Официальное учебное пособие для самоподготовки

MCSA/MCSE

Экзамен **70-290**

конкурс
«Читатель месяца»
см. последнюю страницу

Управление и поддержка Microsoft® Windows Server™ 2003

Дэн Холме
Орин Томас

Учебный курс

РУССКАЯ РЕДАКЦИЯ

Microsoft®

MCSA/MCSE

Trainining Kit

Exam70-290

Managing and Maintaining

a Microsoft*

Windows Server™ 2003 Environment

Dan Holme and Orin Thomas

***Microsoft** Press*

Учебный курс
MCSA/MCSE

Экзамен 70-290

Управление и поддержка

Microsoft*

Windows Server™ 2003

Дэн Холме, Орин Томас

Официальное пособие Microsoft
для самостоятельной подготовки

Москва 2004

РУССКАЯ РЕДАКЦИЯ

УДК 004
ББК 32.973.26-018.2
Х72

Холме Дэн, Томас Орин

Х72 Управление и поддержка Microsoft Windows Server 2003. Учебный курс MCSA/MCSE / Пер. с англ. — М. : Издательско-торговый дом «Русская Редакция», 2004. — **448** стр. : ил.

ISBN 5-7502-0201-1

Это официальное пособие Microsoft посвящено внедрению, управлению и поддержке среды Microsoft Windows Server 2003. Здесь рассмотрены все основные аспекты эксплуатации Windows Server 2003, включая установку ОС, управление учетными записями пользователей, групп и компьютеров, управление файлами, папками и принтерами, управление дисками и другими аппаратными устройствами, резервное копирование данных, контроль за работой ОС и методики восстановления ее работоспособности в случае сбоев.

Книга адресована всем, кто хочет научиться администрировать среду Microsoft Windows Server 2003, а также самостоятельно подготовиться к сдаче экзамена по программам сертификации MCSA (Microsoft Certified Systems Administrators) и MCSE (Microsoft Certified Systems Engineer) № 70-290: *Managing and Maintaining a Microsoft Windows Server 2003 Environment.*

Издание состоит из 13 глав и предметного указателя. На прилагаемом компакт-диске находятся демонстрационная версия теста, учебные материалы для подготовки к экзамену, приложение, словарь терминов и другие справочные материалы.

УДК 004
ББК 32.973.26-018.2

Подготовлено к изданию по лицензионному договору с Microsoft Corporation, Редмонд, Вашингтон, США.

ISBN 0-7356-1437-7 (англ.)
ISBN 5-7502-0201-1

Содержание

Об этой книге

Мы рады представить вам учебный курс, посвященный управлению и поддержке Microsoft Windows Server 2003. Структура этой книги разработана так, чтобы вы эффективно подготовились к сдаче экзамена и получили знания, необходимые для развертывания ОС в корпоративной сети. Надеемся, с нашей помощью вы без труда поймете суть базовых технологий Windows Server 2003, разберетесь в многочисленных параметрах настройки и сложностях взаимодействия разнообразных компонентов, так что легко сможете справиться с задачами, которые ставят перед вами современные информационные технологии. Кроме того, вы сможете подготовиться к сдаче экзамена № 70-290 по программе сертификации Microsoft Certified Professional.

Примечание Подробно о программе сертификации MCP — в разделе «Программа сертификации специалистов Microsoft».

Кому адресована эта книга

Данный курс предназначен администраторам компьютеров под управлением Microsoft Windows Server 2003, а также всем, кто хочет сдать сертификационный экзамен 70-290: *Managingand Maintaininga Microsoft Windows Server 2003 Environment*.

Примечание Конкретное содержание любого экзамена определяется компанией Microsoft и может быть изменено без предварительного уведомления.

Предварительные требования

Для изучения данного курса необходимо:

- иметь минимум 12—18 месяцев опыта администрирования Windows в сетевой среде;
- знать основные сведения о службе Active Directory и связанных технологиях, включая групповую политику.

Содержимое компакт-диска

На прилагаемом компакт-диске содержится ряд вспомогательных средств, которые помогут вам в изучении курса.

- **Примерные экзаменационные вопросы** в системе Microsoft Press Readiness Review Suite, поддерживающей разные режимы тестирования, позволят вам получить представление о сертификационном экзамене, а также выяснить, насколько полно вы усвоили материал этого курса.

- **Электронные книги.** На компакт-диске записана полная электронная версия этой книги на английском языке, книги *Microsoft Encyclopedia of Networking, Second Edition* и *Microsoft Encyclopedia of Security,* а также избранные главы из книг издательства Microsoft Press по Windows Server 2003.
- **Подготовка** к экзамену. Изучив материал этого раздела, вы познакомитесь с основными типами вопросов, которые могут встретиться на экзамене, а задания по программе экзамена и примерные вопросы помогут понять, какие темы усвоены недостаточно и нуждаются в повторении.

  Примечание Полный список экзаменов с программами курсов см. по адресу *http://www.microsoft.com/traincert/mcp.*

  Содержимое этого раздела упорядочено по темам экзамена. Каждая глава освещает важную группу тем, составляющую раздел программы, и содержит перечень проверяемых на экзамене навыков и список дополнительной литературы.
  Раздел объединяет логически связанные темы экзамена, по каждой из которых вам будут предложены примерные вопросы с указанием верных и неверных ответов с пояснениями.

  Примечание Эти вопросы входят в состав пробного экзамена, который также находится на прилагаемом компакт-диске.

- Приложение «Сервер терминалов».
- Словарь терминов.

Дополнительные сведения о данном курсе и прилагаемом компакт-диске (включая ответы на типичные вопросы об установке и использовании) см. на Web-узле технической поддержки издательства Microsoft Press по адресу *http://www.microsoft.com/mspress/support.* Вы также можете отправить письмо по адресу *tkinput@microsoft.com* или написать в издательство Microsoft Press обычным образом: Microsoft Press Technical Support, One Microsoft Way, Redmond, WA 98052-6399.

Структура книги

Для повышения эффективности обучения главы этой книги разбиты на разделы:

- каждая глава начинается с раздела «Темы экзамена», где перечисляются освещаемые в ней разделы программы экзамена, за ним идет раздел «В этой главе» с кратким обзором содержания главы; следующий раздел «Прежде всего» поможет подготовиться к изучению главы;
- главы делятся на занятия, посвященные отдельным темам. Каждое занятие включает теоретическую часть и лабораторную работу, которая позволит вам закрепить полученные знания и поэкспериментировать с приложениями, о которых шла речь;
- занятия завершаются разделами «Закрепление материала». Вопросы этого раздела помогут проверить, насколько твердо вы усвоили материал. Ответы на вопросы приводятся в конце главы;
- в разделах «Пример из практики» и «Практикум по устранению неполадок» в конце главы вам будет предложено проанализировать реальную ситуацию и найти способ устранения тех или иных неполадок, чтобы научиться решать проблемы, возникающие в реальных сетях;

- каждое занятие завершается разделом «Резюме», где подводятся краткие итоги занятия, а каждая глава — разделом «Резюме главы», в нем формулируются основные выводы с указанием основных терминов и понятий, необходимых для сдачи экзамена.

Примечания

В книге встречаются различные виды примечаний.

- **Совет** — подсказывает более быстрый или нетривиальный способ решения задач, а также содержит полезный опыт других специалистов;
- **Внимание!** — содержит сведения, критические для выполнения поставленной задачи или предупреждение о возможной потере данных и повреждении системы.
- **Примечание** — содержит дополнительную информацию.
- **Подготовка к экзамену** — отмечает моменты, важные для подготовки к экзамену.
- **На заметку** — практический совет, как эффективно применить навыки, полученные на занятии.

Обозначения

- Названия элементов интерфейса Windows, с которыми вы работаете при помощи мыши или клавиатуры, набраны буквами **полужирного** начертания, первыми приводятся названия из русскоязычной версии Windows 2003 Server, а за ними в скобках — названия тех же элементов из англоязычной версии этой ОС; пример: кнопка **Пуск (Start).**
- *Курсив* в операторах указывает, что в этом месте следует подставить собственные значения; новые понятия и термины, а также названия служб и инструментов также напечатаны *курсивом*.

ш Имена файлов и каталогов начинаются с Прописных Букв (за исключением имен, которые вы задаете сами). Кроме особо оговоренных случаев, для ввода имен файлов и каталогов в диалоговых окнах или в командной строке можно использовать строчные буквы.

- Расширения имен файлов набраны строчными буквами.
- Аббревиатуры напечатаны ПРОПИСНЫМИ БУКВАМИ.
- Примеры кода, текста, выводимого на экран, а также вводимого в командной строке и различных полях выделены моноширинным шрифтом.
- В квадратные скобки, [ ], заключаются необязательные элементы. Например, наличие в синтаксисе команды элемента *[filename]* показывает, что здесь можно ввести имя файла. Сами скобки вводить не надо.
- В фигурные скобки, {}, заключаются обязательные элементы. Так, наличие в синтаксисе команды элемента *{filename}* показывает, что здесь необходимо ввести имя файла, сами скобки вводить не надо

Сочетания клавиш

- Знак «+» между названиями клавиш означает, что их следует нажать одновременно. Например, выражение «Нажмите Alt+Tab» обозначает, что, удерживая нажатой клавишу Alt, нужно нажать Tab.
- Запятая между названиями клавиш означает их последовательное нажатие. Например, выражение «Нажмите Alt, F, X» означает, что надо последовательно нажать и

отпустить указанные клавиши. Если же указано «Нажмите Alt+W, L», то сначала следует нажать клавиши Alt и W вместе, потом отпустить их и нажать клавишу L.

Начало работы

Учебный курс содержит упражнения, которые помогут вам научиться внедрять, поддерживать и устранять неполадки Windows Server 2003. Используйте этот раздел для подготовки своей учебной среды. Большинство упражнений можно выполнить на одном тестовом компьютере в лабораторной среде. Для нескольких необязательных приложений необходим второй компьютер под управлением Microsoft Windows XP, который должен быть подключен к сети с вашим тестовым сервером.

Примечание Упражнения, равно как и изменения на тестовом компьютере, могут иметь нежелательные последствия, если вы подключены к более крупной сети. Перед выполнением проконсультируйтесь с администратором вашей сети.

Аппаратное обеспечение

Тестовый компьютер должен соответствовать приведенной ниже минимальной конфигурации. Желательно, чтобы все аппаратное обеспечение соответствовало списку устройств, совместимых с Microsoft Windows Server 2003; см. *список совместимых устройств* (Hardware Compatibility List, HCL) по адресу *http://www.microsoft.com/windowsserver2003/evaluation/sysreqs/default.mspx*.

- Процессор с частотой минимум 133 МГц для компьютеров на базе процессоров x86 (рекомендуется 733 МГц) и 733 МГц для компьютеров на базе процессоров Itanium.
- Не менее 128 Мб оперативной памяти (рекомендуется 256).
- 1,5 Гб свободного пространства на жетском диске для компьютеров на базе процессоров x86 и 2,0 Гб для компьютеров на базе процессоров Itanium.
- Монитор, с разрешением 800x600 или выше.
- Привод CD-ROM или DVD-ROM.
- Мышь Microsoft или другое совместимое устройство.

Программное обеспечение

Для выполнения упражнений вам потребуется следующее ПО.

- Windows Server 2003 Enterprise Edition.
- Windows XP Professional (для нескольких необязательных практикумов).

Подготовка компьютера к выполнению практических занятий

Настройте компьютер согласно инструкциям изготовителя. Сервер сконфигурируйте следующим образом:

- Windows Server 2003 Enterprise Edition;
- имя компьютера: ServerOl;
- контроллер в домене *contoso.com;*
- 1 Гб нераспределенного места на диске.

Если вы можете самостоятельно установить Windows Server 2003, сконфигурируйте сервер, следуя приведенным выше рекомендациям. В противном случае используйте инструкции по установке, приведенные в главе 1.

Второй компьютер будет исполнять роль клиента Windows XP в ряде необязательных практических упражнений курса.

Внимание! Если ваш компьютер подключен к большой сети, *непременно* согласуйте с ее администратором имя компьютера, домена и другие параметры, чтобы избежать конфликтов с настройками сети. Если конфликт все же произошел, попросите администратора предоставить другие значения параметров, которые следует использовать в дальнейшем.

Вопросы пробного экзамена

На компакт-диске находится пробный экзамен из 300 вопросов, а также 125 дополнительных вопросов для повторения основных тем. Используйте их, чтобы закрепить материал и выявить темы, которые желательно повторить.

Чтобы установить на жесткий диск вопросы пробного экзамена, выполните следующие действия.

1. Вставьте прилагаемый компакт-диск в привод CD-ROM.

   Примечание Если на вашем компьютере отключена функция автозапуска, следуйте указаниям из файла Readme.txt на компакт-диске.

2. В открывшемся меню щелкните Readiness Review Suite и следуйте указаниям программы

Электронные книги

На прилагаемом компакт-диске вы найде электронную версию этой книги на английском языке, а также *Microsoft Encyclopedia of Security* и *Microsoft Encyclopedia of Networking, Second Edition* в формате PDF, для просмотра электронных книг пользуйтесь программой Adobe Acrobat Reader.

Чтобы установить электронные книги, сделайте следующее.

1. Вставьте прилагаемый компакт-диск в привод CD-ROM.

   Примечание Если на вашем компьютере отключена функция автозапуска, следуйте указаниям из файла Readme.txt на компакт-диске.

2. В открывшемся меню щелкните IVaining Kit eBook и следуйте указаниям программы, аналогично можно установить или просмотреть другие электронные книги, имеющиеся на компакт-диске.

Программа сертификации специалистов Microsoft

Программа сертификации специалистов Microsoft (Microsoft Certified Professional, MCP) — отличная возможность подтвердить ваше знание современных технологий и программных продуктов этой фирмы. Лидер отрасли в области сертификации, Microsoft разработала современные методы тестирования. Экзамены и программы сертификации подтвердят вашу квалификацию разработчика или специалиста по реализации решений на основе технологий и программных продуктов Microsoft. Сертифицированные Microsoft профессионалы квалифицируются как эксперты и высоко ценятся на рынке труда.

Примечание Полный список преимуществ сертифицированных специалистов см. по адресу *http://www.microsoft.com/traincert/start/itpro.asp*.

Типы сертификации

Программа сертификации специалистов предлагает несколько типов сертификации по разным специальностям.

- *Сертифицированный специалист Microsoft (Microsoft Certifted Professional, MCP)* — предполагает доскональное знание, по крайней мере, одной ОС из семейства Windows или ключевой платформы Microsoft. Такой специалист обладает навыками внедрения продукта или технологии Microsoft как части бизнес-системы предприятия.
- *Сертифицированный разработчик программных решений Microsoft (Microsoft Certifted Solution Developer, MCSD)* — проектирование и разработка решений для бизнеса с использованием средств разработки, платформ и технологий корпорации Microsoft, включая Microsoft .NET Framework.
- *Сертифицированный разработчик приложений Microsoft (Microsoft Certified Application Developer, MCAD) для платформы Microsoft .NET* — способен создавать, тестировать, развертывать и поддерживать мощные приложения с использованием средств и технологий от Microsoft , включая Visual Studio .NET и Web-сервисы XML.
- *Сертифицированный системный инженер Microsoft (Microsoft Certified System Engineer, MCSE) на Windows 2000* — предполагает умение эффективно анализировать потребности компаний, а также проектировать и реализовать инфраструктуры для бизнес-решений на базе Windows Server 2003 и других ОС корпорации Microsoft.
- *Сертифицированный системный администратор Microsoft (Microsoft Certifted System Administrator, MCSA)* — занимается вопросами управления и устранения неполадок в существующих сетях и системах на основе Windows Server 2003 и других версий Windows.
- *Сертифицированный администратор баз данных Microsoft (Microsoft Certified Database Administrator, MCDBA)* — разработка, реализация и администрирование БД Microsoft SQL Server.
- *Сертифицированный преподаватель Microsoft (Microsoft Certifted Trainer, MCT)* — теоретическая и практическая подготовка для ведения соответствующих курсов с использованием учебных материалов Microsoft Official Curriculum (MOC) в *сертифицированных центрах технического обучения Microsoft* (Microsoft Certified Technical Education Centers, CTECs).

Требования к соискателям

Требования к соискателям определяются специализацией, а также служебными функциями и задачами.

Соискатель сертификата Microsoft должен сдать экзамен, подтверждающий его глубокие знания в области программных продуктов Microsoft. Экзаменационные вопросы, подготовленные с участием ведущих специалистов компьютерной отрасли, отражают реалии применения программных продуктов Microsoft.

- На звание *Сертифицированного специалиста Microsoft* сдают экзамен по работе с одной из операционных систем. Кандидат может сдать дополнительные экзамены, которые подтвердят его право на работу с другими продуктами, инструментальными средствами или прикладными программами Microsoft.

- На звание *Сертифицированного разработчика программных решений на основе Microsoft* сдают три ключевых экзамена и один по выбору (соискатели сертификата MCSD для Microsoft .NET сдают четыре ключевых экзамена и один по выбору).
- На звание *Сертифицированного разработчика приложений* сдают два ключевых экзамена и один по выбору.
- На звание *Сертифицированного системного инженера Microsoft* сдают семь экзаменов: пять ключевых и два по выбору.
- На звание *Сертифицированного системного администратора Microsoft* сдают три ключевых экзамена и один по выбору.
- На звание *Сертифицированного администратора баз данных Microsoft* сдают три ключевых экзамена и один по выбору.
- На звание *Сертифицированного преподавателя Microsoft* надо подтвердить свою теоретическую и практическую подготовку для ведения соответствующих курсов в авторизованных учебных центрах Microsoft. Участие в программе требует соответствия требованиям, предъявляемым при ежегодном обновлении статуса сертифицированного преподавателя. Более подробные сведения о сертификации по этой программе можно получить на сайте *http://www.microsoft.com/traincert/mcp/mct* или в местном отделении компании Microsoft.

Техническая поддержка

Мы постарались сделать все от нас зависящее, чтобы и учебный курс, и прилагаемый к нему компакт-диск не содержали ошибок. Издательство Microsoft Press публикует постоянно обновляемый список исправлений и дополнений к своим книгам по адресу *http://mspress.microsoft.com/support*.

Если все же у вас возникнут вопросы или вы захотите поделиться своими предложениями или комментариями, обращайтесь в издательство Microsoft Press по одному из указанных ниже адресов:

Электронная почта:
TKINPUT@MICROSOFT.COM
Почтовый адрес:
Microsoft Press
Attn: *MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment,* Editor
One Microsoft Way
Redmond, WA 98052-6399

Дополнительные сведения о данном курсе и прилагаемом компакт-диске (включая ответы на типичные вопросы об установке и использовании) см. на Web-узле технической поддержки издательства Microsoft Press по адресу *http://www.microsoft.com/mspress/support*. Самостоятельно найти ответы на свои вопросы можно в базе знаний Microsoft Press Knowledge Base на сайте *http://www.microsoft.com/mspress/support/search.asp*. Консультацию по вопросам, связанных с поддержкой программных продуктов Microsoft, можно получить по адресу *http://support.microsoft.com*.

ГЛАВА 1

Знакомство с Microsoft Windows Server 2003

В этой главе

В данной главе вы познакомитесь с различными редакциями Windows Server 2003 и сможете выбрать оптимальный вариант для своей организации. Затем вы научитесь устанавливать Microsoft Windows Server 2003 и настраивать компьютер — контроллер домена Active Directory.

Прежде всего

Здесь описан процесс настройки компьютера под управлением Windows Server 2003 для выполнения практических упражнений. Компьютер должен быть оснащен минимум одним жестким диском, который можно очистить и использовать для установки Windows Server 2003.

Занятие 1. Семейство Windows Server 2003

Windows Server 2003 безусловно является наиболее безопасной, надежной, отказоустойчивой и удобной в управлении ОС из всех предыдущих версий Windows. В этом занятии приведены краткие сведения о семействе Windows Server 2003 и показаны различия между редакциями.

Изучив материал этого занятия, вы сможете:

- ✓ описать основные различия редакций Windows Server 2003.

Продолжительность занятия — около 5 минут.

Редакции Windows Server 2003

Если у вас уже есть опыт работы с серверами Windows 2000, переход на Windows Server 2003 будет относительно прост, поскольку она является следующим шагом в обновлении платформы и технологий Windows 2000.

Обширный список новых функций вы сможете найти во множестве книг по новым системам. На самом деле список изменений Windows Server 2003 по сравнению с предыдущей версией достаточно велик, и в нем есть функции, которые заинтересуют практически каждого администратора.

Вас могут привлечь значительные улучшения и новые функции Active Directory, новые средства, поддерживающие популярные, но сложные объекты групповой политики (ОГП), улучшения корпоративной защиты, усовершенствования *Служб терминалов* (Terminal Services) и ряд других расширенных возможностей новой ОС. Если вы собираетесь перейти на Windows Server 2003, посетите Web-узел Microsoft http://www.microsoft.com/windowsserver2003 и решите, какие нововведения действительно важны для вашей среды.

Помимо обширного списка новых возможностей, Windows Server 2003 интересна еще и потому, что предлагается в 32-разрядном, 64-разрядном и *встроенном* (embedded) вариантах. Тем не менее, наиболее важные отличия касаются четырех редакций ОС, которые перечислены ниже в порядке функциональности и, соответственно, цены:

- Windows Server 2003 Web Edition;
- Windows Server 2003 Standard Edition;
- Windows Server 2003 Enterprise Edition;
- Windows Server 2003 Datacenter Edition.

Редакция Web Edition

Чтобы Windows Server 2003 могла конкурировать с другими Web-серверами, Microsoft выпустила усеченную, но вполне функциональную редакцию специально для Web-служб. Набор функций и лицензирование упрощают развертывание Web-страниц, Web-узлов, Web-приложений и Web-служб.

Windows Server 2003 Web Edition поддерживает 2 Гб ОЗУ и *двухпроцессорную симметричную обработку* (symmetric multiprocessor, SMP). Эта редакция поддерживает неограниченное количество анонимных Web-соединений, но только 10 входящих соединений *блока серверных сообщений* (server message block, SMB), и этого более чем достаточно для публикации содержимого. Такой сервер не может выступать в роли интернет-шлюза, DHCP- или факс-сервера. Несмотря на возможность удаленного управления сервером с помощью ПО Remote Desktop, он не может играть роль сервера терминалов в традиционном понимании: он может принадлежать домену, но не может быть его контроллером. Прилагаемая версия Microsoft SQL Server Database Engine поддерживает до 25 параллельных соединений.

Редакция Standard Edition

Данная редакция — надежный, многофункциональный сервер, предоставляющий службы каталогов, файлов, печати, приложений, мультимедийные и Web-службы для небольших и средних предприятий. Обширный (по сравнению с Windows 2000) набор функций дополнен рядом компонентов: MSDE (Microsoft SQL Server Database Engine) — версией сервера SQL Server, поддерживающего пять параллельных соединений к БД размером до 2 Гб; бесплатной преднастроенной службой POP3 (Post Office Protocol v3), которая

совместно со службой SMTP (Simple Mail Transfer Protocol) позволяет узлу играть роль небольшого автономного почтового сервера; полезным инструментом NLB (Network Load Balancing), который присутствовал только в Windows 2000 Advanced Server.

Редакция Standard Edition поддерживает до 4 Гб ОЗУ и четырехпроцессорную SMP-обработку.

Примечание В рамках выпуска Release Candidate (RC) 1 операционной системы Windows Server 2003 бета-версии поддерживали только два процессора. Это ограничение было снято в выпуске RC2, так что редакция Standard Edition поддерживает четыре процессора. Документация и другие ресурсы, созданные до выхода окончательной версии, могут содержать недостоверную информацию о поддержке SMP.

Редакция Enterprise Edition

Windows Server 2003 Enterprise Edition нацелена стать мощной серверной платформой для средних и крупных предприятий. К ее корпоративным функциям относятся поддержка восьми процессоров, 32 Гб ОЗУ, восьмиузловая кластеризация [включая кластеризацию на основе *сетей хранения данных* (Storage Area Network, SAN) и территориально распределенную кластеризацию], плюс совместимость с 64-разрядными компьютерами на базе Intel Itanium, что позволяет поддерживать уже 64 Гб ОЗУ и восьмипроцессорную SMP-обработку.

Ниже перечислены другие отличия Enterprise Edition от Standard Edition:

- поддержка служб MMS (Microsoft Metadirectory Services), позволяющих объединять каталоги, БД и файлы со службой каталогов Active Directory;
- *«горячее» добавление памяти* (Hot Add Memory) — вы можете добавлять память в поддерживаемые аппаратные системы без выключения или перезагрузки;
- *диспетчер системных ресурсов Windows* (Windows System Resource Manager, WSRM), поддерживающий распределение ресурсов процессора и памяти между отдельными приложениями.

Редакция Datacenter Edition

Редакция Datacenter Edition доступна только в качестве OEM-версии, предлагаемой в комплекте с серверами класса high-end, и поддерживает практически неограниченную масштабируемость: для 32-разрядных платформ — 32-процессорная SMP-обработка и 64 Гб ОЗУ, для 64-разрядных — 64-процессорная SMP-обработка и 512 Гб ОЗУ. Существует также версия, поддерживающая 128-процессорную SMP-обработку на базе двух 64-процессорных секций.

64-разрядные редакции

По сравнению с 32-разрядными, 64-разрядные редакции Windows Server 2003, работающие на компьютерах Intel Itanium, эффективнее используют скорость процессора и быстрее выполняют операции с плавающей точкой. Улучшения в коде и обработке существенно ускорили вычислительные операции. Возросшая скорость доступа к огромному адресному пространству памяти позволяет улучшить работу сложных, требовательных к ресурсам приложений, например приложений для работы с большими БД, научно-исследовательских приложений и подверженных высоким нагрузкам Web-серверов.

Однако некоторые функции в 64-разрядных редакциях недоступны. Например, 64-разрядные редакции не поддерживают 16-разрядные Windows-приложения, приложения реального режима, приложения POSIX и службы печати для клиентов Apple Macintosh.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Вы планируете развернуть компьютеры под управлением Windows Server 2003 в отделе из 250 служащих. Сервер будет хранить домашние каталоги, общие папки и обслуживать несколько принтеров. Какая редакция Windows Server 2003 является наиболее выгодным решением?
2. Вы собираетесь развернуть компьютеры под управлением Windows Server 2003 для нового домена Active Directory в крупной корпорации, содержащей несколько отдельных доменов Active Directory, каждый из которых обслуживается дочерними компаниями корпорации. Компания приняла решение использовать Exchange Server 2003 в качестве единой платформы для обмена сообщениями между дочерними предприятиями и планирует использовать службу MMS (Microsoft Metadirectory Services) для синхронизации соответствующих свойств объектов по всей организации. Какая редакция Windows Server 2003 является наиболее выгодным решением?
3. Вы размещаете серверы, чтобы предоставить доступ к приложениям электронной коммерции вашей компании через Интернет, и решили использовать четыре сервера под клиентские Web-приложения и один — для надежной и активной БД SQL. Какие редакции Windows Server 2003 будут наиболее выгодным решением?

Резюме

- Существуют 64- и 32-разрядная версии Windows Server 2003.
- Основные различия между версиями Windows Server 2003 заключены в редакциях Web Edition, Standard Edition, Enterprise Edition и Datacenter Edition, каждая из которых поддерживает набор характерных функций.
- В целом Windows Server 2003 является обновлением Windows 2000. Но при этом значительно улучшены функциональность и безопасность, и вы, вероятно, обнаружите, что некоторые усовершенствования просто необходимы для вашей среды.

Занятие 2. Установка и настройка Windows Server 2003 и Active Directory

В вопросах экзамена мало внимания уделяется самой службе каталогов Active Directory, однако некоторые из них касаются управления объектами Active Directory: пользователями, группами, компьютерами, принтерами и общими папками. В последующих главах подробно обсуждаются вопросы экзамена, а практические упражнения станут важным компонентом приобретения навыков работы с системой. Для выполнения этих упражнений понадобится настроенный контроллер домена под управлением Windows Server 2003. Если вы умеете настраивать контроллер домена и создавать основные учетные записи пользователей, групп и компьютеров, можете пропустить это занятие. Если

же вы не очень хорошо знакомы со службой каталогов Active Directory, то здесь вы найдете необходимые базовые сведения для дальнейшего изучения Windows Server 2003.

Изучив материал этого занятия, вы сможете:

- ✓ установить Windows Server 2003;
- ✓ описать ключевые структуры и концепции Active Directory;
- ✓ создать контроллер домена;
- ✓ создать объекты Active Directory, включая пользователей, группы и организационные подразделения (ОП).

Продолжительность занятия — около 60 минут.

Установка и настройка Windows Server 2003

Как администратор, вы, несомненно, потратили много времени на установку платформ Windows. Ниже перечислены важные особенности, которые следует учитывать при установке Windows Server 2003.

- **Установка с загрузочного компакт-диска.** Windows Server 2003 продолжает традицию установки с компакт-диска. Однако есть и нововведение: установка с дискет больше не поддерживается.
- **Улучшенный графический пользовательский интерфейс во время установки.** Во время установки Windows Server 2003 использует графический пользовательский интерфейс (GUI), похожий на интерфейс Windows XP. Он более точно описывает текущее со-, стояние установки и время, оставшееся до ее завершения.
- **Активация продукта.** Розничная и пробная версии Windows Server 2003 требуют активации. Такие массовые программы лицензирования, как Open License, Select License или Enterprise Agreement не требуют активации.

Характерные этапы установки Windows Server 2003 описаны в упражнении 1.

После установки и активации W/ndows можно настроить сервер, используя хорошо продуманную страницу **Управление данным сервером (Manage Your Server)** (рис. 1-1), которая автоматически открывается при входе в систему. Эта страница упрощает установку некоторых служб, инструментов и конфигураций в зависимости от роли сервера. Щелкните кнопку **Добавить или удалить роль (Add Or Remove A Role),** появится окно *Мастера настройки сервера* (Configure Your Server Wizard).

Если установить переключатель **Типовая настройка для первого сервера (Typical Configuration For A First Server),** мастер сделает сервер контроллером нового домена, установит службы Active Directory и при необходимости службы DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol) и RRAS (Routing And Remote Access).

Если установить переключатель **Особая конфигурация (Custom Configuration),** мастер может настроить следующие роли.

- **Файловый сервер (File Server).** Обеспечивает централизованный доступ к файлам и каталогам для пользователей, отделов и организации в целом. Выбор этого варианта позволяет управлять пользовательским дисковым пространством путем включения и настройки средств управления дисковыми квотами и ускорить поиск в файловой системе за счет активизации *Службы индексирования* (Indexing Service).

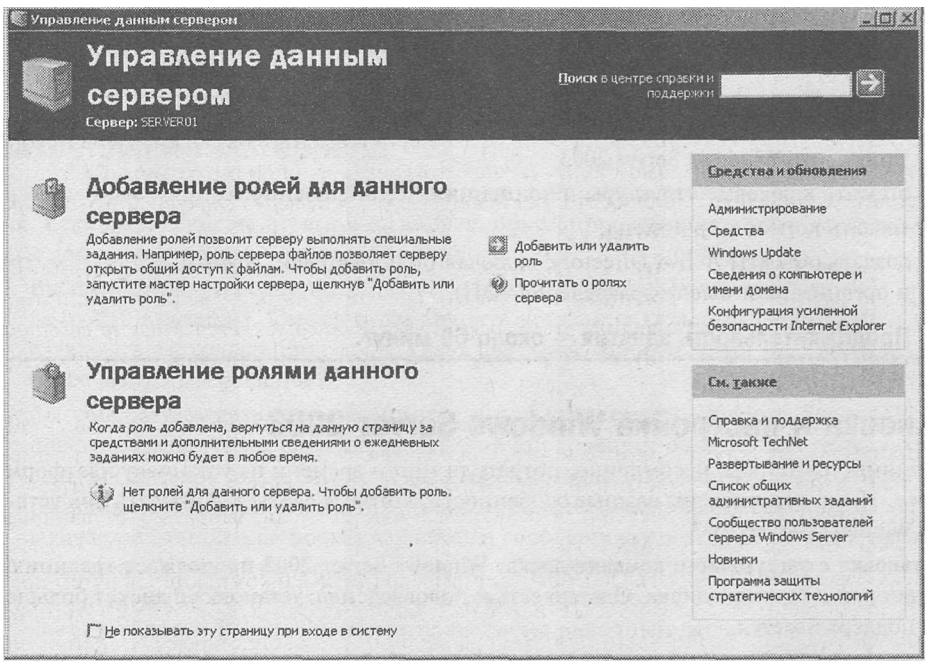


Рис. 1-1. Страница *Управление данным сервером*

- **Сервер печати (Print Server).** Обеспечивает централизованное управление печатающими устройствами, предоставляя клиентским компьютерам доступ к общим принтерам и их драйверам. Если выбрать этот вариант, запустится *Мастер установки принтеров* (Add Printer), позволяющий установить принтеры и соответствующие драйверы. Кроме того, мастер устанавливает службы IIS 6.0 (Internet Information Services), настраивает протокол печати IPP (Internet Printing Protocol) и Web-средства управления принтерами.
- **Application Server IIS, ASP.NET (Сервер приложений IIS, ASP.NET).** Предоставляет компоненты инфраструктуры, которые требуются для поддержки размещения Web-приложений. Эта роль устанавливает и настраивает IIS 6.0, ASP.NET и COM+.
- **Mail Server POP3, SMTP (Почтовый сервер POP3, SMTP).** Устанавливает POP3 и SMTP, чтобы сервер мог выступать в роли почтового сервера для клиентов POP3.
- **Сервер терминалов (Terminal Server).** Позволяет множеству пользователей с помощью клиенского ПО *Службы терминалов* (Terminal Services) или *Дистанционное управление рабочим столом* (Remote Desktop) подключаться к приложениям и ресурсам сервера, например принтерам или дисковому пространству, как если бы эти ресурсы были установлены на их компьютерах. В отличие от Windows 2000, Windows Server 2003 предоставляет *Дистанционное управление рабочим столом* автоматически. Роли сервера терминалов требуются, только когда нужно размещать приложения для пользователей на сервере терминалов.
- **Сервер удаленного доступа или VPN-сервер (Remote Access/VPN Server).** Обеспечивает маршрутизацию по нескольким протоколам и службы удаленного доступа для коммутируемых, локальных (LAN) и глобальных (WAN) вычислительных сетей. *Виртуальная частная сеть* (virtual private network, VPN) обеспечивает безопасное соединение пользователя с удаленными узлами через стандартные интернет-соединения.

- **Контроллер домена Active Directory (Domain Controller Active Directory).** Предоставляет службы каталогов клиентам сети. Этот вариант позволяет создать контроллер нового или существующего домена и установить DNS. Если выбрать эту роль, запускается *Мастер установки Active Directory* (Active Directory Installation Wizard).
- **DNS Server (DNS-сервер).** Обеспечивает разрешение имен узлов: DNS-имена преобразуются в IP-адреса (прямой поиск) и обратно (обратный поиск). Если выбрать этот вариант, устанавливается служба DNS и запускается *Мастер настройки DNS-сереера* (Configure A DNS Server Wizard).
- **DHCP-сервер (DHCP Server).** Предоставляет службы автоматического выделения IP-адресов клиентам, настроенным на динамическое получение IP-адресов. Если выбрать этот вариант, устанавливаются службы DHCP и запускается *Мастер создания области* (New Scope Wizard), позволяющий определить один или несколько диапазонов IP-адресов в сети.
- **Сервер потоков мультимедиа (Streaming Media Server).** Предоставляет службы WMS (Windows Media Services), которые позволяют серверу передавать потоки мультимедийных данных в интрасети или через Интернет. Содержимое может храниться и предоставляться по запросу или в реальном времени. Если выбрать этот вариант, устанавливается сервер WMS.
- **WINS-сервер (WINS Server).** Обеспечивает разрешение имен компьютеров путем преобразования имен NetBIOS в IP-адреса. Устанавливать службу WINS (Windows Internet Name Service) не требуется, если вы не поддерживаете старые ОС, например Windows 95 или NT. Такие ОС, как Windows 2000 и XP не требуют WINS, хотя старым приложениям, работающим на этих платформах, может понадобиться разрешать имена NetBIOS. Если выбрать этот вариант, устанавливается сервер WINS.

Для выполнения практических упражнений этой главы присвойте компьютеру имя ServerOl и сделайте его контроллером домена contoso.com. Настройка контроллера домена с помощью *Мастера настройки сервера* (Configure Your Server Wizard) описана в упражнении 2.

Служба каталогов Active Directory

Проектированию, внедрению и поддержке Active Directory посвящено много книг. Если у вас есть опыт работы с этой службой каталогов, вы поймете, что следующий материал максимально упрощен, поскольку подробное описание заняло бы не одну книгу. Цель этого раздела — выделить сведения, необходимые для сдачи экзамена.

Сети, службы каталогов и контроллеры доменов

Сети были созданы в один прекрасный день, когда пользователю надоело бегать по коридору, чтобы обмениваться данными с другим пользователем. В конце концов, цель любой сети — обеспечить удаленный доступ к ресурсам. Когда-то это были файлы, папки и принтеры. Со временем к ним добавились другие ресурсы, наиболее важными из которых являются электронная почта, базы данных и приложения. Потребовался механизм, позволяющий отслеживать ресурсы и предоставляющий как минимум каталог пользователей и групп, чтобы предотвратить нежелательный доступ к ресурсам.

Сети Microsoft Windows поддерживают две модели служб каталогов: *рабочую группу* (workgroup) и *домен* (domain). Для организаций, внедряющих Windows Server 2003, модель домена наиболее предпочтительна. Модель домена характеризуется единым каталогом ресурсов предприятия — Active Directory, — которому доверяют все системы безопасности, принадлежащие домену. Поэтому такие системы способны работать с

субъектами безопасности (учетными записями пользователей, групп и компьютеров) в каталоге, чтобы обеспечить защиту ресурсов. Служба Active Directory, таким образом, играет роль идентификационного хранилища и сообщает «кто есть кто» в этом домене.

Впрочем, Active Directory — не просто база данных. Это коллекция файлов, включая журналы транзакций и системный том (Sysvol), содержащий сценарии входа в систему и сведения о групповой политике. Это службы, поддерживающие и использующие БД, включая протокол LDAP (Lightweight Directory Access Protocol), протокол безопасности Kerberos, процессы репликации и службу FRS (File Replication Service). БД и ее службы устанавливаются на один или несколько контроллеров домена. Контроллер домена назначается *Мастером установки Active Directory,* который можно запустить с помощью *Мастера настройки сервера* (как вы сделаете в упражнении 2) или командой DCPROMO из командной строки. После того как сервер становится контроллером домена, на нем хранится копия (реплика) Active Directory, и изменения БД на любом контроллере реплицируются на все остальные контроллеры домена.

Домены, деревья и леса

Active Directory не может существовать без домена и наоборот. Домен — это основная административная единица службы каталогов. Однако предприятие может включить в свой каталог Active Directory более одного домена. Когда несколько моделей доменов совместно используют непрерывное пространство имен DNS, они образуют логические структуры, называемые *деревьями* (tree). Например, домены contoso.com, us.contoso.com и europe.contoso.com совместно используют непрерывное пространство имен DNS и, следовательно, составляют дерево.

Домены Active Directory с разными корневыми доменами образуют несколько деревьев. Они объединяются в самую большую структуру Active Directory — *лес* (forest). Лес Active Directory содержит все домены в рамках службы каталогов. Лес может состоять из нескольких доменов в нескольких деревьях или только из одного домена. Когда доменов несколько, приобретает важность компонент Active Directory, называемый *глобальным каталогом* (global catalog): он предоставляет информацию об объектах, расположенных в других доменах леса.

Объекты и организационные подразделения

Ресурсы предприятия представлены в Active Directory в виде объектов или записей в БД. Каждый объект характеризуется рядом атрибутов или свойств. Например, у пользователя есть атрибуты имя пользователя и пароль, у группы — имя группы и список пользователей, которые в нее входят.

Для создания объекта в Active Directory откройте консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) в группе программ **Администрирование (Administrative Tools).** Раскройте домен, чтобы увидеть его контейнеры и организационные подразделения. Щелкните контейнер или ОП правой кнопкой и в контекстном меню выберите **Создать (New) тип_объекта.**

Служба Active Directory способна хранить миллионы объектов, включая пользователей, группы, компьютеры, принтеры, общие папки, сайты, связи сайтов, объекты групповой политики (ОГП) и даже зоны DNS и записи узлов. Можно представить, в какой кошмар превратился бы доступ к каталогу и его администрирование без определенной структуры.

Структура — цель введения характерного типа объекта, называемого *организационным подразделением* (organization unit, OU). ОП представляют собой контейнеры внутри домена, позволяющие группировать объекты, управляемые или настраиваемые одинаковым образом. Однако задача ОП — не только организовать объекты Active Directory, они обес-

печивают важные возможности управления, поскольку образуют точку, куда могут делегироваться функции управления и с которой можно связать групповые политики.

Делегирование управления

Делегирование прав управления основано на простой идее, что администраторы на местах должны иметь возможность сменить пароль для определенного подмножества пользователей. У каждого объекта в Active Directory (в нашем случае — у объектов пользователей) есть *таблица управления доступом*[1] (access control list, ACL), которая определяет разрешения доступа к этому объекту, аналогично тому, как файлы на томе жесткого диска обладают таблицей ACL, определяющей доступ к этим файлам. Например, ACL объекта пользователя будет определять, каким группам разрешено сбрасывать свой пароль. Было бы неправильно заставлять администратора изменять пароль каждого пользователя: проще поместить всех нужных пользователей в одно ОП и разрешить администратору менять в нем пароли. Это разрешение будет наследоваться всеми объектами пользователей в ОП, так что администратор сможет изменить разрешения для всех пользователей.

Сброс паролей пользователей — один из примеров делегирования административных полномочий. Существуют тысячи комбинаций разрешений, которые можно было бы назначить группам, отвечающим за администрирование и поддержку Active Directory. ОП позволяют предприятию создавать активное представление административной модели и указывать, кто и что может делать с объектами в домене.

Групповая политика

ОП также используются для объединения одинаково настроенных объектов — компьютеров и пользователей. Групповая политика Active Directory позволяет централизованно управлять практически любыми конфигурационными изменениями системы. С ее помощью можно указать настройки безопасности, развернуть ПО и настроить поведение ОС и приложений, даже не прикасаясь к компьютерам пользователей. Вы просто реализуете свою конфигурацию в рамках одного ОГП.

ОГП состоят из сотен возможных конфигурационных параметров: от прав и привилегий пользователя до ПО, которое разрешено запускать на системе. ОГП подключается к контейнеру внутри Active Directory (обычно к ОП, но может и к доменам или даже сайтам), и после этого его настройки распространяются на всех пользователей и компьютеры внутри этого контейнера.

На экзамене вам наверняка встретятся вопросы по групповой политике. Важно запомнить, что групповая политика — средство централизованной реализации конфигурации, что одни настройки применяются только к компьютерам, а другие — только к пользователям, и что политика распространяется только на компьютеры и пользователей из ОП, с которым она связана.

Дополнительные сведения

Как уже было сказано, служба каталогов Active Directory — это большая и сложная тема, заслуживающая глубокого изучения, если вы собираетесь использовать Windows Server 2003 в качестве контроллера домена. Рекомендуем прочитать следующие издания:

- Active Directory for Microsoft Windows Server 2003 Technical Reference;
- MCSE Self-Paced Training Kit (Exam 70-294): Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure[2].

[1] Или *список управления доступом*. — *Прим. ред.*

[2] Планирование, внедрение и поддержка Active Directory Microsoft Windows Server 2003. Учебный курс MCSE. Сеотификационный экзамен № 70-294. Планируется к выходу в конце 2004 г. — *Прим. ред.*

Лабораторная работа. **Установка Windows Server 2003**

На этой лабораторой работе вы настроите компьютер для работы под управлением Windows Server 2003. Затем вы сделаете сервер контроллером домена contoso.com.

Упражнение 1. Установка Windows Server 2003

Это упражнение следует выполнять на компьютере, совместимом с Windows Server 2003. Предполагается, что основной жесткий диск полностью чист. Если диск уже разбит на разделы, можно изменить упражнение согласно конфигурации вашей системы.

1. В BIOS компьютера или контроллера диска задайте загрузку с CD-ROM. Если вы не знаете, как это сделать, обратитесь к соответствующей документации.
2. Вставьте установочный компакт-диск Windows Server 2003 в привод CD-ROM и перезагрузите компьютер.
3. Если основной диск не пуст, появится сообщение с предложением нажать любую клавишу, чтобы загрузить компьютер с компакт-диска. Если вы увидите такое сообщение, нажмите любую клавишу.

   После загрузки компьютера ненадолго появится сообщение об анализе конфигурации системы, а затем откроется окно **Установка Windows (Windows Setup).**
4. Если компьютеру нужны специальные драйверы для запоминающих устройств, которых нет в комплекте Windows Server 2003, нажмите F6, когда появится соответствующее сообщение, и предоставьте соответствующие драйверы.
5. Система предложит нажать F2, чтобы выполнить *автоматическое аварийное восстановление системы* (Automated System Recovery, ASR). Это новая функция Windows Server 2003, пришедшая на смену функции *диск аварийного восстановления* (Emergency Repair Disk) в предыдущих версиях Windows (см. главу 13). Не нажимайте F2 на этом этапе. Установка продолжится.

   Заметьте: серый индикатор внизу экрана показывает, что выполняется проверка компьютера и загрузка файлов. Это необходимо для запуска ОС с минимальным набором драйверов.
6. Если вы устанавливаете пробную версию Windows Server 2003, откроется окно Setup Notification, прочитайте информацию и для продолжения нажмите клавишу Enter.

   Программа установки отобразит окно приветствия.

   Заметьте, что помимо установки Windows Server 2003 на чистый диск, программу Setup можно использовать для восстановления поврежденной системы Windows. *Консоль восстановления* (Recovery Console) обсуждается в главе 13.
7. Прочитайте информацию в окне **Вас приветствует программа установки (Welcome To Setup)** и для продолжения нажмите клавишу Enter. Появится окно **Лицензионное соглашение (License Agreement).**
8. Прочитайте лицензионное соглашение: для прокрутки текста вниз нажимайте клавишу Page Down.
9. Нажмите F8, чтобы принять условия соглашения.

   Откроется окно Windows Server 2003 Setup с предложением выбрать область свободного пространства или существующий раздел, куда будет установлена ОС. На данном этапе вы можете создать или удалить разделы на жестком диске.

   Для выполнения упражнений необходимо создать достаточно большой раздел, на котором поместится ОС (рекомендуется не менее 3 Гб), и минимум 1 Гб нераспределенного пространства. Дальнейшие действия предполагают, что размер вашего дис-

ка не менее 4 Гб и он в данный момент чист. Вы можете скорректировать процедуру по ситуации.

10. Нажмите клавишу С, чтобы создать раздел.
11. Чтобы создать раздел размером 3 Гб, в поле **Создать раздел размером (МБ) [Create Partition Of Size (In MB)]** введите 3072 и нажмите Enter.
12. Убедитесь, что ваш вариант разбивки диска аналогичен показанному на рис. 1-2. Напомним, что для выполнения практических упражнений рекомендуется использовать раздел С: размером не менее 3 Гб плюс 1 Гб нераспределенного пространства.

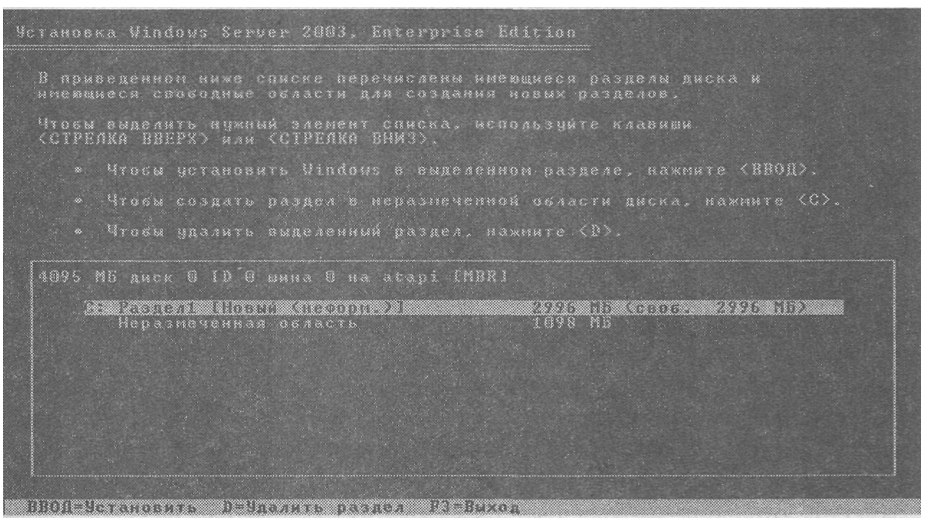


Рис. 1-2. Разбивка жесткого диска на разделы при установке

13. Выберите **С: Раздел1 [Новый (неформ.)] (C: Partitionl [New (Raw)])** и нажмите клавишу Enter.

    Вам будет предложено выбрать файловую систему для этого раздела.
14. Убедитесь, что установлен переключатель **Форматировать раздел в системе NTFS (Format The Partition Using The NTFS File System)** и нажмите Enter.

    Программа установки отформатирует раздел под NTFS, проверит жесткий диск **на** наличие физических ошибок, которые могут помешать установке, скопирует файлы **на** жесткий диск и начнет установку. Это займет несколько минут.

    После этого появится красная строка состояния, отсчитывающая назад 15 секунд до перезагрузки компьютера и перехода процесса установки в графический режим.
15. После завершения установки в текстовом режиме система перезагружается. Не нажимайте клавишу для загрузки с компакт-диска, если появится соответствующее **сообщение.**

    Windows Setup запустит графический пользовательский интерфейс, демонстрирующий на левой панели процесс установки. Вы увидите, что отмечены флажки **Сбор информации (Collecting Information), Динамическое обновление (Dynamic Update)** и **Подготовка к установке (Preparing Installation).** Сбор информации был завершен до перехода в графический режим, а динамическое обновление не применяется при запуске с компакт-диска. Теперь система готовится к установке и копирует файлы на жесткий диск.
16. На странице **Язык и региональные стандарты (Regional And Language Options)** выберите необходимые параметры и щелкните **Далее (Next).**

Совет Вы сможете изменить региональные параметры после установки ОС, используя элемент **Язык и региональные стандарты (Regional And Language Options)** из *Панели управления*.

Программа установки отобразит страницу **Настройка принадлежности программ (Personalize Your Software),** где вам будет предложено указать свое имя и название организации.

17. В поле **Имя (Name)** введите свое имя, а в поле **Организация (Organization)** — название организации, после чего щелкните **Далее** (Next).

    Откроется страница **Ключ продукта (Your Product Key).**

18. Введите ключ продукта, прилагаемый к установочному компакт-диску Windows Server 2003, и щелкните **Далее** (Next).

    Откроется диалоговое окно **Режимы лицензирования (Licensing Modes)** с предложением выбрать режим лицензирования.

19. Убедитесь, что в поле **«На сервер». Число одновременных подключений (Per Server Number Of Concurrent Connections)** указано 5, и щелкните **Далее** (Next).

Внимание! Такой вариант лицензирования и пять одновременных подключений — рекомендуемые значения для самостоятельного обучения. Вы должны вводить количество одновременных подключений согласно приобретенной лицензии. Также можно выбрать вариант **«На устройство или на пользователя» (Per Device Or Per User).**

Откроется страница **Имя компьютера и пароль администратора (Computer Name And Administrator Password).**

Заметьте, что программа установки предлагает имя компьютера на основе названия вашей организации. Если вы оставили это поле пустым, программа установки сгенерирует часть имени компьютера, используя ваше имя.

20. В поле **Имя компьютера (Computer Name)** введите ServerOl.

    Имя компьютера отображается заглавными буквами независимо от того, в каком регистре вы его вводите. В практических упражнениях всего курса будет упоминаться ServerOl.

Внимание! Если ваш компьютер подключен к сети, посоветуйтесь с сетевым администратором, прежде чем назначать имя.

21. В полях **Пароль администратора (Administrator Password)** и **Подтверждение пароля (Confirm Password)** введите сложный пароль для учетной записи *Администратор* (Administrator) (такой, который нельзя просто угадать). Запомните его, поскольку при выполнении большинства практических упражнений курса вы будете входить в систему под учетной записью *Администратор*.

Внимание! Если вы устанавливаете Windows Server 2003 вручную, то не сможете перейти к последующим шагам, пока не введете пароль администратора, удовлетворяющий требованиям сложности. Допускается ввести пустой пароль, хотя это крайне нежелательно.

Если на сервере установлен модем, откроется диалоговое окно **Сведения о модеме (Modem Dialing Information).**

22. Введите междугородний телефонный код вашей местности и щелкните **Далее (Next).** Откроется страница **Настройка времени и даты (Date And Time Settings).**
23. Введите точную дату, время и часовой пояс и щелкните **Далее (Next).**

Внимание! Работа служб Windows Server 2003 зависит от настроек даты и времени. Убедитесь, что дата и время заданы точно и указан правильный часовой пояс для вашей местности.

24. На странице **Сетевые параметры (Networking Settings)** выберите **Обычные параметры (Typical Settings)** и щелкните **Далее (Next).**
    Откроется страница **Рабочая группа или домен (Workgroup Or** Computer **Domain).**
25. Убедитесь, что выбран первый вариант, а имя группы — Workgroup, после чего щелкните **Далее** (Next).
    Программа Setup установит и настроит остальные компоненты ОС. После завершения установки компьютер автоматически перезагрузится, и откроется диалоговое окно **Операционная система Windows (Welcome To Windows).**
26. Нажмите Ctrl+Alt+Delete, чтобы инициировать вход в систему, и введите пароль, который вы задали для учетной записи *Администратор* (Administrator).

Примечание Некоторые редакции Windows Server 2003, в том числе пробная, поставляемая с данной книгой, требуют активации через Интернет или по телефону в течение 14 дней после установки. Лицензию на Windows Server 2003 не требуется активировать, если она приобретена в рамках одной из массовых программ лицензирования Microsoft.

27. Щелкните подсказку на системной панели, чтобы начать активацию Windows Server 2003. Следуйте инструкциям на экране.

Примечание Для активации через Интернет необходимо подсоединить ServerOl к сети и при необходимости указать нужный IP-адрес, маску подсети, шлюз по умолчанию и адрес DNS-сервера в настройках протокола TCP/IP для сетевой платы.

Упражнение 2. Настройка сервера

В этом упражнении вы сделаете сервер первым контроллером в домене Active Directory с именем contoso.com.

Примечание Описанный ниже процесс установки предполагает, что *Мастер установки Active Directory* запускается в изолированной сети. Если вы подключены к сети с другим контроллером домена, процесс установки будет отличаться, и вы можете либо изменить выбор согласно конфигурации вашей сети, либо отключиться от сети перед выполнением этого упражнения.

1. Откройте страницу **Управление данным сервером (Manage Your Server)** в группе программ **Администрирование (Administrative Tools).**
2. Щелкните **Добавить или удалить роль (Add Or Remove A Role).** Откроется окно *Мастер настройки сервера* (Configure Your Server Wizard).
3. Щелкните **Далее (Next),** мастер попытается определить сетевые параметры.

4. Щелкните **Типовая настройка для первого сервера (Typical Configuration For A First Server),** а затем **Далее (Next).**
5. **В** поле **Имя домена в Active Directory (Active Directory Domain Name)** введите contoso.com.
6. Убедитесь, что в поле **NetBIOS-имя домена (NetBIOS Domain Name)** указано CONTOSO, и щелкните Далее (Next).
7. Убедитесь, что окно **Сводка выбранных параметров (Summary Of Selections)** соответствует показанному на рис. 1-3, и щелкните **Далее (Next).**

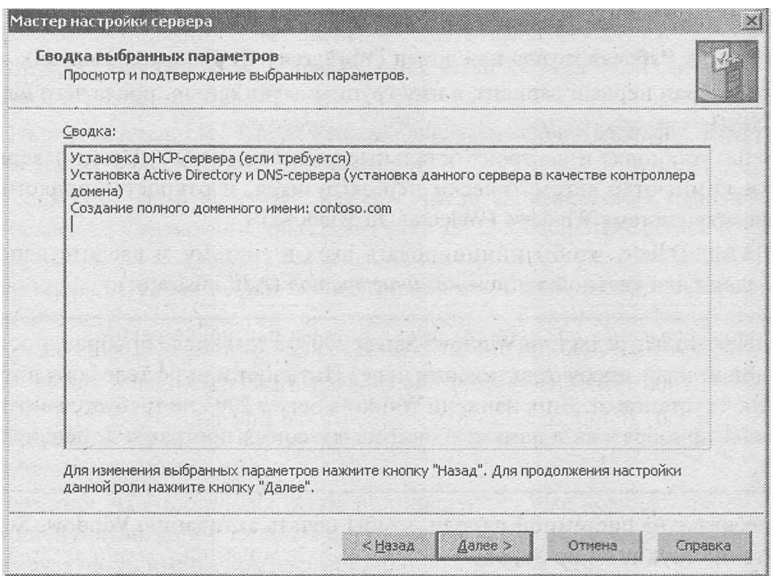


Рис. 1-3. Окно *Сводка выбранных параметров* мастера настройки сервера

8. Мастер напомнит, что система будет перезагружена, и попросит закрыть все открытые программы.
9. Щелкните **Да (Yes).**
10. После перезагрузки войдите в систему *как Администратор* (Administrator).
11. Мастер настройки сервера резюмирует установку (рис. 1-4).
12. Щелкните **Далее (Next),** а затем **Готово (Finish).**
13. Откройте консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers). Убедитесь, что домен contoso.com создан: раскройте его и найдите учетную запись компьютера для ServerOl в ОП Domain Controllers.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Какие из перечисленных версий Windows Server 2003 требуют активации? (Выберите все подходящие варианты.)
   a. Windows Server 2003 Standard Edition, розничная версия.
   b. Windows Server 2003 Enterprise Edition, пробная версия.

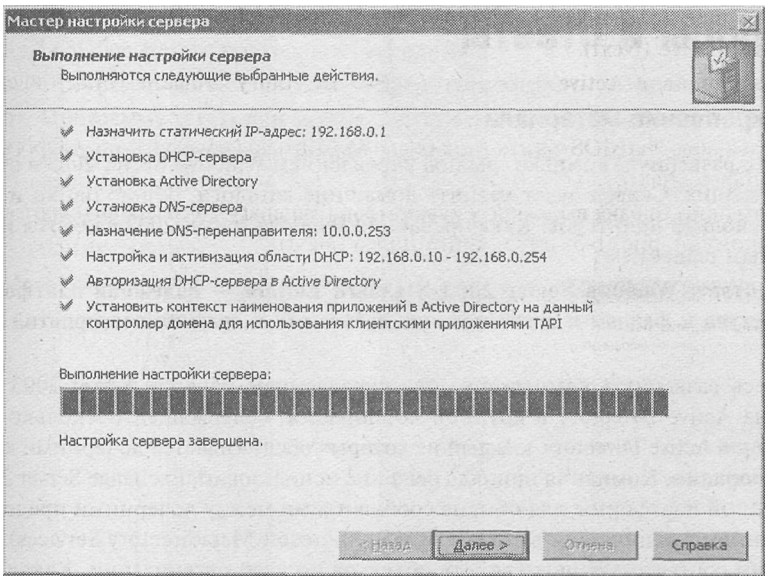


Рис. 1-4. Окно *Выполнение настройки сервера* мастера настройки сервера

c. Windows Server 2003 Enterprise Edition, версия Open License.
d. Windows Server 2003 Standard Edition, версия Volume License.

2. Чем отличаются домен, дерево и лес в Active Directory?
3. Какие из следующих утверждений о программе установки Windows Server 2003 верны? (Выберите все подходящие варианты.)
   a. Программу установки можно запустить, загрузив компьютер с компакт-диска.
   b. Программу установки можно запустить, загрузив компьютер с дискет.
   c. Программа установки просит ввести непустой пароль, удовлетворяющий требованиям сложности.
   d. Программа установки позволит ввести идентификатор продукта, состоящий из одних единиц.

Резюме

- Розничная и пробная версии Windows Server 2003 требуют активации.
- Страница **Управление данным сервером (Manage Your Server)** и *Мастер настройки сервера* (Configure Your Server Wizard) помогают установить и настроить дополнительные службы согласно предполагаемой роли сервера.
- Служба каталогов Active Directory устанавливается с помощью *Мастера установки Active Directory* (Active Directory Installation Wizard), который можно запустить с помощью *Мастера настройки сервера* (Configure Your Server Wizard) или исполнив DCPROMO из командной строки.

Вопросы и ответы

Занятие 1. Закрепление материала

1. **Вы** планируете развернуть компьютеры под управлением Windows Server 2003 в отделе из 250 служащих. Сервер будет хранить домашние каталоги, общие папки и обслуживать несколько принтеров. Какая редакция Windows Server 2003 является наиболее выгодным решением?

   Правильный ответ: Windows Server 2003 Standard Edition — надежная платформа для служб доступа к файлам и принтерам для небольших и средних предприятий или отделов.

2. Вы собираетесь развернуть компьютеры под управлением Windows Server 2003 для нового домена Active Directory в крупной корпорации, содержащей несколько отдельных доменов Active Directory, каждый из которых обслуживается дочерними компаниями корпорации. Компания приняла решение использовать Exchange Server 2003 в качестве единой платформы для обмена сообщениями между дочерними предприятиями и планирует использовать службу MMS (Microsoft Metadirectory Services) для синхронизации соответствующих свойств объектов по всей организации. Какая редакция Windows Server 2003 является наиболее выгодным решением?

   Правильный ответ: Windows Server 2003 Enterprise Edition — наиболее дешевое решение, поддерживающее MMS. Редакции Standard и Web не поддерживают MMS.

3. Вы размещаете серверы, чтобы предоставить доступ к приложениям электронной коммерции вашей компании через Интернет и решили использовать четыре сервера **под** клиентские Web-приложения и один — для надежной и активной БД SQL. Какие редакции Windows Server 2003 будут наиболее выгодным решением?

   Правильный ответ: Windows Server 2003 Web Edition — наиболее дешевая платформа для этих четырех серверов интернет-приложений, однако она не поддерживает такие корпоративные приложения, как SQL Server; версия MSDE из состава Web Edition допускает только 25 одновременных подключений. Таким образом, наиболее выгодное решение — Windows Server 2003 Standard Edition.

Занятие 2. Закрепление материала

1. Какие из перечисленных версий Windows Server 2003 требуют активации? (Выберите все подходящие варианты.)
   a. Windows Server 2003 Standard Edition, розничная версия.
   b. Windows Server 2003 Enterprise Edition, пробная версия.
   c. Windows Server 2003 Enterprise Edition, версия Open License.
   d. Windows Server 2003 Standard Edition, версия Volume License.

   Правильный ответ: a, b.

2. Чем отличаются домен, дерево и лес в Active Directory?

   Правильный ответ: домен — это основная административная единица Active Directory. Лес определяет границы действия Active Directory и должен содержать как минимум один домен. Домены, совместно использующие непрерывное пространство имен DNS (т. е. обладающие общим корневым доменом), образуют дерево. Домены, не использующие непрерывное пространство имен DNS, образуют разные деревья в данном лесу.

3. Какие из следующих утверждений о программе установки Windows Server 2003 верны? (Выберите все подходящие варианты.)
   a. Программу установки можно запустить, загрузив компьютер с компакт-диска.
   b. Программу установки можно запустить, загрузив компьютер с дискет.
   c. Программа установки просит ввести непустой пароль, удовлетворяющий требованиям сложности.
   d. Программа установки позволит ввести идентификатор продукта, состоящий из одних единиц.

   Правильный ответ: a, c.

ГЛАВА 2

Администрирование Microsoft Windows Server 2003

Темы экзамена

- Удаленное управление серверами:
  - с помощью служебной программы *Удаленный помощник* (Remote Assistance);
  - средствами служб терминалов в режиме удаленного администрирования;
  - с помощью доступных служебных программ.
- Устранение неполадок при работе служб терминалов:
  - диагностика и решение проблем, связанных с безопасностью служб терминалов;
  - диагностика и решение проблем, связанных с клиентским доступом к службам терминалов.

В этой главе

В повседневной работе системный администратор часто использует служебные программы для конфигурирования учетных записей пользователей, модификации ПО и параметров служб, установки нового оборудования и т. д. Консоль MMC (Microsoft Management Console) консолидирует и организует наиболее часто используемые утилиты. Кроме того, консоли MMC можно настраивать и приспосабливать под конкретные потребности, поэтому ряд задач можно делегировать другим администраторам.

Если требуется более тонкая настройка удаленного компьютера, которую нельзя выполнить удаленно средствами MMC, можно задействовать две служебных программы: *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration)

и *Удаленный помощник* (Remote Assistance). В целом, *Удаленный рабочий стол для администрирования* можно рассматривать как клиент-серверное приложение, позволяющее отображать в окне клиентского компьютера локальную консоль сервера; в итоге вы можете управлять клавиатурой и мышью, как если бы вы вошли в систему локально, запустив консоль на сервере. Программа *Удаленный помощник* аналогична по функциональности, но область ее применения ограничена компьютерами, где установлена ОС Microsoft Windows Server 2003 или семейства Windows XP. Пользователь на таком компьютере запрашивает помощь, и к его рабочему столу можно подключиться с удаленного компьютера.

Прежде всего

Для изучения материалов этой главы вам потребуются:

- компьютер с установленной ОС Windows Server 2003 (для полного соответствия примерам сервер должен иметь имя ServerOl и быть контроллером домена contoso.com);
- служебная программа *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration), установленная на ServerOl, с включенными функциями *Дистанционное управление рабочим столом* (Remote Desktop) и *Удаленный помощник* (Remote Assistance);
- сконфигурированная и работающая по протоколу TCP/IP сеть, к которой могут подключаться консоль и удаленно администрируемые компьютеры.

Занятие 1. **Консоль управления MMC**

Основное средство администрирования в Windows Server 2003 — консоль MMC (Microsoft Management Console) — предоставляет стандартный интерфейс для одного или нескольких приложений, называемых *оснастками* (snap-in), которые применяются для конфигурирования элементов вашей среды. Эти оснастки приспособлены для решения конкретных задач, их можно упорядочивать и группировать в рамках консоли MMC согласно вашим предпочтениям.

Например, преднастроенная консоль *Active Directory — пользователи и компьютеры* (Active Directory Users and Computers) разработана специально для администрирования участников безопасности (пользователей, групп и компьютеров) в домене. Консоли в рамках MMC (но не сама MMC) — это и есть используемые вами средства администрирования.

Примечание Консоли MMC работают под управлением Windows Server 2003, Windows 2000/NT 4/XP/98.

Изучив материал этого занятия, вы сможете:

- ☑ настраивать консоль MMC, содержащую отдельную оснастку;
- ☑ настраивать консоль MMC, содержащую несколько оснасток;
- ☑ сохранять консоль MMC в авторском и пользовательском режимах.

Продолжительность занятия — около 15 минут.

Консоль MMC

Консоль управления MMC — подобие *Проводника Windows,* только с меньшим количеством кнопок. Функциональные компоненты MMC содержатся в так называемых оснастках: меню и панель инструментов предоставляют команды для управления родительскими и дочерними окнами, а сама консоль (состоящая из оснасток) определяет требуемую функциональность. Помимо этого, в зависимости от ситуации консоль MMC можно сохранять с различными параметрами и в разных режимах.

Навигация в консоли MMC

Пустая консоль управления MMC показана на рис. 2-1. Заметьте, что ей присвоено имя, и у нее есть узел **Корень консоли (Console Root).** Именно в этот корень консоли будут помещаться все необходимые оснастки.

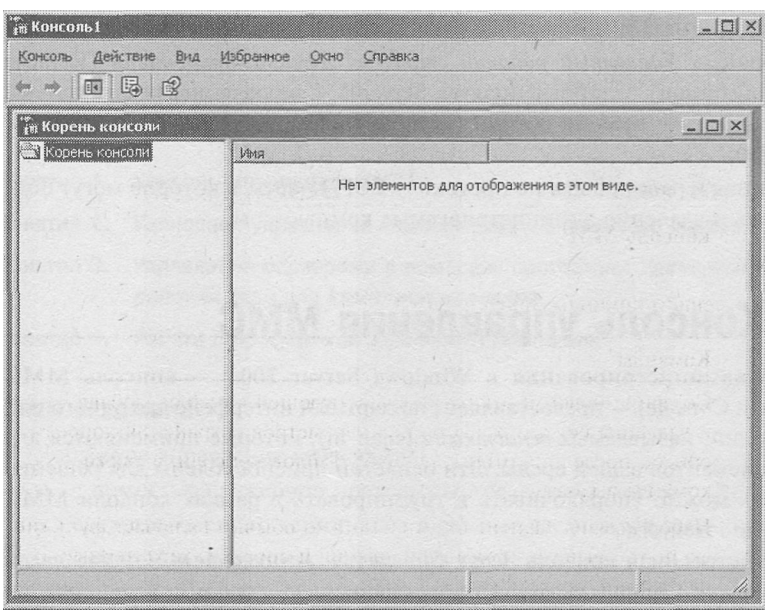


Рис. 2-1. Пустая консоль MMC

В каждой консоли имеется дерево (отображается слева), меню и панели инструментов, а также панель подробных сведений (отображается справа). Содержимое этих элементов зависит от назначения и функциональных возможностей используемой консоли. На рис. 2-2 показана консоль MMC с двумя загруженными оснастками, а также дочерним окном оснастки *Диспетчер устройств* (Device Manager).

Работа с меню и панелью инструментов консоли MMC

Хотя каждая оснастка добавляет собственные уникальные элементы в меню и на панель инструментов, есть несколько ключевых меню и команд, используемых во многих ситуациях и типичных для большинства оснасток (табл. 2-1).

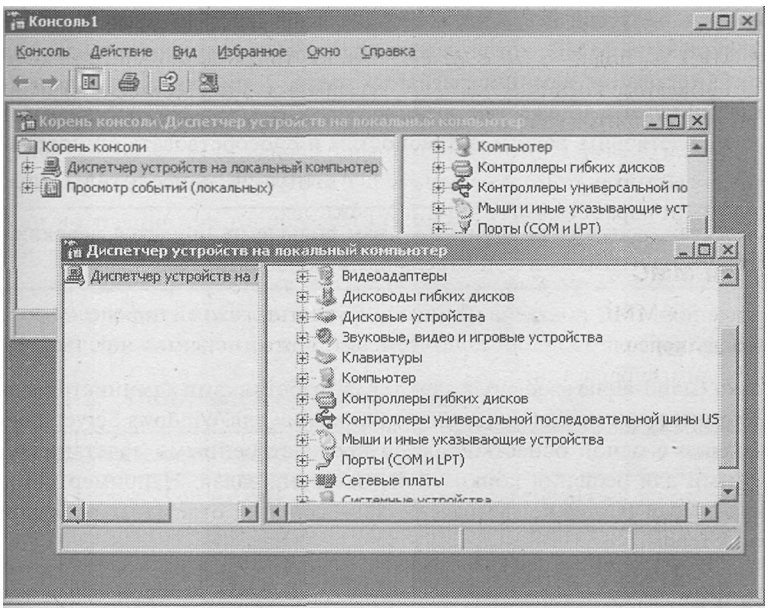


Рис. 2-2. Заполненная консоль MMC

Табл. 2-1. Типичные меню и команды консоли MMC

Меню	Команды
Консоль (Console)	Создание новой и открытие существующей консоли, добавление и удаление оснасток, настройка параметров сохранения консоли, список последних открывавшихся файлов консоли, а также команда выхода
Действие (Action)	Набор команд зависит от оснастки, но обычно включает функции экспорта, вывода, конфигурирования и справки, характерные для данной оснастки
Вид (View)	Набор команд зависит от оснастки, но обычно включает параметры для изменения общих характеристик отображения консоли
Избранное (Favorites)	Добавление и организация сохраненных консолей
Окно (Window)	Открытие нового окна, размещение внутренних окон каскадом или сверху вниз, а также переключение между открытыми дочерними окнами данной консоли
Справка (Help)	Стандартное справочное меню консоли MMC, а также модули справки загруженных оснасток

Создание собственной консоли MMC

Каждая консоль содержит набор из одной или нескольких *оснасток* (snap-in), которые расширяют возможности консоли, добавляя функции управления, специфичные для какой-либо задачи. Предусмотрено два типа оснасток: изолированные и оснастки-расширения.

Вы можете объединить одну или несколько оснасток либо их составные части для создания собственных консолей MMC, которые в дальнейшем можно использовать для централизации и комбинирования административных задач. Хотя для задач администрирования можно использовать множество преднастроенных консолей, собственные консоли будут лучше удовлетворять вашим потребностям и способствовать стандартизации вашей среды.

Совет После создания собственной консоли MMC вам больше не придется переключаться между различными программами или отдельными консолями.

Изолированные оснастки

Изолированные оснастки (stand-alone snap-in) создаются разработчиками административного приложения. Например, все средства администрирования для Windows Server 2003 являются либо консолями с одной оснасткой, либо преднастроенными сочетаниями оснасток, используемыми для решения конкретной категории задач. Например, консоль *Управление компьютером* (Computer Management) — сборник отдельных оснасток для управления компьютером.

Оснастки-расширения

Оснастки-расширения (extension snap-in), или просто *расширения,* предназначены для работы совместно с одной или несколькими изолированными оснастками на основе их функциональности. Когда вы добавляете расширение, Windows Server 2003 помещает его в соответствующее место в рамках изолированной оснастки.

Многие оснастки обладают изолированной функциональностью и, помимо этого, способны расширять функциональность других оснасток. Например, оснастка *Просмотр событий* (Event Viewer) отображает журналы событий компьютеров. Если в консоли имеется объект *Управление компьютером* (Computer Management), то оснастка *Просмотр событий* автоматически дополняет все экземпляры этого объекта и предоставляет средства просмотра журнала событий. С другой стороны, оснастка *Просмотр событий* может работать в изолированном режиме, и не отображаться при этом в иерархии дерева ниже узла **Управление компьютером (Computer Management).**

На заметку Потратьте несколько минут на анализ повседневных задач и сгруппируйте их по типу функциональности и частоте выполнения. Создайте две или три пользовательских консоли, содержащих наиболее часто применяемые средства. Этим вы сэкономите время на открытие и закрытие приложений и переключение между ними.

Параметры консоли

Параметры консоли определяют порядок работы MMC: какие узлы в дереве консоли можно открывать, какие оснастки добавлять и какие окна создавать.

Авторский режим

Когда вы сохраняете консоль в авторском режиме (по умолчанию), то получаете полный доступ ко всей функциональности MMC, в том числе вы можете:

- добавлять и удалять оснастки;
- создавать окна;

- создавать панели задач и задачи;
- просматривать узлы дерева консоли;
- изменять параметры консоли;
- сохранять консоль.

Пользовательские режимы

Если вы планируете распространять консоль MMC, реализующую характерные функции, то можете задать требуемый пользовательский режим, а затем сохранить консоль. По умолчанию файлы консоли записываются в папку *Администрирование* (Administrative Tools) в профиле пользователя. В табл. 2-2 перечислены пользовательские режимы, доступные при сохранении консоли MMC.

Табл. 2-2. Пользовательские режимы консоли MMC

Тип пользовательского режима	Описание
Полный доступ (Full Access)	Позволяет перемещаться по оснасткам, открывать окна и обращаться ко всем узлам дерева консоли
Ограниченный доступ, несколько окон (Limited Access, Multiple Windows)	Пользователи не вправе открывать новые окна или обращаться к узлам дерева, но могут просматривать в консоли несколько окон
Ограниченный доступ, одно окно Limited Access, Single Window	Пользователи не вправе открывать новые окна или обращаться к узлам дерева и могут просматривать в консоли только одно окно

Примечание Консоль MMC сохраняется с расширением .msc. Например, файл консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) назван Dsa.msc (сокращение от Directory Services Administrator.Microsoft Saved Console).

Лабораторная работа. **Создание и сохранение консолей**

На этой лабораторной работе вы создадите, настроите и сохраните консоль MMC.

Упражнение. Консоль *Просмотр событий*

1. Щелкните **Пуск (Start)\Выполнить (Run).**
2. **В** поле **Открыть (Open)** введите mmc, затем щелкните **OK.**
3. Разверните окна **Консоль1 (Console1)** и **Дерево консоли (Console Root).**
4. **В** меню **Файл (File)** выберите **Параметры (Options),** чтобы узнать, какой режим настроен для консоли.
5. Убедитесь, что в раскрывающемся списке **Режим консоли (Console Mode)** выбрано **Авторский режим (Author mode),** затем щелкните **OK.**
6. В меню **Файл (File)** щелкните **Добавить или удалить оснастку (Add/Remove Snap-In).** Откроется диалоговое окно **Добавить или удалить оснастку (Add/Remove Snap-In)** с выбранной вкладкой **Изолированная оснастка (Standalone).** Заметьте, что консоль пуста.

7. В окне **Добавить или удалить оснастку** щелкните **Добавить (Add),** чтобы раскрыть окно **Добавить изолированную оснастку (Add Standalone Snap-In).**
8. Выберите оснастку **Просмотр событий (Event Viewer),** затем щелкните **Добавить (Add).** Откроется диалоговое окно **Выбор компьютера (Select Computer),** в котором можно указать, какой компьютер вы хотите администрировать. Вы можете добавить оснастку **Просмотр событий** для работы с локальным или удаленным компьютером.
9. В окне **Выбор компьютера (Select Computer)** выберите **Локальный компьютер (Local Computer),** затем щелкните **Готово (Finish).**
10. **В** окне **Добавить изолированную оснастку (Add Standalone Snap-In)** щелкните **Закрыть (Close),** а затем в окне **Добавить/удалить оснастку (Add/Remove Snap-Ins)** щелкните **OK**. В дереве консоли появится новый узел — **Просмотр событий (локальных) [Event Viewer (Local)].** Отрегулируйте мышью ширину панели дерева консоли, чтобы увидеть полное имя узла; вы также можете раскрывать любые узлы этой консоли.
11. Самостоятельно добавьте оснастку *Диспетчер устройств на локальный компьютер* [(Device Manager (local)].
12. Сохраните консоль MMC под именем MyEvents.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. В каком режиме по умолчанию создаются консоли MMC?
2. Может ли оснастка одновременно отображать информацию о локальном и удаленном компьютерах?
3. Если требуется ограничить доступ к оснастке, как сконфигурировать содержащую ее консоль MMC?

Резюме

Консоль MMC — это полезное средство организации и консолидации оснасток либо небольших служебных программ, применяемых для администрирования компьютеров и сети. Иерархическое отображение информации, аналогичное *Проводнику Windows,* представляет функции консоли в хорошо знакомом виде папок. Существует два типа оснасток: изолированные и расширения. При этом расширения отображаются и функционируют в рамках консоли MMC в зависимости от контекста расположения. Любую консоль можно настроить для работы в одном из двух режимов, авторском или пользовательском, причем в пользовательском режиме функциональность сохраненной консоли можно ограничить.

Занятие 2. Удаленное управление компьютерами с помощью консоли MMC

Предположим, вы работаете в одноранговой сети и должны помогать другим пользователям создавать на их компьютерах учетные записи пользователей и групп для общего доступа к локальным папкам. Вы можете сэкономить время, не наведываясь в офисы коллег, если будете подключаться к компьютерам пользователей из консоли *Управление*

компьютером (Computer Management), как показано на рис. 2-3. Или, возможно, вам необходимо отформатировать жесткие диски либо выполнить другие задачи на удаленном компьютере. Практически любую задачу, которую можно сделать локально, вы можете выполнить и на удаленном компьютере.

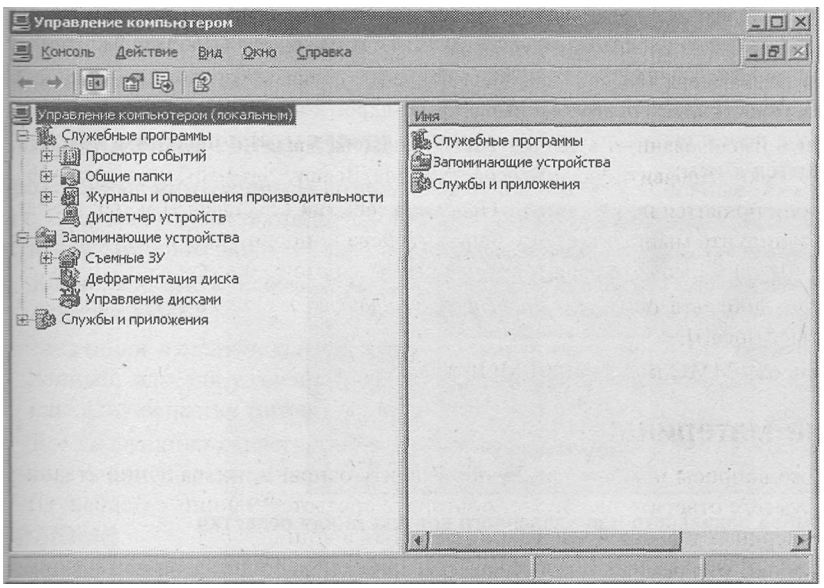


Рис. 2-3. Подключение к компьютеру пользователя из консоли *Управление компьютером*

Изучив материал этого занятия, вы сможете:

- ✓ создавать консоли MMC для удаленного управления компьютером.

Продолжительность занятия — около 10 минут.

Настройка оснастки для работы в удаленном режиме

Чтобы с помощью консоли *Управление компьютером* (Computer Management) подключиться к другой системе и управлять ею, необходимо запустить эту консоль на удаленном компьютере под учетной записью с административными реквизитами. Если ваши реквизиты не обладают достаточными привилегиями на нужном компьютере, вам удастся загрузить оснастку, но вы не сможете получить информацию с удаленного компьютера.

Совет Чтобы запустить консоль с реквизитами, отличными от тех, с которыми вы вошли в систему, задействуйте команду **Запуск от имени (Run As),** т. е. выполните вторичный вход в систему.

Подготовив все к управлению удаленной системой, вы можете открыть существующую консоль с загруженной оснасткой либо сконфигурировать новую консоль MMC с

оснасткой, настроенной на удаленное подключение. Например, если вы хотите настроить существующую консоль *Управление компьютером,* сделайте следующее.

1. Откройте консоль *Управление компьютером* (Computer Management): щелкните правой кнопкой **Мой компьютер (My Computer)** и выберите **Управление (Manage).**
2. **В** дереве консоли щелкните правой кнопкой **Управление компьютером (Computer Management)** и выберите **Подключиться к другому компьютеру (Connect To Another Computer).**
3. В диалоговом окне (рис. 2-4) введите имя или IP-адрес компьютера (либо щелкните кнопку рядом с полем ввода для поиска нужного компьютера) и щелкните **OK**, чтобы подключиться к нему.

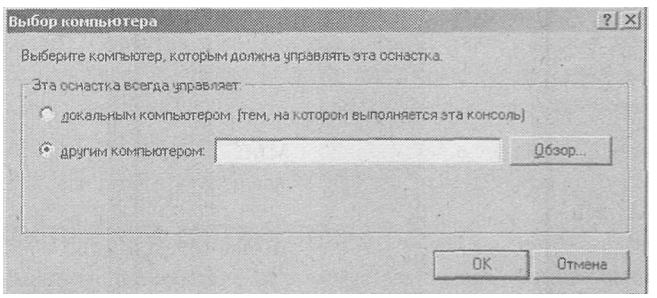


Рис. 2-4. Выбор локального или удаленного контекста для оснастки

Подключившись к удаленному компьютеру, вы сможете выполнять на нем административные задачи.

Лабораторная работа. **Добавление компьютера для удаленного управления (необязательная)**

Примечание Для выполнения этой работы необходим компьютер, к которому можно подключаться удаленно, и у вас должны быть на нем административные привилегии.

Упражнение. Удаленное подключение из консоли MMC

В этом упражнении вы настроите существующую консоль MMC для подключения к удаленному компьютеру.

1. Откройте консоль MMC, которую вы сохранили, выполняя упражнение занятия 1 (консоль MyEvents).
2. В меню **Файл (File)** щелкните **Добавить или удалить оснастку (Add/Remove Snap-In).**
3. В окне **Добавить или удалить оснастку (Add/Remove Snap-In)** щелкните **Добавить (Add),** чтобы раскрыть окно **Добавить изолированную оснастку (Add Standalone Snap-In).**
4. Выберите оснастку **Управление компьютером (Computer Management),** затем щелкните **Добавить (Add).**
5. **В** окне **Управление компьютером (Computer Management)** выберите **другим компьютером (Another Computer).**

6. Введите имя или IP-адрес компьютера либо щелкните **Обзор (Browse),** найдите нужный компьютер, затем щелкните **Готово (Finish),** чтобы подключиться к нему.
7. Щелкните **Закрыть (Close)** в окне **Добавить изолированную оснастку (Add Standalone Snap-In),** а затем OK, чтобы загрузить оснастку *Управление компьютером* (Computer Management) в консоль MyEvents.

Теперь вы можете использовать средства администрирования для управления удаленным компьютером.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. **Ответы** для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Какие реквизиты необходимы для администрирования удаленного компьютера из консоли MMC?
2. Можно ли изменить контекст существующей оснастки MMC с локального на удаленный, или для удаленного подключения необходимо загружать в консоль MMC еще одну оснастку того же типа?
3. Все ли функции оснастки, применяемые на локальном компьютере, можно использовать при удаленном подключении?

Резюме

В консоль MMC можно загружать множество разных средств администрирования, предъявленных в виде оснасток. Некоторые из этих оснасток способны подключаться и к локальному, и к удаленным компьютерам. Подключение к удаленному компьютеру можно устанавливать, когда вы загружаете оснастку в консоль, либо уже после ее загрузки, щелкнув объект оснастки правой кнопкой и выбрав **Подключиться к другому компьютеру (Connect To Another Computer).** Чтобы использовать любые программы, конфигурирующие удаленный компьютер, необходимо обладать административными привилегиями на этом компьютере.

Занятие 3. Управление серверами с помощью программы *Удаленный рабочий стол для администрирования*

В семействе Windows 2000 Server был впервые реализован тесно интегрированный набор программных средств и технологий, позволяющих выполнять удаленное администрирование и совместно использовать приложения с помощью *Служб терминалов* (Terminal Services). Эволюция продолжилась: отныне службы терминалов — неотъемлемый компонент семейства Windows Server 2003, а инструмент *Дистанционное управление рабочим столом* (Remote Desktop) усовершенствован и позиционируется как стандартная функция. Так что теперь достаточно одного щелчка мыши, и компьютер с Windows Server 2003 будет параллельно обрабатывать до двух подключений удаленного администриро-

вания. Добавив компонент *Сервер терминалов* (Terminal Server) и настроив соответствующую лицензию, администратор добьется еще большего эффекта: множество пользователей смогут запускать приложения на сервере. На этом занятии вы научитесь работать со служебной программой *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration).

Изучив материал этого занятия, вы сможете:

- ✓ включать на сервере программу *Удаленный рабочий стол дляадминистрирования;*
- ✓ включать пользователей в соответствующую группу, чтобы разрешить им удаленно администрировать сервер;
- ✓ подключаться к серверу с помощью программы *Удаленный рабочий стол дляадминистрирования*.

Продолжительность занятия - около 15 минут.

Включение и конфигурирование программы *Удаленныйрабочийстолдляадминистрирования*

Службы терминалов позволяют совместно использовать приложения с помощью таких инструментов, как *Дистанционное управление рабочим столом* (Remote Desktop), *Удаленный помощник* (Remote Assistance) и *Сервер терминалов* (Terminal Server). По умолчанию служба устанавливается вместе с Windows Server 2003 и настраивается в программе *Дистанционное управление рабочим столом* для работы в режиме удаленного администрирования: допускает только два параллельных удаленных подключения и не содержит компоненты для совместного использования приложений из состава *Сервера терминалов*. Следовательно, *Дистанционное управление рабочим столом* создает очень небольшую дополнительную нагрузку на систему, причем не требует дополнительного лицензирования.

Примечание Поскольку *Службы терминалов* и *Дистанционное управление рабочим столом* являются стандартными компонентами Windows Server 2003, каждый сервер способен поддерживать удаленные подключения к своей консоли. Термин «сервер терминалов», таким образом, теперь по праву можно применить к любому компьютеру под управлением Windows Server 2003, обеспечивающему совместное использование приложений несколькими клиентами за счет добавления компонента *Службы терминалов*.

Другие компоненты — *Сервер терминалов* и службу *Лицензирование сервера терминалов* (Terminal Server Licensing) — нужно добавлять с помощью функции *Установка и удаление программ* (Add Or Remove Programs). Тем не менее, все средства администрирования для настройки и поддержки клиентских подключений и управления сервером терминалов устанавливаются по умолчанию на все компьютеры с Windows Server 2003. Эти средства и их функции описаны в табл. 2-3.

Табл. 2-3. Стандартные компоненты *Сервер терминалов* и *Подключение к удаленному рабочему столу*

Установленное ПО	Назначение
Настройка служб терминалов (Terminal Services Configuration)	Настройка свойств сервера терминалов, в том числе параметров сеанса, сети, клиентского рабочего стола и удаленного управления клиентом
Диспетчер служб терминалов (Terminal Services Manager)	Отправка сообщений клиентам, подключенным к серверу терминалов, отключение или завершение сеансов, а также инициирование удаленного управления или маскировки сеансов
*Подключение к удаленному рабочему столу (*Установочные файлы клиента Remote Desktop Connection)	Установка клиентского приложения *Дистанционное управление рабочим столом* (Remote Desktop) для Windows Server 2003 или Windows XP. 32-разрядное клиентское ПО *Дистанционное управление рабочим столом* устанавливается в папку %Systemroot%\System32\Clients\Tsclient\Win32 на сервере терминалов
Лицензирование служб терминалов (Terminal Services Licensing)	Настройка лицензий для клиентских подключений к серверу терминалов. Это средство не подходит для сред, где используется только *Удаленный рабочий стол для администрирования*

Чтобы разрешить подключения *Дистанционное управление рабочим столом* (Remote Desktop) на компьютере под управлением Windows Server 2003, в *Панели управления* выберите Система (System Properties). На вкладке Удаленное использование (Remote) выберите Разрешить удаленный доступ к этому компьютеру (Allow Users To Connect Remotely To This Computer).

Примечание Если сервер терминалов является контроллером домена, необходимо также настроить групповую политику контроллера, чтобы разрешить группе *Пользователи удаленного рабочего стола* (Remote Desktop Users) подключение посредством служб терминалов. На серверах, не являющихся контроллерами домена, подключение через службы терминалов пользователям из этой группы разрешено по умолчанию.

Подключение к удаленному рабочему столу

Подключение к удаленному рабочему столу (Remote Desktop Connection) — это клиентское приложение, используемое для подключения к серверу в контексте режима *Дистанционное управление рабочим столом* (Remote Desktop) или *Сервер терминалов* (Terminal Server). Для клиента нет функциональных различий между этими двумя конфигурациями сервера.

На компьютерах с Windows XP и Windows Server 2003 программа *Подключение к удаленному рабочему столу* установлена по умолчанию, но глубоко запрятана: **Пуск (Start)\ В :е программы (All Programs)\Стандартные (Accessories)\Связь (Communications)\Подключение к удаленному рабочему столу (Remote Desktop Connection)**.

На других платформах программу *Подключение к удаленному рабочему столу* можно установить с компакт-диска Windows Server 2003 либо из установочной папки клиента (%Systemroot%\System32\Clients \Tsclient\Win32) на любом из компьютеров под управлением Windows Server 2003. Установочный пакет MSI можно распространять на системы Windows 2000 с помощью групповой политики или средствами SMS (Systems Management Server).

Совет Рекомендуется обновить предыдущие версии клиента *Служб терминалов,* установив последнюю версию *Подключение к удаленному рабочему столу,* чтобы обеспечить наиболее оптимальную, безопасную и стабильную среду, поскольку в этом случае будет доступен улучшенный пользовательский интерфейс, 128-битное шифрование и выбор альтернативных портов.

На рис. 2-5 показан клиент программы *Дистанционное подключение к рабочему столу,* настроенный для подключения к серверу Server01 в домене contoso.com.

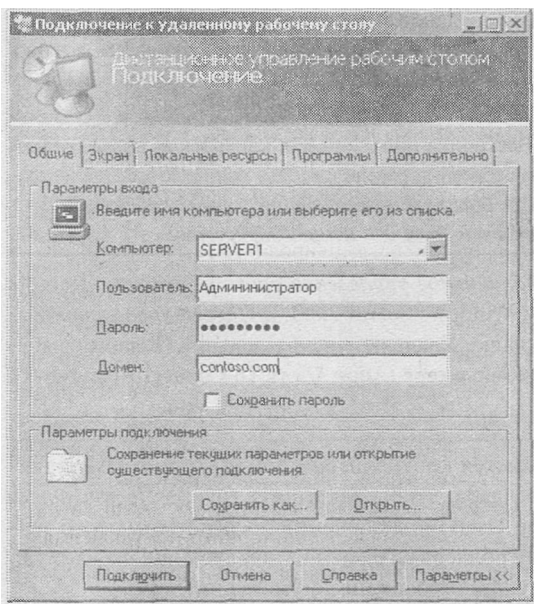


Рис. 2-5. Клиент программы *Удаленное подключение к рабочему столу*

Настройка клиента удаленного подключения к рабочему столу

Вы можете управлять множеством аспектов дистанционного подключения как со стороны клиента, так и со стороны сервера. В табл. 2-4 перечислены конфигурационные параметры и их назначение.

Табл. 2-4. Параметры программы *Удаленное подключение к рабочему столу*

Параметры	Назначение
Параметры клиента	
Общие (General)	Параметры выбора компьютера, к которому необходимо подключаться, настройка статических реквизитов для входа в систему, а также сохранение параметров для данного подключения
Экран (Display)	Задает размер окна клиента, глубину цвета, а также доступность панели подключений при работе в полноэкранном режиме
Локальные ресурсы (Local Resources)	Параметры передачи звуковых событий на локальный компьютер, помимо стандартных выходных сигналов мыши, клавиатуры и экрана. Также параметры на этой вкладке определяют, как удаленный компьютер интерпретирует комбинации клавиш Windows (например Alt+Tab), и доступны ли в сеансе удаленного доступа такие устройства, как локальные диски, принтеры и последовательные порты
Программы (Programs)	Задает путь и папки расположения для любых программ, которые необходимо запустить после установки соединения
Дополнительно (Experience)	Категории функций экрана можно включать или отключать в зависимости от пропускной способности канала связи между локальным и удаленными компьютерами. Предусмотрены параметры для отображения фона рабочего стола, содержимого окна при перетаскивании, визуальных эффектов при прорисовке меню и окон, тем рабочего стола; также вы можете активировать режим кэширования растровой графики, при котором после каждого интервала обновления передаются только изменения, а не весь экран целиком
Параметры сервера	
Параметры входа (Logon Settings)	Позволяет задать статические реквизиты для подключения вместо реквизитов, предоставляемых клиентом
Сеансы (Sessions)	Чтобы перекрыть настройки клиента, задайте здесь параметры завершения прерванного сеанса, ограничения длительности сеанса и времени его простоя, а также допустимость повторного подключения
Среда (Environment)	Перекрывает настройки из профиля пользователя для данного подключения в отношении запуска программы: здесь вы можете переопределить запускаемую при подключении программу. Заданный здесь путь и папка запуска приоритетнее настроек, сделанных программой *Подключение к удаленному рабочему столу*
Разрешения (Permissions)	Позволяет задавать дополнительные разрешения для данного подключения
Удаленное управление (Remote Control)	Указывает, можно ли удаленно управлять сеансом *Подключение к удаленному рабочему столу,* и если так, то должен ли пользователь выдавать разрешение на инициализацию сеанса удаленного управления. Дополнительные параметры позволяют ограничить сеанс удаленного управления только функцией просмотра либо разрешить полную интерактивность с сеансом клиента *Дистанционное управление рабочим столом*

Табл. 2-4. *(окончание)*

Параметры	Назначение
Параметры клиента (Client Settings)	Позволяют перекрыть параметры из конфигурации клиента, изменить глубину цвета и отключить различные коммуникационные порты (порты ввода-вывода)
Сетевой адаптер (Network Adapters)	Указывает, какие сетевые платы на сервере будут принимать удаленные подключения для администрирования
Общие (General)	Задает уровень шифрования и механизм проверки подлинности для подключений к этому серверу

Устранение неполадок при работе со службами терминалов

При использовании программы *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration) создается подключение к консоли сервера. Есть несколько потенциальных причин неудачных подключений или сеансов с ошибками.

- **Сбои сети.** Ошибки в работе стандартной TCP/IP-сети могут вызывать сбои или разрывы подключений *Дистанционное подключение к рабочему столу* (Remote Desktop). Если не функционирует служба DNS, клиент не сможет найти сервер по имени. Если не функционирует маршрутизация либо неверно настроен порт *Служб терминалов* (Terminal Services) (по умолчанию это порт 3389) на клиенте или сервере, соединение установить не удастся.
- **Реквизиты входа.** Для успешного подключения к серверу средствами программы *Удаленный рабочий стол для администрирования* пользователи должны быть включены в группу *Администраторы* (Administrators) или *Пользователи удаленного рабочего стола* (Remote Desktop Users).

  Подготовка к экзамену Если подключиться через *Удаленный рабочий стол для администрирования* не удается из-за запрета доступа, проанализируйте членство в группах. В предыдущих версиях *Сервера терминалов* (Terminal Server) для подключения к серверу требовалось быть участником группы *Администраторы* (Administrators), хотя специальные разрешения можно было выдать вручную. Сервер терминалов поддерживает только два удаленных подключения.

- **Политика.** Только администраторам разрешено подключаться средствами программы *Дистанционное подключение к рабочему столу* (Remote Desktop) к контроллерам доменов. Чтобы разрешить подключаться остальным пользователям, нужно настроить политику безопасности на контроллере домена.
- **Слишком много** параллельных **подключений.** Если сеансы прерывались без выхода из системы, сервер может посчитать, что достигнут предел одновременно обрабатываемых подключений, даже если в данный момент к серверу не подключены два пользователя. Например, администратор может завершить сеанс без выхода из системы. Если еще два администратора попытаются подключиться к серверу, это удастся только одному из них.

Примечание Подробнее о *Службах терминалов* (Terminal Services) и последних усовершенствованиях клиента программы *Дистанционное подключение к рабочему столу* (Remote Desktop) — по адресу http://www.microsoft.com/technet/treeview/default.asp?url/technet/prodtechnol/windowsserver2003/proddocs standard/sag_Server_Trouble_Topnode.asp.

Лабораторная работа. **Установка служб терминалов и удаленное администрирование**

На этой лабораторной работе вы настроите на сервере ServerOl подключения через *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration). Затем вы оптимизируете Server01, чтобы обеспечить доступность неиспользуемого подключения и разрешить лишь одно подключение в любой момент времени. После этого вы установите сеанс удаленного администрирования с Server02 (либо с другого удаленного компьютера).

Если в вашем распоряжении только один компьютер, можно использовать клиент программы *Дистанционное подключение к рабочему столу* (Remote Desktop) для подключения к службам терминалов на том же компьютере. В этом случае ссылки на удаленный компьютер на этой лабораторной работе будут относится к локальному компьютеру.

Упражнение 1. Настройка удаленного подключения к рабочему столу

В этом упражнении вы активируете удаленное подключение к рабочему столу, измените число разрешенных одновременных подключений на сервере и настроите параметры завершения подключения.

1. Войдите на ServerOl как *Администратор* (Administrator).
2. В Панели управления выберите **Система (System Properties).**
3. На вкладке **Remote** включите **Remote Desktop.** Закройте окно **Система (System Properties).**
4. Откройте консоль *Настройка служб терминалов* (Terminal Services Configuration) из группы программ *Администрирование* (Administrative Tools).
5. В консоли tscc (Terminal Services Configuration\Connections) на правой панели щелкните правой кнопкой подключение **RDP-tcp** и выберите **Свойства (Properties).**
6. На вкладке **Сетевой адаптер (Network Adapter)** установите значение параметра **Максимальное число подключений (Maximum Connections)** равным 1.
7. На вкладке **Сеансы (Sessions)** установите оба флажка **Заменить параметры пользователя (Override User Settings)** и измените настройки следующим образом: все прерванные любыми способами (или по любой причине) сеансы пользователей закрываются через 15 минут, активный сеанс не ограничивается по времени, сеансы завершаются после 15 минут бездействия.
   - **Завершение отключенного сеанса (End a disconnected session):** 15 минут,
   - **Ограничение активного сеанса (Active session limit): никогда (never),**
   - **Ограничение активного сеанса (Active session limit):** 15 минут.
   - **При превышении ограничений или разрыве подключения (When session limit is reached or connection is broken): Отключить сеанс (Disconnect from session).**

   Такая конфигурация обеспечивает следующее: только один пользователь одновременно подключен к серверу терминалов, любой прерванный сеанс закроется через

15 минут и неактивный сеанс прервется через 15 минут. Эти параметры позволяют избежать ситуации, когда прерванный или бездействующий сеанс мешает подключаться средствами программы *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration).

Упражнение 2. Подключение к серверу с помощью клиента удаленного подключения к рабочему столу

1. На Server02 (или на другом удаленном компьютере либо прямо с ServerOl, если удаленного компьютера нет) в группе Стандартные\Связь (Accessories\Communications) щелкните **Подключение к удаленному рабочему столу (Remote Desktop Connection),** подключитесь к Server01 и войдите в его систему.
2. На сервере Server01 откройте консоль tscc.msc: **Администрирование (Administrative tools)\Настройка служб терминалов (Terminal Services Configuration).** В открывшейся консоли выберите **Подключения (Connections).** Вы должны увидеть сведения о сеансе удаленного подключения к Server01.
3. Не выполняйте никаких действий в этом сеансе 15 минут либо закройте клиент программы *Удаленное подключение к рабочему столу* (Remote Desktop), не завершив сеанс *Сервера терминалов* (Terminal Server) явно: сеанс должен будет завершиться автоматически через 15 минут.

В данный момент вы подключены к ServerOl удаленно и можете выполнять на нем любые задачи, допустимые в интерактивном режиме на консоли.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Сколько одновременных подключений разрешено к серверу терминалов, работающему в режиме удаленного администрирования? Почему?
2. Как оптимальным образом предоставить администраторам возможность удаленного управления сервером через службы терминалов?
   a. Не выполнять никаких действий; они уже имеют доступ, поскольку являются администраторами.
   b. Удалить группу *Администраторы* (Administrators) из списка разрешений в подключении к серверу терминалов и поместить их административную учетную запись в группу *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration).
   c. Создать отдельную пользовательскую учетную запись с более низким уровнем авторизации для повседневного использования группой *Администраторы* и поместить ее в группу *Удаленный рабочий стол для администрирования*.
3. Какое программное средство используется на сервере для включения удаленного подключения к рабочему столу?
   a. *Диспетчер служб терминалов* (Terminal Services Manager).
   b. *Настройка служб терминалов* (Terminal Services Configuration).
   c. *Система* (System Properties) из Панели управления.
   d. *Лицензирование служб терминалов* (Terminal Services Licensing).

Резюме

Администраторы и члены группы *Пользователи удаленного рабочего стола* (Remote Desktop Users) вправе подключаться к серверу с помощью программы *Подключение к удаленному рабочему столу* (Remote Desktop Connection). Службы терминалов установлены на Windows Server 2003 по умолчанию и допускают не более двух одновременных подключений средствами программы *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration). Клиент подключения к удаленному рабочему столу, стандартный компонент Windows XP и Windows Server 2003, можно установить на любой 32-битной платформе Windows с компакт-диска Windows Server 2003 либо с общего ресурса, открытого на любом компьютере под управлением Windows Server 2003. Конфигурирование подключений средствами программы *Удаленный рабочий стол для администрирования* выполняется посредством настройки параметров на клиенте *[Подключение к удаленному рабочему столу* Remote Desktop Connection)] и на сервере *[Сервер терминалов* (Terminal Server)]. Основные параметры подключений могут быть переопределены сервером.

Занятие 4. Работа с программой *Удаленный помощник*

Пользователи, особенно неопытные в техническом плане, часто не могут правильно настроить параметры или задают вопросы об использовании ПО, на которые специали- тоддержки трудно ответить по телефону. *Удаленный помощник* (Remote Assistance) предоставляет пользователям возможность получить помощь, облегчает и удешевляет работу корпоративных служб поддержки.

Изучив материал этого занятия, вы сможете:

- ✓ включать прием запросов к программе *Удаленный помощник;*
- ✓ применять один из доступных способов установки сеанса удаленной помощи.

Продолжительность занятия - около 30 минут.

Создание запроса помощи

В справке Windows Server 2003 есть раздел на основе мастеров, посвященный программе *Удаленный помощник* (Remote Assistance), его первая страница показана на рис. 2-6.

Подключение на основе мастеров позволяет отправлять запросы посредством учетной записи Microsoft .NET Passport или через обычную почтовую учетную запись путем отправки сохраненного файла, а также с помощью Windows Messenger. Для выполнения запроса посредством электронной почты на обоих компьютерах должен работать почтовый клиент, совместимый с интерфейсом MAPI (Messaging Application Programming Interface).

Чтобы использовать службу Windows Messenger для подключения удаленного помощника, псевдоним помощника в Windows Messenger должен числиться в вашем списке контактов, а сам запрос должен выполняться из клиента Windows Messenger. Windows Messenger будет отображать два его состояния: подключен к Интернету или нет. Удаленную помощь можно запросить только напрямую, когда помощник подключен к Интернету, Для работы программы *Удаленный помощник* (Remote Assistance) необходимо, чтобы на обоих компьютерах была установлена ОС Windows XP или семейства Windows Server 2003.

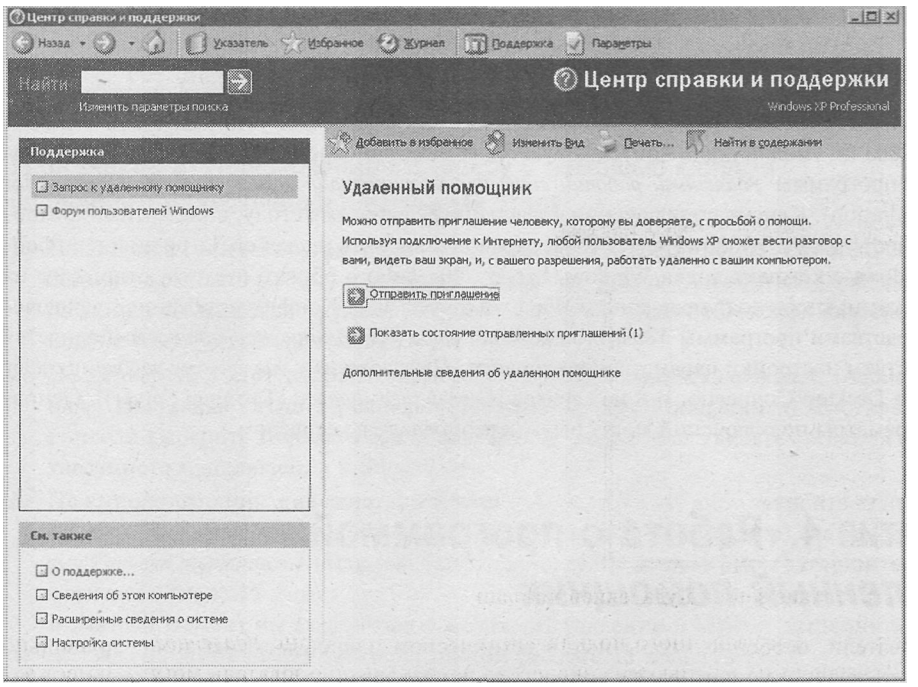


Рис. 2-6. Первый экран программы *Удаленный помощник* в *Центре справки и поддержки*

Примечание Индикатор подключения к Интернету р окне справки программы *Удаленный помощник* не динамический: обновите экран, чтобы получить актуальное состояние.

Получив запрос, помощник (эксперт) может удаленно подключиться к компьютеру и устранить проблему, видя ваш экран. Когда вы инициируете запрос помощи, клиент программы *Удаленный помощник* отправляет помощнику билет, зашифрованный на основе языка XML (Extensible Markup Language), с предложением принять ваше приглашение.

Внимание! Если *Удаленный помощник* включен, клиент подключается к компьютеру с пониженными условиями безопасности. Поэтому всегда проверяйте, что разрешаете доступ только доверенным помощникам.

Работа с программой *Удаленный помощник*

Пользователь может запросить помощь у другого пользователя Windows Messenger, размещая запрос в *Центре справки и поддержки* или прямо через Windows Messenger. Оба приложения применяют одинаковые механизмы, чтобы определять доступность эксперта в сети и создавать запрос помощи. На рис. 2-7 показано создание запроса помощи в Windows Messenger.

В окне Windows Messenger пользователь выбирает учетную запись эксперта. Эксперт получает приглашение в виде обычного мгновенного сообщения. Когда эксперт щелкает **Принять (Accept),** инициируется сеанс удаленного помощника. Запросивший помощь пользователь подтверждает начало сеанса, щелкая Да **(Yes).**

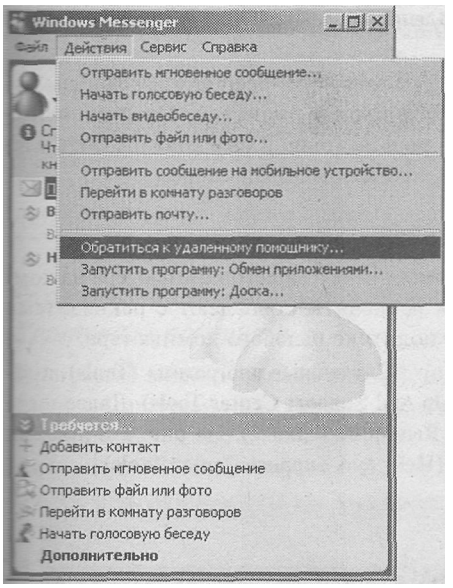


Рис. 2-7. Создание запроса удаленной помощи

После установки удаленного подключения начинается сеанс *Удаленного помощника* (Rmote Assistance) на компьютере эксперта. Эксперт и пользователь могут совместно управлять рабочим столом, передавать файлы и использовать окно беседы (чат), в котором они обсуждают возникшую проблему.

Внимание! Если для получения помощи пользователь решит отправить сообщение по электронной почте или запрос в виде файла, для установки сеанса удаленного помощника потребуется ввести общий секретный пароль. Пользователь должен задать строгий пароль и сообщить его эксперту по отдельному каналу связи (по телефону или в защищенном электронном письме).

Предложение помощи средствами программы *Удаленный помощник*

Удаленный помощник (Remote Assistance) особенно полезен, когда нужно устранить неисправность на компьютере пользователя. Для этого необходимо включить параметр локальной групповой политики **Предложение удаленной помощи (Offer Remote Assistance)** на целевом локальном компьютере.

1. На компьютере пользователя щелкните **Пуск (Start)\Выполнить (Run)** и введите gpedit.msc. Откроется редактор локальной групповой политики, в котором можно настраивать политику на локальной машине.

   Примечание Групповая политика домена может запрещать изменение этой политики.

2. Раскройте узлы **Конфигурация компьютера (Computer Configuration), Административные шаблоны (Administrative Templates), Система (System)** и затем щелкните **Удаленный помощник (Remote Assistance).**

3. Дважды щелкните **Разрешить предложение удаленной помощи (Offer Remote Assistance)** и выберите **Включен (Enabled).**
4. Затем щелкните **Показать (Show)** и укажите пользователей-экспертов, которым будет разрешено предлагать помощь в контексте данной политики. Помощников в список следует добавлять в форме домен\имя_пользователя, и они должны быть членами группы локальных администраторов на локальном компьютере.

Инициализация сеанса удаленного помощника

Теперь можно инициировать сеанс удаленного помощника с вашего компьютера на компьютеры пользователей при условии, что ваши реквизиты совпадают с реквизитами помощника, заданными в локальной групповой политике целевого компьютера.

1. Откройте *Центр справки и поддержки,* щелкните **Служебные программы (Tools),** а затем **Средства центра справки и поддержки (Help And Support Center Tools).** Далее щелкните **Предложение удаленной помощи (Offer Remote Assistance).** На рис. 2-8 показан раздел **Средства центра справки и поддержки (Help And Support Center Tools).**

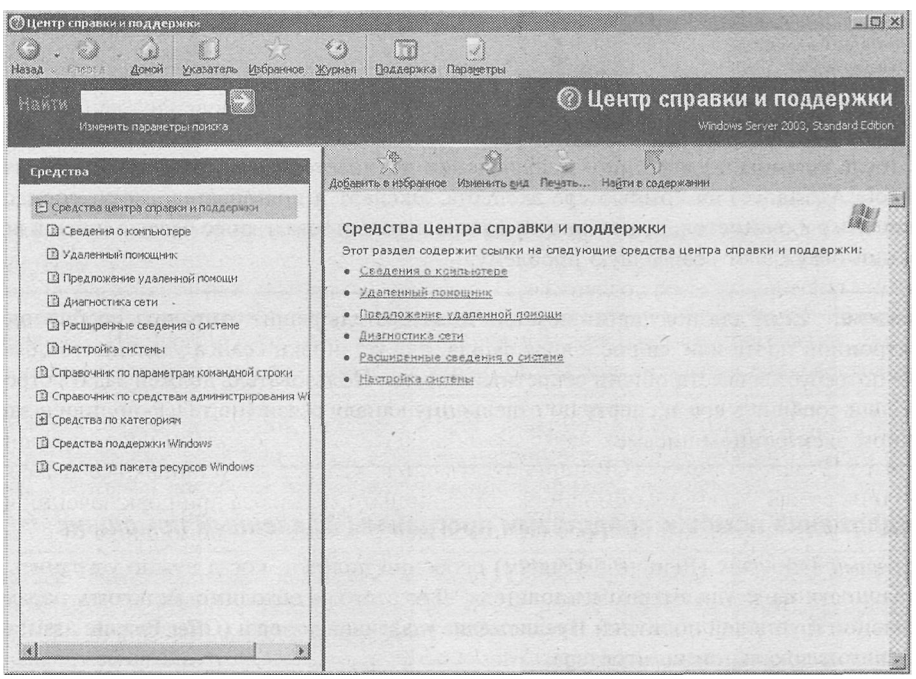


Рис. 2-8. Раздел *Средства центра справки и поддержки*

2. **В** этом диалоговом окне введите имя или IP-адрес целевого компьютера, затем щелкните **Подключиться (Connect).** (Если появится сообщение, что в системе несколько человек, выберите сеанс пользователя.) Затем щелкните **Запустить удаленного помощника (Start Remote Assistance).**

   На компьютере пользователя появляется сообщение, что специалист службы поддержки инициирует сеанс удаленного помощника.
3. Пользователь соглашается, и удаленный помощник может начать работу.

Внимание! При управлении и администрировании с помощью программы *Удаленный помощник* (Remote Assistance) в корпоративной среде или крупной организации следует учесть несколько моментов. Вы можете сформировать открытую среду, в которой пользователи смогут получать удаленную помощь из-за пределов корпоративного брандмауэра, либо ограничить действие программы средствами групповой политики и указать различные уровни разрешений (например разрешить работу удаленного помощника только в пределах корпоративного брандмауэра). Для подключений извне откройте порт 3389.

Ограничения брандмауэра, влияющие на работу программы *Удаленныйпомощник*

Программа *Удаленный помощник* (Remote Assistance) основана на технологии служб терминалов, поэтому она должна использовать тот же порт, что и *Службы терминалов* (Terminal Services): 3389. *Удаленный помощник* не будет работать, если исходящий трафикк порта 3389 заблокирован. Кроме того, существует еще несколько аспектов, касающихся работы брандмауэра, в частности относительно протокола NAT (Network Address Translation).

- *Удаленный помощник* поддерживает UPnP (Universal Plug and Play) для передачи трафика сквозь NAT-устройства. Это полезно при работе в небольших офисных сетях, поскольку механизм ICS (Internet Connection Sharing) из Windows XP поддерживает технологию UPnP (в Windows 2000 — нет).

Подготовка к экзамену Будьте внимательны при ответе на вопросы, относительно использования Windows 2000 ICS для удаленной помощи небольшим филиалам со стороны корпоративных служб поддержки. Поскольку механизм ICS из Windows 2000 не поддерживает UPnP, возникнет множество проблем при работе с программой *Удаленный помощник*.

- Удаленный помощник определит публичный IP-адрес и номер TCP-порта на устройстве UPnP NAT и вставит адрес в зашифрованный билет удаленного помощника. Этот IP-адрес и номер TCP-порта будут использоваться для установки сеанса со стороны рабочей станции помощника или инициатора запроса при подключении через NAT-устройство. Затем запрос на подключение удаленного помощника будет перенаправлен NAT-устройством клиенту.
- Подключение удаленного помощника невозможно, если инициатор запросил помощь по электронной почте и использует NAT-устройство без поддержки UPnP Если приглашение отправляется через Windows Messenger, NAT-устройство без поддержки UPnP будет работать, если один из компьютеров в паре эксперт — пользователь находится за NAT-устройством. Если компьютеры и эксперта, и пользователя находятся за NAT-устройствами без поддержки UPnP, подключение удаленного помощника установить не удастся.

Если дома вы пользуетесь программным персональным брандмауэром или NAT, то можете использовать *Удаленный помощник* без специальных настроек, если же вы используете аппаратный брандмауэр, действуют те же ограничения: для работы программы необходимо открыть порт 3389.

Примечание Собственно служба мгновенных сообщений Instant Messenger работает через открытый порт 1863.

Лабораторная работа. **Удаленная помощь средствами Windows Messenger**

Для выполнения этой лабораторной работы нужен либо партнер, либо второй компьютер для инициирования сеанса удаленного помощника. На компьютерах Server01 и Server02 должен быть установлен Windows Messenger с двумя разными учетными записями. Если в вашем распоряжении только один компьютер, можно инициировать сеанс удаленного помощника с использованием двух разных учетных записей Windows Messenger (далее мы будем называть их #1 и #2), сконфигурированных на одном компьютере, но вы не сможете управлять экраном.

1. На Server02 (или на другом компьютере) откройте Windows Messenger и войдите под учетной записью #2.
2. В Windows Messenger, куда вы вошли под учетной записью #1, в меню **Действия (Actions)** выберите **Обратится к удаленному помощнику (Ask For Remote Assistance).**
3. **В** окне **Обратится к удаленному помощнику (Ask For Remote Assistance)** выберите учетную запись #2 и щелкните OK.
4. Последует серия запросов и подтверждений между двумя приложениями Windows Messenger. Чтобы установить сеанс удаленного помощника, всегда выбирайте **Принять (Accept)** или **OK.**
5. Первоначально сеанс удаленного помощника открывается в режиме **Отображение экрана (Screen View Only).** Чтобы перехватить управление компьютером пользователя, выберите **Взять управление (Take Control)** вверху окна **Удаленный помощник (Remote Assistance).** Пользователь должен принять ваш запрос на управление компьютером.

   Примечание И пользователь, и эксперт могут прервать управление или завершить сеанс в любой момент.

Получает эксперт управление компьютером пользователя или нет, функции просмотра экрана, передачи файлов и чата в реальном времени включены.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. В чем сходство программ *Удаленный помощник* (Remote Assistance) и *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration)? Чем они различаются?
2. Какие выгоды приносит использование программы *Удаленный помощник* (Remote Assistance)?
3. Какие из перечисленных условий работы удаленного помощника связаны с брандмауэрами?
   a. Порт 3389 должен быть открыт.
   b. Нельзя использовать NAT.
   c. Нельзя использовать механизм *Общий доступ к подключению Интернета* (Internet Connection Sharing).
   d. Нельзя использовать программу *Удаленный помощник* (Remote Assistance) в виртуальной частной сети (VPN).

Резюме

Удаленный помощник (Remote Assistance) — двунаправленная программа: пользователь может попросить эксперта о помощи или (если соответствующим образом настроена групповая политика) эксперт может сам инициировать сеанс помощи. В обоих случаях пользователь должен явно подтверждать установку сеанса и в любой момент может разрешить или запретить эксперту управлять своим рабочим столом. Ни в коем случае эксперт не сможет управлять рабочим столом пользователя без запроса. *Удаленный помощник* основан на технологии служб терминалов и использует интерфейс справочной системы и программу Windows Messenger для инициирования сеанса, чата, просмотра, управления экраном и передачи файлов. Технологии *Службы терминалов* (Terminal Services) и *Удаленный помощник* (Remote Assistance) связаны настолько тесно, что обе службы используют один сетевой порт, 3389, который должен быть открыт в брандмауэре, чтобы можно было устанавливать сеанс удаленного помощника.

Пример из практики

Ваша компания активировала *Удаленный помощник* (Remote Assistance) на всех компьютерах в рамках корпоративной программы удаленного администрирования. Торговые представители вашей компании часто бывают в командировках и во время разъездов работают на мобильных компьютерах.

Во внутренней сети для прямой связи с клиентами и для работы с удаленным помощником применяется Windows Messenger. Однако интернет-трафик Instant Messenger запрещен, для чего на брандмауэре закрыт порт 1863.

Вы хотите предоставлять помощь удаленным пользователям, но не можете соединяться с ними через Windows Messenger, чтобы определять, подключены они к сети или нет.

Возможно ли в такой ситуации помогать удаленным пользователям средствами программы *Удаленный помощник* (Remote Assistance)? Если да, то как это реализовать?

Запросить помощь можно одним из следующих способов.

1. **По электронной почте.** Из *Центра справки и поддержки* отправьте сообщение эксперту. Щелкнув ссылку в письме, он сможет инициировать сеанс удаленного помощника.
2. **С помощью файла.** Создайте файл запрса удаленной помощи средствами *Центра справки и поддержки.* Отправьте его по электронной почте либо предоставьте доступ к нему через общий ресурс. Когда эксперт перейдет по ссылке в файле, он сможет инициировать сеанс удаленного помощника.

В обоих вариантах настоятельно рекомендуется создать пароль для сеанса удаленной помощи и сообщить его эксперту по защищенному каналу, чтобы исключить несанкционированный доступ к этому сеансу.

Практикум по устранению неполадок

Вы пытаетесь подключиться к серверу Windows Server 2003 в своей среде средствами программы *Подключение к удаленному рабочему столу* (Remote Desktop Connection), но постоянно получаете сообщение, показанное на рис. 2-9.

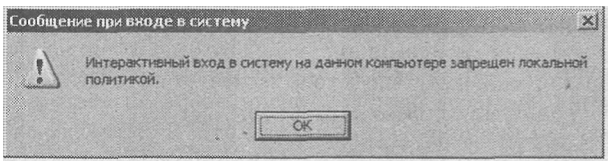


Рис. 2-9. Сообщение об ошибке входа в систему при подключении к консоли *Удаленный рабочий стол для администрирования*

Вы проверили параметры на сервере и убедились в следующем:

- вы участник группы *Пользователи удаленного рабочего стола* (Remote Desktop Users);
- вы не являетесь членом группы *Администраторы* (Administrators);
- вы можете подключаться к общим ресурсам на сервере терминалов, и тот отвечает на тестовые опросы, которые вы можете выполнить командой Ping.

Какие еще параметры вы проверите на сервере терминалов, чтобы устранить эту проблему?

Вероятно, данный сервер терминалов является контроллером домена, и активирована стандартная групповая политика контроллера домена, разрешающая удаленные подключения группе *Пользователи удаленного рабочего стола* (Remote Desktop Users). Локальная групповая политика на контроллерах домена запрещает удаленные подключения не под административными учетными записями, и ее следует изменить. Простейший способ изменения локальной политики — перекрыть ее стандартной групповой политикой контроллера домена.

Резюме главы

- Консоли MMC — базовый интерфейс для системных служебных программ в Windows Server 2003.
- Оснастки — это отдельные служебные программы, которые можно загружать в консоль MMC.
- Некоторые оснастки можно использовать для конфигурирования удаленных компьютеров, другие — только для доступа к локальному компьютеру.
- Консоли MMC можно сохранять в авторском (полный доступ) или в пользовательском (ограниченный доступ) режиме. Режим консоли MMC не ограничивает и не расширяет круг действий пользователей или их возможности доступа к ресурсам: все определяет авторизация и набор предоставленных разрешений.
- *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration) позволяет управлять удаленным сервером так же, как если бы вы запустили консоль на локальной системе.
- *Удаленный рабочий стол для администрирования* для настольных ОС доступен только в составе Windows XP.
- *Удаленный помощник* (Remote Assistance) позволяет взаимодействовать с удаленным рабочим столом так же, как *Удаленный рабочий стол для администрирования,* обеспечивая удаленный просмотр и управление компьютером с Windows XP.
- *Удаленный помощник* (Remote Assistance) также применим к серверам под управлением Windows Server 2003.

- В работе программы *Удаленный помощник* участвуют два пользователя: тот, кому помогают, — на одном компьютере, и эксперт-помощник — на другом. Оба пользователя должны согласовывать управляющие действия в ходе сеанса, причем сеанс может быть прерван каждой из сторон в любое время.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно. Вернитесь к тексту соответствующих занятий и просмотрите раздел «Дополнительная литература» в части 2, где приведены ссылки на необходимые источники по темам, затрагиваемым на экзамене.

Основные положения

- Консоли MMC — это контейнеры для оснасток.
- Оснастки можно использовать в локальном или удаленном контексте, но их нельзя подключить к локальному и удаленному компьютерам одновременно.
- Оснастки можно комбинировать в одной консоли согласно предпочтениям администратора.
- Консоли MMC можно сохранять в пользовательском режиме, чтобы ограничить возможности их конфигурирования, однако выполнение задач с помощью служебных программ регламентируется разрешениями, а не ограничениями в отношении конкретной консоли. Если у пользователя достаточно привилегий для администрирования компьютера, он может создавать консоли MMC с любыми оснастками.
- Для работы программы *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration) необходимы разрешения на подключение с помощью клиента *Дистанционное управление рабочим столом* (Remote Desktop). По умолчанию это разрешено только группе *Администраторы* (Administrators).
- *Удаленный помощник* (Remote Assistance) — это средство активации сеанса помощи по согласованию двух сторон. Без согласия пользователя эксперт не может управлять его компьютером.
- Порт 3389, также используемый программой *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration), должен быть открыт на брандмауэре, чтобы можно было инициировать сеансы удаленного помощника.

Основные термины

***Удаленный помощник* (Remote Assistance) и *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration).** *Удаленный помощник* позволяет инициировать сеанс удаленного управления со стороны эксперта в ответ на приглашение пользователя. Реквизиты для проверки подлинности предоставляются в форме общего секретного пароля, созданного, когда пользователь запрашивал помощь. В работе программы *Удаленный рабочий стол для администрирования* участвует лишь один пользователь, удаленно подключенный к компьютеру, на котором запущена служба *Сервер терминалов* (Terminal Server) и разрешены подключения с помощью программы *Дистанционное управление рабочим столом* (Remote Desktop).

Microsoft Management Console (MMC). Какие функции доступны при удаленном подключении консоли, и какие реквизиты необходимо предоставить для подключения.

***Удаленный рабочий стол для администрирования* ~ Remote Desktop for Administration.** Реквизиты и конфигурация сервера, необходимые для установления подключений средствами программы *Удаленный рабочий стол для администрирования*.

Вопросы и ответы

Занятие 1. Закрепление материала

1. В каком режиме по умолчанию создаются консоли MMC?

   Правильный ответ: по умолчанию консоли MMC создаются в авторском режиме (Author).

2. **Может ли** оснастка одновременно отображать информацию о локальном и удаленном компьютерах?

   Правильный ответ: нет. Оснастки можно настроить для подключения либо к локальному, либо к удаленному компьютеру.

3. Если требуется ограничить доступ к оснастке, как сконфигурировать содержащую ее консоль MMC?

   Правильный ответ: нужно сохранить консоль в одном из пользовательских режимов в **зависимости от требуемых условий ограничения доступа.**

Занятие 2. Закрепление материала

1. Какие реквизиты необходимы для администрирования удаленного компьютера из консоли MMC?

   Правильный ответ: для управления удаленным компьютером вы должны иметь на этом компьютере административные реквизиты.

2. Можно ли изменить контекст существующей оснастки MMC с локального на удаленный, или для удаленного подключения необходимо загружать в консоль MMC еще одну оснастку того же типа?

   Правильный ответ: контекст оснастки можно изменить, перенастроив ее свойства. Для изменения конфигурации оснастки ее не нужно повторно загружать в консоль.

3. **Все** ли функции оснастки, применяемые на локальном компьютере, можно использовать при удаленном подключении?

   Правильный ответ: нет, доступна не вся функциональность. Например, компонент Диспетчер устройств (Device Manager) в консоли Управление компьютером (Computer Management) можно использовать только для просмотра конфигурации удаленного компьютера, но изменять конфигурацию устройств на удаленном компьютере нельзя.

Занятие 3. Закрепление материала

1. Сколько одновременных подключений разрешено к серверу терминалов, работающему в режиме удаленного администрирования? Почему?

   Правильный ответ: три; два удаленных и одно — с локальной консоли (несправедливо, правда?). Значит, технически допускается лишь два подключения, поскольку вместе со

службой Сервер терминалов (Terminal Server), настроенной для удаленного администрирования в режиме Дистанционное управление рабочим столом (Remote Desktop), не устанавливаются компоненты для совместного использования приложений.

2. Как оптимальным образом предоставить администраторам возможность удаленного управления сервером через службы терминалов?
   a. Не выполнять никаких действий; они уже имеют доступ, поскольку являются администраторами.
   b. Удалить группу *Администраторы* (Administrators) из списка разрешений в подключении к серверу терминалов и поместить их административную учетную запись в группу *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration).
   c. Создать отдельную пользовательскую учетную запись с более низким уровнем авторизации для повседневного использования группой *Администраторы* (Administrators) и поместить ее в группу *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration).

   Правильный ответ: c. Лучше всего войти в систему под учетной записью с минимальными полномочиями, а затем запустить средства администрирования с реквизитами более высокого уровня с помощью команды Запуск от имени (Run As).

3. Какое программное средство используется на сервере для включения удаленного подключения к рабочему столу?
   a. *Диспетчер служб терминалов* (Terminal Services Manager).
   b. *Настройка служб терминалов* (Terminal Services Configuration).
   c. *Система* (System Properties) из Панели управления.
   d. *Лицензирование служб терминалов* (Terminal Services Licensing).

   Правильный ответ: c.

Занятие 4. Закрепление материала

1. В чем сходство программ *Удаленный помощник* (Remote Assistance) и *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration)? Чем они различаются?

   Правильный ответ: Удаленный **помощник (Remote Assistance) позволяет удаленно управлять компьютером, как если бы пользователь физически работал с консолью на сервере; то же касается и подключения к серверу терминалов средствами программы Удаленный рабочий стол для администрирования (Remote Desktop for Administration).**
   Средство Удаленный рабочий стол для администрирования (Remote Desktop for Administration) могут использовать лишь те учетные записи, локальные или доменные, которым разрешены подключения Сервер терминалов (Terminal Server) на данном компьютере. Удаленный помощник (Remote Assistance) требует подтверждать начало сеанса между пользователем и экспертом-помощником.

2. Какие выгоды приносит использование программы *Удаленный помощник* (Remote Assistance)?

   Правильный ответ: для получения помощи не требуется присутствия эксперта на месте. Теперь в массе случаев не придется по телефону решать проблему и консультировать пользователей.

3. Какие из перечисленных условий работы удаленного помощника связаны с брандмауэрами?
   a. Порт 3389 должен быть открыт.
   b. Нельзя использовать NAT.
   c. Нельзя использовать механизм *Общий доступ к подключению Интернета* (Internet Connection Sharing).
   d. Нельзя использовать программу *Удаленный помощник* (Remote Assistance) в виртуальной частной сети (VPN).

   Правильный ответ: a.

ГЛАВА 3

Учетные записи пользователей

Темы экзамена

- Создание и управление учетными записями пользователей.
- Создание и модификация учетных записей пользователей при помощи консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers).
- Создание и модификация учетных записей пользователей средствами автоматизации.
- Импорт учетных записей пользователей.
- Управление локальными, перемещаемыми и обязательными профилями пользователей.
- Устранение проблем с учетными записями пользователей.
- Обнаружение заблокированных учетных записей и их разблокирование.
- Диагностирование и устранение проблем со свойствами учетных записей пользователей.
- Устранение ошибок, связанных с проверкой подлинности пользователей.

В этой главе

Перед тем как сотрудники вашей компании смогут обращаться к нужным ресурсам, необходимо настроить проверку подлинности пользователей. Конечно, главный компонент проверки — личность пользователя, сведения о котором хранятся в виде учетной записи в службе каталогов Active Directory. Изучив эту главу, вы сможете проверить и расширить свои знания о создании, поддержке и устранении проблем с учетными записями пользователей и проверкой подлинности, а также познакомитесь с консолью *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) и мощными служебными программами, запускаемыми из командной строки.

