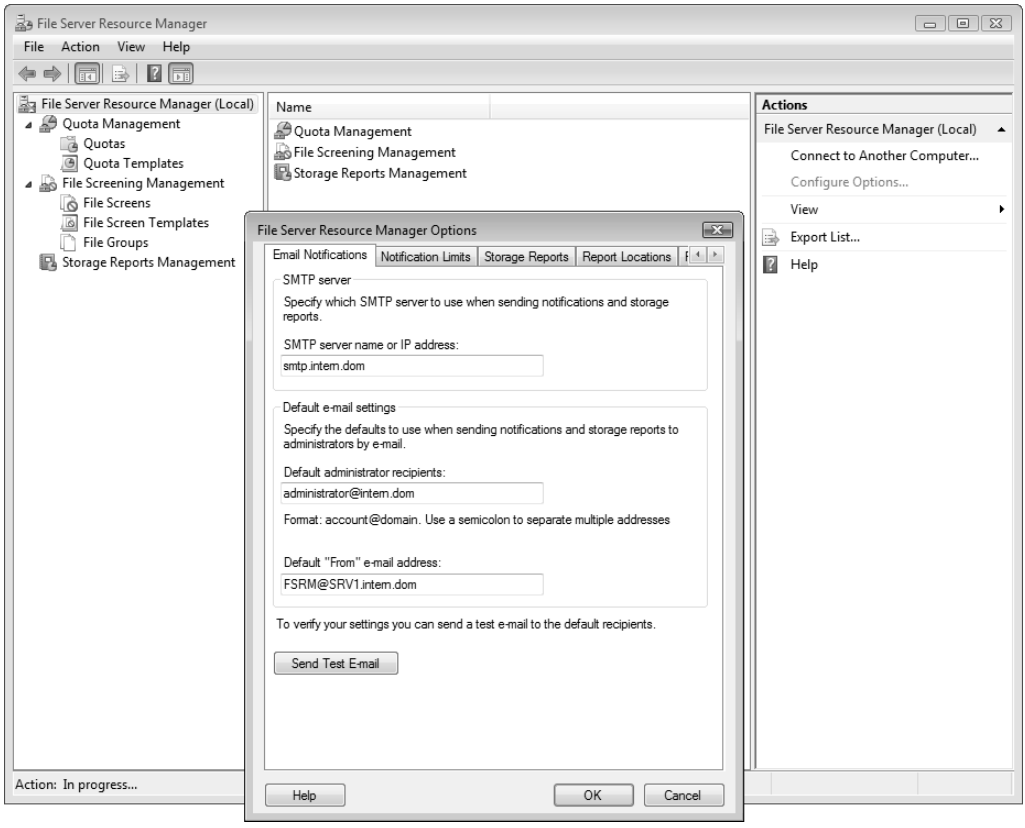


Рис. 4.32. Главное окно оснастки **File Server Resource Manager** и окно ее основных параметров

В окне параметров оснастки (см. рис. 4.32) 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 томов и папок

Для управления квотами используются так называемые *шаблоны квот*, которые хранятся в папке **Quota Templates** (Шаблоны квоты) (рис. 4.33). Изначально здесь представлены стандартные шаблоны, которые редактировать не рекомендуется — при необходимости изменения параметров следует на их основе создавать собственные шаблоны с требуемыми значениями. Шаблон квоты определяет пороговое значение для дискового пространства и реакцию на превышение квоты: для "жестких" (hard) квот это отказ в доступе, для "мягких" (soft) — предупреждение.

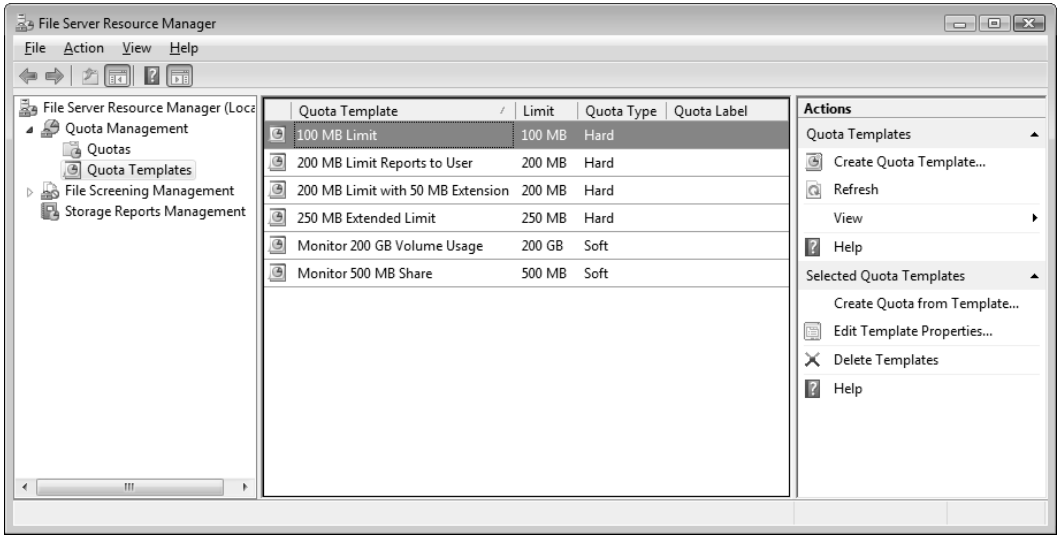


Рис. 4.33. Папка шаблонов квот

При создании своего шаблона (рис. 4.34) можно скопировать исходные параметры из имеющегося шаблона (раскрывающийся список в верхней части окна), после чего отредактировать их в соответствии со своими потребностями. 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. 4.36). 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 выбрать шаблон квот (рис. 4.35). 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.

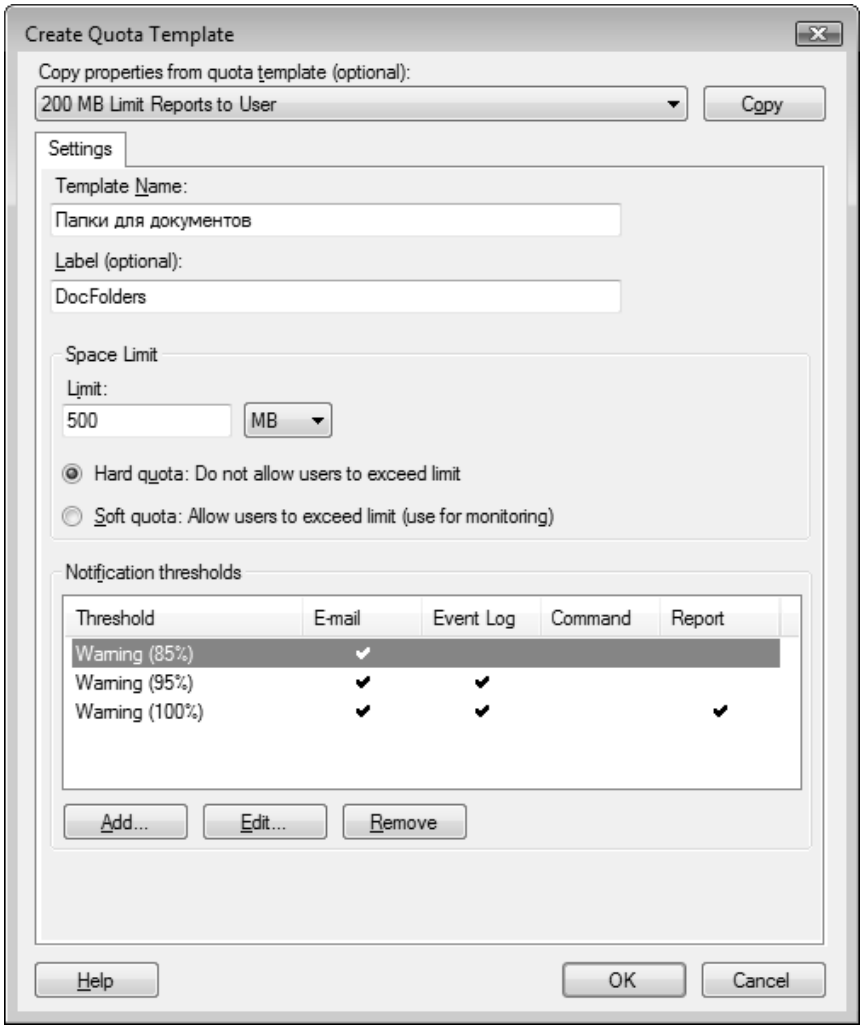


Рис. 4.34. Окно параметров нового шаблона квот

В папке **Quotas** (Квоты) (рис. 4.36) видны все установленные квоты с их параметрами, а также текущее состояние папки, на которую действует выделенная квота. Здесь параметры квот можно редактировать, создавать новые квоты и отключать установленные.

Если пользователь пытается записать данные в папку, на которую установлена квота с "жестким" ограничением, и превышает пороговое значение, то он получает сообщение об ошибке, указывающей о нехватке свободного места, и должен либо отказаться от операции, либо прямо из окна сообщения вызвать служебную утилиту и очистить целевую папку от ненужной информации — после этого операцию записи можно продолжить (повторить, не закрывая окна).

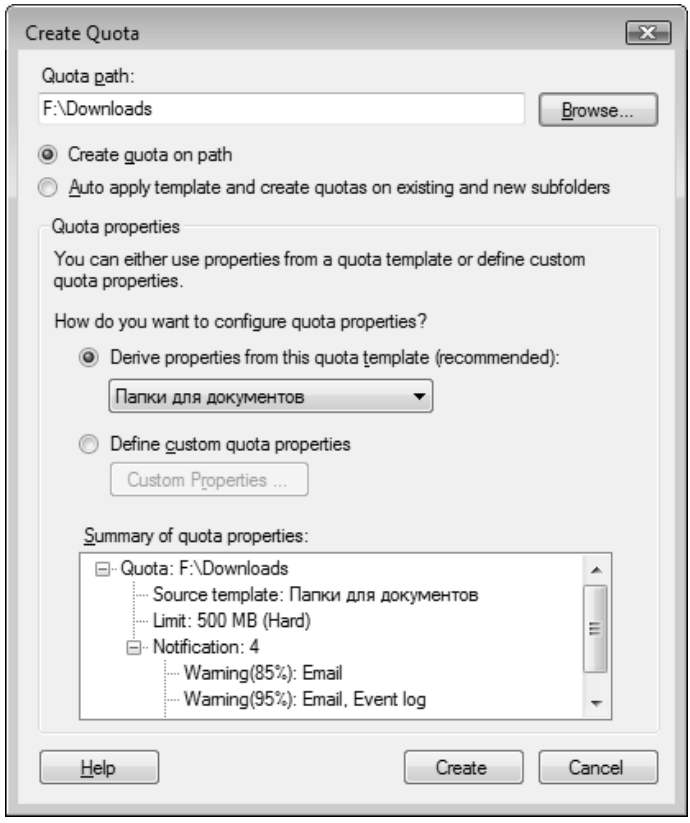


Рис. 4.35. Окно устанавливаемой квоты

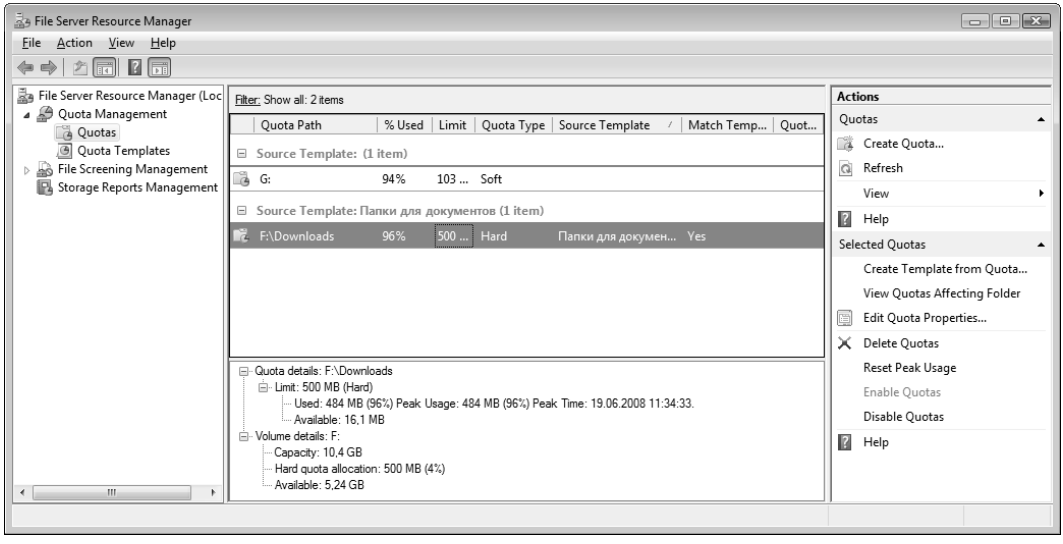


Рис. 4.36. Список активных квот

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 кво-
ты..., текущее использование ...% от предела.)
```

Таким образом, можно видеть, что с помощью средств оснастки **File Server Resource Manager** (Диспетчер ресурсов файлового сервера) легко эффективно контролировать использование дискового пространства на любых томах или отдельных папках. При этом администратор централизованно получает всю детальную информацию о загруженности ресурсов и конфликтных ситуациях.

Блокировка копирования и создания файлов

Принцип настройки механизма блокировки файлов такой же, как описанная выше процедура установки квот на папки и тома: выбирается правило (шаблон) фильтрации файлов и указывается папка, на которую это правило действует.

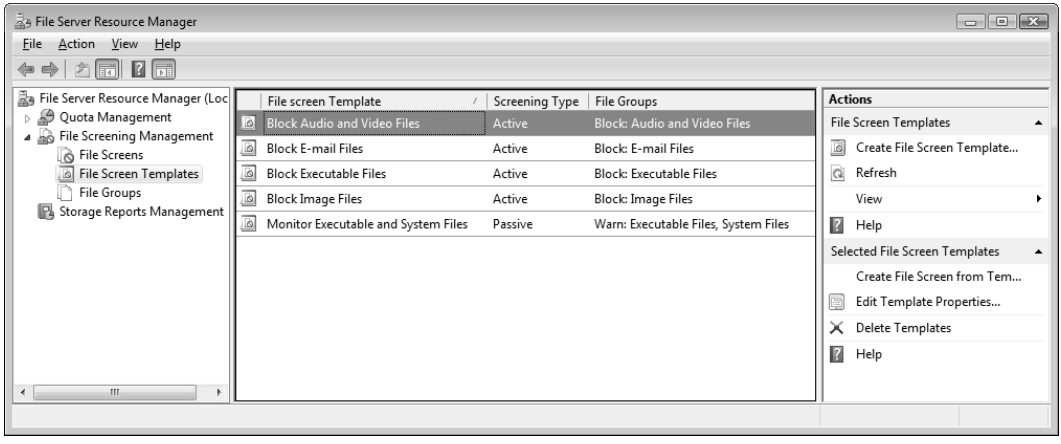


Рис. 4.37. Перечень шаблонов для блокировки файлов

Все предопределенные (стандартные) и создаваемые шаблоны хранятся в папке **File Screen Templates** (Шаблоны фильтра блокировки файлов) (рис. 4.37), 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 свои собственные. Каждый шаблон использует одну или несколько *групп файлов*. *Активные* шаблоны за-

прещают запись файлов установленного типа, *пассивные* — только информируют администратора о создании таких файлов.

Перед использованием любых шаблонов обязательно нужно просмотреть свойства шаблона и скорректировать адрес электронной почты администратора, который будет получать информацию о блокировке файлов.

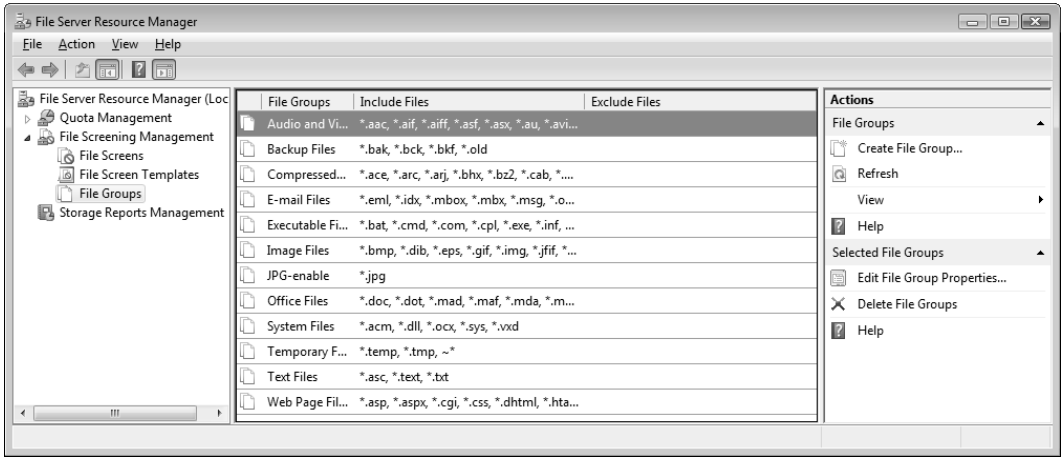


Рис. 4.38. Группы файлов различного типа

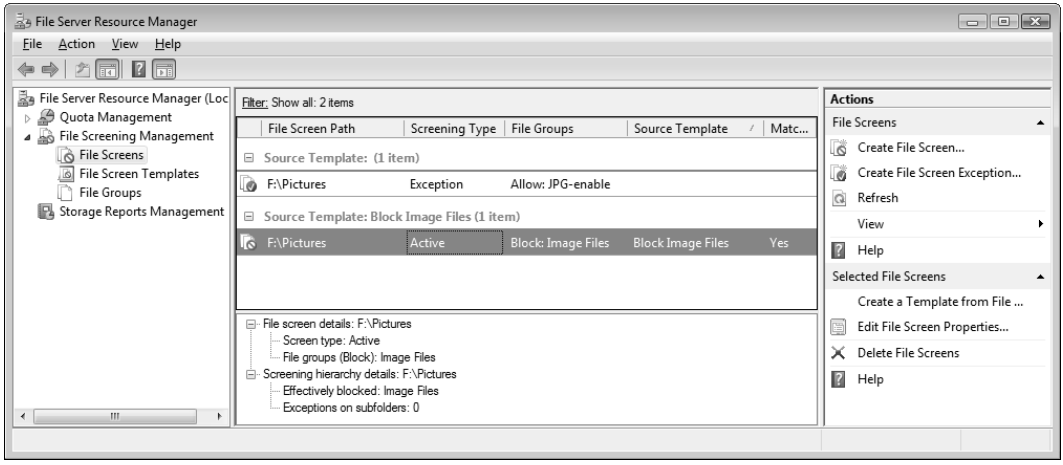


Рис. 4.39. Активные фильтры блокировки файлов

В папке **File Groups** (Группы файлов) (рис. 4.38) 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. 4.39). 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.

Анализ использования дисковых ресурсов

В папке **Storage Reports Management** (Управление ресурсами хранилища) (рис. 4.40) можно создавать запросы на получение отчетов с заданными критериями для дисковых томов или папок.

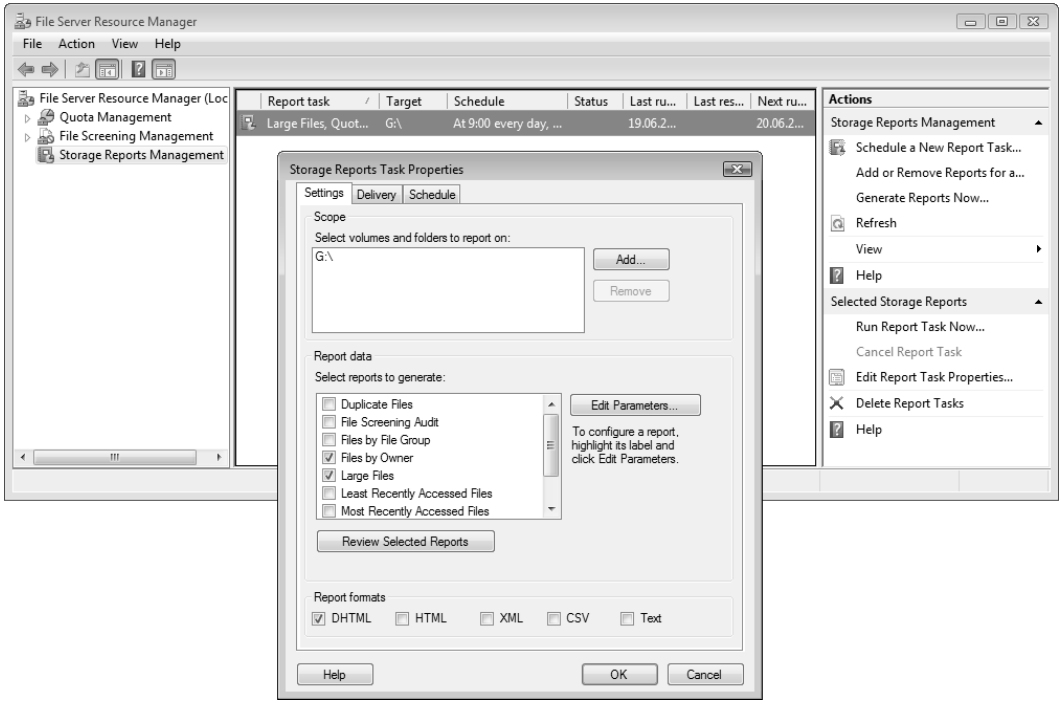


Рис. 4.40. Запланированные запросы и свойства запроса на получение отчетов

Эти запросы могут быть разовыми и тут же выполняться, а 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), определяются типы генерируемых отчетов (вкладка **Settings**) и их пара-

метры (**Edit Parameters**), задаются получатели отчета (вкладка **Delivery**). Для планируемых запросов также определяется расписание (вкладка **Schedule**).

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. 4.32).

Созданные отчеты представляют собой весьма информативные документы (обычно в формате HTML), содержащие таблицы, цветные диаграммы, аналитическую информацию и т. п. Их очень легко просматривать, и можно быстро принимать решения на основе собранных данных.

Настройка параметров доступа к общим сетевым папкам и принтерам

Если даже на сервере и разрешен общий доступ к папкам и принтерам, то 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 отчасти 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.

Нужные для работы сетевые параметры и настройки безопасности проще всего выбрать с помощью средств Центра управления сетями и общим доступом (Network and Sharing Center) *(см. главу 6)*. В его главном окне (рис. 4.41) видны 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 щелкните по стрелке, расположенной справа от индикатора текущего состояния.

Совокупность перечисленных ниже опций позволяет определить необходимые и безопасные параметры доступа к общим ресурсам, а также быстро менять их при подключении к другим сетям. (Можно проследить за тем, какие параметры бранд-

мауэра меняются, если открыть вкладку **Exceptions** (Исключения) (см. рис. 6.45) *до* изменения опций доступа и *после* него.)

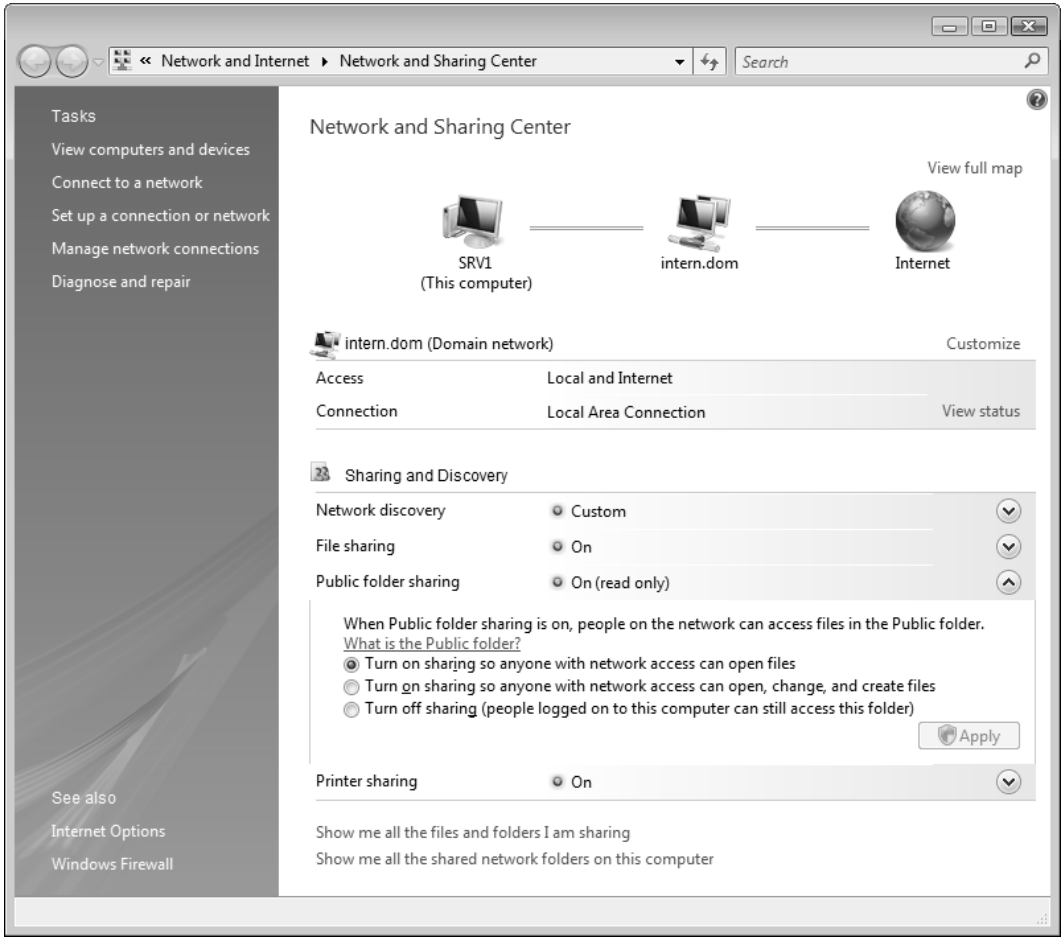


Рис. 4.41. Настройка доступа к общим ресурсам

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 на вкладке **Exceptions** (Исключения) в окне параметров брандмауэра Windows сбрасывается флажок **File and Printer Sharing** (Общий доступ к файлам и принтерам), 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. 4.41). 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. 4.42). При отключении парольной защиты доступ к общим ресурсам получают *любые* пользователи (поскольку разблокируется учетная запись Guest (Гость)).

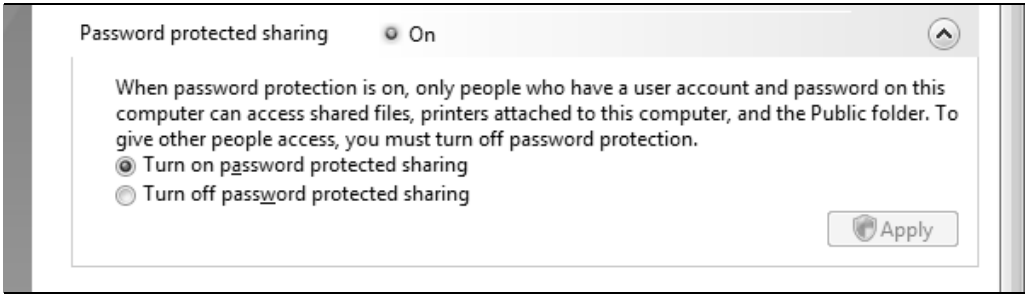


Рис. 4.42. Выбор доступа с парольной защитой

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). Сравните этот список ресурсов с результатами, получаемыми при помощи команды `net share`. Для понимания принципов управления доступом полезно также проанализировать изменения в этом окне, когда будут переопределяться опции доступа в окне Центра управления сетями.

Распределенная файловая система DFS

Распределенная файловая система (Distributed File System, DFS) упрощает управление данными в сети и облегчает их поиск. Она позволяет объединить файловые

[1] В русскоязычных версиях это неудачный перевод, сбивающий с толку: имеется в виду не доступ к общим папкам *вообще*, а доступ к стандартной папке **Public** (Общие) *(см. главу 2)*.

ресурсы, находящиеся на различных компьютерах, в единое пространство имен. Благодаря DFS пользователи работают не с физической сетью, состоящей из большого количества машин с собственными именами и общими папками, а могут видеть единую структуру логических имен общих файловых ресурсов.

В системах Windows Server 2008 средства управления DFS стали проще, поэтому администратор может без особых усилий развернуть пространство имен DFS и обеспечивать его связь с физическими объектами.

Установка компонентов DFS и начальное конфигурирование

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. 4.1):

- *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 же, с помощью мастера, создать пространство имен DFS. 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 (убедитесь в том, что это соответствует вашим планам). При использовании оснастки **DFS Management** (Управление DFS) корень можно создавать на любом доступном сервере.

На начальном этапе мастер установки просит ввести *имя* пространства имен. В дальнейшем это имя будет фигурировать в качестве основного логического названия общего ресурса.

На следующем шаге (рис. 4.43) 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.

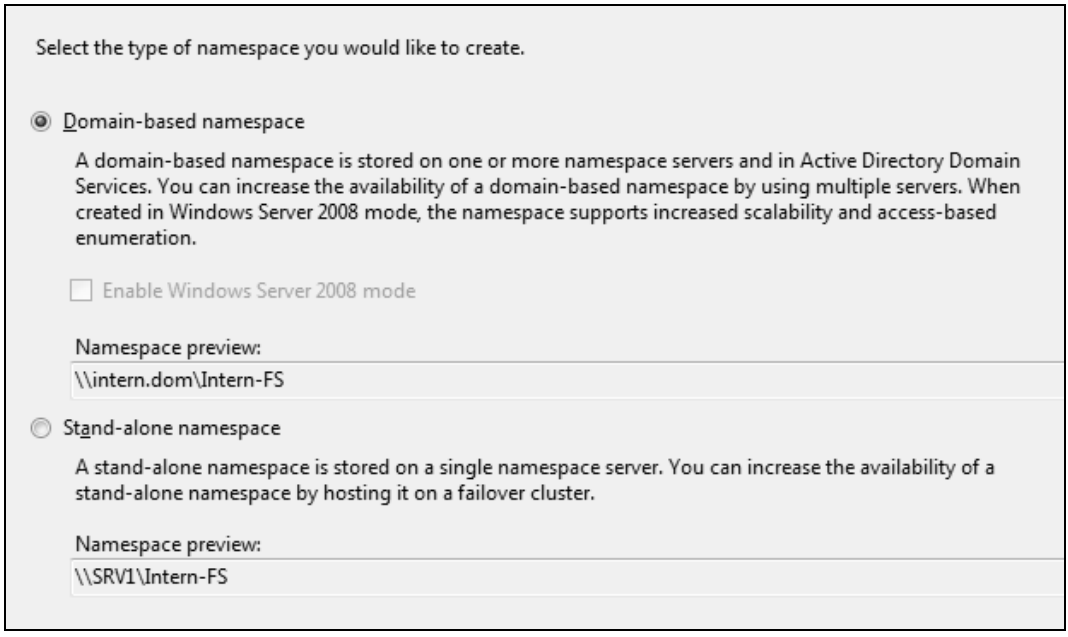


Рис. 4.43. Выбор типа пространства имен DFS

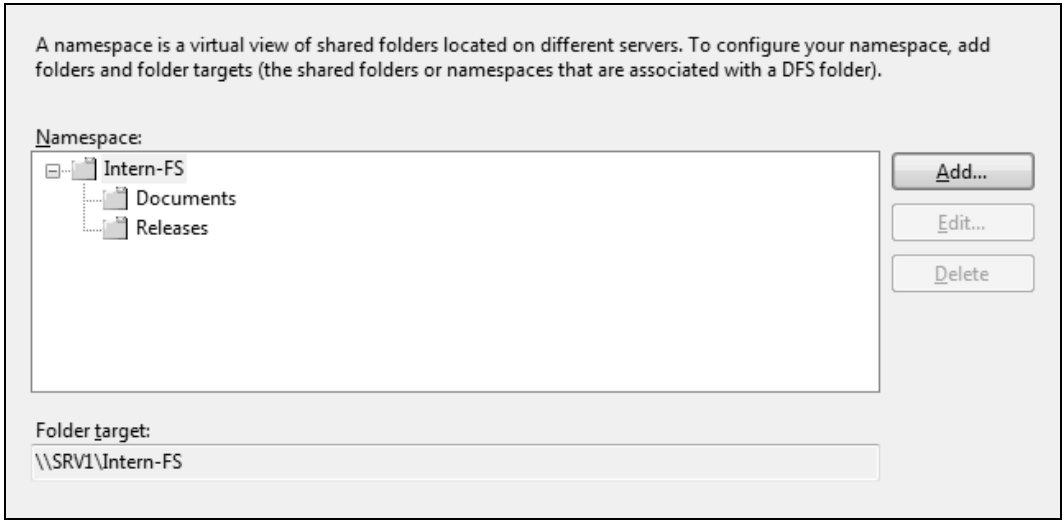


Рис. 4.44. Создание папок,
входящих в новое пространство имен DFS

Затем мастер позволяет создать папки DFS — виртуальные каталоги, связанные с общими папками, хранящимися на различных серверах (рис. 4.44). При добавлении папок (кнопка **Add**) необходимо в формате \\<*имяСервера*>\<*имяОбщейПапки*> указывать имя реального общего ресурса и произвольное имя папки в пространстве имен DFS (рис. 4.45). После того как пространство папок DFS будет хотя бы частично сформировано, можно нажать кнопку **Install** (Установить) и начать установку и конфигурирование служб DFS.

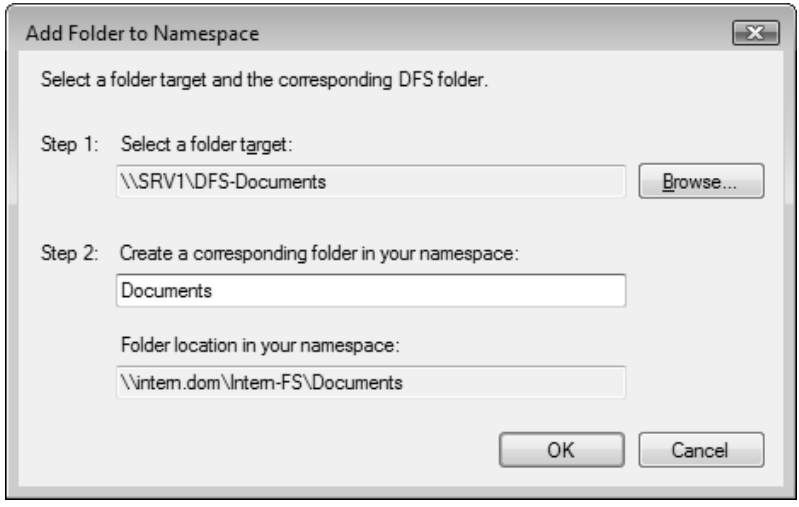


Рис. 4.45. Выбор общей папки и определение ее имени в пространстве имен DFS

Управление DFS

Управление распределенной файловой системой выполняется централизованно с помощью оснастки **DFS Management** (Управление DFS; dfsmgmt.msc) (рис. 4.46), 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.

При первом запуске оснастки **DFS Management** (Управление DFS) на ее главной странице (см. рис. 4.46) 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.

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).

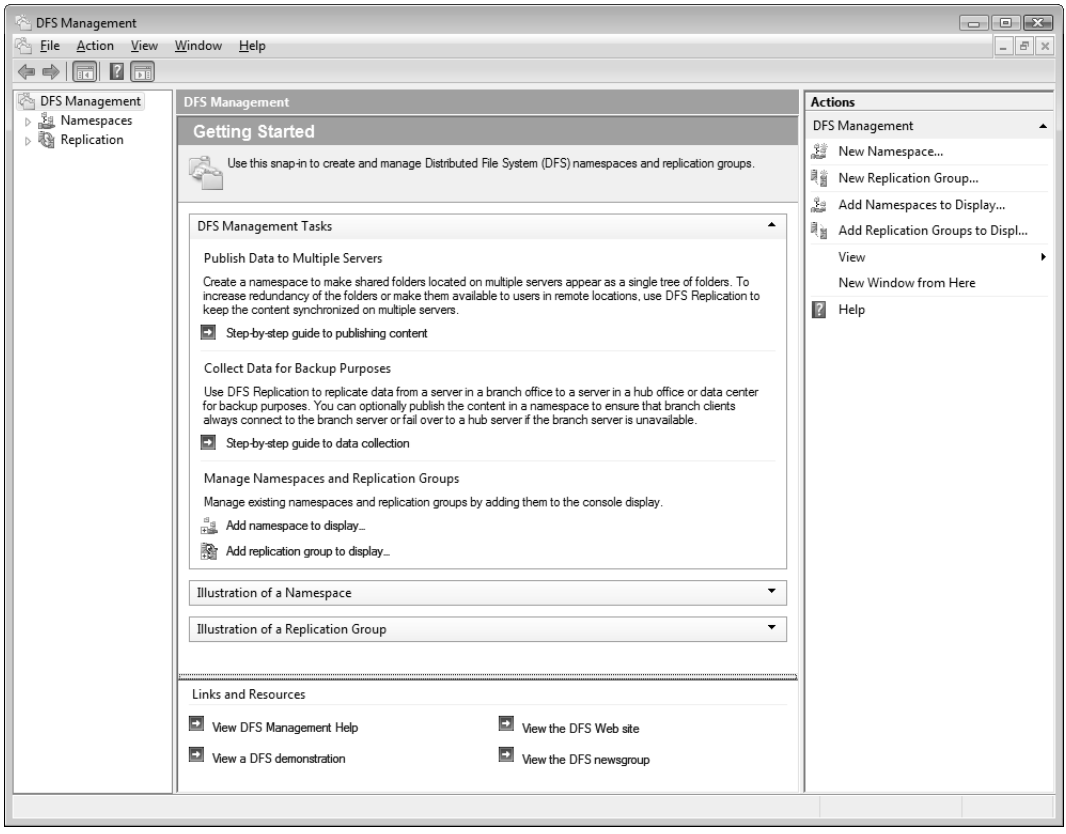


Рис. 4.46. Главная страница оснастки **DFS Management**

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 выполните следующие операции:

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. На следующей странице мастера выберите компьютер, который будет выполнять роль сервера пространства имен.

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.

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).

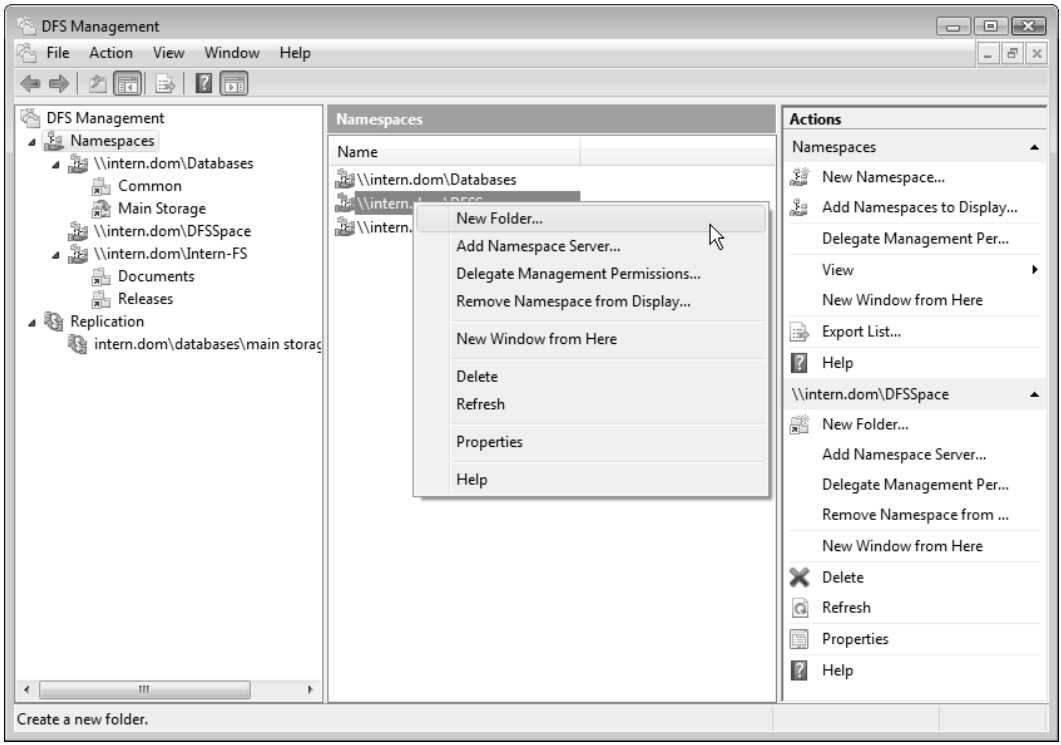


Рис. 4.47. Примеры пространств имен, открытых в окне оснастки **DFS Management**

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. 4.47 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.

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).

Для создания дополнительной папки DFS требуются следующие операции:

1. Укажите пространство имен и в контекстном меню выберите команду **New Folder** (Создать папку) (см. рис. 4.47).
2. В окне **New Folder** (Создать папку) (рис. 4.48) 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.

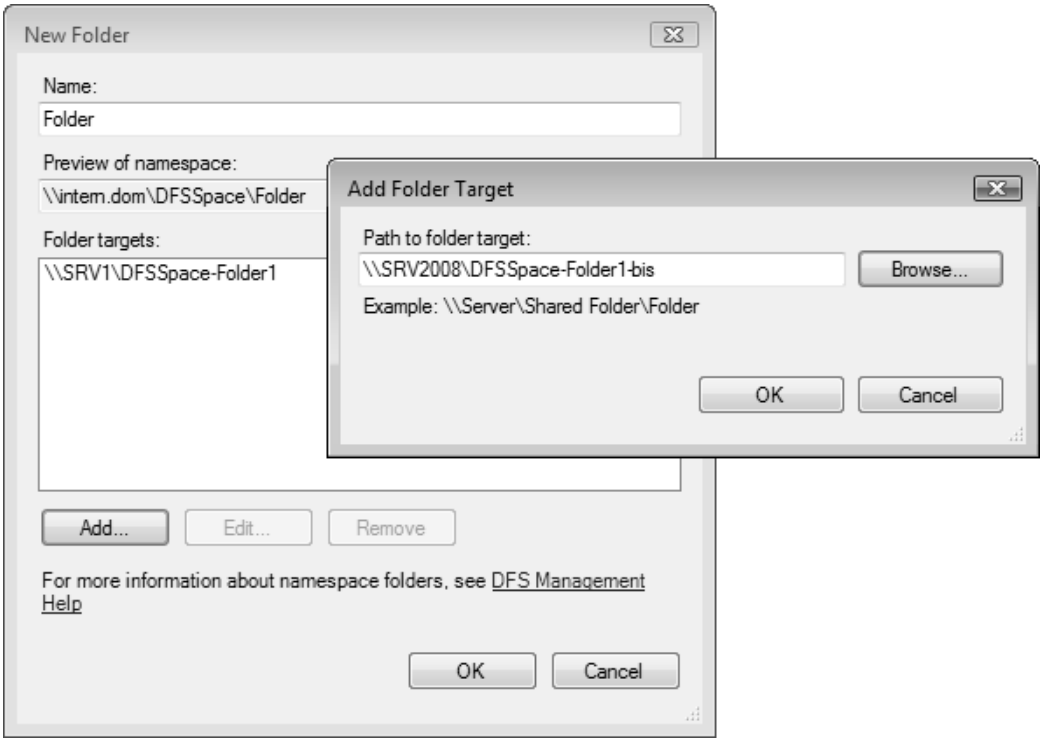


Рис. 4.48. Создание дочернего логического имени (папки) DFS

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, выберите общую папку — после этого мастер предложит создать группу репликации для синхронизации указанных папок.
3. В случае согласия на следующем шаге укажите произвольное имя для группы репликации.

4. Проверьте правильность параметров для папок, выбранных в качестве участников репликации DFS (рис. 4.49) (в этом окне не должно быть сообщений об ошибках). При необходимости можно вернуться назад и выбрать другие папки.

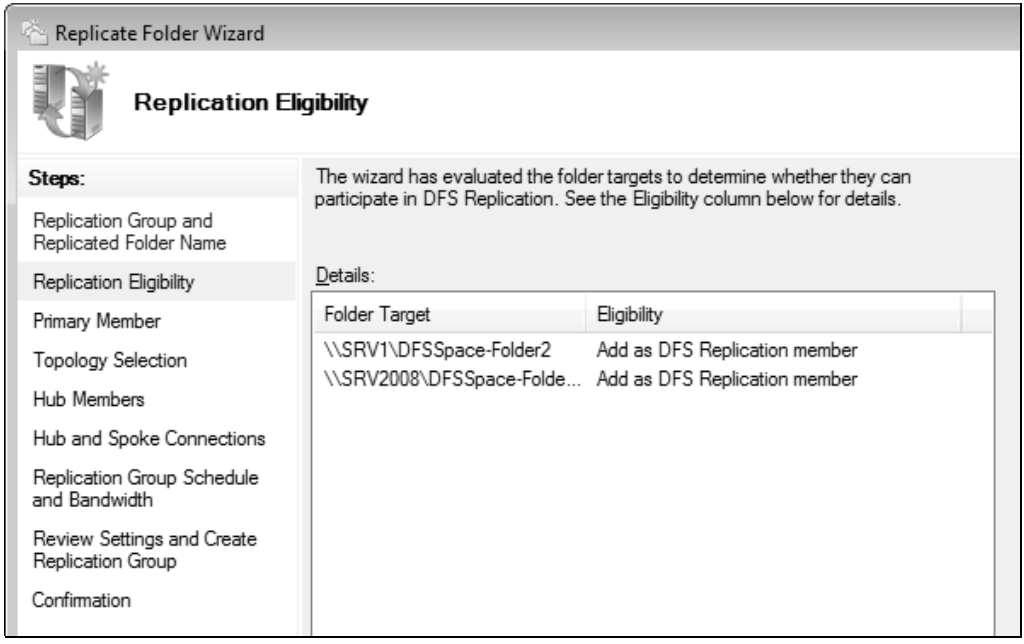


Рис. 4.49. Просмотр папок, выбранных в качестве членов группы репликации

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 впоследствии изменить в любой момент, выбрав группу репликации в папке **Replication** (Репликация).
7. На следующем шаге укажите (при необходимости) скорость, с которой будет выполняться репликация, или выберите 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. 4.50). В случае возникновения ошибок на вкладке **Errors** (Ошибки) появится их подробное описание. В этом случае необходимо внести коррективы и повторить операцию.

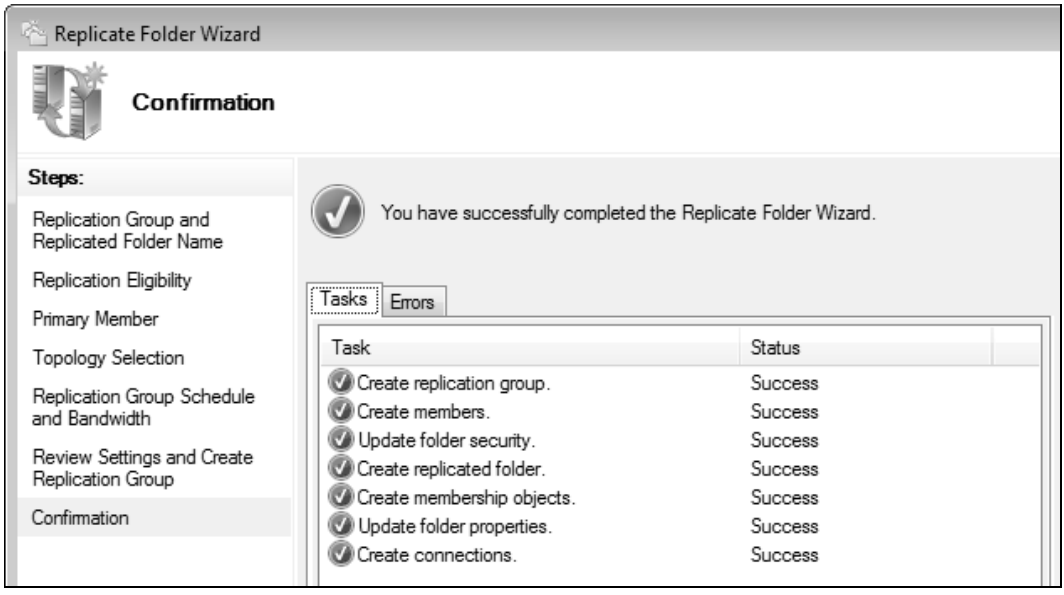


Рис. 4.50. Предупреждение о необходимости настройки репликации для альтернативного ресурса

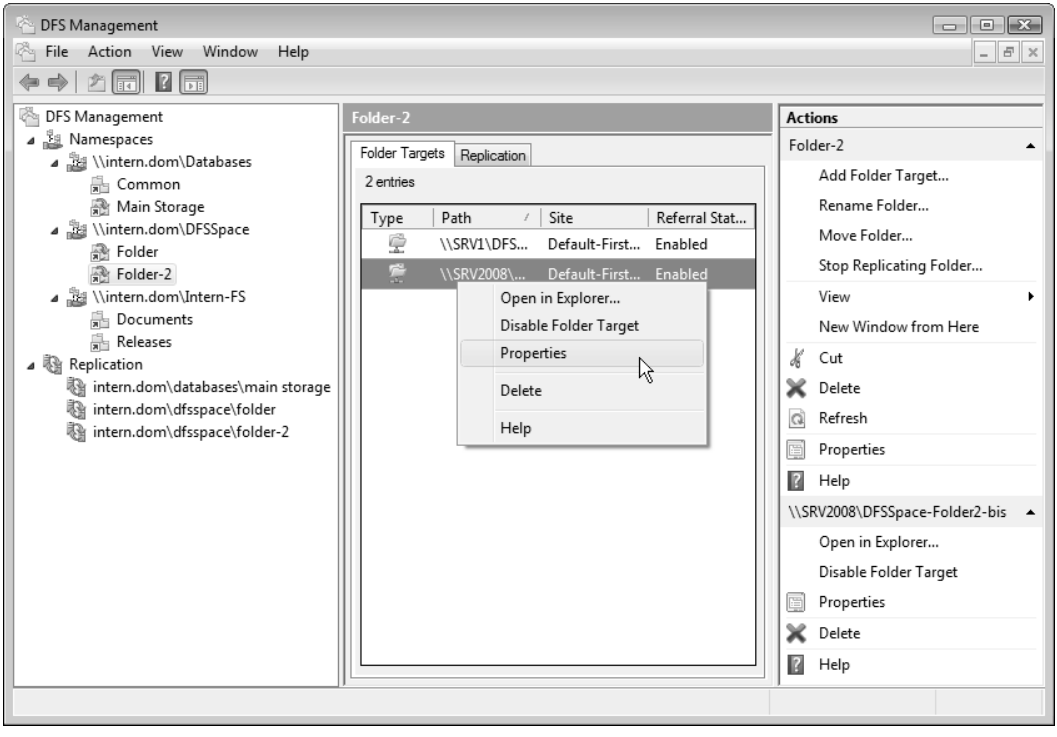


Рис. 4.51. Просмотр конечных объектов для выбранной папки DFS

Теперь при выборе папки DFS в окне оснастки будет видно, что для нее имеются два конечных объекта (рис. 4.51) и возможна репликация между ними. Любую конечную общую папку можно открыть в окне программы Windows Explorer (Проводник) (команда **Open in Explorer**). На показанном рисунке обратите внимание на набор команд, имеющихся для выбранного объекта на панели **Actions** (Действия). С их помощью легко управлять конфигурацией конечных объектов.

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).

Когда пользователь подключается к общему ресурсу, представленному корнем DFS или одной из папок, в окне свойств этого ресурса он увидит новую вкладку — **DFS** (рис. 4.52), 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.

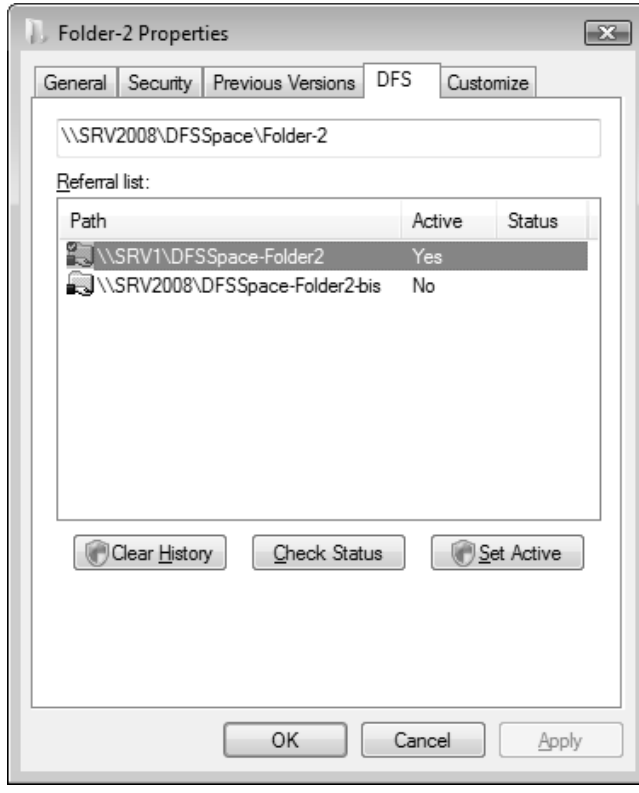


Рис. 4.52. Окно свойств файлового ресурса, представленного ссылкой DFS, имеющей две реплики

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. 4.53). 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)).

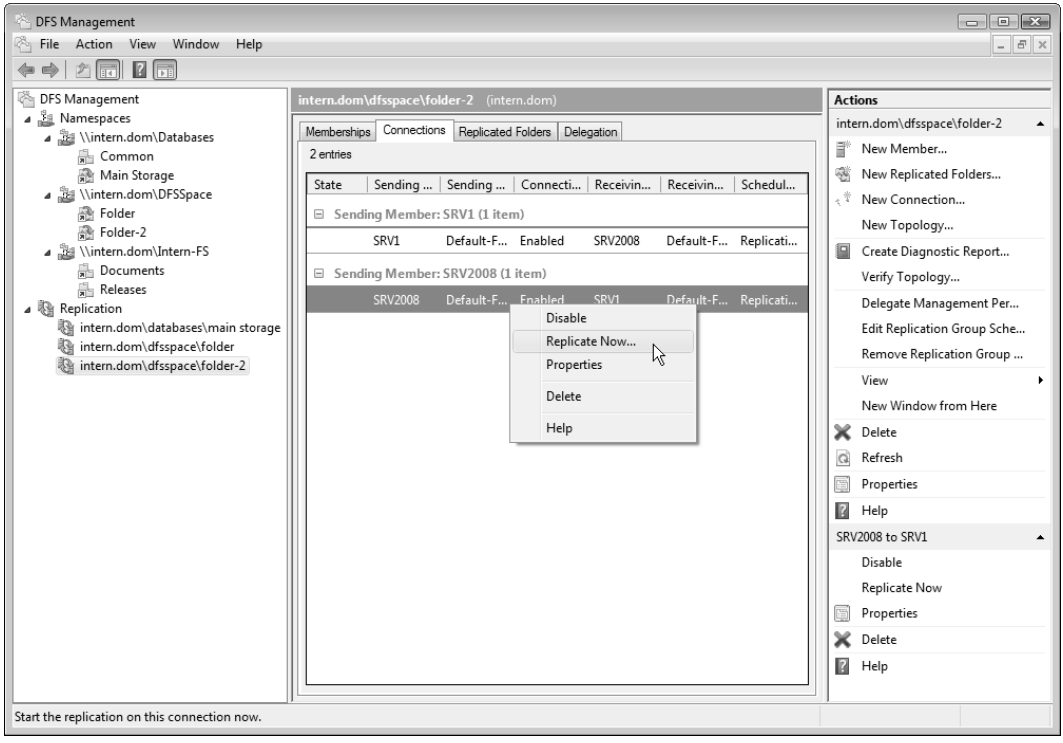


Рис. 4.53. Окно связей репликации альтернативных общих папок

Важной операцией является проверка топологии, запускаемая с панели **Actions** (Действия) с помощью соответствующей команды (ссылка **Verify Topology**). Команда настройки расписания репликации (ссылка **Edit Replication Group Schedule**) позволяет просмотреть и скорректировать время синхронизации конечных 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. 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.

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.

> ***Примечание***
>
> Для централизованной настройки параметров EFS можно использовать групповые политики.

Обязательные требования при выполнении операций шифрования

Главной ошибкой при работе с EFS является переустановка операционной системы на автономных компьютерах, где пользователи шифровали данные, но не выполнили дополнительных операций по сохранению сертификатов. В этом случае ***данные будут безвозвратно утеряны***, поскольку изначально 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 информа-

цию. 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.
>
> Управление сертификатами, их импорт и экспорт осуществляются с помощью оснастки **Certificates** (Сертификаты). Пользователи, включая администратора, могут управлять только своими собственными сертификатами. Оснастка позволяет видеть личные сертификаты пользователя — в частности, сертификат, который система автоматически выдала пользователю (от его имени) при первом выполнении операции шифрования файла или папки. Назначение сертификата отображается в соответствующем столбце (Intended Purposes).

Для того чтобы избежать ошибок, связанных с отсутствием экспортированного сертификата пользователя, зашифровавшего информацию, в системах Windows Vista/Windows Server 2008 появились дополнительные меры по защите от подобных ситуаций. Рассмотрим их работу на конкретном примере.

Шифрование файлов и папок

Поскольку операция шифрования выполняется автоматически и "прозрачно" для пользователя, работа с файлом продолжается так же, как и до включения криптозащиты. Однако 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).

3. В группе **Compress or Encrypt attributes** (Атрибуты сжатия и шифрования) установите флажок **Encrypt contents to secure data** (Шифровать содержимое 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. 4.54. Предупреждение системы EFS

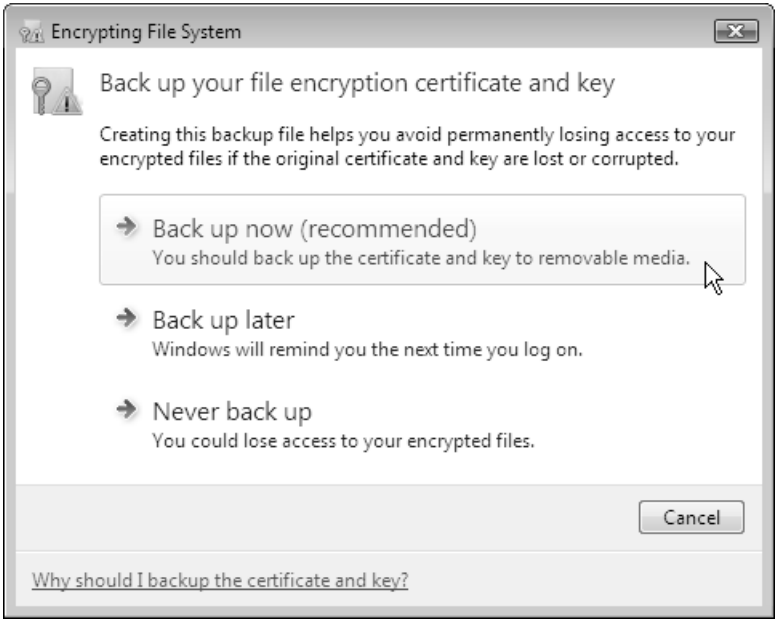


Рис. 4.55. Запрос на экспорт ключа EFS

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. 4.54). (Это предупреждение появляется только при первом выполнении операции шифрования данных, но 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).

Если щелкнуть по значку EFS на панели задач, то появится окно, в котором следует выбрать опцию **Back up now** (Архивировать сейчас) (рис. 4.55). 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. 4.56), 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.

Теперь при необходимости сохраненный сертификат можно при помощи оснастки **Certificates** (Сертификаты) и операции импорта установить в любой системе и использовать для дешифрования данных.

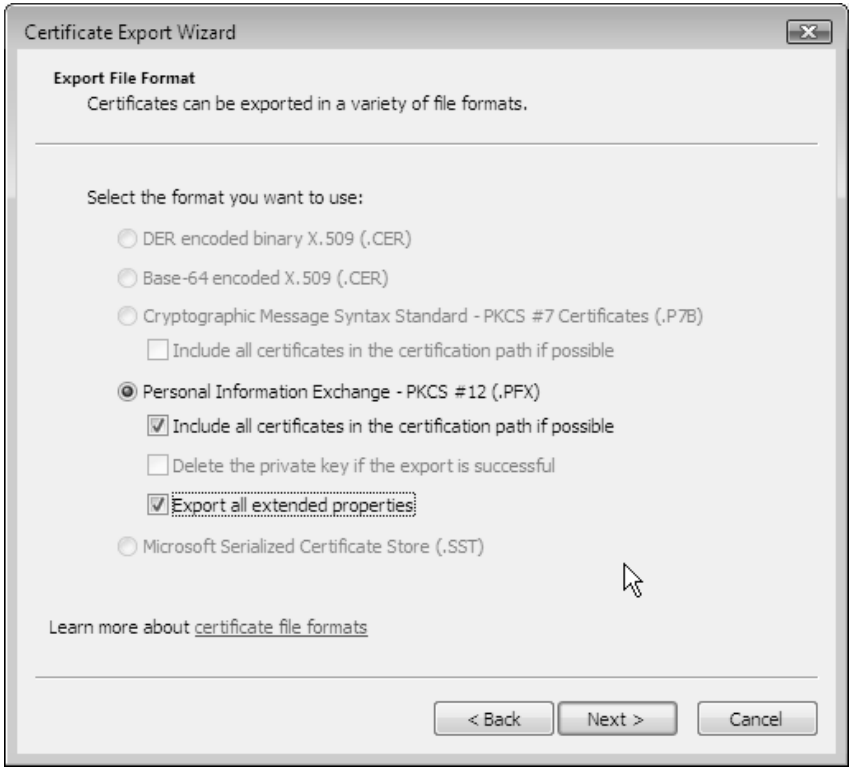


Рис. 4.56. Параметры экспортируемого ключа EFS

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.

В системах Windows Server Core шифрование *поддерживается* файловой системой NTFS, однако средства управления EFS (включая утилиту cipher.exe) отсутствуют. Таким образом включать и выключать шифрование файлов и папок можно, но только при подключении к дисковым ресурсам с удаленного компьютера.

Шифрование файлов для совместного использования

Системы Windows Server 2008 поддерживают совместный доступ к зашифрованным *файлам*, расположенным на общих сетевых ресурсах или на локальных дисках. Дополнительные разрешения можно давать только для каждого отдельного файла — совместный доступ к зашифрованным *папкам* разрешать нельзя.

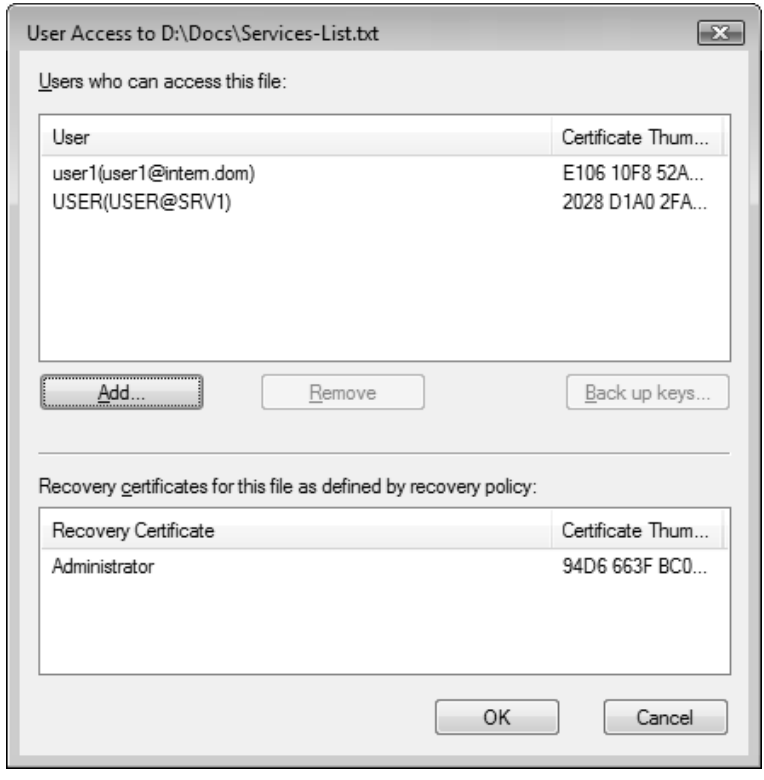


Рис. 4.57. Список пользователей, имеющих доступ к зашифрованному файлу

Внимание!

Перед тем как разрешать совместный доступ к зашифрованным файлам, необходимо предварительно импортировать сертификат нового пользователя.

После того как владелец-создатель зашифровал папку со вложенными файлами или отдельный файл, он может снова открыть окно **Advanced Attributes** (Дополнительные атрибуты) *(см. выше)* и нажать кнопку **Details** (Подробно). Появится окно, аналогичное изображенному на рис. 4.57. 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 указать, какие пользователи смогут также работать с зашифрованным файлом. 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 5*. В процессе архивации зашифрованные данные будут скопированы на указанный носитель без дешифрования.



Глава 5

Архивация и восстановление информации

Средства резервного копирования и восстановления информации в системах Windows Server 2008 претерпели капитальное обновление по сравнению с предыдущими версиями Windows (включая Windows Vista). 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).

> ***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 отключены; для того чтобы ими можно было пользоваться, необходимо с помощью оснастки **Server Manager** (Диспетчер сервера) 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.

> ***Внимание!***
>
> 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).

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 лучше проконтролировать этот момент, особенно при первом запуске). Чтобы оснастка **Windows Server Backup** (Система архивации данных Windows Server) могла подключаться к удаленным компьютерам, установите в брандмауэре исключение *Remote Administration* (Удаленное администрирование).

Для установки элементов системы архивации можно также использовать утилиту *ServerManagerCmd.exe*. (Этот путь является единственным для Windows Server Core.) С помощью команды `ServerManagerCmd -query` легко получить названия компонентов:

