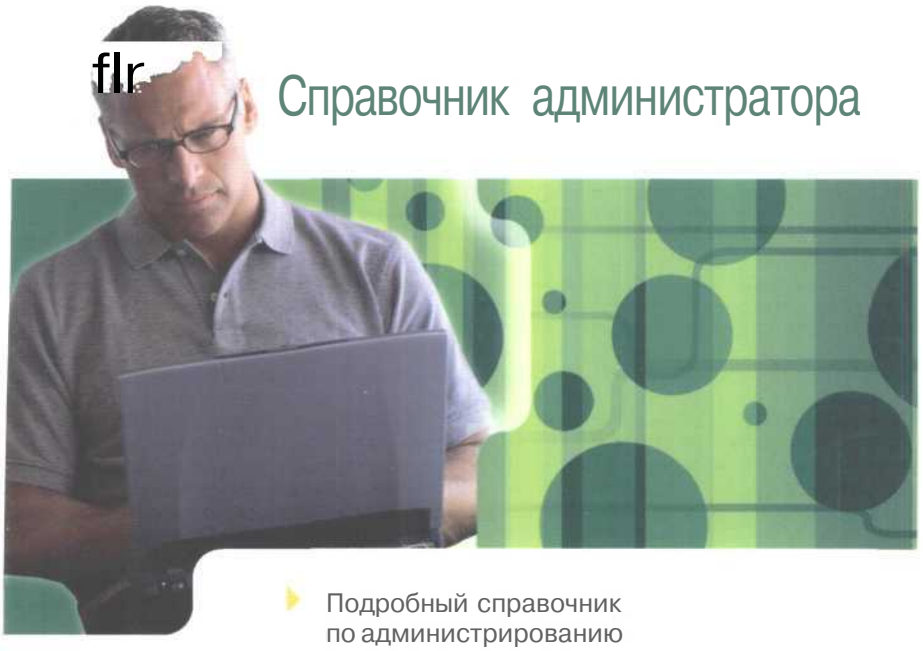
Уильям Р. **Станек**

Microsoft® Windows® Server 2003

Справочник администратора



- Подробный справочник по администрированию Microsoft Windows Server 2003
- Таблицы, пошаговые инструкции, подробный предметный указатель

IT Professional

РУССКАЯ РЕДАКЦИЯ

Microsoft®

William R. Stanek

Microsoft® Windows® Server 2003

Administrator's **Pocket** Consultant

Microsoft Press

Уильям Р. Станек

Microsoft®
Windows®

Server 2003

Справочник администратора

Москва 2004

РУССКИ РЕДАКЦИЯ

УДК 004.738.5
ББК 32.973.202
С 76

Уильям Р. Станек

С76 Microsoft Windows Server 2003. Справочник администратора/ Пер. с англ. — М.: Издательско-торговый дом «Русская Редакция», 2003. - 640 с.: ил.

ISBN 5-7502-0245-3

Данная книга — краткий и исчерпывающий справочник для администраторов Microsoft Windows Server 2003. Здесь рассматриваются все основные вопросы, связанные с выполнением стандартных задач администрирования сервера и домена Microsoft Windows Server 2003, в том числе управление службой каталогов Active Directory, основными сетевыми службами (DHCP, WINS и DNS), учетными записями пользователей и групп. Отдельно обсуждается работа с оборудованием, в частности с базовыми и основными жесткими дисками, RAID-массивами и принтерами, а также устранение неполадок этих компонентов. Описаны все основные новшества Microsoft Windows Server 2003,

Книга адресована системным администраторам Microsoft Windows Server 2003, опытным пользователям, которым приходится выполнять административные функции, а также администраторам, переходящим на Windows Server 2003 с других платформ.

Издание богато иллюстрировано, состоит из 20 глав, оглавления и предметного указателя.

УДК 004.738.5
ББК 32.973.202

ISBN 0-7356-1354-0 (англ.)
ISBN 5-7502-0245-3

Оглавление

Благодарности

Работа над этой книгой доставила мне массу удовольствия, будучи вместе с тем довольно трудоемкой. Вы сами убедитесь, что этот справочник сильно отличается от предшествующих изданий, и мне пришлось порядком потрудиться, чтобы сделать его максимально точным. Окончательную версию никак нельзя было назвать карманным справочником, а ведь задумывалась эта книга именно так! Изначально планировалось сделать ее такой, чтобы было удобно носить с собой — проникнувшись этой мыслью, я вернулся к началу книги и переработал текст, сохранив в нем лишь ключевые сведения об администрировании Windows Server 2003. Результат моих стараний вы держите в руках — на сегодняшний день это один из наиболее практичных и компактных справочников по Windows Server 2003.

Приятно видеть, как выработанные тобой методики и приемы превращаются в печатное слово и становятся достоянием многих. Но человек не всесилен, и я не написал бы эту книгу без помощников, которых я считаю своим долгом упомянуть. Я уже неоднократно писал, что команда Microsoft Press выше всяких похвал. Пока я работал над книгой, Джули Миллер (Julie Miller) помогала мне не сбиться с пути и обеспечивала всем, что требовалось для работы. Она руководила процессом создания книги со стороны Microsoft Press, причем неизменно была на высоте. Не могу забыть и такого профессионала, как Эрин Конафтон (Erin Connaughton) из корпорации nSight. Я высоко ценю их умение, тщание и внимание к малейшим деталям!

К несчастью для автора (и к счастью для читателей) написанием книги процесс публикации не ограничивается. Рукопись необходимо тщательно редактировать. Нигде не приходилось мне встречать столь качественного издательского процесса, как в Microsoft Press, — а я повидал многих издателей. Особых благодарностей заслужили Джули и Эрин. Техническим редактором книги стал Тоби Эндрюс (Toby Andrews).

Работа с ним была настоящим удовольствием. Я благодарен за сотрудничество редактору Джозефу Густатису (Joseph Gustaitis). Он редактировал все написанные мною карманные справочники, и я никогда не жалел об этом!

Чем ближе мы были к окончанию работы над книгой, тем больше людей нам помогало. Огромное спасибо Майклу Болинджеру (Michael Bolinger), Джеффу Коху (Jeff Koch) и Джулиане Элдус Эткинсон (Juliana Aldous Atkinson). Их сосредоточенность, увлеченность и мастерство изрядно помогли мне. В тяжелые времена Джим Крамер (Jim Kramer) помогал с макетированием, а Джиллиан Андерсон (Gillian Anderson) содействовала с редактированием текста. Без них книга не получилась бы.

Надеюсь, я никого **не** забыл, но если **все-таки забыл, то не нарочно.** *Честно-честно!* ;-)

Введение

Книга «Microsoft Windows Server 2003. Справочник администратора» задумана как краткий и исчерпывающий источник информации для администраторов Microsoft Windows Server 2003, руководство, которое в любой момент должно быть под рукой. В этой книге есть все, что нужно для успешного решения базовых административных задач на серверах, работающих под управлением Windows Server 2003. Поскольку я постарался вместить максимум информации в небольшой формат, вам не придется перелистывать сотни страниц в поисках нужных сведений. Вы прочитаете только то, что нужно для работы.

Говоря коротко, эта книга — источник, к которому вы обращаетесь за разрешением любых вопросов, связанных с повседневным администрированием Windows Server 2003. В ней рассказано об основных процедурах и часто решаемых задачах, описаны типичные примеры и приведены списки параметров, пусть не всегда полные, но достаточно представительные. Моя цель — сочетание краткости и полноты: только так удается создать руководство к действию, а не тысячестраничный том и не стостраничную памятку. Надеюсь, что мой справочник поможет вам легко и быстро справиться с повседневными задачами и с реализацией современных технологий Windows — Active Directory, Dynamic Host Configuration Protocol (DHCP), Windows Internet Name Service (WINS) и Domain Name System (DNS).

Кому адресована эта книга

Справочник администратора Microsoft Windows Server 2003 охватывает все версии этой операционной системы (ОС) — Standard, Enterprise, Web и Datacenter. Книга адресована:

- администраторам Windows Server 2003;
- опытным пользователям, временами исполняющим функции администратора;

- администраторам, переходящим на Windows Server 2003 с предыдущих версий Windows;
- администраторам, переходящим на Windows Server 2003 с других платформ.

Чтобы не отвлекаться на бесконечные пояснения, я подразумевал, что вы знакомы с работой компьютерных сетей, разбираетесь в основах Windows Server 2003 и что ОС Windows Server 2003 уже установлена на вашем компьютере. Иными словами, в книге нет глав об архитектуре Windows Server 2003, о ее установке и о процессе запуска и завершения работы. С другой стороны, я рассказал о настройке Windows Server 2003, групповых политиках, безопасности, аудите, архивировании данных, восстановлении системы и многом другом. Я полагаю, что вы хорошо знакомы с командами ОС Windows и с ее интерфейсом. Если все же чего-то вы не знаете, обратитесь к документации Windows.

Структура книги

Эта книга — справочник, а не учебник, поэтому ее основу составляют решения конкретных задач, а не описание компонентов ОС.

Важная черта справочника — легкость, с которой в нем удается отыскать нужную информацию. В эту книгу включены развернутое оглавление и подробный предметный указатель. Выполняемые задачи расписаны по пунктам и снабжены списками параметров, таблицами и ссылками на другие разделы книги. Книга разделена на части и главы. Каждая часть начинается с краткого описания рассматриваемых в ней вопросов.

Часть I посвящена основам администрирования Windows Server 2003. В главе 1 приводится обзор административных инструментов, приемов и концепций Windows Server 2003. Глава 2 посвящена управлению системами Windows Server 2003. В главе 3 описана работа со службами, процессами и событиями. Глава 4 посвящена групповым политикам и автоматизации типичных административных задач, Из главы 5 вы узнаете, как работать со службами поддержки и удаленным рабочим столом.

Часть II посвящена администрированию учетных записей пользователей, компьютеров и групп. Глава 6 познакомит вас со структурой Active Directory и основами работы с домена-

ми Active Directory. В главе 7 рассматриваются основы администрирования Active Directory. Вы научитесь управлять учетными записями компьютеров, контроллерами домена и организационными подразделениями. В главе 8 объясняется, как применять системные учетные записи, встроенные группы и возможности, а также неявные группы. В таблицах все эти компоненты подробно описаны. Созданию учетных записей пользователей и групп посвящена глава 9, а из главы 10 вы узнаете, как управлять этими записями.

В части III рассматриваются вопросы управления данными. Глава 11 начинается описанием процессов установки жестких дисков и разбиения их на разделы. Далее там же рассмотрены вопросы обслуживания дисков файловых систем — дефрагментирование, сжатие, шифрование и т. д. В главе 12 вы найдете сведения по управлению наборами томов и массивами RAID, а также рекомендации по восстановлению дисков. Глава 13 посвящена управлению файлами и папками. Из главы 14 вы узнаете, как открыть общий доступ к файлу, папке или диску для пользователей сети и Интернета, а также о безопасности и аудите объектов Active Directory. Архивация данных описана в главе 15.

Более сложные административные задачи, связанные с работой сети, рассмотрены в части IV. В главе 16 приводится обзор установки, настройки и тестирования параметров TCP/IP на системах Windows Server 2003 — от установки сетевой платы до подключения компьютера к домену Windows Server 2003. Глава 17 посвящена проблемам печати: диагностике принтерных проблем, установке и настройке сетевых и локальных принтеров, а также серверов печати. В главах 18, 19 и 20 рассмотрены ключевые службы Windows Server 2003: DHCP, WINS и DNS.

Условные обозначения

Чтобы текст было удобнее читать, я ввел в него несколько дополнительных элементов. Коды и листинги набраны моноширинным шрифтом. Команда или текст, которые нужно ввести с клавиатуры, выделены полужирным начертанием. Сетевые адреса и новые термины выделяются *курсивом*. Дополнительные сведения приводятся в следующих разделах:

Примечание — комментарий к описываемой процедуре или технологии;

Совет — подсказка или рекомендация, связанная с описываемым действием;

Внимание! — предупреждение о потенциальных проблемах.

Я искренне надеюсь, что книга «Microsoft Windows Server 2003. Справочник администратора» поможет вам администрировать системы Windows Server 2003 с максимальной быстротой и легкостью. Я буду счастлив, если вы поделитесь со мною своими впечатлениями, прислав их по адресу *williamstanek@aol.com,* Спасибо!

Поддержка

Издательский коллектив приложил все усилия, чтобы обеспечить точность информации в книге. Список замеченных опечаток, если таковые окажутся, вы найдете по адресу *http://wwvMicrosoft.com/rnspress/support/defauit.asp*.

Ваши замечания, вопросы и предложения по этой книге направляйте в Microsoft Press. Наш почтовый адрес:

Microsoft Press

Attn: Editor, Microsoft Windows Server 2003 Administrator's Pocket Consultant

One Microsoft Way

Redmond, WA 98052-6399

Электронная почта:

mspinput@microsoft.com

Обратите внимание, что поддержка продуктов по указанным адресам не осуществляется. Сведения о поддержке продуктов вы найдете по адресу *http://www.microsoft.com/support.*

Об авторе

За плечами Уильяма Р. Станека (William R. Stanek) 20-летний опыт программирования и разработки приложений, и сейчас он считается одним из ведущих экспертов в области компьютерных технологий. Его советы помогли миллионам программистов, разработчиков и сетевых инженеров из разных стран. На счету Уильяма немало наград за писательский труд — он написал более двух десятков книг о компьютерах. В том числе «Microsoft Windows XP Professional. Справочник администратора», «Microsoft Windows 2000. Справочник администратора», «Microsoft Windows Server 2003. Справочник администратора» и «Microsoft IIS 6.0 Administrator's Pocket Consultant».

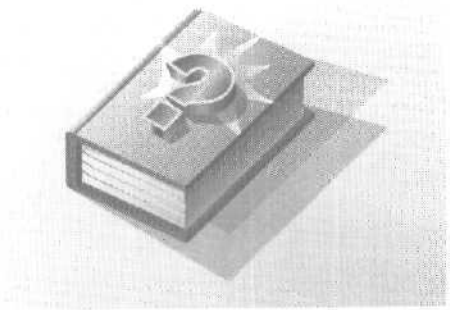
С 1991 г. Станек участвовал в разработке коммерческих Интернет-проектов. Его бизнес-качества и профессиональный опыт сформировались за 11 лет армейской службы. Уильям обладает большим опытом разработки серверных технологий, шифрования и Интернет-решений. Он написал массу технических статей и курсов лекций по проблемам широкого диапазона, и весьма популярен как компьютерный эксперт, имеющий опыт практической работы.

Станек имеет степень магистра информационных систем с отличием и степень бакалавра информатики *magna cum laude*. Он гордится участием в боевых действиях в Персидском заливе в составе экипажа самолета радиоэлектронной борьбы. В его послужном списке несколько боевых вылетов в Ирак и девять медалей за воинскую службу, включая одну из высших авиационных наград США — Крест Военно-Воздушных Сил с отличием. В настоящее время Станек с женой и детьми живет на севере Тихоокеанского побережья США.

Часть I

Основы администрирования Windows Server 2003

Часть I посвящена основам администрирования Microsoft Windows Server 2003. В главе 1 дан обзор понятий, средств и методик администрирования Windows Server 2003. В главе 2 рассматриваются средства управления системами Windows Server 2003. В главе 3 говорится о мониторинге служб, процессов и событий. Глава 4 посвящена групповым политикам, а также автоматизации типичных задач администрирования. В главе 5 рассказывается, как работать со службами поддержки, а также как установить удаленное соединение с помощью служб терминалов.



Глава 1

Обзор системного администрирования Windows Server 2003

Microsoft Windows Server 2003 — самая мощная ОС для ПК. В ней реализованы совершенно новые средства управления системой и администрирования, впервые появившиеся в Windows 2000. Вот некоторые из них:

- **Active Directory** — расширяемая и масштабируемая служба каталогов, в которой используется пространство имен, основанное на стандартной Интернет-службе именования доменов (Domain Name System, DNS);
- **IntelliMirror** — средства конфигурирования, поддерживающие зеркальное отображение пользовательских данных и параметров среды, а также центральное администрирование установки и обслуживания программного обеспечения;
- **Terminal Services** — службы терминалов, обеспечивающие удаленный вход в систему и управление другими системами Windows Server 2003;
- **Windows Script Host** — сервер сценариев Windows для автоматизации таких распространенных задач администрирования, как создание учетных записей пользователей и отчетов по журналам событий.

Хотя у Windows Server 2003 масса других возможностей, именно эти четыре наиболее важны для выполнения задач администрирования. В максимальной степени это относится к Active Directory, поэтому для успешной работы системному администратору Windows Server 2003 необходимо четко понимать структуру и процедуры этой службы.

Со способами решения административных задач теснейшим образом связана и архитектура системы безопасности Windows

Server 2003. Active Directory и административные шаблоны позволяют применять параметры безопасности ко всем рабочим станциям и серверам вашего учреждения. Иными словами, вы настраиваете защиту данных не каждого конкретного компьютера, а всего предприятия в целом.

Одно из самых масштабных нововведений связано с изменением структуры семейств продуктов. Клиентские системы отныне входят в семейство Windows XP, а серверные системы — в семейство Windows Server 2003. Эта книга посвящена управлению ОС из семейства Windows Server 2003. Подробнее об управлении Windows XP — в справочнике «Microsoft Windows XP Professional, Справочник администратора» (Русская Редакция, 2002).

Microsoft Windows Server 2003

Семейство ОС Windows Server 2003 состоит из версий Standard Edition, Enterprise Edition, Datacenter Edition и Web Edition. У каждой — свое назначение.

- **Windows Server 2003, Standard Edition,** разработана для предоставления служб и ресурсов другим системам в сети. Она сменила Windows NT 4.0 Server и Windows 2000 Server. Эта ОС обладает богатым набором функций и **конфигурационных** параметров. Windows Server 2003 поддерживает до двух центральных процессоров и до 4 Гбайт оперативной памяти.
- **Windows Server 2003, Enterprise Edition,** расширяет возможности Windows Server 2003, Standard Edition, обеспечивая поддержку служб кластеров, служб метакаталогов и служб для Macintosh. В ней также поддержи каются 64-разрядные процессоры Intel Itanium, оперативная память с возможностью «горячей» замены и неоднородный доступ к памяти (nonuniform memory access, NUMA). Эта версия поддерживает до 32 Гбайт оперативной памяти на процессорах x86, до 64 Гбайт оперативной памяти на процессорах Itanium и до 8 центральных процессоров.
- **Windows Server 2003, Datacenter Edition,** — самый надежный Windows-сервер. Эта версия поддерживает более сложную кластеризацию и способна работать с большими объемами оперативной памяти — до 64 Гбайт на процессорах x86 и до 128 Гбайт на процессорах Itanium. Минимальное количество процессоров для работы Datacenter Edition — 8, максимальное — 32.

- Windows Server 2003, Web Edition, предназначена для запуска служб Web при развертывании Web-узлов и Web-приложений. Для решения этих задач в данную версию включены Microsoft .NET Framework, Microsoft Internet Information Services (IIS), ASP.NET и функции для равномерного распределения нагрузки на сеть, Многие другие функции, в частности Active Directory, в ней отсутствуют. Строго говоря, из стандартных компонентов Windows в этой версии предусмотрены лишь распределенная файловая система DFS, шифрованная файловая система EFS и удаленный рабочий стол. Версия Windows Server 2003, Web Edition, поддерживает до 2 Гбайт оперативной памяти и до двух центральных процессоров.

Примечание Все версии поддерживают одни и те же базовые функции и средства администрирования. Т. е. методики, описанные в этой книге, можно применять независимо от того, какой версией Windows Server 2003 вы пользуетесь. Помните, что в версии Web Edition нет Active Directory, поэтому сервер, работающий под управлением этой версии, нельзя сделать контроллером домена. Он, тем не менее, может быть частью домена Active Directory.

При установке Windows Server 2003 система конфигурируется согласно ее роли в сети. Серверы обычно становятся частью рабочей группы или домена.

- Рабочие группы — это свободные объединения компьютеров, в которых каждый компьютер управляется независимо.
- Домены — это объединения компьютеров, коллективно управляемых с помощью контроллеров домена, т. е. систем Windows Server 2003, регулирующих доступ к сети, базе данных каталога и общим ресурсам.

Во всех версиях Windows Server 2003 допускается использование двух различных представлений меню Пуск (Start).

- **Классическое меню Пуск (Classic Start Menu)** применялось в предыдущих версиях Windows. По щелчку кнопки Пуск (Start) на экране появляется меню, открывающее доступ к остальным меню и командам.

  Чтобы с помощью классического меню получить доступ к средствам администрирования, щелкните кнопку Пуск (Start), затем Программы (Programs), затем Администрирование (Administrative Tools). Доступ к Панели управления

(Control Panel) открывает одноименная команда из подменю Настройка (Settings).

- **Упрощенное меню Пуск (Simple Start Menu)** позволяет быстро запускать часто используемые программы и команды. В нем, например, имеется команда непосредственно для выключения компьютера.

  Чтобы с помощью упрощенного меню получить доступ к средствам администрирования, открывать промежуточное меню не нужно — в нем самом есть команда Администрирование (Administrative Tools). Другая команда сразу же откроет Панель управления (Control Panel).

Контроллеры домена и рядовые серверы

При установке Windows Server 2003 систему можно конфигурировать как рядовой сервер, контроллер домена или изолированный сервер. Различия между этими типами серверов чрезвычайно важны. Рядовые серверы являются частью домена, но не хранят информацию каталога. Контроллеры домена хранят данные каталога и выполняют службы аутентификации и каталога в рамках домена. Изолированные серверы не являются частью домена и имеют собственную БД пользователей, поэтому изолированный сервер также аутентифицирует запросы на вход.

Windows Server 2003 не различает основные и резервные контроллеры домена, так как поддерживает модель репликации с несколькими хозяевами. В этой модели любой контроллер домена может обрабатывать изменения каталога и затем автоматически реплицирует их на другие контроллеры домена. В модели репликации с одним хозяином в Windows NT все происходит не так: основной контроллер домена хранит главную копию каталога, а резервные — ее копии. Кроме того, Windows NT распространяет только БД диспетчера учетных записей безопасности (security access manager, SAM), а Windows Server 2003 — весь каталог информации, называемый *хранилищем данных* (data store). В нем есть наборы объектов, представляющие учетные записи пользователей, групп и компьютеров, а также общие ресурсы, например серверы, файлы и принтеры.

Домены, в которых применяются службы Active Directory, называют доменами Active Directory, чтобы отличать их от доменов Windows NT. Хотя Active Directory работает только с одним контроллером домена, в домене можно и нужно создать до-

полнительные контроллеры. Если один контроллер выходит из строя, для выполнения аутентификации и других важных задач можно задействовать другие.

В домене Active Directory любой рядовой сервер разрешается повысить до уровня контроллера домена без переустановки ОС, как того требовала Windows NT. Для превращения рядового сервера в контроллер следует лишь установить на него компонент Active Directory. Возможно и обратное действие: понижение контроллера домена до рядового сервера, если он не является последним контроллером домена в сети. Вот как повысить или понизить уровень сервера посредством мастера установки Active Directory.

1. Щелкните Пуск (Start).
2. Щелкните Выполнить (Run).
3. Наберите dcpromo в поле Открыть (Open) и щелкните OK.

Роли серверов

В Windows Server 2003 конфигурация сервера основана на службах, которые он предоставляет. Службы можно добавлять или удалять в любой момент, используя Мастер настройки сервера (Configure Your Server).

1. Щелкните Пуск (Start).
2. Щелкните Программы (Programs) или Все программы (АИ Programs).
3. Щелкните Администрирование (Administrative Tools) и выберите Мастер настройки сервера (Configure Your Server).
4. Дважды щелкните Далее (Next). Windows Server 2003 соберет информацию о текущих ролях сервера. В окне Роль сервера (Server Role) отобразится список доступных ролей с указанием, заданы ли они уже. Добавить или удалить роль очень просто.
   - Если роль не настроена и вы хотите ее добавить, выделите ее название в столбце Роль сервера (Server Role) и щелкните Далее (Next). Затем следуйте инструкциям.
   - Если роль настроена и вы хотите ее удалить, выделите ее название в столбце Роль сервера (Server Role) и щелкните Далее (Next). Внимательно прочитайте все предупреждения, а затем следуйте инструкциям.

Любой сервер может поддерживать одну или более следующих ролей.

- **Контроллер домена (Domain controller)** — сервер, на котором работают службы каталогов и располагается хранилище данных каталога. Контроллеры домена также отвечают за вход в сеть и поиск в каталоге. При выборе этой роли на сервере будут установлены DNS и Active Directory.
- **Почтовый сервер (POP3, SMTP) [Mail server (POP3, SMTP)] -** сервер, на котором работают основные почтовые службы POP3 (Post Office Protocol 3) и SMTP (Simple Mail Transfer Protocol), благодаря чему почтовые POP3-клиенты домена могут отправлять и получать электронную почту. Выбрав эту роль, вы определяете домен по умолчанию для обмена почтой и создаете почтовые ящики. Эти службы удобны в небольших компаниях или при удаленном соединении, когда электронная почта необходима, но вполне может обойтись без функциональности Microsoft Exchange Server.
- **Сервер печати (Print server)** — сервер, организующий доступ к сетевым принтерам и управляющий очередями печати и драйверами принтеров. Выбор этой роли позволит вам быстро настроить параметры принтеров и драйверов.
- **Сервер потоков мультимедиа (Streaming media server)** — сервер, предоставляющий мультимедийные потоки другим системам сети или Интернета. Выбор этой роли приводит к установке служб Windows Media. Эта роль поддерживается только в версиях Standard Edition и Enterprise Edition.
- **Сервер приложений (Application server)** — сервер, на котором выполняются Web-службы XML, Web-приложения и распределенные приложения. При назначении серверу этой роли на нем автоматически устанавливаются IIS, COM+ и Microsoft .NET Framework. При желании вы можете добавить к ним серверные расширения Microsoft FrontPage, а также включить или выключить ASP.NET.
- **Сервер терминалов (Terminal Server)** — сервер, выполняющий задачи для клиентских компьютеров, которые работают в режиме терминальной службы. Выбор этой роли приводит к установке Terminal Server. Для удаленного управления сервером устанавливать Terminal Server не нужно. Необходимый для этого удаленный рабочий стол (Remote Desktop) устанавливается автоматически вместе с ОС.

- **Сервер удаленного доступа или VPN-сервер (Remote access/** VPN server) — сервер, осуществляющий маршрутизацию сетевого трафика и управляющий телефонными соединениями и соединениями через виртуальные частные сети (virtual private network, VPN). Выбрав эту роль, вы запустите Мастер настройки сервера маршрутизации и удаленного доступа (Routing and Remote Access Server Setup Wizard). С помощью параметров маршрутизации и удаленного доступа вы можете разрешить только исходящие подключения, входящие и исходящие подключения или полностью запретить доступ извне.
- Узел кластера серверов (Server cluster node) — сервер, действующий в составе группы серверов, объединенных в кластер. Выбор этой роли приводит к запуску Мастера создания кластера (New Server Cluster Wizard), позволяющего создать новую кластерную группу, или Мастера добавления узлов (Add Nodes Wizard), который поможет добавить сервер к существующему кластеру. Эта роль поддерживается только в версиях Enterprise Edition и Datacenter Edition.
- Файл-сервер (File server) — сервер, предоставляющий доступ к файлам и управляющий им. Выбор этой роли позволит вам быстро настроить параметры квотирования и индексирования. Вы также можете установить Web-приложен ие для администрирования файлов. В этом случае будет установлен IIS и включены страницы ASP (Active Server Pages).
- **DHCP-сервер** (DHCP Server) — сервер, на котором запущен DHCP (Dynamic Host Configuration Protocol), позволяющий автоматизировать назначение IP-адресов клиентам сети. При выборе этой роли на сервере будет установлен DHCP и запущен Мастер создания области (New Scope Wizard).
- DNS-сервер (DNS Server) — сервер, на котором запущена служба DNS, разрешающая имена компьютеров в IP-адреса и наоборот. При выборе этой роли на сервере будет установлена DNS и запущен Мастер настройки DNS-сервера (Configure DNS Server Wizard).
- **WINS-сервер (WINS** server) — сервер, на котором запущена служба WINS (Windows Internet Name Service), разрешающая имена NetBIOS в IP-адреса и наоборот. Выбор этой роли приводит к установке WINS.

Управление выбранными ролями сервера осуществляется с помощью программы Управление данным сервером (Manage Your Server), в окне которой сосредоточены все основные инструменты для управления Windows Server 2003. В частности, здесь перечислены текущие роли сервера (рис. 1-1). Чтобы открыть это окно, воспользуйтесь меню Администрирование (Administrative Tools).

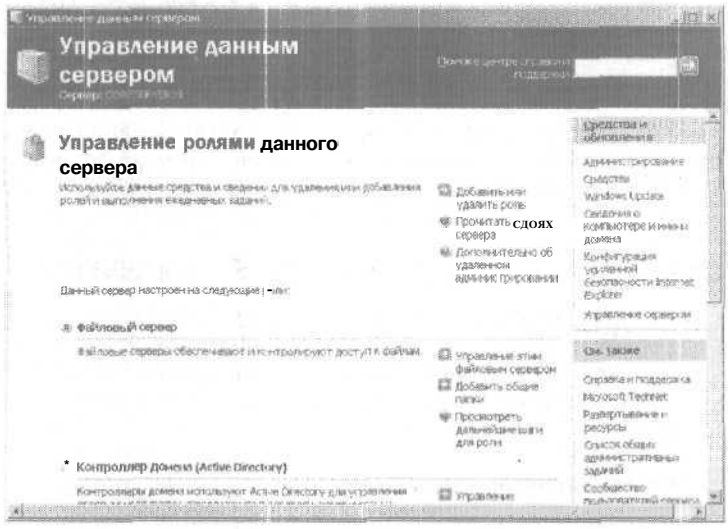


Рис. 1-1. Окно Управление данным сервером (Manage Your Server) открывает быстрый доступ к часто используемым командам и сведениям

Совет С помощью значков со стрелками справа от названия роли вы можете отобразить или скрыть информацию о ней. Не пренебрегайте командами из групп Средства и обновления (Tools and Updates) и См. также (See Also). Они откроют вам быстрый доступ к командам Администрирование (Administrative Tools), Windows Update и другим. Наконец, воздержитесь от искушения установить флажок Не показывать эту страницу при входе в систему (Don't display this page at logon) в нижнем левом углу окна. Мой опыт свидетельствует, что чаще всего рабочий день администратора все равно начинается с команд, собранных в этом диалоговом окне.

Другие ресурсы Windows Server 2003

Перед изучением средств администрирования обратимся к другим ресурсам, которые можно использовать, чтобы упростить администрирование Windows Server 2003. Один из лучших ресурсов системного администратора — дистрибутивные диски Windows Server 2003. Они содержат всю необходимую информацию для внесения изменений в систему. Держите диски под рукой при изменении конфигурации системы. Скорее всего они вам понадобятся.

Чтобы не запускать дистрибутивный диск Windows Server 2003 всякий *раз* при проведении системных изменений, можно скопировать папку \i386 на сетевой диск. Когда система предложит вставить компакт-диск и указать исходную папку, просто выберите папку на сетевом диске. Такая методика удобна и экономит время. Другие полезные ресурсы описаны далее.

Средства поддержки Windows Server 2003

С дистрибутивного компакт-диска можно установить комплект ресурсов Windows Server 2003 Support Tools. Средства поддержки — это универсальный набор утилит для выполнения любых сервисных задач от диагностики системы до сетевого мониторинга.

Установка средств поддержки

Средства поддержки устанавливаются следующим образом.

1. Вставьте установочный компакт-диск Windows Server 2003 в CD-ROM-дисковод.
2. Когда откроется окно автозапуска, щелкните кнопку Выполнение иных задач (Perform additional tasks), а затем — Обзор этого компакт-диска (Browse this CD) — запустится Проводник (Explorer).
3. В открывшемся окне дважды щелкните папку Support, а затем — Tools.

Примечание В этой книге я упоминаю двойной щелчок как наиболее распространенный способ открытия папок и запуска программ. Однократный щелчок выделяет элемент, двукратный — открывает (запускает) его. В Windows Server 2003 также можно настроить открытие/запуск одним щелчком. При этом наведение указателя мыши на элемент вы-

бирает его, а щелчок — открывает (запускает). Параметры щелчка изменяются с помощью инструмента Свойства папки (Folder Options) из Панели управления (Control Panel). На вкладке Общие (General) установите переключатель Открывать одним щелчком, выделять указателем (Single-click to open item) вместо Открывать двойным, а выделять одним щелчком (Double-click to open item).

4. Щелкните дважды Suptools.msi. Запустится мастер установки средств поддержки. Щелкните Next[1].
5. Прочитайте лицензионное соглашение, щелкните I agree, если соглашение не вызывает у вас возражений, а затем — Next.
6. Введите пользовательскую информацию и щелкните Next.
7. По умолчанию средства поддержки устанавливаются в папку *%ProgramFiles%*\SupportTools. Чтобы установить их в другую папку, введите путь к ней или найдите нужную папку с помощью кнопки Browse. Средства поддержки занимают на диске около 23 Мбайт.
8. Щелкните Install Now.

Примечание Строкой %ProgramFiles% обозначена переменная среды ProgramFiles. В ОС Windows с помощью переменных среды задаются многие системные и пользовательские параметры. Я довольно часто буду указывать переменную среды именно таким образом — %ИмяПеременной%.

Использование средств поддержки

После установки доступ к средствам поддержки можно получать из управляющей консоли Центр справки и поддержки (Help and Support Tools) Windows Server 2003 (рис. 1-2). Щелкните кнопку Пуск (Start) и раскройте меню Программы (Programs) или Все программы (All Programs), щелкните Windows Support Tools, а затем выберите Support Tools Help.

Как видно из рисунка, средства упорядочены по имени файла, имени средства и категории. Щелкнув имя средства, вы откроете страницу со справочной информацией о нем. На этой странице также имеется команда для запуска средства.

---

[1] Во время подготовки к печати русского издания этот пакет был доступен только в англоязычном варианте. — *Прим. перев.*

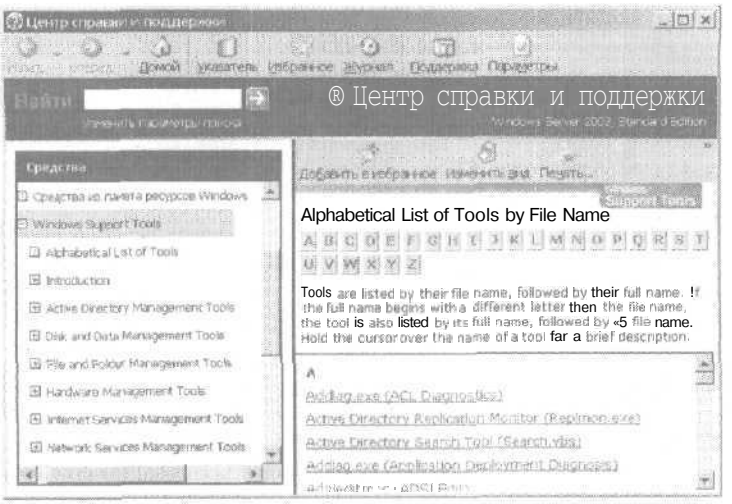


Рис. 1-2. Применяйте средства поддержки для выполнения таких задач, как диагностика системы и сетевой мониторинг

Часто используемые средства

Есть много способов администрирования систем Windows Server 2003. Чаще всего применяются следующие.

- **Панель управления** — набор средств для управления конфигурацией системы Windows Server 2003. В классическом меню Пуск (Start) доступ к этим средствам открывает подменю Настройка (Settings), в упрощенном меню Пуск (Start) команда Панель управления (Control Panel) доступна сразу.
- **Графические средства администрирования** — ключевые средства для управления компьютерами в сети и их ресурсами, Доступ к необходимому средству можно получить, щелкнув его значок в подменю Администрирование (Administrative Tools).
- **Мастера администрирования** — средства автоматизации ключевых административных задач. В отличие от Windows NT мастера не сосредоточены в центральном месте — доступ к ним происходит посредством выбора соответствующих параметров меню в других средствах администрирования.

- **Функции командной строки.** Большинство административных действий можно выполнять из командной строки.

В следующих разделах кратко описаны эти функции администрирования. Далее в книге многие из них обсуждаются подробнее. Помните: для применения этих программ вам может понадобиться учетная запись с привилегиями администратора.

Программы панели управления

Панель управления содержит программы для настройки системы. Вид панели управления зависит от используемого представления, т. е. способа расположения и отображения инструментов. Основные программы панели управления перечислены далее.

- **Дата и время (Date/Time)** используется для просмотра или установки дня, времени и часового пояса. Вместо установки времени на отдельных компьютерах в домене вручную можно применить средство автоматической синхронизации времени Windows Time Service.
- **Лицензирование (Licensing)** служит для управления лицензиями и изменения режима лицензирования установленных продуктов.
- **Назначенные** задания (Scheduled **Tasks)** позволяет просматривать, добавлять и редактировать назначенные задания. Подробнее об этом — в главе 4.
- **Принтеры и факсы (Printers and Faxes)** обеспечивает быстрый доступ к папке Принтеры и факсы (Printers and Faxes), откуда можно управлять устройствами печати. Об управлении сетевыми принтерами — в главе 17.
- **Свойства** папки **(Folder Options)** регулирует многие параметры папок и файлов, включая режимы просмотра папок, автономный режим использования файлов, а также количество щелчков для открытия файлов.
- **Сетевые подключения (Network Connections)** служит для просмотра сетевых реквизитов, добавления сетевых компонентов и установки сетевых соединений. Эта функция также годится для изменения имени компьютера и домена. Подробнее об этом — в главе 16.
- **Система (System)** используется для отображения и редактирования свойств системы, включая свойства запуска/остановки, переменные среды, профили оборудования и пользователей (см. также главу 2).

- **Установка и удаление программ (Add/Remove Programs)** служит для установки и удаления прикладных программ, а также компонентов Windows Server 2003. Например, если при установке ОС вы не установили службы сертификации, их можно добавить позже.
- Установка оборудования (Add/Remove Hardware) запускает Мастер установки оборудования (Add/Remove Hardware Wizard), который применяется для установки и обслуживания оборудования.
- Экран **(Display)** используется для конфигурации фонов, хранителей экрана, режима видеоизображения и параметров видео. Эта функция также позволяет настраивать вид значков на рабочем столе или визуальных эффектов, например постепенное свертывание меню.

Графические средства администрирования

В Windows Server 2003 предусмотрено несколько типов средств системного администрирования. Графические средства чаще всего применяются для управления той системой, на которой вы в настоящий момент работаете, а также для управлениям другими системами в домене Windows Server 2003. Например, чтобы в консоли Службы компонентов (Component Services) выбрать компьютер, с которым вы хотите работать, щелкните правой кнопкой элемент Просмотр событий (Event Viewer) в левой панели и выберите команду Подключиться к другому компьютеру (Connect to Another Computer). Откроется диалоговое окно Выбор компьютера (Select Computer), показанное на рис. 1-3. Щелкните переключатель Другим компьютером (Another Computer) и введите имя компьютера.

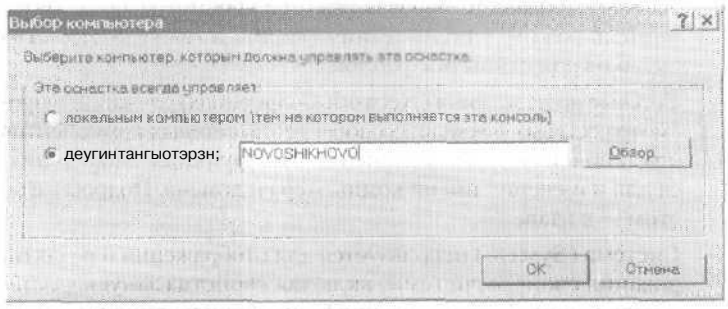


Рис. 1-3. Подключение к другому компьютеру позволяет управлять удаленными ресурсами

Основные графические средства администрирования

Ниже перечислены основные графические **средства** администрирования и их назначение **(табл.** 1-1). Для **работы с** ними **выберите соответствующую команду в** подменю **Администрирование** (Administrative **Tools)** или щелкните дважды **одноименный инструмент** панели управления.

Таблица 1-1. Краткий справочник основных средств администрирования Windows Server 2003

Средство администрирования	Назначение
Active Directory — домены и доверие (Active Directory Domains and Trusts)	Управление доверительными отношениями между доменами
Active Directory — пользователи и компьютеры (Active Directory Users and Computers)	Управление пользователями, группами, компьютерами и другими объектами Active Directory
Active Directory — сайты и службы (Active Directory Sites and Services)	Создание сайтов для управления репликацией Active Directory
DHCP	Конфигурация и управление службой DHCP
DNS	Управление службой системы доменных имен (DNS)
WINS	Управление службой WINS, преобразующей имена NetBIOS в IP-адреса
Администратор кластеров (Cluster Administrator)	Управление службой Cluster
Администратор серверных расширений (Server Extensions Administrator)	Управление серверными расширениями, например FrontPage
Внешнее хранилище (Remote Storage)	Управление службой Remote Storage
Диспетчер служб Интернета (Internet Information Services Manager)	Управление Web-, FTP- и SMTP-серверами
Диспетчер служб терминалов (Terminal Services Manager)	Управление и мониторинг пользователей, сеансов и процессов Terminal Service
Источники данных (ODBC) [Data Sources (ODBC)]	Добавление, удаление и настройка источников данных и драйверов ODBC (Open Database Connectivity)

Таблица 1-1. Краткий справочник основных средств администрирования Windows Server 2003 *(продолжение)*

Средство администрирования	Назначение
Контроль допуска QpS (QoS Admission Control)	Управление службой Quality of Service (QpS) Admissions Control для регулировки пропускной способности сети
Лицензирование (Licensing)	Управление лицензированием доступа клиентов к серверным продуктам
Маршрутизация и удаленный доступ к сети (Routing and Remote Access)	Конфигурация и управление службой Routing and Remote Access, контролирующей интерфейсы маршрутизации, динамическую IP-маршрутизацию и удаленный доступ
Настройка сервера (Configure Your Server)	Добавление, удаление и конфигурация служб Windows для сети
Настройка служб терминалов (Terminal Services Configuration)	Управление настройкой протокола Terminal Service и параметрами сервера
Пакет администрирования диспетчера подключений (Connection Manager Administration Kit)	Конфигурирование и настройка диспетчера подключений
Политика безопасности домена (Domain Security Policy)	Просмотр и редактирование политики безопасности в домене
Политика безопасности контроллера домена (Domain Controller Security Policy)	Просмотр и редактирование политики безопасности для организационного полразделения контроллера домена
Производительность (Performance)	Отображение графиков производительности системы и настройка журналов и сигналов оповещения
Просмотр событий (Event Viewer)	Управление событиями и журналами
Распределенная файловая система DI-"S (Distributed File System)	Создание и управление распределенными файловыми системами, объединяющими общие папки из разных компьютеров
Сетевой монитор (Microsoft Network Monitor)	Мониторинг сетевого трафика и устранение неисправностей в сети
Службы (Services)	Управление запуском и настройка служб Windows

Таблица 1-1. Краткий справочник основных средств администрирования Windows Server 2003 (*окончание*)

Средство администрирования	Назначение
Службы компонентов (Component Services)	Конфигурация и управление приложениями COM+, управление событиями и службами
Удаленные рабочие столы (Remote Desktop)	Настройка удаленных подключений и просмотр сеансов удаленных подключений
Управление компьютером (Computer Management)	Запуск и остановка служб, управление дисками и доступ к другим средствам управления системой
Центр сертификации (Certification Authority)	Управление сертификационными службами

Средства управления и конфигурация

Набор доступных средств администрирования на вашей системе зависит от ее конфигурации. При добавлении служб на сервере устанавливаются средства управления этими службами. В Windows XP Professional или па другом сервере они могут быть недоступны. Чтобы воспользоваться ими на рабочей станции, установите пакет Windows Server 2003 Administration Tools.

t. Зарегистрируйтесь на рабочей станции по учетной записи *с* привилегиями администратора.

2. Встаньте в CD-ROM-дисковод установочный диск Windows Server 2003.

3. Когда появится окно автозапуска, щелкните кнопку Выполнение иных задач (Perform additional tasks) а затем Обзор этого компакт-диска (Browse this CD) — запустится Проводпик (Explorer).

4. Дважды щелкните папку I386, а затем дважды щелкните Adminpak.msi. На рабочей станции или сервере будет установлен полный набор срсдстн управления Windows Server 2003.

Примечание Средства администрирования Windows 2000 несовместимы ни с Windows XP Professional, ни с Windows Server 2003. При переходе на Windows XP Professional с Windows 2000 Professional вы обнаружите, что многие из средств администрирования Windows 2000 перестали работать. Удали-

те их и установите на администраторских системах Windows XP Professional пакет Windows Server 2003 Administration Tools Pack (Adminpak.msi). Средства администрирования Windows Server 2003 совместимы как с Windows 2000, так и с Windows XP Professional,

Функции командной строки

В Windows Server 2003 масса утилит командной строки. Многие из них используют протокол TCP/IP, поэтому его следует предварительно установить.

Как администратору, вам следует знать следующие утилиты командной строки.

- ARP отображает и управляет программно-аппаратной привязкой адресов, используемой Windows Server 2003 для отправки данных по сети TCP/IP.
- AT назначает автозапуск программ по расписанию.
- **DNSCMD** отображает и управляет конфигурацией службы DNS.
- FTP запускает встроенный FTP-клиент.
- **HOSTNAME** отображает имя локального компьютера.
- **IPCONFIG** отображает свойства TCP/IP для сетевых адаптеров, установленных в системе. Также используется для обновления и освобождения выданных службой DHCP адресов.
- **NBTSTAT** отображает статистику и текущее соединение для протокола NetBIOS поверх TCP/IP.
- **NET** отображает список подкоманд команды NET.
- **NETSH** отображает и управляет сетевой конфигурацией локального и удаленных компьютеров.
- **NETSTAT** отображает текущие TCP/IP-соединения и статистику протокола.
- **NSLOOKUP** проверяет статус узла или IP-адреса при использовании с DNS.
- **PATHPING** проверяет сетевые пути и отображает информацию о потерянных пакетах.
- **PING** тестирует соединение с удаленным узлом.
- **ROUTE** управляет таблицами маршрутизации в системе.

- **TRACERT** во время тестирования определяет сетевой путь к удаленному узлу.

Чтобы научиться применять эти средства, наберите имя команды R командной строке без параметров: в большинстве случаев Windows Server 2003 выведет справку по ее использованию.

Использование команды NET

Большинство задач, соответствующих подкомандам команды NET, проще решить с помощью графических средств администрирования и инструментов панели управления, Тем не менее эти подкоманды удобны для быстрого выполнения некоторых действий или для оперативного получения информации, особенно во время сеансов Telnet с удаленными системами.

- NET SEND отправляет сообщения пользователям, зарегистрированным в указанной системе.
- NET START запускает службу в системе.
- NET STOP останавливает службу в системе.
- NET TIME отображает текущее системное время или синхронизирует системное время с другим компьютером.
- NET USE подключает и отключает от общего ресурса.
- NET VIEW выводит список доступных сетевых ресурсов.

Чтобы научиться использовать команду NET, введите NET HELP и имя подкоманды, например **NET** HELP SEND. Windows Server 2003 выведет необходимые справочные сведения.

Глава 2

Управление серверами Windows Server 2003

Серверы — основа любой сети Microsoft Windows. Одна из основных функций администратора — управлять ими. Ключевой инструмент для этого — консоль Управление компьютером (Computer Management), предоставляющая единый интегрированный интерфейс для:

- управления сеансами и соединениями пользователя;
- управления пользованием файлами, папками и общими ресурсами;
- настройки административных оповещений;
- управления приложениями и сетевыми службами;
- конфигурации аппаратных устройств;
- просмотра и конфигурации дисков и съемных носителей информации.

Консоль Управление компьютером (Computer Management) оптимальна для удаленного управления сетевыми ресурсами, но вам необходимо также средство для более тонкой настройки параметров и свойств системной среды. И здесь мы вспоминаем про инструмент Система (System). Он предназначен для:

- конфигурации производительности приложения, виртуальной памяти и параметров реестра;
- управления системными и пользовательскими переменными среды;
- настройки стартовых и восстановительных системных параметров;
- управления аппаратными и пользовательскими профилями.

Управление сетевыми системами

Консоль Управление компьютером (Computer Management) разработана для выполнения основных задач системного администрирования на локальных и удаленных системах. Вы будете часто работать с ней и должны знать ее детально. Для запуска консоли Управление компьютером (Computer Management) используется команда из меню Администрирование (Administrative Tools).

Главное окно консоли разделено на две панели (рис. 2-1) и похоже на окно Проводника (Windows Explorer). Дерево консоли в левой панели служит для навигации и выбора средств, которые делятся на три категории:

- **Служебные** программы **(System Tools)** — средства общего назначения для управления системами и просмотра системной информации;
- Запоминающие устройства (Storage) — здесь отображена информация о съемных и логических дисках и предоставляется доступ к средствам управления дисками;
- Службы и приложения (Services and Applications) — обзор и управление свойствами служб и приложений, установленных на сервере.

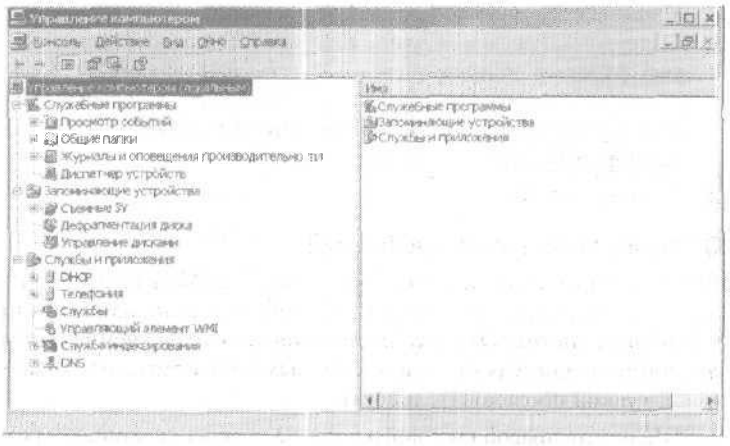


Рис. 2-1. Консоль Управление компьютером (Computer Management)

Выделив самый первый элемент в дереве консоли Управление компьютером (Computer Management), имя которого совпадает с именем консоли, вы получаете доступ к трем важным функциям, позволяющим:

- соединяться с другими компьютерами;
- отправлять консольные сообщения;
- экспортировать списки.

В следующих разделах разбираются эти задачи, а затем подробно рассматривается работа с консолью Управление компьютером (Computer Management).

Соединение с другими компьютерами

Консоль Управление компьютером (Computer Management) предназначена для работы с локальными и удаленными системами. Компьютер для управления можно выбрать, выполнив следующие действия.

1. Щелкните правой кнопкой элемент Управление компьютером (Computer Management) в дереве консоли и выберите команду Подключиться к другому компьютеру (Connect to another Computer) в контекстном меню. Откроется диалоговое окно Выбор компьютера (Select Computer).
2. Установите переключатель Другим компьютером (Another Computer) и введите полное имя компьютера, *с* которым хотите работать, например *engsvr01.iecfmology.microsoft.com,* где *engsvr01* — имя компьютера, а *technology.microsoft.com* — имя домена. Щелкните кнопку Обзор (Browse), чтобы найти компьютер, имя которого вы не помните.
3. Щелкните OK.

Отправка консольных сообщений

Консоль Управление компьютером (Computer Management) позволяет отправлять сообщения пользователям локальной или удаленных систем. Эти сообщения появляются в специальном диалоговом *окне. Сообщения* удаленным *пользователям* отправляют в такой последовательности.

1. Щелкните правой кнопкой элемент Управление компьютером (Computer Management) в дереве консоли. В контекстном меню выберите Все задачи (All Tasks), а затем — Отправка сообщения консоли (Send Console Message). Откроется диалоговое окно, показанное на рис. 2-2.

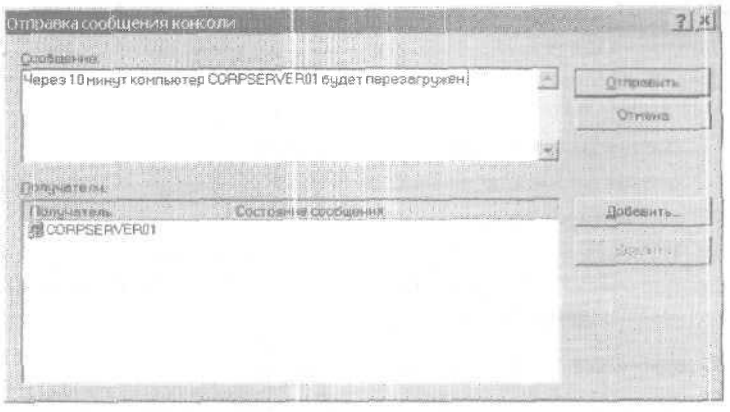


Рис. 2-2. Диалоговое окно Отправка сообщения консоли (Send console message) позволяет отправлять сообщения на другие системы

2. Введите текст сообщения в поле Сообщение (Message). В поле Получатели (Recipients) вы увидите имя компьютера, с которым связываетесь.
3. Чтобы отправить сообщение пользователям этой системы, щелкните Отправить (Send). Кнопками Добавить (Add) и Удалить (Remove) можно добавить или удалить адресатов из списка. Подготовив сообщение к отправке, щелкните Отправить (Send).

Примечание Получать сообщения будут только пользователи, зарегистрированные на выбранной системе. Для отправки и получения консольных сообщений в системах Windows NT, Windows 2000, Windows XP и Windows Server 2003 должна работать Служба сообщений (Messenger). На системах с Windows 95/98 отправка и получение сообщений производятся с помощью программы WinPopup.

Экспорт информационных списков

Возможность экспорта списков — одна из моих любимых функций консоли Управление компьютером (Computer Management), и, если вы ведете записи системных сведений или регулярно работаете со сценариями Windows, она нам тоже пригодится. Функция Экспортировать список (Export List) позволяет сохранять информацию, отображаемую на правой панели, в текстовом

файле, разделяемом запятыми или табуляторами. В частности, она позволяет сохранять подробные сведения обо всех службах, работающих в системе.

1. В консоли Управление компьютером (Computer Management) разверните интересующий вас элемент.
2. Щелкните правой кнопкой пустое пространство в правой панели и выберите в контекстном меню Экспортировать список (Export List).
3. Укажите в списке Папка (Save In) место для сохранения, затем введите имя файла для экспорта.
4. Выберите в списке Тип файла (Save As Type) нужный формат. Столбцы информации можно разделять табулятором или запятыми и сохранять текст в кодировке ASCII или Unicode. Чаще используется текст в кодировке ASCII.
5. Щелкните Сохранить (Save).

Служебные программы

Элемент Служебные программы (System Tools) в узле Управление компьютером (Computer Management) служит для управления системами и просмотра сведений о них. В нем содержатся следующие узлы:

- **Просмотр событий** (Event **Viewer)** — средство для просмотра журналов событий на выбранном компьютере (см. главу 3);
- **Общие папки (Shared Folders)** — управление свойствами общих папок, сеансами пользователей и открытыми файлами (см. главу 13);
- **Локальные пользователи и группы (Local Users and Groups)** — управление локальными пользователями и группами на выбранном компьютере (см. часть II книги);

Примечание Локальные пользователи и локальные группы пользователей не являются частью Active Directory и управляются из консоли Локальные пользователи и группы (Local Users and Groups). У контроллеров домена записей в этой консоли нет.

- **Журналы и оповещения производительности (Performance Logs and Alerts)** — контроль за работой системы и ведение журналов. Это средство также применяется для оповещения пользователя о различных событиях (см. главу 3);

- Диспетчер устройств (Device Manager) — основное средство проверки состояния любого устройства, установленного на компьютере, и обновления драйверов. Его также можно использовать для устранения неполадок. Об управлении устройствами — далее в этой главе.

Запоминающие устройства (Storage)

Элемент Запоминающие устройства (Storage Tools) узла Управление компьютером (Computer Management) служит для отображения сведений о дисках и предоставляет доступ к средствам управления ими:

- Съемные ЗУ (Removable Storage) — управление съемными устройствами и ленточными библиотеками. Отслеживает очередь и запросы, относящиеся к съемным носителям;
- **Дефрагментация диска (Disk Defragmenter)** — выполнение дефрагментации, т.е. поиск и объединение фрагментированных файлов;
- **Управление дисками (Disk** Management) — управление жесткими дисками, разделами, наборами томов и RAID.

О работе с файлами, дисками и носителями рассказано в части III книги.

Службы и приложения (Services and Applications)

Любую относящуюся к приложению или службе задачу, которую можно выполнить средствами отдельной оснастки, удается выполнить и из узла Службы и приложения (Services and Applications). Например, если в системе установлен сервер DHCP, управляют им как посредством команды DHCP из меню Администрирование (Administrative Tools), так и с помощью узла Службы и приложения (Services and Applications).

Это возможно, потому что диспетчер DHCP является оснасткой консоли управления Microsoft. Если вы выбираете команду DHCP в меню Администрирование (Administrative Tools), оснастка отображается в отдельной консоли. Если вы добрались до нее через узел Службы и приложения (Services and Applications), оснастка отображается в консоли Управление компьютером (Computer Management). О работе со службами и приложениями рассказано в главе 3 и следующих главах.

Управление средой, профилями и свойствами системы

Инструмент Система (System) служит для управления средой, профилями и свойствами системы. Запустите его, дважды щелкнув одноименный значок в Панели управления (Control Panel). Откроется диалоговое окно Свойства системы (System Properties) с шестью вкладками (рис. 2-3).

Рис. 2-3. Диалоговое окно свойств системы

Вкладка Общие (General)

Общие сведения о системе на любом сервере Windows 2003 доступны из вкладки Общие (General). К ним относятся:

- версия ОС и пакета обновления;
- имя зарегистрированного владельца;
- серийный номер Windows;
- тип компьютера;
- объем ОЗУ компьютера;
- тип процессора;
- общий объем ОЗУ системы.

Вкладка Имя компьютера (Computer Name)

Вкладка Имя компьютера (Computer Name), показанная на рис. 2-4, предназначена для изменения параметров сетевой иден-

тификации компьютера, не являющегося контроллером домена. На ней отображены полное имя компьютера и данные о членстве в домене. Полное имя — это по сути DNS-имя компьютера, помимо прочего определяющее его место в иерархии Active Directory.

Рис. 2-4. Вкладка Имя компьютера (Computer Name) позволяет изменить сетевую идентификацию системы

Щелкнув кнопку Изменить (Change), вы сможете отредактировать имена системы и домена, связанные с этим компьютером.

Вкладка Оборудование (Hardware)

На серверах Windows Server 2003 разрешается использовать разные профили оборудования. Особенно это удобно для переносных серверов, например установленных па портативных компьютерах. Можно создать один профиль для работы в стыковочном узле, а другой — для самостоятельной работы.

Настройка профилей оборудования

Для настройки профилей оборудования откройте вкладку Оборудование (Hardware) окна свойств системы и щелкните кнопку Профили оборудования (Hardware Profiles). Откроется одноименное диалоговое окно, показанное на рис. 2-5. Здесь можно выполнить следующие действия:

- задать профиль по умолчанию, поставив его первым в списке Имеющиеся профили оборудования (Available Hardware Profiles);

- указать время ожидания выбора профиля при загрузке в поле Выбрать первый профиль в списке, если выбор не сделан за... (Select the first profile listed if I don't select a profile in...). По умолчанию система ждет 30 секунд;
- установить переключатель Дождаться явного указания от пользователя (Wait until I select a hardware profile), чтобы система не производила загрузку до явного выбора профиля.

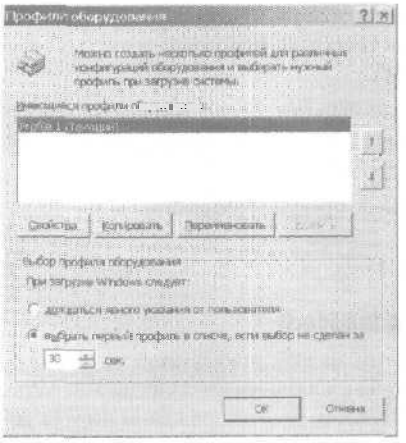


Рис. 2-5. Для любой системы на базе Windows Server 2003 можно настроить несколько профилей оборудования

Настройка профилей для работы со стыковочным узлом

1. В списке Имеющиеся профили оборудования (Available Hardware Profiles) выберите профиль по умолчанию и щелкните кнопку Копировать (Copy).
2. В диалоговом окне Копирование профиля (Copy Profile) введите имя профиля для работы в стыковочном узле, например Docked, и щелкните OK.
3. Выделите новый профиль и щелкните кнопку Свойства (Properties).
4. Установите флажок Это портативный компьютер (This is a portable computer) и переключатель Компьютер пристыкован (The computer is docked).
5. Установите флажок Всегда выводить этот профиль как вариант при загрузке Windows (Always include this profile as an option when Windows starts). Щелкните OK.

6. Выделите профиль по умолчанию в списке Доступные профили оборудования (Available Hardware Profiles) и щелкните Копировать (Copy).
7. В диалоговом окне Копирование профиля (Copy Profile) введите имя профиля для работы вне стыковочного узла,
8. Выберите новый профиль и щелкните кнопку Свойства (Properties).
9. Установите флажок Это портативный компьютер (This is a portable computer) и переключатель Компьютер отстыкован (The computer is undocked).
10. Установите флажок Всегда выводить этот профиль как вариант при загрузке Windows (Always include this profile as an option when Windows starts). Щелкните OK.
11. Сделайте один из созданных профилей профилем по умолчанию,
12. Щелкните OK.

Вкладка Дополнительно (Advanced)

На вкладке Дополнительно (Advanced), показанной на рис. 2-6, собраны средства для управления ключевыми функциями Windows, в частности быстродействием, использованием виртуальной памяти, профилем пользователя, переменными среды, загрузкой и восстановлением.

Рис. 2-6. Здесь задаются параметры быстродействия, переменные среды, порядок запуска и восстановления

Настройка быстродействия системы

Графический интерфейс Windows Server 2003 значительно расширен. Добавлены визуальные эффекты для меню, панелей инструментов, окон и панели задач. Чтобы обеспечить высокую производительность сервера, при начальной установке эти возможности по умолчанию отключены. Это сокращает объем работы, выполняемой сервером, когда администратор локально входит в систему для выполнения каких-либо задач, и изменять этот параметр не рекомендуется. Но если корректировать параметры интерфейса все-таки требуется, вот как это делается.

1. Откройте окно со свойствами системы и перейдите па вкладку Дополнительно (Advanced). Щелкните кнопку Параметры (Settings) в группе Быстродействие (Performance). Откроется диалоговое окно Параметры быстродействия (Performance Options).
2. Перейдите на вкладку Визуальные эффекты (Visual Effects), которая обычно открыта по умолчанию. На ней имеются следующие параметры для управления визуальными эффектами.
   - Восстановить значения по умолчанию (Let Windows choose what's best for my computer) — операционная система сама выбирает значения параметров, исходя го конфигурации оборудования. Как правило, для сервера это означает включение только флажка Использование стилей отображения для окон и кнопок (Use visual styles on windows and buttons); все остальные флажки сброшены.
   - **Обеспечить наилучший вид (Adjust for best appearance)** - включаются все визуальные эффекты для всех элементов графического интерфейса. В меню и панели задач используются эффекты перехода и тени. Экранные шрифты сглаживаются, списки снабжены плавной прокруткой, в папках используется Web-представление и так далее. Для этого требуется большой объем памяти и системных ресурсов, что в случае сервера необоснованно. Рекомендуется не использовать эту возможность.
   - Обеспечить наилучшее быстродействие (Adjust for best performance) — отключаются визуальные эффекты, которые требуют больших системных ресурсов. Иногда это означает отключение всех визуальных эффектов.

- Особые эффекты (Custom) — выборочная настройка визуальных эффектов. Установите или сбросьте флажки визуальных эффектов самостоятельно.

3. Завершив настройку визуальных эффектов, щелкните (Ж, а затем еще раз OK.

Настройка быстродействия приложений

Производительность приложений в Windows Server 2003 определяется параметрами распределения времени процессора и кэширования. От того, как происходит распределение времени процессора, зависит время отклика активного приложения (в противовес фоновым приложениям, которые также могут выполняться на системе). Распределение физической памяти может быть оптимизировано для приложений или для системного кэша.

Производительность приложений регулируется следующим образом.

1. Откройте окно со свойствами системы и перейдите на вкладку Дополнительно (Advanced). Щелкните кнопку Параметры (Settings) в группе Быстродействие (Performance). Откроется диалоговое окно Параметры быстродействия (Performance Options).
2. Перейдите на вкладку Дополнительно (Advanced) и выберите нужный параметр в группе Распределение времени процессора (Processor Scheduling):
   - Программ (Programs) — оптимизирует время отклика и доступа к ресурсам для активного приложения, рекомендуется для серверов приложений, Web-серверов и серверов потоков мультимедиа;
   - Служб, работающих в фоновом режиме (Background services) — оптимизирует время отклика для фоновых приложений, рекомендуется для серверов Active Directory, файловых серверов, серверов печати, серверов сети и связи.
3. Выберите нужный параметр в группе Использование памяти (Memory Usage):
   - Программ (Programs) — оптимизирует распределение физической памяти в пользу приложений, рекомендуется для серверов приложений, Web-серверов и серверов потоков мультимедиа;

- Системного кэша (System Cache) — оптимизирует распределение физической памяти в пользу системного кэша, рекомендуется для серверов Active Directory, файловых серверов, серверов печати, серверов сети и связи.

4. Щелкните OK.

Настройка виртуальной памяти

Виртуальная память позволяет задействовать дисковое пространство для расширения доступной оперативной памяти. Эта функция используется, начиная с процессора Intel 386, — оперативная память записывается на диски путем подкачки страниц. При постраничной подкачке установленный объем оперативной памяти, например 32 Мбайт, записывается на диск как файл подкачки, и к нему при необходимости можно получить доступ на диске.

Первый файл подкачки создается автоматически для диска, содержащего ОС. Другие диски по умолчанию не содержат файлов подкачки, и их придется создавать вручную. При создании файла подкачки указывается начальный и максимальный размер. Файлы подкачки записываются на том под именем PAGEFILE.SYS.

Совет Microsoft рекомендует создавать файл подкачки для каждого физического тома в системе. В большинстве систем несколько файлов подкачки увеличивают производительность виртуальной памяти. Вместо одного большого файла подкачки лучше иметь несколько небольших. Помните: съемным носителям файлы подкачки не требуются.

Вот как сконфигурировать виртуальную память.

1. Откройте диалоговое окно Параметры быстродействия (Performance Options) и перейдите на вкладку Дополнительно (Advanced).
2. Щелкните кнопку Изменить (Change), чтобы открыть окно Виртуальная память (Virtual Memory), показанное на рис. 2-7. В нем приводятся следующие сведения.
   - Диск [метка тома] (Drive [Volume Label]) — текущая настройка виртуальной памяти. Каждому тому соответствует свой файл подкачки. Диапазон значений соответствует исходному и максимальному размерам.

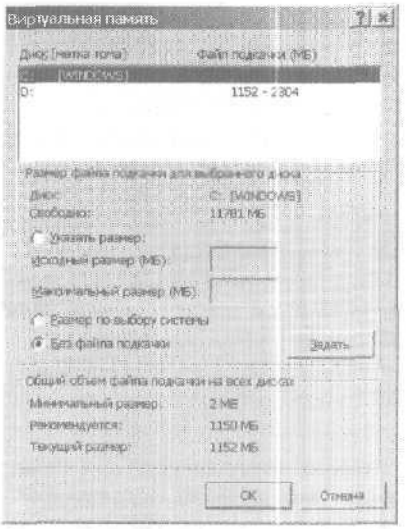


Рис. 2-7. Виртуальная память расширяет объем оперативной памяти на системе .

- Размер файла **подкачки для выбранного диска (Paging file size for selected drive)** — сведения о выбранном в данный момент диске. В поле Свободно (Space Available) показан размер свободного места на диске. Здесь задается размер файла подкачки для выделенного диска.
- **Общий объем файла подкачки на всех дисках (Total paging file size for all drives)** — рекомендуемый объем виртуальной оперативной памяти в системе и реально распределенный объем. Если вы настраиваете виртуальную память впервые, то заметите, что ее объем для системного диска уже задан (в большинстве случаев).

Совет Хотя в Windows Server 2003 предусмотрена возможность расширения файлов подкачки наращиванием их по мере надобности, в результате иногда появляются фрагментированные файлы, что замедляет работу системы. Для оптимальной производительности задайте одинаковое значение для первоначального и максимального размера. В результате файл подкачки станет последовательным, и его можно записать в отдельный непрерывный файл (если это позволит объем тома). В большинстве случаев рекомендуется задать размер файла подкач-

ки, равный удвоенному объему физического ОЗУ системы. Например, для компьютера с объемом ОЗУ 512 Мбайт следует задать общий объем файла подкачки для всех дисков не менее 1024 Мбайт. Однако для серверов с объемом ОЗУ 2 Гбайт и более в отношении размеров файла подкачки следует выполнять рекомендации изготовителя.

3. В списке Диск (Drive) выберите том, с которым собираетесь работать.
4. В группе Размер файла подкачки для выбранного диска (Paging file size for selected drive) сконфигурируйте файл полкачки для диска. Установите переключатель Указать размер (Custom Size), введите исходный и максимальный размеры и щелкните Задать (Set) для сохранения изменений.
5. Повторите пункты 3 и 4 для каждого тома, который хотите настроить.

Примечание Файл подкачки также используется в целях отладки, когда в системе происходит ошибка STOP. Если файл подкачки на системном диске меньше минимального объема, требуемого для записи сведений по отладке в файл подкачки, то эта функция будет отключена. Если вы хотите использовать отладку, минимальный размер файла должен быть равен объему оперативной памяти на системе. Например, система со 256 Мбайт ОЗУ требует файла подкачки размером 256 Мбайт на системном диске.

6. Щелкните OK и, если потребуется, Да (Yes).
7. Закройте окно свойств системы.

Примечание Если вы обновили параметры используемого в данный момент файла подкачки, на экране появится предложение перезагрузить систему, чтобы изменения вступили в силу. Перезагрузку сервера следует проводить в нерабочее время.

Настройка переменных среды для системы и пользователя

Переменные среды системы и пользователя конфигурируются в диалоговом окне Переменные среды (Environment Variables), показанном на рис. 2-8. Чтобы открыть его, откройте окно свойств системы и на вкладке Дополнительно (Advanced) щелкните кнопку Переменные среды (Environment Variables).

Рис. 2-8. Диалоговое окно Переменные среды (Environment Variables) позволяет настраивать переменные среды для системы и пользователя

Создание переменной

Переменные среды создаются следующим образом.

1. Щелкните кнопку Создать (New) под списком Переменные среды пользователя (User Variables) или Системные переменные (System Variables) *в* зависимости от того, какого типа переменную хотите создать. Откроется окно Новая пользовательская переменная (New User Variable) или Новая системная переменная (New System Variable).
2. В поле Имя переменной (Variable Name) введите имя переменной, а в поле Значение переменной (Variable Value) — ее значение.
3. Щелкните OK.

Редактирование переменной

Существующую переменную среды можно изменить.

1. Выберите переменную в списке Переменные среды пользователя (User Variables) или Системные переменные (System Variables).
2. Щелкните кнопку Изменить (Edit) под нужным списком. Откроется диалоговое окно Изменение пользовательской переменной (Edit User Variable) или Изменение системной переменной (Edit System Variable).

3. Введите новое значение в поле Значение переменной (Variable Value).
4. Щелкните OK.

Удаление переменной среды

Переменную среды можно удалить, выбрав в списке и щелкнув кнопку Удалить (Delete).

Примечание При создании или редактировании системных переменных среды изменения вступают в силу только после перезагрузки. При создании или корректировке пользовательских переменных изменения вступают в силу, когда пользователь в следующий раз входит в систему.

Настройка запуска и восстановления системы

Свойства запуска и восстановления системы задаются в диалоговом окне Загрузка и восстановление (Startup and Recovery), показанном на рис. 2-9. Чтобы открыть его, откройте окно свойств системы, перейдите на вкладку Дополнительно (Advanced) и щелкните кнопку Настройка (Settings) в группе Загрузка и восстановление (Startup and Recovery).

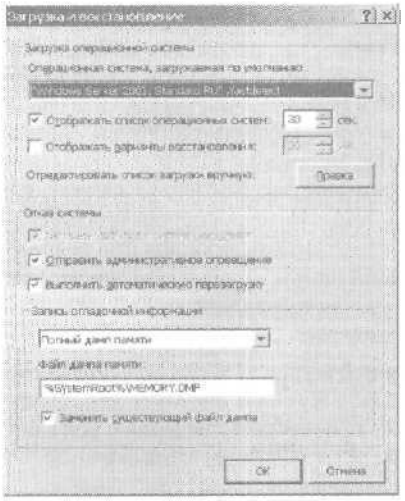


Рис. 2-9. Процедура запуска и восстановления системы конфигурируется в диалоговом окне Загрузка и восстановление (Startup and Recovery)

Настройка параметров запуска

Параметры группы Загрузка операционной системы (System Startup) управляют запуском системы. Выберите ОС по умолчанию из списка Операционная система, загружаемая по умолчанию <Default Operating System). Эти параметры берутся из раздела ОС в системном файле BOOT.INI.

При загрузке Windows Server 2003 по умолчанию отображает меню запуска ОС в течение 30 секунд. Сбросив флажок Отображать список операционных систем (Time to display list of operating systems), вы зададите немедленную загрузку ОС по умолчанию. Установив этот флажок, мы можете задать время в секундах, в течение которого список доступных ОС будет отображаться на экране перед загрузкой ОС по умолчанию. Обычно на большинстве систем для выбора достаточно 3-5 секунд.

Когда система загружается в режиме восстановления, на экране может появиться список вариантов восстановления. Аналогично вариантам стандартного запуска вы можете выбрать один из двух вариантов запуска при восстановлении. Если вы сбросите флажок Отображать варианты восстановления (Time to display recovery options when needed), то сразу начнет загружаться вариант восстановления по умолчанию. Если вы установите его, доступные варианты восстановления будут отображаться в течение заданного вами времени задержки.

Настройка параметров восстановления

Параметры из групп Отказ системы (System Failure) и Запись отладочной информации (Write Debugging Information) в окне Загрузка и восстановление (Startup and Recovery) позволяют управлять восстановлением системы. Изменяя параметры восстановления, администраторы контролируют ситуацию при возникновении в системе неисправимой ошибки (известной также, как ошибка STOP). В области Отказ системы (System Failure) можно установить следующие параметры:

- Записать событие в системный журнал (Write an event to the system log) — запись ошибки в журнале системы, что позволяет администраторам позже просмотреть сведения о ней с помощью консоли Просмотр событий (Event Viewer);
- Отправить административное оповещение (Send an administrative alert) — отправка сообщения заданным адресатам;
- **Выполнить автоматическую перезагрузку (Automatically Restart).**

Примечание Автоматическая перезагрузка не всегда годится. Иногда нужно просто остановить работу ОС, чтобы вы обратили внимание на ошибку, а не сразу перезагрузить систему. Иначе вы узнаете, что ОС перезагружалась, лишь когда просмотрите системный журнал или случайно взглянете на монитор в момент перезагрузки.

Список Запись отладочной информации (Write debugging information) позволяет выбрать тип отладочной информации, которая будет записан в файл дампа. Возможны следующие варианты:

- Отсутствует (None) — выберите этот вариант, если не хотите записывать отладочную информацию в файл;
- **Малый** дамп **памяти (Small Memory Dump)** — в этом варианте записывается только сегмент физической памяти, в котором произошла ошибка. Этот дамп имеет объем 64 кбайт.
- **Дамп памяти ядра (Kernel Memory Dump)** — *Б* этомварианте записывается физическая память, используемая ядром Windows. Размер файла дампа зависит от размера ядра Windows;
- **Полный дамп памяти (Complete Memory Dump)** — в этом варианте записывается вся физическая память, используемая в момент сбоя. Максимальный размер файла дампа равен общему объему физической памяти.