Прежде всего

В этой главе обсуждаются навыки и концепции, относящиеся к учетным записям пользователей в Active Directory. Предполагается, что у вас есть минимум 18-месячный опыт работы с Active Directory, MMC и консолью *Active Directory — пользователи и компьютеры*. Для изучения материалов этой главы вам потребуются:

- компьютер под управлением Microsoft Windows Server 2003 (Standard или Enterprise), установленный как ServerOl и настроенный в качестве контроллера домена contoso.com;
- организационные подразделения (ОП) первого уровня: Administrative Groups, Employees и Security Groups;
- глобальные группы Sales Representatives и Sales Managers в ОП Security Groups;
- консоль *Active Directory — пользователи и компьютеры* или пользовательская консоль с такой оснасткой.

Занятие 1. Создание и управление объектами пользователей

Active Directory требует, чтобы перед разрешением доступа к ресурсам проводилась проверка подлинности пользователя на основе его учетной записи, которая содержит имя для входа в систему, пароль и уникальный *идентификатор безопасности* (security identifier, SID). В процессе входа в систему Active Directory проверяет подлинность имени и пароля. После этого подсистема безопасности может создать маркер доступа, представляющий этого пользователя. В маркере доступа содержатся SID учетной записи пользователя и SID всех групп, к которым относится пользователь. При помощи этого маркера можно проверить назначенные пользователю права, в том числе право локально входить в систему, а также разрешить или запретить доступ к ресурсам, защищенным *таблицами управления доступом* (access control list, ACL).

Учетная запись пользователя интегрирована в объект пользователя в Active Directory. В объекте пользователя хранятся не только имя, пароль и SID, но также контактная информация (например номера телефонов и адреса), организационная информация, в том числе должность, прямые подчиненные и руководитель, сведения о членстве в группах и конфигурации, например параметры перемещаемого профиля, служб терминалов, удаленного доступа и удаленного управления. На этом занятии вы узнаете, как объекты пользователей обрабатываются в Active Directory.

Изучив материал этого занятия, вы сможете:

- ✓ создавать объекты пользователей в Active Directory в консоли *Active Directory — пользователи и компьютеры;*
- ✓ настраивать параметры объектов пользователей;
- ✓ уяснить важные свойства учетных записей, назначение которых не совсем понятно из их названия;
- ✓ одновременно изменять свойства нескольких пользователей.

Продолжительность занятия — около 15 минут.

Создание объектов пользователей в консоли *Active Directory — пользователи и компьютеры*

Создать объект пользователя можно в консоли *Active Directory — пользователи и компьютеры*. Хотя их можно создавать в домене или в любом **из** контейнеров по умолчанию, рекомендуется делать это в ОП, чтобы **в** полной мере задействовать делегирование административных полномочий и объекты групповой политики (ОГП).

Чтобы создать объект пользователя, выберите нужный контейнер, затем в меню **Действие (Action)** щелкните **Создать (New)\Пользователь (User).** (Для этого вы должны быть членом групп *Администраторы предприятия* (Enterprise Admins), *Администраторы домена* (Domain Admins) или *Операторы учета* (Account Operators), либо вам должны быть делегированы административные полномочия. В противном случае команда создания будет недоступна.)

Откроется диалоговое окно **Новый объект — Пользователь (New Object—User),** показанное на рис. 3-1. На первой странице этого окна необходимо ввести сведения об имени пользователя (табл. 3-1).

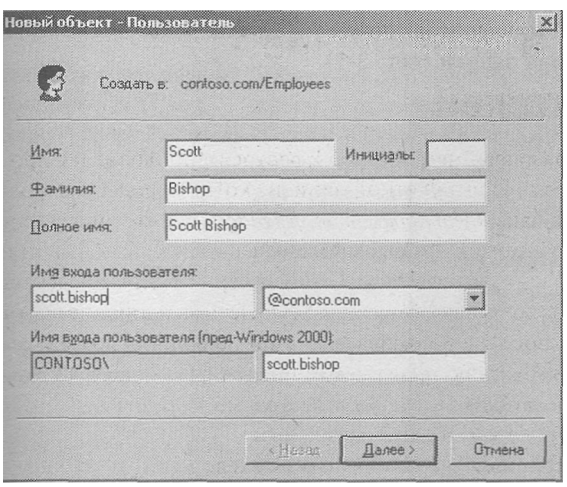


Рис. 3-1. Диалоговое окно *Новый объект — Пользователь*

Табл. 3-1. Свойства пользователя на первой странице окна *Новый объект — Пользователь*

Свойство	Описание
Имя (First Name)	Имя пользователя. Необязательное
Инициалы (Initials)	Инициалы (отчество) пользователя. Необязательное
Фамилия (Last Name)	Фамилия пользователя. Необязательное
Полное имя (Full Name)	Полное имя пользователя. Если вы указали имя или фамилию пользователя, значение этого свойства будет подставлено автоматически. Впрочем, можно изменить предложенное значение. Это обязательное поле. На основе введенного здесь имени генерируется несколько свойств объекта пользователя, в частности CN (обычное имя), DN (различающееся имя), name (имя) и displayName (отображаемое имя). Поскольку значение CN должно быть в контейнере уникальным, введенное здесь имя должно быть уникальным среди остальных объектов в ОП (или другом контейнере), где вы создаете объект пользователя

Табл. 3-1. *(окончание)*

Свойство	Описание
Имя входа пользователя (User Logon Name)	*Имя участника-пользователя* (user principal name, UPN) состоит из имени пользователя для входа и суффикса UPN, которым по умолчанию является DNS-имя домена, в котором вы создаете объект. Это свойство обязательно, а UPN-имя в целом (в формате имя_для_входа@суффикс_иРМ) должно быть уникальным в лесу Active Directory. Например, UPN-имя может быть таким: someone@contoso.com. UPN можно использовать для входа в систему Windows 2000/XP или Windows Server 2003
Имя входа пользователя (пред-Windows 2000) [User Logon Name (Pre-Windows 2000)]	Это имя используется для входа в систему с клиентов под управлением более ранних версий Windows, например Windows 9x/Me/NT 4 или Windows NT 3.51. Это поле является обязательным и должно быть уникальным в домене

Закончив ввод значений, щелкните **Далее (Next).** На второй странице окна **Новый объект — Пользователь (New Object—User)** необходимо ввести пароль пользователя и установить управляющие флажки учетной записи (рис. 3-2).

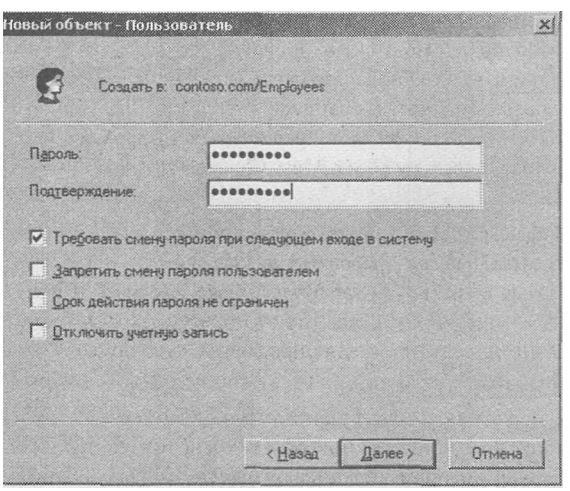


Рис. 3-2. Вторая страница окна *Новый объект — Пользователь*

Внимание! Политика учетных записей по умолчанию в домене Windows Server 2003, которая настраивается в ОГП Default Domain Policy, требует задания сложного пароля длиной не менее семи символов. Под сложностью понимается, что в пароле должны применяться символы трех или четырех типов: прописные и строчные буквы, цифры и специальные символы.

При работе с Windows Server 2003 в тестовой или лабораторной среде следует применять те же методики, что и в производственной сети. То есть при изучении этой книги для создаваемых учетных записей рекомендуется задавать надежные пароли (вам придется запоминать их для упражнений, требующих входа в систему под именами тестовых пользователей).

В табл. 3-2 перечислены свойства со второй страницы окна **Новый объект — Пользователь (New Object—User).**

Табл. 3-2. Свойства пользователя на второй странице окна *Новый объект — Пользователь*

Свойство	Описание
Пароль (Password)	Этот пароль будет использоваться для проверки подлинности пользователя. В целях безопасности пароль необходимо задавать всегда. Во время ввода символы будут скрыты
Подтверждение (Confirm Password)	Подтвердите пароль, набрав его еще раз
Требовать смену пароля при следующем входе в **систему (User Must Change Password At Next Logon)**	Установите этот флажок, если хотите, чтобы пользователь изменил пароль, введенный вами при первом входе в систему. Если вы выбрали **Срок действия пароля не ограничен (Password Never Expires),** изменить значение этого параметра нельзя. При выборе этого параметра флажок исключающего его параметра **Запретить смену пароля пользователем (User Cannot Change Password)** будет автоматически снят
Запретить смену пароля пользователем (User Cannot Change **Password)**	Установите этот флажок, если одной учетной записью в домене пользуются несколько человек [допустим, учетной записью *Гость* (Guest)] или если необходимо контролировать пароли учетной записи этого пользователя. Обычно этот параметр используется для управления паролями учетных записей служб. Его нельзя выбрать, если вы установили флажок **Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon)**
Срок **действия пароля не ограничен (Password Never Expires)**	Установите этот флажок, если хотите, чтобы срок действия пароля не истекал. При этом флажок **Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon)** будет автоматически снят, так как это взаимоисключающие параметры. Обычно используется для управления паролями учетных записей служб
Отключить учетную запись (Account is disabled)	Установите этот флажок для отключения учетной записи пользователя, допустим, при создании объекта для только что нанятого сотрудника, которому пока не требуется входить в сеть

На заметку При создании объектов новых пользователей для каждого из них выбирайте уникальные сложные пароли, не отвечающие какому-либо предсказуемому шаблону. Включите параметр, который заставляет пользователя сменить пароль при следующем входе в систему. Если пользователь не будет входить в сеть долгое время, отключите его учетную запись. Когда пользователю в первый раз потребуется доступ к сети, убедитесь, что его учетная запись включена. Система попросит пользователя задать новый уникальный пароль, известный только ему.

Некоторые из параметров учетных записей, перечисленных в табл. 3-2, могут противоречить политикам, настроенным в домене. Например, в политике домена по умолчанию хранение паролей с использованием обратимого шифрования выключено. Однако в редких случаях, требующих обратимого шифрования, значение свойства учетной за-

писи **Хранить пароль, используя обратимое шифрование (Store Password Using Reversible Encryption)** для данного объекта пользователя будет иметь приоритет. Также в домене может быть указан максимальный срок действия пароля, или пользователь должен будет изменить пароль при следующем входе в систему. Если объект пользователя настроен так, что срок действия пароля не ограничен, эти настройки перекроют политики домена.

Управление объектами пользователей из консоли *Active Directory — пользователи и компьютеры*

При создании объекта пользователя требуется настроить общие свойства пользователя, в том числе имена для входа и пароль. На самом деле объекты пользователей поддерживают множество различных свойств, которые вы можете в любой момент настроить при помощи консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers). Эти свойства упрощают управление объектами и их поиск.

Чтобы настроить свойства объекта пользователя, выберите объект и в контекстном меню или в меню **Действие (Action)** щелкните **Свойства (Properties).** Откроется окно **Свойства (Properties)** для этого объекта пользователя (рис. 3-3).

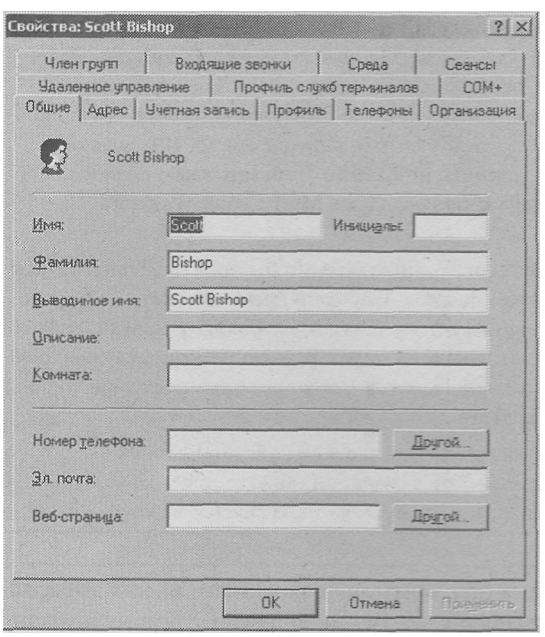


Рис. 3-3. Диалоговое окно *Свойства* для объекта пользователя

Свойства на вкладках этого окна разбиты на несколько основных категорий.

- **Свойства учетной записи: вкладка Учетная запись (Account).** Некоторые из этих свойст! настраиваются при создании объекта пользователя, в том числе имена для входа пароль и управляющие флаги учетной записи.
- **Личная информация: вкладки Общие (General), Адрес (Address), Телефоны (Telephones и Организация (Organization).** На вкладке **Общие** перечислены свойства учетного имени, которые настраивают при создании объекта пользователя.

- **Управление настройками пользователя: вкладка Профиль (Profile).** Здесь можно указать путь к профилю пользователя, сценарий входа и местоположение домашних папок.
- **Членство в группах: вкладка Член групп (Member Of).** Можно добавить и удалить группы пользователей, а также выбрать основную группу для пользователя.
- **Службы терминалов: вкладки Профиль служб терминалов (Terminal Services Profile), Среда (Environment), Удаленное управление (Remote Control) и Сеансы (Sessions).** Здесь можно настраивать и управлять работой пользователя во время сеанса служб терминалов.
- **Удаленный доступ: вкладка Входящие звонки (Dial-in).** Предназначена для включения и настройки разрешения на удаленный доступ.
- **Приложения: вкладка COM+.** Назначает пользователю наборы разделов Active Directory COM+. Эта новая функция Windows Server 2003 помогает управлять распределенными приложениями.

Свойства учетной записи

Особого внимания заслуживают свойства учетной записи пользователя на вкладке **Учетная запись (Account)** диалогового окна **Свойства (Properties)** пользователя (рис. 3-4).

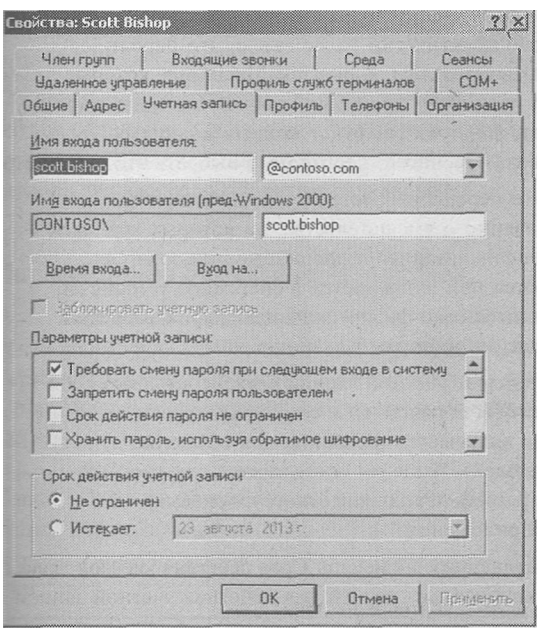


Рис. 3-4. Вкладка *Учетная запись* для объекта пользователя

Некоторые из этих свойств описаны в табл. 3-2. Они были настроены при создании объекта пользователя, и их, как и большой набор других свойств учетной записи, можно изменить на вкладке **Учетная запись (Account).** Значения некоторых свойств не совсем очевидны, они описаны в табл. 3-3.

Табл. 3-3. Свойства учетной записи пользователя

Свойство	Описание
Время входа (Logon Hours)	Щелкните **Время входа (Logon Hours),** чтобы настроить время, когда пользователю разрешено входить в сеть
Вход на (Log On To)	Щелкните **Вход на (Log On To),** если хотите запретить пользователю входить в систему с некоторых рабочих станций. В других разделах интерфейса это называется **Ограничения компьютера (Computer Restrictions).** Чтобы при помощи этой функции ограничивать возможности пользователей, необходимо включить передачу NetBIOS поверх TCP/IP, так как ограничение применяется к имени компьютера, а не к MAC-адресу (Media Access Control) его сетевой платы
Хранить пароль, используя обратимое шифрование (Store Password Using Reversible Encryption)	Этот параметр, который разрешает хранение пароля в Active Directory без использования мощного алгоритма для необратимого шифрования хешированием, предназначен для поддержки приложений, которым требуется знать пароль пользователя. Если в этом нет крайней необходимости, не включайте этот параметр, так как он существенно ослабляет безопасность пароля. Пароли, которые хранятся с использованием обратимого шифрования, — это практически то же самое, что пароли, записанные открытым текстом. Клиентам Macintosh, которые подключаются по протоколу AppleTalk, необходимо знать пароль пользователя. Если пользователь будет входить в систему при помощи клиента Macintosh, необходимо выбрать этот параметр
Для интерактивного входа в сеть нужна смарт-карта (Smart Card Is Required For Interactive Logon)	Смарт-карты — это переносные устройства, защищенные от несанкционированного вмешательства, на которых хранится уникальная идентификационная информация пользователя. Они присоединяются или вставляются в системное устройство и являются дополнительным физическим идентификационным компонентом процесса проверки подлинности
Учетная запись доверена для делегирования (Account Is Trusted For Delegation)	Этот параметр позволяет учетной записи службы выдавать себя за пользователя, чтобы обращаться к сетевым ресурсам от его имени. Обычно не включается (особенно для объектов, представляющих людей). Чаще он используется для учетных записей служб в трехуровневых (или многоуровневых) инфраструктурах приложений
Срок действия учетной записи (Account Expires)	При помощи управляющих элементов **Срок действия учетной (Account Expires)** задается дата окончания действия учетной записи

Одновременное управление свойствами нескольких учетных записей

Windows Server 2003 позволяет одновременно изменять свойства нескольких учетных записей пользователей. Достаточно выбрать несколько объектов пользователей (например, удерживая клавишу Ctrl) и в меню **Действие (Action)** щелкнуть **Свойства (Properties).** Можно выбирать только однотипные объекты, например только пользователей.

Для нескольких объектов пользователей одновременно можно изменить следующие свойства.

- Вкладка **Общие (General):** свойства **Описание (Description), Комната (Office), Номер телефона (Telephone Number), Факс (Fax), Веб-страница (Web Page), Адрес электронной почты (E-mail).**
- Вкладка **Учетная запись (Account):** свойства **Суффикс UPN (UPN Suffix), Время входа (Logon Hours), Вход на (Logon Workstations), Параметры учетной записи (Account Options), Срок действия учетной записи истекает (Account Expires).**
- Вкладка **Адрес (Address):** свойства **Улица (Street), Почтовый ящик (PO Box), Город (City), Штат/Область (State/Province), Почтовый индекс (ZIP/Postal Code), Страна/Регион (Country/Region).**
- Вкладка **Профиль (Profile):** свойства **Путь к профилю (Profile Path), Сценарий входа (Logon Script)** и **Домашняя папка (Home Folder).**
- Вкладка **Organization (Организация):** свойства **Должность (Title), Отдел (Department), Организация (Company), Руководитель (Manager).**

Совет Вы обязательно должны знать, какие свойства можно изменить одновременно для нескольких пользователей. Сценарии экзаменов, в которых требуется максимально быстро изменить свойства нескольких объектов пользователей, часто предназначены для проверки того, насколько четко вы представляете себе работу с несколькими объектами.

Остается еще множество свойств, которые для каждого пользователя должны настраиваться отдельно. Кроме того, определенные административные задачи, в том числе изменение паролей и переименование учетных записей, также должны выполняться отдельно для каждого объекта пользователя.

Перемещение объекта пользователя

Если пользователь переводится на другую должность, вам может понадобиться переместить его объект, чтобы отразить изменения в управлении или настройках объекта: выберите его в *Active Directory — пользователи и компьютеры* (Active Directory Users and Computers) и в контекстном меню или в меню **Действие (Action)** щелкните **Переместить (Move).**

Совет Одна из новых возможностей Windows Server 2003 — поддержка в консолях операций перетаскивания (drag-and-drop). Можно перемещать объекты между ОП, просто перетаскивая их в консоли *Active Directory — пользователи и компьютеры.*

Лабораторная работа. **Создание и управление объектами пользователей**

На этой лабораторной работе вы создадите три объекта пользователей и измените их свойства.

Упражнение 1. Создание объектов пользователей

1. Войдите на ServerOl как *Администратор* (Administrator).
2. Откройте консоль *Active Directory — пользователи и компьютеры.*

3. Выберите ОП Employees.
4. Создайте учетную запись пользователя со следующей информацией, причем задайте надежный пароль:

Поле	Введите
Имя (First Name)	**Dan**
Фамилия (Last Name)	Holme
Имя входа пользователя (User Logon Name)	**Dan.Holme**
Имя входа пользователя (пред-Windows 2000) [User Logon Name (Pre-Windows 2000)]	Dholme

5. Создайте второй объект пользователя со следующими свойствами:

Поле	Введите
Имя (First Name)	Hank
Фамилия (Last Name)	Carbeck
Имя входа пользователя (User Logon Name)	Hank.Carbeck
Имя входа пользователя (пред-Windows 2000) [User Logon Name (Pre-Windows 2000)]	Hcarbeck

6. Создайте объект пользователя для себя, следуя тем же соглашениям для имен входа, что и для двух предыдущих объектов.

Упражнение 2. Изменение свойств объекта пользователя

1. Откройте окно **Свойства (Properties)** для вашего объекта пользователя.
2. Задайте подходящие свойства объекта пользователя на вкладках **Общие (General), Адрес (Address), Профиль (Profile), Телефоны (Telephones)** и **Организация (Organization).**
3. Изучите остальные свойства, связанные с вашим объектом пользователя, но пока не изменяйте их.
4. Щелкните ОК.

Упражнение 3. Изменение свойств нескольких объектов пользователей

1. Раскройте *Active Directory — пользователи и компьютеры* и перейдите к ОП Employees Contoso.com. Выберите ОП Employees в дереве: справа будут перечислены объекты пользователей, которые вы создали в упражнении 1.
2. Щелкните объект пользователя Dan Holme.
3. Удерживая клавишу Ctrl, щелкните объект пользователя Hank Carbeck.
4. В меню **Действие (Action)** выберите **Свойства (Properties).**
5. Обратите внимание на различия между появившимся окном и более подробным окном свойств, с которым вы работали в упражнении 2. Изучите свойства, доступные при выборе нескольких объектов, но не изменяйте их.

6. Задайте следующие свойства для двух объектов пользователей:

Вкладка	Поле	Введите
Общие (General)	**Описание (Description)**	Научил меня всему, что необходимо знать о Windows Server 2003
Общие (General)	**Номер телефона (Telephone Number)**	(425) 555-0175
Общие (General)	**Веб-страница (Web Page)**	*http://www.microsoft.com/mspress*
Адрес (Address)	**Улица (Street)**	One Microsoft Way
Адрес (Address)	**Город (City)**	Redmond
Адрес (Address)	**Область/край (State/Province)**	Washington
Адрес (Address)	**Почтовый индекс (ZIP/Postal Code)**	98052
Организация (Organization)	**Должность (Title)**	Писатель
Организация (Organization)	**Организация (Company)**	Microsoft Press

7. Щелкните **OK**.
8. Откройте окно свойств для объекта Dan Holme.
9. Удостоверьтесь, что свойства, которые вы задали на шаге 6, действительно были применены к объекту. Щелкните OK.
10. Щелкните объект пользователя Dan Holme.
11. Удерживая клавишу Ctrl, щелкните объект пользователя Hank Carbeck. Щелкните меню **Действие (Action).**
12. Заметьте: при выборе нескольких объектов пользователей команда **Смена пароля (Reset Password)** недоступна. Какие еще команды недоступны, если выбрано несколько объектов? Поэкспериментируйте, открывая меню **Действие (Action),** когда выбран один или два пользователя.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Вы настраиваете объекты пользователей в своем домене с помощью консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) и можете изменять свойства адреса и номера телефона для объекта представляющего вас пользователя. Однако команда **Новый пользователь (New User)** недоступна. В чем причина?
2. Вы создаете набор объектов пользователей для временных сотрудников организации. Они будут работать по контракту ежедневно с 9:00 до 17:00. Работа начнется через месяц, а закончится через два месяца с сегодняшнего числа. Эти сотрудники не будут работать в неурочное время. Какие из следующих свойств следует сразу настроить, чтобы гарантировать максимальную безопасность объектов этих пользователей?
   a. **Пароль (Password).**
   b. Время входа (Logon Hours).
   c. Срок действия учетной записи (Account Expires).

d. **Хранить пароль, используя обратимое шифрование (Store password using reversible encryption).**
e. **Учетная запись доверена для делегирования (Account is trusted for delegation).**
f. Требовать **смену пароля при следующем входе в систему (User must change password at next logon).**
g. **Отключить учетную запись (Account is disabled).**
h. **Срок действия пароля не ограничен (Password never expires).**

3. Какие из следующих свойств и административных задач можно настраивать или изменять одновременно для нескольких объектов пользователей?
   a. **Фамилия (Last Name).**
   b. **Имя входа пользователя (User Logon Name).**
   c. **Disable Account (Отключить учетную запись).**
   d. **Включить учетную запись (Enable Account).**
   e. **Смена пароля (Reset Password).**
   f. **Срок действия пароля не ограничен (Password Never Expires).**
   g. **Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon).**
   h. **Время входа (Logon Hours).**
   i. **Ограничения компьютера (Рабочие станции для входа в систему) [Logon Workstations (Computer Restrictions)].**
   j. **Должность (Title).**
   k. **Прямые подчиненные (Direct Reports).**

Резюме

- Чтобы создавать объекты пользователей, вы должны быть членом групп *Администраторыпредприятия*(EnterpriseAdmins),*Администраторыдомена*(DomainAdmins) или *Операторы учета* (Account Operators), либо вам должны быть делегированы административные полномочия.
- Объекты пользователей содержат свойства, обычно связанные с учетной записью пользователя, в том числе имена для входа и пароль, а также уникальный для каждого пользователя идентификатор безопасности (SID).
- Кроме того, объекты пользователей включают свойства, относящиеся к представляемому ими человеку: личную информацию, членство в группах и административные настройки. Некоторые из этих свойств Windows Server 2003 позволяет одновременно изменять для нескольких пользователей.

Занятие 2. Создание нескольких объектов пользователей

Иногда требуется быстро создать множество объектов пользователей, например для целого класса новых учащихся в школе или группы новых сотрудников организации. В таких ситуациях необходимо знать, как эффективно упростить или автоматизировать создание объектов пользователей, чтобы не создавать учетные записи по одной. На занятии 1 вы научились создавать и управлять объектами пользователей с помощью кон-

соли *Active Directory — пользователи и компьютеры* (Active Directory Users and Computers). На этом занятии вы научитесь создавать объекты пользователей при помощи шаблонов, импортированных объектов и сценариев командной строки.

Изучив материал этого занятия, вы сможете:

- ✓ создавать и использовать шаблоны объектов пользователей;
- ✓ импортировать объекты пользователей из файлов с разделителем — запятой;
- ✓ использовать новые инструменты командной строки для создания и управления объектами пользователей.

Продолжительность занятия — около 15 минут.

Создание и использование шаблонов объектов пользователей

Очень часто объекты обладают одинаковыми свойствами. Например, все торговые представители могут принадлежать одной группе безопасности, им всем может быть разрешен вход в систему в одно и то же время, а их домашние папки и перемещаемые профили могут храниться на одном сервере. В таких случаях при создании объекта пользователя полезно предварительно задать для него общие свойства. Для этого можно создать общий объект пользователя, часто называемый *шаблоном,* и копировать его, создавая новые объекты пользователей.

Чтобы сгенерировать шаблон, создайте объект пользователя и настройте его свойства. Поместите пользователя в требуемые группы.

Внимание! Чтобы гарантировать, что эта учетная запись не будет использована для доступа к сетевым ресурсам, обязательно отключите данного пользователя, так как это всего лишь шаблон.

Для создания объекта пользователя укажите нужный шаблон и в меню **Действие (Action)** щелкните **Копировать (Copy).** Вам потребуется задать некоторые свойства, как при создании нового объекта пользователя: имя и фамилию, инициалы, имя входа, пароль и параметры учетной записи. После создания объекта вы увидите, что свойства были скопированы из шаблона согласно следующему алгоритму для вкладок:

- **Общие (General)** — свойства не копируются;
- **Адрес (Address)** — копируются все свойства, кроме **Улица (Street);**
- **Учетная запись (Account)** — копируются все свойства, кроме имени входа, которое вам будет предложено ввести при копировании шаблона;
- **Профиль (Profile)** — копируются все свойства, а пути к профилю и домашней папке изменяются в соответствии с именем для входа нового пользователя;
- **Телефоны (Telephones)** — свойства не копируются;
- **Организация (Organization)** — копируются все свойства, кроме **Должность (Title);**
- **Член групп (Member Of)** — копируются все свойства;
- **Входящие звонки (Dial-in), Среда (Environment), Сеансы (Sessions), Удаленное управление (Remote Control), Профиль служб терминалов (Terminal Services Profile), COM+** — свойства не копируются.

Совет Пользователь, объект которого был сгенерирован путем копирования шаблона, по умолчанию участвует в тех же группах, что и шаблон, то есть получает разрешения и права, назначенные этим группам. Однако разрешения и права, назначенные самому шаблонному объекту пользователя, не копируются и не переназначаются, поэтому у объектов пользователей, генерируемых по шаблону, их не будет.

Импорт объектов пользователей при помощи CSVDE

CSVDE — это средство командной строки, позволяющее импортировать и экспортировать объекты в Active Directory из/в текстовый файл с разделителями — запятыми, формат которого широко распространен и читается такими программами, как *Блокнот* (Notepad) и Microsoft Excel. Эта команда представляет собой мощный инструмент для быстрой генерации объектов. Ее базовый синтаксис таков:

```
csv-{}-de [-ij [-f имя_файла] [-k]
```

где:
-i — включает режим импорта; если не указан, по умолчанию включается режим экспорта;
-f *имя_файла* — указывает имя импортируемого файла;
-к — во время импорта игнорирует ошибки, в том числе *объект уже существует, нарушение ограничения* и *атрибут или значение уже существует,* и продолжает обработку.

Импортируемый файл является текстовым файлом с разделителями — запятыми (*.csv или *.txt), где первая строка представляет собой список имен в формате протокола LDAP для импортируемых атрибутов, вслед за которой на отдельных строках перечисляются все объекты. Для каждого объекта должны быть указаны в точности те атрибуты, которые перечислены в первой строке. Например, файл может быть таким:

```
DN,objectClass,sAMAccountName,sn,givenName, userPrincipalName
"CN=Scott Bishop,OU=Employees, DC=contoso,DC=com",
user,sbishop,Bishop,Scott,scott.bishop@contoso.com
```

Если импортировать этот файл, то в ОП Employees будет создан объект пользователя с именем Scott Bishop. Имена для входа, имя и фамилия задаются согласно данным из файла. Первоначально этот объект будет отключен, включить его можно после смены пароля.

Примечание Подробнее о команде CSVDE, ее параметрах и способах применении для экспорта объектов каталога — в *Центре справки и поддержки* (Help and Support Center) Windows Server 2003. Команда LDIFDE, которая также подробно рассматривается в справке, позволяет импортировать и экспортировать учетные записи с использованием форматов LDAP. Эта команда и ее файловая структура не столь интуитивно понятна администраторам, как CSV-файлы, поддерживаемые CSVDE.

Использование средств командной строки Active Directory

Windows Server 2003 поддерживает множество мощных средств командной строки, упрощающих управление Active Directory:

- DSADD — добавляет объекты в каталог;
- DSGET — отображает («получает») свойства объектов каталога;

- DSMOD — изменяет выбранные атрибуты существующего объекта каталога;
- DSMOVE — перемещает объект из текущего контейнера в новое местоположение;
- DSRM — удаляет объект или все дерево ниже объекта по иерархии, либо удаляет и объект, и дерево;
- DSQUERY — запрашивает в Active Directory объекты, отвечающие указанным условиям поиска; эту команду часто используют для создания списка объектов, который затем передается по каналу другому средству командной строки для анализа или модификации.

В параметрах этих команд используются следующие компоненты (один или несколько).

- **Тип целевого объекта.** Одно из предопределенных значений, соответствующих классу объекта в Active Directory. Например: computer (компьютер), user (пользователь), OU (ОП), group (группа) и server (сервер, то есть контроллер домена).
- **Идентификатор целевого объекта.** *Различающееся имя* (distinguished name, DN) объекта, в отношении которого выполняется команда. DN объекта — это атрибут каждого объекта, представляющий его имя и местоположение в лесу Active Directory. Например, в упражнении 1 первого занятия вы создали объект пользователя с таким DN: CN=Dan Holme, OU=Employees, DC=Contoso, DC=com.

  Примечание Указывая DN в качестве параметра команды, заключайте имя в кавычки, если оно содержит пробелы. Если подкомпонент DN содержит обратную косую черту или запятую, обратитесь к указанной далее теме оперативной справки.

- **Сервер.** Можно указать контроллер домена, в отношении которого выполняется команда.
- **Пользователь.** Можно указать имя пользователя и пароль, с которыми следует выполнить команду. Это удобно, если вы вошли в систему не с административными реквизитами, но хотите выполнить команду с реквизитами более высокого уровня.

Кроме того, в параметрах регистр букв не различается, и их можно указывать после дефиса («-») или косой черты («/»).

Примечание На этом занятии мы сфокусируемся на наиболее типичных командах и параметрах и на применении этих команд к объектам пользователей. Чтобы подробнее узнать об этих средствах и получить полный список параметров выполните в справке поиск по фразе **«средства командной строки службы каталогов» («directory service command-line tools»)** и обязательно заключите фразу в кавычки. Щелкнув кнопку **Найти (Search),** вы увидите справочник по командной строке в перечне разделов на панели **Результаты** поиска **(Search Results).**

Команда DSQUERY

Команда DSQUERY запрашивает в Active Directory объекты, отвечающие указанному набору условий. Ее базовый синтаксис таков:

```
dsquery тип_объекта [{начальный_узел | forestroot | domainroot}] [-o {dn |
rdn | samid}]
[-scope {subtree | onelevel | base}] [-name имя] [-desc описание] [-upn UPN]
[ - samid имя_SAM] [-inactive число_недель] [-stalepwd число_дней] [-disabled]
[{-s сервер [ -d домен}] [-u имя_пользователя] [-p {пароль | *}]
```

Совет Помните, что эта команда будет часто использоваться для генерации списка объектов, в отношении которых будут выполняться другие средства командной строки. Это достигается за счет пересылки по каналу выходных данных второй команде. Например, следующая команда запрашивает в Active Directory объект пользователя, имя которого начинается с «Dan» и передает набор результатов команде DSMOD, которая отключает все объекты из этого набора:

```
dsquery user -name Dan* | dsmod user -disabled yes
```

Совет Прочие средства принимают на входе DN-имена, которые также являются выходным типом по умолчанию.

Основные параметры для команды DSQUERY перечислены в табл. 3-4.

Табл. 3-4. Параметры для команды DSQUERY

Параметр	Описание
Область запроса	
тип_объекта	Необходимый параметр. Тип объекта представляет класс(ы) объектов, среди которых будет производиться поиск. Можно указывать типы объектов computer (компьютер), contact (контакт),' group (группа), OU (ОП), server (сервер), user (пользователь) или использовать групповой символ «*» для представления всех классов объектов. На данном занятии мы используем эту команду для получения объектов пользователей
{начальный_узел forestroot | domainroot}	Необязательный параметр. Указывает узел, с которого начинается поиск. Можно указать корень леса (forestroot), корень домена (domainroot) или различающееся имя узла *(начальный_узел).* Если задан корень леса, поиск будет выполняться в глобальном каталоге. Значение по умолчанию — domainroot
-scope {subtree | onelevel | base}	Задает область поиска. Значение subtree (поддерево) задает в качестве области поддерево с корнем в начальном узле. Значение onelevel (один уровень) задает поиск только в дочерних объектах первого уровня, считая от начального узла. Значение base (база) задает поиск в одном объекте, представленном как начальный узел. Если *начальный_узел* — forestroot (корень леса), единственная допустимая область поиска — subtree (поддерево). Область поиска по умолчанию — subtree
Вывод набора результатов	
-o {dn, rdn, samid}	Определяет формат вывода списка записей, найденных в результате поиска. Значение dn задает отображение различающегося имени каждой записи. Значение rdn задает отображение относительного различающегося имени каждой записи. Значение samid задает отображение имени учетной записи SAM (Security Accounts Manager) каждой записи. Формат по умолчанию — dn

Табл. 3-4. *(окончание)*

Параметр	Описание
Условие запроса	
-name *имя*	Ищет объекты пользователей, у которых атрибуты имени (значение атрибута CN) соответствуют имени. Можно использовать метасимволы, например «jon*» или «*ith» или «j*th»
-desc *описание;*	Ищет пользователей, атрибут описания которых соответствует значению описания. Можно использовать метасимволы
-upn *UPN*	Ищет пользователей, атрибут UPN которых совпадает с указанным UPN
-samid *имя_SAM;*	Ищет пользователей, имя учетной записи SAM которых соответствует значению *имя_SAM.* Можно использовать метасимволы
-inactive *число недель*	Ищет всех пользователей, которые не входили в систему указанное количество недель
-stalepwd *числодней*	Ищет всех пользователей, которые не изменяли свои пароли в течение указанного количества дней
-disabled	Ищет всех пользователей, учетные записи которых отключены
Контроллер домена и реквизиты, используемые в команде	
{-s *сервер* | -d *домен};*	Подключается к указанному удаленному серверу или домену
-и *имя_пользователя;*	Задает имя пользователя для входа на удаленный сервер. По умолчанию параметр -и использует имя, под которым пользователь вошел в систему. Имя пользователя можно указать в любом из следующих форматов: • имя пользователя (например Linda); • домен\имя пользователя (например, *widgets\Linda);* • имя участника-пользователя (UPN) (например *Linda@widgets.microsoft.com)*
-p {*пароль* \ *}.	Задает использование пароля или звездочки (*) для входа на удаленный сервер. Если вы введете *, появится окно с просьбой ввести пароль

Совет Период неактивности измеряется неделями, а периоды времени между изменениями пароля — днями.

Команда DSADD

Команда DSADD предназначена для создания объектов в Active Directory. Для создания Объекта пользователя используйте команду DSADD USER. Параметры DSADD позво-[юпот настраивать определенные свойства объекта. Значение параметров интуитивно ронятно, однако при желании вы можете получить их подробное описание в справке Windows Server 2003. Базовый синтаксис таков:

dsadduser*DN_пользователя...*

Параметр *DN пользователя...* — это одно или несколько различающихся имен для новых объектов пользователей. Если в DN есть пробел, заключите все имя в кавычки. Параметр *DN_пользователя...* можно вводить следующими способами:

- передача по каналу списка DN-имен, полученного при выполнении другой команды, например DSQUERY;
- указание всех DN-имен в командной строке через пробел;
- без указания параметра DN: тогда вы сможете ввести все DN-имена по одному с клавиатуры в ответ на приглашение команды. Нажимайте Enter после ввода каждого DN. После ввода последнего DN нажмите Ctrl+Z и затем Enter.

Для команды DSADD USER после DN можно указать следующие необязательные параметры.

- -samid имя_*SAM;*
- -upn *UPN;*
- -fn *имя;*
- -mi *инициал* (отчество);
- -ln *фамилия;*
- -display *отображаемое_имя;*
- -empid *идентификатор_сотрудника;*
- -pwd {*пароль* | *}, где * обозначает ввод пароля по запросу;
- -desc *описание;*
- -memberof *DN_группы;...* ;
- -office *комната;*
- -tel *номер_телефона;*
- -email *адрес_электронной_почты;*
- -hometel *номер_домашнего_телефона;*
- -pager *номер_пейджера;*
- -mobile *номер_сотового_телефона;*
- -fax *номер_факса;*
- -iptel *номер_IP-телефона;*
- -webpg *Web-страница;*
- -title *должность;*
- -dept *отдел;*
- -company *организация;*
- -mgr *DN_руководителя;*
- -hmdir *домашний_каталог;*
- -hmdrv *буква_диска: ;*
- -profile *путь к профилю;*
- -loscr *путь_к_сценарию;*
- -mustchpwd {yes | no};
- -canchpwd {yes | no};
- -reversiblepwd {yes | no};
- -pwdneverexpires {yes | no};
- -acctexpires *число дней;*
- -disabled {yes | no}.

Так же, как для команды DSQUERY, можно добавить параметры -s, -u и -p, чтобы указать контроллер домена, для которого будет выполнена DSADD, а также имя и пароль пользователя (реквизиты), с которыми будет выполняться эта команда:

- {-s *сервер* | -d *домен};*
- -u *имя пользователя;*
- -p {*пароль* | *}.

Имя учетной записи SAM в значениях параметров -email, -hmdir, -profile и -webpg можно заменять специальным маркером $username$ (в нем не различаются прописные и строчные буквы). Например, если имя учетной записи SAM равно Denise, параметр -hmdir можно записать в любом из следующих форматов:

- -hmdir\users\Denise\home;
- -hmdir\users\$username$\home.

Команда DSMOD

Команда DSMOD изменяет свойства одного или нескольких существующих объектов.

```
dsmod user DN_пользователя ... параметры
```

Эта команда воспринимает параметр *DN_пользователя...* точно так же, как команда DSADD, и для нее указываются те же параметры. Но, конечно, вместо добавления объекта с определенными свойствами она модифицирует существующий объект. Обратите внимание на исключения: при помощи команды DSMOD USER нельзя изменять *имя_SAM* (параметр -samid) и членство в группах (параметр -memberof) объекта пользователя. Для изменения членства в группах из командной строки можно воспользоваться командой DSMOD GROUP, которая рассматривается в главе 4.

Для команды DSMOD также можно указать параметр -c, который включает непрерывный режим DSMOD, когда команда выдает отчеты, об ошибках, но продолжает модифицировать объекты. Если параметр -c не указан, DSMOD прекратит выполняться после первой ошибки.

Команда DSGET

Команда DSGET получает и выводит выбранные свойства одного или нескольких существующих объектов. Ее базовый синтаксис таков:

```
dsget user DN_пользователя ... параметры
```

Эта команда воспринимает параметр *DN_пользователя...* точно так же, как DSADD, и для нее указываются те же параметры, за исключением того, что DSGET принимает только параметр, но не связанное с ним значение. Например, DSGET поймет параметр -samid, но не пару, состоящую из параметра и значения: -samid имя_*SAM*. Причина проста: вы всего лишь отображаете, а не добавляете и не изменяете свойство. Кроме того, DSGET не поддерживает параметр -password, так как она не может отображать пароли. Для DSGET можно указывать параметры -dn и -sid, которые отображают, соответственно, различающееся имя и SID объекта пользователя.

Подготовка к экзамену Необходимо понимать разницу между DSQUERY и DSGET. Команда DSQUERY находит и возвращает набор объектов согласно условию поиска, где описаны свойства. Команда DSGET возвращает свойства одного или нескольких указанных объектов.

Команда DSMOVE

Команда DSMOVE предназначена для перемещения или переименования объекта в домене. Перемещать объекты между доменами при помощи этой команды нельзя. Ее базовый синтаксис таков:

dsmove *DN_объекта* [-newname *новое_имя]* [-newparent *DN_родителя]*

DSMOVE также поддерживает параметры -s, -u и -p, описанные в разделе, посвященном DSQUERY.

Объект указывается по его различающемуся имени в параметре *DN объекта*. Чтобы переименовать объект, укажите для него новое обычное имя в параметре *новое_имя*. Если вы укажете различающееся имя контейнера в параметре *DN_родителя,* объект будет перемещен в этот контейнер.

Команда DSRM

Команда DSRM предназначена для удаления объекта, его поддерева или объекта вместе с поддеревом. Ее базовый синтаксис таков:

dsrm *DN_объекта ...* [-subtree [- exclude]] [-noprompt] [-c]

DSRM поддерживает параметры -s, -u и -p, описанные в разделе, посвященном DSQUERY.

Объект указывается по его различающемуся имени в параметре *DN_объекша.* Параметр -subtree говорит DSRM, что, если объекты являются контейнерами, необходимо удалить их содержимое. Параметр -exclude исключает из рассмотрения сам объект, и его можно использовать только с параметром -subtree. Если указаны параметры -subtree и -exclude, то содержимое ОП и его поддерево будут удалены, но ОП останется нетронутым. По умолчанию, если параметры -subtree или -exclude не указаны, удаляется только сам объект.

Удаление каждого объекта придется подтвердить, если только вы не зададите параметр -noprompt. Параметр -c включает непрерывный режим DSRM, когда команда выдает отчеты об ошибках, но продолжает обрабатывать дополнительные объекты. Если параметр -c не указан, процесс прекратится после первой ошибки.

Лабораторная работа. **Создание нескольких объектов пользователей**

На этой лабораторной работе вы создадите и настроите объекты пользователей при помощи шаблонов и средств командной строки.

Упражнение 1. Создание шаблона объекта пользователя

1. Войдите на Server01 *как Администратор* (Administrator).
2. Откройте консоль *Active Directory — пользователи и компьютеры*.
3. В дереве выберите ОП Employees.
4. Создайте учетную запись пользователя со следующими данными:

Поле	Введите
Имя (First Name)	Template
Фамилия (Last Name)	Sales Representative
User Logon Name (Имя входа пользователя)	Template.sales.rep
Имя входа пользователя (пред-Windows 2000) [User Logon Name (Pre-Windows 2000)]	Templatesalesrep

5. Щелкните **Далее (Next).**
6. Выберите **Отключить учетную запись (Account Is Disabled).** Щелкните Далее (Next).
7. Раскроется сводка по объекту. Щелкните **Готово (Finish).**

Примечание Как уже упоминалось в разделе «Прежде всего», вам необходимо создать группу Sales Representatives в ОП Security Groups. Если вы ее не создали, сделайте это сейчас. Настройте глобальную группу безопасности с именем Sales Representative.

8. Раскройте свойства объекта Template Sales Representative.
9. Задайте следующие свойства для шаблонной учетной записи:

Вкладка	Поле	Значение
Член групп (Member Of)	**Член групп (Member Of)**	Sales Representatives
Учетная запись (Account)	**Время входа (Logon Hours)**	Понедельник — пятница с 9:00 до 17:00
Учетная запись (Account)	**Истекает (Expires)**	Три месяца от текущей даты
Организация (Organization)	**Организация (Company)**	Contoso
Профиль (Profile)	**Путь к профилю (Profile path)**	\\Server1\Profiles\%Username%

10. Щелкните **OK.**

Упражнение 2. Создание объектов пользователей путем копирования шаблона

1. В дереве выберите ОП Employees.
2. Выберите объект Template Sales Representative.
3. В меню **Действие (Action)** щелкните **Копировать (Copy).**
4. Создайте новую учетную запись пользователя со следующими данными:

Поле	Введите
Имя (First Name)	Scott
Фамилия (Last Name)	Bishop
Имя входа пользователя (User Logon Name)	Scott. Bishop
Имя входа пользователя (пред-Windows 2000) [User Logon Name (Pre-Windows 2000)]	Sbishop
Отключить учетную запись (Account is disabled)	Снимите флажок
Пароль/Подтверждение (Password/Confirm Password)	Введите и подтвердите пароль, удовлетворяющий описанным ранее условиям сложности

5. Щелкните **Далее (Next),** а затем **Готово (Finish).**
6. Откройте диалоговое окно свойств для объекта Scott Bishop.
7. Удостоверьтесь, что информация, заданная для шаблона на вкладках свойств **Член групп (Member Of), Учетная запись (Account)** и **Организация (Organization),** была скопирована в новый объект.

8. Так как эта учетная запись понадобится для других упражнений, измените значения двух свойств: на вкладке **Учетная запись (Account)** дли параметра **Срок действия учетной записи (Account Expires)** задайте значение **Не ограничен (Never),** а параметр **Время входа (Logon Hours)** настройте так, чтобы вход в систему был разрешен в любое время.

Упражнение 3. Импорт объектов пользователей при помощи CSVDE

1. Откройте *Блокнот* (Notepad).
2. Наберите следующую информацию, создав три строки текста:

```
DN,objectClass,sAMAccountName,sn,givenName,userPrincipalName

"CN=Danielle Tiedt,OU=Employees,
DC=contoso,DC=com",use r,dtiedt,Tiedt, Danielle,danielle.tiedt§contoso.com

"CN=Lorrin Smith- Bates,OU=Employees, DC=contos-
o, DC=coin", user, lsmithbates, Smith-Bates, Lor-
rin,lorrin.smithbates@contoso.com
```

3. Сохраните файл под именем "C:\USERS.CSV"; обязательно заключите имя в кавычки (в противном случае он будет сохранен как C:\USERS.CSV.TXT).
4. Из командной строки исполните следующую команду:

```
csvde -i -f c:\users.csv
```

5. Если команда выдаст подтверждение об успешном выполнении, раскройте *Active Directory — пользователи и компьютеры,* чтобы убедиться, что объекты были созданы. Если команда выдает сообщение об ошибках, раскройте файл USERS.CSV в *Блокноте* (Notepad) и внесите исправления.
6. Далее в этой главе вам потребуется входить в систему под именами этих пользователей. Так как пользователи были импортированы без паролей, их нужно назначить. После задания паролей включите учетные записи. Команды **Смена пароля (Reset Password)** и **Включить учетную запись (Enable Account)** можно найти в меню **Действие (Action)** или в контекстном меню соответствующих объектов.
7. Если у вас есть доступ к приложению, которое может работать с CSV-файлами, например Microsoft Excel, откройте C:\USERS.CSV. Структуру файла проще понять, если он отображается как таблица, а не в виде строк текстового файла, как в *Блокноте* (Notepad).

Упражнение 4. Использование средств командной строки Active Directory

1. Из командной строки исполните следующую команду:

```
dsquery user "OU=Employees, DC=Contoso,DC=Com" - stalepwd 7
```

2. Эта команда ищет объекты пользователей, которые не меняли свои пароли в течение семи дней. Она должна вывести сведения, по крайней мере, об объектах, созданных вами в упражнениях 1 и 2. Если вы не добавляли пользователей, создайте один или два новых объекта пользователей и выполните шаг 1.
3. Исполните следующую команду:

```
dsquery user "OU=Employees, DC=Contoso,DC=Com" - stalepwd 7 | dsmod user -
mustchpwd yes
```

4. Здесь результаты выполнения DSQUERY передаются на вход команде DSMOD, которая включает для каждого объекта параметр **Требовать Смену пароля при следующем входе в систему (User must change password at next logon).** На вкладке **Учетная запись (Account)** окна свойств соответствующих объектов удостоверьтесь, что команда выполнена успешно.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Как наиболее эффективно создать 100 новых объектов пользователей с одинаковыми путями к профилю и домашней папке и с одинаковыми значениями параметров **Должность (Title), Веб-страница (Web Page), Организация (Company), Отдел (Department)** и **Руководитель (Manager)?**
2. Какая команда поможет найти учетные записи, не использовавшиеся в течение двух месяцев?
   a. DSADD.
   b. DSGET.
   c. DSMOD.
   d. DSRM.
   e. DSQUERY.
3. Какую переменную можно использовать в командах DSMOD и DSADD для создания домашних папок и папок профилей для определенных пользователей?
   a. *%Username%*.
   b. $Username$.
   c. *CN=Username*.
   d. *<Username>*.
4. При помощи какой команды можно вывести номера телефонов всех пользователей вОП?
   a. DSADD.
   b. DSGET.
   c. DSMOD.
   d. DSRM.
   e. DSQUERY.

Резюме

- Шаблон объекта пользователя — это объект, путем копирования которого создаются
- новые пользователи. Если шаблон не является «настоящим» пользователем, его следует отключить. Из шаблонов копируется только подмножество свойств пользователя.
- Команда CSVDE позволяет импортировать объекты каталога из CSV-файла с разделителями — запятыми.
- Windows Server 2003 поддерживает новые мощные средства командной строки,
- позволяющие создавать и удалять объекты каталога и управлять ими: DSQUERY, DSGET, DSADD, DSMOVE, DSMOD и DSRM. Часто набор объектов, возвращенный DSQUERY, передается по каналу другим командам.

Занятие 3. Управление профилями пользователей

Вероятно, вы бы не стали читать эту книгу, если бы вам не приходилось обеспечивать работу пользователей, и вы знаете, что в системе есть элементы, отсутствие которых усложняет жизнь. Например, если пользователь войдет в систему и не сможет получить доступ к папке **Избранное (Favorites)** в Internet Explorer, или не увидит знакомых ярлыков и документов на рабочем столе, или ему придется заново настраивать словарь, производительность его труда резко снизится, а в службу поддержки поступит звонок. Все эти примеры относятся к компонентам профиля пользователя. Профили можно настраивать, повышая их доступность, безопасность и надежность. На этом занятии вы научитесь управлять локальными, перемещаемыми, групповыми и обязательными профилями пользователей.

Изучив материал этого занятия, вы сможете:

- ✓ понять назначение локальных и перемещаемых профилей пользователей;
- ✓ настроить перемещаемый профиль пользователя;
- ✓ создать преднастроенный перемещаемый групповой или пользовательский профиль;
- ✓ настроить обязательный профиль.

Продолжительность занятия — около 15 минут.

Профили пользователей

Профиль пользователя (user profile) — это набор папок и файлов данных, содержащих элементы среды рабочего стола конкретного пользователя. Профиль состоит из:

- ярлыков в меню **Пуск (Start),** на рабочем столе и на панели быстрого запуска;
- документов на рабочем столе и, если не настроена переадресация, в папке **Мои документы (My Documents);**

Совет Свойства папки **Мои документы (My Documents)** и политик перенаправления папок в групповой политике позволяют настраивать хранение папок **Мои документы** в сети. Таким образом, содержимое папки можно хранить на сервере, где ее можно архивировать и проверять на наличие вирусов. Кроме того, вы можете обеспечить пользователю доступ к своей папке, даже если он перейдет на другой компьютер в сети организации. Также папку **Мои документы** можно сделать доступной в автономном режиме, чтобы пользователи могли обращаться к своим файлам локально, без подключения **к** сети.

- избранных страниц и файлов «cookie» в Internet Explorer;
- сертификатов (если они внедрены в сети);
- специальных файлов приложений, например пользовательского словаря, шаблонов и списка автотекста в Microsoft Office;
- содержимого папки **Сетевое окружение (My Network Places);**
- параметров отображения рабочего стола, например его вида, фона и заставки.

Эти важные элементы у каждого пользователя свои. Желательно, чтобы они не изменялись между входами в систему, были доступны, если пользователю потребуется войти в другую систему, и их можно было восстановить в случае, если система даст сбой и ее потребуется переустановить.

Локальные профили пользователей

По умолчанию профили пользователей хранятся локально в папке %Systemdrive%\Documents and Settings\%Username% и работают следующим образом.

- Когда пользователь входит в систему впервые, система создает для него профиль путем копирования профиля *Пользователь по умолчанию* (Default User). Имя для нового профиля формируется на основе имени для входа, указанного при первом входе в систему.
- Все изменения рабочего стола пользователя и программной среды хранятся в локальном профиле пользователя. Для каждого пользователя существуют отдельные профили, поэтому все параметры индивидуальны.
- Пользовательская среда расширена за счет профиля *Все пользователи* (All Users), который может включать ярлыки на рабочем столе или в меню Пуск (Start), адреса компьютеров в сети и даже данные приложений. Для создания среды пользователя элементы профиля *Все пользователи* (All Users) соединяются с профилем пользователя. По умолчанию только члены группы *Администраторы* (Administrators) могут модифицировать профиль *Все пользователи* (All Users).
- Профиль является локальным в полном смысле. Если пользователь входит в другую систему, документы и параметры, являющиеся частью его профиля, не перемещаются. Вместо этого, когда пользователь впервые входит в систему, она генерирует для него новый локальный профиль.

Перемещаемые профили пользователей

Если пользователь работает на нескольких компьютерах, вы можете настроить *перемещаемый профиль пользователя* (roaming user profile, RUP), чтобы гарантировать сохранность и неизменность его документов и параметров вне зависимости от того, в какую систему он входит. RUP хранит профили на сервере, а значит их можно архивировать, проверять на наличие вирусов и централизованно управлять ими. Даже в среде, где пользователи не перемещаются, RUP обеспечивает сохранность важной информации провидя. Если система пользователя дала сбой и ее необходимо переустановить, RUP гарантирует, что новая пользовательская среда будет идентичная предыдущей.

Чтобы настроить RUP, создайте общую папку на сервере. В идеальном случае это должен быть файловый сервер, на котором часто проводится архивирование.

Примечание Настройте общий доступ так, чтобы всем (Everyone) был разрешен полный контроль над папкой (Full Control). Стандартные разрешения общего доступа в Windows Server 2003 позволяют только чтение (Read) папки, но этого недостаточно для настройки перемещаемого профиля.

На вкладке Профиль (Profile) диалогового окна Свойства (Properties) пользователя введите **Путь к профилю (Profile Path)** в следующем формате: ***\\<имя_сервера>\<имя_общего_ресурса>\%Username%.***

Вместо переменной *%Username%* будет автоматически подставлено имя входа пользователя.

Как видите, это очень просто. При следующем входе система найдет местоположение перемещаемого профиля.

Подготовка к экзамену Перемещаемый профиль пользователя — это всего лишь общая папка и путь к папке профиля пользователя в пределах этого общего ресурса, указанный в свойстве объекта пользователя. Перемещаемые профили никоим образом не являются свойством объекта компьютера.

Когда пользователь выходит из системы, его профиль выгружается на сервер профилей. Теперь пользователь может входить в эту или в любую другую систему в домене, и его документы и настройки, являющиеся частью RUP, всегда будут под рукой.

Примечание Windows Server 2003 представляет новую политику: *Разрешать использование только локальных профилей* (Only Allow Local User Profiles). Эта политика, связанная с ОП, содержащим учетные записи компьютеров, не позволяет использовать на данных компьютерах перемещаемые профили. Вместо этого пользователи работают с локальными профилями.

Когда пользователь с RUP впервые входит в новую систему, та не копирует профиль *Пользователь по умолчанию* (Default User), а загружает RUP из сетевого ресурса. Когда пользователь выходит из системы или входит в систему, на которой работал ранее, копируются только измененные файлы.

Синхронизация перемещаемого профиля

В отличие от предыдущих версий, Windows 2000\XP и Windows Server 2003 не загружают и не выгружают весь профиль пользователя при входе и выходе, а синхронизируют его. Между локальной системой и сетевой папкой для хранения RUP перемещаются только измененные файлы. Это означает, что вход и выход из системы с использованием RUP выполняется существенно быстрее, чем в предыдущих версиях Windows. Организации, которые не внедряли RUP из-за опасения, что такие профили будут отрицательно влиять на процесс входа в систему и сетевой трафик, должны еще раз оценить ситуацию с учетом этого момента.

Создание преднастроенного профиля пользователя

Для упорядочения и предварительной настройки рабочего стола и программной среды можно создавать настроенные профили пользователя, чтобы:

- создать продуктивную рабочую среду с простым доступом к необходимым сетевым ресурсам и приложениям;
- исключить доступ к ненужным ресурсам и прирложениям;
- упростить работу службы поддержки по устранению неполадок благодаря более понятному и единообразному рабочему столу.

Для создания преднастроенного профиля пользователя не требуются никакие специальные средства. Просто войдите в систему и измените рабочий стол и настройки приложений по своему усмотрению. Лучше использовать для этого отдельную учетную запись, чтобы без необходимости не изменять собственный профиль.

Создав профиль, войдите в систему с административными реквизитами. Из *Панели управления* раскройте окно **Система (System),** перейдите на вкладку **Дополнительно**

(Advanced) и в области **Профили пользователей (User Profiles)** щелкните **Параметры (Settings).** Выберите созданный профиль и щелкните **Копировать (Copy To).** Введите путь к профилю в стандартном формате записи пути (UNC): \\<*имя_сервера*>\<*имя_общего_ресурса*>\<*имя_пользователя*>. В области **Разрешить использование (Permitted To Use)** щелкните **Изменить (Change),** чтобы выбрать пользователя, для которого вы настроили этот профиль. Таблица управления доступом (ACL) для папки профиля будет настроена так, чтобы разрешить доступ этому пользователю. Пример показан на рис. 3-5. Щелкните **OK** — профиль будет скопирован из сетевого ресурса.

Примечание Для копирования профиля необходимо быть членом группы *Администраторы* (Administrators).

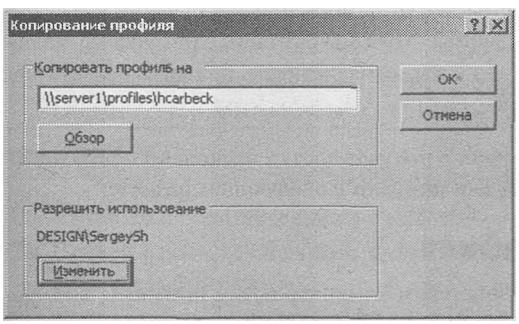


Рис. 3-5. Копирование преднастроенного профиля пользователя на сетевой ресурс

Теперь раскройте свойства объекта пользователя и на вкладке **Профиль (Profile)** в поле **Путь к профилю (Profile Path)** введите тот же UNC-путь. И все! При следующем входе пользователя в домен этот профиль будет загружен и определит среду пользователя.

Совет Будьте осторожны при использовании преднастроенных (да и всех остальных) перемещаемых профилей, помните о потенциальных проблемах, связанных с различным аппаратным обеспечением систем, на которых может работать пользователь. Например, если ярлыки на рабочем столе организованы под разрешение XGA (1024x768), а пользователь входит в систему с видеоадаптером, который поддерживает только разрешение SVGA (800x600), возможно, некоторые ярлыки не отобразятся.

Также профили не всегда обладают межплатформенной совместимостью. Профиль, созданный для Windows 98, будет неправильно работать в системе Windows Server 2003. Несоответствия будут возникать даже при перемещении между системами Windows Server 2003 и Windows XP или Windows 2000 Professional.

Создание преднастроенного группового профиля

При помощи перемещаемых профилей можно создать стандартную среду рабочего стола для нескольких пользователей с одинаковыми должностными обязанностями. Этот процесс схож с процессом создания преднастроенного профиля для одного пользователя, но результирующий профиль будет доступен нескольким пользователям.

Создайте профиль, выполнив описанные выше действия. При копировании профиля на сервер укажите такой путь: \\<*имя_сервера*>\<*имя_общего_ресурса*>\<*имя_группо-*

вого_профиля>. Необходимо разрешить доступ всем пользователям, которые будут использовать этот профиль. Для этого в области **Разрешить использование (Permitted To Use)** щелкните **Изменить (Change)** и выберите группу, в которую входят все пользователи, или группу BUILTIN\USERS, которая включает всех пользователей домена. В действительности профиль будет применен только к тем пользователям, для объектов которых вы указали путь к этому профилю.

После того как профиль скопирован в сеть, необходимо настроить путь к нему для тех пользователей, которым он предназначен. Windows Server 2003 упрощает эту задачу — путь к профилю можно изменить одновременно для нескольких выбранных пользователей. Введите тот же UNC, который вы указали при копировании профиля в сеть, например \\<*имя_сервера*>\<*имя_общего_ресурса*>\<*имя_группового_профиля*>.

Совет Путь к профилю настраивается как свойство одного или нескольких объектов пользователей. Он не назначается объекту группы. Хотя мы считаем, что профиль является групповым, не попадитесь в ловушку — не пытайтесь связать профиль с объектом самой группы.

И наконец, поскольку к групповому профилю получат доступ несколько пользователей, его необходимо сделать обязательным, как описано в следующем разделе.

Настройка обязательного профиля

Обязательный профиль не позволяет пользователям изменять среду профиля. Точнее, обязательный профиль не сохраняет изменения от сеанса к сеансу. Хотя пользователь и может внести изменения, при следующем входе в систему его рабочий стол будет выглядеть так же, как раньше.

Обязательные профили удобны в ситуациях, когда вы хотите зафиксировать состояние рабочего стола. То есть в практическом смысле обязательные профили полезны, если, создавая групповые профили, вы не хотите, чтобы изменения, которые внесет один пользователь, повлияли на среду других пользователей.

Чтобы сделать профиль обязательным, просто переименуйте файл в корневой папке профиля. Интересно, что обязательные профили не настраиваются путем назначения разрешений. Файл, который вам требуется переименовать, — Ntuser.dat. Это скрытый файл, поэтому убедитесь, что в программе *Свойства папки* (Folder Options) из *Панели управления* вы включили параметр Показывать скрытые **файлы и папки (Show hidden files and folders),** или запустите из командной строки программу attrib, чтобы снять атрибут **Скрытый (Hidden).** Возможно, вам понадобится включить в *Проводнике Windows* отображение расширений файлов.

Найдите файл Ntuser.dat в профиле, который собираетесь сделать обязательным. Переименуйте его в Ntuser.man. Профиль (перемещаемый или локальный) теперь является обязательным.

Лабораторная работа. **Управление профилями пользователей**

На этой лабораторной работе вы создадите перемещаемый и преднастроенный перемещаемые профили пользователя, а также обязательный групповой профиль. Вам придется несколько раз входить и выходить из системы. Так как стандартным учетным записям пользователя запрещено локально входить в систему на контроллере домена, для начала

вы добавите пользователей в группу *Операторы печати* (Print Operators), которой это разрешено.

Упражнение 1. Настройка объектов пользователей для входа на контроллер домена

В реальной среде вы вряд ли захотите разрешить пользователям локально входить на контроллер домена, но в нашей тестовой среде с одной системой такая возможность необходима. Существует несколько способов задать необходимое разрешение, но самый простой — добавить группу *Пользователи домена* (Domain Users) в группу *Операторы печати* (Print Operators), которой разрешено входить в систему локально.

1. Откройте консоль *Active Directory — пользователи и компьютеры.*
2. В дереве выберите контейнер Builtin.
3. Раскройте окно свойств группы *Операторы печати* (Print Operators).
4. На вкладке **Члены группы (Members)** добавьте группу *Пользователи домена* (Domain Users).

Упражнение 2. Создание общего ресурса для профилей

1. На диске C: создайте папку Profiles.
2. Правой кнопкой щелкните папку Profiles и выберите **Общий доступ и безопасность (Sharing and Security).**
3. Перейдите на вкладку **Доступ (Sharing).**
4. Откройте общий доступ к этой папке, оставив предложенное по умолчанию имя ресурса — Profiles.
5. Щелкните кнопку **Разрешения (Permissions).**
6. Установите флажок **Полный доступ (Full Control).**
7. Щелкните **OK.**

Внимание! При создании общего ресурса Windows Server 2003 по умолчанию ограничивает к нему доступ. В большинстве организаций для общего ресурса включают разрешение **Полный доступ (Full Control),** а особые разрешения применяют при помощи свойств на вкладке **Безопасность (Security).** Впрочем, если администратор не защитил ресурс до того, как открыть к нему общий доступ, Windows Server 2003 в целях безопасности допускает небольшую ошибку, назначая этому ресурсу доступ только для чтения.

Упражнение 3. Создание шаблона профиля пользователя

1. Создайте учетную запись пользователя, которая будет применяться исключительно для создания шаблонов профилей, по следующим данным:

Поле	Введите
Имя (First Name)	Profile
Фамилия (Last Name)	**Учетная запись (Account)**
Имя входа пользователя (User Logon Name)	Profile
Имя входа пользователя **(пред-Windows** 2000) **[User Logon Name (Pre-Windows 2000)]**	Profile

2. Завершите сеанс на Server01.
3. Войдите в систему под учетной записью Profile.
4. Настройте рабочий стол, например создайте ярлыки для локальных или сетевых ресурсов, допустим, для системного диска C:.
5. Настройте рабочий стол при помощи приложения *Экран* (Display) из *Панели управления*. На вкладке **Рабочий стол (Desktop)** диалогового окна **Свойства экрана (Display Properties)** можно изменить фон рабочего стола и, щелкнув **Настройка рабочего стола (Customize Desktop),** добавить значки **Мои документы (My Documents), Мой компьютер (My Computer), Сетевое окружение (My Network Places)** и **Internet Explorer.**
6. Завершите сеанс учетной записи Profile.

Упражнение 4. Работа с преднастроенным профилем пользователя

1. Войдите в систему как *Администратор* (Administrator).
2. В *Панели управления* дважды щелкните **Система (System).**
3. Перейдите на вкладку **Дополнительно (Advanced).**
4. **В** области **Профили пользователей (User Profiles)** щелкните **Параметры (Settings).** Откроется диалоговое окно **Профили пользователей (User Profiles).**
5. Выберите профиль, который вы настроили для учетной записи Profile.
6. Щелкните **Копировать (Copy To).**
7. **В** поле **Копировать профиль на (Copy Profile To)** введите \\server01\profiles\hcarbeck.
8. В области **Разрешить использование (Permitted To Use)** щелкните **Изменить (Change).**
9. Введите **Hank** и щелкните OK.
10. Подтвердите значения, введенные в окне **Копирование профиля (Copy To),** и щелкните OK.
11. После того как профиль будет скопирован в сеть, щелкните **OK** в окнах **Профили пользователей (User Profiles)** и **Свойства системы (System Properties).**
12. Откройте папку C:\Profiles и убедитесь, что папка профиля Hcarbeck создана.
13. В дереве консоли *Active Directory — пользователи и компьютеры* выберите ОП Employees.
14. Откройте свойства объекта пользователя Hank Carbeck.
15. Перейдите на вкладку **Профиль (Profile).**
16. В поле **Путь к профилю (Profile Path)** введите \\server01\profiles\%username%.
17. Щелкните **Применить (Apply)** и убедитесь, что вместо переменной *%Usemame%* было подставлено имя hcarbeck. Важно, чтобы путь к профилю соответствовал фактическому сетевому пути к папке профиля.
18. Щелкните OK.
19. Проверьте, что преднастроенный перемещаемый профиль пользователя работает правильно. Для этого выйдите из системы и войдите под именем hank.carbeck@contoso.com. Вы должны увидеть изменения, которые внесли на рабочем столе под учетной записью Profile.

Упражнение 5. Работа с преднастроенным обязательным групповым профилем

1. Войдите в систему как *Администратор* (Administrator).
2. В *Панели управления* дважды щелкните **Система (System).**

3. Перейдите на вкладку **Дополнительно (Advanced).**
4. **В** области **Профили пользователей (User Profiles)** щелкните **Параметры (Settings).**
5. Выберите профиль, который вы настроили для учетной записи Profile.
6. Щелкните **Копировать (Copy To).**
". В поле **Копировать профиль на (Copy Profile To)** введите \\server01\profiles\sales.
8. В области **Разрешить использование (Permitted To Use)** щелкните **Изменить (Change).**
9. Введите Users и щелкните OK.
10. Подтвердите значения, введенные в окне **Копирование профиля (Copy To),** и щелкните OK.
11. После того как профиль будет скопирован в сеть, щелкните OK в окнах **Профили пользователей (User Profiles)** и **Свойства системы (System Properties).**
12. Откройте папку C:\Profiles и убедитесь, что папка профиля Sales создана.
13. В *Панели управления* раскройте **Свойства папки (Folder Options)** и проверьте, что на вкладке **Вид** (View) в области **Дополнительные параметры (Advanced Settings)** выбран параметр **Показывать скрытые файлы и папки (Show Hidden Files And Folders).**
14. Раскройте папку C:\Profiles\Sales и переименуйте файл Ntuser.dat в Ntuser.man. Этот профиль станет обязательным.
15. В дереве консоли *Active Directory — пользователи и компьютеры* выберите ОП Employees.
16. Выберите в дереве следующие объекты (щелкните первый объект и, удерживая клавишу Ctrl, — остальные): Scott Bishop, Danielle Tiedt, Lorrin Smith-Bates.
17. В меню **Действие (Action)** выберите **Свойства (Properties).**
18. Перейдите на вкладку **Профиль (Profile)** и установите флажок **Путь к профилю (Profile Path).**
19. В поле **Путь к профилю (Profile Path)** введите \\server01\profiles\sales.
20. Щелкните OK.
21. Проверьте, что преднастроенный перемещаемый профиль пользователя настроен правильно; для этого выйдите из системы и войдите под именем danielle.tiedt@contoso.com.
22. Удостоверьтесь, что профиль обязательный, изменив вид рабочего стола. Вы сможете внести изменения, но они не сохранятся для будущих сеансов.
23. Выйдите из системы и войдите как Danielle Tiedt. Так как профиль обязательный, вы не увидите изменений, сделанных на предыдущем шаге.
24. Выйдите из системы и войдите как Scott Bishop с именем пользователя scott.bishop@contoso.com. Должен появиться рабочий стол без изменений.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Опишите, как формируется рабочий стол пользователя, если перемещаемые профили не применяются.
2. Расположите по порядку шаги, в результате которых создается преднастроенный перемещаемый профиль пользователя. Задействуйте все перечисленные шаги.
   a. Настройка рабочего стола и среды пользователя.
   b. Вход под именем пользователя с разрешениями, достаточными для изменения свойств учетной записи пользователя.

c. Копирование профиля в сеть.
d. Создание учетной записи пользователя таким образом, чтобы профиль можно было сформировать, не изменяя текущие профили остальных пользователей.
e. Вход в систему под учетной записью профиля.
f. Ввод UNC-пути к профилю на странице свойств **Профиль (Profile)** объекта пользователя.
g. Вход в систему в качестве локального администратора или администратора домена.

3. Как сделать профиль обязательным?
   a. Настроить разрешения для папки на странице свойств Безопасность (Security), чтобы запретить запись.
   b. Настроить разрешения для папки на странице свойств **Доступ (Sharing),** чтобы разрешить только чтение.
   c. Изменить атрибуты папки с профилем, оставив лишь атрибут **Только чтение (Read Only).**
   d. Переименовать Ntuser.dat в Ntuser.man.

Резюме

- Windows Server 2003 создает индивидуальные профили для всех пользователей, которые входят в систему. По умолчанию профили хранятся на локальной системе в папке *%Systemdrive%\Documents* and Settings\%Username%.
- Для применения перемещаемых профилей необходимо лишь настроить общую папку и указать путь к профилю в свойствах объекта пользователя.
- Преднастроенные — это обычные профили, которые копируются в каталог профилей до того, как путь к нему указывается в объекте пользователя.
- Групповые профили должны быть обязательными, для этого необходимо переименовать Ntuser.dat в Ntuser.man, чтобы изменения, внесенные одним пользователем, не влияли на других.

Занятие 4. Проверка подлинности: безопасность и устранение неполадок

После настройки объектов пользователей перед вами встают еще две проблемы: уязвимость, которая при легкомысленном к ней отношении может привести к нарушению целостности сети всего предприятия, и вопросы социотехники, связанные с вашими стараниями сделать сеть и проверку подлинности в целом надежными и дружественными для пользователей. К сожалению, эти тенденции развиваются в противоположных направлениях: чем безопаснее сеть, тем неудобнее в ней работать. На этом занятии мы рассмотрим вопросы, связанные с проверкой подлинности пользователей. Вы узнаете о действии политик учетных записей домена, в том числе политик паролей и блокировки учетных записей. Также вы научитесь настраивать аудит для событий, связанных со входом в систему, и выполнять различные задачи проверки подлинности применительно к объектам пользователей.

Изучив материал этого занятия, вы сможете:

- ✓ перечислить политики учетных записей домена и пояснить, как они влияют на требования к паролям и проверку подлинности;
- ✓ настраивать аудит для событий, связанных со входом в систему;
- ✓ изменять атрибуты объектов пользователей, относящиеся к проверке подлинности.

Продолжительность занятия — около 15 минут.

Настройка безопасности проверки подлинности при помощи политик

Active Directory в Windows Server 2003 поддерживает политики безопасности, обеспечивающие сложность паролей и их безопасное использование в рамках предприятия. Конечно, вы должны разработать политику паролей, эффективно защищающую от злоумышленников, но в то же время удобную для пользователей, чтобы они не забывали свои пароли (иначе возрастет количество звонков в службу поддержки) или, что еще хуже, где-то записывали их.

Рядовой сервер под управлением Windows Server 2003 поддерживает политику для своих локальных учетных записей пользователей, которая настраивается из оснастки *Локальная политика безопасности* (Local Security Policy).

Наиболее часто вы будете настраивать политику в отношении объектов пользователей домена. Политика учетных записей домена управляется посредством ОГП Default Domain Policy. Для изучения и модификации этой политики откройте консоль *Active Directory — пользователи и компьютеры* (Active Directory Users and Computers), щелкните узел домена и в меню **Действие (Action)** выберите **Свойства (Properties).** Перейдите на **вкладку Групповая политика (Group Policy).** Первый ОГП в списке — это объект политики, который управляет политиками учетных записей домена (обычно Default Domain Policy). Выберите эту политику и щелкните кнопку **Изменить (Edit).** Откроется консоль *Редактор объектов групповой политики* (Group Policy Object Editor), в окне которой **будет** выбрана политика Default Domain Policy. Раскройте узлы **Конфигурация компьютера (Computer Configuration),** Конфигурация **Windows (Windows Settings), Параметры** безопасности **(Security Settings) и Политики учетных записей (Account Policies).**

Политика паролей

Политики паролей домена позволяют защищать сеть путем внедрения лучших методик управления паролями, проверенных практикой. Эти политики описаны в табл. 3-5.

Табл. **3-5. Политики паролей**

Политика	Описание
Требовать неповторяемости паролей (Enforce tesword History)	Когда политика включена, Active Directory хранит список недавно использованных паролей и не разрешает пользователю задавать пароль из этого списка. В результате, когда пользователю предлагается сменить пароль, он не может повторно ввести тот же пароль, то есть увеличить срок его действия. Эта политика включена по умолчанию, причем максимальное значение для нее равно 24. Во многих ИТ-организациях задают значение 6 или 12

Табл. 3-5. *(окончание)*

Политика	Описание
Макс, срок действия пароля (Maximum Password Age)	Эта политика определяет, когда пользователю необходимо сменить пароль. Неизменные или редко изменяемые пароли более уязвимы, и злоумышленники могут использовать их для доступа к сети под существующей учетной записью. Значение по умолчанию — 42 дня. Обычно в ИТ-организациях пароль меняют каждые 30—90 дней
Мин. срок действия пароля (Minimum Password Age)	Когда пользователю необходимо сменить пароль, то, даже если включена история паролей, он может просто несколько раз изменить пароль, чтобы обойти требования и снова ввести исходный пароль. Политика *Минимальный срок действия пароля* предотвращает такую ситуацию, требуя, чтобы между сменами паролей проходило определенное количество дней. Конечно, администратор или сотрудник службы поддержки с соответствующими разрешениями может в любое время сменить пароль в Active Directory. Но пользователю запрещено менять пароль более одного раза в течение указанного в этом параметре периода времени
Мин. длина пароля (Minimum Password Length)	Эта политика задает минимальное количество символов в пароле. По умолчанию в пароле Windows Server 2003 должно быть 7 символов
Пароль должен отвечать требованиям сложности (Passwords Must Meet Complexity Requirements)	Эта политика включает правила (фильтры) для новых паролей. В Windows Server 2003 требования фильтра паролей по умолчанию (passfilt.dll) следующие: • пароль не должен быть основан на имени учетной записи пользователя; • в пароле должно быть не менее 6 символов; • пароль должен содержать символы следующих типов (минимум три): • заглавные алфавитные символы (A...Z); а строчные алфавитные символы (a...z); • арабские цифры (0...9); • не алфавитно-цифровые символы (например ! $ # , %) . По умолчанию в Windows Server 2003 эта политика включена

Примечание Изменение требований к длине и сложности паролей не влияет на существующие пароли. После включения этих политик изменения будут влиять только на новые учетные записи и изменяемые пароли.

Политика блокировки учетной записи

В общем смысле блокировка учетных записей подразумевает, что после нескольких неудачных попыток входа в систему та должна решить, что злоумышленник пытается подобрать пароль, чтобы воспользоваться учетной записью, и в целях безопасности заблокировать эту учетную запись и пресечь дальнейшие попытки входа в систему. Политики блокировки учетных записей определяют предел для неавторизованных входов в систему, то есть количество неудачных попыток за период времени и требования, выполнение которых позволит разблокировать учетную запись, — пользователю придется про-

сто подождать или обратиться к администратору. В табл. 3-6 перечислены политики блокировки учетной записи.

Табл. 3-6. Политики блокировки учетной записи

Политика	Описание
Пороговое значение блокировки (Account Lockout Threshold)	Задает количество неудачных попыток входа в систему, влекущее блокировку учетной записи. Допустимые значения — от 0 до 999. Если вы выберете слишком маленькое значение (допустим, три), учетные записи могут блокироваться из-за обычных «человеческих» ошибок. Если значение равно 0, учетные записи не блокируются никогда. Значение счетчика блокировки не изменяется при попытке входа в систему на заблокированных рабочих станциях
Блокировка учетной записи на (Account Lockout Duration)	Определяет период времени, который должен пройти после блокировки до того, как Active Directory автоматически разблокирует учетную запись пользователя. Эта политика не включается по умолчанию, и ее полезно использовать только в сочетании с политикой *Пороговое значение блокировки* (Account Lockout Threshold). Хотя допустимыми являются значения от 0 до 99 999 минут, то есть около 10 недель, небольшие значения (от 5 до 15 минут) могут существенно снизить количество атак, причем пользователи, заблокированные по ошибке, не будут при этом испытывать серьезных неудобств. Если выбрано значение 0, пользователю придется обратиться к соответствующему администратору, который разблокирует учетную запись вручную
Сброс счетчика блокировки через (Reset Account Lockout Counter After)	Этот параметр указывает время, которое должно пройти после неудачной попытки входа в систему до того, как значение счетчика будет сброшено до 0. Допустимые значения — от 1 до 99 999 минут, причем значение параметра должно быть меньше или равно продолжительности блокировки учетной записи

Вопросы совместимости разных платформ

В организациях часто сосуществуют службы каталогов, серверы и клиентские платформы разного типа. В средах, где в домене Active Directory присутствуют системы Windows 9x/Me или Windows NT 4, администраторам следует знать о нескольких возможных проблемах.

- Пароли — если в Windows 2000, Windows XP Professional и Windows Server 2003 поддерживаются пароли из 127 символов, то в Windows 9x/Me максимальная длина пароля — 14 символов.
- Active Directory Client — можно загрузить с Web-узла Microsoft и установить в системах Windows 9x/Me/NT 4. Он позволяет этим платформам использовать многие функции Active Directory, доступные в Windows 2000 Professional и Windows XP Professional, такие как:
- знание сайта — система с клиентом Active Directory Client будет пытаться входить на контроллер домена в своем сайте, а не на любой контроллер домена на предприятии;
- *интерфейсы служб Active Directory* (ADSI) — использование сценариев для управления Active Directory;

- *распределенная файловая система* (Distributed File System, DFS) — позволяет обращаться к общим ресурсам DFS на серверах под управлением Windows 2000 и Windows Server 2003;
- проверка подлинности при помощи протокола NTLM версии 2 — использование расширенных функций NTLM версии 2;
- адресная книга Active Directory Windows Address Book (WAB) — страницы свойств;
- возможность поиска в Active Directory, интегрированная в команды **Пуск\Найти (Start\Find)** и **Пуск\Поиск (Start\Search).**

Следующие возможности, которые поддерживаются в Windows 2000 Professional и Windows XP Professional, не поддерживаются клиентом Active Directory на платформах Windows 9x/NT 4:

- проверка подлинности Kerberos V5;
- групповая политика и поддержка управления изменениями и настройкой;
- *имя службы-участника* (SPN) или взаимная проверка подлинности.

Кроме того, вам следует знать о следующих проблемах в смешанных средах.

- Windows 98 поддерживает пароли длиной до 14 символов. Windows 2000/XP и Windows Server 2003 поддерживают 127-символьные пароли. Помните об этом при настройке паролей для пользователей, которые входят в сеть из Windows 98.
- Без клиента Active Directory пользователи систем с версиями до Windows 2000 могут изменять свои пароли, только если у системы есть доступ к контроллеру домена — хозяина операций эмулятора *основного контроллера домена* (PDC). Чтобы выяснить, какая система эмулирует PDC в домене, раскройте *Active Directory — пользователи и компьютеры,* щелкните узел домена, в меню **Действие (Action)** выберите **Хозяева операций (Operations Masters)** и перейдите на вкладку **PDC.** Если эмулятор PDC недоступен (допустим, он работает в автономном режиме или находится на удаленном конце разорванного сетевого подключения), пользователи не могут менять свои пароли.
- Как вы узнали из этой главы, объекты пользователей поддерживают два свойства имен пользователей для входа. Имя для входа пред-Windows 2000, или имя SAM, — это эквивалент имени пользователя в Windows 9x/NT 4. При входе в систему пользователи должны ввести свое имя и выбрать домен в поле Вход на **(Log On To)**. В прочих ситуациях имя пользователя можно вводить в формате <имяломена>\<имя_входа_пользователя>.
- Пользователи систем Windows 2000 или более поздних платформ могут делать это тем же образом или применять более удобное UPN-имя *<имя_входа_пользователя>@<суффикс UPN>,* где *суффикс UPN* — DNS-имя домена (по умолчанию), которому принадлежит объект пользователя. Если в систему входят по UPN, необязательно выбирать домен в поле **Вход на (Log On To)**. После того как вы введете символ *«@»,* это поле будет отключено.

Аудит проверки подлинности

Если вы считаете, что на систему могут производиться атаки с целью выявления паролей пользователей, или вам необходимо решить проблемы проверки подлинности, можно настроить политику аудита так, чтобы в журнале безопасности создавались записи о подозрительных действиях.

Политики аудита

Следующие политики расположены в узле **Конфигурация компьютера (Computer Configuration\Конфигурация Windows (Windows Settings)\Параметры безопасности (Security Settings)\Локальные политики (Local PoIicies)\Политика аудита (Audit Policy)** в редакторе объектов групповой политики [или в оснастке *Локальная политика безопасности* (Local Security Policy)]. Вы можете настроить аудит успешных или неудачных событий.

- ***Аудит событий входа в систему*** **(Audit Account Logon Events).** Эта политика производит аудит всех входов в систему пользователя, для которого требуется проверка подлинности на контроллере домена. Для контроллеров домена эта политика определена в ОГП Default Domain Controllers. Во-первых, она создает запись в журнале безопасности на контроллере домена каждый раз, когда пользователь интерактивно или по сети входит в систему под доменной учетной записью. Во-вторых, помните, что для всесторонней оценки результатов аудита вам необходимо анализировать журналы безопасности на всех контроллерах домена, так как проверка подлинности пользователей распределена по всем контроллерам в сайте или домене.
- *Аудит управления* ***учетными*** *записями* **(Audit Account Management).** Включает аудит таких действий, как создание, удаление и модификация учетных записей пользователей, групп или компьютеров. Когда включена эта политика, события смены пароля также регистрируются.
- ***Аудит*** *входа* ***в систему*** **(Audit Logon Events).** События входа — это вход и выход из системы (интерактивно или по сетевому подключению). Если вы включили политику *Аудит событий входа в систему* (Audit Account Logon Events) для регистрации входа, успешно выполняемого на контроллере домена, вход на рабочие станции не будет генерировать события аудита. События входа в систему будут генерироваться только интерактивными или сетевыми входами на контроллер домена. *Событие входа учетной записи* (account logon event) генерируется на локальных компьютерах для локальных учетных записей, а на контроллере домена — для сетевых учетных записей. *Событие входа в систему* (logon event) генерируется, где бы ни осуществлялся вход в систему.

Совет Важно отличать вход в систему под учетной записью и общий вход. Когда пользователь входит на рабочую станцию под доменной учетной записью, эта станция регистрирует *событие входа* (logon event), а контроллер домена — *событие входа учетной записи* (account logon event). Когда пользователь подключается к общей папке на сетевом сервере, тот регистрирует событие входа, а контроллер домена — событие входа учетной записи.

Журнал событий безопасности

После того как вы настроили аудит, журналы безопасности начинают заполняться сообщениями о событиях. Сообщения можно просмотреть, выбрав Безопасность (Security) в оснастке *Просмотр событий* (Event Viewer) и дважды щелкнув нужное событие.

Подготовка к экзамену Помните, что события входа в систему учетных записей необходимо проверять на всех контроллерах домена. События входа в систему необходимо проверять на всех системах.

Управление проверкой подлинности пользователей

Когда пользователи забывают свои пароли, перемещаются или отключаются, вам необходимо соответственно управлять объектами этих пользователей. Наиболее распространенные административные задачи, связанные с учетными записями пользователей, — это разблокирование учетной записи, смена пароля, отключение, включение, переименование и удаление объектов пользователей.

Разблокирование учетной записи пользователя

Политика блокировки учетных записей требует, чтобы при превышении предела неудачных попыток входа учетная запись пользователя блокировалась и в течение указанного периода времени или до разблокирования учетной записи администратором попытки входа в систему были невозможны.

Чтобы разблокировать учетную запись пользователя, щелкните объект пользователя и в меню **Действие (Action)** выберите **Свойства (Properties).** Перейдите на вкладку **Учетная запись (Account)** и снимите флажок **Заблокировать учетную запись (Account Is Locked Out).**

Смена паролей пользователей

Если пользователь забыл пароль, необходима смена пароля. Для этого не требуется знать старый пароль пользователя. Просто щелкните объект пользователя и в меню **Действие (Action)** выберите **Смена пароля (Reset Password).** Дважды введите новый пароль, чтобы подтвердить изменение. Кроме того, общепринятая практика в таких случаях — установить флажок **Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon).**

Включение, отключение, переименование и удаление объектов пользователей

Изменения в штате могут потребовать отключения, включения и переименования объектов пользователей. Эти действия выполняются схожим образом. Щелкните объект пользователя и в меню **Действие (Action)** выберите нужную команду:

- **отключение и включение** — если пользователю в течение длительного периода времени не требуется доступ к сети, отключите его учетную запись, а когда пользователю снова потребуется войти в сеть, включите ее. Заметьте, что в зависимости от текущего состояния объекта в меню **Действие (Action)** вы увидите только одну из команд: **Отключить (Disable)** или **Включить (Enable);**
- **удаление** — если пользователь уволился, а замены в скором времени не ожидается, удалите его объект. Помните, что, удалив пользователя, вы удалите сведения о его членстве в группах и (из-за удаления SID) его права и разрешения. Если вы затем создадите объект пользователя с тем же именем, у него будет другой SID, и вам потребуется переназначить права, разрешения и группы;
- **переименование** — объект пользователя потребуется переименовать, допустим, если он изменил фамилию или уволился, но для него планируется замена, и вы хотите сохранить права, разрешения, сведения о членстве в группах и большинство свойств.

Совет Необходимо четко уяснить разницу между отключением и удалением объекта, а также между включением и разблокированием пользователя.

Лабораторная работа. **Проверка подлинности: безопасность и устранение неполадок**

На этой лабораторной работе вы настроите политики аудита в домене. Затем вы сгенерируете события входа. В заключение вы проанализируете результаты этих входов и устраните неполадки.

Упражнение 1. Настройка политик

1. Откройте консоль *Active Directory — пользователи и компьютеры.*
2. Щелкните узел домена Contoso.com.
3. В меню **Действие (Action)** выберите **Свойства (Properties).**
4. На вкладке **Групповая политика (Group Policy)** выберите Default Domain Policy и щелкните **Изменить (Edit).**
5. Раскройте узлы **Конфигурация компьютера (Computer Configuration), Конфигурация Windows (Windows Settings), Параметры безопасности (Security Settings), Политики учетных записей (Account Policies)** и **Политика блокировки учетной записи (Account Lockout Policy).**
6. Дважды щелкните политику **Блокировка учетной записи на (Account Lockout Duration).**
7. Установите флажок **Определить следующий параметр политики (Define This Policy Setting).**
8. Установите продолжительность периода в 0 и щелкните **Применить (Apply).**
   Система потребует подтверждения на изменение порога блокировки учетной записи и сброс политик счетчика. Щелкните **OK.**
9. Щелкните **OK**, чтобы подтвердить введенные параметры, затем щелкните **OK** в окне **Политика (Policy).**
10. Убедитесь, что значение политики **Блокировка учетной записи на (Account Lockout Duration)** — 0, пороговое значение — 5 и сброс политики счетчика произойдет через 30 минут.
11. Закройте окно **Редактор объектов групповой политики (Group Policy Object Editor).**
12. Щелкните **OK,** чтобы закрыть диалоговое окно **Свойства (Properties)** для домена contoso.com.
13. Щелкните контейнер **Контроллеры домена (Domain Controllers),** расположенный по иерархии ниже узла домена.
14. В меню **Действие (Action)** выберите **Свойства (Properties).**
    На вкладке **Групповая политика (Group Policy)** выберите Default Domain Controllers Policy и щелкните **Изменить (Edit).**
16. Раскройте узлы **Конфигурация компьютера (Computer Configuration), Конфигурация Windows (Windows Settings), Параметры безопасности (Security Settings), Локальные политики (Local Policies)** и **Политика аудита (Audit Policy).**
17. Дважды щелкните политику ***Аудит событий входа в систему*** **(Audit Account Logon Events).**
18. Выберите **Определить следующий параметр политики (Define These Policy Settings),** установите флажки **Успех (Success)** и **Отказ (Failure)** и щелкните **OK.**
19. Дважды щелкните политику **Аудит входа в систему (Audit Logon Events).**
20. Выберите **Определить следующий параметр политики (Define These Policy Settings),** установите флажки **Успех (Success)** и **Отказ (Failure)** и щелкните **OK**.

21. Дважды щелкните политику **Аудит управления учетными записями (Audit Account Management).**
22. Выберите **Определить следующий параметр политики (Define These Policy Settings),** установите флажок **Успех (Success)** и щелкните **OK.**
23. Закройте окно **Редактор объектов групповой политики (Group Policy Object Editor).**
24. Щелкните OK, чтобы закрыть окно свойств для окна Domain Controllers Properties.

Упражнение 2. Генерация событий входа в систему

1. Завершите сеанс на Server01.
2. Сгенерируйте два события неудачного входа в систему, дважды попытавшись войти с именем пользователя sbishop и неверным паролем.
3. Войдите в систему правильно (как пользователь sbishop).
4. Выйдите из системы.

Упражнение 3. Генерация событий управления учетными записями

1. Войдите в систему как *Администратор* (Administrator).
2. Откройте консоль *Active Directory — пользователи и компьютеры*.
3. В дереве выберите ОП Employees.
4. В правой панели выберите объект пользователя Scott Bishop и раскройте меню **Действие (Action).**
5. Выберите команду **Смена пароля (Reset Password).**
6. Введите и подтвердите новый пароль для Scott Bishop, затем щелкните **OK.**

Упражнение 4. Анализ событий безопасности, сгенерированных проверкой подлинности

1. Откройте консоль *Управление компьютером* (Computer Management) из группы **Администрирование (Administrative Tools).**
2. Раскройте узел **Просмотр событий (Event Viewer)** и щелкните **Безопасность (Security).**
3. Расширьте столбец **Категория (Category),** чтобы видеть типы зарегистрированных событий.
4. Изучите события, сгенерированные действиями, которые вы только что выполнили. Обратите внимание на события неудачного и удачного входа в систему, а также на смену пароля для пользователя Scott Bishop.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Для своего домена вы включаете политику надежных паролей. Опишите требования к паролям, а также условия, при которых соблюдение этих требований приведет к результату.
2. Вам нужно вести мониторинг потенциальных атак по словарю в отношении паролей пользователей предприятия. Какую политику аудита достаточно включить? Какой журнал или журналы следует анализировать?

3. Пользователь, забыв пароль, несколько раз пытается войти в систему с неверным паролем и в конце концов получает сообщение, что учетная запись отключена или заблокирована. Он обращается к администратору. Что следует сделать?
   a. Удалить объект пользователя и заново создать его.
   b. Включить объект пользователя.
   c. Разблокировать объект пользователя.
   d. Изменить пароль для объекта пользователя.

Резюме

- Политика Default Domain Policy управляет политиками учетных записей, в том числе политиками паролей и блокировки.
- Политика Default Domain Controllers Policy управляет ключевыми политиками аудита для контроллеров домена.
- Аудит проверки подлинности генерирует события в журнале безопасности на каждом контроллере домена.

Пример из практики

Один из конкурентов Contoso недавно заявил, что стал жертвой взлома системы безопасности паролей, вследствие чего были утеряны важные данные. Вы решаете включить **аудит** конфигурации безопасности и формулируете следующие требования.

- **Требование 1.** Поскольку вы обновили контроллеры домена с Windows 2000 Server до Windows Server 2003, действует политика учетных записей домена, настроенная в Windows 2000 Server. Политики учетных записей домена требуют, соблюдения следующих условий:
  - пароли меняются каждые 60 дней;
  - длина пароля — не менее 8 символов;
  - пароль должен быть достаточно сложным;
  - минимальный срок действия пароля — неделя;
  - должна храниться история из 20 паролей;
  - учетная запись должна блокироваться после пяти неудачных попыток входа в течение одного часа;
  - для разблокирования учетных записей необходимо вмешательство администратора.
- **Требование 2.** Нужно гарантировать, что эти политики вступают в силу в течение 24 часов. Политики паролей срабатывают, когда пользователь меняет свой пароль, и не влияют на существующие пароли. Следовательно, вы требуете, чтобы пользователи изменяли пароли как можно быстрее. Вы не хотите затрагивать учетные записи, используемые службами. Учетные записи служб хранятся в ОП Service Accounts для Contoso. Учетные записи пользователей хранятся в ОП Employees и в 15 подчиненных ему ОП.
- **Требование 3.** Рабочие столы торговых представителей должны быть отключены, чтобы они не могли устанавливать свои Web-панели инструментов, программы получения прогноза погоды, средства автоматической смены обоев или другое ПО, которое может подключиться к Интернету и открыть рабочий стол для атаки.

Требование 1

Первое требование касается изменения параметров паролей и блокировки учетных записей.

1. Какой элемент следует изменить для соблюдения требования 1?
   a. Шаблон безопасности контроллера домена Hisecdc.inf.
   b. Политика домена по умолчанию (Default Domain).
   c. Политика контроллера домена по умолчанию (Default Domain Controller).
   d. Шаблон безопасности контроллера домена Ssetup Security.inf.

   Правильный ответ: b.
2. Какую политику нужно настроить, чтобы для разблокирования учетной записи пользователь обращался в службу поддержки вашей организации?
   a. *Блокировка учетной записи на* (Account Lockout Duration): 999.
   b. *Пороговое значение блокировки* (Account Lockout Threshold): 999.
   c. *Блокировка учетной записи на* (Account Lockout Duration): 0.
   d. *Пороговое значение блокировки* (Account Lockout Threshold): 0.

   Правильный ответ: c.

   Настройте соответствующие политики домена. Инструкции вы найдете в упражнении 1 занятия 4.

Требование 2

Требование 2 подразумевает, что пользователей нужно заставить изменить свои пароли как можно быстрее. Вы знаете, что для учетных записей пользователей установлен флажок **Требовать смену пароля при следующем входе** в **систему (User Must Change Password At Next Logon).**

1. Укажите самый быстрый и эффективный способ настройки учетных записей, чтобы при следующем входе в систему пользователи сменили пароль.
   a. Выбрать учетную запись пользователя. Раскрыть ее свойства и на вкладке **Учетная запись (Account)** выбрать **Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon).** Повторить для учетных записей всех пользователей.
   b. Нажать Ctrl+A для выбора всех пользователей в ОП Employees. В меню **Действие (Action)** щелкнуть **Свойства (Properties)** и на вкладке **Учетная запись (Account)** выбрать **Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon).** Повторить для всех ОП.
   c. Использовать команду DSADD.
   d. Использовать команду DSRM.
   e. Использовать команды DSQUERY и DSMOD.

   Правильный ответ: e.
2. Команда DSQUERY позволяет создавать списки объектов на основе местоположения или свойств этих объектов и передавать их по каналу команде DSMOD, которая модифицирует объекты. Из командной строки исполните следующую команду:

   ```
   DSQUERY user "OU=Employees,DC=Contoso,DC=Com"
   ```

   Эта команда выдаст список всех объектов пользователей в ОП Employees. Ее преимущество в том, что она учитывает пользователей в подчиненных ОП, расположен-

ных ниже ОП Employees в иерархии. В требовании указано, что в ОП Employees содержится 15 других ОП. Все они будут обработаны командой DSQUERY.

Теперь, чтобы соблюсти требование, исполните следующую команду:

```
DSQUERY user "OU=Employees,OC=Contoso,DC=Com" | DSMOD user -mustchpwd yes
```

Требование 3

Это требование предполагает, что вам необходимо модифицировать профили пользователей для торговых представителей.

1. Какой тип профиля наиболее удобен для поддержки защищенного от записи Рабочего стола, общего для всех торговых представителей?
   a. Локальный профиль.
   b. Локальный обязательный профиль.
   c. Профиль *Все пользователи* (All Users).
   d. Преднастроенный перемещаемый групповой профиль.
   e. Преднастроенный перемещаемый обязательный групповой профиль.

   Правильный ответ: b.
2. В упражнении 5 занятия 3 вы создали профиль с именем Sales. Вы сделали его обязательным, переименовав Ntuser.dat в Ntuser.man, затем назначили его нескольким пользователям. Как можно гарантировать, что любой новый торговый представитель будет использовать один и тот же профиль?

   Правильный ответ: Измените шаблон учетной записи Sales Representative, который вы создали в упражнении 1 занятия 2. На вкладке Профиль (Profile) введите следующий путь: \\server01\profiles\sales. Убедитесь, что задание было выполнено **успешно, скопировав шаблон для создания новой учетной записи пользователя; затем войдите в систему под именем этого пользователя. Измените рабочий стол, выйдите из системы и войдите снова. Изменения профиля не сохранились между сеансами.**

Практикум по устранению неполадок

На этом практикуме вы сгенерируете несколько ошибок входа в систему и ошибок, связанных с учетными записями. Затем вы установите причины ошибок и исправите их.

Для выполнения этого упражнения понадобится несколько учетных записей пользователей. Учетные записи, которые упоминаются в этом упражнении, были **сгенерированы** в упражнении 3 занятия 2. Также необходимо, чтобы политики учетных записей **домена** были настроены, как в упражнении 1 занятия 4.

Упражнение 1. Генерация ошибок входа в систему и ошибок, связанных с учетными записями

1. Завершите сеанс на ServerOl.
2. Вызовите блокировку учетной записи, шесть раз попытавшись войти в систему с именем пользователя lsmithbates и неверным паролем. Обратите внимание на различия между сообщениями, которые вы получали после очередных попыток, и сообщением, полученным после блокировки учетной записи.
3. Войдите в систему как Danielle Tiedt с именем пользователя dtiedt.

4. Нажмите Ctrl+Alt+Del и измените пароль.
5. Нажмите Ctrl+Alt+Del и попытайтесь изменить пароль на исходный. Это возможно? Почему?
6. Попытайтесь задать другой новый пароль. Это возможно? Почему?
7. Выйдите из системы.

Упражнение 2. Наблюдение и идентификация событий входа в систему и событий управления учетными записями

1. Войдите в систему как *Администратор* (Administrator).
2. Откройте консоль *Управление компьютером* (Computer Management) из группы **Администрирование** (Administrative **Tools).**
3. Раскройте узел **Просмотр событий (Event Viewer)** и щелкните **Безопасность (Security).**
4. Расширьте столбец **Категория (Category),** чтобы видеть типы зарегистрированных событий.
5. Изучите события, сгенерированные действиями, которые вы только что выполнили. Обратите внимание на неудачные попытки входа, блокировку и попытки изменить пароль пользователя Danielle Tiedt.

Упражнение 3. Решение проблем, связанных с проверкой подлинности и учетными записями

1. Откройте консоль *Active Directory — пользователи и компьютеры.*
2. В дереве выберите ОП Employees.
3. В правой панели выберите объект пользователя Danielle Tiedt.
4. В меню **Действие (Action)** выберите **Смена пароля (Reset Password).**
5. Введите исходный пароль пользователя Danielle Tiedt. Почему вы можете изменить пароль таким образом, хотя, будучи в системе под именем Danielle Tiedt, не могли это сделать?
6. Выберите объект пользователя Lorrin Smith-Bates.
7. В меню **Действие (Action)** выберите **Свойства (Properties).**
8. На вкладке **Учетная запись (Account)** снимите флажок **Заблокировать учетную запись (Account Is Locked Out).**
9. Щелкните **OK.**

Резюме главы

- Чтобы создавать объекты пользователей, вы должны быть членом групп *Администраторы предприятия* (EnterpriseAdmins), *Администраторы домена* (DomainAdmins) или *Операторы учета* (Account Operators) либо вам должны быть делегированы административные полномочия.
- Объекты пользователей содержат свойства, обычно связанные с учетной записью пользователя, в том числе имена для входа и пароль, и уникальный для каждого пользователя идентификатор безопасности (SID). Также объекты пользователя включают

свойства, относящиеся к представляемому ими человеку: личную информацию, членство в группах и административные настройки. Windows Server 2003 позволяет одновременно изменять некоторые из этих свойств для нескольких пользователей.

- Шаблон объекта пользователя — это объект, путем копирования которого создаются новые пользователи. Если шаблон не является «настоящим» пользователем, его следует отключить. Из шаблонов копируется только подмножество свойств пользователя.
- Команда CSVDE позволяет импортировать объекты каталога из текстового CSV-файла с разделителями — запятыми.
- Windows Server 2003 поддерживает новые средства командной строки, позволяющие создавать и удалять объекты каталога и управлять ими: DSQUERY, DSGET, DSADD, DSMOVE, DSMOD и DSRM. Часто набор объектов, возвращенных DSQUERY, передается по каналу другим командам.
- Windows Server 2003 создает индивидуальные профили для всех пользователей, которые входят в систему. По умолчанию профили хранятся на локальной системе в папке *%Systemdrive%\Documents* and Settings\%Username%.
- Для применения перемещаемых профилей необходимо лишь настроить общую папку и указать путь к профилю в свойствах объекта пользователя.
- Преднастроенные профили — это обычные профили, которые копируются в каталог профилей до того, как путь к нему указывается в объекте пользователя.
- Групповые профили должны быть обязательными, для этого необходимо переименовать Ntuser.dat в Ntuser.man, чтобы изменения, внесенные одним пользователем, не влияли на других.
- Политика Default Domain Policy управляет политиками учетных записей, в том числе политиками паролей и блокировки учетных записей, а Default Domain Controllers Policy — ключевыми политиками аудита для контроллеров домена.
- Аудит проверки подлинности генерирует события в журнале безопасности на каждом контроллере домена.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Членство в группах и разрешения, необходимые для создания учетных записей пользователей.
- Инструменты, предусмотренные для создания и управления несколькими учетными записями пользователей: шаблоны объектов пользователей, средства импорта, программы командной строки. Необходимо понимать, чем они отличаются, а также плюсы и минусы каждого из них.
- К свойствам можно обращаться и модифицировать их при создании объекта пользователя, изменении объекта в консоли *Active Directory — пользователи и компьютеры* (Active Directory Users and Computers), копировании шаблона, выполнении запроса командой DSQUERY, а также добавлении и изменении объектов пользователей командами DSADD и DSMOD.

- Процесс настройки перемещаемого профиля пользователя, преднастроенного перемещаемого профиля пользователя или преднастроенного обязательного группового профиля.
- Влияние групповой политики на настройки паролей и параметры блокировки учетных записей.
- Как производить аудит событий проверки подлинности пользователей.

Основные термины

Шаблон учетной записи пользователя ~ user account template — шаблон учетной записи берется за основу для новых учетных записей. Он копируется для создания нового объекта пользователя, а также копируются некоторые из его свойств, главное из которых — членство в группах. Его могут называть иначе, но суть не меняется.

Отключенная и заблокированная учетная запись- disabled account versus locked account — учетная запись отключается, если срок ее действия истек, или же вручную администратором. Учетная запись блокируется, если ее использовали для неудачных входов в систему и при этом превысили порог, указанный в политике блокировки учетных записей.

Обязательный профиль ~ mandatory profile — профиль пользователя, который между сеансами не сохраняет изменения. Пользователь может изменить обязательный профиль, но эти изменения не сохранятся, после того как он выйдет из системы. Групповые профили должны быть обязательными, иначе изменения, внесенные одним пользователем, повлияют на остальных.

Вопросы и ответы

Занятие 1. Закрепление материала

1. Вы настраиваете объекты пользователей в своем домене с помощью консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) и можете изменять свойства адреса и номера телефона для объекта представляющего вас пользователя. Однако команда **Новый пользователь (New User)** недоступна. В чем причина?

   Правильный ответ: у вас нет достаточных привилегий для создания объектов пользователей в контейнере. Набор команд в консоли изменяется в зависимости от ваших административных возможностей. Если у вас нет права создавать объекты, соответствующая команда Новый (New) будет недоступна.

2. Вы создаете набор объектов пользователей для временных сотрудников организации. Они будут работать по контракту ежедневно с 9:00 до 17:00. Работа начнется через месяц, а закончится через два месяца с сегодняшнего числа. Эти сотрудники не будут работать в неурочное время. Какие из следующих свойств следует сразу настроить, чтобы гарантировать максимальную безопасность объектов этих пользователей?

   a. **Пароль (Password).**

   b. Время входа (Logon Hours).

   c. Срок действия учетной записи (Account Expires).

d. **Хранить пароль, используя обратимое шифрование (Store password using reversible encryption).**
e. **Учетная запись доверена для** делегирования **(Account is trusted for delegation).**
f. **Требовать смену пароля при следующем входе в систему (User must change password at next logon).**
g. **Отключить учетную запись (Account is disabled).**
h. **Срок действия пароля не ограничен (Password never expires).**

Правильный ответ: a, Ь, c, f, g.

5 Какие из следующих свойств и административных задач можно настраивать или изменять одновременно для нескольких объектов пользователей?

a. **Фамилия (Last Name).**
b. **Имя входа пользователя (User Logon Name).**
c. **Disable Account (Отключить учетную запись).**
d. **Включить учетную запись (Enable Account).**
e. **Смена пароля (Reset Password).**
f. **Срок действия пароля не ограничен (Password Never Expires).**
g. **Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon).**
h. **Время входа (Logon Hours).**
i. **Ограничения компьютера (Рабочие станции для входа в систему) [Logon Workstations (Computer Restrictions)].**
j. **Должность (Title),**
k. **Прямые подчиненные (Direct Reports).**

Правильный ответ: c, d, f, g, h, i, j.

Занятие 2. Закрепление материала

1. Как наиболее эффективно создать 100 новых объектов пользователей с одинаковыми путями к профилю и домашней папке и с одинаковыми значениями параметров **Должность (Title), Веб-страница (Web Page), Организация (Company), Отдел (Department) и Руководитель (Manager)?**

   Правильный ответ: наиболее удобный вариант — команда DSADD. В одной строке команды можно ввести все параметры. Не указав значение для параметра *DN_пользователя,* вы сможете вводить различающиеся имена пользователей по одному в окне командной строки. Шаблон объекта пользователя не разрешает настраивать такие параметры, как Title (Должность), Telephone Number (Номер телефона) и Web Page (Веб-страница). По сравнению с этим создание текстового CSV-файла займет слишком много времени и будет слишком сложным решением для случая, когда есть столько одинаковых параметров.

2. Какая команда поможет найти учетные записи, не использовавшиеся в течение двух месяцев?

a. DSADD.
b. DSGET.
c. DSMOD.
d. DSRM.
e. DSQUERY.

Правильный ответ: e.

3. Какую переменную можно использовать в командах DSMOD и DSADD для создания домашних папок и папок профилей для определенных пользователей?
   a. *%Username%*.
   b. $Username$.
   c. *CN=Username.*
   d. *<Username>*.
   Правильный ответ: b.
4. При помощи какой команды можно вывести номера телефонов всех пользователей в.ОП?
   a. DSADD.
   b. DSGET.
   c. DSMOD.
   d. DSRM.
   e. DSQUERY.
   Правильный ответ: b, e. DSQUERY создаст список объектов пользователей в ОП и может передать этот список по каналу команде DSGET, которая, в свою очередь, может выдать отдельные свойства, например номера телефона.

Занятие 3. Закрепление материала

1. Опишите, как формируется рабочий стол пользователя, если перемещаемые профили не применяются.
   Правильный ответ: когда пользователь входит в систему впервые, она копирует профиль Default User и создает профиль специально для этого пользователя в папке с именем *%Systemdrive%\Documents* and Settings*%Username%*. Пользователь работает в среде, которая является комбинацией его профиля и профиля Все пользователи (All Users).
2. Расположите по порядку шаги, в результате которых создается преднастроенный перемещаемый профиль пользователя. Задействуйте все перечисленные шаги.
   a. Настройка рабочего стола и среды пользователя.
   b. Вход под именем пользователя с разрешениями, достаточными для изменения свойств учетной записи пользователя.
   c. Копирование профиля в сеть.
   d. Создание учетной записи пользователя таким образом, чтобы профиль можно было сформировать, не изменяя текущие профили остальных пользователей.
   e. Вход в систему под учетной записью профиля.
   f. Ввод UNC-пути к профилю на странице свойств **Профиль (Profile)** объекта пользователя.
   g. Вход в систему в качестве локального администратора или администратора домена.
   Правильный ответ: d, e, a, g, c, b, f.
3. Как сделать профиль обязательным?
   a. Настроить разрешения для папки на странице свойств **Безопасность (Security),** чтобы запретить запись.
   b. Настроить разрешения для папки на странице свойств **Доступ (Sharing),** чтобы разрешить только чтение.
   c. Изменить атрибуты папки с профилем, оставив лишь атрибут **Только чтение (Read Only).**
   d. Переименовать Ntuser.dat в Ntuser.man.
   Правильный ответ: d.

Занятие 4. Закрепление материала

1. Для своего домена вы включаете политику надежных паролей. Опишите требования к паролям, а также условия, при которых соблюдение этих требований приведет к результату.

   Правильный ответ: пароль не должен зависеть от имени учетной записи пользователя, в нем должно быть не менее 6 символов. В пароле должно быть хотя бы по одному символу трех категорий: прописные и строчные буквы, арабские цифры, специальные символы. Требования вступают в силу немедленно для всех новых учетных записей. Для существующих **учетных записей этих условия будут проверены при очередной смене пароля.**

2. Вам нужно вести мониторинг потенциальных атак по словарю в отношении паролей пользователей предприятия. Какую политику аудита достаточно включить? Какой журнал или журналы следует анализировать?

   Правильный ответ: в данном случае наиболее эффективна политика аудита для аудита отказов при входе учетных записей. Неудачные входы в систему будут генерировать события в журналах безопасности на всех контроллерах домена.

3. Пользователь, забыв пароль, несколько раз пытается войти в систему с неверным паролем и в конце концов получает сообщение, что учетная запись отключена или заблокирована. Он обращается к администратору. Что следует сделать?

   a. Удалить объект пользователя и заново создать его.
   b. Переименовать объект пользователя.
   c. Включить объект пользователя.
   d. Разблокировать объект пользователя.
   e. Изменить пароль для объекта пользователя.

   Правильный ответ: d, e. Хотя в сообщении, отображаемом в Windows 2000 и предыдущих **версиях Windows, говорится, что учетная запись отключена, на самом деле она заблокирована. Windows Server 2003 отображает верное сообщение о том, что учетная запись фактически заблокирована.** Так **что вы можете сразу выявить проблему, узиав, чем вызвано сообщение: пользователь забыл свой пароль. Следует разблокировать учетную запись и изменить ее пароль.**

ГЛАВА 4

Учетные записи групп

Темы экзамена

- Создание и управление группами:
  - создание и управление группами с помощью консоли Active Directory — пользователи и компьютеры;
  - идентификация и изменение области действия группы;
  - управление членством в группах;
  - автоматизация создания и изменения групп.

В этой главе

Пользователи, группы и компьютеры — ключевые объекты в службе каталогов Active Directory, так как они позволяют всем, кто использует компьютер в сети, идентифицировать себя в качестве участника безопасности. Без такой идентификации персонал не сможет получить доступ к компьютерам, программам и данным, необходимым для повседневной работы. Хотя для минимальной идентификации достаточно знать имя пользователя и компьютера, управление участниками безопасности для отдельного пользователя серьезно усложнится, если не организовать пользователей в группы. На определенном этапе назначать разрешения каждому из множества пользователей станет просто невозможно,' однако при разумном использовании групп назначение разрешений и управление ими сильно упрощается.

В Windows Server 2003 существует два типа групп, каждая из которых может иметь три области действия. Понимание их структуры в рамках соответствующей области действия гарантирует оптимальное распределение административных ресурсов при управлении правами доступа к ресурсам. Возможности конструкции группы также зависят от того, в каком режиме работает их родительский домен или лес Windows Server 2003: основном, промежуточном или смешанном. В Windows Server 2003 несколько групп уже созданы предварительно, или встроены. Вы можете создать дополнительно столько групп, сколько пожелаете.

Прежде всего

Для изучения материалов этой главы вам потребуется:

- компьютер под управлением Microsoft Windows Server 2003, установленный как Server01 и настроенный в качестве контроллера домена contoso.com.

Занятие 1. Понятие типа группы и области действия

Группы (groups) — это контейнеры, содержащие объекты пользователей и компьютеров. Если разрешения безопасности для группы заданы в *таблице управления доступом* (access control list, ACL) для некоего ресурса, то их получают все члены группы.

В Windows Server 2003 существует два типа групп: безопасности и распространения. *Группы безопасности* (security groups) используют для назначения разрешений доступа к сетевым ресурсам. *Группы распространения* (distribution groups) применяются для объединения пользователей в списки рассылки электронной почты. Группу безопасности можно использовать в качестве группы распространения, но не наоборот. Правильное планирование структуры групп влияет на производительность и масштабируемость, особенно в корпоративных средах, содержащих множество доменов.

Совет Хотя в таблицах ACL можно задавать параметры для отдельных участников безопасности (пользователей и компьютеров), эта практика должна быть скорее исключением щз общего правила. Если вы обнаружите, что задаете в ACL слишком много исключений *щзя* пользователя какой-либо группы, пересмотрите его членство в этой группе.

Изучив материал этого занятия, вы сможете:

- ☑ описать два типа групп и способы их использования;
- ☑ описать три типа областей действия группы и способы их использования;
- ☑ пояснить разницу между обычными и специальными группами.

Продолжительность занятия — около 15 минут.

Функциональные уровни доменов

В Windows Server 2003 доступны четыре функциональных уровня домена: смешанный Windows 2000 (выбирается по умолчанию), основной Windows 2000, промежуточный Windows Server 2003 и основной Windows Server 2003.

- **Смешанный режим Windows 2000.** Поддерживает контроллеры доменов Windows NT 4/2000 и Windows Server 2003.
- **Основной режим Windows 2000.** Поддерживает контроллеры доменов Windows 2000 и Windows Server 2003.
- **Промежуточный режим Windows Server 2003.** Поддерживает контроллеры доменов Windows 4 и Windows Server 2003.
- **Windows Server 2003.** Поддерживает контроллеры доменов Windows Server 2003.

Ограничения в отношении свойств групп, обсуждаемые в этой и других главах книги, будут относиться к этим функциональным уровням доменов.

Область действия группы

Область действия группы (group scope) определяет, каким образом участникам группы назначаются разрешения. В Windows Server 2003 и группы безопасности, и группы распространения классифицируют по трем областям действия: локальная доменная, глобальная и универсальная.

Примечание Хотя локальные группы не классифицируются по области действия Windows Server 2003, они включены для полноты картины.

Локальные группы

Локальные группы (local groups), или локальные группы компьютеров, используются в основном для обратной совместимости с Windows NT 4. На компьютерах с Windows Server 2003 существуют локальные пользователи и группы, сконфигурированные как рядовые серверы. Контроллеры доменов не используют локальные группы.

- Локальные группы могут содержать участников из любого домена в пределах леса, из доверенных доменов в других лесах и более низкого уровня.
- Локальная группа действует в пределах конкретного компьютера и может предоставлять разрешения для ресурсов только на этом компьютере.

Локальные группы домена

Локальные группы домена (domain local groups) главным образом используются для назначения глобальным группам разрешений на доступ к локальным ресурсам домена. Характерные черты локальных групп домена таковы.

- Существуют во всех режимах работы доменов и лесов — смешанном, промежуточном и основном.
- Доступны в пределах всего домена только в доменах основного режима Windows 2000 или доменах Windows Server 2003. Локальная группа домена функционирует подобно локальной группе на контроллере домена, пока домен работает в смешанном режиме.
- Могут содержать участников из любого домена в пределах леса, из доверенных доменов в других лесах и более низкого уровня.
- Действуют в пределах домена в основном режиме Windows 2000 и режиме Windows Server 2003 и могут использоваться для предоставления прав на ресурсы на любом компьютере с Windows Server 2003 в том домене, где определена группа.

Глобальные группы

Глобальные группы (global groups) чаще используются для предоставления категоризированного членства в локальных группах доменов для отдельных участников безопасности и для прямого назначения разрешений (в частности, в доменах смешанного или промежуточного режимов). Часто глобальные группы применяются для объединения пользователей или компьютеров в одном домене и совместного исполнения одной работы, роли или функции. Характеристики глобальных групп таковы.

- Существуют во всех режимах работы доменов и лесов — смешанном, промежуточном и основном.
- Могут содержать только членов из своего домена.

- Могут сами являться членами локальной группы компьютера или домена.
- Могут получать разрешения в любом домене, включая доверенные домены в других лесах и домены пред-Windows 2003.
- Могут содержать другие глобальные группы, но только в домене, работающем в основном режиме Windows 2000 или в режиме Windows Server 2003.

Универсальные группы

Универсальные группы (universal groups) в основном применяют для предоставления доступа к ресурсам во всех доверенных доменах. Однако такие группы могут использоваться только как участники безопасности (то есть как группы безопасности) в доменах, работающих в основном режиме Windows 2000 или в режиме Windows Server 2003.

- Универсальные группы могут содержать участников из любого домена в лесу.
- В домене основного режима Windows 2000 или режима Windows Server 2003 универсальным группам могут предоставляться разрешения в любом домене, включая доверенные домены в других лесах.

Совет Универсальные группы помогают представить и объединить группы, которые распределены по разным доменам и выполняют типичные функции в рамках вашей организации. Рекомендуется делать универсальными широко используемые и редко изменяемые группы.

Преобразование групп

Область действия группы определяется в момент ее создания. Однако в домене основвого режима Windows 2000 или режима Windows Server 2003 локальные группы домена и глоовальныегруппы можно преобразовать в универсальные, если исходные группы не участвуют в других группах с той же областью действия. Например, глобальную группу, водящую в состав другой глобальной группы, нельзя преобразовать в универсальную. Варианты использования доменных групп Windows Server 2003 в качестве участников безопасности приведены в табл. 4-1 (тип: группа безопасности).

Табл. 4-1. Область действия групп и допустимые объекты

Область действия группы	Допустимые объекты
Домен основного режима Windows 2000 или режима Windows Server 2003	
Локальная группа домена	Учетные записи компьютеров, пользователи, глобальные группы и универсальные группы из любого леса или доверенного домена. Локальные группы домена из того же домена. Вложенные локальные группы домена из того же домена
Глобальные группы	Пользователи, компьютеры и глобальные группы из того же домена. Вложенные глобальные группы (из того же домена), локальные группы домена или универсальные группы
Универсальные группы	Универсальные группы, глобальные группы, пользователи и компьютеры из любого домена в лесу. Вложенные глобальные группы, локальные группы домена или универсальные группы

Табл. 4-1. *(окончание)*

Область действия группы	Допустимые объекты
Домен смешанного режима Windows 2000 или промежуточного режима Windows Server 2003	
Локальная группа домена	Учетные записи компьютеров, пользователи, глобальные группы из любого домена. Не могут быть вложенными
Глобальные группы	Только пользователи и компьютеры из того же домена. Не могут быть вложенными
Универсальные группы	Недоступны

Специальные группы

Существует также несколько *специальных групп* (special identity), которые управляются самой ОС. Их нельзя создать, удалить или изменить их состав. Специальные группы не отображаются в консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) и другими средствами управления компьютером, однако им можно назначить разрешения в ACL ресурса. Некоторые специальные группы Windows Server 2003 (их также называют особыми) перечислены в табл. 4-2.

Табл. 4-2. Специальные группы и их представление

Специальная группа	Представление
Все (Everyone)	Представляет всех пользователей сети, в том числе вошедших под гостевой учетной записью, а также пользователей из других доменов. Каждый раз при входе в систему пользователь автоматически добавляется в группу *Все* (Everyone)
Сеть (Network)	Представляет пользователей, которые в настоящий момент обращаются к данному ресурсу по сети (в отличие от тех, кто обращается к ресурсу локально). При любом обращении к данному ресурсу по сети пользователь автоматически добавляется в группу *Сеть* (Network)
Интерактивные (Interactive)	Представляет всех пользователей, которые локально обращаются к ресурсу (в отличие от тех, что обращаются к ресурсу по сети). При любом обращении к данному ресурсу пользователь автоматически добавляется в группу *Интерактивные* (Interactive)
Анонимный вход (Anonymous Logon)	В эту группу зачисляются те, кто использует сетевые ресурсы, не пройдя проверку подлинности
Прошедшие проверку (Authenticated Users)	В эту группу входят все пользователи, которые прошли проверку подлинности при входе в сеть, предоставив действительную учетную запись. При назначении разрешений можно вместо *Все* (Everyone) использовать группу *Прошедшие проверку* (Authenticated Users), чтобы избежать анонимного доступа к ресурсам

Табл. 4-2. *(окончание)*

Специальная группа	Представление
Создатель-владелец (Creator Owner)	В эту группу зачисляется пользователь, который создал ресурс или получил право владения им. Например, если пользователь создал ресурс, но *Администратор* (Administrator) получил право владения им, в группе *Создатель-владелец* (Creator Owner) будет указан *Администратор*
Удаленный доступ (Dialup)	В группу *Удаленный доступ* (Dialup) зачисляют всех, кто подключен к сети через коммутируемое соединение

Внимание! Этим группам можно назначить разрешения на сетевые ресурсы, однако соблюдайте при этом осторожность. Члены этих групп могут не всегда проходить проверку подлинности в домене. Например, если вы предоставите все права на общий ресурс группе *Все* (Everyone), пользователи, подключающиеся из других доменов, также получат доступ к этому ресурсу.

Лабораторная работа. **Изменение типа и области действия группы**

На этой лабораторной работе вы создадите группы и измените их области действия.

Упражнение. Создание и изменение группы

В этом упражнении вы измените тип группы и ее область действия.

1. В консоли *Active Directory — пользователи и компьютеры* раскройте контейнер Users и создайте в нем глобальную группу распространения Agents.
2. Щелкните правой кнопкой группу Agents и выберите **Свойства (Properties).**

   Можете ли вы изменить область действия и тип этой группы? Почему?

   Если вы не можете изменить тип и область действия группы, ваш домен работает в смешанном режиме Windows 2000 или в промежуточном режиме Windows Server 2003. Чтобы изменить тип или область действия группы, необходимо перевести домен в основной режим Windows 2000 или в режим Windows Server 2003.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Какой тип доменной группы больше всего похож на локальную группу на рядовом сервере? В чем их сходство?
2. Вы используете универсальные группы в своем домене или в лесу, и вам нужно предоставить санкционированный доступ членам универсальной группы. Какая конфигурация необходима для использования универсальной группы?
3. Какие участники безопасности могут быть членами глобальной группы в домене, работающем в режиме Windows Server 2003?

Резюме

- Существует два типа групп: безопасности и распространения. Группам безопасности можно назначать разрешения, а группы распространения используются для рассылки электронной почты и им нельзя назначать разрешения доступа к ресурсам.
- Разрешения безопасности для группы назначаются в ACL, как и для любого другого участника безопасности, например пользователя или компьютера.
- В доменах основного режима Windows 2000 или режима Windows Server 2003 группы безопасности и распространения могут иметь конструкцию локальной группы домена, глобальной или универсальной группы, причем в каждом случае у них может быть разная область действия, что определяет, какие участники безопасности могут входить в эти группы.

Занятие 2. Управление учетными записями групп

Консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) является основным средством, которое вы будете использовать для управления объектами (пользователями, группами и компьютерами) в домене. При создании групп вы будете указывать область действия, тип и состав. Также с помощью этой консоли вы сможете изменить состав существующих групп.

Изучив материал этого занятия, вы сможете:

- ✓ создавать группы;
- ✓ изменять состав группы;
- ✓ находить доменные группы, к которым относится пользователь.

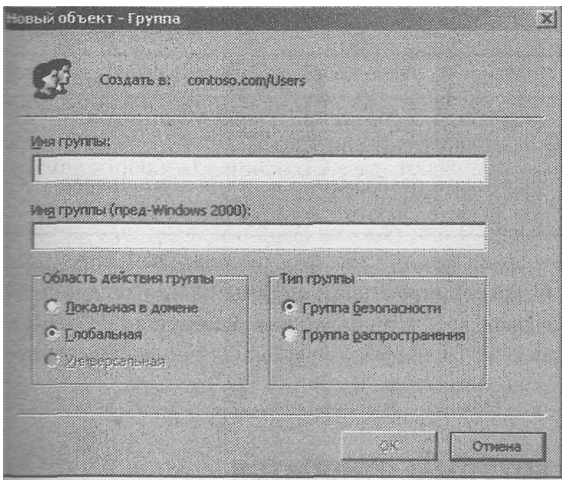
Продолжительность занятия — около 10 минут.

Создание группы безопасности

Обычно группы создают из консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers), ярлык которой расположен в группе программ **Администрирование (Administrative Tools).** В окне консоли щелкните правой кнопкой в правой панели контейнера, где вы хотите создать группу, и выберите **Создать (New)\Группа (Group).** Затем определите тип и область действия создаваемой группы.

Чаще всего вы будете создавать группы безопасности, поскольку им можно назначать разрешения в ACL. В домене смешанного или промежуточного режима группа безопасности может быть только глобальной или локальной группой домена. В таком домене нельзя создать группу безопасности с универсальной областью действия (рис. 4-1).

Впрочем, локальную группу домена, глобальную или универсальную группу в доменах смешанного или промежуточного режима можно создать в виде группы распространения. Группы безопасности в таком домене могут иметь локальную доменную или глобальную область действия.



Ряс. 4-1. Группы безопасности в доменах смешанного или промежуточного режима

Изменение состава группы

Добавление или удаление членов группы также выполняется из консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers). Щелкните правой кнопкой любую группу и выберите Свойства (Properties). На рис. 4-2 показано окно свойств для глобальной группы безопасности Sales.

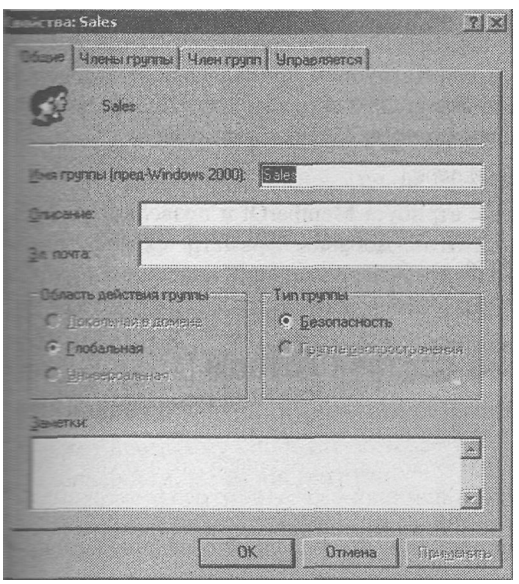


***Рис.* 4-2. Окно свойств группы безопасности Sales**

В табл. 4-3 описаны вкладки этого окна свойств для настройки членства.

Табл. 4-3. Настройка членства

Вкладка	Назначение
Члены группы (Members)	Добавление, удаление и отображение списка участников безопасности — членов этого контейнера
Член групп (Member 00	Добавление, удаление и отображение перечня контейнеров, членом которых является данный контейнер

Примечание Об использовании средств командной строки службы каталогов для просмотра и изменения состава группы — в главе 3. К этим средствам относятся DSQUERY, DSGET, DSMOD и DSGROUP. Команда DSGET особенно удобна для получения списка всех групп, членом которых является пользователь.

Поиск доменных групп, к которым относится пользователь

Служба каталогов Active Directory предоставляет гибкий и удобный механизм вложения групп.

- Глобальные группы могут быть вложены в другие глобальные, универсальные группы или локальные группы домена.
- Универсальные группы могут участвовать в других универсальных группах или локальных группах домена.
- Локальные группы домена могут участвовать в других локальных группах домена.

Вместе с тем, такая гибкость повышает сложность, и без соответствующих инструментов было бы трудно точно определить, к каким группам принадлежит пользователь (прямо или косвенно). К счастью, в Windows Server 2003 есть команда DSGET, которая решает эту проблему. Из командной строки исполните следующую команду:

dsget user *DN_пользователя* -memberof [-expand]

Параметр -memberof возвращает значение атрибута MemberOf и позволяет увидеть, к каким группам явно принадлежит пользователь. Добавив параметр -expand, можно провести рекурсивный поиск в группах и получить исчерпывающий список всех групп в домене, к которым принадлежит пользователь.

Лабораторная работа. Изменение состава группы

На этой лабораторной работе вы познакомитесь со вложенными группами, а также изучите возможные комбинации членства.