```
[ ] Windows Server Backup Features  [Backup-Features]
    [ ] Windows Server Backup  [Backup]
    [ ] Command-line Tools  [Backup-Tools]
```

Основные элементы устанавливаются с помощью команды `ServerManagerCmd -install Backup`.

В системе Hyper-V Server список компонентов легко получить с помощью команды `oclist`. Система архивации устанавливается с помощью следующей команды:

```
start /w ocsetup WindowsServerBackup
```

Для удаления компонента в команду нужно добавить параметр `/uninstall`.

Способы архивации и восстановления данных и системных файлов

В системах Windows Server 2008 набор средств, обеспечивающих архивацию и восстановление данных и системных файлов, минимален, однако он позволяет устранить любую аварийную ситуацию, возникшую при работе сервера. Доступ ко всем возможностям обеспечивает оснастка **Windows Server Backup** (Система ар-

хивации данных Windows Server. wbadmin.msc) или утилита командной строки *Wbadmin.exe*. Функции системы архивации перечислены в табл. 5.1.

Таблица 5.1. *Возможности системы архивации данных в Windows Server 2008*

Сохраняемая информация	**Используемое средство**	**Способ применения**
Персональные файлы пользователей и данные прикладных программ	Архив тома	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
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 всех старых версий данных

В системах Windows Server 2008 архивируемую информацию можно сохранять на следующих носителях:

- ❒ жесткие диски (внутренние и общие сетевые);
- ❒ съемные диски (USB, FireWare и т. п.);
- ❒ записываемые и перезаписываемые DVD-диски.

Нельзя копировать архивы на ленту. Архивируются только тома, имеющие файловую систему NTFS.

Архив представляет собой файл в формате VHD; кроме того, в целевой папке создаются служебные XML-файлы, необходимые для работы системы архивации.

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).

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.

С использованием службы VSS тесно связана функция, называемая *Previous Versions* (Предыдущие, или прежние, версии), — она будет рассматриваться далее в отдельном разделе этой главы. Ранее аналогичная возможность называлась *Shadow Copies* (Теневые копии).

Средства управления системой архивации в Windows Server 2008

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). Основным инструментом является оснастка **Windows Server Backup** (Система архивации данных Windows Server; wbadmin.msc) (ее аналог при работе в окне командной строки, включая Windows Server Core и Hyper-V Server, — утилита *Wbadmin.exe*).

Окно оснастки **Windows Server Backup** (Система архивации данных Windows Server) представлено на рис. 5.1. В нем легко видеть текущее состояние служб — на панели **Status** (Состояние) отображается время последней и очередной операции архивации, количество выполненных операций и их результат (в поле **Messages**). Дважды щелкнув по выделенной строке, можно получить подробную информацию о параметрах операции. Список выполненных операций архивации и восстановления обновляется даже в том случае, если операция запускалась из командной строки с помощью утилиты Wbadmin. Наличие запланированных архиваций и параметры используемого для этого физического диска показаны на панели **Scheduled Backup** (Архивация по расписанию).

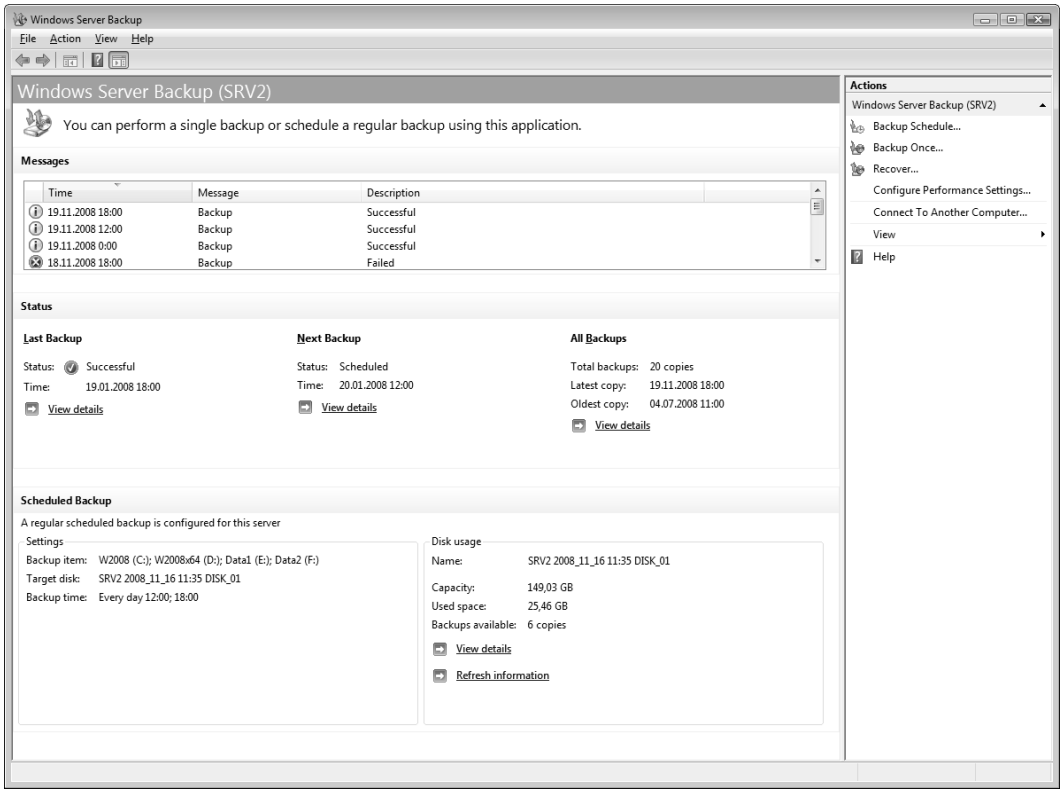


Рис. 5.1. Окно оснастки **Windows Server Backup**

С помощью ссылок на панели **Actions** (Действия) запускаются операции архивации и восстановления (они будут рассмотрены позже). Оснастку можно подключать как к локальному, так и к удаленному компьютеру (это касается полных версий, а также Windows Server Core и Hyper-V Server).

Ссылка **Configure Performance Settings** (Настройка параметров производительности) позволяет перейти в окно, где указывается тип архивирования — полный (full) или инкрементный (добавочный, incremental) — для каждого тома. При необходимости можно выбрать индивидуальные параметры в зависимости от нагрузки на конкретный диск.

Архивация 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).

Настройка автоматической архивации томов

Автоматическое резервное копирование критических и некритических томов выполняется программой архивации в соответствии с установленным 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 по умолчанию не будет виден в окне программы Windows Explorer (Проводник) (поскольку ему не назначается буква диска); он применяется только в целях архивации и восстановления данных.

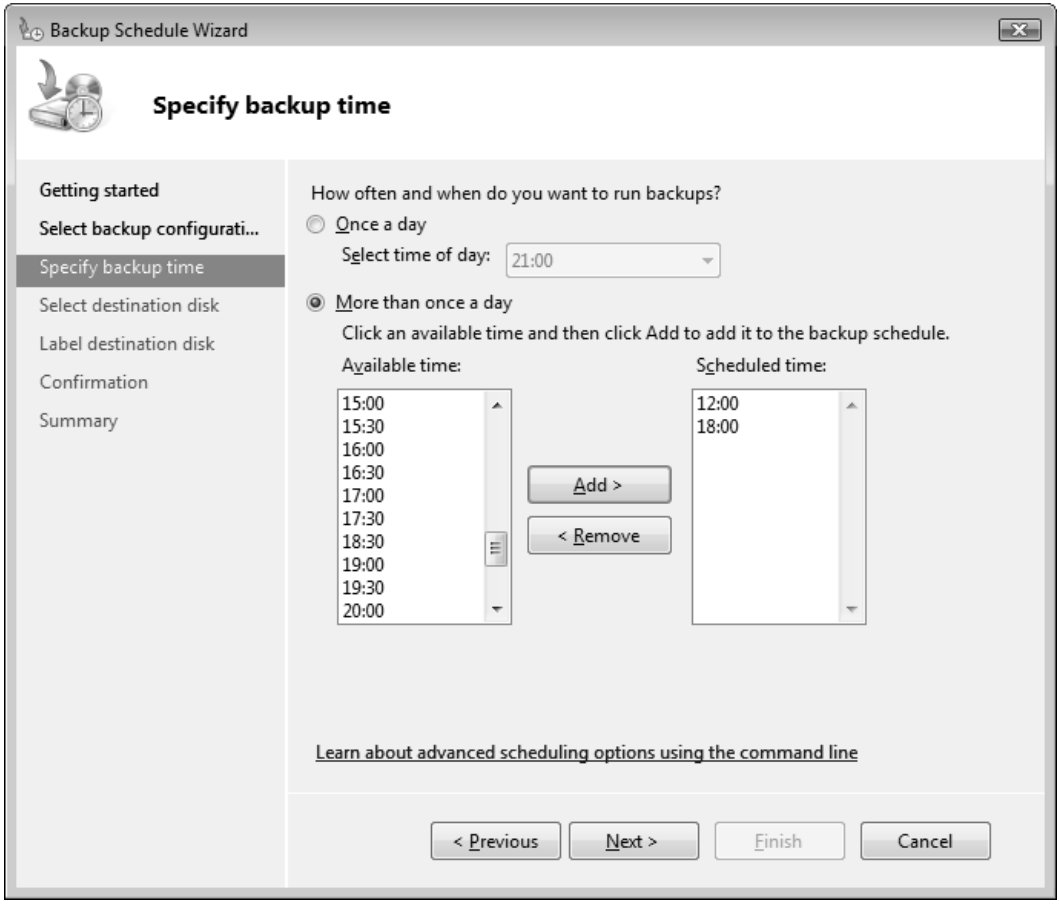


Рис. 5.2. Расписание автоматической архивации данных

Для настройки режима архивации по расписанию выполните следующие действия:

1. В окне оснастки **Windows Server Backup** (Система архивации данных Windows Server) (см. рис. 5.1) выберите ссылку **Backup Schedule** (Расписание архивации)

и следуйте указаниям мастера *Backup Schedule Wizard* (Мастер расписания архивации).

2. Сначала необходимо выбрать — весь сервер будет копироваться или только отдельные тома. В случае архивации отдельных томов укажите те тома, которые будут включены в архив.

3. Выберите расписание для выполнения процедуры автоматической архивации (рис. 5.2) (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 фактически 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.

4. Укажите физический диск для хранения архива. В начальный момент мастер может сообщить, что не найдены внешние диски или диски, подключенные к портам USE или FireWire. В этом случае нажмите кнопку **Show All Available Disks** (Показать все доступные диски) и в появляющемся окне выберите диск, подходящий для работы. Имя диска появится в окне **Available disks** (Доступные диски), где его следует отметить флажком (рис. 5.3). После нажатия кнопки **Next** (Далее) появится предупреждение о том, что ***все тома и данные на диске будут уничтожены*** — необходимо подтвердить правильность использования выбранного диска.

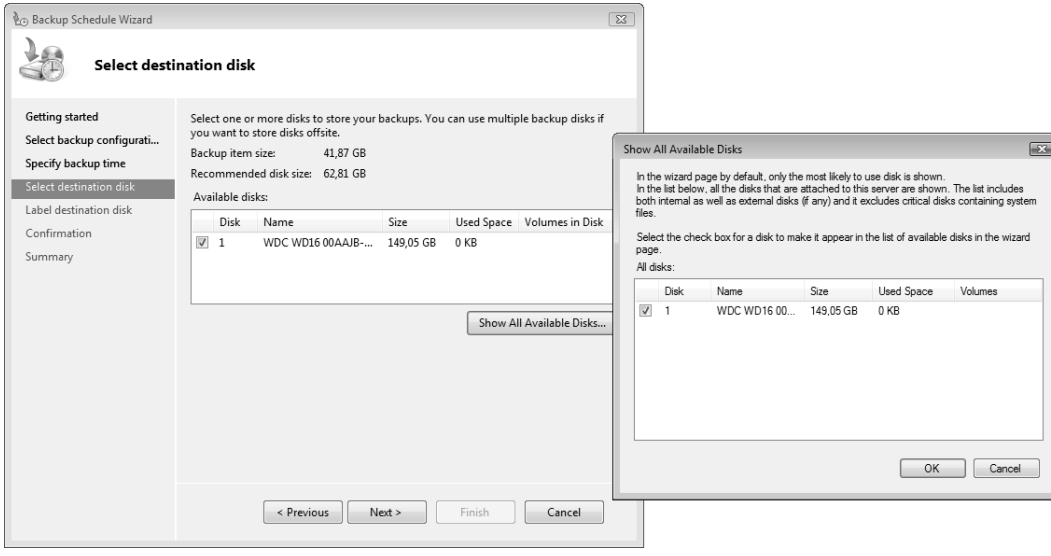


Рис. 5.3. Выбор целевого диска для хранения архивов, создаваемых по расписанию

5. 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.

6. На последнем этапе необходимо проверить правильность параметров и нажать кнопку **Finish** (Готово). 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.

При повторном запуске мастера Backup Schedule Wizard можно просмотреть все параметры автоматической архивации (это можно также сделать с помощью команды `wbadmin ENABLE BACKUP`), а также изменить их. Новые параметры будут учитываться при следующих запусках согласно расписанию.

Если при наличии сконфигурированного режима автоматической архивации выбрать ссылку **Backup Once** (Однократная архивация) и согласиться с выбором параметров, заданных для архивации по расписанию, то можно сразу же начать запланированную операцию.

Использование утилиты архивации

Для Windows Server Core и Hyper-V Server единственным инструментом для работы с системой архивации является утилита Wbadmin.exe.

Сначала следует проанализировать дисковую конфигурацию. Ниже в качестве примера приведены сообщения для системы с двумя дисками — внутренним (содержащим четыре тома) и внешним (пустым):

```
C:\>wbadmin GET DISKS

Disk name       : ST3160815AS ATA Device
Disk number     : 0
Disk identifier : {08260825-0000-0000-0000-000000000000}
Total space     : 149.05 GB
Used space      : 41.87 GB
Volumes         : C:[W2008],D:[W2008x64],E:[Data1],F:[Data2]


Disk name       : WDC WD16 00AAJB-00WRA0 USB Device
Disk number     : 1
Disk identifier : {e1f29bf5-0000-0000-0000-000000000000}
Total space     : 149.05 GB
```

```
Used space        : 0 bytes
Volumes           : Unable to get volume information.
```

Идентификатор диска требуется для настройки системы архивации. Например, чтобы на внешнем диске автоматически создавался полный архив (архив всех имеющихся томов), требуется выполнить следующую команду:

```
C:\>wbadmin ENABLE BACKUP -addtarget:{e1f29bf5-0000-0000-0000-000000000000}
-schedule:12:00,18:00 -include:C:,D:,E:,F:

wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Retrieving volume information...

The scheduled backup settings:

Volumes in backup: W2008(C:),W2008x64(D:),Data1(E:),Data2(F:)
Location to store backup: WDC WD16 00AAJB-00WRA0 USB Device
Times of day to run backup: 12:00, 18:00


Do you want to enable backups with the above settings?

[Y] Yes [N] No y


The scheduled backup is enabled.
```

В отличие от настройки с помощью оснастки **Windows Server Backup** (Система архивации данных Windows Server), указанный целевой диск не обязательно форматируется: если на нем уже имеются архивы, то утилита выдаст запрос и позволит сохранить их.

Параметры автоматической архивации можно посмотреть с помощью команды `wbadmin ENABLE BACKUP`. Команда `wbadmin START BACKUP` позволяет в любой момент запустить архивацию с заданными параметрами.

С помощью команды `wbadmin DISABLE BACKUP` автоматическая архивация отключается, и все параметры удаляются.

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. 5.1) выберите ссылку **Backup Once** (Однократная архивация) — запустится мастер *Backup Once Wizard* (Мастер однократной архивации).
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* — сделайте соответствующий выбор. (Далее будет рассматриваться случай с новыми индивидуальными параметрами.)
3. На следующем этапе указывается, какой архив будет создаваться — *полный образ* системы (опция **Full Server**) или архив *отдельных томов* (опция **Custom**). Образ всей системы будет занимать значительный объем, и это нужно учитывать при выборе целевой папки или носителя.

Совет

Если выбрать полный образ, но в качестве целевого указать один из присоединенных дисков, то содержимое этого диска будет исключено из архива и, следовательно, фактически получится архив остальных томов. Поэтому даже при использовании внешнего накопителя нужно сначала настроить автоматическую архивацию на этот диск, а потом принудительно выполнить однократную операцию.

4. При выборе опции **Custom** (Настраиваемый) можно указать, какие именно диски войдут в состав архива (рис. 5.4). 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 отдельные некритические тома.
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. (Полный 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.)

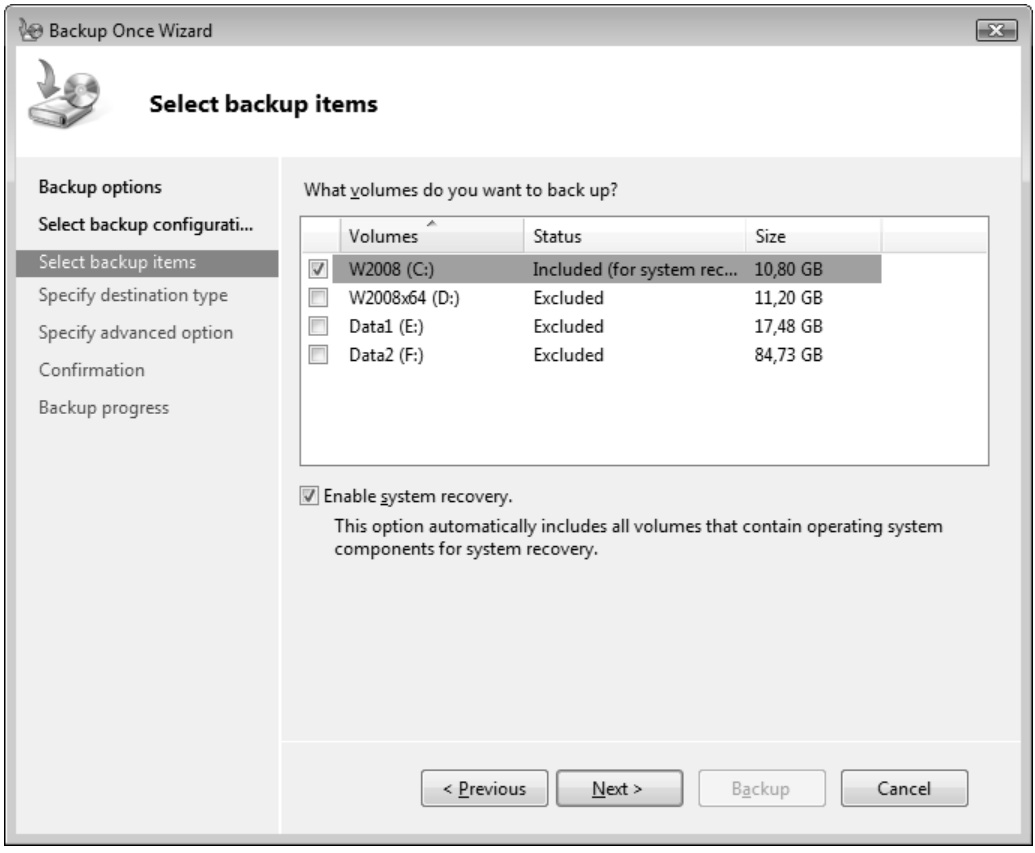


Рис. 5.4. Список дисков, которые будут включены в образ системы

Совет

Посмотреть, какие общие папки имеются на удаленном сервере, можно при помощи команды `net view \\<имяСервера>`.

6. На следующем шаге укажите 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 непосредственно в окне программы-мастера. Если это окно закрыть, то за выполнением операции можно следить в окне оснастки на панели **Messages** (Сообщения) или же в окне консоли, выполнив команду `wbadmin GET STATUS`.

В процессе 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 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.

Выполнение архивации из командной строки

Ниже приведен пример выполнения однократно операции архивации выбранного тома (D:) на удаленном компьютере (\\SRV2) в общей папке (\Data2) (в этом случае обязательно нужно указывать имя и пароль пользователя, имеющего право на выполнение операции для данного компьютера):

```
C:\>wbadmin START BACKUP -backupTarget:\\SRV2\Data2 -include:D:
-user:SRV2\administrator -password:psw

wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Retrieving volume information...

This would backup volume SYS(D:) to \\SRV2\Data2.

Do you want to start the backup operation?

[Y] Yes [N] No y


Backup to \\SRV2\Data2 is starting.

Creating the shadow copy of volumes requested for backup.

Running backup of volume SYS(D:), copied (0%).

Running backup of volume SYS(D:), copied (0%).

...
```

Нажав клавиши <Ctrl> + <C>, можно прервать вывод сообщений о ходе операции, при этом сама операция будет продолжаться. Увидеть ее текущее состояние позволяет команда `wbadmin GET STATUS`.

Если текущую операцию архивации или восстановления требуется прекратить, введите команду `wbadmin STOP JOB`.

Восстановление информации

Теперь можно рассмотреть операции, связанные с использованием созданных архивов. Помимо простого извлечения данных из архивов, в системах Windows Server 2008 имеется функция получения прежних версий файлов, которая для пользователя выглядит так же, как в Windows Vista (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. 5.1) 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 восстановлении файлов и папок можно указать конкретные объекты, которые требуется выбрать из архива (рис. 5.5). 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)).

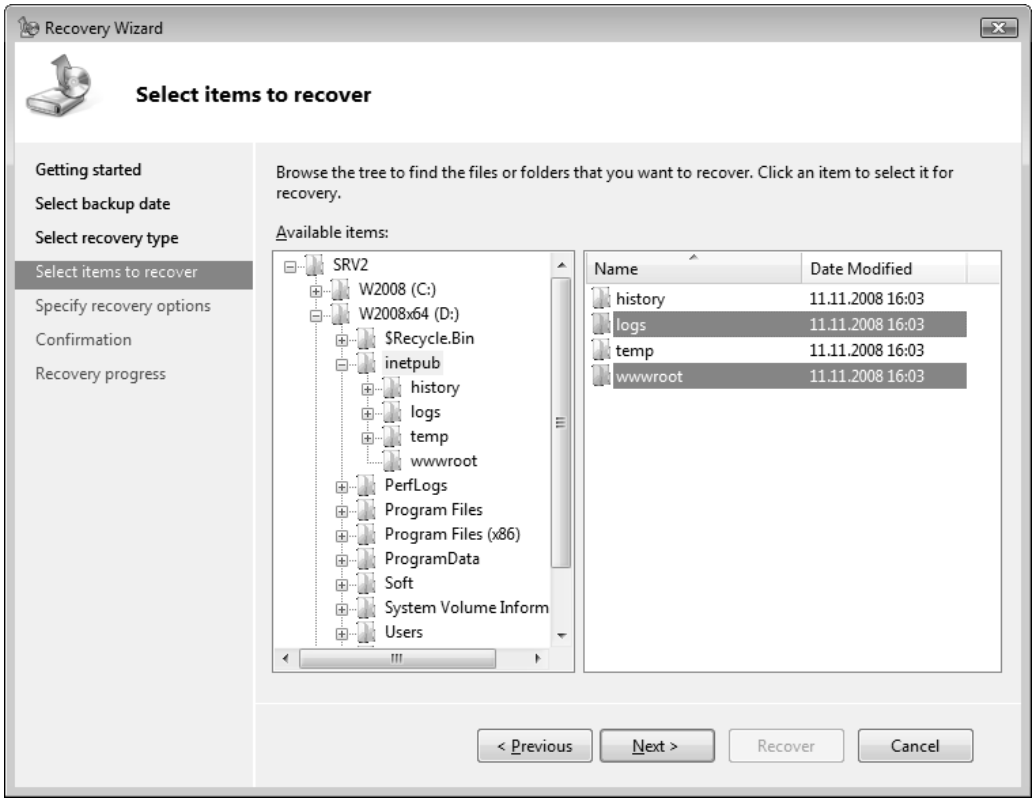


Рис. 5.5. Выбор отдельных файлов и папок для восстановления

6. Укажите местоположение для восстанавливаемых данных: файлы могут записываться в исходное место или в произвольно выбранную папку. 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 **Recover** (Восстановить).

Выполнение операции восстановления из командной строки

Эта операция требует некоторых предварительных действий.

Сначала с помощью команды `wbadmin GET VERSIONS` нужно посмотреть, какие архивы имеются в указанном месте (в удаленной папке, на физическом или логиче-

ском диске). Например, следующая команда позволяет увидеть список архивов, сохраненных на указанном томе (F:) — здесь нужно ориентироваться на идентификаторы версий:

```
wbadmin GET VERSIONS -backupTarget:F:
```

Затем можно просмотреть, какие элементы содержатся в конкретном архиве (хотя это и необязательно, если вы уверены, что нужная информация в архиве присутствует):

```
C:\>wbadmin GET ITEMS -version:11/20/2008-20:06

wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.


Volume Id = {493283ed-d0c5-11dd-93a3-806e6f6e6963}
Volume 'W2008', mounted at C:

Application = Registry

Component = Registry (\Registry)
```

Для восстановления элементов из архива необходимо, как минимум, указать идентификатор версии, тип элемента и список этих элементов. Например, следующая команда позволяет восстановить в исходное место указанный файл (C:\Docs\text.txt) и перезаписать имеющийся файл:

```
wbadmin START RECOVERY -version:11/20/2008-20:06 -itemType:File
-items:C:\Docs\text.txt -overwrite:Overwrite
```

Чтобы восстановить целиком том (C:), достаточно выполнить команду

```
wbadmin START RECOVERY -version:11/20/2008-20:06 -itemType:Volume -items:C:
```

Список дополнительных параметров команд можно получить, введя их название без дополнительных ключей.

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 пользователям сервера и сетевым клиентам, которые обращаются удаленно к общим папкам.

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 теневые (shadow) копии, то в окне свойств на вкладке

Previous Versions (Предыдущие версии) (рис. 5.6) можно увидеть список сохраненных вариантов файла или папки, просмотреть их и восстановить на исходное место (кнопка **Restore** (Восстановить)) или в альтернативную папку (кнопка **Copy** (Копировать)).

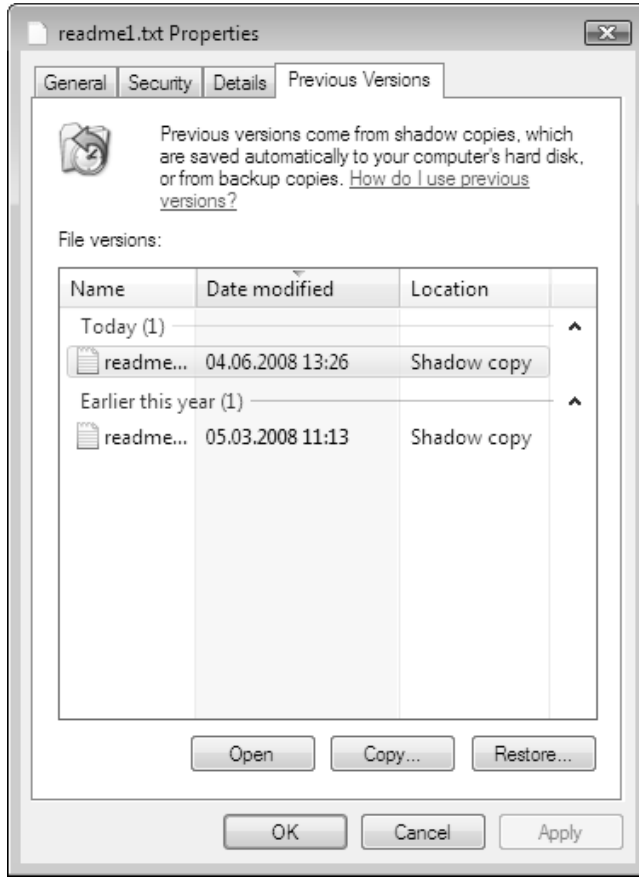


Рис. 5.6. Выбор предыдущей версии файла для восстановления или копирования

Однако для того чтобы функция предыдущих версий файлов заработала, 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). (Альтернативный вариант — запустить оснастку **Shared Folders** (Общие папки, fsmgmt.msc), открыть контекстное меню для корневого узла и выбрать аналогичную команду в подменю **All Tasks** (Все задачи).)

2. В списке томов, имеющихся на сервере (рис. 5.7), укажите нужный том и нажмите кнопку **Enable** (Включить).

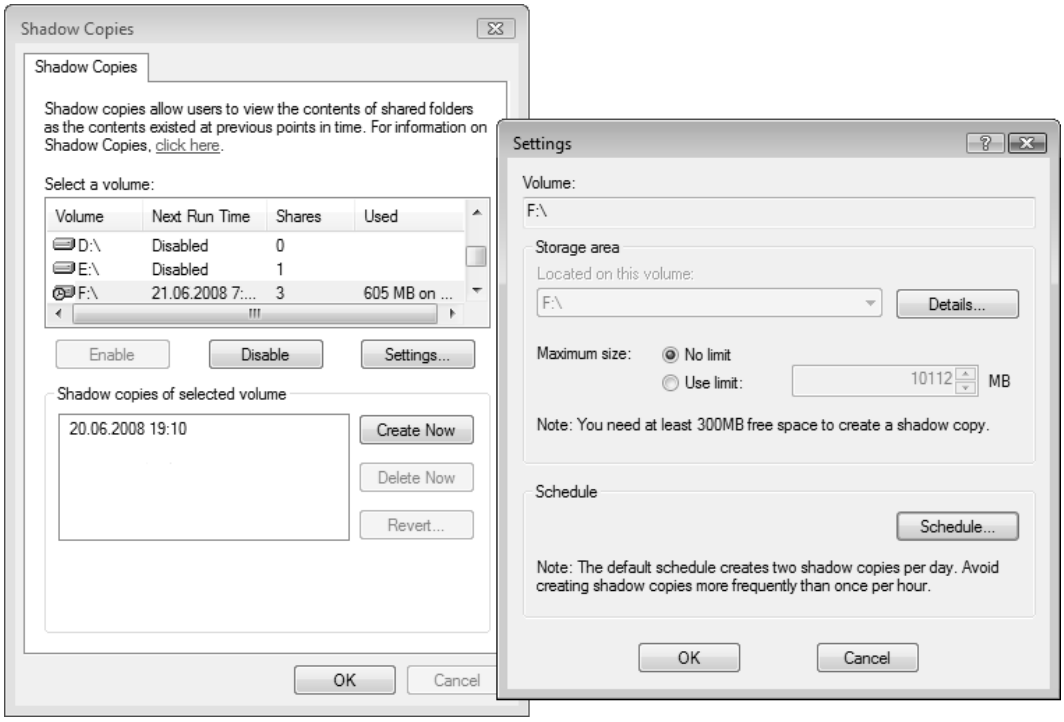


Рис. 5.7. Окно просмотра теневых копий, имеющихся на сервере, и окно параметров для выбранного диска

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. Поэтому стандартные параметры нужно проверить и при необходимости скорректировать.

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. 5.7) позволяет просмотреть параметры теневых копий для выбранного диска. 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. 1.5).

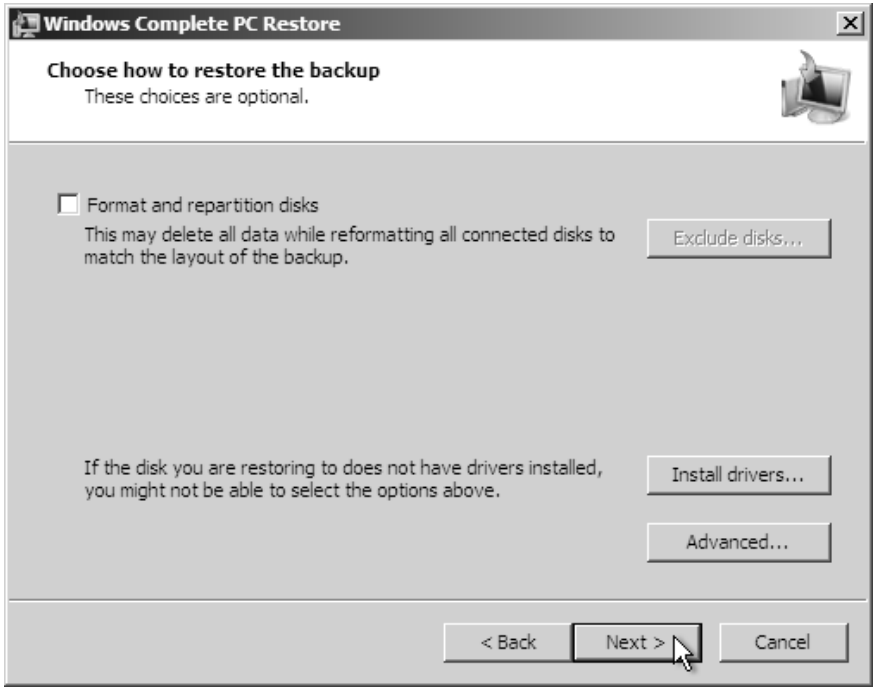


Рис. 5.8. Опция выполнения форматирования

3. В окне **System Recovery Options** (Параметры восстановления системы) (см. рис. 1.23) выберите опцию **Windows Complete PC Restore** (Восстановление архива Windows Complete PC).
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 образы на подключенных дисках, то необходимо уточнить, какой из архивов будет использоваться. (Автоматически выбирается самый "свежий" архив.)
5. После выбора архива нужно убедиться в правильности информации и определить состояние флажка, указывающего, будет ли выполняться разметка и форматирование дисков (рис. 5.8). 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. Если в состав полного архива входят критические и некритические тома, то в данном окне появится также флажок, при установке которого будут восстанавливаться только критические тома (те, которые необходимы для загрузки системы).

   Нажав кнопку **Advanced** (Дополнительно), можно определить параметры перезагрузки системы после восстановления и необходимость проверки дисков (по умолчанию обе операции выполняются).
6. В последнем окне мастера после нажатия кнопки **Finish** (Готово) 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.

Сохранение и восстановление состояния системы (System State)

Для сохранения состояния системы во всех версиях 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 рабочих файлов следует применять обычные архивные копии.

> ***Внимание!***
>
> В доменах Active Directory на базе Windows Server 2003 можно создавать дополнительные контроллеры домена, используя состояние системы, сохраненное с помощью программы архивации. В системах Windows Server 2008 для этих целей необходимо использовать утилиту Ntdsutil.exe *(см. главу 7)*.

Для сохранения состояния системы используется утилита командной строки Wbadmin. Ниже приведены сообщения, появляющиеся при выполнении операции с использованием локального тома (E:):

```
C:\>wbadmin START SYSTEMSTATEBACKUP -backupTarget:E:
...

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.
...

Search for system state files complete
Starting backup of files

...