Если вы решили записать файл дампа, укажите его местонахождение. По умолчанию малые дампы размещаются в *%SystemRoot%*\Minidump, а все остальные — в *%SystemRoot%*\Memory.dmp. Обычно имеет смысл установить флажок Заменять существующий файл дампа (Ovenvrite any existing file), чтобы новый файл дампа записывался поверх существующего.

Примечание Дамп памяти удается создать только при правильной настройке системы. Системный диск должен иметь файл подкачки достаточно большого размера, а на диске, куда будет записан файл дампа, необходимо свободное место. Например, на моем сервере 256 Мбайт оперативной памяти, поэтому файл подкачки на системном диске имеет тот же размер. Поскольку тот же диск используется под файл дампа, на нем должно быть минимум 512 Мбайт свободного места для корректного сохранения отладочных сведений (256 Мбайт для файла подкачки и еще 256 Мбайт для дампа).

Включение и отключение отчетов об ошибках

В Windows Server 2003 встроена функция отчетов об ошибках в системе и приложениях. Она передает информацию об ошибках в компанию Microsoft или размещает ее на корпоративном общем диске, где с ней может ознакомиться администратор. По умолчанию во всех версиях Windows Server 2003 создание отчетов об ошибках активизировано. Отдельно отслеживают ошибки следующих категорий:

- **Операционной системы Windows (Windows Operating System)** — создастся отчет о критических системных ошибках, которые привели к появлению печально известного «синего экрана*. Отчет содержит всю информацию, которая выводится на «синий экран»;
- Незапланированных завершений работы (Unplanned Machine Shutdowns) — создается отчет о выключениях сервера, отмеченных как внеплановые. Это позволяет вести статистику времени работы сервера и времени, затраченного на его обслуживание;
- Программ (Programs) — создается отчет о некорректных операциях и внутренних ошибках в прикладных программах, которые приведи к прекращению их выполнения. Вы можете указать, какие программы должны контролироваться на предмет ошибок, а какие — нет. В этом варианте параметром Применять режим очереди для ошибок программ (Force queue mode for program errors) задают режим, когда при следующем входе администратора в систему на экран выводятся последние 10 ошибок. Если этот параметр не задан, сообщается только о последней ошибке.

Способ сообщения об ошибке зависит от того, где она произошла. Когда возникает ошибка в компоненте или программе, на экране появляется диалоговое окно с вопросом, хотите ли вы передать отчет об ошибке. В случае положительного ответа отчет передается через Интернет в компанию Microsoft и на экране появляется диалоговое окно с благодарностью и дополнительной информацией, которая поможет вам устранить проблему. Когда возникает ошибка в операционной системе, отчет об ошибке не создается до тех пор, пока вы не выполните успешную перезагрузку и не войдете в систему.

Вот как включить и настроить отчетность об ошибках.

1. Откройте окно свойств системы, перейдите на вкладку Дополнительно (Advanced) и щелкните кнопку Отчет об ошибках (Error Reporting).
2. Установите переключатель Включить отчет об ошибках (Enable Error Reporting) и укажите, что нужно контролировать.

Совет По умолчанию в отчет включаются все программные ошибки, независимо от изготовителя программ. Выбрав создание отчетности о программах, вы можете изменить параметры по умолчанию. В диалоговом окне Отчет об ошибках (Error Reporting) выберите вариант Программ (Programs), затем щелкните кнопку Выбор программ (Choose Programs) и установите переключатель Только в программах из следующего списка (All programs in this list). Теперь укажите программы, которые хотите добавить в список для создания отчета, и отключите отчетность для программ Microsoft и компонентов Windows. Кроме того, если необходимо, задайте программы, для которых *не нужно* создавать отчет.

3. Дважды щелкните OK.

Вот как выключить отчетность об ошибках.

1. Откройте окно свойств системы, перейдите на вкладку Дополнительно (Advanced) и щелкните кнопку Отчет об ошибках (Error Reporting).
2. Установите переключатель Отключить отчет об ошибках (Disable Error Reporting) и затем щелкните OK.

Способ создания отчета об ошибках также задают с помощью групповых политик, которые подробно рассматриваются в главе 4 и других. Здесь я лишь укажу, где находятся политики, которые позволят вам управлять отчетностью об ошибках. В консоли для работы с групповыми политиками откройте последовательно узлы Конфигурация компьютера (Computer Configuration), Административные шаблоны (Administrative Templates), Система (System) и Отчет об ошибках (Error Reporting).

Совет Сообщения об ошибках отвлекают внимание пользователей, но информация о них помогает Microsoft разрешать соответствующие проблемы. Чтобы не мешать работе и в то же время содействовать улучшению Windows в будущем, отключите политику Отображать уведомления об ошибках (Display Error Notification). В этом случае отчет об ошибке автоматически передается в Microsoft, но пользователи о ней не извещаются.

Ниже описаны две полезные политики отчетности об ошибках.

- Отображать уведомления об ошибках (Display Error Notification) — управляет извещением пользователей о произошедших ошибках. Если эта политика не настроена, параметры сообщений об ошибках задаются в окне свойств системы. Если политика установлена, но отключена, пользователи не получают извещения об произошедших ошибках (при этом отчетность об ошибках не запрещается). Если эта политика включена, пользователи извещаются о произошедшей ошибке и могут создать отчет о ней.
- Отправлять отчет об ошибках (Report Errors) —управляет отчетностью о произошедших ошибках. Если эта политика не настроена, параметры сообщений об ошибках задаются в окне свойств системы. Если эта политика установлена, но отключена, то пользователи не могут создавать отчеты об произошедших ошибках, хотя могут получать сообщения о них. Если эта политика активна, то информация об ошибках передается в компанию Microsoft или на общий диск.

Совет Сохранение отчетов об ошибках в файле коллективного доступа поможет вам, если пользователи не сообщают о проблемах, считая их нормальным явлением.

Вкладка Автоматическое обновление (Automatic Updates)

Вкладка Автоматическое обновление (Automatic Updates) окна свойств системы служит для управления конфигурацией автоматического обновления на сервере. Эта функция рассматривается в главе 5.

Вкладка Удаленное использование (Remote)

Вкладка Удаленное использование (Remote) окна свойств системы служит для управления удаленным помощником (Remote Assistance) и соединениями с помощью удаленного рабочего стола (Remote Desktop). Подробнее — и главе 5.

Управление устройствами и драйверами

В Windows Server 2003 имеется четыре основных инструмента для управления аппаратными устройствами и драйверами:

- Диспетчер устройств (Device Manager);
- Мастер установки оборудования (Add Hardware Wizard);

- Мастер обновленияоборудования (Hardware Update Wizard);
- Программа устранения неполадок (HardwareTroubleshooter).

Эти средства используются при установке, удалении или устранении неисправностей устройств и драйверов. Прежде всего, вам следует ознакомиться с основными сведениями о подписанных (signed) и неподписанных (unsigned) драйверах, а также с системными параметрами, которые могут блокировать применениенеподписанныхдрайверов.

Работа с подписанными и неподписанными драйверами

Microsoftрекомендует по возможности пользоваться подписанными драйверами устройств. Они снабжены цифровой подписью, которая подтверждает, что они прошли строгую проверку в лаборатории Windows Hardware Quality. Кроме того, цифровая подпись означает, что драйвер не подделан.

А что, если для устройства, установленного на сервере, подписанный драйвер отсутствует? Прежде всего следует поискать подписанный драйвер па Web-сайте изготовителя. Возможно, что он есть, но вместе с устройством или на дистрибутивном диске Windows Server 2003 не поставляется. Если найти подписанный драйвер не удалось, придется использовать неподписанный драйвер. В этом случае есть несколько вариантов.

- Установите неподписанный драйвер, например драйвер для Windows 2000. Однако при этом система может стать неустойчивой, что чревато ее «падением», потерей данных и даже невозможностью перезагрузки.
- Совсем откажитесь от этого устройства или подберите на замену устройство с подписанным драйвером. При принятии решения стоимость устройства важный, но не единственный фактор. На борьбу с неустойчивой работой системы вам придется потратить время и средства.

По умолчанию Windows Server 2003 выводит на экран предупреждение, если вы пытаетесь установить неподписанный драйвер. Если вы не хотите, чтобы предупреждение отвлекало вас, измените конфигурацию. Можно также задать условие, чтобы неподписанный драйвер не удавалось установить в систему. Вот один из способов сделать это.

1. Откройте окно свойств системы. Перейдите на вкладку Оборудование (Hardware) и щелкните кнопку Подписывание драйверов (Driver Signing).

2. Выберите действие, которое должна выполнять система при попытке установить неподписанный драйвер. Возможны следующие варианты:
   - Пропускать (Ignore) — установить драйвер в любом случае, не спрашивая подтверждения;
   - Предупреждать (Warn) — выводить предупреждение с предложением выбрать действие;
   - Блокировать (Block) - не устанавливать неподписанные драйверы устройств.
3. Если выбранные параметры должны действовать только для данного пользователя, сбросьте флажок Использовать действие в качестве системного по умолчанию (Make this action the system default).
4. Дважды щелкните OK.

Чтобы назначить параметры драйверов устройств для всех пользонателеи, примените групповую политику Подписывание драйверов устройств (Code signing for device drivers), размещенную в папке Система (System) узла Конфигурация пользователя\Административные шаблоны (User Configuration\Administrative Templates). Если эта политика включена, вы можете указать, какое действие следует предпринять: игнорировать, предупреждать или блокировать.

Совет Если вы пытаетесь установить устройство и обнаружили, что вам не удается установить неподписанный драйвер, прежде всего проверьте параметры настройки для подписи драйверов в окне свойств системы. Если включен параметр Блокировать (Block) и вы не можете его изменить, значит включена политика Подписывание драйверов устройств (Code signing for device drivers) и в ней задан параметр Блокировать (Block). Чтобы установить неподписанный драйвер, необходимо переопределить групповую политику.

Просмотр и управление аппаратными устройствами

Вы можете просмотреть подробный список всех аппаратных устройств, установленных в системе.

1. **Раскройте** меню Администрирование (Administrative **Tools) и** щелкните команду Управление компьютером **(Computer** Management).

2. В консоли Управление компьютером (Computer Management) щелкните значок «плюс» (+) рядом с узлом Служебные программы (System Tools).
3. Выберите Диспетчер устройств (Device Manager). Появится полный список устройств, по умолчанию упорядоченный по их типу.
4. Щелкните значок «плюс» (+) рядом с категорией, чтобы открыть список устройств данного типа.
5. Щелкнув правой кнопкой запись устройства, задайте нужное действие с помощью команд контекстного меню. Доступные команды зависят от типа устройства, но практически всегда включают следующие:
   - **Отключить (Disable)** отключает устройство, но не удаляет его;
   - **Задействовать (Enable)** включает отключенное устройство;
   - **Свойства (Properties)** отображает диалоговое окно свойств устройства;
   - **Удалить (Uninstall)** удаляет устройство и его драйвер;
   - **Обновить драйвер (Update Driver)** позволяет установить более современную версию драйвера.

Совет Если устройство работает с ошибками, в списке рядом с ним отображаются предупреждающие символы. Желтый символ с восклицательным знаком указывает, что с устройством возникли проблемы. **Красный** значок свидетельствует, что **устройство** неправильно установлено или почему-либо отключено пользователем или администратором.

Команды в меню Вид (View) консоли Управление компьютером (Computer Management) позволяют изменять параметры отображения устройств и способа их перечисления.

- **Устройства по типу (Devices by type)** — отображение по тину установленного устройства, например группировка жестких дисков или принтеров (вид по умолчанию).
- **Устройства по подключению (Devices by connection)** — отображение по типу подключения, например, в этом виде отображается системная плата и диспетчер логических дисков.
- **Ресурсы по типу (Resources by** type) — отображение состояния выделенных ресурсов по типу устройства, их использующего. Под

типами ресурсов подразумеваются DMA-каналы, порты ввода-вывода, запрос прерывания (IRQ) и адреса памяти.

- Ресурсы по подключению (Resources by connection) — отображение состояния всех выделенных ресурсов по типу подключения, а не по типу устройства.
- Показать скрытые устройства (Show hidden devices) — отображение устройств, не поддерживающих Plug and Play, а также устройств, отключенных от компьютера, драйверы которых не были удалены.

Настройка драйверов устройств

Для работы ряда устройств, например звуковой платы или адаптера дисплея, требуются драйверы. В Windows Server 2003 имеются удобные инструменты для их настройки и обновления. Они позволяют просматривать информацию о драйверах, устанавливать и обновлять версии драйверов, возвращаться к драйверу, установленному ранее, и удалять драйверы устройств.

Просмотр информации о драйвере

С каждым устройством в системе связан файл драйвера. Вот как можно посмотреть место расположения файла драйвера и его свойства.

1. В консоли Управление компьютером (Computer Management) щелкните знак «плюс» (+) рядом с узлом Служебные программы (System Tools).
2. Выберите Диспетчер устройств (Device Manager). Откроется полный список устройств, установленных в системе. По умолчанию список упорядочен по типам устройств.
3. Щелкните правой кнопкой нужное устройство и выберите команду Свойства (Properties). Откроется диалоговое окно свойств данного устройства. Перейдите на вкладку Драйвер (Driver).
4. Щелкните кнопку Сведения (Driver Details), чтобы открыть диалоговое окно Сведения о файлах драйверов (Driver File Details). Появится информация о следующих параметрах:
   - Файлы драйверов (Driver Files) — список мест размещения файлов драйвера в папке *%SystemRoot%*;
   - Поставщик (Provider) — разработчик драйвера;
   - **Версия файла (File Version).**

Установка и удаление драйверов устройств

Для поддержки устойчивой работы устройств важно иметь текущие версии драйверов. Вот как их установить и обновить.

1. В консоли Управление компьютером (Computer Management) щелкните знак «плюс» (+) рядом с узлом Служебные программы (System Tools).
2. Выберите Диспетчер устройств (Device Manager).
3. Щелкните правой кнопкой нужное устройство и выберите команду Обновить драйвер (Update Driver) для запуска мастера обновления драйверов.

Совет Не устанавливайте последнюю версию драйвера на рабочий сервер без тестирования в лабораторной среде.

4. Укажите, установить драйверы автоматически или вручную, выбрав из списка или указав место размещения драйвера (рис.2-10).

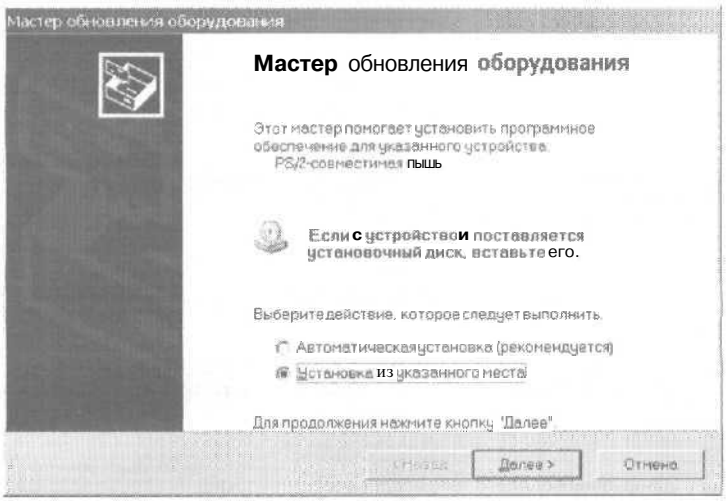


Рис. 2-10. Решите, искать ли нужные драйверы или выбрать из списка известных драйверов

5. При автоматической установке драйвера Windows ищет более позднюю версию драйвера, чем текущая, и, если находит, устанавливает ее. Если более поздняя версия не найдена, сохраняется текущая версия драйвера. В обоих случаях щелк-

ните Готово (Finish) для завершения процесса и пропустите следующие пункты.

6. При руч ной установке драйвера выберите один из следующих вариантов:
   - Выполнить **поиск наиболее подходящего драйвера в указанных местах (Search for the best driver in these locations)** — мастер просматривает системную БД драйверов, а также любые дополнительные места размещения драйверов, которые вы укажете, например дискету или компакт-диск. Отобразятся любые совместимые драйверы, из них можно выбрать подходящий;
   - Не **выполнять** поиск. Я выберу нужный драйвер самостоятельно **(Don't** search. I will choose the driver to install) — в следующем окне мастер показывает список совместимого оборудования и список рекомендуемых драйверов для этого оборудования (рис. 2-11). Если требуемый драйвер есть в списке, укажите его. Если же нет, сбросьте флажок Только совместимые устройства (Show Compatible Hardware). Теперь отобразится список изготовителей, в котором следует найти изготовителя вашего устройства. Щелкните нужное название изготовителя и выберите в списке Модель (Model) подходящий драйвер.

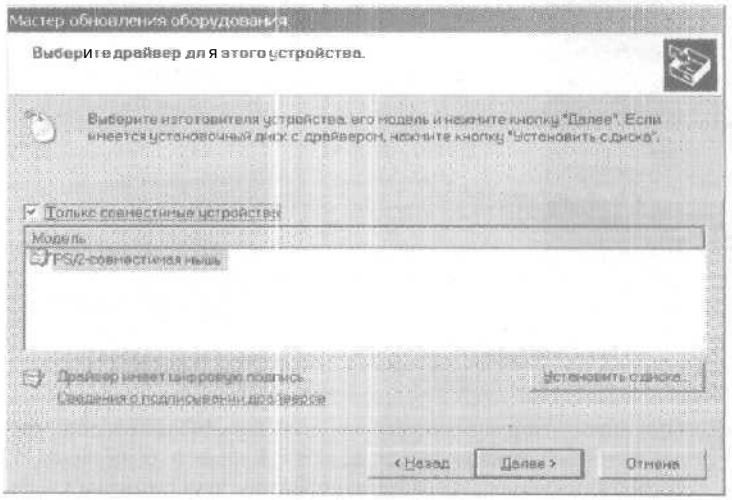


Рис. 2-11. Выберите драйвер устройства по его модели

Возврат к ранее использовавшимся драйверам

Иногда установленный драйвер устройства вызывает неполадки в устройстве или другие серьезные проблемы в системе. Не волнуйтесь, вы можете вернуть в систему ранее установленный драйвер устройства. Вот как это делается.

1. В консоли Управление компьютером (Computer Management) щелкните знак «плюс» (+) рядом с узлом Служебные программы (System Tools).
2. Выберите Диспетчер устройств (Device Manager).
3. Щелкните правой кнопкой нужное устройство и выберите команду Свойства (Properties).
4. Перейдите па вкладку Драйвер (Driver) и щелкните кнопку Откатить (Roll Back Driver). Щелкните Да (Yes).
5. Щелкните OK.

Примечание Если драйвер устройства не обновлялся, то файл резервной копии драйвера отсутствует. В этом случае на экран выводится сообщение, что для этого устройства не создавались резервные копии драйверов.

Удаление драйверов для отсутствующих устройств

Как правило, если вы извлекаете устройство из компьютера, Windows Server 2003 обнаруживает это и автоматически удаляет драйверы для этого устройства. Однако иногда удалять их приходится вручную. Вот как это делается.

1. В консоли Управление компьютером (Computer Management) щелкните знак «плюс» (+) рядом с узлом Служебные программы (System Tools).
2. Выберите Диспетчер устройств (Device Manager).
3. Щелкните правой кнопкой устройство, которое хотите удалить, и выберите команду Удалить (Uninstall).
4. Щелкните OK.

Отмена установки драйверов устройств

При отмене установки драйвера происходит также удаление связанного с драйвером устройства. Если устройство работает неправильно, вы можете отменить установку драйвера, перезагрузить систему, а затем повторно установить драйвер устройства, чтобы восстановить нормальную работу. Вот как это сделать.

1. В консоли Управление компьютером (Computer Management) щелкните знак «плюс» (+) рядом с узлом Служебные программы (System Tools).
2. Выберите Диспетчер устройств (Device Manager).
3. Щелкните правой кнопкой нужное устройство и выберите команду Удалить (Uninstall).
4. Щелкните OK.
5. Перезагрузите систему. Windows обнаружит наличие устройства и автоматически повторно установит требуемый драйвер. Если устройство не было повторно установлено автоматически, установите его вручную, как описано в разделе «Установка нового оборудования» этой главы.

Совет Чтобы предотвратить автоматическую повторную установку устройства, не удаляйте его, а просто отключите.

Управление оборудованием

Технология Plug and Play, реализованная в Windows Server 2003, хорошо справляется с задачей обнаружения и настройки нового оборудования. Однако, если оборудование не поддерживает Plug and Play или не обнаруживается автоматически, вам придется сообщить о нем Windows Server 2003 с помощью Мастера установки оборудования (Add Hardware Wizard). Он же поможет устранить неполадки существующего устройства.

Установка нового оборудования

Вот как установить новое оборудование с помощью Мастера установки оборудования (Add Hardware Wizard).

1. В Панели управления (Control Panel) дважды щелкните значок Установка оборудования (Add Hardware), чтобы запустить мастер. Щелкните Далее (Next).
2. Установите один из двух переключателей.
   - Если вы уже подсоединили оборудование, щелкните переключатель Да, устройство уже подключено (Yes, I have already connected the hardware) и затем кнопку Далее (Next). Откроется окно мастера установки оборудования (рис. 2-12). Переходите к пункту 3.

- Если вы еще не подсоединили оборудование, щелкните переключатель Нет, это устройство еще не подключено (No, I have not added the hardware yet) и затем кнопку Далее (Next). Теперь вам остается только щелкнуть кнопку Готово (Finish). Подсоедините устройство (для чего может потребоваться отключить компьютер) и снова запустите мастер установки оборудования. Остальные пункты пропустите.

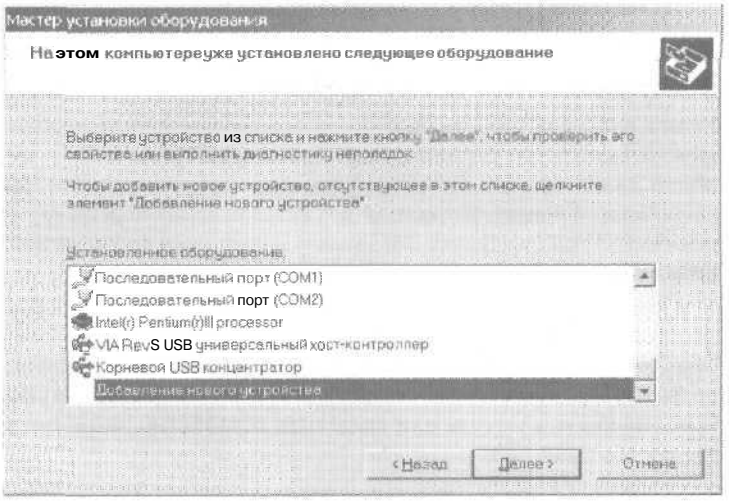


Рис. 2-12. Мастер поможет установить устройство, удалить его или устранить неисправности

3. Чтобы добавить покое оборудование, выберите вариант Добавление нового устройства (Add a new hardware device) в списке Установленное оборудование (Installed Hardware) и щелкните Далее (Next). Этот вариант располагается к самой нижней части списка. В следующем окне определите, должен ли мастер искать новое оборудование или вы хотите выбрать его из списка.
   - Если вы выберете поиск, мастер автоматически обнаружит новое оборудование. Процесс прохождения через псе типы устройств и параметры займет несколько минут. Когда поиск будет завершен, отобразятся все найденные новые устройства и вы сможете выбрать нужное.

- Если вы выберете вариант ввода вручную или если новые устройства не будут найдены автоматически, вам придется самому указать тип оборудования, например Модем (Modem) или Сетевая плата (Network Adapter). Затем щелкните Далее (Next). Найдите в списке изготовителя устройства, а затем в списке справа выберите его модель.

4. Закончив процедуру выбора и установки, щелкните кнопку Далее (Next), а затем — Готово (Finish). Теперь новое устройство готово к работе.

Отключение и включение устройства

Если в работе устройства возникли неполадки, иногда необходимо отменить его установку или отключить. При отмене установки удаляется его сопоставление с драйвером, как если бы устройство физически удалили из системы. При очередном перезапуске Windows Server 2003 может попытаться вновь установить его.

Отключенное устройство не работает, но при этом Windows Server 2003 «в курсе», что оно осталось в системе. Поскольку отключенное устройство не использует системные ресурсы, можно быть уверенным в том, что оно не создает конфликтов в системе. Чтобы отключить или включить устройство, выполните следующие действия.

1. В консоли Управление компьютером (Computer Management) щелкните знак «плюс» (+) рядом с узлом Служебные программы (System Tools),
2. Выберите Диспетчер устройств (Device Manager).
3. Щелкните правой кнопкой нужное устройство и выберите один из следующих вариантой:
   - Задействовать (Enable), чтобы включить устройство;
   - Удалить (Uninstall), чтобы отменить установку устройства;
   - Отключить (Disable), чтобы отключить его.
4. При необходимости щелкните Да (Yes) или OK.

Устранение неполадок оборудования

Мастер установки оборудования позволяет также устранять неполадки оборудования.

1. В Панели управления (Control Panel) дважды щелкните значок Установка оборудования (Add Hardware), чтобы запустить мастер. Щелкните Далее (Next).
2. Установите переключатель Да, устройство уже подключено (Yes, I have already connected the hardware) и щелкните кнопку Далее (Next).
3. В списке устройств выберите то, которое хотите проверить, и щелкните кнопку Далее (Next). В последнем диалоговом окне мастера показан статус устройства. Когда вы щелкнете кнопку Готово (Finish), мастер выполнит одно из двух действий:
   - если вместе со статусом устройства выводится код ошибки, мастер ищет ее описание в справочной системе. Там же должны содержаться и рекомендации по устранению ошибки;
   - мастер запускает программу устранения неполадок оборудования (Hardware Troubleshooter), которая пытается устранить неполадку, анализируя ваши ответы на задаваемые ею вопросы. Для решения проблемы выполняйте советы программы поиска неполадок оборудования.

К программе устранения неполадок можно обращаться и непосредственно.

1. В консоли Управление компьютером (Computer Management) откройте Диспетчер устройств (Device Manager).
2. Щелкните правой кнопкой устройство, неполадки которого хотите устранить, и выберите в контекстном меню команду Свойства (Properties).
3. На вкладке Общие (General) щелкните кнопку Диагностика (Troubleshoot).

Управление динамически подключаемыми библиотеками

Администратору иногда приходится устанавливать динамически подключаемые библиотеки (dynamic-link libraries, DLL) или отменять их установку. Для работы с DLL используется утилита Regsvr32. Она запускается из командной строки. Для установки DLL вводят команду

```
regsvr32 <имя>.dll
```

При необходимости можно отменить регистрацию DLL, задав команду

```
regsvr32 /u <имя>.dll
```

Примечание Защита файлов Windows запрещает замену системных файлов. Вы сможете заменить только те DLL, которые были установлены Windows Server 2003 в составе «заплаток» (hot fix), пакетов обновления или при переходе к новой версии Windows. Защита файлов Windows является важной составной частью архитектуры защиты Windows Server 2003.

Глава 3

Мониторинг процессов, служб и событий

Задача администратора сводится к обеспечению работы сетевых систем. Статус системных ресурсов и их загруженность радикально меняются со временем, причем не всегда так, как хочется. Останавливаются службы, файловая система испытывает недостаток свободного места, ошибки приложений приводят к системным проблемам, в сеть пытаются проникнуть неавторизованные пользователи. В этой главе рассказано, как обнаружить и решить эти и многие другие проблемы с системой.

Управление приложениями, процессами и производительностью

При запуске приложения или вводе команды в командной строке Windows Server 2003 начинает один или несколько процессов. Обычно процессы, запускаемые таким образом (с помощью клавиатуры или мыши), называются *интерактивными* (interactive). Интерактивный процесс, соответствующий приложению или программе, управляет клавиатурой и мышью, пока вы не завершите работу приложения или не перейдете к другой программе. Процесс, осуществляющий такое управление, называется *активным* (foreground).

Процессы могут быть и *фоновыми* (background). Для процесса, запущенного пользователем, это означает, что он продолжает работу, но, как правило, не обладает тем же приоритетом, что активный процесс. Фоновые процессы можно настроить на работу независимо от сеанса пользователя; такие процессы обычно запускает ОС. Примером может служить командный файл, в определенное время запускаемый командой AT. При правильной настройке разрешений файл будет запущен независимо от того, зарегистрирован ли пользователь в системе.

Диспетчер задач

Чтобы открыть основной инструмент управления системными процессами и приложениями — Диспетчер задач (Task Manager), — нужно выполнить одно из перечисленных действий:

- нажать Ctrl+Shift+Esc;
- нажать Ctrl+Alt+Delete и щелкнуть кнопку Диспетчер задач (Task Manager);
- набрать taskmgr в окне Запуск программы (Run) или в командной строке;
- щелкнуть правой кнопкой панель задач и выбрать в контекстном меню команду Диспетчер задач (Task Manager).

Администрирование приложений

На вкладке Приложения (Applications) Диспетчера задач (Task Manager) показан статус программ, работающих в данный момент в системе (рис. 3-1). Кнопки в нижней части вкладки предназначены для выполнения следующих действий.

- Остановка работы приложения — выберите приложение и щелкните кнопку Снять задачу (End Task).
- Переход к приложению — выберите приложение и щелкните кнопку Переключиться (Switch To).

Рис. 3-1. Вкладка Приложения (Applications) Диспетчера задач (Task Manager) показывает статус программ, работающих в системе

- Запуск новой программы — щелкните кнопку Новая задача (New Task) и введите команду для запуска приложения. Кнопка Новая задача (New Task) функционально аналогична команде Выполнить (Run) из меню Пуск (Stare).

Совет В столбце Состояние (Status) указано, нормально ли выполняется приложение. Статус Не отвечает (Not Responding) свидетельствует, что приложение, возможно, «зависло» и вам надо завершить связанные с ним процессы. Однако некоторые приложения не отвечают на запросы ОС в ходе выполнения интенсивных расчетов. Поэтому, прежде чем закрыть приложение, убедитесь, что оно действительно «зависло».

Контекстное меню списка приложений

При щелчке правой кнопкой приложения или группы приложений в списке на вкладке Приложения (Applications) отображается контекстное меню, позволяющее:

- переходить к приложению и делать его активным;
- переводить приложение на передний план;
- сворачивать и восстанавливать приложение;
- изменять расположение окоп приложений;
- закрывать приложение;
- выделять на вкладке Процессы (Processes) процесс, связанный с этим приложением.

Примечание Команда Перейти к процессу (Go to process) полезна. когда вы пытаетесь найти основной процесс для приложения, запустившего несколько процессов.

Администрирование процессов

Подробная информация о выполняемых процессах отображается на вкладке Процессы (Processes), показанной на рис. 3-2. По умолчанию там перечислены только процессы, запущенные ОС, локальными службами, сетевыми службами и интерактивным пользователем, т. е. пользователем, зарегистрировавшимся на локальном компьютере. Чтобы увидеть процессы, запущенные удаленными пользователями, например подключившимися с помощью удаленного рабочего стола, установите флажок Отображать процессы всех пользователей (Show processes from all users).

Рис. 3-2. Подробная информация о процессах на вкладке Процессы (Processes)

В полях на вкладке Процессы (Processes) содержится информация о выполняемых процессах. Она позволяет выявить те из них, что поглощают системные ресурсы, например процессорное время и память. По умолчанию отображаются следующие поля:

- Имя образа (Image Name) — имя процесса или исполняемого файла, запустившего процесс;
- Имя пользователя (User Name) — имя пользователя или системной службы, запустившей процесс;
- ЦП (CPU) — доля ресурсов ЦП (в процентах), занимаемая данным процессом;
- Память (Mem Usage) - объем памяти, занятой процессом В данный момент.

Выбрав в меню Вид (View) команду Выбрать столбцы (Select Columns), вы откроете диалоговое окно, из которого на вкладку Процессы (Processes) можно добавить другие столбцы. Некоторые из них могут оказаться полезными при поисках причин системной проблемы.

- Базовый приоритет (Base Priority) — мера объема системных ресурсов, выделенных процессу Чтобы задать приоритет процесса, щелкните его правой кнопкой мыши, раскройте подменю Приоритет (Set Priority) и выберите нужный вариант — Низкий (Low), Ниже среднего (Below Normal), Средний (Nor-

mal), Выше среднего (Above Normal), Высокий (High) и Реального времени (Real-Time). Большинству процессов по умолчанию назначен средний приоритет. Наивысший приоритет назначается процессам реального времени.

- Время ЦП (CPU Time) — процессорное время, затраченное на выполнение процесса с момента его запуска. Чтобы найти процессы, на выполнение которых расходуется больше всего времени, отобразите этот столбец и щелкните его заголовок, чтобы отсортировать процессы по содержимому столбца.
- Выгружаемый пул (Paged Pool), Невыгружаемый пул (Nonpaged Pool) — выгружаемым пулом называется область системной памяти, предназначенная для объектов, которые при ненадобности можно хранить на диске. Невыгружаемый пул — это область системной памяти для объектов, которые на диск записывать нельзя. Стоит обращать внимание на процессы, которым требуется значительный объем невыгружаемой памяти. Если на сервере недостаточно свободной памяти, эти процессы могут стать причиной большого количества ошибок.
- Ошибок страницы (Page Faults) — ошибка страницы возникает, если процесс запрашивает страницу памяти, а система не находит ее по указанному адресу. Если запрашиваемая страница хранится в другой области памяти, ошибка называется *программной* (soft page fault). Если запрашиваемую страницу приходится считывать с диска, ошибка называется *ошибкой физической памяти* (hard page fault). Процессоры, как правило, справляются с большинством программных ошибок. Ошибки физической памяти могут существенно замедлить работу системы.
- Память — максимум (Peak Memory Usage) — максимальный объем памяти, использованной процессом. На разницу между этим параметром и текущим объемом памяти, занятой процессом, тоже следует обращать внимание. Если приложению, например Microsoft SQL Server, в моменты пиковых нагрузок требуется гораздо больше памяти, чем при обычной работе, возможно, стоит сразу при запуске выделять ему больше памяти.
- Счетчик дескрипторов (Handle Count) — полное число дескрипторов файлов, поддерживаемых процессом. Эта характеристика позволяет оценить, насколько процесс зависит от фай-

ловой системы. С некоторыми процессами связаны тысячи дескрипторов открытых файлов, и каждый из них занимает некоторый объем системной памяти.

- Счетчик потоков (Thread Count) — текущее число потоков, используемых процессом. Большинство серверных приложений являются многопотоковыми, что позволяет одновременно выполнять несколько запросов процесса. Некоторые приложения способны динамически управлять числом одновременно исполняемых потоков, что позволяет повысить их производительность. Чрезмерное увеличение количества потоков ухудшает производительность, так как ОС приходится слишком часто переключать контексты потоков.
- Число чтений (I/O Reads), Число записей (I/O Writes) — полнос число операций чтения с диска и записи на диск с момента запуска процесса. Этот параметр показывает, насколько активно процессом используется диск. Если рост числа операций ввода-вывода не согласуется с реальной активностью сервера, процесс, вероятно, не способен кэшировать файлы или кэширование файлов неверно настроено.

Примечание В списке процессов на вкладке Процессы (Processes) вы заметите процесс Бездействие системы (System Idle Process). Он отслеживает объем неиспользуемых ресурсов. Так, число 99 в столбце ЦП (CPU) означает, что 99% системных ресурсов в настоящий момент не используется. Приоритет этого процесса задать нельзя.

Просматривая информацию о процессах, помните, что одно приложение может породить несколько процессов. Обычно все они зависят от центрального процесса и формируют расходящееся от него *дерево процессов* (process tree). Чтобы найти главный процесс для данного приложения, на вкладке Приложения (Applications) щелкните приложение правой кнопкой и выберите команду Перейти к процессу (Go To Process). Чтобы корректно завершить работу приложения с помощью диспетчера задач, останавливайте либо само приложение, либо его главный процесс. Не останавливайте по отдельности зависимые процессы.

Остановить главный процесс приложения и порожденные им вторичные процессы можно несколькими способами:

- выделите приложение на вкладке Приложения (Applications) и щелкните кнопку Снять задачу (End Task);

- на вкладке Процессы (Processes) щелкните правой кнопкой главный процесс приложения и выберите команду Завершить процесс (End Process);
- на вкладке Процессы (Processes) щелкните правой кнопкой главный или вторичный процесс приложения и выберите команду Завершить дерево процессов (End Process Tree).

Мониторинг загруженности системы

На вкладке Быстродействие (Performance) в виде фафиков и статистических данных отображается степень использования процессора и памяти (рис. 3-3). Эта информация позволяет быстро оценить нагрузку па системные ресурсы. Чтобы получить более подробные сведения, используйте консоль Производительность (Performance).

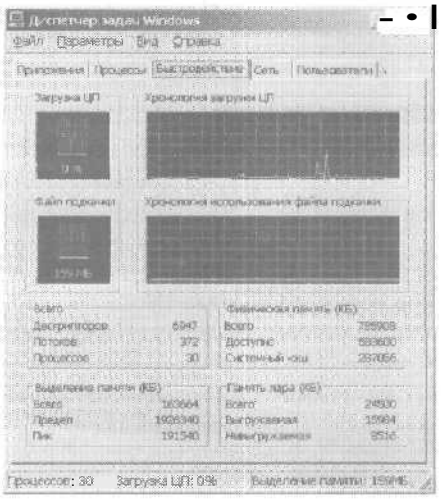


Рис. 3-3. Вкладка Быстродействие (Performance) позволяет быстро проверить использование системных ресурсов

Графики на вкладке Быстродействие (Performance)

На графиках вкладки Быстродействие (Performance) отображена следующая информация:

- **Загрузка ЦП (CPU Usage)** — процент используемых в данный момент ресурсов процессора;

- Хронология загрузки ЦП (CPU Usage History) — трафик изменения нагрузки на процессор. Частоту обновления информации на графике можно настраивать. Чтобы увеличить диаграмму, щелкните ее дважды. Повторный двойной щелчок вернет обычный режим просмотра;
- Файл подкачки (PF Usage) — объем файла подкачки (т. е. виртуальной памяти), занятый системой в настоящий момент;
- **Хронология использования файла подкачки (Page File Usage History) — график использования файла подкачки.**

Примечание Если нагрузка на процессор остается неизменно высокой даже в обычных условиях, для выяснения причин этого стоит, вероятно, заняться более детальным исследованием работы системы. Зачастую причина снижения производительности скрыта в памяти. Проверьте эту возможность, прежде чем принимать решение об обновлении процессора или о добавлении новых процессоров. Подробнее — далее в этой главе.

Настройка и обновление отображения графиков

Настроить или обновить отображение графиков помогут команды меню Вид (View).

- Команда Скорость обновления (Update Speed) позволяет изменить скорость обновления графиков, а также приостановить обновление. Вариант Низкая (Low) соответствует обновлению каждые 4 секунды, вариант Обычная (Normal) — обновлению каждые 2 секунды, вариант Высокая (High) — обновлению дважды в секунду.
- Команда Загрузка ЦП (CPU History) в многопроцессорных системах позволяет задать отображение графиков для отдельных процессоров — отдельная диаграмма для каждого процессора или все графики на одной диаграмме.
- Команда **Вывод времени ядра (Show Kernel Times) позволяет** отобразить процессорное время, использованное ядром ОС. Ресурсы, используемые ядром, на графиках отображаются красными линиями.

Под графиками приведены статистические данные.

- Всего (Totals) — общая информация о загрузке процессора. В поле Дескрипторов (Handles) указано количество используемых дескрипторов ввода-вывода, в поле Потоков (Thre-

ads) — число потоков, в поле Процессов (Processes) — число процессов.

- **Выделение памяти (Commit Charge)** — информация об общем объеме памяти, используемой ОС. В поле Всего (Total) отображается объем физической и виртуальной памяти, используемой в данный момент, в поле Предел (Limit) — вся доступная физическая и виртуальная память, в поле Пик (Peak) — максимальный объем памяти, использованный системой с момента загрузки. Если значение в поле Пик (Peak) отличается от значения в поле Предел (Limit) менее, чем на 10%, в систему нужно установить дополнительную физическую память или увеличить объем виртуальной памяти.
- **Физическая память (Physical Memory)** — информация об общем объеме оперативной памяти в системе. В ноле Всего (Total) указан объем **физической** оперативной памяти, в поле Доступно (Available) — оперативная память, не используемая в данный момент, в поле Системный кэш (System cache) — память, используемая ОС для кэширования. Если доступный объем памяти невелик (скажем, менее 5% всей физической памяти), стоит подумать об установке дополнительной памяти.
- **Память ядра** (Kernel **Memory)** — информация о памяти, используемой ядром ОС. Значительная часть ядра должны работать в оперативной памяти и не может выгружаться в виртуальную память. Объем этой памяти указан в иоле Невыгружаемая (Nonpaged). Объем памяти ядра, которую допустимо выгружать в виртуальную память, отображен в поле Выгружаемая (Paged). Общий объем памяти, используемой ядром, указан в поле Всего (Total).

Мониторинг производительности сети

На вкладке Сеть (Networking) приводятся сведения о сетевых адаптерах, используемых системой, — процент загрузки, скорость соединения и статус.

Если в системе установлен единственный сетевой адаптер, на сводной диаграмме (рис. 3-4) показана информация об изменении со временем трафика через этот адаптер. Если сетевых адаптеров в системе несколько, на диаграмме отображается сводный показатель использования всех сетевых подключений. По умолчанию это суммарное количество байт, переданных но сети. Что-

бы вынести другую характеристику, щелкните меню Вид (View), раскройте подменю Журнал сетевого адаптера (Network History) и выберите в нем команду Отправлено байт (Bytes Sent), Получено байт (Bytes Received) или обе. Отправленные байты выделены красным цветом, полученные — желтым. Суммарное количество байт отображается зеленым цветом.

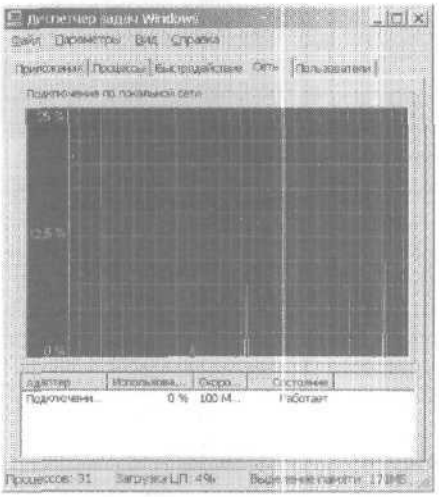


Рис. 3-4. Сведения о производительности сети

В полях вкладки Сеть (Networking) содержится множество сведений о входящем и исходящем сетевом трафике сервера. С их помощью можно, например, установить объем поступающих на сервер данных. По умолчанию отображаются следующие поля:

- Адаптер (Adapter Name) — имя, под которым адаптер значится в папке Сетевые подключения (Network Connections);
- Использование сети (Network Utilization) — загрузка сети в процентах от исходной скорости подключения для данного интерфейса. Например, адаптер с исходной скоростью подключения 100 Мбит/с и текущим трафиком 10 Мбит/с загружен на 10%;
- **Скорость линии (Link Speed)** — скорость подключения через данный интерфейс;
- **Состояние (State)** — состояние сетевого адаптера.

Совет Если загрузка адаптера часто достигает 50% или больше, повнимательнее следите за сетевой активностью сервера и подумайте о приобретении дополнительных сетевых адаптеров. Но будьте осторожны, планируя модернизацию: проблем в этом процессе больше, чем кажется, причем связанных не только с сервером, но и с сетью в целом. Подумайте, не превысите ли вы полосу пропускания, выделенную вам провайдером внешнего соединения — на ее увеличение может уйти не один месяц.

Для исследования работы сети вам могут понадобиться дополнительные столбцы на вкладке Процессы (Processes). Выберите в меню Вид (View) команду Выбрать столбцы (Select Columns) и установите один из флажков:

- **Пропускная способность отправки (Bytes SentThroughput)** - процент использования текущей полосы пропускания исходящим трафиком;
- **Пропускная способность получения (Bytes Received Throughput)** — процент использования текущей полосы пропускания входящим трафиком;
- **Пропускная способность всего (Bytes Throughput)** — процент использования текущей полосы пропускания всем трафиком через данный адаптер;
- **Отправлено байт (Bytes Sent)** — полное число байт, отправленных по данному подключению;
- **Получено байт (Bytes Received)** — полное число байт, полученных по данному подключению;
- **Байт (Bytes Total)** — полное число байт, переданных по данному подключению в обоих направлениях.

Мониторинг удаленных подключений

Удаленные пользователи подключаются к системе через службы терминалов или удаленные рабочие столы. Подключения с помощью удаленного рабочего стола активизируются автоматически при установке Windows Server 2003. Диспетчер задач (Task Manager) предоставляет один из способов управления такими подключениями. Перейдите на вкладку Пользователи (Users), где перечислены интерактивные пользовательские сеансы как для локальных, так и для удаленных пользователей.

Для каждого подключения указаны имя пользователя, код сеанса, состояние, клиентский компьютер и тип сеанса. Пользователю, зарегистрировавшемуся локально, соответствует тип сеанса Console. Для других пользователей в этом столбце указаны тип и протокол подключения, например RDP-TCP для подключения с помощью протокола RDP (Remote Desktop Protocol) и транспортного протокола TCP. Щелкнув сеанс правой кнопкой мыши, вы получите доступ к следующим командам:

- **Подключить (Connect)** — подключение неактивного сеанса;
- Отключить (Disconnect) — насильственное отключение пользовательского сеанса. завершение всех запущенных пользователем приложений без сохранения данных;
- Выход из системы (Log Off) — нормальное завершение пользовательского сеанса. Данные приложений и состояния системы сохраняются, как при обычном выходе из системы;
- Удаленное управление (Remote Control) — задание «горячей клавиши» для завершения сеанса удаленного управления (по умолчанию Ctrl+*);
- **Отправить сообщение (Send Message)** — отправка сообщения консоли пользователям, зарегистрировавшимся на удаленных системах.

Управление системными службами

Службы предоставляют ключевые функции системам Windows Server 2003. Для управления системными службами предназначена программа Службы (Services) из консоли Управление компьютером (Computer Management), которая открывается следующим образом.

1. Щелкните кнопку Пуск (Start), откройте подменю Администрирование (Administrative Tools) и выберите в нем команду Управление компьютером (Computer Management).
2. Щелкните правой кнопкой элемент Управление компьютером (Computer Management) в дереве консоли и выберите команду Подключиться к другому компьютеру (Connect to another computer). Теперь можно выбрать систему, службами которой вы хотите управлять.
3. Откройте узел Службы и приложения (Services and Applications), щелкнув значок «плюс» (+) рядом с ним, затем выберите элемент Службы (Services).

Примечание В Windows Server 2003 предусмотрены и другие способы доступа к службам, например, через элемент Службы (Services) консоли Службы компонентов (Component Services).

Взгляните на узел Службы (Services) консоли Управление компьютером (Computer Management), показанной на рис. 3-5. Основные поля этого окна перечислены ниже:

- Имя (Name) — имя службы. Здесь перечислены только службы, установленные в системе. Дважды щелкните имя службы, чтобы задать параметры ее запуска;

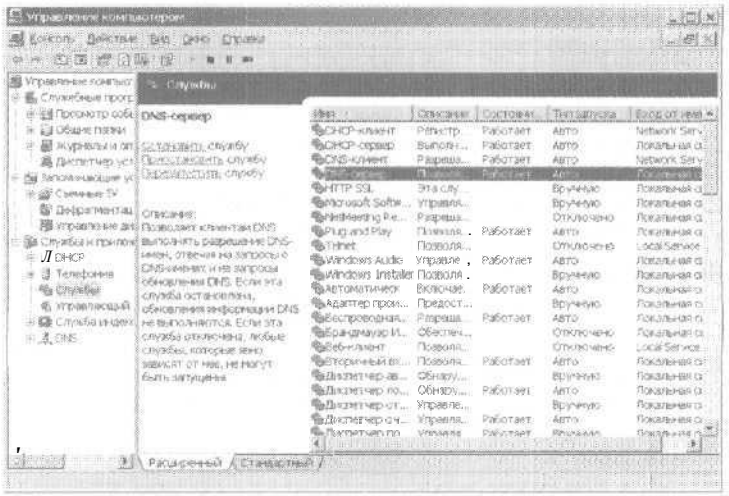


Рис. 3-5. Узел Службы (Services) для управления службами на серверах и рабочих станциях

- Описание (Description) — краткое описание службы и ее назначения;
- Состояние (Status) — состояние службы: работает, приостановлена или остановлена (для остановленных служб этот столбец пуст);
- Тип запуска (Startup Type) — параметры запуска службы. Автоматические службы запускаются при загрузке системы. Ручные службы запускаются пользователями или другими службами. Отключенные службы не запустятся, пока вы их не включите;

- Вход от имени (Log On As) — учетная запись, под которой служба входит в систему. Обычно по умолчанию используется локальная учетная запись системы.

Для просмотра узла Службы (Services) можно использовать два представления — расширенное (extended) и стандартное (standard). Чтобы выбрать нужное представление, щелкните соответствующий ярлычок в нижней части панели Службы (Services). В расширенном представлении помимо списка служб приводятся также гиперссылки для управления ими. Щелкните ссылку Запустить (Start), чтобы запустить остановленную службу Ссылка Перезапустить (Restart) позволяет остановить и тут же снова запустить службу. Кроме того, при выделении службы в расширенном представлении на экране отображается ее краткое описание.

Примечание Возможность отключения службы предоставлена как пользователям, так и самой ОС. Обычно Windows Server 2003 отключает службу, если она конфликтует с другой службой.

Запуск, остановка и приостановка служб

Чтобы запустить, остановить или приостановить службу Windows Server 2003, нужно выполнить следующие действия.

1. Откройте консоль Управление компьютером (Computer Management).
2. Щелкнув правой кнопкой узел Управление компьютером (Computer Management) в дереве консоли, выберите команду Подключиться к другому компьютеру (Connect to another computer). Теперь можно указать систему, службами которой собираетесь управлять.
3. Откройте узел Службы и приложения (Services and Applications), щелкнув значок «плюс» (+) рядом с ним, затем выберите элемент Службы (Services).
4. Щелкните правой кнопкой нужную службу и выберите в контекстном меню команду Пуск (Start), Стоп (Stop), Перезапустить (Restart) или Пауза (Pause). Чтобы возобновить работу приостановленной службы, выберите команду Продолжить (Resume).

Примечание Если системе не удается запустить службу, для которой задан автоматический запуск, она обычно сообщает об этом с помощью информационного окна (можно также задать добавление записи об этом сбое в журнал событий си-

стемы). Поле состояния для этой службы остается пустым. При желании вы можете указать ОС действие, которое она должна выполнить при неудачном запуске службы, например попытаться перезапустить ее. Подробнее об этом — в разделе «Настройка восстановления службы».

Настройка запуска службы

Службу Windows Server 2003 можно настроить на ручной или автоматический запуск, а также вообще выключить.

1. В консоли Управление компьютером (Computer Management) установите соединение с компьютером, службами которого хотите управлять.
2. Откройте узел Службы и приложения (Services and Applications), щелкнув значок «плюс» (+) рядом с ним, затем выберите элемент Службы (Services).
3. Щелкните правой кнопкой службу, которую хотите настроить, и выберите команду Свойства (Properties).
4. На вкладке Общие (General) в списке Тип запуска (Startup Type) задайте параметры запуска (рис. 3-6). Выберите вариант Авто (Automatic), чтобы запускать службу при загрузке системы, вариант Вручную (Manual), чтобы запускать службу вручную, или Отключено (Disabled), чтобы отключить ее.
5. Щелкните OK.

Рис. 3-6. В списке Тип запуска (Startup Type) задается способ запуска службы

Совет Если на сервере задано несколько профилей, вы можете независимо включать и выключать службы в каждом из них. Прежде чем навсегда отключить службу, создайте специальный проверочный профиль и убедитесь, что сервер будет нормально работать без нее. Чтобы отключить или включить службу в конкретном профиле, перейдите на вкладку Вход в систему (Logon) окна со свойствами службы. Выделите нужный профиль в списке Профиль оборудования (Hardware Profile) и щелкните кнопку Разрешить (Enable) или Запретить (Disable).

Настройка входа службы в систему

Службу Windows Server 2003 можно настроить на вход в систему с учетной записью системы или конкретного пользователя.

1. В консоли Управление компьютером (Computer Management) установите соединение с компьютером, службами которого собираетесь управлять.
2. Откройте узел Службы и приложения (Services and Applications), щелкнув значок «плюс» (+) рядом с ним, затем выберите элемент Службы (Services).
3. Щелкните правой кнопкой службу, которую хотите настроить, и выберите команду Свойства (Properties).
4. Перейдите па вкладку Вход в систему (Log On), показанную на рис. 3-7.
5. Установите переключатель С системной учетной записью (Local System Account), если служба должна регистрироваться под учетной записью системы (по умолчанию для большинства служб). Если у службы есть пользовательский интерфейс, установите флажок "Разрешить взаимодействие с рабочим столом (Allow service to interact with desktop), чтобы пользователи могли к нему обратиться.
6. Установите переключатель С учетной записью (This Account), если служба регистрируется под учетной записью конкретного пользователя. Введите в соответствующих полях имя учетной записи и пароль. Учетную запись можно также найти посредством кнопки Обзор (Browse).
7. Щелкните OK.

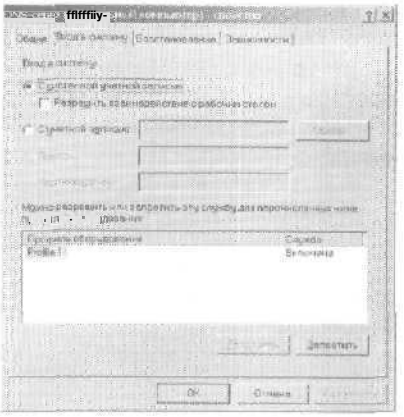


Рис. 3-7. Вкладка Вход в систему (Log On) служит для настройки учетной записи службы

Внимание! Администратор должен пристально следить за всеми учетными записями, которые используются службами. При неправильном конфигурировании эти учетные записи могут стать источником серьезных проблем с безопасностью. Назначайте учетным записям служб лишь те права, которые необходимы им для работы; во всем остальном их следует ограничить строжайшим образом. Относитесь к ним, как к административным учетным записям: назначайте им безопасные пароли, тщательно отслеживайте их использование и т. д.

Настройка восстановления службы

В Windows Server 2003 можно задать действие, которое будет выполняться в случае сбоя службы, например запуск приложения или попытку перезапуска службы. Чтобы настроить параметры восстановления службы, сделайте следующее.

1. В консоли Управление компьютером (Computer Management) установите соединение с компьютером, который собираетесь управлять.
2. Откройте узел Службы и приложения (Services and Applications), щелкнув значок «плюс» (+) рядом с ним, затем выберите элемент Службы (Services).
3. Щелкните правой кнопкой службу, которую хотите настроить, и выберите команду Свойства (Properties).

4. Перейдите на вкладку Восстановление (Recovery), показанную на рис. 3-8.

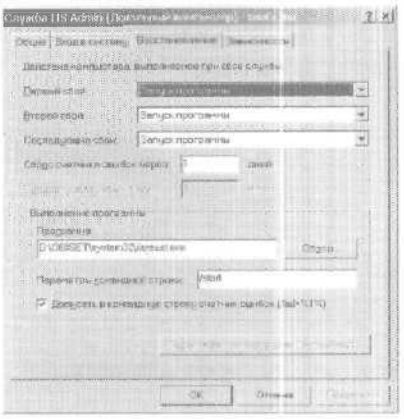


Рис. 3-8. Вкладка Восстановление (Recovery) позволяет определить действия на случай сбоя службы

Примечание При установке Windows Server 2003 автоматически задается восстановление некоторых важных системных служб. На рис. 3-8 видно, что служба IIS Admin настроена на запуск программы iisreset.exe, которая устраняет проблемы в службе, не нарушая работу зависимых US-служб. Обратите внимание, что для iisreset.exe задан параметр командной строки /start.

5. Теперь можно настраивать параметры восстановления для первой, второй и дальнейших попыток восстановления. Доступны следующие варианты:

   - **Не выполнять никаких действий (Take No Action) — при** сбое ОС не будет делать ничего, но это не означает, что при последующих или предыдущих сбоях также не были или не будут предприняты какие-либо действия;
   - **Перезапуск службы (Restart the Service) —** служба будет остановлена, а затем после небольшой паузы запущена снова;
   - **Запуск программы (Run a File)** — в случае неудачного запуска службы будет запущена программа, командный файл или сценарий Windows. Если вы выберете этот вариант, вам придется задать полный путь к программе и необходимые параметры командной строки;

- Перезагрузка компьютера (Reboot the Computer) — компьютер будет выключен и включен снова. Прежде чем выбрать этот вариант, перепроверьте параметры запуска и восстановления системы и настройку профилей (подробнее об этом — в главе 2).

Совет При первых двух сбоях важной службы ее можно попробовать перезапустить, при третьем сбое — перезагрузить сервер.

6. Задайте другие параметры, основываясь на выбранных параметрах восстановления. Если вы решили выполнить программу, задайте параметры в области Выполнение программы (Run Program). Если вы решили перезапустить службу, определите задержку перезапуска. После остановки службы Windows Server 2003 ждет в течение указанного срока до попытки запустить службу. Обычно достаточно подождать 1-2 минуты.
7. Щелкните OK.

Отключение ненужных служб

В задачу администратора входит обеспечение безопасности сервера и сети, а ненужные службы потенциально угрожают этой безопасности. Во многих организациях, безопасность сетей в которых мне приходилось проверять, я обнаруживал серверы с запущенными службами WWW Publishing Service, SMTP и ETP Publishing Service, хотя надобности в них совершенно не было. А ведь эти службы открывают доступ к серверу анонимным пользователям. Если сервер при этом не очень продуманно сконфигурирован, последствия могут оказаться печальными.

Есть несколько способов избавиться от ненужных служб. Некоторые из них, например IIS Admin и DNS, устанавливаются как отдельные компоненты Windows, поэтому для их удаления можно воспользоваться инструментом Установка и удаление программ (Add/Remove Programs) панели управления. Альтернативный вариант — просто отключить службу. Как правило, стоит начать с отключения служб, не прибегая сразу к отмене установки. Представьте себе, что вы отключили службу, но тут же посыпались жалобы пользователей, которые лишились возможности выполнять определенное действие. В этом случае отключенную службу легко активизировать снова.

Чтобы отключить службу, выполните следующие действия,

1. Щелкните правой кнопкой службу, которую хотите отключить, и выберите команду Свойства (Properties).

2. На вкладке Общие (General) выберите в списке Тип запуска (Startup Type) вариант Отключено (Disabled).

Отключение службы не останавливает ее немедленно. Она *всею* лишь не будет запущена при следующей загрузке компьютера. Чтобы остановить отключенную службу, щелкните кнопку Стоп (Stop) на вкладке Общие (General) диалогового окна со свойствами службы, а затем щелкните OK.

Создание и просмотр журналов

В журналах событий хранится хронологическая информация, которая помогает выявлять проблемы в системе и обеспечивать безопасность. События в системах Windows Server 2003 контролирует служба Журнал событий (Event Log). Если она запущена, вы можете проследить действия пользователя и события, связанные с обращением к системным ресурсам по следующим журналам:

- **Безопасность (Security)** — события аудита, заданные с помощью локальной или глобальной групповой политики. Расположение по умолчанию *%SystemRoot%*\system32\config\SecEvent.Evt;

Примечание Чтобы получить доступ к журналу безопасности, пользователь должен обладать правом Управление аудитом и журналом безопасности (Manage Auditing And Security Log). По умолчанию оно назначено членам группы Администраторы (Administrators). О назначении прав пользователя — в главе 9.

- **Приложение (Application)** — события, порожденные приложениями, например сбой MS SQL при доступе к базе данных. Расположение по умолчанию — *%SystemRoot%*\system32\config\AppEvent.Evt;
- **Система (System)** — события, записанные в журнал ОС или ее компонентами, например сбой в запуске службы при перезагрузке. Расположение по умолчанию — *%SystemRoot%*\system32\config\SysEvent.Evt;
- **Служба репликации файлов (File Replication Service)** — события, связанные с репликацией файлов. Расположение по умолчанию — *%SystemRoot%*\system32\config\NtFrs.Evt;
- **Служба каталогов (Directory Service)** — события, порожденные Active Directory и относящимися к ней службами. Расположение по умолчанию — *%SystemRoot%*\system32\config\NTDS.Evt;

- DNS-сервер **(DNS** Server) — запросы и ответы на них, а также другие действия DNS. Расположение по умолчанию — *%SystemRoot%*\system32\config\DNSEvent.Evt.

Совет Администраторы, внимательно просматривающие журналы приложений и системы, иногда забывают о журнале безопасности. А ведь он — один из важнейших, и пренебрегать им нельзя. Если в журнале безопасности сервера нет ни одной записи, вы, скорее всего, не настроили локальную политику аудита или же аудит проводится на уровне домена. В последнем случае журнал безопасности нужно просматривать на контроллере домена, а не на рядовом сервере.

Работа с журналами

Доступ к журналам событий осуществляется так.

1. С помощью консоли Управление компьютером (Computer Management) установите соединение с компьютером, журналы событий которого хотите просмотреть.
2. Откройте узел Служебные программы (System Tools) и щелкните дважды элемент Просмотр событий (Event Viewer).
3. Выделите журнал, который хотите просмотреть. На экране появится список записанных в него событий (рис. 3-9).

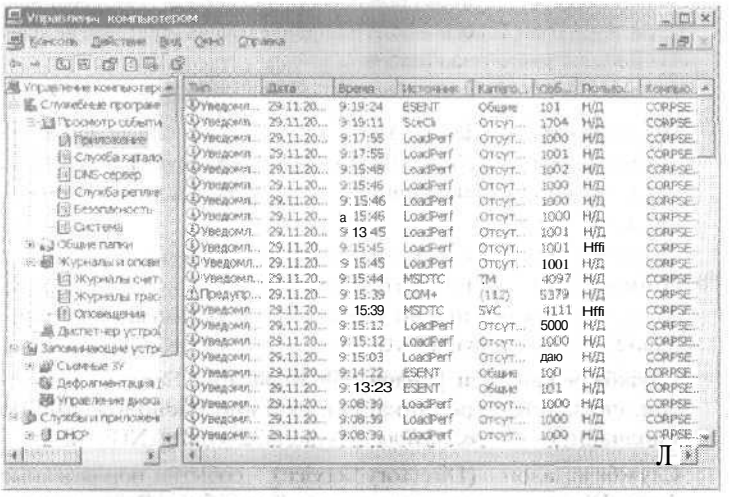


Рис. 3-9. Справа показаны события для выбранного журнала

На правой панели оснастки Просмотр событий (Event Viewer) показано, когда, где и что произошло. Чтобы получить подробную информацию о событии, дважды щелкните его. В первом столбце указан тип события:

- **Уведомление (Information)** — событие, как правило, связанное с успешным действием;
- **Аудит успехов (Success Audit)** — событие, связанное с успешным выполнением действия;
- **Аудит отказов (Failure Audit)** — событие, связанное со сбоем в выполнении действия;
- **Предупреждение (Warning)** — событие, в будущем способное вызвать проблемы с системой;
- **Ошибка (Error)** — ошибка, например, неудачный запуск службы.

Помимо тина, даты и времени, в краткой и подробной записи о событии содержите я следующая информация:

- **Источник (Source)** — приложение, служба или компонент, записавший событие;
- **Категория (Category)** — категория события, иногда используемая для его более подробного описания;
- **Событие (Event)** — код события;
- **Пользователь (User)** — учетная запись пользователя, действовавшая в момент события;
- **Компьютер (Computer)** — имя компьютера, на котором произошло событие;
- **Описание (Description)** — текстовое описание события;
- **Данные (Data)** — любые данные, сгенерированные событием, или связанный с ним код ошибки.

Настройка параметров журнала событий

Размер и способ ведения журналов событий можно настраивать. По умолчанию максимальный размер файлов журналов событий — 512 кбайт. По умолчанию, когда размер журнала достигает этого предела, новые события переписываются поверх старых. Чтобы изменить этот порядок, выполните следующие действия.

1. В консоли Управление компьютером (Computer Management) щелкните дважды элемент Просмотр событий (Event Viewer). Появится список журналов событий.

2. Щелкните правой кнопкой журнал событий, параметры которого хотите настроить, и выберите в контекстном меню команду Свойства (Properties). Откроется диалоговое окно, показанное на рис. 3-10.

Рис. 3-10. Задайте параметры журнала

3. Введите новое значение в поле Максимальный размер журнала (Maximum Log Size). Убедитесь, что на диске хватает свободного места для файлов заданного размера. По умолчанию файлы журналов хранятся в папке *%SystemRoot%*\system32\config.
4. Задайте действие при достижении максимального размера журнала:
   - Затирать старые события по необходимости (Overwrite events as needed) — события в журнале переписываются при достижении максимального размера файла. Как правило, это оптимальный вариант;
   - Затирать события старее ... дней (Overwrite events older than ... days) — при достижении максимального размера файла события в журнале переписываются, только если они старше заданного срока. Если таких событий нет, система выдает сообщение об ошибке переполнения журнала;
   - **Не затирать события (очистка журнала вручную) [Do not overwrite events (clear log manually)]** — при достижении максимального размера файла система сообщает об ошибке переполнения журнала.

5. Щелкните OK.

Примечание В системах, где безопасность и ведение журналов событий очень важны, следует использовать перезапись только старых событий или полностью отказаться от перезаписи журналов. При этом журналы нужно периодически архивировать и очищать, чтобы система не выдавала сообщения об ошибке.

Очистка журналов событий

Когда журнал событий заполнен, его следует очистить.

1. В консоли Управление компьютером (Computer Management) дважды щелкните элемент Просмотр событий (Event Viewer). Появится список журналов событий.
2. Щелкните правой кнопкой нужный журнал и выберите команду Стереть все события (Clear All Events).
3. Щелкните кнопку Да (Yes), чтобы перед очисткой сохранить записи, или Нет (No), если сохранять их не требуется.
4. Если система попросит подтвердить очистку журнала, щелкните Да (Yes).

Архивирование журналов событий

На некоторых ключевых системах, например контроллерах домена и серверах приложений, журналы необходимо хранить несколько месяцев. Но вряд ли стоит для этого увеличивать максимальный размер журнала. Достаточно его периодически архивировать.

Форматы архивов журналов

Журналы можно архивировать в трех форматах:

- двоичном для просмотра в оснастке Просмотр событий (Event Viewer);
- текстовом с разделением полей табулятором;
- текстовом с разделением полей запятыми.

В последнем случае записи **о событиях выглядят так.**

```
17.09.2003,15:12:31,MSDTC,Уведомления,SVC,4097,Нет
данных,ZETA,Выполнен запуск MS DTC.

21.09.2003,7:21:09,WINSCTRS,Ошибка,Отсутствует,4314,Нет
данных,ZETA,Счетчикам системного монитора WINS не удалось
получить статистику WINS.
```

Формат записей таков:

дата, время, источник, тип, категория, событие, пользователь, компьютер, описание.

Архивирование журналов в двоичном формате

Архив журнала в двоичном формате создается так,

1. В консоли Управление компьютером (Computer Management) дважды щелкните Просмотр событий (Event Viewer). Появится список журналов событий.
2. Щелкнув правой кнопкой нужный журнал, выберите команду Сохранить файл журнала как (Save Log File As).
3. В открывшемся окне выберите папку и имя файла для сохранения журнала.
4. Задайте нужный тип журнала и щелкните Сохранить (Save). Обычно нужный формат — Журнал событий (*.evt) [Event Log (*.evt)] — задан по умолчанию.

Совет Создайте специальную папку для архивных журналов — это облегчает их поиск. Файлу журнала давайте имя, по которому можно определить тип журнала и время архивирования. Скажем, если вы архивируете системный файл журнала за январь 2003 г., можете использовать имя файла System Log Jan 2003.

Совет Удобнее всего архивировать журналы в формате оснастки Просмотр событий (Event Viewer) — .evt. Текстовые форматы понадобятся вам для просмотра журналов в других приложениях. Иногда перед импортом в базу данных или в электронную таблицу текстовый файл с разделителями-табуляторами или запятыми приходится дополнительно редактировать. Если вы сохранили журнал в формате .evt, позже его можно открыть в оснастке Просмотр событий (Event Viewer) и сохранить в текстовом формате.

Просмотр архивов журналов

Архивы журналов в текстовом формате можно просматривать в любом текстовом редакторе. Чтобы просмотреть архивы журналов в оснастке Просмотр событий (Event Viewer), выполните следующие действия.

1. В консоли Управление компьютером (Computer Management) щелкните правой кнопкой элемент Просмотр событий (Event Viewer) и выберите в контекстном меню команду Открыть

файл журнала (Open Log File). Откроется диалоговое окно, показанное на рис. 3-11.

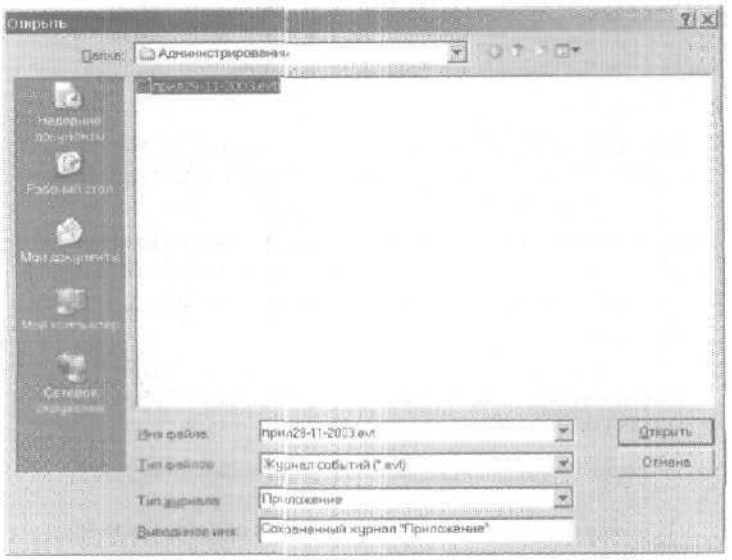


Рис. 3-11. Диалоговое окно для открытия сохраненного журнала события

2. Выберите папку и имя файла. Если журнал сохранен не в формате .evt, выберите в списке Тип файлов (Files of Type) вариант Все файлы (All Files).
3. В списке Тип журнала (Log Type) укажите вариант, соответствующий типу журнала.
4. Щелкните Открыть (Open). Архивированный журнал появится в отдельном окне оснастки Просмотр событий (Event Viewer).

Мониторинг деятельности сервера

Мониторинг сервера следует производить обдуманно и по плану. Главная задача мониторинга — устранение неполадок в работе сервера, например разрешение проблем с подключением к нему пользователей. Другая типичная задача — повышение производительности сервера путем оптимизации дисковых операций, снижения нагрузки на процессор и сокращения сетевого трафи-

ка. К сожалению, для некоторых ресурсов оптимизация невозможна. Например, при увеличении числа пользователей, получающих доступ к серверу, сократить сетевой трафик вы уже никак не сможете. Вам останется улучшить производительность сервера, например балансируя нагрузку или распределяя ключевые файлы данных по разным дискам.

Подготовка к мониторингу

До начала мониторинга следует выяснить опорную метрику производительности сервера. Для этого производительность измеряется в разные моменты времени и при разных условиях нагрузки. Затем сравните базовую производительность с производительностью в последующие моменты времени. Метрика, превышающая опорную, указывает на области, где сервер следует оптимизировать или перенастроить.

После определения опорной метрики составьте план мониторинга, включив в него следующие этапы.

1. Определение событий, мониторинг которых необходим для достижения ваших целей.
2. Установка фильтров для сокращения количества собираемой информации.
3. Настройка счетчиков и сигналов оповещения.
4. Архивирование журналов событий.
5. Анализ данных в консоли Производительность (Performance).

В большинстве случаев мониторинг без плана лучше не проводить, но иногда можно ограничить количество этапов. Например, анализировать собираемые данные по ходу дела, не архивируя их для последующего анализа.

Консоль Производительность (Performance)

Консоль Производительность (Performance) графически отображает статистику для ряда выбранных параметров производительности, называемых *счетчиками* (counters). Интервал обновления графика по умолчанию равен 1 секунде, но его можно изменить. Набор доступных счетчиков обновляется при установке служб и дополнительных компонентов. Например, после установки на сервере службы DNS консоль Производительность (Performance) пополняется рядом объектов и счетчиков для отслеживания ее работы.

Выбор счетчиков для мониторинга

Консоль Производительность (Performance) отображает информацию только для отслеживаемых счетчиков. Счетчики организованы в группы — *объекты производительности* (performance objects). Например, все счетчики, связанные с процессором, объединены в объект Процессор (Processor).

Счетчики выбираются так.

1. Выберите в меню Администрирование (Administrative Tools) команду Производительность (Performance). Откроется одноименная консоль.
2. Выделите в левой панели элемент Системный монитор (System Monitor), как показано на рис. 3-12.

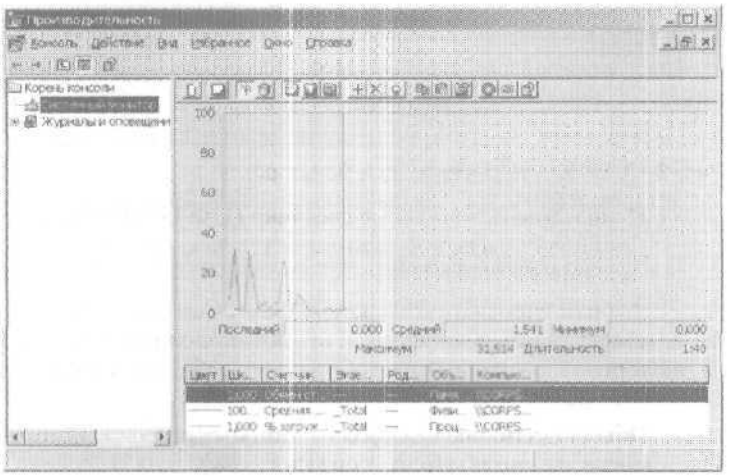


Рис. 3-12. Счетчики отображаются в нижней части окна Производительность (Performance)

3. У системного монитора несколько режимов просмотра. Для включения режимов Просмотр текущей активности (Current Activity) и Просмотр диаграммы (View Graph) щелкните одноименные кнопки на панели инструментов.
4. Чтобы добавить счетчики, щелкните кнопку Добавить (Add) на панели инструментов. Появится диалоговое окно Добавить счетчики (Add Counters), показанное на рис. 3-13. Далее перечислены его основные параметры.

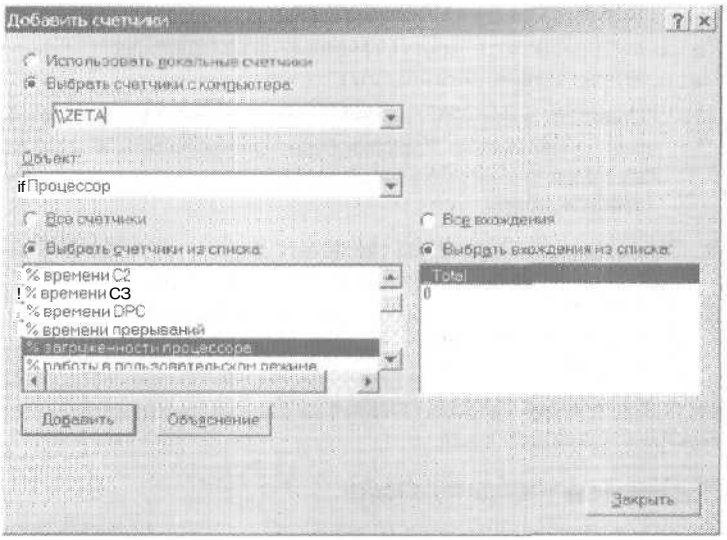


Рис. 3-13. Выберите счетчики для мониторинга

- **Использовать локальные счетчики (Use Local Computer Counters)** — задаст **отслеживание** производительности локального **компьютера.**
- **Выбрать счетчики с компьютера (Select Counters From Computer)** — позволяет ввести или выбрать в списке UNC-имя сервера, с которым вы собираетесь работать, например \\ZETA.
- **Объект (Performance Object)** — тип объектапроизводительности, например Процессор (Processor).