Упражнение. Вложенные группы

1. Домен должен работать в режиме Windows Server 2003. Если это не так, измените режим домена в консоли *Active Directory — пользователи и компьютеры*.
2. Создайте три глобальные группы в ОП Users: Group1, Group 2 и Group 3.
3. Добавьте три учетные записи пользователей: User 1, User 2 и User 3.
4. Добавьте User I, User 2 и User 3 в группу Group 1.
5. Добавьте Group 1 в группу Group 2.

   Какие группы теперь можно преобразовать в универсальные? Проверьте свои теоретические знания (вы должны без проблем преобразовать две из трех этих групп).

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. На какой вкладке в окне свойств группы можно добавить в нее пользователей?
2. Вы хотите, чтобы группа IT Administrators, члены которой администрируют участников группы Sales, была вложена в Sales и имела доступ к тем же ресурсам (определенным разрешениями в ACL), что и Sales. На какой вкладке в окне свойств группы IT Administrators можно выполнить такую настройку?
3. Если в вашей системе два домена (на базе Windows Server 2003 и Windows NT 4), группы какой области действия можно использовать, чтобы назначить разрешения для любого ресурса на любом компьютере в домене?

Резюме

- Состав групп настраивают в консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers).
- Если вы открыли окно свойств для участника безопасности, которого нужно включить в группу, членство в группах настраивается на вкладке **Член групп (Members Of)**. Если вы открыли окно свойств для контейнера (группы), куда нужно добавить участников, членство настраивается на вкладке **Члены группы (Members).**
- Группы могут быть вложенными, если они находятся в домене, работающем в основном режиме Windows 2000 или в режиме Windows Server 2003. Если домен работает в смешанном или промежуточном режимах, то есть подразумевается, что вы поддерживаете контроллеры домена на базе Windows NT 4, вкладывать группы друг в друга нельзя.
- Изменение типа или области действия группы допустимо, только когда домен работает в основном режиме Windows 2000 или в режиме Windows Server 2003.

Занятие 3. Автоматизация управления учетными записями групп

Хотя консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) — удобный инструмент для создания и изменения отдельных групп, она не эффективна при массовом создании участников безопасности. Windows Server 2003 содержит программу Ldifde.exe, которая упрощает массовый импорт и экспорт участников безопасности, в том числе групп.

Изучив материал этого занятия, вы сможете:

- ✓ импортировать участников безопасности средствами LDIFDE;
- ✓ экспортировать участников безопасности средствами LDIFDE;
- ✓ использовать команды DSADD и DSMOD для создания и изменения групп.

Продолжительность занятия — около 30 минут.

Команда LDIFDE

Формат обмена данными по протоколу LDAP (LDIF) — это проект интернет-стандарта на формат файла, который можно использовать для массовых операций в LDAP-каталогах. Формат LDIF можно использовать для массового экспорта и импорта данных, например для добавления, создания и изменения элементов в каталоге Active Directory. В состав Windows Server 2003 включена программа LDIFDE для пакетной обработки файлов формата LDIF.

LDIFDE — это средство командной строки, доступное во всех редакциях Windows Server 2003. LDIFDE запускается из командной строки или командной оболочки с подходящими параметрами. На рис. 4-3 показаны основные параметры LDIFDE. Полный перечень можно просмотреть, исполнив в командной строке ldifde /?.

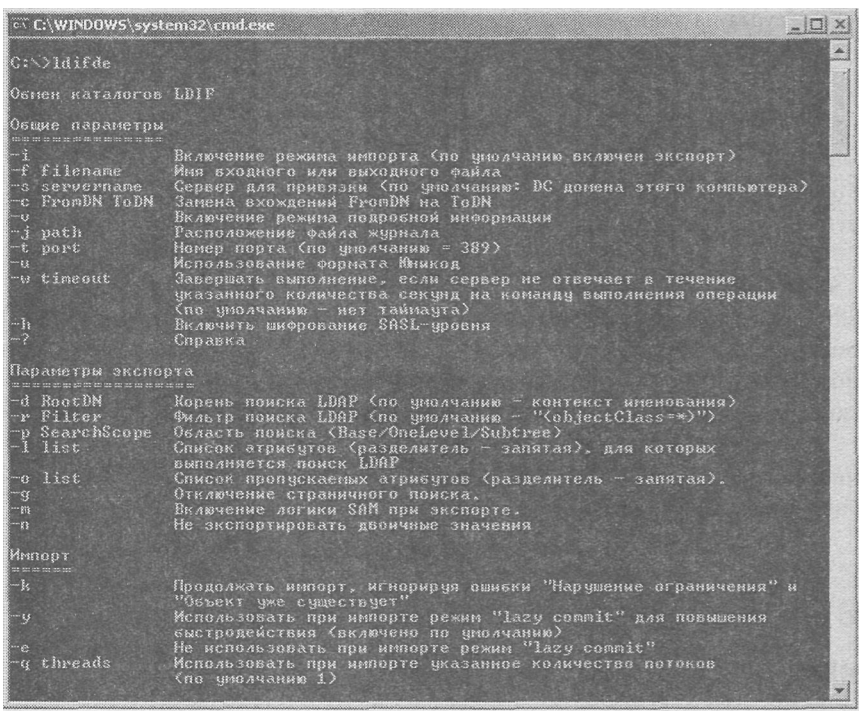


Рис. 4-3. **Справка по** команде **LDIFDE**

В табл. 4-4 подробно рассмотрены основные параметры LDIFDE.

Табл. 4-4. Основные параметры команды LDIFDE

Параметр	Использование
Общие параметры	
-i	Включает режим импорта; по умолчанию программа работает в режиме экспорта
-f *имя_файла*	Указывает *имя_файла* для импорта или экспорта
-s *имя_сервера*	Определяет сервер (контроллер домена), выполняющий операцию импорта или экспорта

Табл. 4-4. *(окончание)*

Параметр	Использование
-c *строка1 строка2*	Заменяет вхождения *строка1* на *строка2;* обычно в качестве таких строк указывают исходное и целевое различающиеся имена
-v	Включение режима вывода дополнительной информации
-j *путь*	Путь к файлу журнала
-t *номер_порта*	Указывает номер порта LDAP, по умолчанию — 389
-?	Выводит справочную информацию
Параметры экспорта	
-d *различающееся_имя_базы*	Корень поиска LDAP, по умолчанию — контекст именования
-г *фильтрLOAP*	Фильтр поиска LDAP, по умолчанию — «(objectClass=*)»
-р *область поиска*	Область поиска, одно из трех константных значений: Base/OneLevel/Subtree
-l *список_атрибутов_LDAP*	Список атрибутов, разделенных запятыми, которые следует искать в LDAP
-o *список_атрибутов_LDAP*	Список атрибутов, разделенных запятыми, которые следует исключить из выборки
-g	Отключает постраничный поиск
-m	Включает логику диспетчера учетных записей безопасности (SAM) для экспорта. Позволяет пропускать атрибуты, применяемые только к объектам Active Directory, например ObjectGUID, objectSID, pwdLastSet и samAccountType
-n	Отключает экспорт двоичных значений
Параметры импорта	
-к	Игнорирование ошибок **«нарушение ограничения» («Constraint Violation»)** и **«объект уже существует» («Object Already Exists»)** и ряда других при импорте
Параметры учетных данных (реквизитов)	
-a *DN_пользователя*	Указывает, что команда должна быть запущена с указанным различающимся именем пользователя и паролем. Например: «cn=administrator,dc=contoso, dc-com password»
-b *имя_пользователя имя_домена*	Указывает, что команда должна быть запущена от имени пользователя в домене с заданным паролем. По умолчанию команда выполняется с теми реквизитами, которые пользователь указал при входе в систему

Примечание Программа LDIFDE включена в состав Windows Server 2003, ее также можно скопировать на компьютер под управлением Windows 2000 Professional или Windows XP. Затем ее можно «привязать» к Active Directory на компьютере с Windows Server 2003 и использовать через удаленное соединение.

Создание учетных записей

Часто приходится иметь дело с набором данных, уже содержащим часть информации, которую вы хотели бы поместить в Active Directory. Эти данные могут находиться в домене более низкого уровня [Windows NT 4/2000, NDS (Novell Directory Services)] или в базе данных иного типа (допустим, в БД отдела кадров).

Если у вас есть данные о пользователях, вы можете загрузить их в Active Directory. Существует много средств, облегчающих извлечение данных, например Addusers для Windows NT 4 или LDIFDE для Windows 2000. Кроме того, в большинстве СУБД имеются средства экспорта данных в файл с разделителями — запятыми (Comma-Separated-Value, CSV), который затем можно импортировать командой LDIFDE. Если вы решите использовать CSV-файлы, то вам следует знать, что некоторые элементы обязательны для создания объекта и их отсутствие в таком файле вызовет ошибки импорта. Впрочем, для создания группы требуется знать лишь ее различающееся имя (CN=User) и местоположение (DC=Domain, DC=OU), которые вы вряд ли пропустите.

Совсем несложно добавить в импортируемый файл данные об ОП и группах, чтобы с помощью LDIFDE быстрее сформировать каталог Active Directory.

Создание групп командой DSADD

Команда DSADD, которую мы обсуждали в главе 2, добавляет объекты в Active Directory. Для добавления группы используется следующий синтаксис:

dsadd group *DN_группы...*

Параметр *DN_группы...* задает одно или несколько различающихся имен для новых объектов групп. Если в DN есть пробел, заключите все имя в кавычки. Параметр *DN_группы...* можно вводить следующими способами.

- Передача по каналу списка DN-имен, полученного при выполнении другой команды, например DSQUERY.
- Указание всех DN-имен в командной строке через пробел.
- Без указания параметра DN: тогда вы сможете ввести все DN-имена по одному с клавиатуры в ответ на приглашение команды. Нажимайте Enter после ввода каждого DN. Нажмите Ctrl+Z и Enter после ввода последнего DN.

Для команды DSADD GROUP после DN можно указать следующие необязательные параметры:

- -secgrp {yes | no} указывает тип группы: безопасности (yes, значение по умолчанию) или распространения (no);
- -scope {l | g | u} определяет, является ли группа локальной в домене (l), глобальной (g, значение по умолчанию) или универсальной (u);
- -samid *имя_SAM;*
- -desc *описание;*
- -memberof *DN_группы...* указывает группу, в которую надо добавить новую группу;
- -members *DN_члена...* указывает различающиеся имена членов, которые будут добавлены в группу.

Так же, как для команды DSQUERY, можно добавить параметры -s, -u и -p, чтобы указать контроллер домена, для которого будет выполнена DSADD, а также имя и па-

роль пользователя (реквизиты), с которыми будет выполняться эта команда (см. также главу 3):

- {-s *сервер* | -d *домен);*
- -u *имя_пользователя;*
- -p {*пароль* | *}.

Изменение групп командой DSMOD

Команда DSMOD, которую обсуждалась в главе 2, изменяет объекты в Active Directory. Для изменения группы используется следующий синтаксис:

dsmod group *DN_группы...*

Эта команда принимает многие параметры, используемые в DSADD, в том числе -samid, -desc, -secgrp и -scope. Впрочем, изменять эти атрибуты для существующей группы обычно не требуется. Наиболее полезные параметры — те, что позволяют изменять состав группы:

- -addmbr DN_члена_группы... добавляет членов в группу, указанную в параметре DN_группы;
- -rmmbr DN_члена_группы... удаляет членов из группы, указанной в параметре DN_группы

Здесь, как и для всех служебных команд, работающих со службой каталогов, DN обозначает полное различающееся имя другого объекта Active Directory (если в имени есть пробелы, заключите его в кавычки).

Примечание В вызове команды DSMOD GROUP можно использовать -addmbr или -rmmbr. Нельзя использовать оба этих параметра в команде DSMOD GROUP.

Лабораторная работа. Управление учетными записями групп с помощью команды LDIFDE

В следующих упражнениях вы выведете список параметров команды LDIFDE, экспортируете сведения о пользователях из каталога Active Directory и создадите в каталоге объект группы.

Упражнение 1. Запуск LDIFDE

В этом упражнении нужно вывести список доступных параметров команды LDIFDE.

1. Откройте окно командной строки.
2. Чтобы вывести список параметров исполните команду `ldifde /?`.

Упражнение 2. Экспорт сведений о пользователях из одного ОП

В этом упражнении вы экспортируете содержимое ОП Marketing из состава домена contoso.com.

1. В домене contoso.com (с контроллером ServerOl) создайте ОП Marketing.
2. Добавьте в ОП Marketing двух или трех пользователей. Дайте им произвольные имена.
3. Из командной строки исполните следующую команду LDIFDE (символ «» обозначает продолжение на следующей строке):

```
ldifde -f marketing.ldf -s server01 :
-d "ou=Marketing,dc=contoso,dc=com" :
-p subtree -r : "(objectCategory=CN=Person,CN=Schema,CN=Configuration,:
DC=contoso,DC=com)"
```

На рис. 4-4 показано исполнение этого кода.

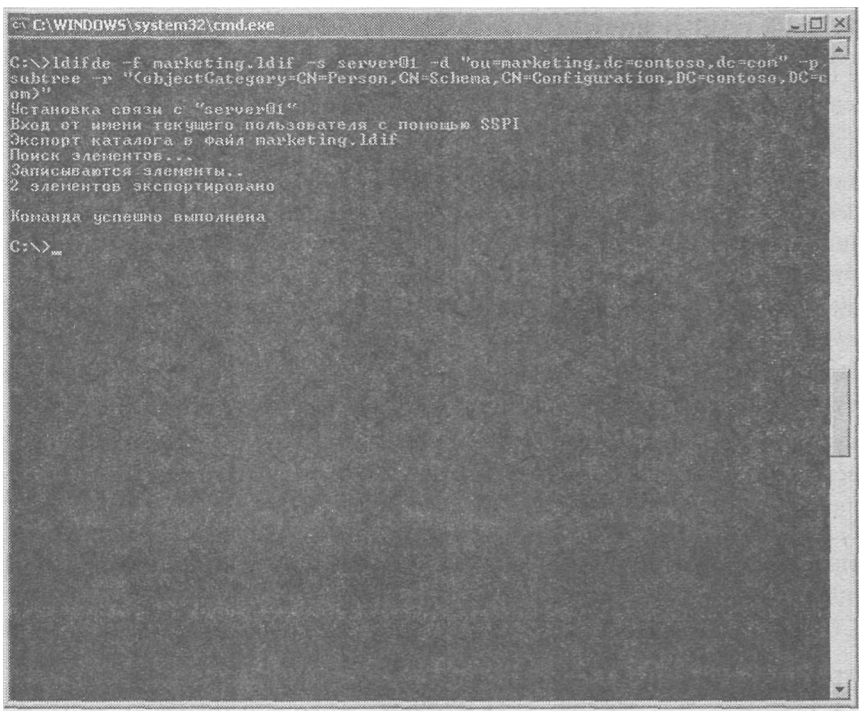


Рис. 4-4. Выходные данные команды LDIFDE **во время** экспорта **ОП Marketing**

В результате подключения к Server01 и поиска всех объектов категории Person в поддереве ОП Marketing создается файл формата LDIF с именем Marketing.ldf.

Упражнение 3. Создание группы командой LDIFDE

В этом упражнении с помощью команды LDIFDE вы добавите группу Management в ОП Marketing из состава домена contoso.com.

1. Запустите текстовый редактор, например *Блокнот* (Notepad), и создайте текстовый файл Newgroup.ldf. (Сохраните этот файл с указанным расширением!)
2. Добавьте в файл Newgroup.ldf следующий код:

```
dn: CN=Management,OU=Marketing,DC=contoso,DC=com
changetype: add
en: Management
objectClass: group
samAccountName: Marketing
```

3. Сохраните и закройте файл.
4. Из командной строки исполните следующую команду:

```
ldifde -i -f newgroup.ldf -s server01
```

Совет Проследите, чтобы в файле не было «пустот»: лишних символов табуляции, возврата каретки, перевода строки или пробелов. Лишние символы могут вызвать сбой команды.

5. В консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) проверьте, что новая группа создана.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Какой из следующих параметров переключает команду LDIFDE в режим импорта?
   a. -i.
   b. -t.
   c. -f.
   d. -s.
2. Какие классы объектов можно экспортировать и импортировать средствами LDIFDE?
3. У вас есть база данных пользователей, позволяющая экспортировать информацию в CSV-файлы. Можно ли использовать такой файл для импорта или придется вручную создать файл *.ldf?

Резюме

- Команда LDIFDE — встроенное средство Windows Server 2003, позволяющее импортировать и экспортировать данные в/из Active Directory.
- Если у вас есть каталог с данными о пользователях, с помощью LDIFDE из него можно экспортировать необходимые данные в Active Directory. Как правило, это более эффективно, чем создание каждого отдельного элемента вручную. Вы можете использовать для обмена CSV-файлы, если в них правильно отформатированы данные, а также присутствуют все необходимые элементы в надлежащем порядке.
- Программу LDIFDE можно скопировать из Windows Server 2003 на систему с Windows 2000/XP и работать с каталогом Active Directory.

Пример из практики

Вы формируете каталог Active Directory и располагаете определенными данными о пользователях (имя, фамилия, адрес и номер телефона), предоставленными отделом кадров. Правила компании требуют, чтобы имя входа пользователя являлось комбинацией его имени или инициала и фамилии (например bsmith для пользователя Ben Smith).

В вашей системе 500 пользователей, 30 групп и 10 ОП. Как максимально быстро и просто сформировать каталог Active Directory?

Хотя однозначно ответить на этот вопрос нельзя, есть несколько вариантов различной степени сложности. Возможно, лучший вариант — сочетание разных способов с учетом следующих рекомендаций.

- При необходимости можно минимально отредактировать данные о пользователях, а затем загрузить их в Active Directory командой LDIFDE.

- Создать ОП можно одновременно с объектами пользователей, загрузив все данные из одного файла, предварительно минимально изменив его. Для создания и наполнения ОП можно также применить команду LDIFDE.
- С группами можно поступить иначе. Поскольку членство в группе в Active Directory является многозначным атрибутом, список членов должен быть уникальным образом определен для каждой группы в момент ее создании. Если делать это в том же файле, можно запутаться и допустить ошибки. Поэтому лучше определять состав для каждой группы отдельно.

Практикум по устранению неполадок

Создавать отдельные объекты (пользователей, групп и компьютеров) в каталоге Active Directory несложно, но в крупной системе найти объекты и связи между ними иногда трудно. В крупной системе с множеством доменов (или небольшой, но сложной системе) решить проблемы доступа к ресурсам может быть нелегко. Например, если пользователь имеет доступ к некоторым, но не всем ресурсам, которые ему предназначены, возможно, он не включен в группы с соответствующими разрешениями.

Если у вас несколько доменов с множеством ОП в каждом из них и множеством вложенных групп в каждом из этих ОП, вам потребуется немало времени, чтобы проверить состав всех групп и выяснить, является ли пользователь членом нужных групп. В такой ситуации консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) — не лучший инструмент.

Чтобы получить исчерпывающий список всех групп, к которым относится пользователь, вы воспользуетесь командой DSGET. В этом упражнении вы будете работать с объектом пользователя Ben Smith, расположенным в ОП Users домена contoso.com.

1. Выберите в каталоге Active Directory объект пользователя, на котором вы протестируете дальнейшие действия. Если вам не удается создать подходящую конструкцию, создайте несколько вложенных групп в нескольких ОП и сделайте пользователя членом только некоторых из них.
2. Из командной строки исполните следующую команду, подставив имя выбранного пользователя и ОП вместо данных о пользователе Ben Smith:

   ```
   dsget user "CN=Ben Smith,CN=Users,DC=contoso,DC=com"
   -memberof -expand
   ```

   На экран будет выведен полный список всех групп, членом которых является этот пользователь.

Резюме главы

- Группы можно создавать в любом ОП в пределах Active Directory.
- Существует два типа групп: безопасности и распространения.
- Существует три типа области действия групп: локальная доменная, глобальная и универсальная.

- Вручную группы можно создать из консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers).
- Для автоматизированного создания групп служит программа командной строки LDIFDE.
- Средства службы каталогов, например DSQUERY, DSGET и DSMOD, могут использоваться для создания и изменения групп и их членов, а также для вывода списка членов группы.
- Типы групп можно изменять, только если уровень домена не ниже основного режима Windows 2000.
- Вложенность групп поддерживается, только если уровень домена не ниже основного режима Windows 2000.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Типы групп и доступные для них операции зависят от режима домена.
- Области действия групп и разные вложенные конструкции для этих областей зависят от режима домена.
- Основные операции в консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) для создания групп и изменения их состава.
- Основные параметры команды LDIFDE для экспорта групп из одного каталога в другой и для создания групп.
- Основные параметры команды DSGET для вывода полного перечня групп, к которым относится пользователь.

Основные термины

Локальная группа домена (область действия) ~ domain local group (scope) — в смешанном или промежуточном режимах домена такие локальные группы доступны только на контроллерах доменов, но не во всем домене.

Глобальная **группа (область действия) ~ global group (scope)** — группа, доступная во всем домене и во всех режимах домена.

Универсальная группа (область действия) ~ universal group (scope) — группа, доступная во всем домене и во всех режимах домена. В доменах смешанного режима Windows 2000 и промежуточного режима Windows Server 2003 может быть только группой распространения.

Группа **безопасности (тип) ~ security group (type)** — такой группе можно назначать разрешения в ACL.

Группа распространения (тип) ~ distribution group (type) — такой группе нельзя назначать разрешения в ACL.

Вопросы и ответы

Занятие 1. Закрепление материала

1. Какой тип доменной группы больше всего похож на локальную группу на рядовом сервере? В чем их сходство?

   Правильный ответ: локальные группы домена очень похожи на локальные группы на рядовом сервере тем, что их область действия, если домен работает в смешанном режиме или в промежуточном режиме Windows Server 2003, ограничена компьютером, на котором они размещены (для локальных групп домена это его контроллер). Пока домен не будет переведен в основной режим Windows 2000 или режим Windows Server 2003, локальные группы домена нельзя использовать для назначения разрешений на других серверах домена помимо его контроллеров.

2. **Вы** используете универсальные группы в своем домене или в лесу, и вам нужно предоставить санкционированный доступ членам универсальной группы. Какая конфигурация необходима для использования универсальной группы?

   Правильный ответ: для использования универсальной группы необходимо следующее.

   - **Домен должен работать в основном режиме Windows 2000 или в режиме Windows Server 2003.**
   - **Универсальная группа должна быть группой безопасности, но не распространения.**

3. Какие участники безопасности могут быть членами глобальной группы в домене, работающем в режиме Windows Server 2003?

   Правильный ответ:

   а пользователи;

   а **компьютеры;**

   - **универсальные группы;**
   - **глобальные группы.**

Занятие 2. Закрепление материала

1. На какой вкладке в окне свойств группы можно добавить в нее пользователей?

   Правильный ответ: для добавления членов в группу используют вкладку Члены группы (Members).

2. Вы хотите, чтобы группа IT Administrators, члены которой администрируют участников группы Sales, была вложена в Sales и имела доступ к тем же ресурсам (определенным разрешениями в ACL), что и Sales. На какой вкладке в окне свойств группы IT Administrators можно выполнить такую настройку?

   Правильный ответ: для добавления группы IT Administrators в группу Sales надо использовать вкладку Член групп (Members Of).

3. Если в вашей системе два домена (на базе Windows Server 2003 и Windows NT 4), группы какой области действия можно использовать, чтобы назначить разрешения для любого ресурса на любом компьютере в домене?

   Правильный ответ: в домене промежуточного **режима Windows Server 2003, который необходим для поддержки домена Windows NT 4, только глобальные группы можно использовать в качестве участников безопасности. Локальные группы доменов будут полезны только на контроллерах в домене Windows Server 2003, а универсальные группы**

нельзя использовать в качестве групп безопасности в доменах промежуточного режима Windows Server 2003.

Занятие 3. Закрепление материала

1. Какой из следующих параметров переключает команду LDIFDE в режим импорта?
   a. -i.
   b. -t.
   c. -f.
   d. -s.

   Правильный ответ: a. Параметр -i перенастраивает команду LDIFDE для импорта; по умолчанию она экспортирует данные.
2. Какие классы объектов можно экспортировать и импортировать средствами LDIFDE?
   Правильный ответ: средствами LDIFDE можно экспортировать и импортировать любой объект Active Directory, в том числе объекты пользователей, групп, компьютеров или ОП. Кроме того, с помощью LDIFDE можно изменить любые свойства этих объектов.
3. У вас есть база данных пользователей, позволяющая экспортировать информацию в CSV-файлы. Можно ли использовать такой файл для импорта или придется вручную создать файл *.ldf?

   Правильный ответ: CSV-файл можно использовать для импорта данных о пользователях в каталог Active Directory. Вместо пропущенных значений Windows Server 2003 подставит (где возможно) значения по умолчанию, но, если пропущен обязательный элемент, в ходе импорта произойдет ошибка, и объект не будет создан.

ГЛАВА 5

Учетные записи компьютеров

Темы экзамена

- Создание и управление учетными записями компьютеров в службе каталогов Microsoft Active Directory.
- Устранение неполадок с учетными записями компьютеров:
  - диагностика и решение проблем с учетными записями компьютеров при помощи оснастки *Active Directory — пользователи и компьютеры* консоли управления MMC;
  - смена учетной записи компьютера.

В этой главе

Как и пользователю, компьютеру можно присвоить учетную запись с именем и паролем, при помощи которой будет создана безопасная связь этого компьютера с доменом и которая также может потребовать смены пароля или отключения.

В этой главе рассказывается, как создавать объекты компьютеров, включающие параметры безопасности, необходимые для использования этих объектов в качестве «учетных записей», и управлять ими при помощи *графического интерфейса пользователя* (graphical user interface, GUI) оснастки *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers), а также мощных средств командной строки Microsoft Windows Server 2003. Также здесь описан процесс присоединения компьютера к домену, чтобы вы научились определять потенциальные источники ошибок, эффективнее устранять неполадки и восстанавливать учетные записи компьютеров.

Прежде всего

В этой главе обсуждаются концепции, относящиеся к учетным записям компьютеров в Active Directory.

Для изучения материалов этой главы вам потребуются:

- компьютер под управлением Windows Server 2003 Standard или Enterprise, установленный как Server01 и настроенный в качестве контроллера домена contoso.com;
- ОП первого уровня: Administrative Groups, Desktops и Servers;
- глобальная группа безопасности Deployment в ОП Administrative Groups;
- консоль *Active Directory — пользователи и компьютеры* или пользовательская консоль с такой оснасткой;
- для одного упражнения (присоединения компьютера к домену) требуется второй компьютер под управлением Microsoft Windows 2000 Professional, XP или Windows Server 2003, подключенный к ServerOl. Службы DNS должны быть правильно сконфигурированы на Server01 или где-либо еще, а второй компьютер должен быть настроен на использование данного сервера DNS, чтобы он мог найти в сети ServerOl — контроллер домена contoso.com.

Занятие 1. Присоединение компьютера к домену

В стандартной конфигурации Windows Server 2003 и всех ОС Microsoft Windows компьютер принадлежит какой-либо рабочей *группе* (workgroup). В рабочей группе компьютер на базе Windows NT (включая Windows NT 4, 2000, XP и Windows Server 2003) может проверять подлинность пользователей только из своей локальной БД *диспетчера учетных записей безопасности* (Security Accounts Manager, SAM). Такая система автономна во всех смыслах. Принадлежность к рабочей группе позволяет лишь видеть список компьютеров своей группы в *Проводнике*. Хотя пользователь такого компьютера и может подсоединяться к общим ресурсам на других машинах в рабочих группах или доменах, он на самом деле не входит в систему под доменной учетной записью.

Чтобы пользователь входил в систему под доменной учетной записью, компьютер должен принадлежать какому-нибудь домену: необходимо создать учетную запись компьютера и настроить его для присоединения к домену по этой учетной записи, чему и посвящено это занятие.

Учетная запись компьютера, как и учетная запись пользователя, содержит имя, пароль и *идентификатор безопасности* (security identifier, SID). Эти свойства встроены в класс объекта компьютера в Active Directory. Подготовка к включению компьютера в домен, таким образом, очень похожа на подготовку объекта пользователя для добавления в домен: вам нужно создать в Active Directory объект компьютера.

Изучив материал этого занятия, вы сможете:

- ✓ создавать учетные записи компьютеров в консоли *Active Directory — пользователиикомпьютеры;*
- ✓ создавать учетные записи компьютеров командами DSADD и NETDOM;
- ✓ присоединять компьютер к домену, изменяя параметры сетевой идентификации;
- ✓ понять, почему важно создавать учетные записи компьютеров до их присоединения к домену.

Продолжительность занятия — около 20 минут.

Создание учетных записей компьютеров

Для создания объекта компьютера в Active Directory необходимо быть членом групп *Администраторы* (Administrators) или *Операторы учета* (Account Operators) на контроллерах домена. Члены групп *Администраторы домена* (Domain Admins) и *Администраторы предприятия* (Enterprise Admins) по умолчанию являются участниками группы *Администраторы* (Administrators). Также можно делегировать административные права, чтобы другие пользователи или группы могли создавать объекты компьютеров.

Впрочем, пользователи домена также могут создавать объекты компьютеров косвенным путем. Когда компьютер присоединяется к домену, а учетная запись еще не создана, Active Directory по умолчанию автоматически создает объект компьютера в контейнере Computers. Каждому пользователю из группы *Прошедшие проверку* (Authenticated Users) (то есть всем пользователям) разрешается присоединять к домену до 10 компьютеров и, следовательно, создавать до 10 объектов компьютеров.

Создание объектов компьютеров в консоли *Active Directory - пользователи и компьютеры*

Чтобы создать объект компьютера, или его учетную запись, откройте консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) и выберите контейнер или ОП, в котором нужно создать объект. В меню Действие (Action) или в контекстном меню выберите команду **Создать (New)\Компьютер (Computer).** Откроется диалоговое окно **Новый объект — Компьютер (New Object-Computer),** показанное на рис. 5-1.

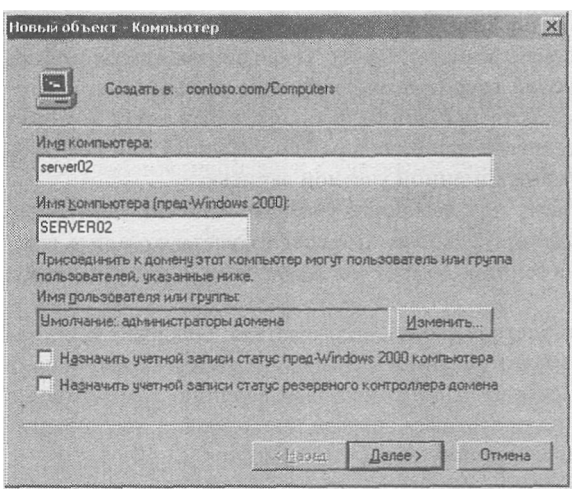


Рис. 5-1. Диалоговое окно *Новый объект — Компьютер*

В окне Новый **объект — Компьютер** (New **Object—Computer)** введите имя компьютера. Другие свойства из этого окна обсуждаются на следующем занятии. Щелкните Далее (Next). На следующем шаге запрашивается глобально уникальный идентификатор (GUID). GUID используется для предварительной настройки учетной записи компьютера для развертывания системы с помощью *служб удаленной установки* (Remote Installation Services, RIS). Здесь этот процесс не обсуждается. При создании учетной записи компьютера, который будет присоединяться к домену другими способами, вводить GUID не требуется . Поэтому просто щелкните Далее (Next), а затем Готово **(Finish).**

Создание объектов компьютеров командой DSADD

Скорее всего, вам уже доводилось делать нечто подобное. Но прогресс не стоит на месте — Windows Server 2003 предоставляет удобную команду DSADD, позволяющую создавать объекты компьютеров из командной строки или в ходе выполнения командного файла.

В главе 2 команда DSADD использовалась для создания объектов пользователей. Для создания объекта компьютера просто введите dsadd computer *DN_компьютера...*, где *DN_компьютера,..* — это различающееся имя данного компьютера, например CN=Desktop123,OU=Desktops,DC=contoso,DC=com.

Если в DN компьютера есть пробел, заключите все имя в кавычки. Параметр *DN_компьютера...* может включать множество различающихся имен для новых объектов компьютеров, что делает команду DSADD Computer удобным средством для массовой генерации таких объектов. Этот параметр можно вводить следующими способами.

- Передача по каналу списка DN-имен, полученного при выполнении другой команды, например DSQUERY.
- Указание всех DN-имен в командной строке через пробел.
- Без указания параметра DN: тогда вы сможете ввести все DN-имена по одному с клавиатуры в ответ на приглашение команды. Нажимайте Enter после ввода каждого DN. Нажмите Ctrl+Z и затем Enter после ввода последнего DN.

Для команды DSADD Computer после DN можно указать следующие необязательные параметры.

- -samid *имя_SAM;*
- -desc описание;
- -loc размещение..

Создание учетной записи компьютера командой NETDOM

Программа NETDOM входит в комплект средств поддержки и устанавливается из каталога Support\Tools компакт-диска Windows Server 2003. Эта программа также содержится на компакт-дисках Windows 2000 и XP. Используйте версию, подходящую для вашей платформы. Команда NETDOM позволяет выполнять из командной строки множество операций, связанных с учетными записями доменов и безопасностью.

Чтобы создать в домене учетную запись компьютера, введите следующую команду:

netdom add *имя_компьютера* / domain:*имя_домена* /userd:*пользователь* / PasswordD:пароль_пользователя [/ou:*DN_ОП*]

Эта команда создает учетную запись для компьютера *имя_компьютера* в домене *шмя_домена* от имени *пользователя* домена с паролем *пароль_пользователя.* Параметр /ou приводит к созданию объекта в ОП с различающимся именем *DN_ОП.* Если имя целевого ОП не указано, по умолчанию учетная запись компьютера создается в контейнере Computers. Безусловно, инициатор команды должен обладать разрешениями на создание объектов компьютеров.

Присоединение компьютера к домену

Собственно учетной записи компьютера недостаточно для создания необходимых безопасных отношений между доменом и компьютером. Компьютер нужно присоединить к домену.

1. Щелкните правой кнопкой **Мой компьютер (My Computer)** и выберите **Свойства (Properties).** Перейдите на вкладку **Имя компьютера (Computer Name).**
   - **В** *Панели управления* выберите **Система (System)** и в диалоговом окне **Свойства системы (System Properties)** перейдите на вкладку **Имя компьютера (Computer Name).**
   - Откройте окно свойств **Имя компьютера (Computer Name).** К свойствам компьютера на этой вкладке можно получить доступ несколькими способами.

Примечание В Windows 2000 вкладка **Имя компьютера (Computer Name)** называется **Сетевая идентификация (Network Identification),** а кнопка **Изменить (Change) — Свойства (Properties).** Тем не менее, работают они одинаково.

2. В *Панели управления* откройте **Сетевые подключения (Network Connections)** и в меню **Дополнительно (Advanced)** выберите **Сетевая идентификация (Network Identification).**
3. На вкладке **Имя компьютера (Computer Name)** щелкните кнопку **Изменить (Change).** Диалоговое окно **Изменение имени компьютера (Computer Name Changes)** позволяет изменить имя компьютера и его принадлежность к домену и рабочей группе (рис. 5-2).

Подготовка к экзамену Нельзя изменять имя компьютера или его членство, если вы вошли в систему не с администраторскими реквизитами. Кнопка **Изменить (Change)** доступна только пользователям из локальной группы *Администраторы* (Administrators).

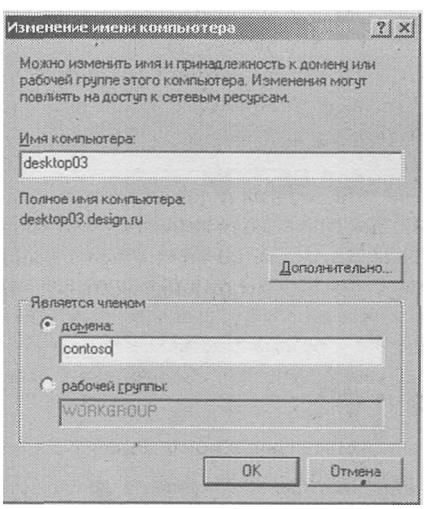


Рис. 5-2. Диалоговое окно *Изменение имени компьютера*

4. В окне **Изменение имени компьютера (Computer Name Changes)** установите переключатель в положение **домена (Domain)** и введите нужное имя домена.

Совет Хотя нужный домен обычно можно найти по «плоскому» NetBIOS-имени, возьмите за правило вводить DNS-имя целевого домена. Конфигурация DNS жизненно важна для компьютера с Windows 2000/XP или Windows Server 2003. Используя для домена DNS-имя, вы активизируете предпочтительный процесс разрешения имен и проверяете конфигурацию DNS на данном компьютере. Если компьютер не сможет найти домен, к которому вы пытаетесь присоединить его, проверьте правильность параметров DNS-сервера, заданных в свойствах сетевого подключения.

5. Щелкните **OK**. Компьютер попытается связаться с контроллером домена. Если связаться с доменом не удается, проверьте сетевые подключения и их параметры, а также конфигурацию DNS.

Когда компьютер успешно свяжется с доменом, появится приглашение (рис. 5-3) для ввода имени пользователя и пароля, у которого есть привилегии присоединять компьютер к домену. Заметьте: запрошенные имя и пароль — это доменное имя и пароль.

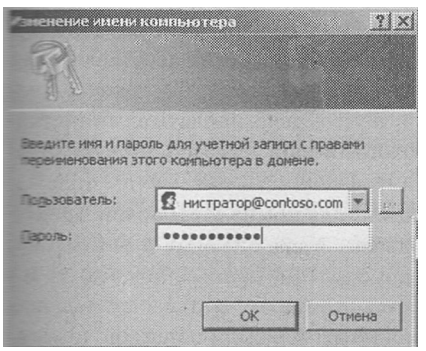


Рис. 5-3. Запрос реквизитов пользователя для присоединения компьютера к домену

Если в домене заранее не была создана учетная запись компьютера с тем же именем, во умолчанию Active Directory автоматически создаст такую учетную запись в контейнере Computers. После того как доменная учетная запись компьютера найдена или создана, компьютер установит доверительные отношения с доменом, изменит свой SID, чтобы он совпадал с SID этой доменной учетной записи, и изменит свое членство в группах. Для завершения процесса компьютер необходимо перезагрузить.

Примечание Для присоединения рабочей станции или сервера к домену также можно применять команду NETDOM JOIN. Ее функции идентичны возможностям диалогового окна Изменение имени компьютера (Computer Name Changes), но она позволяет задать еще и ОП, в котором будет создана учетная запись, если соответствующего объекта компьютера еще нет в Active Directory.

Сравнение контейнера Computers и ОП

По умолчанию Active Directory помещает объекты компьютеров в контейнер Computers. После модернизации домена Windows NT 4 до Windows 2000 все учетные записи компьютеров сначала находятся в этом контейнере. Более того, если к домену присоединяется компьютер, для которого в этом домене еще нет учетной записи, объект компьютера создается автоматически.

Совет Комплект ресурсов Microsoft Windows Server 2003 содержит средство REDIRCOMP, позволяющее автоматически создавать объекты компьютеров в ОП по выбору, при этом домен должен обладать функциональными возможностями Windows Server 2003, то есть все его контроллеры должны работать под управлением этой ОС. Такое средство полезно для организаций, где создание учетных записей компьютеров контролируется не очень строго. Поскольку объекты компьютеров автоматически создаются в определенных ОП, ими можно управлять посредством политик, связанных с этими ОП. Подробное описание REDIRCOMP см. в документах по Комплекту ресурсов Windows Server 2003.

Хотя по умолчанию объекты компьютеров помещаются в контейнер Computers, это не лучшее место для их хранения. В отличие от ОП, такие контейнеры, как Computers, Users и Builtin не могут быть связаны с политиками, ограничивающими возможную область действия групповой политики в отношении компьютеров. На практике стоит включить в структуру Active Directory минимум одно ОП для компьютеров. Обычно для компьютеров создают несколько ОП на основании структуры организации, местоположения компьютеров или назначения ОП, чтобы можно было отдельно администрировать ноутбуки, рабочие станции, серверы файлов, печати или приложений. Например, в Active Directory есть ОП, предназначенное по умолчанию для контроллеров домена, связанное с политикой Default Domain Controller Policy. Создавая в организации одно или несколько ОП для компьютеров, можно делегировать администрирование и более гибко управлять конфигурацией компьютеров через групповую политику.

Если в организации создано одно или несколько ОП для компьютеров, вам придется перемещать все объекты компьютеров, автоматически создаваемые в контейнере Computers, в соответствующие ОП. Для перемещения отметьте нужный компьютер и в меню **Действие (Action)** выберите **Переместить (Move).** Кроме того, для перемещения можно использовать новую функцию перетаскивания (drag-and-drop) объектов, поддерживаемую MMC.

Совет Поскольку никакой объект компьютера в контейнере Computers не управляется групповыми политиками для ОП, выделенных для компьютеров, и поскольку необходимы дополнительные действия по переносу объекта компьютера из контейнера Computers в соответствующее ОП, рекомендуется создавать объекты компьютеров до присоединения к домену. Вы можете сначала создать объект компьютера в нужном ОП, чтобы сразу после присоединения к домену он управлялся политиками, связанными с данным ОП.

Можно также перемещать объект компьютера или любой другой объект командой DSMOVE. Ее синтаксис таков:

dsmove *DN_объекта* [-newname *новое_имя]* [-newparent *DN_родителя]*

Параметр -newname позволяет переименовать объект. Параметр -newparent позволяет перемещать объект. Для перемещения компьютера DesktopABC из контейнера Computers в ОП Desktops введите следующую команду:

```
dsmove ?CN=DesktopABC, CN=Computers, DC=Contoso, DC=com? -newparent
?OU=Desktops, DC=Contoso, DCcom?
```

В этой команде вы вновь видите отличие контейнера (CN) Computers от организационного подразделения (OU) Desktops.

Для перемещения объектов в Active Directory необходимы соответствующие разрешения. По умолчанию членам группы *Операторы учета* (Account Operators) разрешается перемещать компьютеры между контейнерами, включая контейнер Computers, и любыми ОП, за исключением ОП Domain Controllers. Администраторы, включая членов групп *Администраторы домена* (Domain Admins) и *Администраторы предприятия* (Enterprise Admins), вправе перемещать объекты компьютеров между любыми контейнерами, включая контейнер Computers, ОП Domain Controllers и любые другие ОП.

Лабораторная работа. **Присоединение компьютера к домену Active Directory**

На этой лабораторной работе вы создадите учетные записи компьютеров при помощи консоли *Active Directory — пользователи и компьютеры* (Active Directory Users and Computers) и команды DSADD. Затем вы присоедините компьютер к домену, если у вас есть доступ ко второму компьютеру.

Упражнение 1. Создание объектов компьютеров в консоли *Active Directory-пользователиикомпьютеры*

1. Откройтеконсоль*ActiveDirectory—пользователиикомпьютеры*.
2. В ОП Servers создайте объект для компьютера с именем SERVER02. Задайте только имя компьютера. Не меняйте значения других параметров по умолчанию.
   Заметьте, что у компьютера, как и у пользователя, два имени — указанное имя компьютера и имя в формате пред-Windows 2000, На практике лучше, чтобы эти имена оставались одинаковыми.

Упражнение 2. Создание учетных записей компьютеров командой DSADD

Из командной строки исполните следующую команду:

```
dsadd computer ?cn=desktop03, ou=servers, dc=contoso,dc=com?
```

Упражнение 3. Перемещение объекта компьютера

1. Откройтеконсоль*ActiveDirectory—пользователиикомпьютеры*.
2. Командой **Переместить (Move)** переместите компьютер Desktop03 из ОП Servers в ОП Desktops.
3. Перетащите значок Server02 из контейнера Servers в Computers.
   Выберите контейнер Computers и убедитесь, что Server02 появился в нужном месте., При перетаскивании объектов можно ошибиться.

   На заметку MMC печально известна тем, что может вызвать небольшую панику. Она не обновляет содержимое окна автоматически. После таких изменений, как перемещение объекта, необходимо обновить консоль командой **Обновить (Refresh)** или клавишей **F5**.

   Откройте окно свойств для контейнера Computers. Вы увидите, что здесь нет вкладки **Групповая политика (Group Policy)**, в отличие от ОП, например Servers. Это одна из гричин, почему принято создавать одно или несколько дополнительных ОП для объектов компьютеров.
6. Из командной строки исполните следующую команду:

   ```
   csmove ?CN=Server02,CN=Computers,DC=contoso,DC=com? -newparent
   ?OU=Servers, DOcontoso, DC=com?
   ```

   Эта команда, как легко догадаться, перемещает объект компьютера обратно в ОП Servers.
7. Проверьте, что этот компьютер снова находится в ОП Servers.

Упражнение 4 (необязательное). Присоединение компьютера к домену

Для этого упражнения необходим второй компьютер, подключенный к Server01. Кроме того, нужно правильно сконфигурировать DNS, чтобы для Server01 была создана запись ресурса службы (SRV). На втором компьютере DNS должна быть сконфигурирована так, чтобы он мог находить Server01 как контроллер домена contoso.com.

1. Если у вас есть второй компьютер, который можно в следующем упражнении присоединить к вашему домену, создайте для него учетную запись в ОП Desktops при помощи консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) или команды DSADD. Убедитесь, что используемое вами имя совпадает с именем этого компьютера.
2. Войдите в систему на этом компьютере. Чтобы изменять членство этого компьютера в доменах, нужно войти в систему под учетной записью локальной группы *Администраторы* (Administrators).
3. Откройте вкладку **Имя компьютера (Computer Name).** Для этого дважды щелкните **Система (System)** в *Панели управления* или в папке **Сетевые подключения (Network Connections),** в меню **Дополнительно (Advanced)** выберите **Сетевая идентификация (Network Identification).**
4. Щелкните **Изменить (Change).**
5. Установите переключатель в положение **домена (Domain)** и введите DNS-имя домена: contoso.com.
6. Щелкните **OK**.
7. По запросу введите имя и пароль учетной записи администратора домена contoso.com.
8. Щелкните **OK**.
9. Вам будет предложено перезагрузить систему. Щелкайте **OK** в ответ на все сообщения и закройте все диалоговые окна. Перезагрузите систему.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Каковы минимальные полномочия, необходимые для создания учетной записи компьютера с Windows Server 2003 в ОП в домене? Перечислите все этапы этого процесса. Считайте, что в Active Directory еще нет учетной записи для этого компьютера.
   a. *Администраторы домена* (Domain Admins).
   b. *Администраторы предприятия* (Enterprise Admins).
   c. *Администраторы* (Administrators) на контроллере домена.
   d. *Операторы учета* (Account Operators) на контроллере домена.
   e. *Операторы сервера* (Server Operators) на контроллере домена.
   f. *Операторы учета* (Account Operators) на данном сервере.
   g. *Операторы сервера* (Server Operators) на данном сервере,
   п. *Администраторы* (Administrators) на данном сервере.
2. Где в интерфейсе можно изменить членство компьютера под управлением Windows Server 2003 в домене?
   a. Окно свойств **Мой компьютер (My Computer).**
   b. Приложение **Система (System)** из *Панели управления*.

c. Консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers).
d. Папка Сетевые подключения (Network Connections).
e. Приложение Пользователи (Users) из *Панели управления*.

3. Какая команда позволяют создать доменную учетную запись компьютера в Active Directory из командной строки?
a. NETDOM.
b. DSADD.
c. DSGET.
d. NETSH.
e. NSLOOKUP.

Резюме

- Создавать объекты компьютеров в Active Directory по умолчанию разрешено членам групп *Администраторы* (Administrators) и *Операторы учета* (Account Operators).
- Создавать учетные записи компьютеров можно с помощью консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers), а также командами DSADD и NETDOM.
- Для изменения членства компьютера в домене необходимо войти в систему под учетной записью локальной группы *Администраторы* (Administrators).

Занятие 2. Управление учетными записями компьютеров

На поедыдушем занятии вы узнали о главных элементах, необходимых для установления отношений между компьютером и доменом: учетной записи компьютера и присоединении его к домену. На этом занятии объект компьютера в Active Directory рассматривается более подробно. Вы узнаете о других свойствах и разрешениях, позволяющих объектам компьютеров работать, и о том, как управлять ими при помощи графического инерфейса или средств командной строки.

Изучив материал этого занятия, вы сможете:

- ☑ назначать разрешения для нового объекта компьютера в Active Directory;
- ☑ настраивать свойства нового объекта компьютера в Active Directory;
- ☑ находить учетные записи компьютеров в консоли *Active Directory — пользователи и компьютеры* и управлять ими.

Продолжительность занятия — около 10 минут.

Управление разрешениями для объекта компьютера

На занятии 1 вы узнали, что могли бы присоединить компьютер к домену, введя реквизиты администратора домена в ответ на запрос компьютера. Однако соображения безопасности требуют использовать для достижения конкретной цели минимальных полномо-

чий, и привлечение учетной записи из группы *Администраторы домена* (Domain Admins) для добавления к домену рабочей станции выглядит стрельбой из пушки по воробьям.

К счастью, Active Directory позволяет определить с высокой точностью, какие группы или пользователи вправе сопоставлять компьютер его доменной учетной записи. Хотя по умолчанию такой группой является *Администраторы домена* (Domain Admins), присоединять компьютер к доменной учетной записи можно разрешить любой группе, например с названием Installers. Легче всего это делать во время создания объекта компьютера.

При создании объекта компьютера на первом шаге в окне **Новый объект — Компьютер (New Object—Computer),** показанном на рис. 5-1, отображается поле **Присоединить к домену этот компьютер могут пользователь или группа пользователей, указанные ниже (The Following User Or Group Can Join This Computer To A Domain).** Щелкните **Изменить (Change),** и вы сможете выбрать любого пользователя или группу и изменить для данного объекта набор разрешений.

На следующем шаге в окне **Новый объект — Компьютер** потребуется ввести *глобально уникальный идентификатор* (GUID) добавляемого компьютера, который необходим при развертывании системы при помощи *служб удаленной установки* (Remote Installation Services, RIS). О службах RIS — в базе знаний Microsoft по адресу *http://support.microsoft.com*.

Если компьютер, который будет использовать создаваемую учетную запись, работает под управлением версии Windows младше 2000, установите флажок **Назначить учетной записи статус пред-Windows 2000 компьютера (Assign This Computer Account As A Pre-Windows 2000 Computer).** Если эта учетная запись предназначена для резервного контроллера домена Windows NT, установите флажок **Назначить учетной записи статус резервного контроллера домена (Assign This Computer Account As A Backup Domain Controller).**

Совет Помните, что принадлежать домену могут только компьютеры, на которых установлена ОС на основе технологий Windows NT, поэтому компьютеры под управлением Windows 9x/Me не могут присоединяться к доменным учетным записям компьютеров или обрабатывать их. Поэтому данный флажок фактически подразумевает наличие Windows NT 4.

Настройка свойств объекта компьютера

Объекты компьютеров обладают некоторыми свойствами, которые не отображаются в пользовательском интерфейсе во время создания учетной записи компьютера. Откройте окно свойств для объекта компьютера, чтобы задать его расположение и описание, настроить членство в группах и разрешения удаленного доступа или связать его с объектом пользователя — владельца данного компьютера. Страница свойств **Операционная система (Operating System)** доступна только для чтения. Эта информация публикуется в Active Directory автоматически. Данная страница остаётся незаполненной, пока компьютер не присоединится к домену по этой учетной записи.

Несколько классов объектов в Active Directory поддерживают свойство Manager, которое отображается на странице **Управляется (Managed By)** в окне свойств объекта компьютера. Это связанное свойство создает перекрестную ссылку на объект пользователя. Все остальные свойства (адреса и номера телефонов) не хранятся в самом объекте компьютера, а берутся напрямую из этого объекта пользователя.

Команда DSMOD, как говорилось в главе 2, также может изменять некоторые свойства объекта компьютера. В следующем разделе вы увидите работу команды DSMOD применительно к устранению неполадок с учетными записями компьютеров.

Поиск и подключение к объектам в Active Directory

При обращении пользователя вам может понадобиться информация о том, какая ОС и какой пакет обновления установлены на его компьютере. Как вы уже знаете, эта информация хранится в свойствах объекта компьютера. Так что остается только найти этот объект, что, впрочем, может быть непросто в структуре Active Directory с несколькими иоменами и множеством ОП.

Консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) предоставляет удобный доступ к мощному средству поиска с графическим интерфейсом. Это средство позволяет находить объекты многих типов. Здесь вы будете искать объект типа Computer. Щелкните кнопку **Поиск объектов в службе каталогов Active Directory (Find Objects In Active Directory)** на панели инструментов консоли. Откроется окно, показанное на рис. 5-4. Перед тем как щелкнуть **Найти (Find Now)**, вы можете выбрать тип объекта в списке **Найти (Find)**, область поиска в списке **в (In)** и указать условия поиска.

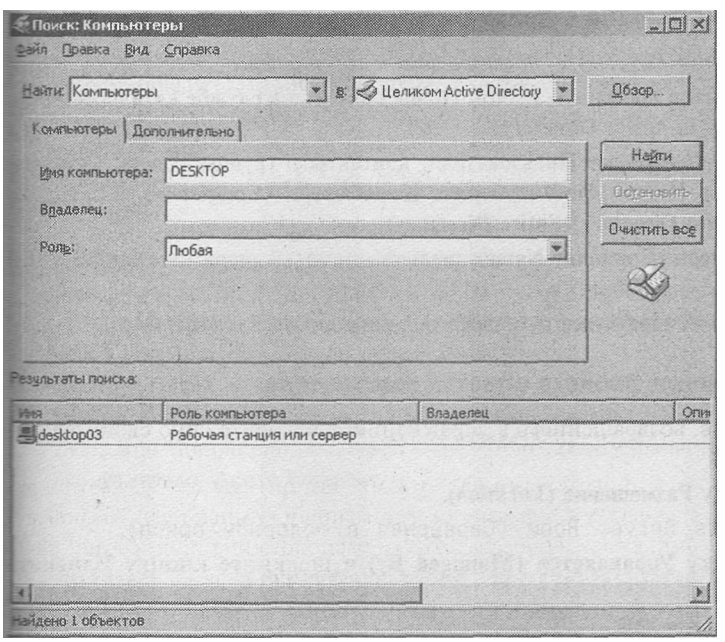


Рис. 5-4. Диалоговое окно *Поиск: Компьютеры* с результатами успешного поиска

Перечень результатов позволяет выбрать объект и посредством меню **Файл (File)** или контекстного меню выполнить с выделенным объектом типичные операции. Многим администраторам нравится возможность открыть консоль *Управление компьютером* (Computer Management) по команде **Управление (Manage)** контекстного меню и напрямую подключиться к этому компьютеру, после чего работать на нем с журналами событий, диспетчером устройств, информацией о системе, конфигурациями дисков и служб, а также локальными учетными записями пользователей и групп.

Лабораторная работа. **Управление учетными записями компьютеров**

На этой лабораторной работе вы найдете объект компьютера и измените его свойства.

Упражнение 1. Управление учетными записями компьютеров

1. Откройте консоль *Active Directory — пользователи и компьютеры.*
2. Выберите ОП Security Groups и создайте глобальную группу безопасности с именем Deployment.
3. Выберите ОП Desktops.
4. Создайте учетную запись для компьютера Desktop04. На первой странице окна **Новый объект — Компьютер (New Object—Computer)** щелкните **Изменить (Change)** ниже строки **Присоединить к домену этот компьютер могут пользователь или группа пользователей, указанные ниже (The Following User Or Group Can Join This Computer To A Domain).** Введите deployment в окне **Выбор: «Пользователь» или «Группа» (Select User or Group),** затем щелкните **OK**.
5. Завершите создание объекта компьютера Desktop04.

Упражнение 2. Поиск объектов в Active Directory

1. Откройте консоль *Active Directory — пользователи и компьютеры.*
2. На панели инструментов щелкните значок **Поиск объектов в службе каталогов Active Directory (Find Objects in Active Directory).**
3. По умолчанию выбран вариант **Пользователи, контакты и группы (Users, Contacts, and Groups).** В списке **Найти (Find)** выберите **Компьютеры (Computers),** а в списке **в (In) — Целиком Active Directory (Entire Directory).**
4. **В** поле **Имя компьютера (Computer Name)** введите server и щелкните **Найти (Find Now).**

   В наборе результатов поиска будет отображаться компьютер Server01.

Упражнение 3. Изменение свойств объекта компьютера

1. Из набора результатов, возвращенного в упражнении 1, откройте окно свойств компьютера Server01.
2. Перейдите на вкладку **Размещение (Location).**
3. Введите Headquarters Server Room (Серверная в головном офисе).
4. Перейдите на вкладку **Управляется (Managed By)** и щелкните кнопку **Изменить (Change).**
5. Введите Hank и щелкните **OK.**
6. Заметьте: отображается имя этого пользователя и его контактная информация.
7. Перейдите на вкладку **Операционная система (Operating System).** Заметьте: отображается версия используемой ОС и уровень пакета обновления.
8. (Необязательная операция.) Если **в** упражнении 4 занятия 1 вы присоединили к домену второй компьютер, откройте окно его свойств и просмотрите свойства ОС этого компьютера.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Какие платформы можно присоединять к домену?
   a. Windows 95.
   b. Windows NT 4.
   c. Windows 98.
   d. Windows 2000.
   e. Windows Me.
   f. Windows XP.
   g. Windows Server 2003.
2. Вы открываете объект компьютера, но на вкладке **Операционная система (Operating System)** его окна свойств нет никакой информации. Почему значения свойств не отображаются?
3. У руководителя есть ноутбук с именем TopDog, на котором установлена Windows XP. Нужно разрешить этому компьютеру присоединяться к домену и гарантировать, чтобы на этот компьютер распространялись групповые политики, привязанные непосредственно к ОП Desktops. Как достичь этой цели?
4. Почему на практике обычно создают в домене учетную запись компьютера до его присоединения к домену?

Резюме

- Любому пользователю или группе можно разрешить присоединять компьютер к доменной учетной записи при помощи свойства **Присоединить к домену этот компьютер могут пользователь или группа пользователей, указанные ниже (The Following User Or Group Can Join This Computer To A Domain).**
- Кнопка **Поиск объектов в службе каталогов Active Directory (Find Objects In Active Directory)** в консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) позволяет находить и затем управлять компьютерами и другими объектами Active Directory.

Занятие 3. Устранение неполадок с учетными записями компьютеров

Домены Active Directory считают компьютеры участниками безопасности. Это значит, что у компьютера, как и у пользователя, есть учетная запись, или, точнее, свойства объекта компьютера: имя, пароль и SID. На этом занятии обсуждаются основные понятия, связанные с устранением неполадок объектов компьютеров.

Изучив материал этого занятия, вы сможете:

- ✓ понять различие между удалением, отключением и переустановкой учетных записей компьютеров;
- ✓ распознавать симптомы проблем с учетными записями компьютеров;
- ✓ устранять неполадки с учетными записями компьютеров путем их удаления, отключения, переустановки и повторного присоединения при помощи средств командной строки и средств с графическим интерфейсом.

Продолжительность занятия — около 20 минут.

Удаление, отключение и переустановка учетных записей компьютеров

Учетные записи компьютеров, как и учетные записи пользователей, обладают уникальным SID, позволяющим администратору предоставлять разрешения компьютерам. Как и учетные записи пользователей, компьютеры можно включать в группы. Следовательно, как и для учетных записей пользователей, важно понимать последствия удаления учетной записи компьютера. Когда учетная запись компьютера удаляется, его членство в группах и SID теряются. Если удаление было случайным, и с этим именем создается другая учетная запись компьютера, это будет совершено новая учетная запись с новым SID. Отношения с группами потребуется восстановить, и все разрешения, назначенные удаленному объекту компьютера, необходимо переназначить новой учетной записи. Удаляйте объекты компьютеров, только когда абсолютно уверены, что атрибуты безопасности этого объекта больше не понадобятся.

Для удаления учетной записи компьютера в оснастке *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) щелкните нужный объект компьютера, а затем в меню **Действие (Action)** или, в контекстном меню выберите **Удалить (Delete).** Вас попросят подтвердить удаление, и, поскольку это необратимая операция, ответом по умолчанию принято **Нет** (No). Щелкните Да **(Yes),** чтобы удалить объект.

Команда DSRM, описанная в главе 3, позволяет удалить объект компьютера из командной строки:

DSRMDN_объекта

Здесь *DN_объекта* — различающееся имя компьютера, например «CN=Desktop15, OU=Desktops,DC=contoso,DC=com». Снова появится запрос на подтверждение удаления.

Совет Когда компьютер отсоединяется от домена (например, если администратор присоединяет его к другой рабочей группе или домену), он пытается удалить свою учетную запись из домена. Если это нельзя сделать (из-за отсутствия связи, проблем с сетью или недостаточных разрешений), учетная запись остается в Active Directory. Она сразу или со временем будет отображаться как отключенная. Если эта учетная запись больше не нужна, удалите ее вручную.

Если компьютер отключают от сети или не будет использоваться долгое время, его учетную запись можно отключить. Такое действие отвечает принципу безопасности, по которому список участников безопасности разрешает проверку подлинности только минимальному числу учетных записей, необходимому для решения задач организации. Отключение учетной записи не изменяет SID компьютера или его членство в группах, поэтому, когда компьютер подключат к сети, его учетную запись можно снова включить.

В контекстном меню и в меню **Действие (Action)** для выбранного объекта компьютера предусмотрена команда **Отключить учетную запись (Disable Account).** Отключенные учетные записи обозначаются в оснастке *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) крестом (рис. 5-5).

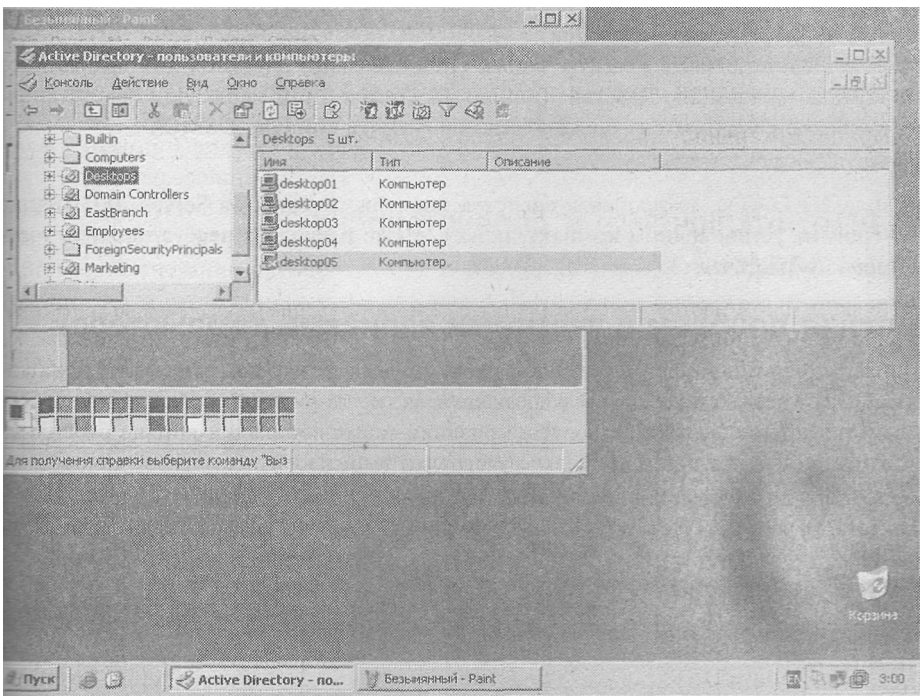


Рис. 5-5. Отключенная учетная запись компьютера

Когда учетная запись отключена, компьютер не может установить с доменом безопасную связь. В результате пользователи, ранее не входившие в систему на этом компьютере и реквизиты которых не были на нем кэшированы, не смогут входить в систему, пока учетная запись данного компьютера не будет включена и безопасный канал не будет восстановлен.

Для включения учетной записи компьютера просто выделите нужный компьютер и в меню **Действие (Action)** или в контекстном меню выберите команду **Включить учетную вались (Enable Account)**.

Отключать и включать компьютер из командной строки можно командой DSMOD, которая изменяет объекты Active Directory:

```
DSMOD COMPUTER DN_ компьютера -DISABLED YES
DSMOD COMPUTER DN_компьютера -DISABLED NO
```

Если членство в группах и SID учетной записи компьютера, а также разрешения, назначенные этому SID, важны для функционирования домена, не следует удалять такую учетную запись. Что же делать, если компьютер заменяется новой системой с современным оборудованием? Это одна из ситуаций, когда может понадобиться переустановка учетной записи компьютера.

При переустановке учетной записи компьютера пароль на вход удаляется, но сохраняются все остальные свойства объекта. Без пароля данная учетная запись фактически

становится «доступной» для использования. Любой компьютер теперь может присоединиться к домену по этой учетной записи, в том числе ваша новая система.

На самом деле компьютер, который уже был присоединен к домену с этой учетной записью, тоже может использовать переустановленную запись, просто ему нужно повторно присоединиться к этому домену. Эти ситуации будут подробно рассмотрены в практикуме по устранению неполадок.

Команда **Переустановить учетную запись (Reset Account)** доступна для выбранного объекта компьютера в меню **Действие (Action)** и в контекстном меню. Для переустановки учетной записи компьютера также можно применять команду DSMOD:

```
DSMOD computer DN_компьютера -reset
```

Команда NETDOM, входящая в средства поддержки Windows Server 2003 (папка Support\Tools на установочном компакт-диске), также позволяет переустановить учетную запись компьютера.

Выявление проблем с учетными записями компьютеров

Учетные записи компьютеров и безопасные отношения между компьютерами и их доменом работают весьма надежно. В редких случаях, когда учетная запись или безопасный канал перестают функционировать, признаки такой неполадки вполне очевидны. Наиболее типичные признаки проблем с учетными записями компьютеров таковы:

- сообщения при входе в систему о том, что связь с контроллером домена не может быть установлена, отсутствует учетная запись для данного компьютера или доверительные (то есть безопасные) отношения между компьютером и доменом были потеряны (см. пример на рис. 5-6);

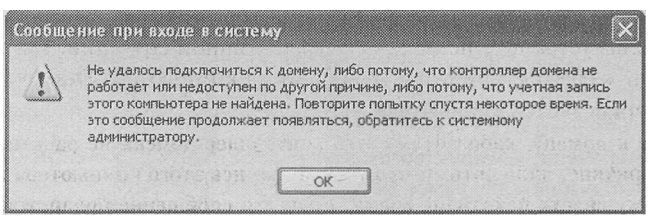


Рис. 5-6. Сообщение, выдаваемое клиентом Windows XP при входе в систему, о возможных проблемах с учетной записью компьютера

- сообщения об ошибках или записи в журнале событий о подобных проблемах или предположения об ошибке паролей, доверительных отношений, безопасных каналов или отношений с доменом или контроллером домена;
- отсутствие учетной записи компьютера в Active Directory.

В каждой из таких ситуаций необходимо устранить проблему с учетной записью. Вы уже знаете, как удалять, отключать и переустанавливать учетную запись компьютера, а также как присоединять компьютер к домену.

При устранении неполадок с учетными записями компьютеров придерживайтесь следующих правил.

A. Если данная учетная запись компьютера существует в Active Directory, ее нужно переустановить.

B. Если данной учетной записи компьютера нет в Active Directory, ее нужно создать.

C. Если компьютер еще принадлежит домену, его нужно удалить из домена, включив в какую-либо рабочую группу. Имя рабочей группы не имеет значения. Лучше всего методом проб найти имя, которое точно не используется.

D. Снова присоединить этот компьютер к домену; или присоединить другой компьютер, но его имя должно совпадать с именем данной учетной записи.

Для устранения любой неполадки с учетной записью компьютера применяйте все четыре правила. Они могут применяться в произвольном порядке, за исключением правила D, связанного с присоединением компьютера к домену, — эту операцию выполняйте в последнюю очередь. Рассмотрим две ситуации.

В первой ситуации пользователь жалуется: при попытке входа в систему выдается сообщение, что учетная запись для данного компьютера, возможно, отсутствует. Применяя правило A, вы открываете консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) и обнаруживаете, что данная учетная запись существует. Вы переустанавливаете учетную запись. Правило B не применяется — учетная запись существует. Затем, согласно правилу C, вы отсоединяете данную систему от домена, после чего по правилу D снова присоединяете ее.

Во второй ситуации предположим, что учетная запись компьютера переустановлена случайно, тогда сначала применим правило A. Хотя переустановка и случайна, необходимо продолжить восстановление согласно остальным трем правилам. Правило B не применяется, поскольку данная учетная запись существует в домене. Правило C говорит, что раз компьютер еще присоединен к домену, его нужно удалить из домена, а затем, по правилу D, снова присоединить.

По этим четырем правилам вы сможете, как на работе, так и на экзамене, принять осознанное решение о том, как поступить в каждой ситуации сбоя функционирования учетной записи компьютера.

Лабораторная работа. **Устранение неполадок с учетной записью компьютера**

На этой лабораторной работе вы устраните неполадку в реалистичной ситуации. Пользователь в домене contoso.com жалуется: при входе в систему на компьютере Desktop03 выдется сообщение об ошибке:

> **«Не удалось подключиться к домену, либо потому, что контроллер домена не работает или недоступен по другой причине, либо потому, что учетная запись этого компьютера не найдена. Повторите попытку спустя некоторое время. Если это сообщение продолжает появляться, обратитесь за помощью к системному администратору» («Windows cannot connect to the domain, either because the domain controller is down or otherwise unavailable, or because your computer account was not found. Please try again later. If this message continues to appear, contact your system administrator for assistance»).**

Пользователь подождал, снова попробовал войти в систему, получил то же сообщение, подождал еще и поучил это сообщение в третий раз. На попытки входа в систему он потерял уже 20 минут. Явно расстроенный, пользователь обращается к вам за помощью.

Упражнение 1. Устранение неполадок с учетными записями компьютеров

1. Определите наиболее вероятную причину проблемы пользователя.
   a. Пользователь ввел неверное имя.
   b. Пользователь ввел неверный пароль.
   c. Пользователь выбрал неверный домен из списка **Вход на (Log On To).**
   d. Безопасный канал связи компьютера с доменом разорван.

e. Реестр данного компьютера поврежден.
f. На компьютере установлена политика, запрещающая данному пользователю интерактивный вход в систему.

Правильный ответ, как вы, наверное, догадались, — d. У компьютера нет безопасного канала связи с доменом.

2. Перечислите, какие действия из следующего списка необходимо предпринять для устранения проблемы. Определите порядок действий. Не обязательно использовать все перечисленные шаги.
   a. Включить учетную запись этого компьютера.
   b. Присоединить компьютер Desktop03 к домену contoso.com.
   c. Определить, существует ли данная учетная запись компьютера в Active Directory.
   d. Переустановить эту учетную запись компьютера или создать ее снова.
   e. Включить Desktop03 в какую-либо рабочую группу.
   f. Удалить учетную запись этого компьютера.
   g. Отключить учетную запись этого компьютера.

Правильный ответ — это шаги e, c, d и b. Шаг e не обязательно выполнять в первую очередь, лишь бы он был выполнен до шага b. Шаги c и d должны следовать (именно в этом порядке) до шага b, который должен быть последним.

Упражнение 2. Устранение проблем с учетной записью компьютера

1. В консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) щелкните на панели кнопку **Поиск объектов в службе каталогов Active Directory (Find Objects In Active Directory)** и найдите компьютер Desktop03.
2. Desktop03 отображается в результатах поиска, поскольку вы создали этот объект на занятии 1.
3. Убедившись, что эта учетная запись компьютера существует, переустановите ее. щелкнув Desktop03 правой кнопкой и выбрав **Переустановить учетную запись (Reset Account).**

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Ваша организация расширилась и создала второй домен. В последние выходные несколько компьютеров из вашего домена были переведены в новый домен. Открыв консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers), вы видите, что эти компьютеры все еще отображаются в вашем домене, но помечены красным крестом «X». Какие действия лучше всего предпринять?
   a. Включить эти учетные записи.
   b. Отключить эти учетные записи.
   c. Переустановить эти учетные записи.
   d. Удалить эти учетные записи.
2. Пользователь жалуется: при попытке входа в систему появляется сообщение, что данный компьютер не может связаться с доменом, потому что контроллер домена выключен или учетная запись для данного компьютера отсутствует. Открыв консоль

Active Directory — пользователи и компьютеры (Active Directory Users And Computers), вы видите, что учетной записи этого компьютера действительно нет. Что следует предпринять?

3. Пользователь жалуется: при попытке входа в систему появляется сообщение, что данный компьютер не может связаться с доменом, потому что контроллер домена выключен или учетная запись для данного компьютера отсутствует. Открыв консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers), вы видите, что учетная запись этого компьютера в порядке. Что следует предпринять?

Резюме

- Для компьютеров существуют учетные записи, которые, как и учетные записи пользователей, содержат SID и описывают членство в группах. Будьте осторожны при удалении объектов компьютеров. Отключение объектов компьютеров позволяет включить эти объекты снова, если потребуется присоединить соответствующий компьютер к домену.
- Проблемы с учетными записями компьютеров обычно вполне очевидны: выводятся сообщения или регистрируются события о том, что есть неполадки с учетной записью, паролем, безопасным каналом или доверительными отношениями.
- Применяя четыре правила из занятия 3, вы сможете устранять практически любые неполадки с учетными записями компьютеров.

Пример из практики

Компания Contoso решила открыть два филиала: восточный и западный. В каждом филиале приобрели 10 компьютеров для торговых представителей. Инвентарные номера этих компьютеров приведены в следующей таблице.

Восточный филиал	Западный филиал
EB-2841	WB-3748
EB-2842	WB-3749
EB-2843	WB-3750
EB-2844	WB-3751
EB-2845	WB-3752
EB-2846	WB-3753
EB-2847	WB-3754
EB-2848	WB-3755
EB-2849	WB-3756
EB-2850	WB-3757

Вам нужно подготовить Active Directory для развертывания этих компьютеров.

Упражнение 1. Создание ОП

Создайте два ОП в домене contoso.com: EastBranch и WestBranch. Введите имена так, как показано. Не разделяйте слова пробелами.

Упражнение 2. Сценарий для создания учетных записей компьютеров

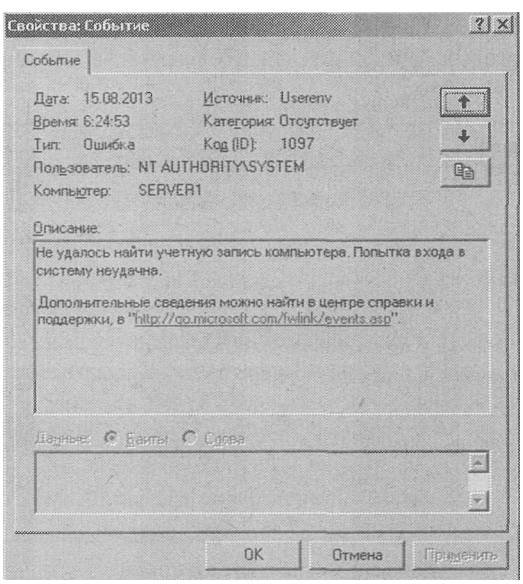
1. Откройте *Блокнот* (Notepad).
2. Введите следующую строку для каждого компьютера:

   ```
   DSADD COMPUTER ?CN=EB-2841,OU=EastBranch,DC=Contoso,DC=COM? -desc ?Sales Rep Computer? -loc ?East Branch Office?
   ```

   Убедитесь, что для каждого компьютера параметр CN= совпадает с его инвентарным номером, а параметры OU= и -loc отражают название и расположение филиала, где установлен компьютер.
3. Сохраните этот файл под именем «C:\ScriptComputers.bat». Не забудьте заключить имя в кавычки, иначе *Блокнот* автоматически добавит расширение .txt.
4. Откройте окно командной строки и исполните команду c:\scriptcomputers.
5. Убедитесь в успешном создании учетных записей компьютеров, просмотрев ОП EastBranch и WestBranch. Консоль MMC не обновляет окно автоматически, поэтому, если вы сразу не увидите новые компьютеры, нажмите **F5**.

Практикум по устранению неполадок

После выходных, во время которых консультант выполнил техническое обслуживание компьютеров в восточном филиале, пользователи стали жаловаться на проблемы с входом в систему. Вы просмотрели журнал событий на одном из компьютеров филиала и обнаружили следующую запись:



Это похоже на проблему с учетной записью компьютера.

Какие из следующих действий необходимо выполнить для устранения проблемы?

1. Удалить учетные записи этих компьютеров.
2. Сменить пароль для учетных записей этих пользователей.

3. Присоединить эти компьютеры к рабочей группе.
4. Отключить учетные записи этих компьютеров.
5. Переустановить учетные записи этих компьютеров.
6. Включить учетные записи этих компьютеров.
7. Создать новые учетные записи компьютеров.
8. Присоединить эти компьютеры к домену.

Правильный ответ: 5, 3 и 8. Это наиболее эффективное решение; оно состоит в переустановке учетных записей компьютеров и повторном присоединении компьютеров к домену.

Упражнение 1 (необязательное). Моделирование проблемы

Если на занятии 1 вы присоединили второй компьютер к домену Contoso, переместите его объект в ОП EastBranch. Затем в консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) переустановите учетную запись этого компьютера.

Перезагрузив компьютер, попытайтесь войти в домен. Получилось? Сможете ли вы войти в систему под учетными записями домена Contoso, с помощью которых вы раньше входили в систему на этом компьютере? Почему? (Подсказка: кэширование входов в систему.)

Сможете ли вы войти в систему с новыми доменными учетными записями, которые никогда не использовались на этом компьютере? При попытке сделать это вы получите типичное сообщение о возможном отсутствии учетной записи компьютера.

Войдите в систему как локальный администратор и просмотрите журнал событий. Какие сообщения об ошибках вы видите?

Упражнение 2. Переустановка всех учетных записей компьютеров восточного филиала

Самый быстрый способ переустановить учетные записи компьютеров (к тому же все они находятся в одном ОП) — использовать средство командной строки.

1. Из командной строки исполните следующую команду:

   ```
   DSQUERY COMPUTER ?OU=EastBranch,DC=contoso,DC=com?
   ```

   Эта команда получает из Active Directory список компьютеров в ОП EastBranch. Он должен совпадать со списком учетных записей компьютеров, созданных при разборе примера из практики.
2. Исполните следующую команду:

   ```
   DSQUERY COMPUTER ?OU=EastBranch,DC=contoso,DC=com? | DSMOD COMPUTER -RESET
   ```

   Здесь мы передаем по каналу результаты команды DSQUERY на вход команды DSMOD. Команда DSMOD COMPUTER -RESET переустановит все полученные учетные записи. Задание выполнено.

Упражнение 3 (необязательное). Повторное присоединение к домену

Если у вас есть второй компьютер, переустановите его учетную запись. Теперь поупражняйтесь в удалении этого компьютера из домена, включив его в какую-либо рабочую группу. После перезагрузки снова присоедините компьютер к домену.

Резюме главы

- Для создания объектов компьютеров в Active Directory необходимо иметь соответствующие разрешения. Такими разрешениями обладают группы *Администраторы* (Administrators) и *Операторы учета* (Account Operators), эти разрешения можно делегировать другим пользователям или группам.
- При создании объекта компьютера можно указать, какие пользователи или группы вправе присоединять компьютер к домену при помощи этой учетной записи.
- Оснастка *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) позволяет создавать, изменять, удалять, отключать, включать и переустанавливать объекты компьютеров.
- Из командной строки можно создавать объект компьютера командой DSADD Computer и изменять его свойства командой DSMOD Computer.
- Команда DSMOD Computer также используется для переустановки, отключения и включения объекта компьютера. Команда DSRM удаляет объект компьютера. Команда из средств поддержки, NETDOM, содержит множество параметров для выполнения аналогичных задач.
- Типичная процедура устранения неполадок включает повторное создание или переустановку учетной записи компьютера, удаление компьютера из домена и повторное присоединение его к домену.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Перечислите минимальные разрешения, необходимые для создания объекта компьютера в Active Directory, а также разрешения для изменения членства компьютера в группах и доменах.
- Запомните синтаксис команд DSADD, DSMOD и DSRM. Учтите, что в командах DSMOD и DSADD нужно указать в качестве параметра одно или несколько различающихся имен. Команда DSQUERY может получить такие имена и передать их по каналу команде DSMOD.
- Четко уясните различия между отключением, переустановкой и удалением учетной записи компьютера. Что происходит в результате каждой из этих операций с объектом компьютера, его SID и членством в группах, а также с самим компьютером?
- Запомните и применяйте четыре правила устранения неполадок с учетными записями компьютеров.
- Потренируйтесь в поиске объектов в Active Directory и управлении ими из окна с результатами поиска. Эти навыки применимы ко многим объектам в Active Directory и к нескольким темам экзамена.

Основные термины

Учетная запись компьютера ~ computer account — Учетная запись в Active Directory, однозначно идентифицирующая компьютер в домене.

Вопросы и ответы

Занятие 1. Закрепление материала

1. Каковы минимальные полномочия, необходимые для создания учетной записи компьютера с Windows Server 2003 в ОП в домене? Перечислите все этапы этого процесса. Считайте, что в Active Directory еще нет учетной записи для этого компьютера.
   a. *Администраторы домена* (Domain Admins).
   b. *Администраторы предприятия* (Enterprise Admins).
   c. *Администраторы* (Administrators) на контроллере домена.
   d. *Операторы учета* (Account Operators) на контроллере домена.
   e. *Операторы сервера* (Server Operators) на контроллере домена.
   f. *Операторы учета* (Account Operators) на данном сервере.
   g. *Операторы сервера* (Server Operators) на данном сервере,
   h. *Администраторы* (Administrators) на данном сервере.

   Правильный ответ: d, h. Группа **Операторы учета (Account Operators) на контроллере домена обладает минимальными разрешениями, необходимыми для создания объекта компьютера в домене. Для изменения членства в домене нужно быть членом локальной группы Администраторы (Administrators) на этом сервере.**
2. Где в интерфейсе можно изменить членство компьютера под управлением Windows Server 2003 в домене?
   a. Окно свойств Мой компьютер (My Computer).
   b. Приложение **Система (System)** из *Панели управления.*
   c. Консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers).
   d. Папка **Сетевые подключения (Network Connections).**
   e. Приложение **Пользователи (Users)** из *Панели управления.*

   Правильный ответ: a, b, d.
3. Какая команда позволяют создать доменную учетную запись компьютера в Active Directory из командной строки?
   a. NETDOM.
   b. DSADD.
   c. DSGET.
   d. NETSH.
   e. NSLOOKUP.

   Правильный ответ: a, b.

Занятие 2. Закрепление материала

1. Какие платформы можно присоединять к домену?
   a. Windows 95.
   b. Windows NT 4.
   c. Windows 98.
   d. Windows 2000.

e. Windows Me.
f. Windows XP.
g. Windows Server 2003.

Правильный ответ: b, d, f, g.

2. Вы открываете объект компьютера, но на вкладке **Операционная система (Operating System)** его окна свойств нет никакой информации. Почему значения свойств не отображаются?

Правильный ответ: ни один компьютер не присоединен к домену при помощи этой учетной записи. Когда какая-нибудь система присоединяется к домену, по умолчанию ее свойства отображаются на вкладке Операционная система (Operating System).

3. У руководителя есть ноутбук с именем TopDog, на котором установлена Windows XP. Нужно разрешить этому компьютеру присоединяться к домену и гарантировать, чтобы на этот компьютер распространялись групповые политики, привязанные непосредственно к ОП Desktops. Как достичь этой цели?

. **Правильный ответ: нужно создать в ОП Desktops объект для компьютера TopDog. При создании учетной записи компьютера выберите учетную запись руководителя в свойстве Присоединить к домену этот компьютер могут пользователь или группа пользователей, указанные ниже (The Following User Or Group Can Join This Computer To A Domain).**

4. Почему на практике обычно создают в домене учетную запись компьютера до его присоединения к домену?

Правильный ответ: существует несколько причин, по которым лучше создавать учетную запись компьютера в домене до его присоединения к домену. Первая причина связана с тем, что если учетная запись не была создана заранее, то при присоединении компьютера к домену она будет создана автоматически, по умолчанию — в контейнере Computers. В результате политики компьютеров, которые обычно связаны с определенными ОП, не будут применяться к этому новому компьютеру. И поскольку в большинстве организаций есть специальные ОП для компьютеров, вам придется совершать дополнительную операцию: перемещать объект этого компьютера в нужное ОП после присоединения его к домену. Наконец, создавая объект компьютера, можно указать, каким группам (или пользователям) разрешено присоединять компьютеры к домену при помощи этой учетной записи. Короче говоря, у вас будет больше возможностей и контроля при развертывании.

Занятие 3. Закрепление материала

1. Ваша организация расширилась и создала второй домен. В последние выходные несколько компьютеров из вашего домена были переведены в новый домен. Открыв консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers), вы видите, что эти компьютеры все еще отображаются в вашем домене, но помечены красным крестом «X». Какие действия лучше всего предпринять?

a. Включить эти учетные записи.
b. Отключить эти учетные записи.
c. Переустановить эти учетные записи.
d. Удалить эти учетные записи.

Правильный ответ: d. Когда компьютеры были удалены из домена, их учетные записи не были удалены, возможно, из-за настроек разрешений. Теперь эти компьютеры относятся к другому домену. Их учетные записи больше не нужны.

2. Пользователь жалуется: при попытке входа в систему появляется сообщение, что данный компьютер не может связаться с доменом, потому что контроллер домена выключен или учетная запись для данного компьютера отсутствует. Открыв консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers), вы видите, что учетной записи этого компьютера действительно нет. Что следует предпринять?

   Правильный ответ: нужно создать учетную запись компьютера, отсоединить его от домена и снова присоединить.

3. Пользователь жалуется: при попытке входа в систему появляется сообщение, что данный компьютер не может связаться с доменом, потому что контроллер домена выключен или учетная запись для данного компьютера отсутствует. Открыв консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers), вы видите, что учетная запись этого компьютера в порядке. Что следует предпринять?

   Правильный ответ: нужно переустановить учетную запись этого компьютера, отсоединить его от домена и снова присоединить.

ГЛАВА 6

Файлы и папки

Темы экзамена

- Настройка доступа к общим папкам.
  - Управление разрешениями общего ресурса.
- Настройка разрешений файловой системы:
  - проверка действующих разрешений при предоставлении разрешений;
  - смена владельцев файлов или папок.
- Устранение неполадок, связанных с доступом к файлам и общим папкам.
- Управление Web-сервером:
  - управление службами IIS;
  - управление безопасностью IIS.

В этой главе

Помимо прочего, администратору ежедневно приходится решать такие задачи, как поддержка сетевых файлов и папок. Когда пользователь не может получить доступ к нужному ресурсу, в службе технической поддержки начинает звонить телефон. В результате вы тратите время и деньги, меняя разрешения или принадлежность к группам. Когда к важному ресурсу получает доступ тот, кому он не предназначен, снова звонит телефон, и в результате вам приходится тратить время и деньги на поиск новой работы.

В этой главе вы познакомитесь с основными концепциями, получите навыки управления общими папками и изучите возможности оснастки *Общие папки* (Shared Folders). Вы научитесь работать с редактором *таблицы управления доступом* (Access Control List, ACL). Рассмотрев различные сочетания разрешений, вы научитесь определять *действующие разрешения* (effective permissions) — сумму разрешений пользователя и групп, членом которых он является, и настраивать аудит, позволяющий отследить доступ и операции над определенными файлами. Наконец, мы обсудим службу IIS, которая, подобно *Службе доступа к файлам и принтерам сетей Microsoft,* предлагает альтернативный способ обеспечения доступа к файлам и папкам.

Прежде всего

Для изучения материалов этой главы вам потребуются:

- компьютер под управлением Microsoft Windows Server 2003 (Standard или Enterprise), установленный как ServerOl и настроенный в качестве контроллера домена contoso.com;
- ОП первого уровня: Security Groups и Employees;
- группа *Пользователи домена* (Domain Users) в составе группы *Операторы печати* (Print Operators), чтобы при выполнении упражнений «обычные» пользователи могли войти на контроллер домена;
- пять локальных групп безопасности домена в ОП Security Groups: Project 101 Team, Project 102 Team, Engineers, Managers, Project Contractors;
- учетные записи пользователей Scott Bishop, Danielle Tiedt и Lorrin Smith-Bates в ОП Employees; пользователь Scott Bishop должен входить в группы Engineers, Project Contractors и Project 101 Team, Danielle Tiedt — в группы Engineers и Project 101 Team, а Lorrin Smith-Bates — в группы Managers и Project 101 Team;
- доступ к оснастке *Общие папки* (Shared Folders) из консоли *Управление компьютером* (Computer Management), консоли *Управление файловым сервером* (File Server Management), доступной на странице **Управление данным сервером (Manage Your Server),** или из собственной консоли MMC.

Занятие 1. Настройка общих папок

У нас бы не было сетей и работы, если бы организации не ценили возможность предоставления ресурсов в общий доступ. Создание общих папок для обеспечения удаленного доступа является, таким образом, одной из важных задач сетевого администратора. Для управления общими папками в Windows Server 2003 служит оснастка *Общие папки* (Shared Folders).

Изучив материал этого занятия, вы сможете:

- ✓ создать общую папку с помощью *Проводника Windows* и оснастки *Общиепапки;*
- ✓ настроить разрешения и другие свойства общих папок;
- ✓ управлять сеансами пользователей и открытыми файлами.

Продолжительность занятия — около 15 минут.

Открытие общего доступа к папке

Открытие общего доступа к папке указывает *Службе доступа к файлам и принтерам сетей Microsoft* (File And Printer Sharing For Microsoft Networks) разрешить клиентам, на компьютерах которых запущена служба *Клиент для сетей Microsoft* (Client For Microsoft Networks), подключаться к этой папке и ее подпапкам. Вы, безусловно, знаете, как создавать общие папки с помощью *Проводника Windows:* щелкнуть папку правой кнопкой, выбрать **Общий доступ и безопасность (Sharing And Security)** и установить переключатель **Открыть общий доступ к этой папке (Share This Folder).**

Однако знакомая вкладка **Доступ (Sharing)** окна свойств папки в *Проводнике Windows* доступна, только когда вы входите в систему локально или с помощью служб терминалов, и создать общую папку на удаленном компьютере нельзя. Поэтому мы рассмотрим создание, свойства, конфигурацию и управление общими папками с помощью оснастки *Общие папки* (Shared Folders), которую можно использовать как на локальной, так и на удаленной системах.

Открыв оснастку *Общие папки* (Shared Folders) в настраиваемой консоли MMC или в консолях *Управление компьютером* (Computer Management) или *Управление файловым сервером* (File Server Management), вы сразу заметите, что в Windows Server 2003 уже настроено несколько стандартных административных общих ресурсов: системный каталог (обычно C:\Windows) и корень каждого жесткого диска. Имя ресурса для таких общих папок заканчивается знаком доллара ($). Знаком доллара в конце сетевого имени обозначают скрытые общие папки. Они не видны в обозревателе, но к ним можно подключиться по UNC-имени вида \\имя_сервера\имя_общего_ресурса$. К административным общим ресурсам могут подключаться только администраторы.

Для открытия общего доступа к папке, подключитесь к нужному компьютеру из оснастки *Общие папки:* щелкните корневой узел **Общие папки (Shared Folders)** правой кнопкой и выберите **Подключиться к другому компьютеру (Connect To Another Computer).** Выбрав компьютер, щелкните узел **Общие папки (Shares),** а затем в контекстном меню или в меню **Действие (Action)** выберите **Новый общий ресурс (New[4] Share).** Мастер создания общих ресурсов содержит следующие страницы и настройки.

- **Страница Folder Path (Путь к папке).** Укажите путь к общей папке на локальном жестком диске, например, если папка находится на диске D: сервера, путь к ней будет иметь вид D:\имя_папки.
- **Страница Name, Description, and Settings (Имя, описание и параметры).** Введите имя общего ресурса. Если к сети подключены устаревшие клиенты (например компьютеры под управлением DOS), старайтесь придерживаться правил именования 8.3, чтобы обеспечить им доступ к общим папкам. Имя ресурса вместе с именем сервера образуют UNC-имя вида \\имя_сервера\имя_общего_ресурса. Добавьте знак доллара в конце сетевого имени, чтобы сделать общий ресурс скрытым. В отличие от встроенных скрытых административных общих ресурсов, к скрытым общим папкам, созданным вручную, может подключиться любой пользователь, причем его права ограничиваются только разрешениями общего ресурса.
- **Страница Разрешения (Permissions).** Выберите подходящие разрешения общего ресурса.

Управление общей папкой

Узел **Общие папки (Shares)** в оснастке *Общие папки* (Shared Folders) содержит список всех общих ресурсов компьютера и для каждого из них предоставляет контекстное меню, которое позволяет прекратить доступ, открыть общий ресурс в *Проводнике* или настроить его свойства. Все свойства, которые предлагает заполнить мастер *Мастер создания общих ресурсов* (Share A Folder Wizard), можно изменить в окне свойств общего ресурса (рис. 6-1).

Окно свойств общей папки содержит следующие вкладки.

- **Общие (General).** Здесь можно указать сетевое имя, путь к папке, описание, количество одновременных подключений пользователей и параметры работы с файлами в автономном режиме. Имя общего ресурса и путь к нему предназначены только для чтения. Чтобы переименовать общий ресурс, нужно сначала закрыть доступ, а затем создать общий ресурс с новым именем.

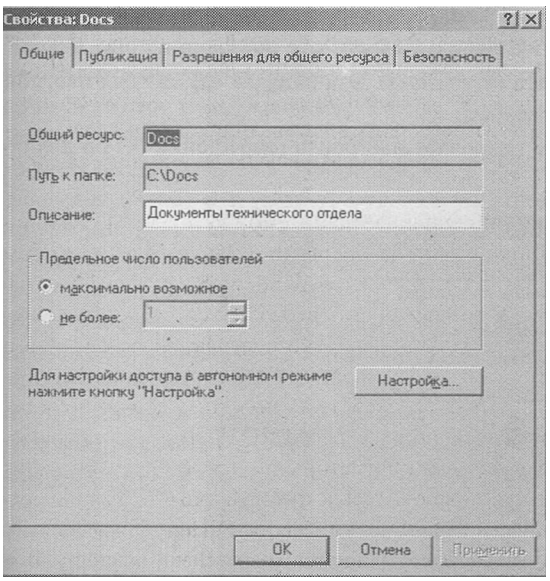


Рис. 6-1. Вкладка *Общие* диалогового окна свойств общей папки

- **Публикация (Publish).** Если установить флажок **Опубликовать этот общий ресурс в Active Directory (Publish This Share In Active Directory),** как показано на рис. 6-2, в Active Directory будет создан объект, представляющий эту общую папку.

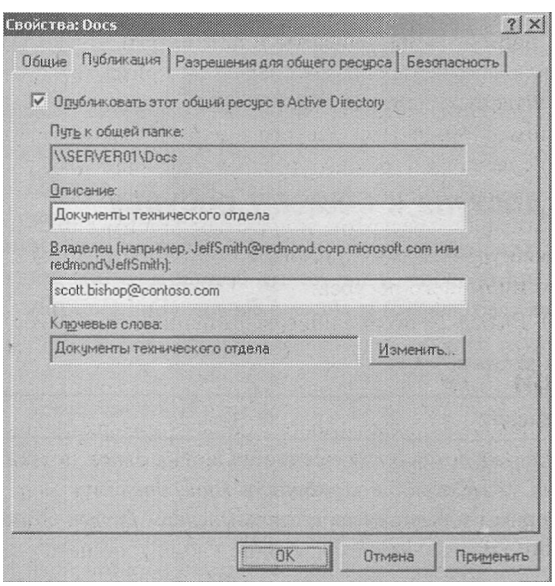


Рис. 6-2. Вкладка *Публикация* диалогового окна свойств общей папки

К свойствам объекта относятся описание и ключевые слова, по которым общую папку можно найти, используя диалоговое окно **Поиск: Пользователи, контакты и группы (Find Users, Contacts and Groups).** Если в раскрывающемся списке **Найти (Find)**

выбрать значение **Общие папки (Shared Folders),** это диалоговое окно трансформируется в окно **Поиск: Общие папки (Find Shared Folders),** как показано на рис. 6-3.

- **Разрешения для общего ресурса (Share Permissions).** Эта вкладка служит для настройки разрешений доступа к общему ресурсу.
- **Безопасность (Security).** Эта вкладка позволяет настроить разрешения NTFS для общей папки.

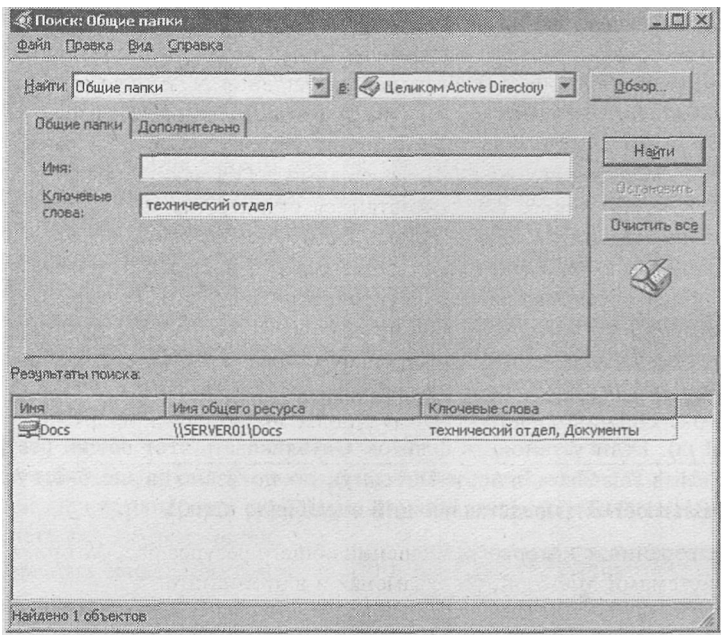


Рис. 6-3. Поиск общей папки

Настройка разрешений доступа к общему ресурсу

Доступные разрешения общего ресурса перечислены в табл. 6-1. Хотя они не настолько подробны, как разрешения NTFS, но позволяют настроить основные типы доступа к общей папке: *Чтение* (Read), *Изменение* (Change) и *Полный доступ* (Full Control).

Табл. 6-1. Разрешения для общего ресурса

Разрешение	Описание
Чтение (Read)	Пользователи могут просматривать имена папок, а также имена, содержимое и атрибуты файлов, запускать программы и обращаться к другим папкам внутри общей папки
Изменение (Change)	Пользователи могут создавать палки, добавлять файлы и редактировать их содержимое, изменять атрибуты файлов, удалять файлы и папки и выполнять действия, допустимые разрешением *Чтение* (Read)
Полный доступ (Full Control)	Пользователи могут изменять разрешения файлов, становится владельцами файлов и выполнять все действия, допустимые разрешением *Изменение* (Change)

Разрешения общего ресурса можно предоставлять или отменять. Действующим набором разрешений общего ресурса называют сумму разрешений, предоставленных пользователю и всем группам, членом которых он является. Например, если пользователь входит в группу с разрешением *Чтение* (Read) и в группу с разрешением *Изменение* (Change), действующим разрешением считается *Изменение.* Тем не менее, запрет всегда приоритетнее разрешения. Например, если пользователь входит в группу с разрешением *Чтение* (Read) и в группу, которой запрещено разрешение *Полный доступ* (Full Control), он не сможет прочитать файлы и папки внутри общего ресурса.

Разрешения общего ресурса определяют максимальные действующие разрешения для всех файлов и папок внутри общей папки. Назначая разрешения NTFS для отдельных файлов и папок, доступ можно ужесточить, но не расширить. Другими словами, доступ пользователя к файлу или папке определяется наиболее жестким набором из разрешений общего ресурса и разрешений NTFS. Если разрешения NTFS дают группе полный доступ к папке, а разрешения общего ресурса остаются стандартными — группе *Все* (Everyone) предоставлено разрешение *Чтение* (Read) или даже *Изменение* (Change) — разрешения NTFS ограничиваются разрешением общего ресурса. Этот механизм означает, что разрешения общего ресурса усложняют управление доступом к ресурсам. Это одна из причин, по которой в организациях обычно назначают общим ресурсам открытые разрешения: группе *Все* (Everyone) дается разрешение *Полный доступ* (Full Control), а для защиты папок и файлов используют только разрешения NTFS. Прочитайте врезку «Три точки зрения на разрешения общего ресурса» с более подробной информацией.

Три точки зрения на разрешения общего ресурса

Важно понять точки зрения, с которых разрешения общего ресурса рассматриваются реальными системами Microsoft, на экзаменах и в этой книге.

Ограничения разрешений общего ресурса

Разрешения общего ресурса имеют ряд существенных ограничений.

- Область **действия.** Разрешения общего ресурса применяют только для ограничения удаленного доступа через службу *Клиент для сетей Microsoft* (Client for Microsoft Networks); они не распространяются ни на локальный доступ, ни на доступ через службы терминалов, ни на любые другие типы удаленного доступа, например по протоколам HTTP, FTP, Telnet и т. п.
- . **Репликация.** Разрешения общего ресурса игнорируются *Службой репликации файлов* (File Replication Service, FRS).
- **Устойчивость.** Разрешения общего ресурса не сохраняются при архивировании или восстановлении тома данных.
- **Хрупкость.** Разрешения общего ресурса теряются при перемещении или переименовании папки.
- **Недостаточно детальный контроль.** Разрешения общего ресурса не поддерживают тонкую настройку; они предлагают один шаблон разрешений, который применяется ко всем файлам и папкам внутри общей папки. Нельзя расширить или ограничить доступ к файлам и папкам внутри общей папки без применения разрешений NTFS.
- Аудит. Нельзя настроить аудит на основе разрешений общего ресурса.

- NTFS — **более продуманная система.** Разрешения NTFS обеспечивают надежный, безопасный способ управления доступом к файлам и папкам. Разрешения NTFS реплицируются, сохраняются при архивировании и восстановлении тома данных, подлежат аудиту и обеспечивают чрезвычайную гибкость и удобство управления.
- **Сложность.** При назначении разрешений общего ресурса вместе с разрешениями NTFS вступает в силу наиболее строгий набор разрешений, в результате усложняется анализ действующих разрешений и устранение неполадок доступа к файлам.

Использование разрешений общего ресурса для решения реальных задач

Из-за этих ограничений разрешения общего ресурса применяются только в очень редких случаях, когда том отформатирован под файловую систему FAT или FAT32, которые не поддерживают разрешения NTFS. Иначе, правило «реального мира» звучит так: предоставьте группе *Все* (Everyone) разрешение общего ресурса *Полный доступ* (Full Control), а для ограничения доступа к содержимому общей папки используйте разрешения NTFS.

Microsoft ужесточает разрешения общего ресурса

До появления Windows XP группа *Все* (Everyone) по умолчанию получала разрешение общего ресурса *Полный доступ* (Full Control). Это стандартное разрешение позволяло легко придерживаться политики «реального мира»: администраторы не изменяли разрешения общего ресурса и сразу настраивали разрешения NTFS. В Windows Server 2003 по умолчанию группе *Все* (Everyone) назначается разрешение *Чтение* (Read), а группе *Администраторы* (Administrators) — *Полный доступ* (Full Control). Это проблематично, поскольку теперь обычным пользователям во всем дереве общей папки разрешено только чтение.

Microsoft преследовала при этом благородную цель: повысить безопасность, чтобы общие ресурсы изначально были менее уязвимы. После создания общей папки администраторы часто забывали назначить разрешения NTFS, и ресурс оставался «слишком доступным». Назначая общей папке разрешение *Чтение* (Read), Microsoft помогает администраторам избежать этой проблемы. К сожалению, большинство организаций избегают разрешений общего ресурса из-за связанных с ними ограничений и для защиты ресурсов используют только разрешения NTFS. Теперь администраторам нужно не забыть о настройке разрешений общего ресурса и явно разрешить группе *Все* (Everyone) полный доступ.

Темы сертификационного экзамена

Существует третья точка зрения на разрешения общего ресурса: темы сертификационного экзамена. Хотя разрешения общего ресурса обычно реализуются в соответствии со строгой политикой организации (всем предоставлен полный доступ), сам факт, что когда-нибудь значение по умолчанию может измениться и что данные могут быть сохранены на томе FAT или FAT32, где разрешения общего ресурса являются единственным способом управления доступом, означает, что для сдачи экзамена вы должны разбираться в этой теме. Особое значение имеют

сценарии с применением и разрешений общего ресурса, и разрешений NTFS, где при обращении к ресурсу через службу *Клиент для сетей Microsoft* (Client for Microsoft Networks) в действие вступает наиболее жесткий набор разрешений доступа.

Так что уделите внимание разрешениям общего ресурса. Изучите их нюансы. Научитесь определять действующие разрешения в сочетании с разрешениями NTFS. Затем настройте общие папки согласно принципам вашей организации, которые, вероятно, предполагают изменение стандартного разрешения общего ресурса в Windows Server 2003 и назначение группе *Все* (Everyone) разрешение *Полный доступ* (Full Control).

Управление сеансами пользователей и открытыми файлами

Иногда сервер для обслуживания приходится переводить в автономный режим, например для архивирования или выполнения других задач, требующих, чтобы пользователи были отключены, а файлы закрыты и не заблокированы. В таких случаях используется оснастка *Общие папки* (Shared Folders).

Узел **Сеансы (Sessions)** оснастки *Общие папки* (Shared Folders) позволяет отследить количество пользователей, подключенных к определенному серверу и при необходимости отключить их. Узел **Открытые файлы (Open Files)** содержит список всех открытых файлов и блокировок файлов для одного сервера и позволяет отключить все открытые файлы.

Перед выполнением этих операций полезно известить пользователя об отключении, чтобы он успел сохранить данные. Вы можете отправить текстовое сообщение, щелкнув правой кнопкой узел **Общие папки (Shares)** и выбрав соответствующую команду. Сообщения пересылаются службой Messenger, которая использует имя компьютера, а не пользователя. По умолчанию служба Messenger в Windows Server 2003 отключена; ее необходимо настроить для автоматического или ручного запуска перед передачей сообщения.

Лабораторная работа. Настройка общих папок

На этой лабораторной работе вы настроите общую папку и измените ее разрешения. Затем вы подключитесь к общей папке и имитируете обычные действия, предшествующие переводу сервера в автономный режим.

Упражнение 1. Открытие общего доступа к папке

1. Создайте папку Docs на диске C:, но пока не делайте ее общей.
2. Откройте страницу **Управление данным сервером (Manage Your Server)** из группы программ **Администрирование (Administrative Tools).**
3. В категории **Файловый сервер (File Server)** щелкните **Управление этим файловым сервером (Manage This File Server).** Если на вашем сервере не настроена роль **Файловый сервер (File Server),** добавьте ее или запустите консоль *Управление файловым сервером* (File Server Management), используя следующий совет.

Совет Консоль *Управление файловым сервером* очень помогает в работе, поэтому можно создать для нее ярлык на рабочем столе. Путь к ней: %SystemRoot%\System32\Filesvr.msc.

4. Выберите узел **Общие папки (Shares).**
5. Щелкните **Создать общую папку (Add A Shared Folder)** в списке задач на правой панели, в меню **Действие (Action)** или в контекстном меню.
6. Откроется окно *Мастер создания общих ресурсов* (Share A Folder Wizard). Щелкните **Далее (Next).**
7. Введите путь c:\docs и щелкните **Далее (Next).**
8. Оставьте предложенное имя — docs — и щелкните **Далее (Next).**
9. На странице **Разрешения (Permissions)** выберите **Использовать особые права доступа к общей папке (Use Custom Share And Folder Permissions)** и щелкните кнопку **Настроить (Customize).**
10. Установите флажок **Разрешить (Allow)** для разрешения *Полный доступ* (Full Control) и щелкните OK.
11. Щелкните **Готово (Finish),** а затем **Закрыть (Close).**

Упражнение 2. Подключение к общей папке

1. **В** консоли *Управление файловым сервером* (File Server Management) щелкните узел **Сеансы (Sessions).** Если узел содержит сеансы, в списке задач щелкните **Отключить все сеансы (Disconnect All Sessions),** а затем **Да (Yes).**
2. **В** меню **Пуск (Start)** выберите **Выполнить (Run).** Введите UNC-путь к общей папке \\server01\docs и щелкните OK.
   Используя UNC вместо физического пути c:\docs, вы создаете сетевое подключение к общей папке, так же, как это мог бы делать какой-нибудь пользователь.
3. В консоли *Управление файловым сервером* (File Server Management) щелкните узел **Сеансы (Sessions).** Заметьте: ваша учетная запись присутствует в списке сеансов сервера. Чтобы обновить окно консоли, нажмите F5.
4. Щелкните узел **Открытые файлы (Open Files).** Заметьте: список содержит открытую папку C:\Docs.

Упражнение 3. Имитация подготовки к переводу сервера в автономный режим

1. В консоли *Управление файловым сервером* (File Server Management) щелкните правой кнопкой узел **Общие папки (Shares)** и выберите Все задачи\Отправка **сообщения консоли (All Tasks\Send Console Message).**

   Совет На целевом компьютере должна быть запущена *Служба сообщений* (Messenger). Поскольку не предполагается, что пользователь будет интерактивно работать с консолью на сервере, *Служба сообщений* по умолчанию отключена. Чтобы отправить сообщение самому себе в этом упражнении, из консоли *Службы* (Services) настройте *Службу сообщений* для автоматического или ручного запуска, а затем запустите ее.

2. Наберите сообщение, что сервер переходит в автономный режим и пользователю следует завершить работу.
3. Щелкните **Отправить (Send).**
   Если у вас есть второй компьютер, можно подключиться к общей папке docs удаленно и отправить сообщение другому пользователю.
4. Щелкните узел **Открытые файлы (Open Files).**

5. Выберите папку C:\Docs, которая открыта через ваше подключение к общей папке.
6. Закройте этот файл. Выберите соответствующую команду в меню **Действие (Action),** списке задач или в контекстном меню.
7. Выберите узел **Сеансы (Sessions).**
8. В списке задач щелкните **Отключить все сеансы (Disconnect All Sessions).** После этого файловый сервер можно перевести в автономный режим.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Какие из следующих средств служат для администрирования общих папок на удаленном сервере? Выберите все подходящие варианты.
   a. Оснастка *Общие папки* (Shared Folders).
   b. *Проводник Windows,* запущенный на локальном компьютере и подключенный к общей папке на удаленном сервере или к скрытому общему диску.
   c. *Проводник Windows,* запущенный на удаленном компьютере в сеансе служб терминалов или дистанционного подключения к рабочему столу.
   d. Консоль *Управление файловым сервером* (File Server Management).
2. Общая папка находится на томе FAT32. Группе Project Managers назначено разрешение *Полный доступ* (Full Control). Группе Project Engineers назначено разрешение *Чтение* (Read). Пользователь Julie входит в группу Project Engineers. Она получила повышение и стала членом группы Project Managers. Какие разрешения доступа к этой папке для нее действуют?
3. Общая папка со стандартными разрешениями общего ресурса находится на томе NTFS. Группе Project Managers назначено NTFS-разрешение *Полный доступ* (Full Control). Пользователь Julie из группы Project Managers жалуется, что не может создать файлы в этой папке. Почему Julie не удается создать файлы?

Резюме

- *Проводник Windows* можно использовать для настройки общих папок только на локальном томе. То есть, чтобы использовать *Проводник для* управления общими папками, нужно войти на сервер локально (интерактивно) или подключиться к нему с помощью службы *Дистанционное подключение к рабочему столу* (Remote Desktop) (фактически, средствами служб терминалов).
- Оснастка *Общие папки* (Shared Folders) позволяет управлять общими ресурсами на локальном или удаленном компьютере.
- Скрытые общие ресурсы, которые не видны в списке обозревателя, можно создать, добавив знак доллара ($) к имени ресурса. Для подключения к таким ресурсам используют формат UNC: \\имя_сервера\имя_общего_ресурса$.
- Разрешения общего ресурса определяют действующие эффективные разрешения для всех файлов и папок, к которым обращаются через подключения службы *Клиент для сетей Microsoft* (Client for Microsoft Networks).

  Разрешения общего ресурса не распространяются на доступ через службы терминалов, IIS, локальный (интерактивный) и другие типы доступа.

Занятие 2. Настройка разрешений файловой системы

Серверы Windows поддерживают детализированный механизм управления доступом к файлам и папкам — разрешения NTFS. Разрешения доступа к ресурсам хранятся в виде *записей управления доступом* (access control entries, ACE) в таблице ACL, которая является частью дескриптора безопасности каждого ресурса. При обращении к ресурсу маркер безопасности доступа пользователя, содержащий *идентификаторы защиты* (security identifier, SID) учетной записи пользователя и групп, членом которых тот является, сравнивается с идентификаторами SID в ACE-записях таблицы ACL. Этот процесс авторизации практически не изменился со времен Windows NT. Тем не менее детали реализации авторизации, средства управления доступом к ресурсам и специфика настройки доступа изменялись с каждой версией Windows.

На этом занятии обсуждаются особенности и новые функции управления доступом к ресурсам в Windows Server 2003. Вы научитесь использовать редактор ACL для управления шаблонами разрешений, наследованием, особыми разрешениями и узнаете, как определить итоговые действующие разрешения для пользователя или группы.

Изучив материал этого занятия, вы сможете:

- ✓ настроить разрешения с помощью редактора ACL для Windows Server 2003;
- ✓ управлять наследованием ACL;
- ✓ определить итоговые, то есть действующие разрешения;
- ✓ проверить действующие разрешения;
- ✓ сменить владельцев файлов или папок;
- ✓ передать права владения файлами и папками.

Продолжительность занятия — около 30 минут.

Настройка разрешений

Проводник Windows является наиболее распространенным средством управления разрешениями доступа к ресурсам, как на локальном томе, так и на удаленном сервере. В отличие от общих папок, *Проводник* позволяет настраивать разрешения локально и удаленно.

Редактор таблицы управления доступом

Как и в предыдущих версиях Windows, для настройки безопасности файлов и папок на любом томе NTFS нужно щелкнуть ресурс правой кнопкой, в контекстном меню выбрать **Свойства (Properties)** [или **Общий доступ и безопасность (Sharing And Security)]** и перейти на вкладку **Безопасность (Security).** Открывшееся диалоговое окно может называться по-разному: **Разрешения (Permissions), Параметры безопасности (Security Settings),** вкладка **Безопасность (Security)** или **Редактор таблицы управления доступом** (редактор ACL). Независимо от названия оно выглядит одинаково. Пример вкладки **Безопасность (Security)** окна свойств папки Docs см. на рис. 6-4.

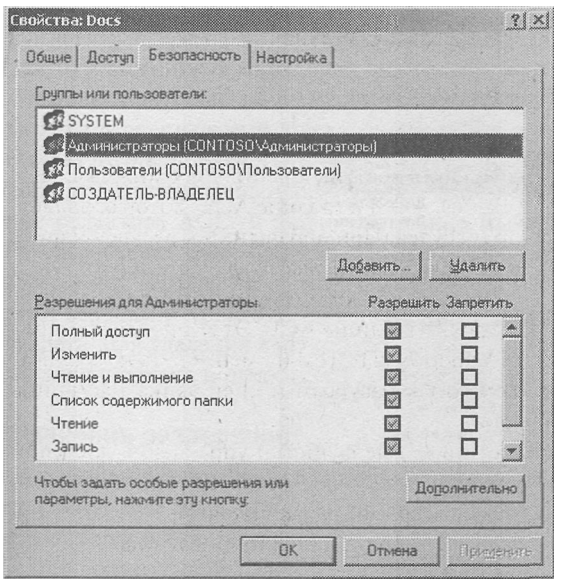


Рис. 6-4. Редактор ACL в окне свойств папки Docs

До появления Windows 2000 разрешения были довольно простыми, но в Windows 2000 и последующих версиях Microsoft предоставила более гибкие и мощные способы управления доступом к ресурсам. Мощь добавила сложности, и теперь редактор ACL состоит из трех диалоговых окон.

Первое диалоговое дает общую картину настроек безопасности и разрешений для ресурса и позволяет выбрать отдельную учетную запись, для которой определен доступ, чтобы просмотреть шаблоны разрешений, назначенные этому пользователю, группе или компьютеру. Каждый шаблон в этом окне — совокупность разрешений, которые вместе обеспечивают некий типичный уровень доступа. Например, чтобы пользователь мог прочитать файл, необходимо предоставить несколько разрешений низкого уровня. Чтобы скрыть эту сложность, вы можете применить шаблон **Чтение и выполнение (Read & Execute),** а ОС сама настроит нужные разрешения доступа к файлу или папке.

Чтобы более подробно изучить данную таблицу ACL, щелкните кнопку **Дополнительно (Advanced),** откроется второе окно редактора ACL — **Дополнительные параметры безопасности для Docs (Advanced Security Settings For Docs),** показанное на рис. 6-5. Здесь перечислены конкретные записи управления доступом, назначенные данному файлу или папке. Сведения в этом перечне максимально приближены к реальной информации, которая хранится в самой таблице ACL. Второе диалоговое окно позволяет также настраивать аудит, управлять правами владения и определять действующие разрешения.

Если выбрать разрешение в списке **Элементы разрешений (Permission Entries)** и щелкнуть **Изменить (Edit),** откроется третье диалоговое окно редактора ACL. В окне **Элемент разрешения для Docs (Permission Entry For Docs),** показанном на рис. 6-6, перечислены подробные, наиболее детализированные разрешения, которые составляют элемент разрешений в списке **Элементы разрешений (Permissions Entries)** во втором диалоговом окне и в списке **Разрешения для (Permissions For)** в первом окне.

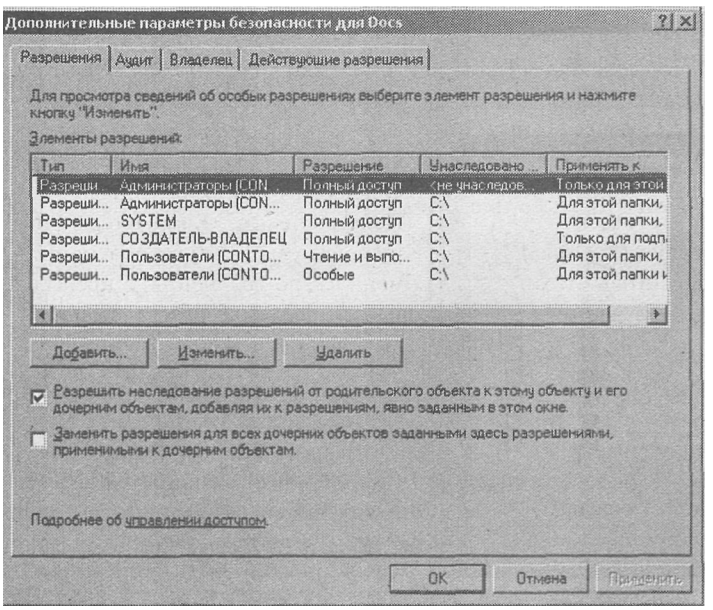


Рис. 6-5. Диалоговое окно *Дополнительные параметры безопасности* редактора ACL

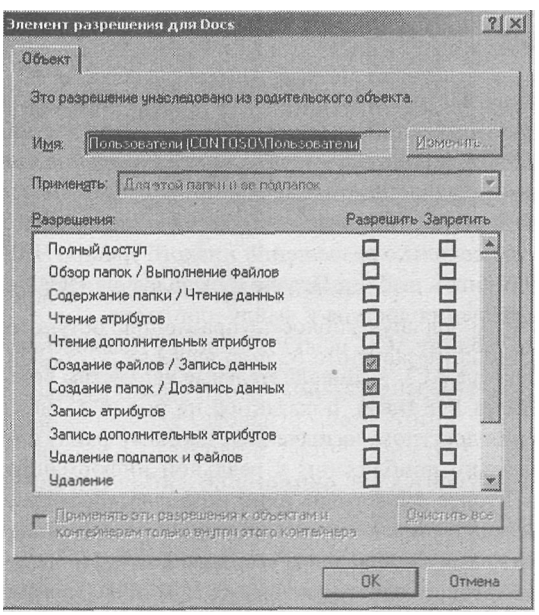


Рис. 6-6. Диалоговое окно *Элемент разрешения* редактора ACL

Подготовка к экзамену Оснастка *Общие папки* (Shared Folders) также позволяет открыть редактор ACL. Откройте свойства общей папки и перейдите на вкладку **Безопасность (Security).**

Добавление и удаление элементов разрешений

Любому участнику безопасности можно предоставить или запретить доступ к ресурсу. В Windows Server 2003 допустимые участники безопасности: пользователи, группы, компьютеры и специальный класс объектов InetOrgPerson (см. RFC 2798), который представляет пользователей в некоторых ситуациях при совместной работе разных платформ. Чтобы добавить разрешение, щелкните Добавить **(Add)** в первом или втором диалоговом окне редактора ACL. В диалоговом окне **Выбор: «Пользователи», «Компьютеры» или «Группы» (Select User, Computer Or Group)** выберите нужного участника безопасности и разрешения. Интерфейс диалоговых окон слегка изменился по сравнению с предыдущими версиями Windows, но не настолько, чтобы опытный администратор не смог им овладеть. Для удаления явного разрешения, которое вы добавили в ACL, выберите нужный пункт списка и щелкните **Удалить (Remove).**

Изменение разрешений

Для изменения разрешения достаточно на вкладке **Безопасность (Security)** окна свойств установить или снять флажки **Разрешить (Allow)** или **Запретить (Deny),** в результате чего применяется соответствующий шаблон разрешений.

Для более тонкой настройки щелкните кнопку **Дополнительно (Advanced),** выберите элемент разрешения и щелкните кнопку **Изменить** (Edit). Изменить можно только явные разрешения. Унаследованные разрешения обсуждаются далее на этом занятии.

Диалоговое окно **Элемент разрешения для Docs (Permission Entry For Docs),** показанное на рис. 6-6, позволяет изменить разрешения и указать границы наследования разрешений в раскрывающемся списке **Применять (Apply Onto).**

Внимание! Вы должны хорошо понимать влияние изменений, сделанных в этом диалоговом окне. Вы можете благодарить Microsoft за возможность тонкой настройки, но с ростом детализации повышается сложность и вероятность допустить ошибку.

Новые участники безопасности

Windows Server 2003, в отличие от Windows NT 4, позволяет добавлять компьютеры или группы компьютеров в ACL, обеспечивая этим большую гибкость управления доступом к ресурсам на основе клиентских компьютеров, независимо от пользователя, который пытается получить доступ. Предположим, вы намерены установить компьютер с общим доступом в комнате отдыха сотрудников, но не хотите, чтобы руководители просматривали с него секретные данные. Если добавить этот компьютер в таблицы ACL и запретить с него доступ к секретным данным, руководитель не сможет обратиться к секретным данным из комнаты отдыха и будет работать с ними только с собственного компьютера.

Windows Server 2003 также позволяет управлять доступом к ресурсу в зависимости от способа входа в систему. Вы можете добавить в ACL особые учетные записи: *Интерактивные* (Interactive) — пользователи, которые зарегистрировались локально, *Сеть* (Network) — сетевое подключение, например система Windows, на которой запущена служба *Клиент для сетей Microsoft* (Client for Microsoft Networks), и *Пользователь сервера терминалов* (Terminal Server User) — пользователи, подключившиеся через службу *Дистанционное управление рабочим столом* (Remote Desktop) или службы терминалов.

Шаблоны разрешений и особые разрешения

Шаблоны разрешений на вкладке **Безопасность (Security)** первого диалогового окна представляют собой совокупность особых разрешений, которые полностью перечислены в третьем диалоговом окне **Элемент разрешения (Permissions Entry).** Большинство шаблонов и особых разрешений говорят сами за себя, а другие мы не будем обсуждать в этой книге. Однако некоторые моменты заслуживают упоминания.

- ***Чтение и выполнение* (Read & Execute).** Чтобы позволить пользователям открывать и читать файлы и папки, достаточно назначить им этот шаблон разрешений. Он также позволяет пользователю скопировать ресурс, если тот имеет разрешение на запись для целевой папки или носителя. В Windows нет разрешений, запрещающих копирование. Подобные функции станут возможными благодаря технологиям цифрового управления правами — Digital Rights Management, когда они будут встроены в платформы Windows.
- ***Запись* (Write) и *Изменение* (Modify).** Шаблон *Запись* (Write) позволяет создавать новые файлы и папки (когда применен к папке) и изменять содержимое и атрибуты файлов (скрытый, системный, только для чтения) и дополнительные атрибуты, определяемые приложением, которое отвечает за этот документ (когда применяется к файлу). Шаблон *Изменение* (Modify) дополнительно разрешает удалить объект.
- ***Смена разрешений* (Change Permissions).** Поработав с таблицами ACL некоторое время, вы можете заинтересоваться, кто вправе изменять разрешения. В первую очередь, конечно, владелец ресурса (см. далее). Кроме того, это может сделать любой пользователь с действующим разрешением *Смена разрешений* (Change Permissions), которое задают с помощью третьего диалогового окна **Элемент разрешения для Docs (Permission Entry For Docs)** редактора ACL. Это разрешение также входит в шаблон *Полный доступ* (Full Control).

Наследование

Windows Server 2003 поддерживает наследование разрешений, которое просто означает, что по умолчанию разрешения папки распространяются на все ее файлы и подпапки. Любые изменения родительской таблицы ACL будут отражаться на всем содержимом папки. Наследование позволяет управлять ветвями ресурсов в единых точках администрирования с помощью одной таблицы ACL.

Понятие наследования

Наследование работает благодаря двум характеристикам дескриптора безопасности ресурса. В первую очередь, по умолчанию разрешения наследуются. Разрешение *Чтение и выполнение* (Read & Execute) на рис. 6-5 распространяется на саму папку, подпапки и файлы. Тем не менее, одного этого недостаточно, чтобы наследование работало. Вторая причина в том, что по умолчанию при создании новых объектов установлен флажок **Разрешить наследование разрешений от родительского объекта к этому объекту... (Allow Inheritable Permissions From The Parent To Propagate To This Object...),** видимый на том же рисунке.

Таким образом, созданный файл или папка будут наследовать разрешения у своего родителя, а изменения разрешений родителя будут отражаться на дочерних файлах и папках. Важно понять такую двухэтапную реализацию разрешений, поскольку она дает нам два способа управления наследованием: со стороны родительского и дочернего объектов.

Унаследованные разрешения по-разному отображаются в каждом окне редактора ACL. В первом и третьем диалоговых окнах [на вкладке **Безопасность (Security)** и в окне **Элемент разрешения (Permissions Entry)]** унаследованные разрешения отображаются в виде «серых» флажков, чтобы отличать их от явных разрешений, то есть назначенных ресурсу напрямую. Второе диалоговое окно — **Дополнительные параметры безопасности (Advanced Security Settings)** — содержит папки, от которых наследуется каждый элемент разрешения.

Перекрытие наследования

Наследование позволяет настраивать разрешения на вершине дерева папок. Эти разрешения и их изменения будут распространяться на все файлы и папки в дереве, для которых по умолчанию разрешено наследование.

Впрочем, иногда требуется изменить разрешения подпапки или файла, чтобы расширить или ограничить доступ пользователя или группы. Унаследованные разрешения нельзя удалить из ACL. Их можно перекрыть (заменить), назначив явные разрешения. Либо можно отменить наследование и создать ACL, содержащую только явные разрешения.

Для замены унаследованных разрешений явными просто установите соответствующий флажок. Например, если папка наследует разрешение *Чтение* (Read), предоставленное группе Sales Reps, а вы не хотите, чтобы эта группа могла обращаться к папке, установите для этой группы флажок **Запретить (Deny)** напротив разрешения *Чтение* (Read).

Чтобы отменить все унаследованные разрешения, откройте диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings)** ресурса и снимите флажок **Разрешить наследование разрешений от родительского объекта к этому объекту... (Allow Inheritable Permissions From The Parent To Propagate To This Object...).** Все разрешения, унаследованные от родительского объекта, будут заблокированы. После этого вам придется назначить явные разрешения, чтобы проконтролировать доступ к ресурсу.

Windows помогает задать явные разрешения, когда наследование отменяется. Появ**ится** окно (рис. 6-7) с вопросом, как поступить с разрешениями: **Копировать (Copy) или Удалить (Remove).**

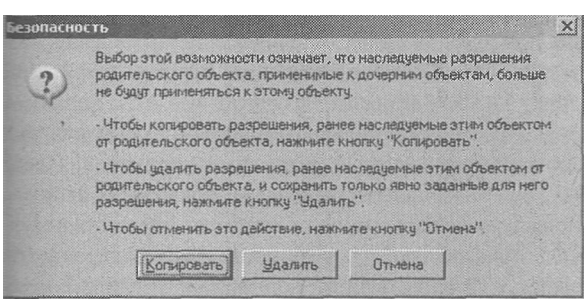


Рис. 6-7. Копирование или удаление элементов разрешений

По щелчку **Копировать (Copy)** создаются явные разрешения, идентичные унаследованным. Затем можно удалить отдельные элементы разрешений, которые не должны влиять на ресурс. Если же вы выберете **Удалить (Remove),** предлагается пустая таблица ACL, которую вы сами заполняете элементами разрешений. Результат одинаков в обоих случаях: таблица ACL заполнена явными разрешениями. Вопрос в том, что проще: заполнить пустую ACL или «довести до ума» копию унаследованных разрешений. Если

новая ACL сильно отличается от унаследованной, щелкните **Удалить (Remove),** если незначительно, лучше щелкните **Копировать (Copy).**

Снимая флажок **Разрешить наследование разрешений от родительского объекта к этому объекту... (Allow Inheritable Permissions From The Parent To Propagate To This Object...),** вы полностью блокируете наследование. Доступ к ресурсу регулируется только явными разрешениями, назначенными для файла или папки. Любые изменения ACL родительской папки не будут влиять на ресурс; даже если родительские разрешения являются наследуемыми, дочерний ресурс не наследует их. Старайтесь как можно реже отменять наследование, поскольку это затрудняет управление, определение прав и устранение неполадок доступа к ресурсу.

Восстановление наследования

Наследование можно восстановить двумя способами: со стороны дочернего ресурса или со стороны родительской папки. Результаты немного различаются. Восстановить наследование для ресурса может понадобиться, если вы случайно отменили его или изменились бизнес-требования организации. Просто установите флажок **Разрешить наследование разрешений... (Allow Inheritable Permissions...)** в диалоговом окне **Дополнительные параметры безопасности (Advanced Security Settings).** Наследуемые разрешения родительской папки будут распространяться на дочерний ресурс. Однако останутся все явные разрешения, назначенные ресурсу. Итоговая ACL будет содержать совокупность явных разрешений, которые вы можете решить удалить, и унаследованных разрешений. По этой причине вы не увидите некоторые унаследованные разрешения в первом и третьем диалоговых окнах редактора ACL. Например, если группе Sales Reps явно назначено разрешение *Чтение и выполнение* (Read & Execute) в отношении какого-нибудь ресурса, которое назначено и родительской папке, то при восстановлении наследования со стороны дочернего ресурса, ему назначаются и унаследованные, и явные разрешения. Вы увидите флажок в первом и третьем диалоговых окнах; поскольку явные разрешения при отображении скрывают унаследованные. Однако унаследованное разрешение существует, о чем свидетельствует второе диалоговое окно — **Дополнительные параметры безопасности.**

Второй метод восстановления наследования — со стороны родительской папки. В диалоговом окне **Дополнительные параметры безопасности** для родительской папки установите флажок **Заменить разрешения для всех дочерних объектов заданными здесь разрешениями, применимыми к дочерним объектам (Replace Permission Entries On All Child Objects With Entries Shown Here That Apply To Child Objects).** Результат: все ACL подпапок и файлов удалены. На дочерние ресурсы распространяются разрешения родительской папки. Это можно представить как сквозное применение разрешений родителя. После выбора этого варианта любые явные разрешения, назначенные подпапкам и файлам, удаляются (в отличие метода восстановления наследования со стороны дочерних ресурсов). Наследование восстанавливается, поэтому любые изменения ACL родительской папки отражаются на подпапках и файлах. В этот момент подпапкам и файлам можно назначить новые явные разрешения. Флажок **Заменить разрешения... (Replace Permissions...)** выполняет свою функцию, только когда вы его отмечаете, однако в дальнейшем разрешения родительской папки не будут заменять собой явные разрешения.

Действующие разрешения

Часто пользователи принадлежат к нескольким группам с разными уровнями доступа к ресурсам. Когда ACL содержит несколько элементов, вы должны уметь определять раз-

решения пользователя, исходя из разрешений групп, членом которых он является. Конечные разрешения называют *действующими* (effective permissions).

Подготовка к экзамену Действующие разрешения — типичная тема большинства ключевых экзаменов по Microsoft Windows Server 2003. Уделите особое внимание следующему материалу и любым практическим вопросам, касающимся действующих разрешений.

Понятие действующих разрешений

Ниже перечислены правила, по которым определяют действующие разрешения.