Overall progress - 98% (Currently backing up files reported by 'System
Writer')
Backup of files reported by 'System Writer' completed
Overall progress - 99% (Currently backing up files reported by 'Registry
Writer')
Backup of files reported by 'Registry 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 additional system state files)
```

```
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'
```

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. Поскольку архив включает все системные файлы, операция сохранения состояния системы выполняется довольно долго, а сам архив занимает значительное место (свыше 5—6 Гбайт).

Для восстановления состояния системы используется команда `wbadmin START SYSTEMSTATERECOVERY`. Если ее запустить без дополнительных ключей, то выводится список необходимых параметров.

Глава 6



Сетевые компоненты и службы

Данная глава посвящена использованию систем Windows Server 2008 в сети и включает описание основных сетевых служб, которые применяются в сетях, построенных на базе стека протоколов TCP/IP. Будут охвачены все вопросы, необходимые для развертывания каждой службы в локальной сети.

Сначала мы рассмотрим основные понятия и типовые операции, необходимые при работе в сетевой среде (например, создание и настройка сетевых подключений). Затем описываются сетевые службы, которым в системах Windows Server 2008 соответствуют следующие роли сервера, добавляемые с помощью оснастки **Server Manager** (Диспетчер сервера):

- DHCP Server (DHCP-сервер)
- DNS Server (DNS-сервер)
- Network Policy and Access Services (Службы политики сети и доступа)

В этой последовательности мы и будем рассматривать службы более подробно.

В завершении главы описывается встроенный брандмауэр Windows, являющийся одним из главных средств обеспечения сетевой безопасности компьютеров, и даются примеры по настройке сетевых параметров и брандмауэра при работе в окне командной строки.

Сетевые средства, удаленные из Windows Server 2008

В системах Windows Vista и Windows Server 2008 прекращена поддержка некоторых протоколов и служб; перечислим их в алфавитном порядке:

- Asynchronous Transfer Mode (ATM);

- 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.

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 параметров утилиты легко получить, введя в командной строке имя утилиты без ключей.

Особенности использования некоторых сетевых компонентов

В составе систем Windows Server 2008 имеются следующие сетевые компоненты, утилиты и сервисы, 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 сетевым средствам, необходимо сначала установить соответствующие компоненты с помощью оснастки **Server Manager** (Диспетчер сервера).

Категории сетей (сетевое размещение) и профили встроенного брандмауэра

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).

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 настройки совместно используемых ресурсов и 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 тот или иной *профиль* (profile) — т. е. установленные для этой категории *исключения* (exceptions) или *правила* (rules) (если говорить о

расширенной конфигурации — *см. далее*), блокируя или, наоборот, открывая на вход или на выход 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 виден сам и не видит другие компьютеры в сети; есть доступ только к Интернету.

> ***Внимание!***
>
> В процессе работы следует следить за тем, какая категория сети выбрана, и не поменялась ли она из-за каких-то изменений в сетевой конфигурации или после перезагрузки системы. В противном случае — если выбраны более строгие параметры (общественная сеть) — могут возникнуть проблемы с видимостью компьютера в сети, доступом к общим ресурсам и т. п.

Если выбрать 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 4)*, 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 на компьютере в сетевой среде

Интерфейс управления сетевыми функциями в Windows Server 2008 заметно изменился по сравнению с Windows Server 2003[2]. Поэтому рассмотрим кратко основные особенности настройки сетевых параметров. Поначалу такой способ организации сетевых функций кажется непривычным, однако суть и количество операций по настройке сети практически не изменились по сравнению с предыдущими версиями Windows.

---

[1] Для Windows Vista категория сети указывается явно при установке и начальном конфигурировании системы.

[2] Впрочем, пользователям Windows Vista все новшества уже будут знакомы.

При наличии сетевого адаптера (с правильно установленными драйверами) система автоматически создает *подключение по локальной сети* (Local Area Connection) — его значок по умолчанию отображается на панели задач в области уведомлений. Если *навести* на него курсор мыши, то появится всплывающее окно, 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.)

Если *щелкнуть* по значку подключения по локальной сети, то появится окно (рис. 6.1), 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). Если щелкнуть по ссылке **Network and Sharing Center** (Центр управления сетями и общим доступом), то откроется главное окно всех сетевых настроек системы *(см. ниже)*.

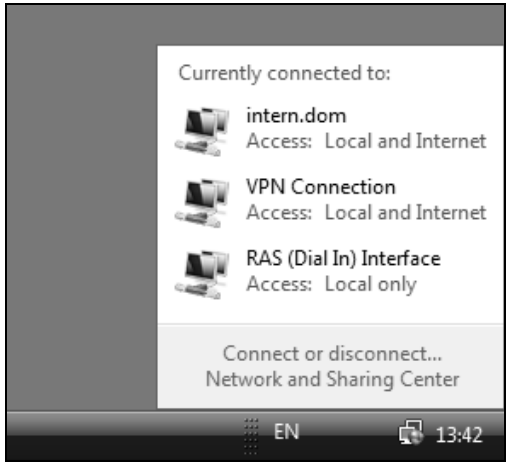


Рис. 6.1. Окно активных сетевых подключений

При выполнении команды подключения к сети в специальном окне (рис. 6.2) 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. 6.11.)

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.

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.

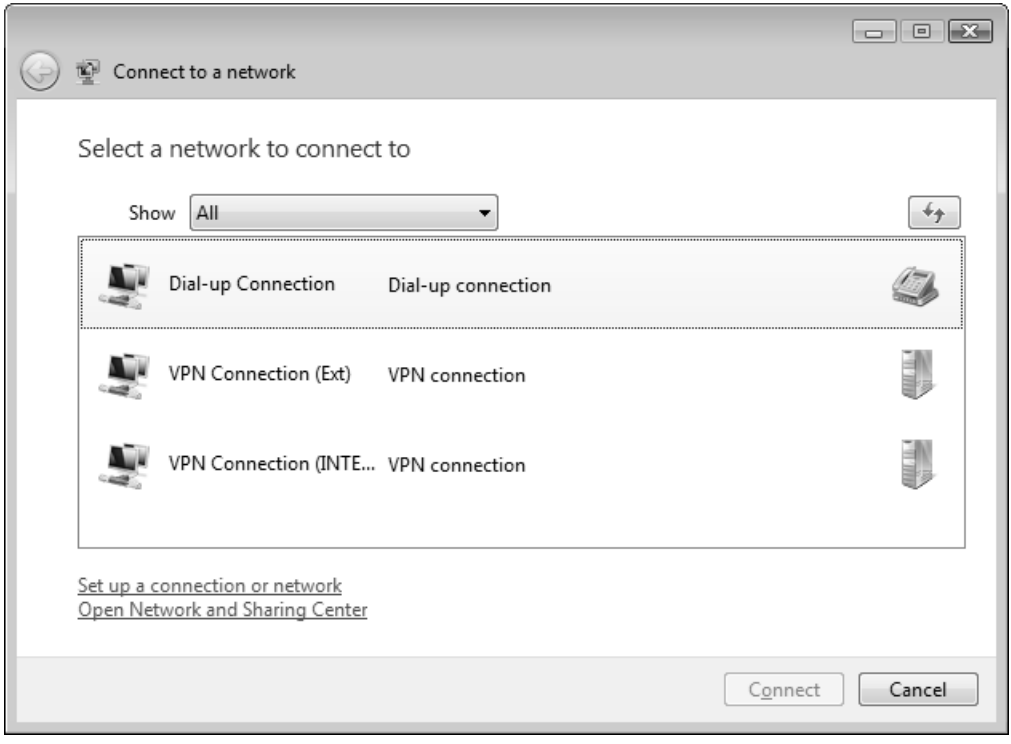


Рис. 6.2. Окно выбора подключаемой сети

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. 6.3) — здесь можно видеть все активные подключения, менять их параметры, управлять общим доступом к фай-

лам и принтерам, а также инициировать операции подключения к сетям, создания и конфигурирования новых подключений.

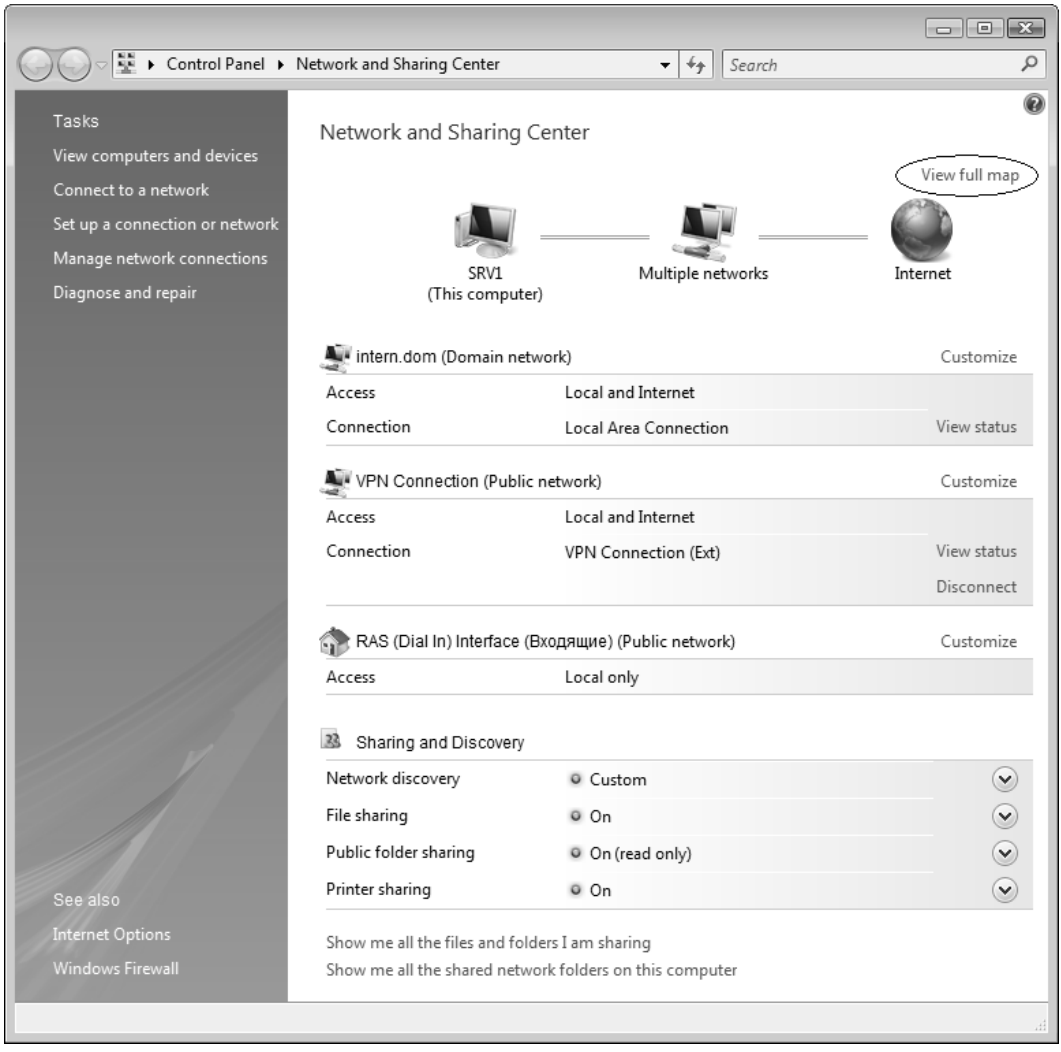


Рис. 6.3. Главное окно управления сетевыми функциями системы — **Network and Sharing Center**

Окно **Network and Sharing Center** (Центр управления сетями и общим доступом) можно открыть с панели управления, из окна активных подключений (см. рис. 6.1) или из контекстного меню подключения. В этом окне 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. 6.3)

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. 6.4) 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.

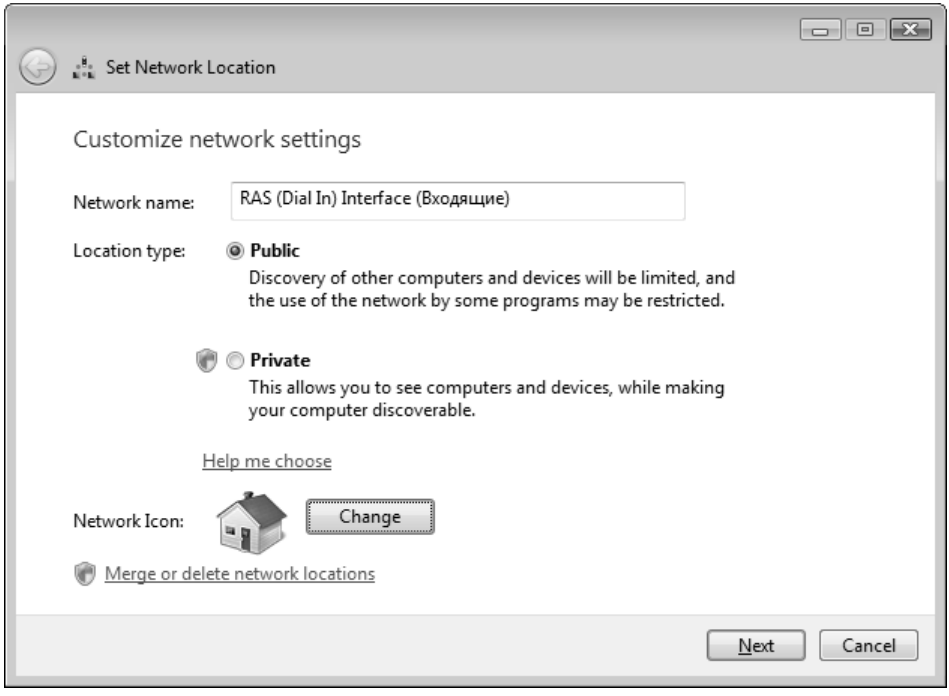


Рис. 6.4. Выбор категории сети (сетевого размещения)

Для компьютера, подключенного к домену, сетевое размещение изменить нельзя — это видно на примере, приведенном на рис. 6.5. Можно только изменить сетевое имя, в качестве которого по умолчанию используется DNS-имя 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 обычно этого сообщения опасаться не стоит, поскольку на работоспособности сетевого подключения это не сказывается.

Ссылка **View full map** (Просмотр полной карты) (см. рис. 6.3) позволяет увидеть так называемую *карту сети* (network map) для выбранного подключения (рис. 6.6). На этой карте представлены компьютеры, с которыми имеется связь; можно быст-

ро 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 имеющихся у компьютера общих сетевых ресурсов (папок и принтеров).

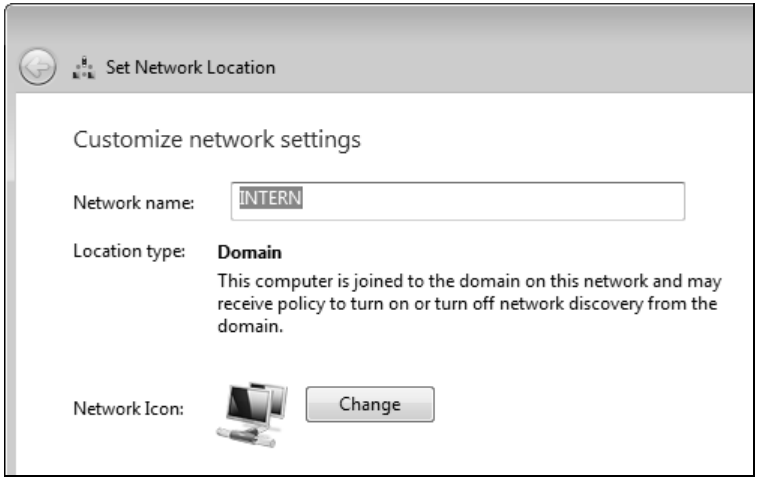


Рис. 6.5. Сетевое размещение для компьютера, входящего в состав домена

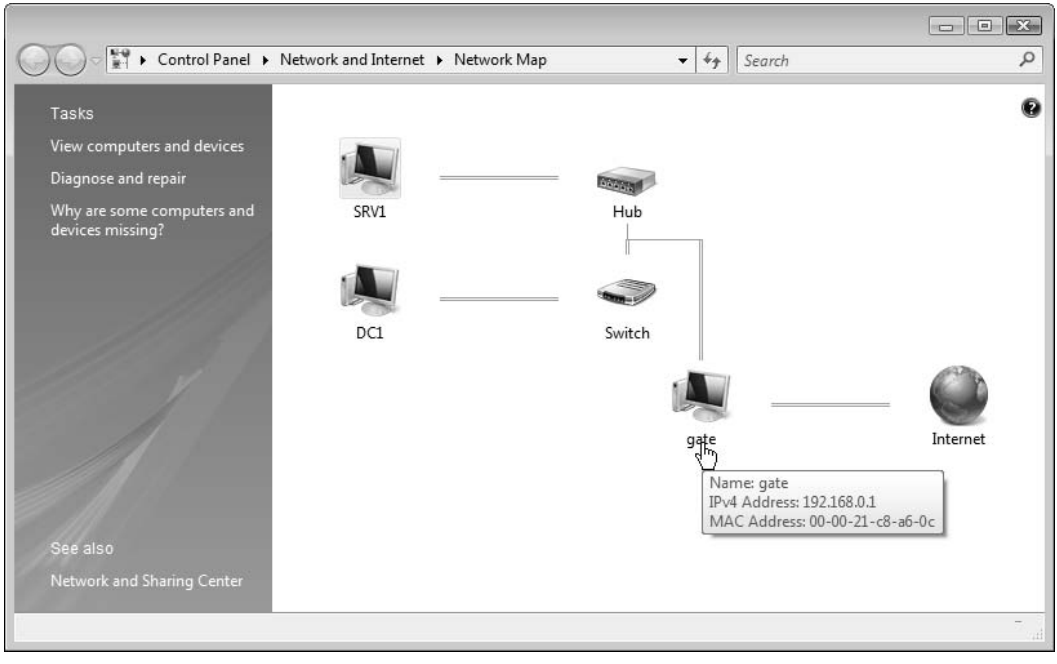


Рис. 6.6. Карта сети для выбранного подключения

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 1*), 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)).

В нижней части окна Центра управления сетями (см. рис. 6.3) 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 4*. 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. 6.3), можно попасть в традиционное 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. 6.7 в качестве примера показано окно свойств VPN-подключения.

Внимание!

Для просмотра сетевых параметров и управления сетевыми подключениями, протоколами и компонентами можно также использовать мощную и многофункциональную утилиту командной строки *Netsh.exe* (для редакций Windows Server Core и Hyper-V Server это — основное средство настройки сети!) *(см. далее примеры в*

разд. "Настройка сетевых параметров и брандмауэра из командной строки"). Для просмотра параметров конфигурации стека TCP/IP обычно используется утилита *Ipconfig.exe*, которая позволяет также инициализировать запрос на выдачу IP-адреса, запускать регистрацию адресов в службе DNS, очищать кэш DNS-клиента и т. п.

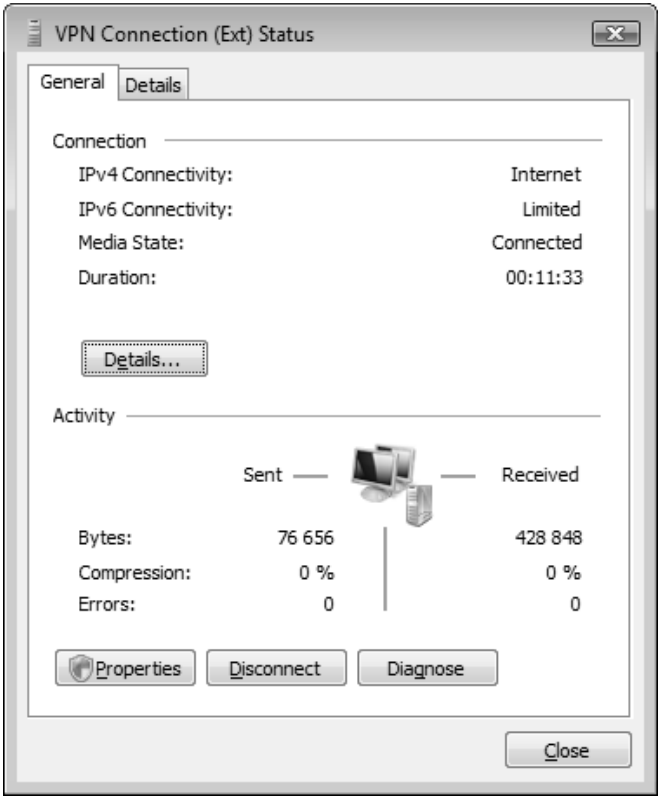


Рис. 6.7. Окно состояния сетевого подключения

Нажав в окне состояния подключения (см. рис. 6.7) 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.

На рис. 6.8, слева, в качестве примера показаны дополнительные параметры подключения по локальной сети, а на рис. 6.8, справа, — параметры входящего подключения, где также указаны тип сервера, методы аутентификации и шифрования.

Кнопка **Diagnose** (Диагностика) в окне состояния подключения (см. рис. 6.7) 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); он 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. Если ошибка исправлена, то появляется соответствующее сообщение, и сведения об ошибке можно отправить компании Microsoft.

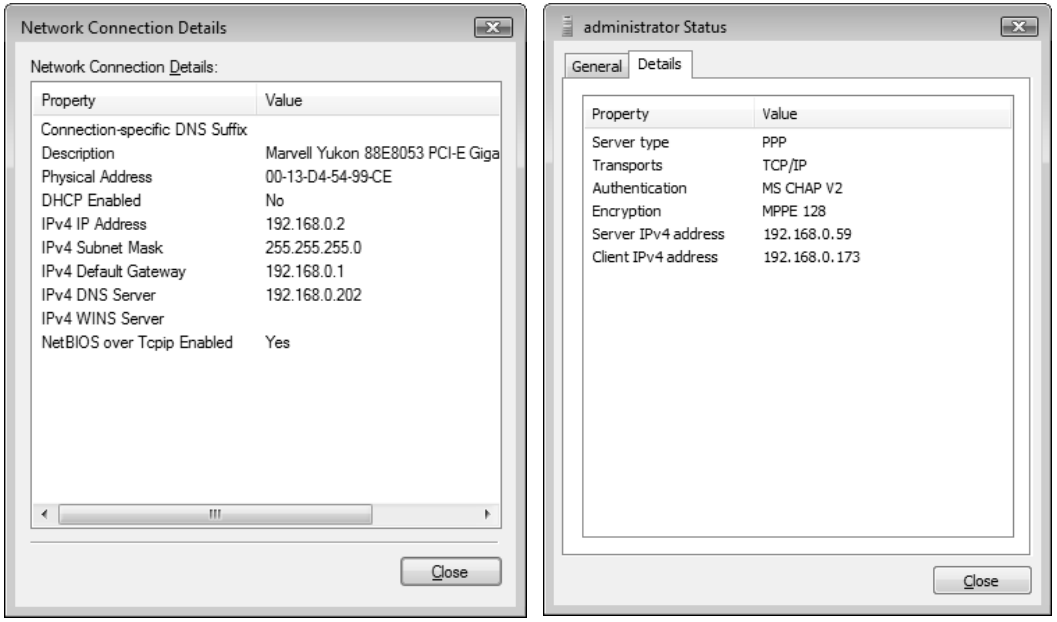


Рис. 6.8. Дополнительные свойства сеанса связи

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.

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. 6.9). 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. 6.10 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).

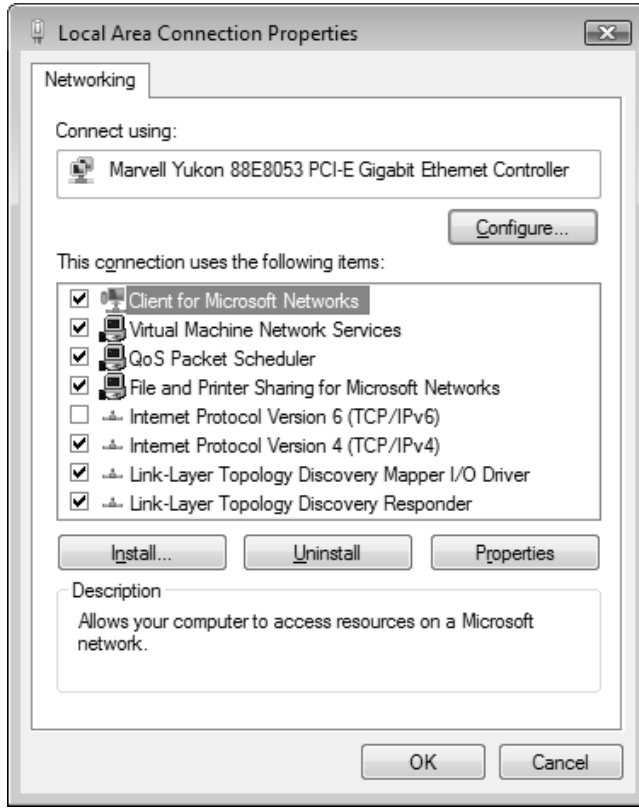


Рис. 6.9. Окно свойств подключения по локальной сети

В окне свойств сетевого подключения (см. рис. 6.10) на вкладке **Networking** (Сеть) можно запросить установку дополнительных клиентов, протоколов и служб: при нажатии кнопки **Install** (Установить) появляется окно выбора типа компонентов. (Следует, однако, отметить, что практически все стандартные сетевые компоненты, имеющиеся в составе Windows Server 2008, уже присутствуют в показанном на рис. 6.9 окне свойств подключения; можно лишь добавить *Reliable Multicast Protocol* (RMP; Надежный многоадресный протокол) или же устанавливать компоненты с дискет и других носителей.)

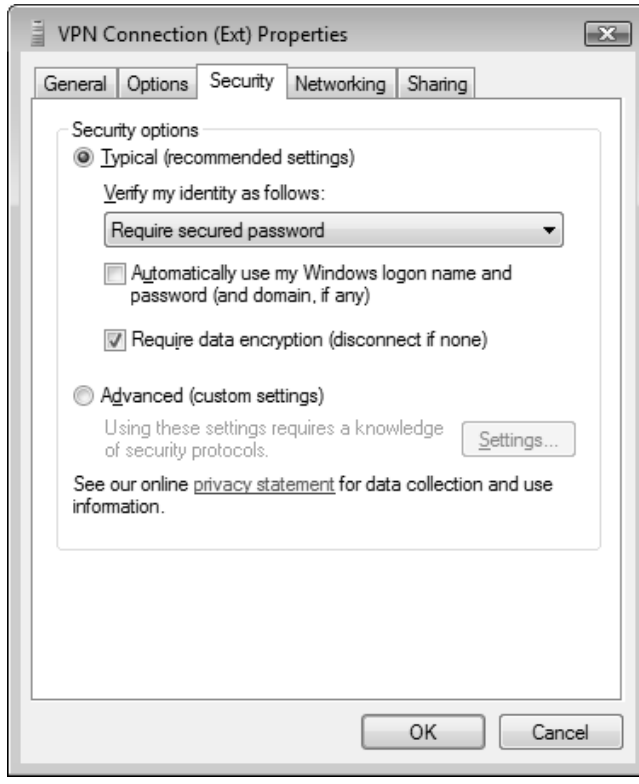


Рис. 6.10. Окно свойств VPN-подключения

Управление подключениями

Вернемся к окну Центра управления сетями (см. рис. 6.3) 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.

По ссылке **Connect to a network** (Подключить к сети) из окна Центра управления сетями можно попасть в окно имеющихся в системе дополнительных подключений (см. рис. 6.2), где также можно выбирать активную беспроводную сеть (если компонент беспроводной связи *Wireless LAN Service* установлен 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. 6.11) 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.

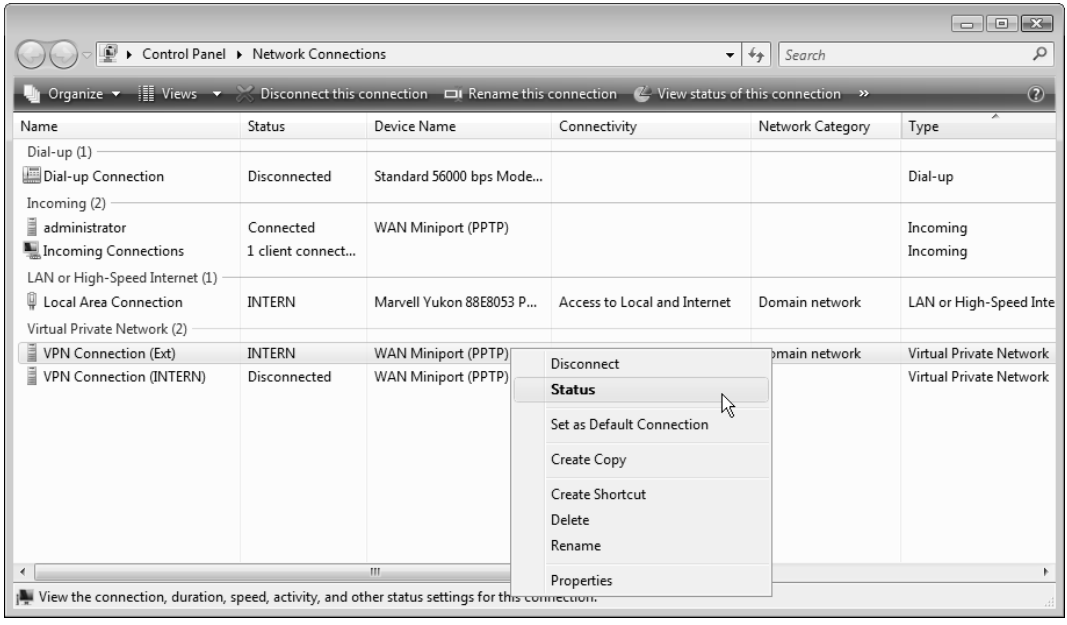


Рис. 6.11. Окно сетевых подключений

Совет

Если в процессе работы требуется частый доступ к окну состояния (см. рис. 6.7) некоторого сетевого подключения, откройте окно сетевых подключений (см. рис. 6.11), 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)).

Если приходится часто обращаться к окну сетевых подключений, то найдите в папке C:\Windows\System32 файл ncpa.cpl, создайте для него ярлык и перенесите в нужное место — на рабочий стол или в меню **Start** (Пуск).

В контекстном меню коммутируемых и VPN-подключений имеется команда **Set as Default Connection** (Сделать подключением по умолчанию) (см. рис. 6.11). С ее помощью можно выбрать подключение, которое будет автоматически устанавливаться в том случае, если компьютер не связан с сетью, но какие-то программы пытаются обратиться к сетевым ресурсам.

Создание новых подключений

Для создания дополнительных подключений в левой части окна Центра управления сетями (см. рис. 6.3) используется ссылка **Set up a connection or network** (Установка подключения или сети).

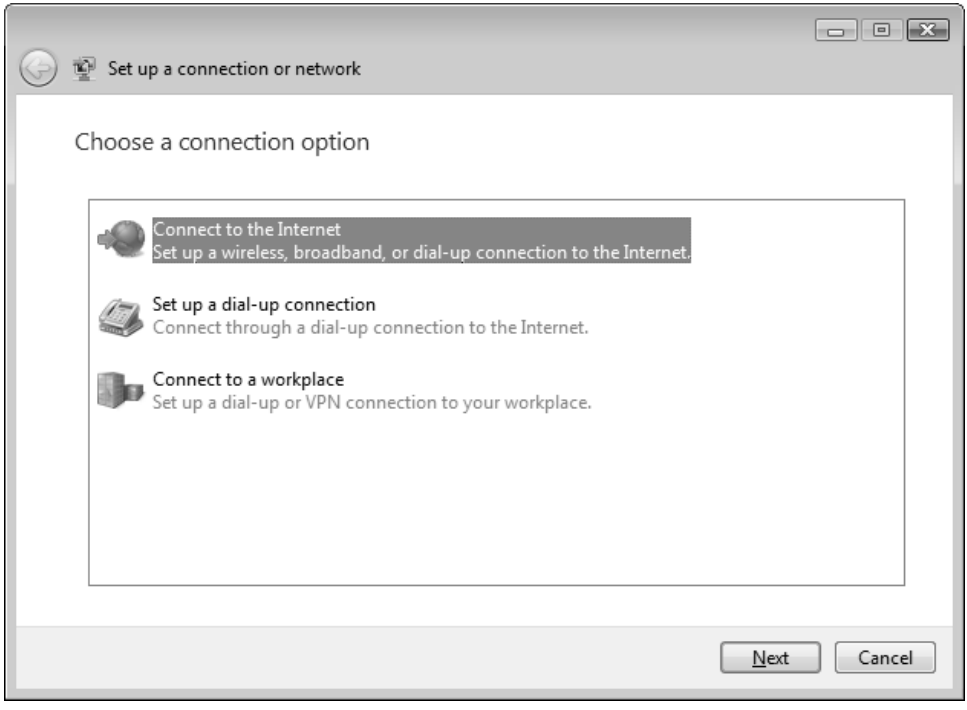


Рис. 6.12. Выбор типа создаваемого сетевого подключения

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. 6.12).

Процесс создания новых сетевых подключений выполняется в диалоговом режиме в окне мастера и не вызывает никаких сложностей, поэтому мы отметим лишь основные шаги; подробнее будут рассмотрены только VPN- и входящие подключения.

> ***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.

Типы сетевых подключений

Как и предшествующие версии Windows, системы Windows Server 2008 поддерживают пять типов сетевых подключений, которые перечислены в табл. 6.1.

Таблица 6.1. *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 локальные сети или подключающие компьютер к корпоративным сетям через Интернет или другую сеть общего пользования (public network)	Безопасное соединение с корпоративной сетью через Интернет

Таблица 6.1 *(окончание)*

Тип подключения	Технология связи	Пример
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. 6.11) 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 следует установить компонент с помощью оснастки **Server Manager** (Диспетчер сервера).

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. 6.11). 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. 6.12) выберите одну из трех опций, которые позволят создать подключение — конкретный выбор определяется лишь назначением подключения. 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).

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). По завершении операции новый значок или запись появляется в окне сетевых подключений (см. рис. 6.11).

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*);
- на другом — в окне мастера подключений (см. рис. 6.12) выбрать опцию **Connect to a workplace** (Подключение к рабочему месту), после чего в окне

выбора типа соединения (рис. 6.13) указать на использование VPN-подключения (**Use my Internet connection (VPN)**).

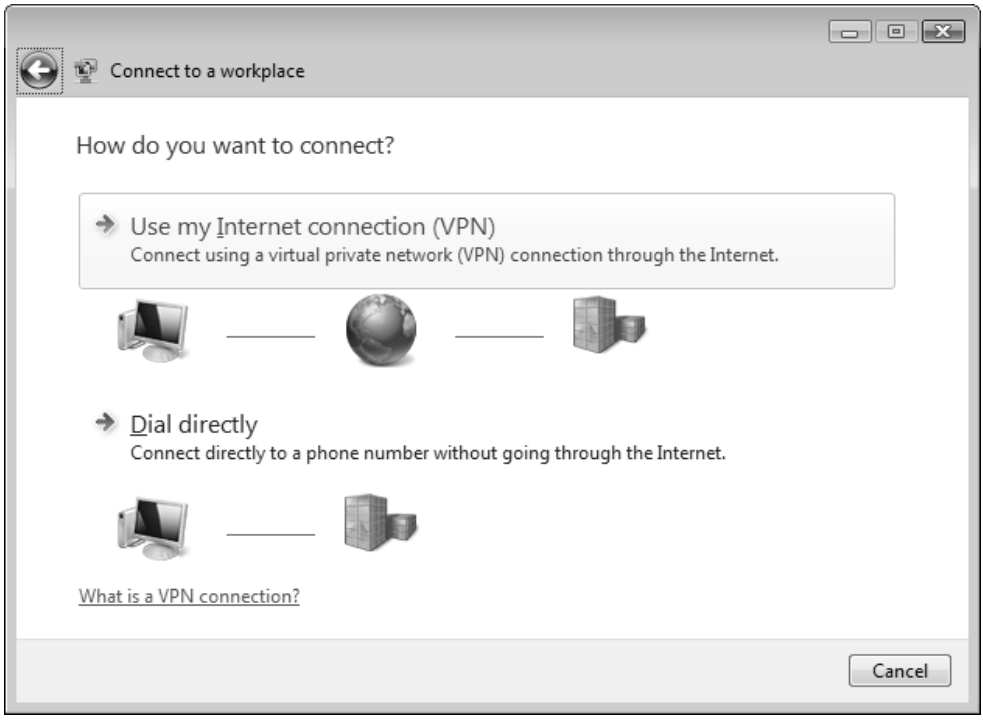


Рис. 6.13. Выбор способа подключения к удаленному рабочему месту

Далее следует ввести DNS-имя или IP-адрес VPN-сервера и дать VPN-подключению произвольное имя. Для регистрации на сервере нужно указать имя учетной записи и пароль, а также имя домена (сервера). Подключение может устанавливаться сразу или в будущем (см. соответствующий флажок в окне мастера). Когда подключение создано (и установлено), можно закрыть окно мастера.

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*).

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 разрешении *входящих подключений* компьютер под управлением Windows Server 2008 будет 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*.

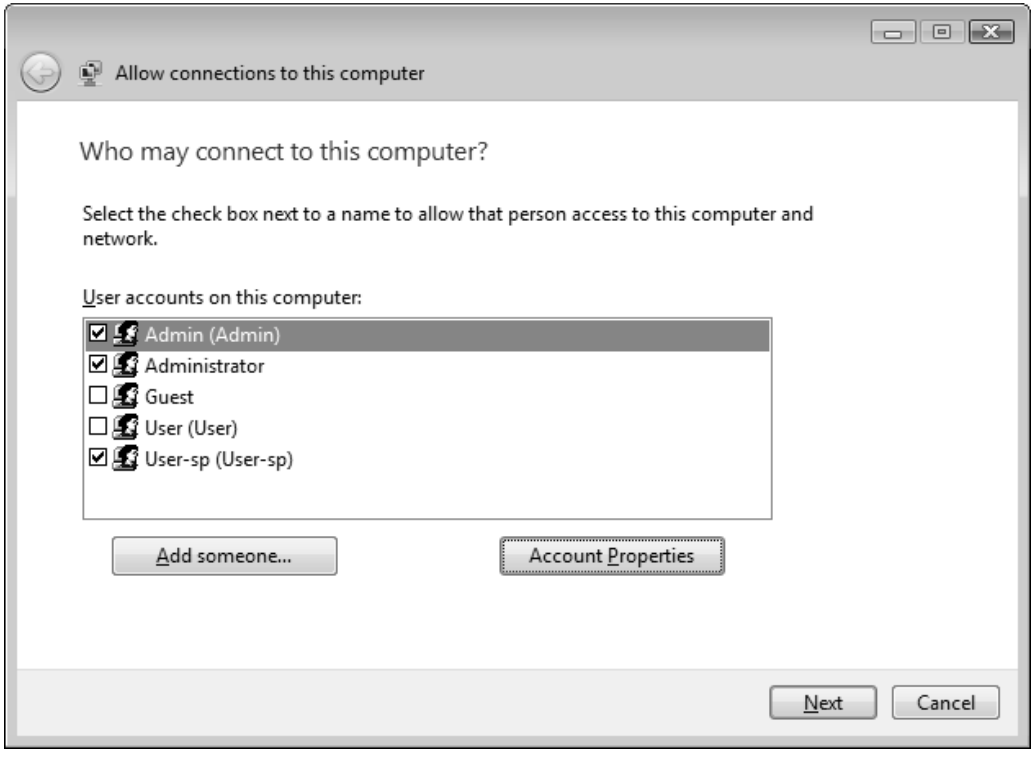


Рис. 6.14. Выбор учетных записей, которые смогут получить удаленный доступ к данному компьютеру

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. 6.11) 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. 6.14). По умолчанию в списке представлены имеющиеся локальные или доменные учетные записи; в этом же окне можно создать и новых пользователей.

На следующем шаге укажите тип входящих подключений, которые будут использоваться (рис. 6.15). 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).

Затем выберите службы и протоколы для входящих подключений (рис. 6.16) и, что очень важно, определите свойства протоколов (поскольку они указывают на возможность доступа к локальной сети и способ назначения IP-адресов — см. на рис. 6.16 окно свойств протокола IPv4). Когда все параметры заданы, нужно нажать кнопку **Allow access** (Разрешить доступ). Теперь удаленные клиенты смогут подключаться к серверу.

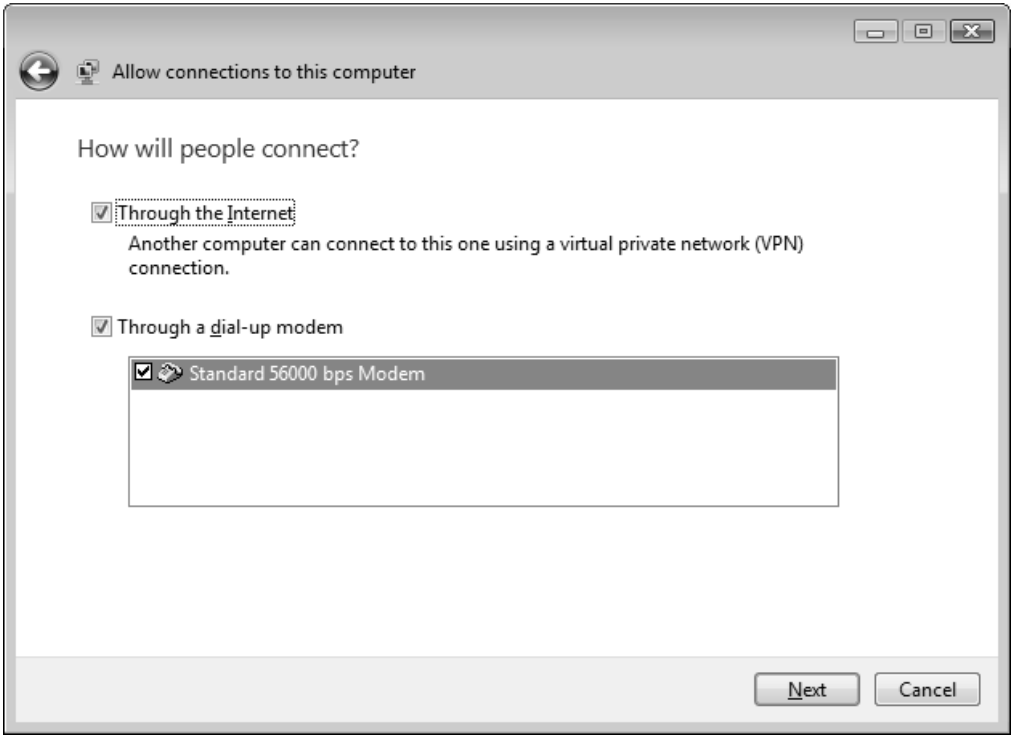


Рис. 6.15. Выбор типа разрешенных входных подключений

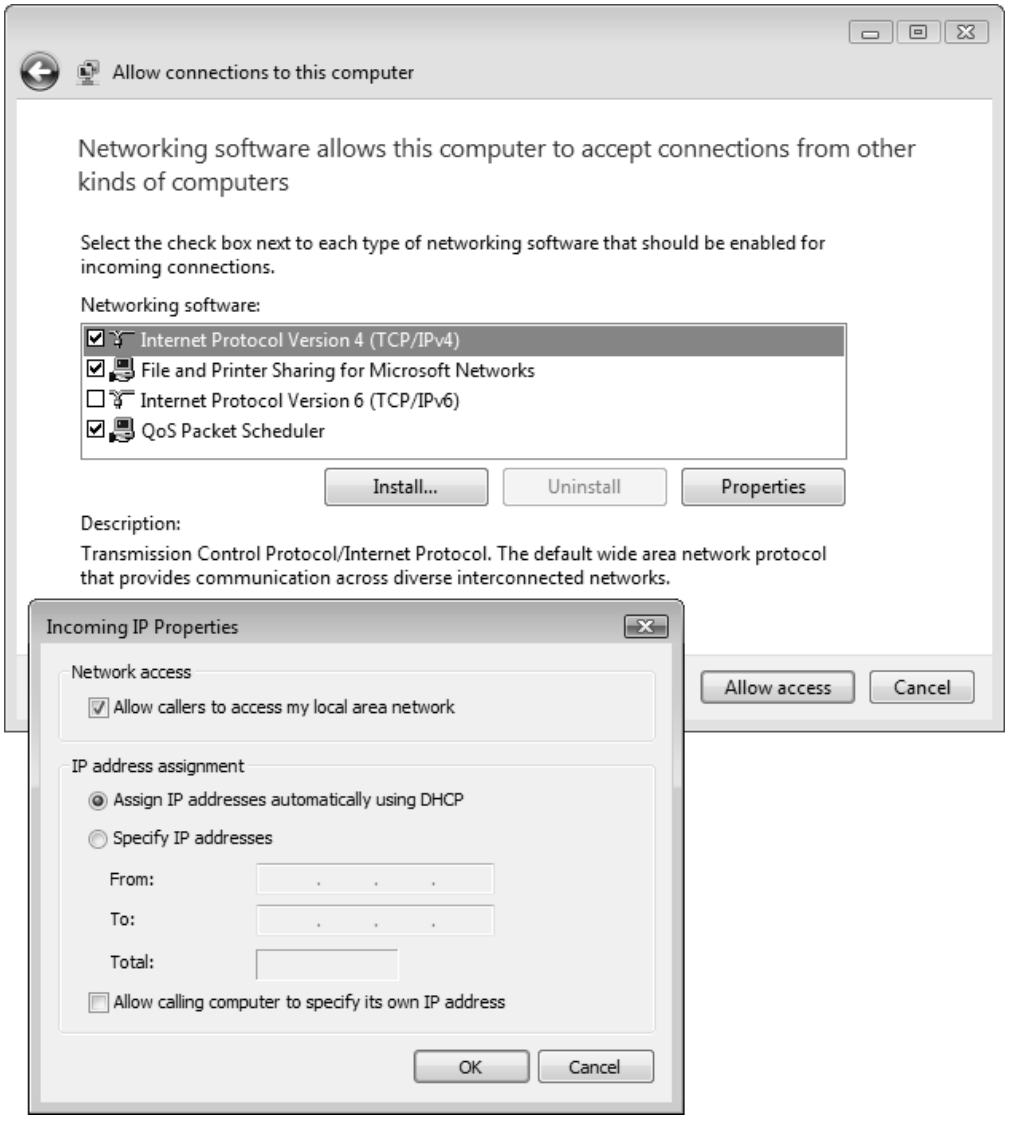


Рис. 6.16. Выбор протоколов и служб, используемых входящими подключениями

Серверы DHCP

Среди сетевых серверных служб первой мы рассмотрим службу DHCP, поскольку она является базовым сервисом для развертывания сетевой среды, в которой используется протокол TCP/IP. От параметров, задаваемых этой службой, зависит конфигурация клиентов и других сетевых сервисов.

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 каталоге 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

Перечислим основные понятия протокола DHCP и сразу же покажем на примерах, как соответствующие функции реализованы в DHCP-сервере, входящем в состав Windows Server 2008.

- **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. 6.17 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).

  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 (на-

пример, 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.

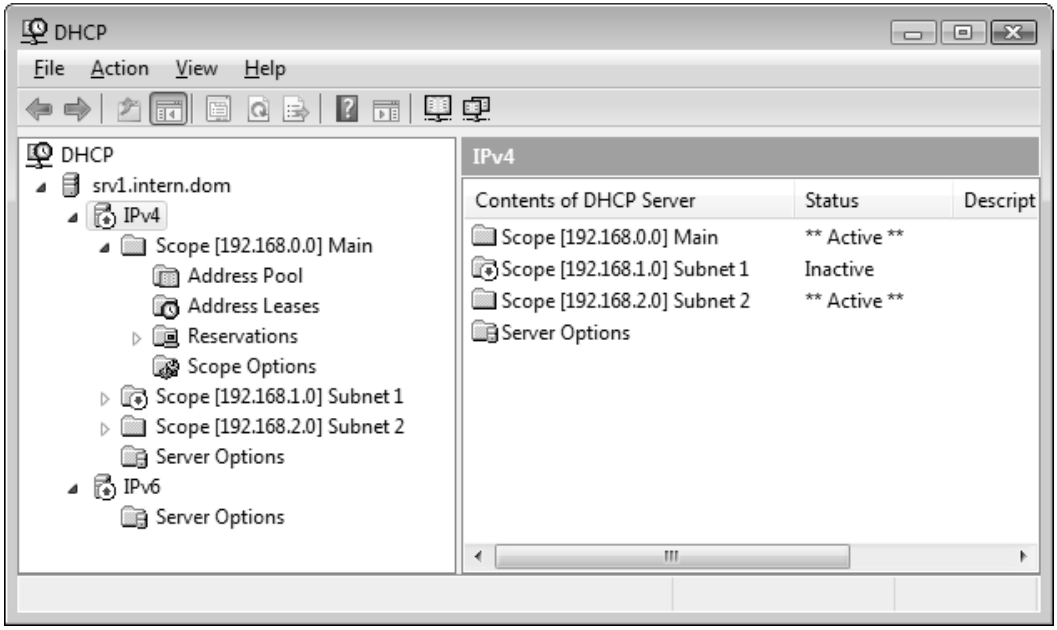


Рис. 6.17. Пример областей действия, созданных на DHCP-сервере

- **Пул адресов** (address pool). Диапазон разрешенных к сдаче в аренду адресов некоторой области DHCP называется *пулом адресов* (для этой области) (см. рис. 6.18).
- **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. 6.18 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.

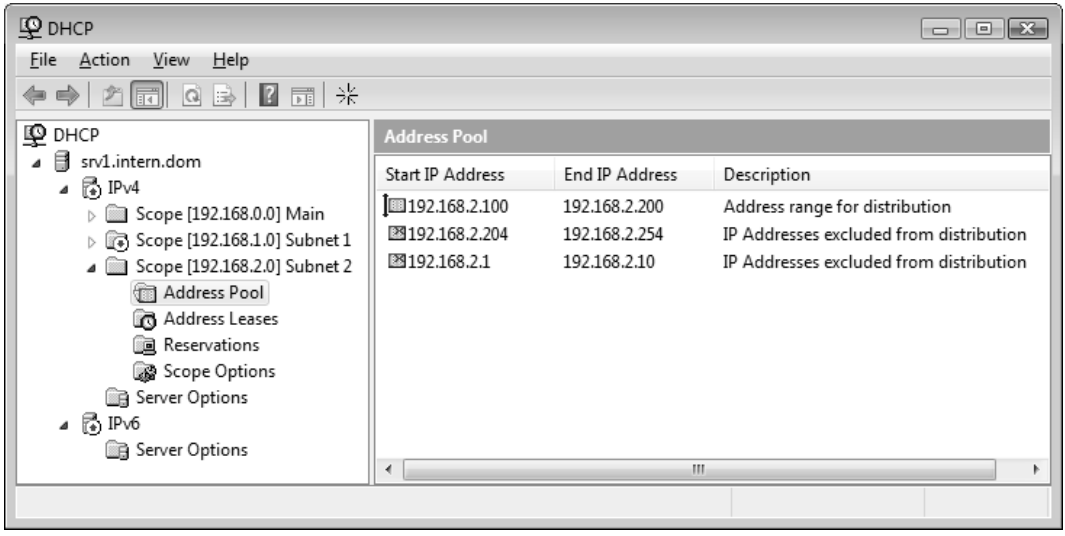


Рис. 6.18. Пример адресного пула для области действия

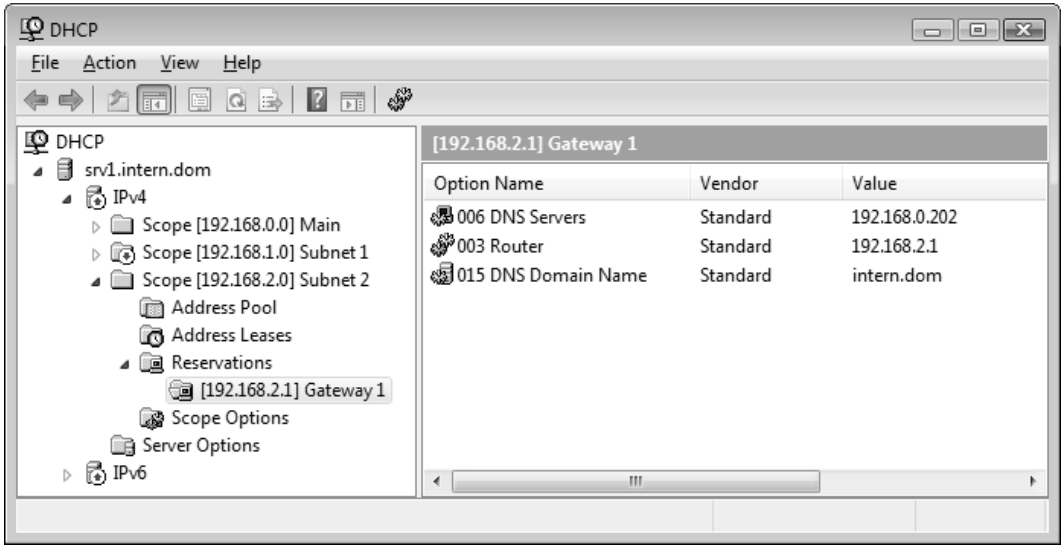


Рис. 6.19. Пример зарезервированного адреса

Как видно на рис. 6.19, адрес 192.168.2.1 зарезервирован для конкретного компьютера (он будет выдаваться только компьютеру с заданным MAC-адресом, например, 0013D45499CE[1]). Для резервирования можно задавать индивидуальные параметры DHCP: в этом примере компьютеру указывается адрес DNS-сервера.

(Значки около названия параметра позволяют понять, на каком "уровне" эти значения были определены: в данном примере имя DNS-домена (DNS Domain Name) задано в параметрах DHCP-сервера, адрес шлюза (Router) в параметрах области действия, а адрес DNS-сервера (DNS Servers) — 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).

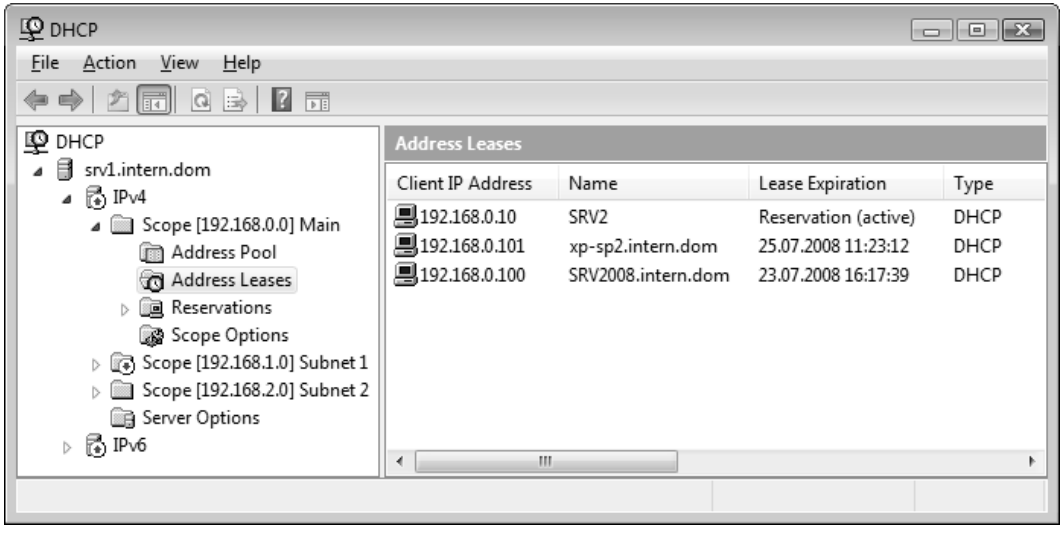


Рис. 6.20. Список выданных адресов со сроками истечения аренды

На рис. 6.20 показан список адресов, уже 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

[1] MAC-адрес состоит из двенадцати символов в шестнадцатеричной нотации.

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`).

- **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. 6.19 показан пример параметров DHCP для резервирования (конкретного клиента), где параметры определены на различных уровнях. Также 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).

Установка и настройка DHCP-сервера

Для развертывания в сети службы DHCP необходимо, как минимум, выполнить следующие действия:

1. Установить DHCP-сервер.

[1] Поэтому не нужно удивляться тому, что в папке **Scope Options** могут отображаться параметры, которые там и не определялись.

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.

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. Укажите имя домена, в котором сервер будет работать, и адрес предпочитаемого DNS-сервера, используемого клиентами домена. 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. 6.21). В окне параметров области (scope) необходимо указать ее имя и диапазон адресов. По необходимости можно задать адрес шлюза по умолчанию, тип подсети (он определяет длительность аренды адресов для проводных и беспроводных сетей) и необходимость немедленной активации области действия.
3. Если в сети отсутствуют клиенты с адресами IPv6, то на следующем шаге можно запретить режим *DHCPv6 stateless mode*.
4. Укажите 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 бу-

дет обслуживать клиентов). Для автономного DHCP-сервера, работающего в сети без доменов, авторизация, в принципе, не требуется.

5. После проверки всех введенных параметров нажмите кнопку **Install** (Установить), и установка DHCP-сервера начнется.

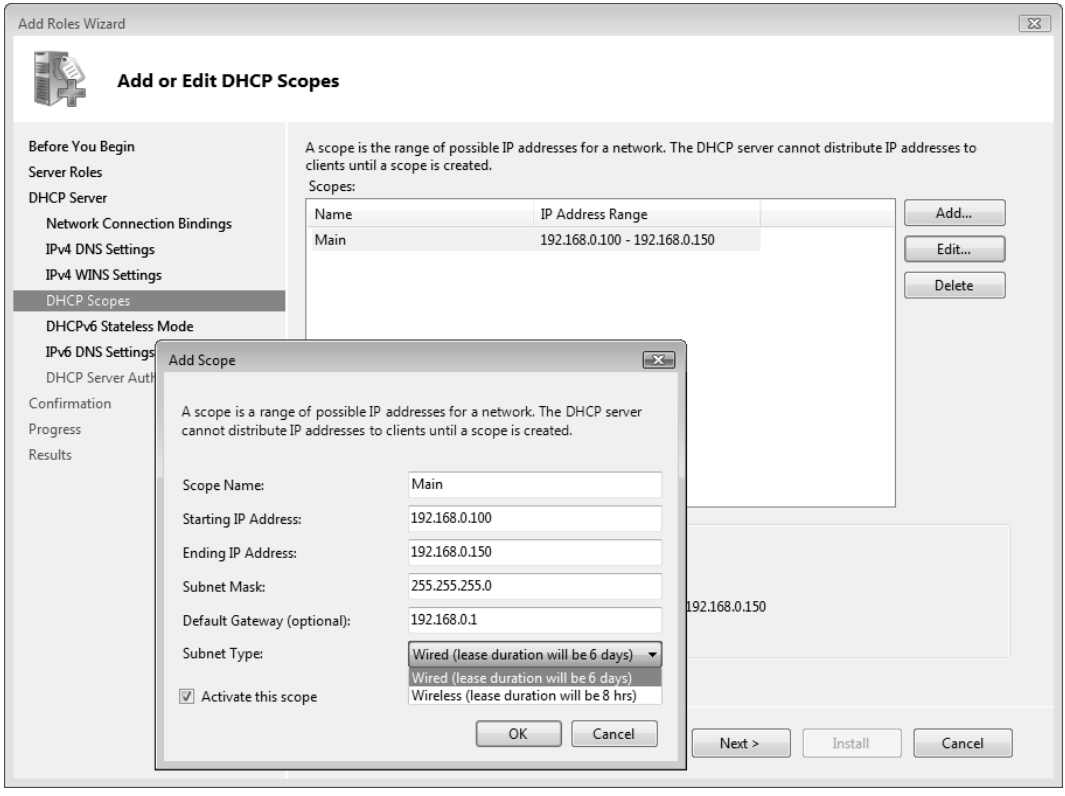


Рис. 6.21. Создание новых областей действия (scopes) для устанавливаемого DHCP-сервера

После добавления роли запуск DHCP-сервера можно проверить 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.

> ***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).

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. Для авторизации других серверов нужно нажать кнопку **Authorize** (Авторизовать) и указать IP-адрес DHCP-сервера. Команда **Authorize** (Авторизовать) имеется также в контекстном меню объектов, 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 новой 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 задать некоторые 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. 6.22 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.

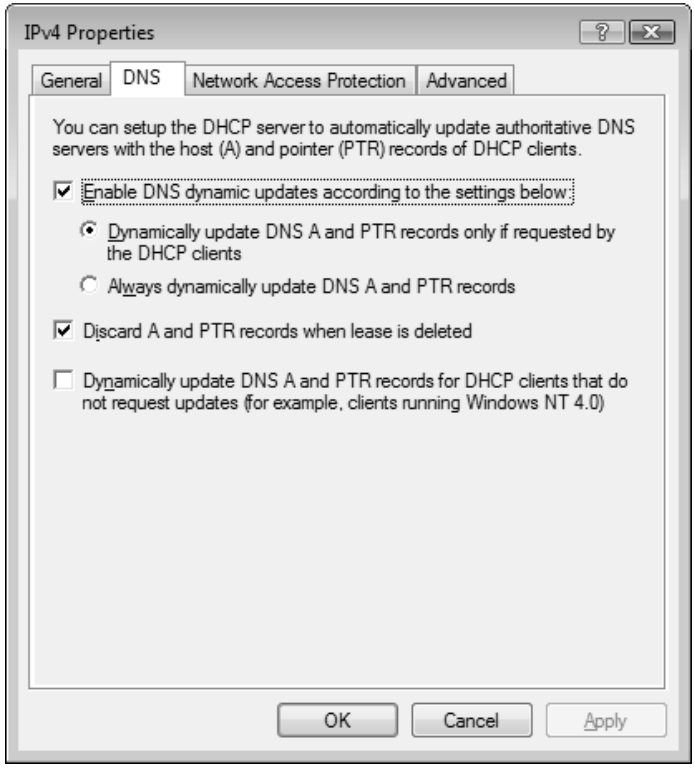


Рис. 6.22. Активизация режима автоматической регистрации доменных имен в базе данных DNS

Приведенные на рис. 6.22 установки подразумевают, что клиенты сети 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 со-

ответствующая строка была вручную удалена из списка выданных адресов (из папки **Address Leases**).

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 и восстановление 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,
```

где `dhcp-show.txt` — текстовый командный файл, содержащий следующие директивы для утилиты Netsh:

```
interface
dhcp
server 192.168.0.2
dump
```

Здесь `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)).