Совет Изучите все объекты и счетчики в окне Добавить счетчики (Add Counters). Выберите объект в списке Объект (Performance Object), щелкните кнопку Объяснение (Explain) и выделяйте счетчики в списке, чтобы прочитать поясняющий текст о них.

- **Все счетчики (All Counters)** — для текущего объекта будут выбраны все счетчики.
- **Выбрать счетчики из списка (Select Counters From List) — выбор** одного **или нескольких счетчиков** для текущего объекта.
- **Все вхождения (All Instances)** — выбор всех экземпляров счетчиков для мониторинга.

- **Выбрать вхождения из списка (Select Instances From *list)*** — выбор одного или нескольких экземпляров счетчика для мониторинга.

Совет Не выбирайте слишком много счетчиков или экземпляров одновременно. Графики будет сложно читать, к тому же вы повысите нагрузку на ресурсы системы — процессорное время и память.

5. Задав нужные параметры, щелкните Добавить (Add). Повторите этот процесс, чтобы добавить другие параметры.
6. Щелкните Закрыть (Попе), завершив добавление счетчиков.

Чтобы удалить счетчик, щелкните соответствующий элемент в нижней части окна Производительность (Performance), а затем щелкните кнопку Удалить (Delete) на панели инструментов или нажмите клавишу Delete.

Журналы производительности

Журналы производительности позволяют контролировать производительность сервера. Запись параметров в журналы производительности осуществляется независимо от графиков в консоли Производительность (Performance). Обновление данных в журналах счетчиков можно производить автоматически или вручную. В первом случае набор ключевых параметров записывается через определенный интервал времени, например каждые 10 секунд, во втором вы сами определяете, когда это делать. Доступны два типа журналов производительности:

- Журналы счетчиков (Counter Logs) — сюда по истечении заданного интервала обновления записываются данные о выбранных счетчиках;
- Журналы трассировки (Trace Logs) — сюда записываются данные о производительности, когда происходят заданные события.

Создание журналов производительности и управление ими

Журналы производительности создаются так.

1. Выберите в меню Администрирование (Administrative Tools) команду Производительность (Performance).
2. Раскройте узел Журналы и оповещения производительности (Performance Logs and Alerts). Выделите элемент Журналы счетчиков (Counter Logs) или Журналы трассировки (Trace

Logs). В правой панели появится список текущих журналов (рис. 3-14). Зеленый значок указывает, что журнал в настоящий момент ведет запись данных; красный — что запись данных приостановлена.

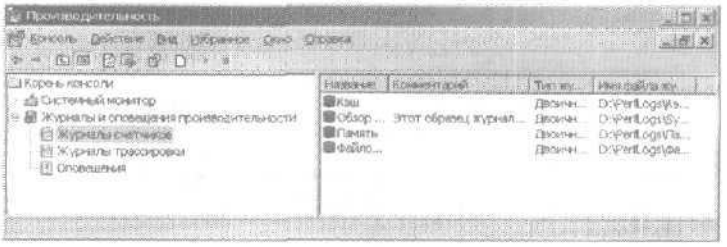


Рис. 3-14. Текущие журналы производительности

3. Щелкните правой кнопкой правую панель и выберите в контекстном меню команду Новые параметры журнала (New Log Settings). Появится одноименное окно, в котором нужно задать имя нового журнала.

Чтобы изменить параметры существующего журнала, щелкните его правой кнопкой и выберите команду:

- **Запуск (Start)** для активизации журнала;
- Остановка (Stop) для остановки журнала;
- Сохранить параметры как (Save Settings As) для сохранения параметров журнала в виде Web-страницы, которую можно просматривать в браузере, например Internet Explorer, и импортировать в новый журнал счетчиков с помощью команды Новые параметры журнала из (New Log Settings From);

Примечание В Web-странице, созданной таким образом, имеется встроенная диаграмма. Опубликовав эту страницу в папке IIS, вы сможете контролировать работу компьютера с удаленной системы.

- Удалить (Delete) для удаления журнала;
- Свойства (Properties) для отображения окна свойств журнала.

Создание журналов счетчиков

В журналах счетчикои данные о выбранных параметрах регистрируются через определенный интервал времени. Например, можно собирать данные о производительности процессора каждые 15 минут. Журнал счетчика создается так.

1. **Щелкните правой** кнопкой **Журналы счетчиков (Counter Logs)** и выберите **команду** Новые параметры **журнала** (New Log Settings).
2. Введите имя журнала и щелкните OK.
3. **Чтобы включить в** журнал **все счетчики для конкретного объекта,** щелкните **кнопку** Добавить **объекты (Add Objects) и выберите** нужные **объекты.**
4. Чтобы добавить отдельные счетчики, щелкните кнопку Добавить счетчики (Add Counters).
5. В поле Снимать показания каждые (Sample Data Every) введите интервал и выберите единицу измерения времени (секунды, минуты, часы или дни).

Совет Журналы быстро разбухают. Если вы собираетесь отслеживать значения счетчиков на протяжении длительного времени, поместите файл журнала на диске с большим объемом свободного пространства. Помните: чем чаще вы снимаете показания, тем больше нужно места на диске и тем выше нагрузка на процессор.

6. В поле От имени (Run As) введите учетную запись, под которой будет работать журнал, и щелкните кнопку Задать пароль (Set Password). Введя пароль и подтвердив его, щелкните OK, чтобы закрыть диалоговое окно Установка пароля (Set Password). Чтобы счетчик работал под системной учетной записью по умолчанию, введите *<по умолчанию>* (*<Default>*).
7. Перейдите на вкладку Файлы журналов (Log Files), показанную на рис. 3-15. По умолчанию журналы счетчиков сохраняются в двоичных файлах в папке *%SystemDrive%*\PerfLogs. При желании можно изменить их параметры.
   - В списке Тип файла журнала (Log file type) задается тип файла журнала по умолчанию. Используйте Текстовый файл с разделителями-запятыми [Text file (Comma Delimited)] для файла с разделением запятыми, Текстовый файл (разделитель - табуляция) [Text file (Tab Delimited)] для файла с разделением табулятором, Двоичный файл (Binary File) для двоичного файла, который можно читать посредством консоли Производительность (Performance), Двоичный циклический файл (Binary Circular File) для двоичного файла, в котором новые данные записываются

поверх старых, когда размер файла достигает определенного предела, База данных SQL (SQL Database) для записи данных в базу данных SQL.

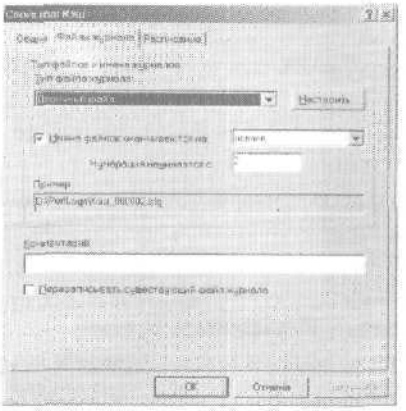


Рис. 3-15. Настройка формата и способа использования файла журнала

- В списке **Имена файлов оканчиваются на (End file names with)** задается автоматический суффикс для каждого нового файла, создаваемого при запуске журнала. Это может быть просто номер или дата в одном из нескольких форматов.
- Если вы выбрали числовую нумерацию файлов журнала, в поле **Нумерация начинается с (Start numbering at)** можно задать номер первого журнала.
- Поле **Комментарий (Comment)** предназначено для дополнительного описания журнала.

8. Щелкните кнопку Настроить (Configure), чтобы задать размещение файла журнала. Если вы выбрали тип журнала База данных SQL (SQL Database), в диалоговом окне Настройка журналов SQL (Configure SQL Logs) укажите одно из системных имен источников данных (data source name, DSN). Имя DSN используется для подключения к SQL-совместимой базе данных. Если вы указали другой тип, задайте имя и папку для файла. Тут же можно задать максимально допустимый размер журнала.
9. Перейдите на вкладку Расписание (Schedule), показанную на рис. 3-16.

Рис. 3-16. Определите, когда начинать и заканчивать ведение журнала

10. Настройте запуск журнала вручную или автоматически, задав определенные дату и время.
11. Задайте способ остановки журнала: вручную, по истечении определенного времени (например, через 7 дней), в определенное время или по достижении максимального размера. Задайте действие, которое нужно выполнить при закрытии файла журнала.
12. Щелкните OK.

Создание журналов трассировки

В журналы трассировки данные о производительности записываются при генерации событий их поставщиками — приложениями или службами. Журнал трассировки создается так.

1. Щелкните правой кнопкой Журналы трассировки (Trace Logs) в левой панели консоли Производительность (Performance) и выберите команду Новые параметры журнала (New Log Settings).
2. В диалоговом окне Новые параметры журнала (New Log Settings) введите имя журнала и щелкните OK. Откроется окно, показанное на рис. 3-17.
3. Чтобы контролировать события ОС, установите переключатель События, протоколируемые системным поставщиком (Events logged by system provider) и выберите системные события для трассировки.

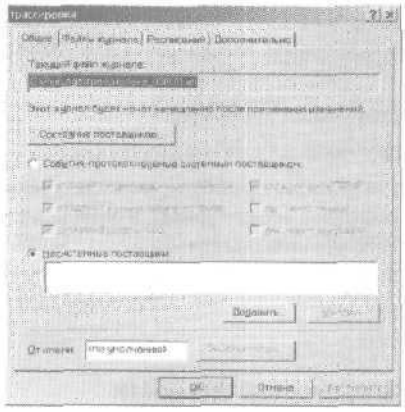


Рис. 3-17. На вкладке Общие (General) выберите поставщика, используемого при трассировке

Внимание! Трассировка страничного обмена и файловых операций сильно загружает сервер и вызывает быстрый рост файлов журнала. Собирайте эти сведения только в течение ограниченного интервала времени.

4. Чтобы отследить другого поставщика, установите переключатель Несистемные поставщики (Nonsystem Providers) и щелкните кнопку Добавить (Add). Появится диалоговое окно Добавление несистемных поставщиков (Add Nonsystem Providers).
5. В поле От имени (Run As) введите учетную запись, под которой будет работать журнал, и щелкните кнопку Задать пароль (Set Password). Введя пароль и подтвердив его, щелкните OK, чтобы закрыть диалоговое окно Установка пароля (Set Password). Чтобы счетчик работал под системной учетной записью по умолчанию, введите *<по умолчанию>* (*<Default>*).
6. Выбрав поставщиков и события, перейдите на вкладку Файлы журналов (Log Files). Настройте файл трассировки, как описано в пунктах 7 и 8 предыдущего раздела. Единственное отличие в доступных типах файлов журнала:
   - Файл последовательной трассировки (Sequential Trace File) — события последовательно записываются в журнал трассировки до достижения максимального размера файла (если он задан);

- **Файл циклической трассировки (Circular Trace File)** — старые данные заменяются новыми, когда файл достигает заданного размера.

7. Перейдите на вкладку Расписание (Schedule).
8. Задайте запуск журнала вручную или автоматически.
9. Задайте способ остановки журнала: вручную, по истечении определенного времени (например, через 7 дней), в определенное время или по достижении максимального размера. Задайте действие, которое нужно выполнить при закрытии файла журнала.
10. Щелкните OK.

Воспроизведение журналов производительности

При устранении проблем часто требуется записывать данные о производительности на протяжении длительного периода времени, а потом воспроизвести их и проанализировать.

1. Задайте автоматическую запись в журнал.
2. В окне Производительность (Performance) выделите элемент Системный монитор (System Monitor) и щелкните правую панель правой кнопкой мыши. Выберите в контекстном меню команду Свойства (Properties). Откроется диалоговое окно Свойства: Системный монитор (System Monitor Properties).
3. Перейдите на вкладку Источник (Source). В группе Источник данных (Data Source) установите переключатель Файлы журнала (Log Files) и щелкните кнопку Добавить (Add), чтобы открыть диалоговое окно Выбор файла журнала (Select Log File). Найдите журнал, который хотите проанализировать.
4. Задайте временной интервал, который хотите проверить. Щелкните кнопку Диапазон времени (Time Range) и задайте начало и конец интервала с помощью бегунков на полосе Весь диапазон (Total Range).
5. Перейдите на вкладку Данные (Data). Чтобы выбрать счетчики, значения которых вас интересуют, щелкните кнопку Добавить (Add). На экране появится диалоговое окно Добавить счетчики (Add Counter).

Примечание В этом окне отображаются лишь те счетчики, которые вы занесли в журнал. Если нужного вам счетчика среди них нет, придется изменить свойства журнала и перезапустить его.

6. Щелкните OK. В системном мониторе с помощью кнопок Просмотр диаграммы (View Graph), Просмотр гистограммы (View Histogram) и Просмотр отчета (View Report) отобразите информацию в нужном формате.

Настройка оповещений

Сигналы оповещения позволяют получать уведомления в ответ на определенные события или при достижении определенных порогов производительности. Оповещения можно отправлять как сетевые сообщения или записывать в журнал событий приложения. Оповещение может запустить какое-либо приложение или журнал производительности.

Чтобы добавить оповещение в консоль Производительность (Performance), выполните следующие действия.

1. Щелкните правой кнопкой элемент Оповещения (Alerts) и выберите команду Новые параметры оповещений (New Alert Settings).
2. В диалоговом окне Новые параметры оповещений (New Alert Settings) введите имя оповещения и щелкните OK. Откроется окно, показанное на рис. 3-18.

Рис. 3-18. Настройка счетчиков, запускающих оповещения

3. На вкладке Общие (General) введите дополнительное описание оповещения. Затем щелкните кнопку Добавить (Add), чтобы открыть окно, показанное ранее на рис. 3-13. .
4. **Добавьте** счетчики, **запускающие** оповещение, и щелкните **Закрыть (Close).**

5. В списке Счетчики (Counters) выберите первый счетчик, затем в поле Оповещать, когда значение... (Alert when value is...) задайте условие, при котором запускается оповещение для этого счетчика. Оповещения могут запускаться, когда значение счетчика становится больше или меньше заданного. Выберите в списке вариант Больше (Over) или Меньше (Under) и установите предельное значение. Единицы измерения — любые, подходящие для выбранного счетчика (счетчиков). Например, для оповещения при загруженности процессора более, чем на 95%, выберите Больше (Over), а затем введите 95. Повторите эту процедуру для других указанных счетчиков.
6. В поле Снимать показания каждые (Sample Data Every) введите интервал и выберите единицу измерения времени (секунды, минуты, часы или дни).

Внимание! Не снимайте показания слишком часто. Это занимает системные ресурсы и может помешать серверу вовремя отвечать на запросы пользователей.

7. В поле От имени (Run As) введите учетную запись, под которой будет работать журнал, и щелкните кнопку Задать пароль (Set Password). Введя пароль и подтвердив его, щелкните OK, чтобы закрыть диалоговое окно Установка пароля (Set Password). Чтобы счетчик работал под системной учетной записью по умолчанию, введите *<поумолчанию>* (*<Default>*).
8. Перейдите на вкладку Действие (Action), показанную на рис. 3-19. Теперь можно определить действие, происходящее при запуске оповещения:
   - Сделать **запись в журнале событий приложений (Log an entry in the application event log);**
   - **Послать сетевое сообщение (Send a network message to) на определенный компьютер;**
   - **Запустить журнал производительности (Start performance** data log), точнее, журнал счетчиков;
   - Запустить программу (Run This Program) — здесь нужно задать полный путь файла программы или пакетного файла, выполняемого при срабатывании оповещения.

Совет Чтобы передать аргументы в сценарий или приложение, щелкните кнопку Аргументы командной строки (Command Line Arguments). Все аргументы могут передаваться как самостоятельные строки. Однако, если вы установите флажок

Строка одиночного аргумента (Single Argument String), аргументы будут передаваться в общей строке с разделением запятыми. Примерный вид аргументов командной строки показан в нижней части вкладки в поле Образец аргументов командной строки (Example Command Line Arguments).

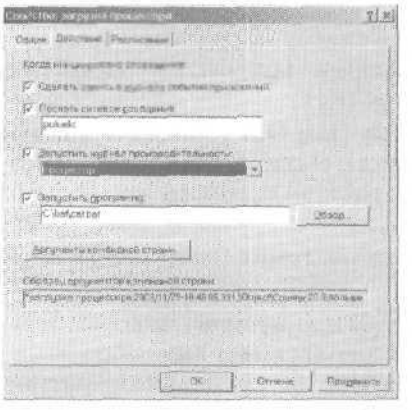


Рис. 3-19. Задайте действия, исполняемые при срабатывании оповещения

9. Перейдите на вкладку Расписание (Schedule) и задайте время запуска и остановки оповещения. Например, можно настроить запуск оповещения в пятницу вечером и остановку в понедельник утром. Каждый раз при срабатывании оповещения в этот период исполняется определенное действие (действия). Можно настроить:
   - запуск оповещений вручную или автоматически в определенный день;
   - остановку оповещений вручную, по истечении определенного срока, например 7 дней, иди в определенный день и время.
10. Щелкните OK. Созданным оповещением можно управлять аналогично тому, как управляют журналами счетчиков и трассировки.

Запуск сценариев в качестве действий

За обработку оповещений отвечает служба Журналы и оповещения производительности (Performance Logs and Alerts). Чтобы использовать в качестве реакции на оповещение сценарий, про-

грамму командной строки или программу, которой требуется доступ к рабочему столу, следует соответствующим образом настроить эту службу, выполнив следующие действия.

1. Откройте одним из доступных способов меню **Администрирование** (Administrative Tools) **и выберите** в нем команду Службы (Services).
2. Щелкните правой кнопкой службу Журналы и оповещения производительности (Performance Logs and Alerts) и выберите команду Свойства (Properties).
3. На вкладке Вход в систему (Log On) установите флажки С системной учетной записью (Local system account) и Разрешить взаимодействие с рабочим столом (Allow service to interact with desktop).
4. На вкладке Общие (General) щелкните Пуск (Start) и затем OK.

После этого служба Журналы и оповещения производительности (Performance Logs and Alerts) сможет выполнять пакетные файлы (.bat, .cmd) и сценарии (.js, .vbs, .wsf) в интерактивном режиме. Однако вводить имя сценария Windows *непосредственно* в поле Запустить программу (Run this program) нельзя. Здесь указывается путь к обработчику сценариев Windows, который нужно запускать при срабатывании оповещения, например C:\WINDOWS\system32\Cscript.exe, а затем через аргументы командной строки передать в него имя нужного сценария.

1. Настройте оповещение. На вкладке Действие (Action) установите флажок Запустить программу (Run this program). Щелкните кнопку Обзор (Browse). Найдите нужный обработчик сценариев и щелкните Открыть (Open).
2. Щелкните кнопку Аргументы командной строки (Command Line Arguments). В открывшемся окне установите флажки Строка одиночного аргумента (Single Argument String) и Текстовое сообщение (Text Message). Все остальные флажки сбросьте.
3. В поле Текстовое сообщение (Text Message) введите полный путь к сценарию, например **c:\scripts\Test.vbs**.
4. Два раза подряд щелкните OK.
5. **Перейдите на вкладку** Расписание (Schedule) и настройте **время запуска и остановки** оповещения.
6. Щелкните OK.

Повышение производительности системы

Теперь вы знаете, как следить за работой системы. Осталось разобраться, как эффективно воспользоваться полученными сведениями. Я подробно расскажу об:

- использовании памяти и кэширования;
- использовании процессора;
- операциях ввод а-вывода;
- работе сети,

Контроль и настройка использования памяти

Память довольно часто становится причиной снижения производительности, поэтому проверку работы системы всегда нужно начинать именно с памяти и лишь потом пытаться найти причину проблемы в других компонентах.

Параметры быстродействия и использования памяти

Эти параметры управляют распределением ресурсов системы. Обычно львиную долю ресурсов следует отдавать ОС и фоновым приложениям. Это особенно верно, если вы используете Active Directory или серверные приложения, обеспечивающие работу файловых, сетевых серверов и серверов печати. С другой стороны, на серверах приложений, баз данных и потоков мультимедиа большую часть ресурсов стоит отдавать активным программам.

Чтобы настроить параметры быстродействия и использования памяти, выполните следующие действия.

1. Откройте панель управления и дважды щелкните инструмент Система (System).
2. Перейдите на вкладку Дополнительно (Advanced) и щелкните кнопку и откройте окно Параметры быстродействия (Performance Options), щелкнув кнопку Параметры (Settings) в группе Быстродействие (Performance). Перейдите на вкладку Дополнительно (Advanced)
3. Параметры группы Распределение времени процессора (Processor Scheduling) управляют распределением процессорного времени. Чтобы отдать больше времени ОС и фоновым приложениям, установите переключатель Служб, работающих в фоновом режиме (Background Services). В противоположном случае установите переключатель Программ (Programs).

4. С помощью параметров группы Использование памяти (Memory Usage) вы управляете распределением памяти. Чтобы отдать больше времени ОС и фоновым приложениям, установите переключатель Системного кэша (System Cache). В противоположном случае установите переключатель Программ (Programs).
5. Щелкните OK.

Параметры **пропускной способности** системы

Эти параметры определяют, насколько эффективно сервер реагирует на запросы пользователей, файловые операции и клиентские подключения. Вам доступно четыре варианта оптимизации, которым соответствуют четыре переключателя:

- **Наименьшая занимаемая память (Minimize memory used)** — сервер оптимизируется для обслуживания небольшого числа пользователей. Для запросов пользователей, дескрипторов файлов и клиентских подключений выделяется очень мало системной памяти, что, соответственно, высвобождает ее для других целей;
- **Сбалансированная оптимизация (Balance)** — сервер оптимизируется для одновременного выполнения нескольких ролей, Время отклика па запросы пользователей, файловые операции и клиентские подключения умеренное;
- **Макс.** пропускная способность доступа к общим файлам (Maximize data throughput for file sharing) — сервер оптимизируется для предоставления в общее пользование файлов и принтеров. Это означает, что на обработку запросов пользователей, дескрипторов файлов и клиентских подключений выделяется максимальный объем ресурсов, что сокращает время отклика;
- **Макс. пропускная способность для сетевых приложений (Maximize data throughput** for network **applications)** — память сервера оптимизируется для распределенных приложений, которые располагают собственным кэшем, например для SQL Server и IIS. Размер системного кэша сокращается, что позволяет выделять больше памяти приложениям.

Для настройки параметров пропускной способности выполните следующие действия.

1. Откройте папку Сетевые подключения (Network Connections).
2. Щелкните правой кнопкой значок Подключение по локальной сети (Local Area Connection) и выберите команду Свой-

ства **(Properties). Если на сервере** установлено **несколько сетевых подключений, их** нужно **настраивать индивидуально.**

3. Выделите компонент Служба доступа к файлам и принтерам сетей Microsoft (File and printer sharing for Microsoft Networks) и щелкните кнопку Свойства (Properties).
4. **Задайте** нужные параметры на вкладке **Оптимизация сервера (Server Optimization) и** щелкните **OK.**
5. **Перезагрузите** сервер.

Проверка использования памяти, кэша и файла подкачки

Теперь, когда ваша система оптимизирована, можно определить, насколько эффективно и корректно она использует память. В таблице 3-1 показан список счетчиков, позволяющих обнаружить проблемные участки в использовании памяти, кэша и файла подкачки. Счетчики упорядочены по категориям возможных проблем.

Таблица 3-1. Проблемы с использованием памяти

Проблема	Счетчики	Описание
Недостаток физической и виртуальной памяти	Объект Память (Memory), счетчики Доступно КБ (Available Kbytes) и Байт выделенной виртуальной памяти (Committed Bytes)	Счетчик Доступно КБ (Available Kbytes) содержит объем физической памяти, доступной процессам, работающим на сервере. Счетчик Байт выделенной виртуальной памяти (Committed Bytes) содержит объем выделенной виртуальной памяти. Как правило, объем доступной памяти должен составлять не менее 5% всей физической памяти сервера. Количество выделенных байт не должно превышать 75% всей физической памяти
Ошибки страничной памяти	Объект Память (Memory), счетчики Ошибок страницы/сек (Page Faults/sec), Ввод страниц/сек (Pages Input/sec) и Чтений страниц/сек (Page Reads/sec)	В счетчик Ошибок страницы/сек (Page Faults/sec) записывается общая скорость, с которой процессор обрабатывает ошибки страничной памяти всех видов. Счетчик Ввод страниц/сек (Pages Input/sec) показывает полное число страниц, считанных с диска в процессе исправления ошибок физической памяти. Полное число считываний с диска для исправления ошибок физической памяти отображается в счетчике Чтений страниц/сек (Page Reads/sec)

Таблица 3-1. Проблемы с использованием памяти *(окончание)*

Проблема	Счетчики	Описание
Ошибки выгружаемого и невыгружаемого пулов	Объект Память Memory), счетчики Байт в выгружаемом страничном пуле (Pool Paged Bytes), Байт в невыгружаемом страничном пуле (Pool Nonpaged Bytes)	Эти счетчики показывают количество байт в выгружаемом и невыгружаемом пулах. Если размер выгружаемого пула велик по сравнению с полным объемом физической памяти системы, на компьютере нужно установить дополнительную память. Если размер невыгружаемого пула велик по сравнению с объемом виртуальной памяти системы, нужно увеличить размер виртуальной памяти

Контроль использования процессора

Именно в процессоре происходит обработка информации вашего сервера. Исследуя производительность сервера, после устранения проблем с памятью, вы должны сосредоточиться на процессорах. Если с ними что-то неладно, то ни добавление памяти, ни установка новых дисков, ни увеличение скорости передачи данных по сети не исправят положение дел. Вместо этого нужно планировать установку более быстрого процессора, использование многопроцессорных решений или перенос приложений, интенсивно использующих процессор, например SQL Server, на другой сервер.

Счетчики, характеризующие работу процессора, перечислены в **таблице** 3-2. Не забывайте, что контролировать следует каждый процессор, установленный в системе.

Таблица 3-2. Проблемы с использованием процессора

Проблема	Счетчики	Описание
Длинная очередь потоков	Объект Сис ема (System), счетчик Длина очереди процессора (Processor Queue Length)	Этот счетчик отображает число потоков, ожидающих очереди на исполнение. Очередь потоков хранится в одной области для всех процессоров системы. Если длина очереди систематически превышает- 2, процессоры нужно обновлять
Излишняя загруженность процессора	Объект Процессор (Processor), счетчик % загруженности процессора (% Processor Time)	Если этот счетчик показывает загруженность процессора на фоне умеренной загруженности диска и сетевого интерфейса, процессор нуждается в обновлении

Контроль использования диска

Современные высокоскоростные диски сами по себе редко становятся причиной снижения производительности сервера. Однако замедление его работы может быть связано с тем, что обращения к диску происходят слишком часто. Чтобы сократить обмен данными с диском, вы должны более эффективно распорядиться памятью. Поскольку управление памятью я уже описал, здесь осталось упомянуть лишь несколько счетчиков, непосредственно связанных с работой диска (табл. 3-3).

Таблица 3-3. Проблемы с использованием диска

Проблема	Счетчики	Описание
Общая производительность диска	Объект Физический диск (Physical Disk), счетчик % активности диска (% Disk Time)	Указанием на проблему с диском служит высокое значение этого счетчика на фоне невысокой загруженности процессора и сетевого интерфейса. Разумеется, показания этого счетчика нужно снимать для всех дисков сервера
Обмен данными с диском	Объект Физический диск (Physical Disk), счетчики Обращений записи на диск/сек (Disk Writes/sec), Обращений чтения с диска/сек (Disk Reads/sec), Средняя длина очереди записи на диск (Avg. Disk Write Queue Length), Средняя длина очереди чтения диска (Avg. Disk Read Queue Length), Текущая длина очереди диска (Current Disk Queue Length)	Количество обращений для чтения и записи в секунду показывает, как активно используется диск. По длине очередей записи и чтения можно судить о том, сколько запросов на чтение и запись ожидают обработки. Как правило, длина обеих очередей должна быть небольшой. Помните, что задержка выполнения запроса пропорциональная длине очереди за вычетом числа дисков в наборе RAID

Контроль использования сети

С точки зрения пользователя, среди факторов, определяющих быстродействие сервера, ни один не сравнится по важности с быстродействием сети, которая соединяет сервер с пользовательским компьютером. Все зависит от времени, прошедшего между отправкой запроса и получением ответа на него. Если это время

велико, пользователь будет считать ваш сервер медленным, даже если на самом деле он самый быстрый на планете.

Вообще говоря, величина задержки в получении ответа на пользовательский запрос находится вне вашей компетенции. Она зависит от типа подключения пользовательского компьютера к сети и от маршрута трафика. Но есть и параметры, которые вы в состоянии изменить, — это общая способность сервера обрабатывать запросы и доступная ему полоса пропускания. Первый фактор зависит от настройки сетевых интерфейсов, второй — от использованной в организации инфраструктуры сети,

Во многих случаях скорость передачи данных ограничена возможностями сетевой платы. На большинстве серверов применяются платы 10/100, которые допускают несколько вариантов настройки. Можно, например, по ошибке настроить плату на работу со скоростью 10 Мбит/сек, хотя сеть допускает большую скорость, или задать использование полудуплексной передачи вместо полнодуплексной. Если вам кажется, что производительность низка из-за сетевой платы, первым делом проверьте ее конфигурацию.

Чтобы определить пропускную способность и загруженность сетевых интерфейсов сервера, следите за следующими счетчиками объекта Сетевой интерфейс (Network):

- Всего байт/сек (Bytes Total/sec);
- Отправлено байт/сек (Bytes Sent/sec);
- Получено байт/сек (Bytes Received/sec);
- Текущая пропускная способность (Current Bandwidth).

Если при умеренной загрузке полное число байт, передаваемых в секунду, превышает 50% максимальной возможности платы, в моменты пиковой загрузки ждите проблем. Чтобы предотвратить их, подумайте о переносе на другой сетевой интерфейс операций, которым требуется значительная часть полосы пропускания, например резервного копирования. Помните, что за перечисленными выше счетчиками нужно следить, не забывая о контроле загруженности диска и процессора. О недостаточной пропускной способности сетевой платы говорит ее высокая загрузка на фоне низкой загруженности диска и процессора. Решить эту проблему можно, перенастроив имеющийся интерфейс или установив дополнительные интерфейсы. Помните: планирование решает все. Чтобы организовать работу нового интерфейса недостаточно просто установить сетевую плату в компьютер.

Глава 4

Автоматизация административных задач

Повседневное выполнение рутинных задач, беготня от компьютера к компьютеру и объяснение пользователям азов работы с ОС — нерациональная трата времени. Ваша работа станет гораздо эффективнее, если вы сможете автоматизировать эти задачи и сосредоточиться на более важных делах. Повышение производительности и возможность меньше заниматься мелочами в пользу решения серьезных проблем — это и есть задача автоматизации.

В Microsoft Windows Server 2003 предусмотрено множество ресурсов, позволяющих автоматизировать административные задачи, политику и процедуры. В этой главе я расскажу об;

- управлении групповой политикой;
- управлении сценариями пользователей и компьютеров;
- шаблонах безопасности;
- планировании выполнения задач.

Управление групповой политикой

Групповая политика упрощает администрирование, предоставляя администраторам централизованный контроль над привилегиями, разрешениями и возможностями пользователей и компьютеров. Групповая политика позволяет:

- создавать централизованно управляемые специальные папки, например Мои документы (My Documents);
- управлять доступом к компонентам Windows, системным и сетевым ресурсам, инструментам панели управления, рабочему столу и меню Пуск (Start);
- настроитьсценарии пользователей икомпьютеров на выполнение задачи в заданное время;

- настраивать политики паролей и блокировки учетных записей, аудита, присвоения пользовательских прав и безопасности (подробнее — в части II этой книги).

Понятие групповой политики

Групповую политику можно рассматривать как набор правил управления пользователями и компьютерами. Групповую политику разрешается применять в нескольких доменах, в индивидуальных доменах, в подгруппах внутри домена или в индивидуальных системах. В индивидуальных системах применяется *локальная групповая политика* (local group policy) — она хранится только на локальной системе. Другие групповые политики представлены как объекты в службе Active Directory.

Чтобы понять, что такое групповая политика, нужно знать структуру службы каталогов Active Directory. В Active Directory логические объединения доменов называются *сайтами* (sites), а подгруппы внутри домена — *организационными подразделениями* (organizational units). Так, в вашей сети могут быть сайты NewYorkMain, CaliforniaMain и WashingtonMain. Внутри сайта WashingtonMain могут быть домены SeattleEast, SeattleWest, SeattleNorth и SeattleSouth. Внутри домена SeattleEast могут быть подразделения Information Services (IS), Engineering и Sales.

Групповая политика применяется только в системах с Windows 2000, Windows XP Professional и Windows Server 2003. Политика для систем на базе Windows NT 4.0 настраивается при помощи System Policy Editor (poledit.exe). Для Windows 95 и Windows 98 нужен редактор System Policy Editor, поставляемый с этими ОС. Созданный с его помощью файл политики следует скопировать в общий ресурс SYSVOL на контроллере домена.

Параметры групповой политики хранятся в объекте групповой политики (Group Policy Object, GPO). К одному и тому же сайту, домену или подразделению разрешено применять несколько объектов GPO. Поскольку политика в реальности представляет собой объект, для нее действительны многие понятия объектно-ориентированного программирования (ООП). Читатель, знакомый с ООП, не удивится, узнав о том, что в отношении политик действуют концепции родительских и дочерних объектов, а также наследования.

С помощью наследования политика, примененная к родительскому контейнеру, передается дочернему контейнеру. Например, если вы применяете политику в домене, ее параметры наследу-

ются подразделениями этого домена. В данном случае объект GPO домена является родительским, а объект GPO подразделения — дочерним.

Порядок наследования таков:

Сайт ® Домен ® Подразделение

Это означает, что параметры групповых политик сайта передаются доменам этого сайта, а параметры домена передаются его организационным подразделениям (ОП).

Разумеется, при желании наследование параметров можно отменить. Допустим, вы назначили в политике для дочернего объекта параметр, который противоречит политике родительского объекта. Применен будет именно он, конечно, при условии, что вы не запретили изменение наследования. Подробнее — далее в этой главе.

Порядок применения политик

Если политик несколько, они применяются в определенном порядке.

1. Политики Windows NT 4.0 (NTConfig.pol).
2. Локальные групповые политики.
3. Групповые политики сайта.
4. Групповые политики домена.
5. Групповые политики ОП.
6. Групповые политики дочернего ОП.

Если параметры политик конфликтуют, то параметры политики, назначенные позже, обладают приоритетом и заменяют заданные ранее. Например, политика ОП приоритетнее групповой политики домена. У правила приоритета есть и исключения (см, раздел «Блокировка, перекрытие и отключение политики»).

Когда применяются групповые политики

Параметры политики делятся на две основные категории:

- для компьютеров;
- для пользователей.

Первые применяются обычно при загрузке системы, вторые — при входе в систему. Точная последовательность событий часто важна при устранении неполадок в системе. Во время загрузки и регистрации происходят следующие события.

1. После запуска сети Windows Server 2003 применяет компьютерные политики. По умолчанию они начинают действовать одна за другой в указанном выше порядке. Интерфейс пользователя при обработке компьютерных политик не отображается.
2. Windows Server 2003 выполняет сценарии загрузки. По умолчанию они исполняются один за другим. Для выполнения очередного сценария нужно, чтобы выполнился предыдущий или истекло его время ожидания. Исполнение сценария на экране не отображается, если это не было задано.
Я. Пользователь нажимает Ctrl+Alt+Delete для входа в систему. Проверив его регистрационные данные, Windows Server 2003 загружает профиль пользователя,
4. Windows Server 2003 применяет пользовательские политики. По умолчанию они применяются одна за другой в указанном выше порядке. При обработке политик пользователя отображается пользовательский интерфейс.
5. Windows Server 2003 выполняет сценарии входа в систему. Сценарии входа в систему из состава групповой политики по умолчанию исполняются одновременно. Исполнение сценария не отображается для пользователя, если это не было задано. Сценарии в общем ресурсе Netlogon выполняются последними в окне обычной командной оболочки, как в Windows NT 4.0.
6. Windows Server 2003 отображает стартовый интерфейс, настроенный в групповой политике. По умолчанию групповая политика обновляется только при выходе пользователя из системы или при перезапуске компьютера. Вы можете изменить интервал обновления, введя в командной строке команду **gpupdate**. Подробнее об этом — в разделе «Обновление групповой политики»

Совет Некоторые параметры пользователей, например перенаправление папок, нельзя обновить в ходе сеанса. Чтобы изменения в них вступили в силу, пользователь должен выйти из системы и войти в нее снова. Чтобы автоматически выйти из системы после обновления политики, воспользуйтесь командой gpupdate **/logoff.** Аналогично, некоторые параметры компьютера обновляются только при его перезапуске. Чтобы

перезагрузить компьютер после обновления, введите в командной строке **gpupdate /boot.**

Требования групповых политик и совместимость версий

Групповые политики впервые появились в Windows 2000 и действуют только в системах, работающих под управлением Windows 2000, Windows XP Professional и Windows Server 2003. Не удивительно, что с каждой новой версией в групповые политики вносились дополнительные изменения. Иногда это приводило к тому, что политика устаревала и в новых версиях Windows работать уже не могла.

Тем не менее в большинстве случаен политики, впервые появившиеся в Windows 2000, способны работать не только в этой ОС, но и в Windows XP Professional и Windows Server 2003. С другой стороны, политики Windows XP Professional, как правило, не совместимы с Windows 2000, а политики Windows Server 2003 не применимы к Windows 2000 или Windows XP Professional. Неприменимость политики к определенной версии Windows означает, что вам не удастся применять данную политику на компьютерах, работающих иод управлением этой версии.

Выяснить, действует ли данная политика в данной версии Windows, очень просто. В окне свойств каждой групповой нолитики имеется поле Поддерживается (Supported On), в котором отмечена совместимость политики с различными версиями Windows. В редакторе объектов групповой политики для просмотра требований к групповой политике нужно перейти к расширенному представлению и выделить ее.

Новые политики добавляются в систему при установке пакетов обновления, приложений и компонентов Windows. Так что вопросы совместимости политики вам придется решать довольно часто.

Управление локальными групповыми политиками

У каждого компьютера с Windows Server 2003 есть одна локальная групповая политика, которой управляют так.

1. Щелкните кнопку Пуск (Start) и выберите команду Выполнить (Run).
2. Введите **mmc** в поле Открыть (Open) и щелкните OK. Откроется пустая консоль MMC (Microsoft Management Console, консоль управления Microsoft).

3. Выберите в меню Консоль (Console) команду Добавить или удалить оснастку (Add/Remove Snap-In). Откроется одноименное диалоговое окно.
4. На вкладке Изолированная оснастка (Standalone) щелкните кнопку Добавить (Add).
5. В диалоговом окне Добавить изолированную оснастку (Add Standalone Snap-In) щелкните Редактор объектов групповой политики (Group Policy Object Editor) и Добавить (Add). Запустится Мастер групповой политики (Group Policy Wizard).
6. В поле Объект групповой политики (Group Policy Object) по умолчанию указан Локальный компьютер (Local Computer). Чтобы отредактировать групповую политику на локальном компьютере, щелкните Готово (Finish). Чтобы изменить политику другого компьютера, щелкните Обзор (Browse). Найдя нужную политику, щелкните OK и Готово (Finish).
7. Щелкните Закрыть (Close) и OK.

Локальные групповые политики хранятся в папке *%SystemRoot%*\System32\GroupPolicy на каждом компьютере Windows Server 2003. Ниже перечислено содержимое подпапок этой папки:

- Adm — файлы административных шаблонов, используемые в данный момент. Файлы имеют расширение .adm. Папка Adm имеется только на контроллерах домена;
- Machine — сценарии компьютера в подпапке Script, а также информацию о политике для раздела реестра HKEY_LOCAL_MACHINE в файле Rcgistry.pol;
- User — сценарии пользователей в подпапке Script и информацию о политике для раздела реестра HKEY CURRENT_USER в файле Registry.pol.

Внимание! Не изменяйте эти **папки** и файлы напрямую — используйте соответствующие свойства консоли Групповая политика (Group Policy).

Управление политиками сайта, домена и ОП

У каждого сайта, домена и ОП может быть одна или несколько групповых политик. Как уже говорилось, групповые политики, настроенные на этом уровне, ассоциируются с Active Directory.

Это гарантирует, что политики сайта правильно применяются в соответствующих доменах и ОП.

Создание и изменение политик сайта, домена и ОП

Для работы с политиками сайтов предназначена оснастка Групповая политика (Group Policy) из консоли Active Directory — сайты и службы (Active Directory Sites and Services). Политики доменов и ОП управляются из оснастки Групповая политика (Group Policy) из консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers). Чтобы создать или изменить политику сайта, домена или ОП, выполните следующие действия.

1. Откройте консоль Active Directory — сайты и службы (Active Directory Sites and Services), если собираетесь работать с политикой сайта, или Active Directory — пользователи и компьютеры (Active Directory Users and Computers), если собираетесь работать с политикой домена или ОП.
2. Щелкните правой кнопкой сайт, домен или ОП, с политикой которого собираетесь работать. Выберите в контекстном меню команду Свойства (Properties).
3. Перейдите на вкладку Групповая политика (Group Policy), Существующие политики перечислены в списке Ссылки на объекты групповой политики (Group Policy Object Links), как показано на рис. 4-1.

Рис. 4-1. С помощью этой вкладки создаются и редактируются групповые политики

4. Чтобы создать новую политику, щелкните кнопку Создать (New). Настройка политики описана далее в разделе «Работа с групповыми политиками».
5. Для редактирования существующей политики, выделите ее и щелкните кнопку Изменить (Edit), О редактировании политики речь идет также в разделе «Работа с групповыми политиками».
6. **Чтобы** изменить приоритет политики, выделите **ее и измените положение политики в** списке **Ссылки на** объекты **групповой политики** (Group Policy Object **Links) кнопками Вверх** (Up) или **Вниз** (Down).

Групповые политики сайта, домена и ОП хранятся в папке *%SystemRoot%*\SYSVOL\domain\policies на контроллере домена. В ней хранятся подпапки для каждой из политик, определенных нами на этом контроллере. Имена этих подпапок образованы из *глобальных уникальных идентификаторов* (Global Unique Identifier, GUID) политик. Значение идентификатора указано в окне свойств политики на вкладке Общие (General). В папке каждой политики имеются подпапки:

- Adm — файлы административных шаблонов с расширением .adm, используемые в данный момент (папка Adm есть только на контроллерах домена);
- **Machine** — сценарии компьютера в папке Script, а также реестровые политики для раздела HKEY_LOCAL_MACHINE (HKLM) в файле Registry.pol;
- **User** — сценарии пользователей в папке Script, а также реестровые политики для раздела HKEY_CURRENT_USER (HKCU) в файле Registry.pol.

Внимание! Не изменяйте эти папки и файлы напрямую — используйте соответствующие свойства консоли Групповая политика (Group Policy).

Блокировка, перекрытие и отключение политики

Наследование политики можно блокировать на уровне сайта, домена и ОП. Это значит, что вы можете блокировать политику, которая в противном случае была бы применена. На уровне сайта и домена также можно выполнить политику, которая в противном случае была бы заменена или блокирована. Это позволяет администраторам высшего звена выполнять политики и пре-

дотвращать их блокировку. Другой доступный параметр — отключение политики. Политику можно отключать частично или полностью, фактически не удаляя ее.

Эти параметры политики **конфигурируются** в следующей последовательности.

1. Откройте вкладку Групповая политика (Group Policy) в диалоговом окне свойств сайта, домена или ОП, как описано в предыдущем разделе.
2. Установите флажок Блокировать наследование политики (Block policy inheritance), чтобы запретить наследование политик более высокого уровня, для которых не задан параметр Не перекрывать (No Override).
3. Установите параметр Не перекрывать (No Override), чтобы политики низшего уровня не блокировали параметры этои политики. Чтобы установить или сбросить этот параметр, нужно дважды щелкнуть соответствующий столбец справа от имени объекта групповой политики. Наличие галочки говорит о том, что параметр установлен.
4. Установите параметр Отключить (Disabled), чтобы отказаться от использования политики. Чтобы установить или сбросить этот параметр, нужно дважды щелкнуть соответствующий столбец справа от имени объекта групповой политики. Наличие галочки свидетельствует, что параметр установлен.

Отключение части групповой политики

Отключить групповую политику разрешено не только целиком, но частично, точнее, можно отдельно отключить параметры конфигурации пользователя или параметры конфигурации компьютера. Отключив неиспользуемую часть политики, вы существенно ускорите ее применение. Чтобы отключить те или иные параметры конфигурации, выполните следующие действия.

1. Откройте вкладку Групповая политика (Group Policy) в диалоговом окне свойств сайта, домена или ОП.
2. Щелкните кнопку Свойства (Properties), а затем установите или сбросьте флажки Отключить параметры конфигурации компьютера (Disable Computer Configuration Settings) или Отключить параметры конфигурации пользователя (Disable User Configuration Settings).

Применение существующей политики к новой области в сети

Любая групповая политика может быть связана с другим компьютером, ОП, доменом или сайтом. Связывая политику с другим объектом, допустимо назначать параметры политики без их повторного определения.

Вот как применить существующую политику к новому месту в сети.

1. Перейдите па вкладку Групповая политика (Group Policy) в окне свойств нужного сайта, домена или ОП.
2. Щелкните кнопку Добавить (Add). Откроется диалоговое окно Добавить ссылку на объект групповой политики (Add a Group Policy Object Link), показанное на рис. 4-2.

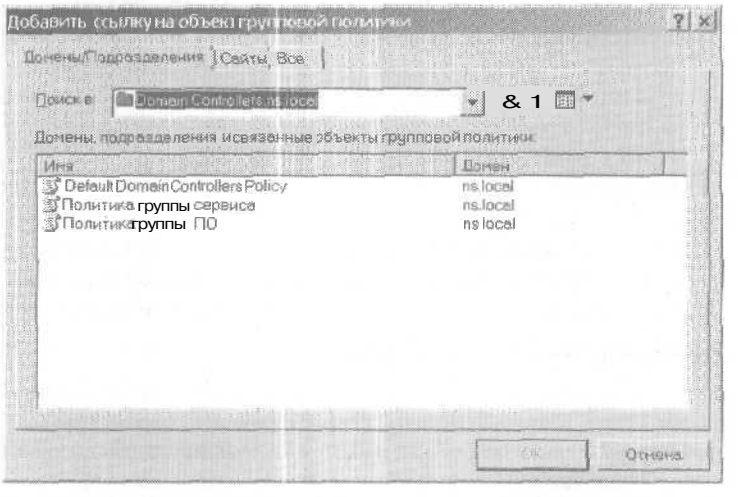


Рис. 4-2. Это диалоговое окно позволяет связать существующие политики с новыми местами без воссоздания политики

3. На вкладках и в полях найдите групповую политику, которую хотите применить к новому месту в сети. Щелкните OK. Active Directory создаст связь между объектом GPO и сайтом, доменом или подразделением, с которыми вы работаете.

Удаление групповой политики

Вы можете отключить или удалить те групповые политики, которые не используете. Для этого следует выполнить следующие действия.

1. Перейдите на вкладку Групповая политика (Group Policy) в окне свойств нужного сайта, домена или ОП.
2. Выделите политику, которую хотите удалить, и щелкните кнопку Удалить (Delete).
3. Если политика связана, можно удалить лишь связь, не затрагивая другие контейнеры, использующие эту политику. Для этого в диалоговом окне Удаление (Delete) установите переключатель Изъять ссылку из списка, не удаляя объект (Remove the link from the list).
4. Если политика связана, связь и соответствующий объект GPO можно удалить, при этом политика удаляется окончательно. Для этого выберите Изъять ссылку и окончательно удалить объект групповой политики (Remove the link and delete the Group Policy Object permanently).

Обновление групповой политики

Изменения, вносимые в групповую политику, применяются немедленно, но их автоматическое распространение не происходит. Клиентский компьютер запрашивает политику при:

- запуске компьютера;
- входе пользователя в систему;
- ручном обновлении политики, запрошенном пользователем или приложением;
- окончании заданного интервала автоматического обновления групповой политики.

Как вы уже знаете, для обновления групповой политики на локальном компьютере используют утилиту командной строки Gpupdate. Можно также задать интервал обновления, чтобы оно периодически происходило в автоматическом режиме. В любом случае обновление производится в фоновом режиме, причем некоторые политики таким образом обновить нельзя. Единственный способ гарантированно обновить все политики пользователя — попросить его выйти из системы. Единственный способ гарантированно обновить все политики компьютера — перезапустить его.

Чтобы задать интервал обновления групповой политики, выполните следующие действия.

1. Откройте консоль Групповая политика (Group Policy) для нужного сайта, домена или ОП.

2. Последовательно разверните узлы Конфигурация компьютера (Computer Configuration), Административные шаблоны (Administrative Templates), Система (System) и Групповая политика (Group Policy).
3. В области сведений дважды щелкните Интервал обновления групповой политики для компьютеров (Group Policy Refresh Interval for Computers). Эта политика управляет интервалом фонового обновления политик компьютера.
4. На вкладке Параметр (Setting) установите переключатель Включен (Enabled) и с помощью параметров задайте интервал. По умолчанию обновление происходит каждые 90 минут со случайным сдвигом от 0 до 30 минут. Благодаря сдвигу снижается вероятность того, что несколько компьютеров затребуют обновление одновременно. Щелкните OK.
5. Откройте узел Конфигурация пользователя\Административные шаблоны\Система\Групповая политика (User Configuration\Administrative Templates\System\Group Policy).
6. В области сведений дважды щелкните Интервал обновления групповой политики для пользователей (Group Policy Refresh Interval for Users). Эта политика управляет интервалом фонового обновления политик пользователя.
7. На вкладке Параметр (Setting) установите переключатель Включен (Enabled) и с помощью параметров задайте интервал. Щелкните OK.

Примечание Интервал обновления, заданный таким образом, применяется только к обычным компьютерам. Чтобы задать интервал обновления для контроллеров домена, воспользуйтесь политикой Интервал обновления групповой политики для контроллеров домена (Group Policy Refresh Interval for Domain Controllers).

Совет Следите за тем, чтобы обновления не выполнялись слишком редко или слишком часто. Чем чаще обновляется политика, тем больше генерируется сетевого трафика. В крупных сетях обычно имеет смысл обновлять политики пореже, особенно если политика затрагивает сотни пользователей и компьютеров. Увеличить интервал обновления следует и когда пользователи жалуются на периодическое замедление работы компьютеров. Помните, что иногда достаточно обновлять политики раз в день и даже раз в неделю.

Работа с групповыми политиками

Выбрав политику для изменения или создав новую, вы будете использовать для работы с ними консоль Групповая политика (Group Policy).

Знакомство с консолью Групповая политика (Group Policy)

В консоли Групповая политика (Group Policy) два основных узла (рис. 4-3):

- **Конфигурация компьютера (Computer Configuration)** — политики, применяемые к компьютерам независимо от того, кто регистрируется;
- **Конфигурация пользователя (User Configuration) — политики,** применяемые к пользователям независимо от того, с какого компьютера они входят в сеть.

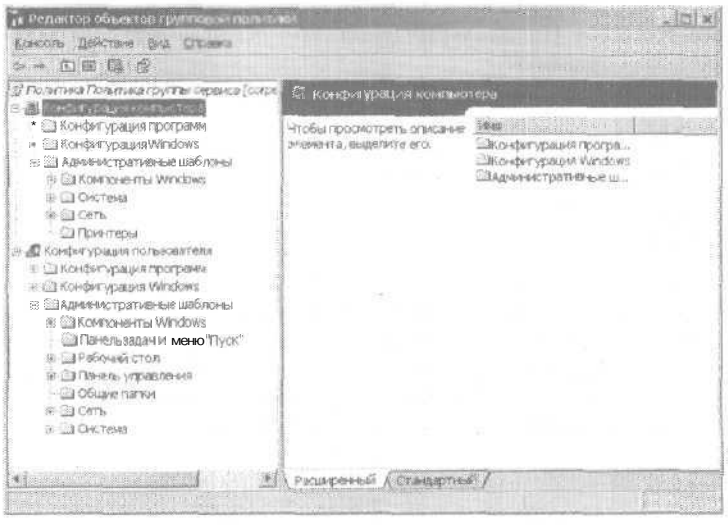


Рис. 4-3. Конфигурация консоли Групповая политика (Group Policy) зависит от типа создаваемой политики и установленных дополнений

Точная структура узлов Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration) зависит от установленных дополнений и типа создаваемой политики. Обычно у них имеются следующие подузлы:

- **Конфигурация программ (Software Settings)** — содержит политики для параметров приложений и для установки ПО;

- Конфигурация **Windows (Windows** Settings) — содержит политики для перенаправления папок, сценариев и безопасности;
- **Административные шаблоны (Administrative Templates) —** содержит политики для ОС, компонентов Windows и прикладных программ.

Примечание Подробное обсуждение всех доступных параметров выходит за рамки этой книги. Далее речь пойдет о перенаправлении папок и административных шаблонах. О сценариях рассказано в разделе «Управление сценариями пользователей и компьютеров», о безопасности — в части II этой книги.

Централизованное управление специальными папками

Можно централизованно управлять специальными папками Windows Server 2003, перенаправляя их в центральную сетевую папку вместо использования стандартных папок на отдельных компьютерах. Специальные папки, которыми можно централизованно управлять;

- Главное меню (Start Menu);
- Мои документы (My Documents);
- Мои рисунки (MyPictures).
- Рабочий стол (Desktop);
- Application Data.

Вы можете перенаправить специальную папку в единую сетевую папку для всех пользователей или назначить папки, исходя из участия пользователей в группах безопасности. В любом случае убедитесь, что нужная вам сетевая панка доступна в качестве общего сетевого ресурса. Подробнее о совместном использовании данных в сети — в главе 14.

Перенаправление специальной папки в единую папку

1. Откройте консоль Групповая политика (Group Policy) для работы с нужным сайтом, доменом или ОП.
2. В узле Конфигурация пользователя (User Configuration) раскройте узел Конфигурация Windows (Windows Settings) и выберите политику Перенаправление папки (Folder Redirection).
3. Щелкнув правой кнопкой папку, с которой хотите работать, например Application Data, выберите команду Свойства (Properties). Откроется окно, показанное на рис. 4-4.

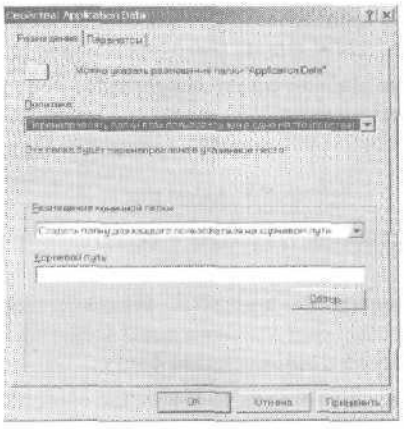


Рис. 4-4. Б этом диалоговом окне задаются параметры перенаправления

4. На вкладке Размещение (Target) в списке Политика (Setting) выберите вариант Перенаправлять папки всех пользователей в одно место (простая) [Basic — Redirect everyone's folder to the same location].
5. Задайте размещение конечной папки с помощью следующих параметров:
   - **Перенаправить на** домашнюю папку **пользователя (Redirect** to the user's home directory) — папка перенаправляется в подпапку домашней папки пользователя. Положение домашней папки задается с помощью переменных среды *%HomeDrive%* и *%HomePath%*;
   - Создать папку для каждого пользователя на корневом пути (Create a folder for each user under the root path) — папка для каждого пользователя создается в расположении, заданном в поле Корневой путь (Root Path). Имя папки совпадает с именем учетной записи пользователя (переменная среды *%UserName%*). Если вы ввели корневой путь \\Zeta\UserDocuments, папка для пользователя WilliamS будет называться \\Zeta\UserDocuments\WilliamS;
   - Перенаправлять в следующее место (Redirect to the following location) — папка перенаправляется в точно указанное расположение. Обычно положение папки для конкретного

пользователя опять же задается с помощью переменных среды, например \\Zeta\UserData*%UserName%*\docs;

- Перенаправлять в место, определяемое локальным профилем (Redirect to the **local userprofile** location) — папка перенаправляется в подпапку папки профиля пользователя. Расположение последней записано в переменной среды *%UserProfile%*.

6. Перейдите на вкладку Параметры (Settings) и задайте дополнительные параметры:
   - **Предоставить права монопольного доступа к... (Grant the user** exclusive rights **to...)** — наделяет пользователей всеми правами доступа к их данным в специальной папке;
   - Перенести содержимое... в новое место (Move the contents **of ...** to the new location) — перемещает данные в специальных папках с индивидуальных систем в центральную сетевую папку (панки).
7. Щелкните OK.

Перенаправление специальной папки в зависимости от членства в группе

1. Откройте консоль Групповая политика (Group Policy) для работы с нужным сайтом, доменом или ОП.
2. В узде Конфигурация пользователя (User Configuration) раскройте узел Конфигурация Windows (Windows Settings) и выберите политику Перенаправление панки (Folder Redirection).
3. Щелкнув правой кнопкой папку, е которой хотите работать, например Application Data, выберите команду Свойства (Properties).
4. На вкладке Размещение (Target) в списке Политика (Setting) укажите вариант Указать различные места для разных групп пользователей (Advanced — Specify locations for various user groups). В диалоговое окно свойств добавится панель Членство *в* группе безопасности (Security Group Membership), как показано на рис. 4-5.
5. Щелкните кнопку Добавить (Add), чтобы открыть окно Выбор группы и размещения (Specify Group and Location), или выберите существующую группу и щелкните Изменить (Edit) для изменения ее параметров.

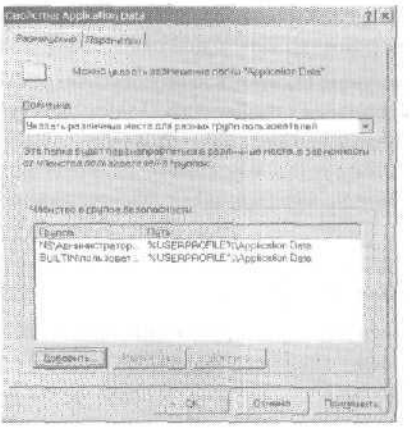


Рис. 4-5. Перенаправление в зависимости от членства в **группе**

6. В поле Членство в группе безопасности (Security Group Membership) введите имя группы безопасности, для которой хотите включить перенаправление, или найдите ее с помощью кнопки Обзор (Browse).
7. Укажите путь к общей папке с помощью параметров, перечисленных в пункте 5 предыдущего раздела.
8. Щелкните OK. Затем повторите пункты 5–7 для других групп.
9. Добавив записи групп, перейдите на вкладку Параметры (Settings) и задайте дополнительные параметры.
10. Щелкните OK.

Отказ от перенаправления

Иногда требуется отменить перенаправление из конкретной специальной папки.

1. Откройте подузел Перенаправление папки (Folder Redirection) консоли Групповая политика (Group Policy).
2. Щелкнув правой кнопкой нужную специальную папку, выберите команду Свойства (Properties),
3. Перейдите на вкладку Параметры (Settings) и установите переключатель в одно из двух положений:
   - **После удаления политики переместить папку (Leave the folder in the new location when policy is removed) — папка**

со всем содержимым остается в новом месте, где пользователи по-прежнему могут получать к ней доступ[1];

- **После удаления политики перенаправить папку обратно в локальный профиль пользователя (Redirect the folder back to the** local **userprofile** location **when** policy is **removed)** — папка со всем содержимым копируется в исходное положение. Заметьте, что содержимое из предыдущего положения не удаляется.

4. При необходимости щелкните Применить (Apply), а затем перейдите на вкладку Размещение (Target).
5. Чтобы удалить все определения перенаправления для специальной папки, в списке Политика (Setting) выберите вариант Не задана (Not Configured).
6. Чтобы удалить перенаправления конкретной группы безопасности, выберите группу безопасности в панели Членство в группе безопасности (Security Group Membership) и щелкните Удалить (Remove).
7. Щелкните OK.

Настройка политик с помощью административных шаблонов

Административные шаблоны облегчают доступ к реестровым параметрам политики, которые иногда требуется конфигурировать.

Просмотр административных шаблонов и политик

Набор административных шаблонов по умолчанию для пользователей и компьютеров конфигурируется в консоли Групповая политика (Group Policy), как показано на рис. 4-6. Административные шаблоны можно добавлять и удалять. Любые изменения в политиках, совершаемые через административные шаблоны, сохраняются в реестре. Конфипфации компьютеров сохраняются в разделе HKEY_LOCAL_MACHINE, а конфигурации пользователей — в HKEY_CURRENT_USER.

Настроенные шаблоны позволяет просмотреть узел Административные шаблоны (Administrative Templates) консоли Групповая политика (Group Policy). Он содержит политики, конфи-

[1] К сожалению, перевод названия этого переключателя в русифицированном интерфейсе не соответствует его смыслу. — *Прим. перев.*

гурируемые для локальных систем, ОП, доменов и сайтов. Наборы шаблонов в узлах Конфигурация компьютера (Computer Configuration) и Конфигурация пользователя (User Configuration) различаются. Добавлять дополнительные шаблоны, содержащие новые политики, можно вручную, а также при настройке новых *компонентов* Windows.

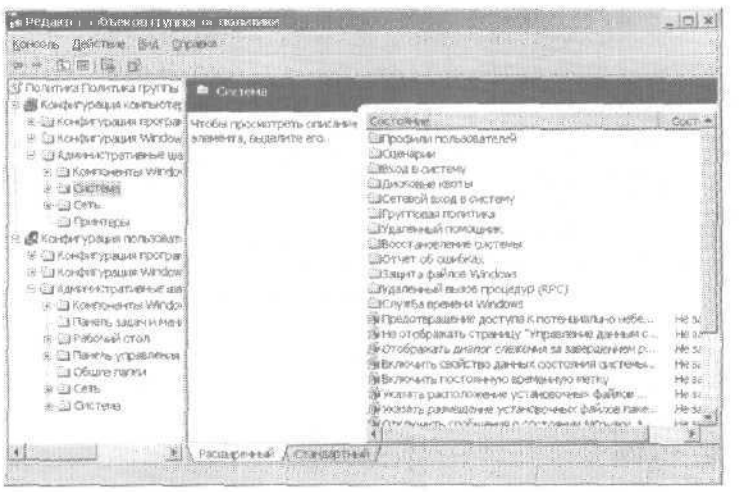


Рис. 4-6. Политики настраиваются при помощи административных шаблонов

Пользовательский интерфейс для узла Административные шаблоны (Administrative Templates) настраивается в файлах с расширением .adm. Эти текстовые файлы в формате ASCII разрешается редактировать или создавать в любом текстовом редакторе. При конфигурации политик в узле Административные шаблоны (Administrative Templates) параметры сохраняются в файлах Registry.pol. Для разделов реестра HKEY_LOCAL_MACHINE и HKEY_CURRENT_USER применяются отдельные файлы Registry.pol.

Чтобы узнать, какие политики административных шаблонов доступны, достаточно просмотреть узлы Административные шаблоны (Administrative Templates) в консоли Групповая политика (Group Policy). Политики находятся в одном из трех состояний:

- Не задана (Not Configured) — политика не используется, ее параметры не сохранены в реестре;

- **Включена (Enabled)** — политика активно выполняется, и ее параметры сохраняются в реестре;
- **Отключена (Disabled)** — политика отключена и не выполняется, если не замещена. Этот параметр сохраняется в реестре.

Включение, отключение и настройка политик

1. Откройте консоль Групповая политика (Group Policy) для работы с нужным сайтом, доменом или ОП.
2. Откройте папку Административные шаблоны (Administrative Templates) в узле Конфигурация компьютера (Computer Configuration) или Конфигурация пользователя (User Configuration) в зависимости от конфигурируемого типа политики.
3. В левой панели щелкните подпапку, содержащую нужные политики. Они отобразятся в правой панели.
4. Щелкните нужную политику правой кнопкой и выберите команду Свойства (Properties).
5. Перейдите на вкладку Объяснение (Explain), чтобы просмотреть описание политики. Описание доступно, если оно определено в соответствующем файле .adm.
6. Чтобы задать состояние политики, перейдите на вкладку Параметр (Setting) и установите переключатель Не задан (Not Configured). Включен (Enabled) или Отключен (Disabled).

Примечание Политики компьютера в Windows Server 2003 обладают приоритетом. При конфликте между параметром компьютерной и пользовательской политики применяется компьютерная политика.

7. Включив политику, настройте любые дополнительные параметры па вкладке Параметр (Setting), затем щелкните Применить (Apply).
8. При необходимости с помощью кнопок Предыдущий параметр (Previous Setting) и Следующий параметр (Next Setting) перейдите к другим политикам из текущей папки. Настройте их тем же образом.
9. Щелкните OK.

Добавление или удаление шаблонов

Панки шаблонов в консоли Групповая политика (Group Policy) можно добавлять и удалять.

1. Откройте консоль Групповая политика (Group Policy) для работы с нужным сайтом, доменом или ОП.
1. Щелкните правой кнопкой папку Административные шаблоны (Administrative Templates) в узле Конфигурация компьютера (Computer Configuration) или Конфигурация пользователя (User Configuration) и выберите команду Добавление и удаление шаблонов (Add/Remove Templates). Откроется одноименное диалоговое окно (рис. 4-7).

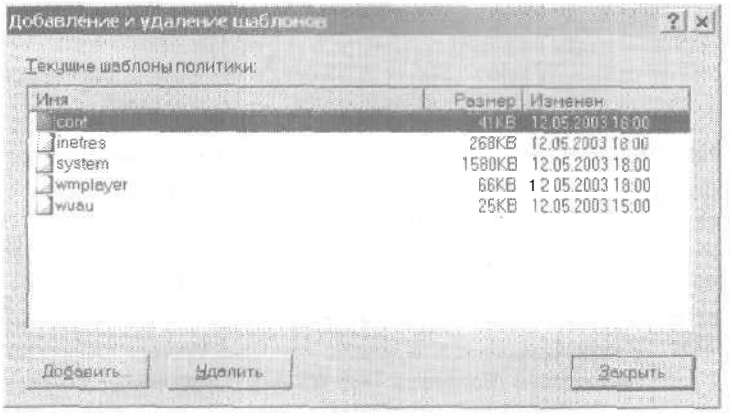


Рис. 4-7. Диалоговое окно Добавление и удаление шаблонов (Add/Remove Templates) позволяет добавить шаблоны или удалить существующие

3. Чтобы добавить новый шаблон, щелкните Добавить (Add). В окне Шаблоны политики (Policy Templates) щелкните добавляемый шаблон, а затем Открыть (Open).
4. Для удаления существующего шаблона выделите его и щелкните Удалить (Remove).
5. Завершив добавление и удаление шаблонов, щелкните Закрыть (Close).

Управление сценариями пользователей и компьютеров

В Windows Server 2003 можно настраивать сценарии четырех типов, которые выполняются:

- во время загрузки компьютера;

- перед завершением работы компьютера;
- при входе пользователя в систему;
- при выходе пользователя из системы.

Эти сценарии могут быть командными файлами с расширением .bat или .cmd или сценариями для Windows Script Host (WSH). WSH — компонент Windows Server 2003 позволяет использовать язык сценариев, например VBSscript, без встраивания его кода в Web-страницу. Для обеспечения универсальной среды исполнения WSH опирается на ядра сценариев — компоненты, определяющие базовый синтаксис и структуру отдельного языка сценариев. Windows Server 2003 оснащена ядрами сценариев VBScript и JScript. Доступны и другие ядра сценариев.

Назначение сценариев загрузки и завершения работы

Сценарии загрузки компьютера и завершения работы назначаются как часть групповой политики. Таким образом, все компьютеры — члены сайта, домена и/или ОП — автоматически исполняют сценарии при загрузке или завершении работы.

Примечание Сценарии загрузки компьютера **можно** указать в виде назначенных заданий с помощью Мастера планирования заданий (Scheduled Task Wizard). Подробнее — в разделе «Назначение заданий».

Сценарий загрузки компьютера или завершения работы назначается так.

1. Для облегчения управления скопируйте нужные сценарии в папку Computer\Scripts\Startup или Computer\Scripts\Shutdown соответствующей политики. Политики хранятся в папке *%SystemRoot%*\SYSVOL\domain\policies на контроллерах домена.
2. Откройте консоль Групповая политика (Group Policy) для работы с нужным сайтом, доменом или ОП.
3. В узле Конфигурация компьютера (Computer Configuration) дважды щелкните папку Конфигурация Windows (Windows Settings). Затем щелкните Сценарии (Scripts).
4. Щелкните правой кнопкой элемент Автозагрузка (Startup) для работы со сценариями загрузки или элемент Завершение работы (Shutdown) для работы со сценариями завершения работы. Выберите команду Свойства (Properties). Откроется диалоговое окно, показанное на рис. 4-8.

Рис. 4-8. Добавление, изменение и удаление сценариев компьютера

5. Щелкните кнопку Показать файлы (Show Files). Если вы скопировали сценарий компьютера в нужное место в папке политик, вы должны увидеть его.
6. Чтобы назначить сценарий, щелкните Добавить (Add). В поле Имя сценария (Script Name) введите имя сценария, скопированного в папку соответствующей политики, — Computer\Scripts\Startup или Computer\Scripts\Shutdown. В поле Параметры сценария (Script Parameters) наберите аргументы командной строки, которые следует передать в сценарий серверу сценариев. Повторите этот пункт, чтобы добавить другие сценарии.
7. Кнопками Вверх (Up) и Вниз (Down) задайте очередность выполнения сценариев при загрузке или завершении работы.
8. Чтобы изменить имя сценария или параметры, выделите сценарий в списке и щелкните Изменить (Edit).
9. Чтобы удалить сценарий, выделите его в списке и щелкните Удалить (Remove).

Назначение сценариев входа и выхода пользователя

Сценарии пользователей назначают одним из трех способов.

- Сценарии входа и выхода назначают как частьгрупповой политики. Таким образом, все пользователи — члены сайта, домена и/или ОП — автоматически исполняют сценарии при входе или выходе.

- Сценарии входа в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) назначают индивидуально. Так, каждому пользователю или группе можно приписать отдельный сценарий входа (см. главу 10).
- Индивидуальные сценарии входа активизируют с помощью Мастера планирования заданий (Scheduled Task Wizard). Подробнее — в разделе «Назначение заданий».

Пользовательский сценарий групповой политики назначается так.

1. Для облегчения управления скопируйте нужные сценарии в палку User\Scripts\Logon или User\Scripts\Logoffсоответствующей политики. Политики хранятся в папке %System#oot%\SYSVOL\domain\policies на контроллерах домена.
2. Откройте консоль Групповая политика (Group Policy) для работы с нужным сайтом, доменом или ОП.
3. В узле Конфигурация пользователя (User Configuration) дважды щелкните папку Конфигурация Windows (Windows Settings). Затем щелкните Сценарии (Scripts).
4. Щелкните правой кнопкой элемент Вход в систему (Logon) для работы со сценариями входа иди элемент Выход из системы (Logoff) для работы со сценариями выхода из системы. Выберите команду Свойства (Properties). Откроется диалоговое окно, показанное на рис. 4-9.

Рис. 4-9. Добавление, изменение и удаление **сценариев пользователя**

5. Щелкните кнопку Показать файлы (Show Files). Если вы скопировали сценарий пользователя в нужное место в папке политик, вы должны увидеть его.
6. Чтобы назначить сценарий, щелкните Добавить (Add). В поле Имя сценария (Script Name) введите имя сценария, скопированного в папку соответствующей политики — User\Scripts\Logon или User\Scripts\Logoff. В поле Параметры сценария (Script Parameters) введите аргументы командной строки, которые нужно передать в сценарий серверу сценариев. Повторите этот пункт, чтобы добавить другие сценарии.
7. Кнопками Вверх (Up) и Вниз (Down) задайте очередность выполнения сценариев при входе в систему или выходе из нее.
8. Чтобы изменить имя сценария или параметры, выделите сценарий в списке и щелкните Изменить (Edit).
9. Чтобы удалить сценарий, выделите его в списке и щелкните Удалить (Remove).

Применение политики безопасности с помощью шаблонов

Жесткая система защиты и продуманные параметры безопасности — залог успешного администрирования. Один из способов назначить политику безопасности — посредством *шаблонов безопасности* (security templates).

Знакомство с шаблонами безопасности

Шаблоны безопасности позволяют централизованно управлять параметрами безопасности рабочих станций и серверов. Они используются для применения наборов политик, связанных с защитой данных. Обычно эти политики из перечисленных далее групп:

- **политики учетных записей** — параметры паролей, **блокирования** учетных **записей** и Kerberos;
- **локальные политики — параметры аудита, прав пользователей** и др;
- **политики журнала событий — параметры безопасности, связанные с ведением журнала событий;**
- **политики ограниченных групп — параметры безопасности, связанные с** администрированием **локальных групп;**

- **политики системных служб** — параметры безопасности и запуска локальных служб;
- политики файловой системы — параметры безопасности локальной файловой системы;
- **политики реестра** — параметры, задающие значения ключей реестра, связанных с безопасностью.

Шаблоны безопасности имеются во всех вариантах Windows Server 2003. Их можно импортировать в любую групповую политику. Шаблоны хранятся в папке %SystemRoot%\Security\Templates и управляются из оснастки Шаблоны безопасности (Security Templates), показанной на рис. 4-10. Средствами этой же оснастки создаются и новые шаблоны. В комплект Windows Server 2003 входят следующие стандартные шаблоны:

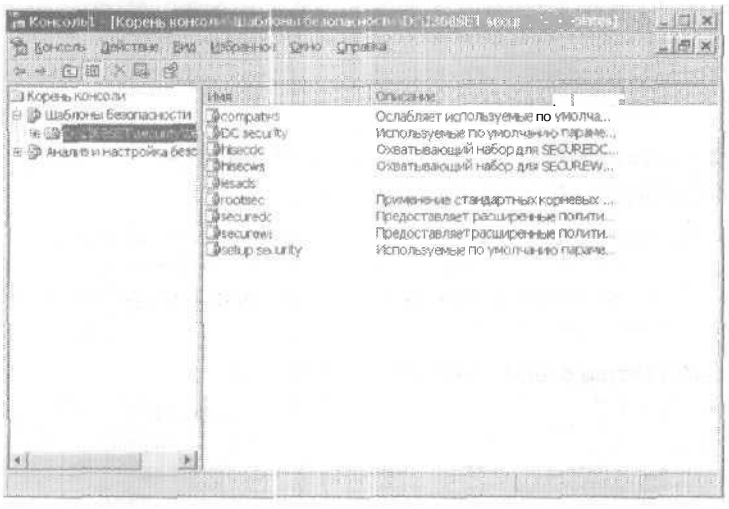


Рис. 4-10. С помощью этой оснастки создаются шаблоны безопасности

- dc security — содержит параметры безопасности по умолчанию для контроллеров домена;
- hisecdc — содержит жесткие параметры безопасности для контроллеров домена;
- hisecws — содержит жесткие параметры безопасности для рабочих станций.

- **securedc** — содержит умеренные параметры безопасности для контроллеров домена;
- **securews** — содержит умеренные параметры безопасности для рабочих станций;
- **setup security** — содержит параметры безопасности по умолчанию для рядовых серверов;

Совет Выбрав необходимый шаблон, тщательно проверьте все его параметры и проанализируйте, как они повлияют на работу вашей сети. Если какой-то из параметров в вашей ситуации не нужен, отредактируйте его или совсем удалите.

Для применения шаблонов используется оснастка Анализ и настройка безопасности (Security Configuration and Analysis). Ее же средствами можно сравнить значение параметра в шаблоне с тем, что в данный момент используется па компьютере.

Чтобы воспользоваться оснастками системы безопасности, выполните следующие действия.

1. Щелкните кнопку Пуск (Start) и выберите команду Выполнить (Run).
2. Введите mmc в поле Открыть (Open) и щелкните OK.
3. В открывшейся консоли выберите в меню Файл (File) команду Добавить или удалить оснастку (Add/Remove Snap-In).
4. В открывшемся окне перейдите на вкладку Изолированная оснастка (Standalone) и щелкните кнопку Добавить (Add).
5. В диалоговом окне Добавить изолированную оснастку (Add Standalone Snap-In) выделите в списке вариант Шаблоны безопасности (Security Templates) и щелкните Добавить (Add).
6. Выделите вариант Анализ и настройка безопасности (Security Configuration and Analysis) и щелкните Добавить (Add).
7. Щелкните Закрыть (Close), а потом — OK.