- **Разрешения файлов приоритетнее разрешений папок.** На самом деле это не совсем правило, но это положение часто встречается в документации и поэтому заслуживает упоминания. Каждый ресурс хранит таблицу ACL, и лишь она отвечает за управление доступом к этому ресурсу. Хотя элементы в этой таблице могли появиться в результате наследования, в любом случае они являются элементами ACL ресурса. Подсистема безопасности вообще не обращается к родительской папке при определении прав доступа. Так что это правило можно интерпретировать следующим образом: значение имеет только ACL самого ресурса.
- **Разрешения, позволяющие доступ, суммируются.** Уровень доступа к ресурсу определяется разрешениями одной или нескольких групп, которым принадлежит пользователь. Разрешения, позволяющие доступ, предоставленные любому пользователю, группе или компьютеру в вашем маркере безопасности доступа, будут применяться и к вашей учетной записи, поэтому ваши действующие разрешения, по сути, есть сумма разрешений, позволяющих доступ. Если для какой-либо папки группе Sales Reps даны разрешения *Чтение и выполнение* (Read & Execute) и *Запись* (Write), а группе Sales Managers — *Чтение и выполнение* и *Удаление* (Delete), пользователь, входящий в обе группы, будет обладать действующими разрешениями, эквивалентными шаблону *Изменение* (Modify), куда входят разрешения *Чтение и выполнение, Запись* и *Удаление*.
- **Разрешения, запрещающие доступ, приоритетнее позволяющих.** Запрет доступа к объекту всегда приоритетнее разрешения доступа. Предположим, в описанном выше примере группе Temporary Employees запрещено чтение. Тогда пользователь, который является временным торговым представителем и принадлежит группам Sales Reps и Temporary Employees, не сможет прочитать данные в этой папке.

  Примечание Рекомендуется как можно реже применять запреты. Вместо этого предоставляйте разрешения для минимального круга ресурсов, необходимых для решения бизнес-задачи. Запреты усложняют администрирование ACL, их следует использовать, только когда действительно необходимо запретить доступ пользователю — члену других групп с этим разрешением.

  Подготовка к экзамену Если пользователю запрещен доступ к ресурсу, который ему действительно нужен, отмените запрет либо удалите пользователя из группы, которой запрещен доступ. Если запрет наследуется, можно явно разрешить доступ.

- **Явные разрешения приоритетнее унаследованных.** Элемент разрешения, явно определенный для ресурса, перекроет конфликтующий с ним унаследованный элемент. Из этого следуют базовые принципы проектирования: родительская папка определяет

«правило» через наследуемые разрешения; если к дочернему объекту требуется предоставить доступ, противоречащий этому правилу, в ACL объекта добавляют явное разрешение, которое имеет преимущество.

Подготовка к экзамену В итоге можно сделать вывод: явное разрешение, позволяющее доступ, перекроет унаследованное разрешения, запрещающее доступ.

Определение действующих разрешений

NTFS поддерживает массу функций управления разрешениями и наследованием, что с одной стороны расширяет возможности системы, а с другой — усложняет ее. Глядя на все эти разрешения, пользователей и группы, как узнать действительные права доступа пользователя?

Microsoft выпустила долгожданное средство, которое помогает ответить на этот вопрос. Вкладка **Действующие разрешения (Effective Permissions)** диалогового окна **Дополнительные параметры безопасности (Advanced Security Settings)** дает довольно точное приближение итоговых разрешений доступа пользователя к ресурсу (рис. 6-8).

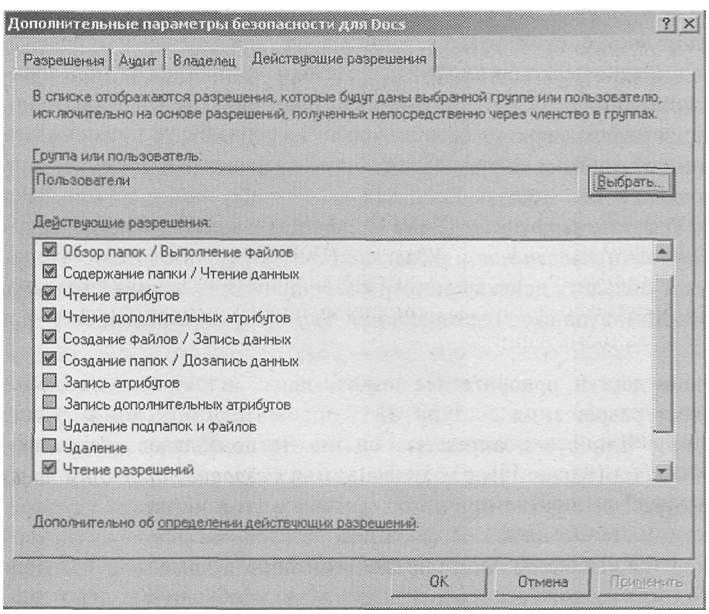


Рис. 6-8. Вкладка *Действующие разрешения* диалогового окна *Дополнительные параметры безопасности*

Щелкните кнопку **Выбрать (Select)** и укажите пользователя, группу или встроенную учетную запись, которую нужно проанализировать. Windows Server 2003 построит список действующих разрешений. Этот список — лишь приближение. В нем не учтены ни разрешения общего ресурса, ни принадлежность учетной записи перечисленным ниже особым группам.

- *Анонимный вход* (Anonymous Logon).
- *Пакетные файлы* (Batch).
- *Группа-создатель* (Creator Group).

- *Удаленный доступ* (Dialup).
- *Контроллеры домена предприятия* (Enterprise Domain Controllers).
- *Интерактивные* (Interactive).
- *Сеть* (Network).
- *Proxy*.
- *Ограниченные* (Restricted).
- *Remote Interactive Logon*.
- *Служба* (Service).
- *System*.
- *Пользователь сервера терминалов* (Terminal Server User).
- *Другая организация* (Other Organization).
- *Данная организация* (This Organization).

Кроме того, ACL может содержать элементы, например, для учетных записей *Сеть* или *Интерактивные,* которые могли бы обеспечивать пользователям различный уровень доступа в зависимости от способа входа в систему — локально или удаленно. Поскольку рассматриваемый пользователь не входит в систему, разрешения, зависящие от способа входа в систему, игнорируются. Впрочем, в качестве дополнительного шага вы можете определить действующие разрешения для таких встроенных или особых учетных записей, как *Интерактивные* и *Сеть*.

Права владения ресурсом

Windows Server 2003 поддерживает специального участника безопасности — *Создатель-владелец* (Creator Owner). Помимо этого, в дескрипторе безопасности ресурса есть запись, определяющая владельца объекта. Чтобы научиться управлять разрешениями доступа к ресурсам и устранять связанные с ними неполадки, необходимо хорошо понимать эти две составляющие механизма защиты.

Создатель-владелец

Когда пользователь создает файл или папку (для чего он должен обладать разрешениями *Создание файлов/Запись данных* (Create Files/Write Data) или *Создание папок/Дозапись данных* (Create Folders/Append Data) соответственно), он становится создателем и первым владельцем этого ресурса. Любые разрешения, предоставленные особой учетной записи *Создатель-владелец* (Creator Owner) для родительской папки, явно назначаются пользователю в отношении этого нового ресурса.

Предположим, для этой папки пользователям предоставлены разрешения *Создание файлов/Запись данных* (Create Files/Write Data) и *Чтение и выполнение* (Read & Execute), а учетной записи *Создатель-владелец* — разрешение *Полный доступ* (Full Control). Такой набор разрешений позволил бы пользователю Maria создать файл. Как создатель файла, Maria имела бы к нему полный доступ. Пользователь Tia также могла бы создать файл и получить к нему полный доступ. Однако Tia и Maria могли бы лишь читать файлы друг друга. При этом Tia могла бы изменить ACL своего файла. Разрешение *Полный доступ* (*Full* Control) включает разрешение *Смена разрешений* (Change Permissions).

Право владения

Если по каким-либо причинам Tia изменила бы ACL своего файла и запретила бы себе полный доступ, она по-прежнему смогла бы изменять ACL этого файла, поскольку вла-

делец объекта всегда имеет такое право; благодаря этому пользователи не могут навсегда заблокировать собственные файлы и папки.

Рекомендуется управлять правами владения объектом так, чтобы объектом всегда владел соответствующий пользователь. Отчасти это необходимо из-за того, что пользователи могут изменять ACL собственных объектов. Кроме того, такие технологии, как квотирование диска, полагаются на атрибут владения при подсчете места на диске, занятого некоторым пользователем. До выхода Windows Server 2003 управление правами владения было затруднено, теперь же появилось новое средство, упрощающее передачу прав владения.

Владелец указан в дескрипторе безопасности объекта. Первоначальным владельцем становится создатель файла или папки. Право владения объектом можно принимать или передавать следующим образом.

- **Администраторы могут становиться владельцами.** Пользователь из группы *Администраторы* (Administrators) или обладающий правом *Смена владельца* (Take Ownership) может получить во владение любой объект в системе.

  Чтобы стать владельцем ресурса, перейдите на вкладку **Owner (Владелец)** в диалоговом окне **Дополнительные параметры безопасности (Advanced Security Settings),** показанном на рис. 6-9. Выберите в списке свою учетную запись пользователя и щелкните **Применить (Apply).** Установите флажок **Заменить владельца подконтейнеров и объектов (Replace Owner On Subcontainers And Objects),** чтобы стать владельцем всех подпапок и файлов.

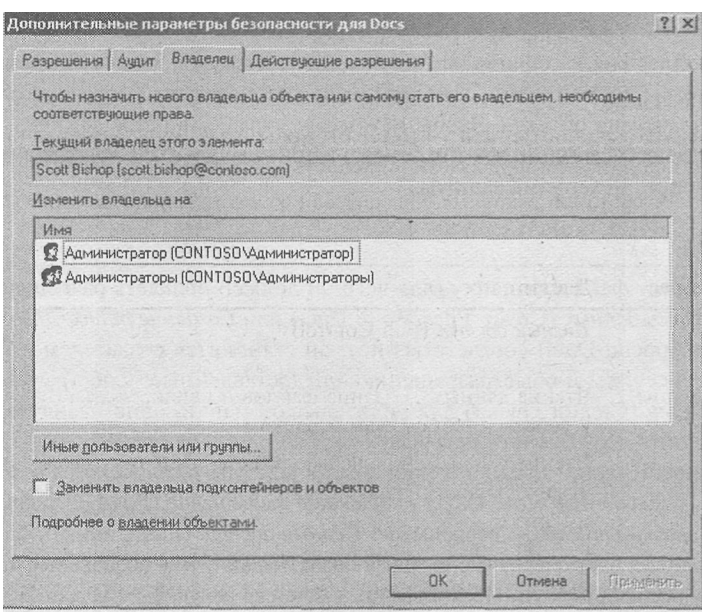


Рис. 6-9. Вкладка *Владелец* диалогового окна *Дополнительные параметры безопасности*

- **Права владения могут принимать пользователи с разрешением *Смена владельца* (Take Ownership).** Особое разрешение *Смена владельца* может быть предоставлено любому пользователю или группе, и они смогут завладеть ресурсом, а значит и изменить ACL чтобы получить достаточные разрешения.

- **Администраторы могут передавать права владения.** Администратор может завладеть любым файлом или папкой. Затем он, как владелец, может изменить разрешения доступа к ресурсу и предоставить разрешение *Смена владельца* другому пользователю, который, в свою очередь, может завладеть этим ресурсом.
- **Привилегия *Восстановление файлов и каталогов* (Restore Files And Directories) разрешает передачу прав владения.** Пользователь с такими полномочиями может передать права владения файлом другому пользователю. Если вам дана привилегия *Восстановление файлов и каталогов,* вы можете щелкнуть кнопку Иные пользователи **или группы** (Other **Users Or Groups)** и выбрать нового владельца. Эта новая функция Windows Server 2003 позволяет администраторам и операторам архивирования управлять правами владения объектом и передавать их без вмешательства пользователя.

Лабораторная работа. **Настройка разрешений файловой системы**

На этой лабораторной работе вы будете использовать редактор ACL для защиты ресурсов, определения действующих разрешений и передачи прав владения файлами. Убедитесь, что учетные записи пользователей и групп настроены согласно описанию в разделе "Прежде всего" этой главы.

Упражнение 1. Настройка разрешений NTFS

1. Откройте папку C:\Docs, к которой вы открыли общий доступ на лабораторной работе занятия 1.
2. Создайте папку с именем Project 101.
3. Откройте редактор ACL: щелкните папку Project 101 правой кнопкой, выберите **Свойства (Properties)** и перейдите на вкладку Безопасность (Security).
4. Настройте доступ согласно следующей таблице. Для этого продумайте и настройте наследование и разрешения для групп.

Участник безопасности	**Доступ**
Администраторы (Administrators)	*Полный доступ* (Full Control)
Пользователи из группы Project 101 Team	Чтение данных, создание файлов и папок, полный доступ к собственным файлам и папкам
Группа Managers	Чтение и изменение любых файлов, запрет на удаление чужих файлов. Полный доступ к собственным файлам и папкам
System	Службы, запущенные под учетной записью System, должны иметь полный доступ

Когда нужные разрешения будут настроены, щелкните **Применить (Apply),** а затем Дополнительно **(Advanced).** Сравните открывшееся окно **Дополнительные параметры безопасности** (Advanced Security Settings) с примером на рис. 6-10.

Для настройки этих разрешений необходимо запретить наследование. Иначе все пользователи,а не только члены группы Project 101 Team, смогут читать файлы в папке Project 101. От родительской папки, C:\Docs, группа *Users* (Пользователи) наследует разрешение *Чтение и выполнение* (Read & Execute). Единственный способ запретить та-

кой доступ — снять флажок **Разрешить наследование разрешений от родительского объекта к этому объекту... (Allow Inheritable Permissions From The Parent To Propagate To This Object...).** Заметьте: требования не указывают запретить чтение группе *Users* (Пользователи), но там и не говорится, что этой группе доступ на чтение необходим. В таких случаях рекомендуется предоставлять минимально требуемый доступ.

После отмены наследования диалоговое окно **Дополнительные параметры безопасности** должно выглядеть, как показано на рис. 6-10.

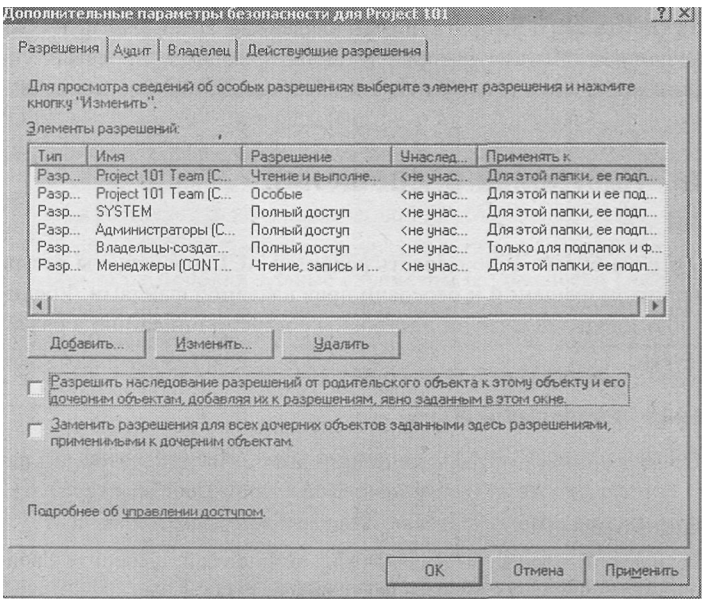


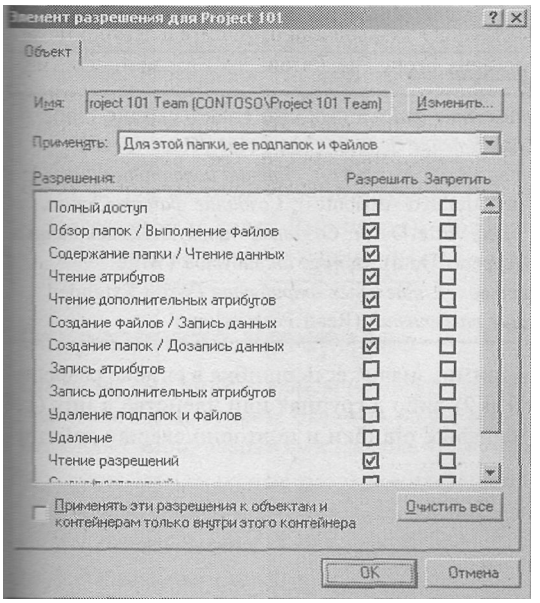
Рис. 6-10. Вкладка *Разрешения* диалогового *ОКАЛ Дополнительные пирометры безопасности*

Флажок, отвечающий за наследование, был снят, и все разрешения отображаются с пометкой **not inherited.** Учетным записям *Администраторы, System* и *Создатель-владелец* предоставлен полный доступ. Помните, что, когда учетной записи *Создатель-владелец* предоставлен полный доступ, пользователь, создавший файл или папку, получает полный доступ к этому ресурсу. Указано, что группа Project 101 обладает особым элементом разрешения. Если выбрать эту запись и щелкнуть **Изменить (Edit),** можно увидеть особые разрешения, назначенные группе Project 101 (рис. 6-11).

Учетной записи Managers предоставлены разрешения *Чтение, Запись и выполнение.* Этот шаблон содержит разрешения на создание файлов и папок. Как и группе Project 101, членам группы Managers при создании новых ресурсов предоставляются разрешения учетной записи *Создатель-владелец.* Этот набор разрешений не позволяет группе Managers удалять файлы других пользователей. Помните, что разрешение *Удаление* содержится в шаблоне *Изменение,* который вы не указали.

Упражнение 2. Использование запретов

1. Предположим, ваша организация наняла группу сотрудников по контракту. Все учетные записи контрактников входят только в группу Project Contractors. Как запретить контрактникам доступ к папке Project 101, которую вы защитили в предыдущем упражнении?



Ньс. 6-11. Особые разрешения, назначенные группе Project 101

Правильный ответ: ничего делать не нужно. Поскольку контрактники не входят в другие группы домена, у них нет разрешений на какой-либо доступ к ресурсам этой папки.

2. Предположим, учетные записи некоторых пользователей, например Scott Bishop, входят в группы Project Contractors и Engineers. Как запретить контрактникам доступ к папке проекта?

   Правильный ответ: в этом случае необходимо запретить доступ группе Project Contractors. Поскольку контрактники получат разрешения, предоставленные другим группам, вы должны перекрыть эти разрешения явным запретом.

3. Отмените разрешение *Полный доступ* (Full Control) для группы Project Contractors.

Упражнение 3. Действующие разрешения

1. Откройте диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings):** в окне свойств папки Project 101 перейдите на вкладку **Безопасность (Security)** и щелкните **Дополнительно (Advanced).**
2. Перейдите на вкладку **Действующие разрешения (Effective Permissions).**
3. Сверьте разрешения каждого из перечисленных в таблице пользователей.

Пользователь	Действующие разрешения
Scott Bishop	Нет разрешений
Danielle Tiedt	*Обзор папок/Выполнение файлов* (Traverse Folder/Execute File), *Содержание папки/Чтение данных* (List Folder/Read Data), *Чтение атрибутов* (Read Attributes), *Чтение дополнительных атрибутов* (Read Extended Attributes), *Создание файлов/Запись данных* (Create Files/Write Data), *Создание папок/Дозапись данных* (Create Folders/Append Data), *Чтение разрешений* (Read Permissions)

(окончание)

Пользователь	Действующие разрешения
Lorrin Smith-Bates	*Обзор папок/Выполнение файлов* (Traverse Folder/Execute File), *Содержание папки/Чтение данных* (List Folder/Read Data), *Чтение атрибутов* (Read Attributes), *Чтение дополнительных атрибутов* (Read Extended Attributes), *Создание файлов/Запись данных* (Create Files/Write Data), *Создание папок/Дозапись данных* (Create Folders/Append Data), *Запись атрибутов* (Write Attributes), *Запись дополнительных атрибутов* (Write Extended Attributes), *Чтение разрешений* (Read Permissions)

Если эти разрешения не совпадают с вашими, значит есть ошибка в списке разрешений (тогда вернитесь к упражнениям 1 и 2) либо в группах или членстве в них (см. раздел «Прежде всего» этой главы). Исправьте ошибки и повторно сверьте действующие разрешения по таблице.

Упражнение 4. Право владения

1. Войдите в систему как Danielle Tiedt.
2. Откройте общую папку, подключившись к \\Server01\Docs.
3. Откройте папку Project 101 и создайте текстовый файл с именем Report.
4. Из окна свойств файла Report откройте окно **Дополнительные параметры безопасности (Advanced Security Settings).**
5. Убедитесь, что все разрешения наследуются от родительской папки. Чем отличаются таблицы ACL этого объекта и папки Project 101?
   Правильный ответ: папка Project 101 дает полный доступ учетной записи *Создатель-владелец* (Creator Owner). Файл Report предоставляет полный доступ Danielle Tiedt. Когда она создала этот файл, ее идентификатору SID были назначены разрешения, которыми владела особая группа *Создатель-владелец*. Кроме того, разрешения *Создание файлов* (Create Files) и *Создание папок* (Create Folders), предоставленные группе Project 101 Team, относятся к папкам, а потому отсутствуют в ACL файла Report.
6. Войдите в систему как *Администратор* (Administrator).
7. Из окна свойств файла Report откройте окно **Дополнительные параметры безопасности (Advanced Security Settings).**
8. Перейдите на вкладку **Владелец (Owner).**
9. Убедитесь, что текущий владелец — Danielle Tiedt.
10. Выберите свою учетную запись и щелкните **Применить (Apply).** Теперь вы стали владельцем данного объекта.
11. Пользователь с привилегией *Восстановление файлов и каталогов* (Restore Files And Directories) может передать права владения другому пользователю. Щелкните **Иные пользователи или группы (Other Users Or Group)** и выберите учетную запись Lorrin Smith-Bates. Когда она появится в списке **Изменить владельца на (Change Owner To).** щелкните **Применить (Apply).**
12. Убедитесь, что Lorrin Smith-Bates теперь владеет файлом Report.
13. По-вашему, обладает ли теперь Lorrin Smith-Bates полным доступом к этому объекту? Почему? Как вы думаете, сохранился ли у Danielle Tiedt полный доступ, или ее разрешения изменились? Сверьте ваши ответы с вкладкой **Действующие разрешения (Effective Permissions).**

Правильный ответ: Lorrin Smith-Bates обладает не полным доступом, а лишь разрешением Изменение (Modify), поскольку входит в группу Managers, которой дано это разрешение. Разрешение Полный доступ (Full Control), предоставленное учетной записи Создатель-владелец, дается пользователю, только когда **тот создает объект.**

Примечание После создания объекта смена владельца никак не отражается на его ACL. Тем не менее новый владелец [или любой пользователь с разрешением *Смена разрешений* (Change Permissions)] может изменить ACL ресурса, и обеспечить себе необходимый доступ к нему.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

Какие минимальные разрешения NTFS требуются, чтобы пользователи могли открывать файлы и запускать программы из общей папки?

a. *Полный доступ* (Full Control).
b. *Изменение* (Modify).
c. *Запись* (Write).
d. *Чтение и выполнение* (Read & Execute).
e. *Список содержимого папки* (List Folder Contents).

Пользователь Bill жалуется, что не может получить доступ к плану отдела. Вы открываете вкладку **Безопасность (Security)** в окне свойств плана и видите, что все разрешения доступа к документу наследуются от родительской папки плана. Для группы, куда включен Bill, разрешение *Чтение* (Read) отменено. Какое из следующих действий позволило бы пользователю Bill получить доступ к плану?

a. Изменить разрешения родительской папки, чтобы предоставить пользователю Bill разрешение *Полный доступ* (Full Control).
b. Изменить разрешения родительской папки, чтобы предоставить пользователю Bill разрешение *Чтение* (Read).
c. Изменить разрешения доступа к плану, чтобы предоставить пользователю Bill разрешение *Чтение* (Read).
d. Изменить разрешения доступа к плану: снять флажок **Разрешить наследование разрешений... (Allow Inheritable Permissions...),** щелкнуть **Копировать (Copy)** и удалить запрет.
e. Изменить разрешения доступа к плану: снять флажок **Разрешить наследование разрешений... (Allow Inheritable Permissions...),** щелкнуть **Копировать (Copy)** и явно разрешить пользователю Bill полный доступ.
f. Удалить пользователя Bill из группы, которой запрещен доступ.

Пользователь Bill звонит снова и сообщает, что по-прежнему не может получить доступ к плану отдела. Вы открываете вкладку **Действующие разрешения (Effective Permissions),** выбираете учетную запись Bill и видите, что на самом деле ему предоставлены достаточные разрешения. Чем можно объяснить расхождение сведений на вкладке **Действующие разрешения** с реальными полномочиями?

Резюме

- Разрешения NTFS настраивают редактором ACL, который состоит из трех диалоговых окон: вкладки **Безопасность (Security),** а также окон **Дополнительные параметры безопасности (Advanced Security Settings)** и **Элемент разрешения для (Permission Entry For).**
- Разрешения можно предоставлять и отменять, явно или в результате наследования. Запрет разрешения приоритетнее его позволения, а явное разрешение перекрывает унаследованное. В итоге предоставление явного разрешения может перекрыть унаследованный запрет.
- Наследование позволяет администратору управлять разрешениями из одной родительской папки, содержащей файлы и папки, которые удовлетворяют одинаковым требованиям доступа. По умолчанию ACL нового объекта содержит разрешения, унаследованные от родительской папки.
- Существует несколько способов изменить влияние унаследованных разрешений на объект. Можно изменить исходное (родительское) разрешение и позволить объекту его унаследовать; можно назначить объекту явное разрешение, которое приоритетнее унаследованного; можно отменить наследование и указать в ACL явные разрешения, определяющие доступ к объекту.
- Вкладка **Действующие разрешения (Effective Permissions)** диалогового окна **Дополнительные параметры безопасности (Advanced Security Settings)** позволяет определить приближенные права доступа для пользователя или группы путем анализа разрешений учетной записи, а также разрешений групп, которым она принадлежит.
- Пользователь вправе в любое время изменить ACL объекта, которым владеет. Пользователь с разрешением *Смена владельца* (Take Ownership) может стать владельцем объекта, а администратор — завладеть любым объектом в системе. Группы *Администраторы* (Administrators), *Операторы архивирования* (Backup Operators) и другие учетные записи с привилегией *Восстановление файлов и каталогов* (Restore Files And Directories) могут передать право владения файлом или папкой любому другому пользователю или группе.

Занятие 3. **Аудит доступа к файловой системе**

Многие организации используют аудит доступа к файловой системе для оценки использования ресурсов и определения потенциально слабых мест в системе защиты. Windows Server 2003 поддерживает подробный аудит на основе учетных записей пользователей или групп и определенных действий этих записей. Для настройки аудита необходимо указать его параметры, включить политику и изучить события в журнале безопасности. На этом занятии обсуждаются эти процессы и рекомендации по организации эффективного аудита, которые помогут настроить аудит согласно бизнес-требованиям и разобраться в массе зарегистрированных событий.

Изучив материал этого занятия, вы сможете:

- ✓ настроить аудит доступа к файлу или папке;
- ✓ включить аудит на изолированном сервере или совокупности серверов;
- ✓ изучить события, зарегистрированные в журнале безопасности.

Продолжительность занятия — около 20 минут.

Настройка параметров аудита

Чтобы указать действия, которые нужно наблюдать, следует настроить параметры аудита в диалоговом окне **Дополнительные параметры безопасности (Advanced Security Settings)** файла или папки. Вкладка **Аудит (Auditing)** (рис. 6-12) поразительно похожа на вкладку **Разрешения (Permissions).** Только вместо элементов разрешений вы добавляете элементы аудита.

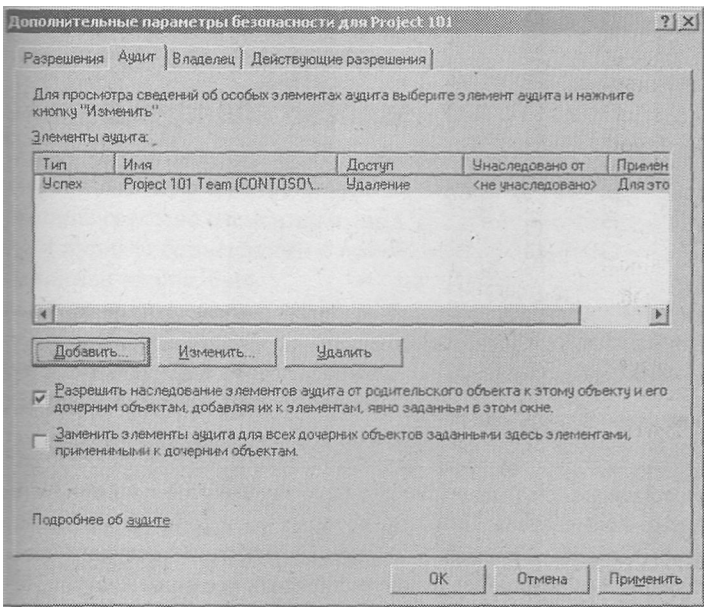


Рис. 6-12. Вкладка *Аудит* диалогового окна *Дополнительные параметры безопасности*

Щелкните кнопку **Добавить (Add),** чтобы выбрать пользователя, группу или компьютер для аудита. Затем в диалоговом окне **Элемент аудита (Auditing Entry)** укажите разрешения, которые нужно отслеживать (рис. 6-13).

Аудиту подлежат успешные и неудачные попытки доступа учетной записи к ресурсу с использованием каждого из назначенных объекту разрешений.

Аудит успешных попыток доступа можно использовать для:

- регистрации попыток доступа к ресурсам для составления отчетов и выписки счетов;
- мониторинга попыток доступа, которые бы указали, что пользователи выполняют непредусмотренные действия, то есть разрешения настроены недостаточно жестко;
- выявления попыток доступа, которые нехарактерны для данной учетной записи; это может быть признаком того, что учетная запись взломана.

Аудит неудачных попыток позволяет:

- обнаружить попытки доступа к секретному ресурсу;
- определить неудачные попытки обращения к файлу или папке, доступ к которой действительно требуется пользователю; это означает, что предоставленных разрешений недостаточно для решения бизнес-задач.

Параметры аудита, как и разрешения, удовлетворяют правилам наследования. Наследуемые параметры аудита распространяются на объекты, разрешающие наследование.

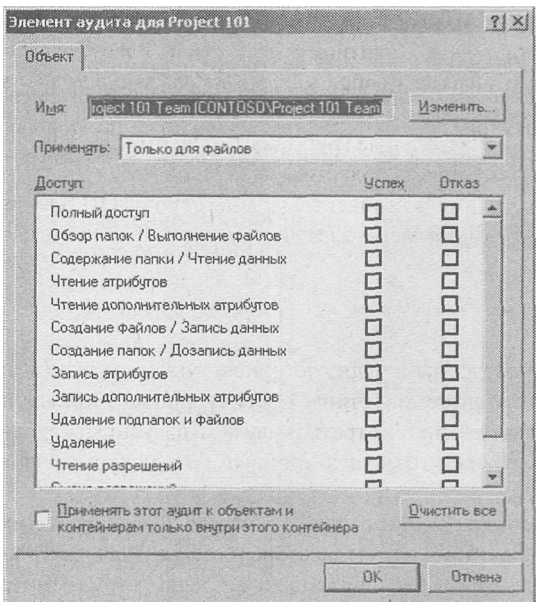


Рис. 6-13. Диалоговое окно *Элемент аудита*

Примечание Журналы аудита довольно быстро растут, поэтому золотое правило аудита — следить за минимальным количеством событий, которых достаточно для решения бизнес-задачи. Если настроить аудит успешных и неудачных попыток доступа к часто используемой папке для группы *Все* (Everyone) и контролировать все виды доступа, будут созданы огромные журналы аудита, которые могут снизить производительность сервера и крайне затруднить поиск нужных событий.

Включение аудита

Настройка элементов аудита в дескрипторе безопасности файла или папки сама по себе не включает аудит. Аудит необходимо включить через политику. После включения аудита подсистема безопасности начинает принимать во внимание параметры аудита и регистрировать соответствующие попытки доступа.

Политику аудита можно включить на изолированном сервере в консоли *Локальная политика безопасности* (Local Security Policy), и на контроллере домена в консоли *Политика безопасности контроллера домена* (Domain Controller Security Policy). Раскройте узел **Локальные политики (Local Policies),** затем **Политика аудита (Audit Policy)** и дважды щелкните политику **Аудит доступа к объектам (Audit Object Access).** Выберите **Определить следующие параметры политики (Define These Policy Settings)** и укажите, какие попытки доступа (успешные, неудачные или **и** те, **и** другие) должны подлежать аудиту.

Примечание Помните, что попытки доступа, которые отслеживаются и регистрируются, — это комбинация элементов аудита для отдельных файлов или папок и параметров политики аудита. Если элементы аудита разрешают регистрацию неудачных попыток доступа, а политика аудита — успешных, журналы аудита останутся пустыми.

Аудит можно включить на одном или нескольких компьютерах, используя объекты групповой политики (ОГП) Active Directory. Узел **Политика аудита (Audit Policy)** расположен в дереве **Конфигурация компьютера (Computer Configuration)\Конфигурация Windows (Windows Settings)\Параметры безопасности (Security Settings)\Локальные политики (Local Policies)\Политика аудита (Audit Policy).** Как и остальные групповые политики, политика аудита влияет на все компьютеры, расположенные в области ее действия. Если вы подключите политику к ОП Servers и включите аудит, все объекты компьютеров в ОП Servers будут подвергаться аудиту доступа к ресурсам согласно элементам аудита файлов и папок, заданным на этих системах.

Анализ журнала безопасности

Когда элементы аудита файлов и папок настроены и аудит доступа к объектам включен через локальную или групповую политику, система начинает регистрировать попытки доступа согласно элементам аудита. Вы можете просмотреть и изучить результаты аудита в журнале безопасности с помощью оснастки *Просмотр событий* (Event Viewer), показанной на рис. 6-14.

Как видите, размер журнала безопасности зависит от типа событий, подлежащих аудиту. Можно отсортировать собранные данные, чтобы быстрее найти события доступа к объекту. Для этого щелкните заголовок столбца **Категория (Category)** и выберите **Доступ к объектам (Object Access).**

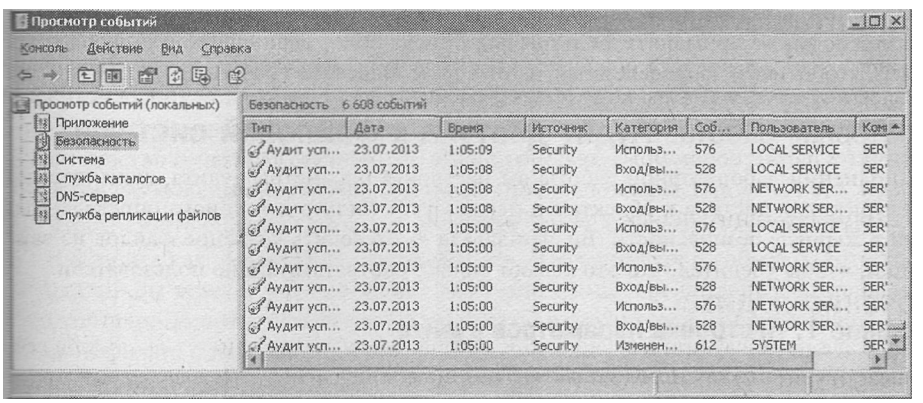


Рис. 6-14. Журнал безопасности в оснастке *Просмотр событий*

Впрочем, сортировка малоэффективна, когда вам нужно детально разобраться в зарегистрированных событиях. Лучше отфильтровать журнал событий. Для этого в меню **Вид (View)** выберите **Фильтр (Filter)** или щелкните узел журнала безопасности и в контекстном меню или в меню **Action (Действие)** выберите **Свойства (Properties),** после чего перейдите на вкладку **Фильтр (Filter).** Эта вкладка позволяет указать условия поиска, включая тип события, категорию, источник, временной диапазон, пользователя и компьютер. Пример фильтрации доступа к объектам по дате показан на рис. 6-15.

Наконец, можно экспортировать журнал безопасности. Для этого в контекстном **меню** журнала нужно выбрать **Сохранить файл журнала как (Save Log File As).** Файлы собственных журналов Windows имеют разрешение .evt. Этот файл можно открыть на другом компьютере с помощью оснастки *Просмотр событий* (Event Viewer). Либо можно сохранить журнал в текстовом файле формате с разделителями — запятыми или симво-

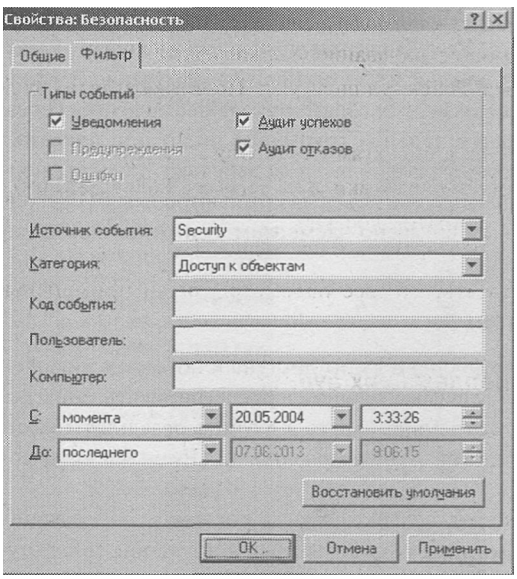


Рис. 6-15. Вкладка *Фильтр*

лами табуляции, который читает большинство средств анализа, включая Microsoft Excel. В Excel можно также применять фильтры для поиска более специфичной информации, например, чтобы найти определенный текст в поле **Описание (Description)** для события.

Лабораторная работа. **Аудит доступа к файловой системе**

При выполнении лабораторной работы вы настроите параметры аудита, включите политики аудита для доступа к объектам и используете фильтр для поиска определенных событий в журнале безопасности. Бизнес-задача — отследить удаление файлов из важной папки, чтобы убедится, что это делают только соответствующие пользователи.

Упражнение 1. Настройка параметров аудита

1. Войдите в систему как *Администратор* (Administrator).
2. Откройте окно **Дополнительные параметры безопасности (Advanced Security Settings)** для папки C:\Docs\Project 101.
3. Перейдите на вкладку **Аудит (Auditing).**
4. Добавьте элемент аудита, позволяющий отслеживать действия группы Project 101 Team. Укажите, что нужно отслеживать успешные и неудачные попытки применения разрешения *Удаление* (Delete).

Упражнение 2. Включение политики аудита

Поскольку вы вошли на контроллер домена, для включения аудита нужно использовать консоль *Политика безопасности контроллера домена* (Domain Controller Security Policy). На изолированном сервере следовало бы использовать консоль *Локальная политика безопасности* (Local Security Policy). Для включения аудита вы также могли бы задействовать ОГП.

1. Откройте консоль *Политика безопасности контроллера домена* (Domain Controller Security Policy) из группы программ **Администрирование (Administrative Tools).**
2. Раскройте узел **Локальные политики (Local Policies)** и щелкните **Политика аудита (Audit Policy).**
3. Дважды щелкните политику **Аудит доступа к объектам (Audit Qbject Access).**
4. Щелкните **Определить следующие параметры политики (Define These Policy Settings).**
5. Включите аудит успешных и неудачных попыток доступа.
6. Щелкните **OK** и закройте консоль.
7. Чтобы обновить политику и гарантировать, что все параметры были применены, в командной строке исполните gpupdate.

Упражнение 3. Генерация событий, подлежащих аудиту

1. Войдите в систему как Danielle Tiedt.
2. Подключитесь к папке \\Server01\Docs\Project 101.
3. Удалите текстовый файл Report.

Упражнение 4. Анализ журнала безопасности

1. Войдите в систему *как Администратор* (Administrator).
2. Откройте консоль *Просмотр событий* (Event Viewer) из группы **Администрирование (Administrative Tools).**
3. Щелкните узел **Безопасность (Security log).**
4. Какие типы событий вы видите в журнале безопасности? Только события доступа к объекту? Другие типы событий? Помните, что политики позволяют отслеживать множество действий, связанных с безопасностью, в том числе доступ к службе каталогов, управление учетными записями, вход в систему и т. п.
5. Чтобы сузить область поиска, в меню **Вид (View)** выберите **Фильтр (Filter).**
6. Настройте как можно более узкий фильтр. Что вы знаете о событии, которое хотите найти? Вы знаете, что оно может быть успешным или неудачным, принадлежит к категории *Доступ к объектам* (Object Access) и что оно произошло сегодня. Сравните свой фильтр с примером на рис. 6-15.
7. Щелкните **Применить (Apply).**
8. Можно ли как-нибудь упростить поиск события, которое свидетельствует об удалении файла Report пользователем Danielle Tiedt? Откройте событие и просмотрите его содержимое. Описание содержит имя пользователя, имя файла и действие. Консоль *Просмотр событий* (Event Viewer) не позволяет задать фильтр по содержанию описания, но это можно сделать, экспортировав файл в другое средство анализа журналов или в Microsoft Excel.
9. (Необязательная операция.) Если у вас есть Microsoft Excel, щелкните узел журнала безопасности правой кнопкой и выберите **Сохранить файл журнала как (Save Log File As).** Введите имя файла и выберите для него тип с разделителем — запятой. Откройте полученный файл в Excel.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Что из следующего нужно сделать, чтобы сгенерировать журнал событий доступа к файлу или папке? Выберите все подходящие варианты.
   a. Настроить разрешения NTFS, позволяющие учетной записи System вести аудит доступа к ресурсу.
   b. Настроить элементы аудита, указав виды доступа, которые нужно отслеживать.
   c. Включить политику *Аудит использования привилегий* (Audit Privilege Use).
   d. Включить политику *Аудит доступа к объектам* (Audit Object Access).
2. Что из следующего является допустимым условием фильтра для поиска событий доступа к файлу или папке в журнале безопасности? Выберите все подходящие варианты.
   a. Дата события.
   b. Имя пользователя — инициатора события.
   c. Тип доступа к объекту, повлекшего событие.
   d. Успех или неудача предпринятого действия.
3. Пользователи из Contoso, Ltd. работают с приложениями Microsoft Office, обращаясь к ресурсам на ServerOl. Ваша задача — отследить операции на ServerOl и убедиться, что разрешения не слишком жесткие и пользователи работают беспрепятственно. Какой журнал и какие типы событий содержат нужную вам информацию?
   a. *Приложение* (Application log), успешные события.
   b. *Приложение* (Application log), неудачные события.
   c. *Безопасность* (Security log), успешные события.
   d. *Безопасность* (Security log), неудачные события.
   e. *Система* (System log), успешные события.
   f. *Система* (System log), неудачные события.

Резюме

- Элементы аудита содержатся в дескрипторе безопасности файлов и папок на томах NTFS. Они настраиваются с помощью *Проводника Windows:* откройте окно свойств файла или папки и перейдите в диалоговое окно **Дополнительные параметры безопасности (Advanced Security Settings).**
- Элементы аудита сами по себе не приводят к заполнению журналов аудита. Для формирования журналов также необходимо включить политику *Аудит доступа к объектам* (Audit Object Access) в политиках *Локальная политика безопасности* (Local Security Policy) или *Политика безопасности контроллера домена* (Domain Controller Security Policy), либо сделать это на уровне ОГП.
- Журнал безопасности можно просмотреть с помощью оснастки *Просмотр событий* (Event Viewer), которая позволяет найти и изучить события доступа к объекту.

Занятие 4. **Администрирование служб IIS**

На первом занятии обсуждались вопросы, связанные с общими папками, которые позволяют пользователям службы *Клиент для сетей Microsoft* (Client for Microsoft Networks) получать доступ к ресурсам на сервере, где запущена служба *Служба доступа к файлам и принтерам сетей Microsoft* (File And Printer Sharing For Microsoft Networks). Впрочем, общие папки — не единственное средство для доступа пользователей к файлам и пап-

кам. Доступ можно также организовать с помощью таких интернет-технологий, как службы FTP и Web (HTTP).

На этом занятии вы научитесь настраивать и управлять службами IIS. Вы узнаете, как настроить Web- и FTP-узлы, виртуальные каталоги и безопасность IIS.

Изучив материал этого занятия, вы сможете:

- ✓ установить IIS;
- ✓ настроить Web- и FTP-узел;
- ✓ настроить Web-страницу по умолчанию;
- ✓ создать виртуальный Web-каталог;
- ✓ изменить параметры проверки подлинности и безопасности IIS.

Продолжительность **занятия — около 20 минут.**

Установка IIS 6.0

Для снижения риска атаки на системы Windows Server 2003 служба IIS по умолчанию не устанавливается. Ее нужно добавить с помощью мастера *Установка компонентов Windows* (Add/Remove Windows Components) из приложения *Установка и удаление программ* (Add Or Remove Programs) в *Панели управления*. Щелкните **Сервер приложений (Application Server),** затем **Состав (Details)** и установите флажок напротив **Службы IIS [Internet Information Services (IIS)].** Мастер позволяет управлять установкой отдельных компонентов IIS, но пока вы не познакомитесь с ролью каждого из них, лучше не удаляйте стандартные компоненты. Впрочем, можете добавить такие компоненты, как ASP.NET, служба FTP или *Серверные расширения FrontPage* (FrontPage Server Extensions).

Администрирование Web-среды

При установке IIS создается стандартный Web-узел, позволяющий легко и быстро реализовать Web-среду, которую затем можно изменить. Windows Server 2003 содержит средства управления службой IIS и ее узлами.

После завершения установки откройте консоль *Диспетчер служб IIS* [Internet Information Services (IIS) Manager] из группы программ **Администрирование (Administrative Tools).** По умолчанию службы IIS настроены на работу только со статическим содержимым. Чтобы активировать динамическое содержимое, выберите узел **Расширения веб-службы (Web Service Extensions).** Изначально все расширения отключены (рис. 6-16). Выберите нужное расширение и щелкните кнопку **Разрешить (Allow).**

Ниже перечислены основные процессы, которые происходят при обращении клиента к ресурсу IIS.

- Клиент вводит URL в одной из следующих форм:
  http://dns.имя.домена/виртуальный_каталог/страница.htm
  или
  ftp://dns.имя.домена/виртуальный_каталог
- Служба DNS (Domain Name Service) преобразует введенное имя в IP-адрес и возвращает его клиенту.
- Клиент подключается к серверу, используя полученный адрес и характерный для службы порт (обычно с номером 80 для HTTP и с номером 21 для FTP).

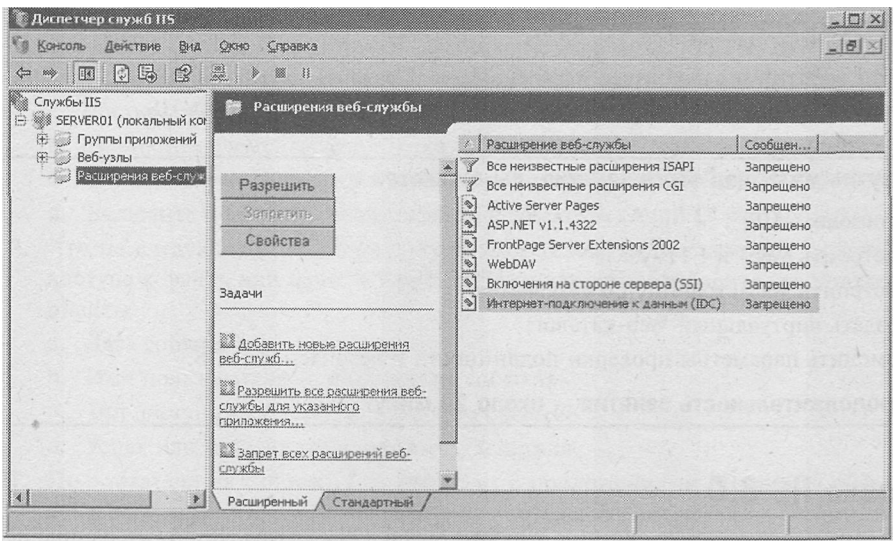


Рис. 6-16. Консоль *Диспетчер служб IIS*

- URL содержит не физический путь к ресурсу на сервере, а его виртуализацию. Сервер преобразует входящий запрос в физический путь и передает соответствующие ресурсы клиенту. Например, сервер может передать список файлов в искомой папке FTP-клиенту или домашнюю страницу HTTP-клиенту.
- Этот процесс можно защитить с помощью механизмов проверки подлинности (заставив пользователей предоставлять имя и пароль) и авторизации (управляя доступом посредством разрешений).

Чтобы увидеть, как работает этот процесс, откройте браузер и введите http://server01. Сервер передаст браузеру страницу **В процессе разработки (Under Construction).**

Настройка и управление Web- и FTP-узлами

При установке IIS настраивается единственный Web-узел — **Веб-узел по умолчанию (Default Web Site).** Хотя IIS в зависимости от аппаратной конфигурации сервера может хранить тысячи или десятки тысяч узлов, даже стандартный *Веб-узел по умолчанию* позволяет изучить функции и способы администрирования Web-узлов средствами IIS. Чтобы обратиться к этому Web-узлу, откройте обозреватель и введите http://server01.contoso.com. Будет отображена страница **В процессе разработки (Under Construction).**

Помните, что запрос браузера к Web-серверу направляется по IP-адресу сервера, который зарегистрирован в DNS для указанного URL. URL включается в запрос и часто содержит только имя узла (например www.microsoft.com). Каким образом сервер получает домашнюю страницу? Изучив вкладку **Веб-узел (Web Site)** в окне свойств Web-узла по умолчанию (см. рис. 6-17), вы увидите, что для данного узла в списке выбора IP-адреса указано **Значения не присвоены (AD Unassigned)** и задан порт 80. Так что запрос достигает порта 80 на сервере, который определяет, что запрос обращен к узлу **Веб-узел по умолчанию (Default Web Site).**

Тогда возникает следующий вопрос: какую информацию нужно вернуть? Если URL содержит только имя узла (например www.microsoft.com или server01.contoso.com), то нужная страница извлекается из домашнего каталога. Вкладка **Домашний каталог (Home Directory),** показанная на рис. 6-18, указывает физический путь к домашнему каталогу (обычно C:\inetpub\wwwroot).

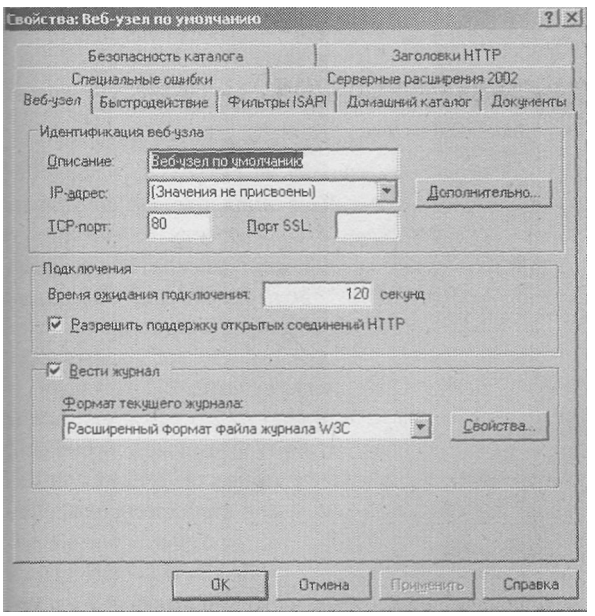


Рис. 6-17. Вкладка *Веб-узел* диалогового окна свойств Web-узла по умолчанию

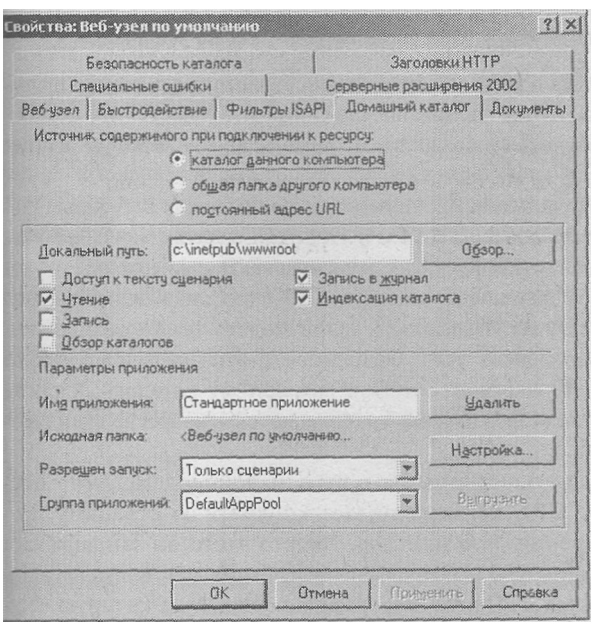


Рис. 6-18. Вкладка *Домашний каталог* диалогового окна свойств Web-узла по умолчанию

Какой именно файл следует вернуть клиенту? Это определяется на вкладке **Документы (Documents),** показанной на рис. 6-19. Служба IIS ищет файлы в указанном порядке. Как только файл с указанным именем по локальном пути к домашнему каталогу найден, запрошенная страница возвращается клиенту и сервер прекращает поиск осталь-

ных соответствий. Если страницу не удается найти, IIS возвращает клиенту ошибку 404 — **Файл не найден (File Not Found).**

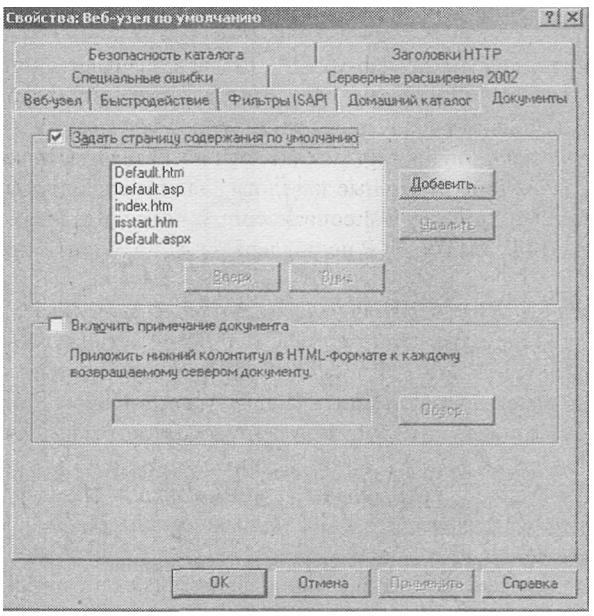


Рис. 6-19. Вкладка *Документы* диалогового окна свойств Web-узла по умолчанию

Браузер мог бы, конечно, сослаться в URL на конкретную страницу, например http://server01.contoso.com/contactinfo.htm. Тогда указанная страница извлекается из домашнего каталога. Если она не найдена, сервер возвращает ошибку 404 — **Файл не найден (File Not Found).**

Чтобы создать Web-узел, откройте консоль IIS Manager, щелкните узел **Веб-узлы (Web Sites)** или существующий Web-узел правой кнопкой и выберите **Создать ^ем^XВеб-узел (Web Site).** Чтобы настроить Web-узел, откройте окно его свойств. Вы можете настроить IP-адрес данного узла. Если серверу назначено несколько IP-адресов, каждцй из них может представлять отдельный Web-узел. Несколько узлов можно также разместить, используя несколько портов или заголовков узла. Особенности этих методов здесь не обсуждаются. Кроме того, вы можете настроить путь к домашнему каталогу, а также изменить список или порядок документов, которые возвращаются в качестве стандартной страницы.

URL может содержать более сложную информацию о пути, например http://www.microsoft.com/windowsserver2003. Этот URL не запрашивает конкретную страницу, поскольку в конце адреса нет расширения .htm или .asp. Вместо этого он запрашивает информацию из каталога windowsserver2003. Сервер воспринимает эту дополнительную часть URL как виртуальный каталог. Папка, содержащая файлы, на которую ссылаются по имени windowsserver2003, может находиться где угодно, в том числе и на другом сервере.

Чтобы создать виртуальный каталог, щелкните Web-узел правой кнопкой и выберите **Создать (New)\Виртуальный каталог (Virtual Directory).** Мастер предложит ввести псевдоним, который можно будет указывать как папку в URL, и физический путь к соответствующему ресурсу на локальном томе или на удаленном сервере.

Подготовка к экзамену Виртуальный Web-каталог на диске NTFS можно создать в окне свойств папки, настроив соответствующие параметры на вкладке **Доступ через веб (Web Sharing).**

FTP-узлы работают и управляются аналогично Web-узлам. IIS устанавливает один FTP-узел — **FTP-узел по умолчанию (Default FTP Site)** — и настраивает его, чтобы тот отвечал на все входящие FTP-запросы, поступающие на порт 21. FTP-узел возвращает клиенту список файлов в папке, указанной на вкладке **Домашний каталог (Home Directory).** FTP-узлы также могут содержать виртуальные каталоги, например запросы по адресам ftp://server01.contoso.com/pub и ftp://server01.contoso.com/vendor-uploads могут возвращать ресурсы с разных серверов. Служба FTP не поддерживает документы по умолчанию.

Мощные IIS-серверы могут содержать десятки тысяч узлов, каждый со своими особыми параметрами. Потеря всей этой конфигурационной информации может быть болезненной: обычное архивирование файловой системы при сбое позволит восстановить файлы данных, но конфигурация будет утеряна. Для защиты конфигурации IIS необходимо заархивировать или восстановить метабазу — XML-документ, в котором хранятся параметры конфигурации. Щелкните узел сервера в IIS Manager правой кнопкой и выберите **Все задачи (All Tasks)\Архивирование и восстановление конфигурации (Backup/Restore Configuration).**

Примечание Подробнее об IIS — в книге Microsoft IIS 6.0 Administrator's Pocket Consultant (Microsoft Press, 2003)[1].

Защита файлов в IIS

Защиту файлов, к которым обращаются через IIS, можно разделить на несколько категорий: проверка подлинности, авторизация через NTFS-разрешения и IIS-разрешения. Проверка подлинности — это процесс анализа реквизитов, предоставленных в форме имени пользователя и пароля. По умолчанию все запросы к IIS выполняются от имени пользователя с учетной записью IUSR_имя_компьютера. Прежде чем ограничивать доступ пользователей к ресурсам, необходимо создать локальные или доменные учетные записи и настроить проверку более высокого уровня, чем стандартная анонимная проверка подлинности.

Настройка методов проверки подлинности

Методы проверки подлинности, которые можно настроить на вкладке **Безопасность каталога (Directory Security)** в окне свойств сервера, Web- или FTP-узла, виртуального каталога или файла, описаны в следующих разделах.

Варианты проверки подлинности средствами Web

- **Анонимная проверка подлинности.** Пользователи могут получить доступ к открытой области Web-узла, не указывая имя пользователя и пароль.
- **Обычная проверка подлинности.** Требует, чтобы у пользователя была локальная или доменная учетная запись. Реквизиты передаются открытым текстом.

[1] Уильям Р. Станек. Microsoft Internet Information Service 6.0. Справочник администратора. — М: Русская Редакция, 2003 г.

- **Краткая проверка подлинности.** Аналог обычной проверки с дополнительной защитой передаваемых по сети реквизитов пользователя. Краткая проверка подлинности полагается на протокол HTTP 1.1.
- **Расширенная краткая проверка подлинности.** Работает, только когда учетная запись пользователя хранится в Active Directory. Подразумевает получение и хранение реквизитов пользователей на контроллере домена. Расширенная краткая проверка требует, чтобы пользователь работал с Internet Explorer версии 5 или выше по протоколу HTTP 1.1.
- **Встроенная проверка подлинности Windows.** Получает информацию посредством безопасной формы проверки подлинности (иногда называемой проверкой Windows NT типа «запрос-ответ»), при которой имя пользователя и пароль хэшируются перед передачей по сети.
- **Проверка подлинности по сертификату.** Добавляет защиту SSL (Secure Sockets Layer), благодаря использованию сертификатов сервера, клиента или обеих сторон. Этот вариант доступен, только когда на компьютере установлены и настроены *Службы сертификации* (Certificate Services).
- **Проверка подлинности в системе .NET Passport.** Предоставляет единую службу входа через SSL, перенаправление HTTP, файлы cookies, Microsoft JScript и стойкое шифрование симметричным ключом.

Варианты проверки подлинности средствами FTP

- **Анонимная проверка подлинности.** Пользователи могут получить доступ к открытой области FTP-узла, не указывая имя пользователя и пароль.
- **Обычная проверка подлинности.** Требует, чтобы пользователь ввел имя и пароль, которые соответствуют действительной учетной записи Windows.

Настройка доступа к ресурсам с помощью разрешений

Когда проверка подлинности настроена, назначают разрешения доступа к файлам и папкам. Разрешения NTFS — наиболее распространенный способ управления доступом к ресурсам через IIS. Поскольку разрешения NTFS назначают файлу или папке, они действуют независимо от способа доступа к ресурсу.

IIS также назначает разрешения узлам и виртуальным каталогам. В отличие от разрешений NTFS, которые определяют некий уровень доступа для существующих учетных записей пользователей или групп Windows, разрешения безопасности каталога, назначенные узлу или виртуальному каталогу, распространяются на всех пользователей и групп.

В табл. 6-2 подробно описаны уровни Web-разрешений.

Табл. 6-2. Разрешения каталогов IIS

Разрешение	Описание
Чтение (Read), используется по умолчанию	Пользователи могут просматривать содержимое и свойства файлов
Запись (Write)	Пользователи могут изменять содержимое и свойства файлов

Табл. 6-2. *(окончание)*

Разрешение	Описание
Доступ к тексту сценария (Script Source Access)	Пользователи могут получить доступ к исходному коду файлов, например сценариев в приложении ASP (Active Server Pages). Этот вариант доступен только при наличии разрешений *Чтение* (Read) или *Запись* (Write). Пользователи получают доступ к исходному коду файлов. Если назначено разрешение *Чтение* (Read), исходный код можно читать. Если назначено разрешение *Запись* (Write), исходный код можно изменять. Учтите: предоставление пользователям разрешений на чтение и запись исходного кода может нарушить безопасность сервера
Обзор каталогов (Directory browsing)	Пользователи могут просматривать списки и коллекции файлов

Разрешения *Выполнение* (Execute) регулируют уровень безопасности выполнения сценариев (табл. 6-3).

Табл. **6-3. Разрешения на выполнение приложений**

Разрешение	Описание
Нет (None)	Запрещает запуск любых приложений или сценариев
Только сценарии (Scripts only)	Позволяет приложению, связанному с ядром сценариев, выполняться в этом каталоге без наличия разрешений, назначенных исполняемым программам. Разрешения *Только сценарии* более безопасны по сравнению с *Сценарии и исполняемые файлы* (Scripts and Executables), поскольку позволяют ограничить приложения, которые можно запускать в каталоге
Сценарии и исполняемые файлы (Scripts and Executables)	Позволяет любому приложению выполняться в этом каталоге, включая приложения, связанные с ядром сценариев, и двоичные программы Windows (файлы .dll и .exe).

Подготовка к экзамену При одновременном использовании разрешений IIS и NTFS, действуют наиболее жесткие из них.

Лабораторная работа. **Администрирование IIS**

На этой лабораторной работе вы установите службу IIS и настроите новый Web-узел и виртуальный каталог.

Упражнение 1. Установка IIS

1. Откройте приложение *Добавление и удаление программ* (Add Or Remove Programs) в *Панели управления* и щелкните **Установка компонентов Windows (Add/Remove Windows Components).**
2. Щелкните **Сервер приложений (Application Server),** а затем **Состав (Details).**
3. Отметьте **Службы IIS [Internet Information Services (IIS)]** и щелкните **Состав (Details).**

4. Убедитесь, что (как минимум) установлены флажки **Общие файлы (Common Files), Служба FTP [File Transfer Protocol (FTP) Service], Служба WWW (World Wide Web Service)** и **Диспетчер служб IIS (Internet Information Services Manager).**
5. Завершите установку.

Упражнение 2. Подготовка образца содержимого Web-узла

1. Создайте папку ContosoCorp на диске C:.
2. Откройте *Блокнот* (Notepad) и создайте файл с текстом «Welcome to Contoso». Сохраните этот файл под именем «C:\ContosoCorp\Default.htm», не забыв заключить имя файла в кавычки.
3. Создайте второй файл с текстом «This is the site for Project 101». Сохраните этот файл под именем «C:\Docs\Project 101\Default.htm», не забыв заключить имя файла в кавычки.

Упражнение 3. Создание Web-узла

1. Откройте консоль *Диспетчер служб IIS* [Internet Information Services (IIS) Manager] из группы программ **Администрирование (Administrative Tools).**
2. Щелкните узел **Веб-узел по умолчанию (Default Web Site)** правой кнопкой и **выберите Остановить (Stop).**
3. Щелкните узел **Веб-узлы (Web Sites)** правой кнопкой и выберите **Создать (New)\Веб-узел (Web Site).**
4. Присвойте узлу имя Contoso и укажите путь C:\ContosoCorp. Остальные стандартные параметры можно не менять.

Упражнение 4. Создание защищенного виртуального каталога

1. Щелкните узел **Contoso** правой кнопкой и выберите **Создать (New)\Виртуальный каталог (Virtual Directory).**
2. Введите псевдоним Project 101 и путь C:\Docs\Project 101.
3. Откройте окно свойств виртуального каталога Project101.
4. Перейдите на вкладку **Безопасность каталога (Directory Security).**
5. На панели **Управление доступом и проверка подлинности (Authentication and Access Control)** щелкните **Изменить (Edit).**
6. Снимите одноименный флажок, чтобы запретить анонимный доступ. Теперь для доступа к файлам узла необходима допустимая учетная запись. Два раза щелкните **OK**.
7. Откройте Internet Explorer и введите адрес http://server01.contoso.com. Должна открыться страница **Вас приветствует Contoso (Welcome To Contoso).**
8. Введите http://server01.contoso.com/Project101. Вам предложат ввести реквизиты. Войдите в систему под учетной записью Scott Bishop, откроется домашняя страница Project101.
9. Измените разрешения на доступ к документу C:\Docs\Project 101\Default.htm, чтобы только администратор мог его прочитать.
10. Закройте и повторно запустите Internet Explorer. Подключитесь к каталогу http://server01.contoso.com/Project101 с реквизитами администратора. Должна открыться домашняя страница.

11. Закройте и повторно запустите Internet Explorer. Теперь подключитесь к тому же URL под именем Scott Bishop. Должно появится сообщение об ошибке из-за отказа в доступе с кодом 401.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Вы настраиваете Web-узел средствами IIS на ServerOl. Этому узлу соответствует доменное имя adatum.com и домашний каталог C:\Web\Adatum. Какой адрес URL должны вводить интернет-пользователи, чтобы получить доступ к файлам домашнего каталога на данном узле?
   a. http://server01.web.adatum.
   b. http://web.adatum.com/server01.
   c. http://server01 .adatum/home.
   d. http://server01.adatum.com.
2. Данные для интрасети вашей организации в настоящее время хранятся на диске D: сервера IIS. Решено, что отдел кадров будет сопровождать информацию о преимуществах и правилах компании со своего сервера. Сведения отдела кадров должны быть доступны по адресу http://intranet.contoso.com/hr. Что нужно настроить?
   a. Новый Web-узел.
   b. Новый FTP-узел.
   c. Виртуальный каталог из файла.
   d. Виртуальный каталог.
3. Вы хотите обеспечить самый высокий уровень безопасности интрасети вашей организации, не развертывая инфраструктуру служб сертификации. Цель — обеспечить прозрачную для пользователей проверку подлинности и защитить ресурсы интрасети с помощью группы учетных записей, существующих в Active Directory. Все пользователи защищены от внешней сети корпоративным брандмауэром. Какой из методов проверки подлинности вы выберете?
   a. *Анонимный доступ* (Anonymous Access).
   b. *Обычная проверка подлинности* (Basic Authentication),
   c- *Краткая проверка подлинности* (Digest Authentication).
   d. *Встроенная проверка подлинности Windows* (Integrated Windows Authentication).

Резюме

- Служба IIS не устанавливается по умолчанию. Ее можно установить с помощью *Мастера компонентов Windows* (Windows Components) в приложении *Установка и удаление программ* (Add Or Remove Programs).
- Домашний каталог Web- или FTP-узла указывает физическое расположение ресурсов, которые обслуживаются данным узлом.
- Виртуальный каталог — это псевдоним и путь, указывающий серверу IIS на расположение ресурсов. URL имеет формат http://dns.имя.сервера/виртуальный_каталог. Ресурсы могут находится на локальном томе или на удаленном сервере.
- IIS поддерживает несколько уровней проверки подлинности. Анонимная проверка (применяется по умолчанию) позволяет любым подключившимся пользователям

получить доступ к открытым областям узла, а встроенная проверка подлинности Windows позволяет назначить NTFS-разрешения ресурсам, которые нужно дополнительно защитить,

- Доступ к ресурсам IIS на томах NTFS контролируется таблицами ACL, так же, как и при обращении через службу *Клиент для сетей Microsoft* (Client for Microsoft Networks).
- IIS поддерживает разрешения доступа к каталогу и приложениям. При одновременном использовании разрешений IIS и NTFS действуют наиболее жесткие из них.

Пример из практики

Компания Contoso, Ltd. хочет настроить узел интрасети для размещения новостей о компании и отделах. Необходимо обеспечить максимально удобный доступ к этому узлу сотрудникам и руководителям, которые будут отвечать за обновление документов. Все сотрудники будут использовать последнюю версию Internet Explorer для просмотра документов в интрасети. Для создания Web-страниц руководители будут использовать другие средства.

Примечание Этот пример является дополнением и подготовкой к следующему разделу — «Практикуму по устранению неполадок». Рекомендуется выполнить оба упражнения, чтобы получить больше опыта работы с системой защиты файлов Windows Server 2003.

Для выполнения упражнений необходимо установить IIS (см. занятие 4, упражнение 1) и создать учетные записи пользователей и групп, как описано в разделе «Прежде всего» этой главы.

Упражнение 1. Создание общей папки и образца содержимого Web-узла

Есть много способов создания общих папок. В данной ситуации используйте методы, описанные ниже.

1. Из командной строки исполните следующие команды:

```
md c:\ContosoIntranetNews
net share News=c:\ContosoIntranetNews
```

2. Откройте *Блокнот* (Notepad) и создайте файл с текстом «Contoso Company News». Сохраните его под именем «C:\ContosoIntranetNews\Default.htm», не забыв заключить имя файла в кавычки.
3. Назначьте папке C:\ContosoIntranetNews разрешение Managers: *Изменение* (Modify) — *Разрешить* (Allow).
4. В окне свойств папки C:\ContosoIntranetNews перейдите на вкладку **Доступ через веб (Web Sharing).**
5. **В** раскрывающемся списке **Общая папка на (Share On)** выберите Contoso. Если вы не пропустили упражнения занятия 4, то не увидите Web-узел Contoso; вместо этого выберите **Веб-узел по умолчанию (Default Web Site).** Щелкните Открыть общий доступ **к** этой **папке (Share This Folder)** и введите псевдоним News. Не меняйте стандартные разрешения. Щелкните OK.

Упражнение 2. Оптимизация доступа внутри сети

В этом упражнении вы проверите правильность работы узла интрасети и сделаете доступ к нему максимально удобным.

1. Откройте Internet Explorer и введите http://server01.contoso.com/News.
2. Вам предложат ввести реквизиты' Войдите под учетной записью *Администратор* (Administrator). Должна открыться страница **Contoso Company News.**
3. Закройте Internet Explorer.

   Вам пришлось ввести реквизиты, поскольку узел Company News не допускает анонимный доступ. При создании виртуального каталога на вкладке **Доступ через веб (Web Sharing)** анонимный доступ запрещен по умолчанию.
4. С помощью IIS Manager откройте окно свойств виртуального каталога News.
5. Перейдите на вкладку **Безопасность каталога (Directory Security)** и в панели **Управление доступом и проверка подлинности (Authentication and Access Control)** щелкните **Изменить (Edit).**
6. Разрешите анонимный доступ.
7. Повторите шаги 1—3, чтобы убедится, что изменения вступили в силу.

Упражнение 3. Проверка возможности изменения содержимого интрасети руководителями

Чтобы имитировать удаленное управление содержимым интрасети, важно правильно указать UNC-путь к папкам и файлам. Не указывайте локальный путь.

1. Выйдите из системы ServerOl и повторно войдите под именем Lorrin Smith-Bates из группы Managers.
2. Откройте *Блокнот* (Notepad) и создайте файл с текстом « Good News Contoso!». Сохраните этот файл под именем: «\\server01\news\goodnews.htm», не забыв заключить имя файла в кавычки и указав UNC-путь, а не локальный путь к папке новостей.
3. Можете ли вы сохранить этот файл?

   Если вы точно следовали инструкциям этого сценария, то вам не удастся это сделать. Перейдите к следующему разделу, чтобы выявить и устранить проблему, с которой только что столкнулись.

Практикум по устранению неполадок

Lorrin Smith-Bates сообщает в службу технической поддержки, что не может сохранить документы в папке новостей на узле интрасети. Ошибка происходит, когда пользователь пытается сохранить созданную в *Блокноте* Web-страницу под именем «\\server01\News\goodnews.htm».

Папка C:\ContosoIntranetNews, к которой открыт общий доступ под именем News, настроена как виртуальный каталог News для Web-узла Contoso. При сохранении файла возникает ошибка **Отказано в доступе (Access Denied).** Значит, несмотря на возможность подключения к серверу с компьютера пользователя, какое-то разрешение или привилегия мешает ему сохранить файл.

Войдите на сервер ServerOl как *Администратор* (Administrator) и сделайте следующее.

Примечание Это упражнение дополняет предыдущий разбор сценария. Рекомендуется выполнить оба упражнения, чтобы получить больше практического опыта работы с системой защиты файлов Windows Server 2003.

Для выполнения упражнений необходимо установить IIS (см. занятие 4, упражнение 1) и создать учетные записи пользователей и групп, как описано в разделе «Прежде всего» этой главы. Кроме того, следует выполнить упражнение 1 из раздела «Пример из практики».

Шаг 1. Проверка членства в группах

Вы совершенно уверены, что Lorrin — член группы Managers, и что этой группе назначено разрешение *Изменение* (Modify) для папки C:\ContosoIntranetNews. Как проверить, является ли Lorrin членом группы Managers?

Команда Dsget отображает список членов указанной группы (см. главу 3). Из командной строки исполните следующую команду:

```
dsget user "CN=Lorrin Smith-Bates,OU=Employees,OC=Contoso,DC=com"
-memberof -expand
```

Вы должны увидеть следующий список групп (он может отличаться в зависимости от того, какие упражнения из этой книги вы уже выполнили).

```
"CN=Managers,OU=Security Groups,DC=contoso;DC=com"

"CN=Project 101 Team,OU=Security Groups,DC=contoso,DC=com"

"CN=Domain Users,CN=Users,DC=contoso,DC=com"

"CN=Print Operators,CN=Builtin,DC=contoso,DC=com"

"CN=Users,CN=Builtin,DC=contoso,DC=com"
```

Как еще проверить, является ли Lorrin членом группы Managers? Откройте консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) и изучите вкладку **Член групп (Member Of)** в окне свойств пользователя Lorrin Smith-Bates.

Шаг 2. Анализ действующих разрешений

Изучите разрешения, назначенные папке C:\ContosoIntranetNews. На вкладке **Безопасность (Security)** окна свойств этой папки и в окне **Дополнительные параметры безопасности (Advanced Security Settings),** вы должны увидеть, что группе Managers дано разрешение *Изменение* (Modify).

Перейдите на вкладку **Действующие разрешения (Effective Permissions)** в окне **Дополнительные параметры безопасности (Advanced Security Settings)** и щелкните учетную запись Lorrin Smith-Bates. Проанализируйте действующие разрешения. Эти разрешения должны предполагать возможность создавать файлы и записывать данные в папке.

Шаг 3. Оценка ситуации

Если действующие разрешения Lorrin Smith-Bates позволяют создавать файлы и записывать данные, почему возникает ошибка **Отказано** в доступе (Access **Denied)?** Если вы до сих пор не догадались, перечитайте резюме занятий 1 и 4.

Источником проблемы могут быть другие разрешения, назначенные папке C:\ContosoIntranetNews. Разрешения доступа общего ресурса, разрешения Web-узла или вирту-

ального каталога определяют максимальный допустимый уровень доступа, поэтому, если одно из них настроено слишком жестко, это может помешать пользователю Lorrin Smith-Bates полностью применять NTFS-разрешение *Изменение* (Modify).

Сохраняя Web-страницу в Notepad, Lorrin Smith-Bates подключался к серверу удаленно. В следующем списке найдите клиентскую программу и службу, которые использовались для подключения:

- *Служба FTP-публикации* (FTP Publishing Service).
- *Служба веб-публикации* (Worldwide Web Publishing Service).
- *Служба Telnet* (Telnet Service).
- *Служба доступа к файлам и принтерам сетей Microsoft* (File and Printer Sharing For Microsoft Networks).
- *Обозреватель Интернета*.
- *Клиент FTP*.
- *Клиент Telnet*.
- *Клиент для сетей Microsoft* (Client for Microsoft Networks).

Lorrin Smith-Bates использует службу *Клиент для сетей Microsoft* для подключения к *Службе доступа к файлам и принтерам сетей Microsoft* на сервере ServerOl. Это следует из пути, который пользователь указывает при сохранении файла: «\\serverO l\News\goodnews.htm». Это UNC-путь, который создает подключение, используя сети Microsoft.

Зная это, вы можете исключить из рассмотрения любые разрешения, назначенные Web-узлу или виртуальному каталогу. Такие разрешения применяются только в отношении подключений Web-клиентов к Web-службе.

Остается единственная возможная причина проблем с разрешениями: разрешения общего ресурса. По умолчанию Windows Server 2003 дает группе *Все* (Everyone) только разрешение общего ресурса *Чтение* (Read). Поскольку разрешения общего ресурса определяют максимально допустимый доступ, они перекрывают NTFS-разрешение *Изменить* (Modify), назначенное папке.

Шаг 4. Решение проблемы

Предоставьте группе *Все* (Everyone) полный доступ к общей папке C:\ContosoIntranetNews.

Теперь для узла новостей в интрасети осталось реализовать бизнес-требование и разрешить пользователям лишь читать документы. Стандартные разрешения NTFS позволяют пользователям создавать файлы и папки и затем, в качестве владельцев, делать с ними что угодно.

Заблокируйте разрешения NTFS для папки, чтобы пользователям было дано разрешение *Чтение и выполнение* (Read & Execute) без особых разрешений *Создание файлов/Запись данных* (Create Files/Write Data) и *Создание папок/Дозапись данных* (Create Folders/Append Data).

Проверьте внесенные изменения, войдя в систему под именем Scott Bishop, который должен видеть http://server01.contoso.com/News. Подключившись к \\serverOl\News, он не должен иметь возможность создать новый или изменить существующий файл.

Затем войдите в систему под именем Lorrin Smith-Bates, который также должен иметь возможность просматривать узел новостей в интрасети, но у него также должно быть право создавать и изменять файлы в общей папке \\server01\News. Вы должны суметь создать документ с новостями, как описано в упражнении 3 раздела «Пример из практики», и обратиться к нему по адресу http://server01.contoso.com/News/goodnews.htm.

Резюме главы

- В состав Windows Server 2003 входят новые консоли и оснастки, предназначенные для управления общими папками, политикой аудита и службой IIS. Для управления таблицами ACL в NTFS по-прежнему используется *Проводник Windows* и оснастка - *Общие папки* (Shared Folder), хотя редактор ACL является более мощным средством.
- Разрешения NTFS можно предоставлять и отменять, явно или в результате наследования. Запрет разрешения приоритетнее его позволения, а явное разрешение перекрывает унаследованное. В итоге предоставление явного разрешения может перекрыть унаследованный запрет.
- Доступ, предоставленный разрешениями NTFS, может далее ограничиваться разрешениями общего ресурса и разрешениями IIS для доступа к FTP- и Web-узлам, виртуальным каталогам и документам. Когда ресурсу назначается два типа разрешений, например разрешения общего ресурса и разрешения NTFS, необходимо оценить каждый набор разрешений и определить, какие из них строже. Этот и будет действующий набор разрешений.
- Дескриптор безопасности файла или папки хранит сведения о владельце объекта. Владелец, как и любой пользователь с разрешением *Изменение* (Change), может изменять ACL. Права владения может принимать на себя любой пользователь с разрешением *Смена владельца* (Take Ownership). Кроме того, пользователь с правом *Восстановление файлов и каталогов* (Restore Files And Directories) может передавать права владения другим пользователям.
- Дескриптор безопасности также содержит элементы аудита, которые при включении политики аудита указывают системе регистрировать попытки доступа определенного типа для заданных пользователей и групп.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Хорошо освойте средства, используемые для настройки общих папок, разрешений NTFS, аудита и службы IIS. Поработайте некоторое время с каждой оснасткой, изучив свойства, которые можно настроить, и их роль в управлении файлами и папками.
- Научитесь быстро определять действующие разрешения: взаимодействие явных, унаследованных, предоставленных и отмененных разрешений для нескольких пользователей, групп, компьютеров и типов входа в систему, например *Интерактивные* (Interactive) и *Сеть* (Network).
- Запомните три шага, необходимых для настройки аудита, и изучите стратегии аудита (регистрация успешных или неудачных попыток), которые вы могли бы использовать для решения конкретной задачи.

- Изучите конфигурацию Web-узла и виртуального каталога. Если у вас нет опыта работы с IIS, обязательно выполните лабораторную работу занятия 4, практикум по устранению неполадок и изучите пример из практики.

Основные термины

Скрытая общая папка ~ hidden shared folder — общую папку можно скрыть, добавив символ $ в конец ее имени ресурса. К такому общему ресурсу можно подключиться по UNC-имени (например \\server01\docs$), но его не будет видно в обозревателе. Windows Server 2003 создает скрытые административные общие ресурсы, например Admin$, Print$, плюс скрытый общий ресурс для корня каждого тома на диске. К скрытым административным общим ресурсам могут подключаться только администраторы.

Наследование ~ inheritance — по умолчанию разрешения, назначенные папке, распространяются на все ее подпапки и файлы. Кроме того, файлы и папки по умолчанию наследуют разрешения родительской папки или тома и содержат их в своих ACL. С помощью этих двух механизмов разрешения, назначенные папке верхнего уровня, распространяются на ее содержимое.

Действующие разрешения ~ effective permissions — разрешения можно предоставлять и отменять, явно или в результате наследования. Они назначаются одному или нескольким пользователям, группам или компьютерам. Действующими называют суммарные разрешения, которые определяют фактический уровень доступа для участника безопасности.

Право владения ~ ownership — у каждого файла и папки на томе NTFS есть свойство, указывающее участника безопасности, который владеет данным ресурсом. Владелец вправе в любое время изменять ACL данного объекта, то есть ему никогда нельзя заблокировать доступ к ресурсу. Права владения могут приниматься или передаваться на основе разрешений *Смена владельца* (Take Ownership) и права пользователя *Восстановление файлов и каталогов* (Restore Files And Directories) соответственно.

Особые учетные записи: Создатель-владелец (Creator Owner), Сеть (Network) и **Интерактивные (Interactive)** — эти участники безопасности являются динамическими и представляют отношения между пользователем и ресурсом. Когда пользователь создает файл или папку, он становится владельцем (Creator Owner) данного ресурса, и любые наследуемые разрешения родительской папки или тома, предоставленные учетной записи Creator Owner, будут явно назначены пользователю для нового объекта. Учетные записи *Сеть* (Network) и *Интерактивные* (Interactive) представляют способ подключения пользователя: подключился он к ресурсу удаленно, либо интерактивно вошел на компьютер, где хранится ресурс.

Политика Аудит доступа к объектам (Audit Object Access), доступная в консоли *Локальная политика безопасности* (Local Security Policy) изолированного компьютера с Windows Server 2003 или в ОГП, определяет, должны ли попытки доступа к файлам, папкам и принтерам регистрироваться в журнале безопасности. Когда эта политика включена, элементы аудита каждого объекта определяют типы регистрируемых действий.

Виртуальный каталог ~ virtual Directory — объект IIS, позволяющий папке на любом локальном или удаленном томе играть роль подпапки Web-узла.

Вопросы и ответы

Занятие 1. Закрепление материала

1. Какие из следующих средств служат для администрирования общих папок на удаленном сервере? Выберите все подходящие варианты.
   a. Оснастка *Общие папки* (Shared Folders).
   b. *Проводник Windows,* запущенный на локальном компьютере и подключенный к общей папке на удаленном сервере или к скрытому общему диску.
   c. *Проводник Windows,* запущенный на удаленном компьютере в сеансе служб терминалов или дистанционного подключения к рабочему столу.
   d. Консоль *Управление файловым сервером* (File Server Management).

   Правильный ответ: a, c, d. **Проводник Windows можно использовать только для администрирования локальных общих ресурсов, поэтому для управления общими ресурсами на сервере необходимо создать сеанс службы Дистанционное управление рабочим столом (Remote Desktop) с этим удаленным сервером и запустить Проводник Windows в этом сеансе. Более распространенный и лучший метод — использовать оснастку Общие папки (Shared Folders) из консоли Управление файловым сервером (File Server Management).**

2. Общая папка находится на томе FAT32. Группе Project Managers назначено разрешение *Полный доступ* (Full Control). Группе Project Engineers назначено разрешение *Чтение* (Read). Пользователь Julie входит в группу Project Engineers. Она получила повышение и стала членом группы Project Managers. Какие разрешения доступа к этой папке для нее действуют?

   Правильный ответ: Полный доступ (Full Control).

3. Общая папка со стандартными разрешениями общего ресурса находится на томе NTFS. Группе Project Managers назначено NTFS-разрешение *Полный доступ* (Full Control). Пользователь Julie из группы Project Managers жалуется, что не может создать файлы в этой папке. Почему Julie не удается создать файлы?

   Правильный ответ: по умолчанию в Windows Server 2003 группе Все (Everyone) предоставлено разрешение Чтение (Read). Разрешения общего ресурса определяют максимальные действующие разрешения для файлов и папок внутри общего ресурса. Разрешения общего ресурса ограничивают NTFS-разрешение полного доступа. Чтобы решить проблему, следует изменить разрешения **общего ресурса и предоставить группе Project Managers, минимум, разрешение Изменение (Change).**

Занятие 2. Закрепление материала

1. Какие минимальные разрешения NTFS требуются, чтобы пользователи могли открывать файлы и запускать программы из общей папки?
   a. *Полный доступ* (Full Control).
   b. *Изменение* (Modify).
   c. *Запись* (Write).
   d. *Чтение и выполнение* (Read & Execute).
   e. *Список содержимого папки* (List Folder Contents).

   Правильный **ответ: d.**

2. Пользователь Bill жалуется, что не может получить доступ к плану отдела. Вы открываете вкладку **Безопасность (Security)** в окне свойств плана и видите, что все разре-

шения доступа к документу наследуются от родительской папки плана. Для группы, куда включен Bill, разрешение *Чтение* (Read) отменено. Какое из следующих действий позволило бы пользователю Bill получить доступ к плану?

a. Изменить разрешения родительской папки, чтобы предоставить пользователю Bill разрешение *Полный доступ* (Full Control).
b. Изменить разрешения родительской папки, чтобы предоставить пользователю Bill разрешение *Чтение* (Read).
c. Изменить разрешения доступа к плану, чтобы предоставить пользователю Bill разрешение *Чтение* (Read).
d. Изменить разрешения доступа к плану: снять флажок **Разрешить наследование разрешений... (Allow Inheritable Permissions...),** щелкнуть **Копировать (Copy)** и удалить запрет.
e. Изменить разрешения доступа к плану: снять флажок **Разрешить наследование разрешений... (Allow Inheritable Permissions...),** щелкнуть **Копировать (Copy)** и явно разрешить пользователю Bill полный доступ.
f. Удалить пользователя Bill из группы, которой запрещен доступ.

Правильный ответ: c, d, f.

3. Пользователь Bill звонит снова и сообщает, что по-прежнему не может получить доступ к плану отдела. Вы открываете вкладку **Действующие разрешения (Effective Permissions),** выбираете учетную запись Bill и видите, что на самом деле ему предоставлены достаточные разрешения. Чем можно объяснить расхождение сведений на вкладке *Действующие разрешения* с реальными полномочиями?

Правильный ответ: вкладка Действующие разрешения (Effective Permissions) дает лишь приближенную картину прав доступа пользователя. Возможно, учетной записи, связанной со способом входа в систему, например Интерактивные (Interactive) или Сеть (Network), назначен элемент разрешения, запрещающий доступ. Разрешения таких групп входа не учитываются на вкладке Действующие разрешения (Effective Permissions). Кроме того, если вы вошли без полномочий администратора домена, то не сможете прочитать все записи членства в группах и получить искаженный отчет о разрешениях.

Занятие 3. Закрепление материала

1. Что из следующего нужно сделать, чтобы сгенерировать журнал событий доступа к файлу или папке? Выберите все подходящие варианты.

a. Настроить разрешения NTFS, позволяющие учетной записи System вести аудит доступа к ресурсу.
b. Настроить элементы аудита, указав виды доступа, которые нужно отслеживать.
c. Включить политику *Аудит использования привилегий* (Audit Privilege Use),
a. Включить политику *Аудит доступа к объектам* (Audit Object Access).

Правильный ответ: b, d.

2. Что из следующего является допустимым условием фильтра для поиска событий доступа к файлу или папке в журнале безопасности? Выберите все подходящие варианты.

a. Дата события.
b. Имя пользователя — инициатора события.
c. Тип доступа к объекту, повлекшего событие.
d. Успех или неудача предпринятого действия.

Правильный ответ: a, b, d.

3. Пользователи из Contoso, Ltd. работают с приложениями Microsoft Office, обращаясь к ресурсам на Server01 Ваша задача — отследить операции на Server01 и убедится, что разрешения не слишком жесткие и пользователи работают беспрепятственно. Какой журнал и какие типы событий содержат нужную вам информацию?
   a. *Приложение* (Application log), успешные события.
   b. *Приложение* (Application log), неудачные события.
   c. *Безопасность* (Security log), успешные события.
   d. *Безопасность* (Security log), неудачные события.
   e. *Система* (System log), успешные события,
   a. *Система* (System log), неудачные события.

   Правильный ответ: d.

Занятие 4. Закрепление материала

1. Вы настраиваете Web-узел средствами IIS на Server01. Этому узлу соответствует доменное имя adatum.com и домашний каталог C:\Web\Adatum. Какой адрес URL должны вводить интернет-пользователи, чтобы получить доступ к файлам домашнего каталога на данном узле?
   a.*http://server01.web.adatum.*
   b. *http://web.adatum.com/server01.*
   c.*http://server01.adatum/home.*
   d.*http://server01.adatum.com.*

   Правильный ответ: d.
2. Данные для интрасети вашей организации в настоящее время хранятся на диске D:\ сервера IIS. Решено, что отдел кадров будет сопровождать информацию о преимуществах и правилах компании со своего сервера. Сведения отдела кадров должны быть доступны по адресу http://intranet.contoso.com/hr. Что нужно настроить?
   a. Новый Web-узел.
   b. Новый FTP-узел.
   c. Виртуальный каталог из файла.
   d. Виртуальный каталог.

   Правильный ответ: d.
3. Вы хотите обеспечить самый высокий уровень безопасности интрасети вашей организации, не развертывая инфраструктуру служб сертификации. Цель — обеспечить прозрачную для пользователей проверку подлинности и защитить ресурсы интрасети с помощью группы учетных записей, существующих в Active Directory. Все пользователи защищены от внешней сети корпоративным брандмауэром. Какой из методов проверки подлинности вы выберете?
   a. *Анонимный доступ* (Anonymous Access).
   b. *Обычная проверка подлинности* (Basic Authentication).
   c. *Краткая проверка подлинности* (Digest Authentication).
   d. *Встроенная проверка подлинности Windows* (Integrated Windows Authentication).

   Правильный ответ: d.

ГЛАВА 7

Архивация данных

Темы экзамена

- Управление процедурами резервного копирования:
  - проверка успешного завершения заданий архивации;
  - управление носителем архива.
- Настройка безопасности операций резервного копирования.
- Составление расписания заданий архивации.
- Восстановление данных из архива.

в этой главе

Здесь обсуждается графический пользовательский интерфейс (GUI) программы *Архивация данных* (Backup), а также ее работа из командной строки. Вы научитесь планировать эффективную стратегию архивации и управления носителями, выполнять операции резервного копирования и корректно восстанавливать данные в различных ситуациях. Вы также познакомитесь с новой *Службой теневого копирования тома* (Volume Shadow Copy Service, VSS), которая обеспечивает ускоренное восстановление потерянных данных. К программе Ntbackup мы еще вернемся, когда будем рассматривать восстановление ОС после сбоя.

Прежде всего

Для изучения материалов этой главы вам потребуются:

- консоль *Active Directory — пользователи и компьютеры;*
- компьютер под управлением Microsoft Windows Server 2003 (Standard или Enterprise), установленный как Server01 и настроенный в качестве контроллера домена contoso.com.

Занятие 1. **Основы архивации**

Успех любой процедуры резервного копирования зависит от правильного выбора средств и планирования. В состав Windows Server 2003 входит надежная, гибкая служебная программа Ntbackup. Она поддерживает большинство функций, которые встречаются в средствах сторонних разработчиков, включая возможность составления расписания архивации и взаимодействия со *Службой теневого копирования тома* (Volume Shadow Copy Service, VSS) и системой RSM (Removable Storage Management). На этом занятии вы рассмотрите концептуальные и процедурные вопросы архивации данных и изучите основы планирования и создания заданий резервного копирования с помощью программы Ntbackup.

Изучив материал этого занятия, вы сможете:

- ✓ архивировать данные на локальном и удаленном компьютерах;
- ✓ описать типы заданий архивации;
- ✓ создать стратегию резервного копирования.

Продолжительность занятия — около 20 минут.

Знакомство с программой *Архивация данных*

Чтобы запустить программу резервного копирования, часто называемую по имени исполняемого файла — Ntbackup, в меню **Пуск (Start)** выберите **Все программы (All Programs)\Стандартные (Accessories)\Служебные (System Tools)\Архивация данных (Backup).** Также ее можно запустить из диалогового окна **Запуск программы (Run)** командой ntbackup.exe.

В первый раз утилита резервного копирования запускается в режиме мастера (см. рис. 7-1). В этой главе обсуждается более распространенный интерфейс программы *Архивация данных.* Если вы, как и большинство администраторов, считаете, что проще использовать стандартный интерфейс, снимите флажок **Всегда запускать в режиме мастера (Always Start In Wizard Mode),** а затем щелкните ссылку **Расширенный режим (Advanced Mode).**

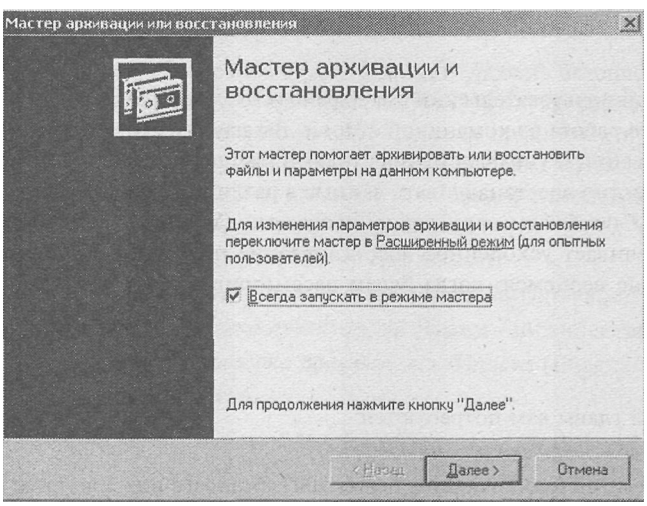


Рис. 7-1. Окно *Мастера архивации или восстановления*

Как видно на вкладке **Добро пожаловать! (Welcome),** резервное копирование можно выполнить вручную, на вкладке **Архивация (Backup),** или с помощью мастера (рис. 7-2). Кроме того, можно составить расписание для автоматического выполнения заданий архивации. Программа Backup позволяет также восстанавливать данные вручную, на вкладке **Восстановление и управление носителем (Restore And Manage Media),** или с помощью мастера **Мастер восстановления (Restore).** Далее в этой главе обсуждается мастер **ASR** (Automated System Recovery), предназначенный для архивации важных файлов ОС.

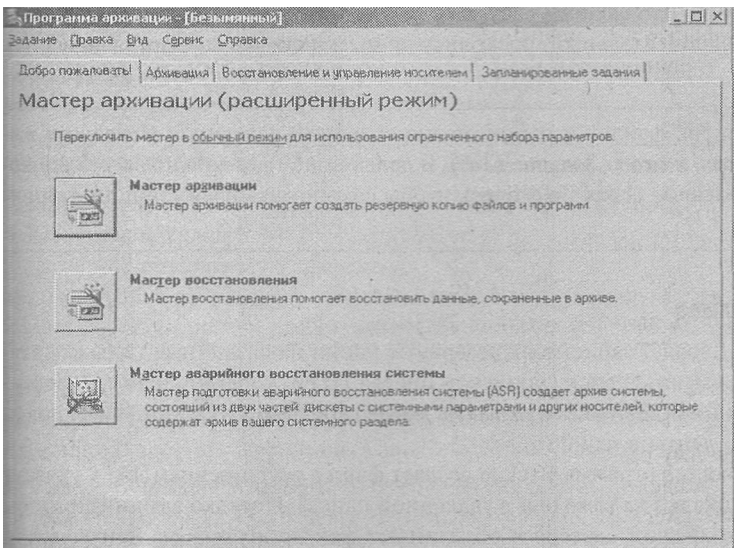


Рис. 7-2. Вкладка *Добро пожаловать!* программы *Архивация данных*

Это занятие посвящено планированию и выполнению архивации данных. Для изучения возможностей программы *Архивация данных* мы будем пользоваться вкладкой **Архивация (Backup),** показанной на рис. 7-3.

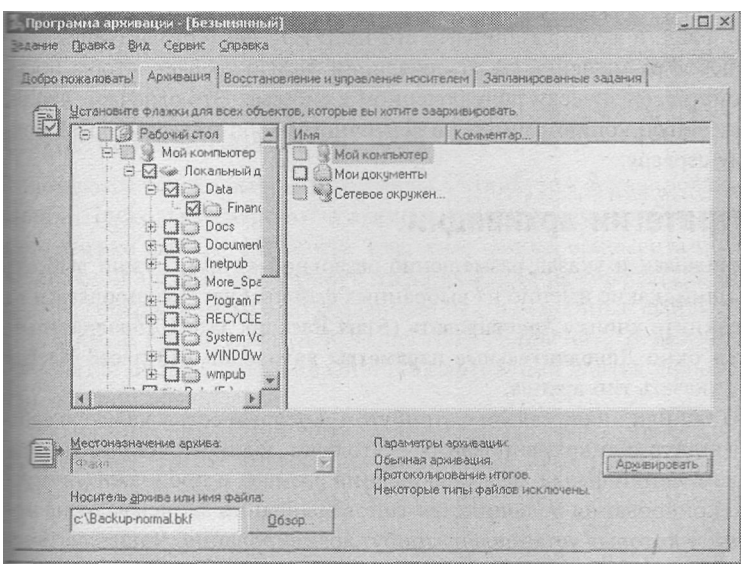


Рис. 7-3. Вкладка *Архивация* программы *Архивация данных*

Выбор файлов для архивации

Вкладка **Архивация (Backup)** позволяет выбрать файлы и папки для архивации. Ресурсы могут находиться на локальных томах или в сетевых папках. Когда папка выбирается целиком, она помечается синим флажком, если же выбираются только некоторые ресурсы — серым (частичная архивация).

Для архивации файлов или папок с удаленного компьютера выберите элементы с сетевого диска или раскройте окно **Сетевое окружение (My Network Places).** Последний способ более трудоемкий (необходимо раскрыть больше уровней, чтобы найти нужные файлы), но и более предпочтительный, поскольку привязки дисков меняются чаще, чем пути UNC.

Совет Выбранный список файлов и папок можно сохранить командой **Сохранить выделенные (Save Selections)** в меню **Задание (Job). В** дальнейшем его можно загрузить командой **Загрузить выделенные (Load Selections),** чтобы сэкономить время при повторном выборе.

Выбор носителя архива

Windows Server 2003 позволяет записывать резервные копии на различные типы носителей: магнитную ленту, сменный диск (такой как Iomega Jaz) и, конечно, непосредственно в файл на дисковом томе. При использовании магнитной ленты указанное имя должно совпадать с именем ленты в накопителе.

При архивации в файл программа Backup создает файл с расширением .bkf в указанном размещении (на локальном томе или в удаленной папке). Нередко администраторы архивируют данные на каждом сервере и объединяют файлы архивов на центральном сервере, с которого затем данные записываются на сменный носитель. При таком подходе в качестве размещения архива указывается UNC-путь к папке центрального сервера или к локальному файлу на каждом сервере; затем этот архив копируется в центральное размещение.

Программа *Архивация данных* имеет два важных ограничения. Во-первых, она не поддерживает перезаписываемые форматы DVD и CD. Чтобы обойти это ограничение, заархивируйте данные в файл, а затем скопируйте его на DVD- или компакт-диск. Во-вторых, архивация в любое размещение (за исключением файла) требует, чтобы носитель находился в устройстве, физически подключенном к системе. Это означает, что вы не сможете создать резервную копию данных на ленточном накопителе, который подсоединен к удаленному серверу.

Определение стратегии архивации

Выбрав файлы для архивации и указав размещение резервной копии, нужно выбрать тип архива, определяющий, какие именно из выбранных файлов будут копироваться на целевой носитель. Щелкните кнопку **Архивировать (Start Backup),** затем **Дополнительно (Advanced)** — откроется окно **Дополнительные параметры архивации (Advanced Backup Options),** позволяющее указать тип архива.

Каждый тип архива так или иначе связан с атрибутом, который есть у каждого файла, — **Архивный (Archive).** Атрибут архивирования — это флаг, который устанавливается при создании или изменении файла. Для уменьшения размера и продолжительности заданий резервного копирования большинство типов архивации записывают на носитель только те файлы, у которых установлен атрибут архивирования. Чаще всего не-

доразумения возникают из-за терминологии. Например, фраза «Файл помечен как заархивированный», на самом деле означает, что атрибут архивирования сброшен после очередного задания архивации. Следующее задание архивации не будет копировать этот файл на носитель. Однако, если этот файл изменится, атрибут архивирования снова будет установлен, и файл запишется на носитель при следующем резервном копировании.

Подготовка к экзамену При изучении типов архивации обратите внимание, как атрибут архивирования используется и воспринимается каждым из них. Запомните преимущества и недостатки каждого типа и способы полного восстановления структуры данных в зависимости от реализованной процедуры резервного копирования.

Обычная архивация

Архивируются все выбранные файлы и папки. Атрибут Архивный (Archive) сбрасывается. Обычная архивация не учитывает атрибут архивирования при определении файлов, подлежащих резервному копированию; все выбранные ресурсы записываются на целевой носитель. Каждая стратегия начинается с обычной архивации, которая по существу создает базовую линию, копируя все файлы в задании архивации.

По сравнению с другими типами обычная архивация выполняется дольше и требует больше места на носителе. Но, поскольку создается полная резервная копия данных, обычная архивация обеспечивает самую высокую скорость восстановления системы. Вам не придется восстанавливать несколько заданий. Обычная архивация сбрасывает атрибут архивирования у всех выбранных файлов.

Добавочная архивация

На целевой носитель копируются только выбранные файлы с установленным атрибутом архивирования, и флаг сбрасывается. Если добавочная архивация выполняется на следующий день после обычной или другой добавочной архивации, копируются только созданные или измененные за последний день файлы.

Добавочная архивация самая быстрая и формирует архив минимального размера. Тем не менее, она не так эффективна, как обычная, поскольку требует восстановления сначала обычного архива, а затем всех последующих добавочных архивов в порядке их создания.

Разностная архивация

Копируются только выбранные файлы с атрибутом архивирования, и флаг не сбрасывается. Поскольку разностная архивация учитывает атрибут архивирования, копируются только файлы, созданные или измененные с момента последней обычной или добавочной архивации. Атрибут архивирования не сбрасывается, поэтому разностные архивы содержат не только созданные или измененные файлы, но и все файлы, скопированные при предыдущей разностной архивации. В результате резервные копии становятся больше, а сама разностная архивация длится дольше, чем добавочная, но меньше, чем обычная.

Разностная архивация, однако, значительно эффективнее добавочной в плане восстановления: требуется восстановить только обычный и последний разностный архивы.

Копирующая архивация

Архивируются все выбранные файлы и папки. Атрибут архивирования не учитывается. Копирующая архивация не применяется для обычного или планового резервного копирования. Ее удобно использовать для перемещения данных между системами или создания архивной копии данных на некоторый момент времени без вмешательства в стандартные процедуры резервного копирования.

Ежедневная архивация

Копируются все выбранные файлы и папки, измененные в течение дня с момента последней ежедневной архивации (на основе даты изменения файла). Атрибут архивирования не используется и не сбрасывается. Если вам нужно создать резервную копию файлов и папок, измененных за день, не составляя расписание, используйте ежедневную архивацию.

Совмещение типов резервного копирования

Хотя создание обычного архива каждую ночь обеспечивает возможность восстановления данных на следующий день с помощью одного задания, обычная архивация требует слишком много времени, и ночное задание может продлиться до утра, снижая производительность в рабочие часы. Чтобы выбрать оптимальную стратегию резервного копирования, необходимо учесть продолжительность и размер задания архивации, а также скорость восстановления системы в случае сбоя. Есть два типичных решения.

- **Обычная и разностная архивация.** В воскресенье выполняется обычная архивация, а с понедельника по пятницу — разностная. Разностная архивация не сбрасывает атрибут архивирования, поэтому каждая операция копирует все изменения, произошедшие с понедельника. В случае сбоя данных в пятницу придется восстановить только обычный архив от воскресенья, и разностный от четверга. Такая стратегия требует больше времени для резервного копирования, особенно если данные изменяются часто, но восстановление происходит быстрее и удобнее, поскольку набор архивации занимает меньше дисков или лент.
- **Обычная и добавочная архивация.** В воскресенье выполняется обычная архивация, а с понедельника по пятницу — добавочная. Последняя сбрасывает атрибут архивирования, поэтому каждая операция архивации включает только файлы, изменившиеся со времени последнего резервного копирования. В случае сбоя данных в пятницу придется восстановить обычный архив, сделанный в воскресенье, и все добавочные архивы с понедельника по пятницу. Такая стратегия требует меньше времени на резервное копирование, но больше на восстановление.

Лабораторная работа. **Различные типы архивации**

На этой лабораторной работе вы создадите несколько заданий архивации и изучите роль атрибута архивирования.

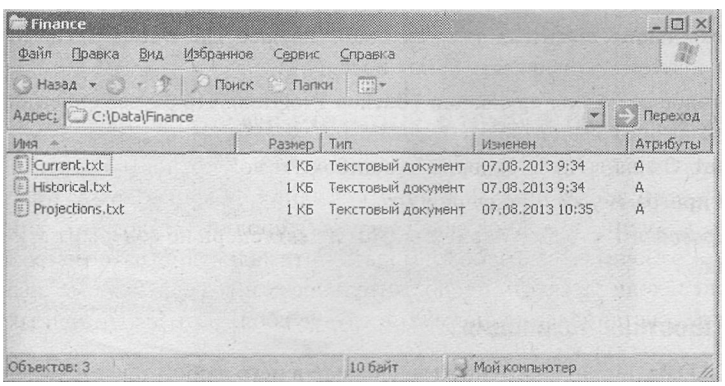
Упражнение 1. Создание данных для примера

1. Откройте *Блокнот* (Notepad) и введите следующий текст.

```
md c:\Data
net share data=C:\Data
```

```
md c:\Data\Finance
cd c:\data\Finance
echo Historical Financial Data > Historical.txt
echo Current Financials > Current.txt
echo Budget > Budget.txt
echo Financial Projections > Projections.txt
```

2. Сохраните файл как «C:\createfiles.bat», заключив имя в кавычки.
3. Откройте окно командной строки и исполните команду cd c:\.
4. Исполните команду createfiles. bat.
5. В *Проводнике* откройте каталог C:\Data\Finance. Вы должны увидеть следующее:



6. Если столбец **Атрибуты (Attributes)** не отображается, щелкните заголовки столбцов, например **Изменен (Date Modified),** правой кнопкой и выберите **Атрибуты (Attributes).** Появится столбец с атрибутами файлов.

Примечание Оставьте *Проводник* открытым на папке C:\Data\Finance, мы к ней еще вернемся.

Упражнение 2. Обычная архивация

1. Запустите программу *Архивация данных* командой Ntbackup.exe, либо в меню **Пуск (Start)\Программы (Programms)\Стандартные (Accesseories)\Служебные (System Tools)** выберите **Архивация данных (Backup).**
2. Снимите флажок **Всегда запускать в режиме мастера (Always Start In Wizard Mode).**
3. Щелкните **Расширенный режим (Advanced Mode).**
4. Перейдите на вкладку **Архивация (Backup).**
5. Раскройте узел **Мой компьютер (My Computer),** диск C:, папку Data, затем щелкните каталог Finance.

   Папка Finance помечена синим флажком, обозначающим полную архивацию, в то время как ее родительская папка помечена серым флажком, обозначающим частичную архивацию. Любые файлы, добавленные в папку Finance, будут включены в архив, но файлы, добавленные в папку Data, — нет.
6. В меню **Задание (Job)** выберите **Сохранить выделенные (Save Selections).**
7. Сохраните список выбранных файлов под именем Finance Backup.bks.

8. В поле **Носитель архива или имя файла (Backup Media Or Filename)** введите c:\backup-normal.bkf.

   Примечание В производственной среде для хранения архивов вы, вероятно, будете применять сменные носители, но, чтобы свести аппаратные требования к минимуму, на практических занятиях мы будем архивировать и восстанавливать данные, используя локальные файлы (при наличии можно использовать ленточный накопитель).

9. Щелкните кнопку **Архивировать (Start Backup),** а затем **Дополнительно (Advanced).**
10. Убедитесь, что в списке **Тип архива (Backup Type)** выбрано **Обычный (Normal),** и щелкните ОК.
11. Щелкните **Затереть данные носителя этим архивом (Replace The Data On The Media With This Backup),** а затем **Архивировать (Start Backup).**
12. Откроется диалоговое окно **Ход архивации (Backup Progress).** После завершения архивации щелкните кнопку **Отчет (Report).**
13. Просмотрите отчет. Он не должен содержать ошибок.
14. Закройте отчет и программу *Архивация данных.*

    Заметьте, что в *Проводнике* столбец **Атрибуты (Attributes)** теперь не содержит атрибуты архивирования.

Упражнение 3. Разностная архивация

1. Откройте файл C:\Data\Finance\current.txt и добавьте в него любой текст. Сохраните и закройте файл.
2. Изучите папку C:\Data\Finance в *Проводнике.* Для каких файлов отображается атрибут архивирования?

   Правильный ответ: только для измененного файла.
3. Запустите программу *Архивация данных* и перейдите на вкладку **Архивация (Backup).**
4. В меню **Задание (Job)** выберите **Загрузить выделенные (Load Selections),** чтобы загрузить список Finance Backup.
5. В поле **Носитель архива или имя файла (Backup Media Or Filename)** введите c:\backup-diff-dayl.bkf.
6. Щелкните **Архивация (Start Backup).**
7. Щелкните **Дополнительно (Advanced)** и выберите тип архива **Разностный (Differential).**
8. Запустите резервное копирование и убедитесь, что оно выполнилось без ошибок.
9. Закройте программу *Архивация данных.*
10. Посмотрите на папку в *Проводнике.* Для каких файлов установлен атрибут архивирования?

    Правильный ответ: для файла Current.txt по-прежнему установлен атрибут архивирования.
11. Откройте файл Budget и внесите какие-либо изменения. Сохраните и закройте фай. Убедитесь, что теперь атрибут архивирования для него установлен.
12. Повторите шаги 3–9, чтобы создать резервную копию **c:\backup-diff-day2.bkf.** Не забудьте просмотреть отчет архивации. Сколько файлов было скопировано в ходе арх хивации?

    Правильный ответ: два.

Упражнение 4. Добавочная архивация

1. Запустите программу *Архивация данных* и перейдите на вкладку **Архивация (Backup).**
2. **В** меню **Задание (Job)** выберите **Загрузить выделенные (Load Selections),** чтобы загрузить список Finance Backup.
3. В поле **Носитель архива или имя файла (Backup Media Or Filename)** введите путь c:\backup-inc-day2.bkf.
4. Щелкните **Архивация (Start Backup).**
5. Щелкните кнопку **Дополнительно (Advanced)** и выберите тип архива **Добавочный (Incremental).**
6. Запустите резервное копирование и после завершения убедитесь, что оно выполнилось без ошибок.
7. Закройте программу *Архивация данных.*
8. Посмотрите на папку в *Проводнике.* Для каких файлов установлен атрибут архивирования?

   Правильный ответ: таких файлов нет.
9. Откройте файл Projections и внесите какие-либо изменения. Сохраните и закройте файл. Для этого файла в *Проводнике* должен появиться атрибут архивирования.
10. Повторите шаги 1—8, чтобы создать резервную копию **c:\backup-inc-day3.bkf.**

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Какие из следующих размещений нельзя использовать для хранения резервной копии системы Windows Server 2003?
   a. Локальный ленточный накопитель.
   b. Локальный привод CD-RW.
   c. Локальный жесткий диск.
   d. Общая папка на удаленном сервере.
   e. Локальный привод DVD+R.
   f. Локальный сменный диск.
   g. Ленточный накопитель на удаленном сервере.
2. Вам поручено каждый вечер создавать резервные копии файлового сервера Windows Server 2003. Вы вручную выполняете обычную архивацию, затем составляете расписание, по которому задание архивации запускается каждый вечер в течение следующих двух недель. Какой из типов архивации завершится быстрее?
   a. Обычная.
   b. Разностная.
   c. Добавочная.
   d. Копирующая.
3. Вам поручено каждый вечер создавать резервные копии файлового сервера Windows Server 2003. Вы вручную выполняете обычную архивацию, затем составляете расписание, по которому задание архивации запускается каждый вечер в течение следую-

щих двух недель. Какой из типов архивации обеспечивает самый простой способ восстановления данных?

a. Обычная.
b. Разностная.
c. Добавочная.
d. Ежедневная.

4. Вам поручено каждый вечер создавать резервные копии файлового сервера Windows Server 2003. Вы выполняете обычную архивацию, а на следующий день решаете, какую архивацию выбрать: добавочную или разностную. Будут ли эти задания архивации отличаться по размеру или скорости выполнения? Если бы на следующий день на сервере произошел сбой, одинаково эффективными были бы операции восстановления?
5. Вспомните текст лабораторной работы. Попробуйте спрогнозировать содержимое следующих заданий архивации:

a backup-normal.bkf;
p backup-diff-dayl.bkf;
p backup-diff-day2.bkf;
p backup-inc-day2.bkf;
p backup-inc-day3.bkf.

Есть ли разница между содержимым backup-diff-day2 и backup-inc-day2?

Примечание Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы. Однако вы можете проверить свой прогноз, выполнив лабораторную работу занятия 2.

Резюме

- Программа *Архивация данных* позволяет архивировать и восстанавливать данные из локальных и удаленных папок.
- Данные можно архивировать в локальный файл, на магнитную ленту, на сменные носители или в общие папки на удаленных серверах. Нельзя архивировать на перезаписываемые носители CD или DVD.
- Обычная архивация — это полное резервное копирование всех выбранных файлов и папок. Она всегда является отправной точкой любой стратегии архивирования.
- При добавочной архивации копируются выбранные файлы, измененные с момента последней обычной или добавочной архивации. Обычная и добавочная архивации сбрасывают атрибут архивирования.
- При разностной архивации копируются все выбранные файлы, изменившиеся с момента последней обычной или добавочной архивации. Разностная архивация не сбрасывает атрибут архивирования.
- Копирующая и ежедневная архивация используются реже. Первая копирует все выбранные файлы, а вторая — файлы, измененные за указанный день. Эти типы не сбрасывают атрибут архивирования, поэтому их можно использовать для копирования и передачи данных, не нарушая обычное расписание архивации.

Занятие 2. **Восстановление данных**

Вместе со стратегией архивации вы должны создать и проверить процедуры восстановления данных и убедиться, что соответствующий персонал обладает необходимыми знаниями и навыками. На этом занятии обсуждаются процессы и параметры, доступные для восстановлении данных с помощью программы *Архивация данных*.

Изучив материал этого занятия, вы сможете:

- ✓ восстановить данные в исходное размещение или в другую папку;
- ✓ настроить параметры восстановления.

Продолжительность занятия - около 10 минут.

Восстановление данных с помощью программы *Архивацияданных*

Восстановление данных — довольно простая процедура. Вкладка **Восстановление и управление носителем (Restore And Manage Media)** программы *Архивация данных* (рис. 7-4) позволяет выбрать набор архивации, с которого нужно восстановить данные. Затем Windows Server 2003 отображает список файлов и папок из набора архивации. Вы можете выбрать отдельные файлы или папки, которые следует восстановить; синий флажок указывает, что файл или папка будут восстановлены целиком, затененный — что будет восстановлена только часть содержимого папки.

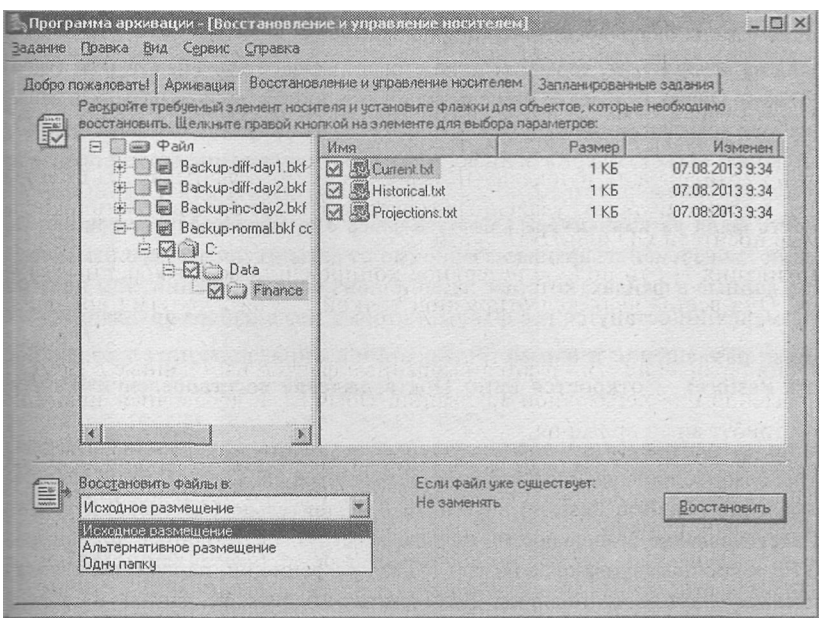


Рис. 7-4. Вкладка *Восстановление и управление носителем* программы *Архивацияданных*

Кроме того, программа предложит указать размещение для восстановления файлов. Можно выбрать один из трех вариантов.

- **Исходное размещение (Original location).** Данные восстанавливаются в исходную папку, из которой они были архивированы. Исходная структура папки сохраняется или, если папки были удалены, создается заново.
- **Альтернативное размещение (Alternate location).** Данные восстанавливаются в папку, указанную в поле *Альтернативное размещение*. Исходная структура папки сохраняется и создается внутри указанной папки, которая считается корнем (томом) архивных данных. Например, если создать резервную копию папки C:\Data\Finance и восстановить ее в папку C:\Restore, вы получите папку C:\Restore\Data\Finance.
- **Одну папку (Single folder).** Файлы восстанавливаются в указанную папку, но структура папки не сохраняется. Все файлы восстанавливаются в одну папку.

Выбрав файлы и размещение, щелкните кнопку **Восстановить (Start Restore).** Щелкните OK, чтобы запустить процесс восстановления. Убедитесь, что все прошло без ошибок.

Параметры восстановления

Windows Server 2003 поддерживает несколько параметров, определяющих ход восстановления файлов. Чтобы их настроить, запустите программу *Архивация данных* и в меню **Сервис (Tools)** выберите **Параметры (Options) (рис. 7-5).**

- **Не заменять файл на компьютере (Do Not Replace The File On My Computer).** Файлы, которые уже находятся в целевом расположении, пропускаются; этот параметр используется по умолчанию. Например, такой способ восстановления подходит, когда некоторые (но не все) файлы удалены из папки, куда идет восстановление. Тогда отсутствующие файлы будут восстановлены из архива.
- **Заменять файл на компьютере, только если он старее (Replace The File On Disk Only If The File On Disk Is Older).** Существующие файлы заменяются, только если они старее файлов из набора архивации. Идея в том, что более свежий файл, который находится в целевой папке, может содержать информацию, которую вы не хотите перезаписывать.
- **Всегда заменять файл на компьютере (Always Replace The File On My Computer).** Все файлы заменяются версией из архива независимо от даты их последнего изменения. Вы потеряете данные в файлах, которые изменились после архивации. Тем не менее в целевом размещении останутся все файлы, которых нет в наборе архивации.

Выбрав файлы, размещение и параметры восстановления, щелкните кнопку **Восстановить (Start Restore)** — откроется окно **Подтверждение восстановления (Confirm Restore).**

Прежде чем подтвердить восстановление, вы можете указать, как должны обрабатываться параметры безопасности файлов в архиве. Для этого в диалоговом окне **Подтверждение восстановления (Confirm Restore)** щелкните **Дополнительно (Advanced)** и установите флажок **Восстановление безопасности (Restore Security).** Если данные архивировались с тома NTFS и восстанавливаются на том NTFS, разрешения, параметры аудита и сведения о владельце будут восстановлены. Если снять этот флажок, данные будут восстанавливаться без дескрипторов безопасности, и все восстановленные файлы будут наследовать разрешения целевой папки или тома.

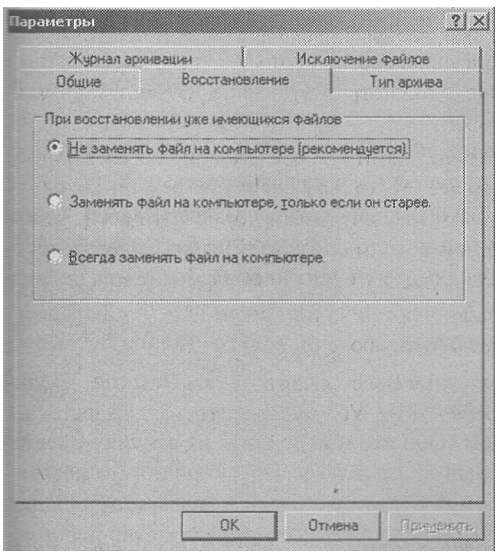


Рис. 7-5. Параметры на вкладке *Восстановление*

Лабораторная работа. **Восстановление данных**

На этой лабораторной работе вы проверите процедуры архивации и восстановления, используя типичный метод: восстановление в тестовое размещение.

Упражнение. Проверка процедур архивации и восстановления

Чаще для проверки процедур архивации и восстановления администраторы выполняют тестовое восстановление набора архивации. Чтобы предотвратить повреждение данных, файлы восстанавливают не в исходное размещение, а в другую папку, которую можно удалить после теста. В производственной среде следует проверить восстановление архива на резервном сервере (перед этим убедитесь, что устройство архивации (допустим, ленточный накопитель) правильно установлено на сервере, который будет хранить данные при отказе основного сервера).

1. Запустите программу *Архивация данных*.
2. Перейдите на вкладку **Восстановление и управление носителем (Restore And Manag Media).**
3. Щелкните знак «+», чтобы раскрыть файл.
4. Щелкните знак «+», чтобы раскрыть файл Backup-normal.bkf.
5. Установите флажок, чтобы выбрать диск C:.
6. Последовательно раскройте узлы C:, Data и Finance. Заметьте: после выбора папки C: будут отмечены ее вложенные папки и файлы.
7. В списке **Восстановить файлы в (Restore Files To)** выберите **Альтернативное размещение (Alternate location).**
8. В поле **Альтернативное размещение (Alternate location)** введите путь C:\TestRestore.
9. Щелкните **Восстановить (Start Restore).**
10. В диалоговом окне **Подтверждение восстановления (Confirm Restore)** щелкните **OK**.

11. После завершения задания восстановления щелкните кнопку **Отчет (Report)** и изучите журнал операции восстановления.
12. Откройте папку C:\TestRestore и убедитесь, что структура папки и файлы восстановлены правильно.
13. Повторите шаги 1—10 для восстановления файла backup-diff-day2.bkf. После завершения задания восстановления перейдите к шагу 14 и изучите отчет.
14. После завершения задания восстановления щелкните кнопку **Отчет (Report),** чтобы просмотреть журнал операции восстановления. Если вы случайно закрыли окно состояния задания, в меню **Сервис (Tools)** щелкните **Отчет (Report),** выберите последний отчет и щелкните **Просмотр (View).**
15. Изучите отчет по последнему заданию восстановления. Сколько файлов было восстановлено?

    Таких файлов нет. Почему? Причина в параметрах восстановления.
16. В меню **Сервис (Tools)** выберите **Параметры (Options)** и перейдите на вкладку **Восстановление (Restore).** Теперь вы можете выявить проблему. По умолчанию программа архивации не заменяет файлы на компьютере. Поэтому при восстановлении из разностного архива файлы, обновленные после обычной архивации, не были перезаписаны.
17. Выберите **Всегда заменять файл на компьютере (Always Replace The File On My Computer).**
18. Еще раз восстановите файл backup-diff-day2.bkf. Отчет должен подтверждать восстановление двух файлов.
19. Итак, вы проверили процедуры архивации и восстановления, и научились изменять параметры восстановления. Удалите папку C:\TestRestore.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Пользователь случайно удалил данные из документа Microsoft Word. Обычная архивация выполнялась на сервере вчера вечером. Какой параметр следует выбрать, чтобы восстановить исходный файл?
   a. **Не заменять файл на компьютере (Do Not Replace The File On My Computer).**
   b. **Заменять файл на компьютере, только если он старее (Replace The File On Disk Only If The File On Disk Is Older).**
   c. **Всегда заменять файл на компьютере (Always Replace The File On My Computer).**
2. Один из руководителей вернулся из деловой поездки. Перед поездкой он скопировал файлы из сетевой папки на жесткий диск своего компьютера. В общей папке хранятся документы других руководителей, которые изменяли свои файлы в его отсутствие. Вернувшись, он скопировал файлы в сетевой ресурс, обновив не столько свои, но и чужие файлы. Другие руководители не были в восторге от того, что их файлы были заменены старыми версиями. К счастью, вчера вечером вы выполнили обычную архивацию этой папки. Какой параметр восстановления следует выбрать?
   a. **Не заменять файл на компьютере (Do Not Replace The File On My Computer).**
   b. **Заменять файл на компьютере, только если он старее (Replace The File On Disk Only If The File On Disk Is Older).**
   c. **Всегда заменять файл на компьютере (Always Replace The File On My Computer).**

3. Вам нужно протестировать процедуру восстановления на сервере, не повредив производственные копии архивных данных. Какое размещение для восстановления лучше выбрать?
   a. **Исходное размещение (Original location).**
   b. Альтернативное размещение (Alternate location).
   c. Одну папку (Single folder).

Резюме

- Программа *Архивация данных* позволяет восстанавливать резервные копии данных.
- При восстановлении потерянного файла или папки лучше выбрать вариант **Исходное размещение (Original location).**
- При тестировании процедуры восстановления следует выбрать вариант **Альтернативное размещение (Alternate location),** чтобы не повредить исходные копии заархивированных файлов и папок.
- Если вы восстанавливаете разностные или добавочные наборы архивации после восстановления обычного набора, следует выбрать вариант **Всегда заменять файл на компьютере (Always Replace The File On My Computer).**
- Если вы восстанавливаете папку, в которой утеряна только часть файлов, следует выбрать вариант **Не заменять файл на компьютере (Do Not Replace The File On My Computer)** или **Заменять файл на компьютере, только если он старее (Replace The File On Disk Only If The File On Disk Is Older).**

Занятие 3. Дополнительные возможности архивации и восстановления

Теперь, когда план архивации создан, процедуры архивации и восстановления проверены, мы более подробно обсудим процессы архивации, чтобы вы могли автоматизировать их и по возможности упростить. На этом занятии обсуждаются технологии, лежащие в основе архивации данных, такие как VSS и RSM, а также параметры для создания сценариев и запуска архивации по расписанию. Кроме того, вы познакомитесь с новой функцией теневого копирования общих папок, которая позволяет пользователям восстанавливать потерянные данные в простых ситуациях без вмешательства администратора.

Изучив материал этого занятия, вы сможете:

- ✓ настраивать членство в группах, чтобы пользователи могли выполнять резервное копирование и восстановление;
- ✓ управлять ленточными носителями с архивами;
- ✓ каталогизировать наборы архивации;
- ✓ настраивать параметры архивации;
- ✓ выполнять архивацию из командной строки;
- ✓ составлять расписание заданий архивации;
- ✓ настраивать и применять функцию теневого копирования общих папок.

Продолжительность занятия — около 30 минут.

Понятие VSS

Windows Server 2003 поддерживает *Службу теневого копирования тома* (Volume Shadow Copy Service, VSS), называемую также *архивацией снимков* (snap backup). VSS позволяет архивировать БД и другие файлы, которые открыты или заблокированы действиями пользователей или системы. Теневое копирование позволяет приложениям продолжать записывать данные на том во время резервного копирования, а администраторам — выполнять архивацию в любое время, не прерывая работу пользователей и не рискуя пропустить файлы.

Хотя VSS — важное расширение возможностей архивации в Windows Server 2003, не стоит использовать эту службу для архивации при низкой нагрузке. Если у вас есть приложения, особым образом контролирующие целостность данных, когда файлы открыты, такой способ архивации может нарушить целостность архива и открытых файлов. При работе с критичными приложениями или такими пакетами, как Microsoft SQL Server, которые обладают встроенными средствами архивации, выясните рекомендуемую процедуру резервного копирования из документации к этому приложению.

Безопасность архивации

Чтобы заархивировать или восстановить файл, необходимо обладать пользовательскими правами *Архивация файлов и каталогов* (Backup Files And Directories) и *Восстановление файлов и каталогов* (Restore Files And Directories) или NTFS-разрешениями *Чтение* (Read) и *Запись* (Write) в целевом размещении. Такими привилегиями обладают группы *Администраторы* (Administrators) и *Операторы архива* (Backup Operators), поэтому, чтобы предоставить учетной записи пользователя, группы или службы минимальные требуемые привилегии, добавьте ее в группу *Операторы архива* на сервере.

Пользователи с правом *Восстановление файлов и каталогов* (Restore Files And Directories) могут удалять NTFS-разрешения с файлов при восстановлении. В Windows Server 2003 они также могут передавать право владения файлами другим пользователям. Поэтому важно контролировать состав группы *Операторы архива* (Backup Operators) и физически защищать архивные ленты, иначе любой специалист сможет восстановить секретные данные и получить к ним доступ.

Управление носителем

Программа *Архивация данных* (Backup) в Windows Server 2003 тесно взаимодействует со службой RSM (Removable Storage Management). Эта служба, разработанная для управления автоматическими библиотеками лент и приводами CD-ROM, принимает от других служб или приложений запросы к носителю и гарантирует, что он правильно смонтирован и загружен.

RSM также позволяет работать с устройствами, куда вручную загружается один носитель, например с ленточными накопителями, приводами CD-ROM или Iomega Jaz. При работе с такими устройствами RSM отслеживает носители по меткам или серийным номерам, и даже в системе архивации с одним носителем у каждой ленты должна быть уникальная метка.

Пулы носителей

Программа *Архивация данных* в Windows Server 2003 управляет лентами через службу RSM, используя пулы носителей (рис. 7-6).

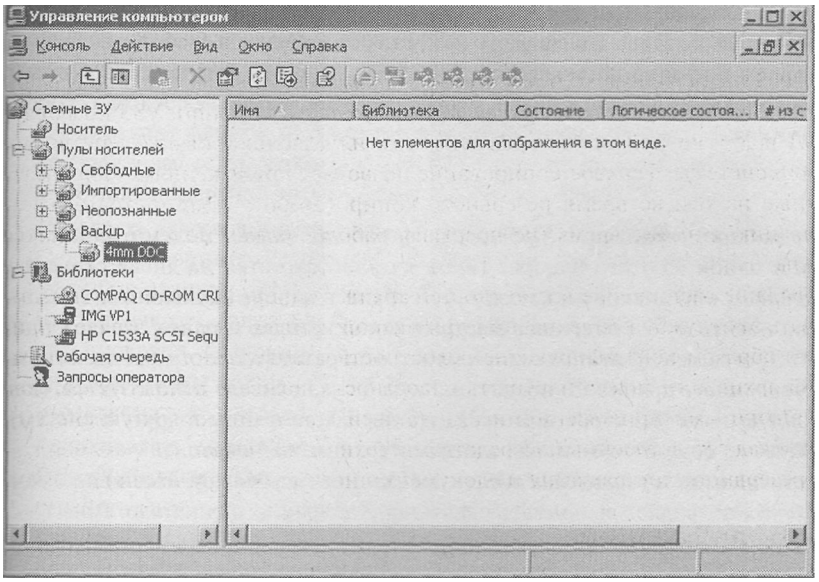


Рис. 7-6. Пулы носителей

С архивацией связаны четыре пула носителей.