Агент ретрансляции DHCP/BOOTP

Работа протоколов BOOTP и DHCP основана на механизмах широковещания. Обычно маршрутизаторы по умолчанию не ретранслируют широковещательные 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.

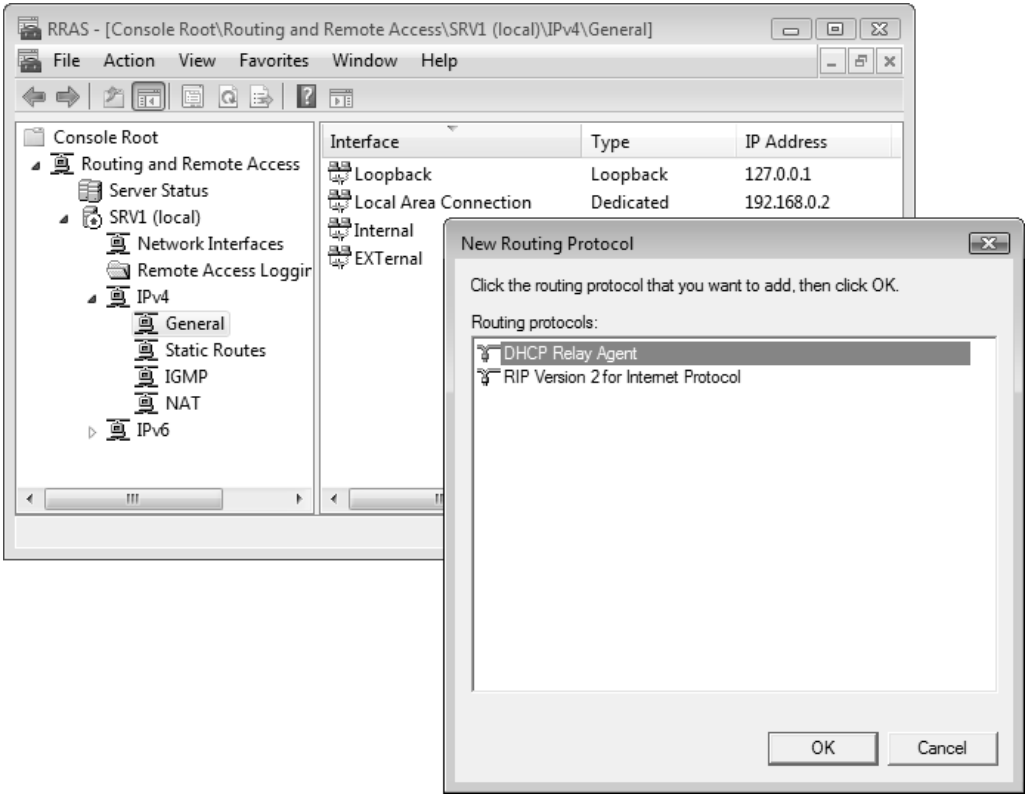


Рис. 6.23. Включение агента ретрансляции DHCP в окне оснастки **Routing and Remote Access**

Для установки агента ретрансляции необходимо использовать (предварительно включив и настроив) службу Routing and Remote Access (Маршрутизация и удален-

ный 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. 6.23).
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.

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 их развертывания нужен хотя бы один DNS-сервер. Иерархия доменов Active Directory "отображается" на пространство имен DNS. Клиенты доменов используют службу DNS для обнаружения контроллеров домена, а контроллеры обращаются к ней для поиска адресов партнеров по репликации. Ошибки, допущенные при проектировании пространства имен DNS (например, неудачный выбор имен доменов или неправильная настройка зон), могут серьезно осложнить внедрение и развитие сети, а в некоторых случаях может даже потребоваться повторное развертывание всего леса доменов.

Возможности DNS-серверов на базе Windows Server 2008

Ниже перечислены основные функциональные возможности серверов DNS в системах Windows Server 2008.

- **Поддержка инкрементных передач зоны между серверами.** Передача зоны осуществляется между DNS-серверами в качестве средства синхронизации от-

дельных 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.

- **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. Зоны могут располагаться в разделе доменных имен, который реплицируется между всеми контроллерами одного домена, но чаще используется более эффективный вариант, когда зоны хранятся в разделах приложений (application partition).

  В том случае, когда DNS-серверы установлены на контроллерах домена, для размещения содержимого зоны могут использоваться два специальных стандартных раздела приложений с именами ForestDnsZones.<*DNSимяЛеса*> и DomainDnsZones.<*DNSимяДомена*>. Эти разделы по умолчанию реплицируют-

ся 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. Это касается интеграции со службами WINS и DHCP (например, устаревшие клиенты не могут непосредственно регистрировать или обновлять свои DNS-имена; однако это возможно с помощью службы WINS, которая будет выполнять нужные действия в DNS).

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. 6.25). 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). В этой зоне располагаются 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 Server 2008 зоны могут храниться в специальных 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. 6.25).

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

Если службы Active Directory и DNS устанавливаются на сервере одновременно (на первом контроллере домена в сети — *см. главу 7*), 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 заранее 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. 7.1). 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 лесу 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 про-

смотра (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. 6.25) 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. 6.24), 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.)

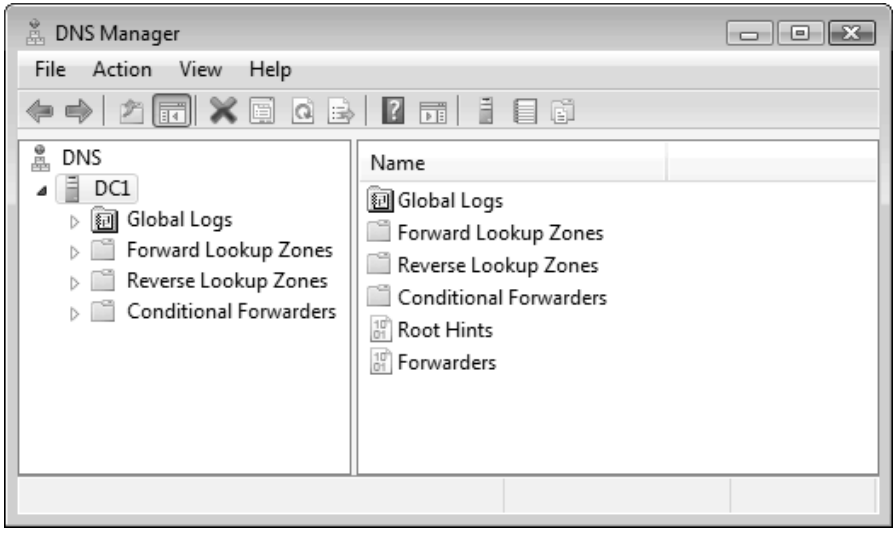


Рис. 6.24. Окно оснастки **DNS** на серверах Windows Server 2008

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.

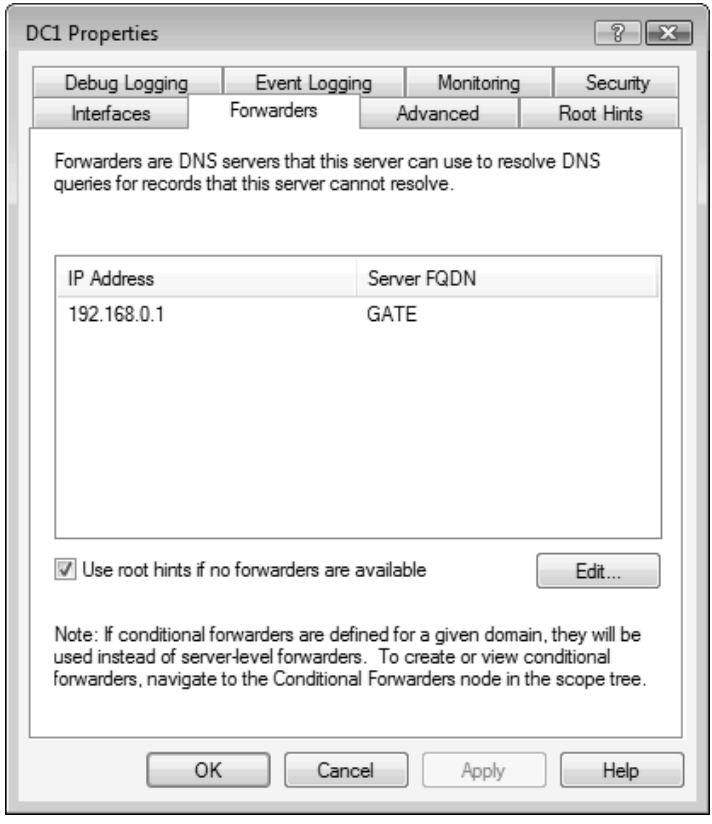


Рис. 6.25. Настройка серверов пересылки для разрешения внешних имен

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 помощью оснастки **DNS**, на вкладке **Forwarders** (Пересылка) в окне свойств DNS-сервера (рис. 6.25).

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).

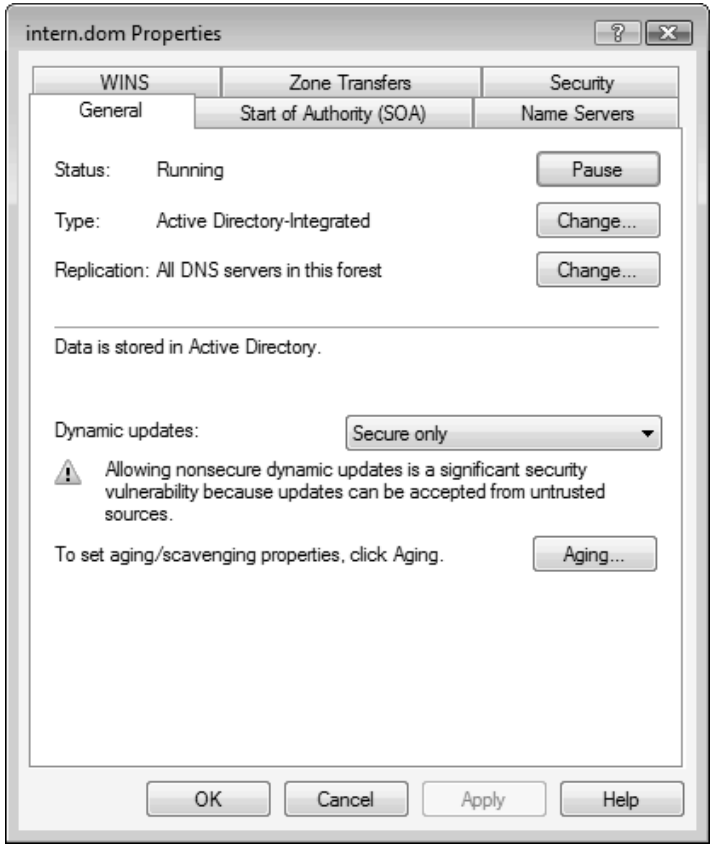


Рис. 6.26. Окно свойств зоны DNS, интегрированной в каталог Active Directory

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.

Окно свойств (рис. 6.26) 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. 6.26). При необходимости его изменения нужно нажать кнопку **Change** (Изменить).

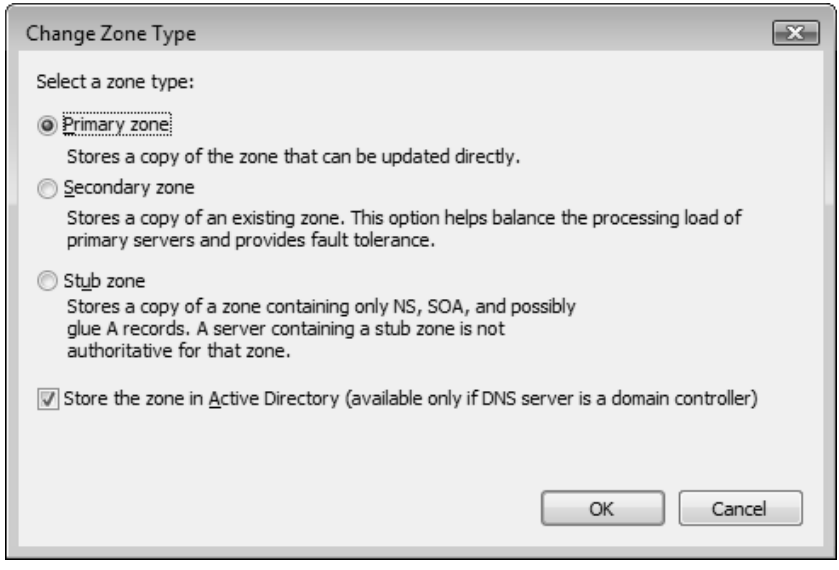


Рис. 6.27. Выбор типа (способа хранения) зоны

В открывшемся окне (рис. 6.27) администратор может 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 использо-

вание 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), позволяющие корневому DNS-серверу (хранящему авторитетную зону леса, например, intern.dom) иметь сведения о серверах, являющихся авторитетными для некоторой дочерней зоны (например, sub.intern.dom).

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. 6.28). Перечень значений, предлагаемых администратору в этом окне, приведен в табл. 6.2.

Таблица 6.2. *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*

Таблица 6.2 *(окончание)*

Область репликации	Описание
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

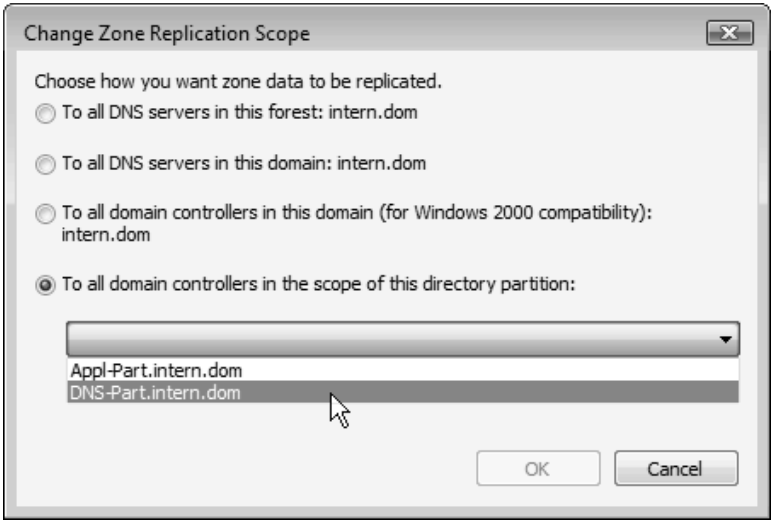


Рис. 6.28. Выбор области репликации зоны

Область репликации зоны можно также изменить с помощью утилиты *DnsCmd.exe*. (Для просмотра содержимого раздела приложений используйте оснастку **ADSI Edit** (Редактирование ADSI) — *см. главу 7*.) Следующая команда позволит быстро найти имена всех контроллеров — хранителей реплики указанного раздела приложений (ForestDnsZones.intern.dom):

```
dnscmd /DirectoryPartitionInfo ForestDnsZones.intern.dom
```

(Имя DNS-сервера можно не указывать, если команда выполняется непосредственно на этом сервере.)

Для перемещения зон в другой раздел каталога применяется 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. 6.26). 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:

```
dnscmd /CreateDirectoryPartition DNS-Part.intern.dom
```

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:

```
C:\>dnscmd /EnumDirectoryPartitions

Enumerated directory partition list:

        Directory partition count = 5

 Appl-Part.intern.dom                    Enlisted
 DNS-Part.intern.dom                     Enlisted
 DomainDnsZones.intern.dom               Enlisted Auto Domain
 DomainDnsZones.sub.intern.dom           Not-Enlisted
 ForestDnsZones.intern.dom               Enlisted Auto Forest

Command completed successfully.
```

(В данном примере три 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 (DC3) хранителем реплики раздела приложений, используется следующая команда:

```
dnscmd dc3.intern.dom /EnlistDirectoryPartition DNS-Part.intern.dom
```

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 /DirectoryPartitionInfo`, которую можно выполнять на любом DNS-сервере.

Следующая команда позволяет удалить реплику раздела приложений с указанного контроллера домена:

```
dnscmd dc3.intern.dom /UnenlistDirectoryPartition DNS-Part.intern.dom
```

И, опять, 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 мо-

гут 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:

```
dnscmd /CreateBuiltinDirectoryPartitions /Forest
```

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.

Кроме утилиты DnsCmd для тестирования DNS можно использовать утилиты *Nslookup.exe*, *Netdiag.exe* (из пакета Support Tools) и *Dcdiag.exe* (с параметром `/test:DNS`).

> ***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 компьютере, 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.

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 dc1.intern.dom /EnumZones

Enumerated zone list:
        Zone count = 6
 Zone name                      Type       Storage         Properties

 .                              Cache      AD-Domain
 _msdcs.intern.dom              Primary    AD-Forest       Update
 0.168.192.in-addr.arpa         Primary    AD-Legacy       Secure Rev
 intern.dom                     Primary    AD-Forest       Secure
 intern-new.dom                 Primary    AD-Domain       Secure
 sub.intern.dom                 Primary    File            Update
```

В приведенном примере `srv1.intern.dom` — имя DNS-сервера, 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 dc1.intern.dom /ZoneInfo intern.dom AllowUpdate

Zone query result:
Dword:  2 (00000002)
```

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, которая (среди прочих тестов) эффективно обнаруживает ошибки в конфигурации DNS для указанного или локального компьютера и позволяет исправить *некоторые* ошибки регистрации записей (параметр `/fix`). (Ее следует запускать с полномочиями администратора!) Например, если следующая команда не выводит никакой информации, то можно считать, что указанный контроллер работает без ошибок:

```
C:\>dcdiag /s:dc1.intern.dom /q
C:\>
```

Не следует пренебрегать проверкой DNS 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`);
- 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), в которое можно попасть из окна свойств системы (см. рис. 2.11); там же можно задать основной DNS-суффикс компьютера, нажав кнопку **More** (Дополнительно). В специальном окне отображается основной DNS-суффикс — обычно это имя того домена, в который входит данный компьютер. (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.

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 до-

мену или разрешения имен следует внимательно проверять конфигурацию DNS непосредственно на компьютере клиента.

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);
- *маршрутизация* — передача 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 протокола 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 адресов 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

Протокол распределения полосы пропускания BAP (Bandwidth Allocation Protocol), а также протокол управления распределением полосы пропускания BACP (Bandwidth Allocation Control Protocol) исключены из состава Windows Vista, однако имеются в Windows Server 2008.

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), в которой можно выбрать отдельные службы (рис. 6.29). После установки роли службу RRAS обязательно нужно *настроить*.

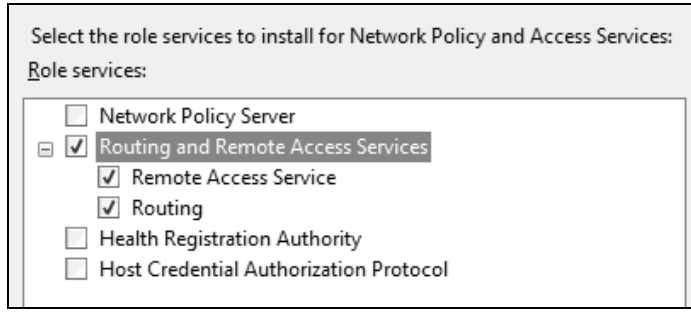


Рис. 6.29. Выбор компонентов RRAS среди других служб роли Network Policy and Access Services

Компонент *Remote Access Service* (Служба удаленного доступа) обеспечивает работу VPN- и коммутируемых подключений; компонент *Routing* (Маршрутизация) включает в себя средства маршрутизации для локальных сетей, NAT и поддержку широковещательной маршрутизации (IGMP Proxy).

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. 6.30).

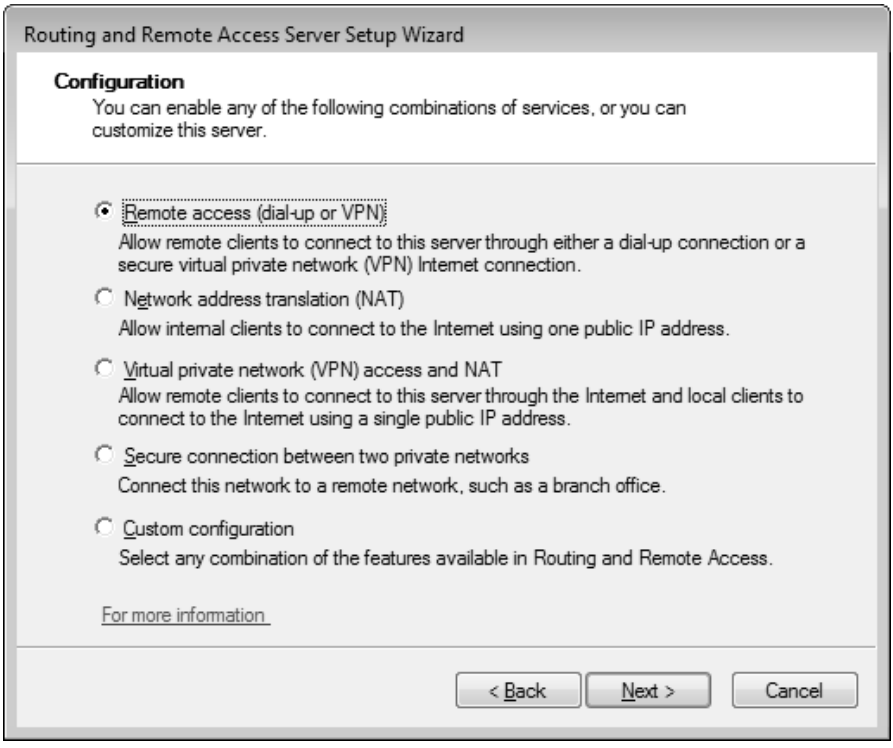


Рис. 6.30. Выбор начальной конфигурации сервера

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 полного 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) или удаленного доступа к рабочему столу.

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 предпоч-

тительным 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;
- **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)).

В окне мастера на странице *Remote Access* (Удаленный доступ) 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 ко внешней сети (Интернету) (рис. 6.31), и разрешить фильтрацию пакетов. По умолчанию устанавливаются статические фильтры, пропускающие через выбранный интерфейс только трафик VPN-подключений.

Далее требуется определить способ предоставления подключающимся клиентам IP-адресов, необходимых для работы в корпоративной сети. По умолчанию адреса выдаются автоматически сервером удаленного 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.



Рис. 6.31. Выбор внешнего интерфейса и разрешение включения статических фильтров

И наконец, на последней странице мастера 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).

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. 6.32). 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.

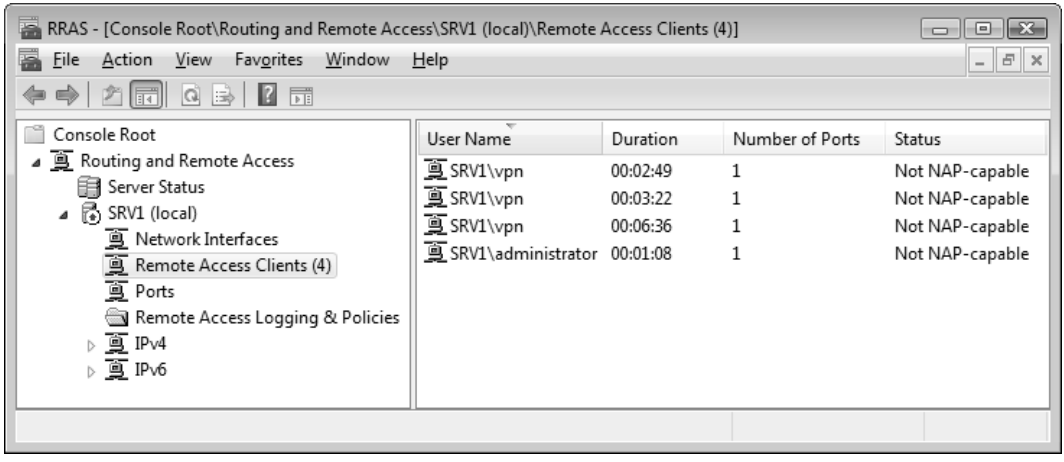


Рис. 6.32. Просмотр сеансов подключения к серверу удаленного доступа

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. ниже)*.

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. 6.30). По сравнению с Windows Server 2003, настройка NAT с помощью мастера стала значительно проще.

В окне мастера на странице *NAT Internet Connection* (Подключение к Интернету на основе NAT) (рис. 6.33) укажите подключение, которое будет использоваться механизмом преобразования имен. Предполагается, что это подключение к Интернету (или другой внешней сети). Переключатель **Use this public interface to connect to the Internet** (Использовать общедоступный интерфейс для подключения к Интернету) позволяет выбрать одно из существующих подключений. В качестве альтернативы можно использовать подключение по требованию, выбрав опцию **Create a new demand-dial interface to the Internet** (Создать интерфейс для нового подключения по требованию к Интернету).

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.

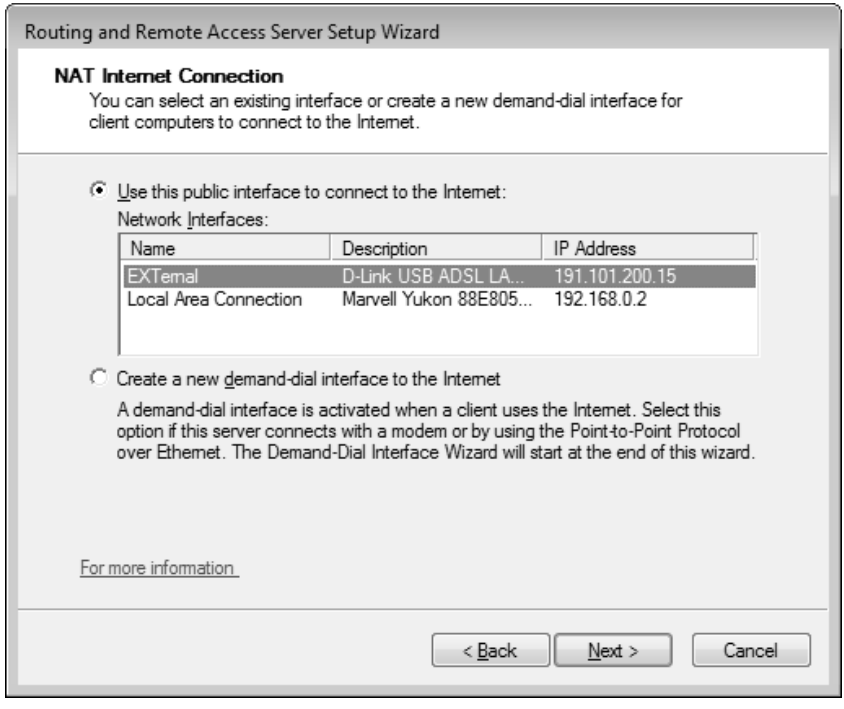


Рис. 6.33. Выбор сетевого интерфейса для работы механизма NAT

На следующем шаге нужно указать, должен ли сервер с устанавливаемым NAT обслуживать DHCP- и DNS-запросы клиентов сети (рис. 6.34). 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).

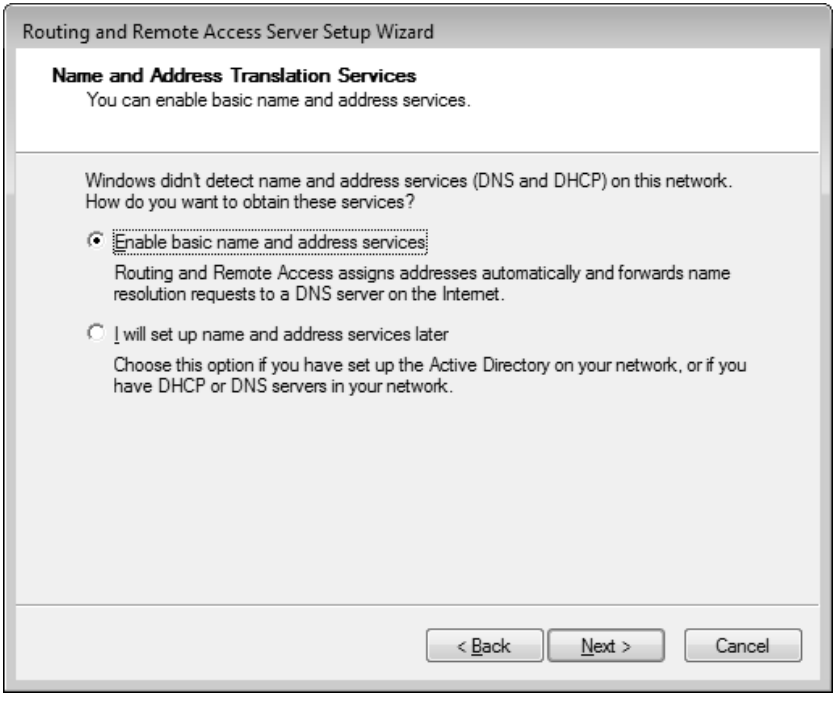


Рис. 6.34. Выбор механизма разрешения DNS-имен и выделения IP-адресов

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. Запустите оснастку **Routing and Remote Access** (Маршрутизация и удаленный доступ).

2. Если в списке активных протоколов (узел **IPv4**) отсутствует объект **NAT**, добавьте к списку протокол преобразования сетевых адресов (NAT). Для этого нужно выделить папку **IPv4** | **General** (IPv4 | Общие), вызвать контекстное меню и выполнить команду **New Routing Protocol** (Новый протокол маршрутизации). В открывшемся окне (рис. 6.35) выберите строку **NAT** и подтвердите свой выбор, нажав кнопку **OK**.

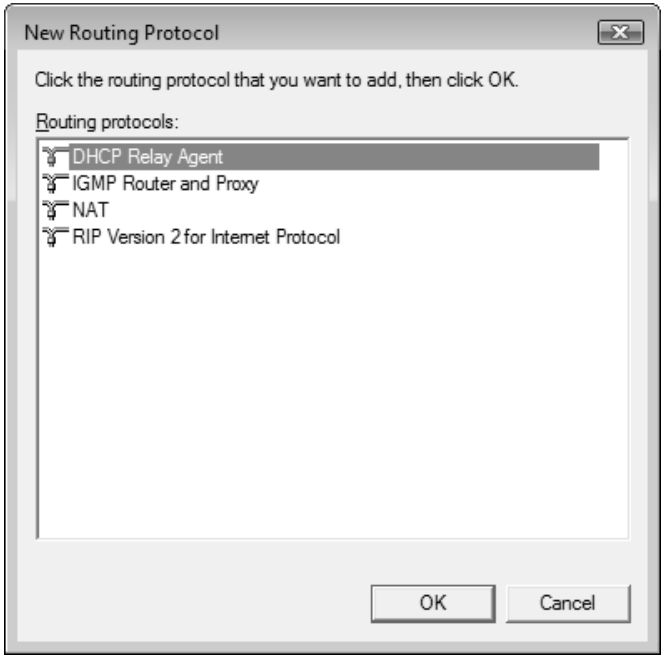


Рис. 6.35. Установка протокола преобразования сетевых имен

3. На следующем этапе требуется выбрать сетевые интерфейсы, которые будут работать с механизмом преобразования сетевых адресов. Вызовите контекстное меню папки **NAT** и выполните команду **New Interface** (Новый интерфейс).
4. Из списка установленных интерфейсов выберите требуемый и нажмите кнопку **OK**. Далее, в открывшемся окне на вкладке **NAT** (рис. 6.36), в зависимости от типа выбранного интерфейса, выполните следующие действия:
   - для сетевого интерфейса, подключенного к Интернету, выберите переключатель **Public interface connected to the Internet** (Общий интерфейс подключен к Интернету) и установите флажок **Enable NAT on this interface** (Включить NAT на данном интерфейсе);
   - для сетевого интерфейса, подключенного к локальной сети, установите переключатель **Private interface connected to the private network** (Частный интерфейс подключен к частной сети).

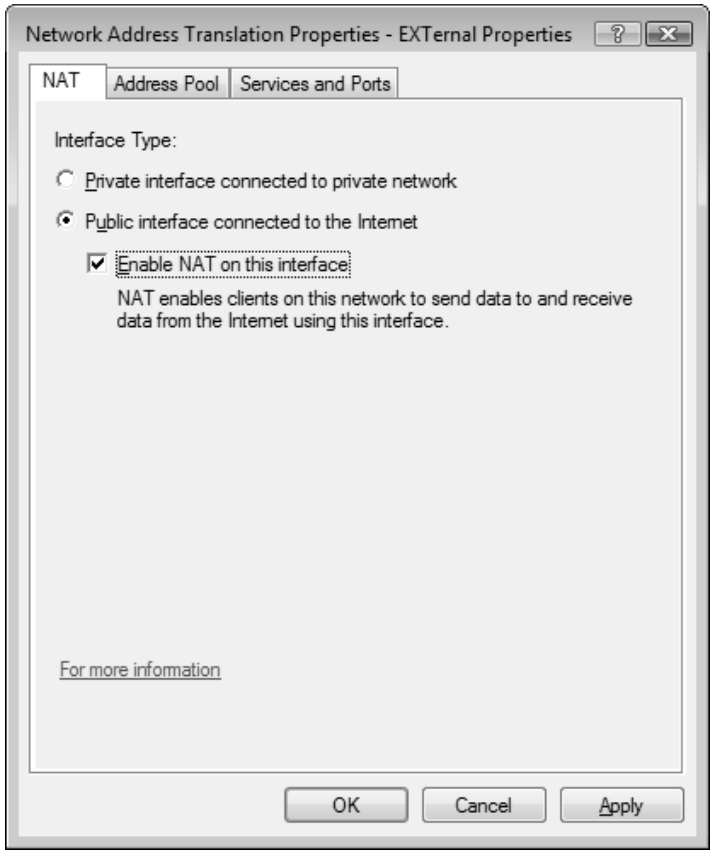


Рис. 6.36. Активизация механизма NAT для выбранного сетевого интерфейса

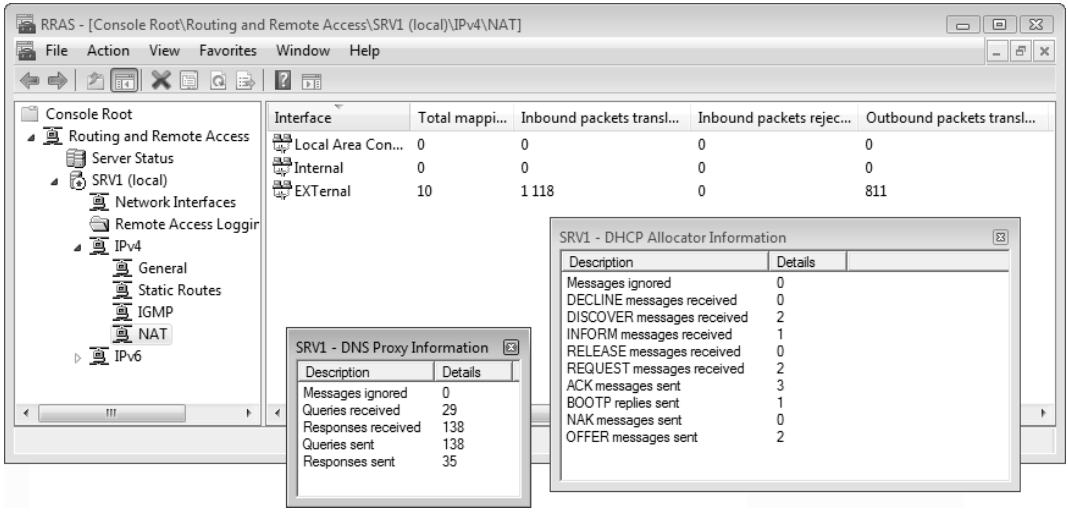


Рис. 6.37. Просмотр статистики по работе NAT

5. Закройте окно, нажав кнопку **ОК**. 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. 6.37).

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, откройте окно свойств папки **NAT**, перейдите на вкладку **Address Assignment** (Назначение адресов) (рис. 6.38) и установите 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.

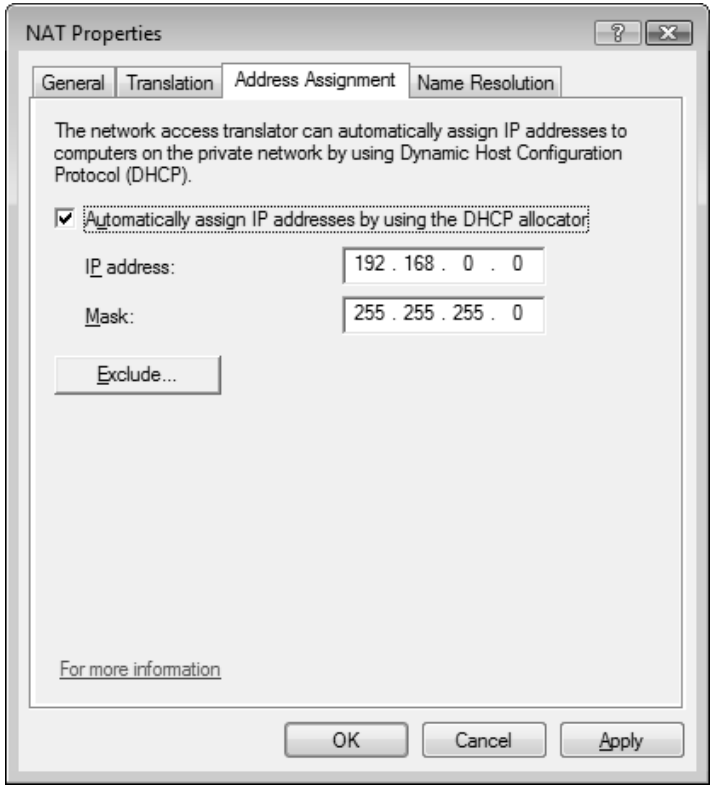


Рис. 6.38. Разрешение использования протокола DHCP для выделения адресов локальным хостам

По умолчанию предлагается весь диапазон адресов (вся подсеть), обслуживаемых локальным интерфейсом. При необходимости, нажав кнопку **Exclude** (Исключить), можно исключить некоторые адреса из этого диапазона.

Функция разрешения 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, откройте окно свойств папки **NAT**, перейдите на вкладку **Name Resolution** (Разрешение имен в адреса) (рис. 6.39) и установите флажок **Clients using Domain Name System (DNS)** (Для клиентов, использующих службу DNS).

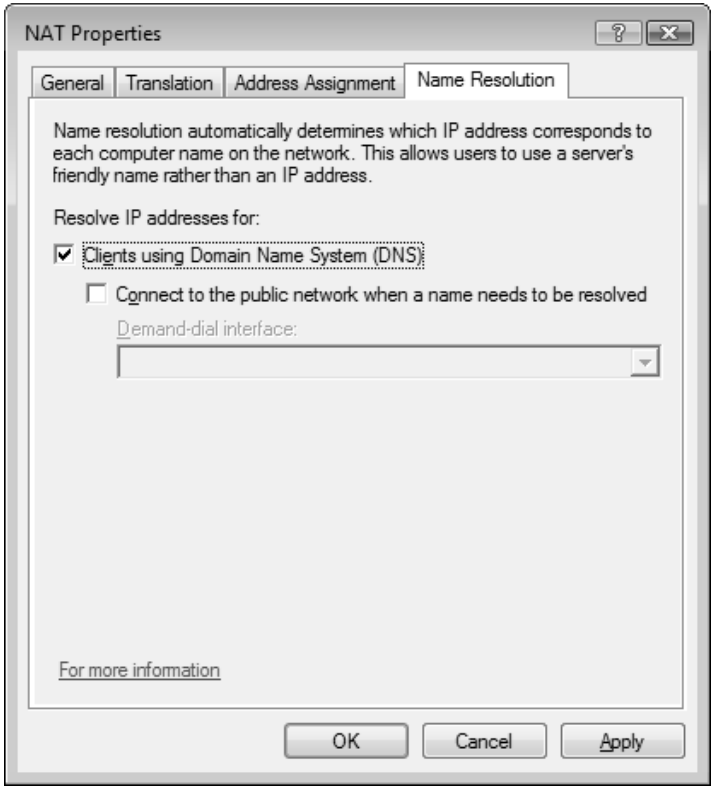


Рис. 6.39. Включение разрешения доменных имен через механизм NAT

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** (Подключаться при этом к пуб-

личной сети) и выбрать в списке **Demand-dial interface** (Интерфейс вызова по требованию) требуемый интерфейс.

Конфигурирование преобразования специальных портов и служб

Администратор может обеспечить более точную настройку механизма NAT, выполнив конфигурирование специальных портов. Фактически администратор задает специфические правила преобразования пакетов, приходящих на определенные порты. Подобное решение позволяет обеспечить прозрачное функционирование корпоративных приложений поверх механизма NAT. Например, администратор может определить порядок преобразования пакетов, приходящих на порт 25 (протокол SMTP).

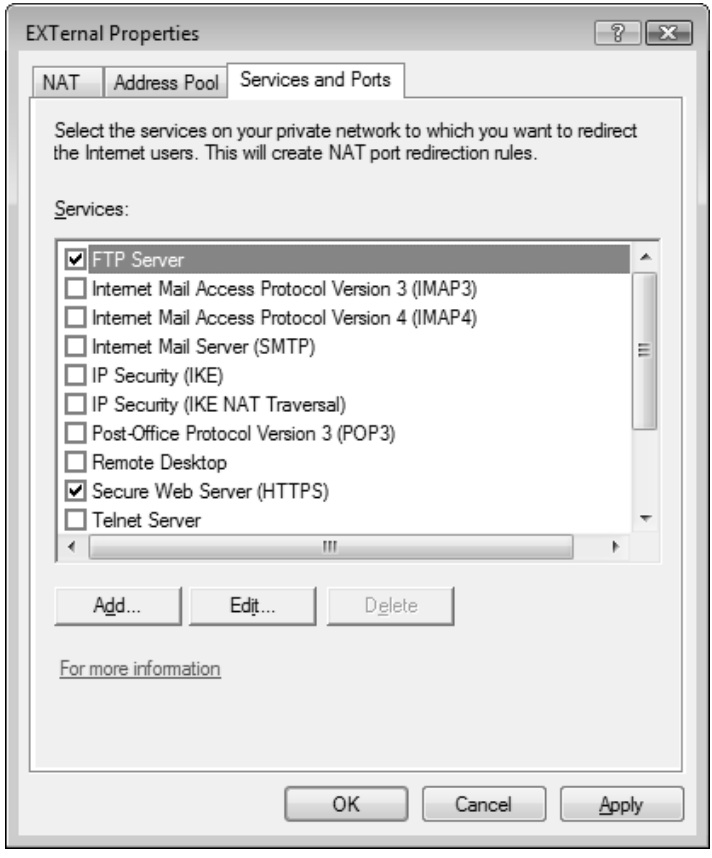


Рис. 6.40. Расширенная настройка преобразователя адресов

Расширенная настройка механизма преобразования портов осуществляется на вкладке **Services and Ports** (Службы и порты) в окне свойств внешнего сетевого

интерфейса, выбранного для NAT (см. рис. 6.36). Администратору предлагается выбор из 13 предопределенных сетевых служб (рис. 6.40). При необходимости можно создать и новые описания служб.

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 создания *нового* описания службы (правила преобразования) администратору необходимо помимо имени определить следующие параметры (рис. 6.41):

- 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) укажите 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;

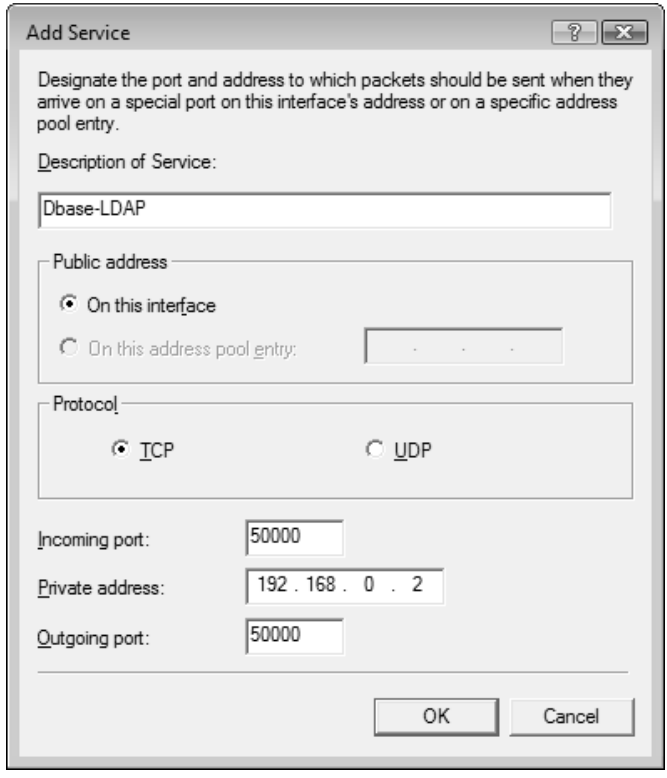


Рис. 6.41. Параметры нового правила преобразования портов

- 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 (статическую или получаемую от DHCP-сервера):

- 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.

Совместное использование интернет-подключения (ICS)

В простейших случаях развертывание службы RRAS может быть нецелесообразным, и можно воспользоваться более простым и традиционным решением. 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, требуются, как минимум, 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).