Применение шаблонов безопасности

Как уже говорилось, оснастка Шаблоны безопасности (Security Templates) предназначена для просмотра имеющихся и для создания *новых* шаблонов. Чтобы *настроить* и *проверить* шаблон, выполните следующие действия.

1. Откройте оснастку Анализ и настройка безопасности (Security Configuration and Analysis).

2. Щелкните правой кнопкой узел Анализ и настройка безопасности (Security Configuration and Analysis) и выберите команду Открыть базу данных (Open Database).
3. Введите в поле Имя файла (File Name) имя новой базы и щелкните Открыть (Open). Откроется диалоговое окно Импортировать шаблон (Import Template).
4. Выделите шаблон безопасности, которым хотите воспользоваться, и щелкните Открыть (Open).
5. Щелкните правой кнопкой узел Анализ и настройка безопасности (Security Configuration and Analysis) и выберите команду Анализ компьютера (Analyze Computer Now). Введите путь к файлу журнала ошибок или сразу щелкните ОК, чтобы использовать путь по умолчанию.
6. Дождитесь завершения анализа шаблона. Затем просмотрите сто результаты и при необходимости отредактируйте шаблон. Для просмотра журнала ошибок щелкните правой кнопкой узел Анализ и настройка безопасности (Security Configuration and Analysis) и выберите команду Показать файл журнала (View Log File).
7. Подготовившись к применению шаблона, щелкните правой кнопкой узел Анализ и настройка безопасности (Security Configuration and Analysis) и выберите команду Настроить компьютер (Configure Computer Now). Введите путь к файлу журнала ошибок или сразу щелкните ОК, чтобы использовать путь по умолчанию.
8. Чтобы просмотреть журнал ошибок настройки, щелкните правой кнопкой узел Анализ и настройка безопасности (Security Configuration and Analysis) и выберите команду Показать файл журнала (View Log File). Отметьте возникшие проблемы и примите меры к их устранению.

Назначение заданий

Обновление или профилактические работы, как правило, желательно проводить в нерабочее время. Но кому из администраторов хочется ради этого приходить на работу в 3 часа ночи в понедельник? К счастью, служба Планировщик заданий (Task Scheduler) позволяет назначить однократное выполнение задания или его автоматическое периодическое выполнение в указанное время дня или ночи.

Задания автоматизируются с помощью сценариев командных процессоров, сценариев Windows Script Host или приложений, исполняющих нужные команды. Например, если вы хотите создавать резервные копии системного диска по будням в полночь, создайте сценарий, выполняющий резервное копирование и записывающий результаты в файл журнала.

Средства назначения заданий

Назначать задания на локальных или удаленных системах в Windows Server 2003 позволяют Мастер планирования заданий (Scheduled Task Wizard), утилита командной строки AT или утилита командной строки SCHTASK. У каждого способа свои преимущества и недостатки.

У мастера удобный графический интерфейс. Это упрощает настройку заданий, освобождая от необходимости думать о синтаксисе. Однако в этом случае у вас нет центрального пункта для проверки назначенных заданий во всей сети, и вам приходится вызывать мастер в каждой системе, которую надо конфигурировать.

Команда AT не имеет дружественного интерфейса: вам придется изучить синтаксис и вводить все параметры вручную. Преимущество AT в том, что вы можете назначить отдельный сервер планировщиком заданий, просматривать и назначать задачи по всей сети с этого сервера.

Утилита SCHTASKS обладает почти той же гибкостью, что и Мастер планирования заданий (Scheduled Task Wizard). Она позволяет создавать расписание выполнения заданий, задавать права на запуск, настраивать команды для выполнения при запуске компьютера, при входе пользователя в систему и во время бездействия процессора. Подобно AT, она позволяет планировать задания для всей сети. Что более важно, с помощью SCHTASKS удается просматривать все запланированные задания системы, включая заданные средствами мастера и команды AT.

Далее рассматривается только использование Мастера планирования заданий (Scheduled Task Wizard). Обсуждение команд AT и SCHTASKS выходит за рамки этой книги. Упомяну лишь, что, если вы хотите использоваться SCHTASKS для просмотра списка заданий, назначенных на одной из систем сети, нужно ввести в командной строке

```
schtasks /query /s <имясистемы>
```

где *<имясистемы>*— имя системы, которую вы хотите проверить.

Подготовка к назначению задания

По умолчанию служба планировщика заданий регистрируется в системе с локальной системной записью LocalSystem, которая обычно нс позволяет выполнять административные задачи. Поэтому желательно задать запуск Планировщика заданий (Task Scheduler) под учетной записью, прав которой достаточно для выполнения административных действий.

Убедитесь также, что служба Планировщик заданий (Task Scheduler) настроена на автоматический запуск на всех системах, на которых вы назначаете задания. Настройка запуска и способа регистрации службы описаны в главе 3.

Сценарий должен задавать значения всех необходимых параметров пользователя, чтобы полностью держать под контролем собственные действия и чтобы обеспечить доступ к доменным пользовательским параметрам.

Назначение заданий с помощью мастера

Мастер планирования заданий (Scheduled Task Wizard) позволяет назначать задания на локальном или удаленном компьютере. Доступ к Мастеру планирования заданий (Scheduled Task Wizard) осуществляется через папку Назначенные задания (Scheduled Tasks).

Доступ к папке Назначенные задания (Scheduled Tasks)

Чтобы получить доступ к папке Назначенные задания (Scheduled Tasks) на локальном компьютере, нужно открыть Панель управления (Control Panel) и дважды щелкнуть значок Назначенные задания (Scheduled Tasks). Чтобы открыть папку Назначенные задания (Scheduled Tasks) на удаленном компьютере, нужно выполнить следующие действия.

1. Запустите Проводник (Windows Explorer) и с помощью узла Сетевое окружение (My Network Places) найдите компьютер, с которым собираетесь работать.
2. Дважды щелкните сначала значок компьютера, а потом значок Назначенные задания (Scheduled Tasks).
3. Чтобы назначить задание на удаленном компьютере, щелкните правой кнопкой область сведений, раскройте подменю Создать (New) и выберите в нем команду Назначенное задание (Scheduled Task). Правда, параметры этого задания вам придется задавать вручную, а не с помощью мастера.

Запуск мастера, изменение и удаление заданий

Записи в папке Назначенные задания (Scheduled Tasks) показывают текущие назначенные задания. Чтобы создать новое задание, щелкните дважды значок Добавить задание (Add Scheduled Tasks). Запустится Мастер планирования заданий (Scheduled Task Wizard). На удаленной системе эта возможность отсутствует, но вы можете создать задание локально с помощью мастера, а потом скопировать его в панку Назначенные задания (Scheduled Tasks) па удаленной системе. Чтобы изменить свойства задания или просто просмотреть их, щелкните дважды значок задания. Чтобы удалить задание, выделите его и нажмите клавишу Delete.

Создание задания с помощью мастера

1. Запустите Мастер планирования заданий (Scheduled Task Wizard), щелкнув дважды значок Добавить задание (Add Scheduled Task) в папке Назначенные задания (Scheduled Tasks). Щелкните Далее (Next).
2. В окне, показанном на рис. 4-11, выделите программу, выполнение которой хотите назначить. В этом окне перечислены ключевые приложения системы, например Очистка диска (Disk Cleanup) и Синхронизация (Synchronize). Сценарии здесь не отображаются.

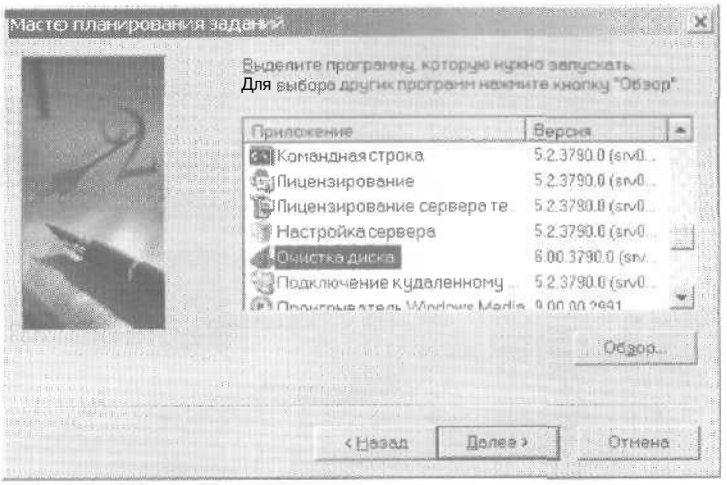


Рис. 4-11. Выбор программы для запуска по расписанию

3. Щелкните кнопку Обзор (Browse) и найдите командный файл или сценарий WSH, выполнение которого нужно запланировать.
4. Введите короткое, но понятное имя задания.
5. Задайте расписание выполнения задания. Его можно запускать как периодически (ежедневно, еженедельно или ежемесячно), так и при запуске компьютера или входе в систему. Щелкните Далее (Next).
6. Если вы задали периодическое выполнение задания, назначьте дату и время для его запуска. Щелкните Далее (Next).
7. Введите имя и пароль пользователя, от имени которого будет выполняться задание. Соответствующая учетная запись должна обладать необходимыми для этого разрешениями. Щелкните Далее (Next).
8. В последнем окне мастера приводится общее описание создаваемой задачи. Щелкните Готово (Finish), чтобы завершить ее создание. Если при этом произошла ошибка, на экране появится информационное окно с сообщением о ней. Щелкните OK. Затем дважды щелкните значок вновь созданной задачи, чтобы исправить ошибку.

Глава 5

Работа со службами поддержки и удаленным рабочим столом

Многие важные усовершенствования Microsoft Windows Server 2003 относятся к службам поддержки, а также к возможности соединения с удаленным рабочим столом с помощью служб терминалов. В этой главе рассказывается об автоматических обновлениях, отправке отчетов об ошибках, удаленном рабочем столе и службах времени.

Знакомство со службами поддержки

В Windows Server 2003 предусмотрено несколько уровней встроенных служб поддержки. Если вы откроете узел Службы (Services) консоли Управление компьютером (Computer Management), то найдете ряд служб системной поддержки, в том числе те, что перечислены ниже.

- **Автоматическое обновление (Automatic Updates) — отвечает за** автоматическое обновление ОС. Как правило, эта служба включена. Управляют ее работой с вкладки Автоматическое обновление (Automatic Updates) диалогового окна свойств системы. На серверах по умолчанию автоматическое обновление запрещено.
- Служба регистрации ошибок (Error Reporting Service) — обеспечивает автоматизированный сбор данных об ошибках и отправку информации о них. Если во время работы этой службы происходит ошибка в приложении или программном компоненте, автоматически создается сообщение об ошибке, которое может быть передано в компанию Microsoft. Регистрация ошибок рассматривается в разделе «Включение и отключение отчетов об ошибках» главы 2.
- Справка и поддержка (Help and Support) — обеспечивает программную среду для автоматического мониторинга системы.

Это основа средств справки и поддержки, встроенных в Windows Server 2003.

- Службы терминалов (Terminal Services) — предоставляют пользователям возможность удаленного подключения к компьютеру и управляют отображением рабочего стола и приложений для этих пользователей. Именно эта служба обеспечивает необходимую среду дли функционирования удаленного рабочего стола (remote desktop), удаленной помощи (remote assistance), быстрого переключения пользователей (fast user switching) и сервера терминалов (terminal server).

Внимание! Не отключайте службы терминалов, чтобы запретить удаленный доступ. Для этого достаточно сбросить флажки Разрешить отправку приглашения удаленному помощнику (Turn on Remote Assistance and allow invitations to be sent from this computer) и Разрешить удаленный доступ к этому компьютеру (Allow users to connect remotely to this computer) на вкладке Удаленное использование (Remote) диалогового окна свойств системы.

- Теневое копирование тома (Volume Shadow Copy) —обеспечивает создание и ведение теневых копий тома с целью резервного копирования и повышения надежности хранения данных. Подробнее об этом — в главе 14.
- Служба времени Windows (Windows Time) — синхронизация системного времени с точным временем. Вы можете задать синхронизацию с определенным сервером времени.

Эти службы являются основой для многих расширенных функций Windows Server 2003. Если они не запущены или неправильно настроены, то при использовании некоторых из них возможны проблемы. В некоторых случаях вся Windows Server 2003 начинает работать неправильно.

Функции поддержки обеспечиваются также многими другими службами, которые нужны в отдельных случаях и обычно не настраиваются на автоматический запуск. Например, службы сервера приложений отключены или настроены на ручной запуск во всех версиях Windows Server 2003, кроме Windows Server 2003, Web Edition.

Автоматизированная справочная система

Автоматизированная справочная система Windows Server 2003 довольно сложна. Она способна автоматически контролировать

состояние ОС, поводить профилактическое обслуживание и сообщать о возникших проблемах. Справочная система состоит из трех основных компонентов;

- **Центра справки и** поддержки (Help and **Support Center) со** встроенными справочными функциями;
- прикладной среды (application framework);
- монитора, который собирает и регистрирует информацию о состоянии системы.

Использование центра справки и поддержки

В Центре справки и поддержки вы найдете системную документацию и службы поддержки. Чтобы запустить Центр, щелкните кнопку Пуск (Start) и выберите команду Справка и поддержка (Help and Support).

Из рис. 5-1 видно, что Центр справки и поддержки (Help and Support Center) сильно отличается от справки, встроенной R предыдущие версии Windows. Начальная страница Центра содержит ссылки на документацию встроенной справочной системы, службы поддержки и другие важные компоненты. Эта возможность органично объединяет информационное наполнение локального компьютера и удаленных сайтов. В целом документация в значительно большей степени ориентирована на конкретные задачи и их решение, чем в предыдущих версиях.

В области Задачи поддержки (Support Tasks) начальной страницы центра справки и поддержки есть ссылка Поддержка (Support). Щелкните ее или кнопку Поддержка (Support) на панели инструментов, чтобы получить доступ к встроенным утилитам поддержки, в том числе к:

- Получить удаленную помощь (Get Remote Assistance) позволяет пользователям получать помощь непосредственно от специалистов;
- **Техническая поддержка Microsoft (Get Help From Microsoft) —** содержит список ресурсов Интернета, позволяющих связаться с сотрудниками технической поддержки, получить доступ к сообществам поддержки и получить дополнительные данные, например узнать статус поданной ранее заявки на поддержку;
- Посетить сообщество серверов Windows Server (Visit The Windows Server Community) — предоставляет пользователям доступ к форуму в Интернете.

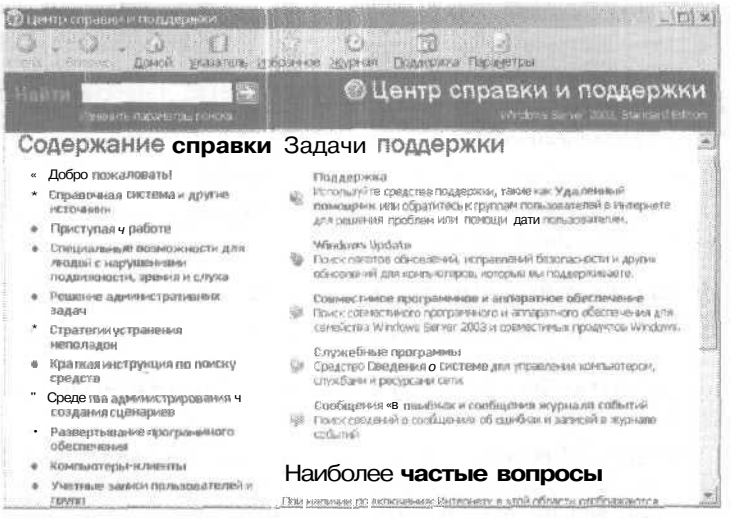


Рис. 5-1. Центр справки и поддержки поможет отыскать подробную техническую информацию и получить необходимую поддержку

Б утилитах Получить удаленную помощь (Get Remote Assistance) и Техническая поддержка Microsoft (Get Help From Microsoft) используется функция Удаленный помощник (Remote Assistance). Она реализована с помощью службы Диспетчер сеанса справки для удаленного рабочего стола (Remote Desktop Help Session Manager). Если вы и есть тот самый специалист, который получает запрос на дистанционное управление, вы увидите на экране панель, предназначенную для просмотра рабочего стола пользователя и отправки ему сообщений. Вы также можете принять на себя управление компьютером пользователя, послать сообщение в систему пользователя или выйти из сеанса, а также настраивать компьютер пользователя, как если бы он находился перед вами, причем пользователь одновременно с вами видит происходящие изменения,

Знакомство с прикладной средой

Центр справки и поддержки и вся справочная система Windows Server 2003 основаны на *прикладной среде* (application framework), предоставляемой службой Справка и поддержка (Help and Support). Администратору Windows Server 2003 не обязательно понимать все тонкости прикладной среды. Однако вам следует

знать, где хранятся необходимые файлы, чтобы вы могли проверить их, если понадобится. В этой связи важно отметить, что служба Справка и поддержка (Help and Support) выполняется в рамках процесса Svchost.exe с параметрами -K NETSVCS. В этом режиме процесс Svchost.exe выступает в роли «слушателя», который контролирует состояние той системы, в которой он запущен. Кроме того, он периодически записывает полную информацию о конфигурации системы в подкаталоги каталога *%SystemRoot%*. В этих файлах содержатся журналы, а также данные периодической записи конфигурации системы и временная память для обработки операций справочной системы.

Данные о конфигурации системы записываются *и* базу данных Hcdata.edb, которая хранится в папке *%System-Root%*\Pchealth\Helpctr\Database. Эта база данных содержит также другие типы информации справочной системы.

Контроль состояния системы

Программа контроля состояния системы Статус (Status) является другим ключевым компонентом справочной системы Windows Server 2003. Она предназначена для сбора информации, которая позволит выявить текущие или потенциальные системные проблемы, например некорректный запуск или нехватку свободной памяти на диске. Затем операционная система может обработать эту информацию и предоставить доступ к ней через Центр справки и поддержки.

Для сбора системной информации программа Статус (Status) использует службу Windows Справка и поддержка (Help and Support). Эта служба запускает исполняемый файл Svchost.exe, который, в свою очередь, использует для сбора системной информации программу Wmiprvse.exe. Информацию, собранную службой провайдера (WMIPRVSE) инструментария управления Windows (Windows Management Instrumentation, WMI), Центр справки и поддержки принимает и выводит на экран с помощью различных исполняемых файлов. Сам Центр работает под управлением исполняемого файла Helpctr.exe, который обеспечивает основной интерфейс, а также использует программы Helphost.exe и Helpsvc.exe.

Просмотр статистики **состояния** компьютера

Вот как можно просмотреть информацию, собранную программой Статус (Status).

1. Щелкните Пуск (Start) и выберите команду Справка и поддержка (Help and Support).
2. Щелкните кнопку Поддержка (Support) на панели инструментов, чтобы попасть в область Поддержка (Support), а затем щелкните ссылку Сведения об этом компьютере (My Computer Information), которая находится под заголовком См. также (See Also).
3. В правой панели щелкните Показать состояние оборудования и программного обеспечения (View the status of my system hardware and software).
4. Вы увидите сводку состояния системы (рис. 5-2). Если существуют текущие или потенциальные проблемы, то они будут отмечены. По возможности будет дана ссылка на справочный документ, в котором описано решение проблемы.

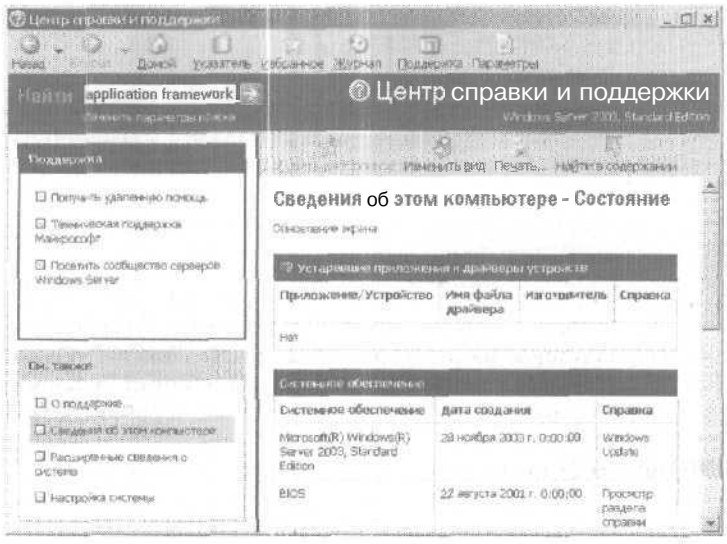


Рис. 5-2. Следует периодически контролировать состояние системы, чтобы убедиться в отсутствии текущих или потенциальных проблем

Примечание Информацию о состоянии системы собирает служба инструментария управления Windows (Windows Management Instrumentation, WMI). WMI предоставляет ряд интерфейсов, в которых реализованы классы объектов для доступа к ОС

и к ее компонентам, а также к значениям их состояния. Одним из таких классов является Win32_Computer со свойством BootupState. В нем отражается, как происходила загрузка системы — нормально, в защищенном режиме и пр. Значение этого и других свойств, которые собираются с помощью WMI, выводятся в Центре справки и поддержки (Help and Support Center) в разделах Сведения об этом компьютере (My Computer Information) и Расширенные сведения о системе (Advanced System Information).

Неполадки при сборе сведений о состоянии компьютера

Для сбора информации программой Статус (Status) следует запустить службу Справка и поддержка (Help and Support). Если параметры состояния недоступны или не обновляются, с помощью консоли Службы (Services) проверьте, запущена ли служба и правильно ли она настроена. Доступ к этой консоли вы получите через консоль Управление компьютером (Computer Management).

Если служба Справка и поддержка (Help and Support) не запущена, щелкните ее правой кнопкой и выберите команду Пуск (Start). Эта служба должна быть настроена на автоматический запуск. Если это не так, дважды щелкните ее, выберите в списке Тип запуска (Startup Type) вариант Авто (Automatic) и щелкните OK.

Другой причиной возникновения проблем при сборе информации о состоянии системы может быть недостаток свободного места на системном диске (где расположена ОС Windows). Служба Справка и поддержка (Help and Support) собирает информацию о состоянии системы и сохраняет ее в папке *%Sys*femfioo£%\Pchealth\Hclpctr\Datacoll. Информация о состоянии системы, собранная программой Статус (Status), хранится в файлах XML. Чтобы справочная подсистема могла обрабатывать эти файлы, они должны быть правильно записаны.

Автоматическое обновление

Автоматическое обновление позволяет вам всегда работать с последней версией ОС Windows Server 2003. Эта служба сравнивает программы, компоненты ОС и драйверы с имеющимся на Web-сайте Microsoft списком и определяет, требуются ли обновления.

Основные сведения об автоматических обновлениях

Настройка автоматических обновлений осуществляется в окне свойств системы. Если автоматические обновления разрешены, при наличии на сайте Microsoft новых компонентов, которые следует загрузить или установить, в системной области панели задач появится значок. Фоновый процесс проверки выполняется службой Автоматическое обновление (Automatic Updates). Автоматические обновления появляются в диалоговом окне Установка и удаление программ (Add/Remove Programs) подобно любой другой установленной программе. Удалить автоматическое обновление можно точно так же, как любую другую программу. Подробнее — в разделе «Удаление автоматических обновлений» этой главы.

Для настройки автоматического обновления предусмотрены различные варианты настройки системы.

- **Выполнять обновление системы (Keep my computer up to date)** — автоматическое обновление разрешено. Если вы сбросите этот флажок, автоматические обновления запрещаются и вы не получите извещений об их появлении. При этом вы вправе вручную загрузить обновления с Web-сайта Windows Update (*http://windowsupdate.microsoft.com/*).
- **Уведомлять о возможности загрузки обновлений, а затем еще раз уведомлять о том, что они готовы к установке (Notify me before downloading any** updates and notify me **again before installing them on my computer)** — ОС запрашивает разрешение и на загрузку, и на установку обновления. Разрешив загрузку обновления, вы вправе отложить его установку. Оно сохраняется в системе, и вы можете установить его позже.
- **Загружать обновления автоматически и уведомлять о том, что они готовы к установке (Download the updates automatically and notify me** when **they are ready to be installed)** — ОС автоматически загружает все доступные обновления, а когда они готовы к установке, спрашивает вашего разрешения. Вы вправе принять обновление или отказаться от него. Принятые обновления устанавливаются. Отвергнутые не устанавливаются, но сохраняются к системе, и вы можете установить их позже.
- **Загружать обновления автоматически и устанавливать** их **по заданному расписанию (Automatically download the** updates, and install them **on the schedule** that **I specify)** — ОС автоматически

загружает и устанавливает все доступные обновления в соответствии с заданным вами графиком. После загрузки обновлений ОС выдает сообщение, и вы имеете возможность просмотреть обновления, включенные в график установки. Обновления предлагается установить сразу или в запланированное время по графику.

Настройка автоматических обновлений

Вот как настроить автоматическое обновление системы.

1 Откройте Панель управления (Control Panel) и дважды щелкните значок Система (System). Перейдите на вкладку Автоматическое обновление (Automatic Updates), показанную на рис. 5-3.

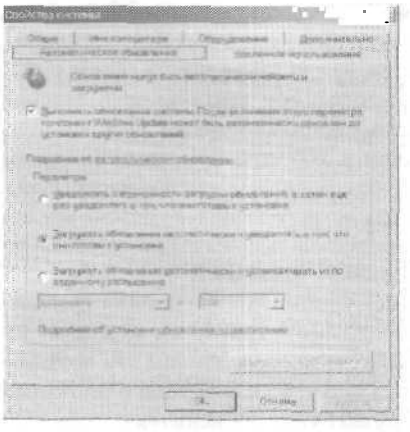


Рис. 5-3. Вы можете по-разному настроить автоматические обновления в зависимости от особенностей системы

2. Чтобы запретить автоматические обновления, сбросьте флажок Выполнять обновление системы (Keep my computer up to date). После этого обновлять систему придется вручную.

Внимание! На важных системах автоматические обновления лучше запретить. Прежде чем устанавливать обновление на рабочие серверы, его следует проверить на сервере, специально предназначенном для тестирования. Продолжительность проверки в большинстве случаев должна составлять от одной до двух недель. После тестирования обновлений вы можете вручную установить их на рабочие системы.

3. Чтобы разрешить автоматические обновления, включите флажок Выполнять обновление системы (Keep my computer up to date) и выберите один из следующих вариантов:
   - Уведомлять о возможности загрузки обновлений, а затем еще раз уведомлять о том, что они готовы к установке (Notify me before downloading any updates and notify me again before installing them on my computer) — полный контроль загрузки и установки обновлений;
   - Загружать обновления автоматически и уведомлять о том, что они готовы к установке (Download the updates automatically and notify me when they are ready to be installed) — оптимальный выбор для некритичных систем;
   - Загружать обновления автоматически и устанавливать их по заданному расписанию (Automatically download the updates, and install them on the schedule that I specify) — хороший вариант, который позволяет устанавливать обновления без помех для производственной деятельности. График обновлений может быть, например, таким: каждый день в заданное время, скажем, в 3:00 утра, или в заданный день недели и в заданное время, положим, каждое воскресенье в 5:00 утра. Если вы зарегистрировались в системе как администратор, вы будете получать сообщения об обновлениях, ожидающих установки. Вы можете отложить их установку. Если в процессе установки обновления требуется перезагрузка, го как администратор вы вправе отложить перезагрузку. Другим пользователям эта возможность недоступна. Локальные пользователи и пользователи терминальных служб будут оповещены о грядущей перезагрузке. Пользователи, запустившие приложение на сервере или работающие с общим файлом, не предупреждаются.

Внимание! Иногда установка обновлений замедляет работу системы и требует перезагрузки. Поэтому обновления лучше устанавливать вручную или планировать их установку на нерабочее время или на период малой нагрузки. Однако это не предотвратит потерю данных, если в момент перезагрузки системы пользователи работают с общими ресурсами.

4. Если вы решили устанавливать обновления по графику, щелкните OK.

Другой способ настройки автоматических обновлений — посредством групповой политики. Наиболее полезны для автоматических обновлений следующие политики:

- **Автоматическое** обновление Windows (Windows Automatic Updates) — при подключении пользователя к Интернету Windows проводит поиск доступных обновлений для этого компьютера. Политика расположена в узле Конфигурация пользователя\Административные шаблоны\Система (User Configuration\Administrative Templates\System);
- Отключить автоматическое обновление **ADM-файлов** (Turn off automatic update of ADM files) — в процессе автоматического обновления групповая политика может быть модифицирована. Как правило, это означает, что вместо нее устанавливается новая политика, которая становится доступной при следующем открытии редактора объектов *групповой политики.* Включите эту политику, чтобы групповые политики не обновлялись в процессе автоматического обновления. Эта политика расположена в *узле Конфигурация пользователя\Административные шаблоны\Система\Групповая* политика (User Configuration\Administrative Templates\System\Group Policy). Значения ее параметров игнорируются, если включена политика Всегда использовать локальные файлы ADM для редактора объектов групповой политики (Always use local ADM files for Group Policy Object Editor);
- Удалить доступ к возможностям Windows Update (Remove access to use all Windows Update **features**) - запрещает доступ ко всем функциям обновления Windows. К их числу относятся вкладка Автоматическое обновление (Automatic Updates) окна свойств системы, команды Windows Update в меню Пуск (Start) и в меню Сервис (Tools) Internet Explorer, обновление драйверов с помощью Web-сайта Windows Update в Диспетчере устройств (Device Manager). Эта политика размещена в узле Конфигурация пользователя\Административные шаблоны\Компоненты Windows\Windows Update (User Configuration*Administrative Templates\Windows Components*Windows Update);
- Настройка автоматического обновления (Configure Automatic Updates) — настраивает параметры обновления для домена, сайта, организационного подразделения или локального компьютера. Если эта политика включена, то вы настраиваете параметры аналогично тому, как это происходит на вкладке

Автоматическое обновление (Automatic Updates) окна свойств системы- Эта политика размещена в узле Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Windows Update (Computer Configuration\Administrative Templates\Windows Components\Windows Update);

- **Укажите расположение службы Windows Update в интрасети (Specify intranet Microsoft update service location)** — задает внутренний Web-сервер вместо Web-сайта Windows Update в качестве места, откуда следует загружать обновления. Эта политика размещена в узле Конфигурация компьютера\ Административные шаблоны\Компоненты Windows\Windows Update (Computer Configuration\Administrative Templates\Windows Components\Windows Update) и рассматривается в следующем разделе.

Настройка серверов обновления

Если сеть состоит из сотен или тысяч компьютеров, процесс автоматического обновления может занимать значительную часть ее полосы пропускания. Нерационально проверять наличие обновлений и устанавливать их через Интернет на каждом компьютере в отдельности. Вместо этого имеет смысл включить политику Укажите расположение службы Windows Update в интрасети (Specify intranet Microsoft update service location), которая предписывает индивидуальным компьютерам проверять наличие обновлений на специальном внутреннем сервере.

Выделенный сервер обновлений должен быть Web-сервером, на котором запущены службы TTS. Позаботьтесь, чтобы у него хватило ресурсов для обработки дополнительной нагрузки, которая может оказаться значительной в больших сетях в часы высокой активности. Кроме того, серверу обновлений необходим доступ к внешней сети через порт 80. Удостоверьтесь, что с этим портом не возникнет никаких проблем из-за брандмауэра или прокси-сервера.

В процессе обновления происходит сбор информации о настройке компьютера и о статистических параметрах его работы. Эта информация может храниться на отдельном сервере статистики (внутреннем сервере со службами IIS) или на самом сервере обновления.

Вот как задать внутренний сервер обновления.

1. Настройте сервер в соответствии с указанными ранее требованиями.
2. В консоли Групповая политика (Group Policy) для нужного домена, сайта или организационного подразделения откройте узел Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Windows Update (Computer Configuration\Administrative Templates\Windows Components\Windows Update) и дважды щелкните политику Укажите расположение службы Windows Update в интрасети (Specify Intranet Microsoft Update Service Location).
3. Установите переключатель Включен (Enabled).
4. Введите URL сервера обновления в поле Укажите службу в интрассти для поиска обновлений (Set the intranet update service for detecting updates). В большинстве случаев URL имеет вид *http://servername*, например *http://CorpUpdateServer01*.
5. Введите URL сервера статистики в поле Укажите сервер статистики в интрасети (Set the intranet statistics server). Не обязательно, чтобы это был отдельный сервер; вы можете указать в этом поле сервер обновления.
6. Щелкните OK.

После обновления соответствующего объекта групповой политики системы под управлением Windows 2000 (с установленным Service Pack 3 или более поздним), Windows XP (с установленным Service Pack 1 или более поздним) и Windows Server 2003 будут обращаться за обновлениями к серверу обновления. В течение нескольких дней или даже недель следует внимательно следить за серверами обновления и статистики, чтобы убедиться в их нормальной работе.

Загрузка и установка автоматических обновлений

О наличии очередного обновления сообщает специальный значок в системной области панели задач. Щелкните его, чтобы открыть окно Обновления (Updates). В этом окне щелкните Установить (Install), если разрешили системе автоматическую загрузку, или Загрузить (Download), если предпочли получать извещение перед загрузкой. Чтобы отложить обновление, щелкните Напомнить позже (Remind Me Later).

Чтобы получить больше информации об обновлении или произвести выборочную установку компонентов обновления, щелк-

ните кнопку Состав (Details). Появится описание каждого обновления. Чтобы запретить обновление какого-либо компонента, сбросьте соответствующий флажок. Закончив подготовку, щелкните Установить (Install),

Внимание! Некоторые обновления требуют перезагрузки компьютера. Чтобы не прерывать процессы на рабочем сервере, продуманно планируйте установку и загрузку.

Удаление автоматических обновлений

Если в результате автоматического обновления в системе возникли проблемы, не огорчайтесь. Можно удалить автоматическое обновление, как любую другую программу.

1. В панели управления дважды щелкните значок Установка и удаление программ (Add/Remove Programs). В открывшемся диалоговом окне перейдите на вкладку Замена или удаление программ (Change or Remove Programs).
2. Выберите автоматическое обновление, которое вы хотите удалить, и щелкните кнопку Заменить (Change) или Удалить (Remove). Чтобы удалить другие обновления, повторите этот шаг.
3. Щелкните Закрыть (Close). Если требуется перезагрузка системы, на экране появится соответствующее сообщение.

Удаленный доступ к серверам

В Windows Server 2003 имеется несколько функций удаленного соединения. *Удаленная помощь* (remote assistance) позволяет отправлять заявки специалистам отдела поддержки на обслуживание компьютера. Через *удаленный рабочий стол* (remote desktop) пользователи могут дистанционно подключаться к компьютеру и получать доступ к его ресурсам. По умолчанию все функции удаленного соединения отключены. Вам придется активизировать их вручную.

Удаленный помощник

Удаленный помощник (Remote Assistance) — полезная функция для службы технической поддержки. Администраторы вправе не только разрешить сотрудникам просматривать рабочий стол сервера, но и передать им управление столом для решения возникшей проблемы. Начинающий же администратор может выполнить какое-либо действие и даже настроить систему под наблю-

денисм более опытного коллеги. Ключевым моментом удаленной помощи является распределение прав доступа.

Вот как настроить удаленную помощь.

1. Дважды щелкните значок Система (System) на панели управления и перейдите на вкладку Удаленное использование (Remote).
2. Чтобы запретить удаленную помощь, сбросьте флажок Разрешить отправку *приглашения* удаленному помощнику (Turn on Remote Assistance and allow invitations to be sent from this computer) и щелкните OK. Остальные пункты пропустите.
3. Чтобы разрешить удаленную помощь, установите флажок Разрешить *отправку приглашения* удаленному *помощнику* (Turn on Remote Assistance and allow invitations to be sent from this computer). Затем щелкните кнопку Подробнее (Advanced). Откроется диалоговое окно, показанное на рис. 5-4.

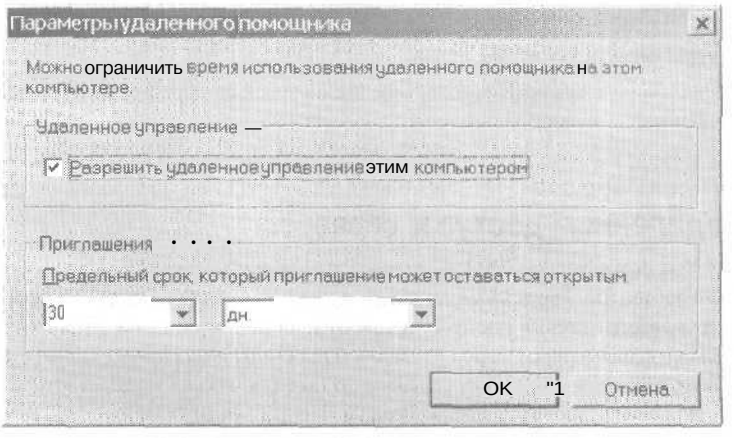


Рис. 5-4. В этом диалоговом **окне** настраивают удаленную помощь

4. Сбросьте флажок Разрешить *удаленное управление* этим компьютером (Allow this computer to be controlled remotely), чтобы компьютер стал доступен только для просмотра. Если флажок установлен, специалисты технической поддержки смогут также управлять компьютером.
5. Параметры группы Приглашения (Invitations) управляют максимальной продолжительностью действия запросов. Ее

задают в минутах, часах или днях (до 30 дней, что указано по умолчанию).

Внимание! Установив максимальную продолжительность действия приглашения, вы тем самым даете сотрудникам технической поддержки определенное время для ответа на вопрос. Но это также означает, что в течение этого времени они имеют доступ к вашему компьютеру. Например, вы посылаете сотруднику технической поддержки запрос, продолжительность действия которого 30 дней. Даже если он решит проблему в первый же день, еще в течение 30 дней у него будет доступ к компьютеру, что нежелательно из соображений безопасности. Чтобы снизить риск, рекомендуется сокращать максимальную продолжительность действия приглашений, скажем, до 1 часа. Если проблема не решена в отведенный срок, можно послать еще один запрос.

6. Закончив настройку удаленной помощи, дважды щелкните OK.

Удаленный рабочий стол

Удаленный рабочий стол предоставляет пользователям несколько уровней доступа.

- Если вы вошли в систему локально, а затем регистрируетесь дистанционно, то локальный рабочий стол автоматически блокируется, и вы получаете доступ ко всем запущенным приложениям, как если бы находились перед локальным компьютером. Эта функция полезна, если вы хотите работать, будучи дома или в отъезде, так как позволяет продолжать работу «с того же самого места».
- Если вы включены в список дистанционного доступа для этого компьютера и не зарегистрированы в системе, вы можете открыть новый сеанс Windows. Он будет проходить так, как если бы вы работали на локальном компьютере, даже если на этом компьютере зарегистрированы другие пользователи. Таким образом, к одному серверу могут одновременно получить доступ несколько пользователей.

Функция Удаленный рабочий стол (Remote desktop) по умолчанию заблокирована. Следует вручную включить ее, тем самым разрешая доступ к компьютеру. Когда она активизирована, к компьютеру может подключиться любой член группы Администраторы (Administrators), Пользователи других групп, чтобы полу-

чить доступ к компьютеру, должны быть указаны в списке удаленного доступа. Вот как настроить удаленный рабочий стол.

1. Дважды щелкните значок Система (System) на панели управления и перейдите на вкладку Удаленное использование (Remote).
2. Чтобы отключить доступ к удаленному рабочему столу, сбросьте флажок Разрешить удаленный доступ к этому компьютеру (Allow users to connect remotely to this computer) и щелкните OK. Остальные пункты пропустите.
3. Чтобы разрешить доступ к удаленному рабочему столу, включите флажок Разрешить удаленный доступ к этому компьютеру (Allow users to connect remotely to this computer). Затем щелкните Выбрать удаленных пользователей (Select Remote Users).
4. Чтобы предоставить пользователю доступ к удаленному рабочему столу, щелкните Добавить (Add). Введите имя пользователя в поле Имя (Name) и щелкните Проверить имена (Check Names). Выберите учетную запись, которую хотите использовать, и щелкните OK. При необходимости повторите этот пункт для других пользователей. По завершении щелкните OK.
5. Чтобы отменить разрешение на удаленный доступ для учетной записи пользователя, выделите ее и щелкните Удалить (Remove).
6. После завершения дважды щелкните OK.

Созданиесоединенияудаленногорабочегостола

Как администратор вы можете создавать соединения удаленного рабочего стола с серверами и рабочими станциями Windows. В Windows 2003 Server для этого необходимо установить службы терминалов (Terminal Services) и настроить их на использование в режиме удаленного доступа. В Windows XP соединения удаленного рабочего стола разрешены по умолчанию и все администраторы автоматически имеют право доступа. В Windows Server 2003 удаленный рабочий стол устанавливается автоматически, но по умолчанию отключен, и вам вручную следует разрешить эту функцию.

Вот один из способов создать соединение удаленного рабочего стола с сервером или с рабочей станицей.

1. Щелкните Пуск (Stan), затем Программы (Programs) или Все программы (All Programs), затем Стандартные (Accessories), затем Связь (Communications), затем Подключение к удаленному рабочему столу (Remote Desktop Connection). Откроется одноименное диалоговое окно.
2. В тюле Компьютер (Computer) введите имя компьютера, с которым хотите установить соединение. Если вы не знаете имени, воспользуйтесь предлагаемым раскрывающимся списком или укажите в списке вариант Поиск других (Browse For More), чтобы открыть список доменов и компьютеров в этих доменах.
3. По умолчанию Windows Server 2003 берет для регистрации на удаленном компьютере текущее имя пользователя, домен и пароль. Если нужна информация другой учетной записи, щелкните Параметры (Options) и заполните поля. Имя пользователя (User Name), Пароль (Password) и Домен (Domain).
4. Щелкните Подключиться (Connect). При необходимости введите пароль и щелкните OK. Если соединение создано успешно, вы увидите окно удаленного рабочего стола выбранного компьютера и получите возможность работать с ресурсами этого компьютера. Если соединение создать не удалось, проверьте введенную вами информацию и повторите попытку

Совет Щелкнув кнопку Параметры (Options) в диалоговом окне Подключение к удаленному рабочему столу (Remote Desktop Connection), вы сможете задать дополнительные параметры создания и сохранения соединений. Они в частности позволяют изменять размеры удаленного рабочего стола, управлять соединениями с локальными ресурсами (принтерами, последовательными портами, дисководами), разрешать и запрещать локальное кэширование и сжатие данных.

С командой Подключение к удаленному рабочему столу (Remote Desktop Connection) работать просто, но она неудобна, если вам приходится создавать удаленные соединения с компьютерами достаточно часто. Вместо нее рекомендуется обращаться к консоли Удаленные рабочие столы (Remote Desktops). В ней можно настраивать соединения с несколькими системами и затем легко переключаться с одного соединения на другое.

На рис. 5-5 показана консоль Удаленные рабочие столы (Remote Desktops) с настроенными соединениями для CorpServer01

и CorpServer02. Чтобы создать новое соединение, щелкните правой кнопкой узел Удаленные рабочие столы (Remote Desktops), выберите команду Добавление нового подключения (Add New Connection) и введите имя сервера (или IP-адрес) и другую необходимую для регистрации информацию.

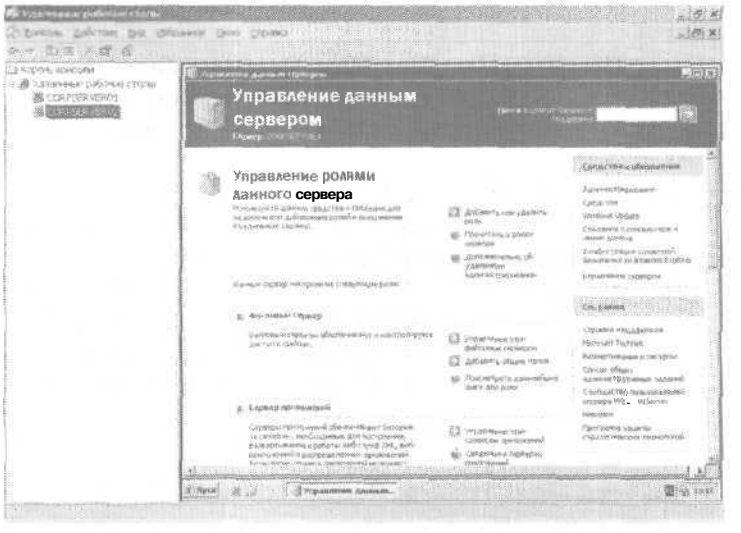


Рис. 5-5. Консоль Удаленные рабочие столы (Remote Desktops)

Чтобы вывести на экран удаленный рабочий стол после того, как соединение установлено, достаточно щелкнуть строку соединения. Если по какой-то причине соединение разорвано, щелкните его строку правой кнопкой и выберите команду Подключиться (Connect).

Настройка системного времени Windows

По мере развития ОС Windows системное время приобретает все большее значение, особенно в связи с системой защиты Kerberos, которая является механизмом аутентификации по умолчанию в Windows Server 2003. Для корректной работы системы Kerberos системные часы должны быть строго синхронизованы. Если часы разных систем идут вразнобой, *билеты проверки подлинности* (authentication tickets) могут стать недействительными, прежде чем достигнут целевого узла.

Поддерживать ход системных часов непросто. То они отстанут, то убегут вперед, то пользователь поставит на них неправильное время — да мало ли что может произойти. Для решения проблем, связанных с системным временем и синхронизацией, предназначена служба времени Windows (Windows Time), которая залает в сети единое время на основе показаний специализированного сервера Интернета.

Службы времени, используемые в настольных компьютерах и на серверах, несколько отличаются между собой. В последующих разделах рассматривается служба времени Windows Server 2003. Подробно о службе времени для Windows XP Professional рассказано в главе 3 книги «Microsoft Windows XP Professional. *Справочник администратора*» (Русская Редакция, 2002).

Служба времени Windows и Windows Server 2003

Отдельные серверы и рядовые серверы настраиваются на автоматическую синхронизацию с *полномочным сервером времени* (authoritative time server). Характер работы службы времени зависит от того, является ли система частью рабочей группы или домена.

Вот как работает служба времени в рабочих группах.

- Системы настраиваются на автоматическую синхронизацию с сервером времени Интернета - полномочным сервером времени. По умолчанию им является сервер time.windows.com. Вы вправе выбрать в качестве полномочного сервера времени другие серверы, например thne.nist.gov.
- С помощью протокола SNTP (Simple Network Time Protocol) служба времени Windows периодически (по умолчанию через каждые четыре часа) опрашивает полномочный сервер времени. Точные значения периодичности опроса задаются параметрами реестра MinPollInterval и MaxPollInterval в узле \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\Config.
- Если обнаружена разница времени между сервером и системой, служба постепенно исправляет время. Точная скорость коррекции задается параметрами реестра UpdateInterval и FrequencyCorrectRate в узле \HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\Config.

Примечание По умолчанию SNTP использует порт 123 протокола UDP. Если этот порт не имеет доступа к Интернету, вам не удастся синхронизировать время.

В доменах эталоном времени автоматически считается контроллер, и другие компьютеры домена синхронизируются с ним. Если этот сервер оказывается недоступным в качестве источника точного времени, эту функцию автоматически принимает на себя другой контроллер домена. Чтобы лучше управлять службой времени Windows в домене, установите соответствующие программные компоненты, из которых ключевыми являются два приложения.

- Клиент **NTP** — устанавливает службу времени Windows и позволяет системе синхронизировать часы с заданными серверами времени. Клиент имеет значительно более широкие возможности настройки, чем стандартная служба времени Windows XP. Групповая политика позволяет весьма тонко управлять службой времени.
- **Сервер NTP** —устанавливает службу времени Windows и настраивает систему в качестве сервера времени. После этого клиенты NTP, которые могут работать под управлением Windows XP или Windows Server 2003, при необходимости синхронизируют время с этим компьютером. Как и в случае клиента NTP, управление службой времени осуществляется средствами групповой политики.

Любая система Windows Server 2003 может быть как клиентом, так и сервером NTP. Обычно серверы NTP также настраиваются и в качестве клиентов NTP. При этом сервер NTP обеспечивает службу синхронизации времени в организации. Сообщения SNTP перелаются как широковещательные в локальной сети и не поступают в Интернет. С другой стороны, сервер NTP является клиентом, который синхронизирует свое время с надежным сервером времени Интернета, например с time.windows.com.

Для включения и настройки клиентов и серверов Windows NTP используются групповые политики, размещенные в узле Конфигурация компьютера\Административные шаблоны\Система\Служба времени Windows (Computer Configuration\Administrative Templates\System\Windows Time Service).

Включение и отключение службы времени

Вот как можно включить или отключить сетевую синхронизацию времени дли одиночного или рядового сервера.

1. На панели управления дважды щелкните значок Дата и время (Date and Time) и перейдите на вкладку Сетевое время (Network Time).

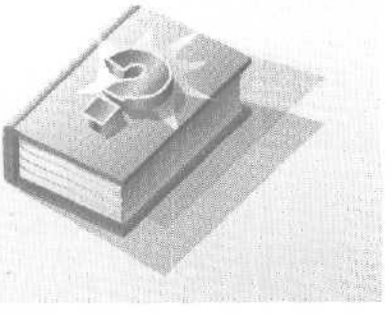
2. Чтобы включить синхронизацию времени, включите флажок Выполнять синхронизацию с сервером времени в Интернете (Automatically synchronize with an Internet time server), а затем выберите сервер времени, который хотите использовать. Чтобы использовать локальный сервер времени или другой внешний сервер, просто введите его DNS-имя в поле Сервер (Server). Кроме того, убедитесь, что Служба времени Windows (Windows Time Service) запущена.
3. Чтобы отключить синхронизацию времени, сбросьте флажок Выполнять синхронизацию с сервером времени в Интернете (Automatically synchronize with an Internet time server).
4. Щелкните OK.

Если вы используете синхронизацию времени, имейте в виду, что в больших сетях гораздо эффективнее установить локальный сервер времени (для доменов это стандартная конфигурация). В случае использования локального сервера времени сообщения SNTP от рабочих станций и серверов передаются в пределах локальной сети и не выходят в Интернет. Внешний трафик, относящийся к службе времени, ограничен лишь обменом сообщениями между локальным и внешним серверами времени.

Часть II

Администрирование служб каталогов Microsoft Windows Server 2003

В этой части описано управление службой каталогов Microsoft Windows Server 2003. В главе 6 вы познакомитесь со службой Active Directory. В главе 7 изучаются основные задачи по ее администрированию. В главе 8 описаны системные учетные записи, встроенные группы, права пользователей, встроенные возможности и неявные группы. О создании учетных записей пользователей и групп рассказано в главе 9. Методика управления существующими учетными записями излагается в главе 10.



Глава 6

Служба Active Directory

Расширяемая и масштабируемая служба каталогов Active Directory позволяет эффективно управлять сетевыми ресурсами.

Знакомство с Active Directory

Служба Active Directory — сердце Microsoft Windows Server 2003. С ней так или иначе связаны практически все административные задачи. Технология Active Directory основана на стандартных Интернет-протоколах и помогает четко определять структуру сети.

Active Directory и DNS

В Active Directory используется доменная система имен (Domain Name System, DNS) — стандартная служба Интернета, организующая группы компьютеров в домены. В отличие от одноуровневой структуры доменов Windows NT 4.0, домены DNS имеют иерархическую структуру, которая составляет основу Интернета. Разные уровни этой иерархии идентифицируют компьютеры, домены организаций и домены верхнего уровня. DNS также служит для преобразования *имен узлов*, например 7eta.webatwork.com, R численные IP-адреса, например 192.168.19.2. Средствами DNS иерархию доменов Active Directory можно вписать в пространство Интернета или оставить самостоятельной и изолированной от внешнего доступа.

Для доступа к ресурсам *к* домене применяется полное имя узла, например zeta.webatwork.com. Здесь zeta — имя индивидуального компьютера, webatwork — домен организации, а com — домен верхнего уровня. Домены верхнего уровня составляют фундамент иерархии DNS и потому называются *корневыми доменами* (root domains). Они организованы географически, с названиями па основе двухбуквенных кодов стран (га для России), по типу организации *(com* для коммерческих организаций) и по назначению *(mil* для военных организаций США).

Обычные домены, например *microsoft.com*, называются *родительскими* (parent domain), поскольку они образуют основу организационной структуры. Родительские домены можно разделить на поддомены разных отделов или удаленных филиалов. Например, полное имя компьютера в офисе Microsoft в Сиэтле может быть *jacob.seattle.microsoft.com*, где Jacob — имя компьютера, seattle — поддомен, а microsoft.com — родительский домен. Другое название поддомена — *дочерний домен* (child domain).

Итак, DNS — неотъемлемая часть технологии Active Directors', причем настолько, что перед установкой Active Directory вы обязаны настроить DNS в сети, если еще не сделали этого (подробнее о работе с DNS — в *главе* 20). Сконфигурировав DNS, установите Active Directory с помощью мастера: в меню Пуск (Start) выберите команду Выполнить (Run), в поле Открыть (Open) введите dcpromo и щелкните OK. Если в сети нет доменов, мастер поможет создать домен и сконфигурировать в нем Active Directory. Мастер также помогает добавлять дочерние домены в существующие структуры.

Примечание Далее в этой главе Active Directory и домены Active Directory мы будем называть просто *каталогом* и доменами, кроме тех случаев, когда надо отличать структуры Active Directory от структур DNS или Windows NT.

Компоненты Active Directory

Active Directory объединяет логическую и физическую структуру для компонентов сети. К логической структуре относятся следующие элементы:

- **организационное подразделение (organizationalunit)** — подгруппа компьютеров, как правило, отражающая структуру компании;
- **домен(domain)** — группакомпьютеров, совместно использующих общую БД каталога;
- **дерево доменов** (domain **tree)** — один или несколько доменов, совместно использующих непрерывное пространство имен;
- **лес доменов (domain forest)** — одно или несколько деревьев, совместно использующих информацию каталога.

К физическим структурам следующие элементы:

- **подсеть (subnet)** — сетевая группа с заданной областью IP-адресов и сетевой маской;

- **сайт** (site) — одна или несколько подсетей. Сайт используется для настройки доступа к каталогу и для репликации.

Работа с компонентами Active Directory

Логические структуры Active Directory помогают организовывать объекты каталога и управлять сетевыми учетными записями и общими ресурсами. К логическим структурам относятся леса доменов, деревья доменов, сами домены и ОП. Сайты и подсети, с другой стороны, являются физическими элементами, которые помогают планировать реальную структуру сети. На основании физических структур формируются сетевые связи и физические границы сетевых ресурсов.

Понятие домена

Домен Active Directory — это просто группа компьютеров, совместно использующих общую БД. Имена доменов Active Directory должны быть уникальными. Например, у вас не может быть двух доменов microsoft.com, но может быть родительский домен microsoft.com с дочерними доменами seattle.microsoft.com и ny.microsoft.com. Если домен является частью закрытой сети, имя, присвоенное новому домену, не должно конфликтовать ни с одним из существующих имен доменов в этой сети. Если домен — часть глобальной сети Интернет, то его имя не должно конфликтовать ни с одним из существующих имен доменов в Интернете. Чтобы гарантировать уникальность имен в Интернете, имя родительского домена необходимо зарегистрировать через любую полномочную регистрационную организацию. Список действующих полномочных регистрационных организаций имеется в InterNIC (*http://www.internic.net*).

В каждом домене действуют собственные политики безопасности и доверительные отношения с другими доменами. Зачастую домены распределяются по нескольким физическим расположениям, т. е. состоят из нескольких сайтов, а сайты — объединяют несколько подсетей. В БД каталога домена хранятся объекты, определяющие учетные записи для пользователей, групп и компьютеров, а также общие ресурсы, например принтеры и папки.

Примечание Об учетных записях пользователей и групп рассказано в главе 8. Об учетных записях компьютеров и разных типах компьютеров, используемых доменами Windows Server 2003, — в разделе «Работа с доменами Active Directory» этой главы.

Функции домена ограничиваются и регулируются режимом его функционирования. Существует четыре функциональных режима доменов:

- **смешанный режим Windows 2000 (mixed mode)** — поддерживает контроллеры доменов, работающие под управлением Windows NT 4.0, Windows 2000 и Windows Server 2003;
- **основной режим Windows 2000 (native mode)** — поддерживает контроллеры доменов, работающие под управлением Windows 2000 и Windows Server 2003;
- **промежуточный режим Windows Server 2003 (interim mode)** — поддерживает контроллеры доменов, работающие под управлением Windows NT 4.0 и Windows Server 2003;
- **режим Windows Server 2003** — поддерживает контроллеры доменов, работающие под управлением Windows Server 2003.

Подробнее функциональные режимы доменов рассмотрены в разделе «Использование доменов Windows NT и Windows 2000 с Active Directory» этой главы.

Леса и деревья

Каждый домен Active Directory обладает DNS-именем типа microsoft.com. Домены, совместно использующие данные каталога, образуют *лес* (forest). Имена доменов леса в иерархии имен DNS бывают *несмежными* (discontiguous) или *смежными* (contiguous).

Домены, обладающие смежной структурой имен, называют деревом доменов (рис. 6-1). На рисунке у корневого домена msnbc.com имеются два дочерних — seattle.msnbc.com и ny.msnbc.com. У них в свою очередь тоже есть поддомены. Все они являются частью одного дерева, так как у них один и тот же корневой домен.

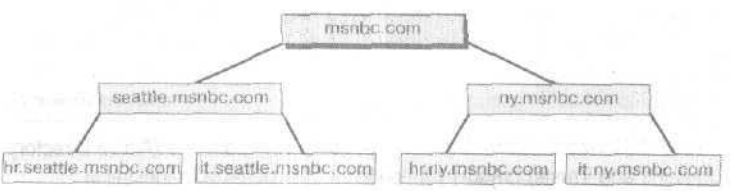


Рис. 6-1. Домены в одном дереве совместно используют смежную структуру имен

Если у доменов леса несмежные DNS-имена, они образуют отдельные деревья доменов в лесу. В лес можно включить одно или несколько деревьев (рис. 6-2). На рисунке домены msnbc.com и microsoft.com образуют корни отдельных деревьев доменов в одном лесу.

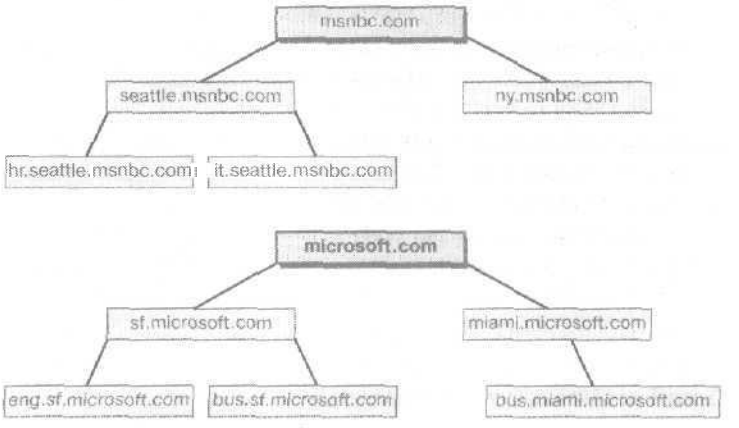


Рис. 6-2. Разные деревья в лесу обладают несмежными структурами имен

Для доступа к доменным структурам предназначена консоль Active Directory — домены и доверие (Active Directory Domains and Trusts), показанная на рис. 6-3. Для каждого корневого домена отображаются отдельные записи. На рисунке показан домен *adatum.com*.

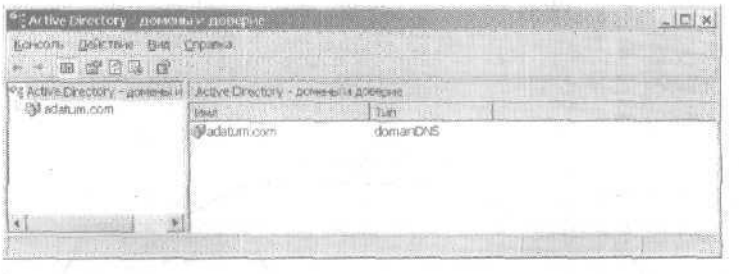


Рис. 6-3. Консоль Active Directory — домены и доверие (Active Directory Domains and Trusts) служит для работы с доменами, деревьями и лесами

Функции лесов ограничиваются и регулируются функциональным режимом леса. Таких режимов три:

- **Windows 2000** — поддерживает контроллеры доменов, работающие под управлением Windows NT 4.0, Windows 2000 и Windows Server 2003;
- **промежуточный (interim) Windows Server 2003** — поддерживает контроллеры доменов, работающие под управлением Windows NT 4.0 и Windows Server 2003;
- **Windows Server 2003** — поддерживает контроллеры доменов, работающие под управлением Windows Server 2003.

Самые современные функции Active Directory доступны в режиме Windows Server 2003. Если все домены леса работают в этом режиме, вы сможете пользоваться улучшенной репликацией глобальных каталогов и более эффективной репликацией данных Active Directory. Также вы получите возможность отключать классы и атрибуты схемы, использовать динамические вспомогательные классы, переименовывать домены и создавать в лесу односторонние, двухсторонние и транзитивные доверительные отношения.

Организационные подразделения

Организационные подразделения (ОП) — это подгруппы в доменах, которые часто отражают функциональную структуру организации. ОГ1 представляют собой своего рода логические контейнеры, в которых размещаются учетные записи, общие ресурсы и другие ОП. Например, вы вправе создать в домене microsoft.com подразделения HumanResourses, IT, Marketing. Потом эту схему можно расширить, чтобы она содержала дочерние подразделения.

В ОП разрешается помещать объекты только из родительского домена. Например, ОП из домена seattle.microsoft.com содержат объекты только этого домена. Добавлять туда объекты из ny.microsoft.com нельзя. ОП очень удобны при формировании функциональной или бизнес-структуры организации. Но это не единственная причина их применения.

- ОП позволяют определять групповую политику для небольшого набора ресурсов в домене, не применяя се ко всему домену
- С помощью ОП создаются компактные и более управляемые представления объектов каталога в домене, что помогает эффективнее управлять ресурсами.
- ОП позволяют делегировать полномочия и контролировать административный доступ к ресурсам домена, что помогает

задавать пределы полномочий администраторов в домене. Вы можете передать пользователю А административные полномочия только для одного ОП и в то же время передать пользователю В административные полномочия для всех ОП в домене.

ОП представлены в виде папок в консоли Active Directory — *пользователи* и *компьютеры* (Active Directory Users and Computers), показанной на рис. 6-4.

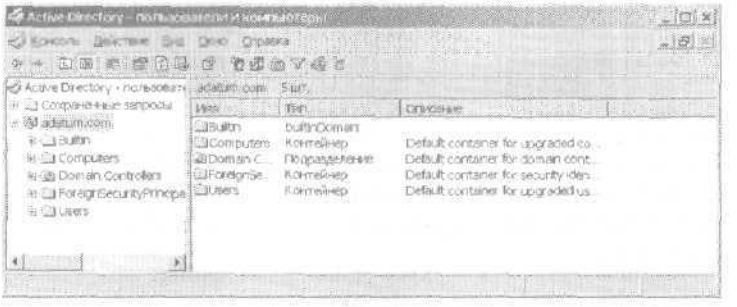


Рис. 6-4. Консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers) позволяет управлять *пользователями*, группами, компьютерами и ОП

Сайты и подсети

Сайт — это группа компьютеров в одной или нескольких IP-подсетях, используемая для планирования физической структуры сети. Планирование сайта происходит независимо от логической структуры домена. Active Directory позволяет создать множество сайтов в одном домене или один сайт, охватывающий множество доменов. Также пет связи между диапазоном IP-адресов сайта и пространством имен домена.

В отличие от сайтов, способных охватывать множество областей IP-адресов, подсети обладают заданной областью IP-адресов и сетевой маской. Имена подсетей указываются в формате *сеть/битовая маска,* например 192.168.19.0/24, где сетевой адрес 192.168.19.0 и сетевая маска 255.255.255.0 скомбинированы в имя подсети 192.168.19.0/24.

Примечание Вам не нужно знать, как создается имя подсети. Чаще всего достаточно ввести сетевой адрес и сетевую маску, а ОС Windows Server 2003 сама сгенерирует имя подсети.

Компьютеры приписываются к сайтам в зависимости от местоположения в подсети или в наборе подсетей. Если компьютеры в подсетях способны взаимодействовать на достаточно высоких скоростях, их называют *хорошо связанными* (well connected). В идеале сайты состоят из хорошо связанных подсетей и компьютеров. Если скорость обмена между подсетями и компьютерами низка, может потребоваться создать несколько сайтов. Хорошая связь дает сайтам некоторые преимущества.

- Когда клиент входит в домен, в процессе аутентификации сначала производится поиск локального контроллера домена в сайте клиента, т. е. по возможности первыми опрашиваются локальные контроллеры, что ограничивает сетевой трафик и ускоряет аутентификацию.
- Информация каталога реплицируется чаще *внутри* сайтов, чем *между* сайтами. Это снижает межсетевой трафик, вызванный репликацией, и гарантирует, что локальные контроллеры доменов быстро получат обновленную информацию. Вы можете настроить порядок репликации данных каталога, используя *связи сайтов* (site links). Например, определить *сервер-плацдарм* (bridgehead) для репликации между сайтами. Основная часть нагрузки от репликации между сайтами ляжет на этот специализированный сервер, а не на любой доступный сервер сайта.

Сайты и подсети настраиваются в консоли Active Directory — сайты и службы (Active Directory Sites and Services), показанной на рис. 6-5.

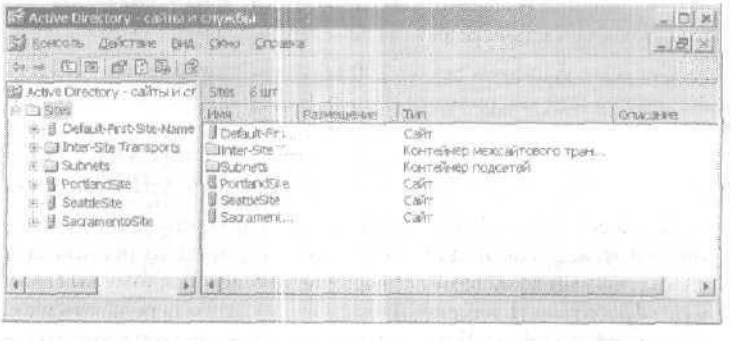


Рис. 6-5. Консоль Active Directory — сайты и службы (Active Directory Sites and Services) позволяет управлять сайтами и подсетями

Работа с доменами Active Directory

В сети Windows Server 2003 служба Active Directory настраивается одновременно с DNS. Тем не менее у доменов Active Directory и доменов DNS разное назначение. Домены Active Directory помогают управлять учетными записями, ресурсами и защитой. Иерархия доменов DNS предназначена, главным образом, для разрешения имен.

Active Directory спроектирована для работы не только с Microsoft Windows Server 2003, но и с Windows 95/98/NT/XP/2000. При установленном клиентском ПО системы Windows 95/98/XP/2000 работают в сети как клиенты Active Directory. Системы Windows NT и другие версии Windows без клиентского ПО Active Directory работают в сети, как если бы они располагались в домене Windows NT, если этот домен настроен и его использование допускается функциональным режимом домена Active Directory.

Использование Windows Server 2003, Windows XP и Windows 2000 с Active Directory

В полной мере воспользоваться преимуществами Active Directory способны компьютеры, работающие под управлением Windows XP Professional и Windows 2000. Они работают в сети как клиенты Active Directory и им доступны транзитивные доверительные отношения, существующие в дереве или лесу доменов. Транзитивное доверие устанавливается автоматически в соответствии со структурой леса и системой разрешений, определенных в нем. Эти отношения позволяют авторизованным пользователям получать доступ к ресурсам в любом домене леса.

Система Windows Server 2003 функционирует как контроллер домена или как рядовой сервер. Рядовые серверы становятся контроллерами после установки Active Directory; контроллеры понижаются до рядовых серверов *после* удаления Active Directory. Оба процесса выполняет мастер установки Active Directory.

В домене может быть несколько контроллеров. Они реплицируют между собой данные каталога по модели репликации с несколькими хозяевами, которая позволяет каждому контроллеру обрабатывать изменения каталога, а затем передавать их на другие контроллеры. Благодаря структуре с несколькими хозяевами все контроллеры по умолчанию обладают равной ответственностью. Впрочем, вы вправе предоставить некоторым кон-

троллерам домена приоритет над другими в определенных задачах, например создать сервер-плацдарм, который обладает приоритетом при репликации данных каталога на другие сайты. Кроме того, некоторые задачи лучше выполнять на выделенном сервере. Сервер, обрабатывающий специфический тип задач, называется *хозяином операций* (operations master). Существует пять различных операций, которые назначают разным контроллерам домена (см. далее в этой главе).

Для всех компьютеров с Windows 2000, Windows XP Professional и Windows Server 2003, присоединенных к домену, создаются учетные записи, хранящиеся, подобно другим ресурсам, в виде объектов Active Directory. Учетные записи компьютеров служат для управления доступом к сети и ее ресурсам, Прежде чем компьютер получает доступ к домену по своей учетной записи, он в обязательном порядке проходит процедуру аутентификации.

Примечание В Windows Server 2003 для аутентификации пользователей и компьютеров используется глобальный каталог Active Directory. Если глобальный каталог недоступен, войти в домен могут только члены группы администраторов домена. Чтобы избежать пододной проблемы, воспользуйтесь возможностью локального кэширования членства в универсальных группах (см. далее в этой главе).

Active Directory и Windows 9x

Компьютеры с Windows 95/98 работают с Active Directory двумя способами. В зависимости от конфигурации сети они получают доступ к сети как часть домена Windows NT или как часть домена Active Directory.

Вход в сеть через домен Windows NT

Если в сети используются системы Windows *9x,* но клиент Active Directory на них не установлен, эти системы получают доступ к сети как часть существующего домена Windows NT.

- Если ActiveDirectory работает в смешанном режиме, в сети для осуществления входа в систему необходим эмулятор главного контроллера домена (primary domain controller, PDC) или резервный контроллер домена (backup domain controller, BDC).
- Если Active Directory работает в основном режиме, для осуществления входа в систему требуется резервный контроллер домена.

- В рамках эмуляции домена Windows NT системы Windows *9x* могут обращаться только к ресурсам, доступным по односторонним доверительным отношениям Windows NT. которые должны быть явно заданы администратором. Это справедливо для доступа и через контроллер Windows Server 2003, и через резервный контроллер Windows NT.

Вход в сеть в качестве клиента Active Directory

Если Active Directory работает в основном режиме, системы Windows *9x* могут получить доступ к сети как часть домена Active Directory. После установки клиентского ПО эти системы в полной мере воспользуются *особенностями* Active Directory и транзитивными доверительными отношениями по всему дереву или лесу.

Установка клиента Active Directory

1. Войдите в систему на компьютере Windows *9x*, который хотите настроить в качестве клиента, и встаньте установочный компакт-диск Windows 2000 Server или Windows Server 2003.
2. Щелкните кнопку Пуск (Start) и выберите Выполнить (Run).
3. Введите ***E:\Clients\Win9X\Dsclient.exe***, где E — обозначение дисковода для компакт-дисков, и щелкните OK.
4. В ходе выполнения программа записывает несколько файлов на компьютер клиента и запускает Мастер установки клиентов службы каталогов (Directory Service Client Setup Wizard). Прочтите текст в окне приветствия и щелкните Далее (Next).
5. Щелкните Далее (Next). Мастер определит конфигурацию системы и установит нужные файлы.
6. Щелкните Готово (Finish) и перезагрузите компьютер.
7. В панели управления дважды щелкните значок Сеть (Network).
8. На вкладке Конфигурация (Configuration), выделите протокол TCP/IP и щелкните кнопку Свойства (Properties). Убедитесь, что параметры TCP/IP позволяют подключиться к домену Active Directory. О настройке TCP/IP см. главу 16.
9. На вкладке Идентификация (Identification) проверьте сведения об имени компьютера и рабочей группе. Имя компьютера и рабочая группа должны быть заданы, как описано в главе 16.

10. Если вы изменили параметры, компьютер, возможно, придется перезагрузить. После перезагрузки войдите в систему по учетной записи с правами доступа в домен Active Directory. Вы должны получить доступ к ресурсам домена.

Примечание Системы Windows 9x в роли клиентов не имеют учетных записей компьютеров и не отображаются в окне Сетевое окружение (Network Neighborhood), но вы можете просмотреть информацию об их сеансе связи. Запустите консоль Управление компьютером (Computer Management), раскройте узлы Служебные программы (System Tools), Общие папки (Shared Folders) и выберите Сеансы (Sessions) — отобразятся текущие сеансы связи пользователей и компьютеров. Об общих ресурсах рассказано в главе 14.

Использование доменов Windows NT и Windows 2000 с Active Directory

Прежде чем компьютер с Windows NT и Windows 2000 станет частью домена, для него следует завести учетную запись. Поддержка доменов Windows NT и Windows 2000 возможна в нескольких функциональных режимах Active Directory.

- **Смешанный** режим Windows 2000 (mixed mode) — поддерживает домены Windows Server 2003, Windows 2000 и Windows NT. Доменам, работающим в этом режиме, недоступны многие функции Active Directory, например универсальные группы, вложение групп, преобразование типов групп, простое переименование контроллера домена, штампы времени входа в систему и номера версий ключей центра распределения ключей Kerberos.
- Основной режим Windows 2000 (native mode) — поддерживает только домены Windows Server 2003 и Windows 2000. Домены Windows NT не поддерживаются. Домены, работающие в этом режиме, не могут использовать простое переименование контроллера домена, штампы времени входа в систему и номера версий ключей центра распределения ключей Kerberos.
- **Промежуточный режим Windows Server 2003 (interim mode)** — поддерживает только домены Windows Server 2003 и Windows NT. Домены Windows 2000 не поддерживаются. Этот режим позволяет обновить домен Windows NT сразу до домена Windows Server 2003, минуя промежуточную стадию Win-

dows 2000. Он аналогичен смешанному режиму Windows 2000, но поддерживает только серверы с Windows NT и Windows Server 2003.

- Режим Windows Server 2003 — поддерживает только домены Windows Server 2003. Домены Windows NT и Windows 2000 не поддерживаются. Домену в режиме Windows Server 2003 доступны все функции Active Directory.

Смешанный режим Windows 2000

Функциональный режим домена Windows Server 2C03 задастся при установке Active Directory на первый контроллер в данном домене. Если в этом домене используются системы Windows NT 4.0 Server, Windows 2000 Server и Windows Server 2003, вам необходим смешанный режим работы (по крайней мере на начальном этапе).

В этом режиме компьютеры, настроенные на работу в домене Windows NT, получают доступ к сети, как если бы они по-прежнему работали в домене Windows NT. Это могут быть компьютеры с Windows *9x*, на которых не запущен клиент Active Directory, рабочие станции и серверы Windows NT. Роль рабочих станций Windows NT неизменна, а вот серверы Windows NT воспринимаются несколько иначе: они способны действовать лишь как резервные контроллеры домена (backup domain controller, BDC) или рядовые серверы. Основного контроллера с Windows NT в домене быть не может. Домен Windows NT подчиняется контроллеру Windows Server 2003, который играет роль контроллера PDC для репликации на резервные контроллеры данных службы каталогов Active Directory (на резервных контроллерах они окажутся доступными только для чтения) и для синхронизации изменений параметров безопасности.

Контроллер домена Windows Server 2003, действующий в качестве контроллера PDC, конфигурируется как хозяин операций эмулятора PDC. Вы можете в любой момент назначить эту роль другому контроллеру домена Windows Server 2003. Контроллер, действующий как эмулятор PDC, поддерживает два протокола аутентификации;

- **Kerberos** — стандартный Интернет-протокол для аутентификации пользователей и систем; главный механизм аутентификации в доменах Windows Server 2003;

- **диспетчер** локальной **сети NT (NT Local Area Network** Manager, **NTLM)** — главный протокол аутентификации Windows NT; используется для аутентификации компьютеров в домене Windows NT.