- ***Неопознанные* (Unrecognized).** Содержит полностью чистые или отформатированные в неизвестном формате ленты.
- *Свободные (Free)*. Содержит только вновь отформатированные ленты плюс те, **что** администратор специально пометил свободными. Свободные носители перемешаются в архивный пул, когда на них записывают набор архивации.
- **Backup.** Содержит носители, записанные программой *Архивация данных* (Backup), которая архивирует только на носитель в свободном пуле (и маркирует ленту именем, которое вы вводите перед началом архивации), а также на носитель в архивном пуле с указанным именем.
- ***Импортированные* (Import).** Содержит ленты, не каталогизированные на локальном диске. При создании каталога такая лента перемещается в архивный пул.

Управление лентами и пулами носителей

Кроме выполнения операций резервного копирования и ротации лент, необходимо управлять включением лент в пулы носителей. На вкладке **Восстановление и управление носителем (Restore And Manage Media)** программы *Архивация данных* доступны следующие возможности.

- **Форматирование ленты.** Щелкните ленту правой кнопкой и выберите **Форматировать (Format).** Форматирование — не безопасный способ уничтожения информации на ленте. Если вам нужно очистить ленты, допустим, из соображений безопасности, используйте программное средство сторонних разработчиков. Форматирование подготавливает ленту и перемещает ее в свободный пул носителей и поддерживается не всеми устройствами.
- **Натяжение ленты.** Щелкните ленту правой кнопкой и выберите **Регулировка натяжения (Retension).** Поддерживается не всеми устройствами.

- **Пометка ленты свободной.** Щелкните носитель правой кнопкой и выберите **Пометить как свободный (Mark As Free).** После этого лента переместиться в свободный пул носителей. При этом информация на ленте сохранится. Если вам нужно стереть ленты, например из соображений безопасности, используйте программное средство сторонних разработчиков.

Каталоги

Одновременно с набором архивации программа *Архивация данных* создает каталог со списком файлов и папок из этого набора. Такой каталог хранится на диске сервера и называется локальным или дисковым каталогом, а также в наборе архивации и называется каталогом на носителе. Он облегчает быстрый поиск файлов и папок, подлежащих восстановлению. Программа *Архивация данных* может отобразить каталог мгновенно, а не загружать его с медленного архивного носителя. Каталог на носителе используется, если локальный каталог выходит из строя или когда вы передаете файлы в другую систему. В этом случае Windows создает локальный каталог из копии на носителе.

Вкладка **Восстановление и управление носителем (Restore And Manage Media)** программы *Архивация данных* позволяет выполнять следующие операции над каталогами.

- **Удаление.** Если вы потеряли или повредили носитель архива или переместили файлы в другую систему и локальный каталог больше не нужен, щелкните набор архивации правой кнопкой и выберите **Удалить каталог (Delete Catalog).** Эта команда не удаляет каталог на носителе.
- **Пополнение.** Не каталогизированная на локальном компьютере лента из другой системы появится в импортированном пуле носителей. Щелкните носитель правой кнопкой и выберите **Каталог** (Catalog). Windows скопирует локальный каталог с ленты или из файла. Эта операция не создает и не изменяет каталог на носителе.

Совет Если у вас есть все ленты набора архивации и они не повреждены, откройте окно **Параметры (Options)** программы *Архивация данных* и на вкладке **Общие (General)** установите флажок **Использовать каталоги носителей для ускорения построения каталогов восстановления на диске (Use The Catalogs On The Media To Speed Up Building Restore Catalogs On Disk).** Если лента в наборе архивации отсутствует или повреждена, снимите этот флажок. Это гарантирует, что каталог будет полным и точным, однако для его создания может потребоваться много времени.

Параметры архивации

Для настройки параметров архивации в меню **Сервис (Tools)** программы *Архивация данных* выберите **Параметры (Options).** Большинство из этих параметров настраивает стандартные значения, которые используют программа *Архивация данных* и средство командной строки Ntbackup. Эти параметры могут быть перекрыты параметрами конкретного задания архивации.

Вкладка *Общие*

На вкладке **Общие (General)** диалогового окна **Параметры (Options)** можно настроить следующие параметры.

- **Оценивать информацию о выборе файлов перед выполнением операций архивации или восстановления (Compute Selection Information Before Backup And Restore Operations).**
  - Программа *Архивация данных* перед началом операции подсчитывает количество и размер файлов, которые будут заархивированы или восстановлены.

- **использовать каталоги носителей для ускорения построения каталогов восстановления на диске (Use The Catalogs On The Media To Speed Up Building Restore Catalogs On Disk).** Позволяет создать локальный каталог для ленты из каталога на носителе. Однако, если ленты с каталогом на носителе нет или носитель в наборе поврежден, вы можете снять этот флажок, и система просмотрит весь набор архивации (или ту его часть, которая у вас есть), чтобы построить каталог на диске. Если набор архивации большой, такая операция может занять несколько часов.
- **Проверять данные после завершения архивации (Verify Data After The Backup Completes).** Система сравнивает содержимое носителя архива с исходными файлами и фиксирует любые отличия. Этот параметр сильно замедляет архивацию. Расхождения обычно появляются, когда данные часто меняются в процессе резервного копирования . или проверки, поэтому не рекомендуется проверять архивы системы, поскольку системные файлы постоянно меняются. Если вы ведете ротацию лент и своевременно избавляетесь от изношенных носителей, сравнивать данные не потребуется.
- **Архивировать содержимое подключенных дисков (Backup The Contents Of Mounted** Drives). Подключенный диск — это дисковый том, спроецированный на папку в пространстве имен другого тома, а не на букву диска. Если этот флажок сброшен, архивируется только путь к папке, подключенной к тому, но не ее содержимое. Если же флажок установлен, архивируется также содержимое подключенного тома. Нет ничего плохого в том, чтобы заархивировать точку подключения, но, если вы архивируете точку подключения и подключенный диск, ваш набор архивации будет содержать две копии Данных.

Если вы сначала заархивировали данные в файл, а затем сохранили его на другом носителе, снимите следующие флажки. Напротив, установите флажки, если вы сразу архивируете на ленту или носитель, управляемый службой **RSM.**

- **Выводить предупреждение, если служба съемных носителей не активна при запуске программы архивации (Show Alert Message When I Start the Backup Utility And Removable Storage Is Not Running).**
- **Выводить предупреждение, если при запуске программы архивации имеется доступный распознаваемый носитель (Show Alert Message When I Start The Backup Utility And There Is Recognizable Media Available).**
- **Выводить предупреждение при вставке нового носителя (Show Alert Message When New Media Is Inserted).**
- **Разрешить всегда использовать распознанный носитель без предупреждения (Always Allow Use Of Recognizable Media Without Prompting).**

Совет Флажок **Разрешить всегда использовать распознанный носитель без предупреждения** можно установить, если вы используете локальные ленточные накопители только для архивации, но не для службы Remote Storage или других функций. Этот флажок избавляет от необходимости выделять свободный носитель через узел **Съемные ЗУ (Removable Storage)** в консоли *Управление компьютером* (Computer Management).

Журнал архивации

Диалоговое окно **Параметры (Options)** содержит вкладку **Журнал архивации (Backup Log). В** журнале регистрируются проблемы, угрожающие жизнеспособности резервной копии, поэтому продумайте стратегию ведения журнала, а также план архивации в целом. Хотя при подробной регистрации фиксируются все заархивированные файлы и пути, журнал

получается столь объемным, что вы, скорее всего, упустите проблемы из вида. Поэтому рекомендуется вести только сводный журнал (это вариант по умолчанию), который содержит сведения о пропущенных файлах и ошибках.

Система хранит 10 журналов архивации в каталоге %UserProfile%\Local Settings\Application Data\Microsoft\Windows NT\Ntbackup\Data. Путь и максимальное количество хранимых журналов изменить нельзя. Хотя, конечно, вы можете включить эту папку в архив и тем самым сохранить старые журналы.

Исключение файлов из архива

Вкладка **Исключение файлов (Exclude Files)** диалогового окна **Параметры (Options)** позволяет указать расширения и отдельные файлы, которые следует пропустить при архивации. По умолчанию программа *Архивация данных* пропускает файл подкачки, временные файлы, кэш на стороне клиента, папку отладки, базу данных и папки *Службы репликации файлов* (File Replication Service, FRS), а также другие локальные журналы и БД.

Файлы можно исключить в зависимости от их владельца. Щелкните кнопку **Добавить (Add New)** под списком **Файлы, исключенные для всех пользователей (Files Excluded For All Users),** чтобы исключить файлы других пользователей. Щелкните кнопку **Добавить** под списком **Файлы, исключенные для пользователя (Files Excluded For User) имя_пользователя,** чтобы исключить только ваши файлы. Вы можете выбрать типы файлов из списка **Зарегистрированный тип файла (Registered File Type)** или указать расширение в поле **Особая маска файла (Custom File Mask).** Наконец, можно исключить файлы из указанной папки или с диска при помощи параметров **Применяется к пути (Applies To Path)** и **Применять ко всем подпапкам (Applies To All Subfolders).**

Дополнительные параметры архивации

Выбрав файлы и запустив резервное копирование кнопкой **Архивировать (Start Backup),** можно настроить дополнительные параметры для конкретного задания, щелкнув кнопку **Дополнительно (Advanced):**

- **Проверять данные после архивации** (Verify **Data After Backup)** — перекрывает значение по умолчанию, указанное в диалоговом окне **Параметры (Options)** программы *Архивация данных;*
- **Если возможно, сжимать архивируемые данные (If Possible, Compress The Backup Data To Save Space)** — включает сжатие данных для экономии места на носителе архива; недоступен, если ленточный накопитель не поддерживает сжатие;
- **Отключить теневое копирование состояния тома (Disable Volume Shadow Copy)** — VSS позволяет архивировать открытые и заблокированные для использования файлы. Если этот флажок установлен, некоторые открытые или используемые файлы могут быть пропущены.

Команда Ntbackup

Команда Ntbackup позволяет создавать сценарии заданий архивации. Ее синтаксис таков:

```
Ntbackup backup {"path to backup" or "@selectionfile.bks"} /j "Job Name" options
```

Первый параметр команды, backup, задает рабочий режим: нельзя восстановить данные из командной строки. За ним следует параметр, указывающий, что именно нужно архивировать. Можно указать путь к локальной папке, сетевому общему ресурсу или

файлу. Кроме того, можно указать путь к файлу выбора архивации (с расширением .bks), используя синтаксис *@файл_выбора.bks* (случае перед именем файла выбора архивации должен стоять символ @). Этот файл содержит информацию о файлах и папках, подлежащих архивации, и должен быть создан из графического интерфейса программы *Архивацияданных*.

Третий параметр, /J *«имя_задания»,* указывает описательное имя задания, которое используется в отчете архивации.

Ниже перечислены остальные параметры командной строки, сгруппированные по типам заданий архивации.

Архивация в файл

Используйте параметр /F *«имя_файла»,* где *имя_файла* — полное имя файла, содержащее путь к логическому диску. Не используется с параметрами /T /P /G.

Следующая команда архивирует удаленный общий ресурс Data на ServerOl в локальный файл на диске E:

```
ntbackup backup "\\serverO1\Data" /J "Backup of Server 01 Data folder" /F
"E:\Backup. bkf"
```

Дозапись в файл или на ленту

Используйте параметр /A для выполнения операции дозаписи. При дозаписи на ленту, а не в файл, с этим параметром необходимо использовать параметр /G или /T. Не используется с параметрами /N или /P.

Следующая команда архивирует удаленный общий ресурс Profiles на Server02 и дозаписывает набор к заданию, созданному в первом примере:

```
ntbackup backup "\\server02\Profiles" /J "Backup of Server 02 Profiles folder" /F
"E:\Backup.bkf" /A
```

Архивация на новую ленту или в файл либо перезапись существующей ленты

Используйте параметр /N *«имя_носителя»,* где *имяносителя* — имя новой ленты. Не используется с параметром /A.

Архивация на новую ленту

Используйте параметр /P *«имя_пула»,* где *имя_пула* — пул, содержащий архивный носитель. Обычно это подпул пула архивных носителей, например 4mm DDS. Не используется с параметрами /A, /G, /F или /T. •

Следующая команда архивирует файлы и папки, перечисленные в файле выбора архивации c:\backup.bks, на ленточный накопитель:

```
ntbackup backup @c:\backup.bks /j "Backup Job 101" /n "Command Line Backup Job" /p
"4mm DDS"
```

Архивация на существующую ленту

Чтобы указать ленту для операции дозаписи или перезаписи, используйте параметр /T или /G вместе с /A (дозапись) или /N (перезапись). Параметр /P нельзя использовать с параметрами /T или /G.

Чтобы указать имя ленты, используйте параметр /T *«имя_ленты»,* где *имя_ленты* — действительная лента в пуле носителей.

Следующая команда архивирует файл выбора и добавляет его на ленту, созданную в предыдущем примере:

```
ntbackup backup @c:\backup.bks /j "Backup Job 102" /a /t "Command Line
Backup Job"
```

Чтобы указать ленту по идентификатору GUID, а не по имени, используйте параметр /G *«имя_GUID»,* где *имя_GUTD* — действительная лента в пуле носителей.

Параметры задания

Для каждого из перечисленных выше типов заданий можно указать дополнительные параметры:

- /M ***{тип_архивации}*** — указывает один из следующих типов архивации: *обычная* (normal), *копирующая* (copy), *разностная* (differential), *добавочная* (incremental) или *ежедневная* (daily);
- **/D *{«описание_набора»}*** — указывает метку для набора архивации;
- **/V:{yes | no}** — проверяет данные по завершении архивации;
- **/R:{yes | no}** — разрешает доступ к ленте только владельцам и членам группы *Администраторы* (Administrators);
- **/L:{f | s | n}** — указывает тип файла журнала: f — полный (full), s — сводный (summary), n — журнал не создается (none);
- **/RS:{yes | no}** — архивирует перенесенные файлы данных, расположенные в узле **Съемные ЗУ (Remote Storage);**

  Совет Параметр /RS не требуется для резервного копирования локальной БД службы Removable Storage, которая содержит файлы-заполнители Remote Storage. При резервном копировании папки %Systemroot%, *программа Архивация данных* автоматически архивирует БД Removable Storage.

- **/HC:{on | off}** — включает аппаратное сжатие на ленточном накопителе, если оно поддерживается;
- **/SNAP: {on | off}** — указывает программе архивации использовать теневое копирование тома.

Планирование заданий архивации

Для архивации по расписанию создайте задание архивации в программе *Архивация данных,* щелкните **Архивировать (Start Backup)** и настройте дополнительные параметры. Затем щелкните кнопку **Расписание (Schedule)** и в окне **Указание учетной записи (Set Account Information)** введите имя пользователя и пароль учетной записи, которая будет использоваться заданием архивации.

Внимание! Рекомендуется создавать учетную запись для каждой службы, а не запускать все под учетной записью *System*. Службу не следует запускать под учетной записью пользователя или от имени *Администратор* (Administrator). Если пароль учетной записи пользователя изменится, вам придется изменить настройки для всех служб, которые запускаются в ее контексте. Учетная запись для задания архивации должна быть включена в группу *Операторы архива* (Backup Operators).

В окне **Параметры запланированного задания (Scheduled Job Options)** введите имя задания и щелкните **Свойства (Properties).** Откроется окно **Запланированное задание (Schedule Job),** показанное на рис. 7-7. Настройте дату, время и периодичность задания. Кнопка **Дополнительно (Advanced)** позволяет настроить дополнительные параметры расписания, включая диапазон дат, когда следует выполнять задание. Вкладка **Параметры (Settings)** окна **Запланированное задание** позволяет точнее описать задание, например указать, что оно должно выполняться, если компьютер простаивает в течение указанного интервала времени.

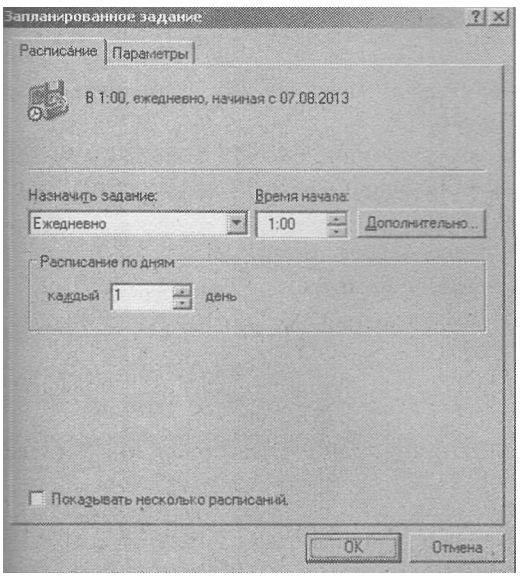


Рис. 7-7. Диалоговое окно *Запланированное задание*

Составленное расписание можно редактировать на вкладке Запланированные задавая (Schedule Jobs) программы *Архивация данных.* Если щелкнуть в календаре задание, откроется его расписание. Кроме того, можно добавить задание архивации, щелкнув кнопку Добавить задание (Add Job) на вкладке Запланированные задания (Schedule Jobs): запустится мастер архивации, позволяющий выбрать файлы, подлежащие архивации, н указать другие свойства задания. Впрочем, большинство администраторов предпочитают создавать задание архивации на вкладке Backup, а затем составлять его расписание, как описано выше.

Теневые копии общих папок

Windows Server 2003 предлагает администраторам и пользователям еще один способ быстрого восстановления поврежденных файлов и папок. Используя VSS, Windows Server 2003 автоматически кэширует копии файлов по мере их изменения. Если пользователь удаляет, перезаписывает или нежелательно изменяет файл, вы можете просто восстановить его предыдущую версию. Тем не менее эта важная функция не исключает архивацию. Она обеспечивает быстрое восстановление при решении простых, повседневных проблем, но не предназначена для восстановления больших объемов потерянных данных.

Включение и настройка теневых копий

Функция **Теневые копии (Shadow Copies)** для общих папок по умолчанию отключена. Чтобы включить ее, откройте окно свойств дискового тома в *Проводнике* или в оснастке *Управление дисками* (Disk Management). На вкладке **Теневые копии (Shadow Copies),** показанной на рис. 7-8, выберите том и щелкните **Включить (Enable).** После включения будут созданы теневые копии для всех общих папок на данном томе; отдельные общие папки на томе выбрать нельзя. Хотя вы можете вручную инициировать теневую копию, щелкнув **Создать (Create Now).**

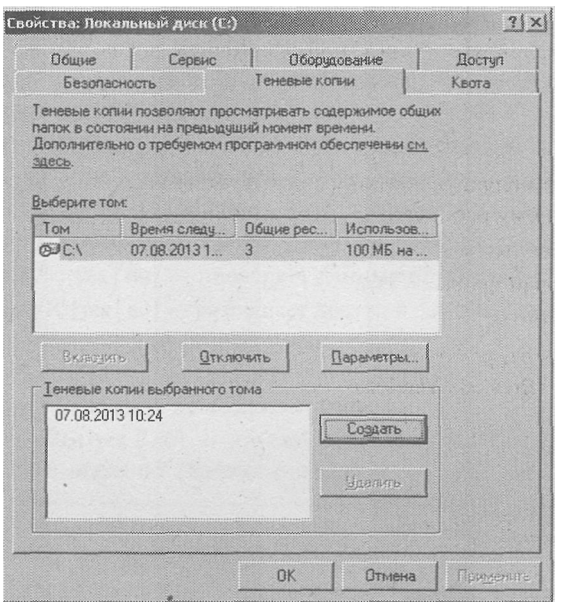


Рис. 7-8. Вкладка *Теневые копии* в окне свойств тома

Внимание! Если щелкнуть **Отключить (Disable),** все копии, созданные службой VSS, будут удалены. Решите, что лучше: отключить VSS для какого-либо тома или изменить расписание так, чтобы предотвратить создание новых теневых копий.

По умолчанию сервер создает копии общих папок с понедельника по пятницу в 7:00 и в полдень. При этом для кэширования теневых копий используется 10 % пространства на том диске, где находится общая папка.

Следующие параметры можно настроить, щелкнув кнопку **Параметры (Settings)** на вкладке **Теневые копии (Shadow Copies).**

- **Место хранения (Storage volume).** Чтобы повысить производительность (но не избыточность), можно переместить теневое хранилище на другой том. Это нужно сделать, когда никакие теневые копии еще не созданы, в противном случае их придется удалить.
- **Сведения (Details).** Если щелкнуть эту кнопку, откроется одноименную диалоговое окно, где перечислены теневые копии и занимаемое ими пространство.
- **Ограничения хранилища (Storage limits).** Не может быть менее 100 Мб. Когда размер теневой копии превышает указанное ограничение, старые версии файлов удаляют-

ся, освобождая место для новых версий. Оптимальное значение этого параметра зависит от суммарного размера общих папок на томе; частоты изменения файлов, размера этих файлов и количества предыдущих версий, которые нужно хранить. В любом случае до момента удаления самой старой версии из теневого хранилища можно сохранить не более 63 версий файла.

- **Расписание (Schedule).** Позволяет настроить расписание, отражающее график работы пользователей, чтобы гарантировать хранение достаточного количества версий файлов и чтобы место хранения не заполнилось преждевременно, вызвав удаление старых версий. Помните, что, когда создается теневая копия, копируются любые файлы, измененные с момента последнего теневого копирования. Если файлы изменились несколько раз между созданием теневых копий, промежуточные версии будут недоступны.

Работа с теневой копией

Теневые копии общих папок позволяют получить доступ к предыдущим версиям файлов, которые сервер кэширует по заданному расписанию. Это позволит:

- восстановить случайно удаленные файлы;
- восстановить случайно перезаписанный файл;
- сравнить версии файлов во время работы.

Чтобы получить предыдущие версии, откройте окно свойств папки или файла и перейдите на вкладку Предыдущие **версии (Previous Versions),** показанную на рис. 7-9.

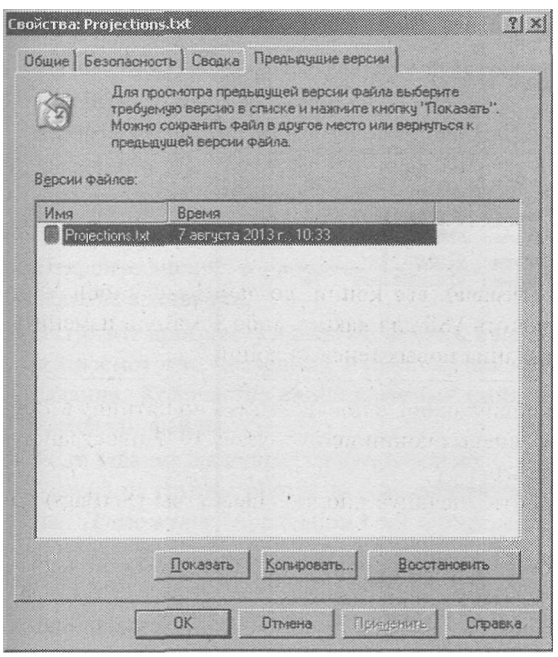


Рис. 7-9. Вкладка *Предыдущие версии* окна свойств общего ресурса

Вкладка **Предыдущие версии** недоступна, если функция **Теневые копии (Shadow Copies)** отключена на сервере или на нем не были сохранены предыдущие версии. Кроме того, она недоступна, если на вашем компьютере не был установлен клиент теневого копиро-

вания. Файл клиента находится в папке %Systemroot%\System32\Clients\Twclient\x86 на системе Windows Server 2003. Файл Windows Installer (.msi) можно развернуть, используя групповую политику, пакет SMS или электронную почту. Наконец, вкладка **Предыдущие версии (Previous Versions)** доступна только при обращении к свойствам файлов через общую папку. Если файл хранится на локальном диске, вы не увидите вкладку **Предыдущие версии,** даже если файл является общим и служба VSS включена. Пример см. в лабораторной работе далее.

Кнопка **Восстановить (Restore)** позволяет восстановить файл в предыдущее размещение, а кнопка **Копировать (Copy)** — в новое.

Подготовка к экзамену В отличие от полноценной операции восстановления, теневое копирование не поддерживает восстановление параметров безопасности предыдущих версий файлов. Если вы восстанавливаете файл в исходное размещение и он там уже существует, предыдущая версия заменяет текущую со своими разрешениями. Когда предыдущая версия файла копируется в другое место или восстанавливается в исходное, но такого файла там нет, предыдущая версия наследует разрешения от родительской папки.

Если файл удален, вы, очевидно, не сможете открыть окно его свойств и перейти на вкладку **Предыдущие версии (Previous Versions).** Вместо этого откройте вкладку **Предыдущие версии** в окне свойств родительской папки и найдите предыдущую версию папки, которая содержит нужный файл. Щелкните кнопку **Показать (View).** Откроется окно, отображающее содержимое папки на момент создания теневой копии (рис. 7-10). Щелкните файл правой кнопкой, выберите **Копировать (Copy)** и вставьте файл в нужную папку.

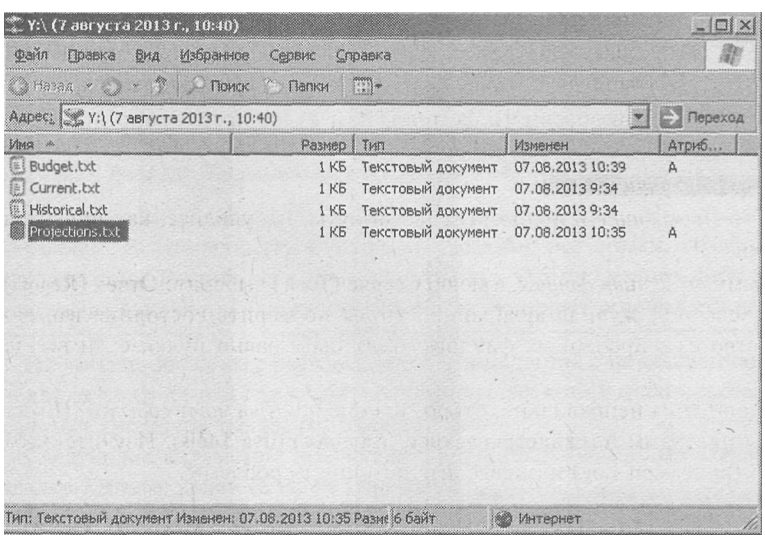


Рис. 7-10. Содержимое родительской папки на вкладке *Предыдущие версии*

Как видите, теневое копирование является полезным дополнением к набору средств для управления файловыми серверами и общими данными. С помощью VSS можно защитить наборы данных в состоянии на запланированные моменты времени. Администраторы и пользователи могут восстанавливать удаленные или поврежденные файлы. а также сравнивать файлы с предыдущими версиями. По мере заполнения кэша VSS старые версии заменяются новыми теневыми копиями.

Если сервер вышел из строя или пользователю нужны данные, которые уже недоступны на вкладке **Предыдущие версии (Previous Versions),** их можно восстановить из архива. Хотя VSS улучшает управление общими файлами и надежность их хранения, альтернативы тщательно спланированной и проверенной процедуре резервного копирования нет.

Лабораторная работа. **Дополнительные возможности архивации и восстановления**

На этой лабораторной работе вы составите расписание задания архивации, выполните архивацию из командной строки и настроите теневое копирование общих папок.

Упражнение 1. Составление расписания архивации

1. Запустите программу *Архивация данных* и перейдите на вкладку **Архивация (Backup).**
2. В меню **Задание (Job)** загрузите файл выбора Finance Backup.
3. В поле **Носитель архива или имя файла (Backup Media Or File Name)** введите путь C:\Backup-Everyday.bkf.
4. Щелкните **Архивация (Start Backup).**
5. Щелкните **Дополнительно (Advanced)** и выберите тип архива **Добавочный (Incremental).** Щелкните OK.
6. Щелкните **Расписание (Schedule).**
7. В окне **Указание учетной записи (Set Account Information)** введите свой пароль и щелкните **OK**.
8. Назовите задание «Daily Incremental Backup» (Ежедневная добавочная архивация).
9. Щелкните **Свойства (Properties).** Настройте задание для ежедневного запуска. Настройте время на две минуты вперед, чтобы сразу увидеть результаты этого задания.
10. Завершите настройку запланированного задания. Вам будет предложено повторно ввести пароль.
11. Закройте программу *Архивация данных.*
12. Откройте диск C: в *Проводнике* и подождите две минуты. Вы увидите, как появится задание архивации.
13. Запустите программу *Архивация данных,* в меню **Сервис (Tools)** выберите **Отчет (Report)** и просмотрите последний журнал архивации, чтобы проверить состояние вашего задания. Количество скопированных файлов может быть равно нулю, если вы не изменяли файлы.
14. Если задание выполняется неправильно, откройте консоль *Просмотр событий* (Event Viewer) из группы программ **Администрирование (Administrative Tools).** Изучите журнал *Приложение* (Application Log) и определите источник проблемы.

Упражнение 2. Запуск программы *Архивация данных* из командной строки

Самый простой способ узнать нужные параметры командной строки — составить расписание архивации (см. упражнение 1) и изучить команду, сформированную для запланированного задания.

1. Задустите программу *Архивация данных* и перейдите на вкладку **Запланированные задания (Schedule Jobs).**
2. Щелкните значок в календаре, соответствующий запланированному заданию.

3. Щелкните **Свойства (Properties).**
4. Выделите команду в поле **Выполнить (Run)** и нажмите Ctrl+C, чтобы ее скопировать.
5. Закройте окно **Запланированное задание (Schedule Job)** и программу *Архивация данных*.
6. Откройте окно командной строки.
7. Щелкните меню окна (значок в левом верхнем углу окна командной строки) и в меню **Изменить (Edit)** выберите **Вставить (Paste).** В командную строку будет вставлен вызов Ntbackup со всеми параметрами. Нажмите Enter. Задание архивации будет выполнено.

Примечание Сейчас рекомендуется удалить запланированное задание архивации, чтобы было легче работать с дополнительными заданиями архивации, которые вы запланируете далее. Запустите программу *Архивация данных,* перейдите на вкладку **Запланированные задания (Schedule Jobs)** и в календаре щелкните значок, соответствующий запланированному заданию. Щелкните **Удалить (Delete).**

Упражнение 3. Включение теневого копирования

1. Убедитесь, что к папке C:\Data открыт общий доступ и группа *Все* (Everyone) обладает для нее разрешением общего ресурса *Полный доступ* (Full Control).
2. Откройте папку **Мой компьютер (My Computer).**
3. Щелкните правой кнопкой диск C: и выберите **Свойства (Properties).**
4. Перейдите на вкладку **Теневые копии (Shadow Copies).**
5. Выберите том C: и щелкните **Включить (Enable).**
6. **В** появившемся окне щелкните Да (Yes) для продолжения.

Упражнение 4. Имитация изменений сетевых файлов

1. Откройте папку C:\Data\Finance, а затем файл Current.txt. Измените содержимое файла, сохраните и закройте его.
2. Удалите файл C:\Data\Finance\Projections.txt.

Упражнение 5. Восстановление файлов с помощью вкладки *Предыдущиеверсии*

1. Откройте общий ресурс: в меню **Пуск (Start)** выберите **Выполнить (Run)** и исполните команду `\\server01\data`.

   Примечание При обращении к общей папке важно использовать UNC, а не локальный путь. Вкладка **Предыдущие версии (Previous Versions)** доступна только при подключении к общей папке по сети.

2. Откройте папку Finance.
3. Щелкните файл Current.txt правой кнопкой и выберите **Свойства (Properties).**
4. Перейдите на вкладку **Предыдущие версии (Previous Versions).**
5. Выберите предыдущую версию файла Current.txt.
6. Щелкните **Копировать (Copy),** выберите **Рабочий стол (Desktop)** в качестве целевого размещения и снова щелкните **Копировать (Copy).**
7. Щелкните OK, чтобы закрыть окно свойств.

8. Откройте файл Current.txt на вашем рабочем столе. Вы увидите, что данная его версия не содержит изменений, сделанных в упражнении 4.
9. Вернитесь к папке \\Server01\Data. В этот раз не открывайте папку Finance.
10. Чтобы восстановить удаленный файл Projections.txt, щелкните папку Finance правой кнопкой и выберите **Свойства (Properties).**
11. Перейдите на вкладку **Предыдущие версии (Previous Versions).**
12. Выберите предыдущую версию папки Finance и щелкните **Показать (View).**
13. Откроется окно с содержимым этой папки на момент создания теневой копии.
14. Щелкните файл Projections.txt правой кнопкой и выберите **Копировать (Copy).**
15. Перейдите к окну, где отображается текущее состояние папки \\server01\data.
16. Откройте папку Finance.
17. Вставьте файл Projections.txt в эту папку. Теперь вы восстановили предыдущую версию файла Projections.txt.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. В удаленном филиале работает 20 человек и нет администратора. Доступ к файлам и принтерам обеспечивает система под управлением Windows Server 2003. На ней установлен ленточный накопитель. Вы хотите дать опытному пользователю Scott Bishop полномочия и привилегии для архивации и восстановления этого сервера. Как лучше всего это сделать?
2. Напишите команду, которая полностью архивирует папку C:\Data\Finance в файл Backup.bkf на общем ресурсе с именем Backup на компьютере Server02. Задание архивации должно иметь имя «Backup of Finance Folder». Затем напишите команду, выполняющую добавочную архивацию и дозаписывающую набор архивации в тот же файл и с тем же именем задания архивации.
3. Пользователь удалил файл в общей папке на сервере. Открыв окно свойств папки, пользователь не видит вкладки **Предыдущие версии (Previous Versions).** Что может являться причиной? (Выберите все подходящие варианты.)
   a. Теневое копирование не включено для данной папки.
   b. Теневое копирование не включено для тома на сервере.
   c. Пользователь не имеет разрешения на просмотр кэша теневого копирования.
   d. Клиент теневого копирования не установлен на компьютере пользователя.
   e. Папка находится на томе FAT.

Резюме

- Для архивации и восстановления файлов программой *Архивация данных* или другими средствами архивации необходимо иметь соответствующие права. По умолчанию таким правом обладают группы *Операторы архива* (Backup Operators) и *Администраторы* (Administrators).
- Диалоговое окно **Параметры (Options)** позволяет настроить параметры архивации и восстановления, большинство из которых становятся значениями по умолчанию и управляют работой программы *Архивация данных* и команды Ntbackup. Эти настройки могут быть перекрыты параметрами конкретного задания, настраиваемыми в окне

Дополнительные параметры архивации (Advanced Backup Options), или параметрами командной строки.

- Команда Ntbackup и полный набор параметров позволяют выполнять задание архивации из командной строки или из пакетного файла.
- Задания архивации могут автоматически выполняться по расписанию во время низкой нагрузки на сервер.
- Служба VSS (Volume Shadow Copy Service) позволяет пользователю получить доступ к предыдущим версиям файлов и папок в сетевом общем ресурсе. Благодаря записи предыдущих версий пользователи могут восстановить удаленный или поврежденный файл или сравнить версии файлов.

Пример из практики

Вам поручили настроить стратегию архивации для общей папки финансового отдела. Архивация должна выполняться автоматически рано утром, поскольку рабочие смены пользователей начинаются в 4:00 и заканчиваются в 24:00 с понедельника по пятницу. Файлы в папке меняются часто: одна половина — раз в неделю, другая — практически ежедневно. Вам сообщили, что в случае отказа жесткого диска сервера, время простоя дорого обойдется компании, поэтому восстановления должно быть максимально быстрым.

1. Зная, что половина файлов меняются почти каждый день, и восстановление должно быть максимально быстрым, какой тип архивации вы выберите для запуска по ночам?

   Подумайте об обычной архивации. Изменения в общей папке происходят настолько часто, что преимущество разностной или добавочной архивации по сравнению с обычной составит менее 50 %. Кроме того, обычная архивация обеспечивает самое быстрое восстановление, поскольку набор архивации содержит все необходимые файлы.
2. Вы настраиваете обычную ежедневную архивацию, чтобы она запускалась в полночь, когда завершается последняя рабочая смена. К сожалению, вы обнаружили, что задание архивации не успевает завершиться к 4:00, когда начинается утренняя смена. Как следует изменить стратегию архивации? \

   Раз в неделю выполняйте обычную архивацию, например в воскресенье, а в течение недели каждую ночь формируйте разностные архивы. Хотя можно применять и разностную, и добавочную архивации, разностная архивация обеспечивает более быстрое восстановление по сравнению с добавочной, поскольку последний разностный набор архивации включает все файлы, измененные с момента обычной архивации.

Упражнение 1. Создание данных для примера

1. Откройте папку **Мой компьютер (My Computer),** а затем диск C:.
2. Удалите папку Data. Появится запрос на подтверждение удаления. Вам также сообщат, что папка общая и ее удаление приведет к удалению общего ресурса. Подтвердите, что вы поняли предупреждение, и продолжите.
3. Из командной строки и исполните команду cd c:\.
4. Исполните команду `createfiles.bat`.

Примечание Если вы не создали файл createfiles.bat в упражнении 1 занятия 1, выполните шаги 1–3 упражнения 1, чтобы создать соответствующий сценарий.

Упражнение 2. Составление расписания архивации

Настройте следующие задания архивации и составьте для них расписание. Если вам нужна помощь для выполнения этих задач, см. инструкции из лабораторных работ в занятиях 1 и 3.

- Обычная архивация папки C:\Data\Finance в файл C:\BackupFinance.bkf (заменяющий носитель) должна выполняться каждое воскресенье в 21:00.
- Разностная архивация той же папки в тот же файл (дозапись на носитель) должна выполняться в 00:15 со вторника по субботу (то есть по ночам с понедельника по пятницу).

Упражнение 3. Имитация запланированных заданий

Вместо того чтобы ждать вечера воскресенья, когда обычное задание архивации выполнится автоматически, вы выполните его из командной строки.

1. Запустите программу *Архивация данных.*
2. Перейдите на вкладку **Запланированные задания (Schedule Jobs).**
3. Щелкните значок в календаре, соответствующий заданию обычной архивации, которое выполняется в воскресенье ночью.
4. Щелкните **Свойства (Properties).**
5. Выделите команду в поле **Выполнить (Run)** и нажмите Ctrl+C, чтобы ее скопировать.
6. Закройте окно **Запланированное задание (Schedule Job)** и программу *Архивация данных.*
7. Откройте окно командной строки.
8. Щелкните меню окна (значок в левом верхнем углу окна командной строки) **и в** меню **Изменить (Edit)** выберите **Вставить (Paste).** В командную строку будет вставлен вызов Ntbackup со всеми параметрами. Нажмите Enter. Задание архивации будет выполнено.
9. Откройте и измените файл C:\Data\Finance\Projections.txt. Сохраните и закройте его.
10. Повторите шаги 1–8, выполнив из командной строки разностное задание архивации, которое запланировано для выполнения по ночам.

Упражнение 4. Проверка процедуры архивации

1. Запустите программу *Архивация данных.*
2. В меню **Сервис (Tools)** выберите **Отчет (Report).**
3. Откройте два последних отчета архивации и убедитесь, что эти задания завершились успешно. Задание обычной архивации должно было заархивировать четыре файла. Задание разностной архивации должно было заархивировать один файл.
4. Выполните тестовое восстановление в папку C:\TestRestore. Восстановите обычный архив, а затем разностный. Если вам нужна помощь, см. лабораторную работу занятия 2.

Внимание! Помните, что перед выполнением разностного задания необходимо настроить параметры восстановления. Для этого в меню **Сервис (Tools)** выберите **Параметры (Options)** и установите флажок **Всегда заменять файл на компьютере (Always Replace The File On My Computer).** Вам также может потребоваться каталогизировать этот файл, чтобы знать, какие наборы архивации он содержит.

Практикум по устранению неполадок

В 13:00 во вторник пользователь из финансового отдела связался с вами и сообщил, что случайно удалил некоторые файлы из папки Finance. Вы уверены, что процедура архивации, которую вы настроили, поможет восстановить удаленные файлы. Тем не менее вы хотите убедиться, что файлы, измененные с момента последней ночной архивации, не будут перезаписаны.

На этом практикуме вы имитируете похожую ситуацию и затем восстановите потерянные данные.

Упражнение 1. Имитация потери данных

1. Откройте папку C:\Data\Finance.
2. Откройте и измените файл Current.txt. Сохраните и закройте его.
3. Откройте и измените файл Budget. Сохраните и закройте его.
4. Удалите файлы Historical.txt и Projections.txt.

Упражнение 2. Планирование восстановления

Просмотрите стратегию архивации, которую вы разработали при разборе сценария: обычная архивация — по ночам в воскресенье, разностная — ночью в будни.

1. Как восстановить потерянные данные?

   Обычная резервная копия включает все выбранные файлы. Это базовая линия, с которой вы начинаете восстановление потерянных данных. Разностная резервная копия содержит все файлы, измененные после обычной архивации. После восстановления обычного архива вы можете восстановить самый свежий разностный архив. Помните, однако, что некоторые файлы (Budget и Current) были изменены пользователями уже после ночной разностной архивации.

2. Как избежать перезаписи этих новых файлов версиями из набора архивации?

   Вкладка **Параметры восстановления (Restore Options)** в окне **Параметры (Options)** позволяет указать способ записи файлов в целевое размещение. Вы можете указать программе *Архивация данных* заменять файлы на диске, только если они старее файлов в наборе архивации. При этом более свежие файлы останутся.

Упражнение 3. Восстановление данных

1. Запустите программу *Архивация данных.*
2. В меню **Сервис (Tools)** выберите **Параметры (Options).**
3. Перейдите на вкладку **Восстановление (Restore).**

4. Настройте параметры восстановления, чтобы новые файлы остались нетронутыми: выберите **Заменять файл на компьютере, только если он старее (Replace The File On Disk Only If The File On Disk Is Older)** и закройте окно **Параметры (Options).**
5. Выберите архивный носитель, который содержит обычную и разностную резервные копии.
6. Восстановите обычный архив в исходное размещение.
7. Восстановите разностный архив в исходное размещение.
8. Откройте файлы Current и Budget. Поскольку эти файлы более свежие, чем файлы в наборе архивации, согласно настроенным вами параметрам восстановления, они должны включать изменения, которые вы внесли в упражнении из раздела «Пример из практики».

Резюме главы

- Для архивации и восстановления файлов программой *Архивация данных* или другими средствами архивации необходимо иметь соответствующие права. По умолчанию таким правом обладают группы *Операторы архива* (Backup Operators) и *Администраторы* (Administrators).
- Программа *Архивация данных* позволяет архивировать и восстанавливать данные из локальных и удаленных папок в локальные файлы, на магнитную ленту, сменный носитель или в общие папки на удаленных серверах. Нельзя архивировать на перезаписываемые носители CD или DVD.
- Стратегия архивации, как правило, начинается с обычной и следующей за ней добавочной или разносной архивацией. Добавочные задания ускоряют архивацию, а разностные — восстановление. Задания могут выполняться по расписанию в периоды низкой нагрузки.
- Копирующая и ежедневная архивация применяются для копирования файлов без вмешательства в расписание архивации.
- Программа *Архивация данных* позволяет восстанавливать данные в исходное или альтернативное размещение. Последний способ полезен для проверки процедур восстановления. На вкладке **Восстановление (Restore)** в окне **Параметры (Options)** можно контролировать, какие файлы будут заменены при восстановлении.
- Команда Ntbackup и полный набор параметров позволяют выполнять задание архивации из командной строки или из пакетного файла.
- Служба VSS (Volume Shadow Copy Service) позволяет пользователю получить доступ к предыдущим версиям файлов и папок в сетевом общем ресурсе. Благодаря записи предыдущих версий пользователи могут восстановить удаленный или поврежденный файл или сравнить версии файлов.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Перечислите, какие права и членство в каких группах необходимы для выполнения операций архивации или восстановления.
- Создайте стратегию архивации с учетом всех требований, включая время, которое потребуется для архивации и восстановления.
- Уясните, как восстанавливать данные в различных условиях, включая полную или частичную потерю данных. Сопоставьте время потери данных с расписанием архивации, чтобы определить, какие наборы архивации нужно восстановить. Определите, в каком порядке должны восстанавливаться наборы архивации, и как должны заменяться существующие файлы на жестком диске.
- Составьте расписание и настройте параметры архивации.
- Включите теневое копирование общих папок и восстановите данные с помощью вкладки **Предыдущие версии (Previous Versions)** в окне свойств файла или папки.

Основные термины

Копирующая (copy), ежедневная (daily), разностная (differential), добавочная (incremental) и **обычная (normal) архивация.** Эти пять типов архивации определяют файлы, подлежащие резервному копированию, по определенному условию. *Копирующая* и *обычная* архивируют все файлы; *ежедневная* архивирует файлы, измененные за указанную дату; *разностная* и *добавочная* архивируют файлы, для которых задан атрибут **Архивный (Archive).** *Обычная* и *добавочная* архивация также сбрасывают атрибут архивирования.

Атрибут архивирования ~ archive attribute — атрибут, который устанавливается при создании или изменении файла. Добавочная и разностная архивация копирует файлы с установленным атрибутом архивирования. Добавочная архивация сбрасывает атрибут.

Служба VSS (Volume Shadow Copy Service) — служба Windows Server 2003, позволяющая архивировать открытые или заблокированные для использования файлы.

Пулы носителей: неопознанные (unrecognized), импортированные (import), свободные (free),,архивные **(backup).** Представляют четыре категории сменных носителей. Ntbackup архивирует только на носители в свободном или архивном пулах.

Теневые копии общих папок ~ shadow copies of shared folders — функция Windows Server 2003, которая после настройки на сервере и клиентских компьютерах позволяет пользователям извлекать предыдущие версии файлов без вмешательства администратора.

Вопросы и ответы

Занятие 1. Закрепление материала

1. Какие из следующих размещений нельзя использовать для хранения резервной копии системы Windows Server 2003?
   a. Локальный ленточный накопитель.
   b. Локальный привод CD-RW.

c. Локальный жесткий диск.
d. Общая папка на удаленном сервере.
e. Локальный привод DVD+R.
f. Локальный сменный диск.
g. Ленточный накопитель на удаленном сервере.

Правильный ответ: b, e, g.

2. Вам поручено каждый вечер создавать резервные копии файлового сервера Windows Server 2003. Вы вручную выполняете обычную архивацию, затем составляете расписание, по которому задание архивации запускается каждый вечер в течение следующих двух недель. Какой из типов архивации завершится быстрее?

a. Обычная.
b. Разностная.
c. Добавочная.
d. Копирующая.

Правильный ответ: c.

3. Вам поручено каждый вечер создавать резервные копии файлового сервера Windows Server 2003. Вы вручную выполняете обычную архивацию, затем составляете расписание, по которому задание архивации запускается каждый вечер в течение следующих двух недель. Какой из типов архивации обеспечивает самый простой способ восстановления данных?

a. Обычная.
b. Разностная.
c. Добавочная.
d. Ежедневная.

Правильный ответ: a.

4. Вам поручено каждый вечер создавать резервные копии файлового сервера Windows Server 2003. Вы выполняете обычную архивацию, а на следующий день решаете, какую архивацию выбрать: добавочную или разностную. Будут ли эти задания архивации отличаться по размеру или скорости выполнения? Если бы на следующий день на сервере произошел сбой, одинаково эффективными были бы операции восстановления?

Правильный ответ: во второй вечер можно было бы использовать любой тип архивации. Обычная архивация сбрасывает атрибут архивирования. Как добавочная, так и разностная архивация во второй вечер скопируют все файлы, созданные или измененные за второй день. Содержимое обоих заданий будет одинаковым. Так что и на третий день разницы в операциях восстановления не будет: вам пришлось бы сначала восстановить обычный архив, а затем архив, созданный во второй вечер.

Тем не менее, добавочная и разностная архивации по-разному обрабатывают атрибут архивирования на файлах: добавочная сбрасывает его, а разностная — нет. Таким образом, при следующем резервном копировании разница начнет проявляться. При второй добавочной архивации будут скопированы только файлы, созданные или измененные после первой добавочной архивации. Однако второй разностный архив будет содержать все файлы, созданные или измененные со времени обычной архивации, то есть все файлы, уже скопированные в первый разностный архив.

5. Вспомните текст лабораторной работы. Попробуйте спрогнозировать содержимое следующих заданий архивации:
   - backup-normal.bkf;
   - backup-diff-dayl.bkf;
   - backup-diff-day2.bkf;
   - backup-inc-day2.bkf;
   - backup-inc-day3.bkf.

   Есть ли разница между содержимым backup-diff-day2 и backup-inc-day2?

   Правильный ответ:
   - **backup-normal.bkf: Historical, Current, Budget, Projections;**
   - **backup-diff-dayl.bkf: Current;**
   - **backup-diff-day2.bkf: Current and Budget;**
   - **backup-inc-day2.bkf: Current and Budget;**
   - **backup-inc-day3.bkf: Projections.**

   Содержимое backup-diff-day2 и backup-inc-day2 одинаково. Оба типа архивации будут **копировать файлы с установленным атрибутом архивирования. Поскольку в первый день была выполнена обычная архивация, для всех файлов, измененных с первого дня, будет установлен атрибут архивирования.**

Занятие 2. Закрепление материала

1. Пользователь случайно удалил данные из документа Microsoft Word. Обычная архивация выполнялась на сервере вчера вечером. Какой параметр следует выбрать, чтобы восстановить исходный файл?

   a. Не заменять файл на компьютере (Do Not Replace The File On My Computer).

   b. Заменять файл на компьютере, только если он старее (Replace The File On Disk Only If The File On Disk Is Older).

   c. Всегда заменять файл на компьютере (Always Replace The File On My Computer).

   Правильный ответ: c. Файл существует на сервере, но был поврежден. Следует заменить его файлом из набора архивации.

2. Один из руководителей вернулся из деловой поездки. Перед поездкой он скопировал файлы из сетевой папки на жесткий диск своего компьютера. В общей папке хранятся документы других руководителей, которые изменяли свои файлы в его отсутствие. Вернувшись, он скопировал файлы в сетевой ресурс, обновив не столько свои, но и чужие файлы. Другие руководители не были в восторге от того, что их файлы были заменены старыми версиями. К счастью, вчера вечером вы выполнили обычную архивацию этой папки. Какой параметр восстановления следует выбрать?

   a. Не заменять файл на компьютере (Do Not Replace The File On My Computer).

   b. Заменять файл на компьютере, только если он старее (Replace The File On Disk Onl- **If The File On Disk Is Older).**

   c. Всегда заменять файл на компьютере (Always Replace The File On My Computer).

   Правильный ответ: b. Этот параметр не перезапишет файлы, измененные другими руководителями. Дата изменения этих файлов будет больше, чем у файлов в архиве. Тем не менее он восстановит файлы других руководителей, перезаписав старые версии, которые записал в сеть руководитель, вернувшийся из командировки.

Совет Пользователи должны научиться работать с функцией **Автономные файлы (Offline Files),** чтобы избежать таких, довольно типичных, проблем. Эта функция синхронизирует измененные файлы, поэтому в общую папку скопировались бы только файлы, измененные руководителем во время поездки; чужие файлы не изменились бы.

3. Вам нужно протестировать процедуру восстановления на сервере, не повредив производственные копии архивных данных. Какое размещение для восстановления лучше выбрать?
   a. Исходное размещение (Original location).
   b. Альтернативное размещение (Alternate location).
   c. Одну папку (Single folder).
   Правильный ответ: b. Восстановление в альтернативное размещение сохранит структуру папки и файлы, которые были заархивированы. Вы сможете сравнить содержимое целевого размещения с исходными файлами, чтобы убедиться в успехе восстановления.

Занятие 3. Закрепление материала

1. В удаленном филиале работает 20 человек и нет администратора. Доступ к файлам и принтерам обеспечивает система под управлением Windows Server 2003. На ней установлен ленточный накопитель. Вы хотите дать опытному пользователю Scott Bishop полномочия и привилегии для архивации и восстановления этого сервера. Как лучше всего это сделать?
   Правильный ответ: включите пользователя Scott Bishop в группу Операторы архива (Backup Operators). По умолчанию эта группа обладает привилегией архивировать и восстанавливать файлы и папки.
2. Напишите команду, которая полностью архивирует папку C:\Data\Finance в файл Backup.bkf на общем ресурсе с именем Backup на компьютере Server02. Задание архивации должно иметь имя «Backup of Finance Folder». Затем напишите команду, выполняющую добавочную архивацию и дозаписывающую набор архивации в тот же файл и с тем же именем задания архивации.
   Правильный ответ:

```
ntbackup backup "c:\data\finance" /J "Backup of Finance Folder" /F
"\\server02
\backup\backup.bkf"

ntbackup backup "c:\data\finance" /J "Backup of Finance Folder" /F
"\\serverO1
\backup\backup.bkf" /a /m incremental
```

3. Пользователь удалил файл в общей папке на сервере. Открыв окно свойств папки, пользователь не видит вкладки **Предыдущие версии (Previous Versions).** Что может являться причиной? (Выберите все подходящие варианты.)
   a. Теневое копирование не включено для данной папки.
b. Теневое копирование не включено для тома на сервере.

c. Пользователь не имеет разрешения на просмотр кэша теневого копирования.

d. Клиент теневого копирования не установлен на компьютере пользователя.

Правильный ответ: b, d. Теневое копирование включается на уровне тома, а не папки. Когда теневое копирование включено, любой пользователь, на компьютере которого установлен клиент этой службы, сможет увидеть вкладку Предыдущие версии (Previous Versions) в окне свойств измененного файла или папки. Теневое копирование поддерживается на томах FAT и NTFS.

ГЛАВА 8

Принтеры

Темы экзамена

- Мониторинг очередей печати.
- Мониторинг файловых серверов и серверов печати при помощи оснасток *Диспетчер задач* (Task Manager), *Просмотр событий* (Event Viewer) и *Системный монитор* (System Monitor).

В этой главе

Microsoft Windows Server 2003 предоставляет мощный набор функций поддержки корпоративных служб печати. В этой главе рассказывается о настройке и конфигурировании принтеров в Windows Server 2003, взаимодействии принтеров с Active Directory, подключении клиентов к сетевым принтерам, а также мониторинге и устранении неполадок служб печати. Вы научитесь администрировать локальные', сетевые и интернет-принтеры и конфигурировать их для обеспечения максимальной гибкости и безопасности.

Прежде всего

Здесь рассматриваются практические и теоретические вопросы, связанные с администрированием принтеров в Windows Server 2003. Предполагается, что у вас есть как минимум 18-месячный опыт работы с Active Directory и MMC (Microsoft Management Console). Но, поскольку многие переходят на Windows Server 2003 из других сред управления принтерами, например Novell NetWare, и терминология в этой области претерпела незначительные изменения, первое занятие посвящено обзору основных принципов конфигурирования принтеров. Занятия 2 и 3 базируются на этих принципах и служат для подготовки к всестороннему и гибкому администрированию, поддержке, мониторингу и устранению неполадок принтеров в среде Windows Server 2003.

Оптимальный вариант — наличие принтера и двух компьютеров (Windows Server 2003 и клиент Windows 2000 Professional или XP), однако вы сможете выполнять упражнения и без принтера, с использованием одного компьютера.

Для изучения материалов этой главы вам потребуются:

- компьютер под управлением Microsoft Windows Server 2003 Standard или Enterprise, установленный как ServerOl и настроенный в качестве контроллера домена contoso.com;
- ОП первого уровня *Группы безопасности* (Security Groups);
- консоль *Active Directory — пользователи и компьютеры* или пользовательская консоль с такой оснасткой.

Занятие 1. **Установка и настройка принтеров**

Компьютер под управлением Windows Server 2003 позволяет управлять принтерами, подключенными к нему локально или по сети, и предоставлять к ним доступ для локальных приложений или пользователей на любой клиентской платформе, включая предыдущие версии Windows, а также Netware, UNIX или Apple Macintosh. На этом занятии вы познакомитесь с базовыми понятиями и терминологией и получите навыки настройки принтеров в Windows Server 2003.

Изучив материал этого занятия, вы сможете:

- ✓ понимать модель и терминологию, используемую при печати в Windows;
- ✓ устанавливать логический принтер на сервере печати для принтера, подключенного по сети;
- ✓ готовить сервер печати к обслуживанию клиентов, включая и компьютеры с предыдущими версиями Windows;
- ✓ подключать клиент печати к логическому принтеру на сервере печати;
- ✓ управлять заданиями печати.

Продолжительность занятия — около 15 минут.

Понятие модели принтеров в Windows Server 2003

Windows Server 2003 и все предыдущие версии поддерживают два типа принтеров.

- **Локально подключенные принтеры** — принтеры, подключенные к физическому порту сервера печати, обычно к USB или параллельному порту.
- **Сетевые принтеры** — принтеры, подключенные к сети, а не к физическому порту Сетевой принтер — это узел в сети, серверы печати могут обращаться к нему по сетевому протоколу, например TCP/IP.

Принтеры обоих типов представлены на сервере печати как логические. *Логический принтер* (logical printer) задает характеристики и поведение принтера. Он содержит драйвер, параметры принтера, значения параметров печати по умолчанию и другие свойства, управляющие способом обработки и отправки на выбранный принтер заданий печати. Такая виртуализация до уровня логического принтера позволяет очень гибко конфигурировать службы печати.

Примечание В предыдущих версиях Windows и в ранних версиях документации принтер назывался «печатающим устройством», а логический принтер — «принтером».

Предусмотрено два способа реализации печати на сетевые принтеры. Один из них — установить логические принтеры на всех компьютерах и подключить их напрямую к сетевому принтеру. В этой модели отсутствует сервер печати; каждый компьютер поддерживает собственные параметры, процессор печати и очередь заданий. Когда пользователи просматривают очередь печати, они видят только собственные задания. Кроме того, сообщения об ошибках выдаются только на компьютере, выполняющем текущее задание. Наконец, вся обработка задания печати ведется локально на компьютере пользователя, вместо переноса нагрузки от клиента на сервер печати.

Из-за этих серьезных недостатков наиболее типичная конфигурация принтеров на предприятии предполагает использование трехсторонней модели: собственно физический принтер, размещенный на сервере печати, логический принтер плюс клиенты печати, подключенные к логическому принтеру сервера. На этом занятии рассматривается только такая структура, хотя обсуждаемые понятия и практические вопросы применимы и к другим конфигурациям печати.

Использование сервера печати дает следующие преимущества:

- логический принтер на сервере печати определяет параметры принтера и управляет его драйверами;
- логический принтер создает одну очередь печати, доступную для просмотра на всех клиентских компьютерах, поэтому пользователи могут видеть свои задания печати в общей очереди;
- сообщения об ошибках, например уведомления о том, что бумага закончилась или застряла, отправляются всем клиентам, так что все пользователи знают состояние принтера;
- большинство приложений и драйверов печати перекладывают с клиентского компьютера некоторую (порой значительную) часть нагрузки по обработке заданий печати на сервер: по щелчку кнопки **Печать (Print)** задание отправляется на сервер печати, и пользователь может продолжать работу.
- функции безопасности, аудита, мониторинга и ведения журнала централизованы.

Установка принтера в Windows Server 2003

Чаще всего принтеры управляются из окна **Принтеры и факсы (Printers And Faxes),** объединяющего доступ к функциям принтеров и факсов. *Мастер установки принтеров* (Add Printer Wizard) помогает настроить принтер. Наиболее важные этапы настройки таковы.

- **Локальный или сетевой принтер (Local Or Network Printer).** Эта страница показана на рис. 8-1. В ходе настройки принтера на компьютере Windows Server 2003 термины «локальный принтер» и «сетевой принтер» имеют несколько иные от общепринятых значения. *Локальный принтер* — это логический принтер, обслуживающий принтер, подключенный напрямую к серверу, либо изолированный подключенный к сети принтер. Когда в *Мастере установки принтеров* вы создаете локальный принтер, щелкая **Локальный принтер (Local Printer Attached To This Computer),** сервер может открыть совместный доступ к нему для других клиентов сети. *Сетевой принтер* — это логический принтер, подключающийся к принтеру, напрямую подсоединенному к другому компьютеру, либо к принтеру, управляемому другим сервером печати. Пользовательский интерфейс может ввести в заблуждение, поэтому помните, что в общепринятой реализации сервер печати хранит локальные принтеры (неважно, подключен ли аппаратный принтер напрямую к компьютеру или к сети), а рабочие станции создают подключения сетевых принтеров к общему логическому принтеру сервера.

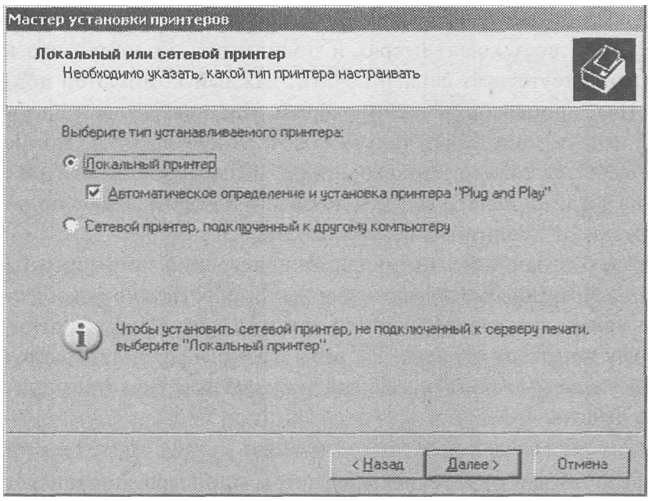


Рис. 8-1. Страница *Локальный или сетевой принтер* мастера установки принтеров

- **Выбор порта принтера.** При создании локального принтера на сервере печати мастер просит указать порт, к которому подсоединен принтер. Существующий порт (локальный, например LPT1, или сетевой, заданный IP-адресом) можно выбрать в раскрывающемся списке **Использовать имеющийся порт (Use The Following Port).** Для создания нового порта щелкните **Создать новый порт (Create A New Port),** выберите **Standard TCP/IP Port** и щелкните Далее (Next). Откроется окно *Мастера добавления стандартного TCP/IP порта принтера* (Add Standard TCP/IP Printer Port Wizard). По щелчку Далее (Next) система предлагает задать IP-адрес или DNS-имя принтера. После добавления порта вы вернетесь к *Мастеру установки принтеров.*
- **Установка программного обеспечения принтера.** Если Plug and Play не определяет и не устанавливает нужный принтер автоматически, вы можете выбрать его из обширного списка, сгруппированного по изготовителям. Если нужного принтера в списке нет, щелкните **Установить с диска (Have Disk)** и установите драйверы принтера, предоставленные изготовителем.
- **Имя принтера** и **имя общего ресурса.** Хотя Windows Server 2003 поддерживает длинные имена принтеров и имена общих ресурсов, включая пробелы и специальные символы, рекомендуется по возможности задать простое и короткое имя. Полное имя, включающее имя сервера (например \\Server01\PSCRIPT), не должно превышать 32 символов.

Имя общего ресурса и принтера отображаются и используются во многих окнах пользовательского интерфейса Windows. Хотя имя общего ресурса не зависит от имени принтера и может от него отличаться, во избежание путаницы часто используется одно имя.

Настройка свойств принтера

После установки логического принтера можно настроить множество его свойств в диалоговом окне **Свойства (Properties),** показанном на рис. 8-2. Вкладка **Общие (General)** позволяет настроить имя, размещение принтера и записать комментарии; все эти параметры были изначально заданы при работе с *Мастером установки принтеров.*

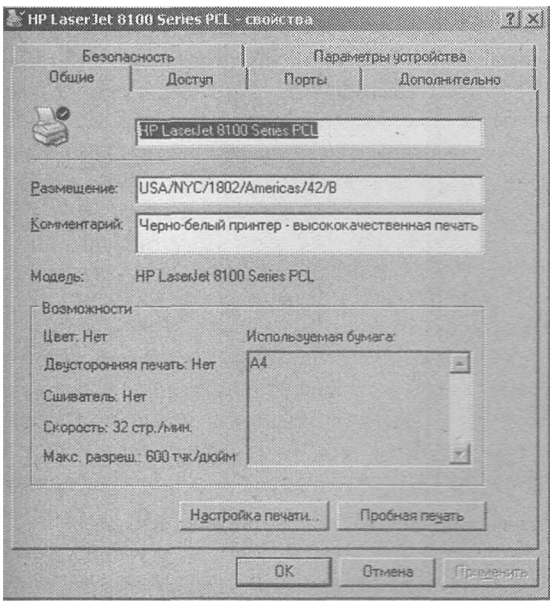


Рис. 8-2. Вкладка *Общие* диалогового окна свойств принтера

Вкладка **Доступ (Sharing),** показанная на рис. 8-3, позволяет указать, является ли логический принтер общим, то есть доступным, остальным клиентам в сети, и публикуется ли он в каталоге Active Directory. По умолчанию общие принтеры публикуются в каталоге, чтобы пользователям было удобнее к ним подключаться.

Примечание На вкладке **Доступ (Sharing)** можно запретить общий доступ к принтеру, например, если нужно перевести принтер в автономный режим и запретить пользователям доступ к нему.

В ходе настройки принтера Windows Server 2003 загружает на сервер печати драйверы для клиентов Windows Server 2003, XP и 2000. Для каждой платформы необходим свой драйвер. Если к общему логическому принтеру будут подключаться с других платформ, установите соответствующие драйверы на сервере, чтобы клиенты Windows загружали их автоматически при подключении. Иначе будут выдаваться сообщения о необходимости установки правильных драйверов для каждого клиента.

На вкладке **Доступ (Sharing)** в окне свойств щелкните **Дополнительные драйверы (Additional Drivers),** чтобы поместить на сервер печати драйверы для версий ОС, вышедших до Windows 2000. При выборе предыдущей версии Windows сервер запросит драйверы для соответствующей платформы и принтера. Эти драйверы можно получить у изготовителя принтера, иногда они содержатся на установочном компакт-диске предыдущей версии Windows.

Загрузка на сервер драйверов для всех клиентских платформ позволяет централизовать и упростить распространение драйверов. Клиентские компьютеры под управлением Windows NT, 2000, XP и Windows Server 2003 загружают нужный драйвер при первом подключении к общему принтеру, а также проверяют актуальность драйвера и загружают более свежую версию при каждой печати. Для таких клиентов необходимо обновлять драйверы принтера только на сервере печати. Клиентские компьютеры под управлением Windows 9x не проверяют наличие обновленных драйверов, и делать это приходится вручную.

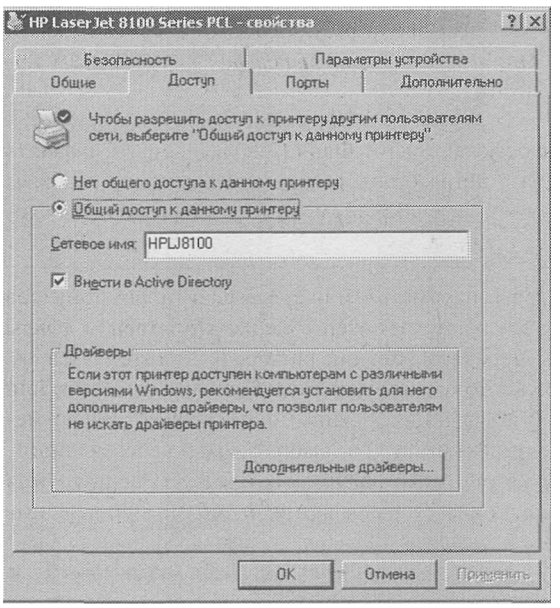


Рис. 8-3. Вкладка *Доступ* диалогового окна свойств принтера

Другие свойства принтера будут рассмотрены далее.

Совет К папкам принтеров на других серверах можно обратиться, просмотрев сетевое окружение или набрав в командной строке *\\имя сервера*. Вы можете скопировать папки **Принтеры и папки (Printer and Faxes)** на доступных серверах в аналогичную папку на своем компьютере, чтобы упростить управление удаленными принтерами.

Подключение клиентов к принтерам

Принтеры, настроенные на сервере печати как логические, могут совместно использоваться другими системами в сети. На этих системах также потребуется установить логические принтеры, представляющие сетевой принтер.

Конфигурирование клиента печати можно выполнять несколькими способами, в том числе с помощью *Мастера установки принтеров,* который запускается из папки **Принтеры и факсы (Printers And Faxes),** либо из окна **Печать (Print),** которое есть практически во всех программах Microsoft, включая Internet Explorer и *Блокнот* (Notepad). На странице **Локальный или сетевой принтер (Local Or Network Printer)** выберите **Сетевой принтер, подключенный к другому компьютеру (A Network Printer Or A Printer Attached To Another Computer).** При появлении запроса на ввод имени принтера вы можете выполнить поиск в Active Directory, ввести путь UNC вида *\\имя_сервера\имя_общего_ресурсапринтера* или URL принтера, либо воспользоваться функцией обзора.

Один из наиболее эффективных способов настройки клиентов печати — поиск принтера в Active Directory. На странице **Укажите принтер (Specify A Printer)** мастера установки принтеров выберите **Найти принтер в Active Directory (Find A Printer In The Directory)** и щелкните **Далее (Next).** Откроется диалоговое окно **Найти принтер (Find Printers),** показанное на рис. 8-4, где вы можете задать условие поиска, в том числе имя принтера, его размещение, модель и характеристики. В условии можно использовать метасимво-

лы. Щелкните **Найти (Find Now),** и просмотрите набор результатов. Выберите нужный принтер и щелкните OK. После этого *Мастер установки принтеров* поможет вам настроить остальные параметры конфигурации.

Совет Вы можете сохранить результаты поиска: в меню **Файл (File)** выберите **Сохранить условия поиска (Save Search).** Будучи администратором, вы можете создавать и сохранять результаты поиска на рабочие столы пользователей, чтобы им было проще находить предварительно заданные группы принтеров.

Логический принтер включает драйверы, параметры и очередь печати для принтера на выбранном порте. Когда вы дважды щелкаете принтер в папке **Принтеры и факсы (Printers And Faxes),** открывается окно с перечнем заданий в очереди принтера. Щелкнув правой кнопкой любое задание, можно приостановить, возобновить, отменить или перезапустить его. Из меню **Принтер (Printer)** также можно приостановить или отменить все задания печати, просмотреть свойства принтера, выбрать его в качестве принтера по умолчанию, а также перевести в автономный режим. Возможность выполнения каждого из этих действий, разумеется, зависит от разрешений в таблице управления доступом (ACL) для принтера.

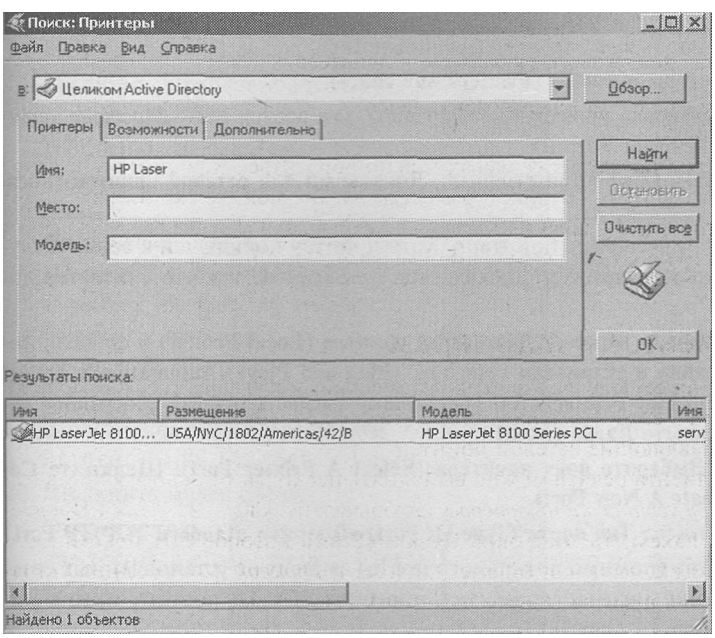


Рис. 8-4. Диалоговое окно *Поиск: Принтеры*

Если вы работаете с Windows Server 2003 или Windows XP со стандартным меню **Пуск (Start),** вместо *Мастера установки принтеров* для настройки клиента печати можно сделать следующее.

1. Щелкните **Пуск (Start),** а затем **Поиск (Search).**
2. На панели **Помощник по поиску (Search Companion)** щелкните **Другие параметры поиска (Other Search Options),** затем **Принтеры, компьютеры или людей (Printers, Computers, Or People),** после чего выберите **Принтер в сети (A Printer On The Network).**

3. Раскроется окно **Поиск: Принтеры (Find Printers),** позволяющее найти нужный принтер по различным условиям.
4. Задав требуемое условие, щелкните **Найти (Find Now).**

Лабораторная работа. **Установка и настройка принтера**

На этой лабораторной работе вы настроите логический принтер на сервере печати и имитируете подключение клиента к общему принтеру. Затем вы отправите задание печати на этот принтер.

Для выполнения упражнений достаточно одного компьютера, но если у вас есть принтер, подключенный к Server01 или к сети, и второй компьютер, настроенный в качестве клиента печати, используйте их.

Упражнение 1. Добавление локального принтера и настройка общей печати

В этом упражнении вы добавите логический принтер на Server01 с помощью *Мастера установки принтеров.* Принтер будет подключаться к сетевому принтеру HP LaserJet 8100 по IP-адресу 10.0.0.51. Для выполнения этого упражнения не требуется аппаратный принтер.

1. Войдите на ServerOl как *Администратор* (Administrator).
2. Откройте папку **Принтеры и факсы (Printers And Faxes).**
3. Дважды щелкните **Установка принтера (Add Printer).** Откроется окно *Мастера установки принтеров* (Add Printer Wizard).
4. Щелкните **Далее** (Next). Откроется страница **Локальный или сетевой принтер (Local Or Network Printer).**

   Вас попросят указать размещение принтера. Хотя принтер подключен к сети, обслуживающий его логический принтер добавляется на ServerOl, так что считается локальным.
5. Убедитесь, что вы выбрали вариант **Локальный принтер (Local Printer)** и флажок **Автоматическое определение и установка принтера «Plug and Play» (Automatically Detect And Install My Plug And Play Printer)** снят (поскольку вы настраиваете фиктивное устройство), затем щелкните **Далее** (Next).
6. Откроется страница **Выберите порт принтера (Select A Printer Port).** Щелкните **Создать новый порт (Create A New Port).**
7. **В** раскрывающемся списке **Тип порта (Type Of Port)** выберите **Standard TCP/IP Port.** Доступные типы портов (помимо локального порта) зависят от установленных сетевых протоколов. В данном случае установлен протокол TCP/IP, поэтому можно выбрать порт на его основе.
8. Щелкните **Далее (Next).** Откроется окно *Мастера добавления стандартного TCP/IP порта принтера* (Add Standard TCP/IP Printer Port Wizard).
9. Щелкните **Далее** (Next).
10. Введите IP-адрес 10.0.0.51 и оставьте имя порта по умолчанию — IP_10.0.0.51.
11. Щелкните **Далее** (Next).

    Поскольку принтер физически не подключен к сети по этому адресу, пройдет некоторое время, пока мастер будет пытаться найти и идентифицировать его. Кроме того, вас попросят указать тип сетевого интерфейса.
12. В качестве типа устройства выберите Hewlett Packard Jet Direct.

13. Щелкните **Далее** (Next), а затем **Готово (Finish).** *Мастер добавления стандартного TCP/IP порта принтера* закроется, и вы вернетесь к *Мастеру установки принтеров*. Мастер попросит вас указать изготовителя и модель принтера. Добавьте принтер HP LaserJet 8100 Series PCL.

Совет Список принтеров отсортирован в алфавитном порядке. Если вы не можете найти имя требуемого принтера, убедитесь, что ищете в нужном месте.

14. В списке **Изготовитель (Manufacturer)** щелкните HP; в списке **Принтеры (Printers)** выберите HP LaserJet 8100 Series PCL и щелкните Далее (Next).
Откроется страница **Назовите ваш** принтер **(Name Your Printer).** По умолчанию имя в поле **Имя принтера (Printer Name)** совпадает с названием модели — HP LaserJet 8100 Series PCL. Имя принтера должно соответствовать правилам именования, принятым в вашей организации. Здесь — HPLJ8100.
15. Введите HPLJ8100 и щелкните **Далее** (Next).
Откроется страница **Использование общих принтеров (Printer Sharing)** с предложением активировать совместный доступ к принтеру. Имя общего ресурса также должно соответствовать правилам именования, принятым в вашей организации. Как уже упоминалось, UNC-путь (вида *\\имя_сервера\имя_общего_ресурса_сервера)* недолжен быть длиннее 32 символов.
16. Убедитесь, что установлен переключатель **Имя общего ресурса (Share Name).**
17. **В** текстовом поле рядом с переключателем **Имя общего ресурса (Share Name)** введите HPLJ8100, затем щелкните Далее (Next).
Откроется страница **Размещение и комментарий (Location And Comment).**

Примечание *Мастер установки принтеров* выводит сведения из полей **Размещение (Location)** и **Комментарий (Comment),** когда пользователь ищет принтер в Active Directory. Вводить эту информацию необязательно, однако она помогает пользователям найти принтер.

18. В текстовом поле **Размещение (Location)** введите USA/NYC/1802Americas/42/B.
19. В текстовом поле **Комментарий (Comment)** введите Black and White Output Laser Printer-High Volume.
20. Щелкните **Далее (Next).**
Откроется окно **Напечатать пробную страницу (Print Test Page).** Успешно напечатанная тестовая страница подтверждает, что принтер настроен правильно.
21. Выберите **Нет** (No), поскольку принтера физически нет, затем щелкните **Далее** (Next). Откроется последняя страница *Мастера установки принтеров,* содержащая сводку по всем параметрам установки принтера.
22. Проверьте правильность параметров установки и щелкните **Готово (Finish).**
Значок принтера появится в окне **Принтеры и факсы (Printers And Faxes).** Заметьте: Windows Server 2003 отображает открытую ладонь под значком принтера. Это означает, что принтер является общим. Также обратите внимание на флажок рядом с именем принтера, означающий, что это принтер по умолчанию на сервере печати.
23. Не закрывайте окно **Принтеры и факсы (Printers And Faxes),** поскольку оно потребуется для выполнения следующего упражнения.

Упражнение 2. Подключение клиента к принтеру

Если у вас есть второй компьютер, на нем также нужно установить принтер, подключающийся к общему принтеру на ServerOl. На этой лабораторной работе необходим только один компьютер (ServerOl), но вы можете имитировать подключение клиента печати к логическому принтеру сервера.

1. Откройте папку **Принтеры и факсы (Printers And Faxes).**
2. Запустите *Мастер установки принтеров* и щелкните **Далее** (Next).
3. На странице **Локальный или сетевой принтер (Local Or Network Printer)** выберите **Сетевой принтер, подключенный к другому компьютеру (A Network Printer, Or A Printer Attached To Another Computer),** затем щелкните **Далее** (Next).
4. Убедитесь, что выбран вариант **Найти принтер в Active Directory (Find A Printer In The Directory),** и щелкните **Далее** (Next). Откроется окно **Поиск: Принтеры (Find Printers).**
5. **В** поле **Место (Location)** введите *NYC* и щелкните **Найти (Find Now).**
6. **В** перечне результатов выберите принтер HPLJ8100 и щелкните OK.
7. На странице **Принтер по умолчанию (Default Printer)** *Мастера установки принтеров* выберите Да (Yes) и щелкните **Далее** (Next).
8. Щелкните **Готово (Finish).**

   Значок нового принтера не появится в папке **Принтеры и факсы (Printers And Faxes),** так как нельзя создать принтер-клиент для логического принтера на том же компьютере. Если упражнение выполняется на втором компьютере, вы увидите значок нового принтера.

Упражнение 3. Перевод принтера в автономный режим и печать тестового документа

В этом упражнении вы переведете созданный принтер в автономный режим: пока принтер недоступен, отправляемые на него документы помещаются в очередь печати. Это позволит избежать сообщений об ошибках о недоступности печатающих устройств при выполнении следующих упражнений. Иначе Windows Server 2003 будет выводить сообщения об ошибках при попытке отправить документы на фиктивное печатающее устройство, фактически недоступное для компьютера.

1. В окне **Принтеры и факсы (Printers And Faxes)** щелкните правой кнопкой значок HPLJ8100.
2. Выберите **Отложенная печать (Use Printer Offline).** Заметьте: значок станет затемненным, обозначая недоступность принтера, а его состояние будет отображаться как **Не подключен (Offline).**
3. Дважды щелкните значок HPLJ8100. Заметьте: список документов, которые должны быть отправлены на печатающее устройство, пуст.
4. В программе *Блокнот* (Notepad) наберите произвольный текст.
5. Разместите окна *Блокнота* и HPLJ8100 так, чтобы видеть содержимое обоих окон.
6. В меню **Файл (File)** программы *Блокнот* выберите **Печать (Print).** Откроется окно **Печать (Print),** позволяющее задать параметры принтера и печати.

   В окне **Печать** содержатся сведения о размещении принтера и комментарии, введенные в ходе создания принтера; HPLJ8100 отображается как принтер по умолчанию, текущее состояние — не подключен.

7. Щелкните **Печать (Print).** В программе *Блокнот* появится сообщение, что документ печатается на вашем компьютере (на «быстром» компьютере сообщение можно и не заметить).
   В окне **HPLJ8100 — Работать автономно (HPLJ810»-Use Printer Offline)** вы увидите документ, ожидающий отправки на печатающее устройство. Документ удерживается в очереди печати, поскольку вы перевели принтер в автономный режим. Если бы принтер был в оперативном режиме, документ отправился бы на печатающее устройство.
8. Закройте *Блокнот* и щелкните **Нет** (No) в ответ на запрос о сохранении изменений в документе.
9. Выберите документ в окне **HPLJ8100,** затем в меню **Принтер (Printer)** выберите **Очистить очередь печати (Cancel All Documents).** Появится окно сообщений **Принтеры (Printers)** с запросом на подтверждение отмены печати всех документов для HPLJ8100.
10. Щелкните Да (Yes). Документ будет удален из списка.
11. Закройте окно **HPLJ8100 — Работать автономно (HPLJ8100-Use Printer Offline).**
12. Закройте окно **Принтеры и факсы (Printers And Faxes).**

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Вы настраиваете принтер на компьютере под управлением Windows Server 2003. Компьютер будет использоваться в качестве сервера печати. Вы планируете использовать принтер, в настоящий момент подключенный к сети как изолированное устройство печати. Принтер какого типа следует добавить на сервер печати? (Выберите все подходящие варианты.)
   a. Сетевой.
   b. Общий.
   c. Локальный.
   d. Удаленный.
2. Вы устанавливаете принтер на клиентском компьютере. Принтер будет подключен к логическому принтеру, установленному на сервере печати Windows Server 2003. Сведения какого типа (типов) нужно предоставить для настройки принтера? (Выберите все подходящие варианты.)
   a. TCP/IP-порт принтера.
   b. Модель печатающего устройства.
   c. URL принтера на сервере печати.
   d. UNC-путь к общему ресурсу печати.
   e. Драйвер принтера.
3. Один из ваших принтеров неисправен, и вы хотите запретить пользователям отправлять задания печати на логический принтер, обслуживающий это устройство. Что нужно сделать?
   a. Прекратить общий доступ к принтеру.
   b. Удалить принтер из Active Directory.
   c. Сменить порт принтера.
   d. Переименовать общий ресурс.

4. Вы администрируете компьютер под управлением Windows Server 2003, настроенный в качестве сервера печати, и хотите выполнить сервисные работы на подключенном к нему принтере. В очереди печати находится несколько документов. Вам нужно, чтобы принтер приостановил печать и обработал задания позже без их перезапуска. Как это лучше сделать?
   a. Открыть окно свойств принтера и на вкладке **Доступ (Sharing)** выбрать **Нет общего доступа к данному принтеру (Do Not Share This Printer).**
   b. Открыть окно свойств принтера и выбрать порт, не связанный ни с одним печатающим устройством.
   c. Открыть окно очереди печати и для каждого задания в меню **Документ (Document)** выбрать **Приостановить (Pause).**
   d. Открыть окно очереди печати и в меню **Принтер (Printer)** выбрать **Приостановить печать (Pause Printing).**

Резюме

- Клиент печати отправляет задание на сервер печати, который, в свою очередь, передает его принтеру. И клиент, и сервер печати содержат логический принтер, представляющий физический принтер.
- Локальным называют принтер, обслуживающий аппаратный принтер, напрямую подключенный к компьютеру или к сети.
- Сетевой принтер подключается к логическому принтеру, обслуживаемому другим компьютером — сервером печати.
- Клиенты Microsoft Windows загружают драйвер принтера автоматически — с логического принтера на сервере печати. Добавлять принтеры можно на вкладке **Доступ (Sharing)** в окне свойств принтера.

Занятие 2. Дополнительная настройка и управление принтерами

На предыдущем занятии вы узнали, что в Windows принтер оптимально используется, когда создан логический принтер для обслуживания физического устройства (подключенного напрямую к компьютеру либо по сети), который доступен клиентам печати. Логический принтер на сервере печати служит центральной точкой конфигурирования и управления. Установленные вами драйверы принтера автоматически загружаются клиентами Windows, а настройки распространяются на все клиенты печати.

На этом занятии рассматривается следующий уровень виртуализации принтеров в качестве логических устройств. После знакомства со свойствами принтера (в том числе касающимися безопасности) вы научитесь создавать пулы принтеров, ускоряющие обработку заданий печати клиентов. Также вы научитесь создавать несколько логических принтеров для одного устройства для конфигурирования, управления и отслеживания заданий печати. Наконец, вы научитесь управлять объектами принтеров в Active Directory и печатью через Интернет.

Изучив материал этого занятия, вы сможете:

- ✓ управлять и настраивать свойства принтера;
- ✓ создавать пул принтеров;
- ✓ настраивать несколько логических принтеров для обслуживания одного устройства печати;
- ✓ управлять и подключаться к принтерам с помощью Active Directory и протокола IPP.

Продолжительность занятия - около 30 минут.

Управление свойствами принтера

Принтерами и заданиями печати управляют из диалоговых окон их свойств. Для конфигурирования принтера в окне **Принтеры** и **факсы (Printers And Faxes)** щелкните его значок правой кнопкой и выберите **Свойства (Properties).** Для конфигурирования задания печати дважды щелкните значок принтера, в очереди печати щелкните правой кнопкой задание и выберите **Свойства (Properties).** Начальные свойства задания печати наследуются от свойств самого принтера. Но свойства задания печати по умолчанию можно изменять независимо от свойств принтера.

Управление безопасностью принтера

Windows Server 2003 позволяет контролировать использование и администрирование принтера путем назначения разрешений на вкладке **Безопасность (Security)** в окне его свойств. Вы можете назначать разрешения на использование и администрирование принтера или документов, обрабатываемых принтером. Типичный вид вкладки **Безопасность (Security)** в окне свойств принтера показан на рис. 8-5.

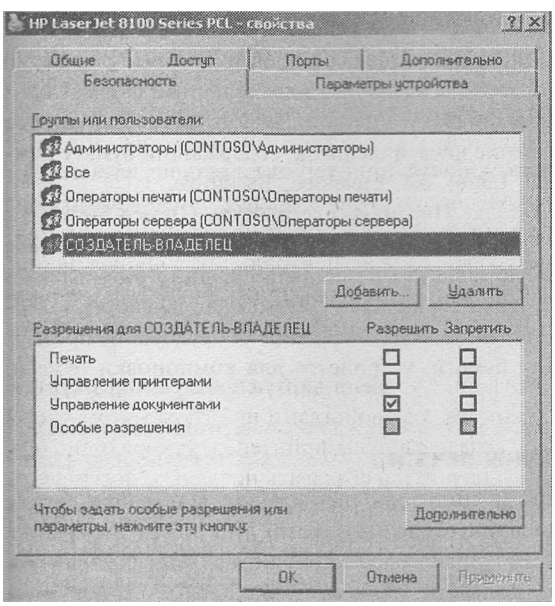


Рис. 8-5. Вкладка *Безопасность* в диалоговом окне свойств принтера

Можно использовать ACL принтера для ограничения его использования и делегирования полномочий управления принтером другим пользователям помимо администраторов. Windows Server 2003 предоставляет три уровня разрешений доступа к принтеру: *Печать* (Print), *Управление принтерами* (Manage Printers) и *Управление документами* (Manage Documents).

По умолчанию разрешение *Печать* (Print) назначено группе *Все* (Everyone). Оно позволяет пользователям отправлять документы на принтер. Для ограничения использования принтера удалите это разрешение и выдайте его другим группам или отдельным пользователям. Как и для ACL в файловой системе, отмененные разрешения перекрывают выданные. Кроме того, как и для ACL в файловой системе, рекомендуется назначать разрешения более узкой группе пользователей, а не предоставлять широкой группе и затем явно отменять для кого-либо.

Разрешение *Управление документами* (Manage Documents) позволяет отменять, приостанавливать, возобновлять и перезапускать задание печати. Оно предоставлено группе *Создатель-владелец* (Creator Owner). Поскольку разрешение этой группы наследуется пользователем, создающим объект, оно позволяет ему отменять, приостанавливать, возобновлять или перезапускать собственное задание печати. Также разрешение *Управление документами* (Manage Documents) назначено группам *Администраторы* (Administrators), *Операторы печати* (Print Operators) и *Операторы сервера* (Server Operators), так что они могут управлять печатью *любого* документа в очереди. Эти три группы обладают и разрешением *Управление принтерами* (Manage Printers), что позволяет им менять параметры и конфигурацию принтера, включая ACL.

Совет Если безопасность принтера не ставится во главу угла, вы можете делегировать права администрирования, выдав группе, например Printer Users, разрешение *Управление документами* или даже *Управление принтерами*.

Назначение форматов лоткам для бумаги

Если в печатающем устройстве предусмотрено несколько лотков, в которые регулярно загружается бумага разных форматов, вы можете назначить определенный формат конкретному лотку. Когда пользователи печатают документ конкретного размера, Windows Server 2003 автоматически направляет задание печати на лоток, содержащий бумагу нужного формата. Примеры форматов: Legal, Letter, A4, Envelope, Executive.

Назначить лотку формат можно на вкладке **Параметры устройства (Device Settings)** в окне свойств принтера (рис. 8-6). Число лотков, отображаемое в разделе **Назначение лотков (Form To Tray Assignment),** напрямую зависит от типа установленного принтера и количества поддерживаемых им лотков. Ниже на вкладке **Параметры устройства** содержатся параметры, показывающие установленное дополнительное оборудование принтера, например дополнительные лотки для бумаги, устройства для компоновки бумаги, модули шрифтов и память принтера.

Параметры по умолчанию для задания печати

На вкладке **Общие (General)** окна свойств принтера есть кнопка **Настройка печати (Printing Preferences),** а на вкладке **Дополнительно (Advanced)** — кнопка **Умолчания (Printing Defaults).** Обе кнопки раскрывают диалоговое окно, позволяющее управлять способом печати заданий на логическом принтере, включая такие параметры документа, как ориентация страницы (портретная или ландшафтная), двусторонняя печать (если

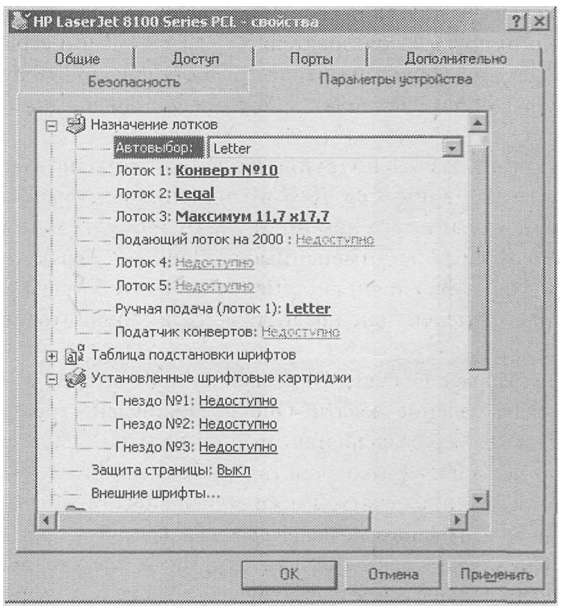


Рис. 8-6. Вкладка *Параметры устройства* в диалоговом окне свойств принтера

поддерживается), источник бумаги, разрешение и др. Эти окна одинаковы, а также идентичны диалоговому окну, которое открывается, когда пользователь щелкает **Свойства (Properties)** в диалоговом окне **Печать (Print).**

Зачем нужны три окна свойств для задания печати? Диалоговое окно **Умолчания (Printing Defaults)** настраивает параметры по умолчанию для всех пользователей данного логического принтера. Если принтер общий, его стандартные параметры печати становятся свойствами по умолчанию для всех принтеров, подключенных от клиентов к данному общему принтеру. Диалоговое окно **Настройка печати (Printing Preferences)** позволяет задать персональные для каждого пользователя параметры принтера. Все параметры в окне **Настройка печати** перекрывают настройки печати по умолчанию. Окно свойств, раскрываемое по щелчку кнопки **Свойства (Properties)** в окне **Печать (Print),** определяет свойства конкретного задания. Эти свойства перекрывают и стандартные, и персональные параметры печати. Такое тройственное представление наборов свойств задания печати позволяет администраторам конфигурировать принтер централизованно, выполняя стандартные настройки на общем логическом принтере. Однако при этом сохраняется возможность гибкого децентрализованного конфигурирования печати для отдельных пользователей и документов.

Расписание работы принтера

Вкладка **Дополнительно (Advanced)** в окне свойств принтера (рис. 8-7), позволяет настраивать ряд дополнительных параметров, управляющих поведением логического принтера, его процессора и очереди печати. Одна из важных и любопытных характеристик — график работы принтера.

Расписание работы логического принтера определяет, когда задание освобождается из очереди и отправляется на физический принтер. Пользователь с разрешением *Печать* (Print) может направлять задание на принтер в любое время, но оно будет удерживаться в очереди, пока, согласно расписанию принтера, его нельзя будет направить на

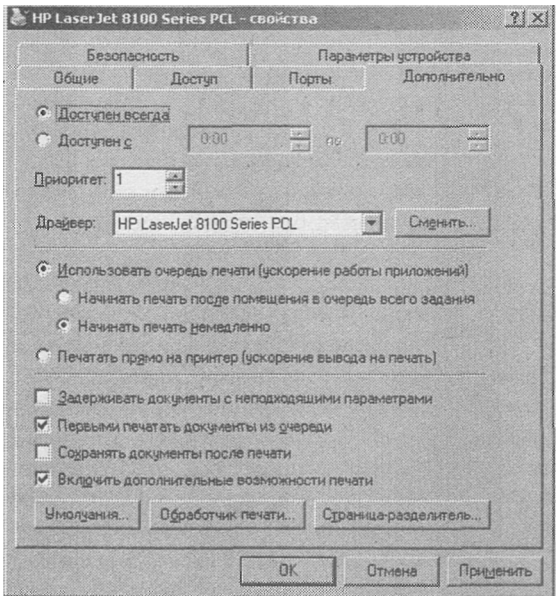


Рис. 8-7. Вкладка *Дополнительно* в диалоговом окне свойств принтера

порт принтера. Такая конфигурация не подходит для обычных, повседневно используемых принтеров. Однако расписание очень помогает в ситуациях, когда пользователи печатают объемные задания, и необходимо, чтобы они печатались после окончания рабочего дня или в периоды снижения нагрузки на принтер. Если настроить принтер для работы по ночам, пользователи будут отправлять задание на него днем, а принтер будет выполнять их ночью.

Совет При настройке пула принтеров размещайте печатающие устройства физически в одном месте, чтобы пользователи могли легко найти свои документы. Когда пользователи печатают на пул принтеров, узнать, на каком конкретно принтере фактически напечатано задание, невозможно.

Настройка пула принтеров

Пул принтеров — это один логический принтер, обслуживающий несколько физических, подключенных к серверу и/или к сети. Когда создан пул принтеров, документы пользователей отправляются на первый свободный принтер. Затем логический принтер, представляющий данный пул, автоматически определяет доступный порт.

Группировка принтеров в пулы настраивается на вкладке **Порты (Ports)** в окне свойств принтера. Чтобы сгруппировать принтеры в пул, установите флажок **Разрешить группировку принтеров в пул (Enable Printer Pooling),** а затем выберите или добавьте порты, на которых функционируют объединяемые печатающие устройства. На рис. 8-8 показан пул из трех подключенных к сети принтеров.

Подготовка к экзамену Драйвер, используемый пулом принтеров, должен быть совместим со всеми принтерами, на которые пул направляет задания печати.

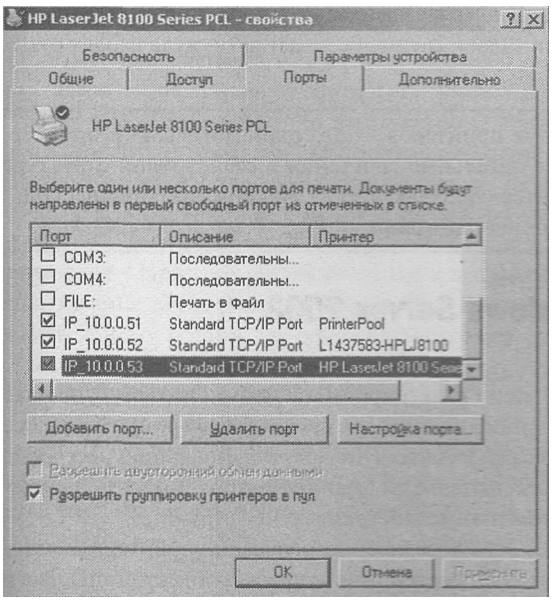


Рис. 8-8. Вкладка *Порты* диалогового окна свойств принтера с пулом из трех принтеров

Настройка нескольких логических принтеров для обслуживания одного принтера

Хотя пул принтеров — это один логический принтер, обслуживающий несколько портов (или принтеров), обратная структура более типична и мощна: несколько логических принтеров, обслуживающих один порт (или принтер). Создав несколько логических принтеров, направляющих задания на один физический принтер, вы можете настраивать различные свойства, параметры печати по умолчанию, параметры безопасности, аудит и мониторинг для каждого логического принтера.

Например, вам может потребоваться разрешить руководителям Contoso, Ltd. немедленно печатать свои задания, приостанавливая печать документов других пользователей. Для этого можно создать второй логический принтер, направляющий задания на тот же порт (тот же физический принтер), что и другие пользователи, но с более высоким приоритетом.

Для создания дополнительного логического принтера используется *Мастер установки принтеров* (Add Printer Wizard). Чтобы реализовать структуру «несколько логических принтеров на один порт», дополнительные принтеры должны использовать тот же порт, что и имеющийся логический принтер. Имя принтера и имя общего ресурса уникальны. После добавления нового логического принтера откройте окно его свойств и настройте драйверы, ACL, параметры печати по умолчанию и т. п.

Чтобы задать высокий приоритет новому логическому принтеру, перейдите на вкладку **Дополнительно (Advanced)** и установите приоритет в диапазоне от 1 (самый низкий) до 99 (самый высокий). Если логическому принтеру руководителей назначить приоритет 99, а принтеру остальных пользователей — 1, документы руководителей будут напечатаны раньше, но не прервут задания печати пользователя: когда принтер свободен, он будет в первую очередь принимать задания от принтера с более высоким приоритетом. Чтобы не допустить печать заданий обычных пользователей на принтере руководства,

настройте его ACL: удалите разрешение печати, назначенное группе *Все* (Everyone), и вместо этого предоставьте разрешение только группе безопасности, куда входят руководители.

Подготовка к экзамену Помните, что пул принтеров — это один логический принтер, обслуживающий несколько портов. Все остальные сочетания в стандартной структуре «клиент печати — сервер печати — принтер» получаются в результате создания нескольких логических принтеров, обслуживающих один порт.

Интеграция принтеров Windows Server 2003 с Active Directory

Подсистема печати Windows Server 2003 тесно интегрирована с Active Directory, упрощая пользователям и администраторам поиск и подключение к принтерам в организации. Все требуемое взаимодействие между принтерами и Active Directory по умолчанию настроено таким образом, чтобы работа велась без вмешательства администратора. Вносить изменения нужно, только если стандартная схема взаимодействия вас не устраивает.

Когда на сервер печати Windows Server 2003 добавляется логический принтер, он автоматически публикуется в Active Directory. Этот сервер печати создает объект printQueue и заполняет его свойства на основе данных драйвера и параметров логического принтера.

На заметку Объекты принтера нелегко обнаружить в консоли *Active Directory — пользователи и компьютеры*. Используйте кнопку **Поиск объектов в службе каталогов Active Directory (Find Objects In Active Directory)** на панели инструментов MMC; либо в меню **Вид (View)** выберите **Пользователи, группы и компьютеры как контейнеры (View Users, Groups, And Computers As Containers),** после чего объекты принтера станут видимыми на сервере печати. В Active Directory принтер помещается в объект — компьютер сервера печати. Этот объект можно переместить в любое ОП.

При любом изменении конфигурации принтера объект принтера в Active Directory обновляется. В хранилище Active Directory повторно отправляется вся конфигурационная информация, даже если ее часть не изменилась.

Примечание Создание и обновление объектов принтеров происходит относительно быстро, но объекты и атрибуты должны реплицироваться до того, как они смогут повлиять на результаты операции **Поиск: Принтеры (Find Printers),** выполняемой клиентом. Задержка репликации зависит от размера вашей организации и топологии репликации.

Если сервер печати больше не используется в сети, его объект принтера удаляется из Active Directory. Служба удаления принтеров подтверждает наличие общих принтеров, представленных в Active Directory, опрашивая их каждые восемь часов, и, если не может связаться с принтером два раза подряд, его объект удаляется. Это может произойти, если сервер печати переведен в автономный режим, например если принтеры, совместно используемые на рабочих станциях Windows 2000 или Windows XP, отключаются на ночь или на выходные дни. Однако сервер печати заново создаст объекты этих принтеров, когда их компьютер будет включен или когда будет перезапущена служба очереди печати. Так что вмешательство администратора опять же не требуется.

Публикация принтеров Windows

Принтеры, добавленные с помощью *Мастера установки принтеров,* публикуются по умолчанию, и отказаться от этого при работе мастера нельзя.

Если вам нужно повторно опубликовать принтер (допустим, после изменения его имени или других свойств), либо если вы не хотите публиковать общий принтер в Active Directory, откройте окно свойства принтера, перейдите на вкладку **Доступ (Sharing)** и установите (или снимите) флажок **Внести в Active Directory (list In The Directory).**

Примечание Принтер, подключенный к локальному порту, обычно определяется и устанавливается автоматически средствами Plug And Play. В таком случае следует предоставить к нему общий доступ и опубликовать данный принтер вручную с помощью вкладки **Доступ (Sharing).**

Логические принтеры, совместно используемые на компьютерах под управлением Windows NT 4 или Windows NT 3.51, не публикуются автоматически, однако их можно опубликовать вручную с помощью консоли *Active Directory — пользователи и компьютеры*. Просто щелкните правой кнопкой ОП или другой контейнер, в котором требуется создать принтер, и выберите **Создать (New)\Принтер (Printer).**

Примечание Добавлять следует только объекты принтеров, соответствующие принтерам на компьютерах пред-Windows 2000. Не добавляйте объекты для принтеров на компьютерах под управлением Windows 2000 или более поздних версий — пусть они публикуются автоматически.

Ручная настройка рабочих характеристик принтера

Все вышеописанные типы поведения системы по умолчанию можно изменить средствами локальной или групповой политики. Политики принтеров размещаются в узле **Конфигурация компьютера (Computer Configuration),** ниже узла **Административные шаблоны (Administrative Templates).** Чтобы просмотреть описание каждой из этих политик, откройте окно свойств соответствующей политики и перейдите на вкладку **Объяснение (Explain).**

Слежение за размещением принтеров

Слежение за размещением принтеров — это отключенная по умолчанию функция, которая значительно облегчает пользователям в крупной организации поиск принтеров за счет предварительного заполнения поля **Размещение (Location)** диалогового окна **Поиск: Принтеры (Find Printers). В** итоге набор результатов фильтруется автоматичес-. ки, так что список найденных принтеров сортируется по географической близости к пользователю.

Чтобы использовать функцию слежения за размещением принтеров, необходимо иметь один или несколько сайтов или одну или несколько подсетей. Объекты сайта и подсети создаются и поддерживаются из консоли *Active Directory — сайты и службы* (Active Directory Sites And Services). Вы также должны настроить вкладку **Размещение (Location)** в окне свойств сайта или подсети, задав иерархию мест размещения, разделенных символами косой черты. Например, размещение USA/NYC/1802Americas/42/B указывает на здание корпорации Americas на улице 1802 Avenue в Манхэттене, 42 этаж, блок B. Размещение может охватывать несколько подсетей или сайтов.

Затем нужно включить функцию слежения за размещением принтеров средствами политики **Заполнение строки поиска принтеров (Pre-Populate Printer Search Location Text).**

Служба Active Directory способна определить принадлежность компьютера к сайту или подсети по его IP-адресу. Когда открывается окно **Поиск: Принтеры (Find Printers),** размещение компьютера, заданное в соответствующем объекте сайта или подсети, будет автоматически поставлено в поле **Размещение (Location).** Также появится кнопка **Обзор (Browse),** позволяющая пользователю просматривать иерархию размещения принтеров в других местах.

Эта мощная функция значительно облегчает администрирование и настройку принтеров. Однако она требует тщательного планирования и настройки на сервере: вам придется описать все подсети, а также разработать и соблюдать продуманные правила именования, отражающие иерархию размещений. Подробнее об этой функции — в *Центре справки и поддержки.*

Печать через Интернет

Благодаря протоколу IPP (Internet Printing Protocol) Windows Server 2003 поддерживает дополнительный набор функций, позволяющий пользователям подключаться к принтерам и передавать задания печати по инкапсулированному протоколу HTTP. Печать через Интернет также дает возможность администраторам управлять и настраивать принтеры с помощью любых Web-браузеров **и** с любых платформ.

Настройка печати через Интернет

В Windows Server 2003 печать через Интернет не устанавливается и не активируется по умолчанию. Необходимо установить IIS (Internet Information Services), как описано в главе 6. Печать через Интернет можно активировать при установке IIS. Чтобы установить средства интернет-печати, сделайте следующее.

1. Откройте, приложение **Добавление и удаление программ (Add Or Remove Programs)** в *Панели управления* и щелкните **Установка компонентов Windows (Add/Remove Windows Components).**
2. Щелкните **Сервер приложений (Application Server),** а затем **Состав (Details).**
3. Отметьте **Службы IIS [Internet Information Services (IIS)]** и щелкните **Состав (Details).**
4. Выберите **Печать через Интернет (Internet Printing).**

После установки IIS и средств печати через Интернет эту функцию можно включать или отключать с помощью оснастки или консоли IIS. Раскройте узел сервера и щелкните **Расширения веб-службы (Web Service Extensions). В** правой панели выберите **Печать через Интернет (Internet Printing)** и щелкните **Запретить (Prohibit)** или **Разрешить (Allow).**

Интернет-печать создает виртуальный каталог Printers на Web-узле по умолчанию. Место хранения этого виртуального каталога — %Systemroot%\Web\Printers. К узлу принтера можно обратиться с помощью браузера Microsoft Internet Explorer 4.01 и выше, введя в поле **Адрес (Address)** адрес сервера печати, продолженный именем виртуального каталога Printers. Например, чтобы открыть страницу печати через Интернет для Server01, введите http://Server01/printers.

Примечание Вы можете настроить проверку подлинности и безопасность доступа для интернет-печати в окне свойств виртуального каталога.

Использование и управление интернет-принтерами

Вы можете обратиться по адресу *http://сервер_печати/printers,* чтобы просмотреть список всех принтеров на этом сервере. Найдите нужный принтер и щелкните его — откроется его Web-страница.

Если вы знаете точное имя принтера, к которому хотите подключиться, можете ввести его адрес в следующем формате: *http://сервер_печати/имя_общего_ресурса_принтера.*

На Web-странице принтера можно подключаться к принтеру или управлять им, если у вас есть на то соответствующие разрешения. Когда вы щелкаете кнопку **Подключиться (Connect)** на Web-странице принтера, сервер создает файл .cab, содержащий файлы драйвера принтера, и загружает этот файл на компьютер клиента. Установленный принтер отображается в папке Printers на клиенте. Затем этот принтер, как любой другой, можно использовать и управлять им из папки **Принтеры и факсы (Printers And Faxes).** Использование браузера для управления принтерами дает несколько преимуществ:

- позволяет администрировать принтеры с любого компьютера, где имеется Web-браузер, независимо от наличия на нем Windows Server 2003 или драйверов данного принтера;
- позволяет настраивать интерфейс. Например, вы можете создать собственную Web-страницу с архитектурным планом, где указаны места размещения принтеров и даны ссылки на них;
- выдает сводную страницу с перечнем состояния всех принтеров на сервере печати;
- функция интернет-печати может сообщать данные о состоянии печатающего устройства в реальном времени, например, находится ли принтер в режиме энергосбережения, если драйвер принтера дает такие сведения. Эта информация недоступна из окна **Принтеры и факсы (Printers And Faxes).**

Лабораторная работа. **Дополнительная настройка и управление принтерами**

На этой лабораторной работе вы сгруппируете принтеры в пул и настроите второй логиевский принтер для одного принтера, подключенного к сети.

Упражнение 1. Группировка принтеров в пул

1. В окне **Принтеры и факсы (Printers And Faxes)** создайте новый принтер. Если вам необходима помощь в создании принтера, выполните упражнение 1 занятия 1 этой главы. Принтер должен направлять задания на сетевой адрес 10.0.0.52 (новый порт). Настройте принтер как HP LaserJet 8100 Series PCL; в качестве имени принтера и имени общего ресурса укажите PrinterPool. Все остальные свойства, включая размещение и комментарий, аналогичны свойствам из упражнения 1 занятия 1.
2. Откройте окно свойств PrinterPool.
3. На вкладке **Порты (Ports)** установите флажок **Разрешить группировку принтеров в** пул **(Enable Printer Pooling),** затем установите флажок рядом с портом IP_10.0.0.51.
4. Щелкните **Применить (Apply).** Теперь выбраны оба сетевых порта.

   Выиграют ли пользователи, отправляющие задания печати на HPLJ8100, от группировки принтеров в пул?

   Нет. Группировка в пул была настроена для общего принтера PrinterPool. Задания печати, отправленные на PrinterPool, могут печататься на принтерах с адресами 10.0.0.51 и 10.0.0.52. Задания печати, отправленные на HPLJ8100, могут печататься только на принтере с адресом 10.0.0.51.

Упражнение 2. Настройка нескольких логических принтеров для обслуживания одного принтера

1. В окне Принтеры и факсы (Printers And Faxes) создайте новый принтер. Если вам не обходима помощь в создании принтера, выполните упражнение 1 занятия 1 этой гла вы. Принтер должен направлять задания на сетевой адрес 10.0.0.52 (заметьте, что этот порт уже существует). Настройте принтер как HP LaserJet 8100 Series PCL в качестве имени принтера и имени общего ресурса укажите PriorityPrinter. Все остальные свойства, включая размещение и комментарий, аналогичны свойствам из упражнения 1 занятия 1.
2. Откройте окно свойств PriorityPrinter.
3. На вкладке Дополнительно (Advanced) присвойте параметру Приоритет (Priority) значение 99 (наивысший).

Упражнение 3. Изучение объектов принтеров в Active Directory

1. Откройте консоль *Active Directory — пользователи и компьютеры.*
2. В меню Вид (View) выберите **Пользователи, группы и компьютеры как контейнеры (Users, Groups, And Computers As Containers).**
3. Раскройте ОП Domain Controllers. Заметьте: ServerOl отображается как подчинен ный контейнер.
4. Щелкните Server01 в дереве.

   Объекты принтеров появятся в панели подробных сведений. Если объекты для принтеров, созданных в упражнениях 1 и 2, не появляются, подождите несколько минут серверу печати может потребоваться некоторое время для публикации принтером Active Directory. Возможно, потребуется нажать F5 (обновить), чтобы увидеть объекты принтера после их публикации.
5. Откройте окно свойств объекта PriorityPrinter.

   Обратите внимание на различия свойств, публикуемых в Active Directory, и свойства принтера, показываемых в папке Принтеры и факсы (Printers And Faxes). Active Directory поддерживает более ограниченный набор свойств — только те, которые обычно используют при поиске принтера. Также заметьте, что при изменении какого-либо свойства в Active Directory аналогичное свойство принтера не меняется, од нако изменение свойства принтера в итоге изменит соответствующее свойство объекта принтера в Active Directory.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Советы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Вы администрируете компьютер под управлением Windows Server 2003, настроенный в качестве сервера печати. Пользователи из группы Marketing жалуются, что не могут печатать документы с помощью принтера на этом сервере. Вы просматривав разрешения в окне свойств принтера. Группе Marketing дано разрешение *Управлвление документами* (Manage Documents). Почему пользователи не могут печатать на этом принтере?

   a. Разрешение *Управление документами* (Manage Documents) должно быть предоставлено группе *Все* (Everyone).

b. Разрешение *Управление документами* (Manage Documents) должно быть предоставлено группе *Администраторы* (Administrators).
c. Группе Marketing должно быть предоставлено разрешение *Печать* (Print).
d. Группе Marketing должно быть предоставлено разрешение *Управление принтерами* (Manage Printers).

2. Вы группируете принтеры в пул на компьютере под управлением Windows Server 2003. Пул принтеров содержит три одинаковых печатающих устройства. Вы открываете окно свойств принтера и на вкладке **Порты (Ports)** устанавливаете флажок **Разрешить группировку принтеров в пул (Enable Printer Pooling).** Что следует сделать далее?
   a. Настроить порт LPT1 для обслуживания трех принтеров.
   b. Выбрать или создать порты, связанные с этими тремя принтерами.
   c. На вкладке **Параметры устройства (Device Settings)** настроить устанавливаемые дополнения для обслуживания двух дополнительных устройств печати.
   d. На вкладке **Дополнительно (Advanced)** настроить приоритет для каждого устройства печати, чтобы распределить задания между тремя устройствами.
3. Вы администрируете компьютер под управлением Windows Server 2003, настроенный в качестве сервера печати, и хотите управлять службами печати из Web-браузера на клиентском компьютере. Сервер называется Mktgl, но вы не знаете имя общего ресурса принтера. По какому URL следует подключаться к принтеру?
   a. http://mktg I/printers.
   b. http://printers/mktgl.
   c. http://windows/web/printers.
   d. http://windows/mktgl.
4. Вам нужно настроить логический принтер так, чтобы большие документы с низким приоритетом печатались по ночам. Какие из следующих параметров необходимо настроить в окне свойств принтера?
   a. **Приоритет (Priority).**
   b. Доступенс/по (Available From/To).
   c. Начинать печать после помещения в очередь всего задания (Start Printing After Last Page Is Spooled).
   d. Печатать прямо на принтер (ускорение вывода на печать) (Print Directly To The Printer).
   e. Сохранять документы после печати (Keep Printed Documents).

Резюме

Модель принтеров в Windows поддерживает творческое и гибкое использование принтеров через механизм логических принтеров. Вы можете добавить один логический принтер, который отправляет задания на несколько устройств (пул принтеров) либо на несколько логических принтеров, отправляющих задания на одно устройство. При этом на каждом логическом принтере можно предварительно настроить параметры принтера, параметры печати по умолчанию и разрешения доступа для обслуживания задач печати определенного типа.

Принтеры публикуют в Active Directory, чтобы пользователям было удобно находить и подключаться к ним. Windows Server 2003 поддерживает функцию слежения за размещением принтеров, еще более упрощающую поиск принтеров. Благодаря протоколу IPP можно управлять принтерами и печатать с их помощью даже по интрасети или через Интернет.

Занятие 3. Обслуживание, мониторинг и устранение неполадок принтеров

После установки, конфигурирования и открытия общего доступа к логическим принтерам на серверах печати, а также после подключения клиентов к этим принтерам, вы должны приступить к обслуживанию и мониторингу логических и физических принтеров. На этом занятии вы научитесь поддерживать драйверы принтера, перенаправлять принтеры, настраивать журналы производительности и использования, а также устранять неполадки принтеров.

Изучив материал этого занятия, вы сможете:

- ✓ управлять драйверами принтера;
- ✓ перенаправлять принтер;
- ✓ наблюдать за производительностью принтера;
- ✓ вести аудит доступа к принтеру;
- ✓ устранять неполадки принтера.

Продолжительность занятия — около 20 минут.

Обслуживание принтеров

Регулярное обслуживание службы печати на компьютере под управлением Windows Server 2003 не требуется. Описанные далее задачи обычно выполняются при необходимости. Помните, что при управлении принтерами ваши действия могут затронуть принтер в целом или все принтеры на данном сервере печати, а не только отдельные задания.

Управление драйверами принтера

Первая группа задач обслуживания относится к драйверам на сервере печати. Как мы уже упоминали на этом занятии, полезно установить драйверы для всех клиентских платформ, которые будут использовать определенный общий принтер. Клиенты Windows загрузят подходящий драйвер автоматически, когда будут подключаться к этому принтеру. Драйверы для различных платформ устанавливаются щелчком кнопки **Дополнительные драйверы (Additional Drivers)** на вкладке **Доступ (Sharing)** в окне свойств принтера.

Чтобы обновить драйверы для одного логического принтера, перейдите на вкладку **Дополнительно (Advanced)** в окне свойств и щелкните **Сменить (New Driver).** После этого вы сможете выбрать дополнительные драйверы: укажите изготовителя и модель либо щелкните **Установить с диска (Have Disk)** и предоставьте драйверы от изготовителя.

Также можно управлять драйверами для сервера печати в целом. В папке **Принтеры и факсы (Printers And** Faxes) в меню **Файл (File)** выберите **Свойства сервера (Server Properties)** и перейдите на вкладку **Драйверы (Drivers).** На ней вы можете добавить, удалить, переустановить и просмотреть свойства всех драйверов на данном сервере печати, и изменения параметров драйверов будут применены ко всем принтерам на этом сервере.

Если вы хотите просмотреть перечень всех файлов, связанных с конкретным драйвером принтера, откройте вкладку Драйверы (Drivers) для сервера печати, щелкните драйвер, а затем Свойства (Properties). Откроются имена и описания всех файлов, являющихся частью конкретного драйвера. Из этого перечня можно просматривать подробные сведения, касающиеся любого из файлов, выбрав нужный файл и щелкнув Свойства (Properties).

Перенаправление заданий печати

Если принтер неисправен, можно пересылать документы из его очереди на другой принтер, подключенный к локальному порту компьютера или к сети. Это называется *перенаправлением* заданий печати: Оно позволяет пользователям отправлять задания на тот же логический принтер и не повторять задания из очереди неисправного принтера.

Чтобы перенаправить принтер, откройте окно свойств принтера и перейдите на вкладку Порты (Ports). Выберите имеющийся порт или добавьте новый. Флажок рядом с портом неисправного принтера сразу же снимается, если только принтеры не сгруппированы в пул (тогда снимите флажок вручную).

Поскольку задания печати уже были подготовлены для модели неисправного принтера, принтер на новом порту должен быть совместим с драйвером, используемым соответствующим логическим принтером. Все задания печати с этого момента перенаправляются на новый порт. Нельзя перенаправлять отдельные документы и уже печатающиеся документы.

Мониторинг принтеров

В Windows Server 2003 предусмотрено несколько способов мониторинга принтеров и ресурсов печати.

Работа с оснастками *Системный монитор* и *Журналы и оповещения производительности*

Оснастки *Системный монитор* (System Monitor) и *Журналы и оповещения производительности* (Performance Logs And Alerts) из консоли *Производительность* (Performance) позволяют следить за производительностью принтеров в реальном времени, регистрировать рабочие показатели для последующего анализа, а также задавать уровни оповещений и реакцию на них. Средства *Системный монитор* и *Журналы и оповещения производительности* подробно обсуждаются в главе 12. Чтобы добавить счетчик в *Системный монитор,* щелкните правой кнопкой графическую область и выберите **Добавить счетчики (Add Counters)**. Выберите объект, производительность которого необходимо контролировать (в данном случае — Очередь печати [Print Queue]), нужные счетчики и экземпляр, представляющий наблюдаемый логический принтер.

Выбрав Очередь печати (Print Queue), вы увидите список всех доступных для него счетчиков производительности. Чтобы узнать смысл конкретного показателя производительности, выберите нужный счетчик и щелкните Объяснение (Explain).

Вот наиболее важные счетчики, контролирующие производительность печати.

- **Печатаемых байт/сек (Bytes Printed/Sec).** Количество байт необработанных данных, отправляемых на принтер в секунду. Низкие значения этого счетчика могут свидетельствовать о низкой нагрузке на принтер из-за отсутствия заданий, неравномерной загрузки очередей печати или слишком высокой нагрузки на сам сервер. Это

значение зависит от типа принтера. В документации к принтеру должна быть описана его приемлемая пропускная способность.

- **Ошибок заданий (Job Errors).** Количество ошибок заданий. Ошибки заданий обычно вызваны неправильной конфигурацией порта: проверьте, правильно ли настроен порт. Один экземпляр заданий печати увеличит значение этого счетчика только однажды, даже если ошибка произойдет неоднократно. Кроме того, некоторые мониторы печати не поддерживают счетчик ошибок заданий, и значение останется равным 0.
- **Заданий (Jobs).** Количество заданий в очереди печати в данный момент.
- **Всего заданий напечатано (Total Jobs Printed).** Количество заданий, отправленных на принтер со времени последнего перезапуска очереди печати.
- **Всего напечатано страниц (Total Pages Printed).** Количество страниц, напечатанных со времени последнего перезапуска очереди печати. Этот счетчик дает близкое приближение количества отпечатанных страниц; отклонения в оценке объемов зависят от типа заданий и свойств документов в этих заданиях.

Подготовка к экзамену Счетчики **Всего заданий напечатано (Total Jobs Printed)** и **Всего напечатано страниц (Total/Pages Printed)** накопительные. Они представляют число заданий или страниц, напечатанных с момента запуска системы или перезапуска очереди печати.

Работа с журналом *Система*

С помощью консоли *Просмотр событий* (Event Viewer) вы можете просматривать журнал *Система* (System) в качестве источника информации об очереди печати и работе принтера. По умолчанию очередь печати регистрирует события, касающиеся создания, удаления и модификации принтеров. Также вы можете обнаружить события, содержащие сведения о трафике принтера, пространстве на жестком диске, ошибках очереди печати и других аспектах эксплуатации.

Чтобы настроить параметры регистрации событий очереди печати, откройте папку **Принтеры и факсы (Printers And Faxes)** и в меню **Файл (File)** выберите **Свойства сервера (Server Properties).** Перейдите на вкладку **Дополнительные параметры (Advanced),** чтобы увидеть нужные свойства (рис. 8-9). Здесь можно настроить регистрацию событий принтера в журнале и уведомления заданий печати, а также переместить папку очереди печати. Это важно для настройки активного сервера печати и при переполнении дискового тома, содержащего очередь печати.

Аудит доступа к принтеру

Как и для файлов и папок, вы можете вести аудит доступа к принтеру. Вы можете указать, аудит каких групп, пользователей и действий следует вести для конкретного принтера. После активации политики аудита доступа к объекту вы можете просмотреть результаты в консоли *Просмотр событий* (Event Viewer).

Чтобы настроить аудит принтера, откройте его окно свойств и на вкладке **Безопасность (Security)** щелкните **Дополнительно (Advanced).** Перейдите на вкладку **Аудит (Auditing)** и добавьте записи для конкретных групп или пользователей. Для каждого участника безопасности, добавленного в список элементов аудита, можно настроить аудит успешного или неудачного доступа на основе стандартных разрешений доступа к принтеру, в том числе *Печать* (Print), *Управление документами* (Manage Documents) и *Управление принтерами* (Manage Printers).

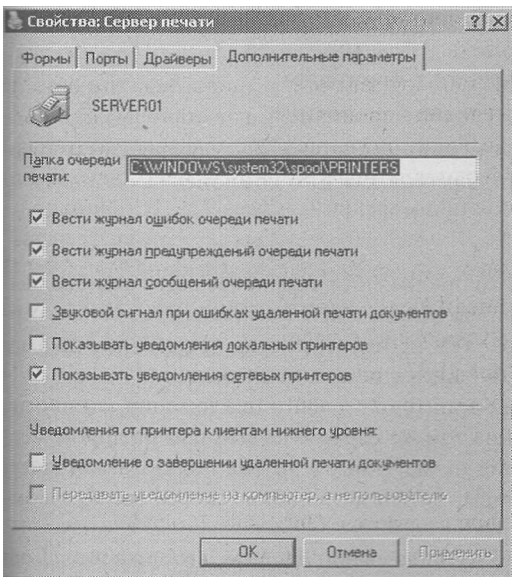


Рис. 8-9. Вкладка *Дополнительные параметры* в диалоговом окне свойств сервера печати

Затем нужно включить политику *Аудит доступа к объектам* (Audit Object Access), размещенную в узле групповой или локальной политики **Конфигурация компьютера (Computer Configuration)\Конфигурация Windows (Windows Settings)\Параметры безопасности (Security Settings)\Локальные политики (Local Policies)\Политика аудита (Audit Policy)**. После вступления этой политики в силу вы можете просматривать в журнале событий *безопасность* (Security) записи аудита принтера.

Совет Аудит принтера создает массу записей даже для одного задания печати. Поэтому рн полезен только для устранения очень специфичных проблем. Аудит принтера не следует применять для контроля использования принтера или выставления счета за услуги печати. Для этого рекомендуется анализировать счетчики производительности, например **Всего заданий напечатано (Total Jobs Printed) или Всего напечатано страниц (Total Pages Printed)**.

Устранение неполадок принтеров

Устранение неполадок — важная часть управления принтером. Приведенная ниже информация поможет вам понять, выявить и устранить типичные инциденты и проблемы, которые могут возникнуть при печати в Windows Server 2003.

При устранении неполадок помните, что печать, как правило, включает несколько компонентов:

- приложение, выполняющее печать;
- логический принтер на компьютере, где выполняется приложение;
- сетевое подключение между клиентом печати и общим логическим принтером на сервере;

- логический принтер на сервере: его очередь печати, драйверы, параметры безопасности и т. п.;
- сетевое подключение между сервером печати и принтером;
- сам принтер: его оборудование, конфигурация и состояние.

Эффективный способ решения большинства проблем печати — логический и методический подходы к устранению неполадок в работе каждого компонента.

Определение области сбоя

Если пользователь может печатать из другого приложения, вероятнее всего ошибка связана с неудачно выполнившим задание приложением, а не с компьютером, сетью, сервером печати или оборудованием принтера. Тем не менее, иногда применение другого драйвера или типа данных может устранить ошибки печати приложения.

Если пользователь не может печатать на принтер из любого приложения, выясните, может ли он печатать на другие принтеры на том же сервере печати или на другие серверы печати. Если все варианты печати ему недоступны, а другие пользователи могу? выполнять печать на те же сетевые принтеры, источник ошибки, скорее всего, в компьютере пользователя.

Попробуйте создать локальный принтер на проблемной системе, который указывает непосредственно на порт принтера. Другими словами, обойдите сервер печати. Если это поможет, проблема в сервере печати, с каналом связи между системой пользователя с сервером печати либо с подключениями принтеров на клиенте.

Проверьте подключение клиента к серверу печати

Вы можете проверить подключение между клиентом и сервером печати, открыв окно принтера из папки Принтеры и факсы (Printers And Faxes) на компьютере клиента. Если окно принтера открывается, отображая документы в очереди печати, значит клиент успешно подключается к общему принтеру. Ошибка при открытии окна принтера может свидетельствовать о потенциальной проблеме в сети, проверке подлинности или разрешениях безопасности. Попробуйте командой Ping опросить IP-адрес сервера. Щелкните **Пуск (Start)\Выполнить (Run)** и введите \\сервер_печати. Если открывается окно с папкой **Принтеры и факсы (Printers And Faxes)** и какими-либо общими папками, клиент подключается к серверу. Перепроверьте разрешения безопасности на логическом принтере.

Проверьте исправность принтера

Проверьте сам принтер и убедитесь, что он готов к печати. Напечатайте пробную страницу с консоли принтера. Проверьте кабель, подключающий принтер к серверу печати или к сети. Если принтер подключен к сети, проверьте, что индикатор сетевой платы горит, подтверждая подключение.

Проверьте, есть ли доступ к принтеру с сервера печати

Большинство принтеров могут выводить свой IP-адрес на своей консоли или печатая страницу конфигурации. Убедитесь, что IP-адрес принтера совпадает с IP-адресом порта логического принтера. IP-адрес порта можно просмотреть на вкладке **Порты (Ports)** в окне свойств принтера. Проверьте возможность связи с принтером по сети, опроси командой Ping его IP-адрес.

Проверьте, что службы сервера печати запущены

Из консоли *Службы* (Services) проверьте, что необходимые принтеру службы работают корректно. Например, проверьте, запущена ли на сервере печати служба *Удаленного вызова процедур* (Remote Procedure Call, RPC): она необходима для стандартных сетевых подключений к общим принтерам. Также убедитесь, что на сервере запущена служба очереди печати.

Совет Для перезапуска службы очереди печати можно выполнить команды Net Stop Spooler и Net Start Spooler из командной строки. Если служба очереди печати перезапускается из командной строки или средствами пользовательского интерфейса, все документы из всех очередей печати на сервере удаляются.

Также можно просмотреть объем папки очереди печати, чтобы убедиться, что для очереди хватает места на диске. Размещение папки очереди печати можно узнать и изменить в окне **Свойства: Сервер печати (Server Properties)**, которое открывается из папки **Принтеры и факсы (Printers And Faxes)** командой **Файл (File)\Свойства сервера (Server Properties)**.

Примечание Место хранения папки очереди печати по умолчанию — %System-root%\System32\Spool\Printers. Если нагрузка на сервер печати высока, рекомендуется переместить папку очереди в тот раздел, где не хранится система и с которого не производится загрузка. Если раздел, где размещается папка очереди, заполнен до отраза заданиями печати, печать прекращается и, что более важно, ОС может работать нестабильно.

Также следует просмотреть журнал *Система* (System) на тот случай, если очередь печати записала туда какие-либо ошибки, и убедиться, что в папке **Принтеры и факсы (Printers And Faxes)** для принтера не активирован режим отложенной печати.

Попробуйте напечатать задание из какого-либо приложения на сервере печати. Если Можно печатать на принтер с сервера печати, проблема не связана с принтером. Если печать на принтер из приложения на сервере печати невозможна, создайте новый принтер, направленный на тот же порт, и попробуйте печатать на него. Если задание выполняется, проблема заключается в конфигурации исходного логического принтера. Если задание не выполняется, источник проблемы — связь с принтером или с самим оборудованием.

Лабораторная работа. **Устранение неполадок принтера**

На этой лабораторной работе вы перенаправите принтер, что полезно и при упреждающем, и при реактивном устранении неполадок. Если вы планируете перевести принтер в автомный режим, можно перенаправить его логический принтер (принтеры) на другое устройство, совместимое с драйвером данного логического принтера. Если отказ принтера вызван замятием бумаги или другой ошибкой, уже отправленные на логический принтер и помещенные в очередь задания также можно перенаправить, чтобы пользователям не пришлось ждать или повторять задания.

Заметьте: дополнительный практикум по устранению неполадок включен в разделы Пример из практики» и «Практикум по устранению неполадок» этой главы.

Упражнение. Перенаправление принтера

При сбое печатающего устройства задания с него можно перенаправить на другой принтер. Предположим, ваше задание поставлено в очередь печати на HPLJ8100. Однако при печати предыдущего задания в принтере застряла бумага.