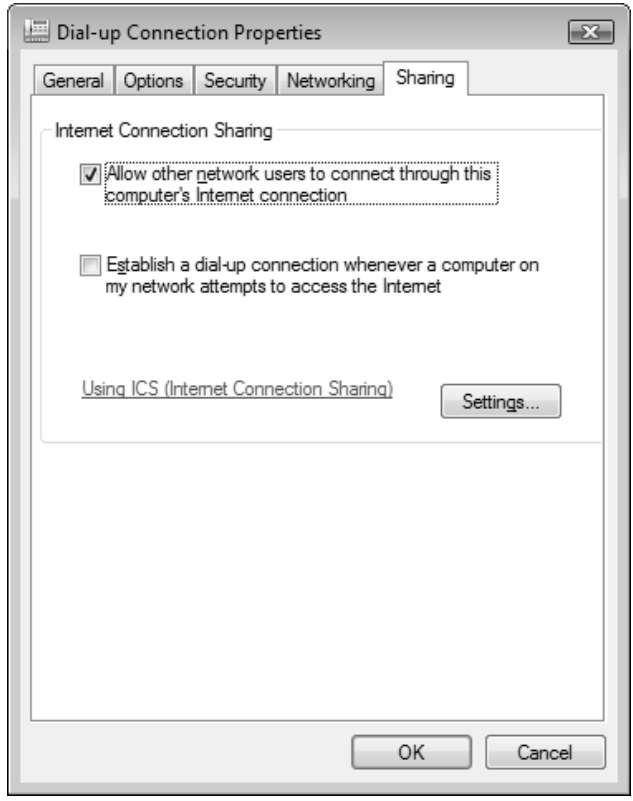


Рис. 6.42. Включение режима ICS на выбранном сетевом подключении

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 некоторого подключения, выберите его в окне сетевых подключений (см. рис. 6.11), откройте окно свойств и на вкладке **Sharing** (Доступ) установите флажок **Allow other network users to connect through this computer's Internet connection** (Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера) (рис. 6.42).

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]. В системах Windows Server 2008 другие пользователи сети не имеют возможности управлять общим интернет-подключением.

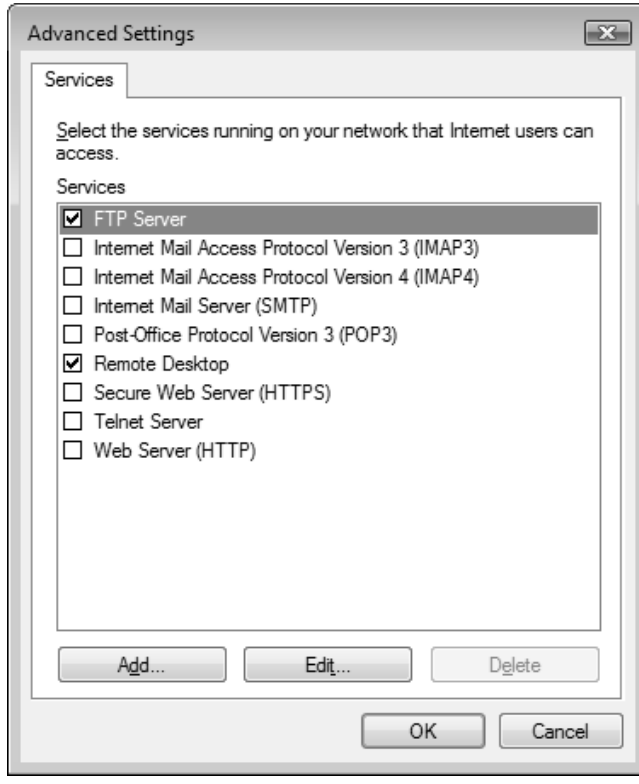


Рис. 6.43. Выбор сервисов, к которым будет разрешен доступ для пользователей Интернета

[1] У постоянных подключений типа ADSL этот флажок отсутствует.

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. 6.42) следует нажать кнопку **Settings** (Настройка) и в открывшемся окне (рис. 6.43) установить флажки рядом с именами служб, которые должны быть доступны.

Защита сетевых подключений с помощью встроенного брандмауэра Windows Firewall

Данный раздел завершает описание сетевых средств, поскольку в системах Windows Server 2008 встроенный брандмауэр является одним из центральных компонентов системы и защищает все сетевые подключения, а также весь трафик, проходящий через службу RRAS.

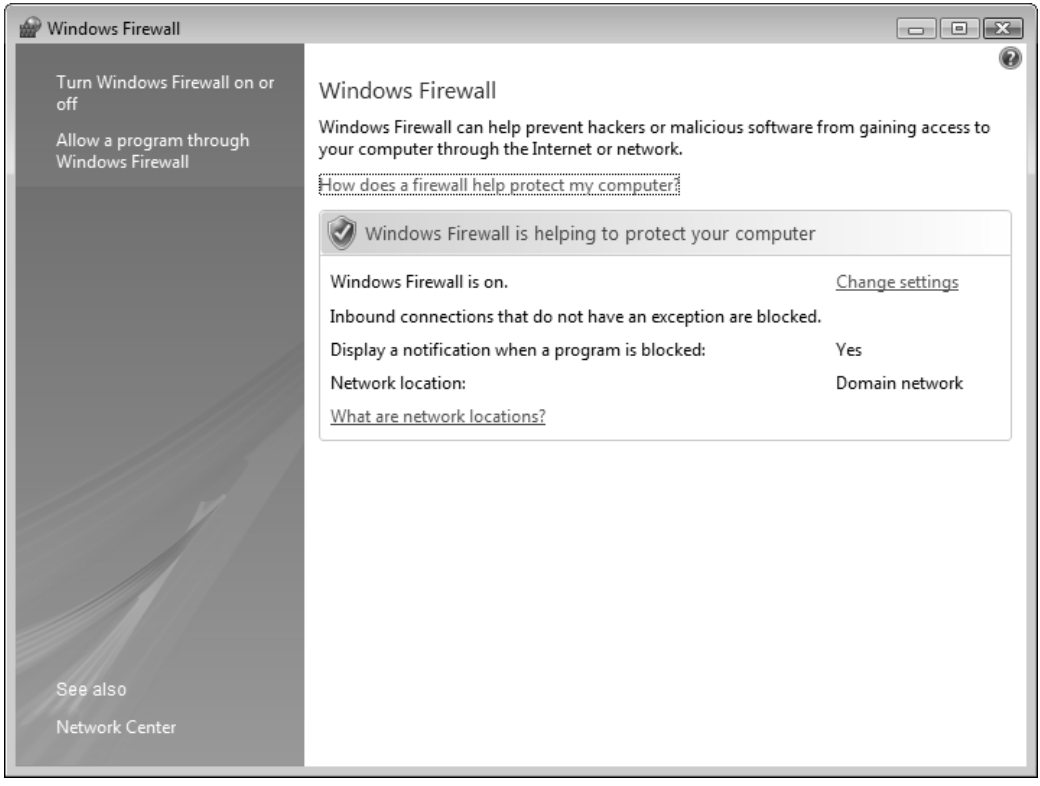


Рис. 6.44. Главное окно брандмауэра Windows

Брандмауэр *Windows Firewall* (Брандмауэр Windows), входящий в состав Windows Vista и Windows Server 2008, представляет собой модифицированный и значительно расширенный вариант средства Internet Connection Firewall (ICF), реализованного в предыдущих версиях 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.

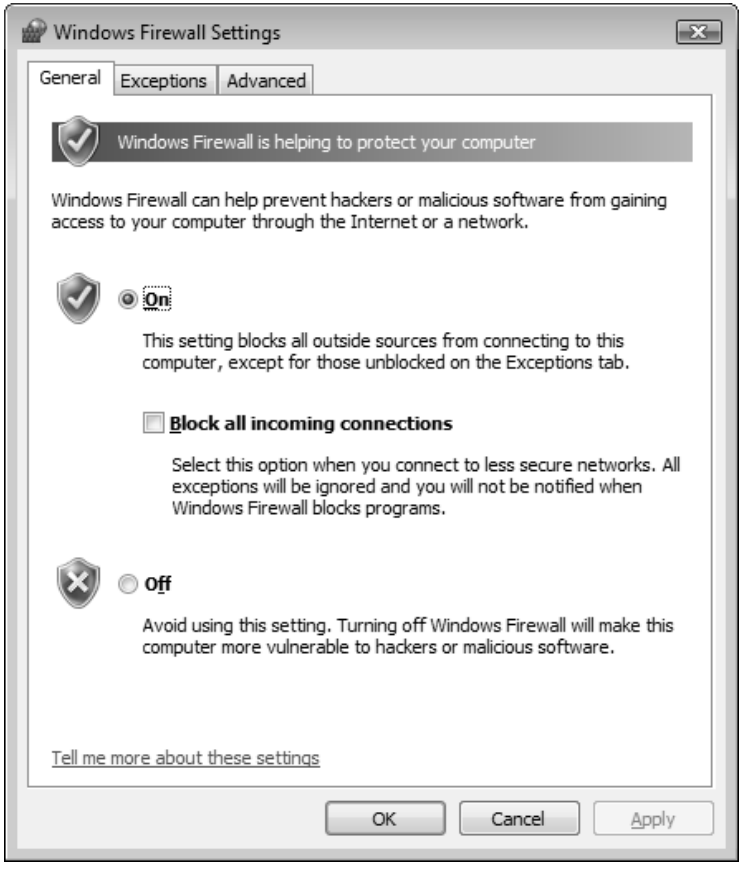


Рис. 6.45. Окно управления состоянием и параметрами брандмауэра Windows

Брандмауэр Windows Firewall можно запустить с панели управления (категория **Security** (Безопасность)) или из окна Центра управления сетями (см. рис. 6.3). На рис. 6.44 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).

В окне параметров (рис. 6.45), 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**).

Самой важной в интерфейсе брандмауэра является вкладка **Exceptions** (Исключения) (рис. 6.46) — здесь указываются программы и сервисы, которым *разрешен* доступ по сети.

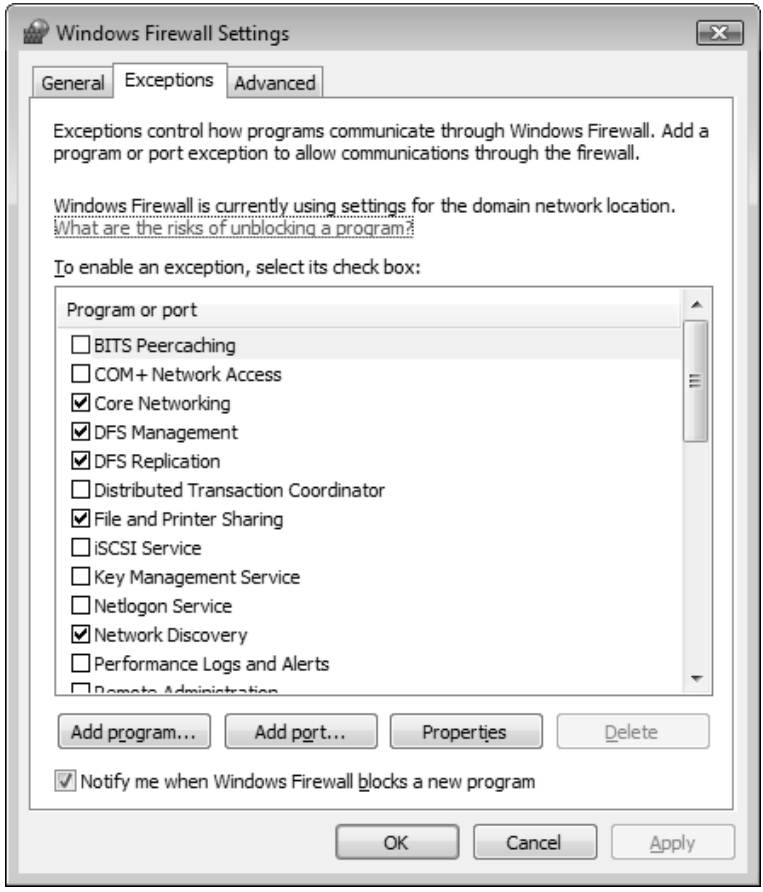


Рис. 6.46. Выбор разрешенных служб, доступных из внешней сети

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.

Флажок **Notify me when Windows Firewall blocks a new program** (Уведомлять, когда брандмауэр блокирует новую программу) (см. рис. 6.46) лучше держать установленным — в этом случае при попытке любой новой программы установить сетевое соединение брандмауэр будет сообщать об этом администратору и ожидать от него разрешения на работу программы (рис. 6.47). Если программа будет разблокирована, то брандмауэр включит порты, запрашиваемые приложением, в число разрешенных. После этого программа сможет работать беспрепятственно. Такой подход позволяет более строго следить за работой приложений, обращающихся к сети.



Рис. 6.47. Запрос на разрешение входящих подключений для запущенной программы

Нажав кнопку **Add port** (Добавить порт) (см. рис. 6.46), можно затем вручную указать дополнительные порты TCP или UDP, работа по которым будет разрешена (рис. 6.48). Для точного определения типа сети или диапазона адресов, которым будет разрешено обращаться к указанному порту, нажмите кнопку **Change scope** (Изменить область) и выберите нужные параметры (рис. 6.49). Аналогичным образом изменяется область допустимых адресов и для прикладных программ *(см. далее)*.

Кнопка **Add program** (Добавить программу) на вкладке исключений (см. рис. 6.46) позволяет перейти в окно выбора приложений (рис. 6.50), которые смогут взаимодействовать с другими компьютерами через сеть. Для программ, как и для дополнительных портов, можно указывать область допустимых адресов компьютеров (кнопка **Change scope**).

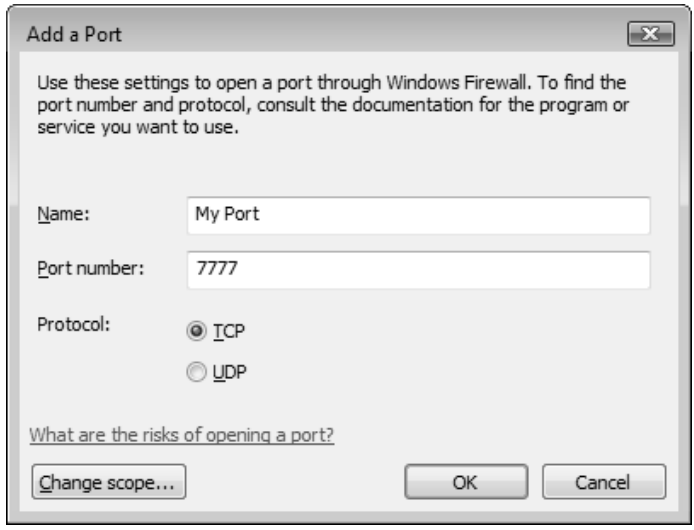


Рис. 6.48. Определение параметров порта, доступ через который будет разрешен брандмауэром Windows

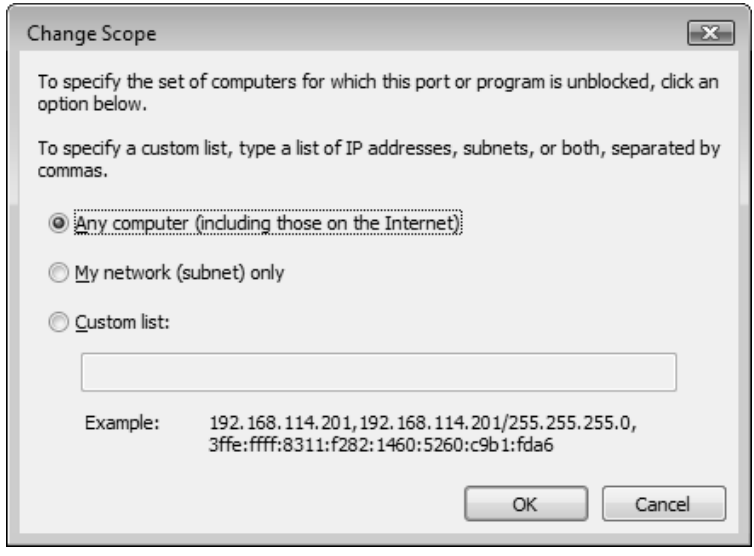


Рис. 6.49. В этом окне можно ограничить список компьютеров, получающих доступ к определенной программе или работающих с протоколом, разблокированным брандмауэром Windows

На вкладке **Advanced** (Дополнительно) (рис. 6.51) можно указать, с какими сетевыми подключениями будет работать брандмауэр (параметры будут одинаковыми для всех подключений). В 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.

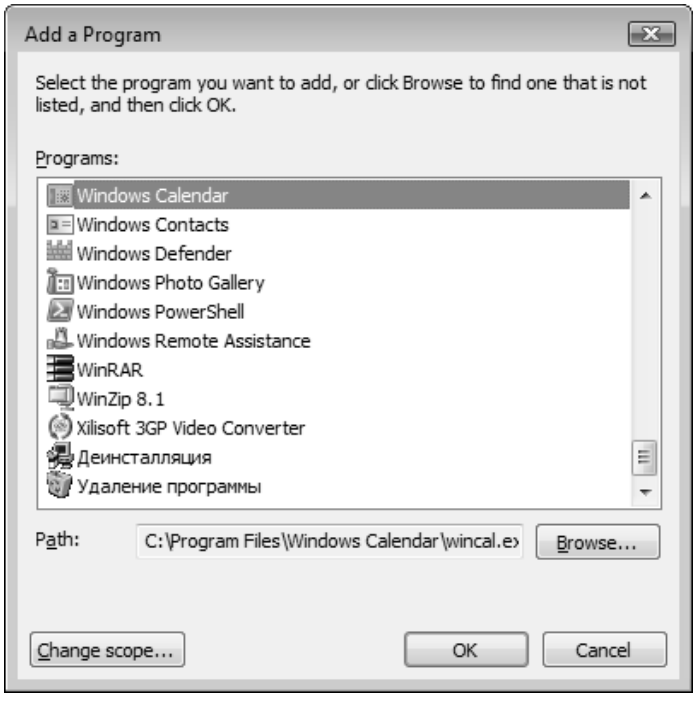


Рис. 6.50. Выбор программ, с которыми можно будет взаимодействовать через сеть

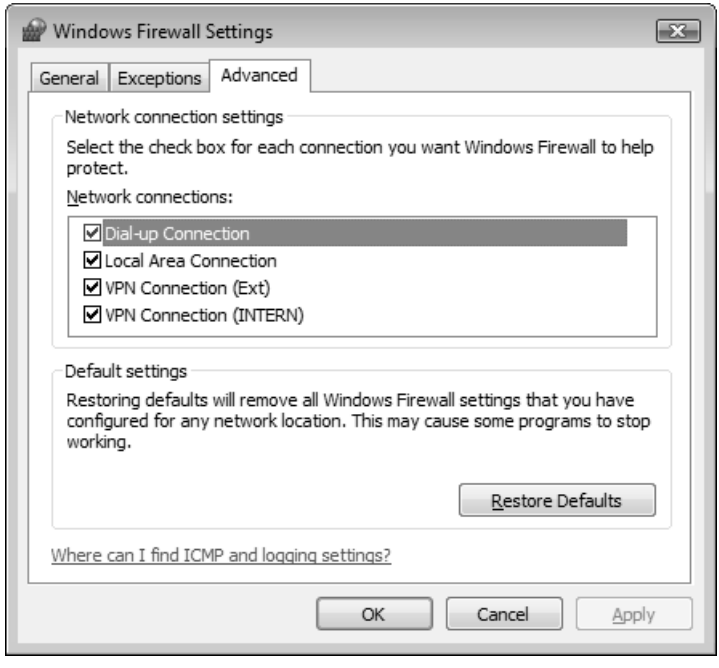


Рис. 6.51. Окно выбора дополнительных параметров брандмауэра

Кнопка **Restore Defaults** (По умолчанию) (см. рис. 6.51) позволяет восстановить все стандартные значения параметров, принятые для выбранной категории сети.

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.

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).

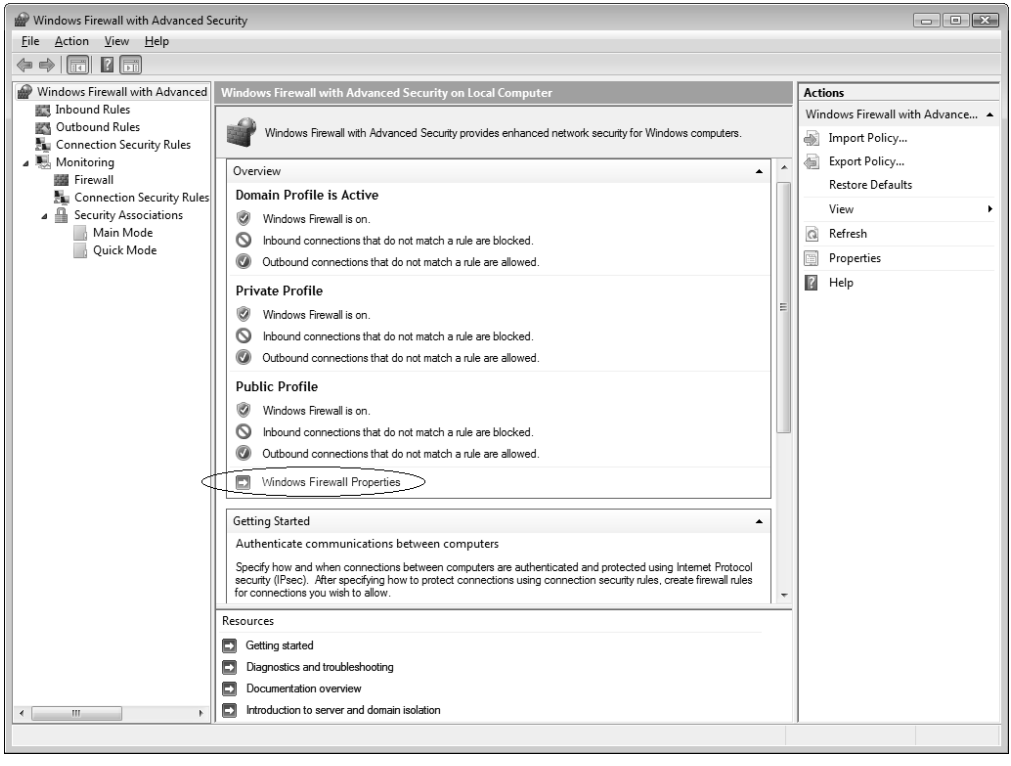


Рис. 6.52. Главное окно оснастки **Windows Firewall with Advanced Security**

В главном окне (рис. 6.52) сразу после запуска оснастки можно видеть основные параметры, заданные для каждого сетевого профиля (связанного с размещением компьютера, или категорией сети).

Кнопка **Windows Firewall Properties** (Свойства брандмауэра Windows) в центре начальной страницы позволяет перейти в окно настроек (рис. 6.53), 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.

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 соответствии со своими представлениями о требованиях безопасности (в данном случае речь идет о наборе разрешенных портов), предъявляемых к каждой категории сети.

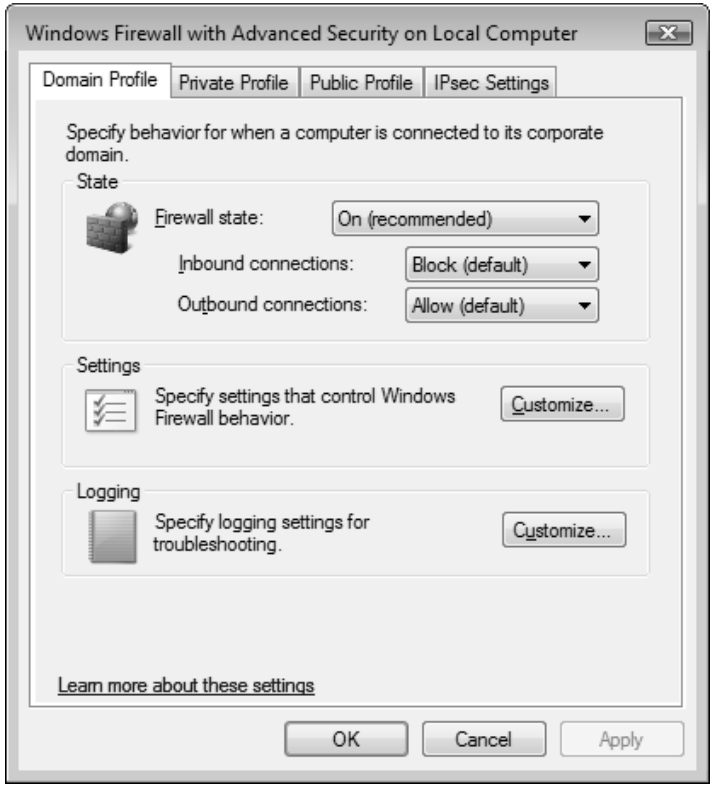


Рис. 6.53. Глобальные параметры брандмауэра для каждого типа сетевого профиля и для протокола IPSec

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. 6.54, в системе имеется множество предустановленных правил, многие параметры которых менять нельзя. Разрешенные правила отмечены значками зеленого цвета.

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. 6.55 в качестве примера показано предустановленное правило, регламентирующее доступ к общим папкам и принтерам по протоколу SMB).

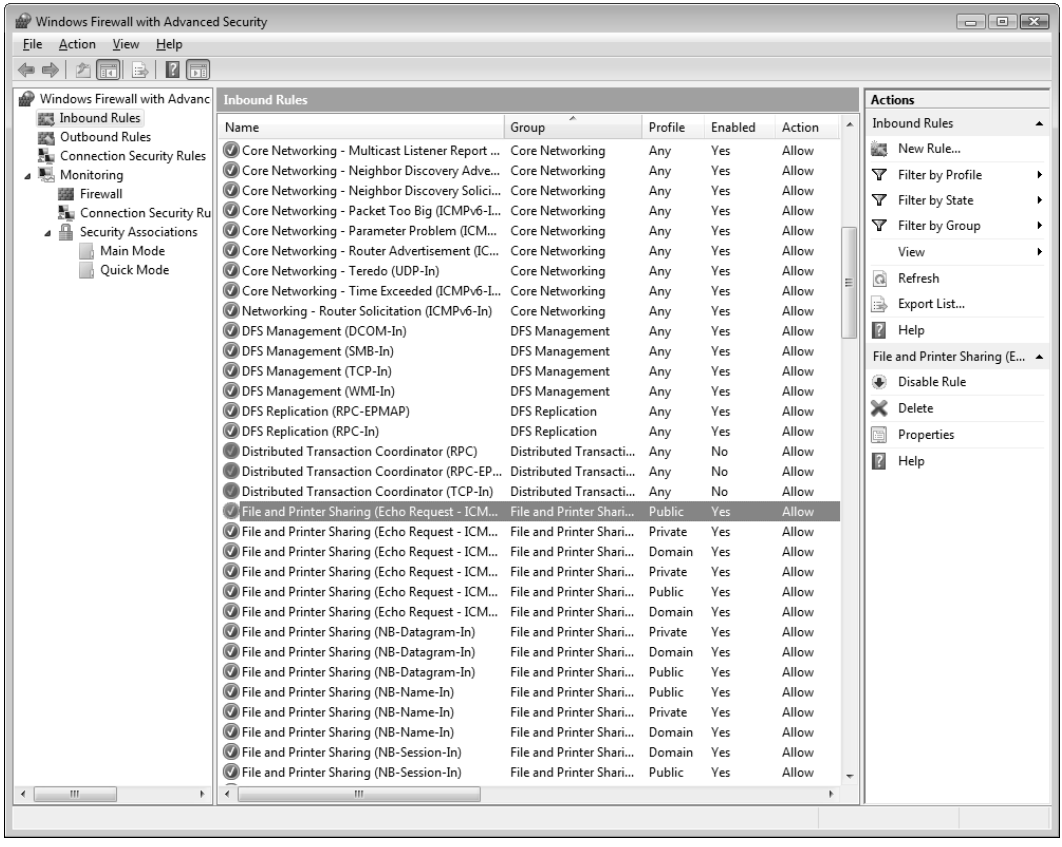


Рис. 6.54. Перечень правил, установленных для входящих соединений

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 распространяться только на те протоколы и порты, адреса и компьютеры, которые заданы в окне свойств (рис. 6.56); на вкладке **Advanced** (Дополнительно) также можно указать, для какого именно профиля будет использоваться данное правило.

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.

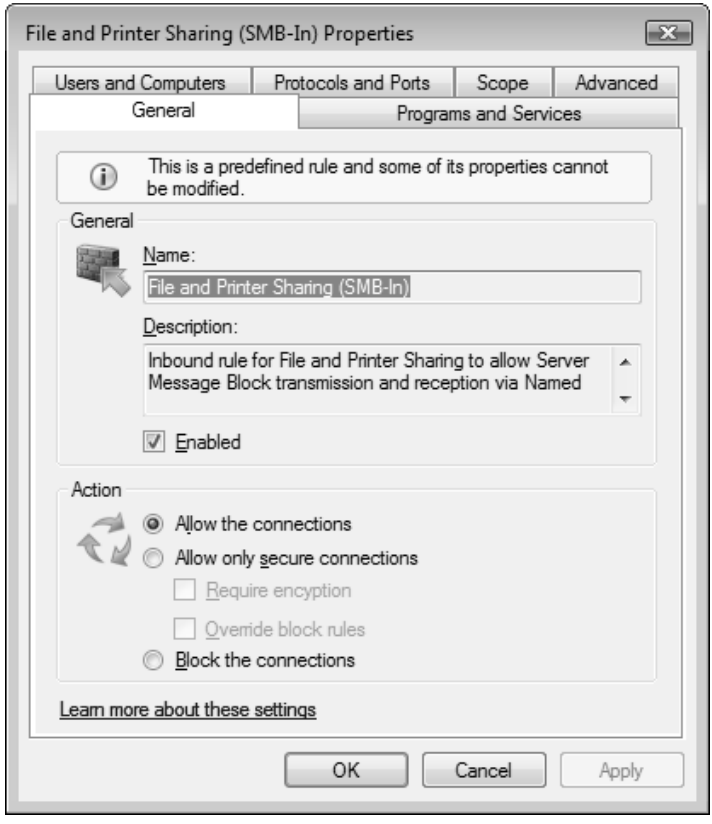


Рис. 6.55. Определение действий для выбранного правила

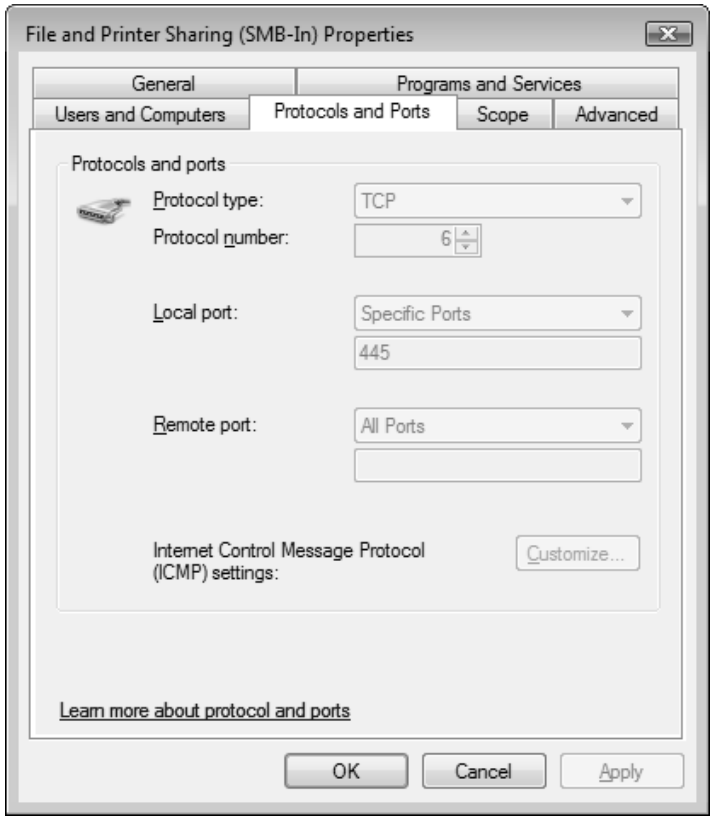


Рис. 6.56. Протокол и порт, на которые распространяется данное правило

Настройка сетевых параметров и брандмауэра из командной строки

Утилита командной строки *Netsh.exe* предназначена для настройки параметров сетевых подключений и может использоваться в любых версиях Windows Server 2008 (включая Windows Server Core и Hyper-V Server). Утилита запускается в интерактивном или командном режиме. В первом случае администратор пошагово выбирает нужный *контекст* (набор сетевых параметров, относящихся к определенному компоненту или протоколу) и выполняет имеющиеся команды. Во втором — все параметры задаются утилите при запуске, и она выполняет конкретную задачу (этот режим можно использовать и из командных файлов). Для каждого контекста легко получить набор допустимых команд, введя слово `help` или просто символ вопроса. Рассмотрим на примерах некоторые возможности утилиты Netsh.

Назначение IP-адресов

Для просмотра текущих параметров стека TCP/IP (для протокола IPv4 или IPv6) используется следующая команда:

```
netsh interface ipv4 show config
```

Она позволяет видеть название интерфейсов; например, подключение по локальной сети в англоязычных версиях обычно называется "Local Area Connection". Также имена интерфейсов можно получить с помощью команды `netsh interface ipv4 show interfaces`.

Имя интерфейса важно знать при изменении параметров стека. Например, следующая команда назначает подключению по локальной сети статический IP-адрес (192.168.0.2 с маской 255.255.255.0) и адрес шлюза (192.168.0.1 с метрикой 1):

```
netsh interface ipv4 set address "Local Area connection" static 192.168.0.2
255.255.255.0 192.168.0.1 1
```

Чтобы включить получение адреса от сервера DHCP, используется команда `netsh interface ipv4 set address name="Local Area Connection" source=dhcp`.

Для назначения подключению статического адреса предпочитаемого (preferred) DNS-сервера (192.168.0.1) можно выполнить такую команду:

```
netsh interface ipv4 set dnsserver "Local Area Connection" static 192.168.0.1
primary
```

Дополнительный адрес DNS-сервера задается с помощью параметра `add dnsserver`.

Управление брандмауэром

Многочисленные возможности утилиты Netsh 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).

С помощью команды `netsh firewall show state` можно увидеть текущее состояние брандмауэра Windows (включая выбранный сетевой профиль); также удобна команда `netsh firewall show opmode`. Для просмотра параметров, установленных для всех профилей, служит команда `netsh firewall show config`.

Группы параметров брандмауэра 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.

Команда `netsh firewall set opmode mode = DISABLE` позволяет полностью ***выключить*** брандмауэр; при использовании параметра `ENABLE` брандмауэр ***активизируется***.

Для работы с брандмауэром Windows в режиме повышенной безопасности используется контекст "netsh advfirewall".

С помощью следующей команды можно увидеть параметры всех правил для входящих (`in`) или исходящих (`out`) соединений (если параметр `dir` отсутствует, то отображаются все имеющиеся правила):

```
netsh advfirewall firewall show rule name=all dir=in
```

Можно указать имя конкретного правила, например (регистр букв в имени значения не имеет):

```
netsh advfirewall firewall show rule name="Winsock FTP Client" dir=in
```

Названия правил можно также видеть на панели правил входящих и исходящих соединений в окне оснастки **Windows Firewall with Advanced Security** (Брандмауэр Windows в режиме повышенной безопасности) (см. рис. 6.54). Здесь отображаются и названия *групп* правил. (Название правила легко скопировать из окна его свойств и вставить в нужную команду в окне консоли.)

Включать и выключать правила можно как для отдельного имени (параметр `name`), так и для группы имен (параметр `group`). Например, следующая команда позволяет запретить эхо-ответы для всех профилей (при использовании параметра `profile` можно назначить операцию для конкретного профиля):

```
netsh advfirewall firewall set rule name="File and Printer Sharing (Echo Request - ICMPv4-In)" new enable=no
```

Следующая команда разрешает все правила, входящие в группу Remote Administration, для всех профилей:

```
netsh advfirewall firewall set rule group="Remote Administration" new enable=yes
```



Глава 7

Доменные службы Active Directory и групповые политики

В этой главе рассматриваются основные задачи, возникающие при развертывании леса доменов Active Directory, и средства их администрирования. Описываются возможности групповых политик и способы их использования в доменах, где политики являются главным способом централизованного управления пользовательской средой и рабочими параметрами компьютеров.

> ***Примечание***
>
> Некоторые административные оснастки и утилиты используются также для работы со службами *Active Directory Lightweight Directory Services* (Службы Active Directory облегченного доступа к каталогам (AD LDS)), которые позволяют устанавливать на серверах "автономные" экземпляры каталогов Active Directory, не зависящих от наличия службы доменов.

Конфигурирование службы DNS для развертывания доменов Active Directory

Рассмотрим особенности настройки службы DNS, которые администратор должен учитывать для сети с доменами Active Directory. Эта служба является базовым и обязательным компонентом для развертывания леса доменов, и от правильности ее параметров во многом зависит работоспособность доменной среды в целом. В силу того, что существует множество сетевых конфигураций и требований к корпоративной сети, сложно дать однозначные рекомендации по настройке DNS, и мы изложим основные решения, которые можно комбинировать и адаптировать к конкретным условиям. (Хотя в простейших случаях вмешательство администратора в настройку DNS-сервера вообще не требуется.)

Автоматическая настройка DNS-сервера

Простейшая ситуация — когда при создании первого контроллера в лесу доменов разрешается установка DNS-сервера (см. рис. 7.4). В этом случае мастер установки Active Directory после установки служб каталога сам устанавливает и конфигурирует DNS-сервер на этом контроллере, 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 с именем intern.dom представлен на рис. 7.1.

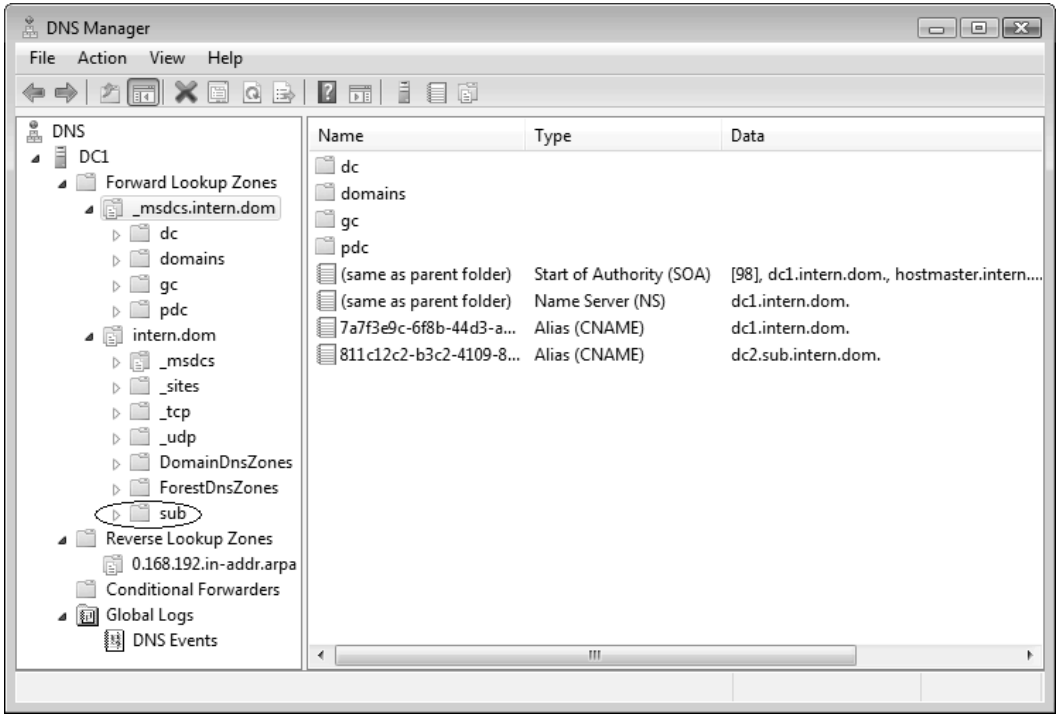


Рис. 7.1. Зоны DNS для корневого домена леса intern.dom, созданные и сконфигурированные мастером установки Active Directory

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.

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).)

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.

Можно заранее установить службу DNS 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 не будет отличаться от той, которая была описана в предыдущем разделе.

---

[1] Имена подобного вида являются зарезервированными в домене (поскольку используются особым образом), и не следует создавать собственные разделы с такими именами.

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. Примером несмежного имени для леса с корневым доменом intern-dom будет домен intern-new.dom;
- DNS-поддомены в авторитетной зоне дерева доменов Active Directory создаются на предпочитаемом DNS-сервере автоматически при создании первого контроллера *дочернего домена*. На рис. 7.1 отмечена зона домена sub.intern.dom (входящего в лес intern.dom). Поскольку при создании этого домена на контроллере одновременно устанавливался DNS-сервер, то был 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 авторитетные зоны можно вручную создавать и заранее (до развертывания самих доменов). В этом случае их можно будет конфигурировать независимо от родительских зон.

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.

Установка и удаление контроллеров домена

Термины "создание контроллера домена", "установка доменных служб Active Directory" и "повышение роли сервера" (promotion) описывают один и тот же про-

цесс — нельзя создать контроллер домена, не установив доменные службы Active Directory (аналогично можно говорить об "удалении контроллера", "удалении Active Directory" или о "понижении роли контроллера").

В отличие от доменных служб Active Directory, экземпляры служб *Active Directory Lightweight Directory Services* (Службы Active Directory облегченного доступа к каталогам (AD LDS)) никак не связаны с контроллерами домена и могут устанавливаться на любых серверах Windows Server 2008, причем на одном сервере может находиться несколько разных каталогов (с различными именами). Даже если службы AD LDS развертываются и на контроллере (контроллерах) домена, то их топология репликации не связана с доменом и выполняется с помощью других механизмов (прямых RPC-вызовов).

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.

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). 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.

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* (Windows Time, сервис W32Time).

Особенности создания 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 Controllers 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. Otherwise, type any
other key and press ENTER to quit.

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>
```

[1] Обратите внимание на имена LDF-файлов, совпадающие с номером схемы. Последняя версия — 44.

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*** этот домен имеет функциональный уровень не выше *Windows 2000 native*. При создании нового домена на базе серверов Windows Server 2003 необходимо, чтобы функциональный уровень леса Windows Server 2008 бы не выше *Windows 2000*. (Нужно понимать, что во всех этих случаях номер схемы каналога будет соответствовать уровню Windows Server 2008.) В случае более высоких функциональных уровней при установке службы Active Directory на серверах Windows Server 2003 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 леса 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.

Запуск мастера установки Active Directory

В полных версиях Windows Server 2008 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) или в окне **Run** (Выполнить).

В любом случае на первом этапе 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 продолжения 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 содержимого файла ответов будет приведен ниже. Автоматическую установку контроллеров удобно выполнять при работе с системами Windows Server Core, поскольку подготовить файл ответа проще, чем выбирать множество параметров для утилиты Dcpromo.

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 мастер вызывается непосредственно, то после копирования двоичных файлов (при этом всегда отображается специальное информационное окно) появится его первое окно. Имеющийся в этом окне флажок **Use advanced mode installation** позволяет выключить дополнительные возможности при работе мастера установки Active Directory (это соответствует выполнению команды `dcpromo` с параметром `/adv`). Данные возможности перечислены в табл. 7.1.

Таблица 7.1. *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)
Дополнительный контроллер домена в существующем домене	**Install from Media** (Установка из архива) (см. рис. 7.5) **Source Domain Controller** (Исходный контроллер домена) **Specify Password Replication Policy** (Указать политику репликации паролей) (только при установке RODC-контроллера) (см. рис. 7.6)
Создание учетной записи для RODC-контроллера	**Specify Password Replication Policy** (Указать политику репликации паролей)

Таблица 7.1 *(окончание)*

Этап установки	Дополнительные опции выбора параметров
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 без расширенных возможностей, то нужно помнить о том, что некоторые параметры будут устанавливаться по умолчанию и определенные возможности (перечисленные в табл. 7.1) будут недоступны.

Первое, что делает мастер установки Active Directory — предупреждает о новых значениях параметров безопасности, которые могут помешать клиентам подключаться к доменам. Нужно учесть все изложенные соображения и ознакомиться с указанной статьей базы знаний Microsoft (KB).

В общем случае при установке Active Directory существуют четыре возможности (рис. 7.2); от выбора опции зависят дальнейшие шаги установки и параметры, которые потребуется ввести на этих этапах[1].

Каждый вариант интуитивно понятен, и требуется лишь ответить на вопросы мастера. Мы рассмотрим начальное развертывание доменов Active Directory, 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[2]:

- 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 лесу) — дочерний домен любого имеющегося домена (sub.intern.dom);

[1] Опции мастера установки Active Directory немного изменились по сравнению с версией, имеющейся в Windows Server 2003, однако логика работы и количество вариантов создания контроллеров фактически остались прежними.

[2] Имена доменов условные, выбраны для примера.

- **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).

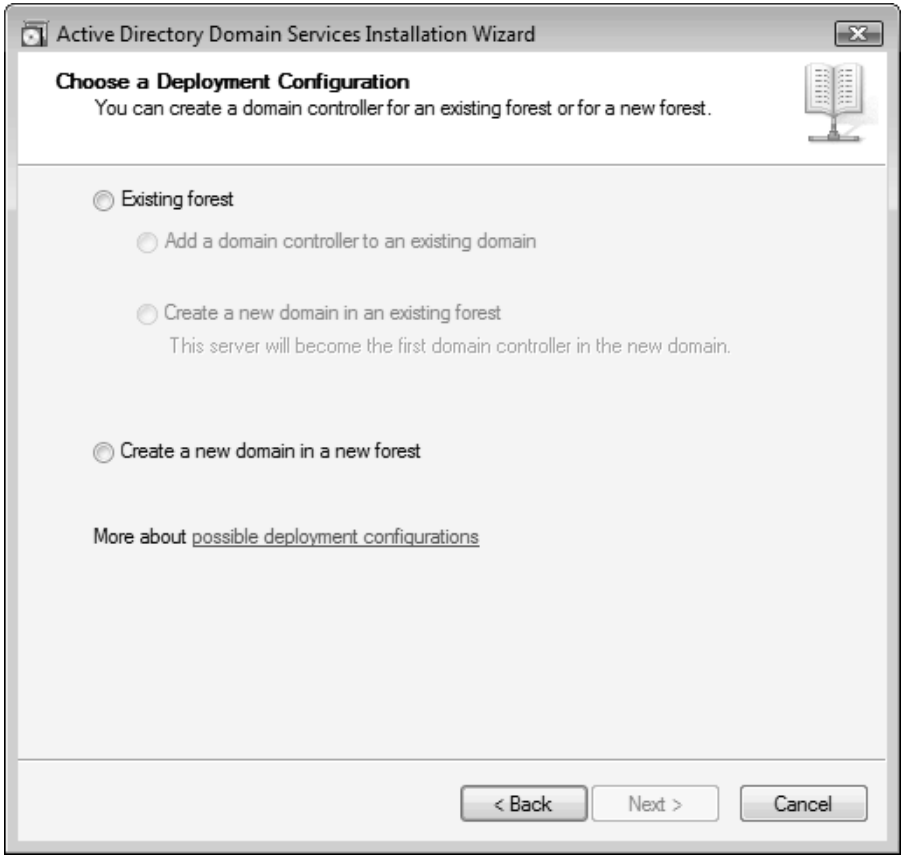


Рис. 7.2. Выбор местоположения нового контроллера в топологии доменов Active Directory

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 выглядит следующим образом (рассматривается создание нового леса):

1. Введите имя корневого домена леса. В зависимости от сделанного ранее выбора это имя будет использоваться для создания 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.
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.)

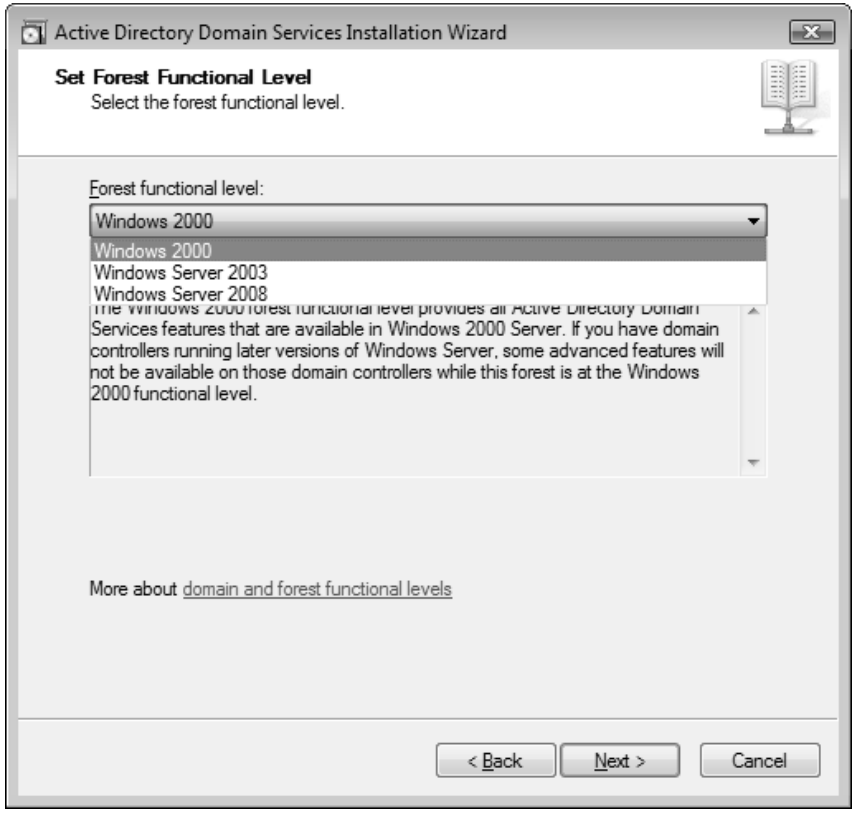


Рис. 7.3. Выбор функционального уровня нового леса

3. Затем, в отличие от контроллеров на базе Windows Server 2003, можно сразу установить функциональный уровень (режим работы) нового *леса*, отличный от "ми-

нимального" (рис. 7.3). Соответственно все домены, создаваемые в этом лесу, должны (и будут) иметь уровень не ниже того, который выбран на этом этапе.

4. Аналогичным образом при установке контроллера также можно задать сразу функциональный уровень нового *домена*. 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.

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. 7.4).

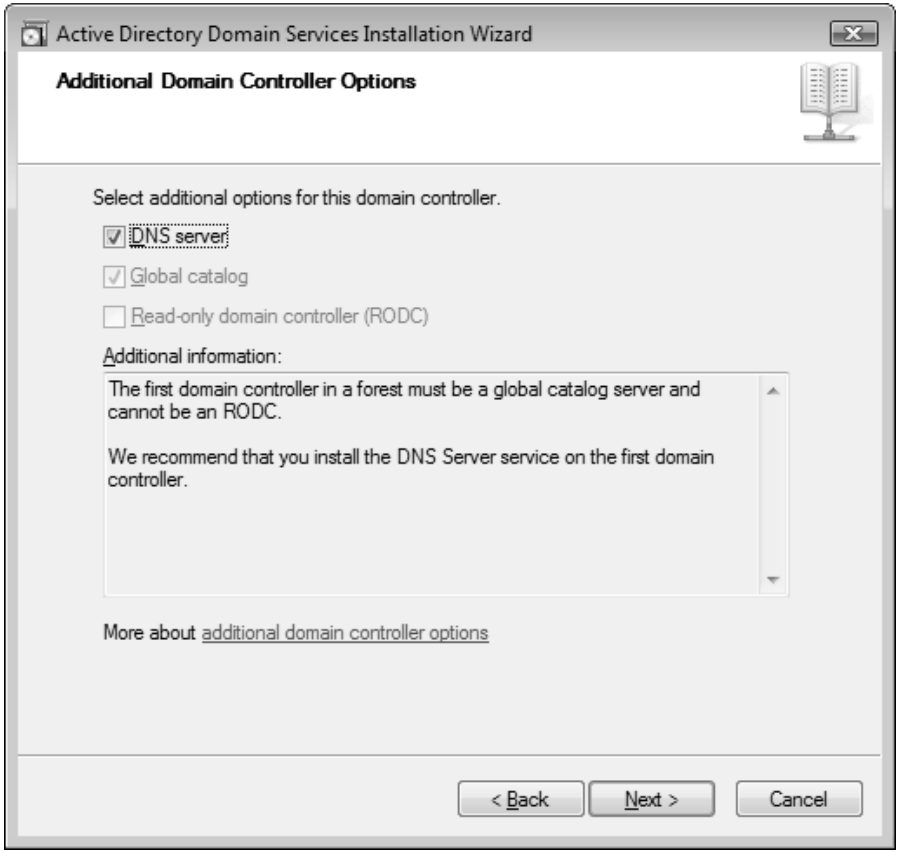


Рис. 7.4. Выбор дополнительных свойств нового контроллера домена

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 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.

6. На следующем этапе мастер проверяет конфигурацию службы DNS. Если появляется сообщение о невозможности регистрации имени нового контроллера домена, 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.

7. Укажите местоположение файлов базы данных Active Directory, журналов и тома SYSVOL. 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. 1.21).

9. В итоговом окне мастера проверьте правильность выбранных параметров. В случае ошибок можно вернуться на любой описанный выше шаг 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).

   Ниже приведен пример файла ответов для конфигурации нового контроллера домена, рассмотренной выше (это обычный текстовый файл в формате txt; необходимо указать пароль режима восстановления — после выполнения операции он будет автоматически удален из файла!):