Перевод домена в основной режим Windows 2000

Обновив PDC и другие системы Windows NT до Windows 2000, можно сменить рабочий режим на основной и задействовать в домене только ресурсы Windows 2000 и Windows Server 2003. Однако, перейдя в основной режим Windows 2000, вы уже не сможете вернуться к смешанному. Поэтому переходите на основной режим, только если вы уверены, что вам не понадобятся прежняя структура домена Windows NT или резервные контроллеры домена Windows NT.

После перехода на основной режим Windows 2000 вы обнаружите, что:

- репликация NTLM более не поддерживается;
- эмулятор PDC более не способен синхронизировать данные с резервными контроллерами Windows NT (если они имеются);
- вы не можете добавлять в этот домен контроллеры Windows NT

Промежуточный режим Windows Server 2003

Если вы обновляете домен Windows NT до Windows Server 2003, вам не нужно прибегать к смешанному режиму. Воспользуйтесь вместо этого промежуточным режимом Windows Server 2003, который доступен только при первом обновлении контроллера домена Windows NT до Windows Server 2003. Запустите обновление PDC Windows NT 4.0. В ходе его выполнения вам будет предложено выбрать функциональный режим леса: укажите промежуточный режим Windows Server 2003. Работа домена в промежуточном режиме Windows Server 2003 очень похожа на работу в смешанном режиме Windows 2000. Единственное исключение — не поддерживаются контроллеры домена Windows 2000.

После обновления PDC вы сможете обновить оставшиеся резервные контроллеры. Microsoft рекомендует настроить автономный резервный контроллер домена (backup BDC offline), чтобы переключаться на него в случае неполадок. Убедившись в том, что псе работает нормально, повысьте функциональный режим домена и леса, чтобы в полной мере использовать преимущества новых функций Active Directory.

Режим Windows Server 2003

Обновив домены Windows NT, стоит перейти к обновлению контроллеров доменов Windows 2000 до контроллеров доменов Windows Server 2003. Затем при желании измените режим, чтобы поддерживать только домены Windows Server 2003.

Прежде чем вы сможете обновить контроллеры домена Windows 2000, вам будет предложено подготовить домен к работе с Windows Server 2003. Для этого потребуется обновить лес домена и его схему, чтобы они стали совместимыми с доменами Windows Server 2003. Для автоматического обновления предусмотрена программа Adprep.exe. Запустите ее на *хозяине операций схемы* (schema operations master), а затем на *хозяине операций инфраструктуры* (infrastructure operations master) для каждого домена леса. Как всегда, предварительно проверьте процедуру в лабораторных условиях.

Вот как выполнить обновление.

1. Проверьте возможность обновления на хозяине операций схемы и на хозяине операций инфраструктуры для каждого домена леса. Вставив в дисковод компакт-диск Windows Server 2003, щелкните Пуск (Start) и затем Выполнить (Run). В поле Открыть (Open) введите **E:\i386\winnt32.exe** /checkupgradeonly, где E — дисковод для компакт-дисков, и щелкните OK. Запустится программа Консультант по обновлению Microsoft Windows (Microsoft Windows Upgrade Advisor). Выберите Пропустить этот шаг (No, skip this step) и щелкните Далее (Next). Программа-консультант проведет анализ оборудования системы и определит возможность обновления до Windows Server 2003. Если обнаружены несоответствия, устраните их, прежде чем продолжить обновление.
2. Все контроллеры доменов Windows 2000 в лесу должны предварительно пройти обновление до пакета обновления Service Pack 2 или более позднего. Чтобы проверить текущую версию сервисного пакета, в Панели управления (Control Panel) дважды щелкните Система (System). Сведения об установленном пакете обновления находятся на вкладке Общие (General).
3. Войдите в систему с компьютера — хозяина операций схемы для первого домена леса, который вы хотите обновить, и вставьте в дисковод компакт-диск Windows Server 2003. Щелкните Пуск (Start) и затем Выполнить (Run). В поле Открыть (Open) введите **E:\i386\adprep.exe /forestprep**, где

E — дисковод *для* компакт-дисков, и щелкните OK. Внимательно прочитайте инструкции и нажмите C, чтобы продолжить, или любую другую букву, чтобы закрыть окно.

Примечание Чтобы определить, какой именно сервер является в данное время хозяином операций схемы в домене, введите в командной строке **dsquery server -hasfsmo schema.** Программа выведет строку пути службы каталогов с указанием имени сервера, например: «CN=CORPSERVER01 ,CN=Servers, CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=microsoft,DC=com». Из этой строки можно определить, что хозяин операций схемы — это CORPSERVER01 в домене microsoft.com.

4. Войдите в систему с компьютера — хозяина операций инфраструктуры для первого домена леса, который вы хотите обновить, и вставьте в дисковод компакт-диск Windows Server 2003. Щелкните Пуск (Start) и затем Выполнить (Run). В поле Открыть (Open) введите E:\i386\adprep.exe **/domainprep**, где E — дисковод для компакт-дисков, и щелкните OK. Внимательно прочитайте инструкции и нажмите C, чтобы продолжить, или любую другую букву, чтобы закрыть окно.

Примечание Чтобы определить, какой именно сервер является в данное время хозяином операций инфраструктуры, введите в командной строке **dsquery server -hasfsmo** infr.

5. При необходимости повторите действия 3 и 4 для других доменов в лесу.

После обновления всех контроллеров доменов Windows NT и Windows 2000 и рядовых серверов вы можете повысить функциональный режим доменов и леса, чтобы получить возможность использовать все новые функции Active Directory. Однако в этом случае вам будут доступны только ресурсы домена Windows Server 2003. Кроме того, перейдя в режим Windows Server 2003 для домена или леса, вы не сможете вернуться к любому другому режиму. Поэтому используйте режим Windows Server 2003, лишь если уверены, что нам не понадобятся старый домен Windows NT, резервные контроллеры домена Windows NT или домен Windows 2000.

Повышение функционального режима домена и леса

Домены, работающие в режиме Windows Server 2003, могут использовать самые современные функциональные возможности

доменов Active Directory, в том числе универсальные группы, вложенность групп, преобразование типов групп, штампы времени входа в систему и номера версий ключей центра распределении ключей Kerberos. Кроме того, в этом режиме администратор имеет возможность:

- переименовать контроллеры домена без предварительного понижения;
- переименовать домены,работающие под управлением контроллеров Windows Server 2003;
- создавать расширенные двухсторонние доверительные отношения между двумя лесами;
- изменять структуру доменной иерархии,переименовывая домены и перемещая их по уровням;
- пользоваться расширенными возможностями репликации для отдельных членов группы и глобальных каталогов.

Лесам доменов, работающим в режиме Windows Server 2003, доступны все последние *усовершенствования* лесов Active Directory, а именно: усовершенствованная репликация глобальных каталогов, более эффективная репликация в пределах одного сайта и между различными сайтами, а также возможность устанавливать односторонние, двухсторонние и транзитивные доверительные отношения.

Примечание Процесс обновления доменов и леса генерирует большой объем сетевого трафика, так как информация реплицируется по сети. В некоторых случаях для завершения процесса обновления требуется 15 минут и больше. В течение этого времени наблюдается замедление отклика при обмене с серверами и увеличение задержки при работе с сетью. Поэтому процесс обновления рекомендуется выполнять в нерабочее время, Полезно также предварительно провести всестороннюю проверку на совместимость с существующими приложениями (особенно с теми, которые не поддерживают Windows Server 2003), прежде чем выполнять обновление.

Нот как повысить функциональный режим домена.

1. Откройте консоль Active Directory — домены и доверие (Active Directory Domains and Trusts).
2. В дереве консоли щелкните правой кнопкой домен, с которым хотите работать, и выберите Изменение режима работы доме-

па (Raise Domain Functional Level). В одноименном диалоговом окне появится имя текущего домена.

3. Выберите в списке новый режим и щелкните Изменить (Raise). Имейте в виду, что это необратимое действие. Прежде чем выполнить его, тщательно обдумайте возможные последствия.
4. Щелкните OK. Новый режим будет реплицирован на все контроллеры в этом домене. В большой сети на это требуется немало времени.

Вот как повысить уровень функциональности леса.

1. Откройте консоль Active Directory — домены и доверие (Active Directory Domains and Trusts).
2. В дереве консоли щелкните правой кнопкой узел Active Directory — домены и доверие (Active Directory Domains and Trusts) и выберите Изменение режима работы леса (Raise Forest Functional Level). В одноименном диалоговом окне появится имя текущего леса.
3. Выберите в списке новый режим и щелкните Изменить (Raise). Имейте в виду, что это необратимое действие. Прежде чем выполнить его, тщательно обдумайте возможные последствия.
4. Щелкните OK. Новый режим леса будет реплицирован на все контроллеры всех доменов в этом лесу. В большой сети на это может потребоваться значительное время.

Структура каталога

Данные каталога предоставляются пользователям и компьютерам через *хранилища данных* (data stores) и *глобальные каталоги* (global catalogs). Хотя большинство функций Active Directory затрагивают хранилище данных, глобальные каталоги (ГК) не менее важны, поскольку используются для входа в систему и поиска информации. Больше того, если ГК недоступен, обычные пользователи не смогут войти в домен. Единственный способ обойти это условие — локальное кэширование членства *к* универсальных группах. У него есть свои достоинства и недостатки, но об этом чуть позже.

Доступ и распространение данных Active Directory обеспечиваются средствами *протоколов доступа к каталогу* (directory access protocols) и *репликации* (replication). Протоколы позволя-

ют клиентам связываться с компьютерами, на которых работает Active Directory. Репликация нужна для распространения обновленных данных на контроллеры. Главный метод распространения обновлений — репликация с несколькими хозяевами, но некоторые изменения обрабатываются только специализированными контроллерами — *хозяевами операций* (operations masters).

Способ выполнения репликации с несколькими хозяевами в Windows Server 2003 также изменился благодаря появлению *разделов каталога приложений* (application directory partitions). Посредством их системные администраторы, входящие в группу администраторов предприятия, могут создавать в лесу доменов разделы репликации, которые представляют собой логические структуры, используемые для управления репликацией в пределах леса доменов. Например, вы вправе создать раздел, который будет ведать репликацией информации DNS в пределах домена. Другим системам домена репликация информации DNS запрещена.

Разделы каталога приложений могут быть дочерним элементом домена, дочерним элементом другого прикладного раздела или новым деревом в лесу доменов. Реплики разделов разрешается размещать на любом контроллере домена Active Directory, включая глобальные каталоги. Хотя разделы каталога приложений полезны в больших доменах и лесах, они увеличивают издержки на планирование, администрирование и сопровождение.

Хранилище данных

Хранилище содержит сведения о важнейших объектах службы каталогов Active Directory — учетных записях, общих ресурсах, ОП и групповых политиках. Собственно, иногда хранилище данных и называют просто *каталогом* (directory). На контроллере домена каталог хранится в файле NTDS.DIT, расположение которого определяется при установке Active Directory (это обязательно должен быть диск NTFS). Некоторые данные каталога можно хранить и отдельно от основного хранилища, например групповые политики, сценарии и другую информацию, записанную в общем системном ресурсе SYSVOL.

Предоставление информации каталога в совместное пользование называют *публикацией* (publish). Например, открывая принтер для использования в сети, вы его публикуете; публикуется информация об общей папке и т. п.

Контроллеры доменов реплицируют большинство изменений в хранилище но схеме с несколькими хозяевами. Администратор небольшой или среднего размера организации редко управляет репликацией хранилища, поскольку она осуществляется автоматически, но вы имеете право настроить ее согласно специфике сетевой архитектуры.

Реплицируются не все данные каталога, а только:

- данные домена — информация об объектах в домене, включая объекты учетных записей, общих ресурсов, ОП и групповых политик;
- данные конфигурации —сведения о топологии каталога: список всех доменов, деревьев и лесов, а также местоположения контроллеров и серверов ГК;
- данные схемы — информация обо всех объектах и типах данных, которые могут храниться в каталоге; стандартная схема Windows Server 2003 описывает объекты учетных записей, объекты общих ресурсов и др.: вы вправе расширить ее, определив новые объекты и атрибуты или добавив атрибуты для существующих объектов.

Глобальный каталог

Если локальное кэширование членства *в* универсальных группах не производится, вход в сеть осуществляется на основе информации о членстве в универсальной группе, предоставленной ГК. Он также обеспечивает поиск в каталоге по всем доменам леса. Контроллер, выполняющий роль сервера ГК, хранит полную реплику всех объектов каталога своего домена и частичную реплику объектов остальных доменов леса.

Примечание Для входа в систему и поиска нужны лишь некоторые свойства объектов, поэтому возможно использование частичных реплик. Для формирования частичной реплики при репликации нужно передать меньше данных, что снижает сетевой трафик.

По умолчанию сервером ГК становится первый контроллер домена. Поэтому, если в домене только один контроллер, то сервер ГК и контроллер домена — один и тот же сервер. Вы также вправе расположить ГК на другом контроллере, чтобы сократить время ожидания ответа при входе в систему и ускорить поиск. Рекомендуется создать по одному ГК в каждом сайте домена.

Контроллеры, хранящие ГК, должны иметь скоростную связь с контроллерами — хозяевами инфраструктуры, Хозяин инфраструктуры — одна из пяти ролей хозяина операций, которую можно назначить контроллеру домена. В домене хозяин инфраструктуры отвечает за обновление ссылок объектов. Он сравнивает свои данные с данными ГК, находит устаревшие ссылки и запрашивает обновленные сведения из ГК. Затем он реплицирует изменения на остальные контроллеры в домене. О ролях хозяина операций рассказано в разделе «Роли хозяина операций».

Если в домене только один контроллер, вы можете назначить роль хозяина инфраструктуры и ГК одному контроллеру домена. По если в домене два или более контроллеров, ГК и хозяин инфраструктуры должны быть на разных контроллерах. Иначе хозяин инфраструктуры не найдет устаревших данных и в итоге никогда не реплицирует изменения. Единственное исключение — когда ГК хранится па всех контроллерах домена. Тогда не важно, какой из них — хозяин инфраструктуры. Несколько ГК в домене нужны, главным образом, чтобы гарантировать, что каталог всегда доступен для обслуживания входа в сеть и запросов поиска.

Поиск в ГК очень эффективен, поскольку ГК содержит информацию об объектах во всех доменах леса. Это позволяет обслуживать запросы на поиск в локальном домене, а не обращаться в домен в другой части сети. Локальное разрешение запросов снижает нагрузку на сеть и обычно ускоряет ответ.

Внимание! Если вход в систему замедлился или пользователи долго ждут ответа на запрос, создайте дополнительные ГК. Но помните, что большое количество ГК влечет передачу большего объема данных по сети.

Кэширование членства в универсальных группах

В крупной организации нерационально хранить ГК в каждом офисе. Однако в случае потери связи между удаленным офисом и офисом, в котором хранится ГК, возникнет проблема со входом в сеть: запросы на вход в систему должны направляться в ГК, а при отсутствии связи это невозможно. Если в данном офисе нет собственной копии ГК, обычные пользователи потеряют возможность входа в систему. Она останется только у администраторов домена.

Есть несколько способов решения этой проблемы. Разумеется, можно создать сервер ГК на одном из контроллеров домена в удаленном офисе (подробнее — в главе 7). Недостаток этого способа — увеличение нагрузки на сервер ГК, что может потребовать дополнительных ресурсов и тщательного планирования времени работы этого сервера.

Другой способ решения проблемы — локальное кэширование членства в универсальных группах. При этом любой контроллер домена может обслуживать запросы на вход в систему локально, не обращаясь к серверу ГК. Это ускоряет процедуру входа в систему и облегчает ситуацию в случае выхода сервера ГК из строя. Кроме того, при этом снижается трафик репликации. Вместо того чтобы периодически обновлять весь ГК по всей сети, достаточно обновлять информацию в кэше о членстве в универсальной группе. По умолчанию обновление происходит каждые восемь часов на каждом контроллере домена, в котором используется локальное кэширование членства в универсальной группе.

Членство *а* универсальной группе индивидуально для каждого сайта. Напомним, что сайт — это физическая структура, состоящая из одной или нескольких подсетей, имеющих индивидуальный набор IP-адресов и сетевую маску. Контроллеры домена **Windows** Server 2003 и ГК, к которому они обращаются, должны находиться в одном сайте. Если у вас имеется несколько сайтов, вам придется настроить локальное кэширование на каждом из них. Кроме того, пользователи, входящие в сайт, должны быть частью домена Windows Server 2003, работающего в режиме леса Windows Server 2003. Процедура настройки кэширования рассмотрена в главе 7.

Репликация и Active Directory

В каталоге хранятся сведения трех типов: данные домена, данные схемы и данные конфигурации. Данные домена реплицируются на все контроллеры отдельного домена. Схема и данные конфигурации реплицируются на все домены дерева или леса. Кроме того, все объекты индивидуального домена и часть свойств объектов леса реплицируются в ГК. Это означает, что контроллер домена хранит и реплицирует схему для дерева или леса, информацию о конфигурации для всех доменов дерева или леса и все объекты каталога и свойства для собственного домена.

Контроллер домена, на котором хранится ГК, содержит и реплицирует информацию схемы для леса, информацию о конфи-

гурации для всех доменов леса и ограниченный набор свойств для всех объектов каталога в лесу (он реплицируется только между серверами ГК), а также все объекты каталога и свойства для своего домена.

Чтобы понять суть репликации, рассмотрим такой сценарий настройки новой сети.

1. Вы устанавливаете в домене А первый контроллер. Этот сервер — единственный контроллер домена. Он же является и сервером ГК. Репликация в такой сети не происходит, поскольку нет других контроллеров.
2. Бы устанавливаете в домене А второй контроллер, и начинается репликация. Можно назначить один контроллер хозяином инфраструктуры, а другой — сервером ГК. Хозяин инфраструктуры следит за обновлениями ГК и запрашивает их для измененных объектов. Оба этих контроллера также реплицируют данные схемы и конфигурации.
3. Бы устанавливаете в домене А третий контроллер, на котором нет ГК. Хозяин инфраструктуры следит за обновлениями ГК, запрашивает их для измененных объектов, а затем реплицирует изменения на третий контроллер домена. Все три контроллера также реплицируют данные схемы и конфигурации.
4. Вы создаете новый домен Б и добавляете в него контроллеры. Серверы ГК в домене А и домене Б реплицируют все данные схемы и конфигурации, а также подмножество данных домена из каждого домена. Репликация в домене А продолжается, как описано выше, плюс начинается репликация внутри домена Б.

Active Directory и LDAP

Упрощенный протокол доступа к каталогам (Lightweight Directory Access Protocol, LDAP) — стандартный протокол Интернет-соединений в сетях TCP/IP. LDAP спроектирован специально для доступа к службам каталогов с минимальными издержками. В LDAP также определены операции, используемые для запроса и изменения информации каталога.

Клиенты Active Directory применяют LDAP для связи с компьютерами, на которых работает Active Directory, при каждом входе в сеть или поиске общих ресурсов. LDAP можно использовать и для управления Active Directory.

LDAP — открытый стандарт, предназначенный и для других служб каталога. Он упрощает взаимосвязь каталогов и переход на Active Directory с других служб каталогов. Для повышения совместимости используйте интерфейсы служб Active Directory (Active Directory Service Interfaces, ADSI). ADSI поддерживает стандартные API-интерфейсы для LDAP, совместимые с Интернет-стандартом RFC 1823. Для управления объектами Active Directory из сценариев интерфейс ADSI применяется совместно с сервером сценариев Windows (Windows Script Host, WSH).

Роли хозяина операций

Хозяин операций решает задачи, которые неудобно выполнять в модели репликации с несколькими хозяевами. Существует пять ролей хозяина операций — вы можете назначить их одному или нескольким контроллерам доменов. Одни роли должны быть уникальны на уровне леса, для других достаточно уровня домена. В каждом лесе Active Directory должны существовать следующие роли.

- Хозяин схемы (schema master) управляет обновлениями и изменениями схемы каталога. Для обновления схемы каталога вам необходим доступ к хозяину схемы. Чтобы определить, какой сервер в данное время является хозяином схемы в домене, откройте окно командной строки и введите dsquery server -hasfsmo schema.
- Хозяин именования доменов (domain naming master) управляет добавлением и удалением доменов в лесу. Чтобы добавить или удалить домен, вам требуется доступ к хозяину именования доменов. Чтобы определить, какой сервер в данное время является хозяином именования доменов, откройте окно командной строки и введите dsquery server -hasfsmo name.

Эти роли, общие для всего леса в целом, должны быть в нем уникальными. Иными словами, вы можете настроить только один хозяин схемы и один хозяин именования доменов для леса.

В каждом домене Active Directory в обязательном порядке существуют следующие роли.

- **Хозяин относительных идентификаторов (relative ID master)** выделяет относительные идентификаторы контроллерам доменов. Каждый раз при создании объекта пользователя, *группы* или компьютера контроллеры назначают объекту уникальный идентификатор безопасности, состоящий из идентифи-

катора безопасности домена и уникального идентификатора, который был выделен хозяином относительных идентификаторов. Чтобы определить, какой сервер в данное время является хозяином относительных идентификаторов в домене, откройте окно командной строки и введите **dsquery server -hasfsmo rid.**

- **Эмулятор PDC (PDC emulator)** в смешанном или промежуточном режиме домена действует как главный контроллер домена Windows NT. Он аутентифицирует вход в Windows NT, обрабатывает изменения пароля и реплицирует обновления на BDC. Чтобы определить, какой сервер в данное время является эмулятором PDC в домене, откройте окно командной строки и введите dsquery **server -hasfsmo pdc.**
- **Хозяин инфраструктуры (infrastructure** master) обновляет ссылки объектов, сравнивая данные своего каталога с данными ГК. Если данные устарели, он запрашивает из ГК обновления и реплицирует их на остальные контроллеры в домене. Чтобы определить, какой сервер в данное время является хозяином инфраструктуры в домене, откройте окно командной строки и введите **dsquery server -hasfsmo infr.**

Эти роли, общие для всего домена, должны быть в нем уникальными. Иными словами, вы можете настроить только один хозяин относительных идентификаторов, один эмулятор PDC и один хозяин инфраструктуры для каждого домена.

Обычно роли хозяина операций назначаются автоматически, но вы вправе их переназначить. При установке ноной сети все роли хозяев операций получает первый контроллер первого домена. Если вы позднее создаете новый дочерний домен или корневой домен в новом дереве, роли хозяина операций также автоматически назначаются первому контроллеру домена. В новом лесу доменов контроллеру домена назначаются все роли хозяина операций. Если новый домен создается в том же лесу, его контроллеру назначаются роли хозяина относительных идентификаторов, эмулятора PDC и хозяина инфраструктуры. Роли хозяина схемы и хозяина именования доменов остаются у первого домена леса.

Если в домене только один контроллер, он выполняет все роли хозяев операций. Если в вашей сети один сайт, стандартное расположение хозяев операций оптимально. Но по мере добавления контроллеров домена и доменов иногда требуется переместить роли хозяев операций на другие контроллеры доменов.

Если в домене два или более контроллеров, сконфигурируйте два контроллера домена для выполнения ролей хозяина операций. Например, назначьте один контроллер домена основным хозяином операций, а другой — запасным, который понадобится при отказе основного. Убедитесь, что контроллеры доменов — прямые партнеры по репликации и соединены скоростным каналом связи.

По мере роста структуры доменов можно разнести роли хозяина операций по отдельным контроллерам. Это ускорит отклик хозяев на запросы. Всегда тщательно планируйте ролевые обязанности будущего контроллера домена.

Примечание Две роли, которые не следует разбивать, — хозяин схемы и хозяин именования доменов. Всегда назначайте их одному серверу. Для наибольшей эффективности желательно, чтобы хозяин относительных идентификаторов и эмулятор PDC также находились на одном сервере, хотя при необходимости эти роли можно разделить. Так, в большой сети, где большие нагрузки снижают быстродействие, хозяин относительных идентификаторов и эмулятор PDC должны быть размещены на разных контроллерах. Кроме того, хозяин инфраструктуры не следует размещать на контроллере домена, хранящем ГК (см. раздел «Глобальный каталог»).

Глава 7

Основы администрирования Active Directory

Ежедневно с помощью службы Active Directory вам придется создавать учетные записи компьютеров, подключать их к домену и т. д. В этой главе вы изучите средства управления Active Directory и методы управления компьютерами, контроллерами домена и организационными подразделениями (ОП).

Средства управления службами Active Directory

Для управления Active Directory предназначены средства администрирования и поддержки.

Средства администрирования Active Directory

Перечисленные ниже инструменты реализованы в виде оснасток консоли MMC:

- **Active Directory — пользователи и компьютеры** (Active Directory Users and **Computers)** позволяет управлять пользователями, группами, компьютерами и организационными подразделениями (ОП);
- Active **Directory — домены и доверие (Active Directory Domains and** Trusts) служит для работы с доменами, деревьями доменов и лесами доменов;
- **Active Directory — сайты** и службы **(Active Directory Sites and Services)** позволяет управлять сайтами и подсетями;
- **Результирующая** политика **(Resultant Set of Policy)** используется для просмотра текущей политики пользователя или системы и для планирования изменений в политике.

В Microsoft Windows 2003 Server можно добавить соответствующие оснастки в любую настраиваемую консоль или по-

лучить доступ к ним напрямую из меню Администрирование (Administrative Tools). Если па вашем компьютере установлена другая версия Windows и есть доступ к домену Windows 2003, средства не будут доступны, пока вы их не установите. Подробнее об установке — в главе 1. Вы также можете создать пакет установки ПО для инструментов, которые будут распространяться и устанавливаться через Active Directory.

В Windows Server 2003 эти инструменты значительно усовершенствованы. Ниже перечислены возможности, которых в Windows 2000 не было. Теперь вы можете:

- выделять одновременно несколько ресурсов, по очереди щелкая их левой кнопкой при нажатой клавише Ctrl;
- выделять группу ресурсов, щелкая первый и последний ресурс группы при нажатой клавише Shift;
- **перетаскивать ресурсы в новые положения мышью;**
- **редактировать свойства нескольких ресурсов одновременно —** выделите нужную группу объектов и щелкните ее правой кнопкой мыши, а затем выберите в контекстном меню нужную команду.

Еще одно средство администрирования — оснастка Схема Active Directory (Active Directory Schema) — позволяет управлять и модифицировать схему каталога. Если вы загрузили пакет AdminPak, для добавления оснастки Схема Active Directory (Active Directory Schema) в консоль MMC нужно выполнить следующие действии.

1. Введите в командной строке **regsvr32 schmmgmt.dll**, чтобы зарегистрировать схему Active Directory.
2. Щелкните кнопку Пуск (Start) и выберите команду Выполнить (Run).
3. Введите mmc в поле Открыть (Open) и щелкните OK. Откроется пустая консоль MMC.
4. Выберите в меню Консоль (Console) команду Добавить или удалить оснастку (Add/Remove Snap-In). Откроется одноименное диалоговое окно.
5. Перейдите на вкладку Изолированная оснастка (Standalone) и щелкните Добавить (Add).
6. В диалоговом окне Добавить изолированную оснастку (Add Standalone Snap-In) выделите оснастку Схема Active

Directory (Active Directory Schema) и щелкните Добавить (Add).

7. Щелкните Закрыть (Close), а затем — OK.

Утилиты командной строки Active Directory

В этом разделе кратко описаны утилиты для управления Active Directory из командной строки. Для получения более подробной справочной информации о команде введите ее с переключателем «/?».

- DSADD — добавляет в Active Directory компьютеры, контакты, группы, ОП и пользователей. Для получения справочной информации введите **dsadd *<имя_объекта>*/?**, например dsadd **computer /?**.
- **DSGET** — отображает свойства компьютеров, контактов, групп, ОП, пользователей, сайтов, подсетей и серверов, зарегистрированных в Active Directory. Для получения справочной информации введите dsget *<имя_объекта>*/?, например dsget subnet */?*.
- DSMOD — изменяет свойства компьютеров, контактов, групп, ОП, пользователей и серверов, зарегистрированных в Active Directory. Для получения справочной информации введите **dsmod *<имя_объекта>*/?**, например dsmod server /?.
- **DSMOVE** — перемещает одиночный объект в новое расположение в пределах домена или переименовывает объект без перемещения.
- **DSQUERY** — осуществляет поиск компьютеров, контактов, групп, ОП, пользователей, сайтов, подсетей и серверов в Active Directory по заданным критериям.
- **DSRM** — удаляет объект из Active Directory.
- **NTDSUTIL** — позволяет просматривать информацию о сайте, домене или сервере, управлять *хозяевами операций* (operations masters) и обслуживать базу данных Active Directory.

Средства поддержки Active Directory

Вот несколько средств, которые помогут настроить, управлять и устранять неполадки Active Directory (табл. 7-1).

Таблица 7-1. Краткий перечень средств поддержки Active Directory

Средство поддержки	Имя исполняемого файла	Описание
Active Directory Administration Tool	Ldp.exe	Осуществляет в Active Directory операции по протоколу LDAP (Lightweight Directory Access Protocol)
Active Directory Replication Monitor	Replmon.exe	Управляет репликацией и отображает ее результаты в графическом интерфейсе
Directory Services Access Control Lists Utility	Dsacls.exe	Управляет списками управления доступом для объектов Active Directory
Distributed File System Utility	Dfsutil.exe	Управляет распределенной файловой системой (Distributed File System, DFS) и отображает сведения о ее работе
DNS Server Troubleshooting Tool	Dnscmd.exe	Управляет свойствами серверов, зон и записей ресурсов DNS
Move Tree	Movetree.exe	Перемещает объекты из одного домена в другой
Replication Diagnostics Tool	Repadmin.exe	Управляет репликацией и отображает ее результаты в окне командной строки
Security Descriptor Check Utility	Sdcheck.exe	Анализирует распространение, репликацию и наследование списков управления доступом
Security ID Checker	Sidwalker.exe	Задает списки управления доступом для объектов, в прошлом принадлежавших перемещенным, удаленным или потерянным учетным записям
Windows Domain Manager	Netdom.exe	Позволяет управлять доменами и доверительными отношениями из командной строки

Консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers)

Это главное средство администрирования Active Directory, которое используется для выполнения всех задач, связанных с пользователями, группами и компьютерами, а также для управления ОП.

Открытие консоли

Для запуска Active Directory — пользователи и компьютеры (Active Directory Users and Computers) выберите одноименную команду в меню Администрирование (Administrative Tools). Также можно добавить Active Directory — пользователи и компьютеры (Active Directory Users and Computers) как оснастку в любую настраиваемую консоль.

1. Б меню Файл (File) консоли MMC выберите команду Добавить или удалить оснастку (Add/Remove Snap-In). Откроется одноименное окно.
2. На вкладке Изолированная оснастка (Standalone) щелкните Добавить (Add).
3. В окне Добавить изолированную оснастку (Add Standalone Snap-In) выделите Active Directory — пользователи и компьютеры (Active Directory Users and Computers) и щелкните Добавить (Add).
4. Щелкните Закрыть (Close), а затем — OK.

Основы работы с консолью

По умолчанию консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers) работает с доменом, к которому относится ваш компьютер. Вы можете получить доступ к объектам компьютеров и пользователей в этом домене через дерево консоли (рис. 7-1) или подключиться к другому домену. Средства этой же консоли позволяют просматривать дополнительные параметры объектов и осуществлять их поиск.

Получив доступ к домену в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers), вы увидите стандартный набор папок:

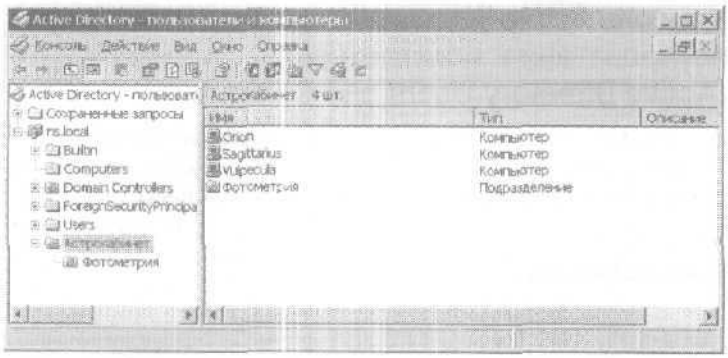


Рис. 7-1. Консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers)

- **Сохраненные запросы (Saved Queries)** — сохраненные критерии поиска, позволяющие оперативно повторить выполненный ранее поиск в Active Directory;
- **Builtin** — список встроенных учетных записей пользователей;
- **Computers** — контейнер по умолчанию для учетных записей компьютеров;
- **Domain Controllers** — контейнер по умолчанию для контроллеров домена;
- **ForeignSecurityPrincipals** — содержит информацию об объектах ил доверенного внешнего домена. Обычно эти объекты создаются при добавлении в группу текущего домена объекта из внешнего домена;
- **Users** — контейнер по умолчанию для пользователей.

Некоторые папки консоли по умолчанию не отображаются. Чтобы вывести их на экран, выберите в меню Вид (View) команду Дополнительные функции (Advanced Features). Вот эти дополнительные папки:

- **LostAndFound** — «осиротевшие», т. е. потерявшие владельца, объекты;
- **NTDS Quotas** — данные о квотировании службы каталогов;
- **Program Data** — сохраненные в Active Directory данные для приложений Microsoft;

- **System** — встроенные параметры системы.

Вы также можете добавить в дерево консоли папки для ОП.

Соединение с контроллером домена

Соединение с контроллером домена позволяет решать несколько задач. Если после запуска Active Directory — пользователи и компьютеры (Active Directory Users and Computers) вы не видите нужного объекта, следует связаться с контроллером другого домена, чтобы проверить, нет ли этого объекта там. Вы можете также связаться с контроллером домена, если подозреваете, что репликация выполняется неправильно. Подключившись, вы выявите несоответствия в недавно обновленных объектах.

Чтобы связаться с контроллером домена, выполните следующие действия.

1. В дереве консоли щелкните правой кнопкой элемент Active Directory — пользователи и компьютеры (Active Directory Users and Computers) и выберите команду Подключение к контроллеру домена (Connect to Domain Controller). Откроется одноименное окно (рис. 7-2).

Рис. 7-2. Выбор контроллера домена в окне Подключение к контроллеру домена (Connect to Domain Controller)

2. В списке Доступные контроллеры (Available Controllers) перечислены доступные контроллеры заданного домена. По умол-

чанию выбран вариант Любой контроллер домена с возможностью записи (Any writable domain controller). Если вы сохраните этот параметр, то свяжетесь с контроллером, который первым ответит на запрос. При необходимости выберите конкретный контроллер, с которым нужно связаться.

3. Щелкните OK.

Соединение с доменом

Если у вас есть соответствующие права доступа, в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) разрешается работать с любым доменом в лесу. Вот как связаться с доменом.

1. В дереве консоли щелкните правой кнопкой элемент Active Directory — пользователи и компьютеры (Active Directory Users and Computers) и выберите Подключение к домену (Connect to Domain).
2. В одноименном окне отображается текущий или принятый по умолчанию домен. Введите имя нового домена и щелкните OK или щелкните Обзор (Browse), а потом укажите домен в диалоговом окне.

Поиск учетных записей и общих ресурсов

В консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) предусмотрена встроенная функция поиска учетных записей, общих ресурсов и других объектов каталога в текущем или указанном домене или во всем каталоге.

1. В дереве консоли щелкните правой кнопкой текущий домен или конкретный контейнер, в котором хотите вести поиск, и выберите команду Найти (Find). Откроется окно Поиск (Find), подобное показанному на рис. 7-3.
2. Выберите в списке Найти (Find) нужный вариант:
   - Пользователи, контакты и группы (Users, Contacts, and Groups) — учетные записи пользователей и групп, а также контакты, перечисленные в службе каталогов;
   - Компьютеры (Computers) — учетные записи компьютеров, отсортированные по типу, имени и владельцу;
   - Принтеры (Printers) —принтеры, отсортированные по имени, модели и свойствам;

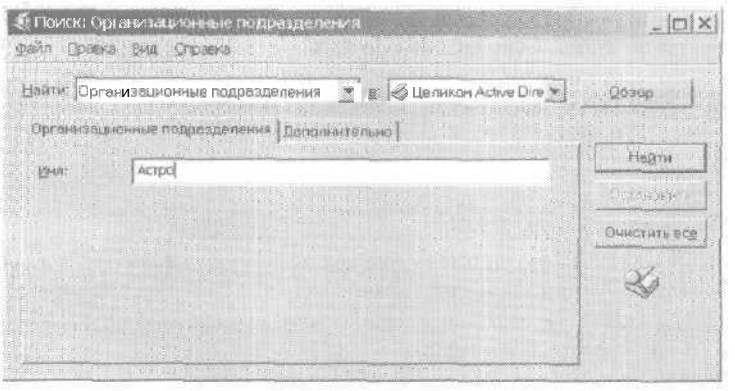


Рис. 7-3. Это диалоговое окно предназначено для поиска ресурсов в Active Directory

- **Общие папки (Shared Folders)** — общие папки, отсортированные по имени или ключевому слову;
- **Организационные подразделения (Organizational Units)** — ОП, отсортированные по имени;
- **Пользовательский поиск (Custom Search)** — углубленный поиск или запрос по протоколу LDAP;
- **Общие запросы (Common Queries)** — упрощенный поиск имен и описаний учетных записей, отключенных учетных записей, паролей с неограниченным сроком действия и др.

3. Задайте область поиска в списке В (In). Если вы до этого щелкнули правой кнопкой контейнер, например Computers, он будет выбран по умолчанию. Чтобы искать все объекты в каталоге, выберите в списке вариант Целиком Active Directory (Entire Directory).
4. Введя параметры поиска, щелкните Найти (Find Now). Все отвечающие условиями поиска разделы отображаются в нижней части окна (рис. 7-4). Дважды щелкните объект для просмотра или изменения его свойств. Щелкните объект правой кнопкой для отображения меню команд управления объектом.

Примечание Тип поиска определяет, какие поля и вкладки доступны в диалоговом окне Поиск (Find). Как правило, вы просто вводите имя искомого объекта в поле Имя (Name), но есть и другие параметры поиска. Например, вы можете ис-

кать цветной принтер, принтер, который может печатать на обеих сторонах листа, и т. п.

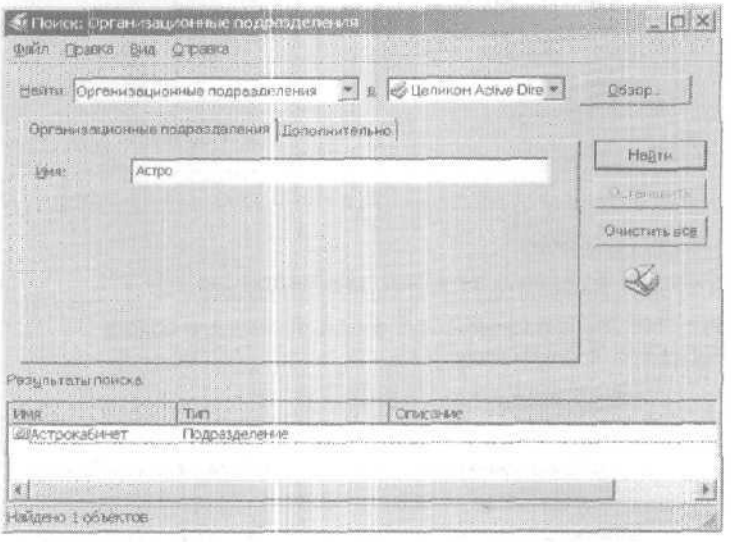


Рис. 7-4. Отвечающие условиями поиска объекты отображаются в нижней части окна

Управление учетными записями компьютеров

Учетные записи компьютеров хранятся как объекты Active Directory и используются для управления доступом к сети и ее ресурсам. Вы можете добавлять учетные записи компьютеров в любой контейнер консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers). Лучше всего использовать контейнеры Computers, Domain Controllers и любые созданные вами ОП.

Примечание Компьютеры с Windows 9*x* получают доступ к сети как клиенты Active Directory, но у них нет учетных записей компьютера. Подробнее о получении доступа к доменам Active Directory — в главе 6.

Создание учетных записей компьютера на рабочей станции или сервере

Простейший способ создать учетную запись для данного компьютера — зарегистрироваться на нем и присоединиться к домену, как описано в разделе «Присоединение компьютера к домену или рабочей группе» этой главы. Когда вы это сделаете, нужная учетная запись компьютера автоматически создается и помещается в папку Computers или Domain Controllers. Можно также создавать учетные записи компьютеров непосредственно в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers).

Создание учетной записи компьютера

Вот как создать учетную запись компьютера с помощью консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers).

1. В дереве консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) щелкните правой кнопкой контейнер, в котором хотите разместить учетную запись компьютера.
2. Щелкните Создать (New), а потом — Компьютер (Computer). Будет запущен мастер Новый объект - компьютер (New Object — Computer), первое окно которого показано на рис. 7-5. Введите имя клиентского компьютера.

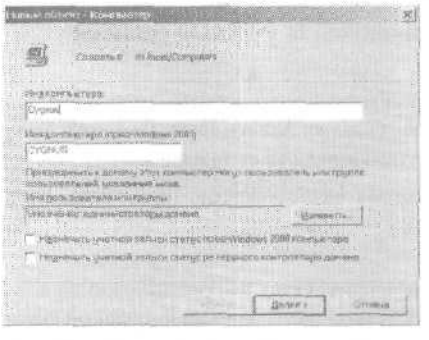


Рис. 7-5. Создание новой учетной записи компьютера

3. По умолчанию присоединять компьютеры к домену вправе только члены группы Администраторы домена (Domain Admins). Чтобы разрешить это другим пользователям или груп-

пам, щелкните Изменить (Change) и укажите их учетные записи.

Примечание Вы можете выбрать любую существующую учетную запись пользователя или группы. Это позволяет делегировать полномочия на присоединение учетной записи компьютера к домену.

4. Если с этой учетной записью будут работать системы Windows NT, установите флажок Назначить учетной записи статус пред-Windows 2000 компьютера (Assign this computer account as a pre-Windows 2000 computer).
5. Два раза щелкните Далее (Next), а потом — Готово (Finish),

Просмотр и редактирование свойств учетной записи компьютера

1. Запустите Active Directory — пользователи и компьютеры (Active Directory Users and Computers).
2. В дереве консоли раскройте узел домена, щелкнув значок «плюс» (+) рядом с его именем.
3. Найдите контейнер или ОП, в котором расположена учетная запись компьютера.
4. Щелкните правой кнопкой нужную учетную запись и выберите Свойства (Properties).

Удаление, отключение и включение учетных записей компьютера

Если вам больше не нужна учетная запись какого-то компьютера, вы можете навсегда удалить ее из Active Directory или временно отключить, чтобы активизировать ее позднее.

1. В меню Администрирование (Administrative Tools) выберите команду Active Directory — пользователи и компьютеры (Active Directory Users and Computers).
2. В дереве консоли щелкните контейнер, где расположена учетная запись компьютеру. Затем щелкните правой кнопкой саму запись компьютера.
3. Выберите одну из команд контекстного меню:
   - Удалить (Delete), чтобы навсегда удалить учетную запись;

- **Отключить учетную запись (Disable Account),** чтобы временно отключить учетную запись (отключенные записи отмечены красным крестиком);
- **Включить учетную запись (Enable Account),** чтобы разрешить вновь использовать выключенную учетную запись.

Внимание! Отключить используемую учетную запись невозможно. Следует предварительно выключить компьютер или прервать рабочий сеанс средствами папки Сеансы (Sessions) консоли Управление компьютером (Computer Management).

Сброс заблокированных учетных записей компьютера

У учетных записей компьютеров, как и у учетных записей пользователей, есть пароли. Разница в том, что работа с компьютерными паролями полностью автоматизирована. Каждой учетной записи компьютера назначен простой пароль и пароль закрытого ключа, необходимый для безопасной связи с контроллерами домена. Оба пароля по умолчанию меняются каждые 30 дней и должны быть синхронизированы. Без синхронизации компьютеру не удастся зарегистрироваться в домене. Если это рассинхронизация же случилась, сбросьте учетную запись компьютера, выполнив следующие действия.

1. В меню Администрирование (Administrative Tools) выберите Active Directory — пользователи и компьютеры (Active Directory Users and Computers).
2. В дереве консоли щелкните контейнер, где расположена учетная запись компьютера. Затем щелкните правой кнопкой саму запись.
3. Выберите Переустановить учетную запись (Reset Account). Если операция удалась, вы увидите окно подтверждения. Щелкните OK.

Перемещение учетных записей компьютера

Учетные записи компьютера обычно хранятся в контейнерах Computers, Domain Controllers или в созданных вами ОП. Чтобы переместить учетную запись в другой контейнер, в Windows Server 2003 вы можете просто перетащить ее мышью. Если этот способ вам почему-либо не подходит, выполните следующие действия.

1. В меню Администрирование (Administrative Tools) выберите Active Directory — пользователи и компьютеры (Active Directory Users and Computers).
2. В дереве консоли щелкните контейнер, где расположена учетная запись.
3. Щелкните правой кнопкой учетную запись компьютера, которую хотите переместить, и выберите Переместить (Move). Откроется одноименное окно (рис. 7-6).
4. Щелкните узел домена, а затем — контейнер, куда хотите переместить компьютер. Щелкните OK.

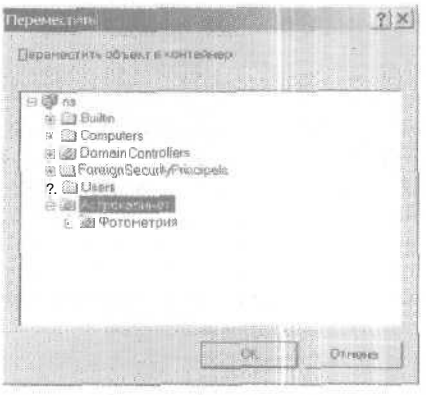


Рис. 7-6. Это диалоговое окно предназначено для перемещения учетных записей компьютеров в контейнеры

Управление компьютерами

Из консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) вы можете открыть консоль Управление компьютером (Computer Management) для нужного компьютера, щелкнув правой кнопкой его учетную запись и выбрав команду Управление (Manage).

Присоединение компьютера к домену или рабочей группе

Эта операция позволяет компьютерам с Windows NT/2000/XP и Windows Server 2003 входить в сеть и получать доступ к домену. Компьютеры с Windows 95/98 не нуждаются в учетных записях компьютера и не присоединяются к сети этим методом, а настраиваются как клиенты Active Directory. Подробности — в главе 6.

Сначала убедитесь, что на компьютере корректно установлены сетевые компоненты. Это, как правило, происходит одновременно с ОС (о настройке TCP/IP-соединений — в главе 16). Если службы DHCP, WINS и DNS правильно установлены в сети, рабочим станциям не потребуются постоянные IP-адреса или специальная настройка. Единственные обязательные параметры — имя компьютера и имя домена, которые вы можете задать непосредственно в процессе присоединения к домену.

Совет В Windows Server 2003 право добавлять рабочие станции в домен автоматически предоставлено всем пользователям, зарегистрировавшимся в домене. Однако в цепях защиты информации количество рабочих станций, которые данный пользователь может добавить в домен, ограничено десятью. Это значение можно изменить посредством утилиты Ldp.exe из набора инструментов поддержки Windows Server 2003 (атрибут ms-DS-MachineAccountQuota), но с точки зрения безопасности делать этого не следует. Надежнее создавать нужные учетные записи компьютеров заранее или назначить избранным пользователям специальное разрешение на создание объектов-компьютеров.

Сетевое соединение для компьютера скорее всего уже было настроено но время установки ОС. Также вы могли ранее присоединить компьютер к домену или рабочей группе. Если так, вам удастся присоединить компьютер к новому домену или рабочей группе (последовательность действий в Windows 2000 Professional, Windows 2000 Server, Windows XP Professional и Windows Server 2003 практически одна и та же).

1. Войдите в систему на рабочей станции или сервере, который хотите сконфигурировать.
2. Откройте панельуправления и дважды щелкните значок Система (System). В окне свойств системы перейдите на вкладку Имя компьютера (ComputerName), показанную на рис. 7-7.
3. Щелкните кнопку Изменить (Change).
4. Чтобы переименовать компьютер, введите новое имя в поле Имя компьютера (Computer Name), например **Zeta**.
5. Чтобы присоединиться к новому домену, в области Является членом (Member of) выберите вариант Домена (Domain) и введите локальную часть имени домена, например Seattle для домена seattle.microsoft.com.

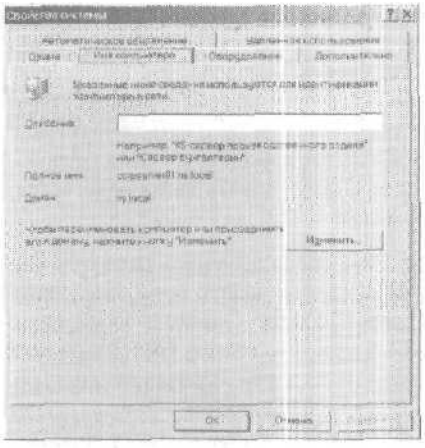


Рис. 7-7. Изменение сетевой идентификации компьютера

6. Чтобы присоединиться к новой рабочей группе, в области Является членом (Member of) выберите Рабочей группы (Workgroup) и введите имя группы, например **TestDevGroup**.
7. Закончив внесение изменений, щелкните OK. В ответ на запрос введите имя и пароль учетной записи администратора, имеющего полномочия на такие коррективы. Снова щелкните OK.
8. Если изменения успешны, вы увидите на экране окно подтверждения. Щелкните OK, чтобы перезагрузить компьютер.
9. Если изменения не удались, вы увидите сообщение об ошибке, например, что учетная запись уже используется. Последнее означает, что вы изменяете имя компьютера, уже подключенного к домену и имеющего в этом домене активные сеансы. Закройте приложения, которые могут соединяться с доменом, например Проводник (Windows Explorer), подключенный к общей папке в сети, и повторите процесс.

Управление контроллерами домена, ролями и каталогами

Контроллеры доменов выполняют важные задачи в доменах Active Directory. Многие из этих задач обсуждались в главе 6.

Установка и понижение контроллеров домена

Чтобы создать контроллер домена, нужно установить Active Directory на рядовом сервере. Если затем вы решите, что сервер больше не должен выполнять задачи контроллера, его можно понизить обратно до уровня рядового сервера. Операции установки Active Directory и понижения контроллера схожи. Перед выполнением этих задач проанализируйте их влияние на сеть и освежите и памяти главу 6.

Как вы помните, когда вы устанавливаете контроллер домена, требуется передать роли хозяина операций и переконфигурировать структуру глобального каталога. Кроме того, перед установкой Active Directory в сети должна работать DNS, а целевой жесткий диск — иметь формат NTFS 5.0 или более поздний. О преобразовании дисковых форматов рассказано в главе 11. Перед понижением контроллера нужно передать все его ключевые обязанности другим контроллерам домена, т. е. при необходимости переместить глобальный каталог с сервера и передать все его роли хозяина операций.

Примечание В Windows Server 2003 допускается переименование контроллера домена без понижения до рядового сервера. Единственная возможная проблема в том, что во время переименования сервер недоступен пользователям. Не исключено, что вам придется вручную обновить каталог, чтобы восстановить соединения с сервером. Переместить контроллер домена в другой домен нельзя. Сначала его придется понизить.

Вот как установить или понизить контроллер домена.

1. Войдите на сервер, который хотите настроить.
2. В меню Пуск (Start) выберите команду Выполнить (Run).
3. Наберите **dcpromo** и щелкните OK. Запустится мастер установки Active Directory.
4. Если компьютер — рядовой сервер, то запускается мастер установки службы каталогов Active Directory. Вам нужно указать, будет ли это контроллер нового домена или дополнительный контроллер существующего домена.
5. Если компьютер — контроллер домена, тот же мастер понизит его до рядового сервера.

Примечание В Windows Server 2003 появилась возможность установки контроллера домена с резервного носителя. На одном

из контроллеров домена создайте резервную копию состояния системы (System State) и восстановите ее на другом сервере под управлением Windows Server 2003. При этом вы избавляетесь от необходимости реплицировать базу данных каталога по сети — немаловажное преимущество, если в базе данных тысячи записей, а у сети невысокая пропускная способность.

Просмотр и передача доменных ролей

Консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers) позволяет просмотреть или изменить расположение доменных ролей хозяина операций. На уровне домена вы можете работать с ролями хозяина относительных идентификаторов (Relative ID, RID), эмулятора PDC и хозяина инфраструктуры.

Примечание О роли хозяина операций рассказано в главе 6. Для настройки роли хозяина именования служит консоль Active Directory — домены и доверие (Active Directory Domains and Trusts), а для изменения роли хозяина схемы — Схема Active Directory (Active Directory Schema).

Вот как передать роль хозяина операций.

1. В дереве консоли щелкните правой кнопкой элемент Active Directory — пользователи и компьютеры (Active Directory Users and Computers) и выберите Хозяева операций (Operations Masters). Откроется окно, показанное на рис. 7-8.

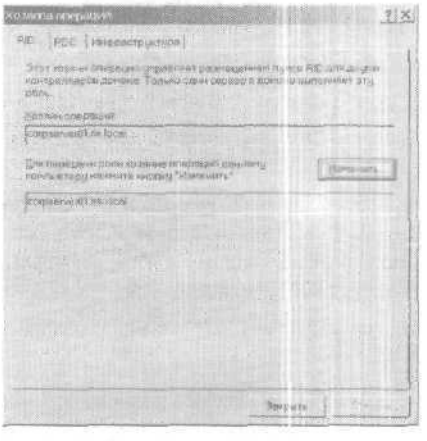


Рис. 7-8. Это диалоговое окно позволяет передавать роль хозяев операций

2. На вкладке RID показано местоположение текущего хозяина относительных идентификаторов. Щелкните Изменить (Change) и выберите новый контроллер домена для передачи роли.
3. На вкладке PDC показано местоположение текущего эмулятора PDC. Щелкните Изменить (Change) и выберите новый контроллер домена для передачи роли.
4. На вкладке Инфраструктура (Infrastructure) показано местоположение текущего хозяина инфраструктуры. Щелкните Изменить (Change) и выберите новый контроллер домена для передачи роли. Щелкните OK.

Просмотр и передача роли хозяина именования домена

Консоль Active Directory — домены и доверие (Active Directory Domains and Trusts) позволяет просмотреть или изменить расположение хозяина именования домена в лесу. В ней корневой уровень дерева консоли соответствует выбранному домену.

Вот как передать роль хозяина именования домена.

1. Откройте консоль Active Directory — домены и доверие (Active Directory Domains and Trusts).
2. В дереве консоли щелкните правой кнопкой элемент Active Directory — домены и доверие (Active Directory Domains and Trusts) и выберите Хозяин операций (Operations Master). Откроется окно Изменение хозяина операций (Change Operations Master).
3. В поле Хозяин именования доменов (Domain Naming Operations Master) отображается текущий хозяин именования домена. Щелкните Изменить (Change), а затем укажите новый контроллер. Роль будет передана этому контроллеру.
4. Щелкните Закрыть (Close).

Просмотр и передача роли хозяина схемы

Консоль Схема Active Directory (Active Directory Schema) позволяет просмотреть или изменить расположение хозяина схемы. Делается это так.

1. Добавьте оснастку Схема Active Directory (Active Directory Schema) в консоль MMC.
2. В дереве консоли щелкните правой кнопкой элемент Схема Active Directory (Active Directory Schema) и выберите Изменение контроллера домена (Change Domain Controller).

3. Установите переключатель Любой контроллер (Any Domain Controller), чтобы позволить Active Directory выбрать новый хозяин схемы автоматически, или переключатель Укажите имя (Specify Name), чтобы указать конкретный сервер.
4. Щелкните OK.
5. В дереве консоли щелкните правой кнопкой элемент Схема Active Directory (Active Directory Schema) и выберите Хозяин операций (Operations Master).
6. Щелкните Сменить (Change) и задайте в качестве хозяина другую систему.
7. Щелкните Закрыть (Close).

Передача ролей с помощью командной строки

В этом разделе рассказано, как передать роли с помощью утилиты командной строки Ntdsutil.exe.

1. Локально или с помощью удаленного рабочего стола зарегистрируйтесь на сервере, которому хотите назначить роль нового хозяина операций.
2. Щелкните кнопку Пуск (Start), выберите команду Выполнить (Run), введите **cmd** в поле Открыть (Open) и щелкните OK.
3. В командной строке введите **ntdsutil**.
4. В командной строке утилиты Ntdsutil введите **roles.** Утилита перейдет в режим обслуживания хозяев операций.
5. После приглашения Fsmo Maintenance введите **connections.** Затем после приглашения Server Connections введите **connect to server** и полное доменное имя текущего хозяина схемы для данной роли, например:

```
connect to server engdc01.technology.adatum.com
```

6. Когда соединение будет установлено, введите **quit,** чтобы покинуть приглашение Server Connections, а затем в строке приглашения Fsmo Maintenance введите transfer и идентификатор переносимой роли:
   - pdc — роль эмулятора PDC;
   - **rid master** — роль хозяина относительных идентификаторов;
   - **infrastructure master** — роль хозяина инфраструктуры;
   - **schema master** — роль хозяина схемы;

- **domain naming master** — роль хозяина именования домнов.

7. **Введите quit в строках** приглашения **Fsmo Maintenance и** Ntsdutil.

Захват ролей с помощью командной строки

Изредка возникают ситуации, когда обычная передача роли невозможна. Например, у контроллера домена, который исполнял роль хозяина RID, может выйти из строя жесткий диск. Просто передать роль другому серверу уже не удастся — ее придется захватить.

Внимание! Захват роли — это очень серьезное действие, и прибегать к нему следует лишь в безвыходной ситуации, когда сервер, исполнявший роль, окончательно и бесповоротно вышел из строя. После захвата роли сервера на нем придется переформатировать жесткий диск.

Бот как захватить роль сервера.

1. Убедитесь, что сервер, роль которого вы хотите захватить, действительно нельзя вернуть к жизни. Если сервер может продолжать работу, захватывайте его роль, только если вы собираетесь полностью переустанавливать на нем ОС.
2. Зарегистрируйтесь на сервере, который хотите сделать новым хозяином операций, локально или через удаленный рабочий стол.
3. Щелкните кнопку Пуск (Start), выберите команду Выполнить (Run), введите cmd в поле Открыть (Open) и щелкните OK.
4. В командной строке введите **ntdsutil**.
5. В командной строке утилиты Ntdsutil введите **roles.** Утилита перейдет в режим обслуживания хозяев операций.
6. После приглашения Fsmo Maintenance введите **connections.** Затем после приглашения Server Connections введите **connect** to server и полное доменное имя текущего хозяина схемы для данной роли, например:

```
connect to server engdc01.technology.adatum.com
```

7. Когда соединение будет установлено, введите **quit,** чтобы покинуть приглашение Server Connections, а затем в строке приглашения Fsmo Maintenance введите **seize** и идентифика-

тор захватываемой роли (один из тех, что перечислены в предыдущем разделе).

8. Введите **quit** в строках приглашения Fsmo Maintenance и Ntdsutil.

Настройка глобальных каталогов

Глобальные каталоги играют в сети важную роль (см. главу 6). Иногда их требуется добавлять для ускорения операций поиска, а иногда — удалять. Так, если в сайте два или более глобальных каталога, желательно оставить только один из них. Вот как включить или отключи гь глобальный каталог.

1. Откройте консоль Active Directory — сайты и службы (Active Directory Sites and Services).
2. В дереве консоли раскройте сайт, с которым хотите работать, щелкнув значок «плюс» (+) рядом с его именем.
3. Раскройте папку Servers и щелкните сервер, который хотите использовать для хранения глобального каталога.
4. Щелкните правой кнопкой элемент NTDS Settings и выберите команду Свойства (Properties).
5. Чтобы активизировать глобальный каталог, установите флажок Глобальный каталог (Global Catalog) на вкладке Общие (General), как показано на рис. 7-9.
6. Чтобы отключить глобальный каталог, сбросьте этот флажок.

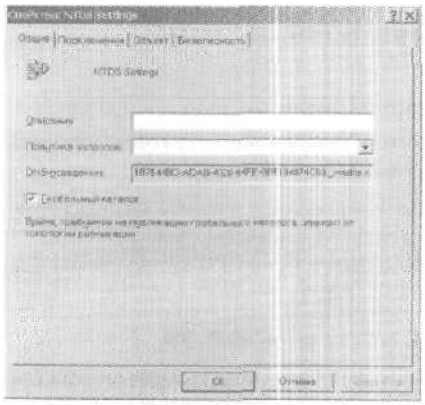


Рис. 7-9. Включение или отключение глобального каталога через NTDS-параметры сервера

Настройка кэширования членства в универсальных группах

Кэширование членства в универсальных группах позволяет регистрироваться в системе независимо от доступности сервера глобального каталога. Если в домене Windows Server 2003 разрешено кэширование членства, любой контроллер домена способен разрешать запросы на регистрацию, не обращаясь к серверу глобального каталога. Подробнее о достоинствах и недостатках этого подхода — в главе 6.

Чтобы разрешить или запретить кэширование членства в универсальных группах на сервере Windows Server 2003, который в данный момент не является сервером глобального каталога, выполните следующие действия.

1. Откройте консоль Active Directory — сайты и службы (Active Directory Sites and Services).
2. В дереве консоли раскройте нужный сайт.
3. Раскройте папку Servers и щелкните нужный сервер.
4. Щелкните правой кнопкой элемент NTDS Settings и выберите команду Свойства (Properties).
5. Чтобы разрешить кэширование, установите флажок Разрешить кэширование членства в универсальных группах (Enable Universal Group Membership Caching) на вкладке Общие (General). Чтобы запретить кэширование, этот флажок нужно сбросить.

Управление организационным подразделением

Как говорилось в главе 6, организационные подразделения (ОП) помогают организовывать объекты, применять групповую политику в ограниченной области и т. п.

Создание ОП

Обычно ОП создают для отражения функциональной или организационной структуры организации. Вы можете создавать ОП как подгруппы домена или дочерние подразделения внутри существующего ОП.

1. Откройте консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers).
2. В дереве консоли раскройте узел домена, щелкнув значок «плюс» (+) рядом с его именем.

3. Щелкните правой кнопкой узел домена или папку существующего ОП, в которую хотите добавить ОП. Выберите в контекстном меню команду Создать (New), а затем — Подразделение (Organizational Unit).
4. Введите название ОП и щелкните OK. Теперь вы можете перемещать в подразделение учетные записи и общие ресурсы.

Просмотр и изменение свойств ОП

1. Откройте консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers).
2. В дереве консоли раскройте узел домена, щелкнув значок «плюс» (+) рядом с именем домена.
3. Щелкните правой кнопкой нужное ОП и выберите команду Свойства (Properties). Откроется окно свойств, позволяющее просматривать и изменять параметры.

Переименование и удаление ОП

1. В консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) щелкните правой кнопкой ОП, с которым хотите работать.
2. Чтобы удалить ОП. выберите Удалить (Delete). Затем подтвердите действие, щелкнув Да (Yes).
3. Чтобы переименовать ОП, выберите Переименовать (Rename). Введите новое имя для ОП и нажмите Enter.

Перемещение ОП

Чтобы переместить ОП в другое положение в пределах домена, в Windows Server 2003 можно просто перетащить его мышью. Если этот способ вам почему-либо не подходит, выполните следующие действия.

1. В консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) щелкните правой кнопкой ОП, которое хотите переместить, и выберите Переместить (Move).
2. В открывшемся диалоговом окне щелкните узел домена, а затем — контейнер, куда хотите переместить ОП. Щелкните OK.

Глава 8

Учетные записи пользователей и групп

Управление учетными записями — одна из основных задач администратора Windows Server 2003. В главе 7 речь шла об учетных записях компьютеров. В этой главе мы рассмотрим учетные записи пользователей и групп. Первые позволяют входить в сеть и получать доступ к сетевым ресурсам индивидуальным пользователям. Вторые применяются для управления ресурсами нескольких пользователей. Разрешения и привилегии, назначаемые пользователям и группам, определяют, какие действия могут выполнять пользователи, а также к каким компьютерным системам и ресурсам у них есть доступ.

Не предоставляйте пользователям широких полномочий: вы должны сбалансировать их потребности в ресурсах, связанных с определенным видом работы, с необходимостью защитить уязвимые ресурсы или конфиденциальные данные. Например, не стоит давать доступ к сведениям о зарплатах всем сотрудникам компании. Следовательно, нужно убедиться, что доступ к этой информации имеют лишь те, кому она нужна.

Модель безопасности Windows Server 2003

Доступ к сетевым ресурсам контролируется с помощью компонентов модели безопасности Windows Server 2003. Основу этой модели составляют компоненты, ответственные за аутентификацию и управление доступом к ресурсам.

Протоколы аутентификации

Процесс аутентификации в Windows Server 2003 разделен на два этапа: интерактивный вход в систему и сетевая аутентификация, В процессе интерактивного входа система аутентифицирует пользователя, подтверждая его подлинность локальному компьютеру, и открывает доступ к службе каталогов Active Directory. За-

тем, всякий раз, когда пользователь обращается к сетевым ресурсам, сетевая аутентификация позволяет определить, есть ли у него на то разрешение.

Windows Server 2003 поддерживает множество протоколов аутентификации. Ключевые протоколы таковы:

- **Kerberos V 5** — стандартный Интернет-протокол аутентификации пользователей и систем (основной механизм аутентификации в Windows Server 2003);
- **NT** LAN **Manager** (NTLM) — основной протокол аутентификации в Windows NT, служит для аутентификации компьютеров в домене Windows NT;
- SSL/TLS (Secure Socket Layer/Transport Layer Security) — основной механизм аутентификации, применяемый при входе на защищенные Web-серверы;
- .NET Passport Authentication — механизм аутентификации Microsoft Internet Information Services (IIS) 6.0, позволяющий использовать информацию Active Directory для аутентификации пользователей Интернета, внутренних и внешних сетей (подробнее — в главе 7 книги «Microsoft IIS 6.0. Administrator's Pocket Consultant». Microsoft Press, 2003).

Главная особенность модели аутентификации Windows Server 2003 — поддержка *однократного ввода пароля* (single sign-on) для входа в систему. Вот как она работает.

1. Пользователь входит в домен, вводя имя и пароль или вставляя смарт-карту в считывающее устройство.
2. Система аутентифицирует доступ пользователя посредством процесса интерактивного входа. Для локальной учетной записи реквизиты аутентифицируются локально, и пользователю предоставляется доступ к локальному компьютеру. Для доменной учетной записи реквизиты аутентифицируются в Active **Directory, и** пользователь получает доступ к сетевым ресурсам.
3. Теперь пользователь может аутентифицироваться на любом компьютере в домене посредством процесса сетевой аутентификации. Для доменных учетных записей сетевая аутентификация выполняется автоматически (пароль вводится лишь раз). Пользователи с локальными учетными записями должны предоставлять имя и пароль при каждом обращении к сетевому ресурсу.

Управление доступом

В Active Directory все пользователи, компьютеры, группы, общие ресурсы и многие другие элементы определены как объекты. Управление доступом к объекту основано на дескрипторе безопасности, в котором:

- перечислены пользователи и группы, имеющие доступ к объекту;
- указаны разрешения, назначенные пользователям и группам;
- записываются события аудита;
- определен владелец объекта.

Отдельные записи в дескрипторе безопасности называют *записями управления доступом* (access control entries, ACE). Объекты Active Directory способны наследовать ACE от родительских объектов, т. е. разрешения родительского объекта могут применяться к дочернему. Например, все участники группы Администраторы домена (Domain Admins) наследуют разрешения, предоставленные этой группе.

При работе с ACE имейте в виду следующее:

- ACE по умолчанию создаются с разрешенным наследованием;
- наследование происходит сразу после создания ACE;
- во всех ACE содержится информация, указывающая, было ли разрешение унаследовано или явно назначено соответствующему объекту.

Различия между учетными записями пользователей и групп

Учетные записи пользователей предназначены отдельным лицам, а учетные записи групп позволяют упростить управление множеством пользователей. Войти в систему вы можете только по учетной записи пользователя. Учетные записи групп обычно называют просто *группами*.

Примечание В Windows Server 2003 поддерживается объект InetOrgPerson. В сущности, он похож на объект-пользователь и может применяться в этом качестве. Однако подлинное назначение объекта InetOrgPerson — обеспечивать совместимость со службами каталогов X.500 и ШАР других разработчиков, в которых он представляет пользователей, а также переход с этих служб каталогов на Active Directory. Если в процессе пе-

рехода к Active Directory с другой службы каталогов вы сталкиваетесь с многочисленными объектами InetOrgPerson, не беспокойтесь. Их можно применять в качестве участников безопасности наравне с пользовательскими учетными записями. Объект InetOrgPerson доступен в полном объеме только в режиме Windows Server 2003. При этом вы вправе задать пароли для объектов InetOrgPerson и при желании изменить класс объекта. В последнем случае объект InetOrgPerson превращается в обычный объект-пользователь.

Учетные записи пользователей

В Windows Server 2003 определены пользовательские учетные записи двух типов.

- **Доменные учетные** записи **(domain** user accounts) определены в Active Directory. Посредством системы однократного ввода пароля такие учетные записи могут обращаться к ресурсам во всем домене. Они создаются в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers).
- **Локальные учетные записи** (local **user accounts)** определены на локальном компьютере, имеют доступ только к его ресурсам и должны аутентифицироваться, прежде чем получат доступ к сетевым ресурсам. Локальные учетные записи пользователей создают в оснастке Локальные пользователи и группы (Local Users and Groups).

Примечание Локальные учетные записи пользователей и групп хранятся только на рядовых серверах и рабочих станциях. На первом контроллере домена они перемещаются в Active Directory и преобразуются в доменные учетные записи.

Имена для входа в систему, пароли и открытые сертификаты

Все учетные записи пользователей распознаются по имени для входа в систему. В Windows Server 2003 оно состоит из двух частей:

- **имя пользователя** — текстовое имя учетной записи;
- **домен** или **рабочая группа, в** которых находится учетная запись.

Для пользователя wrstanec, учетная запись которого создана в домене microsoft.com, полное имя для входа в Windows

Server 2003 выглядит так — vvrstanek@microsoft.com. Имя для предыдущих версий Windows — MICROSOFT\wrstanek. При работе с Active Directory вам также иногда требуется полное имя домена (fully qualified domain name, FQDN) пользователя, состоящее из DNS-имени домена в сочетании с именами контейнера (или ОП) и группы. У пользователя microsoft.com\Users\wrstanek, microsoft.com — DNS-имя домена, Users -- имя контейнера, а wrstanek — имя пользователя.

С учетной записью пользователя могут сопоставляться пароль и *открытый сертификат* (public certificate). В открытом сертификате сочетаются открытый и закрытый ключ для идентификации пользователя. Вход в систему по паролю проходит интерактивно. При входе в систему с открытым сертификатом используются смарт-карта и считывающее устройство.

Идентификаторы безопасности и учетные записи пользователей

Хотя для назначения привилегий и разрешений в Windows Server 2003 применяются имена пользователей, ключевым идентификатором учетной записи является генерируемый при се создании уникальный идентификатор безопасности (security identifier, SID). Он состоит из идентификатора безопасности домена и уникального относительного идентификатора, который был выделен хозяином относительных идентификаторов.

С помощью SID Windows Server 2003 способна отслеживать учетные записи независимо от имен пользователей. Благодаря наличию SID вы вправе изменять имена пользователей и удалять учетные записи, не беспокоясь, что кто-то получит доступ к ресурсам, создав учетную запись с тем же именем.

Когда вы меняете имя пользователя, Windows Server 2003 сопоставляет прежний SID с новым именем. Когда вы удаляете учетную запись, Windows Server 2003 считает, что конкретный SID больше **недействителен.** Если вы затем создадите учетную запись с тем же именем, она не получит привилегий предыдущей записи, так как у нее иной SID.

Учетные записи групп

Помимо учетных записей пользователя в Windows Server 2003 используются группы, позволяющие автоматически предоставлять разрешения схожим типам пользователей и упростить администрирование учетных записей. Если пользователь — член группы, которая вправе обращаться к ресурсу, то он тоже может к нему обратить-

ся. Чтобы предоставить пользователю доступ к нужным ресурсам, вы просто включаете его в подходящую группу.

Поскольку в разных доменах Active Directory могут быть группы с одинаковыми именами, на группы часто ссылаются по полному имени — *домен\имя_группы*, например, WORK\GMarketing соответствует группе GMarketing в домене WORK. При работе с Active Directory к группе иногда нужно обращаться по полному имени, состоящему из DNS-имени домена, имени контейнера или ОП и имени группы. В имени группы microsoft.com\Users\GMarketing, microsoft.com — DNS-имя домена, Users — контейнер или ОП, а GMarketing — имя группы.

Примечание Служащим отдела маркетинга скорее всего понадобится доступ ко всем ресурсам, связанным с маркетингом. Вместо того чтобы открывать доступ к ним индивидуально, стоит объединить пользователей в группу. Если позже пользователь перейдет в другой отдел, вы просто исключите его из группы, и все разрешения доступа будут отозваны.

Типы групп

В Windows Server 2003 используются группы трех типов:

- локальные группы (local groups) определяются и используются только на локальном компьютере, создаются в оснастке Локальные пользователи и группы (Local Users and Groups);
- группы безопасности (security groups) располагают дескрипторами защиты и определяются в доменах посредством консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers);
- группы распространения (distribution groups) используются как списки рассылки электронной почты, не имеют дескрипторов безопасности и определяются в доменах посредством консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers).

Область действия группы

У групп возможны разные области действия — *локальная доменная* (domain local), *встроенная локальная* (built-in local), *глобальная* (global) и *универсальная* (universal). От этого зависит, в какой части сети они действительны.

- Локальные доменные группы предоставляют разрешения в одном домене, В состав локальных доменных групп входят лишь учетные записи (и пользователей, и компьютеров) и группы из домена, в котором они определены.
- Встроенные локальные группы обладают особым и разрешениями в локальном домене. Для простоты их часто также называют локальными доменными группами, но в отличие от обычных групп встроенные локальные группы нельзя создать или удалить — можно лишь изменить их состав. Как правило, говоря о локальных доменных группах, я буду иметь в виду и обычные, и встроенные локальные группы, если не указано обратное.
- Глобальные группыиспользуются для назначения разрешений на доступ к объектам в любом домене дерева или леса. В глобальную группу входят только учетные записи и группы из домена, в котором они определены.
- Универсальные группы управляют разрешениями во всем дереве или лесе; в них входят учетные записи и группы из любого домена в дереве или лесе домена. Универсальные группы доступны только в Active Directory в основном режиме Windows 2000 или в режиме Windows Server 2003.

Примечание Универсальные группы очень полезны на больших предприятиях, имеющих несколько доменов. Состав универсальных групп не должен часто меняться, так как любое изменение надо реплицировать во все глобальные каталоги (ГК) в дереве или лесе. Чтобы уменьшить количество изменений, включайте в универсальную группу только группы, а не сами учетные записи. Подробнее — в разделе «Когда использовать локальные доменные, глобальные и универсальные группы».

От области действия группы зависит, что вы можете с ней делать (табл. 8-1). О создании групп — в главе 9.

Идентификаторы безопасности и учетные записи групп

В Windows Server 2003 учетные записи групп, как и учетные записи пользователей, различаются по уникальным идентификаторам безопасности (SID). Это значит, что нельзя удалить учетную запись группы, а затем создать группу с тем же именем, чтобы у нее появились прежние разрешения и привилегии. У но-

Таблица 8-1. Влияние области действия группы на ее характеристики

Характеристика	Локальная доменная область	Глобальная область	Универсальная область
Состав в основном режиме Windows 2000/ Windows Server 2003	Учетные записи, глобальные и универсальные группы из любого домена, локальные доменные только из того же домена	Учетные записи и глобальные группы только из того же домена	Учетные записи и группы из любого домена независимо от области действия
Состав в смешанном режиме Windows 2000	Учетные записи и глобальные группы из любого домена	Учетные записи только из того же домена	Нельзя создать в домене смешанного режима
Участник других групп	Можно поместить в другие локальные доменные группы и назначить разрешения только в том же домене	Можно поместить в другие группы и назначить разрешения в любом домене	Можно поместить в другие группы и назначить разрешения в любом домене
Смена области действия	Можно преобразовать в универсальную группу, если в составе нет локальных доменных групп	Можно преобразовать в универсальную группу, если она не является участником другой глобальной группы	Нельзя преобразовать ни в какую другую область

вой группы будет новый SID, и все разрешения и привилегии старой группы будут утеряны.