1. Откройте папку **Принтеры и факсы (Printers And Faxes)** и удостоверьтесь, что принтер HPLJ8100 находится в автономном режиме. Если нет, щелкните правой кнопкой принтер и выберите **Отложенная печать (Use Printer Offline).** Это предотвратит генерацию ошибок из-за того, что данный принтер направлен на несуществующий сетевой порт.
2. Откройте *Блокнот* (Notepad) и введите произвольный текст.
3. В меню **Файл (File)** выберите **Печать (Print),** в качестве принтера укажите HPLJ8100.
4. В папке **Принтеры и факсы (Printers And Faxes)** дважды щелкните **HPLJ8100,** чтобы открыть окно принтера. Убедитесь, что ваше задание печати находится в очереди.
5. В меню **Принтер (Printer)** выберите **Свойства (Properties).**
6. Перейдите на вкладку **Порты (Ports),**
7. Согласно конфигурации, выполненной на занятии 1, принтер должен использовать сетевой порт 1P_10.0.0.51.
8. Установите флажок рядом с портом 1P_10.0.0.52.
9. Щелкните **OK**. Теперь вы перенаправили принтер. Все задания из его очереди, кроме тех, что уже выполняются, будут направлены на новый порт. Подключенный к новому порту принтер должен быть совместим с драйвером, используемым этим логическим принтером, поскольку задания уже были обработаны и помещены в очередь имеющимся драйвером.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Компьютер под управлением Windows Server 2003 настроен в качестве сервера печати. В середине рабочего дня выходит из строя предохранитель принтера; его нужно заменить. Пользователи уже отправили задания на этот принтер по IP-адресу 192.168.1.81. Аналогичный принтер использует адрес 192.168.1.217 и обслуживается другими логическими принтерами на данном сервере. Что предпринять, чтобы напечатать задания пользователей, не отправляя их повторно?
   a. В окне свойств неисправного принтера выбрать **Разрешить группировку принтеров в пул (Enable Printer Pooling).**
   b. В командной строке ввести Net Stop Spooler.
   c. В командной строке ввести Net Start Spooler.
   d. В окне свойств неисправного принтера выбрать порт 192.168.1.217.
   e. В окне свойств неисправного принтера щелкнуть **Добавить порт (Add Port).**
   f. В папке **Принтеры и факсы (Printers And Faxes)** щелкнуть правой кнопкой неисправный принтер и выбрать **Отложенная печать (Use Printer Offline).**
2. Вы настраиваете печать на компьютере под управлением Windows Server 2003. Вы подключаете принтер, конфигурируете логический принтер и отправляете документы на печать, однако они не печатаются полностью и иногда искажены. Какова наиболее вероятная причина проблемы?

a. Не хватает места на диске для очереди печати.
b. Используется некорректный драйвер принтера.
c. Выбран неправильный порт.
d. В параметрах устройства используется неверная подстановка шрифтов.

3. Какие из следующих действий дадут наиболее точное представление о нагрузке на принтер, чтобы вы знали расход тонера и бумаги?
   a. Настройка аудита для логического принтера и ведение аудита успешного использования разрешения **Печать (Print)** группой *Все* (Everyone).
   b. Экспорт журнала *Систета* (System) в текстовый файл с разделителями — запятыми и применение Microsoft Excel для анализа событий очереди печати.
   c. Настройка журнала производительности и мониторинг счетчика **Всего напечатано страниц (Total Pages Printed)** для каждого логического принтера.
   d. Настройка журнала производительности и мониторинг счетчика **Заданий (Jobs)** для каждого логического принтера.

Резюме

- Драйверы для логического принтера можно обновлять или добавлять из окна свойств этого принтера, Драйверы можно добавлять, удалять или переустанавливать для всех принтеров на сервере печати с помощью вкладки **Драйверы (Drivers)** в окне **Свойства: Сервер печати (Server Properties).**
- Если принтер необходимо перевести в автономный режим или он уже вышел из строя, можно перенаправить все его задания, кроме тех, что уже выполняются, на другой принтер, добавив или выбрав новый порт принтера в окне свойств исходного логического принтера. Альтернативный порт должен представлять принтер, совместимый с драйвером исходного принтера.
- Счетчики производительности **Всего заданий напечатано (Total Jobs Printed)** и **Всего напечатано страниц (Total Pages Printed)** помогают наблюдать за использованием принтера. Счетчики **Печатаемых байт/сек (Bytes Printed/Sec)** и **Ошибок (Errors)** помогают отслеживать потенциальные проблемы в работе принтера.
- Системные события, регистрируемые службой очереди печати, и события безопасности, регистрируемые средствами ведения аудита принтера после включения политики *Аудит доступа к объектам* (Audit Object Access), предоставляют дополнительную информацию о функциональности принтера.
- Поскольку модель принтеров **в** Windows Server 2003 является модульной, включая сам принтер, логический принтер на сервере печати и принтер на клиенте, подключенный к общему принтеру сервера, вы можете методически устранять неполадки принтера, анализируя каждый компонент и взаимосвязи между ними.

Пример из практики

Нагрузка на принтеры Contoso, Ltd. превысила норму, и руководство попросило вас вести учет их использования отделами маркетинга и сбыта.

Продумайте решение

1. Как наиболее эффективно наблюдать за использованием принтеров, если вам нужно выставить счет за печать?

Windows Server 2003 добавляет объект производительности *Очередь печати* (Printer Queue), который позволяет наблюдать за использованием всех логических принтеров, определенных на данном сервере. Счетчик **Всего напечатано страниц (Total Pages Printed)** предоставляет важные сведения об использовании принтера. Он не безупречен, поскольку определенные свойства документов и специальные функции печати (например печать брошюр или параметр печати нескольких страниц на одном листе» используют оборудование принтера напрямую, так что очередь печати не может отслеживать их влияние. Однако этот счетчик — наилучшее возможное приближение. Настроив журнал производительности и записав данные этого счетчика, вы затем сможете проанализировать журнал и выставить счет за использование принтеров.

2. Как наблюдать счетчик **Всего напечатано страниц (Total Pages Printed)** отдельно для групп Sales и Marketing?

   Счетчик **Всего напечатано страниц** записывает данные о производительности одного логического принтера. Чтобы наблюдать две группы независимо, необходимо настроить два отдельных логических принтера. Каждый из них будет направлен на один порт (на тот же физический принтер), но будет разрешать печать пользователям только одной группы.

Настройте принтеры

Если вы не помните, как установить логический принтер, см. упражнение 1 занятия 1 этой главы. Создайте два принтера с помощью *Мастера установки принтеров* (Add Printer Wizard). Используйте параметры, описанные в следующих таблицах, для ответа на вопросы *Мастера установки принтеров* и *Мастера добавления стандартного TCP/IP порта принтера* (Add Standard TCP/IP Printer Port Wizard).

Табл. 8-1. Принтер группы Sales

Параметр	Описание
Локальный или сетевой принтер (Local Or Network Printer)	Локальный принтер, подключенный к компьютеру. Не используйте Plug and Play для определения принтера
Выберите порт принтера (Select A Printer Port)	**Создать новый порт (Create A New Port):** «Standard **TCP/IP Port»**
Имя принтера или IP-адрес (Printer Name or IP Address)	10.0.0.53
Имя порта (Port Name)	IP_10.0.0.53
Тип устройства (Device Type)	Hewlett Packard Jet Direct
Изготовитель	**HP**
Модель принтера	**HP** LaserJet 8100 Series PCL
Используемый драйвер	Сохранить существующий драйвер
Имя принтера (Printer Name)	SalesPrinter
Принтер по умолчанию	**Нет (No)**
Имя общего ресурса (Share Name)	SalesPrinter
Размещение (Location)	NYC/US/1802Americas/42/B
Комментарий (Comment)	Black and White Output Laser Printer—High Volume
Напечатать пробную страницу? (Print a test page)	**Нет (No)**

Табл. 8-2. Принтер группы Marketing

Параметр	Описание
Локальный или сетевой принтер (Local Or Network Printer)	Локальный принтер, подключенный к компьютеру. Не используйте Plug and Play для определения принтера
Выберите порт принтера (Select A Printer Port)	**Использовать порт (Use the following port) IP10.0.0.53**
Изготовитель	**HP**
Модель принтера	**HP** LaserJet 8100 Series PCL
Используемый драйвер	Сохранить существующий драйвер
Имя принтера (Printer Name)	MarketingPrinter
Принтер по умолчанию	**Нет (No)**
Имя общего ресурса (Share Name)	MarketingPrinter
Размещение (Location)	NYC/US/1802Americas/42/B
Комментарий (Comment)	Black and White Output Laser Printer—High Volume
Напечатать пробную страницу? [Print a test page)	**Нет (No)**

Создайте группы пользователей принтеров

Чтобы назначать разрешения доступа к принтерам, вам потребуются группы безопасности (см. главу 4). Создайте две локальных доменных группы безопасности: Marketing Printer Users, Sales Printer Users.

Назначьте разрешения доступа к принтерам

1. В папке **Принтеры и факсы (Printers And Faxes)** откройте окно свойств SalesPrinter.
2. Перейдите на вкладку **Безопасность (Security).**
3. Щелкните группу *Все* (Everyone), затем **Удалить (Remove).**
4. Щелкните **Добавить (Add).**
5. Введите Sales Printer Users и щелкните **OK**.
6. Предоставьте группе Sales Printer Users разрешение **Печать (Print).**

   Повторите шаги 1–6 и дайте разрешение **Печать (Print)** для принтера MarketingPrinter только группе Marketing Printer Users.

Настройте журнал производительности

1. Откройте консоль *Производительность* (Performance) из группы **Администрирование (Administrative Tools).**
2. Раскройте узел Журналы **и оповещения производительности (Performance Logs And Alerts)** и щелкните Журналы **счетчиков (Counter Logs).**
3. Щелкните правой кнопкой **Журналы счетчиков (Counter Logs)** и выберите **Новые параметры журнала (New Log Settings).**
4. Введите имя журнала: Printer Utilization.
5. Щелкните **OK**. Откроется окно свойств журнала Printer Utilization.
6. Щелкните **Добавить счетчики (Add Counters).**

7. В раскрывающемся списке **Объект (Performance Object)** выберите **Очередь печати (Print Queue).**
8. В списке **Счетчики (Counters)** выберите **Всего напечатано страниц (Total Pages Printed).**
9. В списке экземпляров справа выберите SalesPrinter.
10. Щелкните **Добавить (Add).**
11. В списке экземпляров справа выберите MarketingPrinter.
12. Щелкните **Добавить (Add).**
13. Щелкните **Закрыть (Close).** Диалоговое окно **Printer Utilization** указывает, что с этого момента журнал будет отслеживать счетчик **Всего напечатано страниц (Total Pages Printed)** для каждой очереди печати.
14. Задайте период выборки 30 минут, введя 30 в поле **Интервал (Interval)** и выбрав мин. **(Minutes)** в раскрывающемся списке **Единицы (Units).**

Примечание Поскольку счетчик **Всего напечатано станиц (Total Pages Printed)** накапливает данные с момента запуска сервера печати или перезапуска службы очереди печати, необязательно поддерживать короткий интервал выборки. Показания можно снимать через достаточно длительные интервалы, если по ходу не перезапускаются сервер или служба очереди печати.

15. Щелкните OK, чтобы закрыть окно **Printer Utilization.**
16. Если вы не настроили на этом компьютере больше ни один журнал производительности, вам будет предложено создать папку C:\Perflogs, куда по умолчанию сохраняются журналы. Щелкните Да (Yes) для подтверждения.
17. На правой панели журналов производительности значок журнала Printer Utilization отображается зеленым, то есть он запущен.
18. Остановите запись журнала, щелкнув его правой кнопкой и выбрав **Остановка (Stop).**

После создания журнала производительности его можно просматривать в оснастке *Системный монитор* (System Monitor): на панели инструментов щелкните кнопку **Просмотр данных журнала (View Log Data),** и в открывшемся окне вы сможете добавить сгенерированный вами журнал производительности. Конкретно этот журнал не будет действителен по двум причинам. Во-первых, в журнале должны быть записаны две выборки, чтобы анализ данных журнала в *Системном мониторе* имел смысл. Если вы не подождете 60 минут или не уменьшите интервал выборки, то не сможете загрузить журнал. Во-вторых, значение счетчика **Всего напечатано страниц (Total Pages Printed)** не будет увеличиваться, поскольку принтер не существует и на нем не печатают документы.

Практикум по устранению неполадок

Отдел маркетинга жалуется на качество печати принтера MarketingPrinter. Из приложений Microsoft Office с компьютеров под управлением Windows XP документы печатаются нормально. Но при печати из приложений Adobe результаты не всегда соответствуют ожидаемым. Отдел сбыта, где используются рабочие станции под управлением Windows 2000 и XP, а также пакеты Microsoft Office и Microsoft Customer Relationship Management (CRM), не сообщают о каких-либо проблемах с принтером SalesPrinter.

При изучении проблемы оказалось, что некоторые приложения выдают разные результаты в зависимости от того, какой драйвер (с поддержкой PostScript или без) использует принтер.

Проанализируйте решение

Где в интерфейсе следует добавить драйверы PostScript? (Выберите все подходящие варианты.)

a. Диалоговое окно **Свойства: Сервер печати (Server Properties)** на сервере печати.
b. Диалоговое окно свойств принтера MarketingPrinter.
c. Диалоговое окно свойств принтера SalesPrinter.
d. Принтеры, установленные на компьютерах всех пользователей отдела маркетинга.

Правильный ответ: Ь. Если добавить драйвер PostScript для принтера MarketingPrinter, драйвер будет использовать только данный принтер, но не SalesPrinter. Хотя принтерам всех клиентов также потребуется драйвер PostScript, вам не нужно добавлять его вручную. Клиенты Windows 2000 и XP загрузят новый драйвер автоматически.

Смените драйвер принтера

1. Откройте папку **Принтеры и факсы (Printers And Faxes).**
2. Откройте окно свойств принтера MarketingPrinter.
3. Перейдите на вкладку **Дополнительно (Advanced).**
4. Щелкните **Сменить (New Driver).** Откроется окно *Мастера установки драйверов принтера* (Add Printer Driver Wizard).
5. Щелкните **Далее** (Next).
6. Выберите изготовителя: HP.
7. Выберите модель принтера: HP LaserJet 8100 Series PS.
8. Щелкните кнопку Далее (Next), а затем **Готово (Finish).**
9. Заметьте: драйвер PostScript теперь используется по умолчанию.
10. Раскройте список **Драйвер (Driver)** и вы увидите, что прежний драйвер (PCL) все еще в списке. Если смена драйвера на PostScript не устраняет проблему, можно легко вернуться к драйверу PCL.

Резюме главы

- Реализация принтера в Windows Server 2003 модульная и состоит из собственно аппаратного принтера, сервера печати с общим логическим принтером (представляющим физический принтер посредством его локального или сетевого порта) и логического принтера на клиенте (подключающегося к общему принтеру на сервере печати). Понимание структуры и терминологии очень важно, поскольку документация и пользовательский интерфейс не согласованы и иногда вводят в заблуждение.
- Общие принтеры публикуются в Active Directory, что облегчает пользователям их поиск на основе размещения или других свойств принтера.
- Когда принтер найден в окне **Поиск: Принтеры (Find Printers),** двойной щелчок его значка позволяет установить принтер на компьютер пользователя. Компьютеры под управлением Windows автоматически загружают драйвер с сервера, если администратор добавил все необходимые драйверы в общий принтер.

- Один логический принтер может направлять задания на несколько портов, формируя пул принтеров.
- Один физический принтер (порт) могут обслуживать несколько логических принтеров, каждый их которых может обладать собственными свойствами, драйверами, параметрами, разрешениями или наблюдаемыми показателями. Такая структура позволяет чрезвычайно гибко использовать аппаратные принтеры.
- Управление, установку и печать на принтеры можно выполнять через Web-интерфейс, если на сервере печати установлена и включена функция печати через Интернет.
- Журналы событий и счетчики производительности позволяют наблюдать за работой принтеров: выявлять сигналы потенциальных неполадок или вести статистику использования.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Важно уяснить разницу между аппаратным принтером (также называемым устройством печати или физическим принтером) и логическим принтером, который часто называют принтером.
- Разница между принтером в папке **Принтеры и факсы (Printers And Faxes)** и объектом принтера в Active Directory.
- Как управлять портами принтеров. Понимание разницы между группировкой принтеров в пул и перенаправлением принтера и знание способов выполнения этих задач.
- Как настроить несколько логических принтеров для одного физического принтера. Хорошо разберитесь с различными свойствами, которые можно настраивать отдельно для каждого логического принтера, включая разрешения безопасности.
- Как наблюдать за использованием принтера и устранять его неполадки.

Основные термины

Логический принтер ~ logical printer — представляет физический принтер, обслуживая порт этого принтера. Логический принтер включает очередь печати, драйверы, параметры, разрешения и параметры печати по умолчанию, которые управляют созданием задания печати для принтера.

Сетевой принтер ~ network printer — в контексте пользовательского интерфейса Microsoft Windows это логический принтер, являющийся клиентом общего логического принтера (то есть подключенный к нему) на другом компьютере. Не путайте с подключенным к сети принтером, который обслуживается *локальным принтером* на сервере печати.

Вопросы и ответы

Занятие 1. Закрепление материала

1. Вы настраиваете принтер на компьютере под управлением Windows Server 2003. Компьютер будет использоваться в качестве сервера печати. Вы планируете использовать принтер, в настоящий момент подключенный к сети как изолированное устройство печати. Принтер какого типа следует добавить на сервер печати? (Выберите все подходящие варианты.)
   a. Сетевой.
   b. Общий.
   c. Локальный.
   d. Удаленный.

   Правильный ответ: b, c. Локальным называют принтер, обслуживающий аппаратный принтер, напрямую подключенный к компьютеру, или изолированный принтер, подключенный к сети. На компьютере — сервере печати принтер должен быть общим.
2. Вы устанавливаете принтер на клиентском компьютере. Принтер будет подключен к логическому принтеру, установленному на сервере печати Windows Server 2003. Сведения какого типа (типов) нужно предоставить для настройки принтера? (Выберите все подходящие варианты.)
   a. TCP/IP-порт принтера.
   b. Модель печатающего устройства.
   c. URL принтера на сервере печати.
   d. UNC-путь к общему ресурсу печати.
   e. Драйвер принтера.

   Правильный ответ: c, d. Сетевой принтер можно найти в Active Directory, ввести UNC-путь или URL к нему либо воспользоваться функцией обзора. При подключении принтера модель определяется общим логическим принтером, а драйвер загружается автоматически.
3. Один из ваших принтеров неисправен, и вы хотите запретить пользователям отправлять задания печати на логический принтер, обслуживающий это устройство. Что нужно сделать?
   a. Прекратить общий доступ к принтеру.
   b. Удалить принтер из Active Directory.
   c. Сменить порт принтера.
   d. Переименовать общий ресурс.

   Правильный ответ: a. Если прекратить общий доступ к принтеру, пользователи не смогут печатать на соответствующем устройстве печати. Прекратить общий доступ можно с помощью вкладки Доступ (Sharing) в окне свойств принтера.
4. Вы администрируете компьютер под управлением Windows Server 2003, настроенный в качестве сервера печати, и хотите выполнить сервисные работы на подключенном к нему принтере. В очереди печати находится несколько документов. Вам нужно, чтобы принтер приостановил печать и обработал задания позже без их перезапуска. Как это лучше сделать?
   a. Открыть окно свойств принтера и на вкладке **Доступ (Sharing)** выбрать **Нет общего доступа к данному принтеру (Do Not Share This Printer).**

b. Открыть окно свойств принтера и выбрать порт, не связанный ни с одним печатающим устройством.

c. Открыть окно очереди печати и для каждого задания в меню **Документ (Document)** выбрать **Приостановить (Pause).**

d. Открыть окно очереди печати и в меню **Принтер (Printer)** выбрать **Приостановить печать (Pause Printing).**

Правильный ответ: d. Если выбрать параметр Приостановить печать (Pause Printing), документы останутся в очереди до возобновления печати. Этот параметр применяется ко всем документам в очереди.

Занятие 2. Закрепление материала

1. **Вы** администрируете компьютер под управлением Windows Server 2003, настроенный в качестве сервера печати. Пользователи из группы Marketing жалуются, что не могут печатать документы с помощью принтера на этом сервере. Вы просматриваете разрешения в окне свойств принтера. Группе Marketing дано разрешение *Управление документами* (Manage Documents). Почему пользователи не могут печатать на этом принтере?

   a. Разрешение *Управление документами* (Manage Documents) должно быть предоставлено группе *Все* (Everyone).

   b. Разрешение *Управление документами* (Manage Documents) должно быть предоставлено группе *Администраторы* (Administrators).

   c. Группе Marketing должно быть предоставлено разрешение *Печать* (Print).

   d. Группе Marketing должно быть предоставлено разрешение *Управление принтерами* (Manage Printers).

   Правильный ответ: c. Разрешение Печать (Print) позволяет пользователям отправлять документы на принтер.

2. Вы группируете принтеры в пул на компьютере под управлением Windows Server 2003. Пул принтеров содержит три одинаковых печатающих устройства. Вы открываете окно свойств принтера и на вкладке **Порты (Ports)** устанавливаете флажок **Разрешить группировку принтеров в пул (Enable Printer Pooling).** Что следует сделать далее?

   a. Настроить порт LPT1 для обслуживания-трех принтеров.

   b. Выбрать или создать порты, связанные с этими тремя принтерами.

   c. На вкладке **Параметры устройства (Device Settings)** настроить устанавливаемые дополнения для обслуживания двух дополнительных устройств печати.

   d. На вкладке **Дополнительно (Advanced)** настроить приоритет для каждого устройства печати, чтобы распределить задания между тремя устройствами.

   Правильный ответ: b. Группировка принтеров в пулы настраивается на вкладке Порты (Ports) в окне свойств принтера. Чтобы сгруппировать принтеры в пул, установите флажок Разрешить группировку принтеров в пул (Enable Printer Pooling), а затем выберите или создайте порты, соответствующие принтерам, которые войдут в пул.

3. **Вы** администрируете компьютер под управлением Windows Server 2003, настроенный в качестве сервера печати, и хотите управлять службами печати из Web-браузера на клиентском компьютере. Сервер называется Mktgl, но вы не знаете имя общего ресурса принтера. По какому URL следует подключаться к принтеру?

   a. http://mktgl/printers.

   b. http://printers/mktgl.

c. http://windows/web/printers.

d. http://windows/mktgl.

Правильный ответ: a. Чтобы получить доступ ко всем принтерам на сервере печати из Web-браузера, подключитесь к узлу *http://сервер_печати/printers,* чтобы просмотреть список принтеров. Отсюда вы можете получить доступ к конкретному принтеру. Если вы хотите получить доступ к определенному принтеру без просмотра списка, введите *http://сервер_печати/имя_общего_ресурса_принтера*.

4. Вам нужно настроить логический принтер так, чтобы большие документы с низким приоритетом печатались по ночам. Какие из следующих параметров необходимо настроить в окне свойств принтера?

   a. **Приоритет (Priority).**

   b. Доступен с/по (Available From/To).

   c. Начинать печать после помещения в очередь всего задания (Start Printing After Last Page Is Spooled).

   d. Печатать прямо на принтер (ускорение вывода на печать) [Print Directly To The Printer].

   e. Сохранять документы после печати (Keep Printed Documents).

   Правильный ответ: b. Расписание работы принтера позволяет ему получать задания и хранить их в очереди, пока не наступит указанное время печати. Параметр по умолчанию, Доступен всегда (Always Available), позволяет отправлять задание на принтер, когда он свободен. При настройке параметра Доступен с/по (Available From/To) указывайте время, когда задания можно отправлять на принтер.

Занятие 3. Закрепление материала

1. Компьютер под управлением Windows 2003 Server настроен в качестве сервера печати. В середине рабочего дня выходит из строя предохранитель принтера; его нужно заменить. Пользователи уже отправили задания на этот принтер по IP-адресу 192.168.1.81. Аналогичный принтер использует адрес 192.168.1.217 и обслуживается другими логическими принтерами на данном сервере. Что предпринять, чтобы напечатать задания пользователей, не отправляя их повторно?

   a. В окне свойств неисправного принтера выбрать **Разрешить группировку принтеров в пул (Enable Printer Pooling).**

   b. **В** командной строке ввести Net Stop Spooler.

   c. В командной строке ввести Net Start Spooler.

   d. В окне свойств неисправного принтера выбрать порт 192.168.1.217.

   e. В окне свойств неисправного принтера щелкнуть **Добавить порт (Add Port).**

   f. В папке **Принтеры и факсы (Printers And Faxes)** щелкнуть правой кнопкой неисправный принтер и выбрать **Отложенная печать (Use Printer Offline).**

   Правильный ответ: d. Поскольку другой принтер уже обслуживается логическими принтерами на сервере, добавлять новый порт не нужно. Просто выберите имеющийся порт.

2. Вы настраиваете печать на компьютере под управлением Windows Server 2003. Вы подключаете принтер, конфигурируете логический принтер и отправляете документы на печать, однако они не печатаются полностью и иногда искажены. Какова наиболее вероятная причина проблемы?

   a. Не хватает места на диске для очереди печати.

   b. Используется некорректный драйвер принтера.

c. Выбран неправильный порт.

d. В параметрах устройства используется неверная подстановка шрифтов.

Правильный ответ: Ь. Некорректный драйвер принтера может выдавать испорченные или не полностью напечатанные документы. Установите соответствующий драйвер принтера.

3. Какие из следующих действий дадут наиболее точное представление о нагрузке на принтер, чтобы вы знали расход тонера и бумаги?

a. Настройка аудита для логического принтера и ведение аудита успешного использования разрешения **Печать (Print)** группой *Все* (Everyone).

b. Экспорт журнала *Система* (System) в текстовый файл с разделителями — запятыми и применение Excel для анализа событий очереди печати.

c. Настройка журнала производительности и мониторинг счетчика **Всего напечатано страниц (Total Pages Printed)** для каждого логического принтера.

d. Настройка журнала производительности и мониторинг счетчика **Заданий (Jobs)** для каждого логического принтера.

Правильный ответ: с. Счетчик Всего напечатано страниц (Total Pages Printed) дает наиболее точное представление о расходе тонера и бумаги, поскольку эти значения больше всего зависят от числа напечатанных страниц, а не заданий. События очереди печати и доступа к объекту, регистрируемые в журналах Система (System) и Безопасность (Security), в лучшем случае дадут много лишней информации, но в этой ситуации, скорее всего, окажутся полностью бесполезными.

ГЛАВА 9

Обслуживание операционной системы

Темы экзамена

- Управление инфраструктурой обновления ПО.
- Управление лицензированием ПО на сайты.

В этой главе

В 2002 г. червь Code Red и его потомки Code Red v2 и Code Red II, распространявшиеся через Интернет, использовали дыру в Microsoft Index Server. Хотя сами по себе черви не причиняли большого вреда, поразительная скорость заражения вызвала шок у тысяч ИТ-профессионалов, которым пришлось потратить массу времени на защиту и обновления своих систем. Ситуация выглядела особенно тревожной, поскольку Microsoft выпустила исправление для Index Server за месяц до эпидемии. Всем, как никогда, стала очевидна необходимость своевременного обновления серверов и рабочих станций. Нет ничего хуже, чем тянуть с установкой пакета обновлений 2 до выхода 3, как это многие делали раньше. В настоящее время обновление ПО стало частью стратегии безопасности любой организации.

В этой главе вы научитесь применять службы обновления ПО для поддержания в актуальном состоянии серверов и рабочих мест. Эта служба позволяет предприятию централизовать загрузку, тестирование, утверждение и распространение критических обновлений и компонентов безопасности Windows. Она будет играть важную роль в поддержании целостности корпоративной сети. Вы также научитесь развертывать пакеты обновлений на одном или нескольких компьютерах. Наконец, вы познакомитесь с компонентами лицензирования ПО на сайты.

Прежде всего

Здесь вы познакомитесь с концепциями и получите навыки администрирования служб обновления ПО для Windows, развертывания пакетов обновлений и лицензирования. Желательно иметь в наличии два компьютера (один с Windows Server 2003 и клиент Windows XP или Windows 2000 Professional).

Для изучения материалов этой главы вам потребуются:

- компьютер под управлением Microsoft Windows Server 2003 Standard или Enterprise, установленный как ServerOl и настроенный в качестве контроллера домена contoso.com;
- ОП первого уровня Desktops;
- сеть с возможностью выхода в Интернет.

Занятие 1. **Службы обновления ПО**

Для защиты компьютерной среды важно своевременно устанавливать исправления для системы безопасности. С 1998 г. Microsoft поддерживает сервер Windows Update — Web-источник информации и обновлений. В Windows XP и SP3 для Windows 2000 Microsoft добавила службу *Автоматическое обновление* (Automatic Updates), которая позволяет системе автоматически подключаться к серверу Windows Update и загружать необходимые исправления. Хотя серверы Windows Update и клиенты службы автоматического обновления эффективно решают проблему поддержания системы в актуальном состоянии, многие администраторы сочли бы неправильным, если бы исправления устанавливали пользователи или сами компьютеры, поскольку некорректная установка может нарушить работу бизнес-приложений.

Последнее усовершенствование этих технологий — *службы обновления ПО* (Software Update Services, SUS) — клиент-серверное приложение, позволяющее серверу в вашей интрасети играть роль точки администрирования обновлений. Вы можете утверждать обновления для клиентов SUS, которые автоматически загрузят и установят их без вмешательства местного администратора.

На этом занятии вы научитесь устанавливать SUS и управлять этими службами на компьютере под управлением Windows Server 2003. Кроме того, здесь обсуждаются вопросы, связанные с конфигурацией клиента.

Изучив материал этого занятия, вы сможете:

- ✓ установить и настроить SUS на компьютере под управлением Windows Server 2003;
- ✓ установить и развернуть службу *Автоматическое обновление* для клиентов SUS;
- ✓ управлять службами SUS и *Автоматическое обновление;*
- ✓ наблюдать за работой, устранять неполадки, архивировать и восстанавливать SUS.

Продолжительность занятия — около 30 минут.

Понятие SUS

С 1998 г. ОС семейства Microsoft Windows поддерживают Windows Update — глобальный источник обновлений. Серверы Windows Update взаимодействуют с ПО на стороне клиента, чтобы выявлять критические обновления, компоненты безопасности и улучше-

ния, которые применимы для платформы клиента, и затем загружать утвержденные исправления.

Администраторам необходимо более централизованное решение, которое могло бы обеспечить более четкое управление обновлениями, устанавливаемыми на компьютеры клиентов. Для этого и предназначены службы SUS, которые содержат следующие основные компоненты.

- **Службы обновления ПО, запущенные на сервере IIS.** Компонент на стороне сервера отвечает за синхронизацию информации о доступных обновлениях и, как правило, за загрузку обновлений с интернет-серверов Windows Update или с серверов в интрасети, где работает SUS.
- **Web-узел управления SUS.** Службами SUS управляют через Web-интерфейс. После установки и настройки SUS администрирование обычно подразумевает гарантию успешной синхронизации сервера SUS и утверждение обновлений для распространения сетевым клиентам.
- **Служба *Автоматическое обновление*.** Клиент службы *Автоматическое обновление* отвечает за загрузку обновлений с сервера Windows Update или сервера SUS и их установку по расписанию или по запросу администратора.
- **Параметры групповой политики.** Клиенты службы *Автоматическое обновление* можно настроить для синхронизации с сервером SUS вместо серверов Windows Update. Для этого нужно изменить реестры клиентов или, что более эффективно, настроить политики Windows Update в объекте групповой политики (ОГП).

Установка SUS на компьютере под управлением Windows Server 2003

SUS состоит из клиентского и серверного компонентов. Серверный компонент работает на компьютере под управлением Windows 2000 Server (SP2 или выше) или Windows Server 2003. Службы IIS должны быть установлены до настройки SUS. Как вы узнали из главы 6, в Windows Server 2003 IIS по умолчанию не устанавливается.

Служб SUS нет на установочном компакт-диске Windows Server 2003, но их можно бесплатно загрузить по адресу *http://go.microsoft.com/fwlink/?LinkID=6930*.

Примечание Интерфейс служб SUS переведен не на все языки, для которых есть версии Windows. Однако загружаемый установочный файл служб SUS определяет интерфейс управления и установки только для серверного компонента. Средствами SUS можно загружать исправления для версий ОС на любых языках.

Загрузив последнюю версию SUS, дважды щелкните файл, чтобы запустить программу установки. Согласившись с лицензионным соглашением, выберите Custom setup, после чего мастер установки предложит вам ввести следующую информацию.

- **Choose File Locations.** Каждое исправление Windows Update состоит из двух компонентов: самого файла исправления и метаданных, определяющих платформы и языки, к которым применимо исправление. SUS всегда загружает метаданные, которые вы будете использовать для утверждения обновлений, а клиенты интрасети — получать от SUS. Вы можете указать, нужно ли загружать сами файлы обновлений, и куда их сохранять.

Совет Если вы решили использовать файлы обновлений на серверах Microsoft Windows Update, клиенты службы *Автоматическое обновление* будут подключаться к серверу SUS, чтобы получить список утвержденных обновлений, а затем — к серверам Microsoft Windows Update, чтобы загрузить утвержденные файлы. Таким образом вы можете управлять процессом обновления и пользоваться преимуществами глобальной доступности обновлений от Microsoft.

Если вы выберете **Save The Updates To This Local Folder,** мастер установки по умолчанию создаст папку с именем SUS на диске с наибольшим объемом свободного места. Сохранить файлы можно на любом разделе NTFS; Microsoft рекомендует, чтобы на нем было минимум 6 Гб свободного места.

Примечание Раздел SUS и системный раздел должны быть отформатированы под NTFS.

- **Language Settings.** Хотя интерфейс управления SUS кроме английского переведен всего на несколько языков, исправления выпускаются для всех поддерживаемых языков. Этот параметр определяет локализованные версии серверов и клиентов Windows, которые поддерживаются в вашей среде.
- **Handling New Versions Of Previously Approved Updates.** Иногда обновляются сами обновления. Вы можете указать SUS автоматически утверждать обновления, которые являются новыми версиями ранее утвержденных исправлений, либо по-прежнему утверждать каждое обновление вручную.
- **Ready To Install.** Прежде чем запустить установку, мастер напомнит вам, что клиенты должны использовать URL *http://имя_сервера_SUS*. Запишите этот путь, поскольку он потребуется вам для настройки сетевых клиентов.
- **Installing Microsoft Software Update Services.** Мастер Setup Wizard устанавливает SUS.
- **Completing the Microsoft Software Update Services Setup Wizard.** Последняя страница мастера установки сообщает адрес Web-узла управления SUS — *http://имя_сервера_SUS/SUSAdmin*. Запишите и этот путь, поскольку будете управлять SUS с данного Web-узла. Когда вы щелкните кнопку **Готово (Finish),** автоматически запустится браузер и загрузится административная страница SUS.

Следующие компоненты устанавливаются службами SUS на сервер:

- служба Software Update Synchronization Service, загружающая содержимое сервера SUS;
- Web-узел IIS, обслуживающий запросы на обновление от клиентов службы автоматического обновления;
- Web-страница управления SUS, с которой можно синхронизировать сервер SUS и утверждать обновления.

Мастер IIS Lockdown

На сервере Windows 2000 мастер установки SUS запускает мастер IIS Lockdown, чтобы настроить безопасность IIS 5.0. Windows Server 2003 заблокирован по умолчанию, поэтому запуск IIS Lockdown не требуется.

Установка SUS может нарушить работу Web-приложений на сервере IIS. Вы можете повторно включить фильтры ISAPI и открыть другие компоненты, защищенные мастером IIS Lockdown. Тем не менее, из-за хрупкой натуры обновлений для ОС рекомендуется установить SUS на выделенном сервере, отдельно от других приложений IIS.

Настройка и администрирование SUS

На Web-узле управления SUS (рис 9-1) вы выполните три административные задачи: настроите параметры SUS, синхронизируете и утвердите содержимое. В Internet Explorer 5.5 (или выше) введите адрес *http://имя_сервера_SUS/SUSAdmin* или откройте Microsoft Software Update Services из группы программ **Администрирование (Administrative Tools).** Администрирование SUS осуществляется исключительно через Web-интерфейс.

Примечание Вам может потребоваться добавить Server01 в список надежных узлов локальной интрасети, чтобы получить к нему доступ. Откройте Internet Explorer и в меню **Сервис (Tools)** выберите **Свойства** обозревателя **(Internet Options).** Перейдите на вкладку **Безопасность (Security).** Щелкните значок **Надежные узлы (Trusted Sites),** затем кнопку **Узлы (Sites).** Добавьте ServerOl и Server01.contoso.com в список надежных узлов.

Примечание Правом управления службами SUS обладает только локальный администратор сервера SUS. Это еще одна причина установить SUS на отдельный сервер. Выделенный сервер SUS позволяет делегировать полномочия на администрирование SUS, не рискуя случайно открыть доступ к другим ролям сервера и приложениям.

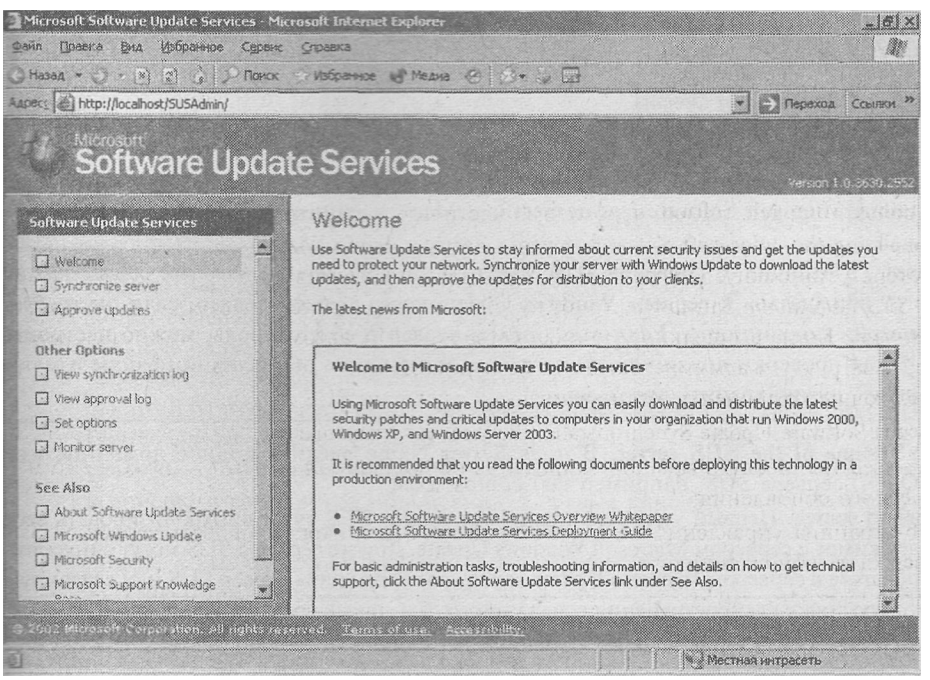


Рис. 9-1. Web-узел администрирования SUS

Настройка служб SUS

Хотя некоторые параметры SUS настраиваются во время выборочной установки, доступ ко всем параметрам можно получить на Web-странице управления SUS: щелкните **Set Options** на навигационной панели слева. Откроется страница **Set Options** (рис. **9-2).**

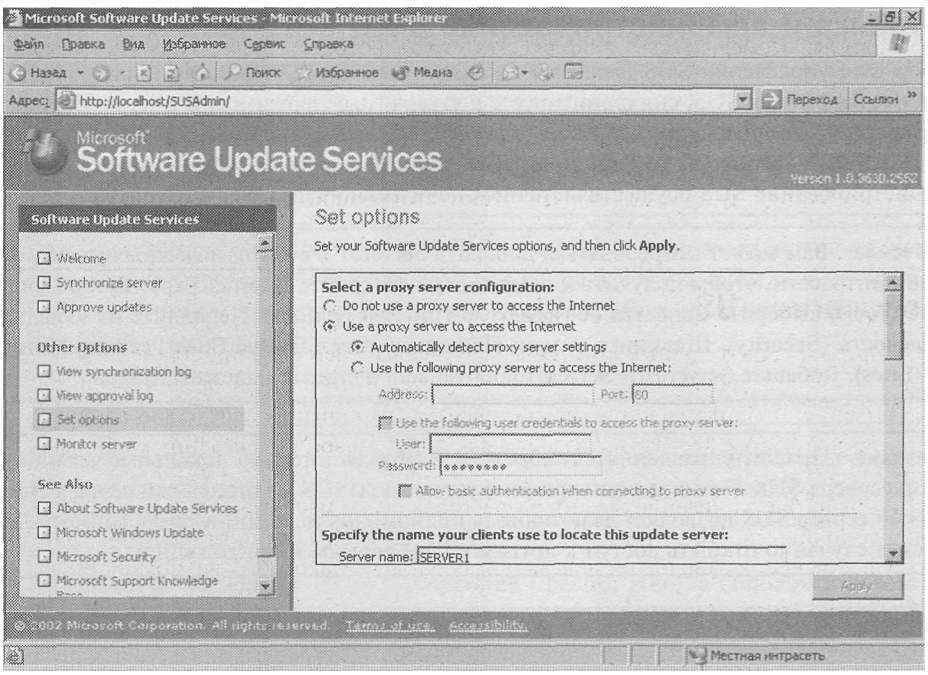


Рис. 9-2. Страница *Set Options*

Параметры конфигурации таковы.

- **Proxy server** configuration. Если сервер SUS соединяется с сервером Windows Update, используя прокси-сервер, необходимо настроить параметры прокси.

  Совет В отличие от серверов SUS, клиенты службы *Автоматическое обновление* не могут обращаться к серверу Windows Update через прокси-сервер, если он требует проверки подлинности. Если ваш прокси-сервер требует пароль, можно настроить SUS для проверки подлинности; тогда все содержимое обновлений (файлы и метаданные) нужно хранить локально.

- **DNS name of the SUS server. В** поле Server Name введите полное доменное имя (FQDN) сервера SUS, например susl.contoso.com.
- **Content source.** Первый установленный вами сервер SUS будет синхронизировать свое содержимое с сервером Microsoft Windows Update. Другие серверы SUS могут синхронизироваться с сервером Windows Update через «родительский» сервер SUS или созданную вручную точку распространения содержимого. См. также врезку «Топология SUS».
- **New versions of approved updates.** Страница **Set Options** позволяет указать, как службы SUS должны обрабатывать новые версии ранее утвержденных обновлений. Данный параметр обсуждался выше.
- **File storage.** Указывает место хранения метаданных и файлов обновлений. Данный параметр также обсуждался выше.

  Совет Если вы перенесли место хранения с сервера Windows Update на локальный сервер, немедленно выполните синхронизацию, чтобы загрузить нужные пакеты в указанное местоположение.

- Languages. Определяет синхронизированные обновления, характерные для конкретной страны. Выберите языки только тех стран, которые поддерживаются в вашей среде.

Совет При удалении поддерживаемого языка уже загруженные пакеты не удаляются, однако клиенты их больше не получат. При добавлении языка выполните синхронизацию вручную, чтобы загрузить соответствующие пакеты для нового языка.

Топология SUS

SUS предоставляют полный контроль над утверждением и распространением обновлений с серверов Microsoft Windows Update. В небольшой организации для размещения SUS достаточно одного сервера, синхронизирующего обновления с серверами Windows Update и предоставляющего список утвержденных обновлений клиентам.

В крупной организации можно разработать более масштабируемую и эффективную топологию SUS. Хотя экзамен требует навыков администрирования только существующих топологий, полезно разобраться в некоторых возможностях **их** построения.

- **Топология из нескольких серверов.** Каждый сервер SUS синхронизирует содержимое с Windows Update и управляет собственным списком утвержденных обновлений. Этот подход — вариация модели с одним сервером; администратор каждого сервера SUS управляет своим списком утвержденных обновлений. Такая топология позволяет организации поддерживать различные конфигурации исправлений и обновлений (по одной для каждого сервера SUS). Клиентов можно направить к серверу SUS, содержащему соответствующий список утвержденных обновлений.
- **Строгая топология родитель — потомок.** Родительский сервер SUS синхронизирует содержимое с сервером Windows Update и хранит обновления в локальной папке. Затем администратор SUS утверждает обновления. Другие серверы SUS предприятия синхронизируют содержимое с родительским сервером. Для этого на странице **Set Options** надо выбрать параметр **Synchronize List Of Approved Items Updated From This Location (Replace Mode),** который указывает дочерним серверам SUS синхронизировать и файлы обновлений, и список утвержденных обновлений. Сетевые клиенты могут получать обновления от сервера SUS в своем или ближайшем сайте. В такой конфигурации **(Synchronize List Of Approved Items)** администраторы дочерних серверов SUS не могут утверждать или отменять обновления; эта задача решается только на родительском сервере SUS.
- **Нестрогая топология родитель — потомок.** Родительский сервер SUS синхронизирует содержимое с сервером Windows Update и хранит обновления в локальной папке. Остальные серверы SUS предприятия синхронизируют содержимое с родительским сервером. В отличие от строгой конфигурации, дополнительные серверы SUS не синхронизируют список утвержденных обновлений, поэтому их администраторы могут утверждать и отменять обновления самостоятельно. Хотя такая топология увеличивает накладные расходы по администрированию, она полезна, когда организация стремится максимально

сократить связь с Интернетом (только родительскому серверу SUS требуется соединение с Интернетом) и использовать (как в модели с несколькими серверами) возможности распределенного утверждения обновлений или различные конфигурации исправлений и обновлений на клиентах.

- **Проверочная/производственная** топология. Эта модель позволяет организации проверять обновления, то есть внедрять их поэтапно. Родительский сервер SUS загружает обновления с сервера Windows Update, и администратор утверждает обновления, которые нужно проверить. Один или несколько клиентов запрашивают обновления у родительского сервера SUS и играют роль проверочных платформ. После утверждения и проверки обновлений содержимое родительского сервера SUS копируется в созданную вручную точку распространения содержимого на втором сервере IIS. Производственные серверы SUS синхронизируют и обновления, и список утвержденных обновлений с этой точкой ручного распространения содержимого (описание ее настройки — в официальном документе по развертыванию служб SUS на Web-узле Microsoft, посвященном SUS).

Синхронизация SUS

На Web-странице управления SUS щелкните Synchronize Server. Страница Synchronize Server (рис. 9-3) позволяет начать синхронизацию вручную или настроить ее расписание. Щелкните Synchronize Now. После завершения синхронизации появится сообщение о ее результатах. Если она выполнена успешно, откроется страница Approve Updates.

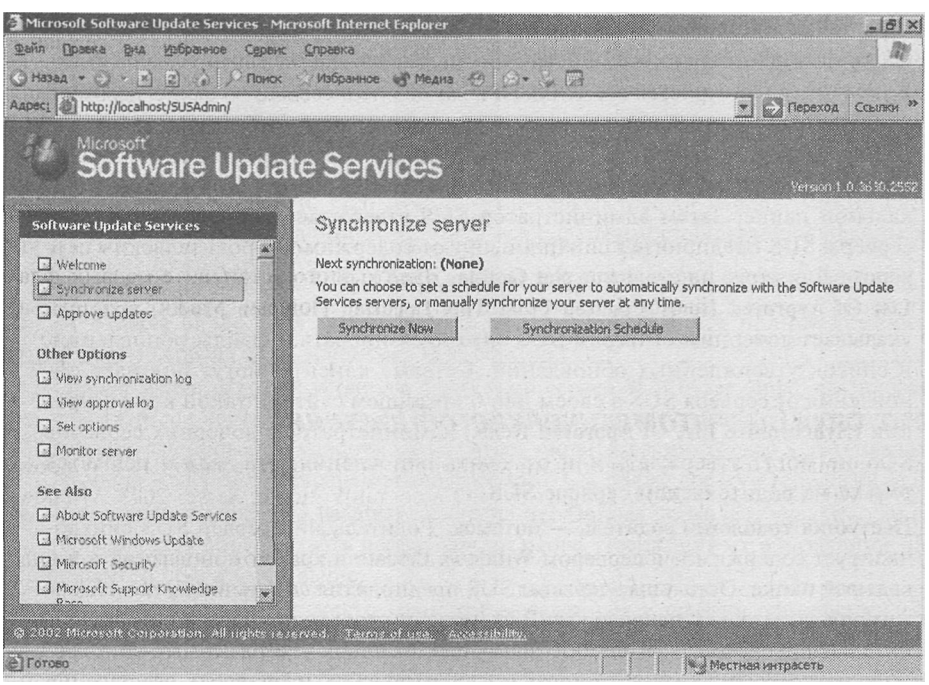


Рис. 9-3. Страница *Synchronize Server*

Чтобы составить расписание синхронизации, щелкните **Synchronization Schedule. В** открывшемся окне (рис. 9-4) можно настроить время и периодичность синхрониза-

ции (ежедневно или по указанным дням недели). Параметр **Number Of Synchronization Retries To Attempt** указывает, сколько раз SUS будет пытаться повторить синхронизацию в случае ее неудачи. Повторные попытки предпринимаются каждые 30 минут.

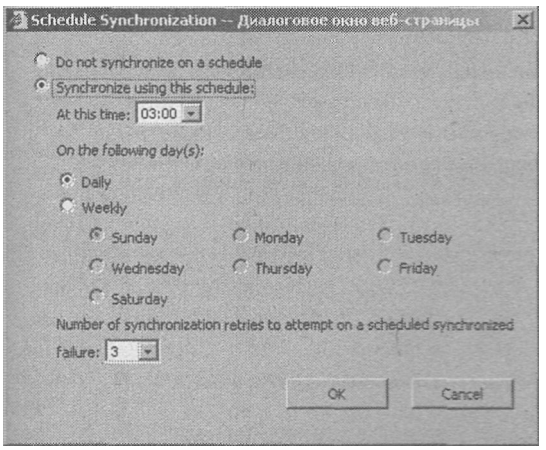


Рис. 9-4. Страница *Schedule Synchronization — Диалоговое окно веб-страницы*

Утверждение обновлений

Чтобы утвердить обновления для распространения на клиентские компьютеры, щелкните **Approve Updates** на навигационной панели слева. Откроется страница **Approve updates** (рис. 9-5). Выберите нужные обновления и щелкните **Approve.** Если вы не уверены в применимости конкретного обновления, щелкните ссылку **Details** в кратких сведениях об обновлении. Откроется страница **Details,** где дана ссылка на фактический файл *.cab, используемый для установки пакета, и ссылка на страницу **Read More** со сведениями об обновлении (открывает статью в базе знаний Microsoft, связанную с данным обновлением).

Совет При первой синхронизации загружается масса обновлений. Просмотреть и утвердить каждое обновление — нелегкая задача. Вместо этого установите первый флажок, дважды нажмите клавишу Tab, чтобы перейти к следующему флажку, а затем нажмите пробел, чтобы выбрать (или исключить) пункт.

Клиент службы *Автоматическое обновление*

Windows Automatic Updates — клиентский компонент SUS, поддерживаемый в Windows 2000, XP и Windows Server 2003. Клиент входит в состав Windows Server 2003, Windows 2000 SP3 и Windows XP SP1.

Для предыдущих версий поддерживаемых платформ клиент можно загрузить в виде отдельной программы с Web-узла SUS по адресу *http://go.microsoft.com/fwlink/?LinkID=6930.* Клиент, распространяемый в виде файла .msi, можно установить на изолированный компьютер или распространить средствами групповой политики [назначьте этот пакет в политике **Конфигурация компьютера (Computer Configuration)\Конфигурация программ (Software Settings)],** с помощью MS SMS или даже через сценарий входа. Если версии клиента для вашего языка нет, на любую локализованную версию Windows можно установить его английскую версию.

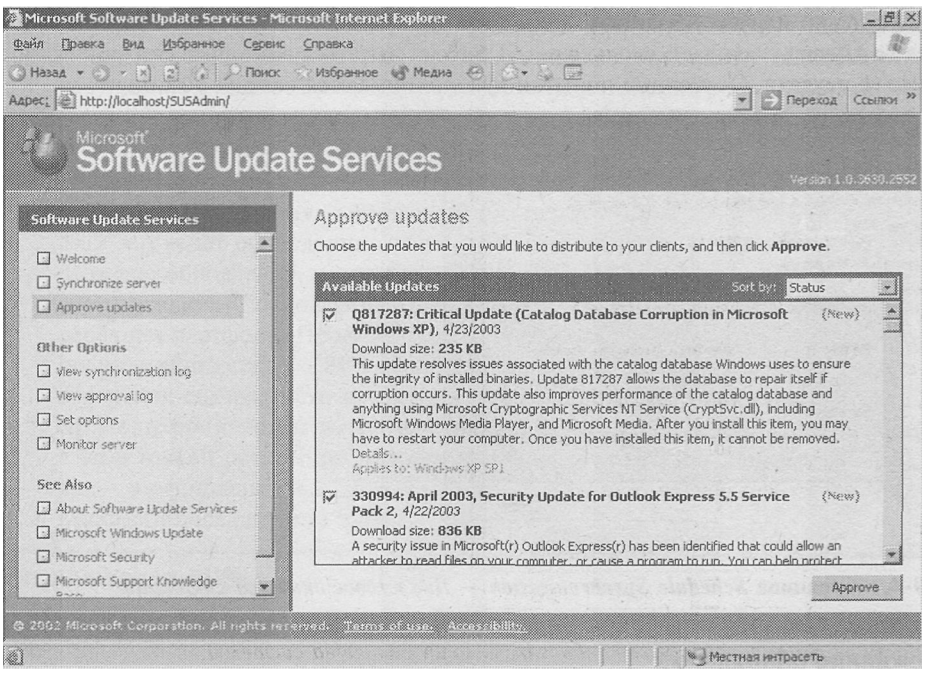


Рис. 9-5. Страница *Approve updates*

По умолчанию клиент службы автоматического обновления в Windows Server 2003 автоматически подключается к серверу Microsoft Windows Update, загружает обновления, а затем предлагает пользователю установить их. Это поведение можно изменить на вкладке **Автоматическое обновление (Automatic Updates)** в окне **Свойства системы (System Properties).** Чтобы открыть его, щелкните значок **Система (System)** в *Панели управления* в Windows XP или Windows Server 2003 или **Automatic Updates** в Windows 2000. Клиент также можно настроить с помощью ОГП или значений в реестре.

Режим загрузки

Клиент службы *Автоматическое обновление* поддерживает два режима загрузки.

- **Автоматический режим.** Обновления загружаются без уведомления пользователя.
- С **уведомлением.** Если клиент настроен на предупреждение пользователя перед загрузкой обновлений, он записывает уведомление о доступном обновлении в журнал событий системы и сообщает об этом администратору, вошедшему на данный компьютер. Если администратор не входит на компьютер, клиент ждет пользователя с реквизитами администратора, чтобы уведомить его всплывающим сообщением на системной панели.

Во время загрузки клиент службы автоматического обновления использует службу BITS (Background Intelligent Transfer Service) для передачи файлов во время моментов простоя сети. BITS гарантирует, что передача файлов не снизит производительность сети. Сервер SUS проверят, чтобы все исправления были подписаны Microsoft. Аналогично, клиент подтверждает подпись Microsoft, плюс вычисляет контрольную сумму (CRC) каждого пакета перед установкой.

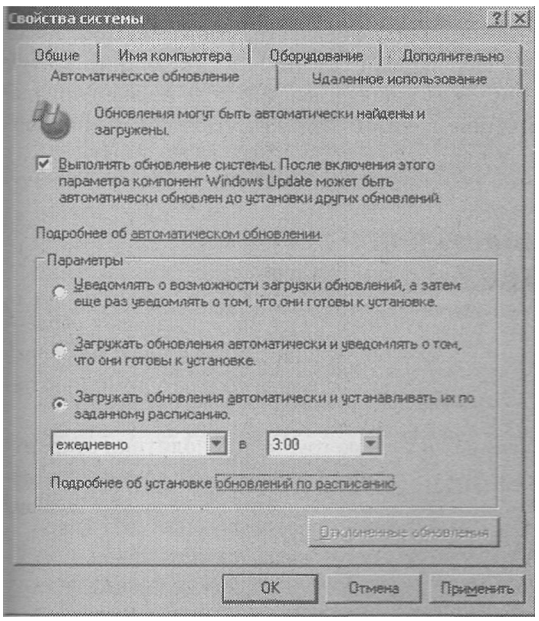


Рис. 9-6. Вкладка *Автоматическое обновление* окна *Свойства системы*

Режим установки

Служба *Автоматическое обновление* поддерживает два режима установки.

- С уведомлением. Служба регистрирует в журнале системы событие, указывающее, что обновления готовы к установке. Уведомление будет показано, когда на компьютер войдет локальный администратор. Когда это произойдет, на системной панели появится всплывающее сообщение. Щелкнув воздушный шарик или значок уведомления, администратор может выбрать нужные обновления из доступных, после чего щелкнуть Install. Если обновление требует перезагрузки компьютера, клиент не сможет определить дополнительные обновления, применимые к вашей системе, без перезагрузки.
- **Automatic (Scheduled).** Когда обновления успешно загружены, в журнал системы записывается соответствующее событие. Если администратор входит в систему, появляется значок уведомления, и установку можно запустить вручную, не дожидаясь запланированного времени.

  Когда наступает момент запланированной установки, вошедшему в систему администратору выдается сообщение с обратным отсчетом времени до установки. В это время можно отменить установку, тогда она откладывается до следующего запланированного в расписании времени. Если в этот момент в системе работает не администратор, появляется предупреждение, однако пользователь не может отложить установку. Если ни один пользователь не вошел в систему, установка выполняется автоматически. Если обновление требует перезагрузки, появляется сообщение с обратным отсчетом пяти минут, информирующее пользователей о скорой перезагрузке. Отменить такую перезагрузку вправе только администратор.

Совет Если компьютер выключен в тот момент, когда должна произойти автоматическая установка, она переносится на следующее запланированное в расписании время. Если в это время компьютер выключен постоянно, установка никогда не выполнится. Убедитесь, что компьютер остается включенным, чтобы автоматическая установка обновлений выполнялась успешно.

Настройка автоматических обновлений средствами групповой политики

Клиент службы *Автоматическое обновление* по умолчанию будет подключаться к серверу Microsoft Windows Update. После установки SUS можно перенаправить клиент на сервер SUS в интрасети, изменив реестр клиентского компьютера вручную или с помощью параметров групповых политик Windows Update.

Для настройки автоматических обновлений с помощью групповой политики откройте ОГП и раскройте узел **Конфигурация компьютера (Computer Configuration)\Административ-ные шаблоны (Administrative Templates)\Компоненты Windows (Windows Components)\Windows Update.** Перечень политик Windows Update показан на рис. 9-7.

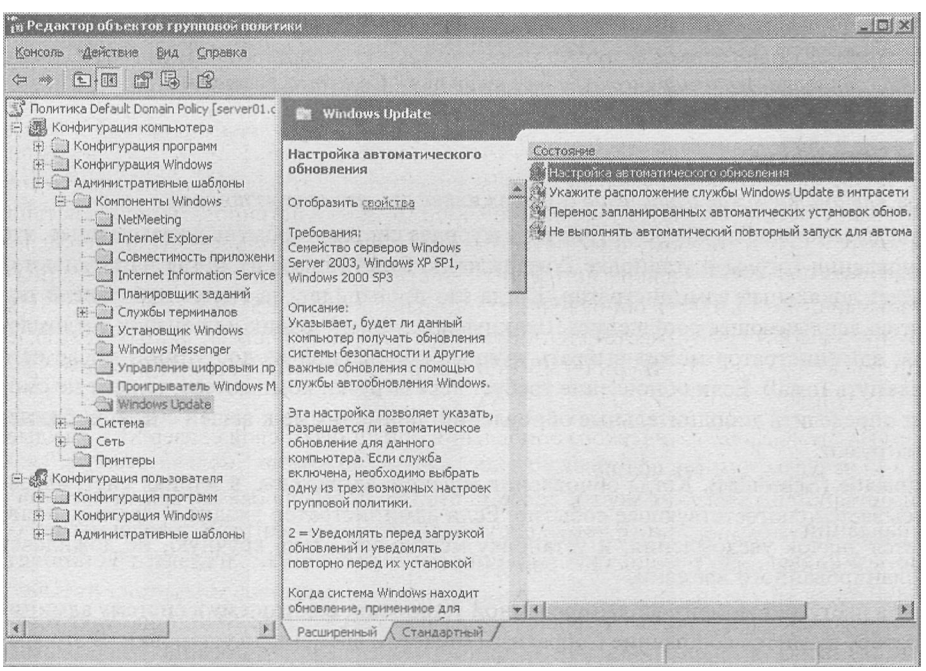


Рис. 9-7. Политики Windows Update

Примечание Если вы редактируете политику на сервере Windows 2000 Active Directory, эти политики могут не отображаться. Политики службы *Автоматическое обновление* описаны в административном шаблоне *%Windir%*\Inf\Wuau.inf, который по умолчанию устанавливается вместе с службой. Если клиент не установлен на контроллере домена, к которому вы подключены (обычно это эмулятор PDC), то щелкните узел **Административные шаблоны (Administrative Templates)** правой кнопкой, выберите **Добавление и удаление шаблонов (Add/ Remove Templates),** щелкните Добавить **(Add)** и найдите шаблон Wuau.inf (возможно, вам придется скопировать его из системы, где установлен клиент службы).

Доступны следующие политики, каждая из которых играет важную роль для настройки эффективного распространения обновлений.

- **Настройка автоматического обновления (Configure Automatic Updates).** Определяет поведение клиента службы автоматического обновления. Предусмотрено три варианта: **Уведомлять перед загрузкой обновлений и уведомлять повторно перед их установкой (Notify For Download And Notify For Install), Загружать автоматически и уведомлять перед установкой (Auto Download And Notify For Install)** и **Загружать автоматически и устанавливать по заданному расписанию (Auto Download And Schedule The Install).** Эти варианты — комбинации режимов установки и загрузки, которые обсуждались ранее.
- **Перенос запланированных автоматических установок** обновлений **(Reschedule Automatic Updates Scheduled Installations).** Если клиентский компьютер выключен в тот момент, когда должна выполняться автоматическая установка, по умолчанию она переносится на следующее запланированное в расписании время. Если этой политике присвоено значение от 1 до 60, обновления будут установлены спустя указанное количество минут после загрузки системы.
- **Не выполнять автоматический повторный запуск для автоматических установок обновлений (No Auto-Restart For Scheduled Automatic Updates Installations).** Запрещает клиенту перезагружать компьютер (как того требует установленное обновление), когда какой-либо пользователь работает в системе. Вместо этого пользователь после уведомления сам решает, когда нужно перезагрузить компьютер. Помните, что служба *Автоматическое обновление* не может обнаружить новые обновления до перезагрузки.
- **Укажите расположение службы Windows Update в интрасети (Specify Intranet Microsoft Update Service Location).** Позволяет перенаправить клиент службы *Автоматическое обновление* на сервер SUS. По умолчанию клиент будет регистрировать свои действия не сервере SUS, к которому подключается. Эта политика позволяет направить клиент на другой сервер IIS для регистрации статистики. Такая «двойная» политика позволяет клиентам загрузить обновления с локального сервера SUS, а статистику SUS регистрировать в одном месте для упрощения поиска и анализа данных, которые хранятся в журнале IIS. Журнал IIS обычно расположен в папке *%Windir%\System32\Logfiles\W3svc1*.

Клиенты службы автоматического обновления опрашивают свой сервер SUS каждые 22 часа минус случайное смещение.

При обнаружении слабых мест в системе безопасности любая задержка установки исправлений недопустима. В таких ситуациях устанавливайте исправления вручную, не дожидаясь, пока ваши системы опросят сервер SUS, загрузят и установят исправления.

После того как утвержденные обновления загружены с сервера SUS, они будут установлены согласно настройкам (вручную или автоматически) в предписанное время. Отмена ранее утвержденного обновления не означает, что его установка также будет отменена, просто оно не будет установлено очередными клиентами. Установленное обновление можно удалить вручную, используя приложение **Установка и удаление программ [Add Or Remove Programs)** из *Панели управления*.

Устранение неполадок SUS

Хотя службы SUS работают стабильно, существуют ситуации, требующие внимания и устранения неполадок.

Наблюдение за работой SUS

Страница **Monitor Server** на Web-узле управления SUS содержит статистику, отражающую количество обновлений, доступных для каждой платформы, а также дату и время последнего обновления. Эти сведения извлекаются из метаданных Windows Update, которые загружаются при каждой синхронизации. Метаданные записываются на диск и хранятся в памяти, чтобы системы быстрее получали запрошенные обновления для своих платформ.

Следующие журналы позволяют следить за SUS и службой *Автоматическое обновление.*

- **Synchronization Log.** Содержит информацию о текущих и прошедших операциях синхронизации и загруженных пакетах. Чтобы просмотреть журнал, щелкните **View Synchronization Log** на навигационной панели слева. Вы также можете открыть файл БД — History-Sync.xml — в любом текстовом редакторе прямо из каталога \AutoUpdate\Administration Web-узла SUS в IIS.
- **Approval Log.** Для получения информации об утвержденных пакетах щелкните **View Approval Log** на навигационной панели слева. Либо откройте файл History-Approve.xml из каталога \AutoUpdate\Administration Web-узла SUS в IIS.
- **Windows Update Log.** Клиенты службы автоматического обновления регистрируют свои действия в журнале % *Windir%*\Wmdows Update.log на локальном жестком диске клиента.
- **Wutrack.bin.** Взаимодействие клиента с сервером SUS регистрируется в журналах IIS на указанном сервере статистики, которые обычно хранятся в папке %Windir%\System32\Logfiles \W3svcl. Эти подробные и непонятные журналы анализируются специальными программами, а не людьми.

Подготовка к экзамену Хотя вы должны знать, какие журналы существуют и где они находятся, для сдачи экзамена необязательно разбираться в их запутанных сообщениях и записях. Официальный документ по развертыванию SUS содержит приложения, где подробно описаны события и синтаксис журналов.

Системные события SUS

Служба синхронизации регистрирует в журнале событий каждую операцию синхронизации или утверждения обновления, выполненную сервером. Эти сообщения можно просмотреть в журнале *Система* (System log) из консоли *Просмотр событий* (Event Viewer). События касаются следующих ситуаций.

- **Подключиться не удалось (Unable to connect).** Служба *Автоматическое обновление* не может подключиться к службе обновления (серверу Windows Update или назначенному для данного компьютера серверу SUS).
- **Готовность к установке — без расписания (Install ready — no recurring schedule).** Обновления, перечисленные в событии, загружены и ожидают установки. Администратор должен щелкнуть значок уведомления, а затем Install.
- **Готовность к установке — по расписанию (Install ready — recurring schedule).** Обновления, перечисленные в событии, загружены и будут установлены в указанную дату и время.
- **Установка выполнена успешно (Installation success).** Обновления, перечисленные всобытии, были успешно установлены.
- **Установка не выполнена (Installation failure).** Обновления, перечисленные в событии установить не удалось.

- **Требуется перезагрузка — без расписания (Restart required — no recurring schedule).** Обновления требуют перезагрузки. Если режим установки требует уведомления, сервер необходимо перезагрузить вручную. Windows не найдет новые обновления, пока компьютер не будет перезагружен.
- **Требуется перезагрузка — по расписанию (Restart required — recurring schedule).** Когда клиент настроен для автоматической установки обновлений, событие регистрируется, если обновление требует перезагрузки компьютера. Перезапуск произойдет в течение пяти минут. Windows не найдет новые обновления, пока компьютер не будет перезагружен.

Устранение неполадок SUS

Для устранения неполадок SUS в Windows Server 2003 могут потребоваться следующие действия.

- **Перезагрузка кэша памяти.** Если с момента последней синхронизации новые обновления не появились, возможно, их просто нет. Однако есть вероятность, что кэши памяти неправильно загружают новые обновления. На Web-узле управления SUS щелкните **Monitor Server,** а затем **Refresh.**
- **Перезапуск службы синхронизации.** Если вы получили сообщение, что служба синхронизации работает неправильно, или вам не удается изменить параметры на странице **Set Options** Web-узла управления SUS, откройте консоль *Службы* (Services), щелкните правой кнопкой узел **Software Update Services Synchronization Service** и выберите **Перезапустить (Restart).**
- **Перезапуск IIS.** Если вам не удается подключиться к Web-узлу управления SUS, или клиенты не могут подключиться к серверу SUS, перезапустите *Службу веб-публикации* (World Wide Web Publishing Service) аналогичным способом.

Если клиенты службы *Автоматическое обновление* не получают обновления правильно, откройте реестр на клиентском компьютере и убедитесь, что раздел HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate содержит следующие значения:

- **WUServer** — должен содержать URL SUS-сервера, например *http://имя_сереера_SUS;*
- **WUStatusServer** — должен содержать URL для того же сервера SUS или для другого сервера IIS, где регистрируется статистика синхронизации.

В подразделе AU:

- **UseWUServer** — должно быть задано значение dword:00000001.

Архивация и восстановление SUS

Как и для других ролей сервера или приложений, вы должны спланировать восстановление службы SUS на случай сбоя сервера.

Архивация SUS

Для создания резервной копии SUS необходимо заархивировать папку с содержимым SUS, Web-узел управления SUS и метабазу IIS.

Подготовка к экзамену Описанный процесс резервного копирования метабазы IIS подходит не только для архивации SUS, но и для копирования любого другого Web-узла или приложения, работающего с Windows Server 2003 и IIS 6.0.

Сначала заархивируйте метабазу — БД в формате XML, содержащую конфигурацию IIS. Откройте оснастку IIS, щелкните копируемый сервер, в меню **Действие (Action)** выберите **Все задачи (All Tasks),** а затем **Архивирование и восстановление конфигурации (Backup/Restore Configuration).** Щелкните **Создать архив (Create Backup)** и введите имя резервной копии. Щелкните **OK**, чтобы заархивировать метабазу.

Затем с помощью Ntbackup или другого средства архивации создайте резервную копию:

- Web-узла по умолчанию, который обычно размещен в папке C:\Inetpub\Wwwroot;
- Web-узла управления SUS; по умолчанию SUSAdmin — подпапка каталога C:\Inetpub\Wwwroot. В этом случае, он будет заархивирован вместе со Web-узлом по умолчанию;
- виртуального каталога AutoUpdate, который также по умолчанию является подпапкой каталога C:\Inetpub\Wwwroot;
- размещения содержимого SUS, указанного при установке или настройке SUS. Если вы забыли, где находится содержимое SUS, в диспетчере IIS щелкните **Веб-узел по умолчанию (Default Web Site)** и посмотрите на правой панели путь к виртуальному каталогу содержимого;
- резервного каталога метабазы, *%Windir%*\System32\Inetsrv\Metaback, который содержит предыдущую копию метабазы.

Примечание Подробнее о программе Ntbackup — в главе 7.

Резервное копирование метабазы и компонентов SUS следует выполнять регулярно, поскольку обновления будут добавляться и утверждаться с определенной частотой.

Восстановление сервера SUS

Для восстановления вышедшего из строя сервера SUS сделайте следующее. Ненужные шаги можно пропускать, но действия должны быть выполнены именно в таком порядке.

1. Отключите сервер от сети, чтобы исключить заражение вирусами.
2. Установите Windows Server 2003 и убедитесь, что серверу присвоено прежнее имя.
3. Установите IIS с теми же компонентами.
4. Установите последний пакет обновлений и исправления безопасности. Если для этого сервер необходимо подключить к сети, примите все меры предосторожности, чтобы предотвратить нежелательный доступ.
5. Установите SUS в прежнюю папку.
6. С помощью Ntbackup восстановите последнюю резервную копию SUS. Она включает папку с содержимым SUS, Web-узел по умолчанию, включая виртуальные каталоги SUSAdmin и AutoUpdate, а также метабазу IIS.
7. Откройте оснастку IIS и выберите сервер, который нужно восстановить. В меню **Действие (Action)** выберите **Все задачи (All Tasks),** затем **Архивирование и восстановление конфигурации (Backup/Restore Configuration)** и укажите нужный архив. Щелкните **Восстановить (Restore).**
8. Убедитесь в успехе восстановления, открыв Web-узел управления SUS и щелкнув **Set Options.** Проверьте, сохранились ли прежние параметры и сведения об утвержденных ранее обновлениях.

имечание Перечисленные действия применимы только к Windows Server 2003. Провосстановления сервера SUS под управлением Windows 2000 описан в документаKSUS.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Вы настраиваете инфраструктуру служб обновления ПО. Один сервер синхронизирует метаданные и содержимое с сервером Windows Update. Остальные серверы (по одному в каждом сайте) синхронизируют содержимое с родительским сервером SUS. Что необходимо, выполнить для окончательной настройки инфраструктуры SUS?
   a. Настроить клиенты службы *Автоматическое обновление,* используя *Панель управления* на каждой системе.
   b. Настроить объекты групповой политики, чтобы направить клиенты на серверы SUS в своих сайтах.
   c. Настроить точку ручного распространения содержимого.
   d. Утвердить обновления на Web-странице управления SUS.
2. Вы настраиваете службу SUS для группы Web-серверов и хотите, чтобы они обновлялись каждую ночь согласно списку утвержденных обновлений на вашем сервере SUS. Иногда по вечерам администратор входит в систему для обслуживания Web-сервера, и вы не хотите, чтобы установка обновлений и возможная перезагрузка ему помешали. Какую конфигурацию политики Windows Update применить в этом случае?
   a. **Уведомлять перед загрузкой обновлений** и **уведомлять повторно перед их установкой (Notify For Download And Notify For Install).**
   b. Загружать автоматически и уведомлять перед установкой (Auto Download And Notify For Install).
   c. Загружать автоматически и устанавливать по заданному расписанию (Auto Download And Schedule The Install).
3. Вы хотите, чтобы сетевые клиенты загружали и устанавливали обновления автоматически по ночам, и уже настроили расписание установки для клиентов. Однако вы обнаружили, что некоторые пользователи выключают свои компьютеры на ночь, и обновления не применяются. Какая политика позволяет решить эту проблему, не меняя расписание установки?
   a. **Укажите расположение службы Windows Update в интрасети (Specify Intranet Microsoft Update Service Location).**
   b. Не выполнять автоматический повторный запуск для автоматических установок обновлений (No Auto-Restart For Scheduled Automatic Updates Installations).
   c. Перенос запланированных автоматических установок обновлений (Reschedule Automatic Updates Scheduled Installations).
   d. Настройка автоматического обновления (Configure Automatic Updates).

Резюме

- SUS — это приложение для интрасети, работающее в среде IIS 6.0 (или IIS 5.0 на сервере Windows 2000) и управляемое через Web-узел *http://имя_сереера_SUS/SUSAdmin*.
- Сервер SUS синхронизирует информацию о критических обновлениях и исправлениях и позволяет администратору централизовать утверждение каждого обновления. Обычно SUS-сервер предприятия также отвечает за загрузку файл:; обновлений.
- Средство *Автоматическое обновление* (Automatic Updates) под управлением Windows 2000, XP или Windows Server 2003 отвечает за загрузку и установку обновлений на клиентском компьютере.
- Групповая политика позволяет настроить *Автоматическое обновление,* чтобы клиент получал исправления с сервера SUS, а не с Windows Update. Управлять загрузкой, установкой и режимом перезагрузки клиентских компьютеров также можно с помощью объектов групповой политики.

Занятие 2. **Пакеты обновлений**

Microsoft выпускает *пакеты обновлений* (Service Pack, SP), чтобы объединить критические обновления, компоненты безопасности, «горячие» исправления, обновления драйверов и улучшения функций. Как говорилось в начале главы, не стоит тянуть с установкой SP2 до выхода SP3. Необходимо постоянно следить за пакетами обновлений, чтобы обеспечивать безопасность и целостность корпоративной сети. Службы обновления ПО. обсуждавшиеся на предыдущем занятии, не распространяют пакеты обновлений. Чтобы клиенты всегда были в актуальном состоянии и получали критические исправления, вы должны научиться распространять пакеты обновлений средствами групповой политики, чему и посвящено данное занятие.

Изучив материал этого занятия, вы сможете:

- ✓ загружать и распаковывать пакет обновлений;
- ✓ развертывать пакет обновлений средствами групповой политики.

Продолжительность занятия — около 5 минут.

Загрузка и распаковка пакетов обновлений

Новый пакет обновлений можно установить прямо с Web-узла Microsoft: на компьютер клиента загружается небольшая служебная программа, которая повторно подключается к серверу Microsoft и управляет загрузкой и установкой всего пакета. Пакеты обновлений обычно достаточно велики, поэтому выполнение такой задачи для каждого компьютера нельзя назвать эффективной стратегией развертывания.

Microsoft также распространяет пакеты обновлений на компакт-дисках и в рамка других ресурсов, таких как TechNet и MSDN. Для корпоративной среды рекомендуется приобретать компакт-диски, поскольку они часто содержат дополнения, например усовершенствованные средства администрирования, новые шаблоны политик и другое ПО.

Если вы хотите развернуть пакет обновлений на нескольких системах, а такого компакт-диска под рукой нет, можно загрузить пакет обновлений в виде одного файла с Web-узла Microsoft. Запуск этого файла позволяет распаковать и получить полную структуру папок и файлов пакета обновлений, аналогичную той, что находится на компакт-дисках (за исключением дополнительного ПО).

Чтобы распаковать пакет обновлений, запустите исполняемый файл из командной строки с параметром -x. Например, чтобы распаковать Windows XP SP1, введите `xpsp1. exe -x`. Вам будет предложено ввести путь к папке, куда следует распаковать пакет. По завершении этого процесса вы получите в указанном каталоге полную структуру папки пакета обновлений. Затем установить пакет можно так же, как с компакт-виска, — дважды щелкнув файл I386\Update\Update.exe.

Развертывание пакетов обновлений средствами групповой политики

Правом установки пакетов обновлений обладают администраторы локального компьютера, если только пакет не устанавливается через групповую политику или сервер SMS Systems Management Server). Поскольку пакеты обновлений применяются к системам, они назначаются через групповую политику, применяемую к компьютерам, а не к пользователям.

Для распространения пакета обновлений создайте общую папку и либо распакуйте куда пакет, либо скопируйте в нее содержимое компакт-диска. Затем с помощью консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) создайте или выберите существующий ОГП. Щелкните Изменить (Edit), чтобы открыть консоль *Редактор объектов групповой политики* (Group Policy Object Editor) с выбранным ОГП.

Раскройте узел **Конфигурация компьютера (Computer Configuration)\Конфигурация программ (Software Settings)**. Щелкните правой кнопкой узел **Установка программ (Software Installation)** и выберите **Создать (New)**, а затем **Пакет (Package)**. Введите путь к файлу Update.msi пакета обновлений. Используйте формат UNC (например *\\имя_сервера\имя_ресурса),* а не локальный путь, вроде *буква_диска:\путь.* В окне **Развертывание программ (Deploy Software)** выберите **Назначено (Assigned)**. Закройте консоль *Редактор шбъектов групповой политики* (Group Policy Object Editor). Компьютеры в области действия данного ОГП (в сайте, домене или в ветви ОП, к которой подключена политика) автоматически развернут пакет обновлений при следующей загрузке.

Совет В системах Windows XP, где настроена функция Logon Optimization, может потребоваться дважды перезагрузить компьютер. Эту функцию можно отключить, включив политику *Всегда ожидать инициализации сети при загрузке и входе в систему* (Always Wait For The Network At Computer Startup And Logon), в политике по пути **Конфигурация компьютера (Computer Configuration)\Административные шаблоны (Administrative Templates)\Система (System)\Вход в систему (Logon)**.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Какую команду следует исполнить, чтобы распаковать файл пакета обновлений?
   a. Setup.exe -u.
   b. Update.exe -x.
   c. Update.msi.
   d. <имя_пакета_обновлений>.exe -x.
2. Каким способом следует распространять пакет обновлений средствами групповоой политики?
   a. Опубликовать в узле **Конфигурация компьютера (Computer Configuration)\Конфигурация программ (Software Settings).**
   b. Назначить в узле **Конфигурация компьютера (Computer Configuration\Конфигурация программ (Software Settings).**
   c. Опубликовать в узле **Конфигурация пользователя (User Configuration)\Конфигурация программ (Software Settings).**
   d. Назначить в узле **Конфигурация пользователя (User Configuration)\Конфигурация программ (Software Settings).**

Резюме

- Распаковать пакет обновлений позволяет параметр -x.
- Пакеты обновлений можно развертывать средствами групповой политики, назначив Update.msi в политике конфигурации программ для компьютера.

Занятие 3. **Администрирование лицензий на ПО**

Лицензионное соглашение конечного пользователя (End User License Agreement, EULA) — это не просто досадное неудобство, которое можно пропустить, чтобы приступить к установке новой ОС, обновления или приложения, это обязательный контракт, предоставляющий законное право на использование ПО. В корпоративной среде управление лицензиями на ПО играет особо важную роль. На этом занятии вы познакомитесь со средствами лицензирования Windows Server 2003, которые служат для регистрации и слежения за лицензиями, а также соблюдения их требований.

Изучив материал этого занятия, вы сможете:

- ✓ описать режимы лицензирования на сервер и на устройство или пользователя;
- ✓ настроить лицензии, используя приложение **Лицензирование (Licensing)** из *Панели управления* или одноименное средство администрирования;
- ✓ создать лицензионную группу.

Продолжительность занятия — около 20 минут.

Получение лицензии на клиентский доступ

Серверная лицензия позволяет установить Windows Server 2003 на компьютер, однако, чтобы пользователь или устройство могли законно подключиться к серверу, необходимо приобрести *лицензию клиентского доступа* (Client Access License, CAL). Лицензии CAL обычно приобретаются партиями и часто, но не всегда, вместе с самой ОС. Копии сертификатов CAL и соглашений EULA следует хранить на случай проверки организации на предмет соблюдения лицензии.

Совет Помните, что при переходе с платформы Windows NT 4 или Windows 2000 на Windows Server 2003, необходимо также приобрести обновленные CAL.

У вас должна быть лицензия CAL для любого подключения к компьютеру под управлением Windows Server 2003, которое использует компоненты сервера, включая службы доступа к файлам и принтерам или проверку подлинности. Только некоторые серверные приложения работают независимо до такой степени, что клиент-серверное соединение не требует CAL. Наиболее значительное исключение к требованию CAL — доступ через Интернет без авторизации. Если при доступе через Интернет не происходит обмен реквизитами, например, пользователи просматривают ваш общедоступный Web-узел, CAL не требуется. Таким образом, лицензии CAL не требуются для Windows Server 2003 Web Edition.

Существует два типа CAL: хтя устройств, позволяющие устройству подключиться к серверу независимо от числа работающих на нем пользователей, и для пользователей, позволяющие подключиться к серверу с любого устройства. Лицензии для устройств выгодны организациям с большим количеством пользователей на одном устройстве, например, когда сотрудники работают сменами. Лицензии для пользователей лучше подходят организации, где сотрудники входят в сеть с нескольких или с неизвестных устройств.

Примечание Для управления обоими типами лицензий служат одни и те же средства лицензирования с одинаковым пользовательским интерфейсом. Лицензии устройств регистрируются косвенно с применением лицензионных групп.

Сколько лицензий вам требуется, и как вы их будете отслеживать, зависит от выБранного режима лицензирования клиентского доступа.

Лицензирование на сервер

Режим *На сервер* (Per-Server) требует лицензии пользователя или устройства для каждого параллельного подключения. Если сервер настроен на 1000 лицензий клиентского доступа, 1001-е параллельное подключение будет отклонено. CAL предназначены для использования на конкретном сервере, поэтому если той же тысяче пользователей потребуется параллельно подключиться к другому серверу, вам придется приобрести для него еще 1000 лицензий.

Лицензирование на сервер выгодно только при ограниченном доступе, например, когда подмножество пользователей обращается к серверному продукту на небольшом количестве серверов. Лицензирование на сервер обходится дороже, когда много пользователей обращаются к большому количеству ресурсов на нескольких серверах. Если вы не уверены, какой режим вам подходит, выберите лицензирование на сервер. Лицензионное соглашение предусматривает бесплатное однократное одностороннее преобразование лицензии на сервер к лицензии на устройство или пользователя, когда это становится вам более выгодным.

Лицензирование на устройство или на пользователя

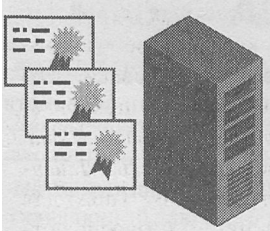
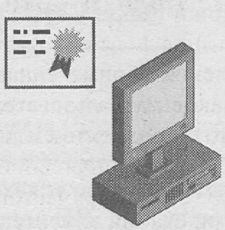
Режим *На устройство или на пользователя* (Per Device or Per User Licensing) отличается от схемы *На рабочее место* (Per Seat) в предыдущих версиях Windows. В этом новом режиме каждому устройству или пользователю, который подключается к серверу, требуется лицензия, но с этой лицензией он может подключаться к нескольким серверам предприятия. Лицензирование на устройство или на пользователя, как правило, — оптимальный вариант для распределенных вычислительных сред, где много пользователей обращаются к множеству серверов.

Например, сотруднику, работающему с портативным и двумя настольными компьютерами требуется только одна пользовательская лицензия Windows. Комплект же из 10 портативных компьютеров, используемых 30 посменными рабочими, потребовал бы лишь 10 лицензий устройств.

Общее количество лицензий равно количеству устройств или пользователей (или их комбинации), которые обращаются к серверам. Лицензии можно переназначать по рят. уважительных причин, например, пользовательскую лицензию можно передать временному сотруднику, пока постоянный отсутствует. Лицензию устройства можно переназначить резервному устройству, пока основное находится в ремонте.

Режимы лицензирования на сервер и на устройство или пользователя проиллюстрированы в табл. 9-1.

Табл. 9-1. Режимы лицензирования

На сервер	На устройство или на пользователя
	
• Лицензирование на сервер обычно применяют, когда в организации несколько серверов, к которым открыт ограниченный доступ. • Требуемое количество лицензий определяется количеством параллельных соединений.	• Лицензирование на устройство или на пользователя обычно применяют, когда в организации много серверов, к которым интенсивно обращается много пользователей. • Обычно этот режим более экономичен, когда требуемое количество лицензий определяется количеством пользователей или устройств (или и тех и других), которым нужен доступ к серверам.

Совет В состав Windows Server 2003 входят службы терминалов, также называемые *Дистанционное управление рабочим столом* (Remote Desktop), которые содержат лицензию на два параллельных соединения для администраторов, подключающихся к удаленному серверу. Чтобы службы терминалов играли роль сервера приложений, позволяющего обычных пользователям подключаться к размещенным на нем приложениям, необходимо приобрести для клиентов лицензии служб терминалов; они входят в комплект Windows XP Professional

Для контроля за лицензиями на ПО и управления ими предусмотрены две служебные программы.

- **Приложение *Лицензирование* (Licensing) из *Панели управления*.** Средство *Выбор режима лицензирования* (Choose Licensing Mode) из *Панели управления* (рис. 9-8) управляет лицензионными требованиями для одного компьютера под управлением Windows Server 2003. Оно применяется для добавления и удаления лицензий на сервере, работающем в режиме лицензирования на сервер, изменения режима лицензирования (от расчета на сервер к лицензированию на устройство или пользователя), а также для настройки репликации лицензий.

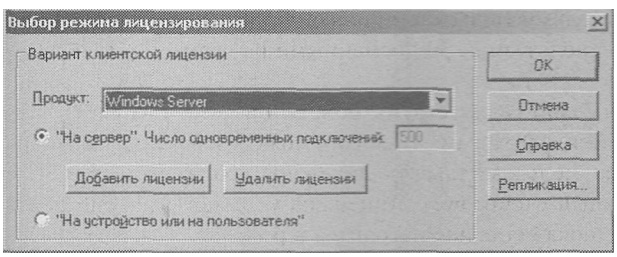


Рис. 9-8. Средство *Выбор режима лицензирования* из *Панели управления*

- **Средство *Лицензирование* (licensing) из группы программ *Администрирование* (Administrative Tools).** Это средство (см. следующий раздел) обеспечивает централизованное управление и репликацию лицензий в рамках сайтов.

Управление лицензиями в сайтах

Служба *Учет лицензий* (License Logging), запущенная на каждом компьютере Windows Server 2003, назначает и отслеживает лицензии при обращении к ресурсам сервера. Чтобы гарантировать соблюдение лицензии, сведения из нее реплицируются в центральную БД лицензий на одном из серверов в сайте. Его называют *сервером лицензий сайта*. Администратор сайта или сервера лицензий сайта может использовать средство *Лицензирование* (Licensing) из группы программ Администрирование (Administrative Tools) для просмотра и управления лицензиями во всем сайте. Эта новая функция позволяет отслеживать и управлять лицензиями не только для служб доступа к файлам и принтерам, но и для IIS, служб терминалов и продуктов BackOffice, например Exchange или SQL Server.

Сервер лицензий сайта

Сервером лицензий сайта обычно является первый контроллер домена, созданный в сайте. Чтобы уточнить сведения, откройте оснастку *Active Directory — сайты и службы* (Active Directory Sites And Services), выберите сайт, щелкните правой кнопкой **Licensing Site Settings** и выберите **Свойства (Properties)**. Появится информация о текущем сервере лицензий сайта (рис. 9-9).

Чтобы назначить роль сервера лицензий сайта другому серверу или контроллеру домена, щелкните **Изменить (Change)** и выберите нужный компьютер. Чтобы сохранить историю лицензирования для вашего предприятия, необходимо сразу после передачи этой роли остановить службу *Учет лицензий* (License Logging) на новом сервере лицензий и скопировать следующие файлы со старого сервера на новый:

- *%Systemroot%*\System32\Cpl.cfg — содержит историю приобретения лицензий для вашей организации;

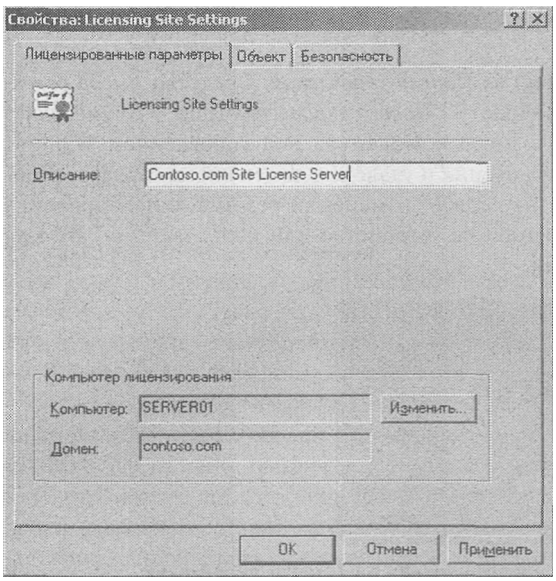


Рис. 9-9. Определение и смена сервера лицензий сайта

- *%Systemroot%*\Lls\Llsuser.lls — содержит информацию о количестве подключений пользователей;
- *%Systemroot/%*\Lls\Llsmap.lls — содержит сведения о лицензионной группе.

Скопировав все файлы, вновь запустите службу *Учет лицензий* (License Logging).

Управление лицензиями в сайте

Определив сервер лицензий сайта, можно просмотреть информацию о лицензиях на нем, запустив средство *Лицензирование* (Licensing) из группы программ **Администрировав» (Administrative Tools).** Вкладка **Обозреватель серверов сети (Server Browser)** в окне программы *Лицензирование* (рис. 9-10) позволяет управлять лицензированием для всего сайт» или предприятия.

Вкладка **Обозреватель серверов сети** позволяет управлять любым сервером в любом сайте или домене, где у вас есть административные полномочия. Вы можете выбрать сервер и, открыв окно его свойств, управлять его лицензиями. Для каждого серверного продукта, установленного на данном сервере, вы можете добавить или удалить лицезйи в расчете на сервер. Кроме того, там, где это разрешено, вы можете изменить режим лицензирования. Помните, что режим лицензирования на сервер выдает лицензию, когда пользователь соединяется с серверным продуктом. Когда пользователь отключается от этого продукта, служба *Учет лицензий* (License Logging) делает лицензию доступной другому пользователю.

Вы также можете настроить репликацию лицензий; для этого запустите приложение *Лицензирование* из *Панели управления* на сервере. По умолчанию информация о лицензиях реплицируется из службы *Учет лицензий* (License Logging) каждого сервера на сервер лицензий сайта каждые 24 часа с небольшими колебаниями времени начал репликации, чтобы избежать перегрузки сервера лицензирования. Если вы хотите управлять расписанием и частотой репликации, вручную настройте параметры **Запустить в (Start**

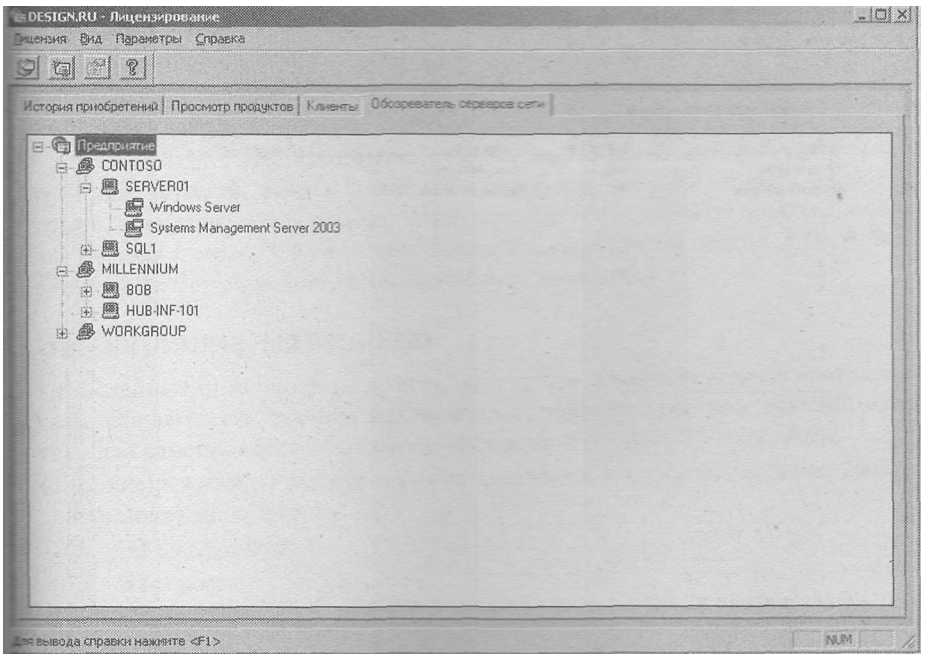


Рис. 9-10. Вкладка *Обозреватель серверов сети* в окне программы *Лицензирование*

At) и **Запускать каждые (Start Every)** для каждого сервера, реплицирующего информацию на определенный сервер лицензий сайта.

Для управления лицензированием на устройство или пользователя щелкните **Лицензирование (Licensing)** в группе программ **Администрирование (Administrative Tools)** и в меню **Лицензия (License)** выберите **Новая лицензия (New License)**. В окне Новая клиентская лицензия **(New Client Access License)** выберите серверный продукт и количество приобретенных лицензий. Лицензии будут добавлены в пул лицензий. Когда устройство или пользователь подключаются к продукту в любом месте сайта, им будет выделена одна лицензия из пула (по одной для каждого устройства или пользователя). Когда пул лицензий опустеет, при обращении следующего пользователя или устройства к продукту произойдет нарушение лицензии.

Вкладка **История приобретений (Purchase History)** в окне **Лицензирование (Licensing)** Предоставляет исторический обзор лицензий, приобретенных для сайта, включая количество, дату и учетную запись администратора, который добавлял или удалял лицензии (рис. 9-11).

Для просмотра сводной информации о лицензировании и соблюдении требований лицензий перейдите на вкладку Просмотр продуктов (Products View). Здесь показано, сколько лицензий было приобретено, сколько выделено пользователям или устройствам (в режиме лицензирования на устройство или пользователя), сколько было приобретено для всех серверов в сайте, а также максимальное зафиксированное количество параллельных подключений до сего дня (в режиме лицензирования на сервер). О соблюдении лицензии можно судить по символам состояния лицензирования (табл. 9-2).

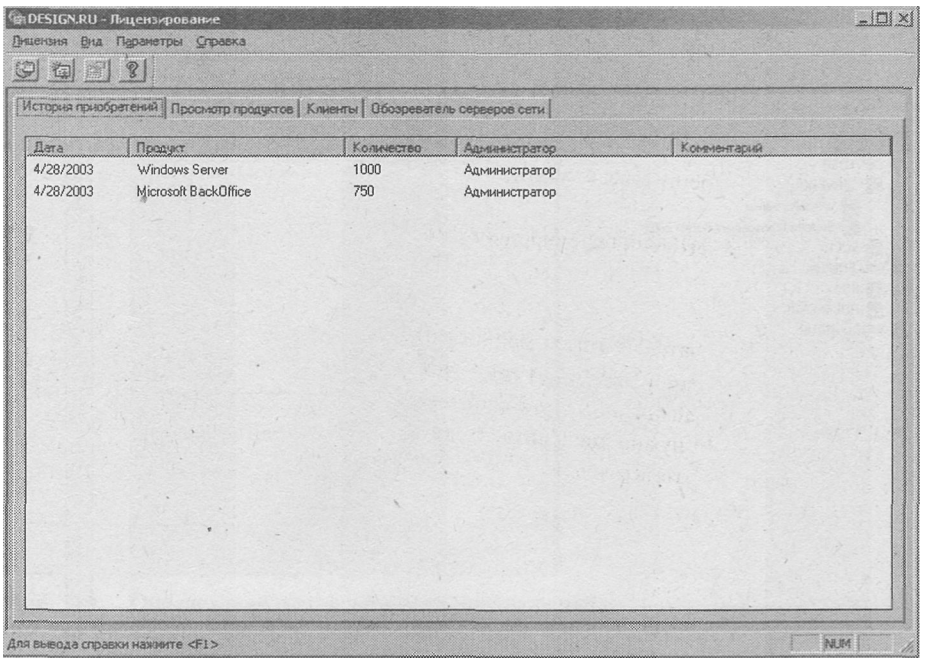


Рис. 9-11. Вкладка *История приобретений* в окне программы *Лицензирование*

Табл. 9-2. Символы состояния лицензирования

Символ	Состояние лицензирования
	Продукт используется согласно требованиям лицензии. Количество подключений не превышает количества приобретенных лицензий
	Продукт используется неправомерно. Количество подключений превышает количество приобретенных лицензий
	Продукт достиг разрешенного предела. Количество подключений равно числу приобретенных лицензий. Если дополнительные устройства или пользователи будут подключаться к серверному продукту, вам придется приобрести и зарегистрировать новые лицензии

Лицензионные группы

Лицензирование на устройство или на пользователя требует одной CAL для каждого устройства. Однако служба *Учет лицензий* (License Logging) назначает и отслеживает лицензии по имени пользователя. Если несколько пользователей совместно используют одно или несколько устройств, необходимо создать лицензионные группы, иначе ~ цензии буду израсходованы слишком быстро.

Лицензионная группа — это совокупность пользователей, совместно использующих одну или несколько лицензий. Когда пользователь подключается к серверному продукту, служба *Учет лицензий* отслеживает пользователя по имени, но назначает лицензию из числа отведенных лицензионной группе. Суть этой методики легче понять на примерах.

- **10 пользователей совместно используют переносное устройство для инвентаризации.** Все десять пользователей входят в лицензионную группу. Лицензионной группе назначается одна лицензия, представляющая одно устройство, с которым они работают.
- **100 студентов иногда работают в лаборатории из десяти компьютеров.** Создается лицензионная группа из этих 100 студентов, которой выделяется десять лицензий.

Чтобы создать лицензионную группу, в меню **Параметры (Options)** выберите **Дополнительно (Advanced),** а затем **Новая лицензионная группа (New License Group).** Введите имя группы и выделите одну лицензию для каждого клиентского устройства, используемого для доступа к серверу. Количество лицензий, выделенных группе, должно соответствовать количеству устройств, используемых ее членами.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Какие режимы лицензирования поддерживаются в Windows Server 2003? Выберите все подходящие варианты.
   a. На пользователя.
   b. На сервер
   c. На место.
   d. На устройство или на пользователя.
2. Чтобы ускорить разработку ПО, вы нанимаете команду программистов, которая будет работать в три смены, по шесть человек в каждой. Каждый программист для разработки и тестирования ПО будет использовать четыре устройства, с каждого из которых будет входить в сеть под управлением Windows Server 2003. Какое минимальное количество лицензий требуется, если серверы используют режим лицензирования на устройство или пользователя?
   a. 6.
   b. 4.
   c. 18.
   d. 24.
3. Какое средство позволяет определить сервер лицензий для сайта?
   a. *Active Directory — домены и доверие* (Active Directory Domains And Trusts).
   b. Приложение *Лицензирование* (Licensing) из *Панели управления.*
   c. *Active Directory — сайты и службы* (Active Directory Sites And Services).
   d. Консоль DNS.
4. Вы управляете сетью для команды из 500 телефонных торговых представителей. У вас есть 550 лицензий, настроенных для режима лицензирования на устройство или пользователя. Начинается новая кампания, и вы собираетесь нанять еще одну смену из 500 представителей. Что сделать для наиболее эффективного отслеживания и соблюдения лицензий?
   a. Отозвать лицензии у существующих клиентов.
   b. Удалить существующие лицензии, затем добавить 500 лицензий.
   c. Создать лицензионную группу.
   d. Перейти на режим лицензирования на сервер.

Резюме

- Windows Server 2003 поддерживает новый режим лицензирования, который позволяет по одной лицензии одному пользователю обращаться к серверному продукту с множества устройств или группе пользователей — с одного устройства. Такой режим называется лицензированием на устройство или на пользователя.
- Если несколько пользователей обращаются к серверному продукту с совместно используемых устройств, добавьте их в лицензионную группу и выделите ей столько лицензий, сколько устройств используют ее участники.
- Информация о лицензиях реплицируется на сервер лицензий сайта каждые 24 часа (по умолчанию).
- Для управления лицензиями служит приложение *Лицензирование* (Licensing) из *Панели управления* или (для более централизованной модели) одноименное средство администрирования из группы программ **Администрирование (Administrative Tools).**

Пример из практики

Вы настраиваете стратегию обновления для сети из 1000 клиентских компьютеров под управлением Windows XP и 2000 и хотите запретить пользователям загружать обновления напрямую с сервера Windows Update и создать структуру, позволяющую вам утверждать критические исправления и компоненты безопасности, которые следует распространять клиентам.

Вы недавно приобрели настольные и портативные компьютеры и развернули на них системы из утвержденных корпоративных образов ОС. К сожалению, эти образы ОС были созданы уже давно. Образ Windows XP вообще не содержит обновлений с даты выхода этой ОС, а образ Windows 2000 содержит лишь обновление SP2. Таким образом, ваша первая задача — довести системы до уровня последнего пакета обновлений, чтобы клиент службы автоматического обновления и все исправления были установлены на этих компьютерах.

Примечание Результаты выполнения этого упражнения можно проверить с помощью второго компьютера: присоедините его к домену и добавьте его учетную запись в OIT Desktops. Если этот компьютер работает под управлением Windows 2000, соответствующим образом измените упражнение по развертыванию пакета обновлений.

Упражнение 1. Загрузка и распаковка пакета обновлений

1. Создайте папку Service Pack на диске C:.
2. С Web-узла Microsoft, *http://www.microsoft.com/downloads* или с Web-узла Windows XP, *http://www.microsoft.com/windowsxp,* загрузите последний пакет обновлений. Сохраните его в папку C:\ServicePack.
3. Из командной строки исполните cd C:\ServicePack, чтобы перейти к папке ServicePack.
4. Исполните команду xpspi. exe -x. Замените xpspl именем загруженного пакета обновлений.
5. Вам предложат указать размещение, куда нужно распаковать пакет обновлений. Введите C: \Se rvicePack.

6. Пакет обновлений будет распакован. Просмотрите структуру созданной папки в *Проводнике Windows*. Обратите внимание на расположение файла update.exe (в папке Update), который запускает установку пакета на одном компьютере, и файла update.msi (в той же папке), который используется для развертывания пакета обновлений средствами групповой политики.

Упражнение 2. Развертывание пакета обновлений средствами групповой политики

1. Откройте общий доступ к папке C:\ServicePack, присвоив ей имя ресурса ServicePack.
2. Откройте консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers).
3. Раскройте домен и найдите (или создайте) ОП Desktops.
4. Создайте объект компьютера в ОП Desktops с именем Desktop0569, соответствующий одной из новых систем.

   Примечание Если у вас есть второй компьютер, с помощью которого можно выполнить данное упражнение, переместите его учетную запись в ОП Desktops.

5. Щелкните правой кнопкой ОП Desktops и выберите **Свойства (Properties).**
6. Перейдите на вкладку **Групповая политика (Group Policy).**
7. Щелкните Создать (New), чтобы создать новый ОГП. Присвойте этому объекту имя SP-Deploy.
8. Выберите ссылку групповой политики SP-Deploy и щелкните **Изменить (Edit).** Откроется окно **Редактор объектов групповой политики (Group Policy Object Editor).**
9. Перейдите к узлу **Конфигурация компьютера (Computer Configuration)\Конфигурация программ (Software Settings).**
10. Щелкните правой кнопкой узел **Установка программ (Software Installation)** и выберите Создать (New), а затем **Пакет (Package).**
11. Введите путь \\server01. contoso. com\servicepack и нажмите клавишу Enter. Диалоговое окно выбора файла откроется на папке, куда был распакован пакет обновлений.
12. Найдите файл Update.msi, на который мы обращали ваше внимание на прошлом упражнении. Выберите файл Update.msi и щелкните **Открыть (Open).**
13. Выберите **Назначено (Assigned)** и щелкните ОК. Пакет создан.
14. Закройте окно **Редактор объектов групповой политики (Group Policy Object Editor)** и окно свойств ОП Desktop.
15. (Необязательная операция.) Если у вас есть второй компьютер, можно протестировать развертывание пакета обновлений. Помните, что компьютеры Windows XP по умолчанию оптимизируют вход в систему, поэтому для применения пакета обновлений может потребоваться перезагрузить такую систему дважды. Чтобы проверить уровень пакета обновлений на компьютере, в меню **Пуск (Start)\Выполнить (Run)** исполните команду winver.

Упражнение 3. Установка SUS

1. В браузере откройте *http://go.microsoft.com/jwlink/?LinkId=6930*. Вам будет предложено добавить этот Web-узел в список надежных узлов, что и следует сделать.

2. Загрузите пакет установки SUS.
3. Запустите установку SUS, дважды щелкнув загруженный файл.
4. В окне приветствия щелкните **Далее** (Next).
5. Прочитайте лицензионное соглашение конечного пользователя и примите его условия, затем щелкните **Далее (Next).**
6. Выберите **Custom installation** и щелкните **Далее (Next).**
7. На странице **Choose File Locations** выберите **Save The Updates To This Local Folder.** Не меняйте каталог C:\SUS\Content, предложенный по умолчанию. Щелкните Далее (Next).

   Примечание Обновления могут занимать несколько сот мегабайт. Если у вас медленное подключение к Интернету, или вы хотите сэкономить время, выберите второй вариант — **Keep The Updates On A Microsoft Windows Update Server.**

8. В списке **Language Settings** выберите **English Only** и щелкните **Далее (Next).**
9. **На** следующей странице выберите **I Will Manually Approve New Versions Of Approved Updates** и щелкните **Далее (Next).**
10. На следующей странице должно быть указано, что файлы будут загружены по адресу *http://SERVER01.* Щелкните **Установить (Install).**
11. По завершении установки щелкните **Готово (Finish).** Откроется Internet Explorer, и вы перейдете на Web-страницу управления SUS. Переходите к упражнению 4.

Упражнение 4. Синхронизация SUS

1. Если вы еще не перешли на Web-страницу управления SUS, откройте Internet Explorer и введите адрес http://SERVER.01/SUSAdmin.

   Примечание Для доступа к Web-узлу управления может потребоваться добавить ServerOl в список надежных узлов локальной интрасети. Откройте Internet Explorer и в меню **Сервис (Tools)** выберите **Свойства обозревателя (Internet Options).** Перейдите на вкладку **Безопасность (Security).** Щелкните значок **Надежные узлы (Trusted Sites),** затем кнопку **Узлы (Sites).** Добавьте ServerOl и Server01.contoso.com в список надежных узлов.

2. Щелкните **Synchronize Server** на навигационной панели слева.
3. Щелкните **Synchronization Schedule.**

   В этом упражнении вы проведете ручную синхронизацию. Можно изучить параметры синхронизации, щелкнув **Synchronize Using This Schedule.** Закончив исследование параметров, щелкните **Cancel.**
4. На странице **Synchronize Server** щелкните **Synchronize Now.** Если вы решили загрузить обновления на свой сервер, синхронизация может занять некоторое время.
5. По завершении синхронизации вы автоматически перейдете на страницу **Approve updates.** Вы также можете щелкнуть **Approve Updates** на навигационной панели слева.
6. Утвердите несколько обновлений, чтобы можно было вернуться к этой странице при дальнейших экспериментов с утверждением и автоматическими обновлениями.
7. Исследуйте другие страницы Web-узла управления SUS. Познакомившись с сайтом, закройте Internet Explorer.

Упражнение 5. Настройка автоматических обновлений

1. Откройте консоль *Active Directory — сайты и службы* (Active Directory Sites And Services).

   Примечание На большинстве предприятий принято подключать ОГП к сайтам, а не ОП или доменам. Тем не менее, политики, связанные с SUS, хорошо применимы к сайтам, поскольку вы направляете клиенты к наиболее подходящему для их сайта серверу SUS.

2. Щелкните правой кнопкой сайт **Default-First-Site-Name** и выберите **Свойства (Properties).**
3. Перейдите на вкладку **Групповая политика (Group Policy).**
4. Щелкните Создать (New) и присвойте новому ОГП имя SUS-Sitel.
5. Щелкните **Изменить (Edit).** Откроется окно **Редактор объектов групповой политики (Group Policy Object Editor).**
6. Перейдите к узлу **Конфигурация компьютера (Computer Configuration)\Административные шаблоны (Administrative Templates)\Компоненты Windows (Windows Components)\Windows Update.**
7. Дважды щелкните политику **Укажите расположение службы Windows Update в интрасети (Specify Intranet Microsoft Update Service Location).**
8. Щелкните **Включен (Enabled).**
9. **В** обоих полях введите http://server01.contoso.com.
10. Щелкните **OK**.
11. Дважды щелкните политику **Настройка автоматического обновления (Configure Automatic Updates).**
12. Щелкните **Включен (Enabled).**
13. В списке **Настройка автоматического обновления (Configure Automatic Updating)** выберите **Загружать автоматически и устанавливать по заданному расписанию (Auto Download And Schedule The Install).**
14. Подтвердите расписание установки: ежедневно в 3:00.
15. Щелкните **OK**.
16. Дважды щелкните политику **Перенос запланированных автоматических установок обновлений (Reschedule Automatic Updates Scheduled Installations).**
17. Щелкните **Включен (Enabled).**
18. В поле **Ждать после запуска системы (минут) [Wait After System Startup (Minutes)]** введите 1.

    Подготовка к экзамену Значение **Ждать после запуска системы** используется для выполнения установки, которая была пропущена. Обычно это происходит, если компьютер был выключен в запланированное время.

19. Щелкните **OK**.
20. Закройте окно **Редактор объектов групповой политики (Group Policy Object Editor)** и окно свойств сайта Default-First-Site-Name.
21. Чтобы подтвердить конфигурацию, можно перезагрузить сервер, который также находится в области действия новой политики. Откройте приложение *Система* (System) из *Панели управления* и перейдите на вкладку **Автоматическое обновление (Automatic Updates).** Вы увидите, что параметры конфигурации нельзя редактировать, поскольку теперь они определяются политикой.

Резюме главы

- Службы Microsoft Software Update Services служат для централизованного управления утверждением и распространением критических обновлений и компонентов безопасности Windows. Один или несколько серверов SUS содержат перечни утвержденных обновлений, и, как правило, сами файлы обновлений. Клиенты службы *Автоматическое обновление* (Automatic Updates) настраиваются (обычно с помощью ОГП) для получения обновлений с серверов SUS в интрасети, вместо серверов Microsoft Windows Update.
- Службы SUS не распространяют пакеты обновлений.
- Пакеты обновлений можно бесплатно загрузить с Web-узла Microsoft. Если вы загрузили пакет обновлений в виде отдельного файла, его можно распаковать из командной строки, добавив к имени файла пакета параметр -x.
- Для развертывания пакетов обновлений в рамках ОГП можно указать пакет установки в политиках конфигурации компьютера, связанных с ПО.
- Управление и слежение за лицензиями и их соблюдением — важная часть работы администратора. Windows Server 2003 позволяет назначать лицензии в зависимости от количества параллельных подключений к конкретному серверу или отслеживать лицензии для каждого устройства или пользователя, которые подключаются к нескольким серверам предприятия.
- Лицензии реплицируются между службой *Учет лицензий* (License Logging) на сервере и сервером лицензий сайта. Сервер лицензий сайта можно определить с помощью консоли *Active Directory — сайты и службы* (Active Directory Sites And Services), однако лицензиями управляют с помощью средства *Лицензирование* (Licensing) из группы программ **Администрирование (Administrative Tools).**
- Лицензионные группы позволяют пользователям совместно использовать одно или несколько устройств. При этом лицензионной группе назначается несколько лицензий устройств Windows.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Изучите процессы установки и настройки SUS. Хотя экзамен не содержит вопросов, напрямую касающихся установки SUS, способ настройки SUS влияет на задачи, которые вы будете выполнять для обслуживания инфраструктуры SUS, поэтому важно иметь полное представление о работе SUS.
- Обратите внимание на задачи администрирования SUS, включая синхронизацию, утверждение обновлений, просмотр журналов и событий, настройку клиента автоматического обновления с помощью приложения *Система* (System) из *Панели управления* (на изолированном компьютере) или средствами групповой политики в большой сети. Помните, что нельзя направить компьютер на сервер SUS, используя свойства службы *Автоматическое обновление* на клиентском компьютере. Необходимо исполь-

зовать групповую политику или запись в реестре, чтобы перенаправить клиента на сервер в интрасети, вместо сервера Microsoft Windows Update.

- Вы должны уметь подсчитать лицензионные требования в режимах *На сервер* (Per Server) или *На устройство или на пользователя* (Per Device or Per User). Помните, что лицензионные группы позволяют множеству пользователей совместно работать с одним или несколькими устройствами.

Основные термины

Лицензия клиентского доступа ~ Client Access License, CAL. Позволяет пользователю или устройству подключаться к серверному продукту для выполнения каких-либо функций, включая службу доступа к файлам и принтерам и средства проверки подлинности.

Режим лицензирования *На сервер* (Per Server). Лицензии выделяются, когда пользователь или устройство подключаются к серверу или продукту. Когда пользователь отключается, лицензия возвращается в пул доступных лицензий. Этот режим требует достаточного количества лицензий для поддержания максимального количества параллельных подключений на каждом сервере.

Режим лицензирования *На устройство или на пользователя* (Per Device or Per User). Лицензионные требования разрешают использовать одну лицензию для авторизации пользователя (который может работать на нескольких устройствах) или устройства (на котором могут работать несколько пользователей) при подключении к любому количеству серверов.

Лицензионная группа. Поскольку служба *Учет лицензий* (License Logging) выделяет лицензии на основе имени пользователя, а не имени устройства, лицензии устройств предоставляются лицензионной группе. Лицензионной группе, состоящей из одного или нескольких пользователей, назначается столько лицензий, сколько устройств используют ее участники для подключения к серверным продуктам.

Вопросы и ответы

Занятие 1. Закрепление материала

1. Вы настраиваете инфраструктуру служб обновления ПО. Один сервер синхронизирует метаданные и содержимое с сервером Windows Update. Остальные серверы (по одному в каждом сайте) синхронизируют содержимое с родительским сервером SUS. Что необходимо выполнить для окончательной настройки инфраструктуры SUS?
   a. Настроить клиенты службы *Автоматическое обновление,* используя *Панель управления* на каждой системе.
   b. Настроить объекты групповой политики, чтобы направить клиенты на серверы SUS в своих сайтах.
   c. Настроить точку ручного распространения содержимого.
   d. Утвердить обновления на Web-странице управления SUS.

   Правильный ответ: b, d.
2. Вы настраиваете службу SUS для группы Web-серверов и хотите, чтобы они обновлялись каждую ночь согласно списку утвержденных обновлений на вашем сервере

SUS. Иногда по вечерам администратор входит в систему для обслуживания Web-сервера, и вы не хотите, чтобы установка обновлений и возможная перезагрузка ему помешали. Какую конфигурацию политики Windows Update применить в этом случае?

a. **Уведомлять перед загрузкой обновлений и уведомлять повторно перед их установкой (Notify For Download And Notify For Install).**
b. **Загружать автоматически и уведомлять перед установкой (Auto Download And Notify For Install).**
c. **Загружать автоматически и устанавливать по заданному расписанию (Auto Download And Schedule The Install).**

Правильный ответ: c. Для автоматического обновления Web-серверов нужно создать расписание обновлений. Тем не менее администратор всегда вправе отменить установку.

3. Вы хотите, чтобы сетевые клиенты загружали и устанавливали обновления автоматически по ночам, и уже настроили расписание установки для клиентов. Однако вы обнаружили, что некоторые пользователи выключают свои компьютеры на ночь, и обновления не применяются. Какая политика позволяет решить эту проблему, не меняя расписание установки?

a. **Укажите расположение службы Windows Update в интрасети (Specify Intranet Microsoft Update Service Location).**
b. **Не выполнять автоматический повторный запуск для автоматических установок обновлений (No Auto-Restart For Scheduled Automatic Updates Installations).**
c. **Перенос запланированных автоматических установок обновлений (Reschedule Automatic Updates Scheduled Installations).**
d. **Настройка автоматического обновления (Configure Automatic Updates).**

Правильный ответ: c. Обновления автоматически загружаются в фоновом режиме во время простоев сети, но установка запускается по расписанию. Если компьютер выключен в запланированное время, установка переносится на следующее запланированное в расписании время. Если присвоить политике Reschedule Automatic Updates Scheduled Installations значение от 1 до 60, клиент автоматического обновления запустит установку обновлений спустя указанное количество минут после загрузки системы.

Занятие 2. Закрепление материала

1. Какую команду следует исполнить, чтобы распаковать файл пакета обновлений?

a. Setup.exe -и.
b. Update.exe -x.
c. Update.msi.
d. <*имя_пакета_обновлений*>.exe -x.

Правильный ответ: d.

2. Каким способом следует распространять пакет обновлений средствами групповой **политики?**

a. Опубликовать в узле **Конфигурация компьютера (Computer Configuration)\Конфигурация программ (Software Settings).**
b. Назначить в узле **Конфигурация компьютера (Computer Configuration)\Конфигурация программ (Software Settings).**
c. Опубликовать в узле **Конфигурация пользователя (User Configuration)\Конфигурация программ (Software Settings).**

d. Назначить в узле **Конфигурация пользователя (User Configuration)\Конфигурация программ (Software Settings).**

Правильный ответ: b.

Занятие 3. Закрепление материала

1. Какие режимы лицензирования поддерживаются в Windows Server 2003? Выберите все подходящие варианты.
   a. На пользователя.
   b. На сервер.
   c. На место.
   d. На устройство или на пользователя.

   Правильный ответ: b, d.
2. Чтобы ускорить разработку ПО, вы нанимаете команду программистов, которая будет работать в три смены, по шесть человек в каждой. Каждый программист для разработки и тестирования ПО будет использовать четыре устройства, с каждого из которых будет входить в сеть под управлением Windows Server 2003. Какое минимальное количество лицензий требуется, если серверы используют режим лицензирования на устройство или пользователя?
   a. 6.
   b. 4.
   c. 18.
   d. 24.

   Правильный ответ: c. Если выделять **лицензии на устройства, понадобится 24 лицензии (6 пользователей x 4 устройства). Дешевле лицензировать пользователей (18).**
3. Какое средство позволяет определить сервер лицензий для сайта?
   a. *Active Directory — домены и доверие* (Active Directory Domains And Trusts).
   b. Приложение *Лицензирование* (Licensing) из *Панели управления.*
   c. *Active Directory — сайты и службы* (Active Directory Sites And Services).
   d. Консоль DNS.

   Правильный ответ: c.
4. Вы управляете сетью для команды из 500 телефонных торговых представителей. У вас есть 550 лицензий, настроенных для режима лицензирования на устройство или пользователя. Начинается новая кампания, и вы собираетесь нанять еще одну смену из 500 представителей. Что сделать для наиболее эффективного отслеживания и соблюдения лицензий?
   a. Отозвать лицензии у существующих клиентов.
   b. Удалить существующие лицензии^ затем добавить 500 лицензий.
   c. Создать лицензионную группу.
   d. Перейти на режим лицензирования на сервер.

   Правильный ответ: c.

ГЛАВА 10

Управление оборудованием и драйверами

Темы экзамена

- Установка и конфигурирование оборудования сервера:
  - настройка параметров подписывания драйверов;
  - настройка параметров ресурсов для устройства;
  - настройка параметров и свойств устройства.
- Мониторинг оборудования сервера с помощью *Диспетчера устройств* (Device Manager), мастера устранения неполадок и соответствующих приложений из *Панели управления*.

В этой главе

Устройство и программное обеспечение, используемое ОС для связи с ним (драйвер), — комбинация, уникальная для устройства и версии ОС, под управлением которой оно работает. Большинство драйверов поддерживают лишь одну ОС, то есть нельзя использовать драйвер, предназначенный для Windows 98, в Windows XP или Windows Server 2003.

Учитывая, что требуется точное соответствие между устройством, драйвером и ОС, ошибки в настройке приводят к сбоям в работе устройств. Корректный драйвер для устройства и целевой ОС должен работать согласно своему назначению, и, как администратор, вы можете свободно обновлять драйверы средствами *Диспетчера устройств* (Device Manager), а также предоставлять некоторым пользователям привилегии по настройке параметров подписывания драйверов.

Прежде всего

Предполагается, что вы имеете четкое представление и практические знания о типичных устройствах компьютера: принтерах, мышах, клавиатурах, сетевых платах и т. п.

Физическая оптимизация, тестирование и устранение физических неисправностей в работе устройств здесь не рассматриваются.

Примеры и упражнения по установке, конфигурированию и устранению неполадок в работе устройств и драйверов будут выполняться в среде Windows Server 2003 со стандартными устройствами. Для выполнения упражнений вам понадобится компьютер под управлением Windows Server 2003, установленный как ServerOl и настроенный в качестве контроллера домена contoso.com.

Занятие 1. Установка оборудования и драйверов

Оборудование «общается» с Windows Server 2003 посредством программных драйверов. Устройства и их драйверы, если они не устанавливаются автоматически в стиле Plug and Play, можно настраивать в оснастке *Диспетчер устройств* (Device Manager).

Изучив материал этого занятия, вы сможете:

- ✓ уяснить взаимосвязь устройств и драйверов;
- ✓ использовать оснастку *Диспетчер устройств* для анализа и установки устройств.

Продолжительность занятия — около 20 минут.

Устройства и драйверы

Легче всего представить устройства и связанные с ними драйверы, разделив их на две логических категории: устройства с поддержкой PnP (Plug-and-Play) и без (низкоуровневые) . Большинство произведенных после 1997 г. устройств поддерживают РпР, а большая часть PnP-драйверов для них содержится на установочном компакт-диске Windows Server 2003. При обнаружении нового устройства Windows Server 2003 находит для него подходящий драйвер, устанавливает и выделяет ему необходимые ресурсы, такие как запросы на прерывание (IRQ) и каналы прямого доступа к памяти (DMA). После этого устройство отображается в определенной категории в оснастке *Диспетчер устройств.*

Если PnP-драйвера нет на компакт-диске Windows Server 2003, для распознавания и установки устройства потребуется драйвер от изготовителя. Для устройств, которые Windows Server 2003 может распознать, система запросит драйвер. Если запрос на драйвер не выдается, Windows Server 2003 помечает в оснастке *Диспетчер устройств* (Device Manager) распознанное, но не сконфигурированное устройство желтым значком предупреждения. Этот значок (рис. 10-1) также применяется, когда в системе присутствуют идентичные устройства, или если существует конфликт между запросами драйверов на ресурсы (что происходит чрезвычайно редко с современными компьютерными системами и устройствами).

Если Windows Server 2003 не может распознать устройство, запрос на драйвер не выдается, и в оснастке *Диспетчер устройств* неизвестное устройство помечается желтым знаком вопроса. Для корректной работы несконфигурированных и нераспознанных устройств их драйверы следует установить вручную.

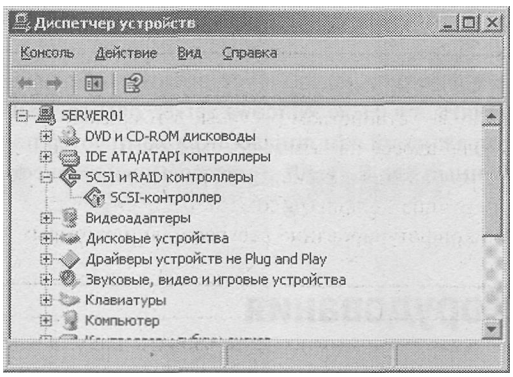


Рис. 10-1. Значок предупреждения в оснастке *Диспетчер устройств*

Работа с оснасткой *Диспетчер устройств*

Диспетчер устройств представляет установленное оборудование в стиле *Проводника*. Вы можете использовать его для обновления драйверов оборудования и изменения параметров устройств. Оснастку *Диспетчер устройств* можно раскрыть из *Панели управления* [выберите **Система (System),** перейдите на вкладку **Оборудование (Hardware)** в окне **Свойства системы (Systems Properties),** а затем щелкните **Диспетчер устройств (Device Manager)]**, либо из папки **Служебные программы (Administrative Tools)** в консоли *Управление компьютером* (Computer Management). В табл. 10-1 описаны задачи, для решения которых можно использовать *Диспетчер устройств*.

Табл. 10-1. Задачи оснастки *Диспетчер устройств*

Задача	Использование
Определение корректности работы установленного оборудования	Корректно сконфигурированные устройства отображаются с сортировкой по категориям. Обнаруженные устройства, которые не конфигурируются из-за отсутствия нужного драйвера либо неразрешимого конфликта ресурсов, помечены желтым значком с восклицательным знаком. Устройства, которые не удалось распознать, помечены желтым значком вопроса
Печать сводки по установленным устройствам	В меню **Действие (Action)** оснастки *Диспетчер устройств* выберите **Печать (Print).** Варианты печати: Сведения **о** системе (System **Summary), О выбранном классе или устройстве (Selected Class or Device), О системе и всех устройствах (All Devices And System Summary)**
Изменение параметров конфигурации оборудования	Чтобы открыть окно свойств устройства, щелкните устройство правой кнопкой и выберите **Свойства (Properties)** либо дважды щелкните устройство
Страницы свойств устройства	
Вкладка **Общие (General)**	Сведения о типе, изготовителе, размещении и состоянии данного устройства. Устройство можно включить или выключить из списка **Применение устройства (Device Usage)**
Вкладка **Драйвер (Driver)**	Просмотр подробных сведений о драйвере устройства (версия, поставщик драйвера, наличие цифровой подписи), установка обновленных драйверов устройства, обновление драйвера устройства, возврат к ранее установленной версии драйвера

Табл. 10-1. *(окончание)*

Задача	Использование
Вкладка Ресурсы **(Resources)**	Перечисляет используемые устройством ресурсы, в том числе диапазоны ввода-вывода, адреса памяти и прерывание. Возможность отключения автоматического конфигурирования (после чего возможно ручное конфигурирование) зависит от устройства: ручное конфигурирование ресурсов для некоторых устройств запрещено

Подготовка к экзамену Оснастку *Диспетчер устройств* можно использовать для управления устройствами только на локальном компьютере. На удаленном компьютере оснастка будет работать в режиме только для чтения.

Список устройств, драйверов и конфигурацию системы можно напечатать с помощью команды **Печать (Print)** из меню **Действие (Action)** оснастки *Диспетчер устройств* либо вывести в текстовый файл с разделителями — запятыми (CSV-файл), с помощью программы командной строки Driverquery, параметры которой перечислены в табл. 10-2.

Табл. 10-2. Параметры команды Driverquery

Параметр	Вывод
/S *система*	Задает имя или IP-адрес удаленного компьютера, к которому нужно подключаться. По умолчанию команда работает с локальным компьютером
/U *домен\пользователь*	Запускает команду в контексте пользователя, указанного параметром *пользователь* или *домен\пользователь*. По умолчанию применяется контекст пользователя, вошедшего на компьютер и исполняющего команду
/P *пароль*	Задает пароль учетной записи пользователя, указанного в параметре /U
/FO *формат* {TABLE | LIST | CSV}	Задает формат вывода сведений о драйверах. Допустимые значения: TABLE, LIST, CSV. Формат по умолчанию - TABLE
/NH	Исключает строку заголовка из выводимых сведений о драйверах. Действует, если параметру /FO задано значение TABLE или CSV
/V	Включает вывод подробных сведений о драйверах. Не допустим для подписанных драйверов
/SI	Включает вывод свойств подписанных драйверов
/?	Отображает справку в командной строке

Установка устройств пользователями и администраторами

Как и для большинства задач по установке, администраторы вправе устанавливать любое устройство и его драйверы. Пользователи, с другой стороны, имеют очень ограниченные возможности по установке устройств на компьютер. По умолчанию им разрешено устанавливать только PnP-устройства, причем со следующими условиями:

- драйвер устройства имеет цифровую подпись;
- для установки устройства не требуется дальнейших действий, требующих от Windows отображения пользовательского интерфейса;
- дистрибутив драйвера устройства уже есть на компьютере.

При нарушении любого из этих условий пользователь не может устанавливать устройства, если ему не делегированы дополнительные административные полномочия.

Подготовка к экзамену Если для установки PnP-устройства не нужно дополнительное вмешательство пользователя и драйвер уже сохранен на компьютер, обычный пользователь может подключить и использовать устройство. Это условие действует для всех устройств с интерфейсами USB, параллельным, ШЕЕ 1394, особенно для принтеров. Право пользователя загружать и выгружать драйверы устройств, настраиваемое средствами групповой политики, не применяется к PnP-драйверам, и его не нужно активировать, чтобы пользователь мог установить РпР-устройство.

Параметры подписывания драйверов

Драйверы устройств и файлы ОС из состава Windows 2000 и выше имеют цифровую подпись Microsoft. *Цифровая подпись* (digital signature) удостоверяет, что конкретный драйвер или файл не был изменен или перезаписан в процессе установки другой программы. Драйверы устройств, поставляемые изготовителями, могут быть не подписаны.

Вы можете управлять реакцией компьютера на неподписанные файлы драйверов в ходе установки. Эти параметры настраиваются в *Панели управления:* выберите **Система (System),** перейдите на вкладку **Оборудование (Hardware)** в окне **Свойства системы (Systems Properties),** щелкните **Подписывание драйверов (Driver Signing),** чтобы открыть окно **Параметры подписывания драйверов (Driver Signing Options)** для данного компьютера. Варианты обработки неподписанных драйверов в ходе установки таковы.

- **Пропускать (Ignore).** Устанавливать все драйверы устройств независимо от того, есть ли у них цифровая подпись. Этот вариант доступен, если вы вошли в систему как администратор или член группы *Администраторы* (Administrators).
- **Предупреждать (Warn).** Выводить предупреждение, позволяющее разрешить или запретить установку драйвера, если программа установки или Windows пытается установить драйвер устройства без цифровой подписи. Это поведение системы по умолчанию.
- **Блокировать (Block).** Запретить установку программами или Windows драйверов устройств без цифровой подписи.

Групповая политика — эффективное средство массовой настройки реакции на подписи драйверов. Чтобы запретить пользователям изменять эту настройку на своих компьютерах, вы должны блокировать им доступ к страницам свойств оборудования в *Панели управления* и отключить оснастку *Диспетчер устройств* в консоли *Управление компьютером.* Это не помешает пользователям устанавливать РпР-устройства.

Лабораторная работа. **Установка драйверов устройств**

На этой лабораторной работе вы установите сетевой адаптер, измените параметры подписывания драйверов, а затем вернете стандартную конфигурацию компьютера.

Упражнение 1. Установка сетевого адаптера

1. Откройте окно **Свойства системы (System Properties)** из *Панели управления,* затем на вкладке **Оборудование (Hardware)** щелкните **Установка оборудования (Add Hardware Wizard).**
2. Щелкните **Далее (Next)** и подождите, пока мастер оборудования проанализирует компьютер на наличие новых устройств. Если вы не добавляли какие-либо устройства, мастер спросит, подключено ли новое устройство.
3. Выберите **Да, устройство уже подключено (Yes, I Have Already Connected The Hardware),** затем щелкните **Далее (Next).**
4. **В** списке **Установленное оборудование (Installed Hardware)** выберите **Добавление нового устройства (Add A New Hardware Device),** затем щелкните **Далее** (Next).
5. Выберите вариант **Установка оборудования, выбранного из списка вручную [Install The Hardware That I Manually Select From A List (Advanced)]** и щелкните **Далее** (Next).
6. В списке **Стандартные типы оборудования (Common Hardware Types)** выберите **Сетевые платы (Network Adapters),** затем щелкните **Далее (Next).**
7. **В** списке **Изготовитель (Manufacturer)** выберите **Microsoft,** а в списке **Сетевой адаптер (Network Adapter) — Адаптер Microsoft замыкания на себя (Microsoft Loopback Adapter),** затем щелкните **Далее (Next).**
8. Щелкните **Далее** (Next), затем **Готово (Finish),** чтобы закрыть окно мастера.

Windows Server 2203 загрузит драйвер и установит устройство. Сетевой адаптер с именем **Адаптер Microsoft замыкания на себя (Microsoft Loopback Adapter)** появится в оснастке *Диспетчер устройств* в категории **Сетевые платы (Network Adapters).**

Упражнение 2. Настройка параметров подписывания драйверов

1. Откройте окно **Свойства системы (System Properties)** из *Панели управления,* затем на вкладке **Оборудование (Hardware)** щелкните **Подписывание драйверов (Driver Signing).**
2. Щелкните **Блокировать (Block).**
3. Щелкните **OK**.

Вы запретили установку драйверов без подписей.