```
; DCPROMO unattend file (automatically generated by dcpromo)
; Usage:
;   dcpromo.exe /unattend:C:\AD-Install-DC1.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=пароль
; Run-time flags (optional)
; RebootOnCompletion=Yes
```

Такой файл ответов можно использовать и для установки контроллера на базе систем Windows Server Core. Обратите внимание, что в этом примере задана установка DNS-сервера на создаваемом контроллере (при этом сервер будет автоматически настроен на использование указанного имени нового леса).

10. После нажатия кнопки **Next** (Далее) в окне просмотра выбранных параметров (Summary) ***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 лесу, 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).

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).

Использование утилиты Dcpromo из командной строки

Использование файлов ответов *(см. выше)* или утилиты Dcpromo с параметрами является единственным способом создания контроллеров домена на базе редакций Windows Server 2008 Core. Необходимые в каждом случае параметры зависят от топологии существующего леса доменов, поэтому мы для примера рассмотрим создание нового леса и добавление контроллера в имеющийся домен. Другие варианты уже не будут отличаться принципиально.

Создание нового леса с установкой DNS-сервера

Следующая команда позволяет создать новый лес с DNS-именем intern.dom (имя произвольное), а также установить и сконфигурировать DNS-сервер:

```
dcpromo /InstallDNS:Yes /NewDomain:Forest /NewDomainDNSName:intern.dom
/ReplicaOrNewDomain:Domain /SafeModeAdminPassword:SafeMode123
```

В команде требуется указать сложный пароль для режима восстановления. После выполнения команды система автоматически перезагружается.

DNS-сервер устанавливать не обязательно, если в сети развернута служба DNS, на компьютере задан предпочитаемый (preferred) DNS-сервер, на котором создана авторитетная зона и разрешено ее обновление.

Установка дополнительного контроллера в имеющемся домене

Чтобы установить дополнительный контроллер в домене с именем intern.dom, достаточно выполнить следующую команду:

```
dcpromo /InstallDNS:No /ReplicaDomainDNSName:intern.dom
/ReplicaOrNewDomain:Replica /SafeModeAdminPassword:SafeMode123
/UserDomain:intern.dom /UserName:administrator /Password:*
```

Как можно видеть, при этом указывается учетная запись пользователя, имеющего право на выполнение операции, ее пароль и имя домена.

Создание дочернего домена

После приведенных примеров команда для создания дочернего домена sub (произвольное имя) для родительского домена intern.dom кажется уже достаточно очевидной:

```
dcpromo /ChildName:sub /InstallDNS:No /NewDomain:Child
/ParentDomainDNSName:intern.dom /ReplicaOrNewDomain:Domain
/SafeModeAdminPassword:SafeMode123 /UserDomain:intern.dom
/UserName:administrator /Password:*
```

Полное DNS-имя дочернего домена будет выглядеть так: sub.intern.dom.

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 C:\InstallationMedia-DC1
Creating snapshot...
Snapshot set {2f19a2a6-b3fd-4103-ba28-692ab4ecc668} generated successfully.
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: C:\InstallationMedia-DC1\Active Directory\ntds.dit
                 Defragmentation  Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................

Copying registry files...
Copying C:\InstallationMedia-DC1\registry\SYSTEM
Copying C:\InstallationMedia-DC1\registry\SECURITY
Snapshot {c81a37c3-75d1-4531-a029-b1544dbc2c27} unmounted.
IFM media created successfully in C:\InstallationMedia-DC1
```

```
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. (Можно также запустить мастер с помощью команды `dcpromo /adv`.) Дальнейшие шаги следующие:

1. После выбора домена, для которого создается резервный контроллер, и дополнительных параметров контроллера (см. рис. 7.4) появится окно **Install from Media** (Установка с носителя) (рис. 7.5). Укажите здесь 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.

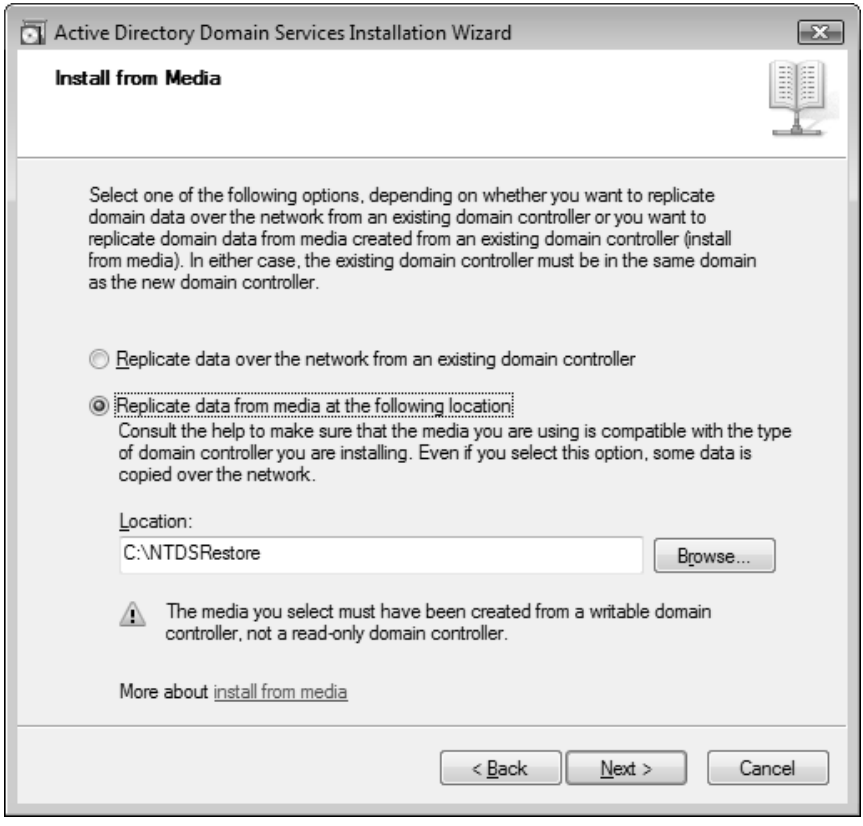


Рис. 7.5. Выбор установки контроллера из архивной копии

2. На следующем шаге можно явно указать, с какого именно контроллера домена будет осуществляться репликация данных каталога (эта опция также 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.

После всех выполненных действий процедура создания контроллера домена выполняется как обычно, все дальнейшие шаги уже были описаны ранее.

При запуске утилиты Dcpromo из окна консоли используется уже приведенный выше *(см. разд. "Установка дополнительного контроллера в имеющемся домене")* набор параметров, к которому добавляется ключ, указывающий папку, в которой хранится копия базы данных Active Directory (C:\InstallationMedia-DC1):

```
dcpromo /InstallDNS:No /ReplicaDomainDNSName:intern.dom
/ReplicaOrNewDomain:Replica /ReplicationSourcePath:C:\InstallationMedia-DC1
/SafeModeAdminPassword:SafeMode123 /UserDomain:intern.dom
/UserName:administrator /Password:*
```

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.

При установке RODC-контроллера необходимо задать политику репликации паролей (рис. 7.6), т. е. определить, пароли каких пользовательских учетных записей будут 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).

Для RODC-контроллера можно создать специальную группу администраторов или пользовательскую учетную запись и указать ее при создании контроллера (рис. 7.7). Данная учетная запись получит право закончить установку контроллера (например,

после физического перемещения компьютера на площадку удаленного подразделения). Также указанная учетная запись будет иметь локальные административные полномочия на данном контроллере.

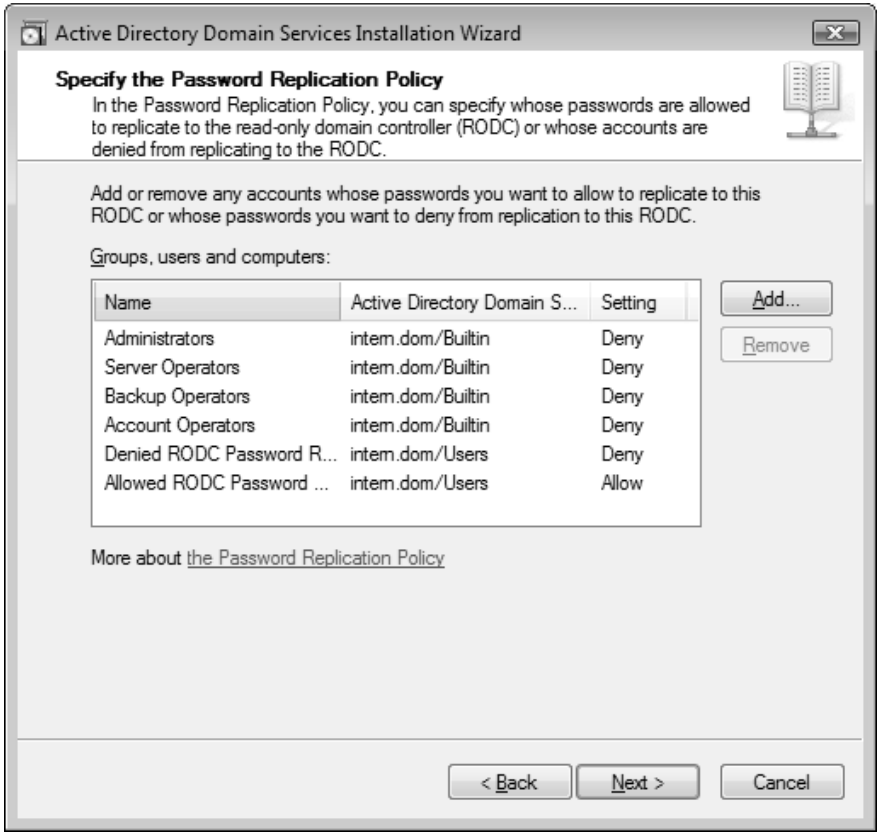


Рис. 7.6. Определение политики репликации паролей

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.

При установке RODC-контроллера из командной строки указывается соответствующий тип реплики (`ReadOnlyReplica`) и появляется дополнительный параметр, определяющий сайт, в котором будет располагаться новый контроллер (по умолчанию имя сайта `Default-First-Site-Name`):

```
dcpromo /InstallDNS:No /ReplicaDomainDNSName:intern.dom
/ReplicaOrNewDomain:ReadOnlyReplica /SafeModeAdminPassword:SafeMode123
/SiteName:Default-First-Site-Name /UserDomain:intern.dom
/UserName:administrator /Password:*
```

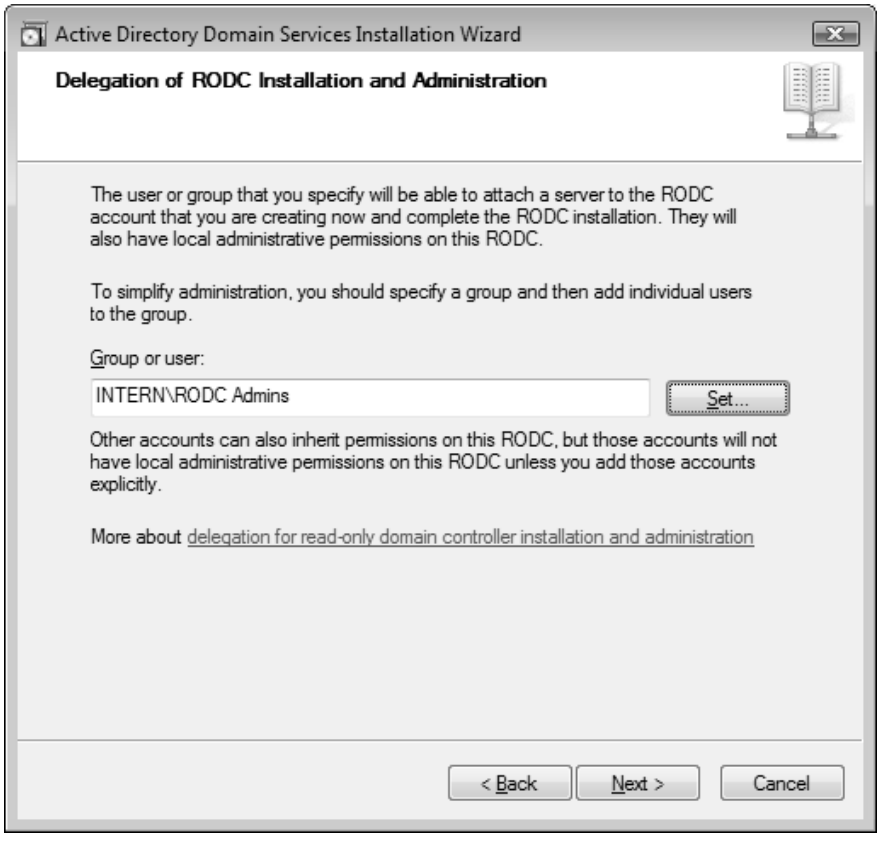


Рис. 7.7. Выбор локальных администраторов для RODC-контроллера

В процессе установки RODC-контроллера на экране отображается список групп, на которых распространяется политика репликации паролей — по умолчанию это группы, перечисленные на рис. 7.6. Если требуется изменить набор групп, для которых разрешена или запрещена репликация паролей, то в приведенной выше строке нужно указать также параметры `/PasswordReplicationAllowed` и/или `/PasswordReplicationDenied`. Например, при использовании следующего параметра вместо стандартной группы Allowed RODC Password Replication Group будет разрешена репликация паролей учетных записей пользователей домена:

```
/PasswordReplicationAllowed:"Domain Users"
```

Тип контроллера домена (DC Type) можно видеть в окне оснастки **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры) или **Active Directory Sites and Services** (Active Directory — сайты и службы) — для RODC-контроллеров указывается "Read-only, DC". Для таких контроллеров команда `repadmin /showrepl` отображает особые опции сервера:

```
DSA Options: DISABLE_OUTBOUND_REPL IS_RODC
```

Как можно видеть, репликация ***от*** RODC-контроллеров запрещена, и они не являются для других контроллеров партнерами по репликации (это можно видеть, выполняя команду `repadmin /showrepl` на других контроллерах домена).

Удаление контроллеров 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). 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`.

Как и при установке контроллера домена, должны быть доступны другие домены Active Directory (родительский или корневой), иначе процесс понижения 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 с уничтожением всего леса).

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.

Запуск мастера установки Active Directory

Для удаления контроллера домена Active Directory запустите на нем мастер установки Active Directory — утилиту Dcpromo.exe.

Если удаляемый контроллер является сервером Глобального каталога (GC), то появится предупреждение — убедитесь в том, что в лесу имеется другой сервер GC. При необходимости создайте *новый* сервер GC, дождитесь момента, когда он будет объявлен, и только тогда продолжайте процесс удаления контроллера домена.

На следующем шаге мастера установки потребуется 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). 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). 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. 7.8. 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 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.

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.

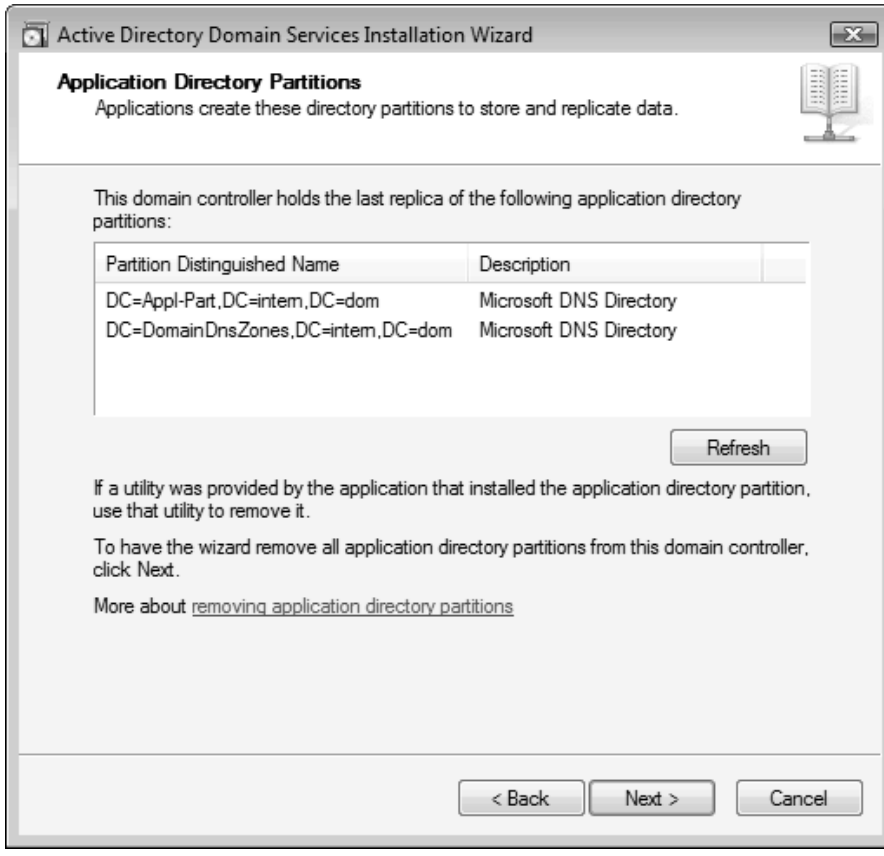


Рис. 7.8. Список последних реплик разделов приложений на данном контроллере домена

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 не забудьте окончательно удалить двоичные файлы служб Active Directory.

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 на контроллер домена в оставшейся структуре каталога Active Directory (например, с помощью оснастки **Active Directory Sites and Services** (Active Directory — сайты и службы)).

Удаление с использованием утилиты командной строки

Для удаления *последнего* контроллера леса можно выполнить на нем следующую команду (также удаляются разделы приложений, если таковые имеются — этот параметр не всегда обязателен):

```
dcpromo /IsLastDCInDomain:Yes /AdministratorPassword:AdmPsw123
/RemoveApplicationPartitions:Yes
```

В команде требуется указать сложный пароль для учетной записи, которая будет использоваться локальным администратором сервера после удаления доменных служб.

Если удаляется дополнительный контроллер и в домене остаются другие контроллеры, то следует использовать параметр `/IsLastDCInDomain:No`. При удалении последнего контроллера в дочернем домене (т. е. при удалении дочернего домена) необходимо использовать параметры /UserDomain, /UserName и /Password, чтобы указать учетные данные пользователя, имеющего права администратора предприятия.

Для принудительного понижения роли вышедшего из строя контроллера, не имеющего возможности синхронизации каталога с имеющимися контроллерами домена, можно использовать следующую команду:

```
Dcpromo /AdministratorPassword:AdmPsw123 /forceRemoval
```

Особенности подключения клиентов домена

Когда клиентский компьютер включается в домен Active Directory, соответствующая учетная запись компьютера *всегда* создается в контейнере Computers. Затем,

[1] Двоеточие обязательно!

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 не ниже *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.

Проблемы с подключением компьютеров в домены Active Directory возникают, в первую очередь, из-за несогласования протоколов для каналов связи между клиентом и контроллером домена — политики безопасности (опции шифрования и подписывания сетевого трафика) на клиентах и на контроллерах домена должны совпадать.

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 шифрования 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 ло-

кально 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 средства администрирования доменов и каталогов Active Directory

Оснастки, необходимые для администрирования доменов Active Directory, автоматически устанавливаются на сервере после назначения ему роли *Active Directory Domain Services (AD DS)* (Доменные службы Active Directory) (некоторые оснастки также появляются после назначения роли *Active Directory Lightweight Directory Services (AD LDS)* (Службы Active Directory облегченного доступа к каталогам)). Эти оснастки перечислены в *Приложении 2* 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. 7.9).

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 упомянутой в *Приложении 2* 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 (поставляется 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 (их имена приведены в *Приложении 2*) для управления удаленными серверами, не регистрируясь на них с учетными записями администраторов (что не приветствуется требованиями безопасности), используйте команду `runas`; например, следующие команды по-

зволяют запустить оснастки управления групповыми политиками или доменными объектами и указать альтернативную учетную запись:

```
runas /noprofile /env /user:DOMAIN\administrator "mmc gpmc.msc"
runas /netonly /user:DOMAIN\administrator "mmc dsa.msc"
```

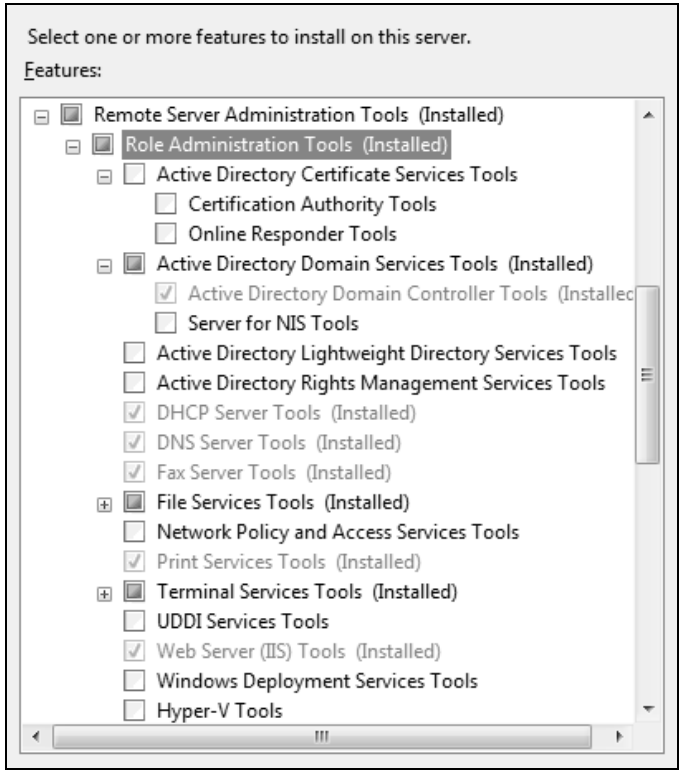


Рис. 7.9. Компоненты для удаленного управления ролями

Утилиты командной строки

Перечисленные ниже утилиты командной строки автоматически устанавливаются на контроллерах домена[1] и при добавлении серверу роли *Active Directory Lightweight Directory Services* (Службы Active Directory облегченного доступа к каталогам (AD LDS)).

- *DsQuery.exe* и *DsGet.exe* — утилиты, использующие протокол LDAP и позволяющие находить в каталогах объекты различного типа, а также отображать их атрибуты. Операции поиска можно выполнять как в отдельном домене, так и во всем лесу.

[1] Это касается как полных версий Windows Server 2008, так и версий Windows Server Core.

- *DsAdd.exe* — создает объекты указанных (предопределенных) типов.
- *DsMod.exe* — модифицирует атрибуты предопределенных типов объектов.
- *DsRm.exe* — удаляет объекты любых типов.
- *DsMove.exe* — перемещает любые объекты из одного контейнера в другой (в пределах домена), а также изменяет имя объектов.
- *Windows Domain Manager* (NetDom.exe) — утилита, позволяющая получать некоторую информацию о свойствах доменов (например, имена хозяев ролей FSMO, список доверительных отношений и т. д.), а также выполнять изменения в конфигурации доменов.

Кроме перечисленных, устанавливаются еще две утилиты — *LDIF Directory Exchange* (LDIFDE, Ldifde.exe) и *CSV Directory Exchange* (CSVDE, Csvde.exe), которые в первую очередь предназначены для выполнения групповых операций с объектами. Обе утилиты работают с файлами, в которые записываются результаты операций или из которых считываются данные и выполняемые команды. Ниже перечисляются операции, которые можно выполнять с помощью этих утилит.

- Экспорт информации из Active Directory в текстовый файл (в формате LDIF или CSV), который легко можно просматривать и/или редактировать. Полученную информацию можно использовать в следующих целях:
  - для документирования сведений об объектах каталога;
  - для выполнения групповых операций редактирования, не реализованных в стандартных административных оснастках;
  - для создания шаблонов для новых пользователей (если стандартная операция копирования пользовательских учетных записей вас не устраивает) или для любых других объектов каталога;
  - для переноса объектов между доменами, относящимися к одному лесу или разным лесам, а также между разными LDAP-совместимыми каталогами;
  - для архивирования существующей доменной конфигурации (в целях безопасности или для переустановки контроллеров домена).
- Импорт информации из файла в Active Directory. Эта операция подразумевает создание новых объектов или изменение атрибутов существующих объектов в пакетном (автоматическом) режиме. Кроме уже упомянутых выше операций экспорта, которые чаще всего также подразумевают импорт (операций группового редактирования, миграции, архивирования и создание шаблонов объектов), импорт информации в Active Directory может осуществляться для решения следующих задач:
  - для развертывания заранее сконфигурированной доменной структуры (кстати говоря, операция импорта выполняется при установке контроллеров домена — для создания стандартной структуры Active Directory использу-

ется утилита CSVDE; эта же утилита и соответствующие файлы-описания новых объектов и атрибутов применяются при обновлении схемы в случае перехода леса доменов к более высокой версии);

- для развертывания Active Directory-ориентированных приложений (при этом возможно расширение схемы).

Для решения конкретных задач можно использовать любую из двух утилит. При этом нужно помнить о двух главных отличиях между ними (с точки зрения пользователя):

- ❒ формат данных — утилита LDIFDE использует файлы в формате LDIF (текст с определенными тегами), а утилита CSVDE поддерживает формат CSV (текст с разделителями);
- ❒ возможные операции — утилита CSVDE обеспечивает только экспорт и импорт данных (создание объектов); утилита LDIFDE также позволяет модифицировать атрибуты и удалять объекты.

Кроме служебных утилит, для работы с объектами каталогов Active Directory можно использовать различные сценарии (ADSI, WMI, PowerShell и т. д.) — это самый гибкий и не очень сложный способ манипулирования объектами Active Directory (особенно для выполнения стандартных часто повторяющихся задач или при работе с большим количеством различных объектов).

Оснастка *Active Directory Users and Computers*

При работе с доменами оснастка **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры) является самым универсальным инструментом администратора и используется, наверное, чаще других оснасток. Основное назначение данной 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-объектами — 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.

Для выбора домена нужно в окне структуры выделить корень оснастки или доменный объект, после чего выбрать команду **Change Domain** (Сменить домен) в меню **Action** (Действие). В окне **Change domain** (Смена домена) следует ввести имя домена в поле **Domain** или нажать кнопку **Browse** (Обзор) и выбрать 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.

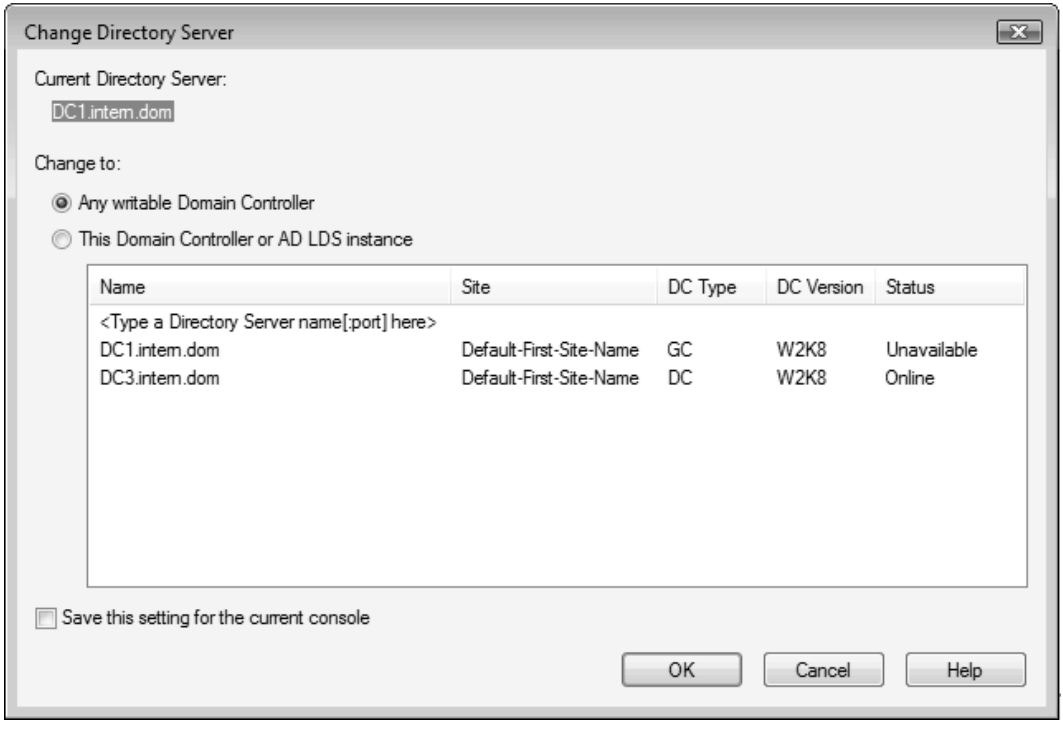


Рис. 7.10. Выбор контроллера домена

Аналогичным образом можно 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 администри-

ровать какой-нибудь сервер Глобального каталога или контроллер домена, владеющий определенной FSMO-ролью, например, PDC Emulator. В окне **Change Directory Server** (Смена сервера каталогов) (рис. 7.10) можно видеть имя текущего контроллера домена и список имеющихся контроллеров (или же можно ввести имя и порт для сервера служб AD LDS).

Управление отображением объектов каталога

Оснастка **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры) имеет вспомогательные 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.

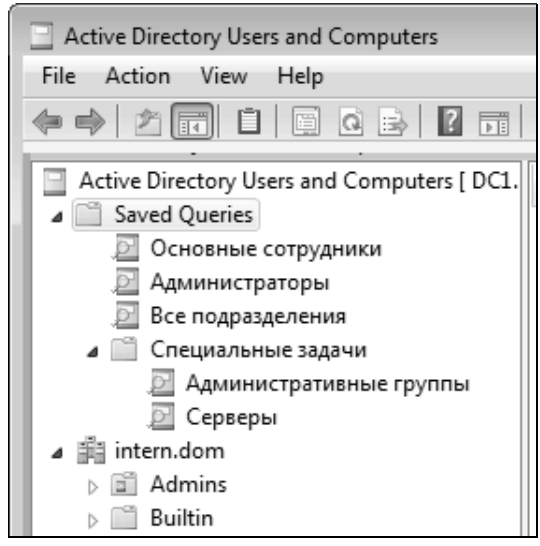


Рис. 7.11. Пример дерева сохраненных запросов

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. 7.11).

Новый запрос можно создавать непосредственно в окне оснастки, а 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. 7.12) заполните поля **Name** (Имя) и **Description** (Описание) (необязательно).

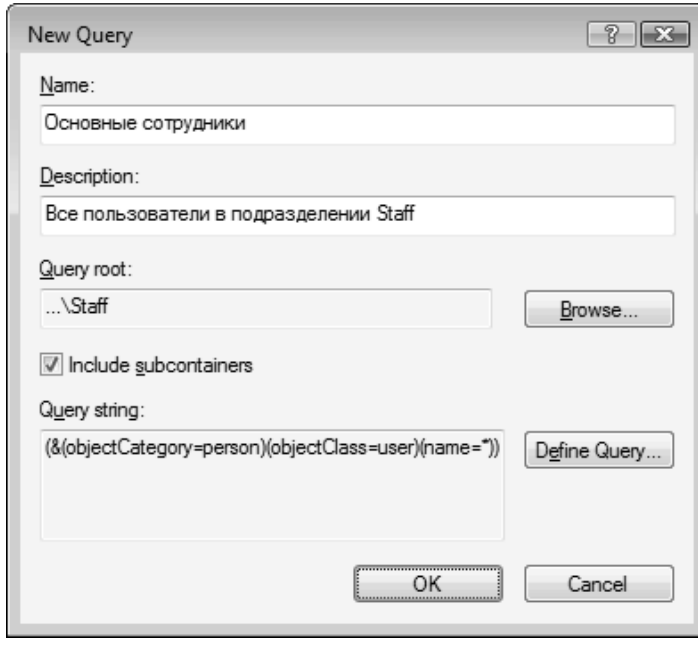


Рис. 7.12. Пример нового сохраненного запроса

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 простой 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. 7.13), 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. 7.14). 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.

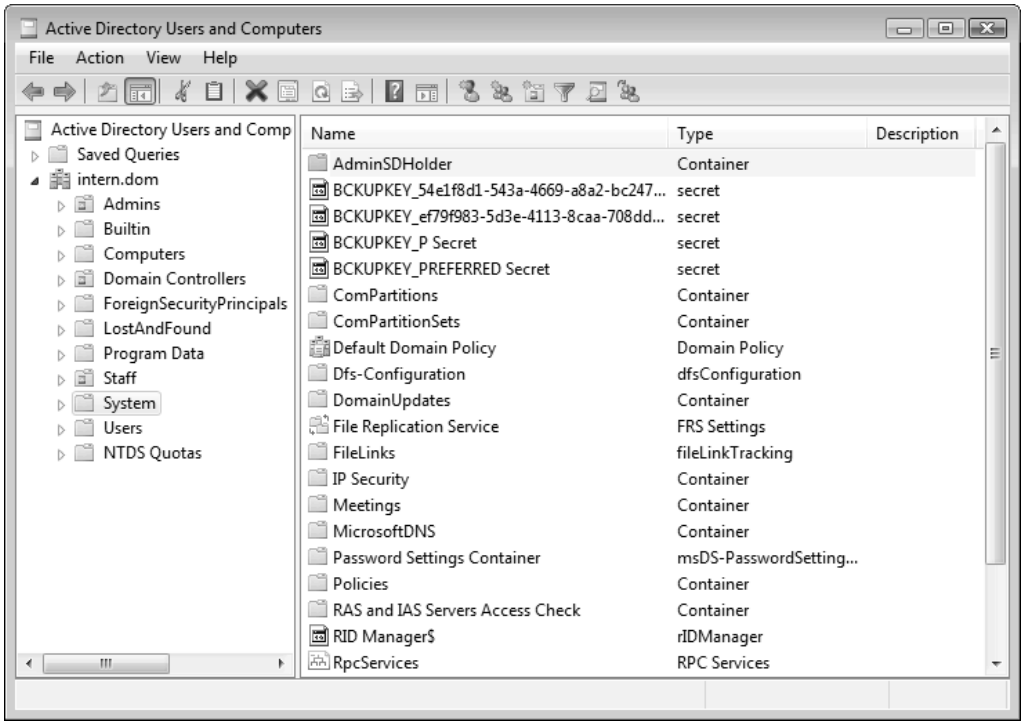


Рис. 7.13. Просмотр дерева доменных объектов в режиме Advanced Features

У всех объектов каталога на вкладке **Object** (Объект) теперь имеется 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. 7.14) 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).

Режим *Users, Contacts, Groups, and Computers as containers* (Пользователи, контакты, группы и компьютеры как контейнеры)

Многие объекты Active Directory являются контейнерами, которые могут содержать другие объекты. По умолчанию это отношение визуально не всегда представлено в окне оснастки **Active Directory Users and Computers** (Active Directory — пользователи и компьютеры).

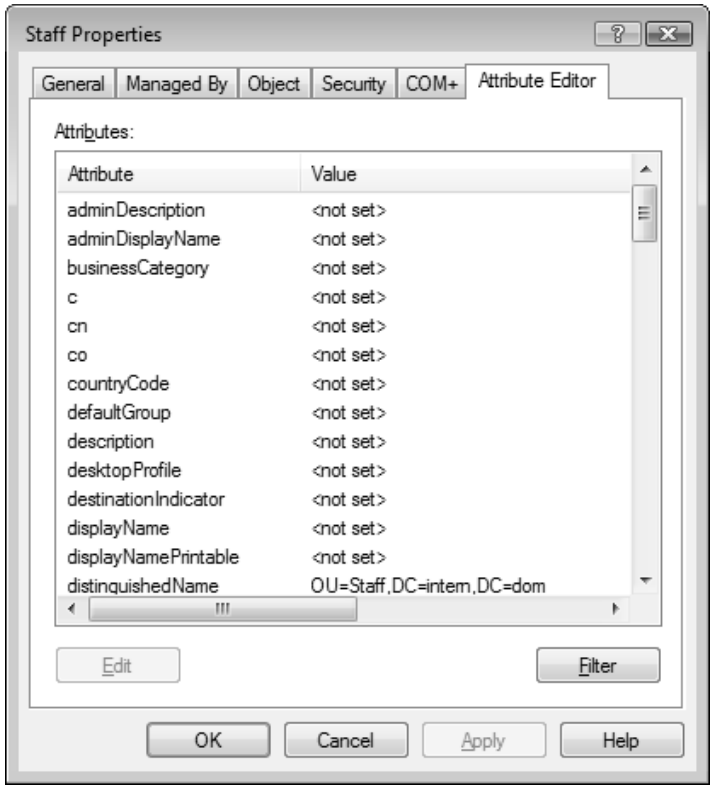


Рис. 7.14. Вкладка редактора атрибутов выбранного объекта каталога

Тем не менее, в некоторых ситуациях необходимо видеть отношения между объектами и для этого в меню **View** (Вид) нужно установить соответствующий флажок.

В этом случае будет, например, видно, что компьютеры (включая контроллеры домена) могут иметь дочерние объекты — в частности, с ними связаны объекты публикуемых ресурсов: принтеров и общих папок. Эти объекты могут быть важны как при администрировании (например, при перемещении объектов принтеров), так и при удалении контейнеров (которые могут содержать важные объекты).

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. 7.15) 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).

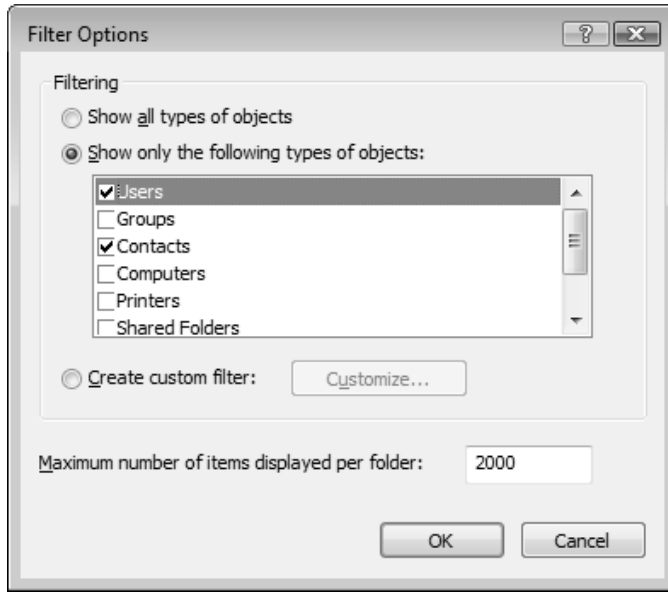


Рис. 7.15. Пример фильтра отображаемых объектов

Внимание!

При использовании фильтров возникает потенциальная опасность при работе с контейнерами (подразделениями). Предположим, что установлен фильтр, который разрешает отобрать только учетные записи компьютеров. При просмотре домена может показаться, что в некотором подразделении нет объектов или оно содержит только ненужные учетные записи компьютеров. Легко забыть о том, что это подразделение может также содержать объекты других типов, и нечаянно удалить подразделение *целиком*, а не только отображаемые объекты[1]. Поэтому не забывайте выключать все фильтры перед выполнением операций удаления или перемещения контейнерных объектов!

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. 7.16). Эта панель включается в окне **Customize View** (Настройка), открывающемся по команде **View** | **Customize** (Вид | Настройка). В нашем примере разрешено отображение пользователей; таких объектов в данном контейнере нет, и он кажется совершенно пустым (0 объектов), хотя в нем располагаются учетные записи контроллеров домена.

[1] Отчасти эта проблема решается, если для контейнера установлен флажок **Protect object from accidental deletion** (Защитить объект от случайного удаления).

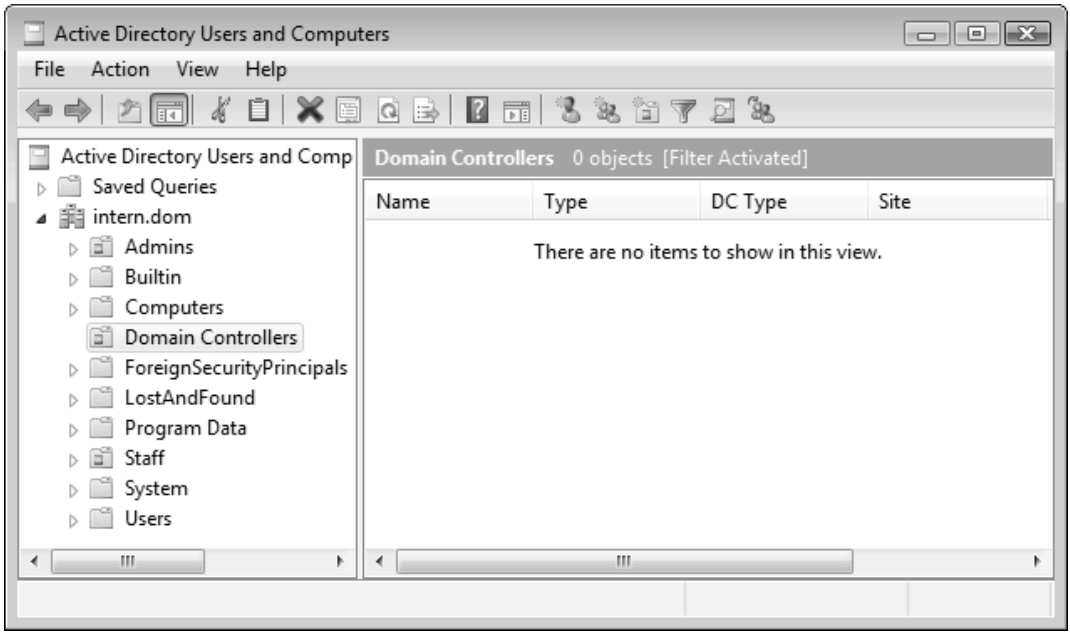


Рис. 7.16. Количество отображаемых объектов и указание на включенный фильтр

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 (см. рис. 7.17), которые имеются для этих объектов в главном окне оснастки.

Пример окна **Find** (Найти) и результаты поиска показаны на рис. 7.17. 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).

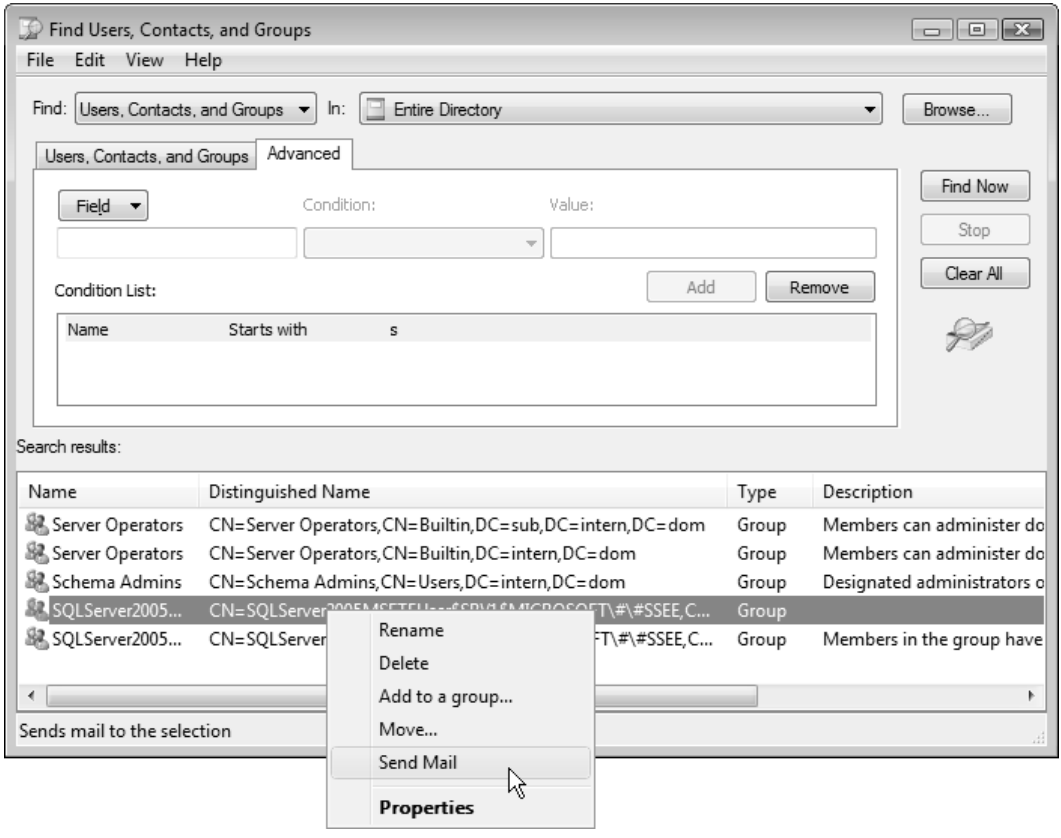


Рис. 7.17. Поиск и просмотр объектов в каталоге Active Directory

Набор столбцов в окне, показанном на рис. 7.17, 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).

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).

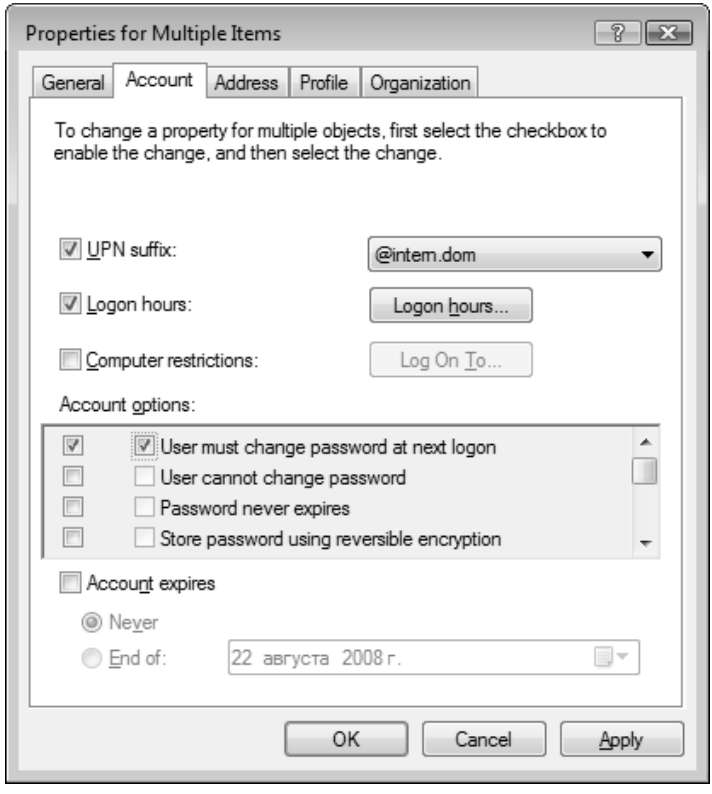


Рис. 7.18. Изменение UPN-суффикса, времени входа в систему и запрос на смену пароля

Если выделено несколько учетных записей, что появляется *модифицированное* окно **Properties** (Свойства). Примеры различных вкладок этого окна показаны на рис. 7.18 и рис. 7.19.

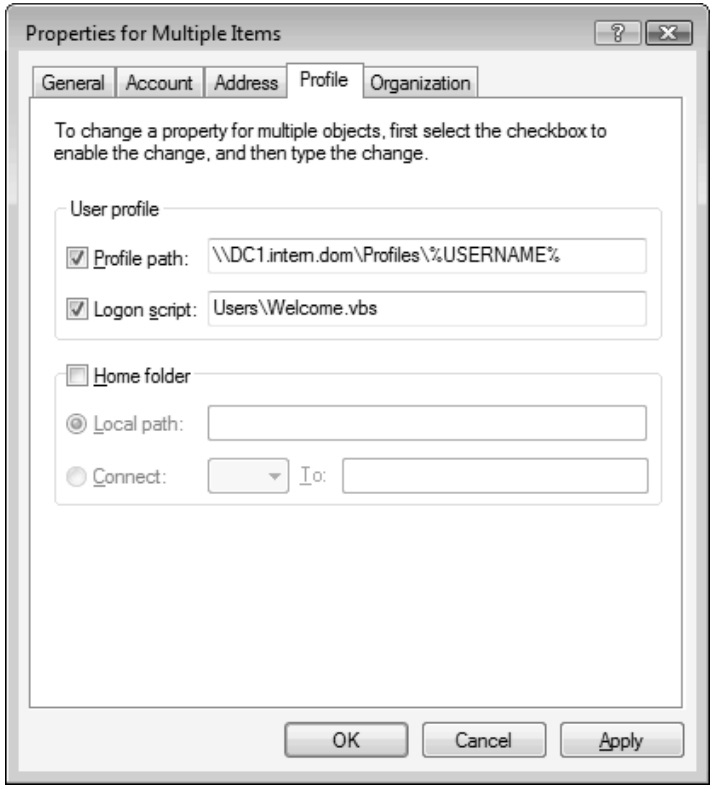


Рис. 7.19. Назначение перемещаемого профиля и сценария входа (справа) для нескольких пользовательских учетных записей

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 которо-

го 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. 7.9).

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.

> ***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. 7.20 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).

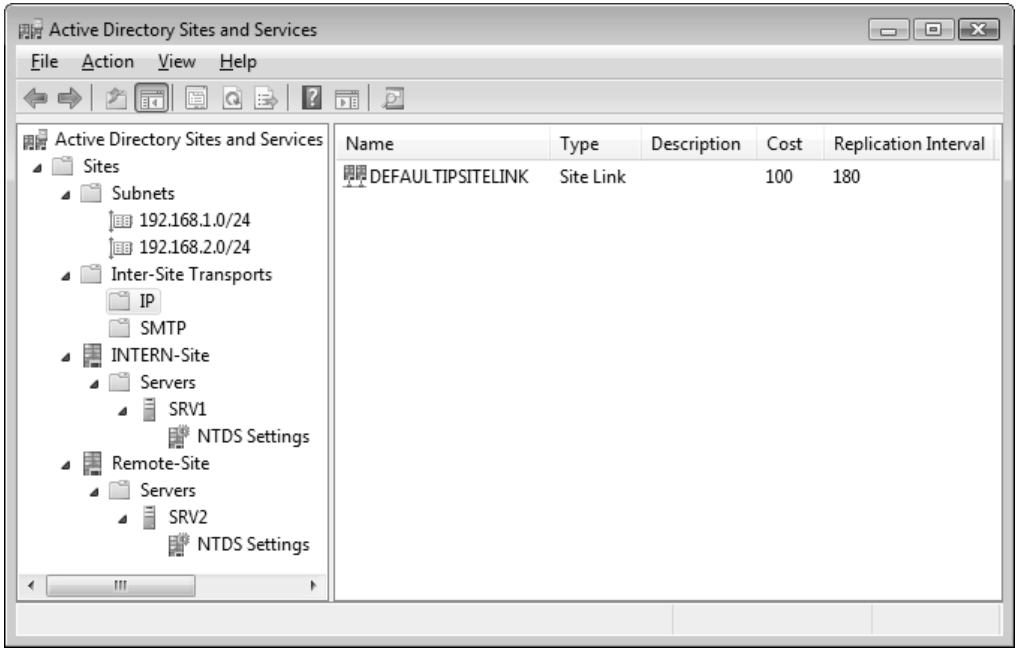


Рис. 7.20. Пример простой сети с двумя сайтами

Разделы каталога Active Directory и механизм репликации

Каталог Active Directory является распределенной сетевой базой данных. Каждый контроллер домена является носителем копии каталога. При этом каждый контрол-

лер домена может вносить изменения в собственную копию каталога, и все произведенные изменения должны быть автоматически распространены на другие копии. Поэтому 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.

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 главы. 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 облегчен-

ного 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).

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. К примеру, если приложение, для которого создается раздел, используется только в двух доменах леса, то и копии раздела приложения должны быть размещены только на контроллерах домена этих доменов, а 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 систем-

ного 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. далее)*. 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.

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 GPO-объекта нарушается.

Управление репликацией из командной строки

Если административные оснастки недоступны или требуется детальный анализ топологии репликации, а также принудительная репликация отдельных разделов каталога, то основным средством для работы становится утилита *Replication Diagnostics Tool* (RepAdmin.exe). Из ее многочисленных возможностей ниже рассматриваются только основные — те, которые необходимы для анализа правильности репликации и запуска частичной репликации. (Мы не будем приводить сообщения, генерируемые утилитой, поскольку это заняло бы очень много места; ограничимся лишь используемыми параметрами.)

Просмотр списка партнеров по репликации

Первым и очень важным шагом в процессе управления репликацией является анализ списка контроллеров-партнеров (соседей), имеющих соединения с указанным контроллером домена, а также просмотр топологии репликации для каждого контекста имен каталога. (Эта информация впоследствии используется как данные для многих параметров утилиты RepAdmin.)

Параметры сервера (DC1 в домене intern.dom) и перечень разделов каталога, реплицируемых ***от*** других контроллеров, можно видеть с помощью следующей команды:

```
repadmin /showrepl dc1.intern.dom
```

Если имя сервера на указывается, то отображается информация для локального контроллера. Эта команда позволяет видеть, насколько успешно выполнялась репликация для имеющихся разделов.

Чтобы также видеть партнеров по исходящей репликации (в направлении от указанного сервера ***к*** другим контроллерам), добавьте к предыдущей команде параметр `/all`).

В случае наличия ошибок полезно включить режим подробного протоколирования — добавить параметр `/verbose`.

Просмотр списка соединений с партнерами по репликации

Самую подробную информацию о соединениях топологии репликации, установленных для контроллера домена, можно увидеть с помощью следующей команды:

```
repadmin /showconn dc1.intern.dom DC3
```

В этой команде можно указать:

- DNS-имя контроллера домена, который будет служить источником информации;
- RDN-имя (или идентификатор GUID или отличительное имя объекта DSA) интересующего вас контроллера.

(Без второго параметра утилита выведет список всех соединений для сайта, в котором находится указанный контроллер домена.)

Эта команда позволяет видеть, какие разделы каталога по каким соединениям реплицируются (и с какими контроллерами); она отображает все неисправные соединения (которые не реплицировались в течение определенного времени), а также возможные причины этих неисправностей. Все ошибки следует тщательно анализировать, поскольку они могут свидетельствовать о серьезных нарушениях работы отдельных контроллеров или домена в целом.

Принудительный запуск репликации

С помощью утилиты RepAdmin можно очень гибко управлять репликацией. Для выбранного контроллера домена возможны следующие виды репликации:

- *один раздел* каталога реплицируется от *другого* контроллера домена;
- *один раздел* каталога реплицируется от *всех партнеров* по репликации;
- *все разделы* каталога реплицируется от *всех партнеров* по репликации;
- раздел каталога реплицируется *между сайтами*;
- репликация в *обратном направлении*: обычно изменения копируются *от* партнеров (pull mode); можно выбрать обратное направление (push mode), когда изменения на контроллере будут копироваться его партнерам по репликации.

Рассмотрим эти виды репликации подробнее.

Репликация между двумя партнерами

Следующая команда позволяет реплицировать раздел доменных имен между двумя указанными контроллерами:

```
repadmin /replicate dc1.intern.dom dc3.intern.dom DC=intern,DC=dom
```

Обычно после ввода команды нужно ждать до тех пор, пока операция не будет закончена. Или же операцию можно запустить в асинхронном режиме (добавить параметр `/async`) и проверять очередь репликации, чтобы увидеть момент окончания этой операции (команда `repadmin /queue`).

Репликация от всех партнеров (ко всем партнерам)

Команда `repadmin /syncall` позволяет синхронизировать раздел каталога между контроллером домена и *всеми* его партнерами. Добавив параметр `/A`, можно также инициировать репликацию всех разделов, хранящихся на указанном контроллере (см. ниже). Например, следующая команда запускает репликацию раздела доменных имен от всех партнеров указанного сервера:

```
repadmin /syncall dc1.intern.dom DC=intern,DC=dom
```

Когда команда выполняется успешно, она отображает имена всех партнеров по репликации и в конце должна выдать сообщение об отсутствии ошибок.

Различие между приведенной выше командой и операцией репликации (**Replicate Now**), которую можно выполнить в окне оснастки **Active Directory Sites and Services** (Active Directory — сайты и службы) для некоторого соединения между контроллерами, состоит в следующем:

- команда выполняет репликацию только *одного раздела*, однако от *всех* источников-партнеров по репликации;
- в окне оснастки можно инициировать репликацию *всех* задействованных в выбранном соединении разделов, однако только от *одного* партнера.

> ***Внимание!***
>
> Если в команде `repadmin /syncall` не указывается контекст имен, то реплицируется только раздел Configuration.

Следующая команда запускает репликацию *всех* разделов контроллера DC1 от *всех* его партнеров по репликации:

```
repadmin /syncall dc1.intern.dom /A
```

Полезны еще два параметра команды:

- `/e` — разрешает репликацию между сайтами;
- `/P` (заглавная буква!) — меняет направление репликации на противоположное. Когда используется этот параметр, изменения распространяются *от* указанного контроллера *ко* всем его партнерам (по умолчанию все наоборот).

Оснастка *Active Directory Domains and Trusts*

Оснастка **Active Directory Domains and Trusts** (Active Directory — домены и доверие) в первую очередь требуется при работе с лесами со множеством доменов, поскольку предоставляет возможность быстрого просмотра леса доменов и выбора администрируемого домена. Также она позволяет управлять доверительными отношениями внутри леса и связями со внешними доменами (лесами).

На рис. 7.21 показано главное окно этой оснастки, где в качестве примера 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).

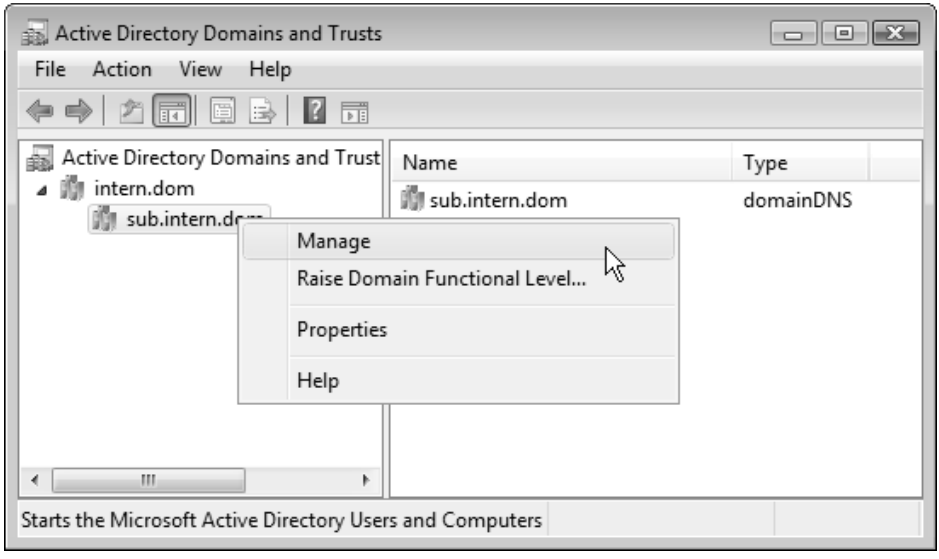


Рис. 7.21. Выбор администрируемого домена в лесу доменов

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 указаны 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 перечислены 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))

(окончание)

Режим работы домена	Функциональные возможности
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
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

Изменение функционального уровня домена

Повышение функционального уровня (functional level) отдельного домена или всего леса осуществляется с помощью оснастки **Active Directory Domains and Trusts** (Active Directory — домены и доверие). 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. 7.21). В следующем окне (рис. 7.22) 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*. Выберите требуемый уровень из списка и нажмите кнопку **Raise** (Изменить).

Если в домене присутствуют контроллеры на базе младших систем (Windows 2000 или Windows Server 2003), возникнет ошибка. Система сообщит о контроллерах, препятствующих повышению функционального уровня (эту информацию можно будет сохранить в файле).

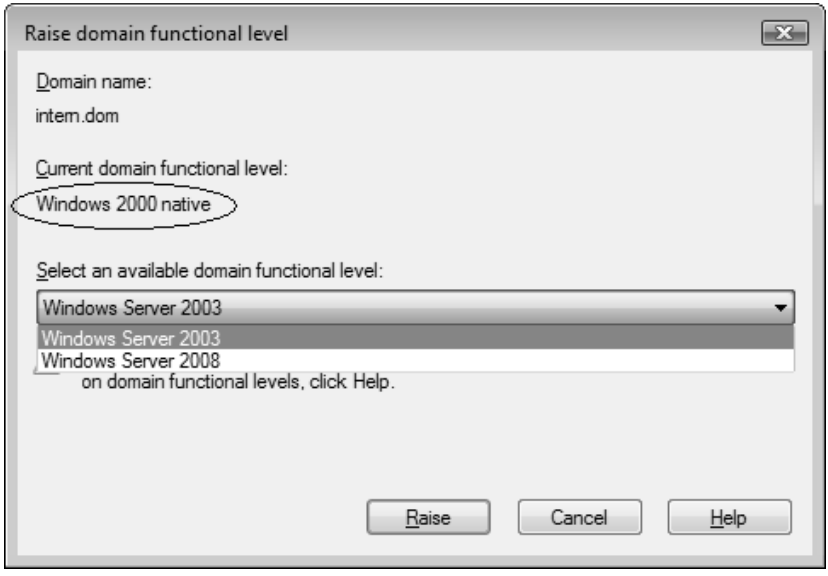


Рис. 7.22. Выбор функционального уровня домена

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.

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) можно проверить 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 воспользуйтесь следующей процедурой:

1. Откройте окно свойств домена.
2. Выберите отношение на вкладке **Trusts** (Доверия) (рис. 7.23) и нажмите кнопку **Properties** (Свойства).

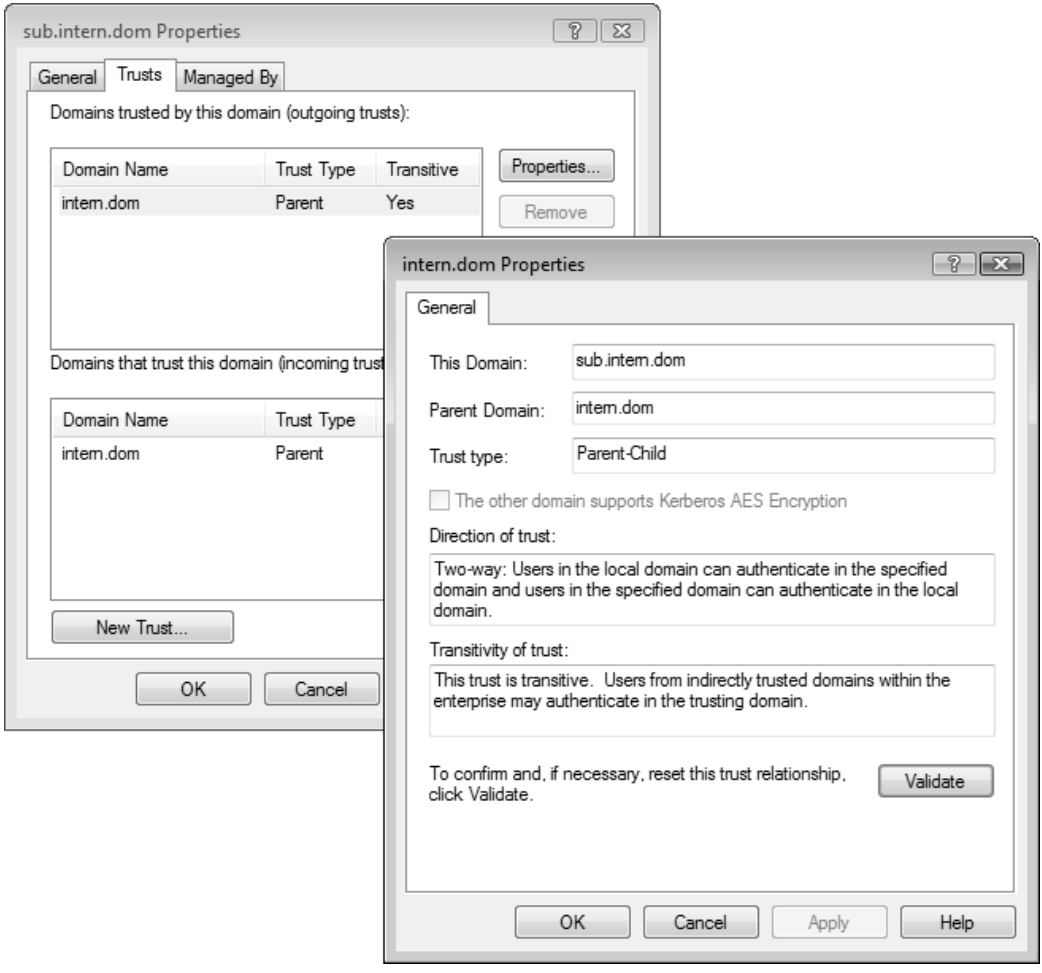


Рис. 7.23. Просмотр свойств доверительных отношений между доменами

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*. Например, следующая команда проверяет отношения Kerberos между двумя доменами в лесу (имя одного домена указывается непосредственно как параметр, а имя другого задается параметром /D; при этом необходимо вводить учетные данные администраторов обоих доменов!):

```
C:\>netdom TRUST sub.intern.dom /D:intern.dom /Kerberos
/UD:INTERN\administrator /PD:* /UO:SUB\administrator /PO:* /Verify
Type the password associated with the domain user: [для домена intern.dom]
Type the password associated with the object user: [для домена sub.intern.dom]

The trust between sub.intern.dom and intern.dom has been successfully verified
(Доверительное отношение между доменом ... и ... успешно проверено)
The command completed successfully.
```

Если вы зарегистрированы в домене intern.dom с правами администратора, то достаточно ввести такую команду:

```
netdom TRUST sub.intern.dom /D:intern.dom /Kerberos /UO:administrator /PO:*
/Verify
```

Для повторной инициализации междоменных отношений в приведенных командах вместо параметра `/Verify` нужно использовать ключ `/Reset`.

Если имеются проблемы, связанные с доверительными отношениями, то их можно локализовать с помощью команд `netdom VERIFY` или `nltest /sc_query`, проверяя отношения между отдельными контроллерами домена, т. е. проверяя их попарно.

Оснастка *ADSI Edit*

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.

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 соответствующих ролей. Также она входит в состав средств удаленного администрирования (см. рис. 7.9).

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:

- ForestDnsZones (DC=ForestDnsZones, DC=*domain*, DC=*com*)
- DomainDnsZones (DC=DomainDnsZones, DC= *domain*, DC= *com*)

На рис. 7.24 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. (Обратите внимание на то, что две службы каталога могут располагаться на одном и том же сервере — DC1.)

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). Для работы можно выбирать любые домены или серверы каталога. При подключении к доменной службе Active Directory обычно используется контроллер, на котором выполнена регистрация.

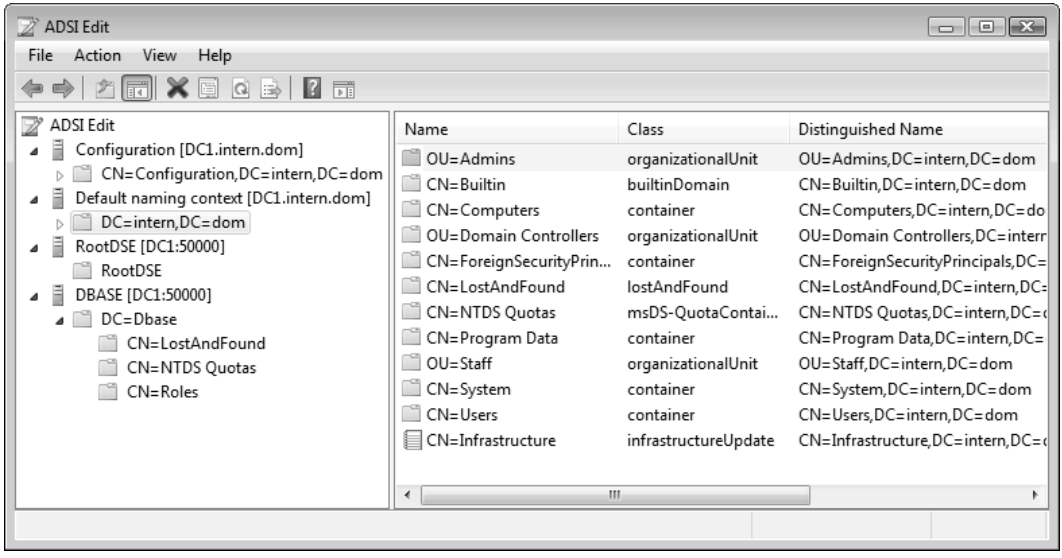


Рис. 7.24. Окно оснастки **ADSI Edit** с примерами подключений к различным разделам каталогов Active Directory

В окне **Advanced** (Дополнительные параметры) (для его вызова в окне **Connection Settings** нажмите кнопку **Advanced**) можно указать альтернативное имя пользователя и его пароль, номер порта и протокол: переключатель **LDAP** или **Global Catalog**. Для просмотра или изменения свойств соединения выполните команду **Settings** в его контекстном меню. Любое соединение можно удалить при помощи команды **Remove**.

Все созданные подключения к разделам каталога сохраняются и автоматически восстанавливаются при последующих запусках оснастки.

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 просматри-

вать 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.)

Оснастка **Active Directory Schema** (Схема Active Directory) по умолчанию присутствует на всех контроллерах домена, но при этом не появляется ни в меню **Start** (Пуск), ни на панели управления — ее нужно вручную добавлять к консоли MMC. Перед этим соответствующую библиотеку DLL необходимо зарегистрировать с помощью следующей команды:

```
regsvr32 schmmgmt.dll
```

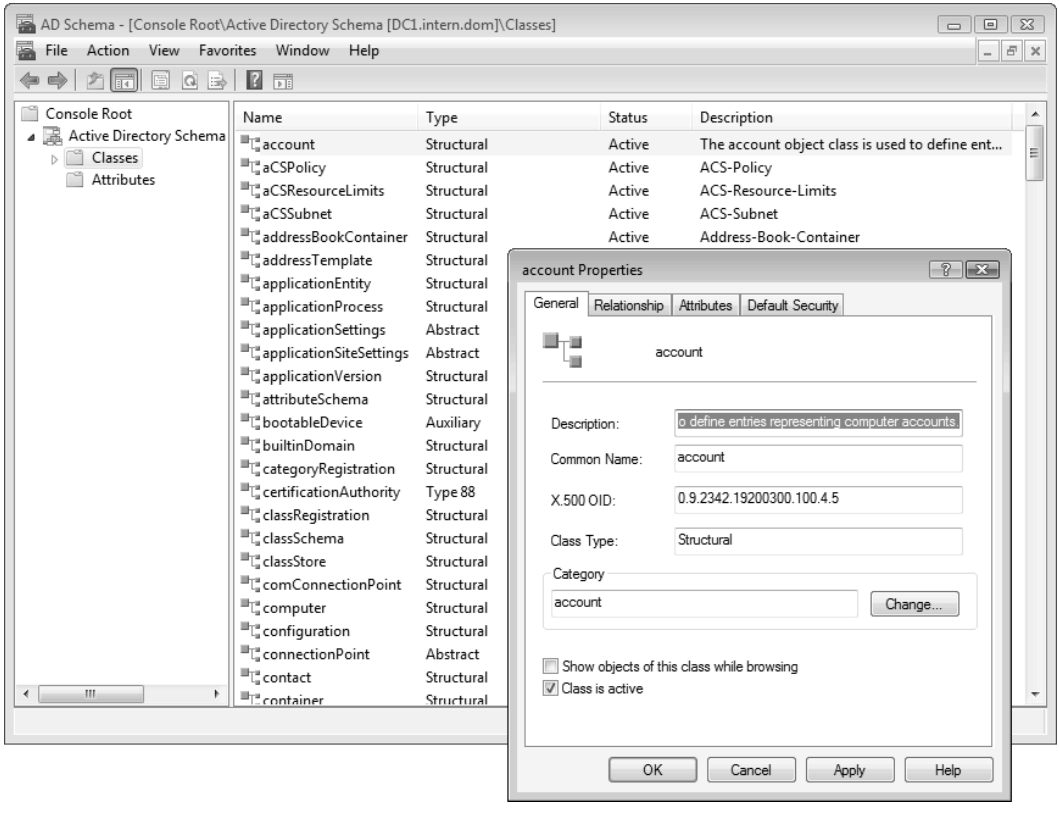


Рис. 7.25. Окно оснастки **Active Directory Schema**

Затем можно создать новый документ MMC (представляющий собой консоль, сохраненную с произвольным именем), содержащий оснастку **Active Directory Schema** (Схема Active Directory) (рис. 7.25), или добавить оснастку к уже существующей пользовательской консоли.

> ***Примечание***
>
> Оснастка **Active Directory Schema** (Схема Active Directory) может также устанавливаться на любом сервере Windows Server 2008 в составе набора инструментов удаленного администрирования каталогов Active Directory (см. рис. 7.9).

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.

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.

Далее перечислены основные принципиально новые возможности групповых политик в Windows Server 2008 и в первую очередь те, которые интересны при работе в доменной среде. Некоторые средства групповых политик были реализованы уже в предыдущих версиях Windows, однако в Windows Vista/Windows Server 2008 они заметно модернизированы и расширены.

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);
- планшетные компьютеры (Tablet PC);
- управление учетными записями (User Account Control, UAC);
- средства диагностики и решения проблем.

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). Теперь параметрами браузера можно управлять централизованно, без необходимости установки расширения Internet Explorer Maintenance (IEM) или пакета Internet Explorer Administration Kit (IEAK).

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 Active Directory на базе Windows Server 2008 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.

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. В окне оснастки **Event Viewer** (Просмотр событий) журнал GroupPolicy можно найти в папке **Application and Services Logs** (Журналы приложений и служб) | **Microsoft** | **Windows**.

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.

Оснастка *Group Policy Management*

Оснастка **Group Policy Management** (Управление групповой политикой, gpmc.msc) позволяет централизованно управлять объектами групповых политик в многодоменных лесах Active Directory, упрощая многие рутинные операции, а также сохранять, восстанавливать и переносить GPO-объекты. Для Windows Server 2003 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. Данная версия оснастки позволяет работать с новым форматом описания политик — ADMX-файлами.

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;
- 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)); 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) (рис. 7.26) 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).

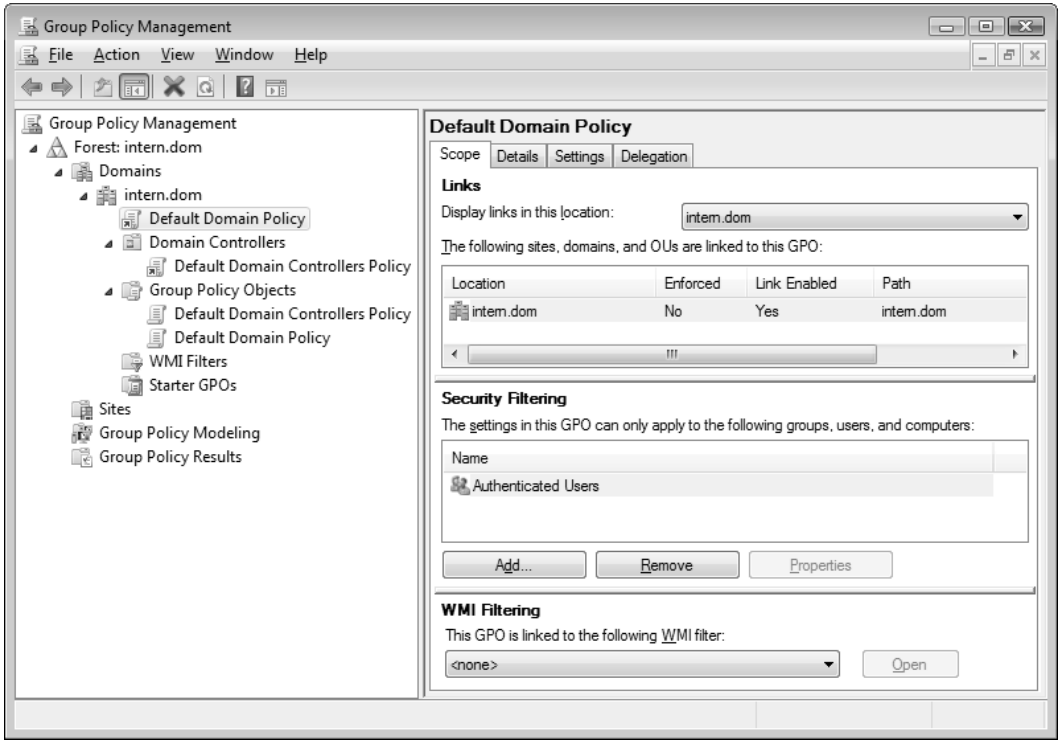


Рис. 7.26. Окно оснастки **Group Policy Management**

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 самым приоритетным (т. е. его парамет-

ры 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 **Group Policy Management** (Управление групповой политикой) 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.

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. 7.27) — все заданные в нем параметры сразу будут перенесены в новый GPO-объект.

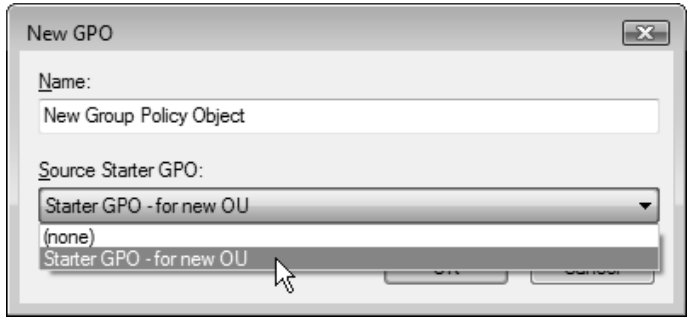


Рис. 7.27. Выбор начального GPO-объекта при создании нового объекта групповой политики

Предпочтения (Preferences)

В доменах Active Directory на базе серверов Windows Server 2008 имеются расширения обычных групповых политик, названные *предпочтениями* (preferences) (рис. 7.28). (Предпочтения имеются только в доменных GPO-объектах!) С помощью предпоч-

тений 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).



Рис. 7.28. Папки предпочтений в доменном GPO-объекте

Предпочтения (а их около двух десятков — см. примеры на рис. 7.28) 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 конкретных случая.

Создание ярлыка для элемента оболочки

Задача: необходимо, 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. Выберите GPO-объект для редактирования.
2. В конфигурации пользователя откройте папку **Preferences** | **Windows Settings** | **Shortcuts** (Настройка | Конфигурация Windows | Ярлыки) (рис. 7.29).

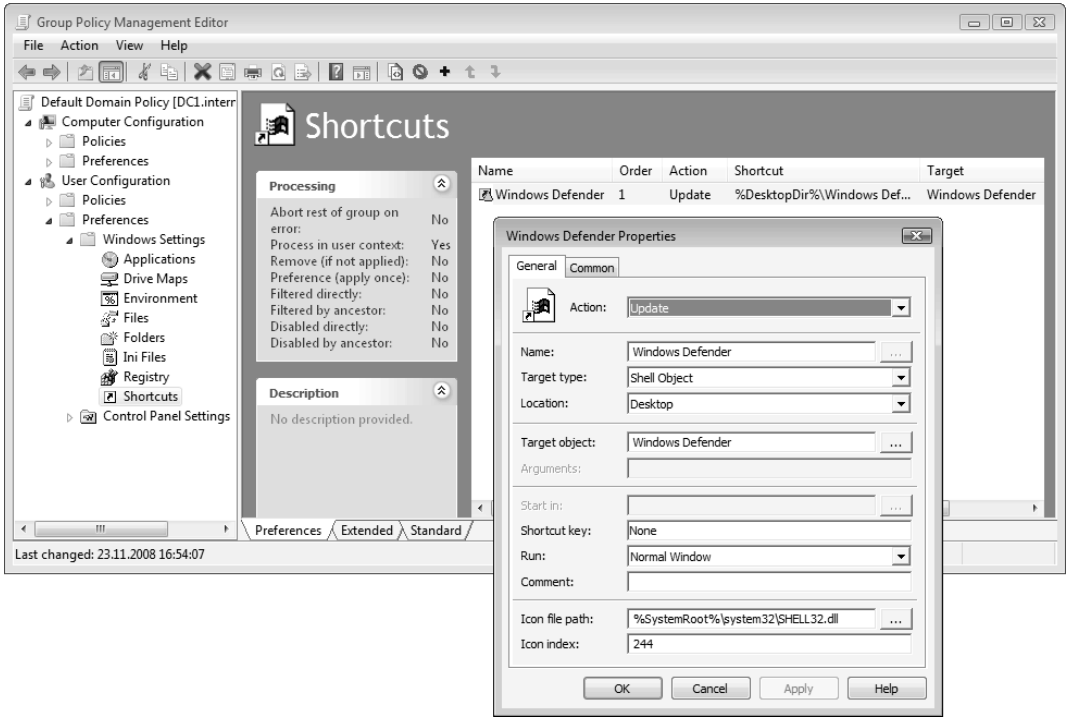


Рис. 7.29. Параметры предпочтения для отображения ярлыка на рабочем столе

3. В правом окне щелкните правой кнопкой мыши и выполните команду **New** | **Shortcut** (Создать | Ярлык).
4. В окне параметров предпочтения задайте нужные параметры (см. рис. 7.29). 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

object; для выбора объекта[1] нужно нажать кнопку справа от поля). Также можно указать значок для ярлыка (поле **Icon file path**).

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).

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

Задача: требуется, 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.)

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 же 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. 7.30). 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 всех клиентов домена появится указанная папка.

Улучшения, касающиеся службы FRS и тома SYSVOL

На работе групповых политик сказываются улучшения, обусловленные возможностью использования службы DFS Replication[2] (Репликация DFS, сервис DFSR) для репликации тома SYSVOL и применение нового формата административных шаблонов (ADMX files). Это позволяет уменьшить трафик в сети, связанный с репли-

[1] Выбирать всегда можно только те объекты, которые имеются на компьютере, где запущена оснастка.

[2] Эта служба обычно применяется для синхронизации папок DFS.

кацией 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*.

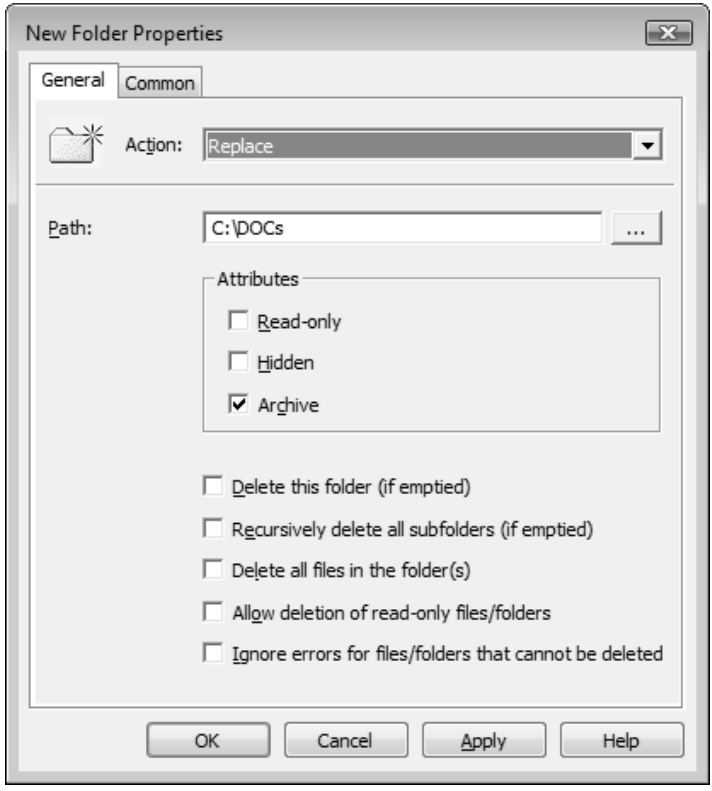


Рис. 7.30. Предпочтение для управления локальной папкой и ее содержимым

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.

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). Некоторые принципы построения GPO-объектов в системах Windows Server 2008 изменились, поэтому далее подробно рассматриваются детали их реализации, которые могут быть важными для администратора.

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 GPO-объекты мы будем называть *доменными*).

Локальные GPO-объекты

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 GPO-объектом, 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. 7.31). 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)*.

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. 7.31.

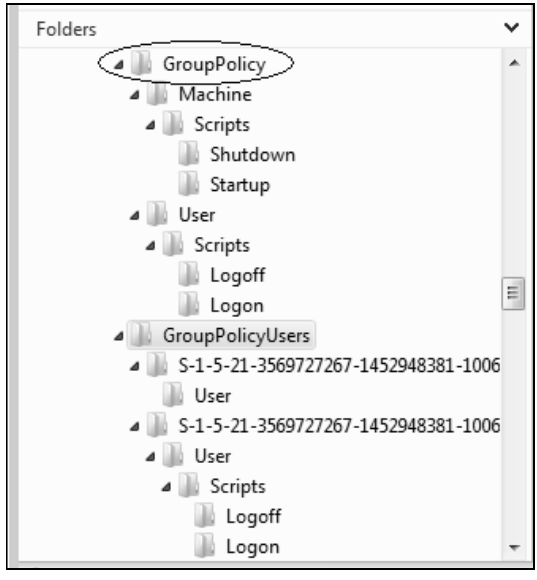


Рис. 7.31. Структура папок локальных объектов групповой политики в Windows Vista/Windows Server 2008

Доменные GPO-объекты

Доменные GPO-объекты 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 каталога Active Directory, в котором хранятся следующие важные свойства GPO-объекта:

- 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-объекта (разрешенные и запрещенные части);
- местоположение (имя шаблона групповых политик) в томе SYSVOL (например, \\intern.dom\sysvol\intern.dom\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}).

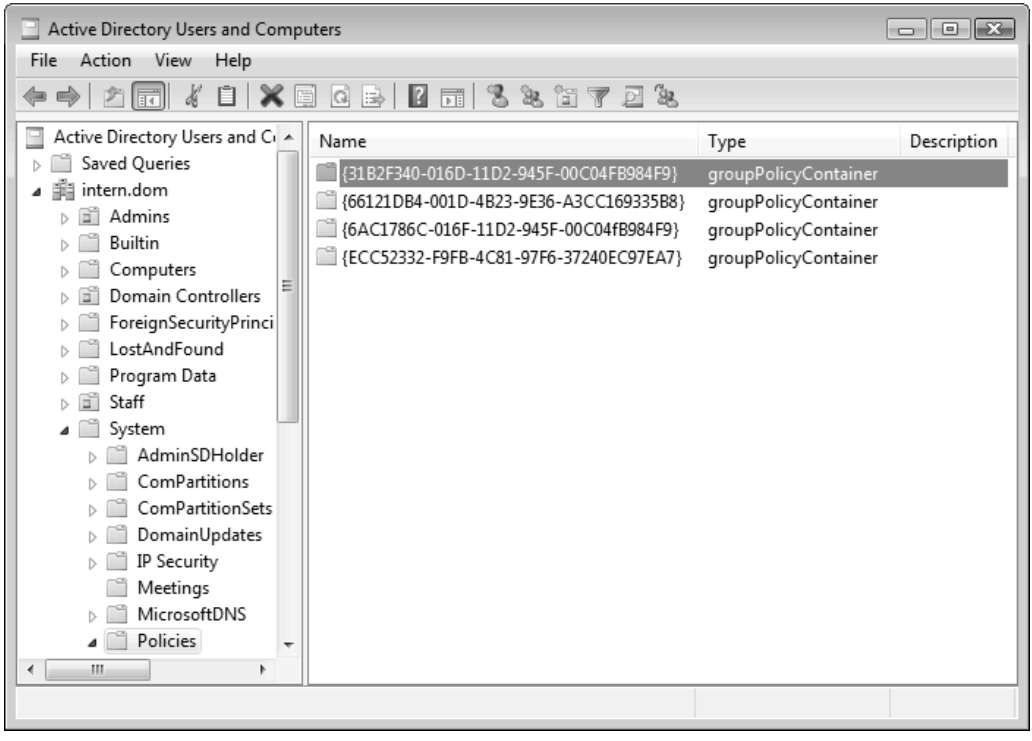


Рис. 7.32. Хранение контейнеров групповых политик в каталоге Active Directory

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. 7.32).

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 GPO-объекта выступает в качестве *глобального уникального идентификатора* (Global Unique Identifier, GUID), однозначно характеризующего данный объект групповой политики (рис. 7.33).

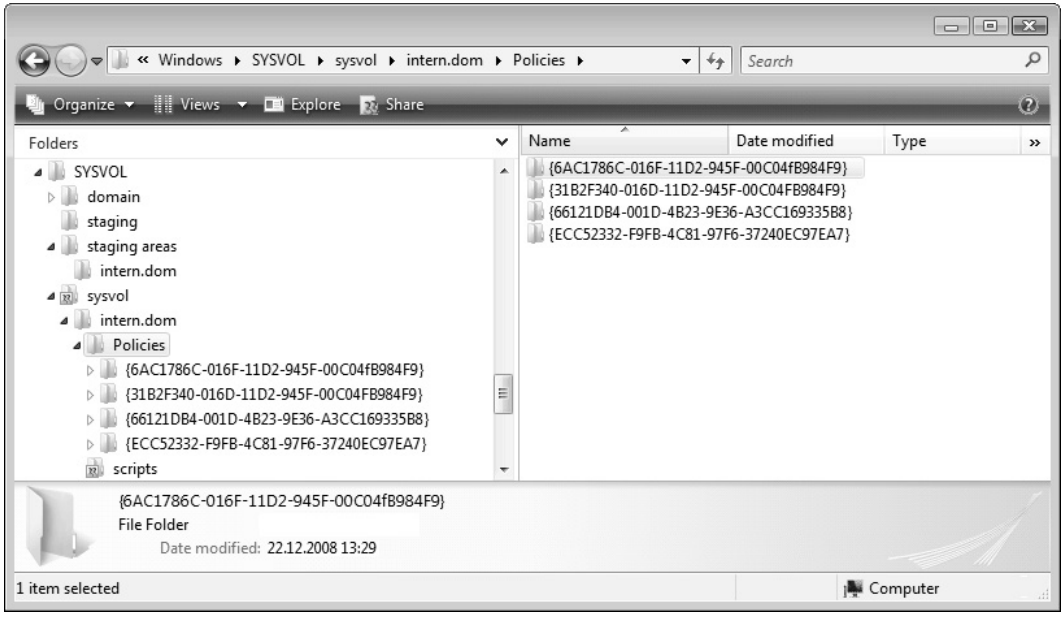


Рис. 7.33. Хранение шаблонов групповых политик на томе SYSVOL

Подкаталоги шаблона групповых политик

Ниже перечислены подкаталоги, содержащиеся по умолчанию внутри папки шаблона групповых политик.

В локальных GPO некоторые из указанных папок отсутствуют.

- **Group Policy**. В этой папке хранится текстовый файл GPE.INI, в котором указаны идентификаторы расширений, реализующие предпочтения (preferences) для конфигурации компьютера и/или пользователя — если эти предпочтения заданы в данном GPO-объекте. В противном случае папка отсутствует.
- **Machine**. Здесь хранится имеющий специальный формат файл Registry.pol со значениями параметров реестра, устанавливаемых для *компьютеров* 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 GPO-объекта. Содержимое папки **Applications** зависит от того, какие приложения назначены компьютеру с помощью данного GPO-объекта. При наличии заданных предпочтений папка **Preferences** содержит подкаталоги (например, **Folders**, **Shortcuts** и т. п.), в которых хранятся XML-файлы, описывающие параметры этих предпочтений.
- **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. Если для пользователей заданы предпочтения, то в папке **User** также появляется подкаталог **Preferences** *(см. выше)*.

Папки **Machine** и **User** появляются сразу же при создании GPO-объекта. 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 GPO-объекта этот файл содержит следующую информацию:

- номер версии GPO-объекта;
- список идентификаторов (GUID) клиентских расширений оснастки **Group Policy Object Editor** (Редактор объектов групповой политики);
- состояние GPO-объекта (какие его части разрешены или запрещены).

Для доменных GPO-объектов файл Gpt.ini хранит:

- номер версии объекта;
- отображаемое имя GPO-объекта (если он не относится к стандартным).

Средства редактирования параметров безопасности и групповых политик

Для настройки параметров безопасности в Windows Server 2008 используются две основные оснастки:

- **Group Policy Object Editor**[1] (Редактор объектов групповой политики). При работе в доменах эта оснастка вызывается при необходимости из оснастки **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 *объектов групповой политики*, или GPO-объектов (Group Policy Object, GPO).

Примечание

Оснастка **Local Security Settings** (Локальная политика безопасности, secpol.msc) (рис. 7.34[2]) 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 груп-

[1] В доменах эта оснастка может использоваться для редактирования различных доменных GPO-объектов и фигурирует под разными именами (если добавлять оснастку к консоли MMC — см. рис. 7.35), однако по сути это одна и та же программа.

[2] Обратите внимание на политику, выбранную для примера в окне оснастки: по умолчанию для удаленного доступа к компьютеру нельзя использовать учетные записи, не имеющие пароля.

повой политики, расположенных 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.

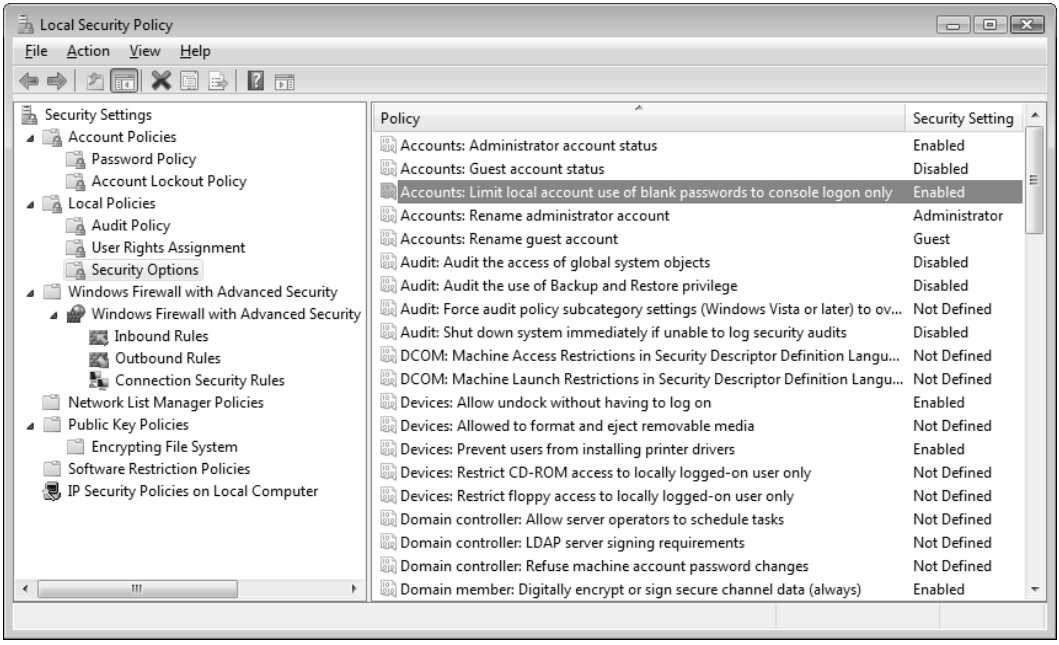


Рис. 7.34. Окно оснастки **Local Security Settings**

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 не привязанных 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).

Внимание!

При подключении оснастки **Group Policy Object Editor** (Редактор объектов групповой политики) к *удаленной* системе не все расширения доступны — например, основные параметры безопасности (Security Settings) можно редактировать только локально! Это нужно учитывать при развертывании систем Windows Server Core и Hyper-V Server, где основным средством настройки становится утилита Secedit.exe *(см. ниже)*.

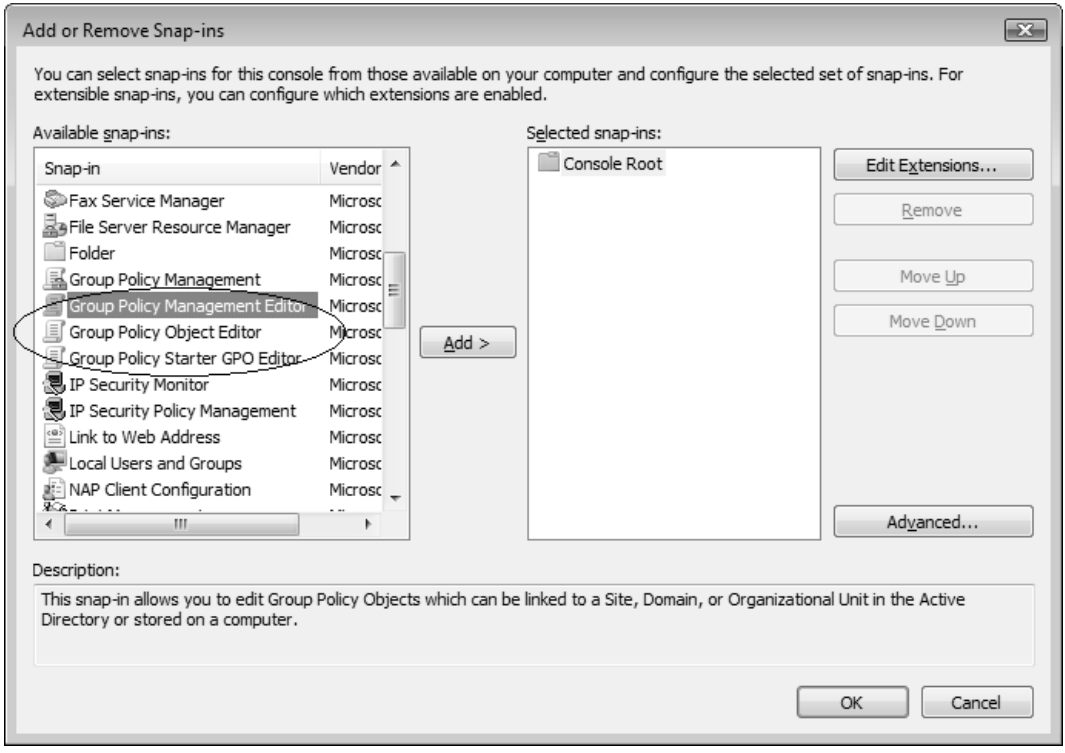


Рис. 7.35. Выбор редактора групповых политик

При добавлении редактора политик к консоли MMC в доменной среде появляются дополнительные варианты использования стандартной оснастки (рис. 7.35). Оснастка **Group Policy Management Editor** (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. 7.36). 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. 7.37). Настройка параметров любых объектов политик осуществляется одинаково.

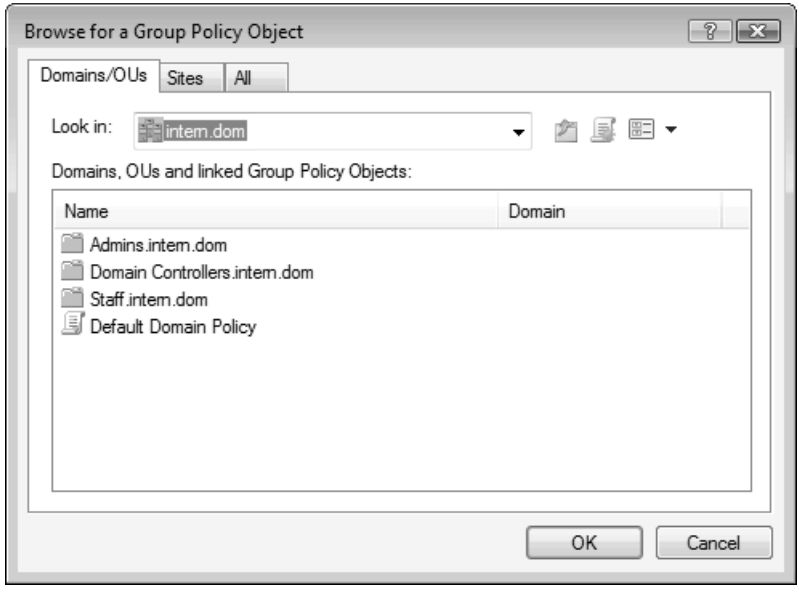


Рис. 7.36. Выбор редактируемого доменного GPO-объекта при подключении оснастки

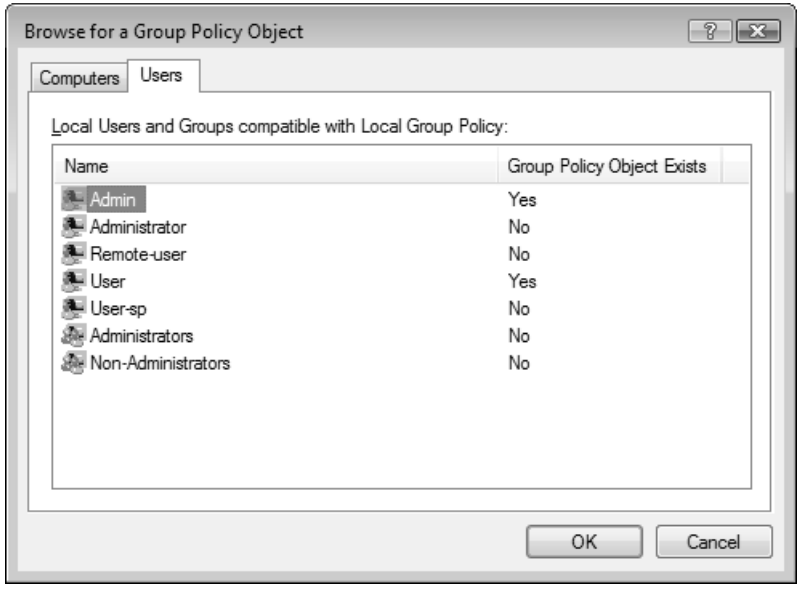


Рис. 7.37. Выбор пользователя,
на которого будут распространяться параметры GPO-объекта

Как можно видеть на рис. 7.37, политики локального GPO-объекта 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).

- Узел **Computer Configuration** (Конфигурация компьютера) содержит параметры всех политик, определяющих работу *компьютера*. Эти политики 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.

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 (рис. 7.38):

- *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. Используются только в доменных GPO-объектах;

- *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)*;

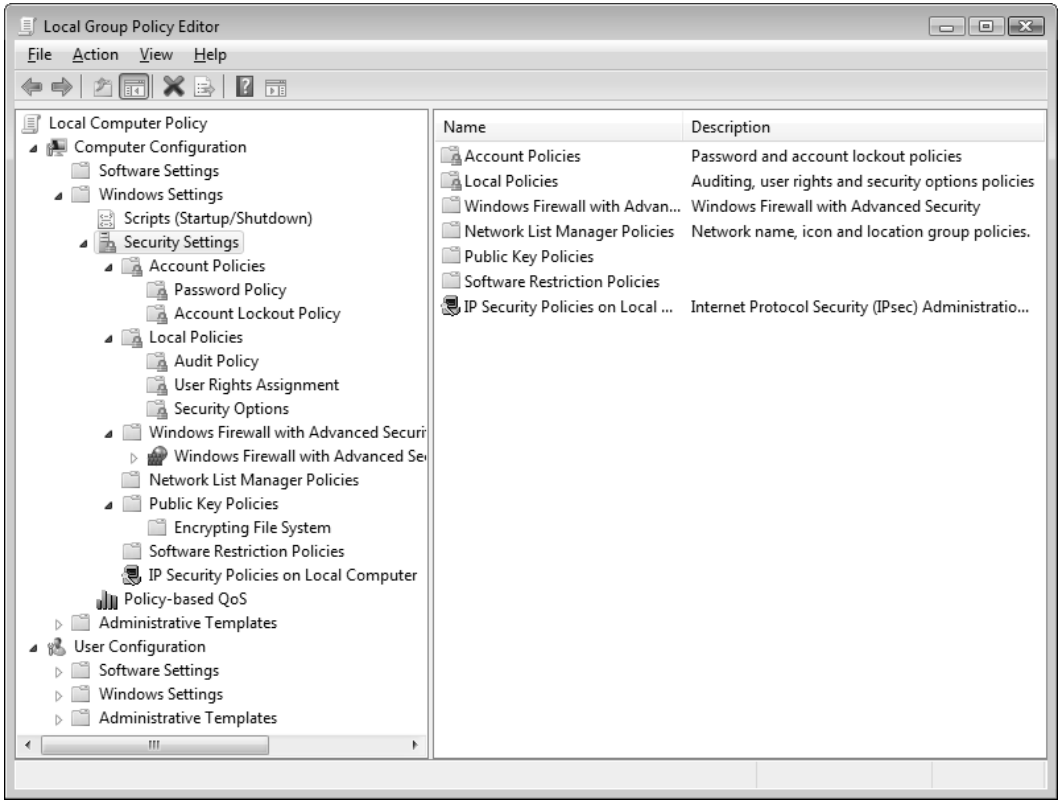


Рис. 7.38. Развернутое дерево объектов оснастки **Group Policy Object Editor**, в котором можно видеть ее основные расширения для локального GPO-объекта

- *Folder Redirection Editor* (Редактор перенаправления папок). Позволяет перенаправлять обращение к пользовательским папкам (**Documents** (Документы),

Pictures (Изображения) и т. д.) на сетевой ресурс. Имеется только в доменных GPO-объектах. В системах Windows Server 2008 можно перенаправлять любые папки, входящие в профиль пользователя, такие как **Videos** (Видео), **Downloads** (Загрузка) и т. п.;

- *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 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 GPO-объектах).

- *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).
- *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.
- *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.

---

[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.

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). Она является единственным средством конфигурирования политик в системах Windows Server Core и Hyper-V Server;
- *мастер Security Configuration Wizard* (Мастер настройки безопасности) — программа-мастер, позволяющая настроить конфигурацию параметров безопасности на "эталонном" компьютере и применять ее на других компьютерах.

Настройка параметров безопасности из командной строки

Групповые политики, хранящиеся в папке административных шаблонов, можно настраивать с помощью оснастки **Group Policy Object Editor** (Редактор объектов групповой политики), подключившись к системе с удаленного компьютера. Однако не все политики в этом случае доступны, и некоторые параметры можно менять только локально. (Речь идет о компьютерах, работающих в составе рабочей группы, поскольку в домене управление политиками централизованное и такой проблемы не стоит.) В том случае, когда инструменты с GUI-интерфейсом недоступны, единственным средством для настройки политик безопасности является утилита *Secedit.exe*. Ее можно использовать во всех версиях Windows Server 2008, включая Windows Server Core и Hyper-V Server.

Рассмотрим на примере, как можно изменить стандартные политики безопасности, работая в окне командной строки. Вся операция состоит из четырех этапов.

1. Экспортируйте в шаблон текущие параметры безопасности. Для этого в окне консоли выполните команду (имя файла произвольное; убедитесь в том, что файл отсутствует на диске!):

   ```
   C:\>secedit /export /cfg sec-pol.inf
   ```

   Результаты работы утилиты можно видеть в файле журнала %windir%\security\logs\scesrv.log. Полезно ознакомиться со структурой файла шаблона, открыв его в текстовом редакторе!

2. Создайте базу безопасности с использованием полученного шаблона. Для этого выполните следующую команду (имя базы данных произвольное):

   ```
   C:\>secedit /import /db sec-pol.sdb /cfg sec-pol.inf /overwrite
   Configuring the current system with this template in the /overwrite mode
   will result in losing the existing security records in the database speci-
   fied. Do you want to continue this operation ? [y/n] y
   ```

3. Отредактируйте файл шаблона, установив нужные значения политик. Это можно сделать с помощью редактора Notepad (Блокнот) (непосредственно в системе или подключившись к диску удаленно).

   Необходимость нужно соблюдать со встроенным редактором Edit.com! Файлы шаблона имеют формат Unicode, который этот редактор не поддерживает. Открывать такие файлы можно только как ***двоичные*** (установив флажок **Binary**) и менять символы, не нарушая форматирования (количества символов). Если же открыть файл в обычном текстовом режиме, то после редактирования и сохранения содержимое файла будет разрушено!

4. Настройте безопасность системы с использованием созданных файлов шаблона и базы данных. Для этого служит команда:

   ```
   C:\>secedit /configure /db sec-pol.sdb /cfg sec-pol.inf
   The task has completed successfully.
   See log %windir%\security\logs\scesrv.log for detail info.
   ```

Если ошибок не произошло, значит, операция закончена успешно.

Можно пойти немного другим путем: создать в редакторе файл шаблона, содержащий приведенную ниже структуру служебных тегов (все строки обязательны!), и вставить только тот параметр, который требуется изменить (он выделен курсивом):