Для каждого сеанса пользователя в системе Windows Server 2003 создает маркер безопасности, содержащий идентификатор учетной записи пользователя и SID всех групп безопасности, к которым относится пользователь. Размер маркера растет по мере того, как пользователь добавляется в новые группы безопасности. Это приводит к следующим последствиям;

- чтобы пользователь вошел в систему, маркер безопасности должен быть передан процессу входа в систему. Поэтому по мере увеличения членства пользователя и группах безопасности продесс входа требует все больше времени;
- чтобы выяснить разрешения доступа, маркер безопасности пересылается на каждый компьютер, к которому обращается

пользователь. Поэтому чем больше маркер безопасности, тем выше сетевой трафик.

Примечание Сведения о членстве в группах распространения не передаются в маркере безопасности, поэтому **состав** этих групп не влияет на размер маркера.

Когда использовать локальные доменные, глобальные и универсальные группы

Локальные доменные, глобальные и универсальные группы содержат множество параметров для настройки групп в масштабе предприятия. В идеале следует использовать области действия групп для создания иерархий, схожих со структурой вашей организации и обязанностями групп пользователей.

- **Локальные доменные группы** обладают наименьшей сферой влияния и хорошо подходят для управления доступом к таким ресурсам, как принтеры и общие папки.
- **Глобальные группы** оптимальны для управления учетными записями пользователей и компьютеров в отдельном домене. Предоставляйте разрешения доступа к ресурсу, включая глобальную группу в состав локальной доменной группы.
- **Универсальные группы** обладают самой широкой сферой влияния. Используйте их для централизации групп, определенных в нескольких доменах. Обычно для этого в универсальную группу добавляется глобальная. Тогда при изменении состава глобальных групп изменения не будут реплицироваться во все ГК, поскольку формально состав универсальных групп не меняется.

Примечание Если в вашей организации всего один домен, универсальные группы не нужны; стройте структуру на локальных доменных и глобальных группах. Если вы затем добавите в дерево или лес другой **домен, вы** легко расширите **иерархию,** чтобы она соответствовала новому **состоянию** сети.

Рассмотрим конкретный сценарий. Пусть ваша компания имеет представительства в Сиэтле, Чикаго и Нью-Йорке. У каждого офиса — собственный домен, являющийся частью одного дерева или леса: Seattle, Chicago и ny. Вы хотите упростить управление сетевыми ресурсами для администраторов из любого офиса и потому создаете идентичную структуру групп. В компании есть отделы маркетинга, ИТ и инженерный, но мы рассмо-

трим лишь структуру отдела маркетинга. Сотрудникам этого отдела в каждом представительстве нужен доступ к общему принтеру MarketingPrinter и общей папке Marketing Data. Вы хотите, чтобы сотрудники могли совместно использовать и печатать документы. Скажем, Бобу из Сиэтла необходимо печатать документы для Ральфа в Нью-Йорке, поэтому ему требуется доступ к квартальному отчету в общей папке в нью-йоркском офисе.

Сконфигурируем группы для отделов маркетинга в трех офисах.

1. Начнем с создания глобальных групп для каждой маркетинговой группы. В домене Seattle создадим группу GMarketing и добавим в нее сотрудников отдела маркетинга из Сиэтла. В домене Chicago создадим группу с тем же именем и добавим в нее сотрудников отдела маркетинга из Чикаго. В домене ny сделаем то же самое.
2. В каждом представительстве создадим локальные доменные группы, предоставив им доступ к обидим принтерам и папкам. Назовем группу с доступом к принтеру LocalMarketingPrinter, а общую папку в домене Нью-Йорка — LocalMarketingData. Домены Seattle, chicago и ny должны обладать собственными локальными группами.
3. Создадим универсальную группу UMarketing в домене каждого представительства. Добавим в нее группы seattle\GMarketing, chicago\GMarketing и ny\GMarketing.
4. Добавим UMarketing в группы LocalMarketingPrinter и LocalMarketingData в каждом представительстве. Теперь сотрудники отдела маркетинга смогут совместно использовать данные и принтеры.

Стандартные учетные записи пользователей и группы

При установке Windows Server 2003 создаются стандартные учетные записи пользователей и группы. Они предназначены для начальной настройки, необходимой для развития сети, Вот три типа стандартных учетных записей:

- встроенные (built-in) учетные записи пользователей и групп устанавливаются вместе с ОС, приложениями и службами;
- предопределенные (predefined) учетные записи пользователей и групп устанавливаются вместе с ОС;

- неявные (implicit) — специальные группы, создаваемые неявно при обращении к сетевым ресурсам; их также называют *специальными объектами* (special identities).

Примечание Удалить пользователей и группы, созданные ОС, нельзя.

Встроенные учетные записи

У встроенных учетных записей пользователей в Windows Server 2003 есть особые цели. Все системы Windows Server 2003 обладают тремя встроенными учетными записями.

- Локальная система (Local System) — учетная псевдозапись для выполнения системных процессов и обработки задач системного уровня, доступная только па локальной системе. Эта запись обладает правом Вход в качестве службы (Log on as a service). Большинство служб работает под локальной системной учетной записью и имеет право взаимодействовать с рабочим столом. Службы, которым требуются дополнительные привилегии или права входа, работают под учетными записями Local Service или Network Service.
- Local Service — учетная псевдозапись для запуска служб, которым необходимы дополнительные привилегии или права входа на локальной системе. Службы, которые работают под этой учетной записью, по умолчанию обладают правами и привилегиями па вход в качестве службы, на изменение системного времени и на создание журналов безопасности. К службам, работающим от имени учетной записи Local Service, относятся Оповещатель (Alerter), Служба сообщений (Messenger), Удаленный реестр (Remote Registry), Смарт-карта (Smart Card), Модуль поддержки смарт-карт (Smart Card Helper), Служба обнаружения SSDP (SSDP Discovery Service), Модуль поддержки NetBIOS через TCP/IP (TCP/IP NetBIOS Helper), Источник бесперебойного питания (Uninterruptible Power Supply) и Веб-клиент (WebClient).
- NetworkService — учетная псевдозапись для служб, которым требуются дополнительные привилегии или права входа на локальной системе и в сети. Службы, которые работают под этой учетной записью, обладают правами на вход в качестве службы, изменение системного времени и создание журналов безопасности. Под учетной записью Network Service работают такие службы, как Координатор распределенных транзак-

ций (Distributed Transaction Coordinator), DNS-клиент (DNS Client), Журналы и оповещения производительности (Performance Logs and Alerts) и Локатор удаленного вылова процедур (Remote Procedure Call Locator).

Когда вы устанавливаете па сервере дополнения или другие приложения, разрешается установить и другие учетные записи по умолчанию. Обычно их можно потом удалить.

Установив IIS (Internet Information Services), вы обнаружите новые учетные записи: IUSR_*имякомпьютера* и IWAM_*имякомпьютера*: первая — встроенная учетная запись для анонимного доступа к IIS, а вторая служит IIS для запуска прикладных процессов. Эти учетные записи определяются в Active Directory, когда они настроены в домене, и как локальные учетные записи, когда они настроены на изолированном сервере или рабочей станции. Еще одна встроенная учетная запись, — TSInternetUser — требуется службам терминала.

Предопределенные учетные записи пользователей

Вместе с Windows Server 2003 устанавливаются некоторые записи: Администратор (Administrator), Гость (Guest), ASPNET и Support. На рядовых серверах предопределенные учетные записи являются локальными для той системы, где они установлены.

У предопределенных учетных записей есть аналоги в Active Directory, которые имеют доступ по всему домену и совершенно независимы от локальных учетных записей на отдельных системах.

Учетная запись Администратор (Administrator)

Эта предопределенная учетная запись обладает полным доступом к файлам, папкам, службам и другим ресурсам; ее нельзя отключить или удалить. В Active Directory она обладает доступом и привилегиями во всем домене. В остальных случаях Администратор (Administrator) обычно имеет доступ только к локальной системе. Файлы и папки можно временно закрыть от администратора, но он имеет право в любой момент вернуть себе контроль над любыми ресурсами, сменив разрешения доступа (см. главу 13).

Совет Чтобы предотвратить несанкционированный доступ к системе или домену, убедитесь, что у административной записи надежный пароль. Кроме того, стандартное имя этой записи всем известно, поэтому переименуйте ее.

Обычно менять основные параметры учетной записи Администратор (Administrator) не требуется, однако иногда следует сменить такие дополнительные параметры, как ее членство в некоторых группах. По умолчанию администратор в домене включен в группы Администраторы (Administrators), Администраторы домена (Domain Admins), Пользователи домена (Domain Users), Администраторы предприятия (Enterprise Admins), Администраторы схемы (Schema Admins) и Владельцы-создатели групповой политики (Group Policy Creator Owners). Подробнее об этих группах читайте в следующем разделе.

Примечание В сети с доменами локальная учетная запись Администратор (Administrator) применяется в основном для управления системой сразу после установки. Вероятно, вы не станете применять ее впоследствии, а включите администраторов в группу Администраторы (Administrators). Это гарантирует, что вы сможете отозвать привилегии администраторов, не изменяя пароли для учетных записей Администратор (Administrator) на каждом компьютере.

В системе, которая является частью рабочей группы и где каждый компьютер управляется независимо от других, эта запись обычно применяется для выполнения административных задач. При этом не следует настраивать индивидуальные учетные записи для каждого сотрудника, обладающего административным доступом к системе. Лучше используйте одну учетную запись Администратор (Administrator) на каждом компьютере.

Учетная запись ASPNET

Учетная запись ASPNET используется в .NET Framework и предназначена для запуска рабочих процессов ASP.NET. Она является членом группы Пользователи домена (Domain Users) и в этом качестве имеет те же привилегии, что и обычные пользователи в домене.

Учетная запись Гость (Guest)

Эта учетная запись предназначена для пользователей, которым нужен разовый или редкий доступ к ресурсам компьютера или сети. Гостевая учетная запись обладает весьма ограниченными системными привилегиями, тем не менее применяйте ее с осторожностью, поскольку она потенциально снижает безопасность.

Поэтому запись Гость (Guest) при установке Windows Server 2003 изначально отключена.

Учетная запись Гость (Guest) по умолчанию является членом групп Гости домена (Domain Guests) и Гости (Guests). Важно отметить, что все гостевые учетные записи являются членами неявной группы Все (Everyone), которая обычно по умолчанию имеет доступ к файлам и папкам и располагает стандартным набором прав пользователя.

Совет Решив задействовать запись Гость (Guest), убедитесь, что она наделена ограниченными правами, и регулярно меняйте для нее пароль. Как и учетную запись Администратор (Administrator), запись Гость (Guest) для вящей предосторожности стоит переименовать,

Учетная запись Support

Учетная запись Support применяется встроенной службой Справка и поддержка (Help and Support). Она является членом групп HelpServicesGroup и Пользователи домена (Domain Users) и имеет право входа в качестве пакетного задания. Это позволяет учетной записи Support выполнять пакетные задания, связанные с обновлением системы.

Примечание Учетной записи Support отказано в праве локального входа (за исключением входа в качестве пакетного задания) и в праве на вход из сети. Эти ограничения важны для обеспечения безопасности системы.

Встроенные и предопределенные группы

Встроенные группы устанавливаются со всеми системами Windows Server 2003. Чтобы предоставить пользователю привилегии и разрешения встроенной группы, включите его в ее состав. Например, чтобы дать пользователю административный доступ к системе, включите его в локальную группу Администраторы (Administrators). Чтобы дать пользователю административный доступ к домену, включите cm в локальную доменную группу Администраторы (Administrators) в Active Directory.

Неявные группы и специальные идентификаторы

В Windows NT неявные группы назначались автоматически при входе в систему, на основе того, как пользователь обращался к се-

тевому ресурсу. Так, если он обращался через интерактивный вход, то автоматически становился участником неявной группы Интерактивные (Interactive). В Windows 2000 и Windows Server 2003 объектный подход к структуре каталога изменил первоначальные правила для неявных групп. Хотя по-прежнему нельзя просмотреть состав неявных системных групп, вы вправе включать в них пользователей, группы и компьютеры.

Состав специальной встроенной группы может варьироваться неявно, например при входе в систему, или явно — через разрешения доступа. Как и в случае других стандартных групп, доступность неявных групп зависит от конфигурации (табл. 8-2).

Таблица 8-2. Доступность неявных групп в зависимости от типа сетевого ресурса

Имя группы	Домен Active Directory	Windows Server 2003 или рядовой сервер
Local Service	Нет	Да
Network Service	Нет	Да
Remote Interactive Logon	Нет	Да
Self	Да	Нет
Анонимный вход (Anonymous Logon)	Да	Да
Все (Everyone)	Да	Да
Группа-создатель (Creator Group)	Да	Да
Интерактивные (Interactive)	Да	Да
Контроллеры домена предприятия (Enterprise Domain Controllers)	Да	Нет
Ограниченные (Restricted)	Да	Нет
Пакетное задание (Batch)	Да	Да
Пользователь служб терминалов (Terminal Server User)	Да	Да
Прокси (Proxy)	Да	Нет

Таблица 8-2. Доступность неявных групп в зависимости от типа сетевого ресурса *(окончание)*

Имя группы	Домен Active Directory	Windows Server 2003 или рядовой сервер
Прошедшие проверку (Authenticated Users)	Да	Да
Сеть (Network)	Да	Да
Система (System)	Да	Да
Служба (Service)	Да	Да
Создатель-владелец (Creator Owner)	Да	Да
Удаленный доступ (Dialup)	Да	Да

Возможности учетных записей

Чтобы назначить пользователю тс или иные права, добавьте его в группы, а чтобы лишить — удалите из соответствующих групп. В Windows Server 2003 учетной записи можно назначить следующие типы прав.

- **Привилегия (privilege)** позволяет выполнять определенную административную задачу, например отключать систему. Привилегии можно назначать как пользователям, так и группам.
- **Права на вход в систему** (logon rights) определяют возможность входа в систему, например локально. Права па вход разрешается назначить и пользователям, и группам.
- **Встроенные возможности (built-in capabilities)** предназначены для групп. Они предопределены и неизменны, но их допустимо делегировать пользователям с разрешением управлять объектами, ОП или другими контейнерами. Например, возможность создавать и удалять учетные записи пользователей, а также управлять ими дается администраторам и операторам учета. Иными словами, пользователь, включенный в состав группы Администраторы (Administrators), тем самым получает право создавать и удалять учетные записи пользователей.
- **Разрешения** доступа **(access permissions)** определяют, какие действия можно выполнять с сетевыми ресурсами, например создавать файл в папке. Можно назначать разрешения

доступа пользователям, компьютерам и группам (см. также главу 14).

Вы не вправе менять встроенные возможности группы, но вы можете изменить ее стандартные права. Так, администратор может отменить сетевой доступ к компьютеру, удалив право группы па доступ к этому компьютеру из сети.

Привилегии

Привилегии назначаются через групповые политики. применяемые к отдельным компьютерам, ОП и доменам. Хотя привилегии можно назначать и пользователям, и группам, их обычно назначают группам, что упрощает управление учетными записями пользователей.

В табл. 8-3 кратко описаны *привилегии*, назначаемые пользователям и группам (см. также главу 9).

Таблица 8-3. Привилегии Windows Server 2003 для пользователей и групп

Привилегия	Описание
Архивирование файлов и каталогов (Back up files and directories)	Позволяет пользователям архивировать систему независимо от разрешений, заданных для файлов и папок
Восстановление файлов и каталогов (Restore files and directories)	Разрешает пользователям восстанавливать из архива файлы и папки независимо от разрешений, заданных для файлов и папок
Добавление рабочих станций *к* домену (Add workstations to domain)	Позволяет пользователям добавлять компьютер в домен
Завершение работы системы (Shut down the system)	Разрешает пользователям выключать локальный компьютер
Загрузка и выгрузка драйверов устройств (Load and unload device drivers)	Позволяет пользователям устанавливать и удалять драйверы устройств Plug and Play. Не влияет на драйверы остальных устройств, которые могут быть установлены только администраторами
Закрепление страниц в памяти (Lock pages in memory)	Позволяет процессам хранить данные в физической памяти, запрещая системе выгружать страницы данных в виртуальную память на диске .
Замена маркера уровня процесса (Replace a process-level token)	Позволяет процессам заменять метку по умолчанию для второстепенных процессов

Таблица 8-3. Привилегии Windows Server 2003 для пользователей и групп (*продолжение*)

Привилегия	Описание
Запуск операции но обслуживанию тома (Perform volume maintenance tasks)	Разрешает администрирование съемных носителей, дефрагментацию диска и управление диском
Извлечение компьютера из стыковочного узла (Remove computer from docking station)	Позволяет извлечь переносной компьютер из стыковочной станции и удалить его из сети
Изменение параметров среды оборудования (Modify firmware environment values)	Разрешает пользователям и процессам изменять переменные системной среды
Изменение системного времени (Changethe system time)	Позволяет пользователям задавать время на системных часах
Настройка квот памяти для процесса (Adjust memory quotas for a process)	Позволяет пользователям настраивать квоты на использованием памяти
Обход перекрестной проверки (Bypass traverse checking)	Позволяет пользователям проходить через папки по пути к объекту независимо от разрешений, заданных для этих папок; не позволяет просматривать содержимое папок
Овладение файлами или иными объектами (Take ownership of files or other objects)	Разрешает пользователям завладевать любыми объектами Active Directory
Олицетворение клиента после проверки подлинности (Impersonate a client after authentication)	Позволяет Web-приложениям работать как клиентам в ходе обработки запросов. Службы и пользователи также могут работать как клиенты
Отладка программ (Debug programs)	Позволяет пользователям выполнять отладку
Принудительное удаленное завершение (Force shutdown of a remote system)	Разрешает пользователям выключать компьютер из удаленной точки сети
Профилирование загруженности системы (Profile system performance)	Разрешает пользователям следить за быстродействием системных процессов
Профилирование одного процесса (Profile a single process)	Разрешает пользователям следить за быстродействием несистемных процессов

Таблица 8-3. Привилегии Windows Server 2003 для пользователей и групп *(окончание)*

Привилегия	Описание
Работа в режиме операционной системы (Act as part of the operating system)	Позволяет процессу аутентифицироваться и получать доступ к ресурсам подобно обычному пользователю. Процессы, которым требуется эта привилегия, должны использовать учетную запись Локальная система (Local System), у которой уже есть эта привилегия
Разрешение доверия к учетным записям при делегировании (Enable user and computer accounts to be trusted for delegation)	Разрешает пользователям или компьютерам изменять или применять параметр Делегирование разрешено (Trusted for Delegation) при условии, что у них есть право на запись объекта
Синхронизация данных службы каталогов (Synchronize directory service data)	Разрешает пользователям синхронизировать данные службы каталогов на контроллерах доменов.
Создание журналов безопасности (Generate security audits)	Позволяет процессам добавлять в журнал безопасности записи аудита доступа к объектам
Создание маркерного объекта (Create a token object)	Позволяет процессам создавать объекты-маркеры, через которые можно получать доступ к локальным ресурсам. Процессы, которым требуется эта привилегия, должны использовать учетную запись Локальная система (Local System), у которой уже есть эта привилегия
Создание постоянных объектов совместного использования (Create permanent shared objects)	Позволяет процессам создавать объекты каталога в диспетчере объектов Windows 2000, Windows XP Professional и Windows Server 2003. У большинства компонентов уже есть эта привилегия, и нет необходимости специально назначать ее
Создание страничного файла (Create a pagefile)	Позволяет пользователям создавать и изменять размер страничного файла для виртуальной памяти
Увеличение приоритета диспетчирования (Increase scheduling priority)	Разрешает процессам повышать приоритет, назначенный другому процессу, при условии, что у них есть право на запись для процесса
Управление аудитом и журналом безопасности (Manage auditing and security log)	Позволяет пользователям задавать параметры аудита и просматривать журнал безопасности (сначала нужно включить аудит в групповой политике)

Права на вход в систему

Бы можете назначать права на вход в систему и пользователям, и группам. Как и привилегии, права на вход в систему назначаются через групповые политики; назначайте их группам, а не пользователям. В табл. 8-4 описаны права на вход в систему, которые можно назначить пользователям и группам (см. также главу 9).

Таблица 8-4. Права на вход в систему для пользователей и групп

Право на вход в систему	Описание
Вход в качестве пакетного задания (Log on as a batch job)	Разрешает вход в систему в качестве пакетного задания
Вход в качестве службы (Log on as a service)	Разрешает вход в систему в качестве службы. Это право по умолчанию дано учетной записи Локальная система (Load System). Это право следует назначать службе, работающей под отдельными учетными записями
Доступ к компьютеру из сети (Access this computer from the network)	Разрешает удаленный доступ к этому компьютеру
Запретить вход в систему через службу терминалов (Deny logon through Terminal Services)	Отказывает в праве на вход в систему через службы терминалов
Локальный вход в систему (Allow logon locally)	Дает право на вход с клавиатуры компьютера. На серверах это право по умолчанию предоставлено только членам следующих групп: Администраторы (Administrators), Операторы учета (Account Operators), Операторы архива (Backup Operators), Операторы печати (Print Operators) и Операторы сервера (Server Operators)
Отказ в доступе к компьютеру из сети (Deny access to this computer from the network)	Запрещает удаленный доступ к этому компьютеру через сетевые службы
Отказ во входе в качестве пакетного задания (Deny logon as batch job)	Отказывает в праве на вход в систему через пакетное задание или сценарий
Отказать во входе в качестве службы (Deny logon as service)	Отказывает службе в праве на вход в систему
Отклонить локальный вход (Deny logon locally)	Отказывает в праве на вход в систему с клавиатуры компьютера

Таблица 8-4. Права на вход в систему для пользователей и групп (окончание)

Право на вход в систему	Описание
Разрешать вход *в* систему через службу терминалов (Allow logon through terminal services)	Разрешает доступ через службы терминалов, что необходимо для использования удаленного помощника и удаленного рабочего стола

Встроенные возможности групп Active Directory

В следующих двух таблицах описаны самые распространенные встроенные возможности групп Active Directory, назначаемые по умолчанию. В табл. 8-5 перечислены стандартные нрава для групп в доменах Active Directory, в том числе привилегии и права на вход в систему. Учтите, любое действие, доступное группе Все (Everyone), доступно все группам, включая Гости (Guests). Это означает, что группа Гости (Guests), не обладающая явным разрешением на обращение к компьютеру из сети, все равно сможет получить доступ к системе, так как группа Все (Everyone) имеет это право.

Таблица 8-5. Стандартные права пользователей для групп Active Directory

Право пользователя	Назначено группам
Архивирование файлов и каталогов (Back up files and directories)	Администраторы (Administrators), Операторы сервера (Server Operators), Операторы архива (Backup Operators)
Восстановление файлов и каталогов (Restore files and directories)	Администраторы (Administrators), Операторы сервера (Server Operators), Операторы архива (Backup Operators)
Вход в качестве пакетного задания (Log on as batch job)	Администраторы (Administrators), IWAM_*имякомпьютера*, IUSR_*имякомпьютера*, Support, Local Service, IIS_WPG
Вход в качестве службы (Log on as a service)	Network Service
Добавление рабочих станций к домену (Add workstations to domain)	Прошедшие проверку (Authenticated Users)
Доступ к компьютеру из сети (Access this computer from the network)	Все (Everyone), Администраторы (Administrators), Прошедшие проверку (Authenticated Users), Контроллеры домена предприятия (Enterprise Domain Controllers), IWAM_*имяком-*

Таблица 8-5. Стандартные права пользователей для групп Active Directory *(продолжение)*

Право пользователя	Назначено группам
	пьютера, IUSR_*имякомпьютера*, Пред-Windows 2000 доступ (Pre-Windows Compatible Access)
Завершение работы системы (Shut down the system)	Администраторы (Administrators), Операторы сервера (Server Operators). Операторы учета (Account Operators), Операторы архива (Backup Operators), Операторы печати (Print Operators)
Загрузка и выгрузка драйверов устройств (Load and unload device drivers)	Администраторы (Administrators). Операторы печати (Print Operators)
Замена маркера уровня процесса (Replace a process level token)	IWAM_*имякомпьютера*, Local Service, Network Service
Извлечение компьютера из стыковочного узла (Remove computer from docking station)	Администраторы (Administrators)
Изменение параметров среды оборудования (Modify firmware environment variables)	Администраторы (Administrators)
Изменение системного времени (Change the system time)	Администраторы (Administrators), Операторы сервера (Server Operators)
Локальный вход в систему (Allow logon locally)	Операторы учета (Account Operators), Администраторы (Administrators), IUSR_*имякомпьютера*, Операторы архива (Backup Operators), Операторы печати (Print Operators), Операторы сервера (Server Operators)
Настройка квот памяти для процесса (Adjust memory quotas for a process)	Администраторы (Administrators), IWAM_*имякомпьютера*, Local Service, Network Service
Обход перекрестной проверки (Bypass traverse checking)	Все (Everyone), Прошедшие проверку (Authenticated Users), Администраторы (Administrators), Пред-Windows 2000 доступ (Pre-Windows Compatible Access)

Таблица 8-5. Стандартные права пользователей для групп Active Directory (окончание)

Право пользователя	Назначено группам
Овладение файлами или иными объектами (Take ownership of files or other objects)	Администраторы (Administrators)
Отказ в доступе к компьютеру из сети (Deny access to this computer from the network)	Support
Отклонить локальный вход (Deny logon locally)	Support
Отладка программ (Debug programs)	Администраторы (Administrators)
Принудительное удаленное завершение (Force shutdown from a remote system)	Администраторы (Administrators), Операторы сервера (Server Operators)
Профилирование загруженности системы (Profile system performance)	Администраторы (Administrators)
Профилирование одного процесса (Profile a single process)	Администраторы (Administrators)
Разрешение доверия к учетным записям при делегировании (Enable user and computer accounts to be trusted for delegation)	Администраторы (Administrators)
Создание журналов безопасности (Generate security audits)	Local Service, Network Service
Создание страничного файла (Create a pagefile)	Администраторы (Administrators)
Увеличение приоритета диспетчирования (Increase scheduling priority)	Администраторы (Administrators)
Управление аудитом и журналом безопасности (Manage auditing and security log)	Администраторы (Administrators)

В табл. 8-6 перечислены стандартные права для локальных групп на рядовых серверах; здесь, так же, как и в табл. 8-5. приведены привилегии и права на вход. Учтите, что на этих системах группа Опытные пользователи (Power Users) обладает привилегиями, которых нет у обычных пользователей.

Таблица 8-6. Стандартные права пользователей для рабочих групп и рядовых серверов

Право пользователя	Назначено группам
Архивирование файлов и каталогов (**Back** up files and directories)	Администраторы (Administrators), Операторы архива (Backup Operators)
Восстановление файлов и каталогов (Restore files and directories)	Администраторы (Administrators), Операторы архива (Backup Operators)
Вход в качестве пакетного задания (Log on as batch job)	IWAM_*имякомпьютера*, ASPNET, Local Service. IIS_WPG
Вход в качестве службы (Log on as a service)	Network Service, ASPNET
Завершение работы системы (Shut down the system)	Администраторы(Administrators), Операторы архива (Backup Operators), Опытные пользователи (Power Users), Пользователи (Users)
Загрузка и выгрузка драйверов устройств (Load and unload device drivers)	Администраторы (Administrators)
Замена маркера уровня процесса (Replace a process level token)	IWAM_*имякомпьютера*, Local Service, Network Service
Запретить вход в систему через службу терминалов (Deny logon through Terminal Services)	**ASPNET**
Извлечение компьютера из стыковочного узла (Remove computer from docking station)	Администраторы (Administrators), Опытные пользователи (Power Users), Пользователи (Users)
Изменение параметров среды оборудования (Modify firmware environment variables)	**Администраторы** (Administrators)

Таблица 8-6. Стандартные права пользователей для рабочих групп и рядовых серверов *(продолжение)*

Право пользователя	Назначено группам
Изменение системного времени (Change the system time)	Администраторы (Administrators), Опытные пользователи (Power Users)
Локальный вход в систему (Allow logon locally)	Администраторы (Administrators), IUSR_*имякомпьютера*, Операторы архива (Backup Operators), Опытные пользователи (Power Users), Пользователи (Users)
Настройка квот памяти для процесса (Adjust memory quotas for a process)	Администраторы (Administrators), IWAM_*имякомпьютера*, Local Service, Network Service
Обход перекрестной проверки (Bypass traverse checking)	Все (Everyone), Администраторы (Administrators), Пользователи (Users), Операторы архива (Backup Operators), Опытные пользователи (Power Users)
Овладение файлами или иными объектами (Take ownership ot" files or other objects)	Администраторы (Administrators)
Олицетворение клиента после проверки подлинности (Impersonate a client afterauthentication)	Администраторы (Administrators), ASPNET, IIS_WPG, Служба (Service)
Отказ в доступе к компьютеру ил сети (Deny access to this computer from the network)	Support
Отклонить локальный вход (Deny logon locally)	Support
Отладка программ (Debug programs)	Администраторы (Administrators)
Принудительное удаленное завершение (Force shutdown from a remote system)	Администраторы (Administrators)
Профилирование загруженности системы (Profile system performance)	Администраторы (Administrators)
Профилирование одного процесса (Profile a single process)	Администраторы (Administrators), Опытные пользователи (Power Users)
Разрешать вход в систему через службу терминалов (Allow logon through Terminal Services)	Администраторы (Administrators), Пользователи удаленного рабочего стола (Remote Desktop Users)

Таблица 8-6. Стандартные права пользователей для рабочих групп и рядовых серверов (*окончание*).

Право пользователя	Назначено группам
Создание журналов безопасности (Generate security audits)	Local Service, Network Service
Создание страничного файла (Create a pagefile)	Администраторы (Administrators)
Увеличение приоритета диспетчирования (Increase scheduling priority)	Администраторы (Administrators)
Управление аудитом и журналом безопасности (Manage auditing and security log)	Администраторы (Administrators)

В табл. 8-7 перечислены возможности, которые можно делегировать другим пользователям и группам. Помните, что учетная запись Администратор (Administrator), учетные записи администраторов и учетные записи групп Администраторы (Administrators), Операторы сервера (Server Operators), Операторы учета (Account Operators), Операторы архива (Backup Operators) и Операторы печати (Print Operators) относятся к записям с ограниченным доступом. Поэтому группа Операторы учета (Account Operators) не может создавать или изменять их.

Стандартные учетные записи групп

Главное свойство стандартных групп — гибкость. Если назначить пользователей в правильные группы, управлять рабочими группами или доменами Windows Server 2003 будет гораздо легче. Однако в таком разнообразии групп понять назначение каждой из них непросто. Мы рассмотрим подробнее группы, используемые администраторами, и неявные группы.

Административные группы

Администратор обладает широким доступом к сетевым ресурсам. Администраторы могут создавать учетные записи, изменять права пользователя, устанавливать принтеры, управлять общими ресурсами и т. п. Основные группы администраторов (табл. 8-8): Администраторы (Administrators), Администраторы домена (Domain Admins) и Администраторы предприятия (Enterprise Admins).

Таблица 8-7. Другие возможности встроенных и локальных групп

Право	Описание	Обычно назначается группам
Изменение членства в группах (Modify the membership of a group)	Добавлять и удалять пользователей из доменных групп	Администраторы (Administrators), Операторы учета (Account Operators)
Назначение прав пользователей (User rights assignment)	Назначать нрава для других пользователей	Администраторы (Administrators)
Переустановить пароли пользователей и установить изменение пароля при **следующей** перезагрузке (Reset user passwords and force password change at next logon)	Сбрасывать пароли учетных записей	Администраторы (Administrators), Операторы учета (Account Operators)
Создание и удаление принтеров (Create and delete printers)	Создавать и удалять принтеры	Администраторы (Administrators), Операторы сервера (Server Operators), Операторы печати (Print Operators)
Создание, удаление и управление группами (Create, delete and manage groups)	Создавать и удалять группы	Администраторы (Administrators). Операторы учета (Account Operators)
Создание, удаление и управление учетными записями пользователей (Create, delete, and manage user accounts)	Администрировать доменные учетные записи пользователей	Администраторы (Administrators), Операторы учета (Account Operators)
Управление принтерами (Manage printers)	Настраивать принтер и управлять очередями печати	Администраторы (Administrators), Операторы сервера (Server Operators), Операторы печати (Print Operators)
Управление ссылками на групповые политики (Manage group policy links)	Применять существующие групповые политики к сайтам, доменам и ОП, для которых у них есть право на запись соответствующих объектов	Администраторы (Administrators)

Таблица 8-7. Другие возможности встроенных и локальных групп *(окончание)*

Право	Описание	Обычно назначается группам
Чтение информации о **всех** пользователях (Read all user information)	Просматривать информацию учетной записи пользователя	Администраторы (Administrators), Операторы сервера (Server Operators), Операторы учета (Account Operators)

Таблица 8-8. Административные группы

Группа	Сетевая среда	Область действия группы	Участники	Администрирование учетной записи группы
Администраторы (Administrators)	Домены Active Directory	Локальная доменная	Администратор (Administrator), Администраторы домена (Domain Admins). Администраторы предприятия (Enterprise Admins)	Администраторы (Administrators)
Администраторы (Administrators)	Рабочие станции, компьютеры вне домена	Локальная	Администратор (Administrator)	Администраторы (Administrators)
Администраторы домена (Domain Admins)	Домены Active Directory	Глобальная	Администратор (Administrator)	Администраторы (Administrators)
Администраторы предприятия (Enterprise Admins)	Домены Active Directory	Глобальная или универсальная	Администратор (Administrator)	Администраторы (Administrators)

Примечание Локальная учетная запись Администратор (Administrator) и глобальные группы Администраторы домена (Domain Admins) и Администраторы предприятия (Enterprise Admins) являются членами группы Администраторы (Administrators). Включение в нее учетной записи Администратор (Administrator) необходимо для доступа к локальному компьютеру. Включение группы Администраторы домена (Domain Admins) позволяет другим администраторам обращаться к системе из любой точки домена. Включение группы Администраторы предприятия (Enterprise Admins) позволяет другим администраторам обращаться к системе из других доменов в том же дереве или лесе. Чтобы предотвратить широкий административный доступ к домену из любой точки предприятия, удалите группу Администраторы предприятия (Enterprise Admins) из локальной группы Администраторы (Administrators).

Администраторы (Administrators) — локальная группа, в зависимости от ее расположения предоставляющая полный административный доступ к отдельному компьютеру или конкретному домену. Чтобы назначить кого-то администратором локального компьютера или домена, достаточно включить его в данную группу. Изменять эту учетную запись вправе только члены группы Администраторы (Administrators).

Глобальная группа Администраторы домена (Domain Admins) призвана помочь в администрировании всех компьютеров в домене. У этой группы есть административный контроль над всеми компьютерами в домене, поскольку по умолчанию она входит в группу Администраторы (Administrators).

Глобальная группа Администраторы предприятия (Enterprise Admins) позволяет администрировать все компьютеры в дереве или лесу. Она имеет административный контроль над всеми компьютерами на предприятии, так как по умолчанию включена в группу Администраторы (Administrators).

Совет В домене Windows Server 2003 локальный пользователь Администратор (Administrator) по умолчанию является членом групп Администраторы домена (Domain Admins) и Администраторы предприятия (Enterprise Admins), т. е. если кто-то войдет на компьютер как администратор и этот компьютер является частью домена, то он получит полный доступ ко всем ресурсам в домене, дереве или лесе. Чтобы избежать этого, удалите локальную учетную запись Администратор (Administrator) из

группы Администраторы домена (Domain Admins) или из группы Администраторы предприятия (Enterprise Admins).

Неявные группы

В Windows Server 2003 есть несколько встроенных системных групп, позволяющих назначить разрешения л конкретных ситуациях. Разрешения лля таких групп обычно определяются неявно, но вы вправе назначать их самостоятельно, когда изменяете объекты Active Directory.

- **Self** — содержит сам объект и позволяет ему изменять себя.
- **Анонимный вход (Anonymous Logon)** — пользователи,обращающиеся к системе через анонимный вход. Применяется для анонимного доступа к таким ресурсам, как Web-страницы на серверах предприятия.
- **Все (Everyone)** — все интерактивные, сетевые, коммутируемые и прошедшие проверку пользователи. Эта группа предоставляет широкий доступ к системным ресурсам.
- **Группа-создатель** (Creator Group) — группа, применяемая для автоматического предоставления разрешений доступа пользователям, которые являются членами той же группы (групп), что и создатель файла или папки.
- **Интерактивные (Interactive)** — пользователи, зарегистрировавшиеся локально. Позволяет разрешить доступ к ресурсу *только локальным* пользователям.
- **Контроллеры** домена **предприятия (Enterprise Domain Controllers)** — контроллеры домена с ролями и обязательствами, действующими на всем предприятии. Включение в эту группу позволяет контроллерам выполнять определенные задачи с использованием транзитивного доверия.
- **Ограниченные (Restricted)** — пользователи и компьютеры с ограниченным доступом. На рядовом сервере или рабочей станции в эту группу включается локальный пользователь из группы Пользователи (Users).
- **Пакетные файлы (Batch)** — пользователи или процессы, обращающиеся к системе как пакетное задание (или через пакетную очередь).
- **Пользователь служб терминалов (Terminal ServerUser)** —пользователи, обращающиеся к системе через службы терминалов.

Позволяет пользователям сервера терминалов обращаться к приложениям сервера и выполнять другие задачи.

- **Прокси (Proxy)** — пользователи и компьютеры, обращающиеся к ресурсам через прокси-сервер (применяется, когда в сети есть прокси-серверы).
- **Прошедшие проверку (Authenticated Users)** — пользователи, обращающиеся к системе через процесс входа. Применяется для организации доступа к общим ресурсам в домене, например к файлам в общей папке, которые должны быть доступны всем сотрудникам организации.
- **Сеть (Network)** — пользователи, обращающиеся к системе через сеть. Позволяет разрешить доступ к ресурсу *только удаленным* пользователям.
- **Система (System)** — сама ОС Windows Server 2003. Используется, когда ОС нужно выполнить функцию системного уровня.
- **Служба (Service)** — службы, обращающиеся к системе. Предоставляет доступ к процессам, выполняемым службами Windows Server 2003.
- **Создатель-владелец (Creator Owner)** — пользователь, создавший данный файл или панку. Применяется для автоматического предоставления разрешений создателю файла или панки.
- Удаленный **доступ (Dial-Up)** — пользователи, обращающиеся к системе через коммутируемое соединение.

Глава 9

Создание учетных записей пользователей и групп

Основной частью работы администратора является создание учетных записей пользователей и групп. Они позволяют Microsoft Windows Server 2003 управлять информацией о пользователях, включая полномочия и права доступа. Для этого предназначены:

- консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers) — средство администрирования учетных записей в домене Active Directory;
- консоль Локальные пользователи и группы (Local Users and Groups) — средство администрирования учетных записей на локальных компьютерах.

В этой главе описано создание учетных записей доменов, локальных пользователей и групп.

Настройка и формирование учетной записи пользователя

Прежде чем создавать учетные записи, вы должны определить политики, которые будете использовать при их настройке в рамках организации.

Политика именования учетных записей

Ключевая политика, которую нужно разработать, — схема именования учетных записей. Учетная запись пользователя имеет *отображаемое* (или *полное) имя* (display name) и *имя для входа* (logon name). Первое видно на экране и применяется в сеансах пользователя. Второе необходимо для входа в домен. Об именах для входа мы кратко говорили в главе 8,

Правила для отображаемых имен

Для учетных записей домена отображаемое имя обычно составляется из имени и фамилии пользователя, но вы можете назначить ему любое строковое значение. При этом соблюдайте следующие правила:

- локальное отображаемое имя должно быть уникальным на индивидуальном компьютере;
- доменные отображаемые имена должны быть уникальными во всем домене;
- отображаемые имена должны содержать не более 64 символов;
- отображаемые имена могут содержать буквенно-цифровые и специальные символы.

Правила имен для входа

Имена для входа назначаются по таким правилам.

- Локальные имена для входа должны быть уникальными на индивидуальном компьютере, а глобальные имена для входа — во всем домене.
- Имена для входа могут содержать до 256 символов, однако имена длиной более 64 символов неудобно использовать.
- Имя для входа, совместимое с Windows NT 4.0 или более ранней версией, дается всем учетным записям и по умолчанию соответствует первым 20 символам имени для входа в Windows. Это имя должно быть уникальным во всем домене.
- Пользователи, входящие в домен с Windows 2000 или поздних версий, могут применять свои стандартные имена для входа как для Windows 2000, так и для Windows NT 4.0 или более ранней версии независимо от рабочего режима домена.
- Имена для входа не могут содержать символов:

  " \ / [ ] : | = , + * ? < >

- Имена для входа могут содержать все другие специальные символы, включая пробелы, точки, тире и символы подчеркивания. Но вообще применение пробелов в именах учетных записей не рекомендуется.

Примечание Хотя Windows Server **2003 хранит имена пользователей в** том регистре, **в котором вы их ввели, от** регистра они не зависят. Так, вы можете **получить** доступ **к учетной запи-**

си Администратор, **введя** «Администратор», «администратор» или «АДМИНИСТРАТОР». Имена пользователей **хранят регистр,** но не чувствительны к нему.

Схемы именования

В небольших организациях стремятся назначить имена для входа, применяя имя или фамилию пользователя. Но в организации любого размера может быть несколько Томов, Диков и Джейн. Поэтому вместо того, чтобы переделывать схему назначения имен для входа, лучше сразу все сделать «по уму». Для назначения имени учетным записям применяйте согласованную процедуру, которая позволит увеличивать вашу базу пользователей, ограничит конфликты имен и гарантирует, что у ваших учетных записей защищенные имена. Имена можно назначать по следующим схемам:

- имя и первая буква фамилии пользователя;
- первая буква имени и фамилия пользователя;
- инициалы и фамилия пользователя;
- инициалы и первые пять букв фамилии пользователя;
- имя и фамилия пользователя.

Примечание В системах, требующих повышенной безопасности, имени для входа можно назначить цифровой код длиной не менее 20 символов. Соединение такого метода назначения имен со смарт-картами и устройствами для их чтения позволяет пользователям быстро войти в сеть. Не беспокойтесь, для пользователей по-прежнему будет отображаться имя, удобное для чтения.

Пароли и политики учетных записей

Для аутентификации доступа к ресурсам сети учетные записи домена используют пароли и открытые сертификаты.

Безопасные пароли

Пароль — это чувствительная к регистру строка до 127 символов длиной для службы каталогов Active Directory и до 14 — для диспетчера безопасности Windows NT. В паролях можно применять буквы, цифры и спецсимволы, Windows Server 2003 сохраняет пароль в зашифрованном виде в базе данных учетных записей.

Однако просто пароль не предотвратит несанкционированного доступа к сетевым ресурсам. Необходимо применять *защищен-*

ные пароли: их труднее разгадать и взломать. Вы затрудните взлом паролей, если будете комбинировать все возможные типы символов, включая буквы верхнего и нижнего регистра, цифры и знаки. Например, вместо строки **happydays** вы можете использовать в качестве пароля **haPPy2Days&**, **Ha**y!dayS** или даже **h*PPY%d*ys**.

К сожалению, не имеет значения, насколько защищенным вы сделали пароль пользователя изначально: со временем пользователь сам выбирает себе пароль. Чтобы он оказался достаточно сложным, вы можете настроить *политики учетных записей* (account policies) — подмножество политик, настраиваемых как групповая политика.

Настройка политик учетных записей

Групповые политики разрешается применять на разных уровнях внутри сетевой структуры. (Об управлении локальными групповыми политиками и глобальными групповыми политиками рассказано в главе 4.)

В контейнере групповой политики вы можете настроить учетные политики.

1. Раскройте узел Политики учетных записей (Account Policies) консоли Групповая политика (Group Policy), как показано на рис. 9-1.

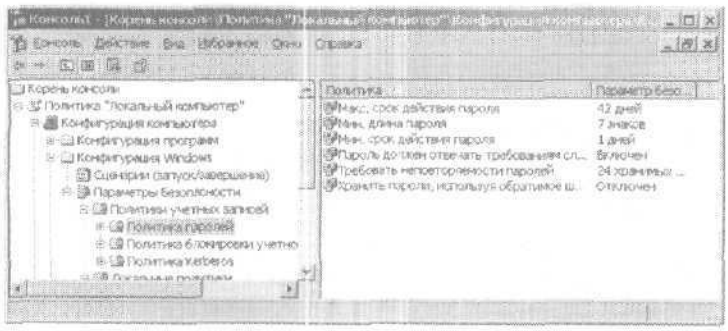


Рис. 9-1. Используйте элементы узла Политики учетных записей (Account Policies) для настройки политик паролей и общих правил использования учетных записей

2. Задайте параметры политик учетных записей в узлах Политика паролей (Password Policy), Политика блокировки учет-

ных записей (Account Lockout Policy) и Политика Kerberos (Kerberos Policy).

Примечание Политики Kerberos не используются на локальных компьютерах. Они доступны только в групповых политиках, которые влияют на сайты, домены и ОП.

3. Для настройки политики дважды щелкните соответствующий элемент или, щелкнув политику правой кнопкой, выберите Свойства (Properties) — откроется окно свойств политики.

   Примерный вид окна свойств локальной политики показан на рис. 9-2. Действующая политика для компьютера в домене отображается, но вы не можете изменить ее. Однако вы вправе корректировать параметры локальной политики для изолированных серверов. В последнем случае пропустите остальные пункты — они применяются для глобальных групповых политик. Окно свойств политики для сайтов, доменов или подразделений показано на рис. 9-3.

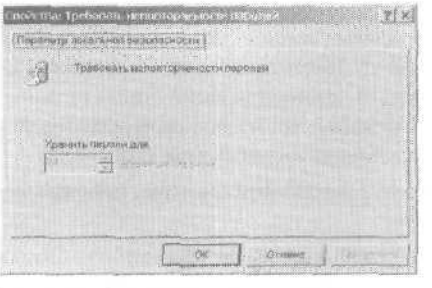


Рис. 9-2. Окно локальных политик позволяет просмотреть действующую политику, так же как и локальную

Рис, 9-3. Создавайте и конфигурируйте глобальные групповые политики из окна свойств

Примечание Политики сайтов, доменов и подразделений имеют приоритет над локальными политиками. Все политики либо определены, либо нет. Политика, не определенная в текущем контейнере, может быть унаследована от другого контейнера.

4. Чтобы включить политику, установите флажок Определить следующий параметр политики (Define this policy setting).

Примечание Некоторые политики имеют отрицательный смысл — их включение означает невозможность выполнения действия. Например, параметр Отказать во входе в качестве службы (Deny log on as a service) является отрицанием параметра Вход в качестве службы (Log on as a service).

О работе с учетными политиками рассказано в разделах «Настройка политики паролей», «Блокировка учетных записей» и «Настройка политики Kerberos» этой главы.

Просмотр действующих политик

При работе с политиками учетных записей и назначением прав пользователей часто необходимо просмотреть **действующую** в системе политику, чтобы выяснить происхождение определенного параметра политики. Действующая политика определяется иерархическим порядком применения политик (см. главу 4).

Политику, действующую на локальной системе, просматривают следующим образом.

1. Щелкните кнопку Пуск (Start) и выберите Выполнить (Run).
2. В поле Открыть (Open) введите mmc и щелкните OK. Откроется пустая консоль MMC.
3. Выберите в меню Файл (File) команду Добавить или удалить оснастку (Add/Remove Snap-In), чтобы открыть одноименное диалоговое окно.
4. На вкладке Изолированная оснастка (Standalone) щелкните кнопку Добавить (Add).
5. В диалоговом окне Добавить изолированную оснастку (Add Standalone Snap-In) щелкните вариант Результирующая политика (Resultant Set of Policy), а затем — Добавить (Add).
6. Щелкните кнопку Закрыть (Close) и затем — OK.
7. Правой кнопкой мыши щелкните узел Результирующая политика (Resultant Set of Policy) и выберите Создать данные

RSoP (Generate RSoP Data). Откроется Мастер результирующей политики (Resultant Set of Policy Wizard). Два раза щелкните Далее (Next).

8. Чтобы просмотреть параметры узла Конфигурация компьютера (Computer Configuration) для локального компьютера, выберите Этот компьютер (This Computer). В противном случае выберите Другой компьютер (Another Computer) и введите его имя. При необходимости щелкните Обзор (Browse), чтобы найти нужную систему. Затем щелкните Далее (Next).
9. Чтобы просмотреть параметры узла Конфигурация пользователя (User Configuration) для текущего пользователя, выберите Текущий пользователь (Current User). В противном случае выберите Другого пользователя (Select a Specific User) и затем выделите учетную запись другого пользователя, зарегистрировавшегося в системе.
10. Два раза щелкните Далее (Next), а затем — Готово (Finish). Теперь, открыв нужный узел консоли Результирующая политика (Resultant Set of Policy), вы увидите текущие параметры соответствующей политики и их источник — объект GPO (рис. 9-4).

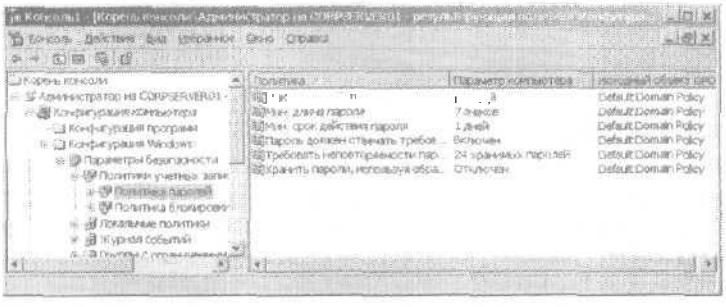


Рис. 9-4. В перечне локальных политик отображаются действующие политики, а также их источник

Настройка политик учетных записей

Как вы уже знаете, существует три типа политик учетных записей: политики паролей, блокировки учетной записи и Kerberos,

Настройка политики паролей

Политики паролей управляют безопасностью паролей и позволяют задать следующие параметры:

- Требовать неповторяемости паролей (Enforce password history);
- Максимальный срок действия пароля (Maximum password age);
- Минимальный срок действия пароля (Minimum password age);
- Минимальная длина пароля (Minimum password length);
- Пароль должен отвечать требованиям сложности (Password must meet complexity requirements);
- Хранить пароль, используя обратимое шифрование (Store password using reversible encryption),

Требование неповторяемости паролей

Эта политика указывает, насколько часто старые пароли разрешено применять повторно. Она также может помешать пользователям менять пароли один на другой из одного общего набора. Windows Server 2003 хранит до 24 паролей для каждого пользователя в предыстории.

Чтобы отключить контроль предыстории, обнулите размер предыстории паролей в поле Хранимых паролей (Passwords Remembered), а чтобы включить — введите количество запоминаемых паролей. С помощью предыстории, уникальной для каждого пользователя, Windows Server 2003 отслеживает старые пароли, и пользователям не разрешается применять заново любой из сохраненных паролей.

Максимальный срок действия пароля

Параметр Макс. срок действия пароля (Maximum Password Age) определяет, как долго пользователи могут применять пароли, прежде чем изменить их. Его применяют, чтобы заставить пользователей периодически изменять свои пароли. Значение этого параметра определяется потребностями вашей сети. Чем важнее для нее безопасность, тем короче должен быть период действия.

Вы можете задать максимальный срок действия пароля от О до 999 дней. О означает, что срок действия пароля не ограничен. При высоких требованиях к безопасности рекомендуется требовать смену пароля каждые 30-90 дней. В остальных случаях — через 120-180 дней.

Примечание Windows Server 2003 уведомляет пользователей, когда срок действия пароля подходит к концу. Когда до конца срока **остается** меньше 30 дней, пользователи при входе

в сеть видят предупреждение о необходимости сменить пароль.

Минимальный срок действия пароля

Параметр Мин. срок действия пароля (Minimum Password Age) определяет, как долго пользователи должны применять пароль, прежде чем смогут изменить его. Он не дает пользователям мошенничать с системой паролей, вводя новый пароль, а затем сразу же изменяя его на старый. Рекомендуемое значение — 3-7 дней. Если минимальный срок действия пароля установлен в ноль, пользователь может изменить свой пароль сразу.

Минимальная длина пароля

Параметр Мин. длина пароля (Minimum Password Length) задает минимальное количество символов для пароля. Если вы до сих пор не изменили значение этого параметра по умолчанию, срочно сделайте это, поскольку в некоторых случаях по умолчанию разрешены пустые пароли (т. е. вход в систему вообще без пароля).

Как правило, длина пароля должна составлять не менее 8 символов. Дело в том, что длинные пароли обычно взломать труднее, чем короткие. Если вы хотите усилить безопасность, задайте минимальную длину пароля в 14 символов (максимально допустимое значение).

Сложность пароля

Помимо основных политик паролей и учетных записей в Windows Server 2003 есть средства дополнительного управления паролями. Они заставляют использовать сложные пароли, которые отвечают следующим требованиям:

- длина пароля не менее 6 символов;
- пароль не должен содержать имени или части имени пользователя;
- в пароле следует применять три из четырех доступных типов символов: буквы нижнего и верхнего регистров, цифры и знаки.

Чтобы эти требования вступили в силу, включите параметр Пароль должен отвечать требованиям сложности (Password must meet complexity requirements).

Хранение паролей с помощью обратимого шифрования

Пароли, хранимые в БД паролей, зашифрованы. Это шифрование обычно необратимо. Чтобы сделать его обратимым (это необходимо в единственном случае: если в вашей организации используются приложения, которым нужно читать пароль), вы можете активировать хранение паролей средствами обратимого шифрования сразу для всех пользователей домена.

Если эта политика включена, пароли можно с тем же успехом хранить в виде простого текста, с соответствующим снижением уровня безопасности. С учетом этого намного более безопасным представляется включение хранения паролей посредством обратимого шифрования для отдельных пользователей, когда это действительно необходимо для их работы.

Блокировка учетных записей

К политикам блокировки учетных записей в домене или на локальной системе относятся:

- Пороговое значение блокировки (Account lockout threshold);
- Блокировка учетной записи на (Account lockout duration);
- Сброс счетчика блокировки через (Reset account lockout counter after).

Максимальное число неудачных попыток

Параметр Пороговое значение блокировки (Account lockout threshold) определяет количество попыток входа и сеть. Установите его значение таким, чтобы оно уравновешивало потребность предотвращения взлома учетной записи с потребностями пользователей, которым не удается сразу получить доступ к своим учетным записям.

Обычно пользователю не удается получить доступ к своей учетной записи, когда он забыл пароль. В этом случае он, разумеется, пытается войти в сеть еще несколько раз. У пользователей рабочих групп могут возникнуть проблемы с доступом на удаленную систему, если их текущий пароль не совпадает с тем, что хранится в удаленной системе. Когда такое происходит, удаленная система может зарегистрировать несколько неправильных попыток входа в сеть еще до того, как пользователь получит приглашение ввести правильный пароль. Дело в том, что Windows Server 2003 пытается войти в удаленную систему автоматически. В среде домена этого обычно не про-

исходит, благодаря функции однократного ввода пароля (Single Log-On).

Возможные значения порога блокировки — от 0 (по умолчанию) до 999. Ноль означает, что учетные записи не будут блокированы в случае неверных попыток входа в сеть. Любое другое значение задает порог блокировки: чем выше его значение, тем выше риск взлома вашей системы. Рекомендуемый диапазон значений для порога — от 7 до 15: это позволяет исключить ошибку пользователя и в то же время помешать взломщикам.

Продолжительность блокировки учетной записи

Параметр Блокировка учетной записи па (Account lockout duration) задает период времени, в течение которого учетная запись будет заблокирована. Возможные значения — от 1 до 99 999 минут. Значение 0 блокирует учетную запись па неопределенное время. Разблокировать ее вправе только администратор. Это предотвращает попытки взломщиков получить доступ к системе повторно и заставляет пользователей, чьи учетные записи заблокированы, искать помощи у администратора. Таким образом, вы можете определить, что пользователь делает неправильно, и помочь ему избежать проблем в дальнейшем.

Примечание Для разблокировки учетной записи откройте окно свойств учетной записи из консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) и на вкладке Учетная запись (Account) сбросьте флажок Учетная запись заблокирована (Account is locked out).

Частота сброса счетчика неудачных попыток

После каждой неудачной попытки входа в сеть Windows Server 2003 увеличивает значение счетчика неправильных попыток входа. Параметр Сброс счетчика блокировки через (Reset account lockout threshold after) определяет, как долго сохраняется значение этого счетчика. В исходное состояние оно возвращается двумя путями: если пользователь вошел в сеть успешно или с момента последней неудачной попытки прошло время, указанное в параметре Сброс счетчика блокировки через (Reset account lockout threshold after).

По умолчанию значение счетчика блокировки сохраняется 1 минуту, но вы можете задать интервал от 1 до 99 999 минут. Как и с порогом блокировки, нужно выбрать значение, которое сбалансирует потребности безопасности и удобства доступа. Рекомендуемое значение — 1-2 часа. Если эта политика не задана или выключена, счетчик обнуляется только при успешном входе пользователя в систему.

Примечание Неправильные попытки входа на рабочую станцию из хранителя экрана, защищенного паролем, не увеличивают значение счетчика. Если вы заблокировали сервер или рабочую станцию, нажав Ctrl+Alt+Delete, неправильные попытки войти в сеть из диалогового окна разблокирования также не считаются.

Настройка политики Kerberos

Протокол Kerberos версии 5 — основной механизм аутентификации в домене Active Directory. Для проверки подлинности пользователей и сетевых служб протокол Kerberos применяет *билеты* (tickets), содержащие зашифрованные данные. Билеты служб необходимы служебным процессам Windows Server 2003, а билеты пользователей — пользовательским процессам.

Вы можете контролировать срок действия билета и возможность его обновления посредством следующих политик:

- Принудительные ограничения входа пользователей (Enforce user logon restrictions);
- Максимальный срок жизни билета службы (Maximum lifetime for service ticket);
- Максимальный срок жизни билета пользователя (Maximum lifetime for user ticket);
- Максимальный срок жизни для возобновления билета пользователя (Maximum lifetime for user ticket renewal);
- Максимальная погрешность синхронизации часов компьютера (Maximum tolerance for computer clock synchronization).

Внимание! Изменять эти параметры должны только администраторы, хорошо знакомые с Kerberos. Неправильная настройка этих параметров порождает серьезные проблемы в сети. Как правило, значения по умолчанию изменять не требуется.

Ограничения входа пользователей

Параметр Принудительные ограничения входа пользователей (Enforce user logon restrictions) гарантирует применение любых ограничений, связанных с учетной записью пользователя. Так, если для пользователя ограничены часы входа в сеть, эта политика реализует это ограничение. По умолчанию этот параметр включен, и следует отключать его только в экстремальных случаях.

Максимальное время жизни билетов

Параметры Максимальный срок жизни билета службы (Maximum lifetime for service ticket) и Максимальный срок жизни билета пользователя (Maximum lifetime for user ticket) задают максимальное время, в течение которого действительны служебные или пользовательские билеты.

Вы можете изменить длительность действия билетов. Для служебных билетов диапазон составляет 0-99999 минут, а для пользовательских — 0-99999 часов. Нулевое значения параметра соответствует неограниченному сроку жизни.

Пользовательский билет, время жизни которого истекло, может быть возобновлен, если это происходит в течение интервала из параметра Максимальный срок жизни для возобновления билета пользователя (Maximum lifetime for user ticket renewal). По умолчанию этот интервал равен 7 дням, допустимый интервал от 0 до 99999 дней. Значение 0 соответствует неограниченному периоду восстановления.

Максимальная погрешность синхронизации часов

Параметр Максимальная погрешность синхронизации часов компьютера (Maximum tolerance for computer clock synchronization) — один из немногих, которые нам, вероятно, понадобится изменить. По умолчанию компьютеры в домене должны быть синхронизированы друг с другом с точностью до 5 минут, иначе аутентификация невозможна. Если у вас есть пользователи, которые входят в домен без синхронизации с сервером времени, задайте значение в интервале 0-99 999.

Настройка политик прав пользователя

В главе 8 мы обсуждали встроенные возможности и права пользователя. Встроенные возможности учетных записей изменять

нельзя, но разрешается управлять правами учетных записей как сделав пользователя членом соответствующей группы или групп, так и настроив их индивидуально.

Примечание Любой член группы, которой назначено определенное право, тоже обладает этим правом.

Права пользователя назначаются через узел Локальные политики (Local Policies) консоли групповых политик. Как и подразумевает имя, локальные политики принадлежат локальному компьютеру, но вы также вправе импортировать их в Active Directory. Локальные политики можно настраивать как часть существующей групповой политики для сайта, домена или подразделения. Тогда они применяются к учетным записям компьютеров в сайте, домене или подразделении.

Политиками прав пользователя управляют так.

1. Раскройте нужный контейнер групповой политики и затем узлы Конфигурация компьютера (Computer Configuration), Конфигурация Windows (Windows Settings), Параметры безопасности (Security Sellings) и Локальные политики (Local Policies).
2. Раскройте узел Назначение прав пользователя (User rights assignments). Для настройки политики щелкните ее дважды или щелкните правой кнопкой и выберите в контекстном меню команду Безопасность (Security).
3. Настройте права пользователя как описано в пп. 1–3 раздела «Локальная настройка прав пользователя» или в пп. 1-6 следующего раздела.

Глобальная настройка прав пользователя

Вы можете настраивать индивидуальные права пользователя на уровне сайта, домена или подразделения.

1. Откройте диалоговое окно свойств для прав пользователя (рис. 9-5). Если эта политика не определена, установите флажок Определить следующие параметры политики (Define this policy setting).

Рис. 9-5. Определите право пользователя, а затем примените его к пользователям или группам

2. Для применения права к пользователю или группе щелкните кнопку Добавить пользователя или группу (Add User or Group). Затем в диалоговом окне Имя группы (Group Name) щелкните кнопку Обзор (Browse) — откроется диалоговое окно Выбор: пользователи, компьютеры или группы (Select Users, Computers, or Groups), показанное на рис. 9-6.

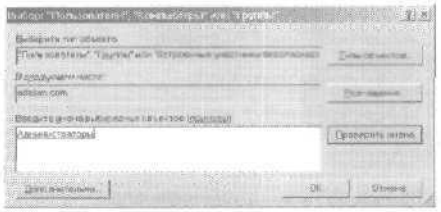


Рис. 9-6. Диалоговое окно Выбор: пользователи, компьютеры или группы (Select Users, Computers, or Groups) позволяет применить права пользователя к пользователям и группам

3. Введите имя пользователя или группы, которое хотите использовать, и щелкните Проверить имена (Check Name). По умолчанию поиск проводится среди встроенных участников безопасности и пользовательских учетных записей. Чтобы добавить в поиск группы, щелкните кнопку Типы объектов (Object Types), выделите Группы (Groups) и щелкните OK.

4. Закончив выбор, щелкните OK. Теперь в окне Добавление пользователей, компьютеров или групп (Add Users, Computers, Or Groups) должны отображаться выбранные учетные записи. Щелкните OK.
5. Диалоговое окно свойств обновится, отображая ваш выбор. Если вы допустили ошибку, выберите имя и удалите его, щелкнув кнопку Удалить (Remove).
6. Щелкните **OK.**

Локальная настройка прав пользователя

На локальных компьютерах права пользователя применяются так.

1. Откройте диалоговое окно свойств, подобное тому, что показано на рис. 9-7.

Рис. 9-7. Определив право пользователя, примените его к пользователям или группам

Примечание Помните, что политики сайтов, доменов или подразделений приоритетнее локальных политик.

2. В диалоговом окне Свойства (Properties) отображаются имена пользователей и групп, которым было дано соответствующее право. Чтобы отменить это назначение, выберите пользователя или группу и щелкните Удалить (Remove).
3. Назначьте право другим пользователям и группам, щелкнув кнопку Добавить пользователя или группу (Add User or Group).

Создание учетной записи пользователя

Вам придется создать учетную запись для каждого пользователя, который хочет обращаться к вашим сетевым ресурсам. Вы можете создать доменную учетную запись в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) или локальную — из консоли Локальные пользователи и группы (Local Users and Groups).

Создание доменной учетной записи пользователя

Создать новые доменные учетные записи можно двумя способами.

- **Создание абсолютно новой учетной записи** пользователя. Щелкните правой кнопкой контейнер, в который вы хотите поместить учетную запись пользователя, выберите в контекстном меню Создать (New), а затем — Пользователь (User). Откроется окно мастера Новый объект — Пользователь (New Object — User), показанное на рис. 9-8. К созданной учетной записи применяются системные параметры по умолчанию.
- **Создание новой учетной записи на основе существующей.** Вызовите контекстное меню правым щелчком учетной записи пользователя, которую хотите скопировать в консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers), и выберите Копировать (Copy). Откроется мастер Копировать объект — Пользователь (Copy Object — User). Созданная копия учетной записи получает большинство значений параметров существующей. О копировании учетных записей рассказано в главе 10.

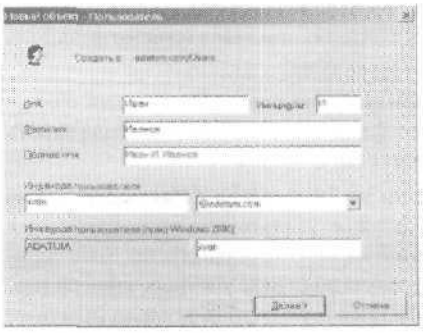


Рис. 9-8. Настройка отображаемого имени и имени для входа

Учетная запись создается с помощью мастеров Новый объект — Пользователь (New Object — User) или Копировать объект — Пользователь (Copy Object — User).

1. Запустите нужный мастер.
2. Введите имя, инициал и фамилию пользователя в соответствующих полях. Эти данные потребуются для создания отображаемого имени пользователя.
3. Отредактируйте полное имя. Оно должно быть уникальным в домене и иметь длину не более 64 символов.
4. Введите имя для входа. С помощью раскрывающегося списка выберите домен, с которым будет связана учетная запись. Это задает полное имя для входа.
5. При необходимости измените имя пользователя для входа в системы с ОС Windows NT 4.0 или более ранними версиями. По умолчанию в качестве имени для входа в системы с предыдущими версиями Windows используются первые 20 символов полного имени пользователя. Это имя также должно быть уникальным в домене.
6. Щелкните Далее (Next). Укажите пароль для пользователя в открывшемся окне (рис. 9-9). Его параметры таковы:
   - Пароль (Password) — пароль учетной записи, соответствующий вашей политике паролей;
   - Подтверждение (Confirm Password) — поле, используемое для подтверждения правильности введенного пароля;
   - Требовать смену пароля при следующем входе в систему (User must change password at next logon) — если этот *флажок* установлен, пользователю придется изменить пароль при следующем входе в систему;
   - **Запретить смену пароля пользователем (User cannot change password)** — если этот флажок установлен, пользователь не может изменить пароль;
   - Срок действия пароля не ограничен (Password never expires) — если этот флажок установлен, время действия пароля для этой учетной записи не ограничено; этот параметр перекрывает доменную политику учетных записей (неограниченный по сроку действия пароль устанавливать не рекомендуется, так как это противоречит самой цели использования паролей);

- **Отключить** учетную **запись** (Account **is disabled)** — если этот флажок установлен, учетная запись не действует; параметр удобен для временного запрета использования кем-либо этой учетной записи.

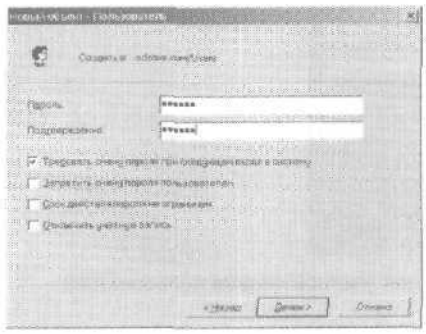


Рис. 9-9. Настройка пароля пользователя

7. Щелкните Далее (Next), а затем Готово (Finish).

Настройка дополнительных параметров учетной записи обсуждается далее в этой главе.

Создание локальных учетных записей пользователя

Локальные учетные записи создаются в консоли Локальные пользователи и группы (Local Users and Groups).

1. Откройте консоль Управление компьютером (Computer Management) с помощью одноименной команды меню Администрирование (Administrative Tools).
2. Щелкните правой кнопкой элемент Управление компьютером (Computer Management) в дереве консоли и выберите Подключиться к другому компьютеру (Connect to Another Computer). Укажите систему, локальными учетными записями которой будете управлять. На контроллерах домена нет локальных пользователей и групп.
3. Разверните узел Служебные программы (System Tools) и выделите Локальные пользователи и группы (Local Users and Groups).
4. Щелкните правой кнопкой элемент Пользователи (Users) и выберите в меню Новый пользователь (New User). Откроется одноименное окно (рис. 9-10) со следующими полями:

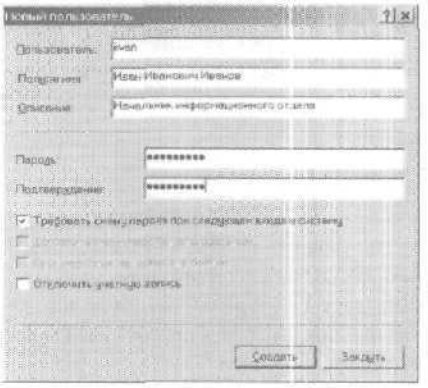


Рис. 9-10. Настройка локальной учетной **записи** пользователя отличается от доменной

- **Пользователь (Username)** — имя для входа учетной записи пользователя; должно соответствовать политике назначения имен локальным пользователям;
- **Полное имя (Full** Name) — полное имя пользователя;
- **Описание (Description)** — дополнительная информация о пользователе (должность, название отдела и т. д.);
- **Пароль (Password)** — пароль; должен соответствовать правилам политики паролей;
- **Подтверждение пароля (Confirm Password) —** поле для подтверждения правильности введенного пароля;
- **Требовать смену пароля при следующем входе в систему (User must change** password **at next logon)** — если отмечено, пользователь должен изменить пароль при следующем входе в систему;
- **Запретить смену пароля пользователем (User cannot change password)** — если отмечено, пользователь не может самостоятельно изменить пароль;
- **Срок действия пароля не ограничен (Password never expires)** — если отмечено, время действия пароля для этой учетной записи не ограничено; этот параметр перекрывает локальную политику учетных записей;
- **Отключить учетную запись (Account is disabled) —** если отмечено, учетная запись заблокирована и не может приме-

няться; это поле удобно для временного запрета использования кем-либо учетной записи.

5. Закончив настройку новой учетной записи, щелкните Создать (Create).

Создание учетной записи группы

Учетные записи групп позволяют управлять привилегиями для нескольких пользователей. Вы можете создавать глобальные учетные записи групп в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers), а локальные — в консоли Локальные пользователи и группы (Local Users and Groups).

Помните, что вы создаете учетные записи групп для сходных типов пользователей. Можно выделить следующие типы групп.

- Группы по отделам организации. Сотрудникам одного отдела обычно требуется доступ к одним и тем же ресурсам. Поэтому вы можете создавать группы для отделов — отдела развития бизнеса, отдела продаж, производственного отдела и т. д.
- Группы по приложениям. Зачастую пользователям нужен доступ к одному приложению и ресурсам для этого приложения. Если вы берете за основу построения групп этот признак, убедитесь, что пользователи получают доступ к необходимым ресурсам и файлам приложения.
- Группы по должностям в организации. Группы можно организовать по должностям пользователей в организации. Так, руководству, вероятно, требуются ресурсы, к которым не обращаются простые пользователи.

Создание глобальной группы

Глобальная группа создается так.

1. Запустите консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers). Щелкните правой кнопкой контейнер, в который хотите поместить учетную запись пользователя. Выберите Создать (New), а затем Группа (Group). Откроется диалоговое окно Новый объект — группа (New Object — Group), показанное на рис. 9-11.

Рис. 9-11. Диалоговое окно Новый объект — группа (New Object — Group) позволяет добавлять новые глобальные группы в домен

2. Введите имя группы. Имена глобальных учетных записей групп следуют тем же правилам, что и отображаемые имена для учетных записей пользователей. Они нечувствительны к регистру и могут содержать до 64 символов.
3. Первые 20 символов имени группы будут соответствовать имени группы в Windows NT версии 4.0 и более ранних версий. Это имя группы должно быть уникальным в домене. Если нужно, измените его.
4. Укажите область видимости группы — Локальная в домене (Domain Local), Глобальная (Global) или Универсальная (Universal).

Примечание Универсальные группы доступны только при работе Active Directory в основном режиме Windows 2000 и Windows Server 2003. Подробнее о режимах — в главе 6.

5. Выберите тип группы: Группа безопасности (Security) или Группа распространения (Distribution).
6. Щелкните OK.

Создание локальных групп и выбор членов группы

Локальные группы создаются в консоли Локальные пользователи и группы (Local Users and Groups).

1. Откройте консоль Управление компьютером (Computer Management) с помощью одноименной команды меню Администрирование (Administrative Tools).

2. Щелкните правой кнопкой элемент Управление компьютером (Computer Management) в дереве консоли и выберите Подключиться к другому компьютеру (Connect to Another Computer). Выберите систему, локальными учетными записями которой будете управлять, На контроллерах домена нет локальных пользователей и групп.
3. Разверните узел Служебные программы (System Tools) и выделите Локальные пользователи и группы (Local Users and Groups).
4. Щелкнув правой кнопкой Группы (Groups), выберите Создать группу (New Group). Откроется диалоговое окно, показанное на рис. 9-12.

Рис. 9-12. Диалоговое окно для создания новой локальной группы

5. Введите имя и описание группы и щелкните кнопку Добавить (Add), чтобы добавить пользователей в группу.
6. В диалоговом окне Выбор: Пользователи (Select Users) введите имя нужного пользователя и щелкните Проверить имена (Check Names). Если совпадения найдены, укажите нужную учетную запись и щелкните OK. Если совпадения не найдены, исправьте введенное имя и выполните поиск снова. При необходимости повторите этот шаг и по окончании щелкните OK.
7. Если вы допустили ошибку, выберите имя пользователя и удалите его, щелкнув кнопку Удалить (Remove).
8. Завершив добавлять или удалять членов группы, щелкните Создать (Create).

Управление членством в глобальных группах

Для настройки членства служит консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers). Работая с группами, помните, что:

- для всех новых пользователей домена основной является группа Пользователи домена (Domain Users), членами которой они становятся при создании их учетной записи;
- для всех новых рабочих станций и серверов домена основной является группа Компьютеры домена (Domain Computers), членами которой они становятся при создании их учетной записи;
- для всех новых контроллеров домена основной является группа Контроллеры домена (Domain Controllers), членами которой они становятся при создании их учетной записи.

Консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers) позволяет:

- включать в группу индивидуальную учетную запись;
- включать в группу сразу несколько учетных записей;
- назначать основную группу для отдельных пользователей и компьютеров.

Выбор группы для учетной записи

Вы можете добавить в группу или удалить из нее учетную запись любого типа.

1. Дважды щелкните имя пользователя, компьютера или группы в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers).
2. В окне свойств выберите вкладку Член групп (Member of).
3. Чтобы сделать учетную запись членом группы, щелкните Добавить (Add). Откроется окно Выбор: Группы (Select Groups). Укажите группы, к которым будет принадлежать текущая учетная запись.
4. Чтобы удалить учетную запись из группы, выберите группу и щелкните Удалить (Remove).
5. Щелкните OK.

Если вы работаете исключительно с пользовательскими учетными записями, вы можете добавить пользователей в группы следующим образом.

1. В консоли Active Directory — пользователи и компьютеры (Active Directory Users And Computers) выделите одну или несколько пользовательских учетных записей (для выделения нескольких записей воспользуйтесь клавишами Ctrl или Shift).
2. Правой кнопкой мыши щелкните выделенные элементы и выберите Добавить в группу (Add To Group) — откроется диалоговое окно Выбор: Группы (Select Groups). Теперь вы можете выбрать группы, членами которых должны быть выделенные учетные записи.
3. Щелкните OK.

Включение в группу нескольких записей

Членством в группе можно управлять и через диалоговое окно свойств группы.