Упражнение 3. Возврат компьютера к обычной конфигурации

1. В оснастке *Диспетчер устройств* щелкните правой кнопкой **Адаптер Microsoft замыкания на себя (Microsoft Loopback Adapter)** и выберите **Удалить (Uninstall).**
2. Щелкните **OK**, чтобы подтвердить удаление устройства.
3. Закройте оснастку *Диспетчер устройств.*
4. Откройте окно настройки подписывания драйверов снова и выберите **Предупреждать (Warn).**
5. Установите флажок **Использовать действие в качестве системного по умолчанию (Make This Action The System Default).**
6. Два раза щелкните **OK**.

Компьютер вернулся к обычной конфигурации.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Вы хотите быть уверены, что на настольных компьютерах в вашей среде не используются драйверы без подписи. Какие параметры подписывания драйверов и связанная конфигурация системы гарантируют это?
2. Пользователю нужно установить USB-принтер. Драйверы для принтера входят в состав Windows Server 2003. Может ли пользователь установить данный принтер?
3. Пользователю нужно установить USB-принтер. Драйвер поставляется изготовителем и не входит в состав Windows Server 2003. Он имеет цифровую подпись. Может ли пользователь установить данный принтер?

Резюме

- *Диспетчер устройств* (Device Manager) выводит список всех обнаруженных устройств и сообщает о проблемах с определением или конфигурацией драйверов.
- Конфигурацию драйверов можно напечатать средствами оснастки *Диспетчер устройств* или вывести в CSV-файл командой Driverquery.
- Пользователь может подключать и устанавливать любое полностью PnP-совместимое устройство. Если в процесс установки требуется вмешательство пользователя, установить устройство не удастся.
- Точки доступа к интерфейсу настройки устройств и драйверов можно заблокировать с помощью локальных и доменных групповых политик.
- Есть три варианта поведения системы в ходе установки неподписанных драйверов: **Пропускать (Ignore), Предупреждать (Warn), Блокировать (Block).**

Занятие 2. Настройка оборудования и драйверов

Обновленные драйверы для устройств могут потребоваться вследствие изменений в Windows Server 2003 или в методике программирования устройства изготовителем. Обновлять драйверы можно из оснастки *Диспетчер устройств*.

Чтобы свести к минимуму вероятность возникновения проблем с новым драйвером, в *Диспетчере устройств* есть функция, позволяющая вернуть предыдущую версию драйвера. Эта функция «отката» доступна в окне свойств устройства.

Иногда автоматической конфигурации ресурсов средствами Windows Server 2003 недостаточно, чтобы приспособить устройство к работе на конкретном компьютере. Если устройству требуется предоставить статические ресурсы (прерывание, порт ввода-вывода, канал DMA или диапазон адресов памяти), можно использовать *Диспетчер устройств* для удаления автоматических настроек и применения параметров, сконфигурированных пользователем/администратором.

Изучив материал этого занятия, вы сможете:

- ✓ использовать оснастку *Диспетчер устройств для* обновления, возврата к предыдущей версии и удаления драйверов;
- ✓ использовать оснастку *Диспетчер устройств* для анализа и настройки ресурсов, используемых устройствами.

Продолжительность занятия — около 15 минут.

Обновление драйверов

Оснастка *Диспетчер устройств* позволяет обновлять драйверы большинства устройств. Обновление драйверов проводят вручную независимо от того, поддерживает устройство РпР или нет. Эту операцию должен выполнять администратор (если пользователям не были представлены на то расширенные привилегии) на консоли локального компьютера.

Примечание Локальную установку можно провести без административных полномочий, если драйвер получен по каналам Windows Update. Подробнее о Software Update Services (SUS) и обновлении Windows — в главе 9.

Процесс обновления драйвера очень похож на установку корректно распознанного устройства, чей драйвер не был обнаружен. После запуска обновления драйвера в оснастке *Диспетчер устройств* мастер установки оборудования запрашивает размещение драйвера, а затем устанавливает его. После установки некоторых системных драйверов может понадобиться перезагрузить компьютер, однако для большинства периферийных устройств это не требуется. Страница свойств, с которой начинается обновление драйвера, показана на рис. 10-2.

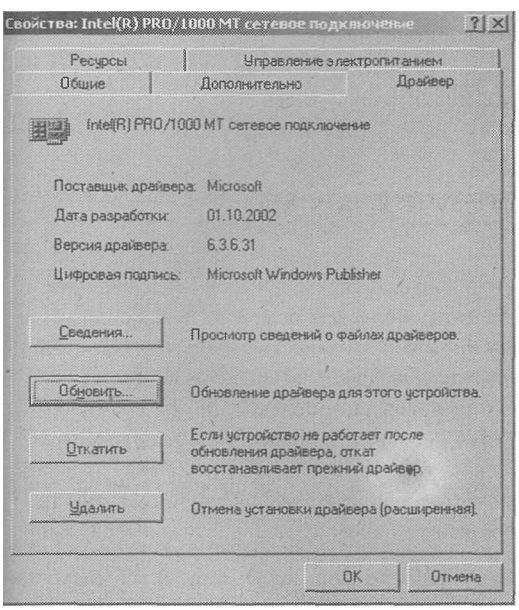


Рис. 10-2. Обновление драйвера

Примечание Если вы решили удалить, а затем повторно установить устройство, которое было настроено средствами РпР, после удаления нужно запустить поиск изменений конфигурации оборудования в *Диспетчере устройств,* поскольку Windows Server 2003 удаляет устройство из конфигурации, даже если оно все еще подключено к компьютеру.

Возврат к предыдущей версии драйвера

Иногда новый драйвер работает некорректно, и его нельзя оставить в конфигурации устройства. Если замененный драйвер функционировал корректно, можно вернуть его средствами *Диспетчера устройств*. Windows Server 2003 автоматически сохраняет резервную копию драйвера, заменяемого в ходе обновления, обеспечивая его доступность при выборе переключателя **Откатить (Roll Back Driver).** Страница свойств, с которой можно «откатить» драйвер, показана на рис. 10-3. Разница между этой функцией и вариантом **Загрузка последней удачной конфигурации (Last Known Good Configuration)** обсуждается на следующем занятии.

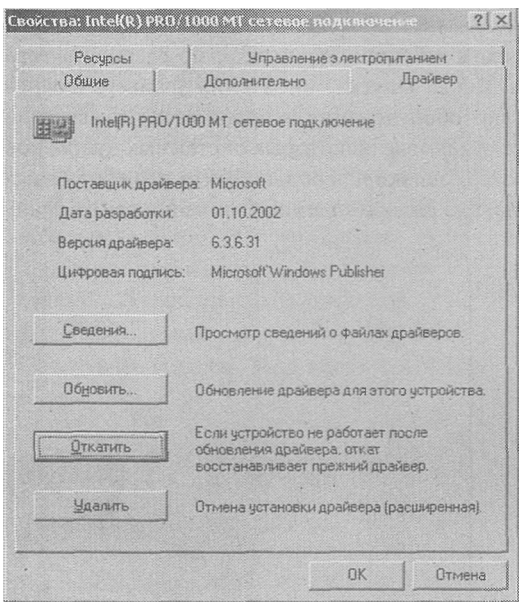


Рис. 10-3. Кнопка *Откатить*

Удаление драйверов

Драйверы можно удалять с помощью *Диспетчера устройств* со страницы свойств, показанной на рис. 10-4.

Удаление драйвера имеет различный эффект в зависимости от того, было устройство распознано и сконфигурировано средствами PnP или нет. Если устройство было настроено средствами PnP, то удаление драйвера приведет также и к удалению устройства из оснастки *Диспетчер устройств*. Если драйвер устройства был добавлен вручную, оно останется в *Диспетчере устройств,* но без сконфигурированного драйвера.

Конфигурирование ресурсов

Устройствам и их драйверам требуются системные ресурсы для обмена данными и их обработки в ОС. Windows Server 2003 конфигурирует эти ресурсы автоматически; иногда несколько устройств совместно используют какие-то ресурсы в рамках системы. *Диспетчер устройств* также позволяет до некоторой степени управлять назначением статических ресурсов для устройств. Если конфигурирование невозможно, используемые устройством и его драйвером ресурсы нельзя распределять вручную. Вкладка **Ресурсы (Resources)** в окне свойств устройства показана на рис. 10-5.

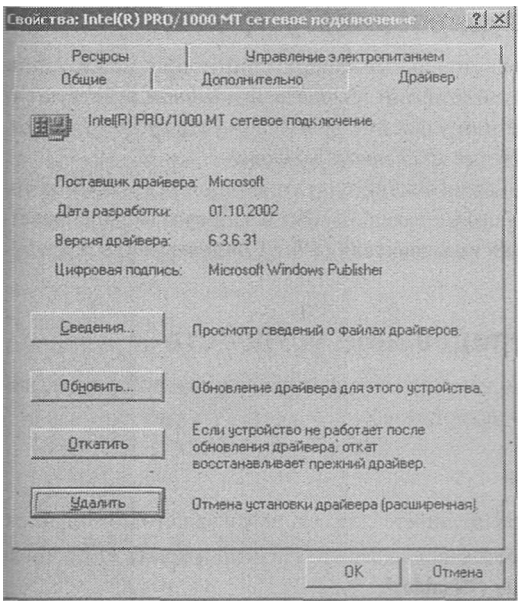


Рис. 10-4. Удаление драйвера

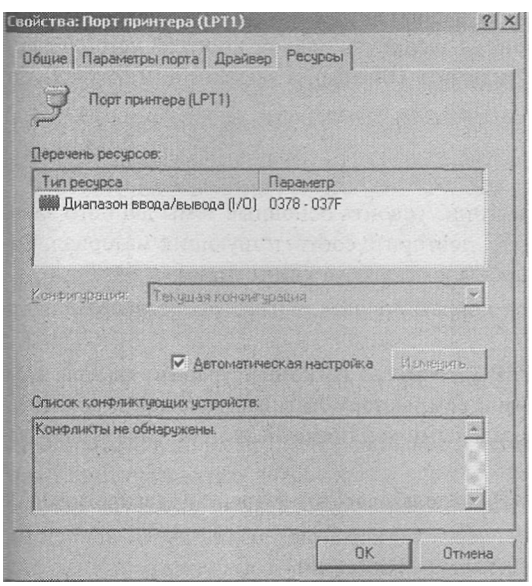


Рис. 10-5. Вкладка *Ресурсы* в окне свойств устройства

Перед тем как вручную настраивать назначение ресурсов, нужно снять флажок **Автоматическая настройка (Use Automatic Settings).**

Внимание! Если какой-либо ресурс был выделен вручную, автоматическое конфигурирование и самих ресурсов, и устройства становится невозможным, что ограничивает возможности Windows Server 2003 по настройке системы. Это может повлечь проблемы с другими устройствами.

Панель управления и конфигурирование устройств

Для некоторых устройств предусмотрены специальные конфигурирующие приложения в *Панели управления*. В отношении таких приложений в *Панели управления* действуют те же ограничения на установку, обновление или удаление драйверов устройств, основанные на правах пользователей, что и в оснастке *Диспетчер устройств*.

Страницы свойств для таких устройств администрируют отдельно средствами групповой политики; просмотр и доступ к ним пользователей можно запретить (см. соответствующий параметр в разделе **Конфигурация пользователя (User Configuration)** в редакторе групповой политики).

Лабораторная работа. Конфигурирование устройств

На этой лабораторной работе вы временно измените конфигурацию сетевой платы, выключив ее из работы без удаления самого устройства.

Упражнение. Отключение устройства

1. В оснастке *Диспетчер устройств* дважды щелкните сетевую плату вашего компьютера.
2. В списке **Применение устройства (Device Usage)** выберите **Не использовать это устройство (запретить) [Do Not Use This Device (Disable)].**

   Теперь устройство выключено из работы в рамках данного профиля оборудования.
3. Откройте окно свойств сетевой платы и выберите **Использовать это устройство (разрешить) [Use This Device (Enable)]**, чтобы заново активировать ее в рамках данного профиля оборудования. Другой вариант — щелкнуть правой кнопкой устройство и выбрать **Задействовать (Enable)** или **Отключить (Disable),** в зависимости от текущего состояния устройства.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. При каких условиях обычно требуется корректировать параметры ресурсов для устройства?
2. Вам необходимо временно удалить PnP-устройство из конфигурации, но при этом оставить его физически подключенным к компьютеру. Активация устройства в дальнейшем должна выполняться с минимальными усилиями. Какой из следующих вариантов оптимален?
   a. В окне свойств устройства выбрать **Не использовать это устройство (запретить) [Do Not Use this Device (Disable)].**
   b. В окне свойств устройства выбрать **Удалить (Uninstall).**
   c. Удалить устройство из *Программы безопасного извлечения устройств* (Safely Remove Hardware).
3. На компьютере пользователя установлен внешний жесткий диск USB, подключенный к USB-концентратору. Пользователь сообщает, что диск подключен корректно, но дисковод G, обычно связанный с ним, недоступен. В ходе изучения проблемы выясняется, что индикатор концентратора не горит, и устройство не отображается s оснастке *Диспетчер устройств*. Отключение и повторное подключение устройстве не помогает. Как быстрее всего восстановить работоспособность диска?

Резюме

- Оснастку *Диспетчер устройств* (Device Manager) можно использовать для отключения и включения отдельных устройств.
- Конфигурировать ресурсы для некоторых устройств можно вручную, но только в случае конфликта с другими ресурсами на данном компьютере. Ручное конфигурирование следует свести к минимуму, предоставив Windows Server 2003 свободу автоматически настраивать ресурсы для всех устройств.
- Обновление драйверов выполняют средствами *Диспетчера устройств*.
- Если необходимо использовать ранее сконфигурированный драйвер устройства, замененный новым драйвером, вернуть предыдущую версию драйвера можно также с помощью *Диспетчера устройств*.
- Чтобы активировать удаленное PnP-устройство, требуется обновить сведения о конфигурации компьютера. Чтобы активировать удаленное устройство без поддержки PnP, его нужно переустановить.

Занятие 3. Устранение неполадок оборудования и драйверов

Проблемы будут возникать, особенно если невозможно сконфигурировать драйвер средствами PnP, либо если обновляются драйверы компонентов ядра системы. Настройка драйвера средствами PnP невозможна, вероятность несоответствия устройств и их драйверов возрастает. Если обновлен драйвер компонента ядра системы, требующий перезагрузки компьютера, проблемы с драйвером не выявляются до перезагрузки.

Изучив материал этого занятия, вы сможете:

- ✓ применять различные способы восстановления после сбоя устройств;
- ✓ понимать и анализировать проблемы в работе драйверов.

Продолжительность занятия — около 15 минут.

Восстановление после сбоя устройства

Иногда при установке или обновлении драйвера устройства возникает проблема с функционированием устройства в системе. В зависимости от важности устройства эта проблема может иметь разные последствия — от раздражения до катастрофических потерь. В особенности это касается таких важных системных компонентов, как видеодрайверы, ошибки в конфигурации которых могут привести к неработоспособности компьютера. Согласитесь, вернуть предыдущую версию драйвера трудно, если вы не видите экран.

К счастью, предусмотрено несколько способов восстановления сбойной конфигурации драйверов. Доступные средства разработаны под различные цели и могут применяться с различным успехом. Средства, которые можно задействовать в случае некорректной конфигурации драйверов, перечислены в табл. 10-3.

Табл. 10-3. Средства восстановления драйверов

Средство	Уровень воздействия	Использование
Возврат предыдущей версии драйвера [Диспетчер устройств (Device Manager)]	Низкий. Большинство системных функций не затрагиваются	Используйте окно свойств устройства, чтобы вернуться к версии драйвера, с которой устройство работало нормально. Обратитесь к изготовителю. чтобы решить проблему с новым драйвером
Загрузка последней удачной конфигурации (Last Known Good Configuration)	Средний/высокий. Обновление драйвера устройства требует перезагрузки, и компьютер не возобновит работу с точки, откуда вы можете войти в систему	При смене драйверов, требующей перезагрузки, в разделе реестра HKLM\System\CurrentControlSet можно восстановить сведения о старом драйвере. Нажав F8 в момент загрузки системы, выберите **Загрузка последней удачной конфигурации (Last Known Good Configuration).** Это позволит восстановить старое значение данного раздела. Если проблема не проявлялась, пока вы успешно не вошли в ристему (что часто бывает при обновлении видеодрайвера), выбор этого варианта вряд ли даст эффект, поскольку последняя удачная конфигурация перезаписывается при успешном входе
Безопасный режим (Safe mode)	Средний/высокий. Система неработоспособна	Нажав F8, в момент загрузки системы выберите **Безопасный режим (Safe mode). В** этом режиме используется только минимально необходимый набор драйверов системы и устройств, достаточный для загрузки компьютера и входа в систему. После загрузки можно из оснастки *Диспетчер устройств* отключить проблемное устройство
Консоль восстановления (Recovery Console)	Высокий. Загрузка последней удачной конфигурации и безопасный режим не дают эффекта	*Консоль восстановления* позволяет входить в систему и обращаться к отдельным частям файловой системы из командной строки. С ее помощью можно отключить проблемный драйвер устройства, но необходимо знать корректное имя устройства или драйвера (либо и то и другое), которое может быть не столь явным

Коды состояний в *Диспетчере устройств*

При сбое устройства в оснастке *Диспетчер устройств* обычно выводится сообщение об ошибке, а рядом с именем устройства отображается желтый восклицательный знак. Если дважды щелкнуть устройство [либо щелкнуть его правой кнопкой и выбрать **Свойства (Properties)]**, откроется окно с перечнем сообщений об ошибках, обнаруженных оснаст-

кой *Диспетчер устройств*. В поле **Состояние устройства (Device Status)** содержится понятное описание неполадки, но для ее устранения может потребоваться знать больше, чем изложено **в** сообщении. Часто вместе с текстом приводится и код ошибки, помогающий решить проблему. Коды и предлагаемые стратегии исправления ошибок перечислены **в** табл. **10-4.**

Табл. 10-4. Устранение неполадок устройств

Код	Пояснение	Стратегия устранения неполадки
1	Устройство сконфигурировано неправильно. Для обновления драйверов этого устройства щелкните **Обновить драйвер (Update Driver).** Если это не помогает, см. документацию к оборудованию	Используйте функцию **Обновить драйвер** для обновления
3	Возможно, поврежден драйвер этого устройства, либо системе не хватает памяти или других ресурсов	Возможно, драйвер поврежден. При попытке загрузки поврежденного файла система может «решить», что требуется дополнительная память. Используйте *Диспетчер задач* (Task Manager), чтобы убедиться, что системе хватает памяти
10	Устройство не запускается. Попробуйте обновить его драйверы	Откройте *Мастер обновления оборудования* (Hardware Update Wizard), щелкнув кнопку **Обновить драйвер (Update Driver),** но не используйте автоматическое распознавание устройств средствами Windows Server 2003. Вместо этого выберите **Установка из указанного места [Install From A List Or Specific Location (Advanced)]** и вручную укажите мастеру нужный драйвер
12	Устройство не может найти достаточно свободных ресурсов для работы. Если вы намерены использовать данное устройство, потребуется отключить одно или несколько других устройств	Перейдите на вкладку **Ресурсы (Resources)** в окне свойств проблемного устройства. Windows Server 2003, вероятнее всего, сможет определить конфликтующее с ним устройство. Удалите или отключите конфликтующее устройство. Затем вы можете повторно добавить только что удаленное устройство и посмотреть, сможет ли оно самостоятельно использовать другие ресурсы либо вам придется назначать их вручную
Большинство других кодов	Различное	Большинство других кодов ошибок указывают, что используется некорректный драйвер, который следует переустановить

Совет Помните: если драйвер подписан, он протестирован на работу с Windows Server 2003. Список подписанных драйверов можно получить с помощью служебной программы *Сведения о системе* (System Information) в узле **Программная среда (Software Environment).** Программу *Сведения о системе* можно открыть из группы программ **Служебные (System Tools),** либо исполнив winmsd из командной строки.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Вы завершили конфигурирование нового драйвера дисплея, и система выдала зг-прос на перезагрузку компьютера, чтобы изменения вступили в силу. Практическж сразу после входа в систему экран гаснет. Какими методиками или средствами устранения неполадок проще всего решить проблему с драйвером дисплея?
   a. *Загрузка последней удачной конфигурации* (Last Known Good Configuration).
   b. Возврат предыдущей версии драйвера.
   c. *Безопасный режим* (Safe mode).
   d. *Консоль восстановления* (Recovery Console).
2. В оснастке *Диспетчер устройств* (Device Manager) есть устройство, рядом с копн рым отображается значок ошибки. В окне свойств этого устройства в поле Состояние устройства (Device Status) значится: «устройство не запускается». Как решить проблему?
3. Изготовитель установленной на вашем компьютере беспроводной сетевой платы выпустил новый драйвер и вы намерены протестировать его. Какой параметр в оснастке *Диспетчер устройств* (Device Manager) следует выбрать для тестирования нового драйвера?

Резюме

- Вариант загрузки *Загрузка последней удачной конфигурации* (Last Known Good Configuration) применяется для возврата ранее используемого драйвера, несовместимого с РпР, но только если вы еще не входили в систему после перезагрузки.
- При запуске компьютера в безопасном режиме загружается минимальный набор драйверов, достаточный для доступа к оснастке *Диспетчер устройств* (Device Manager), где можно отключить, удалить либо вернуться к предыдущей версии драйвера мешающего нормальной работе системы.
- Большинство проблем с драйверами возникают в ходе ручного конфигурирование некорректного драйвера.
- Параметры ресурсов следует настраивать вручную, только если конфликты не устраняются самой ОС.
- Все ресурсы, выделенные вручную, должны быть уникальными.

Пример из практики

Если на компьютере есть конфликты из-за выделения аппаратных ресурсов, профили оборудования позволяют выбрать устройства, которые будут функционировать в оп ределенных ситуациях. Вместо ручного назначения ресурсов устройствам (с рисков никогда не подобрать рабочую конфигурацию) лучше определить профиль оборудования, в котором ненужные устройства отключены, а их ресурсы доступны другому оборудованию.

Профили оборудования также позволяют оптимизировать производительность к в некоторой степени управлять энергопотреблением, отключая устройства и службы.

не используемые в определенных условиях. Например, можно увеличить срок службы батареи питания мобильного компьютера, создав «мобильный» профиль, в котором отключены устройства, не требуемые, когда компьютер не подключен к сети.

В этом упражнении вы отключите сетевую плату в профиле оборудования на мобильном компьютере.

1. На вкладке Оборудование (Hardware) в окне **Свойства системы (System Properties)** щелкните **Профили оборудования (Hardware Profiles)**.
2. Создайте копию текущего профиля. Назовите новый профиль **Mobile** и не меняйте значение параметра **Выбор профиля оборудования (Hardware Profiles Selection)** (этот параметр активирует первый профиль в списке, если выбор не сделан за 30 секунд).
3. Перезагрузите компьютер. В ответ на запрос выбора профиля оборудования укажите Mobile.
4. Войдите в систему и откройте оснастку *Диспетчер устройств* с вкладки **Оборудование (Hardware)** в окне **Свойства системы (System Properties)**.
5. Щелкните правой кнопкой сетевую плату в оснастке *Диспетчер устройств* и выберите Свойства (Properties).
6. В окне свойств сетевой платы в списке Применение устройства (Device Usage) выберите **Не использовать в текущем профиле оборудования (запретить) [Do Not Use This Device In The Current Hardware Profile (disable)]**.

Этим вы запретили использовать сетевую плату в одном профиле. Такую методику можно использовать в различных ситуациях, включая устранение неполадок устройств: воздавайте профили оборудования, в которых включены или отключены определенные устройства, и тестируйте их совместную работу и использование ресурсов.

Практикум по устранению неполадок

Дистрибутив Windows Server 2003 включает большинство драйверов, необходимых для конфигурирования современных аппаратных устройств, так что проблемы с конфигурацией встречаются крайне редко. Если конфликты приходится устранять вручную, то неправильная настройка — типичное явление.

Если изменение конфигурации устройства приводит к сбою при перезагрузке компьютера, функция Загрузка последней удачной конфигурации (Last Known Good Configuration) позволяет вернуть последний успешно работавший драйвер, если с момента установки "сбойного» драйвера вы не входили в систему.

Если вы входили в систему, последняя успешная конфигурация будет перезаписана текущей. Если произошел сбой драйвера и компьютер не работает уже после входа в систему, попробуйте вариант загрузки *Безопасный режим* (Safe mode), в котором загружается только минимальный набор драйверов, достаточный для конфигурирования проблемных устройств и драйверов.

В этом упражнении вы активируете варианты *Загрузка последней удачной конфигурации* и *Безопасный режим* на начальной стадии загрузки компьютера.

1. Перезагрузите компьютер.
2. Когда начнется загрузка, нажмите **F8**.
3. Выберите вариант **Загрузка последней удачной конфигурации (Last Known Good Configuration)**.

С этого момента все драйверы, несовместимые с PnP и установленные после последней перезагрузки и входа в систему, будут возвращены к предыдущим версиям.

4. Перезагрузите компьютер.
5. Когда начнется загрузка, нажмите F8.
6. Запустите компьютер в *Безопасном режиме* (Safe mode).
7. Войдите в систему и запустите оснастку *Диспетчер устройств* (Device Manager). Теперь можно конфигурировать устройства и их драйверы для загрузки в обычном режиме.

Резюме главы

- Для установки устройств, не совместимых с PnP, и их драйверов необходимы административные привилегии.
- Пользователям разрешено устанавливать устройства, полностью поддерживающие PnP. Если при этом требуется добавлять на компьютер драйверы, проводить дополнительное конфигурирование или вводить данные, установка устройства будет запрещена.
- Оснастка *Диспетчер устройств* (Device Manager) показывает с помощью значков различных видов все устройства, которые нельзя настроить из-за невозможности идентифицировать драйвер или решить конфликт ресурсов.
- Доступ пользователей к оснастке *Диспетчер устройств* и любым приложения в *Панели управления,* служащим для настройки оборудования, можно запретить средствами групповой политики.
- Обновленные драйверы можно вернуть к предыдущим версиям с помощью функции Откатить (Roll Back Driver) оснастки *Диспетчер устройств*.
- Устройства можно включать и отключать с помощью оснастки *Диспетчер устройств*.
- PnP-устройства, для которых есть подписанные драйверы на установочном компакт-диске Windows Server 2003, конфигурируются автоматически без вмешательства пользователей.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Повторите материал по использованию оснастки *Диспетчер устройств* (Device Manager для установки, обновления и возврата к предыдущим версиям драйверов устройств, а также отключению и включению устройств в профиле оборудования. Помните, что *Диспетчер устройств* позволяет менять параметры только на локальной системе, доступ к удаленной системе возможен лишь в режиме чтения.
- Пользователи могут устанавливать только PnP-устройства.

- Для установки драйверов, не совместимых с PnP, а также PnP-драйверов от изготовителей требуются административные полномочия.
- Если конфликт ресурсов не удается устранить, следует переустановить драйвер.
- Для устранения конфликта ресурсов сначала нужно снять флажок **Автоматическая настройка (Use Automatic Settings),** а затем задать требуемые значения параметров ресурсов.
- Вариант *Загрузка последней удачной конфигурации* (Last Known Good Configuration) имеет смысл только до завершения цикла «перезагрузка/вход пользователя в систему».
- В безопасном режиме загружается минимальный набор драйверов, достаточный для корректировки настроек.

Основные термины

Сравнение отката драйверов (Roll Back Driver) и загрузи! последней удачной конфигурации (Last Known Good Configuration). Возврат к предыдущей версии драйвера требует входа в систему, тогда как этот вход делает невозможным использование последней удачной конфигурации. Обе функции возвращают предыдущую конфигурацию драйвера устройства.

Сравнение удаления и отключения устройства. При удалении устройство исключается из всех конфигураций. В зависимости от типа устройства при следующем перезапуске системы или выполнении функции *Обновить конфигурацию оборудования* (Scan for Hardware changes) оно может быть обнаружено средствами PnP. При очередном запуске системы или выполнении функции *Обновить конфигурацию оборудования* это устройство будет распознано как новое.

После отключения и последующего включения устройства конфигурация драйвера не изменится, однако в период отключения использовать устройство нельзя.

Сравнение использования безопасного режима и загрузки последней удачной конфигурации. При входе в систему В безопасном режиме загружается минимальный набор драйверов, но той же версии, что обычно, тогда как загрузка последней удачной конфигурации возвращает предыдущую конфигурацию драйверов.

Вопросы и ответы

Занятие 1. Закрепление материала

1. Вы хотите быть уверены, что на настольных компьютерах в вашей среде не используются драйверы без подписи. Какие параметры подписывания драйверов и связанная конфигурация системы гарантируют это?

   Правильный ответ: в групповой политике для настольных компьютеров задайте параметру Security Option for Devices: Unsigned Driver Installation Behavior значение Не разрешать установку (Do Not Allow Installation). Также можно использовать доменные групповые политики, чтобы запретить пользователям настольных компьютеров доступ к окнам свойств оборудования и оснастке *Диспетчер устройств*.

2. Пользователю нужно установить USB-принтер. Драйверы для принтера входят в состав Windows Server 2003. Может ли пользователь установить данный принтер?
Правильный ответ: да. USB-принтер с драйверами, входящими в состав Windows Server 2003, совместим с PnP, и его драйвер подписан, поэтому установка такого устройства возможна без вмешательства пользователя. При этом предполагается, что на данном компьютере нет конфликта ресурсов.
3. Пользователю нужно установить USB-принтер. Драйвер поставляется изготовителем и не входит в состав Windows Server 2003. Он имеет цифровую подпись. Может ли пользователь установить данный принтер?
Правильный ответ: драйвер должен запрашиваться Мастером установки оборудования (Add Hardware Wizard) в Windows Server 2003; это требует участия пользователя посредством интерфейса, что (по умолчанию) запрещено.

Занятие 2. Закрепление материала

1. При каких условиях обычно требуется корректировать параметры ресурсов для устройства?
Правильный ответ: настройка драйверов обычно необходима для устранения конфликтов. При этом обычно конфликтуют устройства, которые не могут быть автоматически сконфигурированы ОС, такие как устаревшие ISA-или PCI-устройства.
2. Вам необходимо временно удалить PnP-устройство из конфигурации, но при этом оставить его физически подключенным к компьютеру. Активация устройства в дальнейшем должна выполняться с минимальными усилиями. Какой из следующих вариантов оптимален?
   a. В окне свойств устройства выбрать **Не использовать это устройство (запретить) [Do Not Use this Device (Disable)].**
   b. В окне свойств устройства выбрать **Удалить (Uninstall).**
   c. Удалить устройс-тво из *Программы безопасного извлечения устройств* (Safely Remove Hardware).
Правильный ответ: a. Этот способ позволяет временно отключить устройство. Чтобы снова использовать устройство, достаточно включить его. Другие варианты активации устройства требуют переустановки либо повторного анализа конфигурации компьютера.
3. На компьютере пользователя установлен внешний жесткий диск USB, подключенный к USB-концентратору. Пользователь сообщает, что диск подключен корректно, но дисковод G, обычно связанный с ним, недоступен. В ходе изучения проблемы выясняется, что индикатор концентратора не горит, и устройство не отображается в оснастке *Диспетчер устройств.* Отключение и повторное подключение устройства не помогает. Как быстрее всего восстановить работоспособность диска?
Правильный ответ: в оснастке Диспетчер устройств (Device Manager) щелкните правой кнопкой USB-концентратор и выберите Обновить конфигурацию оборудования (Scan for Hardware changes). Это активирует распознавание жесткого диска, подключенного к концентратору, как нового оборудования.

Занятие 3. Закрепление материала

1. Вы завершили конфигурирование нового драйвера дисплея, и система выдала запрос на перезагрузку компьютера, чтобы изменения вступили в силу. Практически сразу после входа в систему экран монитора гаснет. Какими методиками или средствами устранения неполадок проще всего решить проблему с драйвером дисплея?

a. *Загрузка последней удачной конфигурации* (Last Known Good Configuration).
b. Возврат предыдущей версии драйвера.
c. *Безопасный режим* (Safe mode).
d. *Консоль восстановления* (Recovery Console).

Правильный ответ: b, c. Вариант Загрузка последней удачной конфигурации (Last Known Good Configuration) использовать нельзя, поскольку вы вошли в систему, утвердив последние изменения. Безопасный режим позволит вернуться к старой версии драйвера с помощью оснастки Диспетчер устройств.

В оснастке *Диспетчер устройств* (Device Manager) есть устройство, рядом с которым отображается значок ошибки. В окне свойств этого устройства в поле **Состояние устройства (Device Status)** значится: **«устройство не запускается».** Как решить проблему?

Правильный ответ: установите подходящий драйвер устройства с помощью функции Обновить драйвер (Update Driver) оснастки Диспетчер устройств.

Изготовитель установленной на вашем компьютере беспроводной сетевой платы выпустил новый драйвер и вы намерены протестировать его. Какой параметр в оснастке *Диспетчер устройств* (Device Manager) следует выбрать для тестирования нового драйвера?

Правильный ответ: нужная вам функция оснастки Диспетчер устройств — Обновить драйвер (Update Driver). Хотя параметр Переустановить драйвер (Reinstall Driver) позволит использовать новый драйвер, при выборе обновления будет создана резервная копия текущего драйвера. Тем самым сохранится возможность возврата к старой версии драйвера в случае его некорректной работы.

ГЛАВА 11

Управление дисковой памятью в Windows Server 2003

Темы экзамена

- Управление базовыми и динамическими дисками.
- Оптимизация производительности серверных дисков.
- Реализация решения RAID.
- Дефрагментация томов и разделов.
- Мониторинг и оптимизация среды сервера для повышения производительности приложений.
- Мониторинг дисковых квот.
- Восстановление после аппаратного сбоя сервера.

В этой главе

Большие организации используют *сети хранения данных* (Storage Area Networks, SAN) — отказоустойчивые массивы дисковых накопителей, соединенные оптоволоконными каналами. Однако обычные жесткие диски, подключаемые к серверам напрямую, не скоро выйдут из употребления, поэтому вы должны быть уверены, что они настроены для оптимального баланса емкости, производительности и отказоустойчивости.

В этой главе рассказывается, как оптимально использовать физические диски в вашей системе хранения. Вы познакомитесь с возможностями хранения в Microsoft Windows Server 2003, включая гибкие структуры, которые упрощают расширение емкости, обеспечивают избыточность и повышают производительность, причем, как правило, без

перезагрузки! Вы научитесь настраивать и восстанавливать RAID-массивы средствами Windows Server 2003. Наконец, вы познакомитесь с программами *Проверка диска* (Check Disk), *Дисковые квоты* (Disk Quotas) и *Дефрагментация диска* (Disk Defragmenter), которые обеспечивают надежную работу дисков и, возможно, отодвигают неизбежный момент, когда место на них закончится.

Прежде всего

Здесь рассматриваются практические и теоретические вопросы, связанные с дисковой памятью. Для изучения материалов этой главы вам потребуются:

- компьютер под управлением Windows Server 2003 Standard или Enterprise, установленный как Server01 и настроенный в качестве контроллера домена contoso.com;
- на компьютере должен быть жесткий диск, на котором есть не менее 1 Гб нераспределенного пространства.

Занятие 1. **Типы дисковой памяти**

Прежде чем приступить к установке и настройке жесткого диска, нужно уяснить некоторые важные понятия, связанные с хранением данных. На этом занятии вы познакомитесь с концепциями, технологиями, функциями и терминологией, связанными с дисковой памятью в Windows Server 2003. Вы узнаете о различиях между базовыми и динамическими дисками и разнообразием логических томов, которые они поддерживают.

Изучив материал этого занятия, вы сможете:

- ✓ уяснить концепции и терминологию дисковой памяти;
- ✓ описать различия между базовыми и динамическими дисками;
- ✓ рассказать о возможностях и ограничениях базовых и динамических дисков;
- ✓ описать типы томов, поддерживаемые в Windows Server 2003.

Продолжительность занятия - около 15 минут.

Физические диски

Физический диск — это конгломерат пластика, металла и кремния, позволяющий пользователям хранить гигантские объемы бесполезных данных и файлов MP3 и (изредка) бизнес-документы. Конечно, это шутка, но вам важно понять разницу между физическими дисками и логическими томами, которые обсуждаются в следующем разделе. Важно также помнить, что современные дисковые подсистемы, например аппаратные RAID-массивы, могут состоять из нескольких физических дисков, но их выделенные аппаратные контроллеры скрывают физическую композицию дискового набора, чтобы Windows Server 2003 воспринимала и представляла такую дисковую подсистему в виде одного физического диска.

Логические тома

Логический том — это основная единица дисковой памяти, подлежащая настройке и управлению. Он может содержать пространство на нескольких физических дисках. Логические тома (или логические диски в контексте мониторинга производительности)

являются физически раздельными единицами хранения и позволяют отдельно хранить информацию разного типа, например ОС, приложения и данные пользователей. Логические тома традиционно обозначаются одной буквой латинского алфавита.

По мере погружения в терминологию, связанную с дисками, вы узнаете о разделах. логических дисках и томах. Во многих источниках эти термины взаимозаменяемы, что допустимо, поскольку технические отличия между ними минимальны, а различные средства помогают разобраться, поскольку оперируют лишь нужным типом логического тома в зависимости от выполняемой задачи. Не старайтесь сразу понять разницу между этими терминами, это придет с опытом.

Смонтированные тома

Обратите внимание, мы сказали, что логические тома традиционно обозначали одной буквой латинского алфавита. Это сильно ограничивает (до 26) количество и гибкость использования логических томов, которые можно создать в системе. Файловая система NTFS в Windows Server 2003 позволяет назначить для тома одну букву алфавита или не назначать ее вовсе. Кроме того, можно смонтировать том к одной или нескольким пустым папкам на существующем томе NTFS. Например, можно создать пустую папку Docs на существующем томе X: и смонтировать новый логический том размером 120 Гб к этой папке. При обращении к папке X:\Docs дисковая подсистема перенаправляет запросы ввода-вывода на новый том. Все это происходит прозрачно для пользователя.

Возможности этой мощной функции, по словам создателей, «не ограничены». Например, с ее помощью можно расширить доступное пространство на существующем томе. Если новый том является отказоустойчивым, а существующий — нет, папка X:\Docs, к которой монтируется том, представляет отказоустойчивую часть пространства имен существующего тома. Теоретически, можно смонтировать все логические тома сервера к папкам на дисках C: или D: и таким образом объединить огромный объем памяти под одной буквой диска.

Отказоустойчивость

Отказоустойчивость — это способность системы продолжить работу при отказе одного из компонентов, в нашем случае — жесткого диска. Windows Server 2003 поддерживает два типа отказоустойчивых логических томов: зеркальный (RAID-1) и чередующийся с четностью (RAID-5). Подробнее эти конфигурации обсуждаются далее. Сейчас важно запомнить несколько фактов об отказоустойчивости Windows Server 2003, часто называемой *программным RAID.*

- В отказоустойчивых конфигурациях используется не менее двух дисков, а пространство для хранения данных распределяется так, чтобы система могла восстановить их при отказе одного из дисков.
- Средства, обеспечивающие отказоустойчивость в Windows Server 2003, не позволяют продолжить работу тома, если из строя выходят два или более его дисков.
- ОС позволяет использовать любые два (или более) диска для создания отказоустойчивых томов. Чтобы создать отказоустойчивую конфигурацию сервера, не нужно приобретать дополнительное аппаратное или программное обеспечение. Тем не менее, при использовании зеркальных или томов RAID-5 в Windows Server 2003 лучше
. на одной шине использовать похожие или одинаковые диски. Излишнее разнообразие дискового оборудования или применение дисководов, подключенных к разным шинам SCSI и/или IDE, может значительно снизить производительность.

- Функции отказоустойчивости Windows Server 2003 используют циклы процессора и другие ресурсы сервера для управления томами. Тома RAID-5 могут значительно снизить производительность сервера. В настоящее время можно приобрести недорогие аппаратные отказоустойчивые дисковые массивы, называемые *аппаратными RAID-массивами,* в которых используются специальные контроллеры, отвечающие за отказоустойчивость. Такие системы обычно превосходят в скорости и гибкости управления и восстановления программные RAID-системы Windows Server 2003.
- Поскольку аппаратные RAID-контроллеры освобождают ОС от задач управления массивами, аппаратный RAID-массив в Windows Server 2003 выглядит как один диск.

Разделение данных

Прежде чем приступить к настройке дисковой подсистемы сервера, следует тщательно проанализировать требования к хранению данных. Администраторы обычно устанавливают ОС на логический том отдельно от приложений и данных. Обособление ОС упрощает защиту и управление дисковым пространством, чтобы для ОС всегда хватало свободного места. Кроме того, для ОС принято настраивать некоторый уровень отказоустойчивости.

Приложения обычно хранятся на втором томе, а данные и файлы пользователей — на третьем. Разделение данных по типам позволяет управлять безопасностью, производительностью и отказоустойчивостью отдельно для каждого типа данных. Если приложения используют журналы транзакций для записи данных в БД, как это делают Active Directory и Microsoft Exchange Server, обычно такие журналы хранятся на томах, расположенных на отдельных от БД физических дисках. Тогда в случае сбоя можно восстановить БД по журналам.

Тщательно проанализировав требования к дисковой памяти в плане типов данных, безопасности, производительности и отказоустойчивости, вы сможете решить, сколько дисков вам потребуется и как их следует настроить.

Базовые и динамические диски

ОС должна иметь возможность управлять физическим пространством на жестком диске. Есть две структуры, которые помогают Windows Server 2003 распределять дисковое пространство: базовые и динамические диски.

Базовые диски, разделы и логические диски

Лучше всего вам, вероятно, знакома структура базовых дисков. Базовые диски разбивают на разделы, каждый из которых функционирует как физически отдельная единица хранения. Информация о расположении и размере каждого раздела хранится на диске в таблице разделов *главной загрузочной записи* (Master Boot Record, MBR). Базовый диск может содержать до четырех разделов: четыре основных либо три основных и один дополнительный.

Логический том на базовом диске — это любой основной раздел или логический диск. Логический том, как уже было сказано, может быть представлен несколькими буквами дисков (либо вовсе не иметь такой буквы) и смонтирован к папке на существующем томе NTFS.

- Основной раздел. Каждому основному разделу соответствует один логический том на базовом диске. Если базовый диск используется для запуска ОС, только один основной раздел может быть также помечен активным.

Совет *Базовая система ввода-вывода* (basic input/output system, BIOS) компьютера просматривает активный раздел в поиске файлов, характерных для данного оборудования и необходимых для загрузки ОС. В технической документации этот раздел называют системным и обычно обозначают буквой «С». После начала загрузки запускается ОС. Большинство серверов настроены для загрузки ОС с диска С:. Раздел, на котором хранится ОС, называют *загрузочным*. Это может сбить с толку, поскольку на этот же том ссылаются по переменной %Sysvol%. К счастью, вам не нужно тратить время на запоминание этих отличий, поскольку в большинстве случаев ОС ставят только на диск С:, и он становится и системным, и загрузочным, и %Sysvol%.

- **Дополнительный раздел.** Базовый диск может содержать один дополнительный раздел. В отличие от основных, дополнительный раздел не форматируется, и ему не назначается буква диска. Вместо этого дополнительный раздел делят на логические диски — логические тома на базовом диске.

В предыдущих версиях ОС Microsoft, включая Windows 9x и MS-DOS, ОС могла «видеть» только основной раздел, на котором она была установлена, и дополнительный раздел диска, если он существовал. Для дальнейшего деления пространства на диске было необходимо настроить дополнительный раздел и разбить его на один или несколько логических дисков. Поскольку Windows NT/2000/XP и Windows Server 2003 могут получить доступ ко всем разделам на диске, дополнительный раздел нужен, только если вам требуется больше четырех логических дисков на одном физическом диске.

Динамические диски и тома

Помимо базовых дисков семейство Windows 2000/XP и Windows Server 2003 поддерживает динамические диски. Единицей хранения на динамическом диске является том, и одно из важнейших отличий динамических дисков от базовых в том, что первые поддерживают неограниченное количество томов, а конфигурационная информация об этих томах хранится в БД, управляемой службой *Диспетчер логических дисков* (Logical Disk Manager).

Логический том на динамическом диске — это том. Это может быть простой том на одном диске. Если на компьютере установлено несколько динамических дисков, у вас есть богатый выбор. Составные, зеркальные (RAID-1), чередующиеся (RAID-0) и чередующиеся с четностью (RAID-5) тома — это логические тома, объединяющие пространство на нескольких физических дисках. Том каждого типа по-своему использует пространство диска и характеризуется разным уровнем отказоустойчивости. Ниже перечислены главные особенности томов каждого типа; нюансы вы узнаете по мере прочтения главы.

- **Простой том.** Эквивалент раздела на базовом диске. Занимает место на одном физическом диске и соответствует одному логическому тому. Простой том можно расширить, добавив нераспределенное пространство того же диска. Это позволяет увеличивать емкость тома по мере увеличения объема данных, которые на нем хранятся. Поскольку простые тома находятся на одном физическом диске, они не устойчивы к отказам.
- **Составной том.** Содержит пространство нескольких физических дисков. Составной том может объединять пространство до 32 физических дисков, причем объем занятого пространства на каждом диске может быть разным. Данные записываются в том,. начиная с первого диска. Когда место на первом диске заканчивается, данные записываются на второй диск и т. д. Составные тома позволяют увеличивать емкость дис-

ковой памяти. Если место на простом или составном томе заканчивается, его можно расширить на новые диски.

Составные тома, тем не менее, не могут участвовать в отказоустойчивых конфигурациях. Поскольку их размер имеет тенденцию к росту и в томе используется несколько физических дисков, риск сбоя увеличивается. Если любой диск в составном томе выходит из строя, теряются все данные тома. Поэтому Windows Server 2003 не позволяет устанавливать ОС на составной том или расширять системный том. Составной том рекомендуется использовать только временно, когда место на существующем томе исчерпано или когда отказоустойчивость обеспечивается другими средствами, например, в большой библиотеке данных, предназначенных только для чтения, которую можно легко восстановить с архивной ленты в случае сбоя.

- **Чередующийся том.** Чередующийся том (RAID-0) объединяет свободное пространство нескольких жестких дисков в один логический том. Однако, в отличие от составного тома, данные равномерно записываются на все физические диски тома. Поскольку одновременно используется несколько физических дисков, скорость операций чтения и записи увеличивается практически геометрически при добавлении новых физических дисков. Как и в случае расширенных простых и составных томов, если один диск выходит из строя, теряются все данные тома.
- **Зеркальный том.** Зеркальный том (называемый *RAID первого уровня,* или *RAID-1)* состоит из двух одинаковых копий простого тома, каждая из которых находится на отдельном жестком диске. Зеркальные тома позволяют продолжать работу, если один из физических дисков выходит из строя.
- **Том RAID-5.** Отказоустойчивый чередующийся том. Объединяет пространство трех или более физических дисков в один том. Данные равномерно записываются на все физические диски, однако, в отличие от RAID-0, данные чередуются с информацией о контрольной сумме, называемой *четностью.* Если один из дисков тома выходит из строя, потерянную информацию можно восстановить, используя оставшиеся данные и информацию о контрольной сумме. Интересно заметить, что данные четности распределяются по всем томам в наборе RAID-5.

Сравнение базовых дисков с динамическими

Теперь, когда вы узнали о базовых и динамических дисках, типах разделов, логических дисках и томах, давайте попытаемся определить, какие из них лучше? Как это часто бывает, ответ зависит от ситуации.

Динамические диски с данными легко переносить с одного сервера на другой; можно перенести диск с вышедшего из строя сервера на работающий за минимальное время. Динамические диски выгодно использовать, когда их в компьютере несколько. Любой компьютер под управлением Windows 2000/XP и Windows Server 2003 может поддерживать одну группу дисков, состоящую из нескольких динамических дисков. БД LDM реплицируется на все диски группы; это повышает надежность хранения информации о конфигурации дисков группы. Кроме того, диски могут работать вместе, образуя различные гибкие и мощные типы томов, в том числе составные, чередующиеся (RAID-0), зеркальные (RAID-1) и чередующиеся с четностью (RAID-5).

Тем не менее, базовые диски будут по-прежнему использоваться по следующим причинам.

- Базовые диски используются в Windows Server 2003 по умолчанию, поэтому все новые, диски будут оставаться базовыми, пока их не преобразуют в динамические (этот простой процесс описан на занятии 2).

- Динамические диски не дают никаких преимуществ на компьютере, где установлен один жесткий диск.
- Структура БД LDM затрудняет перенос динамического диска, с которого запускается ОС, с одного компьютера на другой.
- Динамические диски не поддерживаются для съемных носителей и на портативных компьютерах.
- Базовые диски — промышленный стандарт, поэтому к ним можно обращаться из любой ОС, включая MS-DOS, все версии Microsoft Windows и большинство других ОС (есть и такие). Таким образом, динамические диски нельзя использовать, если вам требуется альтернативная загрузка с одной из предыдущих версий ОС, которой нужен доступ к данному диску. Помните, что мы говорим только о *локальном* доступе. Когда пользователь любой платформы обращается к файлам по сети, тип диска и тома для него не играют роли.

Подготовка к экзамену Альтернативная загрузка стала менее популярной с появлением технологии виртуальных машин (см. *http://www.microsoft.com/windowsserver2003/techinfo/overview/virtualization.mspx)*. Тем не менее, если вы реализовали альтернативную загрузку и одной из ОС является Windows Server 2003, следует установить каждую ОС на отдельный основной раздел. Другие конфигурации по меньшей мере рискованны. Подробнее об альтернативной установке — в *Центре справки и поддержки)*.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Вы устанавливаете новый диск объемом 200 Гб и хотите поделить его на пять логических томов: для ОС, приложений, домашних каталогов пользователей, общих данных и точки распространения ПО. Пространство диска нужно поровну разделить между пятью логическими томами. Кроме того, вы хотите оставить 50 Гб нераспределенного пространства для дальнейшего расширения какого-либо логического тома. Какую конфигурацию выбрать с учетом базовых и динамических дисков и типов поддерживаемых ими логических томов?
2. Что из перечисленного позволяет восстановить данные, когда один жесткий диск выходит из строя?
   a. Основной раздел.
   b. Дополнительный раздел.
   c. Логический диск.
   d. Простой том.
   e. Составной том.
   f. Зеркальный том.
   g. Чередующийся том.
   h. ТОМ RAID-5.
3. Вы настраиваете тестовую систему с альтернативной загрузкой. На первый основной раздел установлена ОС Windows NT 4, а на второй — Windows Server 2003. На диске уже нет места, поэтому вы добавляете новый диск, загружаете Windows Server 2003 и настраиваете новый диск как динамический. Запустив Windows NT 4, вы не видите этот диск. Почему?

4. Чтобы обеспечить отказоустойчивость, максимальную производительность и возможность горячей замены неисправного диска, вы приобрели аппаратный RAID-массив из семи дисков. После установки массива вы увидели в Windows Server 2003 только один новый диск. Почему?

Резюме

- Терминология, связанная с дисками, может сбить с толку, но по сути логический том является практически синонимом терминов *раздел, логический диск* или *том*.
- Windows Server 2003 поддерживает базовые и динамические диски. Базовые диски поддерживают до четырех разделов: четыре основных, либо три основных и один дополнительный, которые, в свою очередь, могут содержать несколько логических дисков. Динамические диски поддерживают простые тома, а если на компьютере несколько таких дисков, то и составные, зеркальные, чередующиеся и тома RAID-5.
- Отказоустойчивость обеспечивают зеркальные тома (RAID-1), содержащие полную копию данных тома на каждом из двух дисков, и чередующиеся с четностью тома (RAID-5), которые распределяют данные по нескольким дискам и используют информацию о четности для восстановления данных любого одного вышедшего из строя диска.
- Простые, составные и чередующиеся (RAID-0) тома, а также все логические диски на базовом диске не являются отказоустойчивыми. Все данные теряются, когда любой из дисков, хранящих такой том, выходит из строя. Чем больше размер и количество физических дисков, из которых состоит том, тем выше вероятность сбоя.

Занятие 2. Настройка дисков и томов

На этом занятии вы получите реальные навыки по установке, настройке и управлению дисковой памятью. Вы узнаете, как использовать оснастку *Управление дисками* (Disk Management) для обнаружения и инициализации нового диска и разбиения его на разделы, логические диски и тома. Вы узнаете, как расширить том, если место на нем закончилось. Вы также научитесь переносить диски с одного сервера на другой. Наконец, вы познакомитесь с новой мощной командой DISKPART, которая позволяет управлять диском из командной строки.

Изучив материал этого занятия, вы сможете:

- ✓ установить и инициализировать физический диск;
- ✓ управлять конфигурацией логических томов на базовых и динамических дисках;
- ✓ смонтировать том к папке на томе NTFS;
- ✓ расширить емкость тома;
- ✓ переносить диски с одного сервера на другой;
- ✓ преобразовывать базовые и динамические диски;
- ✓ выполнять задачи по обслуживанию дисков с помощью команды DISKPART.

Продолжительность занятия — около 25 минут.

Оснастка *Управление дисками*

Для управления дисками служит оснастка *Управление дисками* (Disk Management) из консоли *Управление компьютером* (Computer Management). Откройте оснастку *Управление дисками* или добавьте ее в собственную консоль.

Совет Существует отдельная консоль *Управление дисками,* но ее нельзя запустить из папки **Администрирование (Administrative Tools).** Чтобы сделать это, в меню **Пуск (Start)** выберите **Выполнить (Run)** и исполните команду diskmgmt. msc.

Оснастка *Управление дисками* позволяет управлять дисками на локальном и удаленных компьютерах. Она манипулирует с конфигурацией дисков не напрямую, а взаимодействует со *Службой администрирования диспетчера логических дисков* (Logical Disk Manager Administrative Service) (Dmadmin), которая запускается на компьютере, когда вы открываете оснастку *Управление дисками*.

Интерфейс оснастки *Управление дисками* показан на рис. 11-1. Верхний список содержит сведения обо всех разделах, логических дисках и томах. Внизу в графическом виде изображено распределение пространства на каждом физическом диске так, как это воспринимает Windows Server 2003. Вы можете щелкнуть любой том правой кнопкой, чтобы открыть контекстное меню, позволяющее отформатировать, удалить или назначить для тома букву. Щелкнув правой кнопкой область нераспределенного пространства диска, можно создать раздел или том. Щелкнув правой кнопкой панель состояния диска слева от графического изображения можно инициализировать новый диск, преобразовать базовый диск в динамический (или наоборот) и открыть окно свойств оборудования диска.

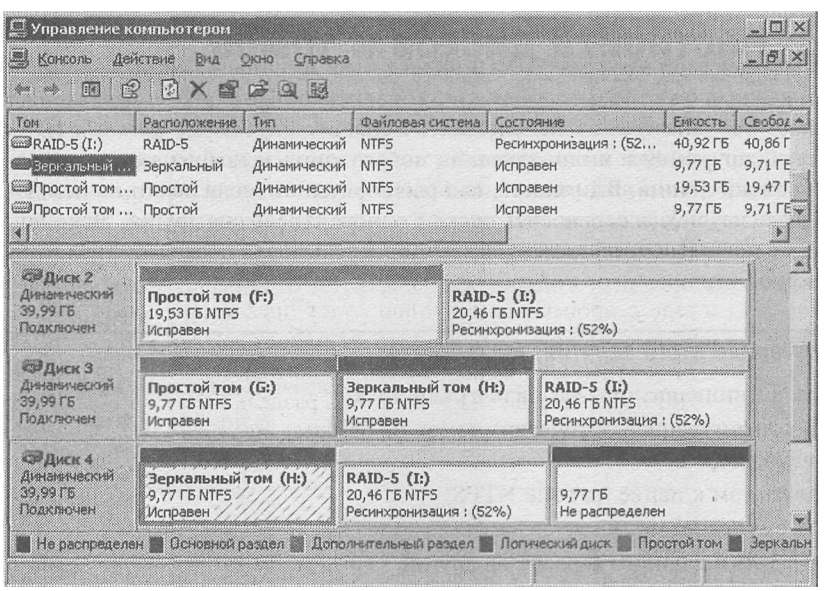


Рис. 11-1. Консоль *Управление дисками*

Настройка дисков и томов

Настройка диска подразумевает следующие действия.

1. Физическая установка диска.
2. Инициализация диска.
3. Создание разделов или логических дисков на базовом диске (для дополнительного раздела) или томов на динамическом диске.
4. Форматирование томов.
5. Назначение букв томам или монтирование томов к пустым папкам на существующих томах NTFS.

Для выполнения этих задач вы должны быть членом групп *Администраторы* (Administrators) или *Операторы архива* (Backup Operators) или иметь делегированные полномочия; форматировать том могут только администраторы.

Установка диска

Чтобы добавить новый диск в компьютер, установите или подключите новый физический диск (или диски). Откройте оснастку *Управление дисками* и, если диск не определился автоматически, щелкните узел **Управление дисками (Disk Management)** правой кнопкой и выберите **Повторить сканирование дисков** (Rescan **Disks).** Если систему нужно перевести в автономный режим для установки нового диска, перезагрузите компьютер, а затем откройте оснастку *Управление дисками.* Если новые диски не определяются автоматически, просканируйте их повторно.

Инициализация диска

После добавления диска на сервер его нужно инициализировать, и уже затем выделять пространство под разделы, логические диски и тома. При инициализации ОС записывает на диск сигнатуру диска, метку конца сектора (также называемую *словом сигнатуры),* а также MBR или таблицу разделов с кодами GUID.

Если запустить консоль *Управление дисками* после установки нового диска, автоматически откроется мастер инициализации дисков. Чтобы инициализировать диск вручную с помощью оснастки *Управление дисками,* щелкните панель состояния диска правой кнопкой и выберите **Инициализировать диск (Initialize Disk).**

Примечание На компьютере с процессором Itanium будет предложено указать стиль раздела. Компьютеры Itanium с несколькими дисками поддерживают два стиля разделов, таблицу разделов: GPT и MBR. Системный раздел на компьютере Itanium использует интерфейс Extensible Firmware Interface (EFI) и стиль раздела GPT для поддержки 64-разрядных редакций Windows Server 2003. Подробнее о разделах GPT и EFI — в *Центре справки и поддержки.*

Создание разделов и томов

После инициализации диска можно приступать к реализации структуры разделов, логических дисков или томов.

По умолчанию инициализированный диск становится базовым. Если вас это устраивает, можно разбить его на основные и дополнительный разделы: щелкните нераспределенное пространство правой кнопкой и выберите **Создать раздел (New Partition).** Созданный основной раздел становится логическим томом. После создания дополнитель-

ного раздела щелкните его правой кнопкой и выберите **Создать логический диск (New Logical Drive).** Как мы уже упоминали, логические диски — это логические тома на дополнительном разделе.

Если вы хотите сделать диск динамическим, щелкните правой кнопкой панель состояния диска в оснастке *Управление дисками* и выберите **Преобразовать в динамический диск (Convert To Dynamic Disk).** Затем щелкните нераспределенное пространство правой кнопкой и выберите **Создать том (New Volume).** Откроется *Мастер создания томов* (New Volume Wizard), который поможет вам создать том нужного типа. Страница **Выбор типа тома (Select Volume Type)** мастера показана на рис. 11-2.

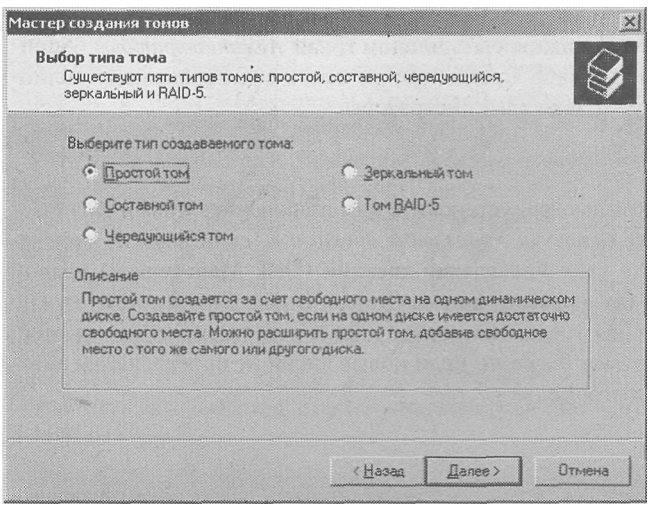


Рис. 11-2. Страница *Выбор типа тома* мастера создания томов

Существующий базовый диск также можно преобразовать в динамический, это обсуждается далее.

Форматирование томов

Windows Server 2003 поддерживает три файловые системы: FAT, FAT32 и NTFS. Сразу упростим дискуссию: используйте FAT или FAT32 только в крайних случаях. Только NTFS предоставляет необходимый организации уровень стабильности, устойчивости, масштабируемости, гибкости и безопасности. Большинство основных компонентов Windows Server 2003, включая защиту файлов и такие службы, как Active Directory и RIS (Remote Installation Services), требуют NTFS. Все современные задачи управления дисками, в том числе многодисковые тома и квотирование дисков, требуют NTFS. Сто раз подумайте, прежде чем выбрать FAT32.

Назначение букв дискам и монтирование томов

Созданному тому автоматически назначается следующая доступная буква алфавита. *Мастер создания томов* (New Volume Wizard) и *Мастер создания разделов* (New Partition Wizard) позволяют указать другое представление для нового логического тома. Можно также щелкнуть существующий том правой кнопкой и выбрать **Изменить букву диска или путь к диску (Change Drive Letter and Paths).**

Том можно обозначать только одной буквой или не обозначать вовсе. Кроме того, можно смонтировать том к одной или нескольким пустым папкам на локальных томах

NTFS. В окне **Изменение буквы диска или путей (Change Drive Letter And Paths)** щелкните кнопку **Удалить (Remove)** или **Изменить (Change),** чтобы удалить или изменить существующую букву диска или монтирование тома к папке.

Примечание Нельзя изменить букву тома, который является системным или загрузочным разделом.

Щелкните кнопку **Добавить (Add),** чтобы добавить букву диска или точку монтирования. На рис. 11-3 показан сервер, где папка Docs на диске X: является точкой монтирования для другого тома. Заметьте: в пространстве имен *Проводника* папка расположена обычным образом, но отображается со значком диска. Когда пользователь открывает такую папку, он автоматически перенаправляется на нужный том.

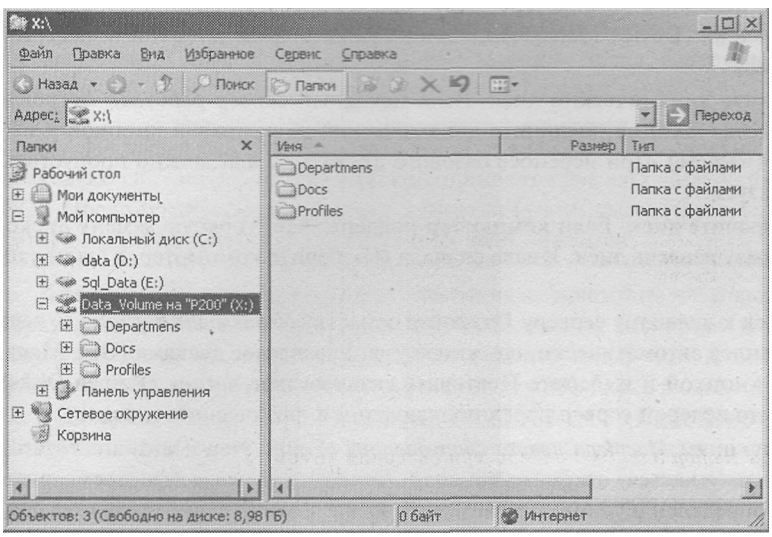


Рис. 11-3. Том, смонтированный к папке

Монтирование тома к папке на существующем томе увеличивает его размер **и** свободное пространство. При этом неважно, находится ли том на базовом или динамическом диске и какой у него тип. Пустая папка, к которой монтируется том, должна находиться на томе NTFS. Смонтированный том (теоретически) можно отформатировать под FAT или FAT32, но делать этого не стоит.

Существующие тома

Другим способом увеличения емкости тома является его расширение. Расширить можно простой или составной том на динамическом диске, если том отформатирован под NTFS и не является системным или загрузочным: щелкните его правой кнопкой, выберите **Расширить том (Extend Volume)** и следуйте инструкциям *Мастера расширения тома* (Extend Volume Wizard), чтобы выбрать нераспределенное пространство динамического диска, на которое нужно расширить существующий том. При расширении простого тома на пространство другого физического диска вы получаете составной том.

Для расширения раздела на базовом диске можно пользоваться командой DISKPART. Основной раздел должен быть отформатирован под NTFS, не должен быть системным или загрузочным и должен расширяться на смежное непрерывное пространство на том

же физическом диске, которое не выделено или не отформатировано либо отформатировано под NTFS.

Перенос дисков с одного сервера на другой

Можно переносить диски с одного компьютера на другой. Например, если вы планируете перевести сервер в автономный режим, можно подключить его физические диски к другому серверу, чтобы пользователи могли обращаться к данным.

1. Проверьте работоспособность диска, пока он подключен к первоначальному серверу. Перед переносом диска рекомендуется открыть оснастку *Управление дисками* (Disk Management) и убедится, что состояние диска — **Исправен (Healthy).** Иначе устраните неполадку диска.
2. Удалите диск на исходном компьютере. Если исходный сервер работает, в оснастке *Диспетчер устройств* (Device Manager) щелкните диск правой кнопкой и выберите **Удалить (Uninstall)**.
3. Правильно удалите динамический диск. Если исходный сервер работает, откройте оснастку *Управление дисками,* щелкните динамический диск правой кнопкой и выберите **Удалить (Remove).** При переносе базового диска этот шаг можно пропустить, или он не реализуем.
4. Физически отключите диск. Если компьютер поддерживает горячую замену дисководов, можно сразу извлечь диск. Иначе сначала выключите компьютер, а затем удалите диск.
5. Подключите диск к целевому серверу. Откройте оснастку *Управление дисками* и, если диск не определился автоматически, щелкните узел **Управление дисками (Disk Management)** правой кнопкой и выберите **Повторить сканирование дисков (Rescan Disks).** Иначе выключите целевой сервер перед подключением физического диска.
6. Следуйте инструкциям *Мастера нового оборудования* (Found New Hardware Wizard). Если мастер не запускается, откройте консоль *Диспетчер устройств* и посмотрите, не был ли диск определен и установлен автоматически. Если нет, запустите программу *Установка оборудования* (Add Hardware) из *Панели управления*.
7. Откройте оснастку *Управление дисками*. Щелкните узел **Управление дисками (Disk Management)** правой кнопкой и выберите **Повторить сканирование дисков (Rescan Disks).**
8. Щелкните любой диск с отметкой **Инородный (Foreign)** правой кнопкой и выберите **Импорт чужих дисков (Import Foreign Disks).** При импорте на новом динамическом диске БД LDM согласуется с существующими дисками.

При переносе дисков учтите следующее.

- Если импортированный диск содержит тома, распространяющиеся на другие физические диски, необходимо подключить и импортировать их до начала работы с томом.
- Если вы переносите диски с нескольких компьютеров на один, делайте это последовательно.
- При переносе на другой компьютер базовому тому назначается следующая доступная буква алфавита. Динамическому тому назначается буква, которой он обозначался на исходном компьютере. Если динамический том не был обозначен буквой на предыдущем компьютере, она не присваивается и на новом компьютере. Если старая буква уже используется, том получает следующую доступную букву алфавита.

- Используйте команды Mountvol /n или DISKPART, чтобы предотвратить автоматическое монтирование нового тома и назначение буквы диска. При использовании этих команд для добавления нового диска нужно вручную монтировать тома и назначать буквы диска и пути.

Преобразование дисковой памяти

Базовый диск можно преобразовать в динамический. Если диск уже содержит разделы и логические диски, они будут преобразованы к соответствующим единицам хранения динамического диска — простым томам. Структура данных на диске не изменяется, поэтому можно преобразовать базовый диск, который уже содержит данные, хотя рекомендуется всегда архивировать диск перед выполнением задач управления дисками.

Чтобы преобразовать базовый диск в динамический, щелкните панель состояния диска правой кнопкой и выберите **Преобразовать в динамический диск (Convert To Dynamic Disk).** Только и всего. При преобразовании диска, содержащего системный или загрузочный разделы, компьютер необходимо перезагрузить.

Совет Не пытайтесь преобразовать базовые диски в динамические, если они содержат несколько ОС (например, если диск используется для альтернативной загрузки с другой ОС). После преобразования диска в динамический вы сможете запустить только ОС, которая использовалась для выполнения этой операции.

К сожалению, обратное преобразование выполняется не настолько просто. При преобразовании к базовому типу теряются все данные на диске. Так что сначала их нужно заархивировать. После этого удалите все существующие тома на динамическом диске, а затем щелкните правой кнопкой панель состояния диска в оснастке *Управление дисками* и выберите **Преобразовать в базовый диск (Convert To Basic Disk).** После воссоздания разделов и логических дисков восстановите данные. Хотя этот метод и можно назвать преобразованием динамического диска в базовый, на самом деле вы просто очищаете диск и строите его с нуля.

Управление дисками из командной строки

Windows Server 2003 содержит следующие программы командной строки для управления дисками:

- **Chkdsk.** Ищет ошибки на диске и, если указано, пытается их исправить.
- **Convert.** Преобразует том FAT или FAT32 в NTFS.
- **Esutil.** Выполняет различные задачи, связанные с управлением томами FAT, FAT32 или NTFS.
- **Mountvol.** Управляет монтированием томов и *точками повторной обработки* (reparse point).

Однако «прадедушкой» всех этих средств командной строки является программа DISKPART. В табл. 11-1 перечислены команды DISKPART, выполняющие типичные задачи управления дисками. Команду DISKPART можно использовать интерактивно или вызывать из сценария. Чтобы запустить ее интерактивно, наберите `diskpart` в командной строке. Когда появится приглашение DISKPART >, введите ?, чтобы получить справку. Встроенная документация будет автоматически отображаться каждый раз, когда вам будет нужна справка. Кроме того, программа хорошо документирована в *Центре справки и поддержки*.

Табл. 11-1. Выполнение типичных задач управления дисками из командной строки

Задача	В приглашении DISKPART >	Описание

Отображение сведений о дисках, разделах и томах	`list disk`
	`list partition`
	`list volume`
		Первая команда отображает сведения о дисках, вторая — о разделах текущего диска, третья — о разделах и томах всех дисков

Создание простого тома	`create volume simple size=500 disk=2`	Введенная на одной строке, эта команда создает простой том размером 500 Мб на диске 2
Назначение буквы диска	`select volume 4` `assign letter j`	Назначает букву J тому 4
Расширение простого тома	`select volume 4` `extend size=250 disk=2`	Увеличивает размер простого тома 4 (на диске 2) на 250 Мб на том же диске
Создание составного тома	`select volume 4` `extend size=250 disk=1`	Увеличивает размер простого тома 4 (на диске 2) на 250 Мб на диске 1
Удаление составного тома	`select volume 4` `delete volume`	Удаляет составной том 4. Если том 4 находился на дисках 1 и 2, все занятое им пространство на обоих дисках становится нераспределенным
Создание точки монтирования тома	`select volume 4` `assign mount=e:\Folder1`	Назначает точку монтирования тому 4 через папку E:\Folderl
Создание чередующегося тома	`create volume stripe size=500 disk=1, 2`	Вводится одной строкой, создает чередующийся том, который занимает по 500 Мб на дисках 1 и 2
Создание зеркального тома	`create volume simple size= 00 disk=1` `add disk 2`	Введенная на одной строке, эта команда создает отказоустойчивый зеркальный том, который в сумме занимает 500 Мб на дисках 1 и 2
Разбиение зеркала	`select volume 5` `break disk 2`	Выбирает зеркало на томе 5 и разбивает зеркало на диске 2
Удаление зеркала	`break disk 2 nokeep`	Удаляет зеркало и данные на диске 2
Создание тома RAID-5	`create volume raid size=500 disk=1,2,3`	Введенная на одной строке, эта команда создает отказоустойчивый том RAID-5, который в сумме занимает 1 Гб на дисках 1, 2 и 3
Преобразование базового диска в динамический	`select disk 2` `convert dynamic`	Преобразует диск 2 из базового в динамический
Преобразование диска с нераспределенным пространством из динамического в базовый	`select disk 2` `convert basic`	Преобразует диск 2 из динамического в базовый

Лабораторная работа. **Настройка дисков и томов**

На этой лабораторной работе вы будете использовать оснастку *Управление дисками* (Disk Management) и программу Diskpart для различных задач управления на диске 0. Диск 0 должен быть базовым и содержать не менее 1 Гб нераспределенного пространства.

Упражнение 1. Настройка раздела с помощью оснастки *Управление дисками*

1. Войдите на Server01 как *Администратор* (Administrator) и откройте оснастку *Управление дисками* (Disk Management) в консоли *Управление компьютером* (Computer Management). На верхней панели появится список томов, а на нижней — их графическое представление.
2. В графическом представлении щелкните нераспределенное пространство на диске 0 правой кнопкой и выберите **Создать раздел (New Partition).** Откроется окно *Мастера создания разделов* (New Partition Wizard).
3. Создайте основной раздел размером 250 Мб. Не меняйте букву диска, назначенную по умолчанию. Присвойте тому метку DataVolume и выполните быстрое форматирование под NTFS.

   Спустя некоторое время появится новый диск DataVolume (*буква_диска*:), где *буква_диска* — это буква, которую назначил разделу мастер. По завершении форматирования состояние раздела будет **Исправен (Healthy).**

Упражнение 2. Преобразование базового диска в динамический из оснастки *Управление дисками*

1. В оснастке *Управление дисками* щелкните панель состояния диска 0 правой кнопкой и выберите **Преобразовать в динамический диск (Convert To Dynamic Disk).** Откроется окно **Преобразование в динамические диски (Convert To Dynamic Disk)** с отмеченным флажком напротив диска 0.
2. Следуйте инструкциям, чтобы преобразовать диск 0 в динамический. Поскольку он является системным, потребуется перезагрузить компьютер.

Упражнение 3. Использование программы DiskPart

1. Из командной строки исполните diskpa rt. Появится приглашение на ввод команд — DISKPART >.
2. Введите ? и нажмите Enter. Появится список команд программы Diskpart.
3. Введите `list disk` и нажмите Enter. Появится список дисков, установленных на ServerOl.
4. Введите `create volume simple size = 250 disk = 0` и нажмите Enter.
5. Введите `list volume` и нажмите Enter.

   Создан новый том. Перед именем тома стоит звездочка. Она указывает, что том выбран. Заметьте: данному тому не назначена буква диска.
6. Введите `assign letter z` и нажмите Enter.
7. Введите `list volume` и нажмите Enter. Выбранному тому назначена буква Z.
8. Введите `extend size=250 disk=0` и нажмите Enter.
9. Введите `list volume` и нажмите Enter. Выбранный том (**Z**) теперь занимает 500 Мб.
10. Введите `exit` и нажмите Enter. Снова откроется окно командной строки.

11. Введите format z:/fs:NTFS /v:Extended_Volume /q и нажмите Enter. Появится предупреждение, что все данные на диске **Z** будут потеряны.
12. Нажмите клавишу Y, а затем Enter. Будет выполнено быстрое форматирование диска Z под NTFS.
13. Введите `exit`, чтобы закрыть окно командной строки.

Упражнение 4. Расширение томов с помощью оснастки *Управление дисками*

1. Откройте оснастку *Управление дисками*.
2. Щелкните том **Extended_Volume** правой кнопкой и выберите **Удалить том (Delete Volume).**
3. Подтвердите удаление тома, щелкнув **Да (Yes).**
4. Щелкните Data_Volume правой кнопкой и выберите **Расширить том (Extend Volume).** Откроется *Мастер расширения тома* **(Extend \blume Wizard).**
5. Щелкните **Далее (Next).**
6. Увеличьте размер тома на 500 Мб.
7. Щелкните **Далее (Next).**
8. Прочитайте сводную **информацию.** Щелкните **Готово (Finish).**

Упражнение 5. Буквы диска и смонтированные тома

1. Щелкните **Data_Volume** правой кнопкой и выберите **Изменить букву диска или путь к диску (Change Drive Letter and Paths).**
2. Измените букву диска на X.
3. Щелкните **Data_Volume (X:)** правой кнопкой и выберите **Открыть (Open).** Откроется окно *Проводника*.
4. Создайте папку с именем Docs.
5. Закройте *Проводник*.
6. Щелкните нераспределенное пространство на диске 0 правой кнопкой и выберите **Создать том (New Volume).**
7. Создайте простой том, занимающий все оставшееся пространство диска. Вместо назначения буквы диска смонтируйте том к папке X:\Docs. Отформатируйте том под NTFS и введите для него метку More_Space.
8. Откройте *Проводник* и убедитесь, что в меню **Вид (View)** отмечен пункт **Строка состояния (Status Bar).** Исследуйте том X:. Сколько на нем свободного места? Сколько свободного места отображается, когда вы открываете папку Docs?

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Этот вопрос является продолжением ситуации, описанной в вопросе 1 занятия 1. Вы установили новый диск объемом 200 Гб, сделали диск базовым и создали три основных раздела по 30 Гб для ОС, домашних каталогов пользователей и общих данных. Вы настроили дополнительный раздел и два логических диска по 30 Гб каждый для установленных приложений и точки распространения ПО. На диске осталось 50 Гб

нераспределенного пространства. Несколько месяцев спустя вы заметили, что места на трех томах практически не осталось. Вы хотите подготовится к вероятному расширению одного или нескольких разделов. Что нужно сделать?

2. Какой тип области диска поддерживает логические диски?
   a. Основные разделы.
   b. Простые тома.
   c. Составные тома.
   d. Дополнительные разделы.
   e. Нераспределенное пространство.
3. Вы недавно добавили диск на компьютер. До этого диск использовался под управлением Windows 2000 Server. Диск появился в консоли *Диспетчер устройств* (Device Manager), но неправильно отображается в оснастке *Управление дисками* (Disk Management). Что нужно сделать?
   a. Импорт чужих дисков.
   b. Форматирование тома.
   c. Повторное сканирование дисков.
   d. Изменение буквы диска или пути.
   e. Преобразование в динамические диски.
4. Вы пытаетесь преобразовать внешний диск FireWire из базового в динамический, но команда преобразования недоступна. Какова наиболее вероятная причина?

Резюме

- Для управления дисками служит оснастка *Управление дисками* (Disk Management) и команда Diskpart.
- Типичные задачи управления дисками подразумевают создание и удаление разделов и томов и назначение букв дисков и точек монтирования.
- Windows Server 2003 позволяет назначить для тома букву или не назначать ее вовсе и, как вариант, смонтировать том к одной или нескольким пустым папкам на томе NTFS.
- Базовые диски можно преобразовать в динамические, но для обратного преобразования необходимо удалить все данные и тома.

Занятие 3. Обслуживание томов дисковой памяти

Тома Windows Server 2003 эффективны и стабильны, если отформатированы под NTFS, чего нельзя сказать про FAT или FAT32. Файловая система NTFS регистрирует все транзакции, связанные с файлами, автоматически заменяет испорченные кластеры и хранит копию ключевой информации для всех файлов на томе NTFS. С помощью этих механизмов NTFS защищает целостность структуры тома и метаданные файловой системы (данные, которые относятся к самой файловой системе). Тем не менее, пользовательские данные могут быть случайно испорчены и, конечно, становятся фрагментируемыми. Кроме того, пользователи имеют вредную привычку хранить *огромное* количество устаревших и не относящихся к делу данных на томах, к которым у них есть доступ. На

этом занятии вы узнаете, как поддерживать целостность томов диска и оптимизировать их, выполняя дефрагментацию и ограничивая хранение с помощью дисковых квот.

Изучив материал этого занятия, вы сможете:

- ✓ обеспечивать целостность диска с помощью программы CHKDSK;
- ✓ наблюдать и улучшать производительность диска с помощью программы *Дефрагментация диска;*
- ✓ настраивать и отслеживать используемое пользователем пространство с помощью дисковых квот.

Продолжительность занятия — около 20 минут.

Программа CHKDSK

Программа CHKDSK (или Check Disk) позволяет проверить том на наличие ошибок файловой системы, протестировать и попробовать восстановить испорченные сектора на жестком диске.

Чтобы запустить программу *Проверка диска* (Check Disk), в *Проводнике* откройте окно свойств тома, который нужно проверить. На вкладке **Сервис (Tools)** щелкните кнопку **Выполнить проверку (Check Now). В** окне **Проверка диска (Check Disk)** выберите задачи, которые собираетесь запустить (рис. 11-4).

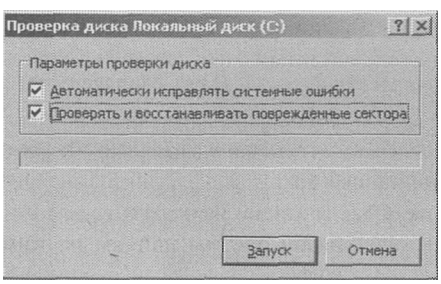


Рис. 11-4. Диалоговое окно *Проверка диска*

Если установить флажок **Автоматически исправлять системные ошибки (Automatically Fix File System Errors),** программа *Проверка диска* будет пытаться исправить противоречия в каталоге файловой системы, например, когда файлов, которые есть в каталоге, нет в папке на томе. *Проверка диска* три раза проходит по диску, изучая метаданные (данные, определяющие способ организации файлов на диске). При этом проверяется согласованность всех файлов в томе с основной таблицей файлов (MFT), правильность структуры каталогов и непротиворечивость дескрипторов безопасности.

Если установить флажок **Проверять и восстанавливать поврежденные сектора (Scan For And Attempt Recovery Of Bad Sectors),** программа *Проверка диска* сделает четвертый проход, чтобы проверить секторы тома, зарезервированные под пользовательские данные (метаданные файловой системы проверяются всегда). При обнаружении испорченного сектора данные из него восстанавливаются и перемещаются на рабочий сектор, если том является отказоустойчивым, иначе данные программой *Проверка диска* восстановить нельзя, и придется воспользоваться резервной копией. Испорченный сектор в дальнейшем не используется, и данные на него не записываются.

Перед запуском программы *Проверка диска* необходимо закрыть все открытые файлы. Если это сделать нельзя (например, программа запускается на системном томе), вам будет предложено отложить выполнение проверки до перезагрузки системы. Во время проверки диска другим процессам запрещено обращаться к тому. Программа интенсивно использует ресурсы процессора и диска. Продолжительность ее работы зависит от размера тома, выбранных параметров проверки и других процессов, запущенных на компьютере.

Программу *Проверка диска* можно запустить из командной строки командой CHKDSK. Без параметров эта команда выполняется в режиме только чтения на текущем диске. После проверки отображается отчет об использовании пространства на диске. Команда CHKDSK поддерживает несколько параметров, позволяющих исправить ошибки файловой системы (/f) и испорченные сектора (/r), так же, как и в версии для *Проводника*.

Программа *Дефрагментация диска*

Единица хранения файлов в томе называется *кластером*. Размер кластера настраивается при форматировании диска; на большинстве томов NTFS используется стандартный размер, равный 4 Кб. Каждый кластер может содержать не более одного файла, даже если тот меньше 4 Кб. Если файл больше, он хранится в нескольких кластерах, в каждом из которых есть указатель на следующий сегмент файла. На новом диске все кластеры свободны, поэтому файлы записываются на диск в смежные кластеры. Однако по мере изменения размера или удаления файлов свободные кластеры перестают образовывать непрерывное пространство, поэтому файлы сохраняются на кластеры, расположенные далеко друг от друга. Фрагментация файлов влияет на скорость операций чтения и записи и со временем может значительно снизить производительность сервера.

В состав Windows Server 2003 входит набор средств (графических и командной строки), с помощью которых можно анализировать и дефрагментировать тома. Эти инструменты значительно усовершенствованы по сравнению с Windows 2000 и позволяют дефрагментировать тома с размером кластера больше 4 Кб, а также MFT. Их можно использовать для дефрагментации любого тома на локальном диске. Для дефрагментации по расписанию или работы с удаленными томами пользуйтесь средствами сторонних разработчиков, например Diskeeper от Executive Software.

Чтобы запустить встроенную программу *Дефрагментация диска* (Disk Defragmenter) (рис. 11-5), откройте окно свойств тома и на вкладке **Сервис (Tools)** щелкните **Выполнить дефрагментацию (Defragment Now).** Оснастку *Дефрагментация диска* можно также открыть из консоли *Управление компьютером* (Computer Management) или из собственной консоли MMC. Выберите том и щелкните кнопку **Анализ (Analyze).** Программа даст рекомендацию. Если она указывает, что том «грязный», значит на диске могут быть искажения, и перед дефрагментацией следует запустить программу CHKDSK.

Если рекомендована дефрагментация, щелкните кнопку **Дефрагментация (Defragment).** Можно дефрагментировать том любого типа: FAT или NTFS, базовый или динамический. На томе допустимы открытые файлы, но они плохо дефрагментируются и снижают скорость процесса, поэтому сначала закройте все файлы. *Программа Дефрагментация диска* перемещает файлы на диске и пытается расположить их на соседних кластерах. Кроме того, свободное пространство также станет непрерывным, что уменьшит вероятность фрагментации новых файлов.

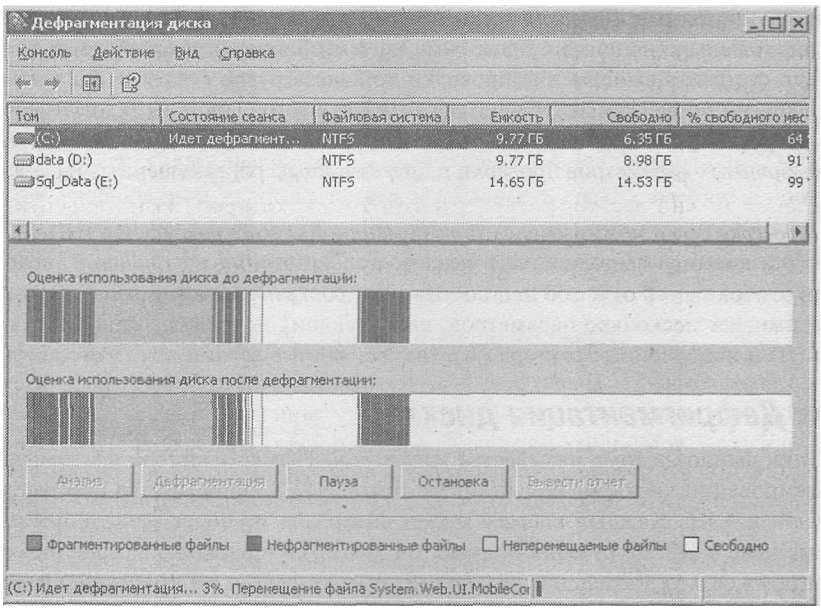


Рис. 11-5. Программа *Дефрагментация диска*

Примечание Для полной дефрагментации тома требуется, чтобы на нем было не менее 15 % свободного места. Оно используется для временного размещения файлов в ходе дефрагментации. Если том содержит очень много фрагментированных больших файлов, требования к доле свободного места будут выше. Том, содержащий менее 15 % свободного места, дефрагментируется только частично.

Дисковые квоты

Встроенная функция управления квотами появилась в Windows 2000. Она позволяла администраторам реализовать ограничения хранения, не используя программы сторонних разработчиков. Windows Server 2003 поддерживает те же функции. При включении квотирования диспетчер квот сравнивает общий размер пространства, занятого файлами пользователя, с заданными ограничениями и сообщает о скором исчерпании квоты или запрещает запись на диск.

Диспетчер квот сообщает пользователю о наличии свободного пространства на томе на основе его квоты. Другими словами, если пользователю предоставлено 50 Мб на RAID-томе размером 500 Гб, он увидит только 50 Мб свободного пространства при первом обращении к тому. Незадолго до исчерпания квоты пользователь получает сообщение, похожее на то, что появляется при заполнении тома: система предупреждает, что осталось мало места и предлагает удалить ненужные файлы.

Подготовка к экзамену Квоты поддерживаются только на томах NTFS.

Настройка квот

Настройка квот подразумевает включение квотирования на томе, настройку стандартных параметров квот, а также настройку записей квот, которые являются исключениями из стандартных значений.

По умолчанию в Windows Server 2003 квоты отключены, и их нужно включать для каждого тома: откройте свойства тома и перейдите на вкладку **Квота (Quota).** Свойства квот для тома показаны на рис. 11-6.

Совет Чтобы открыть окно свойств тома, в документации обычно предлагают щелкнуть диск в *Проводнике* правой кнопкой и выбрать **Свойства (Properties).** К сожалению, таким способом можно настроить только квоты томов, которым назначены буквы: *Проводник* не отображает вкладку **Квота (Quota)** для тома, смонтированного к папке. Поэтому рекомендуется настраивать квоты в оснастке *Управление дисками* (Disk Management). Она позволяет открыть свойства любого тома и перейти на вкладку **Квота (Quota).**

Установите флажок **Включить управление квотами (Enable Quota Management).** Если вы хотите запретить пользователям, превысившим ограничения хранения, возможность записывать файлы на том,' установите флажок **Не выделять место на диске при превышении квоты (Deny Disk Space To Users Exceeding Quota Limit).** Иначе пользователи смогут продолжить записывать данные на том.

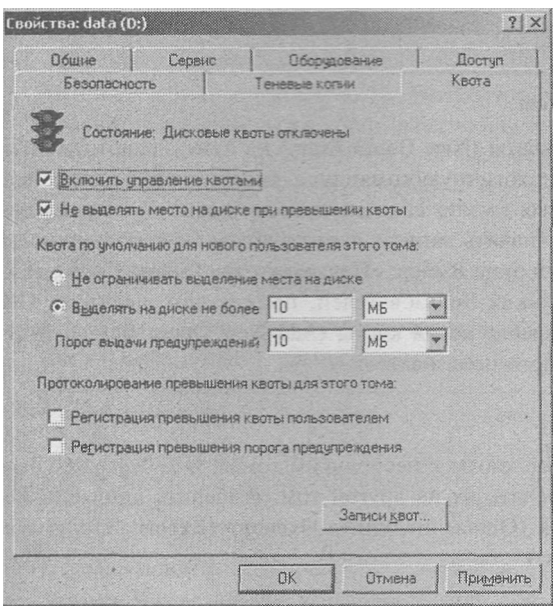


Рис. 11-6. Вкладка *Квота* диалогового окна свойств тома

Управлять квотами можно двумя способами: 1) задать ограничения (или полностью отключить контроль лимита) для отдельных пользователей; 2) задать общие параметры квот, которые будут применяться ко всем пользователям, для которых не заданы индивидуальные квоты. На вкладка **Квота (Quota)** вы можете настроить параметры квоты по умолчанию для максимального количества пользователей. Это поможет сократить количество записей квот, которые потребуется создать для пользователей, чьи ограничения отличаются от стандартных. Заметьте: настраивается не только ограничение дискового пространства, но и уровень предупреждения, который, естественно, не должен превышать лимит.

Наконец, укажите параметры протоколирования. Диспетчер квот записывает события в системный журнал и указывает имя пользователя и какой из порогов (квоты или предупреждения) был превышен.

Настроив стандартные квоты для тома на вкладке **Квота (Quota),** щелкните кнопку **Записи квот (Quota Entries),** чтобы открыть окно, показанное на рис. 11-7.

Подготовка к экзамену Членам группы *Администраторы* (Administrators) назначается запись квоты без лимита. Это позволяет им устанавливать ОС, службы, приложения и записывать данные, не превышая квоту.

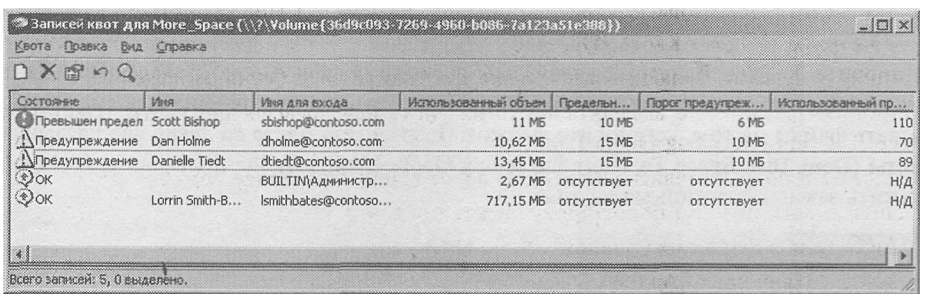


Рис. 11-7. Диалоговое окно *Записи квот*

Щелкните кнопку **Создать запись квоты (New Quota Entry)** на панели инструментов или в меню **Квота (Quota)** выберите аналогичную команду, а затем укажите одного или нескольких пользователей для которых нужно создать запись квоты. К сожалению, Windows Server 2003 не позволяет назначать записи квот группам (как большинство средств сторонних разработчиков), но в окне **Выбор: «Пользователи» (Select Users)** можно, по крайней мере, выбрать нескольких пользователей, прежде чем щелкнуть OK. Ограничения, заданные в окне **Добавление новой квоты (Add New Quota Entry),** будут распространяться на каждого выбранного пользователя.

Экспорт записей квот

Если вам нужно применить одинаковые квоты к нескольким томам NTFS, можно экспортировать записи квот и импортировать их на другой том. Выберите одну или несколько записей квот и в меню **Квота (Quota)** щелкните **Экспорт (Export).** На другом томе выберите команду **Импорт (Import).**

Наблюдение за квотами и занятым пространством

Диалоговое окно **Записи квот (Quota Entries)** показывает пространство, занятое данными каждого пользователя, а также сообщает о достижении порогов предупреждения или превышении квот. Данные можно сортировать по столбцам, чтобы выявлять пользователей, превысивших свои лимиты. В Windows Server 2003 отсутствует механизм уведомления администратора о достижении порогов квот, поэтому нужно следить за данными в окне **Записи квот (Quota Entries)** или системным журналом в консоли *Просмотр событий* (Event Viewer).

Подготовка к экзамену Квотирование диска может быть реализовано только на уровне тома или пользователя. Нельзя назначить квоты группам или отдельным папкам.

Лабораторная работа. **Реализация дисковых квот**

На этой лабораторной работе вы настроите параметры управления квотами по умолчанию, чтобы ограничить размер данных, которые пользователи могут хранить на Server01. Затем вы настроите индивидуальные записи квот для пользователей из отдела маркетинга, поскольку их мультимедийные данные обычно больше по объему, чем документы других пользователей. Кроме того, вы освободите от квот разработчиков.

Упражнение 1. Настройка параметров дисковых квот по умолчанию

1. Откройте оснастку *Управление дисками* (Disk Management).
2. Щелкните том **More_Space** правой кнопкой и выберите **Свойства (Properties).**
3. Перейдите на вкладку **Квота (Quota).**
4. Установите флажок **Включить управление квотами (Enable Quota Management).**
5. Установите флажок **Не выделять** место на **диске при превышении квоты (Deny Disk Space To Users Exceeding Quota limit).**
6. Перейдите в поле **Выделять на диске не более (Limit Disk Space To).**
7. Введите лимит 10 Мб и порог предупреждения 6 Мб.
8. Установите оба флажка журналов.
9. Щелкните **Применить (Apply).**

   Откроется окно **Дисковая квота (Disk Quota)** с предупреждением, что том будет повторно просканирован для обновления статистики об использовании диска, если вы включите квоты. Щелкните **OK** для подтверждения.
10. Не закрывайте окно свойств тома — оно вам понадобится на следующем упражнении.

Упражнение 2. Создание индивидуальных записей квот

1. На вкладке **Квота (Quota)** окна свойств тома MoreSpace щелкните кнопку **Записи квот (Quota Entries),** чтобы открыть окно с квотами.

   На заметку Заметьте: в списке отображается группа Builtin\Administrators. Если вы создавали файлы под учетной записью обычного пользователя, то увидите запись квоты для этого пользователя, поскольку он владеет файлами на данном томе.

   Далее вы настроите записи квот для пользователей Dan Holme и Danielle Tiedt из отдела маркетинга и предоставите им больше места, чем разрешено по умолчанию.
2. В меню **Квота (Quota)** выберите **Создать запись квоты (New Quota Entry)-**
3. Щелкните кнопку **Дополнительно (Advanced),** а затем **Поиск (Find Now).** Откроется список пользователей домена.
4. Выберите учетные записи Dan Holme и Danielle Tiedt и два раза щелкните OK.
5. Задайте лимит 15 Мб и порог предупреждения 10 Мб. Щелкните OK.

   Далее вы создадите новые записи квот для разработчиков Lorrin Smith-Bates и Scott Bishop, которые будут освобождены от квот.
6. Повторите шаги 2—5, чтобы настроить записи квот для Lorrin Smith-Bates и Scott Bishop. Настройте запись квоты, чтобы она не ограничивала использование диска.

Упражнение 3 (необязательное). Проверка дисковых квот

1. Войдите в систему как Danielle Tiedt.
2. Создайте папку Dtiedt в каталоге X:\Docs.
3. Скопируйте папку Support с компакт-диска Windows Server 2003 в папку X:\Docs\Dtiedt. Папка Support занимает 11 Мб и меньше, чем квота Danielle Tiedt. Копирование выполнится успешно.
4. Войдите в систему как Dan Holme.
5. Создайте папку Dholme в каталоге X:\Docs.
6. Скопируйте папку Support с компакт-диска Windows Server 2003 в папку X:\Docs\Dholme. Размер папки меньше квоты Dan Holme, поэтому копирование выполнится успешно.
7. Скопируйте папку Wueadd с компакт-диска Windows Server 2003 в папку X:\Docs\Dholme. Папка занимает 6 Мб, а потому квота Dan Holme будет превышена. Копирование будет прервано.
8. Войдите в систему как *Администратор* (Administrator) и откройте окно **Записи квот (Quota Entries)** для тома MoreSpace. Оцените объем диска, занятый каждым пользователем.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Вы — администратор компьютера под управлением Windows Server 2003, и намерены исправить любые ошибки файловой системы и восстановить испорченные сектора на жестком диске. Каким средством воспользоваться?
   a. *Проверка диска* (Check Disk).
   b. *Дефрагментация диска* (Disk Defragmenter).
   c. DISKPART.
   d. Дисковые квоты.
2. Вы — администратор компьютера под управлением Windows Server 2003. Жесткий диск компьютера содержит два тома данных: D: и E:. ВЫ включаете дисковые квоты на обоих томах с лимитом 20 Мб для всех пользователей. Кроме того, вы хотите задать лимит 10 Мб для домашних папок пользователей, которые хранятся в каталоге D:\Users. Возможно ли это? Почему? Где можно реализовать квоты?
   a. На любом сервере для всех дисков.
   b. На любом физическом диске на всех томах.
   c. На любом томе для всех папок.
   d. На любой папке.
3. Сколько свободного места на томе нужно для выполнения полной дефрагментации?
   a. 5%.
   b. 10%.
   c. 15%.
   d. 25%.
   e. 50%.

Резюме

- Программа *Проверка диска* (Check Disk) позволяет исправить ошибки файловой системы, а также найти и попытаться восстановить испорченные секторы на жестком диске.
- Программа *Дефрагментация диска* (Disk Defragmenter) повышает производительность, перераспределяя файлы так, чтобы их кластеры были расположены непрерывно.
- Дисковые квоты позволяют устанавливать и следить за ограничениями хранения и, если необходимо, запрещать запись пользователям, превысившим эти ограничения. Квоты можно настраивать на уровне пользователя или тома.

Занятие 4. **Реализация RAID**

Дисковая подсистема, включающая конфигурацию RAID, позволяет дискам работать совместно, чтобы повысить производительность или отказоустойчивость. На этом занятии вы познакомитесь с тремя уровнями RAID, которые поддерживает Windows Server 2003. Вы узнаете, как влияет каждый тип тома на производительность, емкость и отказоустойчивость, а также научитесь восстанавливать данные, когда один из дисков в конфигурации RAID выходит из строя.

Изучив материал этого занятия, вы сможете:

- ✓ определить оптимальную конфигурацию RAID на основе требований к емкости, отказоустойчивости и производительности;
- ✓ настроить чередующийся (RAID-0), зеркальный (RAID-1) и чередующийся том с контролем четности (RAID-5);
- ✓ восстановить данные в случае сбоя одного из дисков отказоустойчивого тома.

Продолжительность занятия — около 25 минут.

На занятии 1 вы познакомились с типами томов, которые поддерживает Windows Server 2003. Конфигурации RAID соответствуют чередующиеся, зеркальные и тома RAID-5.

Реализация отказоустойчивости диска

Как было отмечено на занятии 1, отказоустойчивость — это способность компьютера или ОС обойтись без потерь данных и не нарушить процесс работы при таких катастрофических событиях, как отключение питания или аппаратный сбой. В полностью отказоустойчивых системах применяются отказоустойчивые массивы дисков, предотвращающие потерю данных. Отказоустойчивый RAID можно реализовать аппаратно или программно.

Аппаратные RAID

В аппаратной решении созданием и восстановлением избыточной информации управляет интерфейс контроллера диска. Некоторые производители реализуют защиту данных непосредственно в аппаратном обеспечении, например на платах контроллера дискового массива. Поскольку эти методы зависят от производителя и обходятся без отка-

зоустойчивых программных драйверов ОС, они обеспечивают лучшую производительность по сравнению с программной реализацией RAID.

Выбирая между аппаратной и программной реализацией RAID, учтите следующее:

- аппаратная реализация отказоустойчивости дороже программной и может ограничить выбор оборудования одним производителем;
- аппаратная реализация отказоустойчивости, как правило, обеспечивает более высокую скорость дискового ввода-вывода, чем программная;
- аппаратные отказоустойчивые решения могут поддерживать «горячую» замену жестких дисков (неисправный диск можно заменить, не выключая компьютер) и «горячее» резервирование (автоматически подключается запасной диск).

Программные RAID

Windows Server 2003 поддерживает одну незащищенную реализацию RAID (чередующийся том) и две отказоустойчивых — зеркальный том (RAID-1) и чередующийся том с контролем четности (RAID-5). Отказоустойчивые тома RAID можно создать только на динамических дисках, отформатированных под NTFS.

В реализациях **RAID** для Windows Server 2003 сбой нельзя преодолеть, пока вышедший из строя диск не будет восстановлен. Если второй сбой произойдет до того, как будут восстановлены данные, потерянные из-за первого отказа, придется воспользоваться резервной копией.

Чередующиеся тома

Чередующийся том, или RAID-0, состоит из двух и более дисков, на которые записывает данные равномерно. В результате запросы ввода-вывода обрабатываются несколькими дисководами и производительность операций чтения и записи заметно повышается. Чередующиеся тома широко используются в конфигурациях, где важны производительность и большая емкость, например в конструкторских и цифровых мультимедийных приложениях.

Примечание Повышение производительности на IDE заметно только при использовании отдельных контроллеров. Отдельные контроллеры (в идеале по одному на каждый диск) повышают производительность, распределяя запросы ввода-вывода и между контроллерами, и между дисками.

Создание чередующегося тома

Для создания чередующегося тома требуется нераспределенное пространство минимум на двух динамических дисках. Щелкните одно из свободных пространств правой кнопкой и выберите **Создать том (Create Volume).** *Мастер создания томов* (New Volume Wizard) поможет вам выбрать чередующийся том и дополнительное пространство на другом диске. Чередующемуся тому можно назначить букву диска или папку. Он должен быть отформатирован под NTFS.

Чередующийся том может содержать до 32 дисков. Объем пространства на каждом диске тома равен размеру самого маленького пространства тома на любом его диске. Например, если диск 1 содержит 200 Гб нераспределенного пространства, а диск 2 — 120 Гб, чередующийся том может содержать не более 240 Гб, поскольку часть тома на диске 1 не может быть больше части тома на диске 2. Все пространство диска в томе

используется для хранения данных — для обеспечения отказоустойчивости место не резервируется.

Восстановление чередующегося тома

Поскольку данные хранятся на нескольких физических дисках, производительность повышается, но отказоустойчивость наоборот уменьшается — если один диск выйдет из строя, все данные тома теряются. Таким образом, важно создать резервную копию чередующегося тома. Если любой диск чередующегося тома выходит из строя, необходимо удалить том, восстановить диск и заново создать том. Затем нужно восстановить данные из резервной копии.

Подготовка к экзамену Чередующиеся тома обеспечивают максимальную емкость и производительность, но не поддерживают отказоустойчивость. Единственный способ защиты от сбоя — регулярная архивация.

Зеркальные тома

Зеркальный том обеспечивает хорошую производительность и отличную отказоустойчивость. Он состоит из двух дисков, на которые записываются данные. Как и в других конфигурациях RAID, для обеспечения максимальной производительности нужно использовать отдельные контроллеры (добавив контроллер, вы создадите конфигурацию, называемую «дуплексированием»). Зеркальные тома соответствуют аппаратной конфигурации RAID-1.

Создание зеркальных томов

Для создания зеркального тома требуется нераспределенное пространство на двух динамических дисках. Щелкните любое пространство правой кнопкой мыши и выберите команду **Создать том (Create Volume).** *Мастер создания томов* (New Volume Wizard) упрощает процесс выбора зеркального тома и пространства на другом диске. Зеркальному тому можно назначить букву диска или папку. Обе копии зеркала используют одинаковые обозначения.

Существует возможность создать зеркало существующего простого тома, для этого нужно щелкнуть том правой кнопкой мыши, выбрать команду **Добавить зеркальный том (Add Mirror)** и указать диск с достаточным объемом нераспределенного пространства.

После создания зеркала система начнет копировать данные сектор за сектором. Во время этого процесса том находится в состоянии **Ресинхронизация** (Resynching).

Восстановление зеркального тома

Процесс восстановления неисправного диска зеркального тома зависит от типа сбоя. Состояние **Отказавшая избыточность (Failed Redundancy)** обоих разделов зеркального тома свидетельствует о кратковременных ошибках ввода-вывода. Для диска с ошибками будет отображаться состояние **Автономный (Offline)** или **Отсутствует (Missing)** (рис. 11-8).

Устранив источник ошибок ввода-вывода, например плохое соединение кабеля или источника питания, щелкните том на проблемном диске (или сам диск) правой кнопкой и выберите **Реактивизировать том (Reactivate Volume)** или **Реактивизировать диск (Reactivate Disk)** соответственно. Повторная активизация переводит диск или том в оперативный режим. Повторная синхронизация зеркального тома выполняется автоматически.

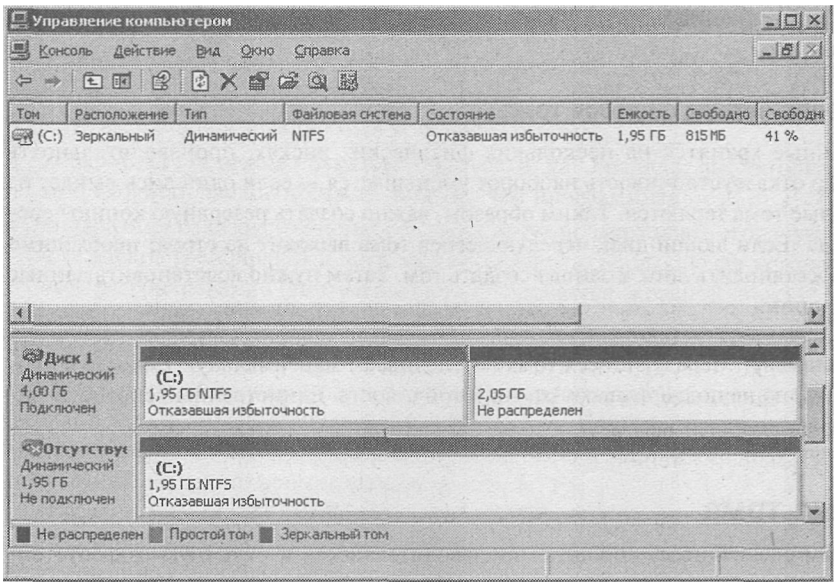


Рис. 11-8. Зеркальный том с неисправным диском

Существует три способа остановить зеркальное отображение, каждый из которых приводит к различным результатам:

- **Удаление тома.** Удаляется том и вся информация на нем. Образовавшееся нераспределенное пространство становится доступным для новых томов.
- **Удаление зеркала.** Зеркало «разбивается» и пространство на одном из дисков становится нераспределенным. На другом диске остается копия данных, но том, естественно, перестает быть отказоустойчивым.
- **Разбиение зеркала.** Зеркало разбивается и на обоих дисках остается копия данных. Диску, который был выбран при выполнении команды **Разделение зеркального тома (Break Mirrored Volume),** назначается старая буква зеркального тома, на нем остаются общие папки, файл подкачки и *точки повторной обработки* (reparse points). Второму диску присваивается следующая доступная буква.

Теперь предположите, как бы вы заменили вышедший из строя диск зеркального тома? После физической замены диска нужно открыть оснастку *Управление дисками* (Disk Management), чтобы повторно просканировать, инициализировать диск и преобразовать его в динамический. После этого вы обнаружите, что нельзя повторно создать зеркало для этого тома, несмотря на то, что вторая копия еще существует. Поскольку оставшийся диск находится в рабочем состоянии, зеркальный том еще существует, неисправна только его избыточная составляющая. Необходимо удалить или разбить зеркало. Щелкните зеркало правой кнопкой и выберите **Удалить зеркало (Remove Mirror).** В одноименном окне важно выбрать половину тома, которая отсутствует; она будет удалена, когда вы щелкните кнопку **Удалить зеркало.** Вторая часть превратится в простой том. После завершения операции щелкните работоспособный простой том правой кнопкой и выберите **Добавить зеркальный том (Add Mirror).** Выберите новый том для повторного создания зеркала.

Подготовка к экзамену Зеркальные тома обеспечивают отказоустойчивость и более высокую производительность, чем тома RAID-5. Тем не менее, поскольку каждый диск зеркального тома содержит полную копию данных, это менее эффективный тип тома с точки зрения использования дискового пространства.

Тома RAID-5

Том RAID-5 состоит как минимум из трех дисков, обеспечивает отказоустойчивость и отличную производительность операций чтения. Стоимость отказоустойчивости снижается в расчете на Мб объема. Данные записываются на все диски. Тем не менее, пространство, равное размеру одного из дисков тратится на хранения информации, называемой четностью, которая играет роль контрольной суммы и обеспечивает отказоустойчивость тома. Поскольку четность вычисляется во время записи, тома RAID-5 интенсивнее используют ресурсы процессора. Однако RAID-5 обеспечивает более высокую производительность чтения, поскольку данные одновременно считываются с нескольких дисков.

Когда файл записывается в том, четность распределяется по всем дискам набора. Однако общий объем пространства, используемого для обеспечения отказоустойчивости, равен размеру одного диска томр.

Таким образом, тома RAID-5 являются более экономными, чем зеркальные. В минимальном томе RAID-5 из трех дисков, только одна треть используется для хранения четности (в отличие от зеркального тома, где для обеспечения отказоустойчивости используется половина пространства). Поскольку том RAID-5 может содержать до 32 дисков, теоретически можно настроить том, использующий только 1/32 пространства для обеспечения отказоустойчивости.

Настройка томов RAID-5

Для создания тома RAID-5 требуется как минимум три динамических диска. Щелкните нераспределенное пространство на одном из дисков правой кнопкой и выберите **Новый том (New Volume).** *Мастер создания томов* (New Volume Wizard) упрощает процесс выбора тома RAID-5 и дисков, из которых он будет состоять.

Емкость тома ограничена наименьшим участком нераспределенного пространства на любом из его дисков. Если диск 2 содержит 50 Гб нераспределенного пространства, а диски 3 и 4 по 100 Гб, том сможет использовать только по 50 ГБ на дисках 3 и 4 — размер пространства на каждом диске должен быть одинаковым. В поле **Размер тома (Volume Size)** *Мастер создания томов* отображает емкость тома за вычетом пространства, которое используется для хранения четности. В рассматриваемом примере размер тома RAID-5 будет составлять 100 Гб — общий размер минус размер пространства на одном из дисков, которое предназначено для хранения четности.

Томам RAID-5 можно назначать букву диска или папку. Они могут быть отформатированы только под NTFS.

Поскольку тома RAID-5 создаются непосредственно из нераспределенного пространства динамических дисков, другие тома нельзя преобразовать к данному типу, не прибегая к архивации и восстановлению данных.

Восстановление неисправного тома RAID-5

Если один диск тома RAID-5 выйдет из строя, вы все равно сможете обратиться к данным. Во время операции чтения отсутствующие данные «на лету» вычисляются из ос-

тавшихся данных и информации о четности. Производительность снизится и, если выйдет из строя второй диск, данные можно будет восстановить только из архива. Зеркальные и RAID-5-тома защищают только от сбоя на одном диске.

После восстановления диска может потребоваться повторное сканирование, затем нужно щелкнуть том правой кнопкой и выбрать **Реактивизировать том (Reactivate Volume).** Система перестроит отсутствующие данные, и том будет полностью восстановлен.

Если команда **Реактивизировать том** недоступна или вы заменили диск, может потребоваться повторное сканирование, инициализация и приведение к динамическому типу, затем нужно щелкнуть том правой кнопкой и выбрать **Восстановить том (Repair Volume).** Затем ОС предложит указать диск, где нужно восстановить отсутствующую часть тома. Выберите новый диск и система восстановит отсутствующие данные.

Сравнение зеркальных и RAID-5-томов

Зеркальные тома (RAID-1) и тома RAID-5 обеспечивают различный уровень отказоустойчивости. Выбор зависит от требуемого уровня защиты и стоимости аппаратного обеспечения. Тома RAID-1 и RAID-5 отличаются главным образом производительностью и стоимостью. В табл. 11-2 перечислены некоторые отличия программной реализации RAID-1 и RAID-5.

Табл. 11-2. Производительность и стоимость RAID

Зеркальные (RAID-1) тома	Чередующиеся с четностью (RAID-5) тома
Могут защитить системный и загрузочный разделы	Не могут защитить системный и загрузочный разделы
Требуют два жестких диска	Требуют от 3 до 32 жестких дисков
Более высокая стоимость в расчете на Мб	Более низкая стоимость в расчете на Мб
Избыточность 50 %*	Максимальная избыточность 33 %*
Отличная производительность чтения и записи	Отличная производительность чтения и умеренная записи
Использует меньше системной памяти	Требует больше системной памяти

* Дисковое пространство, выделяемое на обеспечение отказоустойчивости.

Обеспечение отказоустойчивости системного тома

Поскольку RAID-5 является «родным» типом динамического тома, нельзя установить или запустить ОС Windows Server 2003 с тома RAID-5, созданного отказоустойчивыми технологиями Windows Server 2003.

Совет Аппаратная реализация RAID, тем не менее, является прозрачной для Windows Server 2003, поэтому ОС может (и должна там, где это возможно) быть установлена на аппаратные RAID-массивы.

Таким образом, единственным способом защиты системного тома без использования аппаратных средств является зеркальный том. Зеркальная копия системного тома создается с помощью уже рассмотренной процедуры: щелкните системный том правой кнопкой и выберите **Добавить зеркальный том (Add Mirror). В** отличие от Windows 2000 перезагрузка не требуется и файл BOOT.INI обновляется автоматически, поэтому вы сможете запустится со второго диска, если первый выйдет из строя.

Если диски подключены к контроллерам IDE, вам может потребоваться извлечь неисправный диск, переключить второй диск на основной контроллер и соответствующим образом установить перемычки или положение кабеля, чтобы сделать его главным. В противном случае система может не запуститься со второго диска.

Совет Если вы собираетесь создать зеркало системного тома, приобретите один или два контроллера **SCSI.** При использовании двух контроллеров, убедитесь, что они одинакового типа. Эта конфигурация значительно упрощает поддержку и восстановление.

Модернизация дисков

При модернизации или переносе дисков с предыдущими версиями Windows на Windows Server 2003 учтите два момента.

Во-первых, если диск был настроен на компьютере Windows 2000 как базовый, а затем преобразован в динамический, вы не сможете расширить его простые тома на другие диски, используя Windows Server 2003. Другими словами, если перенести такой диск на компьютер Windows Server 2003 или обновить до нее ОС, вы не сможете создать составной том из простых.

Во-вторых, Windows Server 2003 больше не поддерживает многодисковые массивы, созданные в Windows NT 4. Зеркальные, чередующиеся и чередующиеся с четностью наборы в Windows NT 4 создавались на основе базовых дисков. В Windows 2000 использование таких наборов было разрешено, хотя важно было быстро преобразовать их в динамические, чтобы упростить устранение неполадок и восстановление. Windows Server 2003 не распознает такие тома. При обновлении сервера с Windows NT4 до Windows Server 2003 любые наборы RAID будут невидимы. Перед модернизацией и переносом таких дисков необходимо заархивировать все данные, и восстановить после воссоздания отказоустойчивых наборов в Windows Server 2003.

Лабораторная работа. **Планирование конфигурации RAID**

На этой лабораторной работе вы проверите, удовлетворяет ли сервер и емкость его дисковой памяти требованиям contoso.com и определите подходящую конфигурацию.

Вы администрируете сервер компании Contoso, Ltd. Он оснащен четырьмя дисками SCSI:

- диск 0 — 80 Гб;
- диск 1 — 80 Гб;
- диск 2 — 40 Гб;
- диск 3 — 40 Гб.

Недавно вы выполнили чистую установку Windows Server 2003, заархивировав все данные на дисках, удалив все разделы и установив ОС на раздел размером 20 Гб на диске 0.

Теперь вам требуется настроить остальное дисковое пространство. Данные пользователей не будут храниться на системном томе. Вы хотите максимально эффективно использовать пространство для хранения данных и обеспечить работу системы, даже если один из дисков выйдет из строя. Какую конфигурацию вы выберете, и какая совокупная емкость хранения будет доступна для информации пользователей?

Правильный ответ: комбинация зеркальных томов и томов RAID-5 с суммарной емкостью 140 Гб для данных пользователей.

Чтобы обеспечить работоспособность системы в случае сбоя одного из дисков, необходимо обеспечить отказоустойчивость самой ОС. Для этого подходит только зеркальный том; нельзя установить ОС на том RAID-5. Таким образом, не менее 20 Гб требуется для создания зеркальной копии ОС.

Конфигурация RAID-5 максимально эффективно использует дисковое пространство, не жертвуя отказоустойчивостью. Том RAID-5 может состоять из трех и более дисков. В рассматриваемом примере, создав том RAID-5 из всех четырех дисков, вы получите максимальную емкость хранения данных. Размер полосы тома RAID-5 не может быть больше минимального нераспределенного пространства на одном из его дисков, поэтому, хотя на дисках 0 и 1 осталось соответственно 60 и 80 Гб свободного места, емкость тома кратна размеру наименьших дисков (40 Гб). Четыре диска по 40 Гб в сумме дают 160 Гб, однако RAID-5 использует один из дисков для хранения данных четности, поэтому полезная емкость составит 120 Гб.

На диске 0 осталось 20 Гб нераспределенного пространства, а на диске 1 — 40 Гб. Вы можете создать зеркальную копию системного тома на диске 1, оставив свободными 20 Гб. Оставшееся пространство (по 20 Гб на дисках 0 и 1) можно использовать для создания зеркального тома с дынными пользователей общей емкостью 20 Гб. Простой, составной или чередующийся том не будут обеспечивать отказоустойчивость, а том RAID-5 требует не менее трех физических дисков, поэтому зеркальный том — наиболее эффективный способ использования оставшегося пространства для безопасного хранения данных.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Вы реализуете программный RAID на компьютере под управлением Windows Server 2003 и хотите обеспечить отказоустойчивость системного и загрузочного разделов. Какой тип RAID следует использовать?
   a. RAID-0.
   b. RAID-1.
   c. RAID-5.
   d. Программный RAID нельзя использовать для защиты загрузочного раздела.
2. Вы хотите защитить данные на жестком диске компьютера под управлением Windows Server 2003. Необходимо обеспечить максимальную скорость дискового ввода-вывода и «горячую» замену жестких дисков. Какой тип RAID следует использовать?
   a. RAID-0.
   b. RAID-1.
   c. RAID-5.
   d. Аппаратный RAID.
3. Вы настраиваете том RAID-5 на компьютере под управлением Windows Server 2003 и планируете установить пять дисков по 20 Гб каждый. Какой процент избыточности можно ожидать от такой конфигурации?

a. 20.
b. 25.
c. 33.
d. 50.

4. Вы настраиваете программный RAID на компьютере под управлением Windows Server 2003, чтобы обеспечить отказоустойчивость данных. Этот компьютер используется в качестве сервера БД. Данный сервер чаше выполняет чтение, и гораздо реже — запись. Вам необходимо создать отказоустойчивое решение с отличной скоростью чтения. Какой тип RAID следует использовать?
   a. RAID-0.
   b. RAID-1.
   c. RAID-5.
5. Компьютер, на котором нужно создать том RAID-5, содержит три диска по 2 Гб нераспределенного пространства на каждом. В оснастке *Управление дисками* (Disk Management) вы запускаете *Мастер создания томов* (New Volume Wizard), щелкнув правой кнопкой одну из областей нераспределенного пространства. Когда вы доходите до экрана **Выбор типа тома (Select Volume Type),** вариант RAID-5 недоступен. Какова наиболее вероятная причина?
   a. RAID-5 уже реализован на аппаратном уровне,
   o. Один или два диска являются базовыми.
   c. Все три диска являются динамическими.
   d. Все три диска являются базовыми.
   e. RAID-5 уже реализован программно.
6. Вышел из строя диск зеркального тома. Вы хотите заменить его. Как подготовить зеркальный том к замене диска?

Резюме

- Некоторые уровни RAID обеспечивают отказоустойчивость за счет избыточности данных. Отказоустойчивость RAID реализуется аппаратно или программно.
- Аппаратные решения более быстрые, но, как правило, и более дорогие.
- Windows Server 2003 поддерживает три программных реализации RAID: чередующиеся (RAID-0), зеркальные (RAID-1) и чередующиеся с четностью (RAID-5) тома.
- Чередующийся том (RAID-0) распределяет данные по всем дискам тома, ускоряя операции чтения и записи, но не обеспечивая отказоустойчивость.
- В томах RAID-5 отказоустойчивость достигается за счет хранения информации о четности на каждом разделе тома.
- Зеркальный том использует драйвер отказоустойчивости, чтобы одновременно записывать идентичные данные на каждый из двух физических дисков.
- Тома RAID-1 и RAID-5 отличаются, главным образом, производительностью и стоимостью. RAID-1 обеспечивает хорошую скорость чтения и записи. RAID-5 читает данные быстрее RAID-1, но не намного быстрее записывает.
- Единственный тип программного RAID, способный защитить системный том, — зеркальный том.

Пример из практики

Вы администрируете сервер компании Contoso, Ltd. На файловых серверах компании заканчивается свободное место и требуется модернизация дисков. Раньше компания использовала архивные ленты для обеспечения избыточности данных. Недавний рост не позволяет тратить больше нескольких минут на восстановление сервера после сбоя диска. Вам поручено изучить возможность реализации отказоустойчивого дискового хранилища.

Примечание На данном занятии требуется доступ к Интернету.

Упражнение 1. Выбор отказоустойчивых томов Windows Server 2003

Повторите материал занятия 4, чтобы выбрать наилучший способ настройки отказоустойчивых серверов с помощью динамических дисков Windows Server 2003. Прочитайте лабораторную работу занятия 4, чтобы вспомнить, как настраивать разные типы томов для отказоустойчивости.

Учтите трудности, связанные с дисками IDE. Если ОС установлена на зеркальном диске IDE, то при выходе из строя основного диска вам придется перенастроить перемычки или положение второго диска на кабеле и подключить его к основному каналу IDE. Помня об этом, вы решили, что надежнее использовать два контроллера SCSI, расположив копии зеркала на первых дисках каждой цепочки SCSI. Данная конфигурация обеспечивает быстрое восстановление не только при выходе из строя одного из дисков, но и при отказе одного из контроллеров SCSI.

Теперь рассмотрите вопросы производительности и емкости RAID в Windows Server 2003. Посчитайте, сколько времени займет восстановление из-за неисправности диска (выключение сервера, замена диска, перезагрузка сервера) и воссоздание отсутствующего тома.

Упражнение 2. Выбор аппаратного RAID

Помня об этих трудностях, вы решили оценить возможность применения аппаратного RAID. Каковы преимущества аппаратного RAID? Некоторые ответы см. в занятии 4.

На Web-узлах производителей оборудования найдите сведения о RAID-массивах. Вы найдете RAID-массивы, содержащие диски, RAID-контроллеры и RAID-корпуса, в которые помещают диски. Акцентируйте внимание на готовых решениях и ответьте на следующие вопросы.

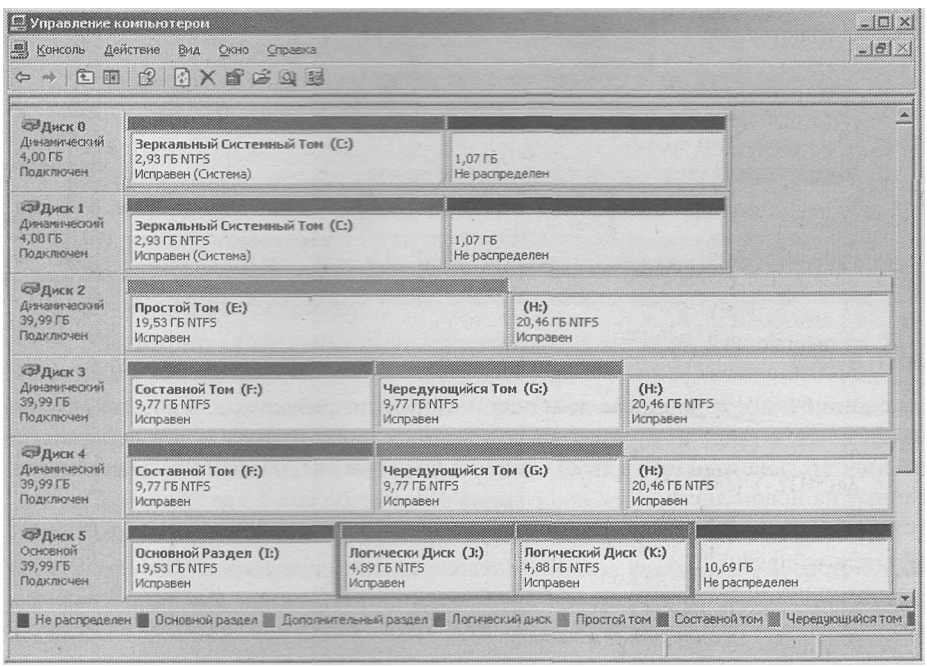
- Какие варианты предлагаются?
- Какие производители выпускают аппаратные RAID-массивы?
- Какова емкость аппаратных RAID-массивов?
- Какие конфигурации реализуют аппаратные RAID-массивы? Существуют ли конфигурации, которые не поддерживаются в Windows Server 2003?
- Каков диапазон цен на аппаратный RAID-массив?
- Сколько стоят RAID-массивы начального уровня?

Когда была написана эта книга, аппаратные RAID-решения емкостью 720 Гб (это ближе к терабайту, чем любой из дисков на большинстве серверов) можно было приобрести меньше чем за $3000.

Как вы объясните достоинства аппаратной RAID-системы своему руководству? Будете ли вы рекомендовать аппаратный RAID вместо программных реализаций Windows Server 2003? Почему?

Практикум по устранению неполадок

Вы администрируете сервер компании Contoso. Ltd. От предыдущего администратора вам достался сервер, содержащий много внутренних дисков SCSI. Вы открываете консоль *Управление дисками* (Disk Management), чтобы определить конфигурацию этих дисков и их томов и видите следующее:

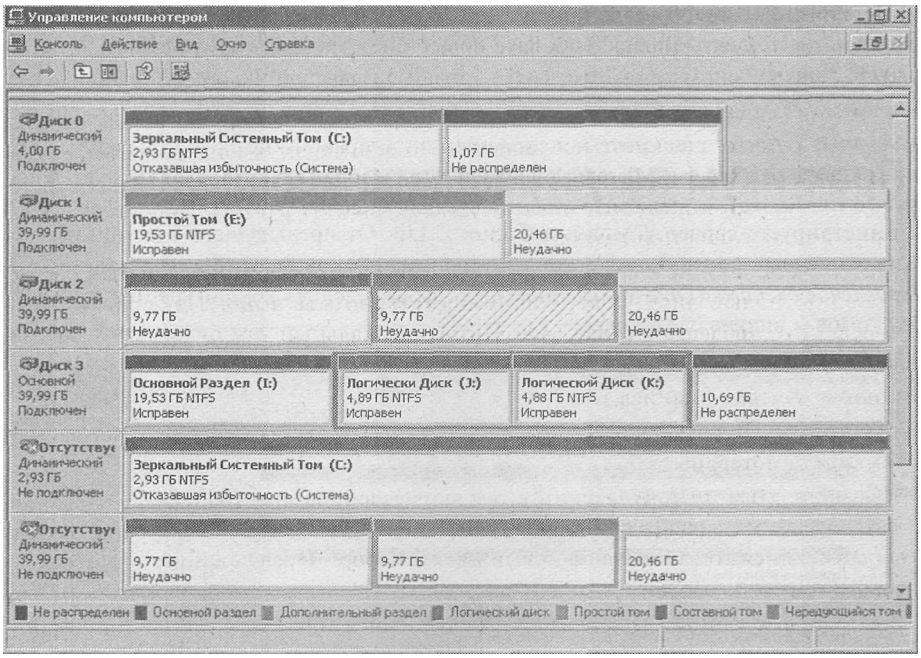


Синоптики сообщили о вероятности урагана завтра утром. Чтобы не рисковать, вы, отправляясь домой, запустили резервное копирование сервера. Прогноз оправдался: ураган был достаточно сильным и все организации не работали несколько дней. Электроснабжение здания Contoso прервалось, в результате разрядились батареи в источниках бесперебойного питания, и серверы выключились. В первые часы после восстановления питания произошло несколько скачков электричества.

Вернувшись, вы попытались загрузить серверы. Один сообщил об ошибке, вы открыли оснастку *Управление дисками* (Disk Management) и увидели удручающую картину дисков и томов, показанную на рис. далее.

Два диска сервера вышли из строя. На одном из них хранилась зеркальная копия системного тома. Другой содержал тома нескольких типов, включая участки томов RAID-0, -1 и -5.

У вас есть новый диск емкостью 80 Гб. Вы выключаете сервер и извлекаете два неисправных диска. После установки нового диска вы перезагружаете сервер.



Упражнение

Возьмите лист бумаги и запишите действия, которые потребуются для восстановления данных на каждом утерянном томе. Будьте внимательны. Включите все действия по очистке отсутствующих дисков и томов, а также по установке, настройке и восстановлению данных на новом диске.

Составив максимально полный список действий, сравните свое решение с ответом.

1. Войдите в систему.
2. Завершите установку нового дисковода. Следуйте инструкциям *Мастера нового оборудования* (Found New Hardware Wizard). Если окно мастера не открывается, откройте оснастку *Диспетчер устройств* (Device Manager) и проверьте, не установились ли диски автоматически. Если диски не отображаются, установите их с помощью приложения *Установка оборудования* (Add Hardware).
3. Откройте оснастку *Управление дисками* (Disk Management).
4. Определите и инициализируйте новый диск. Оснастка *Управление дисками,* скорее всего, обнаружит новый диск и запустит мастер инициализации диска. Если окно мастера не открывается, посмотрите, не появился ли диск в оснастке *Управление дисками* и, если нет, щелкните узел **Управление дисками (Disk Management)** правой кнопкой и выберите **Повторить сканирование дисков (Rescan Disks).** Когда диск появится, щелкните его правой кнопкой и выберите **Инициализировать диск (Initialize Disk).**
5. Восстановите тома (в любом порядке).

   Восстановите том RAID-5.

   a. Преобразуйте новый диск в динамический: щелкните его правой кнопкой и выберите **Преобразовать в динамический диск (Convert To Dynamic Disk).**

b. Щелкните работающую часть тома RAID-5 правой кнопкой и выберите **Восстановить том (Repair Volume).** Выберите новый диск, содержащий достаточно места, чтобы стать членом тома. Том RAID-5 будет создан и синхронизирован.

Восстановите зеркальный том.

a. Удалите зеркало: щелкните неисправный диск правой кнопкой и выберите **Удалить зеркало (Remove Mirror).** Убедитесь, что выбран участок с отметкой **Отсутствует (Missing),** и щелкните **Удалить зеркало (Remove Mirror).** Оставшаяся часть зеркала станет простым томом.

b. Щелкните простой том правой кнопкой и выберите **Добавить зеркало (Add Mirror).** Выберите новый диск, содержащий достаточно места для зеркального тома, и щелкните **Добавить зеркало (Add Mirror).** Зеркальный том будет создан и синхронизирован.

Восстановите чередующийся том.

a. Удалите том. Чередующиеся тома не устойчивы к отказам. Все данные на этом томе были потеряны.

b. Повторно создайте том: щелкните нераспределенное пространство, где находилась часть тома, правой кнопкой и выберите **Создать том (New Volume).** Выберите чередующийся том и добавьте новый диск в набор. Чередующийся том будет создан и отформатирован.

c. Восстановите данные из архива на чередующийся том.