```
[Unicode]
Unicode=yes
[System Access]
MinimumPasswordLength = 1
[Event Audit]
```

```
[Registry Values]
[Privilege Rights]
[Version]
signature="$CHICAGO$"
Revision=1
```

После этого требуется выполнить только шаги 2 и 4.

Для последующих изменений параметров безопасности достаточно только редактировать файл шаблона (шаг 3) и конфигурировать систему (шаг 4).

Определение действующих значений 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 GPO-объектами, 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. Ее удобно использовать для контроля за правильностью применения изменений, внесенных в GPO-объекты. 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 имеется уже ставший привычным 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 GPO-объекта.

Примечание

В доменах удобнее использовать оснастку **Group Policy Management** (Управление групповой политикой), которая имеет множество возможностей по манипулированию GPO-объектами. 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).
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). 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.
4. Укажите компьютер (локальный или удаленный), для которого проверяются параметры групповых политик. 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. 7.39). В этом окне видны все учетные записи пользователей, регистрировавшихся на компьютере и, следовательно, имеющих на нем RSoP-данные. (Выберем для примера пользователя User.) 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**.
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. 7.40), аналогичном окну оснастки **Group Policy Object Editor** (Редактор объектов групповой политики), будут отображаться только те папки (ниже второго уровня), в которых имеются измененные политики.

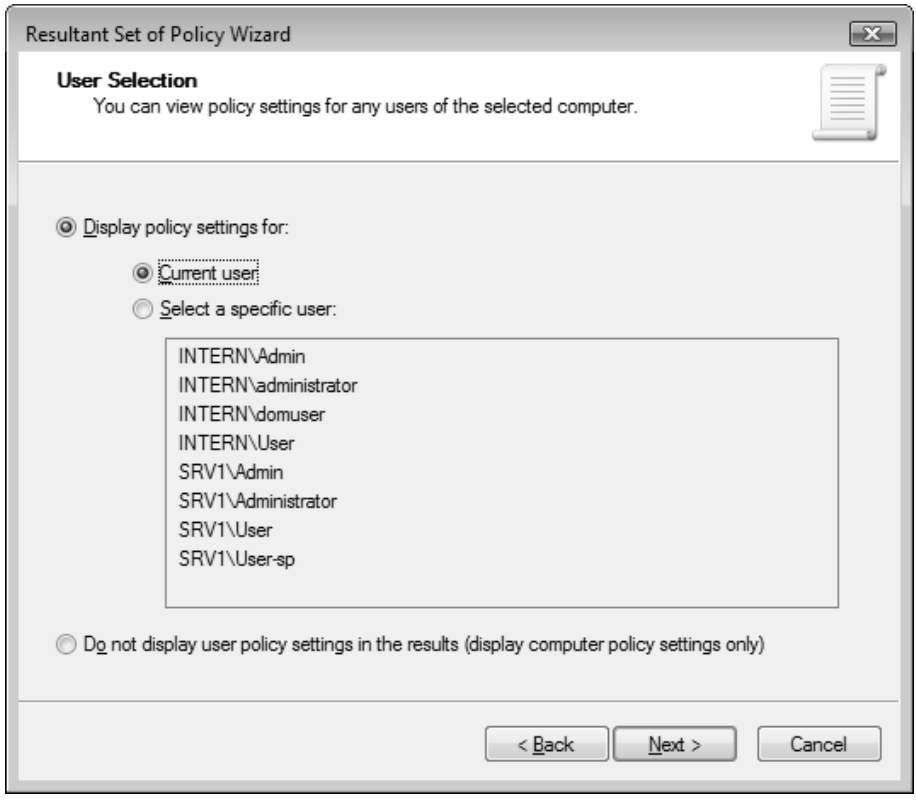


Рис. 7.39. Выбор учетной записи пользователя, для которого будут определяться значения групповых политик

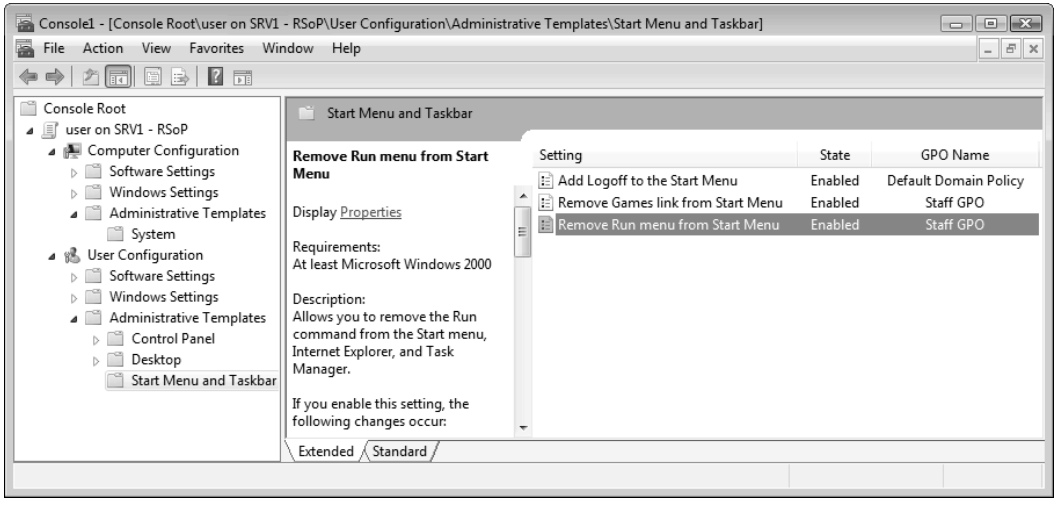


Рис. 7.40. Оснастка **Resultant Set of Policy** позволяет быстро определить, какие политики установлены для компьютера или пользователя

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).

Полученные сведения можно проверить с помощью утилиты GRResult и сравнить результаты (для нашего примере можно использовать команду `gpresult /USER INTERN\User /R /V`). Подобная информация очень полезна в сложных ситуациях, когда компьютер подключен к домену и имеется множество наследуемых групповых политик, заданных разными GPO-объектами.

Внимание!

Недостатком текущих версий оснастки **Resultant Set of Policy** (Результирующая политика) и утилиты GPResult.exe является то, что они не показывают установленные предпочтения (preferences). Наиболее полную информацию можно получить только с помощью оснастки **Group Policy Management** (Управление групповой политикой) *(см. ниже)*.

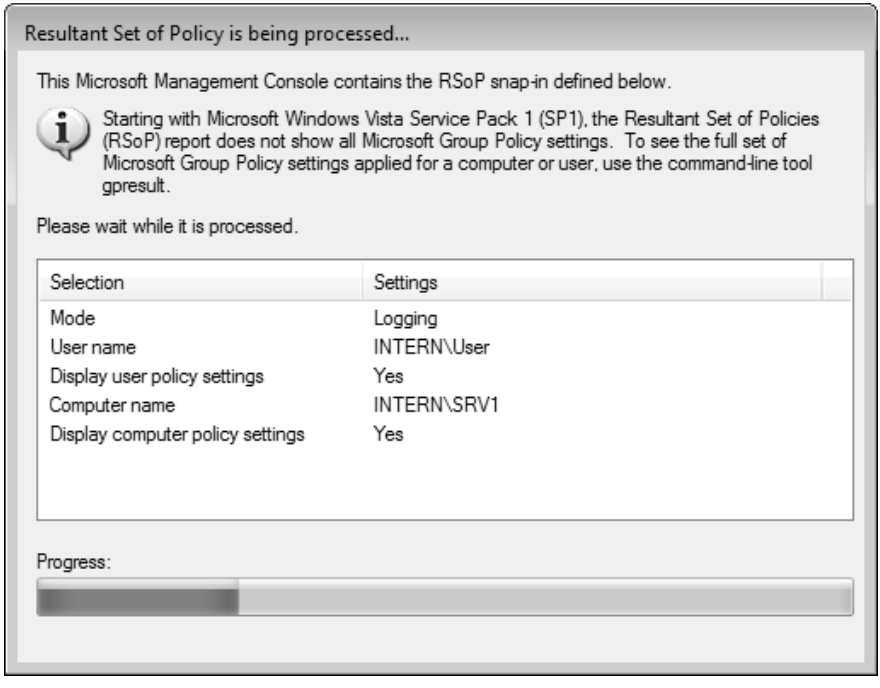


Рис. 7.41. Отображение процесса сбора RSoP-данных для указанного пользователя и компьютера

Обновить результаты для уже сконфигурированной оснастки можно при помощи команды **Refresh Query** (Обновление запросов), которая имеется в контекстном меню узла *<имяПользователя> on <имяКомпьютера> - RSoP* (см. рис. 7.40). 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. 7.41), 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.

Определение политик в домене

Операция по анализу действующих политик в доменах запускается 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) (см. рис. 7.42).

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. 7.42 можно видеть, как выглядят RSoP-данные, полученные для конкретного пользователя указанного домена. Обратите внимание на то, что помимо обычных политик отображаются и предпочтения (узел **Folders** в нижней части окна).

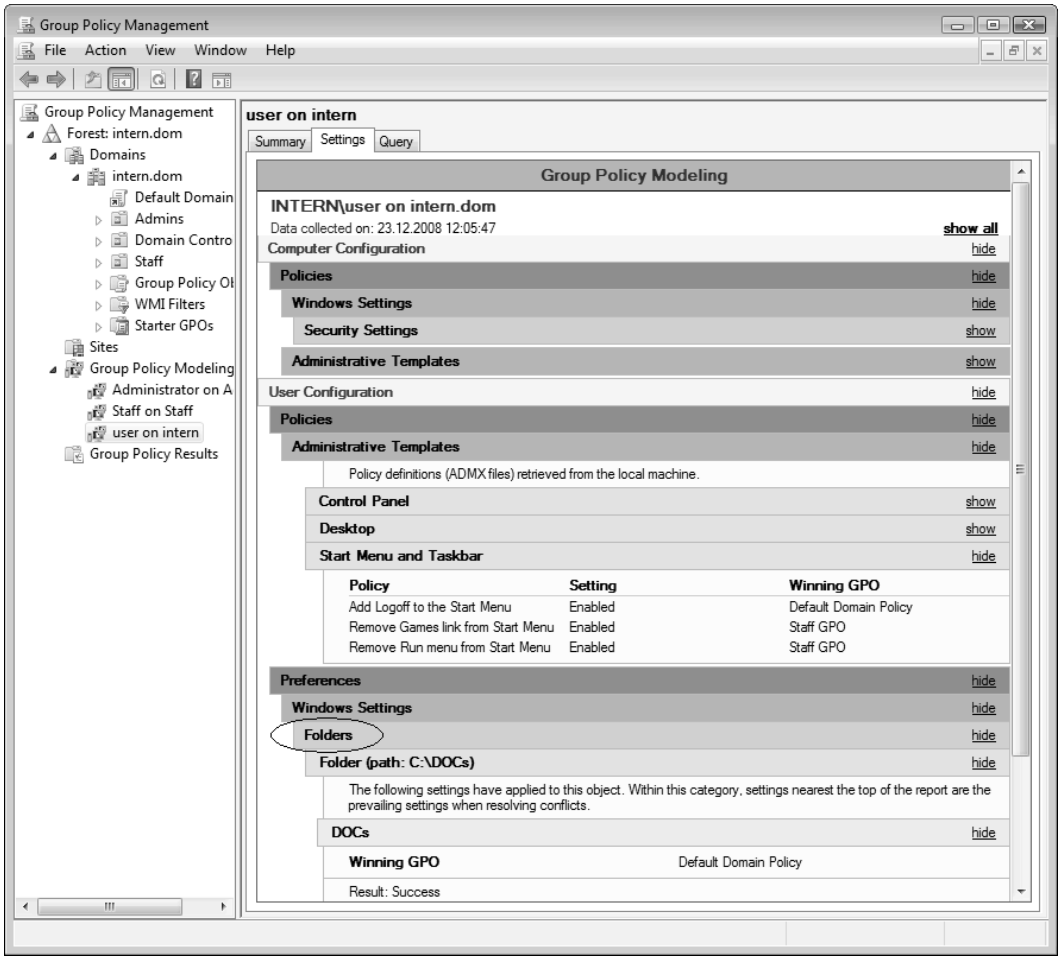


Рис. 7.42. Просмотр RSoP-данных, смоделированных для выбранного пользователя домена

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. 7.26) 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** (Копировать) 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 GPO-объектов и восстанавливать нужные комбинации параметров групповых политик. Команда **Paste** (Вставить) позволяет создать из буфера копию существующего GPO-объекта, причем исходный и новый объекты могут находиться в разных доменах или лесах.



ПРИЛОЖЕНИЯ



Приложение 1

Веб-ссылки

Перечислим адреса некоторых веб-ресурсов, которые должен знать каждый системный администратор, работающий с Windows, и в особенности — с серверными версиями. При необходимости более глубокого знакомства с тем или иным продуктом или технологией основным источником информации являются сайты TechNet и MSDN. При поиске решений по конкретным проблемам лучше всего обращаться к базе знаний Microsoft Knowledge Base. Все основные и развернутые материалы размещаются на англоязычных сайтах, хотя и русскоязычные "зеркала" содержат много полезной информации.

- *Search Microsoft.com* (Поиск на Microsoft.com) — основная страница поиска по сайту Microsoft; по ссылке **Advanced Search** (Расширенный поиск) можно перейти в окно поиска по различным веб-ресурсам Microsoft. Язык поиска и интерфейса страницы можно выбирать:

  search.microsoft.com

- *Microsoft Help and Support* (Справка и поддержка) — главная страница поддержки продуктов. Кнопка **Advanced Search** (Расширенный поиск) позволяет перейти в окно поиска по статьям базы знаний Microsoft (Microsoft Knowledge Base) по каждому поддерживаемому продукту. Язык сайта выбирается автоматически, в соответствии с языком, заданным по умолчанию в браузере:

  support.microsoft.com

- *Microsoft Download Center* (Центр загрузки Microsoft) — на этом сайте можно найти разнообразные утилиты, упоминаемые в книге, а также различные обновления и полезные программы; утилиты нужно искать на главной странице по ключевым словам, по названию или по имени дистрибутивного файла (имеется русскоязычное зеркало):

  www.microsoft.com/downloads

В частности, можно порекомендовать 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, используемой при работе с разнообразными сетевыми компонентами и службами (сетевыми интерфейсами, брандмауэром Windows, службами DHCP, RRAS и т. д.).

❒ *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 легко найти ссылку для скачивания пробной (trial) версии Windows Server 2008 и бета-версии Windows Server 2008 R2.

❒ *Microsoft Hyper-V Server* — главная страница сайта, посвященного этой операционной системе. Имеются ссылки для скачивания полнофункциональной версии Hyper-V Server и бета-версии Hyper-V Server R2:

www.microsoft.com/servers/hyper-v-server

❒ *Microsoft System Center Virtual Machine Manager Home* — главная страница продукта, предназначенного для централизованного управления инфраструктуры виртуальных машин, установленных на различных серверах (Windows Server 2008 с ролью Hyper-V, Microsoft Hyper-V Server и т. д.). Имеется ссылка для скачивания пробной (trial) версии:

www.microsoft.com/systemcenter/virtualmachinemanager

❒ *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 (рус.)

technet.microsoft.com/en-us

❒ *Windows Server TechCenter* (прямые ссылки 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).

- Специальная веб-страница, посвященная технологиям виртуализации:

  www.microsoft.com/rus/virtualization (рус.)

  www.microsoft.com/virtualization

- *Microsoft TechNet: Windows Sysinternals* (системные утилиты от не нуждающихся в представлении 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 модели процессоров, поддерживающих 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



Приложение 2

Оснастки и задачи панели управления систем Windows Server 2008

Оснастки, их имена и назначение

В табл. П2.1 перечислены основные оснастки, имеющиеся в составе полных систем Windows Server 2008 (в версиях Windows Server Core и Hyper-V Server консоль MMC полностью отсутствует). Также упомянуты некоторые оснастки, появляющиеся при установке ролей сервера. 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 П2.1. *Оснастки систем Windows Server 2008*

Оснастка	Назначение
ActiveX Control (Элемент ActiveX)	Добавляет в консоль элемент ActiveX

[1] В обоих случаях обязательно нужно указывать расширение .msc!

Таблица П2.1 *(продолжение)*

Оснастка	Назначение
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
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

Таблица П2.1 *(продолжение)*

Оснастка	Назначение
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
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. Появляется при установке соответствующего компонента сервера

Таблица П2.1 *(продолжение)*

Оснастка	Назначение
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, ServerManager.msc)*	Позволяет контролировать состояние сервера, выполнять общие административные задачи, добавлять или удалять роли и программные компоненты сервера
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, tapimgmt.msc)	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)

Таблица П2.1 *(окончание)*

Оснастка	Назначение
Windows Firewall with Advanced Security (Брандмауэр Windows в режиме повышенной безопасности, WF.msc)*	Тонкая настройка брандмауэра Windows, создание правил для входящих и исходящих подключений
Windows Server Backup (Система архивации данных Windows Server, wbadmin.msc)*	Управляет функциями архивации и восстановления данных на сервере. Появляется при установке соответствующего компонента сервера
WMI Control (Управляющий элемент WMI, WmiMgmt.msc)	Позволяет настраивать и управлять службой WMI

Примечание

Кроме оснасток, перечисленных в табл. П2.1, 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.

В табл. П2.2 перечислены важные дополнительные оснастки Windows Server 2008, устанавливаемые только на контроллерах доменов и используемые для управления службами каталога Active Directory.

Таблица П2.2. *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 П2.2 *(окончание)*

Оснастка	Назначение
ADSI Edit (Редактирование ADSI, adsiedit.msc)*	Низкоуровневый редактор объектов каталога Active Directory (ранее 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). Также отсутствует оснастка **Disk Defragmenter** (Дефрагментация дисков).

Названия служебных утилит и задач панели управления

В табл. П2.3 перечислены задачи (CPL-файлы) панели управления, к которым можно непосредственно обращаться по имени файла из меню **Start** (Пуск), окна консоли и т. п. (расширение .cpl обязательно!). Имя файла указано в скобках, после названия, принятого в локализованной русской версии. Звездочками отмечены две утилиты, которые присутствуют также в версиях Windows Server Core и Hyper-V Server.

Таблица П2.3. *Задачи панели управления, которые можно вызывать непосредственно*

Категория задач	Задача
System and Maintenance (Система и ее обслуживание)	**System** (Система, sysdm.cpl);
Security (Безопасность)	**Internet Options** (Свойства обозревателя, inetcpl.cpl)
Network and Internet (Сеть и Интернет)	**Windows Firewall** (Брандмауэр Windows, Firewall.cpl)

Таблица П2.3 *(окончание)*

Категория задач	Задача
Hardware and Sound (Оборудование и звук)	**Sound** (Звук, mmsys.cpl) **Mouse** (Мышь, main.cpl) **Power Options** (Электропитание, powercfg.cpl) **Phone and Modem Options** (Телефон и модем, telephon.cpl) **Tablet PC Settings** (Параметры планшетного компьютера, TabletPC.cpl)
Programs (Программы)	**Programs and Features** (Программы и компоненты, appwiz.cpl)
Clock, Language, and Region (Часы, язык и регион)	**Date and Time** (Дата и время, timedate.cpl) * **Regional and Language Options** (Язык и региональные стандарты, intl.cpl) *
Отсутствуют на панели управления	**Add Hardware Wizard** (Мастер установки оборудования, hdwwiz.cpl) **Display Settings** (Параметры дисплея, desk.cpl) **Network Connections** (Сетевые подключения, ncpa.cpl) **System Properties** (Свойства системы, sysdm.cpl)

Примечание

Альтернативный вариант прямого доступа к *любой* задаче панели управления описан в *разд. "Непосредственный доступ к задачам панели управления" главы 2.*



Приложение 3

Административные утилиты командной строки

Встроенные утилиты

Количество стандартных утилит командной строки, имеющихся в составе систем Windows Server 2008, значительно увеличилось по сравнению с предыдущими серверными версиями Windows. С помощью утилит можно выполнять практически все операции, которые доступны административным оснасткам. (Этот момент особенно важен при использовании Windows Server 2008 Server Core.) Кроме того, многие утилиты незаменимы при диагностике или выполнении 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 (например, можно скачать справочник по командам консоли — *см. Приложение 1*). Информацию о параметрах конкретной утилиты легко получить, запустив ее в окне командной строки с ключом `/?`.

Ниже перечислены стандартные утилиты командной строки, имеющиеся в составе Windows Server 2008, и указывается их основное назначение:

- AuditPol.exe — управление политиками аудита;
- BcdEdit.exe — редактор опций диспетчера загрузки Windows (Windows Boot Manager);
- Comp.exe и Fc.exe — сравнение двоичных и текстовых файлов;
- Convert.exe — преобразование файловой системы тома из FAT в NTFS;
- Defrag.exe — дефрагментация дисковых томов;
- DiskPart.exe — управление дисками и томами;
- Dsacls.exe — отображение и изменение списков управления доступом (ACL) для объектов каталога Active Directory;

- 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);
- Ldp.exe (Active Directory Administration Tool) — поиск и модификация объектов каталогов Active Directory при помощи LDAP-запросов;
- 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 поставляются в составе пакета, который называется *Windows Support Tools*. Он имеется на дистрибутивных дисках систем Windows Server 2003, а самые последние версии можно скачать в Центре загрузки Microsoft *(см. Приложение 1)*.

Многие из утилит этого пакета включены в состав Windows Server 2008 (некоторые из них становятся доступными в системе только после установки соответствующих ролей сервера — например, утилиты для работы с каталогами Active Directory). Тем не менее, некоторые полезные утилиты (например, NetDiag.exe, Search.vbs, MoveTree.exe, ReplMon.exe, Clonepr.vbs и др.) по-прежнему можно найти только в составе пакета Windows Support Tools. Практически все эти утилиты работают в среде Windows Server 2008.

Отдельно нужно скачивать и утилиту *Active Directory Migration Tool version 3* (ADMT v3), незаменимую при миграции и реорганизации доменов Active Directory.

Предметный указатель

A

Active Directory Administration Tool
  См. Ldp.exe
Active Directory Domain Services
  (сервис NTDS) 376
Active Directory Replication Monitor
  См. Replmon.exe
AD LDS 414
address pool 304
Admin Approval Mode 77
Administrative Template Files, ADMX 431
ADMT 477
ADMX *См.* Administrative Template Files
ADM-файлы 430
adprep.exe 374, 376
ADSL 295
Advanced Features mode 403
Aero 6, 15
Aero Glass 14, 15
answer files 47
Applcation Logs 166
application partitions 316, 327
ASP.NET 25
audit 124
autologon 110

B

Bandwidth Allocation Protocol (BAP) 335
basic disk 194
BCDedit.exe 24
BIOS 98
BitLocker™ Drive Encryption 8, 85
boot partition 19
boot.ini 21, 23
boot.wim 27
BOOTP/DHCP:
  агент ретрансляции 314
Bootsect.exe 21
bridgehead 411

C

Cacls.exe 213
CDFS 20
Certificate Export Wizard 254
cipher.exe 252, 255
commandlet 143
CompMgmtLauncher.exe 40
Computer Configuration 449
Computers, контейнер 394
Conditional forwarding 316, 321
Configuration partition 413
connection 415
contiguous subtree 413
Control Panel 84
Cookies, папка 114
CPL-файлы 26, 86, 473
Csvde.exe 398
custom view (Event Viewer) 168

D

Data Collector Sets 150, 174, 185
Data Recovery Agent 251
Dcdiag.exe 329, 331, 384
Dcpromo.exe 319, 391, 392, 440
Defender 162
defrag.exe 201
demand-dial interface 344
demotion 391
Deny, разрешение 213
Deployment Server (Сервер развертывания) 52
Desktop Experience (Возможности рабочего стола), компонент 91, 104
Devcon.exe 58
devmgmt.msc 57
DFS 239
  группа репликации 246
DFS Namespaces (Пространства имен DFS) 240
DFS Replication (Репликация DFS) 240, 250, 416, 421, 438
dfsmgmt.msc 242
DFSR 438
DfsrAdmin.exe 242
DfsrDiag.exe 242
DfsUtil.exe 242
DfsCmd.exe 242
DHCP 302, 318, 348, 352
  автоконфигурирование IP-адреса 309
  агент ретрансляции (relay) 314
  диапазон исключения 304
  классы параметров (option class) 307
  область действия 303
  параметры (options) 307
  период аренды 306
  пул адресов 304
  резервирование 305
DHCPServer 309
dial-up connection 297
Direct Connection 298
directory partition 413
Directory Services Restore Mode 373
Directory Services Restore Mode Administrator 382
Disk Cleanup (Очистка диска), утилита 100
Disk Defragmenter 200
diskmgmt.msc 195
DiskPart.exe 19, 32, 195, 196, 197, 198
Distributed File System (DFS) 239
DNS 311, 315, 352
  зоны:
    вторичные (secondary) 320
  корневые ссылки (root hints) 318
  основной суффикс 87, 331, 393
  передачи зоны 320
  серверы пересылки (forwarders) 318
DnsAdmins, группа 321
dnscache 317
DnsCmd.exe 321, 326, 327, 330
dnsmgmt.msc 319
DNS-клиент 317
DNS-сервер:
  вторичный 318, 320
  дополнительный 331
  кэширующий 318
  основной 318
  предпочитаемый 331
Domain Name System. *См.* DNS
Domain network 281
Domain partition 413
Domain profile 362
DomainDnsZones 319
Driver Rollback 48
DriverQuery.exe 58
Dsamain.exe 373
Dynamic Host Configuration Protocol. *См.* DHCP

E

EAP 335
EasyBCD, утилита 25
Encrypting File System (EFS) 251, 452
exceptions 281
exclusion range 304
exFAT 20
Extend Volume Wizard 198
Extensible Firmware Interface (EFI) 471

F

Fast User Switching 74
FAT12 20
FAT16 20
FAT32 20
Fdeploy.ini 444
Feature (компонент сервера) 101, 102
File and Printer Sharing 281
File Replication service (FRS) 244, 415, 438
File Services (Файловые службы) 189
forest trusts 423
ForestDnsZones 319
forwarded event 170
Forwarded Events, журнал 166, 171
Forwarders (DNS) 318, 322
FRS *См.* File Replication Service
fsmgmt.msc 207
FSMO-роли:
  Schema Master 374
Fsutil.exe 114, 196, 225
functional levels 419, 422

G

GPC. *См.* Объект групповой политики
GPEdit.msc 441
gpmc.msc 432
GPO *См.* Объект групповой политики
GPResult.exe 455, 458, 459
gpsvc 431
GPT. *См.* GUID partition table
Gpt.ini 445
GptTmpl.inf 441, 444
GPUpdate.exe 455
Group Policy Client 431
Group Policy Container (GPC) 442
Group Policy Object (GPO). *См.* Объект групповой политики
Group Policy Template (GPT) 442
GroupPolicy, папка 440
GroupPolicyUsers, папка 441
GUID partition table 193, 442

H

hardware profile 57
hiberfil.sys 99, 100
Hibernate 95, 98
HVConfig.cmd 61
Hybrid sleep 95, 99
Hyper-V 4, 5, 14, 15, 60
Hyper-V Manager 62
Hyper-V Server *См.* Microsoft Hyper-V Server 2008

I

Icacls.exe 213
ICMP. *См.* Internet Control Message Protocol
ICS. *См.* Internet Connection Sharing
IGMP 335
Indexing Service 117
Infrastructure Masters 375

Initial Configuration Tasks (Задачи начальной настройки) 38
install.wim 27
Integration Services 69
Internet Connection Sharing (ICS) 298, 343, 352
Internet Control Message Protocol (ICMP) 364, 431
Internet Explorer Administration Kit (IEAK) 430
Internet Explorer Maintenance (IEM) 430
Intersite Messaging 376
Ipconfig.exe 289, 307, 310
IsmServ 376
Itanium-системы 4, 192

J

junction points 114

K

kdc 376
Kerberos 451
Kerberos Key Distribution Center 376
Kerberos V5 141
Knowledge Consistency Checker (KCC) 328, 411, 415

L

L2TP 334
L2TP/IPSec 334
Language Interface Pack (LIP) 92
Last Known Good 49
Ldifde.exe 398
Ldp.exe 373, 396
lease 306
Link Layer Topology Discovery (LLTD) responder 288
Local Area Connection 283, 296
Local Group Policy Object (LGPO) 440
logging mode (RSoP) 456

M

Manage Your Server (Управление данным сервером) 39, 100
Master Boot Record (MBR) 192
Microsoft Download Center 465
Microsoft Hyper-V Server 2008 4, 60
mirrored volume 195
msc, расширение 468
MS-CHAP v2 335
Msconfig.exe 25, 83
Msg.exe 280
Msinfo32.exe 150
mstsc, утилита 130
multicast 303, 335
Multilingual User Interface (MUI) 92
multimaster replication 414

N

naming context 413
NAP *См.* Network Access Protection
NAT. *См.* Network Address Translation
ncpa.cpl 294
net 110
  send 280
  share 209
  time 142
  use 210
  view 209

NetDiag.exe 329, 384, 477
NetDom.exe 425
NETLOGON, папка 415
Netsh.exe 288, 295, 313, 365, 466
Network Access Protection (NAP) 9
Network Address Translation (NAT) 334, 342, 352
Network and Sharing Center 237, 284
Network category 281, 285
Network Detection 288
Network Level Authentication 130
network location 281
Network Location Awareness (NLA) 431
network map 286
Nslookup.exe 329
NTDS 373, 376
NTDSutil.exe 327, 373, 382, 386
NTFS 20
NTLDR 21
NTP, протокол 141

O

Oclist.exe 108, 258
Ocsetup.exe 108
oobe.exe 27, 39

P

PAE *См.* Physical Address Extension
partition table 192
PDC Emulator 142
perfmon.msc 174
Performance Monitor 150, 174, 177
Performance Rating 87
Permissions 212
  effective 219
Physical Address Extension (PAE) 13
planning mode (RSoP) 456
Pnputil.exe 58
PolicyDefinitions, папка 451
POP3 280
Power Options 93
power plan 93
power scheme 93
powercfg 99
PowerShell 143
PPTP 334
Preboot eXecution Environment (PXE) 52
preferences, политики 435
pre-shared key 339
previous versions 271
primary DNS suffix 87, 331
Private network 281
Private Profile 362
profile 112
promotion 373
Public network 281
Public Profile 362

Q

qprocess, утилита 154
query definition 403
quota 224

R

RADIUS 341
RAID-0 195
RAID-5 195
RAS-сервер 300
RDP-файл 133
Recovery Console 51
RedirCmp.exe 395
Registry.pol 444

Reliability and Performance Monitor 150, 174
Reliability Monitor 150, 174, 183
remote access policy 342
Remote Access Server 300
Remote Assistance 129
remote control 338
Remote Desktop 129
Remote Desktop Connection 130
Remote Differential Compression (RDC) 240, 439
Remote Installation Services (RIS) 51
RemoteAccess, сервис 336
replication 413
Replication Diagnostics Tool (RepAdmin.exe) 416
replication topology 415
Replmon.exe 396, 411
reservation 305
Resource Monitor 175
Resultant Set of Policy Wizard 456
reverse zones 319
Robocopy.exe 268
RODC 388
role 101
Role Services 101
root hints 322
Routing and Remote Access Service (RRAS, Служба маршрутизации и удаленного доступа) 314, 333
  pre-shared key 334
RSOP
  logging mode 433
  planning mode 433
Runas 396

S

Safe mode 49
Saved Queries 401
sc, утилита 111, 159
Schedule 137
Schema Master 374
Schema partition 413
Schtasks.exe 136
scope (DHCP) 303, 308
screen saver 91
Secedit.exe 453
secedit.sdb 441
Secpol.msc 441, 445
secure channel 395
Security Configuration and Analysis 453
Security Settings 451
Security Templates 453
Send To, команда 115
Serial Line Interface Protocol (SLIP) 280
Server Core. *См.* Windows Server 2008 Server Core
Server Manager 101
server role 101
ServerManager.msc 104
ServerManagerCmd.exe 40, 107
Services for Machintosh (SFM) 280
Setup log 107, 165
setup.exe 27
Sfc.exe 48
Sharing Wizard 203
shutdown 37
SID 441
SID history 420
Sigverif.exe 48
simple volume 195
Single Instance Store (SIS) 52
Sleep 98
SLIP 280
slmgr 30, 46
SMTP 280
SMTP Server 280
SMTP Service 280
Snap-in:
  Computer Management 108, 336
  Device Manager 57

Event Viewer 125, 149, 164
Group Policy 125
Local Security Settings 125
Services 111
snapshot 64
SNMP Services 280
Software Exporer (Проводник программного обеспечения) 150, 162
spanned volume 195
Starter GPO 435
Stub Zones 316, 325
Subsystem for UNIX-based Applications 280
Support Tools 396
svchost.exe 154, 158
sysdm.cpl 87
Sysprep.exe 55
System Configuration (Msconfig.exe), утилита 25, 83
System Information (Msinfo32.exe), утилита 58, 150
System Monitor 150
system partition 19
System State 386
SystemInfo.exe 150
SYSVOL 382, 416, 421, 431, 442, 443
репликация 438

T

Take Ownership, разрешение 220
Task Manager 149, 151
Task Scheduler 136
taskkill, утилита 154
tasklist, утилита 154
taskschd.msc 137
Telnet Client 280
Telnet Server 280
Terminal Services 129, 338
TFTP Client 280
Themes (Темы), сервис 91
Time Service 141
Transport Server (Транспортный сервер) 52
Trivial File Transfer Protocol (TFTP) 52
Trusted Platform Module (TPM) 8, 471
tunneling protocols 334

U

UAC *См.* User Account Control
UDF 20
unattended setup 46
upgrade 33
User Account Control (UAC) 76, 157, 430
управление режимами 81
User Configuration 449
user profile 112
Users, Contacts, Groups, and Computers as Containers 404

V

vds, сервис 195, 222
virtual network 64
Virtual Private Network (VPN) 297, 338
VistaBootPro, утилита 25
VMconnect.exe 70
Volume Shadow Copy Service (VSS) 260
VPN-подключение 297, 333
VPN-сервер 300

W

W32Time 141
WAIK *См.* Windows Automated Installation Kit

Wbadmin.exe 257, 260, 276
wbadmin.msc 260
WDDM 14
WDS *См.* Windows Deployment Services
WDSUtil.exe 53
Web Service-Discovery (WS-Discovery, WSD) 292
Web Services on Devices 292
Wecsvc 171
Welcome screen 73
WerSvc 171
Wevtutil.exe 164
WIM *См.* Windows Imaging
WinDefend 162
Windows Aero 6, 91
Windows Automated Installation Kit (Windows AIK, WAIK) 46, 55
Windows Boot Manager 19, 21
Windows Calendar (Календарь Windows) 104
Windows Defender 162
Windows Deployment Services (Службы развертывания Windows) 51
Windows Error Reporting Service 171
Windows Event Collector Service 171
Windows Firewall 281, 295, 355, 366
  исключения 281
  правила (rules) 281
Windows Imaging (WIM) 6, 26
Windows Longhorn 3
Windows Media Player 104
Windows Photo Gallery (Фотоальбом Windows) 104
Windows PowerShell 143
Windows Remote Management (WinRM) 171
Windows Scripting Host (WSH) 143
Windows Search 117, 121, 181
Windows Search, конфигурирование 120
Windows Server 2008 Server Core 4, 25, 33
Windows Server Backup (Система архивации данных Windows Server) 257
Windows Server Update Services (WSUS) 42
Windows Support Tools 426, 477
Windows System Image Manager 47
Windows System Performance Rating 87
Windows Time Service 141
Windows Update 41
Windows.old 21
Winlogon 431
winnt.exe 27
winnt32.exe 27
WinRM 171
Winrm.exe 171
Wireless LAN Service (Служба беспроводной локальной сети) 296
WMI-фильтры 433
WSearch, сервис 117, 121
WSH 143
WS-Management 171
wuapp.exe 41
wuauserv 41

X

X.25 280
XML 431

Z

zone:
  stub 325

А

Автологон 110
Автоматическая архивация 262
Автоматическое обновление 41
Автоматическая установка 46
Агент восстановления 251
Агент ретрансляции BOOTP/DHCP 314
Активация системы 46
Архивация полного образа или отдельных томов 265
Аудит 124
  активизация 125
  отключение 128

Б

Базовые диски 194, 197
Безопасные каналы 395
БИОС 98
Брандмауэр Windows 281, 355
  исключения 357
Быстрое переключение пользователей 74

В

Виртуализация операций записи в файлы и реестр 78
Виртуальная частная сеть 64, 297, 333
Владелец файла или папки 212, 220
Возможности рабочего стола, компонент 91, 104
Восстановление данных из архива 269
Входящие подключения 299
Выключение компьютера 37

Г

Гибернация 95, 98
Гибридный спящий режим 95, 99
Главная загрузочная запись 192
Группа:
  Administrators (Администраторы) 78
  Remote Desktop Users (Пользователи удаленного рабочего стола) 130
Группы сборщиков данных (Data Collector Sets) 150, 174, 185

Д

Двойная загрузка 20, 50
Действующие разрешения 212
Дефрагментация:
  из командной строки 201
Дефрагментация диска, утилита 200
Дешифрование файлов 251
Динамические диски 195, 198
Диспетчер загрузки Windows 21
Диспетчер задач 149, 151
Диспетчер устройств 87
Доверительные отношения на уровне лесов (forest trusts) 423
Доменная сеть 281
Дополнительные функции, режим 403
Дополнительный раздел 194

Ж

Журнал настройки 107, 165
Журнал событий 124

З

Загрузочный диск 196
Загрузочный раздел диска 19
Заставка экрана 91
Защитник Windows 162
Зона:
  интегрированная 318
  заглушка 316, 325
  обратного просмотра 319

И

Индекс производительности 87

К

Карта сети 286
Категория сети 281, 285, 362
Квота на дисковое пространство 224
  управление из командной строки 225
Клиент групповой политики, служба 431
Командлеты 143
Коммутируемые подключения 297
Компонент (Feature) 101, 102
Консоль восстановления 51
Контейнер групповых политик 442
Контекст имен 413
Контроллер домена:
  создание 372
Контроль учетных записей 86
Конфигурация компьютера 449
Конфигурация пользователя 449
Конфигурация системы, утилита 25, 83
Корневые ссылки 322
Косвенные разрешения 212

Л

Логические диски 194
Локальный объект GPO 432

М

Маршрутизация и удаленный доступ, служба 314
Мастер:
  Active Directory Installation Wizard (Мастер установки Active Directory) 373, 376, 391, 392
  Backup Once Wizard (Мастер однократной архивации) 266
  Backup Schedule Wizard (Мастер расписания архивации) 263
  Certificate Export Wizard (Мастер экспорта сертификатов) 254
  Configure a DNS Server Wizard (Мастер настройки сервера DNS) 321
  Extend Volume Wizard (Мастер расширения тома) 198
  Group Policy Modelling Wizard (Мастер моделирования групповой политики) 459
  Group Policy Results Wizard (Мастер результатов групповой политики) 459
  New Scope Wizard (Мастер создания области) 311
  Recovery Wizard (Мастер восстановления) 269
  Resultant Set of Policy Wizard (Мастер результирующей политики) 456

Routing and Remote Access Server Setup Wizard (Мастер настройки сервера маршрутизации и удаленного доступа) 336
Security Configuration Wizard (Мастер настройки безопасности) 453
Sharing Wizard (Мастер общего доступа) 203
Монитор ресурсов 159, 175
Мониторинг сети 160

Н

Настраиваемые представления (Просмотр событий) 168

О

Области (scope) 308
Обновление системы 33
Общественная сеть 281
Общий доступ к подключению к Интернету (Internet Connection Sharing, ICS) 343, 352
Общий доступ к дискам 201
Объект групповой политики (group policy object, GPO) 440, 445
локальный 440
начальный (стартовый) 435
Окно регистрации 73
Оснастка:
Active Directory Domains and Trusts (Active Directory – домены и доверие) 419
Active Directory Schema (Схема Active Directory) 427
Active Directory Sites and Services (Active Directory – сайты и службы) 410
Active Directory Users and Computers (Active Directory – пользователи и компьютеры) 399
ADSI Edit (Редактирование ADSI) 326, 425
Certificates (Сертификаты) 252
Computer Management (Управление компьютером) 108, 195, 336
Device Manager (Диспетчер устройств) 57
DFS Management (Управление DFS) 240, 242
Disk Defragmenter (Дефрагментация диска) 200
Disk Management (Управление дисками) 195
DNS 319, 321
Event Viewer (Просмотр событий) 125, 149, 164
File Server Resource Manager (Диспетчер ресурсов файлового сервера) 229
Group Policy Management (Управление групповой политикой) 399, 403, 432, 456
Group Policy Object Editor (Редактор объектов групповой политики) 445, 446
Local Security Policy (Локальная политика безопасности) 125, 441, 445
Reliability and Performance Monitor (Монитор производительности и стабильности) 150, 174
Reliability Monitor (Монитор стабильности системы) 150, 174, 183
Resultant Set of Policy (Результирующая политика) 455

Routing and Remote Access (Маршрутизация и удаленный доступ, rrasmgmt.msc) 336
Security Templates (Шаблоны безопасности) 453
Security Configuration and Analisys (Анализ и настройка безопасности) 453
Server Manager (Диспетчер сервера) 39, 101, 104, 150, 164, 167, 396
Services (Службы) 111
Share and Storage Management (Управление общими папками и хранилищами) 222
Shared Folders (Общие папки) 207
Task Scheduler (Планировщик заданий) 136
Windows Deployment Services (Службы развертывания Windows) 52
Windows Firewall with Advanced Security (Брандмауэр Windows в режиме повышенной безопасности) 361
Windows Server Backup (Система архивации данных Windows Server) 260
Оснастки Windows Server 2008 468
Основной DNS-суффикс 87, 331
Основной раздел 194
Основной суффикс DNS 393
Отказ в разрешении 213
Откат драйверов 48
Очистка диска, утилита 100

П

Пакет автоматической установки Windows (WAIK) 46
Панель управления 84
Параметры безопасности (Security Settings), узел GPO 451
Пароль, изменение 36
Перезагрузка компьютера 37
Пересланные события 166
Пересланные события, журнал 171
План (схема) электропитания 93
Планирование заданий 136
Планировщик задач 201
Подключение к домену 37
Подключение к удаленному рабочему столу, утилита 130
Подключение по локальной сети 283, 296
Подключение по требованию 344
Подключение репликации 415
Подписки на события 170
Подсистема для UNIX-приложений 280
Поиск (опция оснастки) 407
Поиск информации на компьютере 116
Пользователи, контакты, группы и компьютеры как контейнеры, режим 404
Право владения 220
Предварительный ключ 339
Предпочтения (preferences) 435
Предыдущие (прежние) версии 271
Преобразование сетевых адресов (NAT) 342
  компоненты 343
  конфигурирование 343
Проводник программного обеспечения 162
Пространства имен DFS 240
Протоколы туннелирования 334, 338
Профиль оборудования (hardware profile) 57
Профиль пользователя 87, 112
Прямые разрешения 212

Р

Раздел диска 194
Разделы каталога 413
  доменный раздел каталога 413
  раздел конфигурации 413
  схема 413
Разделы приложений 316, 327, 414, 426
  DomainDnsZones 319
  ForestDnsZones 319
Разрешения:
  действующие 219
  для файлов и папок 212
  смена владельца 220
  специальные 215
Распределенная файловая система (DFS) 239
Режим ведения журнала (RSoP) 456
Режим входа (RSoP) 456
Режим одобрения администратором 77
Режим планирования (RSoP) 456
Режимы работы доменов 419
Результирующая политика:
  режим планирования 433
  режим ведения журнала 433
Репликация DFS 240, 438
Репликация каталога 412, 417
Репликация с множеством равноправных участников 414
Роли FSMO:
  Schema Master 429
Роль сервера 101

С

Сборщик событий Windows (Wecsvc) 171
Сведения о системе, утилита 150
Сервер времени 142
Сервер сценариев 143
Сервер удаленного доступа 300, 333
Сервер-форпост (сервер-плацдарм) 411
Серверы пересылки 323
Сертификаты 339
Сетевое размещение 281
Сетевой диск 208
Сетевые подключения:
  VPN-подключение 297
  входящие 299
  по локальной сети 296
  прямые 298
  телефонные (коммутируемые) 297
Система архивации данных Windows Server 257
Системные переменные 87
Системный диск 196
Системный монитор 150, 174, 177
Системный раздел диска 19
Системы с двойной загрузкой 20
Служба:
  SMTP 280
  беспроводной локальной сети, компонент 280, 296
  времени Windows 141
  доменных имен (DNS) 315
  доступа к папкам и принтерам (File and Printer Sharing) 288
  индексирования (Indexing Service) 117
    конфигурирование 120
  маршрутизации и удаленного доступа
    предварительный ключ 334
  поиска Windows 117
  регистрации ошибок Windows (WerSvc) 171
  репликации файлов 244, 415
Службы:
  интеграции 69

развертывания Windows 51
роли (Role Services) 101
терминалов 338
удаленного управления Windows (WS-Management) 171
удаленной установки 51
Снимок виртуальной машины 64
Соединение (подключение)
репликации 415
Соединение с виртуальной частной сетью 333
Сон 98
Состояния системы (System State) 275
Сохраненные запросы 401
описание 403
Средства поиска 116
Ссылки (файловой системы)
удаление 114
Стандартные разрешения 215
Схема:
модификация 429
обновление 374
Схемы электропитания 93
Счетчики производительности 177

Т

Таблица разделов 192
Том (дисковый) 195
RAID-5 195
зеркальный 195
простой 195
составной 195
чередующийся 195
Топология репликации 415
Точки повторной обработки (junction points) 114

У

Удаленный доступ 338
политики 342
Удаленный помощник 129
Удаленный рабочий стол 129
Управление данным сервером, утилита 100
Условная пересылка (DNS) 316, 321
Установка:
Windows Server 2008 26
компонентов Windows 101
приложений и компонентов Windows 100
системы 27
Учетная запись:
Гость (Guest) 239

Ф

Файл подкачки 87
Файлы ответов (answer files) 47
Фильтры:
в оснастке 405
Функциональный уровень 422

Ц

Центр загрузки Microsoft 465
Центр обновления Windows 41
Центр управления сетями и общим доступом (Network and Sharing Center) 237, 283, 284

Ч

Частная сеть 281

Ш

Шаблон групповых политик 442
Шифрование файлов 251
  для совместного использования 255
Шифрование файлов и папок 252
Шифрованная файловая система (EFS) 251

Э, Я

Экран приветствия 73
Электропитание 93
Энергосберегающие режимы 98
Языковый пакет (MUI) 92