1. Дважды щелкните название группы в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers). Откроется окно свойств группы.
2. Выберите вкладку Члены группы (Members).
3. Для добавления учетных записей в группу щелкните Добавить (Add) и выберите пользователей, компьютеры и группы, которые должны быть членами текущей группы.
4. Для удаления членов группы выберите учетную запись и щелкните Удалить (Remove).
5. Щелкните OK.

Настройка основной группы для пользователей и компьютеров

Основная группа назначается файлам или папкам, созданным пользователями Windows Server 2003 через службы для Macintosh. Все учетные записи пользователей и компьютеров должны иметь основную группу независимо от того, получает учетная запись доступ к системе, работающей под Windows Server 2003, через службы для Macintosh или нет. Эта группа должна быть глобальной или универсальной, как, например, глобальная группа Пользователи домена (Domain Users) или глобальная группа Компьютеры домена (Domain Computers). Основная группа настраивается так.

1. Дважды щелкните имя пользователя или компьютера в окне консоли Active Directory — пользователи и компьютеры

(Active Directory Users and Computers). Откроется окно свойств.

2. Перейдите на вкладку Член групп (Member of).
3. В списке укажите группу с глобальной или универсальной областью видимости.
4. Щелкните кнопку Задать основную группу (Set Primary Group).

Все пользователи должны быть членами хотя бы одной основной группы. Вы не можете отменить членство в основной группе, пока не выберете для пользователя другую основную группу.

1. Выберите в списке другую группу с глобальной или универсальной областью видимости и щелкните кнопку Задать основную группу (Set Primary Group).
2. В этом же списке выберите предыдущую основную группу и щелкните кнопку Удалить (Remove). Теперь членство в группе отменено.

Глава 10

Управление учетными записями пользователей и групп

В идеале хотелось бы создать пользовательские и групповые учетные записи и никогда больше к ним не обращаться. Но в реальности после формирования учетных записей надо потратить немало времени на управление ими.

Информация о пользователе

Пользовательские учетные записи могут содержать подробную информацию о пользователе, доступную каждому внутри доменного дерева или леса. Она понадобится в качестве критерия для поиска пользователей и создания записей в адресной книге.

Настройка контактной информации

Для каждой учетной записи пользователя можно определить информацию о контактах.

1. Щелкните дважды имя пользователя в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers). Откроется диалоговое окно свойств записи.
2. Заполните поля на вкладке Общие (General), показанной на рис. 10-1:
   - **Имя (First Name), Инициалы (Initials), Фамилия (Last Name)** — поля для ввода **имени,** инициалов и **фамилии** пользователя;
   - Выводимое **имя (Display Name)** определяет, как будет отображаться имя пользователя в Active Directory и при входе в систему;
   - **Описание (Description)** — описание пользователя;

- Комната (Office) — расположение пользователя;
- Номер телефона (Telephone Number) — номер основного служебного телефона; чтобы указать другие телефоны, щелкните кнопку Другой (Other);
- Эл. почта (E-Mail) — служебный почтовый адрес пользователя.
- Веб-страница (Web Page) — URL домашней страницы пользователя в Интернете или в интрасети; чтобы указать другие Web-страницы, щелкните кнопку Другой (Other).

Рис. 10-1. На вкладке Общие (General) указывается основная контактная информация пользователя

Совет Чтобы активизировать функции отправки почты и открытия домашней страницы в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers), обязательно заполните поля Эл. почта (E-Mail) и Веб-страница (Web Page).

3. Перейдите на вкладку Адрес (Address). Введите в соответствующие поля рабочий или домашний адрес пользователя.

Примечание Прежде чем вводить домашний адрес пользователя, обсудите этот вопрос с отделом кадров и с юридическим отделом. Неплохо также заручиться согласием самого пользователя.

4. Перейдите на вкладку Телефоны (Telephones). Введите основные номера контактных телефонов пользователя, например домашнего, мобильного или IP-телефона, а также факса и пейджера.
5. Чтобы ввести дополнительные номера, щелкните кнопку Другой (Other), соответствующую типу номера.
6. Перейдите на вкладку Организация (Organization) и введите должность, отдел и название компании.
7. Чтобы указать руководителя пользователя, щелкните кнопку Изменить (Change). После этого запись пользователя отобразится в графе прямых подчиненных в окне со свойствами учетной записи его руководителя.
8. Щелкните Применить (Apply) или OK.

Поиск пользователей и создание записей в адресной книге

Active Directory упрощает задачу поиска пользователей в каталоге и создания записей в адресной книге на основе результатов этого поиска.

1. В классическом меню Пуск (Start) выберите команду Найти (Search), азатем — Людей (For People) и переходите к шагу 2. В упрощенном меню Пуск (Start) щелкните Поиск (Search). В диалоговом окне Результаты поиска (Search Results) щелкните ссылку Другие параметры поиска (Other Search Options), выберите Принтеры, компьютеры и людей (Printers, Computers, or People), а затем — Людей в адресной книге (People In Your Address Book).
2. В диалоговом окне, показанном на рис. 10-2, в списке Место поиска (Look In) выберите Active Directory и введите имя или адрес электронной почты нужного пользователя.
3. Щелкните Найти (Find Now). Если поиск не завершится успехом, введите новые параметры и запустите поиск снова.
4. Щелкните найденную учетную запись правой кнопкой и выберите Свойства (Properties), чтобы посмотреть свойства записи.
5. Чтобы добавить информацию о пользователе в адресную книгу, выберите имя и щелкните Добавить в адр. книгу (Add To Address Book).

Рис. 10-2. Поиск пользователей в Active Directory и создание записей в адресной книге

Параметры среды пользователя

С учетной записью можно связать профиль, сценарий входа в систему и домашнюю папку. Чтобы задать эти параметры, дважды щелкните имя в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) и перейдите на вкладку Профиль (Profile). Заполните следующие поля (рис. 10-3).

Рис. **10-3.** Профиль пользователя задается на вкладке Профиль (Profile)

- Путь к профилю (Profile Path) — путь к профилю пользователя. В профиле содержатся параметры среды пользователя. При каждом входе в систему профиль служит для определения параметров рабочего стола, панели управления, доступа к параметрам меню и приложениям и т. д. Подробнее — в разделе «Управление профилями пользователей».
- Сценарий входа (Logon Script) — путь к сценарию входа, т. с. пакетному файлу, который запускаются всякий раз при входе пользователя в систему. Подробнее — в главе 4.
- Домашняя папка (Home Folder) — папка, где хранятся файлы пользователя. Здесь можно указать как локальный путь, так и общий сетевой ресурс, к которому пользователь сможет обращаться с любого компьютера сети.

Переменные среды

Переменные среды особенно удобны при работе со сценариями входа в систему и служат для хранения информации о путях, которая может время от времени меняться. Вот самые распространенные переменные среды:

- *%SystemRoot%* —основной каталог ОС, например C:\WINNT;
- *%UserName%*— имя пользователя в учетной записи (например, WRSTANEK);
- *%HomeDrive%* - буква диска домашней папки пользователя (например, C:);
- *%HomePath%*— полный путь к домашней папке пользователя без указания диска (например, \users\mkg\georgej);
- *%Processor_Architecture%*— архитектура процессора компьютера пользователя (например, x86).

На рис. 10-4 показан пример использования переменных среди при создании учетных записей, Переменная *% UserName%* позволяет ОС формировать полный путь для каждого пользователя. Таким образом можно назначить нескольким пользователям один и тот же путь, но каждый пользователь будет работать с собственными параметрами.

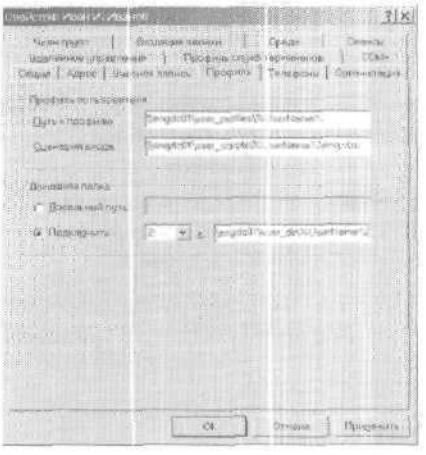


Рис. 10-4. Переменные среды особенно удобны, когда вы создаете учетную запись на основе другой записи

Сценарии входа в систему

Сценарии входа определяют команды, выполняемые при каждом входе в систему. Они позволяют настроить системное время, сетевые принтеры, пути к сетевым дискам и т. д. Сценарии применяются для разового запуска команд; с их помощью не следует изменять переменные среды. Параметры среды, задаваемые сценариями, не сохраняются для последующего использования. Не стоит также применять сценарии входа в систему для автоматического запуска приложений — лучше поместить соответствующие ярлыки в палку Автозагрузка (Startup).

Сценариями входа могут быть:

- файлы сервера сценариев Windows с расширениями .VBS, .JS и др.;
- пакетные файлы с расширением .BAT;
- командные файлы с расширением .CMD;
- программы с расширением .EXE.

Один сценарий применяется как для одного, так и для **нескольких** пользователей; **администратор определяет, с** каким **сценарием** будет **работать конкретный пользователь. Сценарий входа задается так.**

1. В консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) откройте окно свойств пользователя и перейдите на вкладку Профиль (Profile).
2. В поле Сценарий входа (Logon Script) укажите полный путь к сценарию, например \\Zeta\user_logon\eng.vbs.

Примечание Сценарии входа и выхода можно определить иначе. Подробнее — в главе 4.

Практически любая команда, набранная в командной строке, может быть включена в сценарий входа. Стандартная задача, реализуемая в сценариях, — привязка принтеров и сетевых путей с помощью команды NET USE. Вот примеры команд привязки сетевого принтера и дисков:

```
net use lpt1: \\zeta\deskjet
net use g: \\gamma\corp\files
```

Если эти команды записаны в сценарий входа в систему, то сетевой принтер пользователя будет связан с портом LPT1, а сетевой диск получит букву G.

Назначение домашних папок

Windows Server 2003 позволяет назначить каждой учетной записи свою домашнюю папку для хранения и восстановления файлов пользователя. Большинство приложений по умолчанию открывают домашнюю папку для операций открытия и сохранения файлов, что упрощает пользователям поиск своих данных. В командной строке домашняя папка является начальным текущим каталогом.

Домашняя папка может располагаться как на локальном жестком диске пользователя, так и на общедоступном сетевом, Каталог на локальном диске доступен только с одной рабочей станции, к сетевому диску разрешается обращаться с любого компьютера сети.

Совет Несколько пользователей могут иметь одну домашнюю папку, но, как правило, лучше, если у каждого пользователя она будет своя.

Создавать домашнюю папку специально не надо — ее автоматически создает консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers). Но если это сделать не удастся, консоль предложит создать папку вручную.

Чтобы указать локальную домашнюю папку, выполните следующие действия.

1. В консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) откройте окно свойств пользователя и выберите вкладку Профиль (Profile).
2. Щелкните переключатель Локальный путь (Local Path) и введите путь к домашней папке, например **C:\Home\%UserName%**.

Сетевая домашняя папка задается так.

1. В консоли **Active** Directory — пользователи и компьютеры **(Active** Directory Users and Computers) **откройте окно** свойств пользователя и выберите вкладку Профиль (Profile).
2. Щелкните переключатель Подключить (Connect) в области Домашняя папка (Home Folder) и укажите диск для домашней папки. Логично, если на одном диске вы разместите домашние папки для всех пользователей. Убедитесь, что она не будет конфликтовать с текущими локальными или сетевыми дисками.
3. Введите полный UNC-путь к домашней папке, например **\\Gamma\USER_DIRS\%UserName%**. Чтобы обеспечить пользователю доступ к папке с любого компьютера сети, включите *а* путь имя сервера.

Примечание Если домашняя папка не указана, Windows Server 2003 будет использовать локальную домашнюю папку, заданную по умолчанию. Если ОС установлена в режиме обновления, эта папка — \Users\Default, в противном случае — корневой каталог.

Параметры учетных записей

Windows Server 2003 предоставляет несколько способов управления записями пользователей и доступом **пользователей** в сеть. Можно назначить время входа в систему; компьютеры, с которых пользователи могут входить в систему; привилегии коммутируемого доступа и т. д.

Управление временем входа в систему

Windows Server 2003 позволяет настраивать и отслеживать время входа пользователей и систему. Время входа ограничивают для предохранения системы от взлома или иных злоумышленных действий по окончании рабочего дня. В период действия времени входа в систему пользователи могут работать, как обычно:

входить в сеть, обращаться к сетевым ресурсам. Если пользователи находятся в сети и их время входа истекло, выполняется действие, указанное вами в свойствах учетной записи:

- принудительное отключение от всех сетевых ресурсов;
- запрет па новые сетевые соединения без прекращения существующих соединений.

Настройка времени входа в систему

Время входа в систему настраивается так.

1. В копсоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) откройте диалоговое окно свойств пользователя и перейдите на вкладку Учетная запись (Account).
2. Щелкните кнопку Время входа (Logon Hours). В одноименном окне задайте разрешенное и запрещенное время входа в систему (рис. 10-5). В этом диалоговом окне каждый час дня и ночи представлен в виде поля, который можно включить (синий цвет) или выключить (белый цвет).
3. Выделите мышью нужный интервал и установите переключатель в положение Вход разрешен (Logon Permitted) или Вход запрещен (Logon Denied).

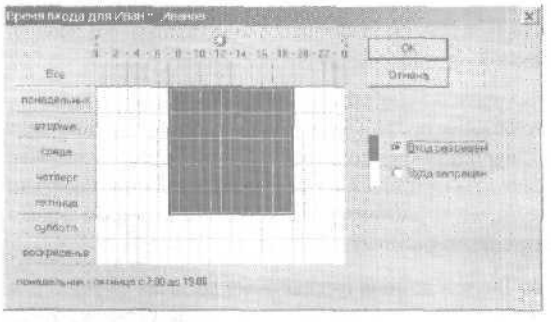


Рис. 10-5. В этом окне конфигурируется время входа в систему

Совет Не слишком усердствуйте в ограничении времени работы пользователей. Помимо стандартного рабочего времени (9-18) добавьте по паре часов до и после рабочего дня. Тогда «жаворонки» смогут раньше входить в систему, а «совы» — продолжать работу после рабочего дня.

Действие по истечении **разрешенного времени входа в** систему

Пользователей, время пребывания в системе которых закончилось, можно отключить.

1. Откройте групповую политику для контейнера, с которым хотите работать.
2. В дереве консоли раскройте узел Конфигурация компьютера\Параметры Windows\Параметры безопасности (Computer Configuration\Windows Settings\Security Settings). Далее раскройте узел Локальные политики (Local Policies) и выберите Параметры безопасности (Security Options).
3. Дважды щелкните политику Сетевая безопасность: Принудительный вывод из сеанса по истечении допустимых часов работы (Network Security: Force Logoff When Logon Hours Expire) — откроется окно ее свойств.
4. Щелкните Включен (Enabled), чтобы активизировать политику, а затем — OK.

Настройка компьютеров, с которых пользователи входят в систему

Вы вправе разрешать или запрещать пользователям работать на определенных компьютерах и входить с них в сеть. На рабочих станциях с Windows Server 2003 пользователям по умолчанию разрешается входить в домен с любого компьютера, по любой действующей учетной записи, включая гостевые.

Разрешая пользователям работать на любой рабочей станции, вы резко снижаете безопасность. Определив список разрешенных рабочих станций, вы закроете потенциальную брешь в защите домена. Теперь хакерам придется отыскивать не только пароль и имя пользователя, но и рабочую станцию, на которой этому пользователю разрешено работать.

Примечание Внутри домена ограничение рабочих станций для входа в систему действует лишь при наличии Windows 2000, Windows NT и Windows XP. На компьютеры с Windows 95 или Windows 98 это ограничение не распространяется: для входа в систему требуется только пароль и имя пользователя.

Рабочие станции для входа в систему задаются так.

1. Раскройте окно свойств пользователя в консоли Active Directory — пользователи и компьютеры (Active Directory

Users and Computers) и перейдите на вкладку Учетная запись (Account).

2. Щелкните кнопку Вход на (Log On To), чтобы открыть диалоговое окно Рабочие станции для входа в систему (Logon Workstations).
3. Установите переключатель Только па указанные компьютеры (The following computers), как показано на рис. 10-6.

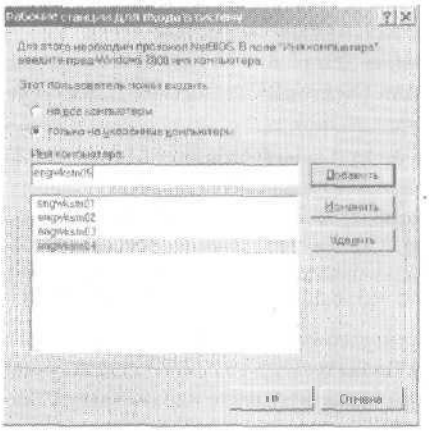


Рис. 10-6. Чтобы ограничить доступ к сети, определите рабочие станции для входа в нее

4. Введите имя рабочей станции и щелкните Добавить (Add). Чтобы указать несколько рабочих станций, повторите эту операцию.
5. Если вы ошиблись при заполнении, выделите ошибочную запись и щелкните Изменить (Edit) или Удалить (Remove).

Настройка привилегий доступа по телефону и через VPN

На вкладке Входящие звонки (Dial-In) окна свойств пользователя можно настроить параметры удаленного доступа к сети, которые управляют подключением к ней по телефону и посредством *виртуальной* частной сети (virtual private network, VPN). По умолчанию привилегии удаленного доступа управляются через Политику удаленного доступа (Remote Access Policy). Можно разрешить или запретить пользователю удаленный и в окне свойств его учетной записи, установив переключатель Разрешить доступ (Allow Access) или Запретить доступ (Deny

Access), как показано на рис. 10-7. В любом случае, прежде чем пользователь сможет получить удаленный доступ к сети, необходимо выполнить следующие действия.

1. Установите Службу удаленного доступа (Remote Access Services) с помощью Мастера настройки сервера (Configure Your Server).
2. В окне редактора групповой политики для нужного сайта, домена или подразделения раскройте узлы Конфигурация пользователя\Административные шаблоны\Сеть (User Configuration\Administrative Templates\Network) и выделите узел Сетевые подключения (Network Connections). Настройте групповую политику.
3. В консоли Управление компьютером (Computer Management) раскройте Службы и приложения (Services and Applications) и выберите Маршрутизация и удаленный доступ (Routing and Remote Access). Включите удаленный доступ, настроив службу Маршрутизация и удаленный доступ (Routing and Remote Access).

Когда пользователь получит разрешение на удаленный доступ к сети, на вкладке Входящие звонки (Dial-In) окна свойств учетной записи нужно настроить дополнительные параметры входящих звонков (рис. 10-7).

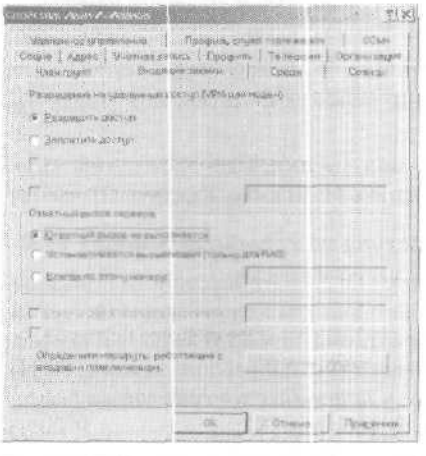


Рис. 10-7. Параметры вызова по телефону регулируют удаленный доступ к сети

1. Если пользователь должен дозваниваться с определенного номера, выберите Проверять код звонящего (Verify Caller-ID), а затем введите номер телефона, с которого пользователь будет входить в систему. При этом ваша телефонная система должна поддерживать функции АОН (автоматического определения номера).
2. Задайте параметры ответного вызова:
   - Ответный вызов не выполняется (No Callback) — пользователь дозванивается, подключается и при необходимости сам оплачивает телефонное соединение;
   - Устанавливается вызывающим (Set by Caller) — сервер узнает номер телефона дозвонившегося пользователя, отключает его и звонит ему сам, при этом телефонное соединение оплачивает компания;
   - Всегда по этому номеру (Always Callback to) — позволяет заранее указать номер ответного вызова с целью повышения безопасности; сервер перезванивает дозвонившемуся пользователю по этому номеру, компания оплачивает телефонное соединение.

Примечание Назначать ответный вызов пользователям, которые дозваниваются через коммутатор, нежелательно. Коммутатор может помешать пользователю правильно подключиться к сети. Также нельзя использовать предварительно назначенные номера ответного вызова на многоканальных линиях. Такие линии не всегда работают надлежащим образом.

3. При необходимости укажите статические IP-адреса и статические маршруты телефонных соединений в полях Статический IP-адрес пользователя (Assign a Static IP Address) и Использовать статическую маршрутизацию (Apply Static Routes). Подробнее — в главе 16.

Настройка параметров безопасности учетной записи

Вкладка Учетная запись (Account) окна свойств пользователя содержит массу параметров, которые применяются для обеспечения безопасности сети и для управления использованием учетных записей:

- Требовать смену пароля при следующем входе в систему (User must change password at next logon) заставляет пользователя сменить свой пароль при следующем входе;

- **Запретить смену пароля пользователем (User cannot change password)** не позволяет пользователю изменять пароль;
- **Срок действия пароля не ограничен (Password never expires)** гарантирует, что срок действия пароля никогда не истечет, т. е. отменяет нормальный срок действия пароля;

Внимание! Выбор этого параметра создает дополнительный риск для безопасности сети. Обычно его назначают для учетной записи администратора, но не для записей пользователей.

- **Хранить** пароль, **используя обратимое шифрование (Store password using reversible encryption)** сохраняет пароль в виде текста, который можно расшифровать;
- **Отключить учетную запись (Account is disabled)** отключает запись, не позволяя пользователю входить в систему и сеть;
- **Для интерактивного входа в сеть** нужна **смарт-карта (Smart card is required for interactive logon)** требует смарт-карту для входа в систему; пользователю не удастся войти в систему, просто набрав имя и пароль;
- **Учетная запись доверена для делегирования (Account is trusted for delegation)** определяет, требуются ли пользователю привилегии управления объектами в Active Directory, а также доверено ли ему выполнять какие-либо действия над объектами, для работы с которыми ему делегированы соответствующие полномочия;

Примечание Не следует доверять делегирование большинству пользователей. Разрешайте это только тем, кому необходимо управлять Active Directory, или пользователям с особыми привилегиями.

- **Учетная запись важна и не может быть делегирована (Account is sensitive and cannot be delegated)** определяет, что пользовательская учетная запись важна и должна управляться с особым тщанием. Пользователю можно ограничить разрешения доступа или запретить ему выполнение определенных действий. Этот параметр предотвращает управление компонентами Active Directory и обычно применяется ко всем учетным записям рядовых пользователей в отличие от полномочных администраторов;
- **Применять DES-шифрование для этой учетной записи (Use DES encryption** types for this **account)** определяет, будет

ли запись пользователя применять стандарт шифрования DES;

- **Без предварительной проверки подлинности Kerberos (Do not require Kerberos preauthentication)** — учетная запись пользователя перед получением доступа к сетевым ресурсам не нуждается в предварительной проверке подлинности Kerberos; вход в систему без такой проверки включается, чтобы идентифицировать пользователей предыдущей или нестандартной версии Kerberos.

Управление профилями пользователей

В профиле *пользователя* содержатся параметры сетевого окружения, например конфигурация рабочего стола и параметры меню. Проблемы, связанные с профилем, могут помешать пользователю войти в систему. Например, если размер экрана, заданный в профиле, не поддерживается системой, на которой он применяется, пользователю не удастся корректно войти в систему. Решить проблемы с профилем не всегда просто — иногда требуется изменить сам профиль.

Windows Server 2003 предоставляет несколько способов управления профилями:

- назначить путь к профилю в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers);
- копировать и удалять локальный профиль, а также изменять его тип из панели управления с помощью значка Система (System);
- задать системные правила, которые не позволят пользователям управлять некоторыми аспектами своего окружения.

Локальный, перемещаемый и обязательный профили

В Windows Server 2003 каждый пользователь обладает профилем. Профили управляют параметрами запуска сеанса пользователя, типами доступных *программ* и приложений, параметрами рабочего стола и т. д. Каждый компьютер, на который входит пользователь, оснащен своей копией профиля пользователя. Профиль хранится на жестком диске; поэтому пользователь, работающий на нескольких рабочих станциях, должен обладать профилем на каждом из них. Другой компьютер сети не может обращаться к профилю, сохраненному локально, или *локальному профилю* (local profile); оче-

видно, что в этом есть свои недостатки. Например, если пользователь работает на трех рабочих станциях, то на каждой системе у него могут быть разные профили. В результате пользователь может запутаться в том, какие сетевые ресурсы доступны ему на каждой из систем,

Чтобы уменьшить путаницу, можно создать профиль, доступный другим компьютерам, — *перемещаемый профиль* (roaming profile). К такому профилю пользователь вправе обращаться с любого компьютера домена. Перемещаемые профили хранятся только на сервере Windows Server 2003. При входе пользователя с перемещаемым профилем в систему создается локальная копия профиля на компьютере пользователя. Когда пользователь выходит из системы, измененный профиль обновляется как на сервере, так и локально.

Примечание Перемещаемые профили совершенно необходимы в организациях, где для защиты данных применяется шифрованная файловая система EFS. Сертификат шифрования, без которого пользователь не получит доступа к файлам, которые он зашифровал, хранится в профиле пользователя. Перемещаемый профиль позволит пользователю работать со своими зашифрованными файлами на других компьютерах.

Администратор может управлять профилями пользователей или позволить им самим распоряжаться своими профилями. Управлять профилями пользователей администратору стоит лишь по одной причине: чтобы убедиться, что у всех пользователей одинаковые параметры сети. Это может уменьшить число проблем, связанных с сетевой средой.

Профили, управляемые администраторами, называются *обязательными* (mandatory). Пользователям с обязательными профилями разрешено производить лишь временные изменения своего окружения, которые не будут сохранены: при следующем входе в систему реализуется первоначальный профиль. Благодаря этому пользователи но смогут произвести необратимых изменений сетевой среды. Главный недостаток обязательных профилей в том, что, если сервер, на котором хранится профиль, недоступен, у пользователя возникнут проблемы со входом в систему. Точнее, если недоступен только сервер, пользователь получит предупреждение, но сможет войти в локальную систему при помощи кэшированного системного профиля. Если не-

доступен и кэшированный профиль, вход в систему окажется невозможным.

Создание локальных профилей

В Windows 2000 и более поздних версиях профили пользователей хранятся в папке по умолчанию или в папке, заданной в поле Путь к профилю (Profile Path) окна свойств пользователя. Стандартное расположение папки профилей зависит от конфигурации рабочей станции.

- ОС Windows установлена в режиме обновления — профиль пользователя расположен по адресу *%SystemRoot%*\Profiles*%UserName%*\NTUSER.DAT, где *%SystemRoot%* - корневой каталог ОС (например, C:\Winnt), а *%UserName%*— имя пользователя.
- ОС Windows установлена в режиме новой установки — профиль пользователя расположен по адресу *%SystemDrive%*\Documents and Settings*%UserName%.%UserDomain%*, например F:\Documents and Settings\wrstanek.adatum\ntuser.dat. На контроллере домена профиль расположен по адресу *%SystemDrive%*\Documentsand Settings*%UserName%*, например F:\Documents and Settings\wrstanek.

Если не изменить каталог по умолчанию, пользователю придется работать с локальным профилем.

Создание перемещаемых профилей

Перемещаемые профили хранятся на серверах Windows Server 2003. Чтобы пользователь имел перемещаемый профиль, его папка должна располагаться на сервере.

1. Создайте общую папку на сервере Windows Server 2003 и убедитесь, что группа Все (Everyone) имеет к пей доступ.
2. В консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) в окне свойств пользователя перейдите па вкладку Профиль (Profile). Введите путь к общей папке в поле Путь к профилю (Profile Path) в виде *имя_сервера**имя_папки_профиля**имя_пользователя*(например, \\Zeta\user_profiles\georgej), где Zeta — имя сервера, user_profiles — общая папка, а georgej — имя пользователя. Перемещаемый профиль будет храниться в файле NTUSER.DATуказанной папки.

Примечание Обычно создавать папку профиля не требуется. Она создается автоматически при входе пользователя в систему.

3. При необходимости создайте профиль пользователя или скопируйте в папку существующий профиль. Если вы этого не сделаете, в следующий раз пользователь войдет в систему по стандартному локальному профилю. Любые изменения этого профиля будут сохранены, когда пользователь выйдет из системы. Таким образом, при очередном входе пользователь получит личный профиль.

Создание обязательных профилей

Обязательные профили хранятся на серверах Windows Server 2003. Чтобы назначить пользователю обязательный профиль, сделайте так.

1. Выполните пункты 1 -2 предыдущего раздела.
2. Переименуйте файл NTUSER.DAT в *%UserName%*\NTUSER.MAN. Теперь при следующем входе в систему пользователь будет обладать обязательным профилем.

Примечание Файл NTUSER.DAT содержит пользовательские параметры системного реестра. Замена расширения файла на NTUSER.MAN заставляет Windows Server 2003 создавать обязательный профиль.

Управление локальными профилями из окна свойств системы

Для управления системными профилями нужно войти на компьютер пользователя и дважды щелкнуть значок Система (System) в Панели управления (Control Panel). Чтобы просмотреть текущий профиль, перейдите на вкладку Дополнительно (Advanced) и щелкните кнопку Параметры (Settings) в области Профили пользователей (User Profiles).

В окне Профили пользователей (User Profiles) отражена информация обо всех профилях на локальной системе (рис. 10-8). Поля имеют следующие значения.

- **Имя (Name)** — имя локального профиля, обычно содержащее имя домена или компьютера и имя записи пользователя. Например, имя webatwork\wrstanek означает, что первоначальный профиль получен от домена webatwork, а запись пользователя — wrstanek.

Примечание Если удалить учетную запись, не удаляя соответствующий профиль, можно увидеть строку Запись удалена (Account Deleted) или Неизвестная запись (Account Unknown). Не беспокойтесь, профиль все еще доступен для копирования.

- **Размер (Size)** - размер профиля. Обычно чем больше файл профиля, тем больше параметров окружения настроил пользователь.
- **Тип (Type)** — тип профиля: локальный или перемещаемый.
- **Состояние (Status)** — текущее состояние профиля.
- **Изменен (Modified)** — дата последнего изменения профиля.

Рис. 10-8. В окне Профили пользователей (User Profiles) можно управлять локальными профилями

Создание профиля вручную

Чтобы создать профиль вручную, надо войти в систему но учетной записи пользователя, полностью настроить среду и выйти. Так как *это* занимает много времени, лучше создать базовую запись пользователя, настроить ее среду, а затем применять ее как основу для других записей.

Копирование профиля в новую учетную запись пользователя

Чтобы скопировать существующий профиль в новую учетную запись, воспользуйтесь окном свойств системы.

1. Щелкните дважды значок Система (System) в панели управления и перейдите па вкладку Дополнительно (Advanced). Затем щелкните кнопку Параметры (Settings) в области Профили пользователей (User Profiles).
2. В списке Профили, хранящиеся на этом компьютере (Profiles stored on this computer) выделите профиль, который нужно скопировать.
3. Щелкните кнопку Копировать (Copy To) и введите путь к новой папке профиля в поле Копировать профиль па (Copy Profile To), как показано на рис. 10-9. Например, если вы создали профиль для пользователя georgej, введите \\Zeta\user_profiles\georgej.

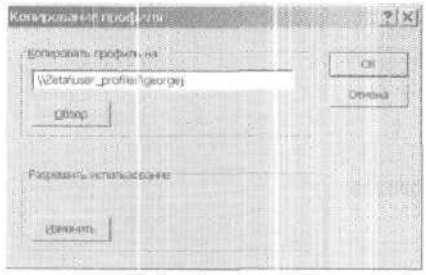


Рис. 10-9. Диалоговое окно Копирование профиля (Copy To) позволяет ввести адрес папки профиля и разрешить ее использование определенному пользователю

4. Теперь нужно открыть пользователю доступ к профилю. Щелкните кнопку Изменить (Change) в области Разрешить использование (Permitted to use) и в диалоговом окне Выбор: Пользователь или группа (Select User Or Group) укажите учетную запись пользователя.
5. Щелкните OK, и Windows Server 2003 скопирует профиль в новый каталог.

Замена одного профиля другим

При работе с, рабочими группами, в которых каждый компьютер управляется независимо, приходится часто копировать профиль пользователя с одного компьютера на другой. Копирование профилей позволяет пользователям работать с едиными параметрами среды на разных компьютерах. Естественно, в домене Windows Server 2003 для реализации этой возможности предназначены

перемещаемые профили. Но даже и в этом случае иногда может понадобиться скопировать существующий локальный профиль поверх перемещаемого профиля пользователя (когда перемещаемый профиль поврежден) или в перемещаемый профиль другого домена.

Копирование профиля поверх существующего производится точно так же, как описано в предыдущем разделе. Разница лишь в том, что в пункте 3 вы вводите путь не к повой, а к уже существующей папке профиля. Когда вы щелкнете ОК в диалоговом окне Копирование профиля (Copy To), на экране появится предупреждение о том, что текущее содержимое папки будет удалено. Щелкните Да (Yes).

Удаление локального профиля и назначение нового

В Windows Server 2003 пользователи, не имеющие перемещаемых профилей, работают с локальными профилями. Кроме того, локальный профиль применяется, если у него более поздняя дата изменения, чем у перемещаемого. В некоторых обстоятельствах локальный профиль приходится удалять, например, если он поврежден. Делается это так.

1. Войдите на компьютер пользователя.
2. Щелкните дважды значок Система (System) в панели управления и перейдите на вкладку Дополнительно (Advanced). Затем щелкните кнопку Параметры (Settings) в области Профили пользователей (User Profiles).
3. Выделите удаляемый профиль и щелкните Удалить (Delete). Затем щелкните Да (Yes).

Примечание Нельзя удалить применяемый профиль. Если пользователь работает на локальной системе (компьютер, с которого вы удаляете профиль), то ему следует выйти из системы, Иногда Windows Server 2003 помечает профили как занятые, хотя на самом деле это не так. Обычно это происходит в результате некорректного изменения среды пользователя. Чтобы исправить эту ошибку, перезагрузите компьютер.

При следующем входе пользователя в систему Windows Server 2003 произведет одну из двух операций: предоставит пользователю локальный профиль системы по умолчанию или найдет перемещаемый профиль пользователя на другом компьютере. Если ни тот, пи другой варианты вас не устраивают, сделайте следующее:

- скопируйте **существующий** профиль в папку профиля **пользователя** (подробнее об этом — в следующем разделе);
- обновите параметры профиля пользователя в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers).

Изменение типа профиля

В окне свойств системы можно изменить тип перемещаемого профиля. Чтобы сделать это, выделите профиль и щелкните кнопку Сменить тип (Change Type). Параметры диалогового окна позволяют:

- **сделать** перемещаемый профиль **локальным**, чтобы пользователь всегда работал па этом компьютере с локальным профилем (исходный перемещаемый профиль остается неизменным);
- **сделать** локальный профиль перемещаемым. Это возможно только в случае, если профиль пользователя изначально был перемещаемым, а затем его преобразовали в локальный.

Примечание Недоступность этих параметров означает, что профиль пользователя изначально определен как локальный.

Обновление учетных записей пользователей и групп

Консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers) позволяет обновить доменную учетную запись пользователя или группы. Для обновления локальной учетной записи пользователя или группы предназначена оснастка Локальные пользователи и группы (Local Users and Groups).

Когда вы работаете е Active Directory, вам иногда требуется полный список учетных записей, например, чтобы найти в нем тех пользователей, которые перестали работать в компании, и отключить их учетные записи. Это можно сделать так.

1. В консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) правой кнопкой мыши щелкните имя домена и выберите Найти (Find). .
2. В списке Найти (Find) выберите вариант Пользовательский поиск (Custom Search). В диалоговом окне Поиск (Find) появится вкладка Пользовательский поиск (Custom Search).

3. В списке В (In) задайте область поиска. Для поиска по всему каталогу выберите Целиком Active Directory (Entire Directory).
4. Щелкните кнопку Поле (Field), раскройте подменю Пользователь (User) и выберите Имя входа (пред-Windows 2000) [Logon Name (Pre-Windows 2000)].

Примечание Убедитесь, что выбираете именно вариант Имя входа (пред-Windows 2000) [Logon Name (Pre-Windows 2000)] — у учетной записи пользователя может не оказаться имени для входа в Windows Server 2003, но имя входа для предыдущих версий Windows есть всегда.

5. В списке Условие (Condition) выберите вариант Присутствует (Present) и щелкните Добавить (Add). При необходимости щелкните Да (Yes).
6. Щелкните Найти (Find Now). В нижней части окна появится список всех пользователей из консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers).
7. Выделите одну или несколько учетных записей, при необходимости воспользовавшись клавишами Ctrl и Shift.
8. Правой кнопкой мыши щелкните выделенные записи и выберите в контекстном меню нужное действие, например Отключить учетную запись (Disable Account).

Примечание С несколькими учетными записями вы можете выполнить следующие действия: добавить их в группу, включить, отключить, удалить и переместить.

Точно таким же образом можно получить список компьютеров, групп или других ресурсов Active Directory.

В следующих разделах рассматриваются другие способы редактирования (переименования, копирования, удаления и включения) учетных записей. Вы также узнаете, как изменить и переустановить пароли и устранять проблемы со входом в систему.

Переименование учетных записей пользователей и групп

1. Раскройте консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers) или Локальные пользователи и группы (Local Users and Groups) и найдите нужную учетную запись.

2. Щелкните ее правой кнопкой, **выберите Переименовать** (Rename) и **введите новое имя.**

Идентификаторы SID

При переименовании учетной записи пользователя ей назначается новое имя. Имена пользователей облегчают управление учетными записями, но реально для идентификации, контроля и обработки учетных записей Windows Server 2003 применяет дескриптор безопасности SID, не зависящий от имени пользователя. SID — уникальный идентификатор, генерируемый при создании учетной записи.

Поскольку для идентификации записи необходимо не ее имя, а SID, при переименовании записи вам не придется заново задавать ее разрешения и привилегии. Windows Server 2003 просто связывает старый STD с новым именем.

Частая причина переименования учетной записи — изменение фамилии пользователя. Например, если Линда Мартин (lindam) вышла замуж, став Линдой Робертс, и захотела изменить свое пользовательское имя на lindar, вы просто переименовываете пользователя lindani в lindar. Все связанные с именем lindam привилегии и разрешения сохранятся и за именем lindar. Если раньше lindam имела доступ к файлу, то теперь доступ открыт для lindar, а имя lindam будет исключено из списка доступа.

Изменение другой информации

Одним только переименованием изменение свойств учетной записи может не ограничиться. Вы вправе изменить следующие параметры:

- Выводимое имя (Display Name);
- Путь к профилю (UserProfile Path);
- Сценарий входа (Logon Script Name);
- Домашняя папка(Home Directory).

Примечание Если пользователь работает в системе, изменение информации, связанной с папками и файлами, может породить определенные проблемы. Поэтому обновление информации лучше производить в нерабочее время или попросить пользователя выйти из системы на некоторое время, а затем вновь войти.

Копирование доменных учетных записей пользователей

Создавать новые доменные учетные записи «на пустом месте» довольно утомительно. В качестве отправной точки можно взять уже существующую запись.

1. Откройте консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers), щелкните правой кнопкой запись, которую нужно скопировать, и выберите Копировать (Copy). Откроется окно Копировать объект — Пользователь (Copy Object — User).
2. Задайте параметры новой учетной записи. Затем при необходимости исправьте свойства, перенесенные из исходной записи.

При копировании учетной записи консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers) переносит в копию не всю информацию из исходной учетной записи, пропуская данные, которые так или иначе потребуют обновления. К сохраняемым свойствам относятся:

- город, область, индекс и страна на вкладке Адрес (Address);
- отдел и компания на вкладке **Организация (Organization);**
- параметры записи, заданные на вкладке Учетная запись (Account);
- допустимое время и рабочие станции для входа в систему;
- срок действия учетной записи;
- членство в группах;
- параметры профиля;
- параметры доступа по телефону.

Примечание Если для определения параметров профиля исходной учетной записи вы использовали переменные среды, то они будут применяться и в копии учетной записи. Например, если переменная в исходной записи — *%UserName%*, то она же будет применяться и в ее копии.

Удаление учетных записей пользователей и групп

Удалив учетную запись, нельзя создать новую с таким же именем для получения тех же полномочий, поскольку SID новой записи не будет совпадать с SID старой.

Windows Server 2003 не позволяет удалять встроенные учетные записи пользователей и групп, так как их удаление может серьезно повлиять на домен. Чтобы удалить учетные записи других типов, надо выбрать их и нажать клавишу Delete, либо щелкнуть их правой кнопкой и выбрать Удалить (Delete), щелкнуть OK, а затем Да (Yes).

Примечание При удалении учетной записи Windows Server 2003 не удаляет профиль пользователя, личные файлы и домашнюю папку. Их зам придется удалить вручную. Если вам часто приходится выполнять эту задачу, создайте сценарий Windows, который будет осуществлять все необходимые действия. Однако не забудьте сохранить файлы и данные, которые могут понадобиться впоследствии.

Изменение и переустановка пароля

Администратору приходится часто изменять или обнулять пароли пользователей. Обычно это требуется, когда пользователь забывает свой пароль или когда время действия пароля истекло.

1. Откройте консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers) или Локальные пользователи и группы (Local Users and Groups) в зависимости от типа учетной записи.
2. Щелкните правой кнопкой имя записи и в контекстном меню выберите Смена пароля (Reset Password) или Задать пароль (Set Password).
3. Введите новый пароль пользователя и подтвердите его. Пароль должен соответствовать набору правил паролей компьютера или домена.
4. Дважды щелкните имя пользователя и при необходимости сбросьте флажок Отключить учетную запись (Account is disabled) или Заблокировать учетную запись (Account is locked out). Эти флажки располагаются на вкладке Учетная запись (Account).

Включение учетных записей пользователей

Учетные записи пользователей могут быть отключены по нескольким причинам: пользователь забыл пароль и пытался угадать его; пользователь нарушил правила учетной записи; другой администратор отключил учетную запись на время отпуска пользователя; закончился срок действия учетной записи.

Включение отключенной учетной записи

Если учетная запись отключена, для ее включения выполните следующие действия.

1. Откройте консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers) или Локальные пользователи и группы (Local Users and Groups) в зависимости от типа учетной записи.
2. Дважды щелкните имя пользователя и сбросьте флажок Отключить учетную запись (Account is disabled). Этот флажок находится на вкладке Учетная запись (Account).

Включение заблокированной учетной записи

Если учетная запись заблокирована, для ее включения выполните следующие действия.

1. Откройте консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers) или Локальные пользователи и группы (Local Users and Groups) в зависимости от типа учетной записи.
2. Дважды щелкните имя учетной записи пользователя и снимите флажок Заблокировать учетную запись (Account is locked out). Этот флажок находится на вкладке Учетная запись (Account).

Примечание Если учетные записи блокируются слишком часто, скорректируйте правила учетных записей в домене: увеличьте количество допустимых попыток входа в систему и сократите продолжительность хранения счетчика неудачных попыток. О настройке политики учетной записи — в главе 9.

Включение просроченной учетной записи

В отличие от локальных учетных записей доменные учетные записи имеют ограниченный срок действия. Если срок действия учетной записи истек, сделайте так.

1. Откройте консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers).
2. Дважды щелкните имя учетной записи пользователя и перейдите на вкладку Учетная запись (Account).
3. В области Срок действия учетной записи (Account Expires) выберите Истекает (End Of) и раскройте список. Появится календарь, в котором можно назначить новый срок действия.

Управление несколькими учетными записями пользователей

С помощью консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) вы можете одновременно изменить свойства нескольких учетных записей. Вот что для этого нужно сделать:

- чтобы «поштучно» выбрать для редактирования несколько имен пользователей, нажмите клавишу Ctrl и, не отпуская ее, щелкните все нужные учетные записи;
- чтобы выбрать для редактирования несколько последовательных имен пользователей, нажмите клавишу Shift и, не отпуская ее, щелкните сначала первую, а затем последнюю запись диапазона.

Выделив все нужные учетные записи, щелкните их правой кнопкой мыши, чтобы открылось контекстное меню. Вам доступны следующие возможности:

- **Добавить в группу (Add to a Group) — открывает диалоговое** окно Выбор: Группа (Select Group); в нем можно выбрать группу, членами которой должны стать выделенные записи;
- **Отключить учетную запись (Disable Account) — выключает все** выделенные учетные записи;
- **Включить учетную запись (Enable Account) — включает все выделенные учетные** записи;
- **Переместить (Move) — перемещает выделенные учетные записи в новый** контейнер или **ОП;**
- **Свойства (Properties)** — позволяет **конфигурировать ограниченный** набор свойств для нескольких учетных записей.

Подробно мы остановимся только на последней возможности. Как видно из рис. 10-10, интерфейс диалогового окна Свойства множественных объектов (Properties On Multiple Objects) отличается от стандартного диалогового окна свойств учетной записи (рис. 10-1). Обратите внимание на следующие изменения:

- поля для ввода имени учетной записи и пароля недоступны. Однако вы вправе задать имя домена DNS (суффикс UPN), время входа, разрешенные компьютеры, параметры учетной записи, срок действия учетной записи и параметры профиля;

- вы должны с помощью флажков указать поля, с которыми хотите работать. После этого введенное в поле значение применяется ко всем выделенным учетным записям.

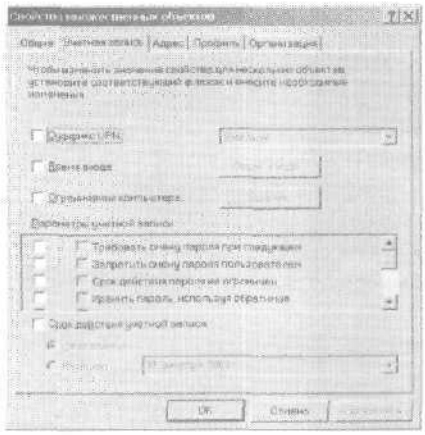


Рис. 10-10. При работе с несколькими учетными записями диалоговое окно свойств учетной записи выглядит иначе

Настройка параметров профиля для нескольких учетных записей

Для настройки информации о профилях служат параметры вкладки Профиль (Profile) окна свойств учетной записи. Выделив несколько учетных записей, вы сможете настроить их профили с помощью одного интерфейса, как правило, воспользовавшись для этого переменной среды *%UserName%*, которая позволяет назначать пути и имена файлов на основе индивидуальных имен пользователей. Например, если вы назначите группе учетных записей сценарий входа с именем *%UserName%*.cmd, Windows заменит переменную именем учетной записи для каждого пользователя, с которым вы работаете. Таким образом, пользователям bobs, janew и ericl будут назначены уникальные сценарии входа Bobs.cmd, Janew.cmd и Ericl.cmd.

Пример назначения информации о профиле среды для нескольких учетных записей показан на рис. 10-11. Обратите внимание на использование переменной *%UserName%* для назначения пути профиля пользователя, имени сценария входа и домашней панки.

Разумеется, использование переменной *%UserName%* не обязательно. В ряде случаев действительно требуется назначить

псем пользователям один и тот же путь к профилю, например при использовании обязательных профилей, или один и тот же сценарий входа.

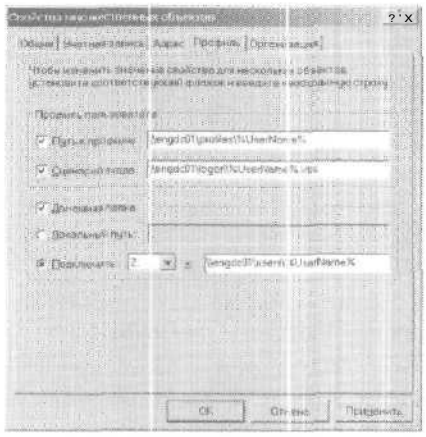


Рис. 10-11. С помощью переменной среды *%UserName%* назначают пути и имена файлов, основанные на именах пользователей

Назначение времени входа для нескольких учетных записей

1. Выделите нужные учетные записи в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers).
2. Щелкните выделенные записи правой кнопкой мыши и выберите Свойства (Properties). В открывшемся диалоговом окне перейдите на вкладку Учетная запись (Account).
3. Установите флажок Время входа (Logon Hours) и щелкните кнопку Время входа (Logon Hours). Задайте допустимое время входа (подробнее — в разделе «Настройка времени входа в систему» этой главы).

Примечание Имейте в виду, что при выделении нескольких учетных записей в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) вы не увидите, какие времена входа были назначены им до этого. И консоль не предупредит вас, что назначаемое вами время входа отличается от предыдущих параметров.

Настройка разрешенных рабочих станций для нескольких учетных записей

Настроить разрешенные рабочие станции для нескольких учетных записей можно в диалоговом окне Рабочие станции для входа в систему (Logon Workstations). Делается это следующим образом.

1. Выделите нужные учетные записи в консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers).
2. Щелкните выделенные записи правой кнопкой мыши и выберите Свойства (Properties). В открывшемся диалоговом окне перейдите на вкладку Учетная запись (Account).
3. Установите флажок Ограничения компьютера (Computer Restrictions) и щелкните кнопку Вход на (Log On To).
4. Чтобы разрешить пользователям регистрироваться на всех рабочих станциях, установите переключатель На все компьютеры (All Computers). Чтобы разрешить использование лишь некоторых рабочих станций, щелкните переключатель Только на указанные компьютеры (The Following Computers) и введите имена до восьми рабочих станций. Когда вы щелкнете OK, эти параметры будут применены ко всем выделенным учетным записям.

Настройка свойств входа, пароля и срока действия для нескольких учетных записей

Параметры, управляющие процессом входа, паролями и сроком действия записи, задаются на вкладке Учетная запись (Account) диалогового окна свойств учетной записи. Когда вы работаете с несколькими учетными записями, вы должны установить на этой вкладке соответствующий флажок в крайнем левом столбце, а затем сделать следующее:

- установите флажок во втором слева столбце, чтобы включить параметр. Например, если вы установите *оба* флажка параметра Срок действия пароля неограничен (Password Never Expires), для указанных пользователей срок действия пароля истекать не будет;
- не устанавливайте флажок во втором слева столбце, чтобы отключить параметр. Например, если вы включите крайний левый флажок для параметра Отключить учетную запись (Account is disabled), а второй слева флажок оставите пус-

тым, учетные записи для выбранных пользователей будут включены.

Чтобы задать срок действия выбранных учетных записей, установите флажок Срок действия учетной записи (Account Expires), а затем укажите соответствующее значение срока действия. Переключателем Не ограничен (Never) вы удалите все существующие ограничения на сроки действия выделенных учетных записей.

Решение проблем со входом в систему

Кроме типичных причин отключения учетной записи, доступу также мешают некоторые некорректно настроенные системные параметры.

- Пользователь не может интерактивно войти в систему. Для данного пользователя не задано право локального входа в систему, и он не является членом группы, обладающей таким правом.

  Пользователь, вероятно, пытается войти на сервер или контроллер домена. Помните, что в домене право локального входа распространяется на все контроллеры домена. Вне домена это право применимо к отдельной рабочей станции. Если пользователю действительно необходим локальный доступ к системе, задайте право пользователя Локальный вход в систему (Logon Locally), как описано в главе 9.

- **Пользователь получил сообщение о том, что система запретила** ему вход. Проверив правильность имени и пароля, убедитесь, что пользователь работает с учетной записью нужного вида. Пользователи иногда пытаются получить доступ к домену через локальную учетную запись. Если проблема не в этом, возможно, недоступен сервер глобального каталога, в результате чего в систему могут входить лишь пользователи с привилегиями администраторов.

- Недоступен компьютер, на котором хранится обязательный профиль пользователя. При входе в систему компьютер, на котором хранится обязательный профиль пользователя, обязательно должен быть доступен.

- Пользователь получил сообщение, что его учетной записи запрещен вход на данную рабочую станцию. Если пользователю необходим доступ к этой рабочей станции, включите ее в спи-

сок разрешенных компьютеров (см. раздел «Настройка компьютеров, с которых пользователи входят в систему»).

Дополнительные разрешения Active Directory

Как вы уже знаете, учетные записи пользователей, групп и компьютеров представлены в Active Directory как объекты. С ними сопоставлены стандартные и расширенные разрешения безопасности, посредством которых вы предоставляете или запрещаете доступ к объектам. Ознакомиться с дополнительными разрешениями безопасности для объектов можно, выполнив следующие действия.

1. Запустите консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers). В меню Вид (View) включите команду Дополнительные функции (Advanced Features) — выберите ее, если возле нее не стоит галочка. Если галочка уже проставлена, делать с командой ничего не нужно.
2. Раскройте нужный контейнер, правой кнопкой мыши щелкните учетную запись пользователя, группы или компьютера, с которой хотите работать, и выберите в контекстном меню команду Свойства (Properties).
3. Перейдите на вкладку Безопасность (Security) диалогового окна свойств учетной записи и выделите пользователя, группу или компьютер, разрешения которых хотите просмотреть. Если флажки затемнены, разрешения наследуются от родительского объекта.

Основные сведения о дополнительных разрешениях

Дополнительные разрешения для объектов Active Directory не так очевидны, как другие разрешения. В частности, они могут быть уникальными для объектов данного типа или для данного контейнера.

Чтобы настроить дополнительные разрешения для объектов Active Directory, выполните следующие действия.

1. Запустите консоль Active Directory — пользователи и компьютеры (Active Directory Users and Computers) и правой кнопкой мыши щелкните учетную запись пользователя, группы или компьютера, с которой хотите работать.

Внимание! Управлять дополнительными разрешениями объектов должны только опытные администраторы, детально раз-

бирающиеся в Active Directory. Некорректная настройка дополнительных разрешений объектов может стать источником проблем, которые очень трудно выявить.

2. Выберите в контекст ном меню команду Свойства (Properties) и перейдите на вкладку Безопасность (Security) диалогового окна свойств учетной записи (рис. 10-12).

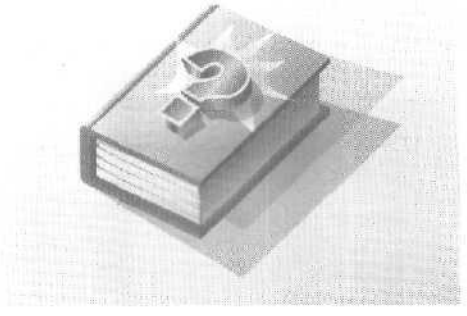
Рис. 10-12. В этом окне настраиваются разрешения объектов

3. Выберите пользователя или группу и задайте или отмените соответствующие разрешения в списке Разрешения для (Permissions for). Флажки унаследованных разрешений затемнены. Чтобы отказаться от наследования, задайте противоположное по смыслу разрешение.
4. Чтобы настроить доступ к разрешениям для пользователей, компьютеров или групп, которые не указаны в окне, щелкните кнопку Добавить (Add).
5. Введите имя пользователя, компьютера или группы и щелкните OK. Затем в списке Разрешения для (Permissions for) задайте или отмените разрешения. При необходимости повторите эти действия для других пользователей, компьютеров или групп.
6. Щелкните OK.

Часть III

Управление данными в Microsoft Windows Server 2003

Третья часть книги посвящена управлению данными в Microsoft Windows Server 2003. В главе 11 объясняется процедура добавления жестких дисков в систему и их разбиения на разделы. Затем обсуждаются типичные задачи по обслуживанию файловых систем и дисков. В главе 12 рассматриваются средства управления наборами томов и RAID-массивами, а также восстановление поврежденных массивов. В главе 13 речь идет об управлении файлами и папками. Из главы 14 вы узнаете, как открыть совместный доступ к файлу, диску или папке для пользователей сети и Интернета. В этой же главе обсуждаются теневые копии, разрешения файлов и папок, аудит и квотирование диска. Глава 15 посвящена архивации и восстановлению данных, в ней объясняется, как организовать пул носителей.



Глава 11

Управление файловыми системами и дисками

Жесткий диск — самое распространенное устройство хранения данных на сетевых рабочих станциях и серверах. На жестких дисках пользователи хранят текстовые документы, электронные таблицы и другие данные. Диски организованы в файловые системы, к которым пользователи могут обращаться как локально, так и удаленно.

- **Локальная файловая система** устанавливается на компьютере пользователя и не требует для доступа сетевого подключения. Пример локальной файловой системы — диск C, доступный на большинстве рабочих станций и серверов. Обращение к диску C производится по пути C:\.
- **Удаленная файловая система** доступна через сетевое соединение с удаленным ресурсом. Для подключения к удаленной файловой системе воспользуйтесь функцией Подключить сетевой диск (Map Network Drive).

Всеми дисковыми ресурсами, где бы они ни находились, управляет администратор системы. В этой главе обсуждаются средства и способы управления файловыми системами и дисками.

Добавление жестких дисков

Прежде чем вы откроете клиентам доступ к жесткому диску, его надо настроить и выбрать способ его использования. Microsoft Windows Server 2003 позволяет по-разному конфигурировать жесткий диск. Выбор методики зависит от тина данных, с которыми вы работаете, и требований сетевой среды. Для обычных пользовательских данных на рабочей станции можно сконфигурировать отдельные диски как автономные устройства хранения данных. Такая пользовательская инфор-

мация **хранится** на жестком **диске** рабочей **станции, где к ней** можно **обращаться** локально.

Хранить данные на одном диске удобно, но ненадежно. Для повышения надежности и производительности можно объединить несколько дисков. Windows Server 2003 поддерживает наборы дисков и технологию RAID.

Физические диски

Независимо от того, что вы используете, — отдельные диски или наборы, в основе лежит физический диск — аппаратное устройство храпения данных. Объем информации, который можно хранить на диске, зависит от его размера и применения сжатия. Объем стандартного диска сейчас достигает сотен гигабайт. Для Windows Server 2003 обычно применяются два типа дисков: SCSI и IDE.

Термины SCSI и IDE относятся к типу интерфейса жесткого диска, применяемого для связи с контроллером диска. В SCSI-дисках применяются SCSI-контроллеры, а в IDE-дисках — IDE-контроллеры. Диски SCSI дороже, чем IDE, но они быстрее и обладают более широкими возможностями.

SCSI-диски

Интерфейс SCSI позволяет подключить к одному контроллеру до 15 дисков. Каждому диску, подключенному к первичному контроллеру, присваивается числовой код от 0 до 15 — SCSI-идентификатор (] D) диска. Код диска 0 — SCSI ID 0, код диска 1 — SCSI ID 1 и т. д. Один из доступных кодов назначается самому контроллеру SCSI.

SCSI-устройства подключаются к контроллеру последовательно, одно за другим. Первое и последнее устройства в цепочке должны быть правильно терминированы. Как правило, SCSI-контроллер сам терминирует первое устройство. Устанавливать настоящий терминатор (специальный резистор) приходится лишь на последнее устройство *в* цепочке. Роль терминатора может выполнять и последний диск в цепочке, если это допускается его конструкцией.

Жесткий диск необходимо форматировать на низком уровне. Обычно изготовители SCSI-дисков сами форматируют их. Если вам потребуется провести низкоуровневое форматирование на месте, используйте служебную программу изготовителя.

IDE-диски

К IDE-контроллеру разрешается подключить до двух дисков. Диску, подключенному к первичному контроллеру, присваивают номер 0 (для первого диска) или 1 (для второго). Диски на вторичных контроллерах обозначаются номерами, следующими за последним занятым номером первичного контроллера. Например, если на первом контроллере два диска, то первый диск на втором контроллере получит номер 2.

Как и в случае SCSI-дисков, перед установкой IDE-диску присваивается номер. Если это первый IDE-диск на контроллере, его нужно сделать *главным* (master). Если на контроллере два диска, второй диск должен быть *подчиненным* (slave). Обычно при установке нового диска старый диск становится главным, а новый — подчиненным.

Примечание Вы не сможете отформатировать IDE-диск на низком уровне — это делает его изготовитель.

Подготовка диска к работе

Установленный диск необходимо сконфигурировать, разбив на разделы и создав в них файловые системы. *Раздел* (partition) — это область физического диска, которая функционирует как отдельное устройство. На дисках применяются разделы двух типов — MBR (Master Boot Record) и GPD (GUID Partition Table). На компьютерах x86 используются разделы MBR. На диске MBR имеется таблица разделов, в которой описывается, как разделы расположены на диске. Первый сектор жесткого диска содержит главную загрузочную запись (Master Boot Record, MBR) и двоичный программный код, который используется для загрузки системы. Этот сектор не включается в разделы и скрыт от просмотра, чтобы защитить систему.

На дисках MBR поддерживаются объемы до 4 терабайт. Разделы MBR бывают двух типов - *основной* (primary) и *расширенный,* или *дополнительный* (extended). Каждый диск MBR может иметь до четырех основных разделов или три основных и один дополнительный. Основные разделы — это части диска, к которым вы можете обратиться непосредственно. Чтобы сделать основной раздел доступным для пользователей, вы создаете па нем файловую систему. К дополнительным разделам у вас нет прямого доступа. Для хранения файлов на них создается один или несколько логических дисков.

На компьютерах с процессорами Itanium и 64-разрядными версиями Windows используются GPT-разделы. **Ключевое** отличие разделов GPT и MBR — в различном хранении данных раздела. На дисках GPT важные данные о разделах сами хранятся в отдельных разделах с избыточными основными и резервными таблицами разделов. К тому же GPT-диски поддерживают объем до 18 экзабайт и до 128 разделов. Впрочем, несмотря на эти отличия между разделами GPT и MBR, большинство задач по обслуживанию диска выполняются на них одинаково.

Оснастка Управление дисками (Disk Management)

Для настройки дисков на локальной или удаленной системе предназначена оснастка Управление дисками (Disk Management). Чтобы открыть ее, выполните следующие действия.

1. Выберите в меню Администрирование (Administrative Tools) команду Управление компьютером (Computer Management).
2. По умолчанию консоль Управление компьютером (Computer Management) запускается для управления локальным компьютером. Для управления жесткими дисками другого компьютера щелкните правой кнопкой элемент Управление компьютером (Computer Management) в дереве консоли и выберите Подключиться к другому компьютеру (Connect to Another Computer). Укажите систему, дисками которой хотите управлять.
3. Раскройте узел Запоминающие устройства (Storage) и щелкните Управление дисками (Disk Management). Теперь вы можете управлять дисками на локальной или удаленной системе.

Совет Если диспетчер логических дисков выдал сообщение об ошибке, прочтите его и щелкните OK. Невозможность подключиться к службе диспетчера логических дисков обычно означает, что она сама или связанные с нею административные службы не запущены на локальной или удаленной системе. На возможность удаленно управлять компьютерами также влияют сетевые политики и отношения доверия.

Окно оснастки Управление дисками (Disk Management) разделено на три части: список томов, графическое представление и список дисков.

Примечание Созданный, но не отформатированный раздел считается свободным местом. Если часть диска не относится к какому-то разделу, она считается неразмеченной.

На рис. 11-1 список томов занимает правый верхний угол, а графическая область — правый нижний. Если вам хочется изменить вид верхней или нижней области окна, выберите в меню Вид (View) команду:

- Верх (Top), чтобы задать представление верхней области окна;
- Низ (Bottom), чтобы изменить представление нижней области окна;
- Низ (Bottom), а затем — Скрыть (Hidden), чтобы скрыть нижнюю область.

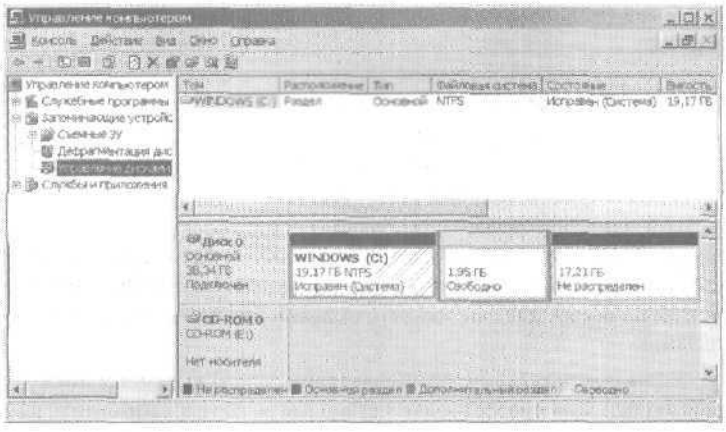


Рис. 11-1. Оснастка Управление дисками (Disk Management)

Отображение более подробной информации о дисках

В окне Управление дисками (Disk Management) можно получить и более подробную информацию по разделу диска, щелкнув его правой кнопкой, а затем выбрав в контекстном меню команду Свойства (Properties). Откроется то же диалоговое окно (рис. 11-2), что и из Проводника (Windows Explorer).

Рис. 11-2. На вкладке Общие (General) диалогового окна Свойства (Properties) содержится дополнительная информация о диске

Установка и проверка нового диска

Горячая замена (hot swapping) — возможность удалять устройство без выключения компьютера. Как правило, диски с поддержкой горячей замены устанавливаются и удаляются с передней панели компьютера. Затем в оснастке Управление дисками (Disk Management) выберите в меню Действие (Action) команду Повторить сканирование дисков (Rescan Disks). Если установленный диск не найден, попробуйте перезагрузить компьютер.

Если компьютер не поддерживает горячую замену дисков, выключите его и установите новый диск. Затем выполните команду Повторить сканирование дисков (Rescan Disks), как описано ранее.

Состояние диска

Знать состояние диска полезно при установке нового диска и при устранении проблем. В оснастке Управление дисками (Disk Management) состояние диска отображается в списке томов и в графическом представлении (табл. 11-1).

Таблица 11-1. Основные состояния **диска и их** описание

Состояние	Описание	Решение
Исправен (Online)	Нормальное состояние диска, означающее, что диск доступен и не имеет ошибок. Применимо как к основным, так и к динамическим дискам	Ничего делать не нужно
Работает (ошибки) [Online (Errors)]	На динамическом диске обнаружены ошибки ввода-вывода	Попробуйте выбрать команду Реактивизировать диск (Reactivate Disk)
Не подключен (Offline)	Динамический диск недоступен или поврежден. Если имя диска изменилось на Отсутствует (Missing), система не способна найти или идентифицировать его	Проверьте диск, контроллер и шлейфы на наличие ошибок. Убедитесь, что диск подсоединен *к* питанию и соответствующим образом подключен. Команда Реактивизировать диск (Reactivate Disk) позволяет снова включить диск (если это вообще возможно)
Чужой (Foreign)	Динамический диск подключен к компьютеру, но еще не импортирован. Чужим иногда считается диск, включенный после сбоя	Для добавления диска в систему используйте команду Импорт чужих дисков (Import Foreign Disks)
Не читается (Unreadable)	Диск временно недоступен, например в процессе повторного сканирования дисков или из-за наличия ошибок ввода-вывода. Применимо как к основным, так и к динамическим дискам	Воспользуйтесь командой Повторить сканирование дисков (Rcscan Disks) или перезагрузите систему
Неолознан (Unrecognized)	Тип диска неизвестен системе и не может использоваться ею. Так может отображаться диск другой ОС (не Windows)	Попробуйте другой диск
Нет носителя (No Media)	Ничего не установлено в CD-ROM-дисковод или дисковод для съемных дисков. Это состояние применимо только к CD-ROM и съемным дискам	Встаньтекомпакт-диск, дискету или съемный диск

Основные и динамические диски

Windows Server 2003 поддерживает два типа дисковых конфигураций.

- **Основной, или базовый[1] (basic)** — стандартный тип дисков, используемый в предыдущих версиях Windows. Основные диски разбиваются на разделы и могут применяться с предыдущими версиями Windows.
- **Динамический** (dynamic) — усовершенствованный тин дисков для Windows 2000, обновляемый (в большинстве случаев) без перезагрузки. Динамические диски делятся на тома и применяются с Windows 2000 и Windows Server 2003.

Примечание Нельзя использовать динамические диски на портативных компьютерах или на съемных носителях.

Использование основных и динамических дисков

При переходе к ОС Windows Server 2003 диски с разделами инициализируются как основные. При установке Windows Server 2003 на новую систему с не разбитыми на разделы дисками диски можно сделать основными или динамическими.

Б основных дисках поддерживаются все **отказоустойчивые** возможности Windows NT 4.0. Основные диски позволяют поддерживать или удалять существующие составные, зеркальные и чередующиеся наборы дисков. Однако основной тин не позволяет создавать новые отказоустойчивые диски; для этого их сл еду ет преобразовать в динамические, а затем создать тома, использующие зеркальное отображение и чередование. Отказоустойчивость и возможность модифицировать диски без перезагрузки — ключевые характеристики, отличающие динамические диски от основных. Прочие доступные характеристики зависят от форматирования диска.

На одном компьютере разрешается применять как основные, так и динамические диски; главное, чтобы том содержал диски одинаковых типов. Например, диски C и D, созданные под Windows NT 4.0 с применением зеркального отображения, можно использовать под Windows Server 2003. Преобразуя тип диска C на динамический, следует модифицировать и диск D.

[1] В русифицированном интерфейсе используются оба варианта. — *Прим. перев.*

О преобразовании основного диска в динамический читайте в разделе «Изменение типа диска».

Процедуры настройки основных и динамических дисков различаются. На основных дисках вы можете:

- форматировать разделы и помечать их как активные;
- создавать и удалять основные и дополнительные разделы;
- создавать и удалять логические диски внутри дополнительных разделов;
- преобразовывать основной диск в динамический.

На динамических лисках разрешается:

- создавать и удалять простые, чередующиеся, составные, зеркальные тома и массивы RAID-5;
- удалять зеркало из зеркального тома;
- расширять простые или составные тома;
- разделить один том на два;
- восстановить зеркальные тома или массивы RAID-5;
- заново активизировать потерянный или отключенный диск;
- отменить преобразование динамического диска в основной (требует удаления томов и перезагрузки),

Диски обоих типов позволяют:

- просматривать свойства дисков, разделов и томов;
- назначать диску букву;
- настраивать безопасность и общий доступ к диску.

Особенности основных и динамических дисков

Работая с основными или динамическими дисками, помните о специальных дисковых разделах.

- Системный (system) раздел (том) содержит файлы, специфичные для оборудования и необходимые для загрузки ОС.
- Загрузочный (boot) раздел (том) содержит ОС и необходимые ей файлы. Системный и загрузочный разделы могут совпадать.
- Активный (active) раздел (том) — область диска, с которой запускается компьютер.

Примечание На компьютерах с несколькими ОС, в число которых входят ранние версии Windows, на активном диске должны содержаться загрузочные файлы для каждой из

них. Он также должен быть основным разделом на основном диске. Сделать существующий динамический том активным нельзя, но вы вправе преобразовать в динамический основной диск, содержащий активный раздел. После завершения обновления раздел становится простым томом, который автоматически будет превращен в активный.

Назначение активного раздела

В Windows Server 2003 поддерживаются две ключевые архитектуры процессоров: x86 и Itanium. Чтобы назначить активный раздел на компьютере x86, выполните следующие действия,

1. Убедитесь, что загрузочные файлы находятся в основном разделе диска, который вы хотите сделать активным. Для Windows NT, Windows 2000 Server и Windows Server 2003 это: BOOT.INI, NTDETECT.COM, NTLDR и BOOTSECT.DOS. Также может потребоваться NTBOOTDD.SYS.
2. Запустите консоль Управление дисками (Disk Management).
3. Щелкните правой кнопкой раздел, который хотите сделать активным, и выберите Сделать раздел активным (Mark Partition As Active).

Изменение типа диска

Основные диски предназначены для применения с предыдущими версиями Windows. Динамические диски позволяют использовать новейшие преимущества Windows. Динамические диски могут работать только на компьютерах с Windows 2000 или Windows Server 2003. Однако их разрешается применять с другими ОС, например с Unix, после создания отдельного тома для прочих (не Windows) систем. Динамические диски нельзя применять в переносных компьютерах.

Windows Server 2003 предоставляет средства для трансформации основного диска в динамический и обратно. При этом разделы автоматически преобразуются в тома соответствующего типа. Тома нельзя преобразовать в разделы. Придется удалить тома на динамическом диске и лишь потом изменить тип диска обратно на основной. Удаление тома уничтожает всю информацию на диске.

Преобразование основного диска в динамический

Перед изменением типа диска с основного на динамический убедитесь, что диск не будет использоваться другими версиями

Windows. Удостоверьтесь, что в конце MBR-диска есть 1 Мбайт свободного места, иначе преобразовать его не удастся. На GPT-дисках вам понадобятся нефрагментированные распознаваемые разделы. Если на GPT-диске содержатся разделы, которые Windows не распознает, например созданные другой операционной системой, нам не удастся преобразовать диск в динамический.

Перед преобразованием дисков обоих типов учтите также следующее:

- нельзя модифицировать диски с размером сектора больше 512 байт. Если размер сектора больше, сначала переформатируйте диск;
- нельзя сделать динамическими диски на портативных компьютерах или съемные диски. Дисковод для этих дисков можно настроить только как основной диск с основными разделами;
- нельзя модифицировать диск, если системный или загрузочный раздел является частью составного тома, массива RAID-5 или тома с чередованием, поэтому перед преобразованием нужно удалить эти функции;
- нельзя преобразовывать диск, если на нем записано несколько версий операционной системы Windows. Если вы все-таки сделаете это, впоследствии вам, вероятно, удастся загрузить только Windows Server 2003;
- можно модифицировать диски с разделами других типов, которые являются частью составного тома, массива RAID-5 или тома с чередованием. Эти тома становятся динамическими томами *соответствующего* типа. Однако *при* этом диски в наборе надо модифицировать все вместе.

Основной диск преобразуется в динамический так.

1. В консоли Управление дисками (Disk Management) в списке дисков или в графической области щелкните правой кнопкой основной диск, который нужно *преобразовать*. Затем выберите Преобразовать в динамический диск (Convert to Dynamic Disk).
2. В окне Преобразование в динамические диски (Convert To Dynamic Disk) отметьте диски, которые следует модифицировать. При преобразовании составных томов, массивов RAID-5 или томов с чередованием, убедитесь, что вы выбрали все диски в наборе, так как их нужно модифицировать одновременно. Щелкните OK.

3. Просмотрите сведения в диалоговом окне Диски для преобразования (Disks To Convert):
   - Имя (Name) — номер диска;
   - Оглавление диска (Disk Contents) — тип и состояние разделов: загрузочный, активный, используется и т. п.
   - Будет преобразован (Will Convert) — это поле указывает, будет ли диск модифицирован:
   - Сведения (Details) —щелкните эту кнопку, чтобы просмотреть тома выбранного диска.
4. Щелкните Преобразовать (Convert). Оснастка Управление дисками (Disk Management) предупредит вас, что, закончив преобразование диска, вы больше не сможете загружать предыдущие версии Windows с томов выбранных дисков. Щелкните Да (Yes).
5. Оснастка Управление дисками (Disk Management) перезагрузит систему, если выбранный диск содержит загрузочный, системный или используемый раздел.

Обратное преобразование динамического диска в основной

Перед обратным преобразованием нужно удалить с диска все динамические тома. Как только вы это сделали, щелкните диск правой кнопкой и выберите Преобразовать в базовый диск (Convert to Basic Disk). Эта операция преобразует динамический диск в основной, после чего можно создавать новые разделы и логические диски.

Реактивация динамических дисков

Если состояние динамического диска отличается от Исправен (Online), зачастую для устранения проблемы достаточно просто реактивизировать диск.

1. В оснастке Управление дисками (Disk Management) щелкните правой кнопкой нужный динамический диск и выберите Реактивизировать диск (Reactivate Disk). Подтвердите действие.
2. Если состояние диска не изменилось, перезагрузите компьютер. Если это не помогло, проверьте дисковод, контроллер и шлейфы на наличие ошибок, также убедитесь, что дисковод правильно подсоединен и подключен к питанию.