Восстановите составной том.

a. Удалите том. Составные тома не устойчивы к отказам. Все данные на этом томе были потеряны.

b. Повторно создайте том: щелкните нераспределенное пространство, где находился том, правой кнопкой и выберите **Создать том (New Volume).** Выберите составной том и добавьте новый диск в набор. Укажите размер тома на новом диске. Составной том будет создан и отформатирован.

c. Восстановите данные из архива на составной том.

6. Удалите отсутствующие диски: щелкните их правой кнопкой и выберите **Удалить том (Remove Volume).** Нельзя удалить диск с отсутствующей зеркальной копией, пока зеркало не будет удалено. Нельзя удалить диск с простыми и составными томами или томами RAID-5, пока эти тома не будут удалены и исправлены.
7. Запустите программу CHKDSK после синхронизации и восстановления всех томов.

Резюме главы

- Windows Server 2003 поддерживает два типа дисков — базовые и динамические — и несколько файловых систем, включая FAT, FAT32 и NTFS. Большинство современных возможностей управления дисками поддерживаются только томами на динамических дисках, отформатированных под NTFS.
- Динамические диски предоставляют гибкие и мощные возможности в конфигурациях из двух и более дисков. В зависимости от требований к емкости, производительности и отказоустойчивости можно использовать составные, зеркальные, чередующиеся и тома RAID-5.
- Тома дисков могут искажаться, фрагментироваться и быстро заполняться. Средства *Проверка диска* (Check Disk), *Дефрагментация диска* (Disk Defragmenter) и дисковые квоты служат для управления томами.

- Не все конфигурации RAID устойчивы к отказам: тома RAID-1 и RAID-5 — отказоустойчивые, а RAID-0 — нет. Ни один из типов томов Windows Server 2003 не обеспечивает отказоустойчивость, если выходит из строя более одного дискв в томе.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Уясните влияние каждого типа тома на емкость, производительность и отказоустойчивость. Вы должны уметь рекомендовать конфигурацию дисков на основе требований к хранению.
- Запомните, как настраиваются дисковые квоты, и как работают стандартные и индивидуальные квоты.
- Распознайте и исправьте том, который временно был переведен в автономный режим, но теперь подключен снова: выполните команды **Повторить сканирование дисков (Rescan Disks)** и **Реактивизировать диск (Reactivate Disk)** или **Реактивизировать том (Reactivate Volume)** и запустите программу CHKDSK.
- Запомните, как перестроить отказоустойчивые тома (зеркальные и RAID-5) на замененном диске и изучите используемые для этого команды: **Повторить сканирование дисков (Rescan Disks), Инициализировать диск (Initialize Disk), Преобразовать в динамический диск (Convert To Dynamic Disk), Разделить зеркальный том (Break Mirrored Volume),** Удалить **зеркало (Remove Mirror)** и **Восстановить том (Repair Volume).**

Основные термины

Простой том ~ simple volume — эквивалент раздела на базовом диске. Поскольку простые тома находятся на одном физическом диске, они не устойчивы к отказам.

Составной том ~ spanned volume — содержит пространство нескольких физических дисков. Поскольку их размер имеет тенденцию к росту и в томе используется несколько физических дисков, риск сбоя увеличивается, а такие тома не устойчивы к отказам.

Чередующийся **том ~ striped volume** — данные одновременно записываются на несколько физических дисков (от 2 до 32). Обеспечивает максимальную емкость и производительность, но не устойчив к отказам.

Зеркальный том ~ mirrored volume — два диска содержат идентичные данные. Единственный тип программного RAID, способный защитить системный том. Хорошая производительность операций чтения и записи, отличная отказоустойчивость; высокая стоимость в расчете на Мб пространства, поскольку 50 % потенциального размера тома заняты избыточными данными.

Том RAID-5 ~ RAID-5 volume — данные одновременно записываются на несколько физических дисков (от 2 до 32) и чередуются с информацией четности для отказоустойчивости на случай выхода из строя одного диска. Хорошая скорость чтения; эффективное использование пространства диска; высокая нагрузка на процессор и умеренная скорость записи, поскольку при записи данных приходится вычислять контрольные суммы.

Вопросы и ответы

Занятие 1. Закрепление материала

1. Вы устанавливаете новый диск объемом 200 Гб и хотите поделить его на пять логических томов: для ОС, приложений, домашних каталогов пользователей, общих данных и точки распространения ПО. Пространство диска нужно поровну разделить между пятью логическими томами. Кроме того, вы хотите оставить 50 Гб нераспределенного пространства для дальнейшего расширения какого-либо логического тома. Какую конфигурацию выбрать с учетом базовых и динамических дисков и типов поддерживаемых ими логических томов?

   Правильный ответ: выделите 150 Гб пространства диска, а 50 Гб оставьте нераспределенными. Это значит, что каждый из пяти логических томов будет занимать 30 Гб. Вы можете настроить на базовом диске от нуля до трех основных разделов, каждый из которых поддерживает один логический диск, который на базовом диске является логическим томом. Остальные 2—5 логических томов будут созданы в виде логических дисков на дополнительном разделе. Если бы этот диск был динамическим, все пять логических томов были бы настроены как простые тома. Хотя обе конфигурации допустимы в данной ситуации, лучше настроить динамический диск (пояснения см. на следующем занятии).

2. Что из перечисленного позволяет восстановить данные, когда один жесткий диск выходит из строя?
   a. Основной раздел.
   b. Дополнительный раздел.
   c. Логический диск.
   d. Простой том.
   e. Составной том.
   f. Зеркальный том.
   g. Чередующийся том.
   h. ТОМ RAID-5.

   Правильный ответ: f, h.

3. **Вы** настраиваете тестовую систему с альтернативной загрузкой. На первый основной раздел установлена ОС Windows NT 4, а на второй — Windows Server 2003. На диске уже нет места, поэтому вы добавляете новый диск, загружаете Windows Server 2003 и настраиваете новый диск как динамический. Запустив Windows NT 4, вы не видите этот диск. Почему?

   Правильный ответ: только семейство Windows XP/2000 и Windows Server 2003 поддерживает динамические диски.

4. Чтобы обеспечить отказоустойчивость, максимальную производительность и возможность горячей замены неисправного диска, вы приобрели аппаратный RAID-массив из семи дисков. После установки массива вы увидели в Windows Server 2003 только один новый диск. Почему?

   Правильный ответ: аппаратная дисковая подсистема с независимым контроллером скрывает структуру физического диска от ОС. Контроллер управляет работой и дисковым вводом-выводом в массиве. Вычисление четности и выполнение зеркальных операций записи не влияют на производительность ОС.

Занятие 2. Закрепление материала

1. Этот вопрос является продолжением ситуации, описанной в вопросе 1 занятия 1. Вы установили новый диск объемом 200 Гб, сделали диск базовым и создали три основных раздела по 30 Гб для ОС, домашних каталогов пользователей и общих данных. Вы настроили дополнительный раздел и два логических диска по 30 Гб каждый для установленных приложений и точки распространения ПО. На диске осталось 50 Гб нераспределенногЬ пространства. Несколько месяцев спустя вы заметили, что места на трех томах практически не осталось. Вы хотите подготовится к вероятному расширению одного или нескольких разделов. Что нужно сделать?

   Правильный ответ: вы должны преобразовать диск в динамический. Раздел на базовом диске может быть расширен только на непрерывное нераспределенное пространство. После преобразования все основные разделы и логические диски станут простыми томами. Простые тома можно расширять на любое нераспределенное пространство.

2. Какой тип области диска поддерживает логические диски?
   a. Основные разделы.
   b. Простые тома.
   c. Составные тома.
   d. Дополнительные разделы.
   e. Нераспределенное пространство.

   Правильный ответ: d.

3. **Вы** недавно добавили диск на компьютер. До этого диск использовался под управлением Windows 2000 Server. Диск появился в консоли *Диспетчер устройств* (Devide Manager), но неправильно отображается в оснастке *Управление дисками* (Disk Management). Что нужно сделать?
   a. Импорт чужих дисков.
   b. Форматирование тома.
   c. Повторное сканирование дисков.
   d. Изменение буквы диска или пути.
   e. Преобразование в динамические диски.

   Правильный ответ: c.

4. Вы пытаетесь преобразовать внешний диск FireWire из базового в динамический, но команда преобразования недоступна. Какова наиболее вероятная причина?

   Правильный ответ: сменный диск нельзя преобразовать в динамический. Внешние дисководы считаются сменными.

Занятие 3. Закрепление материала

1. Вы — администратор компьютера под управлением Windows Server 2003, и намерены исправить любые ошибки файловой системы и восстановить испорченные сектора на жестком диске. Каким средством воспользоваться?
   a. *Проверка диска* (Check Disk).
   b. *Дефрагментация диска* (Disk Defragmenter).
   c. DISKPART.
   d. Дисковые квоты.

   Правильный ответ: a.

2. Вы — администратор компьютера под управлением Windows Server 2003. Жесткий диск компьютера содержит два тома данных: D: и E:. Вы включаете дисковые квоты на обоих томах с лимитом 20 Мб для всех пользователей. Кроме того, вы хотите задать лимит 10 Мб для домашних папок пользователей, которые хранятся в каталоге D:\Users. Возможно ли это? Почему? Где можно реализовать квоты?
   a. На любом сервере для всех дисков.
   b. На любом физическом диске на всех томах.
   c. На любом томе для всех папок.
   d. На любой папке.

   Правильный ответ: c. Квоты можно настроить только для томов. Нельзя настроить квоты для папки Users на томе D:. Квота применяется ко всему тому. Кроме того, вы не сможете установить суммарную квоту 20 Мб для томов D: и E:. Впрочем, можно настроить ограничение 15 Мб на томе D: и 5 Мб на томе E: или любое другое соотношение, в сумме дающее 20 Мб.
3. Сколько свободного места на томе нужно для выполнения полной дефрагментации?
   a. 5%.
   b 10%.
   c. 15%.
   d. 25%.
   e 50%.

   Правильный ответ: c.

Занятие 4. Закрепление материала

1. Вы реализуете программный RAID на компьютере под управлением Windows Server 2003 и хотите обеспечить отказоустойчивость системного и загрузочного разделов. Какой тип RAID следует использовать?
   a. RAID-0.
   b. RAID-1.
   c. RAID-5.
   d. Программный RAID нельзя использовать для защиты загрузочного раздела.

   Правильный ответ: b. Зеркальный том может содержать любой раздел, в том числе загрузочный или системный.
2. **Вы** хотите защитить данные на жестком диске компьютера под управлением Windows Server 2003. Необходимо обеспечить максимальную скорость дискового ввода-вывода и «горячую» замену жестких дисков. Какой тип RAID следует использовать?
   a. RAID-0.
   b. RAID-1.
   c. RAID-5.
   d. Аппаратный RAID.

   Правильный ответ: d. Хотя аппаратный RAID дороже программного, он быстрее выполняет ввод-вывод. Кроме того, аппаратные отказоустойчивые решения могут поддерживать «горячую» замену жестких дисков (неисправный диск можно заменить, не выключая компьютер) и «горячее» резервирование (автоматически подключается запасной диск).

3. Вы настраиваете том RAID-5 на компьютере под управлением Windows Server 2003 и планируете установить пять дисков по 20 Гб каждый. Какой процент избыточности можно ожидать от такой конфигурации?
   a. 20.
   b. 25.
   c. 33.
   d. 50.

   Правильный ответ: a. Тома RAID-5 экономичнее зеркальных, поскольку эффективнее используют дисковое пространство. Чем больше дисков содержит том RAID-5, тем ниже стоимость хранения избыточных данных. Если конфигурация RAID-5 состоит из пяти дисков, избыточная информация занимает 20 %.

4. Вы настраиваете программный RAID на компьютере под управлением Windows Server 2003, чтобы обеспечить отказоустойчивость данных. Этот компьютер используется в качестве сервера БД. Данный сервер чаще выполняет чтение, и гораздо реже — запись. Вам необходимо создать отказоустойчивое решение с отличной скоростью чтения. Какой тип RAID следует использовать?
   a. RAID-0.
   b. RAID-1.
   c. RAID-5.

   Правильный ответ: c. Несмотря на умеренную скорость записи, RAID-5 обеспечивает отличную производительность чтения. RAID-1 обеспечивает хорошую производительность чтения и записи, однако скорость чтения не столь высока, как у RAID-5.

5. Компьютер, на котором нужно создать том RAID-5, содержит три диска по 2 Гб нераспределенного пространства на каждом. В оснастке *Управление дисками* (Disk Management) вы запускаете *Мастер создания томов* (New Volume Wizard), щелкнув правой кнопкой одну из областей нераспределенного пространства. Когда вы доходите до экрана **Выбор типа тома (Select Volume Type),** вариант RAID-5 недоступен. Какова наиболее вероятная причина?
   a. RAID-5 уже реализован на аппаратном уровне.
   b. Один или два диска являются базовыми.
   c. Все три диска являются динамическими.
   d. Все три диска являются базовыми.
   e. RAID-5 уже реализован программно.

   Правильный ответ: b. Для создания тома RAID-5 необходимо не менее трех динамических дисков.

6. Вышел из строя диск зеркального тома. Вы хотите заменить его. Как подготовить зеркальный том к замене диска?

   Правильный ответ: убедитесь, что процессы не обращаются к зеркальному тому и что его выход из строя связан с неисправностью диска, а не контроллера. Затем с помощью программы Diskpart или оснастки Управление дисками (Disk Management) выберите неисправный диск и удалите зеркало. При необходимости выключите компьютер и замените неисправный диск. Перезагрузите компьютер и с помощью программы Diskpart или оснастки Управление дисками восстановите зеркало из оставшейся половины. Когда добавляется зеркало, на новый диск записывается копия данных.

ГЛАВА 12

Мониторинг Microsoft Windows Server 2003

Темы экзамена

- Мониторинг текущей производительности системы.
- Мониторинг и анализ событий.
- Мониторинг и оптимизация производительности приложений на сервере.
- Мониторинг объектов производительности памяти.
- Мониторинг объектов производительности сети.
- Мониторинг объектов производительности процессов.
- Мониторинг объектов производительности дисков.
- Мониторинг узких мест производительности сервера.
- Мониторинг событий.

В этой главе

При первой установке компьютера (с полным набором ресурсов и не обремененного историей использования) кажется, что все в полном порядке. Однако по мере старения и роста нагрузки от дополнительных приложений и пользователей могут возникнуть проблемы. Если не разобраться в применяемых средствах мониторинга и оптимальных способах их использования в вашей среде, производительность может начать снижаться, сначала вызывая раздражение, а затем — серьезные проблемы.

Первые шаги мониторинга нового компьютера под управлением Windows Server 2003 должны включать всеобъемлющий анализ готовности ресурсов и производительности, данные которого следует периодически сравнивать с текущими значениями, чтобы проблемы с приложениями или оборудованием можно было устранить или вообще избе-

жать их. Учитывая значительное число программных средств в составе Windows Server 2003, уважающий себя администратор не допустит, чтобы ошибки застали его врасплох.

Прежде всего

Для изучения материалов этой главы вам потребуется:.

- компьютер под управлением Windows Server 2003, установленный как ServerOl и настроенный в качестве контроллера домена contoso.com.

Занятие 1. Работа с консолью *Просмотр событий*

Windows Server 2003 включает набор файлов журналов, сконфигурированных и размещенных в консоли *Просмотр событий* (Event Viewer). Настраивая параметры каждого из этих журналов под требования своей среды, вы можете собирать данные для устранения неисправностей оборудования, приложений, системы и доступа к ресурсам.

Изучив материал этого занятия, вы сможете:

- ✓ перечислить типы журналов консоли *Просмотр событий;*
- ✓ настроить запись данных в журнал;
- ✓ вывести записанные данные в отфильтрованном виде.

Продолжительность занятия — около 20 минут.

Журналы консоли *Просмотр событий*

Служба *Журнал событий* (Event Log) установлена и запускается автоматически на всех компьютерах под управлением Windows Server 2003. Она регистрирует события в файлах журналов трех видов.

- ***Приложение* (Application).** Разработчики приложений могут запрограммировать в ПО запись в этот журнал изменений конфигурации, ошибок или других событий.
- ***Система* (System).** Windows Server 2003 записывает в этот журнал предопределенные события (запуска или аварийной остановки службы, сбоев устройств и т. п.).
- ***Безопасность* (Security). В** этот журнал записывают события входа в системы и доступа к ресурсам (для ведения аудита). Запись большинства событий производится по желанию администратора.

Примечание Хотя наполнение журналов событий приложений и системы определяют разработчик приложений и ОС соответственно, журнал безопасности следует предварительно настроить для записи событий определенного типа (успех или неудача для каждого вида). Если выбраны события доступа к файлам или объектам, в свойствах безопасности каждого объекта необходимо настроить запись событий аудита в журнал безопасности.

На контроллерах домена Windows Server 2003 предусмотрено два дополнительных журнала.

- *Служба **каталогов*** **(Directory Service).** Содержит сведения, связанные со службой каталогов Active Directory, например о несогласованной репликации объекта или значимых событиях внутри каталога.
- *Служба репликации **файлов*** **(File Replication Service).** Содержит ошибки или значимые события, регистрируемые службой репликации файлов, которые связаны с копированием данных между контроллерами домена в цикле репликации.

Наконец, на DNS-сервере Windows Server 2003 предусмотрен еще один журнал.

- ***DNS-сервер*** **(DNS Server).** Содержит ошибки или значимые события, регистрируемые DNS-сервером.

Настройка журналов средствами консоли *Просмотр событий*

При первом запуске консоли *Просмотр событий* (Event Viewer) отображаются все события, записанные в выбранный журнал. Их перечень может быть очень длинным и содержать массу записей, как информационных, так и предупреждающих. События можно отсортировать по типу, в меню **Вид (View)** выбрав **Фильтр (Filter).**

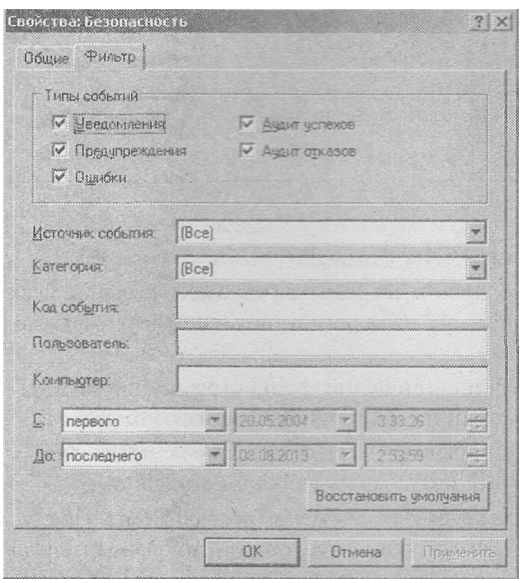


Рис. 12-1. Вкладка *Фильтр* для журнала безопасности

Рядом с вкладкой **Фильтр** расположена вкладка **Общие (General),** позволяющая настроить рабочие параметры журнала, в том числе:

- отображаемое имя журнала;
- максимальный размер журнала;
- следует ли перезаписывать самые старые события из журнала по достижении его максимального размера. Предусмотрено три варианта перезаписи:
  - **Затирать старые события по необходимости [Overwrite Events As Needed (default)]** — старые события перезаписываются новыми;

- **Затирать события старее n дней (Overwrite Events Older Than n Days)** — перезаписываются события, «возраст» которых превышает установленный;
- **Не затирать события (чистка журнала вручную) [Do Not Overwrite Events (Clear Log Manually)]** — события перестают регистрироваться.

Внимание! Если оставить вариант по умолчанию, **Затирать старые события по необходимости,** могут быть перезаписаны важные сведения о доступе к ресурсам или других аспектах безопасности, если журнал контролируется редко. Рекомендуется регулярно проводить анализ. Файлы журналов можно архивировать (т. е. записывать на диск), если нужно сохранять регистрируемые события.

Чтобы гарантированно не потерять записи из журнала безопасности, Windows Server 2003 предусматривает параметр в политике **Конфигурация компьютера (Computer Configuration)\Параметры безопасности (Security Settings),** который принудительно выключает компьютер, если запись сведений аудита в журнал безопасности невозможна. Этот параметр дисциплинирует административные действия, если включена ручная очистка журнала безопасности.

Вкладка **Общие (General)** в окне свойств журнала безопасности показана на рис. 12-2.

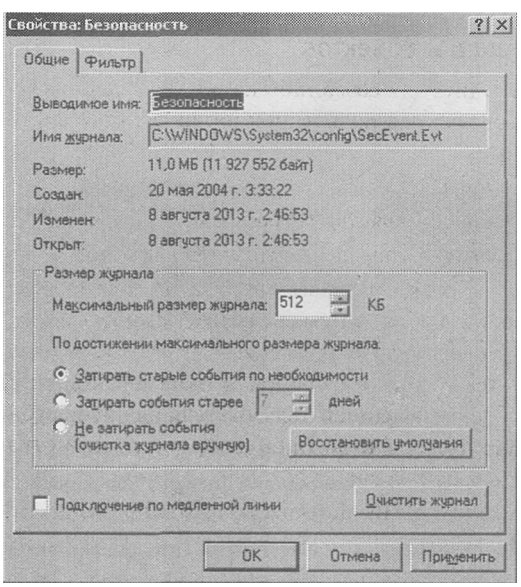


Рис. 12-2. Вкладка *Общие* для журнала безопасности

Лабораторная работа. **Мониторинг событий**

На этой лабораторной работе вы настроите журнал безопасности для записи событий доступа к файлам и объектам, а затем отфильтруете выводимые в нем данные.

Упражнение 1. Настройка журнала безопасности

В этом упражнении вы настроите аудит доступа к файлам и объектам.

1. Войдите на Server01 как *Администратор* (Administrator) и откройте консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers).

2. Щелкните правой кнопкой ОП Domain Controllers и выберите **Свойства (Properties).**
3. На вкладке **Групповая политика (Group Policy)** выберите **Политика контроллеров домена по умолчанию (Default Domain Controllers Policy)** и щелкните **Изменить (Edit).**
4. Раскройте узлы **Конфигурация компьютера (Computer Configuration), Конфигурация Windows (Windows Settings), Параметры безопасности (Security Settings), Локальные политики (Local Policies)** и щелкните **Политика аудита (Audit Policy).**
5. На правой панели дважды щелкните **Аудит доступа к объектам (Audit Object Access).**
6. В открывшемся окне свойств ниже строки **Вести аудит следующих попыток доступа (Audit These Attempts)** щелкните Отказ **(Failure).**
7. Закройте *Редактор объектов групповой политики* (Group Policy Object Editor), щелкните **OK**, чтобы закрыть окно свойств ОП Domain Controllers, затем закройте консоль *Active Directory — пользователи и компьютеры.*
8. Из командной строки исполните gpupdate.
9. После сообщения об обновлении политики компьютера закройте командную строку.

Вы активировали аудит неудачных попыток доступа к объектам на ServerOl (из ОП Domain Controllers) и обновили групповую политику, чтобы изменения вступили в силу немедленно.

Упражнение 2. Настройка аудита файлов и объектов

В этом упражнении вы настроите ведение аудита для созданной папки. Разрешения будут заданы таким образом, чтобы сымитировать попытку несанкционированного доступа пользователя к ресурсу.

1. На рабочем столе создайте папку с именем Data.
2. Щелкните папку правой кнопкой и выберите **Свойства (Properties).**
3. Перейдите на вкладку **Безопасность (Security),** затем щелкните свою учетную запись.
4. Установите флажок **Запретить (Deny)** напротив разрешения *Полный доступ* (Full Control) для вашей учетной записи пользователя, затем щелкните **Да** (Yes) в окне предупреждения.
5. Щелкните кнопку **Дополнительно (Advanced)** и в открывшемся окне перейдите на вкладку **Аудит (Auditing).** Добавьте свою учетную запись пользователя в список аудита **Содержание папки/Чтение данных (List Folder / Read Data)** для регистрации отказов, затем щелкните **OK**, чтобы закрыть все окна свойств.
6. Дважды щелкните папку Data, чтобы открыть ее. Вы должны получить предупреждение **Отказано в доступе (Access Denied).**

Упражнение 3. Чтение журнала безопасности

В этом упражнении вы проверите, что аудит отказа доступа к папке Data работает.

1. Откройте консоль *Управление компьютером* (Computer Management) из группы программ **Администрирование (Administrative Tools).**
2. Раскройте узел **Просмотр событий (Event Viewer)** и щелкните журнал безопасности в левой панели.
3. Вверху списка вы увидите несколько событий **Аудит отказов (Failure Audit)** с идентификатором 560, сгенерированных из-за отказа в доступе к папке Data.
4. Щелкните правой кнопкой журнал безопасности в панели папок, выберите **Вид (View),** а затем **Фильтр (Filter).**
5. В диалоговом окне **Фильтр (Filter)** задайте следующие параметры:

- **Источник события (Event Source): Security;**
- **Категория (Category): Доступ к объектам (Object Access);**
- **Типы событий (Event Types):** флажок **Аудит отказов (Failure)** установлен, остальные сняты.

6. Щелкните **OK**, чтобы применить данный фильтр к журналу безопасности.

Вы отфильтровали данные журнала безопасности, чтобы отображались только события, касающиеся отказа в доступе к объектам.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Какие журналы будут по умолчанию отображаться в консоли *Просмотр событий* (Event Viewer) на контроллере домена с запущенной службой DNS? Что это за журналы, и какие данные в них собраны?
2. Вы настроили на компьютере Windows Server 2003 аудит всех отказов доступа к объектам, и для всех файлов и папок сконфигурировано ведение аудита для **Содержание папки/Чтение данных (List Folder / Read Data).** Все остальные параметры оснастки *Просмотр событий* (Event Viewer) и журнала **Безопасность (Security)** сохраняют значения по умолчанию. Что произойдет, когда объем журнала безопасности достигнет 512 Кб?
3. Необходимо, чтобы данные в журнале *Безопасность* (Security) не перезаписывались, в то же время нужно, чтобы компьютер Windows Server 2003 не прекращал обслуживание сети. Какие параметры нужно задать на сервере?

Резюме

Консоль *Просмотр событий* (Event Viewer) из состава Windows Server 2003 обеспечивает доступ к нескольким журналам, где фиксируются ошибки и значимые события, возникающие во время работы системы. Журнал системы содержит данные, связанные со службами и другими видами внутренней активности ОС. В журнал приложений записываются данные, генерируемые прикладными программами. Журнал безопасности содержит данные аудита успехов и отказов. В отличие от других журналов, состав журнала безопасности контролирует администратор. На контроллерах домена предусмотрены дополнительные журналы для служб репликации файлов и Active Directory. На DNS-серверах ведется отдельный журнал для службы DNS.

В сложных или объемных журналах вывод данных можно отфильтровать по разным условиям, включая дату записи и тип данных, чтобы повысить удобочитаемость. Данные из журналов можно сохранять в файлах следующих типов:

- двоичный файл монитора производительности (*.blg) с циклической перезаписью или без нее;
- текстовый файл (*.txt или *.csv);
- БД формата SQL.

После конфигурирования параметров журнала настройки оснастки *Монитор производительности* (Performance Monitor) можно сохранить в HTML-файле, выбрав команду **Сохранить параметры как (Save Settings** As) из контекстного меню журнала. В дальней-

шем их можно загрузить, выбрав команду **Новые параметры журнала из (New Log Settings From)** в контекстном меню журналов счетчиков.

Для всех журналов в консоли *Просмотр событий* (Event Viewer) можно независимо настраивать максимальный размер файла журнала и поведение системы по достижении этого размера. Варианты действий по достижении максимального размера файла — немедленная перезапись старых данных, перезапись данных только определенного «возраста», либо очистка журнала вручную и запрет перезаписи данных. В соответствующей конфигурации можно активировать групповую политику, чтобы немедленно принудительно отключить компьютер, если запись сведений аудита в журнал безопасности невозможна.

Занятие 2. Работа с консолью *Производительность*

С помощью консоли *Производительность* (Performance) можно оценить работу любого компьютера в сети. Оснастки *Системный монитор* (System Monitor) и *Журналы и оповещения производительности* (Performance Logs And Alerts) являются частью консоли *Производительность* (perfmon.msc). Оснастка *Системный монитор* позволяет просматривать данные о производительности в реальном времени, которые накапливают указанные вами счетчики. Оснастка *Журналы и оповещения производительности* позволяет записывать данные о производительности (в журналы) и определить действия на случай достижения порогового значения счетчика (оповещения). Консоль *Производительность* предоставляет средства для выполнения множества задач, включая:

- сбор и просмотр данных о производительности в реальном времени;
- просмотр данных в журнале;
- представление данных в форме графиков, гистограмм или отчетов;
- создание HTML-страниц из представлений путем импорта настроек файла журнала;
- сохранение конфигураций мониторинга, которые впоследствии можно загружать в *Системный монитор* (System Monitor) на других компьютерах.

Изучив материал этого занятия, вы сможете:

- ✓ отслеживать данные о производительности в реальном времени;
- ✓ записывать данные о производительности в файл журнала;
- ✓ настраивать оповещения системы и производительности.

Продолжительность занятия — около 20 минут.

Настройка оснастки *Системный монитор*

С помощью оснастки *Системный монитор* (System Monitor) можно собирать и просматривать данные, настраивая различные счетчики, которые фиксируют работу оборудования, приложений и служб любого компьютера в вашей сети. Чтобы указать, какие данные нужно собрать, нужно настроить следующие параметры.

- **Тип данных**. Можно указать один или несколько экземпляров счетчиков для объектов мониторинга производительности, по которым нужно собрать данные.

- **Источник данных.** Счетчик может собирать данные на локальном или удаленном компьютере. Вы должны быть локальным администратором или членом группы *Пользователи журналов производительности* (Performance Log Users) на том компьютере, где вы намерены собирать данные.
- **Интервалы снятия показаний.** Данные можно записывать вручную в реальном времени либо в указанные периодические интервалы.

Просмотр данных

При первом открытии оснастки *Системный монитор* загружаются три счетчика, которые начинают сообщать о следующих характеристиках в реальном времени:

- *Память* (Memory): **Обмен страниц в сек (Pages/sec);**
- *Физический диск* (Physical Disk) (Total): **Средняя длина очереди диска (Average Disk Queue Length);**
- *Процессор* (Processor) (_Total): **% загруженности процессора (% Processor Time).**

На рис. 12-3 показана оснастка *Системный монитор* с загруженными по умолчанию счетчиками.

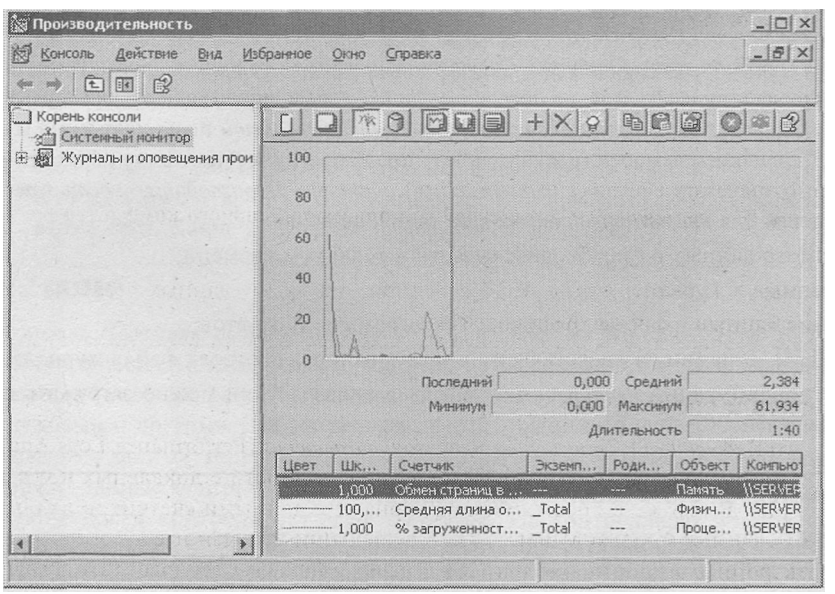


Рис. 12-3. Оснастка *Системный монитор* консоли *Производительность*

Счетчики можно добавлять или удалять: щелкните кнопку Добавить (Add) на панели инструментов (или нажав Ctrl+I), либо щелкните правой кнопкой в любом месте правой панели и выберите Добавить счетчики (Add Counters). В окне Добавить счетчики **(Add Counters)** можно выбрать любые из доступных счетчиков для локального или удаленного компьютера в сети. Счетчики упорядочены по типам объектов, виду счетчика в выбранной категории объекта и экземпляру счетчика.

- Объект. Логический набор счетчиков ресурсов, служб или приложений.
- Счетчик. Элемент, сообщающий данные. Характер данных зависит от типа счетчика.

- **Экземпляр.** Означает одно или несколько вхождений счетчика, пронумерованных в зависимости от конфигурации компьютера. Например, для компьютера с двумя процессорами экземпляр «0» относился бы к первому процессору, экземпляр «1» — ко второму, а «Total» представлял бы совокупность обоих экземпляров. Если счетчик имеет один экземпляр, будут доступны варианты «0» и «Total».

На рис. 12-4 показан счетчик *% загруженности процессора* (% Processor Time) для однопроцессорного компьютера Server01.

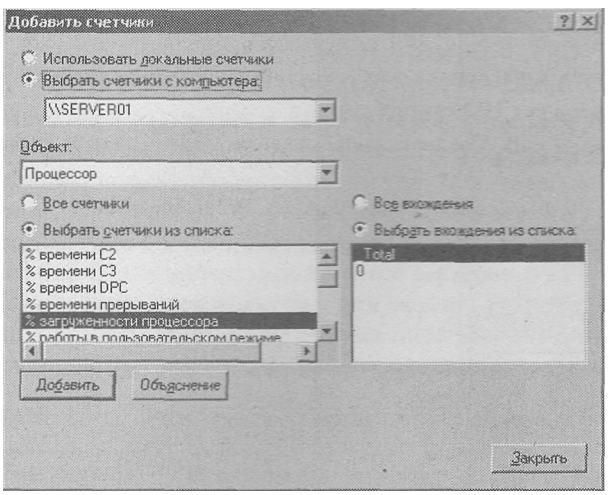


Рис. 12-4. Счетчик *% загруженности процессора* для однопроцессорного компьютера

Подготовка к экзамену Помните, что «_Total» представляет сумму данных от нескольких экземпляров счетчика, если таковые доступны.

Ведение журналов и оповещения

С помощью оснастки *Журналы и оповещения производительности* (Performance Logs And Alerts) можно автоматически собирать данные производительности с локальных и удаленных компьютеров. Вы можете просматривать журналы с данными счетчиков из оснастки *Системный монитор* (System Monitor) либо экспортировать данные в программу для работы с электронными таблицами или БД в целях анализа и генерации отчетов. Любые счетчики, доступные в оснастке *Системный монитор,* можно настроить для использования в оснастке *Журналы и оповещения производительности* со следующими параметрами:

- собирать данные в CSV-файл или файл со значениями, разделенными табуляцией, для последующего экспорта;
- просматривать данные журналов счетчиков параллельно с их записью и дальнейшим сбором;
- формировать журналы трассировки (управляемых событиями) на основе доступных поставщиков;
- определять параметры файла журнала, в том числе время запуска и остановки журнала и его максимальный размер;

- задавать оповещение для счетчика с возможностью отправки административного сообщения, выполнения программы или запуска журнала по достижении порогового значения счетчика.

На рис. 12-5 показано диалоговое окно настройки оповещения на Server01 на тот случай, когда значение счетчика *% свободного места* (% Free Space) опустится ниже 20%.

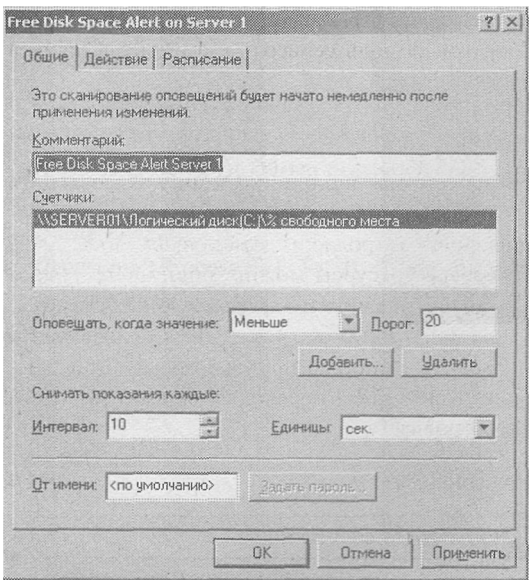


Рис. 12-5. Настройка оповещения о нехватке свободного места на диске

Мониторинг данных производительности

При мониторинге данных о производительности сервера или сети используйте метод «сверху вниз»: оцените наиболее общие параметры (нагрузку на процессор, длину очереди для диска и процессора, использование памяти и активность сетевого ввода-вывода) для определения узких мест. Выявив проблемную область, обратите внимание на использование ресурсов конкретными службами и приложениями; при необходимости также проанализируйте уровни протоколов и потоков. Обычно проблема вызвана ошибками в работе одного из устройств или приложений либо глобальной нехваткой ресурсов в системе. Отдельные устройства можно переконфигурировать или заменить, а глобальные ресурсы можно добавить (увеличить объем памяти, поставить более скоростной процессор и т. п.).

Тем не менее, такой мониторинг может не внести ясность, если у вас нет опорных значений производительности системы, с которыми можно сравнить полученные результаты. Сразу после конфигурирования нового компьютера выполните набор действий по мониторингу работы ключевых объектов — процессора, памяти, сети и процессов (приложений и служб), — чтобы определить, как компьютер функционирует в обычных условиях в состояниях стандартной, пиковой нагрузки или бездействия. Если при дальнейшем мониторинге возникают проблемы или узкие места, сравнение полученных показателей с опорными поможет найти решение.

Как выбирать объекты и счетчики

Объекты счетчиков для опорного или последующего мониторинга производительности сервера можно выбирать двумя способами. Первая методика мониторинга подразумевает оценку роли сервера в вычислительной среде и обязанностей, возлагаемых на него пользователями. Другая методика предполагает анализ таких категорий счетчиков, как *Процессор* (Processor), *Память* (Memory), *Сетевой интерфейс* (Network Interface) и *Физический диск* (PhysicalDisk), с меньшим акцентом на роль сервера, а концентрацией на согласованности подхода к мониторингу.

Роли сервера

Мониторинг по ролям сервера полезен, когда серверы исполняют конкретные роли в сетевой среде. Эти роли определяются службами или ресурсами, которые сервер предоставляет пользователям. Примеры ролей серверов: контроллеры доменов, файловые серверы, Web-серверы. Выявить недостающие серверу ресурсы можно, оценив его производительность с помощью соответствующих объектов счетчиков, измеряющих ресурсы, наиболее интенсивно используемые сервером в данной роли. Сведения последующего мониторинга производительности можно сравнить с опорными значениями, чтобы оптимизировать исполнение той или иной роли. В табл. 12-1 перечислены объекты, часто применяемые для анализа работы серверов по ролям.

Табл. 12-1. Роли сервера и объекты для мониторинга

Роль сервера	Используемые ресурсы	Объекты и счетчики
Серверы приложений	Память, сеть, кэш процессора	*Память* (Memory), *Процессор* (Processor), *Сетевой интерфейс* (Network Interface) и *Система* (System)
Серверы архивации	Процессор, сеть	*Система* (System), *Сервер* (Server), *Процессор* (Processor), *Сетевой интерфейс* (Network Interface)
Серверы БД	Диски, сеть, процессор	*Физический диск* (PhysicalDisk), *Логический диск* (LogicalDisk), *Процессор* (Processor), *Сетевой интерфейс* (Network Interface), *Система* (System)
Контроллеры доменов	Память, процессор, сеть, диск	*Память* (Memory), *Процессор* (Processor), *Система* (System), *Сетевой интерфейс* (Network Interface), объекты протоколов (зависят от сети, но это могут быть TCPv4, UDPv4, ICMP, IPv4, NBT Connection, NWLink IPX, NWLink NetBIOS и NWLink SPX), *Физический диск* (PhysicalDisk), *Логический диск* (LogicalDisk)
Серверы файлов и печати	Память, диск, сетевые компоненты	*Память* (Memory), *Сетевой интерфейс* (Network Interface), *Физический диск* (PhysicalDisk), *Логический диск* (LogicalDisk), *Очередь печати* (Print Queue)
Серверы почты или обмена сообщениями	Процессор, диск, сеть, память	*Память* (Memory), *Кэш* (Cache), *Процессор* (Processor), *Система* (System), *Физический диск* (PhysicalDisk), *Сетевой интерфейс* (Network Interface), *Логический диск* (LogicalDisk)

Табл. **12-1.** *(окончание)*

Роль сервера	Используемые ресурсы	Объекты и счетчики
Web-серверы	Диск, кэш, сетевые компоненты	*Кэш* (Cache), *Сетевой интерфейс* (Network Interface), *Физический диск* (PhysicalDisk), *Логический диск* (LogicalDisk)

Для каждой роли сервера соберите опорные данные производительности, используя счетчики по каждому из применимых к роли объектов, и периодически проверяйте, не происходят ли значительные отклонения в работе серверов.

Категории объектов

В сетевой среде, где серверы исполняют несколько ролей, мониторинг по ролям может оставить «белые пятна» в собранных данных. В таких случаях следует собирать более полные данные от каждой из основных категорий объектов.

Счетчики использования памяти

После определения опорных характеристик использования памяти следует регулярно вести мониторинг для выявления отклонений. Для мониторинга памяти можно использовать следующие счетчики.

- Нехватка памяти: *Память (Memory)\Доступно байт* (Available Bytes), *Доступно КБ* (Available Kbytes) или *Доступно МБ* (Available Mbytes) (чтобы видеть объем в мегабайтах); *Процесс* (Process) (All_processes)*Рабочее множество* (Working Set); *Память* (Metory)*Обмен страниц в сек* (Pages/sec); *Память* (Metory)*Байт кэш-памяти* (Cache Bytes). Эти счетчики показывают объем памяти, занимаемый всеми процессами, и объем доступной памяти.
- Частые ошибки страниц физической памяти: *Память* (Metory)*Обмен страниц в сек* (Pages/sec); *Процесс* (Process) (All_processes)*Рабочее множество* (Working Set); *Память* (Memory)*Ввод страниц/сек* (Pages Input/sec); *Память* (Metory)*Вывод страниц/сек* (Pages Output/sec). Ошибки страниц физической памяти происходят, когда запрашивается страница памяти помещенная в виртуальную память на диске. Чрезмерный обмен страниц между диском и памятью снижает производительность компьютера. Этого можно избежать, снизив нагрузку на систему либо увеличив объем физической памяти.

Счетчики использования сети

Счетчики использования сети регистрируют активность *сетевых интерфейсных плат* (Network Interface Card, NIC), установленных на компьютере, а также сегмента сети, с которым они взаимодействуют. Для измерения производительности компьютера в сети можно использовать следующие счетчики.

- *Сетевой интерфейс* (Network Interface)*Длина очереди вывода* (Output Queue Length); *Всего байт/сек* (Bytes Total\sec). Длина очереди должна быть небольшой, а суммарное число байт — большим; это означает, что сетевая плата передает пакеты быстро и без задержки.
- *Сетевой интерфейс* (Network Interface): *Отправлено байт/сек* (Bytes Sent/Sec); *Текущая пропускная способность* (Current Bandwidth); *Получено байт/сек* (Bytes Received/Sec). Стабильно высокие значения этих счетчиков означают, что в сети передается слишком много трафика. Сегментирование сети на меньшие части или увеличение ее пропускной способности снизит вероятность коллизий из-за чрезмерного трафика.

Примечание Различные типы сетевых конфигураций реализуют разные уровни производительности и объема трафика. К примеру, проведите мониторинг параметра *Использование сети (%)* (% Network Utilization): рекомендуемая максимальной нагрузка для сети Ethernet, в которой нет коммутаторов, — 30 %. Это означает, что сеть Ethernet с пропускной способностью 10 Мбит/сек перестает стабильно работать, когда через нее постоянно проходит больше 3 Мбит данных в секунду. Если значение данного счетчика выше 40 %, коллизии данных становятся помехой и снижают производительность сети.

Счетчики процессов

Практически для каждого запроса системного ресурса существует служебный процесс. Применение счетчиков процессов позволяет анализировать отдельные процессы (включая системные службы), которые используют системные ресурсы. Для сбора данных о производительности на основе процессов предусмотрены следующие важные счетчики.

- Утечки памяти; приложения, интенсивно использующие память: *Память* (Memory)*Распределений в невыгружаемом страничном пуле* (Pool Nonpaged Allocs); *Память* (Memory)*\Байт в невыгружаемом страничном пуле* (Pool Nonpaged Bytes); *Память* (Memory)*\Байт в выгружаемом страничном пуле* (Pool Paged Bytes); *Процесс* (Process) *(имя_процесса)\Байт в невыгружаемом страничном пуле* (Pool Nonpaged Bytes); *Процесс* (Process) *(имя_процесса)\Счетчик дескрипторов* (Handle Count); *Процесс* (Process) *(имя_процесса)\Байт в выгружаемом страничном пуле* (Pool Paged Bytes); *Процесс* (Process) *(имя_процесса)\Байт виртуальной памяти* (Virtual Bytes); *Процесс* (Process) *(имя_процесса)\Байт исключительного пользования* (Private Bytes). Эти счетчики показывают использование памяти отдельными процессами. В результате анализа можно перераспределить требовательные к памяти приложения (или изолировать приложения с утечками памяти) на другие компьютеры.

Примечание Утечку памяти приложения можно обнаружить, запустив его на выделенном сервере и отследив объем используемой памяти во времени без изменений нагрузки. Беспричинный рост занятой памяти может свидетельствовать о ее утечке.

Счетчики использования дисков

Объекты счетчиков *Физический диск* (PhysicalDisk) предоставляют данные о работе каждого жесткого диска, а объекты счетчиков *Логический диск* (LogicalDisk) — о работе указанных томов (C:, D: и т. п.). Мониторинг счетчиков свободного места на логических дисках и производительности физических дисков даст полезную информацию. Для мониторинга физических и логических дисков предусмотрены следующие важные счетчики.

- *Логический диск (LogicalDisk)\% свободного места* (% Free Space). Доля свободного места в процентах от общего доступного пространства а данном логическом томе. Этот счетчик не применяется для физического диска.

  Примечание При подсчете значения для экземпляра _Total счетчики *% свободного места* пересчитывают сумму в виде процентного отношения для каждого диска.

- *Физический диск (PhysicalDisk)\Средний размер одного обмена с диском (байт)* (Avg. Disk Bytes/Transfer); *\Среднее время обращения к диску (сек)* (Avg. Disk sec/Transfer); *Средняя длина очереди диска* (Avg. Disk Queue Length); *\% активности диска* (% Disk Time). Эти счетчики замеряют размер операций ввода-вывода во времени и степень нагруз-

ки на диск. Диск работает эффективно, если передает большие объемы данных относительно быстро, а длина его очереди не превышает двух операций для каждого дисковода.

Лабораторная работа. **Работа с консолью *Производительность***

На этой лабораторной работе вы запишете данные о производительности, проанализируете их с помощью оснастки *Системный монитор* (System Monitor) и экспортируете данные для последующей загрузки в электронную таблицу Microsoft Excel.

Упражнение 1. Запись данных производительности

В этом упражнении вы создадите файл журнала с данными по объектам *Логический диск* (LogicalDisk), *Физический диск* (PhysicalDisk) и *Рабочие очереди сервера* (Server Work Queues).

1. Войдите на Server01 *как Администратор* (Administrator) и откройте консоль *Производительность* (Performance).
2. Раскройте узел **Журналы и оповещения производительности (Performance Logs And Alerts)** и щелкните Журналы **счетчиков (Counter Logs).**
3. Щелкните правой кнопкой в любом месте правой панели и выберите **Новые параметры журнала (New Log Settings).**
4. Создайте файл журнала с именем Test, добавьте в него объекты *Логический диск* (LogicalDisk), *Физический диск* (PhysicalDisk) и *Рабочие очереди сервера* (Server Work Queues) и укажите, что снимать показания нужно каждые восемь секунд. Запомните имя и размещение файла журнала и затем щелкните **OK** для его запуска.
5. После начала записи журнала проделайте какие-либо операции с приложениями на вашем компьютере. По истечении примерно 30 секунд вернитесь в оснастку *Журналы и оповещения производительности* (Performance Logs And Alerts) и остановите запись журнала.
6. В оснастке *Системный монитор* (System Monitor) щелкните **Просмотр данных журнала (View Log Data)** (нажмите Ctrl+L или щелкните четвертую кнопку слева на панели инструментов) и загрузите файл тестового журнала.

График в оснастке *Системный монитор* теперь показывает данные, записанные в вашем сеансе. Можно выбрать представление данных: диаграмма, гистограмма или отчет. Созданный вами файл журнала записан в формате по умолчанию (двоичном) и предназначен исключительно для использования в консоли *Производительность*.

Упражнение 2. Импорт записанных данных

В этом упражнении вы сохраните записанные на упражнении 1 данные, чтобы затем загрузить их в Microsoft Excel.

1. При необходимости заново откройте консоль *Производительность*.
2. Щелкните правой кнопкой файл журнала Test и выберите **Свойства (Properties).**
3. В окне свойств журнала Test на вкладке **Файлы журналов (Log Files)** измените значение параметра **Тип журнала (Log File Type)** с **Двоичный файл (Binary File)** на **Текстовый файл (разделитель — запятая) [Text File (Comma Delimited)].**

4. Щелкните **OK** и начните запись данных в файл журнала. Проделайте какие-либо операции, использующие диск вашего компьютера, в течение примерно 30 секунд, затем остановите запись журнала.

Созданный файл журнала в формате CSV можно открывать, просматривать и анализировать в Microsoft Excel.

Примечание Microsoft Excel открывает файлы в монопольном режиме, поэтому перед просмотром CSV-файла его нужно закрыть в оснастке *Журналы и оповещения производительности*.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Ваша цель — наблюдать за работой всех серверов Windows Server 2003, чтобы дефрагментировать их диски по расписанию и максимально эффективно. Для работы вашей программы дефрагментации диска требуется, минимум, 20 % свободного места на каждом томе. Что нужно сделать?
2. Вы наблюдали за работой одного из серверов Windows Server 2003, сетевая производительность которого была низкой. Были получены следующие результаты.
   - *Процессор* (Processor): *% загруженности процессора* (% Processor Time): Высокий.
   - *Физический диск* (Physical Disk): *% активности диска* (% Disk Time): Низкий.
   - *Память* (Memory): *Обмен страниц в сек* (Pages/sec): Низкий.
   - *Процессор* (Processor): *Прерываний/сек* (Interrupts/sec): Высокий.
   - *Процесс* (Process): *% загруженности процессора* (% Processor Time) для неслужебных процессов: Низкий.
   - *Процесс* (Process): *% загруженности процессора* (% Processor Time) для системных служб: Низкий.

   Какова наиболее вероятная причина проблемы?
3. Сервер для наблюдения за другими серверами в сети не справляется с этой задачей, и вы решили его разгрузить. Что нужно сделать помимо сбора максимально возможного объема данных, чтобы оказать наибольшее влияние на производительность компьютера, ведущего мониторинг?

Резюме

В консоли *Производительность* (Performance) содержится две оснастки: *Системный монитор* (System Monitor) и *Журналы и оповещения производительности* (Performance Logs And Alerts). Первая предназначена для отображения данных в реальном времени в интерфейсе консоли в виде графика, гистограммы и числового отчета, вторая — для записи данных в файл (журнал) и контроля выхода счетчиков за пределы пороговых значений с генерацией оповещений. Журналы, записанные средствами оснастки *Журналы и оповещения производительности,* можно загружать в *Системный монитор* для анализа и экспортировать в файлы разных типов (CSV, HTML и др.) для формирования отчетов.

Занятие 3. Работа с программой *Диспетчер задач*

Диспетчер задач (Task Manager) предоставляет сведения о выполняющихся приложениях и процессах и выводит несколько важных счетчиков производительности процессов.

Изучив материал этого занятия, вы сможете:

- ✓ настраивать *Диспетчер задач* для отображения данных производительности;
- ✓ использовать *Диспетчер задач* для запуска и остановки приложений и процессов.

Продолжительность занятия - около 15 минут.

Знакомство с *Диспетчером задач*

Диспетчер задач можно открыть двумя способами: щелкните правой кнопкой свободную часть панели задач и выберите одноименную команду либо нажмите Ctrl+Alt+Del и щелкните одноименную кнопку. Интерфейс *Диспетчера задач* в Windows Server 2003 по умолчанию содержит пять вкладок для отображения данных разных категорий: **Приложения (Applications), Процессы (Processes), Быстродействие (Performance), Сеть (Networking)** и **Пользователи (Users).**

Вкладка *Приложения*

Вкладка **Приложения (Applications)** показывает состояние программ пользовательского уровня, выполняющихся на данном компьютере. Службы и системные приложения, запущенные не в контексте вошедшего в систему пользователя, не отображаются. Также отсюда можно запустить новую программу кнопкой **Новая задача (New Task),** завершить кнопкой **Снять задачу (End Task)** либо переключиться на другую программу кнопкой **Переключиться (Switch To).** Щелкнув правой кнопкой приложение в списке, можно выбрать команду **Перейти к процессу (Go To Process),** чтобы перейти к соответствующему процессу на вкладке **Процессы (Processes).**

Вкладка *Процессы*

Вкладка **Процессы (Processes)** содержит сведения обо всех процессах, выполняющихся на компьютере, включая приложения пользовательского уровня, службы и другие системные процессы. Выбрав в меню **Вид** (Mew) команду **Выбрать столбцы (Select Columns),** можно добавить или удалить столбцы данных, включая изменение использования памяти, идентификатор процесса и использование процессора. Данные можно отсортировать по любому столбцу, щелкнув его заголовок.

Щелкнув правой кнопкой любой процесс, можно изменить приоритет времени процессора, получаемого этим процессом, задать привязку к процессору на многопроцессорном компьютере, а также завершать процесс (в том числе все дочерние или связанные с ним процессы командой **Завершить дерево процессов (End Process Tree);** например, при необходимости снять почтовое приложение может также потребоваться завершить работу спулера MAPI: щелкните правой кнопкой почтовую программу и выберите **Завершить дерево процессов).**

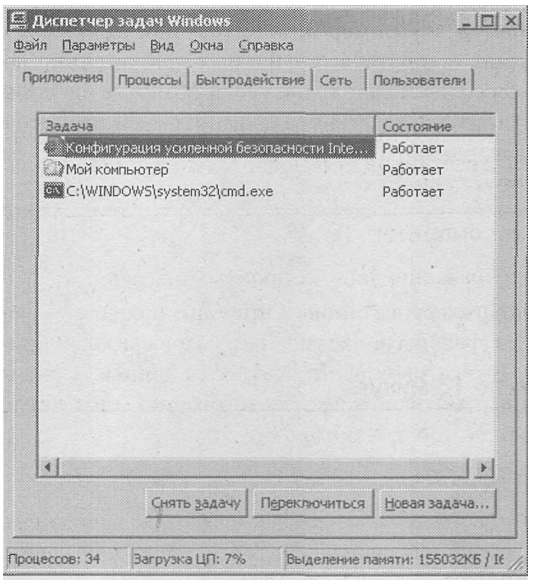


Рис. 12-6. Вкладка *Приложения* в программе *Диспетчер задач*

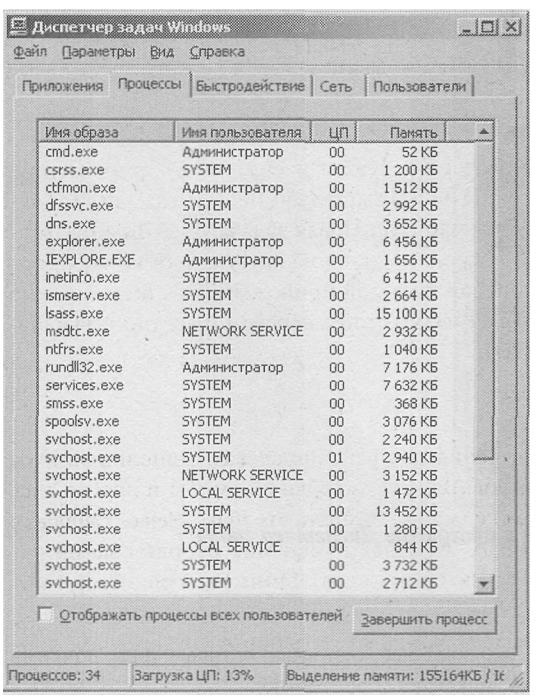


Рис. 12-7. Вкладка *Процессы* в программе *Диспетчер задач*

Внимание! Изменение параметров процесса, например приоритета или привязки к процессору, может снизить производительность других выполняемых приложений. Завершать процесс, а тем более дерево процессов, следует, только если обычные способы завершения не действуют. К счастью, Windows Server 2003 предохраняет свои процессы от завершения средствами *Диспетчера задач,* однако им может не хватить ресурсов из-за неправильного назначения приоритетов другим процессам.

Вкладка *Быстродействие*

Вкладка **Быстродействие (Performance)** отображает в реальном времени ключевые элементы производительности компьютера. На графиках показана нагрузка на каждый процессор системы и использование памяти. В текстовой части выводятся данные о физической памяти, памяти ядра и выделении памяти; помимо этого отображается число используемых активными процессами дескрипторов и потоков.

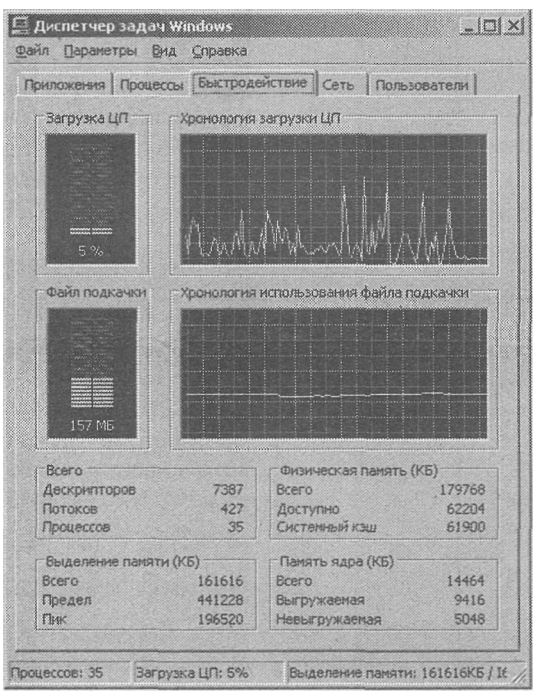


Рис. 12-8. Вкладка *Производительность* в программе *Диспетчер задач*

Вкладка*Сеть*

Вкладка **Сеть (Networking)** (рис. 12.9) показывает все активные сетевые подключения, выводя следующие данные: имя, скорость, нагрузка и состояние.

Вкладка *Пользователи*

Вкладка **Пользователи (Users)** (рис. 12-10) показывает всех вошедших в систему пользователей (локально или по сети), а также позволяет выйти из системы или принудительно отключить какого-либо пользователя. Удаленным пользователям можно отправлять сообщения, выбрав сеанс пользователя и щелкнув кнопку **Отправить сообщение (Send Message).**

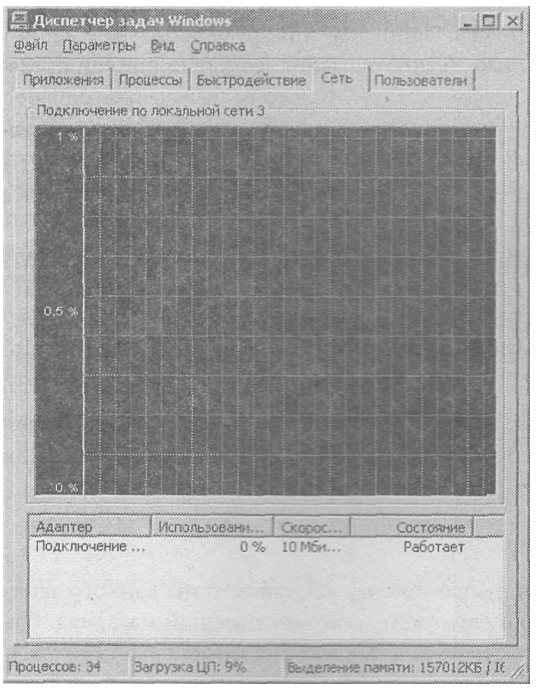


Рис. 12-9. Вкладка *Сеть* в программе *Диспетчер задач*

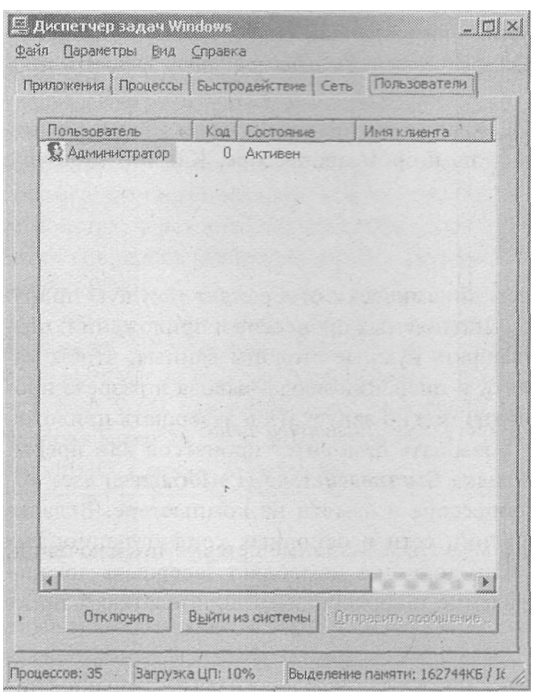


Рис. 12-10. Вкладка *Пользователи* в программе *Диспетчер задач*

Лабораторная работа. **Работа с *Диспетчером задач***

На этой лабораторной работе вы с помощью *Диспетчер задач* запустите приложение и определите его процесс.

1. Щелкните правой кнопкой свободную часть панели задач и выберите **Диспетчер задач (Task Manager).**
2. На вкладке **Приложения (Applications)** щелкните **Новая задача (New Task).** Введите explorer и щелкните OK.

   Откроется *Проводник* с окном по умолчанию, обычно это папка **Мои документы (My Documents).** На вкладке **Приложения** в *Диспетчере задач* появится строка **Мои документы (My Documents)** (или с именем другого раскрывшегося окна).
3. Щелкните правой кнопкой имя только что запущенного приложения и выберите **Перейти к процессу (Go To Process).**

В *Диспетчере задач* фокус перейдет на вкладку **Процессы (Processes):** будет выделен процесс **Explorer.exe.** Отсюда, если потребуется, можно задать приоритет процесса или завершить его.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Какую информацию о производительности приложений может дать *Диспетчер задач?*
2. Ваш компьютер дает сбой примерно через час после каждой загрузки системы. Вы подозреваете, что проблема в приложении, допускающем утечку памяти, что приводит к нехватке памяти в системе. Как средствами *Диспетчера задач* выявить проблемное приложение?
3. На вашем компьютере работает СУБД. Компьютер оснащен двумя процессорами. Необходимо, чтобы СУБД выполнялась на втором процессоре. Как это сделать с помощью *Диспетчера задач?*

Резюме

Программа *Диспетчер задач* (Task Manager) динамически отображает текущую производительность компьютера относительно выполняемых процессов и приложений, позволяет задать интервалы обновления и выбрать нужные столбцы данных, чтобы наблюдать использование процессора, памяти и операции ввода-вывода в разрезе процессов. На вкладке **Приложения (Applications)** можно запускать и завершать приложения, на вкладке **Процессы (Processes)** — повышать приоритет процессов или прерывать их, включая дочерние процессы. Вкладка **Быстродействие (Performance)** дает общее представление об использовании процессора и памяти на компьютере. Вкладка **Сеть (Networking)** сообщает об использовании сети и основных конфигурационных данных. Вкладка **Пользователи (Users),** если доступна, позволяет завершать локальный сеанс или прерывать удаленный. Удаленно подключенным пользователям также можно отправлять сообщения.

Занятие 4. Работа с поставщиком журнала событий WMI

Инструментарий управления Windows (Windows Management Instrumentation, WMI) — это предложенная Microsoft реализация инициативы *управления предприятием на основе Web* (Web-Based Enterprise Management. WBEM). призванной установить стандарты создания, чтения и изменения управленческой информации. WMI совместим с WBEM и поддерживает *универсальную информационную модель* (Common Information Model, CIM) — модель данных, которая описывает объекты, существующие в среде управления. Хранилище WMI — это БД определений объектов, а диспетчер объектов WMI обрабатывает объекты от WMI-поставщиков. WMI-поставщики могут получать разнообразные входные данные от служб, приложений и системных компонентов.

Изучив материал этого занятия, вы сможете:

- ✓ использовать WMI и командную строку WMI (WMIC) для наблюдения за работой служб;
- ✓ применять WMI и WMIC для определения установленных программ;
- ✓ применять WMI и WMIC ля уведомления о событиях.

Продолжительность занятия - около 30 минут.

Как работает WMI

Вкратце, источники информации о'WMI («поставщики») сообщают о своих компонентах (устройствах, службах, приложениях и т. п.) диспетчеру объектов WMI, который записывает ее в БД WMI (хранилище). В зависимости от того, какие данные каждый поставщик принимает и выдает, администратор может соответствующими способами манипулировать компонентами, задавать свойства и указывать события, которые будут оповещать об изменениях в компонентах. К хранилищу WMI можно обращаться средствами администрирования, поставляемыми производителем системы, приложения или устройства; через интерфейсы прикладного программирования (API), программы обработки сценариев (например сервер сценариев Windows) или из командной строки с помощью WMIC.

На заметку Для работы с WMI не обязательно разбираться в сценариях — вы уже применяли WMI, даже если не осознавали этого. Многие программные средства уже используют WMI для наблюдения и настройки объекта поставщика WMI. Примеры из Windows Server 2003 — *Сведения о системе* (System Information), *Свойства системы* (System Properties), *Службы* (Services).

WMIC — интерфейс командной строки для WMI

Интерфейс командной строки для WMI применяется для локального или удаленного управления любым WMI-совместимым компьютером, который способен проверить подлинность пользователя, запустившего WMIC. Чтобы управлять удаленным компьютером с помощью WMIC, на локальном компьютере, с которого вы будете вести монито-

ринг, необходимо лишь наличие WMI — на удаленном компьютере не требуется установка WMIC. С помощью WMIC можно выполнять:

- **локальное управление компьютером** — локальное управление командами WMIC;
- **удаленное управление компьютером** — управление компьютером из консоли другого компьютера;
- **удаленное управление несколькими компьютерами** — управления несколькими компьютерами по одной команде из консоли другого компьютера;
- **составление административных сценариев** — написание управляющего сценария (командного файла), автоматизирующего управление компьютером (локальным, удаленным или несколькими компьютерами).

Администрирование с помощью WMIC

Хотя использование WMIC в рамках WMI здесь не обсуждается, необходимо сделать несколько пояснений, чтобы вы знали, как отвечать на вопросы об эффективном мониторинге средствами WM1 и WMIC. Если не указано иное, здесь предполагается, что вы работаете с WMIC в интерактивном режиме, то есть можете исполнять отдельные команды и видеть их результаты из самой среды WMIC.

Подготовка к экзамену Структура и способ использования команд не зависит от рабочего режима WMIC (интерактивного или автономного). Выбор режима зависит от того, сколько команд вы собираетесь исполнить и нужно ли их вводить вручную или обработать командный файл. Для перехода в интерактивный режим WMIC из командной строке исполните wmic; чтобы выйти — `exit` или `quit`. В автономном режиме используется однострочная команда, начинающаяся с WMIC, в командной строке или в командном файле.

WMI работает в контексте пространства имен, по умолчанию это root\cli (MSFT_cli в таблице стилей XSL), который указывает, какие свойства, методы (действия) и псевдонимы доступны в WMI. При необходимости вы можете добавить псевдонимы, методы и свойства (придется вспомнить программирование), однако имеющегося списка вполне хватает для выполнения большинства задач мониторинга.

Безопасность для WMI настраивается в оснастке *Управляющий элемент WMI* (WMI Control) или из консоли WMI (Wmimgmt.msc). По умолчанию пользователям разрешено читать информацию WMI-поставщика с помощью WMIC на локальном компьютере, но они не могут подключаться удаленно или записывать информацию вне контекста поставщика. Если вы намерены предоставить дополнительные разрешения какому-либо пользователю или группе, это можно сделать из оснастки *Управляющий элемент WMI*.

Псевдонимы WMIC

Первый параметр командной строки WMIC — псевдоним, который должен быть уникальным в схеме пространства имен WMI. Он предоставляет доступ к информации WMI без необходимости запоминать более сложные объекты и свойства схемы. В табл. 12-2 перечислены свойства, соответствующие каждому экземпляру псевдонима. Полные списки псевдонимов и пространства имен, а также другую информацию о псевдонимах WMIC см. в разделе *Пространства имен псевдонимов и классы* (Alias Namespaces and Classes) *Центраспраккиподдержки*.

Табл. 12-2. Псевдонимы WMIC

Свойство	Описание
FriendlyName	Имя псевдонима, должно быть уникальным
Description	Описание псевдонима. Выводится в качестве описания, если в командной строке WMIC ввести /?
Formats	Список, чьи элементы содержат имя и список свойств (объектов класса MSFTCliProperty), которые должны отображаться для данного формата. Все форматы являются объектами класса MSFT_CliFormat
Verbs	Список типов поведения, доступных через данный псевдоним. Существует две формы типов поведения: • стандартные действия, напрямую поддерживаемые данной служебной программой: • определенные пользователем действия, которые должны быть сопоставлены какому-либо методу, определенному для цели данного псевдонима. Все действия яатяются объектами класса MSFT_CliVerb
Qualifiers	Список, сходный со списком квалификаторов WMI. Все квалификаторы являются объектами класса MSFT_Qualifier
Target	Список, сходный со списком квалификаторов WMI. Все квалификаторы являются объектами класса MSFT_Qualifier
PWhere clause	Необязательный оператор WHERE, ограничивающий свойство Target. Для него предусмотрены подстановочные значения, являющиеся параметрами данного псевдонима. Подстановочные значения помечены символом #. Если необходимо несколько параметров, они последовательно сопоставляются с маркерами #
Connection	Подробности: к каким компьютерам следует подключаться, используемый уровень безопасности и т. п. Если подробности подключения не указаны, для компьютеров, к которым требуется подключиться, значение свойства равно /NODE, а значение пространства имен — /NAMESPACE. Если имя пользователя и пароль не заданы, будут использованы значения /USER и /PASSWORD при их наличии (иначе используется текущая учетная запись)
View an alias schema	Чтобы просмотреть схему псевдонима, используйте метапсевдоним, например ALIAS OS

Действия WMIC

Большинство псевдонимов выполняют какие-либо операции, которые инициируются путем ввода псевдонима и действия. Совместно с параметрами и переключателями сочетания «псевдноним — действие» определяют, какая конфигурация задана в рамках приложения или системы или какая информация считывается из хранилища WMI. В табл. 12-3 описаны ключевые действия, используемые при мониторинге. Полный список действий, а также другую информацию о них см. в разделе *Действия WMIC* (WMIC Verbs) *Центра справки и поддержки.*

Табл. 12-3. Действия WMIC

Действие	Операция	Параметры	Пример
CALL метода	Выполнение	Метод и список параметров, если предусмотрен. Параметры в списке разделяют запятыми. Чтобы получить список доступных методов и их параметры для текущего псевдонима, используйте команду SERVICE CALL/?	SERVICE WHERE CAPTION='TELNET' CALL STARTSERVICE
GET	Вывод указанных свойств	Имя свойства или переключатель	PROCESS GET NAME
LIST	Вывод данных	LIST — действие по умолчанию. Существует масса переключателей и модификаторов, используемых совместно с действием LIST (например BRIEF)	PROCESS LIST BRIEF

Использование WMIC при мониторинге

Если WMI выполняется на компьютере и пользователь обладает достаточными административными полномочиями, можно вести локальный или удаленный мониторинг компьютера из командной строки. В автономном режиме несколько команд можно поместить в командный файл, запускаемый вручную либо автоматически по расписанию. Команды WMIC можно вывести в CSV-файл, текстовый файл или HTML-страницу для просмотра и анализа. Ниже даны примеры типичных сценариев мониторинга и выходные данные, иллюстрирующие использование WMIC для мониторинга.

- PRODUCT

  Выводит на консоль результаты запроса обо всем программном обеспечении, установленном на локальном компьютере.
- /OUTPUT:c:\applog.htm NTEVENT WHERE "eventtype<3 AND logfile=Application'" GET Logfile, SourceName, Eventtype, Message, TimeGenerated/FORMAT:htable:"sortby=EventType" Выводит в HTML-файл (C:\applog.htm) все события типов 0, 1 и 2 из журнала приложений на локальном компьютере. Полученный список форматируется в HTML-таблицу (с помощью таблицы стилей XML — htable.xsl) и сортируется по типу события.
- /OUTPUT:c:\applog.csv/NODE:@"c:\serverlist.txt" NTEVENT WHERE "eventtype< 3 AND logfile='Application'" GET Logfile, SourceName, Eventtype, Message, TimeGenerated/ FORMAT:csv:"sortby=EventType"

  Выводит в CSV-файл (C:\applog.csv) все события типов 0, 1 и 2 из журналов приложений на компьютерах, перечисленных в файле serverlist.txt. Полученный список форматируется в перечень значений, разделенных запятыми (с помощью таблицы стилей XML — csv.xsl), и сортируется по типу события.
- OS ASSOC

  Выводит информацию об установленных исправлениях и обновлениях ОС.

Лабораторная работа. **Получение данных WMI из консоли *Просмотр событий***

На этой лабораторной работе вы получите данные из консоли *Просмотр событий* (Event Viewer) и опубликуете их в виде Web-страницы.

1. Войдите на Server01 как *Администратор* (Administrator) и из командной строки исполните wmic. Тем самым вы перевели WMIC в интерактивный режим.
2. В командной строке WMIC введите следующую команду, чтобы обратиться к данным журнала безопасности из упражнения 3 занятия 1:

   ```
   NTEVENT WHERE "EVENTTYPE=5 AND LOGFILE= 'SECURITY'" GET LOGFILE, SOURCENAME, EVENTTYPE, MESSAGE, TIMEGENERATED
   ```

   Эта команда выводит в консоль записи аудита отказов.
3. В командной строке WMIC введите следующую команду, которая выводит ту же информацию на Web-страницу с именем C:\seclog.htm.

   ```
   /OUTPUT:C:\seclog.htm NTEVENT WHERE "EVENTTYPE=5 AND LOGFILE='SECURITY'" GET LOGFILE, SOURCENAME, EVENTTYPE. MESSAGE, TIMEGENERATED/FORMAT:htable
   ```
4. Дважды щелкните файл C:\Seclog.htm. чтобы открыть его в Internet Explorer.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Вам нужно удаленно получить сведения об установленных исправлениях и обновлениях ОС с нескольких серверов в сети. Как сделать это средствами WMI?
2. Вам нужно удаленно получить список всех установленных приложений на 17 компьютерах в отделе разработки. Как сделать это средствами WMI?
3. Вы намерены предоставить небольшой группе специалистов возможность использовать WMI для получения информации с некоторых серверов разработчиков, но не хотите давать им административные привилегии на этих серверах. Как представить доступ?

Резюме

WMI — это WBEM-совместимое программное средство, использующее СШ-совместимую БД управленческой информации. Сведения в эту БД поступают в результате выполнения WMI на каждом компьютере под управлением Windows Server 2003. WMIC — интерфейс командной строки для WMI. Используя последовательности псевдонимов, действий, переключателей и параметров, с его помощью можно изменить конфигурацию компьютерной системы или получить сведения о системе. WMIC может подключаться к компьютеру удаленно при условии, что у инициирующего подключение пользователя достаточно привилегий на удаленном компьютере. Локальному администратору компьютера разрешено удаленное подключение, поэтому все администраторы домена вправе вести удаленное администрирование средствами WMI и WMIC. Для архивирования и получения отчетов данные WMI можно выводить с помощью WMIC в CSV-файлы или HTML-страницы. Команды можно выполнять для нескольких компьютеров — из командной строки или из текстового файла. За исключением необходимости начинать каждую строку с команды WMIC, исполнение команд из командного файла в автономном режиме ничем не отличается от интерактивной работы с WMIC.

Пример из практики

Вас назначили главой ИТ-отдела компании, и вы намерены внедрить лучшие методы работы, чем ранее. Оборудование сервера часто отказывает, и пользователи крайне не довольны работой сети. Предварительные собеседования с администраторами показали, что в последние годы они мало занимались планированием, посвящая почти все время устранению неисправностей.

Вице-президент компании поставил задачу как можно быстрее ликвидировать недостатки и обеспечить секретность важной деловой информации. Необходимо повысить продуктивность работы пользователей, в том числе разобраться, какие приложения установлены ими в обход правил компании.

Вот перечень мероприятий, предлагаемых вами для совершенствования технологической среды.

- Использовать WMI и другие служебные программы для работы с файлами, чтобы получить полный список файловых ресурсов, размещенных на серверах в сети. Полностью документировать структуру разрешений на эти ресурсы и согласовать ее с главами отделов, чтобы убедиться, что вы правильно понимаете потребности доступа к файловым ресурсам.
- м Использовать консоли *Просмотр событий* (Event Viewer) и *Производительность* (Performance) для получения точной картины по наиболее опасным узким местам, которые могут возникнуть из-за отказов устройств, неправильной настройки служб или несовместимости приложений. По необходимости улучшить рабочую среду: заменить оборудование, правильно настроить службы и обновить приложения.
- После определения разрешений начать аудит отказов в доступе, чтобы обнаруживать, кто и какими средствами пытается получить несанкционированный доступ к ресурсам.
- После устранения узких мест с помощью оснастки *Журналы и оповещения производительности* (Performance Logs And Alerts) определить опорные показатели работы серверов. Продолжить наблюдать за изменениями в производительности серверов по сравнению с опорными характеристиками.

Практикум по устранению неполадок

Специалисты службы поддержки создавали собственные Web-страницы для публикации технических данных для остальных сотрудников группы и применяли массу средств для периодического тестирования функциональности и стабильности приложений. Последнее время они неоднократно сообщали, что производительность их компьютеров резко снизилась.

С помощью консоли *Производительность* (Performance) определите опорные значения следующих счетчиков:

- *Кэш* (Cache)*% попаданий при отображении данных* (Data Map Hits %);
- *Кэш* (Cache)*Быстрых чтений/сек* (Fast Reads/sec);
- *Кэш* (Cache)*Страниц «ленивой» записи/сек* (Lazy Write Pages/sec);
- *Логический диск* (Logical Disk)*% свободного места* (% Free Space);
- *Память (Memory)\Доступно байт* (Available Bytes);
- *Память (Memory)\Распределений в невыгружаемом страничном пуле* (Pool Nonpaged Allocs);

- *Память (Memory)\Байт в невыгружаемом страничном пуле* (Pool Nonpaged Bytes);
- *Память (Memory)\Распределений в выгружаемом страничном пуле* (Pool Paged Allocs);
- *Память (Memory)\Байт в выгружаемом страничном пуле* (Pool Paged Bytes);
- *Процессор* (Processor)*(_Total)\% загруженности процессора (%* Processor Time);
- *Система (System)\Контекстных переключений/сек* (Context Switches/sec);
- *Система (System)\Длина очереди процессора* (Processor Queue Length);
- *Процессор* (Processor)*(_Total)\Прерываний/сек* (Interrupts/sec).

Неделю наблюдайте за работой каждого из подозрительных компьютеров в обычном режиме, фиксируя результаты в отдельные файлы журналов. Собирайте данные мониторинга на удаленном компьютере, чтобы не искажать опорные результаты.

Проанализируйте данные на предмет того, имеются ли какие-либо явные узкие места. Данный список счетчиков позволяет в первую очередь оценить работу памяти, дискового ввода-вывода и процессора. Выявив узкое место, проанализируйте работу приложений (процессов), чтобы узнать, какие из них в большей степени вызывают проблему. Затем проблемные приложения можно обновить (если это помогает) или удалить, либо добавить на компьютеры ресурсы для выполнения требуемых задач.

Резюме главы

- Консоль *Просмотр событий* (Event Viewer) представляет данные в форме журналов. На каждом сервере Windows Server 2003 имеются журналы приложений, системы и безопасности. На контроллерах доменов есть два дополнительных журнала, касающихся Active Directory. Другие серверы приложений (например DNS) ведут собственный набор файлов журналов.
- Консоль *Производительность* (Performance) (perfmon.msc) состоит из двух оснасток: *Системный монитор* (System Monitor) и *Журналы и оповещения производительности* (Performance Logs And Alerts). *Системный монитор* отображает в реальном времени данные о производительности на основе объектов счетчиков, и может выводить данные, записанные оснасткой *Журналы и оповещения производительности* в виде журналов счетчиков (опрос через интервалы времени) либо в виде журналов трассировки (управляемых событиями).
- Программа *Диспетчер задач* (Task Manager) служит для просмотра в реальном времени данных о производительности процессов и приложений. С ее помощью можно инициировать и завершать процессы. Также можно повышать или понижать приоритет процессов и привязывать их к конкретному процессору на многопроцессорном компьютере.
- WMI — это система управления, собирающая данные с компьютерных систем. Интерфейс оснастки *Управляющий элемент WMI* (WMI Control) позволяет настраивать разрешения по управлению компьютерами в сети вне рамок стандартных разрешений локального администратора. Хотя с помощью WMI можно настраивать множество типов поведения системы, включая работу пользователей, групп и служб, в этой главе в основном рассказывается об извлечении данных из хранилища WMI средствами WMIC — интерфейса командной строки для WMI. WMIC способен сообщать о запущенных службах и установленных приложениях, а также публиковать данные оснастки *Просмотр событий* (Event Viewer) в CSV- или HTML-файлы для удобства распространения и анализа.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Консоль *Просмотр событий* (Event Viewer) не предназначена для конфигурирования, она собирает данные от различных поставщиков. Фиксируемые данные собираются в соответствующий журнал, их можно фильтровать, сортировать и экспортировать для удобства анализа.
- Программа *Диспетчер задач* (Task Manager) — это средство, используемое только на локальном компьютере; она не позволяет конфигурировать память, процессор или другие параметры и используется исключительно для запуска, остановки, назначения приоритетов приложениям, а также их привязки к определенным процессорам.
- Оснастка *Журналы и оповещения производительности* (Performance Logs And Alerts) не предназначена для конфигурирования. Она служит лишь для записи в журналы счетчиков данных, предоставляемых поставщиками (объектами счетчиков) через указанные интервалы времени, либо для записи в журналы трассировки данных от поставщиков, управляемых событиями.
- Для доступа средствами WMI к удаленному компьютеру и настройки его параметров требуются административные полномочия.
- WMIC не позволяет управлять схемой. Active Directory. WMI поддерживает собственную схему.

Основные термины

Инструментарий управления Windows (WMI) ~ Windows Management Instrumentation (WMI) — предложенная Microsoft реализация инициативы управления предприятием на основе Web (WBEM), призванной установить корпоративные стандарты обра-' ботки данных.

WMIC (Windows Management Instrumentation Control) — служебная программа командной строки, которая предоставляет интерфейс к хранилищу (БД) WMI для управления конфигурацией и мониторинга.

Диспетчер задач ~ Task Manager — средство с графическим интерфейсом для управления процессами.

Системный монитор ~ System Monitor — компонент консоли *Производительность* (Performance) наряду с оснасткой *Журналы и оповещения производительности* (Performance Logs And Alerts), не путайте с окном *Свойства системы* (System Properties).

Вопросы и ответы

Занятие 1. Закрепление материала

1. Какие журналы будут по умолчанию отображаться в консоли *Просмотр событий* (Event Viewer) на контроллере домена с запущенной службой DNS? Что это за журналы, и какие данные в них собраны?

Правильный ответ:

- **Приложение (Application). Разработчики приложений могут запрограммировать в ПО запись изменений конфигурации, ошибок или других событий в этот журнал.**
- **Система (System). Windows Server 2003 записывает в этот журнал предопределенные события (запуск службы или ее аварийная остановка, сбои устройств и т. п.).**
- **Безопасность (Security). В этот журнал по усмотрению администратора записываются события входа в систему и доступа к ресурсам (для ведения аудита).**
- **Служба каталогов (Directory' Service). Содержит сведения, связанные со службой каталогов Active Directory, например о несогласованной репликации объекта или значимых событиях внутри каталога.**
- **Служба репликации файлов (File Replication Service). Содержит ошибки или значимые события, регистрируемые службой репликации файлов, которые связаны с копированием данных между контроллерами домена в цикле репликации.**
- **DNS-сервер (DNS Server). Содержит ошибки или значимые события, регистрируемые DNS-сервером.**

2. Вы настроили на компьютере Windows Server 2003 аудит всех отказов доступа к объектам, и для всех файлов и папок сконфигурировано ведение аудита для **Содержание папки/Чтение данных (list Folder / Read Data).** Все остальные параметры оснастки *Просмотр событий* (Event Viewer) и журнала **Безопасность (Security)** сохраняют значения по умолчанию. Что произойдет, когда объем журнала безопасности достигнет 512 Кб?

   Правильный ответ: по **умолчанию максимальный размер файла журнала составляет 512 Кб и его разрешено перезаписывать, поэтому, когда файл разрастется до 512 Кб, старые данные в этом журнале будут перезаписаны.**

3. Необходимо, чтобы данные в журнале *Безопасность* (Security) не перезаписывались, в то же время нужно, чтобы компьютер Windows Server 2003 не прекращал обслуживание сети. Какие параметры нужно задать на сервере?

   Правильный ответ: в свойствах журнала безопасности задайте параметр Не затирать события (очистка журнала вручную) [Do Not Overwrite Events (Clear Log Manually)]. Не задавайте групповую политику с параметром Параметры безопасности (Security Options)\Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности (Audit: Shut Down System Immediately If Unable To Log Security Audits), поскольку в этом случае сервер перестанет быть доступным в сети после заполнения журнала безопасности. Рекомендуется запланировать регулярный анализ журнала безопасности, однако его частота не будет влиять на отключение сервера из-за несвоевременной очистки журнала.

Занятие 2. Закрепление материала

1. Ваша цель — наблюдать за работой всех серверов Windows Server 2003, чтобы дефрагментировать их диски по расписанию и максимально эффективно. Для работы вашей программы дефрагментации диска требуется, минимум, 20 % свободного места на каждом томе. Что нужно сделать?

   Правильный ответ: настройте оснастку Журналы и оповещения производительности (Performance Logs And Alerts) на рабочей станции (или на относительно свободном сервере) для мониторинга счетчика % свободного места (% Free Space) каждого экземпляра объекта Логический диск (LogicalDisk) для всех удаленных серверов. Кроме того, для каждого счетчика настройте оповещение, срабатывающее, когда на диске свободно мень-

ше 20 % емкости. Наконец, настройте отправку соответствующих предупреждений администратору (и другим пользователям, которым сочтете нужным).

2. Вы наблюдали за работой одного из серверов Windows Server 2003, сетевая производительность которого была низкой. Были получены следующие результаты.
   - *Процессор* (Processor): *% загруженности процессора (%* Processor Time): Высокий.
   - *Физический диск* (Physical Disk): *% активности диска* (% Disk Time): Низкий.
   - *Память* (Memory): *Обмен страниц в сек* (Pages/sec): Низкий.
   - *Процессор* (Processor): *Прерываний/сек* (Interrupts/sec): Высокий.
   - *Процесс* (Process): *% загруженности процессора* (% Processor Time) для неслужебных процессов: Низкий.
   - *Процесс* (Process): *% загруженности процессора (%* Processor Time) для системных служб: Низкий.

   Какова наиболее вероятная причина проблемы?

   Правильный ответ: вероятно, сетевая плата (или другое устройство) неисправно на аппаратном уровне. Большое число прерываний в секунду могло стать причиной того, что процессор занят обработкой запросов на обслуживание от сетевого интерфейса. Поскольку значения остальных счетчиков невелики, вряд ли произошла ошибка приложения или системной службы.

3. Сервер для наблюдения за другими серверами в сети не справляется с этой задачей, и вы решили его разгрузить. Что нужно сделать помимо сбора максимально возможного объема данных, чтобы оказать наибольшее влияние на производительность компьютера, ведущего мониторинг?

   Правильный ответ: нужно увеличить интервал опросов при записи данных с удаленных компьютеров. Уменьшив частоту опроса и варьируя время сбора данных, можно накопить больше данных мониторинга, параллельно снизив нагрузку на ведущий наблюдение компьютер.

Занятие 3. Закрепление материала

1. Какую информацию о производительности приложений может дать *Диспетчер задач?*

   Правильный ответ: программа Диспетчер задач (Task Manager) сообщает об использовании процессора, памяти (включая файл подкачки), вводе-выводе в разрезе процессов.

2. Ваш компьютер дает сбой примерно через час после каждой загрузки системы. Вы подозреваете, что проблема в приложении, допускающем утечку памяти, что приводит к нехватке памяти в системе. Как средствами *Диспетчера задач* выявить проблемное приложение?

   Правильный ответ: запустите все приложения в обычном режиме. В программе Диспетчер задач (Task Manager) в меню Вид (View) выберите Выбрать столбцы (Select Columns) и включите отображение столбца Память — изменение (Memory Usage Delta), затем в окне Диспетчера задач щелкните заголовок этого столбца. Если не выполнять никаких действий в системе, использование памяти запущенными на компьютере процессами должно стабилизироваться. Если в одном из приложений есть утечки памяти, оно будет оставаться на вершине (или поблизости) списка выполняемых процессов, а значение его параметра Память — изменение (Memory Usage Delta) будет расти, даже если никаких действий в системе не выполняется.

3. **На** вашем компьютере работает СУБД. Компьютер оснащен двумя процессорами. Необходимо, чтобы СУБД выполнялась на втором процессоре. Как это сделать с помощью *Диспетчера задач?*

Правильный ответ: щелкните правой кнопкой СУБД на вкладке Приложения (Applications) и выберите Перейти к процессу (Go To Process). Щелкните правой кнопкой процесс и задайте привязку к процессору из контекстного меню.

Занятие 4. Закрепление материала

1. Вам нужно удаленно получить сведения об установленных исправлениях и обновлениях ОС с нескольких серверов в сети. Как сделать это средствами WMI?

   Правильный ответ: используйте псевдоним OS ASSOC с переключателем /node:, чтобы удаленно исполнить команду WMIC на **любом числе компьютеров. С помощью переключателей /output и /format** выведите **данные** в **CSV- или HTML-файл. Например, если бы целями WMIC были компьютеры ServerOl и ServerO2, можно было бы ввести команду** /NODE:"SERVER01","SERVER02" OS ASSOC.

2. Вам нужно удаленно получить **список** всех установленных приложений на 17 компьютерах в отделе разработки. Как сделать это средствами WMI?

   Правильный ответ: введите имена компьютеров в текстовый файл (например computers.txt). Используйте псевдоним WMIC PRODUCT с переключателем /node:®, чтобы получить список приложений, установленных **на каждом из перечисленных компьютеров. С помощью переключателей /output и /format выведите данные в CSV- или HTML-файл. Например, можно было бы получить нужные результаты командой /NODE:@c:\computers.txt PRODUCT.**

3. Вы намерены предоставить небольшой группе специалистов возможность использовать WMI для получения информации с некоторых серверов разработчиков, но не хотите давать им административные привилегии на этих серверах. Как представить доступ?

   Правильный ответ: выдайте всем специалистам (или их группе) разрешение на пространство имен WMI, используя оснастку Управляющий элемент WMI (WMI Control) (Wmimgmt.msc) или из консоли WMI.

ГЛАВА 13

Восстановление системы после сбоя

Темы экзамена

- Автоматическое восстановление системы.
- Восстановление системы сервера.

В этой главе

Хотя Microsoft Windows Server 2003 характеризуется высокой стабильностью и надежностью, источники питания, вентиляторы охлаждения, платы и даже код могут вызвать сбой компьютера. Когда в лесу выходит из строя сервер, страдают все остальные компьютеры. Вы уже научились настраивать и сопровождать сервер так, чтобы свести к минимуму опасность сбоя, узнали, как восстанавливать некоторые службы, драйверы и конфигурации оборудования. В этой главе вы получите навыки, которые требуются для восстановления сервера, когда сама ОС выходит из строя или становится недоступной.

Прежде всего

Для изучения материалов этой главы вам потребуются:

- компьютер под управлением Windows Server 2003. Server01 может быть рядовым сервером или контроллером домена. В первом случае резервное копирование будет выполняться быстрее;
- для выполнения упражнения, демонстрирующего возможности ASR, потребуется второй жесткий диск; после выполнения этого упражнения все данные на диске с системным томом будут стерты. Не выполняйте автоматическое восстановление системы, если хотите сохранить данные.

Занятие 1. Восстановление после сбоя системы

Хуже всего, когда выходит из строя оборудование сервера, и его нельзя восстановить. Чтобы вернуться к работе, необходима полная резервная копия сервера, которую можно восстановить на новом оборудовании. Она должна содержать данные, приложения и саму ОС. В главе 7 вы научились архивировать данные с помощью служебной программы *Архивация данных* (Backup) и средствами Ntbackup. На этом занятии вы узнаете, как использовать эти инструменты для создания резервной копии системы, которая позволяет быстро вернуться к работе даже в самых тяжелых случаях. Кроме того, вы научитесь использовать консоль восстановления хтя решения особых проблем, включая неполадки драйверов и служб.

Изучив материал этого занятия, вы сможете:

- ✓ архивировать данные о состоянии системы:
- ✓ подготовить набор архивации ASR и восстановить компьютер;
- ✓ устанавливать и применять консоль восстановления.

Продолжительность занятия — около 60 минут.

Обзор методов восстановления

Вам уже знакомы методы исправления и восстановления различных неполадок.

- Потеря или искажение данных. В главе 7 обсуждалась архивация и восстановление данных и новая служба теневого копирования (VSS), позволяющая пользователям обращаться к предыдущим версиям файлов в общих папках на серверах или восстанавливать такие папки.
- Обновление драйверов, приведшее к нестабильной работе системы. В главе 10 вы познакомились с новой возможностью «отката» драйверов Windows Server 2003. Если после обновления драйвера система работает нестабильно, драйвер и все новые настройки можно «откатить» к предыдущей версии и состоянию. Прежние драйверы принтера вернуть таким образом нельзя. Вы также узнали, что с помощью оснастки *Диспетчер устройств* (Device Manager) можно легко отключить службу, которая является причиной нестабильности. Если прикладная программа или поддерживающее ПО вызывают неполадки, удалите их с помощью приложения *Установка и удаление программ* (Add Or Remove Programs) из *Панели управления*.
- Установка драйвера или службы привела к тому, что система не запускается. В главе 10 обсуждалось использование варианта **Загрузка последней удачной конфигурации (Last Known Good Configuration),** который возвращал активный набор управления системного реестра к последнему состоянию, когда пользователь мог успешно войти в систему. Если после установки или обновления службы или драйвера система вышла из строя или не может загрузиться до окна ввода пароля, режим **Загрузка последней удачной конфигурации** позволяет восстановить версию реестра, которая использовалась до установки драйвера или службы. Кроме того, вы познакомились с различными параметрами варианта загрузки *Безопасный режим* (Safe mode), позволяющего запустить систему, частично отключив службы и драйверы. Безопасный режим часто позволяет запустить компьютер, который не загружается другим спосо-

бом, и с помощью оснастки *Диспетчер устройств* отключить, удалить или «откатить» проблемный драйвер или службу.

- Сбой дисковой подсистемы. В главе 11 обсуждалась настройка томов RAID-1 (зеркальных) и RAID-5 (с чередованием), а также восстановление после выхода из строя одного из дисков отказоустойчивого тома.

Каждый из этих вариантов предполагает, что систему можно запустить в том или ином виде. Если систему не удается запустить, вернуть ее к жизни помогут функции *Состояние системы* (System State), *Автоматическое восстановление системы* (Automated System Recovery) и *Консоль восстановления* (Recovery Console).

Состояние системы

В Windows 2000 и Windows Server 2003 в процесс архивации введено понятие *состояние системы* (System State). Данные о состоянии системы содержат важные элементы ее конфигурации, включая:

- системный реестр;
- регистрационную БД классов COM+;
- загрузочные файлы boot.ini, ntdetect.com, ntldr, bootsect.dos, ntbootdd.sys;
- системные файлы, защищенные службой *Защита файлов Windows* (Windows File Protection).

Кроме того, если установлены соответствующие службы, в состояние системы добавляется:

- БД служб сертификации на сервере сертификации;
- служба каталогов Active Directory и папка Sysvol на контроллере домена;
- информация службы кластеров на кластерном сервере;
- метабаза IIS на сервере, где установлены службы IIS.

Чтобы заархивировать состояние системы программой *Архивация данных,* включите узел System State в число копируемых объектов. Узел System State и его компоненты показан на рис. 13-1.

Если вы привыкли работать в командной строке, исполните следующую команду:

```
Ntbackup backup systemstate /J "имя_задания_архивации" ...
```

Затем укажите параметр /F для архивации в файл или параметры /T, /G, /N, /P для архивации на магнитную ленту. Полное описание параметров команды Ntbackup см. в главе 7.

При архивации состояния системы учитывайте следующие рекомендации.

- Нельзя архивировать отдельные компоненты состояния системы. Например, нельзя создать резервную копию только регистрационной БД классов COM+. Поскольку компоненты состояния системы зависят друг от друга, его можно архивировать только целиком.
- Команду Ntbackup и программу *Архивация данных* нельзя использовать для архивации состояния системы на удаленном компьютере. Их нужно запускать только на той системе, которая архивируется. Впрочем, вы можете заархивировать данные в файл на удаленном сервере, который затем можно записать на другой архивный носитель, или приобрести программы резервного копирования сторонних фирм, которые позволяют архивировать состояние системы удаленно.

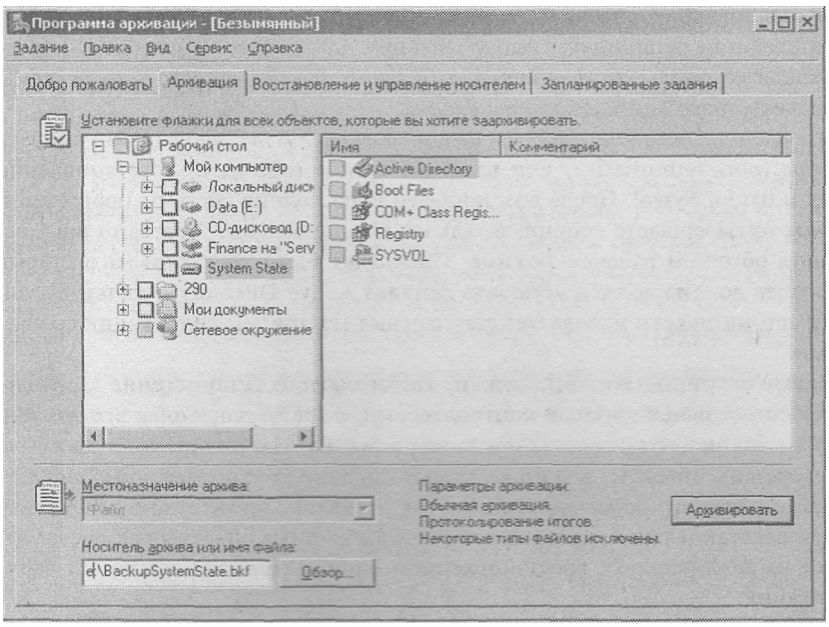


Рис. 13-1. Узел System State

- Состояние системы может содержать не все элементы конфигурации, необходимые для полного восстановления системы. Поэтому при архивации состояния системы рекомендуется создать резервные копии всех загрузочных и системных томов, а также томов данных и приложений. Состояние системы — важнейшая часть полного архива, но только часть.
- Для состояния системы автоматически применяется копирующая архивация, хотя в интерфейсе программы *Архивация данных* это может быть не отражено. Учитывайте это, выбирая, какие еще элементы нужно включить в архив.

Для восстановления состояния системы запустите программу *Архивация данных* и на вкладке **Восстановление и управление носителем (Restore And Manage Media)** установите флажок **System State.** Если компьютер неисправен, вероятно, придется восстанавливать систему с помощью ASR.

Состояние системы на контроллере домена

Состояние системы на контроллере домена включает службу каталогов Active Directory и папку Sysvol. Для резервного копирования состояния системы на контроллере домена нужно, как и на обычном компьютере, использовать программу *Архивация данных* или команду Ntbackup. Как и для любых носителей архива, важно физически защитить носитель с резервной копией Active Directory.

Для восстановления состояния системы на контроллере домена нужно перезагрузить компьютер, нажать F8, чтобы войти в меню вариантов загрузки, и выбрать *Режим восстановления служб каталогов* (Directory Services Restore Mode) — вариацию безопасного режима (см. главу 10). В этом режиме контроллер домена загружается, но не запускает службы Active Directory. Вы можете войти в систему только под учетной записью локального администратора, используя пароль режима восстановления служб каталогов, который был указан при повышении сервера до контроллера домена программой Dcpromo.

В режиме восстановления служб каталогов контроллер домена не проверяет подлинность пользователей и не реплицирует Active Directory. Кроме того, БД Active Directory и поддерживающие ее файлы не блокируются. В итоге данные о состоянии системы можно восстановить программой *Архивация данных*.

При восстановлении состояния системы на контролере домена, необходимо выбрать *непринудительное* (non-authoritative) или принудительное (обычное) восстановление Active Directory и папки Sysvol. После восстановления состояния системы программой *Архивация данных* вы завершаете непринудительное восстановление, перезагрузив контроллер домена в обычном рабочем режиме. Поскольку были восстановлены старые данные, контроллер домена должен обновить реплику Active Directory и папки Sysvol, для чего сервер автоматически использует стандартные механизмы репликации со своими партнерами.

Однако бывают ситуации, когда не нужно, чтобы после восстановления контроллер домена стал согласован с другими контроллерами, а требуется, чтобы все они перешли в то же состояние, что и восстановленная реплика. Например, если из Active Directory были удалены объекты, можно восстановить один контроллер домена из набора архивации, созданного перед удалением этих объектов. Затем нужно выполнить принудительное восстановление, которое помечает выбранные объекты как достоверные и вызывает их репликацию с восстановленного контроллера домена на его партнеры по репликаций.

Для принудительного восстановления необходимо сначала выполнить непринудительное восстановление состояние системы на контроллере домена программой *Архивация данных*. Когда вы завершите восстановление и закроете программу, ОС предложит перезагрузить компьютер. Не перезагружайте восстановленный контроллер домена, щелкнув Нет (No). Откройте окно командной строки и с помощью программы Ntdsutil отметьте всю восстановленную БД или выбранные объекты как достоверные. Информацию о служебной программе Ntdsutil и принудительном восстановлении можно получить, исполнив команду `ntdsutil /?`, либо найти в *Центре справки и поддержки*. Подробное описание процесса восстановления контроллера домена вы найдете в книге The MCSE Training Kit (Exam 70-294): Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure (Microsoft Press, 2003).

Подготовка к экзамену При подготовке к экзамену важно помнить, что состояние системы на контроллере домена можно восстановить только в *Режиме восстановления служб каталогов* (Directory Services Restore Mode). Для этого удаленные объекты Active Directory нужно с помощью программы Ntdsutil пометить как достоверные, а затем выполнить непринудительное восстановление состояния системы программой *Архивация даных*.

Автоматическое восстановление системы

Как правило, восстановление неисправного сервера — утомительная задача, подразумевающая повторную установку ОС, монтирование и каталогизацию архивной ленты и выполнение полного восстановления. *Автоматическое восстановление системы* (Automated System Recovery, ASR) значительно упрощает этот процесс. Для автоматического восстановления необходимо создать набор ASR, содержащий архив важных системных файлов, включая реестр, а также записать на дискету *список* системных файлов Windows, установленных на компьютере. Если сервер выйдет из строя, вы просто загрузите компьютер с компакт-диска Windows Server 2003 и в меню запуска выберите пункт автома-

тического восстановления системы. Для восстановления стандартных драйверов и файлов с компакт-диска Windows Server 2003 применяется дискета ASR, а остальные файлы восстанавливаются из набора архивации ASR.

Для создания набора ASR запустите программу *Архивация данных* (Backup) из группы программ *Стандартные* (Accessories) или выбрав **Пуск (Start)\Выполнить (Run)** и исполнив команду Ntbackup.exe. Если откроется окно мастера, щелкните **Расширенный режим (Advanced Mode).** Затем на вкладке **Добро пожаловать! (Welcome)** или в меню **Сервис (Tools)** щелкните **Мастер аварийного восстановления системы (ASR Wizard).** Следуйте инструкциям *Мастера подготовки аварийного восстановления системы* (Automated System Recovery Preparation). Он попросит вставить дискету емкостью 1,44 Мб, куда будет записан список системных файлов. Окно мастера ASR показано на рис. 13-2.

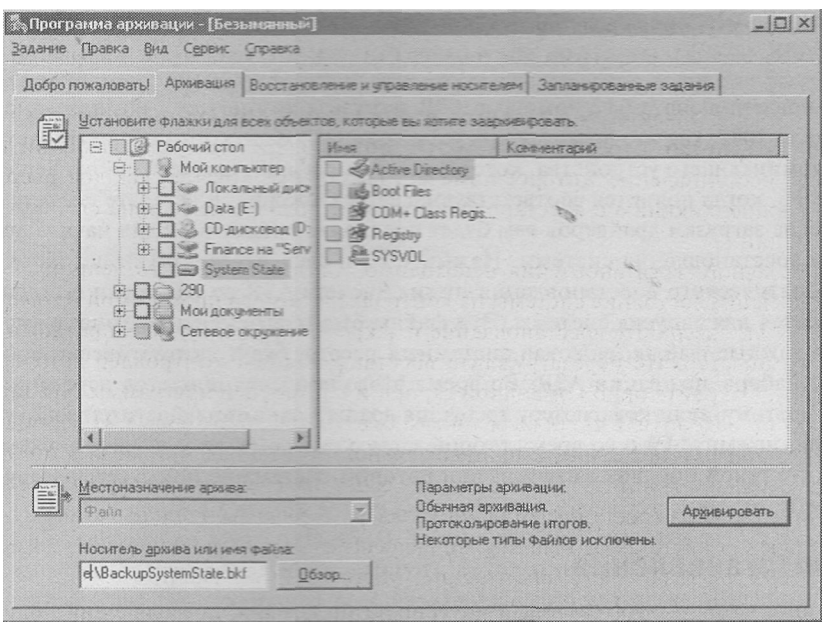


Рис. 13-2. Страница *Местоназначение архива* мастера ASR

Архив, созданный мастером ASR. содержит информацию о конфигурации каждого диска данного компьютера, копию состояния системы, а также копии файлов, включая кэш драйверов. Этот набор архивации может быть довольно большим. Для стандартной установки Windows Server 2003 объем архива ASR превысит 1 Гб.

Дискета ASR, записанная *Мастером подготовки аварийного восстановления системы,* характеризует систему на момент создания набора ASR. Подпишите набор архивации и дискету ASR и храните их вместе.

Дискета ASR содержит два системных файла: Asr.sif и Asrpnp.sif. Если у вас нет нужного дисковода, по завершении работы мастера скопируйте эти файлы из папки %Systemroot%\repair на компьютер с дисководом, а затем — на дискету. В случае потери дискеты эти два файла можно восстановить из папки %Systemroot%\repair в наборе архивации ASR. Для автоматического восстановления системы дискета ASR необходима. Если на восстанавливаемом компьютере нет дисковода для гибких дисков, вам придется его установить.

Совет Набор ASR содержит файлы, необходимые для запуска системы. Он не является исчерпывающей резервной копией всей системы. Таким образом, одновременно с набором ASR рекомендуется создавать полный архив, включающий состояние системы, системный том, приложения и, возможно, данные пользователей.

Для автоматического восстановления системы потребуются:

- установочный компакт-диск Windows Server 2003;
- набор архивации ASR;
- дискета ASR, созданная одновременно с набором архивации ASR.

Совет Кроме того, вам потребуются драйверы запоминающих устройств, которых нет в стандартном наборе Windows Server 2003. Чтобы упростить восстановление, скопируйте их на дискету ASR.

Для восстановления системы с помощью ASR загрузите компьютер с компакт-диска Windows Server 2003, как это делается при установке ОС. Если компьютеру требуется драйвер запоминающего устройства, которого нет на компакт-диске Windows Server 2003, нажмите F6, когда появится соответствующее предложение, и вставьте дискету с драйвером. После загрузки драйверов вам будет предложено нажать F2 для начала автоматического восстановления системы. Нажмите F2 и следуйте инструкциям на экране. Для автоматического восстановления нужна дискета ASR со списками файлов, которые требуются для запуска системы. Эти файлы будут загружены с компакт-диска. Остальные важные файлы, включая системный реестр, будут автоматически восстановлены из набора архивации ASR. Во время этого процесса придется перезагружать систему, поэтому, если компьютеру требуется драйвер запоминающего устройства от изготовителя, нажмите F6 и во время второй загрузки. Кроме того, выньте дискету ASR или укажите такой порядок загрузки, при котором система не попытается загружаться с дискеты.

Консоль восстановления

Консоль восстановления — это текстовый интерпретатор команд, позволяющий получить доступ к жесткому диску компьютера под управлением Windows Server 2003 для выполнения основных задач по устранению неполадок и обслуживанию системы. Когда не удается запустить ОС, консоль можно использовать для диагностики, отключения драйверов и служб, замены файлов и выполнения других процедур восстановления.

Установка консоли восстановления

Чтобы запустить консоль восстановления, загрузите компьютер с компакт-диска Windows Server 2003 и, когда появится соответствующее предложение, нажмите клавишу R. Тем не менее, когда система выходит из строя, необходимо восстановить ее как можно быстрее и не тратить время на поиски компакт-диска и утомительно долгий процесс загрузки. Поэтому рекомендуется заранее установить консоль восстановления.

Чтобы установить консоль восстановления, вставьте компакт-диск Windows Server 2003 и в командной строке введите *буква_привода_cd-rom*: \I386\winnt32 /cmdcons. Мастер установит консоль, занимающую 8 Мб, в скрытую папку Cmdcons, и изменит файл boot.ini так, чтобы консоль восстановления можно было запустить при загрузке системы.

Удаление консоли восстановления

Если вы захотите удалить консоль восстановления, придется удалить «суперскрытые» файлы и папки. Откройте *Проводник* и в меню **Сервис (Tools)** выберите **Свойства папки (Folder Options).** Перейдите на вкладку **Вид (View),** установите флажок **Показывать скрытые файлы и папки (Show Hidden Files and Folders),** снимите флажок **Скрывать защищенные системные файлы (Hide Protected Operating System Files),** щелкните OK и, если появится предупреждение об отображении защищенных системных файлов, щелкните **Да (Yes).**

Удалите папку Cmdcons и файл Cmldr из корня системного диска. Затем удалите параметр запуска консоли восстановления из файла Boot.ini. Запустите приложение *Система* (System) из *Панели управления,* перейдите на вкладку **Дополнительно (Advanced),** щелкните кнопку **Параметры (Settings)** в группе Загрузка и **восстановление (Startup And Recovery)** и в появившемся окне **Загрузка** и восстановление **(Startup And Recovery)** щелкните кнопку **Правка (Edit).** Откроется *Блокнот* (Notepad) с файлом Boot.ini. Удалите запись, которая касается консоли восстановления и выглядит так:

```
c:\cmdcons\bootsect.dat="Microsoft Windows Recovery Console"/cmdcons
```

Сохраните и закройте файл Boot.ini.

Работа в консоли восстановления

После установки консоли восстановления можно перезагрузить систему и в меню загрузки выбрать Microsoft Windows Recovery Console. Если консоль не была установлена или не запускается, загрузитесь с компакт-диска Windows Server 2003 и в окне **Вас приветствует программа установки (Welcome To Setup)** нажмите клавишу R, чтобы выбрать пункт Repair. Загрузка с компакт-диска занимает значительно больше времени, **но** в итоге интерфейс консоли восстановления идентичен интерфейсу консоли, установленной на локальной системе.

После запуска консоли восстановления вам предложат выбрать установку Windows, в которую нужно войти (рис. 13-3). Затем нужно будет ввести пароль локальной учетной записи *Администратор* (Administrator), который на контроллере домена настраивается на странице **Пароль режима восстановления служб каталогов (Directory Services Restore Mode Password)** мастера установки Active Directory.

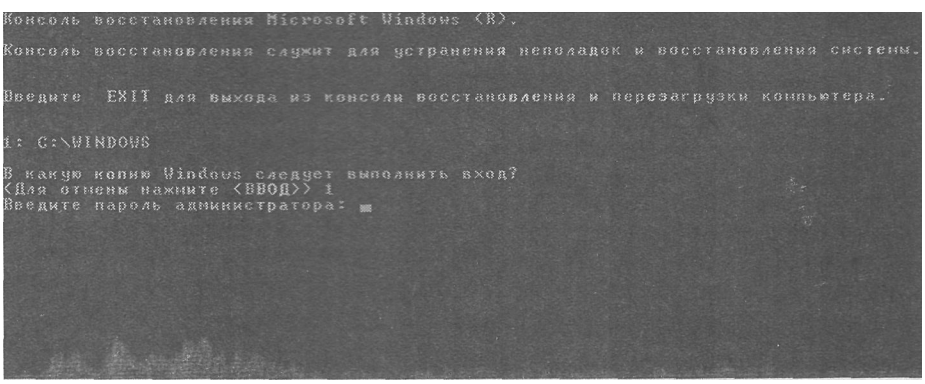


Рис. 13-3. Консоль восстановления

В командной строке консоли можно ввести help, чтобы просмотреть список команд, доступных в консоли, или help *имя_команды,* чтобы получить информацию о конкрет-

ной команде. Большинство этих команд знакомы вам по обычной среде командной строки. Некоторые из них заслуживают особого внимания.

- **Listsvc.** Отображает драйверы и службы, перечисленные в реестре, а также параметры их запуска. Это удобный способ узнать короткое имя службы или драйвера перед выполнением команд Enable и Disable.
- **Enable/Disable.** Управляет запуском службы или драйвера. Если служба или драйвер не позволяют ОС успешно запуститься, отключите проблемный компонент командой Disable, а затем перезагрузите систему и исправьте или удалите его.
- Diskpart. Позволяет создавать и удалять разделы, используя интерфейс, похожий на текстовую часть программы Setup. Затем можно настроить файловую систему раздела командой Format.
- **Bootcfg.** Позволяет управлять меню запуска.

Консоль восстановления имеет ряд ограничений, продиктованных соображениями безопасности. Эти ограничения можно изменить с помощью комбинации политик — они размещены в узле **Конфигурация компьютера (Computer Configuration)\Конфигурация Windows (Windows Settings)\Параметры безопасности (Security Settings)\Локальные политики (Local Policies)\Параметры безопасности (Security Options)** консоли *Локальная политика безопасности* (Local Computer Policy) — и переменных среды консоли восстановления.

- **Доступ к каталогу.** Разрешает просматривать файлы только в корневом каталоге, в папках %Windir% и \Cmdcons. Это ограничение можно отключить, настроив политику *Консольвосстановления:разрешитькопированиедискетидоступковсемдискам и папкам* (Allow Floppy Copy And Access To All Drives And All Folders), а также с помощью команды `set AllowAllPaths = true`. При выполнении команды set следите, чтобы по обеим сторонам от знака равенства стояли пробелы.
- **Копирование файлов.** Вы можете копировать файлы только на локальный жесткий диск, но не с него. Используйте указанную выше политику и команду `set AllowRemovableMedia = true`. При выполнении команды set следите, чтобы по обеим сторонам от знака равенства стояли пробелы.
- **Метасимволы.** Нельзя использовать метасимволы, например звездочку, для удаления файлов. Используйте указанную выше политику, а затем в консоли восстановления исполните команду `set AllowWildCards = true`. При выполнении команды set следите, чтобы по обеим сторонам от знака равенства стояли пробелы.

Лабораторная работа. **Восстановление после сбоя системы**

На этой лабораторной работе вы заархивируете состояние системы и создадите набор ASR, а также установите и примените консоль восстановления для устранения неполадок драйвера или службы. Наконец, если у вас есть второй жесткий диск, вы выполните автоматическое восстановление неисправного сервера.

Упражнение 1. Архивация состояния системы

1. Войдите на Server01 как *Администратор* (Administrator).
2. Запустите программу *Архивация данных* (Backup).
3. Если откроется окно мастера, щелкните **Расширенный режим (Advanced Mode).**

4. Перейдите на вкладку **Архивация (Backup)** и **установите флажок System State.** Также щелкните метку **System State,** чтобы просмотреть список компонентов состояния системы на другой панели диалогового окна.
5. Введите имя файла архивации, например C:\SystemState. bkf.
6. Запустите архивацию.
7. По завершении резервного копирования оцените размер архива состояния системы. Каков размер этого файла?

Упражнение 2. Создание набора ASR

Для выполнения этого упражнения требуется чистая дискета и около 1,5 Гб свободного места на жестком диске. Если на ServerOl установлен второй жесткий диск, сохраните на нем резервную копию, чтобы выполнить автоматическое восстановление системы в упражнении 4.

1. Запустите программу *Архивация данных* (Backup). Если откроется окно мастера, щелкните **Расширенный режим (Advanced Mode).**
2. Щелкните **Мастер аварийного восстановления системы (Automated System Recovery Wizard)** или в меню **Сервис (Tools)** выберите **Мастер аварийного восстановления системы (ASR Wizard).**
3. Следуйте инструкциям на экране. Заархивируйте данные в файл ASRBackup.bkf на диске C: или на втором жестком диске, если он у вас есть.
4. По завершении резервного копирования оцените размер файла ASRBackup.bkf. Каков его размер? Сравним ли он с размером архива состояния системы?

Упражнение 3. Установка и использование консоли восстановления

1. Вставьте компакт-диск Windows Server 2003 в привод CD-ROM.
2. Щелкните **Пуск (Start)\Выполнить (Run)** и в поле **Открыть (Open)** введите команду

   D:\i386\winnt32.exe/cmdcons

   где D: — буква диска привода CD-ROM. Консоль восстановления будет установлена на локальный жесткий диск.
3. Чтобы сымитировать службу, вызывающую неполадки, откройте консоль *Службы* (Services) из группы программ *Администрирование* (Administrative Tools). Найдите **Службу сообщений (Messenger).** Дважды щелкните ее и в списке **Тип запуска (Startup Type)** выберите **Авто (Automatic).**
4. Перезагрузите сервер.
5. Когда появится меню загрузки, выберите вариант **Microsoft Windows Recovery Console.**
6. В ответ на запрос нажмите 1, чтобы выбрать установку Windows Server 2003.
7. Введите пароль локальной учетной записи *Администратор* (Administrator).
8. Когда появится окно ввода команд консоли восстановления (по умолчанию C:\Windows>), введите help, чтобы просмотреть список команд.
9. Введите команду listsvc, чтобы просмотреть список служб и драйверов. Заметьте: краткое имя многих служб не совпадает с полным. Тем не менее, краткое имя службы Messenger такое же — Messenger. Убедитесь, что она запускается автоматически.
10. Введите disable messenger, чтобы отключить эту службу. На экране появится сообщение об успешном выполнении команды и сведения об исходной конфигурации данной службы (в нашем случае — SERVICE_AUTO_START). Рекомендуется всегда

запоминать это значение, чтобы после устранения неполадки можно было вернуть службу в первоначальное состояние.

11. Чтобы выйти из консоли восстановления, введите `exit` и нажмите Enter.

Упражнение 4. Автоматическое восстановление системы средствами ASR

Внимание! Для выполнения этого упражнения требуется второй жесткий диск с архивом ASR, который был создан на упражнении 2. В ходе этого упражнения все данные на жестком диске, содержащем системный и загрузочный разделы, будут удалены. Пропустите это упражнение, если не хотите потерять нужные данные.

1. Выключите компьютер.
2. Загрузите компьютер и войдите в BIOS. Убедитесь, что система поддерживает загрузку с компакт-диска.
3. Вставьте компакт-диск Windows Server 2003 в привод CD-ROM.
4. Перезагрузите ServerOl. В ответ на запрос нажмите клавишу, чтобы загрузить компьютер с компакт-диска.
5. В текстовом режиме программы установки нажмите F2, чтобы запустить автоматическое восстановление системы. Еще раз нажмите F2.
6. Вам будет предложено вставить дискету ASR. Вставьте дискету, созданную на упражнении 2, и нажмите любую клавишу для продолжения.
7. Система подготовится к автоматическому восстановлению системы, после чего будет загружена минимальная конфигурация ОС. На это потребуется несколько минут.
8. Наконец, появится экран программы установки Windows Server 2003.
9. Программа установки Windows Server 2003 разбивает на разделы и форматирует диск, копирует файлы, инициализирует конфигурацию Windows и готовит систему к перезагрузке.
10. Выньте дискету из дисковода и перезагрузите компьютер.

    Установка продолжится. После завершения установки компьютер будет восстановлен в свое предыдущее состояние.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Вы настраиваете задание архивации на компьютере под управлением Windows Server 2003 и намерены архивировать реестр, загрузочные файлы и регистрационную БД классов COM+. Какой вариант архивации следует выбрать?
   a. %Windir%.
   b. %Systemroot%. •
   c. Состояние системы.
   d. Ничего из перечисленного. Реестр заархивировать нельзя.
2. Вы установили сканер на компьютере под управлением Windows Server 2003. После этого ОС перестала загружаться. Каким максимально щадящим методом следует в первую очередь попробовать восстановить систему?

a. Автоматическое восстановление системы.
b. Консоль восстановления.
c. Безопасный режим загрузки.
d. Режим восстановления служб каталогов.

3. Жесткий диск на сервере Windows Server 2003 вышел из строя. Вы заменили диск, загрузили систему, инициализировали новый диск и создали на нем новый том NTFS. Теперь вы намерены восстановить данные, которые хранились на старом диске, из последнего архива. Как следует восстанавливать эти данные?
   a. Скопировать данные на диск с помощью консоли восстановления.
   b. Запустить мастер восстановления из программы *Архивация данных*.
   c. Восстановить данные, используя архив ASR.
   d. Выбрать вариант **Загрузка последней удачной** конфигурации **(Last Known Good Configuration)** в безопасном **режиме,** чтобы настроить новый диск.
4. Файловый сервер в вашей сети перестал загружаться. Испробовав все способы, вы решили восстановить систему с помощью ASR. Вы создали архив ASR сразу после установки Windows Server 2003 и еше один — два месяца назад после установки драйвера устройства. Каждую неделю вы выполняете полную архивацию файлов данных. Какие данные будут восстановлены из архива ASR? (Выберите все подходящие варианты.)
   a. Файлы данных двухмесячной давности.
   b. Файлы данных на момент последней полной архивации.
   c. Конфигурация диска.
   d. Операционная система.
   e. Состояние системы двухмесячной давности.
   f. Состояние системы на момент последней полной архивации.

Резюме

- Состояние системы включает реестр, загрузочные файлы, регистрационную БД классов COM+ и другие важные системные файлы, характерные для служб. Рекомендуется архивировать состояние системы вместе с системным и загрузочным томами.
- Автоматическое восстановление системы напоминает ее установку. После возвращения компьютера в рабочее состояние запускается процесс восстановления файлов из набора архивации ASR. ASR применяется, когда не удается восстановить систему с помощью других, более щадящих методов, например безопасного режима загрузки или консоли восстановления.
- Консоль восстановления — это текстовый интерпретатор команд, позволяющий получить доступ к жесткому диску компьютера под управлением Windows Server 2003.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Состояние системы можно заархивировать программой *Архивация данных* (Backup) или из командной строки, но только локально. Нельзя создать резервную копию состояния системы На удаленном компьютере. Впрочем, можно заархивировать состояние системы локального компьютера в файл на удаленном компьютере, а затем скопировать его на другой архивный носитель.
- Для восстановления системы на контроллере домена нужно перезагрузить сервер в *Режиме восстановления служб каталогов* (Directory Services Restore Mode). Состояние системы включает службу каталогов Active Directory. Восстанавливая состояние системы на контроллере домена, вы применяете непринудительное восстановление, а затем контроллер домена использует стандартные механизмы репликации, чтобы актуализировать свое состояние согласно другим контроллерам. Если вы намерены реплицировать восстановленные объекты на другие контроллеры, нужно использовать служебную программу Ntdsutil для выполнения принудительного восстановления перед перезагрузкой контроллера в обычном рабочем режиме.
- Автоматическое восстановление системы использует каталог системных файлов, хранимый на дискете ASR, для восстановления файлов с компакт-диска Windows Server 2003, плюс полный архив ASR. Набор архивации и дискета ASR создаются мастером ASR в программе *Архивация данных*. Для автоматического восстановления системы загрузите сервер с компакт-диска Windows Server 2003 и, когда появится соответствующий запрос, нажмите F2.
- Консоль восстановления позволяет устранять причины некоторых сбоев системы. С ее помощью вы можете заменить системные файлы и отключить проблемные драйверы или службы, а также выполнять некоторые другие задачи по обслуживанию системы. Консоль восстановления можно запустить с компакт-диска Windows Server 2003 или установить на жесткий диск сервера, исполнив команду `winnt32 /cmdcons`.

Основные термины

Состояние системы ~ System State — набор важных компонентов системы, включая реестр, регистрационную БД классов COM+ и загрузочные файлы. Состояние системы можно заархивировать программой *Архивация данных* (Backup) или командой Ntbackup. Нельзя архивировать его отдельные компоненты.

Автоматическое восстановление системы ~ Automated System Recovery, ASR — новая функция, заменившая процесс аварийного восстановления (Emergency Repair) из предыдущих версий Windows. Автоматическое восстановление системы возвращает компьютер к работе путем повторной установки ОС и восстановления состояния системы из набора архивации ASR.

Консоль восстановления ~ Recovery Console — служебная программа, предоставляющая из командной строки доступ к системным файлам и подмножеству команд для восстановления вышедшей из строя системы.

Вопросы и ответы

Занятие 1. Закрепление материала

1. Вы настраиваете задание архивации на компьютере под управлением Windows Server 2003 и намерены архивировать реестр, загрузочные файлы и регистрационную БД классов COM+. Какой вариант архивации следует выбрать?
   a. %Windir%.
   b. %Systemroot%.
   c. Состояние системы.
   d. Ничего из перечисленного. Реестр заархивировать нельзя.

   Правильный ответ: c
2. Вы установили сканер на компьютере под управлением Windows Server 2003. После этого ОС перестала загружаться. Каким максимально щадящим методом следует в первую очередь попробовать восстановить систему?
   a. Автоматическое восстановление системы.
   b. Консоль восстановления.
   c. Безопасный режим загрузки.
   d. Режим восстановления служб каталогов.

   Правильный ответ: c.
3. Жесткий диск на сервере Windows Server 2003 вышел из строя. Вы заменили диск, загрузили систему, инициализировали новый диск и создали на нем новый том NTFS. Теперь вы намерены восстановить данные, которые хранились на старом диске, из последнего архива. Как следует восстанавливать эти данные?
   a. Скопировать данные на диск с помощью консоли восстановления.
   b. Запустить мастер восстановления из программы *Архивация данных*.
   c. Восстановить данные, используя архив ASR.
   d. Выбрать вариант **Загрузка последней удачной конфигурации (Last Known Good Configuration)** в безопасном режиме, чтобы настроить новый диск.

   Правильный ответ: b.
4. Файловый сервер в вашей сети перестал загружаться. Испробовав все способы, вы решили восстановить систему с помощью ASR. Вы создали архив ASR сразу после установки Windows Server 2003 и еще один — два месяца назад после установки драйвера устройства. Каждую неделю вы выполняете полную архивацию файлов данных. Какие данные будут восстановлены из архива ASR? (Выберите все подходящие варианты.)
   a. Файлы данных двухмесячной давности.
   b. Файлы данных на момент последней полной архивации.
   c. Конфигурация диска.
   d. Операционная система.
   e. Состояние системы двухмесячной давности.
   f. Состояние системы на момент последней полной архивации.

   Правильный ответ: c, d, e.

Предметный указатель

Г

Д

Ж

З

И

Л

О

Т

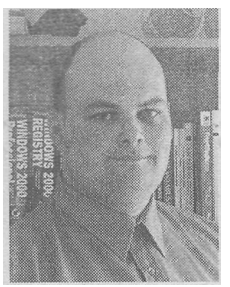
У

Ф

Ц

Э

ДЭН Холме (Dan Holme) Выпускник Йельского университета и школы Thunderbird, Американской высшей школы международного менеджмента (American Graduate School of International Management), Дэн проработал 10 лет в качестве консультанта и инструктора, предоставляя решения десяткам тысяч ИТ-специалистов наиболее известных организаций и корпораций по всему миру. Его клиентами были AT&T. Compaq, HP. Boeing, Home Depot и Intel, а в последнее время он принимал участие в проектировании и развертывании Active Directory на таких предприятиях, как Raytheon, ABN AMRO, Johnson & Johnson, Los Alamos National Laboratories и General Electric. Дэн — директор отдела обучения компании Intelliem. которая специализируется на повышении производительности труда ИТ-специалистов и конечных пользователей, предлагая передовые, легко адаптируемые решения, которые интегрируют конкретную среду и конфигурацию клиентов с услугами в области управления знаниями и подготовки и повышения квалификации специалистов (info@intiiem.com). Дэн выражает свою бесконечную любовь и благодарность тем, без кого ему было бы так трудно: Lyman. Barb и Dick. Bob и Joni, Stan и Marylyn и Sondra, Mark, Kirk, John, Beth, Dan и June, Lena, а также всем остальным членам своей безумной команды.



Орин Томас (Orin Thomas) Орин — писатель, редактор и системный администратор, работающий на консультационном Web-узле Certtutor.net. специализирующемся на вопросах сертификации. Он работал в самых разных сферах ИТ-индустрии: от поддержки работы сети низшего уровня до системного администратора одной из крупнейших австралийских компаний. Орин опубликовал несколько статей в технических изданиях, а также принимал участие в создании руководства «The Insider's Guide to IT Certification» («ИТ-сертификация: взгляд изнутри»). Он имеет сертификаты MCSE, CCNA, CCDA и Linux+. Также он имеет степень почетного бакалавра наук Мельбурнского университета и в настоящее время близок к получению звания доктора философских наук. Орин хотел бы поблагодарить свою жену Оксану за красоту и любовь, о которой он даже не смел мечтать, и сына Руслана, быть отцом которого так легко. Помимо этого, Орин выражает благодарность своим друзьям и близким: маме, Mick, Lards, Gillian, Lee, Neil, Will, Jon, Alexander, Irina, Stas и Kasia, а также всей команде преподавателей Certtutor.net.

Холме Дэн, Томас Орин

Управление и поддержка Microsoft Windows Server 2003

Учебный курс MCSA/MCSE

Перевод с английского под общей редакцией А. В. Иванова
Редактор С. В. Дергачев
Компьютерный дизайн и подготовка иллюстраций Е. Р. Данилов
Технический редактор Н. Г. Тимченко
Дизайнер обложки Е. В. Козлова

Главный редактор А. И. Козлов

Подготовлено к печати издательством «Русская Редакция»
123317. Москва, ул. Антонова-Овсеенко, д. 13. Тел.: (095) 256-5120, тел./факс: (095) 256-4541.
e-mail: info@rusedit.ru, http://www.rusedit.ru

РУССКАЯ РЕДАКЦИЯ

Подписано в печать 07.07.2004 г. Тираж 3000 экз. Формат 70x100/16. Физ. п. л. 28
Заказ №3347

При участии ООО ПФ «Сашко»

Отпечатано с готовых диапозитивов во ФГУП ИПК «Ульяновский Дом печати»
432980, г. Ульяновск, ул. Гончарова. 14

Управление и поддержка Microsoft Windows Server 2003

Учебный курс MCSA/MCSE

Сертификационный экзамен **70-290**

Официальные учебные пособия Microsoft — гарантия вашей квалификации!

Освоив материалы этого курса, вы научитесь устанавливать и настраивать сервер на базе Microsoft Windows Server 2003 и подготовитесь к сдаче экзамена 70-290 «Managing and Maintaining a Microsoft Windows Server 2003 Environment» по программам сертификации MCSA и MCSE.

В этой книге:

- установка Microsoft Windows Server 2003 и службы каталогов Active Directory;
- удаленное управление серверами и удаленная помощь пользователям;
- создание и оптимальная настройка учетных записей пользователей, групп и компьютеров;
- настройка разрешений файловой системы и общих ресурсов;
- планирование и реализация стратегий резервного копирования;
- управление принтерами, типичными аппаратными устройствами и драйверами;
- работа с дисковой памятью;
- мониторинг работы серверов;
- реализация стратегий аварийного восстановления.

На прилагаемом компакт-диске:

- демонстрационная версия экзаменационного теста;
- электронные книги на английском языке;
- раздел «Подготовка к экзамену», сгруппированный по реальным темам экзамена;
- приложение «Сервер терминалов» и словарь терминов.

Windows Server System

Microsoft Learning

ISBN 5-7502-0201-1

Сайт издательства: **www.rusedit.ru**

РУССКАЯ РЕДАКЦИЯ