Повторное сканирование дисков

При повторном сканировании всех дисков ОС обновляет конфигурацию дисководов компьютера. Иногда это решает проблему, если диски отображаются как нечитаемые. В результате повторного сканирования конфигурация дисков может измениться. Вот вам конкретный пример. Типичная конфигурация моего сервера: дисковод для гибких дисков A, логические диски C, D, E, и F, съемный диск G и CD-ROM H. После повторного сканирования съемному диску была назначена буква B, в результате чего изменился помер загрузочного раздела. Windows Server 2003 не выдала по этому поводу никаких предупреждений, а при перезагрузке некорректно указала, что файл NTOSKRNL.EXE о корневой папке Windows Server 2003 нуждается в восстановлении. Чтобы ОС снова заработала нормально, отредактируйте файл BOOT.INI (см. раздел «Обновление загрузочного диска»).

Повторное сканирование дисков системы осуществляется посредством команды Повторить сканирование дисков (Rescan Disk) из меню Действие (Action) оснастки Управление дисками (Disk Management).

Совет Для дополнительной проверки проведенных изменений сделайте снимок экрана конфигурации дисков в оснастке Управление дисками (Disk Management) до и после сканирования.

Перенос динамического диска в новую систему

Задача переноса дисков в Windows Server 2003 решается очень просто.

1. Запустите оснастку Управление дисками (Disk Management) на системе с установленными динамическими дисками.
2. Проверьте состояние дисков, убедитесь, что нужный диск исправен. Если это не так, перед переносом нужно восстановить поврежденные разделы и тома.
3. Удалите букву диска и путь доступа к диску (см. раздел «Назначение путей и букв дискам»).
4. Если диск и обе системы поддерживают функцию горячей замены, просто извлеките диск из одного компьютера и переставьте его в другой. В противном случае выключите компьютеры и переставьте диски со старого компьютера на новый, а затем вновь включите компьютер.

5. На компьютере, кула устанавливаются диски, в меню Действие (Action) выберите Повторить сканирование дисков (Rescan Disks), Когда сканирование дисков закончится, щелкните правой кнопкой диск, отображаемый как Чужой (Foreign), и в контекстном меню выберите Импорт чужих дисков (Import Foreign Disks).

Использование основных дисков и разделов

При установке нового компьютера или модернизации старого часто требуется разбить его диски на разделы. Для этого предназначена оснастка Управление дисками (Disk Management).

Основные сведения о создании разделов

В Windows Server 2003 физический диск MBR может содержать до четырех основных разделов и не более одного дополнительного. Поэтому возможно два варианта конфигурации MBR-дисков: первый — от 1 до 4 основных дисков, второй — от 1 до 3 основных и 1 дополнительный раздел. Диски GPT могут иметь до 128 разделов.

После разбиения диска надо отформатировать разделы, чтобы назначить буквы дисков. Это высокоуровневое форматирование, создающее структуру файловой системы в отличие от низкоуровневого форматирования, которое только подготавливает диск к работе. Вам, конечно, знаком диск C. Он представляет собой просто указатель на раздел диска, Если диск разбивается на несколько разделов, то каждому из них присваивается своя буква. Буквы дисков служат для доступа к файловым системам разделов физического диска. В отличие от MS-DOS, где буквы дискам назначаются автоматически, начиная с C; Windows Server 2003 позволяет определять их самостоятельно (доступны все буквы от C до Z).

Примечание Буква A обычно резервируется для системного дисковода для гибких дисков. Если в системе установлен второй дисковод для гибких дисков, ему присваивается буква B, поэтому в вашем распоряжении только буквы от C до 2. Не забудьте, что CD-ROM, ZIP-дисководы и другие типы носителей также обозначаются буквами. Одновременно разрешается использовать до 24 букв. Если не хватает томов, можно смонтировать их, указав путь к диску.

В Windows NT 4.0 активных томов не бывает более 24. Windows 2000 и Windows Server 2003 обходят это ограничение за счет подключения одного диска к папке, расположенной на другом диске. Обращение к такому диску осуществляется по пути к этой папке, например E:\datal. К папкам разрешено подключать как основные, так и динамические диски. Единственное ограничение — папка, за которой скрывается диск, должна быть пустой и располагаться на томе NTFS.

Для наглядности в оснастке Управление дисками (Disk Management) основные и дополнительные разделы с логическими дисками отмечены разными цветами. Легенда цветовой схемы отображается внизу окна Управление дисками (Disk Management). Цвета меняют в диалоговом окне Настройка вида (View Settings). Чтобы открыть его, выберите в меню Вид (View) команду Настроить (Settings).

Создание разделов и логических дисков

Разделы и логические диски создаются в консоли Управление дисками (Disk Management).

1. Б графической области оснастки Управление дисками (Disk Management) щелкните правой кнопкой область, помеченную Не распределен (Unallocated Space), и выберите Создать раздел (New Partition). Или щелкните правой кнопкой мыши свободное пространство в дополнительном разделе и выберите Создать логический диск (New Logical Drive). Запустится Мастер создания разделов (New Partition Wizard).
2. Щелкните Далее (Next). Теперь можно указать тип раздела (рис. 11-3).

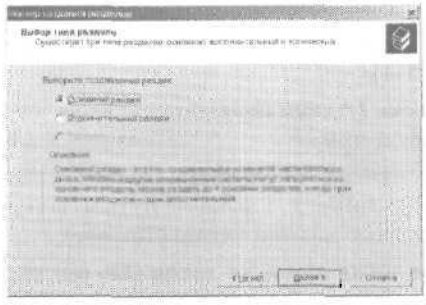


Рис. 11-3. Здесь выбирается тип раздела

- **Основной раздел (Primary Partition) —** создает основной раздел. Основной раздел может занимать как диск целиком, так и его часть, размер которой определяется потребностями рабочей станции или сервера.
- Дополнительный раздел (Extended Partition) — создает дополнительный раздел. Физический диск может содержать один дополнительный раздел, который состоит из нескольких логических дисков (областей раздела со своей файловой системой). Если на диске уже есть дополнительный раздел, этот вариант окажется недоступным. На съемных дисках нельзя создавать дополнительные разделы.
- **Логический диск (Logical Drive) —** создает в дополнительном разделе логический диск.

3. В окне Указание размера раздела (Specify Partition Size) задайте размер раздела в поле Выбранный размер раздела (МБ) [Partition size in MB]. Щелкните Далее (Next).

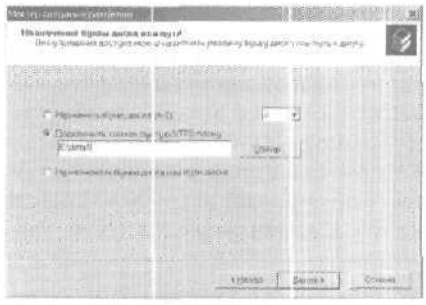


Рис. 11-4. Назначьте диску букву или подключите его к пустой папке

4. Чтобы назначить диску букву или путь, установите один из переключателей (рис 11-4):
   - **Назначить букву диска (Assign the following drive letter)** — выберите букву в списке;
   - **Подключить том как пустую NTFS-папку (Mount in the following empty NTFS folder)** — введите путь к папке или найдите ее с помощью кнопки Обзор (Browse);
   - **Не назначать** буквы диска или пути диска (Do not assign a drive letter or drive path) — это можно сделать позже.

5. Щелкните Далее (Next). В окне Форматирование раздела (Format Partition) укажите, нужно ли форматировать раздел (рис. 11-5). Подробнее о форматировании — в следующем разделе.
6. Щелкните Далее (Next), а затем Готово (Finish). При добавлении разделов на физический диск, содержащий Windows Server 2003, может измениться номер загрузочного раздела. В этом случае ОС выдаст соответствующее предупреждение. Щелкните Да (Yes).

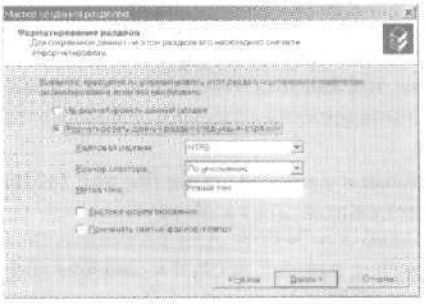


Рис. 11-5. Отформатируйте **раздел,** указав файловую систему и метку **тома**

7. При необходимости внесите изменения в файл BOOT.INI, изменив указатель на загрузочный раздел (см. раздел «Обновление загрузочного диска») и немедленно перезагрузите систему.

Форматирование разделов

В процессе форматирования на разделе создастся файловая система, а вся существующая информация удаляется. Не путайте высокоуровневое форматирование, создающее структуру файловой системы, с низкоуровневым, которое просто подготавливает диск к работе. Чтобы отформатировать раздел, щелкните его правой кнопкой и выберите Форматировать (Format). Откроется диалоговое окно, показанное на рис. 11-6.

Ниже описаны поля этого окна.

- **Метка тома (Volume Label) — текстовое имя раздела.**
- **Файловая система (File System) — тип файловой системы, например FAT, FAT32 или NTFS.**

- Размер кластера (Allocation unit size) — размер основной единицы деления дискового пространства. По умолчанию размер кластера определяется но размеру тома и задается до форматирования, но вы вправе задать собственный размер кластера. Это бывает полезно при использовании большого количества небольших файлов. Если вы уменьшите размер кластера до 512 или 1024 байт, эти файлы будут занимать меньше места на диске.
- Быстрое форматирование (Perform a quick format) — форматирует диск, не проверяя раздел на наличие ошибок. При работе с большими разделами этот параметр может сэкономить несколько минут. Но все же рекомендуется проверять диск на наличие ошибок, так как при этом оснастка Управление дисками (Disk Management) отмечает и блокирует поврежденные сектора,
- Применять сжатие файлов и папок (Enable file and folder compression) — включает сжатие диска. Встроенная система сжатия доступна только для NTFS. Для пользователей механизм сжатия прозрачен, так как доступ к сжатым данным идентичен доступу к обычным данным. После выбора этого параметра файлы и папки на диске автоматически сжимаются. Подробнее о сжатых дисках, файлах и папках рассказано в разделе «Сжатие дисков и данных».

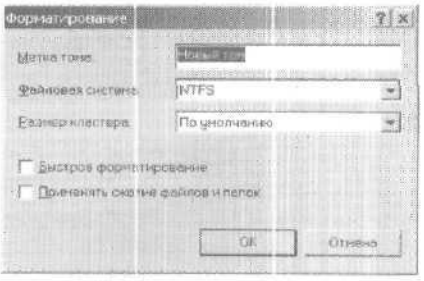


Рис. 11-6. Отформатируйте раздел, назначив ему файловую систему и метку тома

Задав нужные параметры, щелкните OK. При форматировании раздела вся информация на нем уничтожается, поэтому консоль Управление дисками (Disk Management) на данном этапе предоставляет еще одну, последнюю возможность прервать операцию. Щелкните OK, чтобы начать форматирование.

Обновление загрузочного диска

При добавлении разделов на диск, содержащий Windows Server 2003, может измениться номер загрузочного раздела. Если это произошло, внесите соответствующие изменения в системный файл BOOT.INI (обычно расположенный на диске C).

Файл BOOT.INI содержит примерно такие строки:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(3)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(3)\WINNT="Microsoft Windows
Server 2003" /fastdetect
multi(0)disk(0)rdisk(0)partition(2)\WIN2000="Microsoft Windows
2000 Server" /fastdetect
multi(0)disk(0)rdisk(0)partition(1)\WINXP="Microsoft Windows
XP Professional" /fastdetect
```

Примечание Файл BOOT.INI может быть скрытым. Чтобы увидеть его в окне Проводника (Windows Explorer), выберите в меню Сервис (Tools) команду Свойства папки (Folder Options) и перейдите на вкладку Вид (View). Сбросьте флажок параметра Скрывать защищенные системные файлы (Hide Protected Operating System Files) и щелкните OK.

Приведенная ниже строка и другие похожие строки указывают Windows Server 2003, где искать файлы ОС:

```
multi(0)disk(0)rdisk(0)partition(3)\WINNT
```

Рассмотрим ее подробнее.

- **multi(0)** — контроллер диска, в данном случае — контроллер 0. Если вторичное зеркало расположено на другом контроллере, введите его помер. Контроллеры нумеруются от О до 3.

Примечание Элементы файла BOOT.INI написаны в формате ARC (Advanced RISC Computer). На SCSI-системах, не использующих SCSI BIOS, первое поле элемента — scsi(*n*), где *n* — номер контроллера.

- **disk(0)** — SCSI-адаптер (в данном случае — адаптер 0). На большинстве систем этот параметр всегда 0. На системах с многоканальными SCSI-адаптерами вместо него используется параметр scsi(*n*).

- rdisk(O) — порядковый номер диска на адаптере (в данном случае — 0). На SCSI-дисководах со SCSI BIOS поддерживаются номера от 0 до 6. Для остальных SCSI-дисководов этот параметр всегда 0, для IDE — 0 или 1. В большинстве случаев изменять нужно значение именно этого поля.
- partition(3) — раздел, содержащий ОС (в данном случае — 3).

Если загрузочный раздел Windows Server 2003 изменился с 3 на 4. необходимо изменить файл BOOT.INI следующим образом.

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(4)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(4)\WINNT="Microsoft Windows
Server 2003" /fastdetect
multi(0)disk(0)rdisk(0)partition(2)\WIN2000="Microsoft Windows
2000" /fastdetect
multi(0)disk(0)rdisk(0)partition(1)\WINXP="Microsoft Windows
XP Professional" /fastdetect
```

Управление разделами и дисками

В консоли Управление дисками (Disk Management) предусмотрено множество способов управления разделами и дисками. Вы можете назначать дискам буквы, удалять разделы, задавать активный раздел и т. п. Кроме того, в Windows Server 2003 имеются служебные программы для выполнения таких задач, как преобразование тома в NTFS, проверка диска или очистка неиспользуемого дискового пространства,

Назначение путей и букв дискам

Диск можно обозначить буквой и одним или несколькими путями, которые *подключены* (mounted) к папкам на NTFS-дисках. Назначать диску букву или путь не обязательно. Диск без указателей считается неподключенным; подключить его можно в любой момент, назначив букву и путь. Перед переносом на другой компьютер диск следует *отключить* (unmount).

Чтобы изменить букву диска или путь, в консоли Управление дисками (Disk Management) щелкните правой кнопкой нужный диск и выберите Изменение буквы диска и пути диска (Change Drive Letter and Paths). Открывшееся окно (рис. 11-7) предоставляет следующие возможности.

- Чтобы добавить путь к диску, щелкните кнопку Добавить (Add), установите переключатель Подключить том как пустую NTFS-папку (Mount in the following empty NTFS folder), затем введите путь к существующей папке или найдите ее с помощью кнопки Обзор (Browse).
- Чтобы удалить путь к диску, выделите его, щелкните Удалить (Remove), а затем Да (Yes).
- Чтобы назначить букву диска, щелкните Добавить (Add), затем Назначить букву диска (Assign a drive letter) и выберите доступную букву.
- Чтобы изменить букву диска, выберите текущую букву и щелкните Изменить (Change). Затем установите переключатель Назначить букву диска (Assign a drive letter) и выберите другую букву.
- Чтобы удалить букву диска, выберите текущую букву, щелкните Удалить (Remove), а затем Да (Yes).

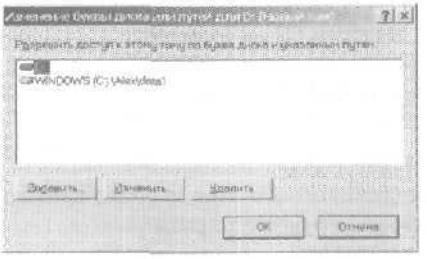


Рис. 11-7. В этом окне можно изменить букву диска и путь

Примечание При попытке изменить букву используемого в данный момент диска ОС выдает соответствующее предупреждение. Выйдите из всех работающих на этом диске программ или позвольте консоли Управление дисками (Disk Management) принудительно внести изменения, щелкнув Да (Yes) в ответ на запрос.

Изменение или удаление метки тома

Метка тома — текстовое описание диска. Она отображается при доступе к диску из разных программ Windows Server 2003, например из Проводника (Windows Explorer), и помогает понять, что хранится на диске. Изменять и удалять метку можно из консоли Управление дисками (Disk Management) или Проводника.

Чтобы измелить или удалить метку в одной из этих программ, выполните следующие действия.

1. Щелкните правой кнопкой раздел и выберите Свойства (Properties).
2. На вкладке Общие (General) окна свойств в поле Метка (Label) удалите старое имя или введите вместо него новое. Щелкните OK.

Удаление разделов и дисков

Чтобы изменить конфигурацию полностью распределенного диска, иногда приходится удалять существующие разделы и логические диски. В результате чего уничтожается файловая система и теряется вся информация на ней. Поэтому перед удалением сделайте резервные копии всех файлов и папок, содержащихся на диске.

Основной раздел или логический диск удаляется следующим образом.

1. В консоли Управление дисками (Disk Management) щелкните правой кнопкой раздел или диск, который планируете удалить, и выберите Удалить раздел (Delete Partition) или Удалить логический диск (Delete Logical Drive).
2. Подтвердите, что хотите удалить раздел, щелкнув Да (Yes).
3. При удалении раздела физического диска, содержащего Windows Server 2003, номер загрузочного раздела может измениться. Если это случилось, отредактируйте файл BOOT.INI, как описано ранее.

Дополнительный раздел удаляется так.

1. Удалите на разделе все логические диски, как описано ранее.
2. Выделите дополнительный раздел целиком и удалите его.

Преобразование тома в NTFS

В комплекте Windows Server 2003 предусмотрена утилита CONVERT.EXE для преобразования FAT-томов в систему NTFS. Она расположена в папке *%SystemRoot%*. При преобразовании тома этой программой структура файлов и папок, а также данные сохраняются. Помните, что программы обратного преобразования (NTFS в FAT) в Windows Server 2003 нет. Единственный способ перейти от NTFS к FAT — удалить раздел, а затем воссоздать раздел как том FAT.

Синтаксис программы преобразования

Convert запускается в окне командной строки. В простейшем случае она выглядит так:

```
convert том /FS:NTFS
```

Здесь *том* — буква диска с двоеточием, путем диска и именем тома. Например, чтобы преобразовать диск D *в* систему NTFS, введите:

```
convert D: /FS:NTFS
```

Полный синтаксис программы Convert таков:

```
convert том/FS: NTFS [/V] [/X] [/CvtArea:имя_файла] [/
NoSecurity]
```

Параметры и переключатели программы Convert имеют следующий смысл:

- *том* — указывает том для преобразования;
- /FS:NTFS — указывает, что осуществляется преобразование в формат NTFS;
- /V — включает режим вывода подробных сведений;
- /X — при необходимости отключает том перед сжатием;
- /CvtArea:*имя_файла*— указывает имя нефрагментированного файла в корневой папке, на месте которого будут размещены системные файлы;
- /NoSecurity — удаляет все атрибуты безопасности и делает все файлы и папки доступными для группы Все (Everyone).

Работа с программой Convert

Перед применением программы Convert проверьте, не является ли преобразуемый раздел активным загрузочным или системным разделом, содержащим файлы ОС. На системах Intel *x*86 активный загрузочный раздел можно преобразовать в NTFS. При этом система должна обладать полным доступом к разделу, что достижимо только во время запуска. Таким образом, при попытке преобразовать активный загрузочный раздел в NTFS Windows Server 2003 спросит, нужно ли преобразовывать диск при очередном перезапуске. Щелкнув Да (Yes), вы перезагрузите систему, а значит, будет выполнен процесс преобразования.

Совет Обычно для полного преобразования активного загрузочного раздела требуется несколько перезагрузок. Так что не волнуйтесь: система знает, что делает.

Системы на базе RISC-процессоров сконфигурированы на аппаратном уровне и не используют активных загрузочных разделов. Однако на RISC-компьютерах применяется системный раздел, содержащий все нужные файлы ОС. На этом разделе должны использоваться файловая система FAT, поэтому на RISC-компьютерах преобразовать системный раздел в NTFS нельзя.

Перед преобразованием диска в NTFS программа Convert проверяет наличие на нем свободного места. Как правило, для ее работы требуется блок свободного места размером около 25% от занятого объема. Если свободного места не хватает, Convert прервет операцию и сообщит, что нужно освободить место на диске. Если места достаточно, Convert начнет преобразование, которое может занять несколько минут (или больше для объемных дисков). Не обращайтесь к файлам и приложениям на диске во время преобразования.

Проверка диска на наличие ошибок и поврежденных секторов

Служебная программа CHKDSK.EXE предназначена для поиска и исправления ошибок па томах FAT, FAT32 и NTFS. Она расположена в папке *%SystemRoot%*.

Программа CHKDSK.EXE способна находить и исправлять большинство ошибок, но в первую очередь она ищет противоречие между файловой системой и связанными с ней метаданными. Один из способов проверки диска, который реализован в этой утилите, — сравнение битовой карты тома с секторами, запятыми файлами. Впрочем, возможности CHKDSK.EXE ограничены. Например, она не восстанавливает поврежденные данные внутри структурно неповрежденных файлов.

Запуск CHKDSK.EXE из командной строки

Программа CHKDSK.EXE запускается как из командной строки, так и из других служебных программ. В режиме командной строки для проверки целостности диска E, введите

```
chkdsk E:
```

Для поиска и исправления ошибок на диске E введите команду

```
chkdsk /f E:
```

Примечание Программа CHKDSK.EXE не способна исправлять используемые в данный момент тома. Если вы попытаетесь это сделать, программа спросит у вас, хотите ли вы запланировать проверку при очередном перезапуске системы.

Полный синтаксис CHKDSK.EXE таков:

```
chkdsk [том[[путь]имя_файла]]] [/F] [/V] [/R] [/X] [/I] [/C]
[/L[:размер]]
```

Параметры и переключатели программы CHKDSK.EXE описаны далее:

- *том* — указывает том для проверки;
- *имя_файла* (только FAT и FAT32) — файлы, которые нужно проверить на фрагментацию;
- /F — задает исправление ошибок на диске;
- /V — в FAT/FAT32 отображает полный путь и имя каждого файла на диске, в NTFS отображает служебные сообщения;
- /R — локализует поврежденные сектора и восстанавливает читаемую информацию (одновременно включает /F);
- /L:*размер* (только NTFS) — изменяет размер файла журнала;
- /X — задает отключение тома перед началом проверки (одновременно включает /F);
- /I (только NTFS) — задает минимальную проверку индексных элементов;
- /C (только NTFS) — отменяет проверку циклов в структуре папок.

Удаленный запуск CHKDSK.EXE

Чтобы запустить CHKDSK.EXE удаленно из окна Проводника (Windows Explorer) или консоли Управление дисками (Disk Management), выполните следующие действия.

1. Щелкните правой кнопкой диск и выберите Свойства (Properties).
2. На вкладке Сервис (Tools) щелкните кнопку Выполнить проверку (Check Now).
3. Задайте необходимые действия или сбросьте оба флажка, чтобы проверить диск, не исправляя ошибки (рис. 11-8).
4. Затем щелкните Запуск (Start).

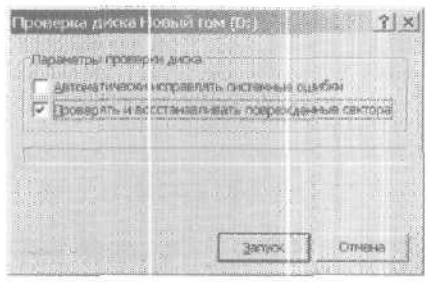


Рис. 11-8. Задайте необходимые действия по проверке диска на ошибки

Дефрагментация дисков

При записи или удалении файлов данные на диске часто разбиваются на фрагменты. Если диск сильно фрагментирован, вам не удастся разместить большой файл в непрерывной области. ОС распределит его по нескольким небольшим участкам диска, из-за чего время доступа к файлу увеличится. Чтобы уменьшить фрагментацию, нужно периодически анализировать и дефрагментировать диски, используя программу Дефрагментация диска (Disk Defragmenter).

Чтобы проанализировать уровень фрагментации диска и дефрагментировать его, выполните следующие действия.

1. В консоли Управление компьютером (Computer Management) раскройте узел Запоминающие устройства (Storage) и выберите Дефрагментация диска (Disk Defragmenter).
2. Щелкните том или логический диск, с которым будете работать (рис. 11-9).
3. Щелкните кнопку Анализ (Analyze). Результаты анализа отобразятся *в нижней* части окна. Фрагментированные, непрерывные и системные файлы, а также свободное место отмечены разными цветами. Легенда с расшифровкой цветов размещается под картой диска (если процесс анализа затянулся, его можно в любой момент остановить).
4. Завершив анализ, программа предложит выполнить дефрагментацию, если диск сильно фрагментирован, или сообщит, что Дефрагментация не требуется.
5. Чтобы начать дефрагментацию, щелкните кнопку Дефрагментация (Defragment). Ход процесса отображается в ниж-

ней части окна (дефрагментацию также можно в любой момент прервать).

6. **Щелкните Вывести** отчет **(View** Report), **чтобы просмотреть** отчет об анализе или дефрагментации.

Рис. 11-9. Чем чаще изменяется информация на диске, тем чаще нужно его дефрагментировать

Сжатие дисков и данных

При форматировании диска в системе NTFS можно воспользоваться встроенной системой сжатия, которая автоматически сжимает все файлы и панки при их создании. Для пользователя эта операция незаметна, так как доступ к сжатым данным ничем не отличается от доступа к обычным данным. Разница лишь в том, что на сжатом диске умещается больше информации, чем на несжатом.

Примечание Помните, что сжатые данные нельзя зашифровать. Сжатие и шифрование на томах NTFS — взаимоисключающие действия. Подробнее об этом — в разделе «Шифрование дисков и данных». Если вы попытаетесь сжать зашифрованнные данныые, Windows Server 2003 автоматически расшифрует данные и затем сожмет их. Если вы попытаетесь зашифровать сжатые данные, Windows Server 2003 сначала разуплотнит их, а потом зашифрует.

Сжатие дисков

Чтобы сгжать диск и все его содержимое, выполните следующие действия.

t. В Проводнике (Windows Explorer) или консоли Управление дисками (Disk Management) правой кнопкой мыши щелкните диск, который нужно сжать, и выберите Свойства (Properties).
2. На вкладке Общие (General) установите флажок Сжимать диск для экономии места (Compress drive to save disk space) и щелкните OK.

Сжатие папок и файлов

В Windows Server 2003 допускается избирательно сжимать папки или файлы. Для этого нужно сделать следующее.

1. В Проводнике (Windows Explorer) щелкните правой кнопкой файл или папку, которую нужно сжать, и выберите Свойства (Properties).
2. На вкладке Общие (General) щелкните кнопку Другие (Advanced). Установите флажок Сжимать содержимое для экономии места на диске (Compress contents to save disk space), как показано на рис. 11-10. Два раза щелкните OK.

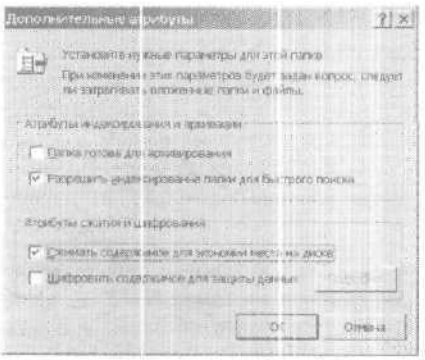


Рис. 11-10. El системе NTFS можно сжать отдельный файл или папку

Если в папке есть подпапки, Windows Server 2003 выдает запрос на их сжатие — установите переключатель К этой папке и ко всем вложенным файлам и папкам (Apply changes to this folder, subfolders, and files) и щелкните OK. Новые файлы

при добавлении и копировании в сжатую панку также автоматически сжимаются.

Примечание При перемещении с несжатого диска на сжатый диск файл сжимается. При перемещении из несжатой папки в сжатую на том же NTFS-диске несжатый файл остается таковым.

Разуплотнение сжатых дисков

Для разуплотнения диска выполните следующие действия.

1. В Проводнике (Windows Explorer) или консоли Управление дисками (Disk Management) правой кнопкой мыши щелкните нужный диск и выберите Свойства (Properties).
2. На вкладке Общие (General) сбросьте флажок Сжимать диск для экономии места (Compress drive to save disk space) и щелкните OK.

Примечание Перед разуплотнением данных Windows всегда проверяет наличие свободного места на диске — не забудьте об этом. Если свободного места мало, разуплотнение может не завершиться.

Разуплотнение сжатых файлов и папок

Для разуплотнения файла или папки выполните следующие действия.

1. Щелкните правой кнопкой файл или папку в окне Проводника (Windows Explorer).
2. На вкладке Общие (General) окна свойств щелкните Другие (Advanced), сбросьте флажок Сжимать содержимое для экономии места на диске (Compress contents to save disk space) и два раза щелкните OK.

Windows Server 2003 отменит сжатие и распакует файл. При разуплотнении папки ОС разуплотняет все файлы в ней. Чтобы отменить сжатие подпапок, в окне с запросом установите К этой папке и ко всем вложенным файлам и папкам (Apply changes to this folder, subfolders, and files) и щелкните OK.

Совет В Windows Server 2003 есть утилиты командной строки COMPACT.EXE для сжатия информации и EXPAND.EXE для разуплотнения.

Шифрование дисков и данных

NTFS имеет немало преимуществ по сравнению с другими файловыми системами Windows Server 2003, и одно из важнейших — возможность автоматически шифровать и расшифровывать данные посредством *шифрованной файловой системы* (Encrypting File System, EFS). Шифрование обеспечивает дополнительную защиту конфиденциальных данных — зашифрованные файлы сумеют прочесть только те. кто их зашифровал.

Основы EFS

Шифрование файлов назначается папкам или отдельным файлам. Любой файл, помещаемый в шифрованную папку автоматически шифруется. Зашифрованные файлы может читать только тот, кто их зашифровал. Чтобы сделать их доступными другим пользователям, файлы нужно расшифровать.

С каждым зашифрованным файлом сопоставляется уникальный *ключ шифрования* (encryption key). Благодаря ему зашифрованный файл можно копировать, перемещать и переименовывать, как любой другой файл. На шифрование данных эти действия в большинстве случаев не повлияют. У пользователя, зашифровавшего файл, доступ к нему есть всегда при условии, что на данном компьютере имеется *сертификат открытого ключа* (public key certificate) для этого пользователя. При этом процессы шифрования и расшифровки для данного пользователя совершенно прозрачны.

За шифрование и расшифровку данных отвечает файловая система EFS. По умолчанию она допускает шифрование файлов пользователями, не имеющими специального разрешения. Файлы шифруются с помощью *открытых* (public) и *закрытых* (private) ключей, которые EFS автоматически генерирует для каждого пользователя. По умолчанию при шифровании используется 56-разрядный алгоритм DESX (Data Encryption Standard eXpanded). Пользователи из США, которым нужна более серьезная защита, могут заказать в Microsoft пакет Enhanced CryptoPAK со 128-разрядным шифрованием. Файлы, зашифрованные с его помощью, доступны только на системах, поддерживающих 128-разрядное шифрование.

Сертификаты шифрования (encryption certificates) сохраняются как часть профиля пользователя. Если пользователь хочет работать с зашифрованными данными на нескольких

компьютерах, администратору придется создать для него *перемещаемый профиль* (roaming profile).

Совет Если создание перемещаемого профиля по каким-то причинам нежелательно, сертификат шифрования можно скопировать на другие компьютеры. Для этого предусмотрена процедура архивирования и восстановления сертификата, которая описана в главе 15. Сертификат архивируется на основном компьютере пользователя и восстанавливается на компьютерах, где пользователю также нужно работать с зашифрованными данными.

В EFS имеется встроенная система восстановления данных, которая защищает от потери информации в случае утраты открытого ключа пользователя. Как правило, это происходит, когда пользователь увольняется и администратор чересчур поспешно удаляет его учетную запись. Чтобы получить доступ к зашифрованным файлам в этих условиях, вам понадобится *агент восстановления* (recovery agent). У агента восстановления имеется доступ к ключу шифрования файла, что позволяет прочитать данные из него. Ни к какой информации о закрытом ключе у агента нет.

Агенты восстановления EFS конфигурируются на двух уровнях.

- На уровне домена агент восстановления настраивается автоматически при установке первого контроллера домена Windows Server 2003. По умолчанию агентом восстановления является администратор. С помощью групповой политики администраторы домена могут назначать других агентов восстановления, а также делегировать полномочия агентов восстановления администраторам безопасности.
- На уровне локального компьютера (как изолированного, так и члена рабочей группы) агентом восстановления по умолчанию является администратор. Можно назначить и дополнительных агентов. Чтобы в домене вместо агентов восстановления уровня домена действовали локальные агенты, удалите политику восстановления из групповой политики домена.

Примечание Для нормального функционирования EFS агенты восстановления обязательно должны быть назначены в системе. Если вы удалите все политики восстановления, шифрование файлов прекратится.

Шифрование папок и файлов

Windows Server 2003 позволяет выбрать для шифрования отдельные файлы и папки на томах NTFS. При этом имейте в виду, что в зашифрованной папке процедура шифрования затрагивает только сохраненные в ней файлы, но не саму панку. Все файлы, создаваемые в зашифрованной папке и перемещаемые в нее, автоматически шифруются.

Чтобы зашифровать папку или файл, выполните следующие действия,

1. Щелкните файл или папку правой кнопкой и выберите Свойства (Properties).
2. На вкладке Общие **(General) щелкните** кнопку Другие **(Advanced) и выберите Шифровать** содержимое для **защиты** данных **(Encrypt** contents to **secure data). Затем два** раза щелкните OK.

Примечание Нельзя шифровать системные файлы, а также файлы, доступные только для чтения. При попытке сделать ото, вы увидите сообщение об ошибке.

Если в папке имеются вложенные папки, на экране появится запрос на их шифрование. Установите переключатель К этой папке и ко всем вложенным файлам и папкам (Apply changes to this folder, subfolders, and files) и щелкните OK.

Примечание На томах NTFS файлы при перемещении, копировании и переименовании остаются зашифрованными. Перед копированием или перемещением зашифрованного файла на диск в формате FAT или FAT32 он автоматически дешифруется.

Работа с зашифрованными файлами и папками

Ранее я говорил, что зашифрованные файлы и папки разрешается копировать, перемещать и переименовывать как любые другие файлы, никак не затрагивая их шифрование. Однако это верно лишь в большинстве случаев. При работе на томах NTFS одного компьютера проблем с зашифрованными файлами у вас практически не будет. Но они обязательно возникнут при работе с другими файловыми системами или другими компьютерами. Чаще всего проблемы возникают в двух случаях:

- при копировании или перемещении из тома NTFS в том FAT/FAT32 на одном компьютере зашифрованный файл перед переносом расшифровывается и переносится, как обычный файл. FAT и FAT32 не поддерживают шифрование;
- при копировании или перемещении из тома NTFS на одном компьютере в том NTFS на другом компьютере зашифрованного файла или папки файлы остаются зашифрованными при условии, что у вас есть право шифровать файлы на целевом компьютере и это допускается доверительными отношениями. В противном случае файлы перед переносом расшифровываются и переносятся, как обычные файлы. То же самое происходит при копировании или перемещении зашифрованного файла в том FAT или FAT32 на другом компьютере.

После переноса важного зашифрованного файла проверьте, что его шифрование сохранилось. Щелкните файл правой кнопкой мыши и выберите Свойства (Properties). На вкладке Общие (General) окна свойств щелкните Другие (Advanced). Флажок Шифровать содержимое для защиты данных (Encrypt contents to secure data) должен быть установлен.

Настройка политики восстановления EFS

На контроллерах домена и рабочих станциях *политики восстановления* (recovery policies) настраиваются автоматически. По умолчанию в домене агентом восстановления являются администраторы *домена*, а на *изолированных* рабочих *станциях* — локальный администратор.

Для просмотра, назначения и удаления агентов восстановления служит консоль Групповая политика (Group Policy). Вот как это делается.

1. Откройте консоль Групповая политика (Group Policy) для локального компьютера, сайта, домена или подразделения, с которыми собираетесь работать. Подробнее о работе с этой консолью — в главе 4.
2. Раскройте последовательно узлы Конфигурация компьютера (Computer Configuration), Конфигурация Windows (Windows Settings), Параметры безопасности (Security Settings), Политики открытого ключа (Public Key Policies) и Агенты восстановления шифрованных данных (Encrypted Data Recovery Agents).

3, На правой панели перечислены агенты восстановления, назначенные в данный момент (рис. 11-11). Также указано, кем выдан сертификат восстановления, срок его действия, назначение и пр.

Л. Чтобы назначить дополнительный агент восстановления, щелкните правой кнопкой элемент Файловая система EFS (Encrypting File System) и выберите Добавить агент восстановления данных (Add Data Recovery Agent). Будет запущен Мастер добавления агента восстановления (Add Recovery Agent Wizard). Щелкните Далее (Next). В окне Выбор агентов восстановления (Select Recovery Agents) щелкните Обзор каталога (Browse Directory) и найдите нужного пользователя.

Примечание Прежде чем назначать дополнительных агентов восстановления, следует определить в домене корневой центр сертификации (Certificate Authority, CA). Затем с помощью оснастки Сертификаты (Certificates) создайте личный сертификат на основе шаблона Агент восстановления EFS (EFS Recovery Agent). Чтобы сертификат стал активным, его должен одобрить корневой центр сертификации.

5. Чтобы удалить агента восстановления, выделите запись его сертификата и правой панели и нажмите Delete. Щелкните Да (Yes), чтобы подтвердить удаление. Если вы удалите все сертификаты, EFS будет выключена, а шифрование файлов прекратится.

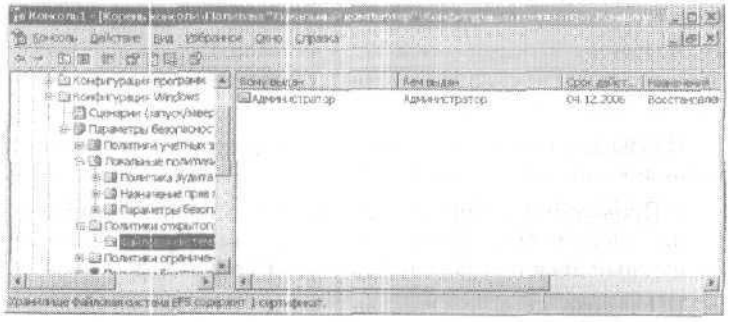


Рис. 11-11. С помощью этого узла назначаются и удаляются агенты восстановления

Расшифровка файлов и папок

Чтобы расшифровать файл или папку, выполните следующие действия.

1. В Проводнике (Windows Explorer) щелкните файл или папку правой кнопкой.
2. На вкладке Общие (General) окна свойств щелкните Другие (Advanced). Сбросьте флажок Шифровать содержимое для защиты данных (Encrypt contents to secure data) и два раза щелкните OK.

Отдельные файлы Windows Server 2003 дешифрует и сохраняет в первоначальном формате. При расшифровке папки Windows Server 2003 дешифрует все вложенные в нес файлы. Чтобы расшифровать и подпапки, в ответ на запрос установите переключатель К этой папке и ко всем вложенным файлам и папкам (Apply changes to this folder, subfolders, and files) и щелкните OK.

Совет В Windows Server 2003 имеется утилита командной строки CIPHER.EXE для шифрования и расшифровки информации. Введя ее без параметров, вы узнаете состояние шифрования всех элементов текущей папки.

Очистка дискового пространства

Утилита Очистка диска (Disk Cleanup) проверяет дисковые накопители на предмет наличия файлов, которые можно удалить. По умолчанию просматриваются папки для временных файлов, Корзина (Recycle Bin) и папки, используемые индексатором содержимого (Content Indexer). Кроме того, утилита находит файлы, которые давно не использовались, и предлагает их сжать. Сжатие старых файлов позволяет освободить значительное пространство на диске.

Чтобы запустить программу Очистка диска (Disk Cleanup), выполните следующие действия.

1. В Проводнике (Windows Explorer) или консоли Управление дисками (Disk Management) щелкните правой кнопкой нужный диск и выберите Свойства (Properties).
2. Щелкните кнопку Очистка Диска (Disk Cleanup). Чем больше файлов на диске, тем дольше продлится поиск. Когда он закончится, вы увидите отчет, подобный тому, что показан на рис. 11-12.

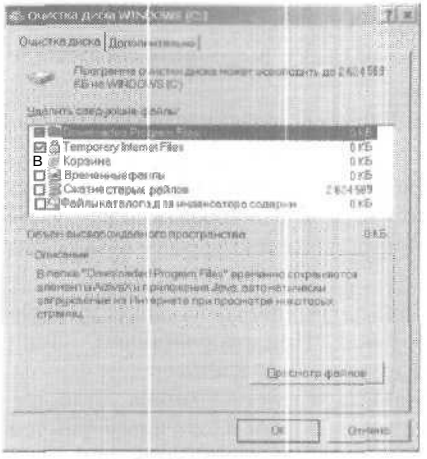


Рис. 11-12. Утилита Очистка Диска (Disk Cleanup) поможет найти файлы, которые можно удалить или сжать

- **Downloaded Program** Files — файлы, загруженные браузером, например элементы управления ActiveX и апплеты Java. Эти файлы удаляйте смело.
- **Temporary Internet** Files — Web-страницы, сохраненные в кэше браузера. Их тоже можно удалять, не задумываясь.
- **Корзина (Recycle Bin)** — файлы, удаленные из рабочих папок, но реально сохраняемые на компьютере. Прежде чем освободить Корзину (Recycle Bin), подумайте, действительно ли вы хотите навсегда избавиться от этих файлов.
- **Временные файлы (Temporary Files)** — как правило, рабочая информация различных приложений.
- **Временные автономные файлы (Temporary Offline Files)** — локальные копии недавно использованных сетевых файлов. Обеспечивают автономный доступ к сетевой информации, их можно удалить.
- **Автономные файлы (Offline Files)** — локальные копии сетевых файлов, на необходимость создания которых вы указали явным образом. Если вы удалите автономные файлы, не отменив этот параметр, они снова будут скопированы в ту же папку при очередном подключении к сети.

- **Сжатие старых файлов (Compress Old Files) — список** файлов, которые давно не использовались. По умолчанию файлы помечаются для возможного сжатия, если они не использовались в течение 50 дней. Этот интервал можно изменить, выделив элемент Сжатие старых файлов (Compress Old Files) и щелкнув кнопку Параметры (Options). Задайте в списке Сжимать после (Compress After) новый интервал и щелкните OK.
- **Файлы каталога для индексатора содержимого (Catalog files for the Content Indexer) — содержит старые каталоги, которые более не нужны. Эти файлы можно удалить.**

3. В списке Удалить следующие файлы (Files to Delete) выделите группы файлов, от которых хотите избавиться, и щелкните OK. Для подтверждения щелкните Да (Yes).

Глава 12

Администрирование наборов томов и RAID-массивов

При работе с серверами Microsoft Windows Server 2003 вам придется довольно часто выполнять дополнительную настройку дисков, например создавать наборы томов или настраивать RAID-массивы.

- **Набор томов** располагается на нескольких накопителях. Пользователи обращаются к нему, как к единому диску, независимо от того, по скольким накопителям том распределен на самом деле. Том, расположенный на одном диске, называется *простым* (simple), на нескольких дисках — *составным* (spanned).
- **RAID-массив, т.** е. *избыточный массив независимых дисков* (redundant array of independent disks, RAID) позволяет защитить данные, а порой и увеличить производительность дисков. В Windows Server 2003 поддерживается три уровня RAID: 0, 1 и 5. Вы можете настроить RAID-массивы для работы с дисками следующих типов — зеркальными, чередующимися и чередующимися с контролем четности.

Тома и массивы RAID создаются на динамических дисках и доступны только из Windows 2000 Server и Windows Server 2003. Если ваш компьютер настроен на загрузку еще и одной из предыдущих версий Windows, динамические диски в ней окажутся недоступны. Впрочем, компьютеры со старыми версиями Windows могут обращаться к таким дискам по сети, как к обычным сетевым дискам.

Использование томов и наборов томов

Том (volume) — это часть диска, где можно напрямую сохранять данные. Создание томов и управление ими во многом схоже с созданием и управлением *разделами* (partitions).

Примечание Если составной или чередующийся том находится на базовых дисках, вы можете только удалить, но не создать или расширить его. Если на базовых дисках располагаются зеркальные тома, вы вправе удалять, восстанавливать и синхронизировать зеркала. Зеркало можно и отключить. Если на базовых дисках находятся чередующиеся тома с контролем четности (RAID 5), вы вправе удалить или восстановить том, но не создать новый.

Основные понятия о томах

В оснастке Управление дисками (Disk Management), показанной на рис. 12-1, тома, как и разделы, выделяются различными цветами в зависимости от типа. Тома имеют следующие параметры:

- Расположение (Layout) — том, как уже говорилось, может быть простым, составным, зеркальным, чередующимся и чередующимся с контролем четности;
- Тип (Type) — у тома в этом столбце всегда указано Динамический (Dynamic);
- **Файловая система (File System) —** FAT, **FAT 32 или NTFS;**
- **Состояние (Status);**
- **Емкость (Capacity).**

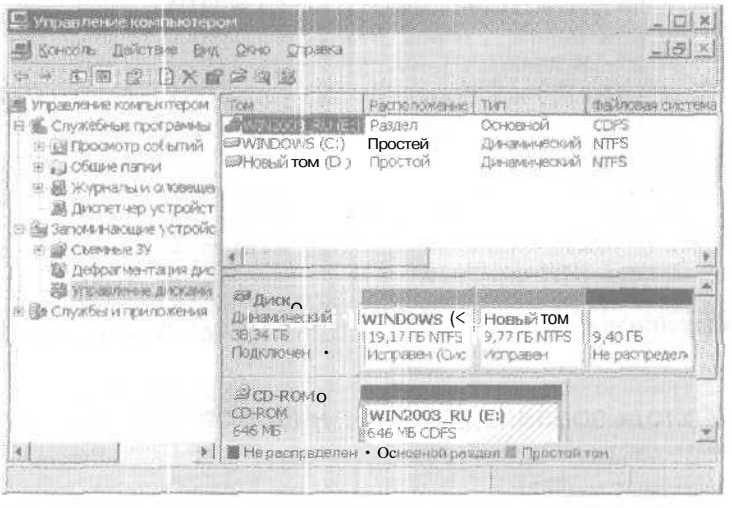


Рис. 12-1. В оснастке Управление дисками (Disk Management) показаны тома и разделы

Важное преимущество динамических томов перед базовыми — возможность вносить изменения *к* тома и диски без последующей перезагрузки системы (в большинстве случаев). Кроме того, тома позволяют задействовать средства отказоустойчивости Windows Server 2003. Хотя динамические диски нельзя использовать с предыдущими версиями Windows, вы вправе установить параллельно с Windows Server 2003 другую ОС, создав для нее отдельный том. Например, вы можете установить Windows Server 2003 на том C, а Linux — на том D.

Тома позволяют:

- назначать дискам буквы и пути (см. главу 11);
- создавать на диске любое количество томов при условии, что на нем есть свободное место;
- создавать тома, распределенные по двум и более дискам, и включать механизмы отказоустойчивости;
- расширять тома;
- назначать активный, системный и загрузочный тома (см. главу 11).

Понятие наборов томов

Наборы томов (volume sets) позволяют создать тома, распределенные по нескольким дискам. Таким образом, вы используете свободное пространство разных накопителей для создания тома, который будет представляться пользователю как единый носитель. Файлы записываются в набор томов последовательно сегмент за сегментом. Первый сегмент свободного пространства первым используется для записи файла. Когда данный сегмент заполнится, включается второй и т. д.

Вы можете создать набор, используя свободное пространство дисковых накопителей — числом до 32. Наборы томов позволяют эффективно задействовать свободное пространство и формируют удобную файловую систему. Но если один из накопителей в наборе откажет, выйдет из строя весь набор томов, т. е, все данные в наборе будут утеряны.

Постоянный контроль за состоянием тома полезен не только для выявления проблем, но и при установке новых томов на тех же накопителях. Текущее состояние тома отображается в оснастке Управление дисками (Disk Management) в графической области и в области списка дисков. Используемые при этом термины описаны в табл. 12-1.

Таблица 12-1. Возможные состояния тома

Состояние	Описание	Действие
Исправен (Healthy)	Никаких проблем на томе не обнаружено	Соответственно и делать ничего не нужно
Неисправен (Failed)	Диск недоступен или поврежден	Убедитесь, что соответствующий динамический диск подключен. При необходимости реактивируйте том
Неполные данные (Data Incomplete)	Составные тома на чужом диске неполны. Вы, вероятно, забыли добавить другие диски из составного набора томов	Добавьте диски с недостающими данными составного тома, а затем импортируйте все диски одновременно
Нет избыточности данных (Data not Redundant)	Отказоустойчивые тома на чужом диске неполны. Вы, вероятно, забыли добавить другие диски из зеркального набора или набора RAID-5	Добавьте остальные диски, а затем импортируйте все диски одновременно
Отказавшая избыточность (Failed Redundancy)	Отключен один из дисков зеркального набора или набора RAID-5	Убедитесь, что соответствующий динамический диск подключен. При необходимости реактивируйте том. Не исключено, что неисправный зеркальный том придется заменить, а неисправный том RAID-5 — восстановить
Регенерация (Regenerating)	Временное состояние. Производится регенерация данных и четности на томе RA1D-5	Дождитесь окончания процесса (в оснастке указано его выполнение в процентах). Затем том должен перейти в состояние Исправен (Healthy)
Ресинхронизация (Resync lung)	Временное состояние. Выполняется ресинхронизация зеркального набора	Дождитесь окончания процесса (в оснастке указано его выполнение в процентах). Затем том должен перейти в состояние Исправен (Healthy)
Устаревшие данные (Stale Data)	Данные на отказоустойчивых чужих дисках не синхронизированы	Повторно отсканируйте диски или перезагрузите компьютер. В столбце должно появиться новое состояние, например Отказавшая избыточность (Failed Redundancy)
Форматирование (Formatting)	Временное состояние. Том форматируется	Дождитесь окончания процесса (в оснастке указано его выполнение в процентах)

Создание томов и наборов томов

Том и набор томов создаются так.

1. В графической панели оснастки Управление дисками (Disk Management) щелкните правой кнопкой любую нераспределенную область динамического диска и выберите Создать том (Create Volume). Запустится Мастер создания томов (Create Volume Wizard). Щелкните Далее (Next).
2. Установите переключатель Простой том (Simple), чтобы создать том на одном диске, или Составной том (Spanned) для создания тома на нескольких дисках (рис. 12-2). Простые тома можно отформатировать под FAT, FAT32 или NTFS. Для упрощения управления дисками отформатируйте тома, объединяющие несколько дисков, под NTFS, так как NTFS позволяет расширять набор томов.

Рис. 12-2. Здесь выбирается тип тома

Примечание Если вам требуется дополнительное пространство на простом или составном томе, его можно расширить, выбрав область свободного пространства и добавив ее к тому. Том разрешается расширить как в пределах одного диска, так и на пространстве другого диска. В последнем случае создается составной том, диски которого должны иметь формат NTFS.

3. В диалоговом окне Выбор дисков (Select Disks) можно выбрать динамический диск для включения в том и задать размер сегмента тома на нем (рис. 12-3).

Рис. 12-3. Окно Выбор дисков (Select Disks) позволяет выбрать диски для размещения тома

4. Доступные динамические диски показаны в списке Доступны (Available). Выберите диск из этого списка и щелкните Добавить (Add), чтобы добавить диск в список Выбраны (Selected). Если вы ошиблись, можете удалить диск из списка, выбрав его и щелкнув Удалить (Remove).
5. Выберите диск из списка Выбраны (Selected) и в списке Выберите размер выделяемого пространства (МБ) [Select the amount of space in MBj задайте размер тома на диске. В поле Максимальное доступное пространство (Maximum available space) показан размер наибольшей области свободного пространства, доступной на выбранном диске. В ноле Общий размер тома (Total Volume Size) показан размер общего дискового пространства, выбранного для тома. Щелкните Далее (Next).

tfy Совет Поскольку простые и составные тома не являются отказоустойчивыми, лучше создать несколько небольших томов, чем один огромный, использующий все доступное пространство.

6. Укажите, будете ли вы назначать накопителю букву или путь, с помощью следующих параметров:
   - **Назначить** букву диска (A—Z) [Assign the following drive letter] — назначить букву диска (буква выбирается из списка);

- **Подключить том как пустую NTFS-папку (Mount in the following empty NTFS folder)** - назначить путь **диска (нужно указать путь к папке);**
- **Не назначать буквы диска или пути диска (Do not assign a drive letter or drive path) — назначить** букву **или путь позже.**

7. Щелкните Далее (Next) и определите, будете ли вы форматировать том (рис. 12-4). Если да, то вам следует задать необходимые параметры.

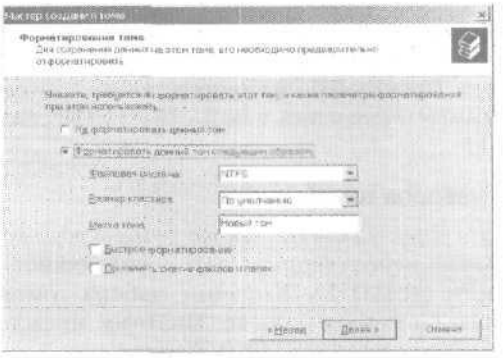


Рис. 12-4. Форматирование тома для определенной файловой системы

- **Файловая система (File System) — здесь выбирать** нечего, **единственный доступный вариант — NTFS.**
- Размер кластера (Allocation unit size) — здесь задастся размер базовой единицы выделения места на диске. По умолчанию размер кластера задается динамически до форматирования на основании размера тома, но вы вправе задать собственный размер. Это имеет смысл, если вы работаете с большим количеством очень маленьких файлов, — задав небольшой размер кластера (512 или 1024 байт), вы сэкономите немало места па диске.
- **Метка тома (Volume Label)** — текстовая метка.
- **Быстрое форматирование (Perform a quick format) —** форматирование выполняется без проверки раздела на наличие ошибок. На большом томе быстрое форматирование сэкономит вам несколько минут, но, по возмож-

ности, избегайте его. При обычном форматировании программа найдет на диске плохие секторы и пометит их, как непригодные для хранения данных.

- **Применять сжатие файлов и папок (Enable file and** folder compression) — включает сжатие данных на диске. Никаких изменений в работе пользователи не заметят: сжатие прозрачно для них. Если вы установите этот флажок, файлы и папки на этом диске будут сжиматься автоматически (подробнее — в главе 11).

8. Щелкните Далее (Next), а затем Готово (Finish). Если вы добавили тома на физический диск, содержащий Windows Server 2003, вы могли по неосторожности изменить номер загрузочного тома. Прочитайте предупреждения, а затем внесите необходимые изменения в файл BOOT.INI, как описано в главе 11.

Удаление томов и наборов томов

Одним и тем же способом удаляют любые тома: простые, составные, зеркальные, чередующиеся или чередующиеся с контролем четности (RAID 5). Удаление набора томов уничтожит файловую систему и данные. Поэтому, прежде чем это сделать, сохраните копии нужных файлов и каталогов с этого набора. Нельзя удалить том, содержащий загрузочные файлы или активные файлы подкачки Windows Server 2003.

Тома удаляют так.

1. В оснастке Управление дисками (Disk Management) правой кнопкой щелкните любой том в наборе и выберите Удалить том (Delete Volume). Вы не сможете удалить часть составного тома, не удалив весь том.
2. Подтвердите удаление тома, щелкнув Да (Yes).

Расширение простого или составного тома

Windows Server 2003 предлагает несколько способов расширения томов NTFS, не являющихся частью зеркального или чередующегося набора. Вы можете расширить простой том, а также существующие наборы томов. При расширении томов вы добавляете к ним свободное пространство.

Примечание При расширении наборов томов существует множество ограничений. Нельзя расширить загрузочные или

системные тома, зеркальные или чередующиеся тома, а также создать том, занимающий более 32 дисков. Нельзя расширить тома FAT или FAT32: сначала следует преобразовать их в NTFS. Нельзя расширить простые или составные тома, преобразованные из базовых дисков.

Вот как расширить том NTFS.

1. В оснастке Управление лисками (Disk Management) правой кнопкой щелкните простой или составной том, который хотите расширить, и выберите Расширить том (Extend Volume). Запустится Мастер расширения тома (Extend Volume Wizard). Прочитайте вступление и щелкните Далее (Next).
2. Выберите динамические диски, которые войдут в том, и задайте размеры сегментов тома на этих дисках, как описано в пп. 3-5 раздела «Создание томов и наборов томов».

Примечание Набор томов на нескольких накопителях не может быть зеркальным или чередующимся — ими могут быть только простые тома.

3. Щелкните Далее (Next), а затем Готово (Finish).

Управление томами

Тома управляются так же, как и разделы (подробнее — в главе 11).

Повышенная производительность и отказоустойчивость RAID-массивов

Важные данные требуют повышенной защиты от сбоев дисков. Для этого вы можете использовать технологию RAID, которая повышает отказоустойчивость системы за счет создания избыточных копий данных, а также позволяет увеличить производительность дисков.

Доступны разные реализации технологии RAID, описываемые уровнями. В настоящее время определены уровни от О до 5. Каждый обладает своими особенностями. В Windows Server 2003 поддерживаются уровни О, 1 и 5:

- RAID 0 позволяет увеличитьпроизводительность дисков;
- RAID 1 и 5повышают отказоустойчивость.

В табл. 12-2 дан краткий обзор поддерживаемых уровней RAID. Эта поддержка является полностью программной.

Таблица 12-2. Поддержка RAID под управлением Windows Server 2003

Уровень RAID	Тип RAID	Описание	Основные преимущества
0	Чередование дисков	Два или более томов, каждый на отдельном накопителе, сконфигурированы как чередующийся набор. Данные разбиваются на блоки, называемые полосами, и последовательно записываются на все диски в наборе	Скорость и производительность
1	Зеркальное отображение дисков	Два тома на двух дисках идентичны. Данные записываются на оба диска. Если один из накопителей отказывает, данные не теряются, так как второй диск содержит их копию	Избыточность. Выше скорость записи, чем у чередующегося набора с контролем четности
5	Чередование дисков с контролем четности	Использует три или более томов, каждый на отдельном накопителе, для создания чередующегося набора с контролем ошибок но четности. При сбое данные могут быть восстановлены	Отказоустойчивость с меньшими затратами, чем при зеркальном отображении. Быстрое чтение по сравнению с зеркальным отображением

На серверах Windows Server 2003 чаще применяют RAID **i (зеркальное** отображение дисков) и 5 (чередование с контролем четности). Первый способ защиты данных менее дорог: здесь используется два одинаковых но размеру тома на двух накопителях для создания избыточного набора данных. Если один из дисков откажет, вы сможете считать данные с другого.

Второй способ требует минимум три диска, но обеспечивает отказоустойчивость с меньшими затратами на единицу емкости, чем первый. Если любой из накопителей откажет, данные будут автоматически восстановлены путем комбинирования блоков данных рабочих дисков с записями четности. Четность (или контрольная сумма) — метод коррекции ошибок, который заключается *в* создании по специальному алгоритму значений, позволяющих восстановить потерянные данные.

Развертывание RAID на серверах Windows Server 2003

На серверных системах Windows Server 2003 поддерживаются зеркальное отображение дисков, чередование дисков и чередование дисков с контролем четности.

Примечание Некоторые ОС, например MS-DOS, не поддерживают RAID. Если на вашем компьютере установлены две ОС и одна из них не поддерживает RAID, RAID-диски будут для нее недоступны.

Развертывание RAID 0

RAID уровня 0 подразумевает чередование дисков. Два или более тома, каждый на отдельном накопителе, сконфигурированы как чередующийся набор. Данные, записываемые в набор, разбиваются па блоки — *полосы* (stripes). Полосы записываются последовательно на все диски чередующегося набора. Вы можете развернуть том чередующегося набора максимум на 32 дисках, по, как правило, наборы с 2-5 томами работают быстрее всего. Если число томов увеличивают, производительность резко падает.

Главное достоинство чередования дисков — скорость. Доступ к данным на нескольких дисках обеспечивается несколькими головками, что заметно повышает производительность. Но за это приходится платить надежностью. Как и в случае с наборами томов, если один из дисков чередующегося набора выйдет из строя, весь набор уже не удается использовать: все данные будут утеряны. Вам придется повторно создать чередующийся набор и восстановить данные из архивов. Об архивировании и восстановлении данных — в главе 15.

Примечание Загрузочные и системные тома не могут быть частью чередующегося набора.

При создании чередующихся томов надо использовать тома приблизительно одинакового размера. *Оснастка* Управление дисками (Disk Management) при вычислении общего объема набора основывается на размере наименьшего тома. В частности, максимальный размер набора кратен размеру наименьшего тома. Так, если у вас три физических диска и размер наименьшего тома — 50 Мбайт, то максимальный размер чередующегося набора будет 150 Мбайт.

Увеличить производительность чередующегося набора можно так:

- использовать диски, управляемые отдельными контроллерами, что позволит системе одновременно обращаться к нескольким дискам;
- не использовать диски, содержащие чередующийся набор, для других задач, чтобы диски только обслуживали набор.

Чередующийся набор создастся следующим образом.

1. В графической панели оснастки Управление дисками (Disk Management) щелкните правой кнопкой нераспределенную область динамического диска и выберите Создать том (Create Volume). Запустится мастер создания томов. Прочитайте вступление и щелкните Далее (Next).
2. Выберите вариант Чередующийся (Striped) и создайте том, как было описано выше. Главное отличие в том, что теперь вам понадобится минимум два динамических диска.

Чередующийся том можно использовать, как любой другой том. Вы не сможете расширить уже созданный чередующийся набор, поэтому аккуратно спланируйте его развертывание.

Развертывание RAID 1

RAID уровня 1 подразумевает зеркальное отображение дисков. При этом для создания избыточного набора данных используется два одинаковых по размеру тома на двух накопителях. На накопители записываются одинаковые наборы данных, и если один из дисков откажет, данные можно считать с другого.

Зеркальное отображение дисков обеспечивает приблизительно такую же отказоустойчивость, что и чередование дисков с четностью. Но поскольку в зеркальных наборах не генерируются контрольные суммы, как правило, запись на них осуществляется быстрее. С другой стороны, чередующиеся диски с четностью обеспечивают большую производительность чтения, так как операция чтения выполняется с нескольких дисков одновременно.

Основной недостаток зеркального набора — двойное сокращение емкости. Так, зеркало для накопителя емкостью 5 Гбайт

требует другого накопителя того же объема. А значит, для хранения 5 Гбайт информации потребуется 10 Гбайт.

Примечание В отличие от чередования дисков, при зеркальном отображении дисков вы можете «отразить» любой том, а значит, в случае необходимости создать зеркало для загрузочных или системных томов.

Как и при чередовании, желательно, чтобы зеркальные диски обслуживались разными дисковыми контроллерами. Это обеспечит большую защиту от сбоев дисковых контроллеров. Если один из контроллеров откажет, применяется диск на другом контроллере. Фактически, используя два дисковых контроллера для дублирования данных, вы реализуете технологию *дублирования дисков* (disk duplexing). При простом зеркальном отображении дисков обычно используют один дисковый контроллер, а при дублировании — два (рис. 12-5).

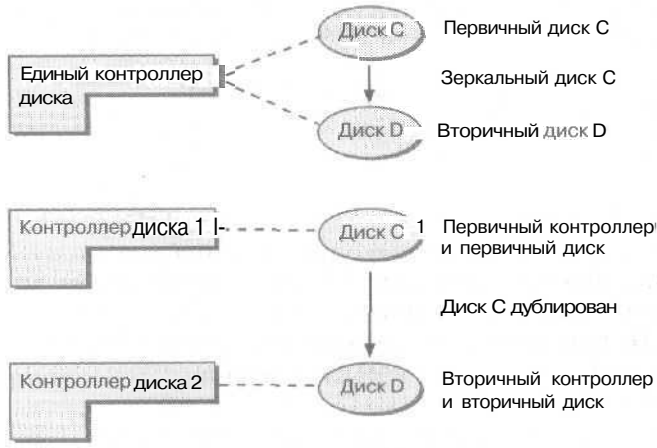


Рис. 12-5. При простом зеркальном отображении дисков используется один дисковый контроллер, а при дублировании - два

Если один из зеркальных дисков откажет, дисковые операции могут продолжаться. При записи и чтении данные записываются на оставшийся в работе диск. Перед восстановлением зеркала его следует отключить (см. раздел «Управление RAID и восстановление после сбоев»).

Создание зеркального набора

1. В графической панели оснастки Управление дисками (Disk Management) щелкните правой кнопкой нераспределенную область динамического диска и выберите Создать том (Create Volume). Запустится мастер создания томов. Щелкните Далее (Next).
2. Выберите Зеркальный (Mirrored) и создайте том, как описано в разделе «Создание томов и наборов томов». Основное отличие в том, что вам необходимо создать два одинаковых по размеру тома на разных динамических дисках.

Как и другие RAID-технологии, зеркальное отображение прозрачно для пользователей. Пользователи видят зеркальный набор, как обычный диск, и могут обращаться к нему, как к любому другому диску.

Примечание Нормальное состояние зеркального набора — Исправен (Healthy). В процессе создания зеркала вы можете увидеть состояние Ресинхронизация (Resynching).

Зеркальное отображение существующих томов

Для создания зеркального набора годится существующий простой том. На втором динамическом диске должно быть столько же неразмеченного пространства, сколько на существующем томе, или больше.

Для зеркального отображения существующего тома в оснастке Управление дисками (Disk Management) необходимо выполнить следующие действия.

1. Правой кнопкой щелкните простой том, для которого хотите создать зеркальное отображение, и выберите Добавить зеркало (Add Mirror). Запустится мастер добавления зеркала.
2. Выберите в списке Диски (Disks) расположение зеркала и щелкните Добавить зеркало (Add Mirror). Windows Server 2003 начнет процесс создания зеркала, в ходе которого в столбце состояния обоих томов будет отображаться Ресинхронизация (Resynching).

Развертывание RAID 5

RAID уровня 5 подразумевает чередование дисков с контролем четности. Для реализации этой технологии нужно минимум

три жестких диска. Оснастка Управление дисками (Disk Management) сделает размеры томов на этих дисках одинаковыми.

По сути, RAID 5 — расширенная и отказоустойчивая версия RAID 1. Отказоустойчивость гарантирует, что сбой одного диска не повлияет на работу всего набора. Набор будет функционировать, направляя дисковые операции на оставшиеся в рабочем состоянии тома.

. Для обеспечения отказоустойчивости RAID 5 записывает вместе с блоками данных контрольную сумму. Если один из дисков набора выйдет из строя, вы сможете использовать информацию о четности для восстановления данных (подробнее об этом процессе — в разделе «Восстановление чередующегося набора с контролем четности».) При отказе двух дисков информации о четности недостаточно для восстановления данных, и вам придется восстанавливать набор из архива.

Создание чередующегося набора с контролем четности

1. В графической панели оснастки Управление дисками (Disk Management) щелкните правой кнопкой нераспределенную область динамического диска и выберите Создать том (Create Volume). Запустится мастер создания томов. Щелкните Далее (Next).
2. Установите переключатель RAID-5 и создайте том, как описано в разделе «Создание томов и наборов томов». Основное отличие — вам нужно выбрать свободное пространство на трех отдельных динамических дисках.

К созданному чередующемуся набору пользователи могут обращаться, как к обычному диску. Но помните: вам не удастся расширить уже созданный чередующийся набор, добавив дополнительные диски или заменив диски на более емкие. Поэтому особенно аккуратно спланируйте набор перед его развертыванием.

Управление RAID и восстановление после сбоев

Управление зеркальными и чередующимися наборами отличается от управления другими дисковыми томами, особенно при восстановлении после сбоя.

Разрушение зеркального набора

Отключают зеркало по двум причинам:

- при отказе одного из дисков зеркального набора операции записи и чтения данных производятся с оставшегося диска. Перед восстановлением зеркала надо разрушить набор;
- зеркальное отображение дисков больше не требуется, и вы хотите освободить место на зеркальном диске в других целях.

Совет Хотя разрушение зеркала не влечет удаления данных, следует всегда делать архивные копии перед выполнением этой процедуры. Тогда при возникновении проблем вы сможете восстановить данные.

Зеркало разрушают с помощью оснастки Управление дисками (Disk Management).

1. Щелкните один из томов зеркального набора правой кнопкой и выберите Разделить зеркальный том (Break Mirrored Volume).
2. Подтвердите желание разрушить зеркало, щелкнув Да (Yes). Будет создано два независимых тома.

Ресинхронизация и восстановление зеркального набора

Windows Server 2003 автоматически синхронизирует зеркальные тома на динамических дисках, но данные на зеркальных дисках могут рассинхронизироваться. Так, если один диск отключается, данные записываются только на подключенный диск.

Вы можете ресинхронизировать или восстановить зеркальные наборы на базовых и динамических дисках, но для этого нужно перестроить набор на базе диска того же типа. Для ресинхронизации отказавшего дискового набора выполните следующие действия.

1. Убедитесь, что оба диска зеркального набора подключены и доступны, и проверьте статус зеркального набора — Отказавшая избыточность (Failed Redundancy). Предпринимаемые вами действия зависят от статуса отказавшего тома.
2. Если в столбце состояния отображается Отсутствует (Missing) или Не подключен (Offline), убедитесь, что на диск подается электропитание и он правильно подключен.

Затем запустите Управление дисками (Disk Management), правой кнопкой щелкните отказавший том и выберите Реактивизировать диск (Reactivate Disk). Статус диска должен измениться на Регенерация (Regenerating), а затем на Исправен (Healthy). Если статус не поменялся на Исправен (Healthy), щелкните том правой кнопкой и выберите Ресинхронизация зеркала (Resynchronize Mirror).

3. Если статус — Работает (ошибки) [Online (Errors)], щелкните правой кнопкой отказавший том и выберите Реактивизировать диск (Reactivate Disk). Статус диска должен измениться на Регенерация (Regenerating), а затем па Исправен (Healthy). Если статус не поменялся на Исправен (Healthy), щелкните том правой кнопкой и выберите Ресинхронизация зеркала (Resynchronize Mirror).
4. Если один или несколько дисков помечены Не читается (Unreadable), вам, возможно, надо повторить сканирование дисков в системе, выбрав команду Повторить сканирование дисков (Rescan Disks) из меню Действие (Action). Если статус дисков не изменился и после этого, перезагрузите компьютер.
5. Если один из дисков так и не вернулся в подключенное состояние, щелкните правой кнопкой отказавший том и выберите Удалить зеркало (Remove Mirror). Затем правой кнопкой щелкните оставшийся том зеркала и укажите Добавить зеркало (Add Mirror). Вам понадобится неразмеченная область для зеркального отображения тома. Если на диске нет свободного места, удалите другие тома или замените отказавший диск.

Восстановление зеркального системного диска с возможностью загрузки

Сбой зеркального диска иногда мешает загрузке системы. Обычно это происходит, когда в процессе зеркального отображения системного или загрузочного диска отказывает основной зеркальный диск. Б предыдущих версиях Windows для возвращения системы в работоспособное состояние приходилось немало потрудиться. В Windows Server 2003 в большинстве случаев от сбоя основного зеркального диска оправиться довольно легко.

При зеркальном отображении системного тома в файл BOOT.INI должна быть добавлена строка, позволяющая загружаться со вторичного зеркального диска. Выглядит она примерно так:

```
multi(0)disk(0)rdisk(2)partition(2)\WINNT="Boot Mirror D: - secondary plex"
```

Загрузившись со вторичного диска, укажите время для восстановления зеркала. Для этого следует выполнить следующие действия.

1. Выключите компьютер и замените неисправный том или установите дополнительный жесткий диск. Включите компьютер.
2. Разделите зеркало, а затем воссоздайте его на замененном диске, обычно диске 0. Щелкните правой кнопкой оставшийся том, который был частью исходного зеркала и выберите Добавить зеркало (Add Mirror). Далее следуйте указаниям из раздела «Зеркальное отображение существующих томов».
3. По завершении создания зеркального отображения повторно разрушьте зеркало из оснастки Управление дисками (Disk Management). Убедитесь, что основной диск в оригинальном зеркальном наборе получил букву, которая ранее была у набора. Если это не так, назначьте соответствующую букву.
4. Правой кнопкой щелкните оригинальный системный том и выберите Добавить зеркало (Add Mirror). Зеркало будет воссоздано.
5. Измените файл BOOT.INI, чтобы система загружалась с исходного системного диска.

Удаление зеркального тома

Из оснастки Управление дисками (Disk Management) можно удалить один из томов зеркального набора. Когда вы это сделаете, все данные с удаленного тома будут стерты, а освободившееся пространство помечается как нераспределенное.

Зеркальный том удаляется так.

1. В оснастке Управление дисками (Disk Management) щелкните правой кнопкой один из томов зеркального набора и выберите Удалить зеркало (Remove Mirror).

2. Укажите диск, с которого следует удалить зеркало.
3. Подтвердите свои действия. Все данные на удаленном томе будут уничтожены.

Внимание! Если на зеркале содержится системный или загрузочный раздел, перед удалением узнайте из файла BOOT.INI, который из дисков зеркала не нужен при загрузке. Например, если для загрузки используется диск rdisk(1) и вы можете удалить зеркало с диска Disk 1 или Disk 2, нужно удалять его с диска Disk 2.

Восстановление чередующегося набора без контроля четности

Такой чередующийся набор не обеспечивает отказоустойчивости. Если один из дисков в наборе откажет, весь набор становится непригодным. Нужно восстановить или заменить отказавший накопитель, воссоздать набор, а затем восстановить данные из архива.

Восстановление чередующегося набора с контролем четности

RAID 5 позволяет восстановить чередующийся набор при отказе одного диска. Об отказе диска вы узнаете по содержимому столбца состояния. Для набора оно изменится на Отказавшая избыточность (Failed Redundancy), а для отдельного тома — на Отсутствует (Missing), Не подключен (Offline) или Работает (ошибки) [Online (Errors)].

Вы можете восстановить RAID 5 на базовых или динамических дисках, по при перестроении набора необходимо использовать тот же тип дисков, что применялся па нем ранее.

1. Убедитесь, что все диски набора RAID 5 подключены. Статус набора должен быть Отказавшая избыточность (Failed Redundancy). Ваши действия зависят от статуса отказавшего тома.

Совет По возможности сделайте архивные копии данных перед выполнением этой процедуры.

2. Если статус — Отсутствует (Missing) или Не подключен (Offline), убедитесь, что на диск подается электропитание и он правильно подключен. Затем запустите оснастку Управление дисками (Disk Management), правой кнопкой

щелкните отказавший том и выберите Реактивизировать диск (Reactivate Disk). Статус диска должен измениться на Регенерация (Regenerating), а затем на Исправен (Healthy). Если стагус не поменялся на Исправен (Healthy), правой кнопкой щелкните том и выберите Восстановить четность (Regenerate Parity).

3. Если статус — Работает (ошибки) [Online (Errors)], правой кнопкой щелкните отказавший том и выберите Реактивизировать диск (Reactivate Disk). Статус диска должен измениться на Регенерация (Regenerating), а затем на Исправен (Healthy). Если статус не поменялся на Исправен (Healthy), щелкните правой кнопкой том и выберите Восстановить четность (Regenerate Parity).
4. Если один или несколько дисков помечены Не читается (Unreadable), возможно, следует отсканировать диски в системе, выбрав команду Повторить сканирование дисков (Rescan Disks) из меню Действие (Action). Если статус дисков не изменился, перезагрузите компьютер.
5. Если один из дисков так и не вернулся к подключенному состоянию, восстановите сбойную область набора RAID 5. Правой кнопкой щелкните отказавший том и щелкните Удалить (Remove). Затем выберите неразмеченную область на отдельном динамическом диске набора. Она должна быть не меньше восстанавливаемой области. Свободное место должно располагаться на диске, не используемом в текущий момент набором RAID 5. Если свободного места не хватает, команда Восстановить том (Repair Volume) недоступна: освободите дисковое пространство, удалив другие тома или заменив отказавший накопитель.

Глава 13

Управление файлами и папками

Microsoft Windows Server 2003 предоставляет мощные средства для работы с файлами и папками. В основе УТИХ средств — два базовых типа файловых систем:

- файловая система, основанная на таблице размещения файлов (File Allocation Table, FAT) и существующая в 16-битной и 32-битной версиях;
- файловая система Windows NT (Windows NT file system, NTFS) версий 4.0 и 5.0.

Файловые структуры Windows Server 2003

Информация, приведенная в этом разделе, поможет вам понять основы организации файлов в Windows Server 2003.

Основные свойства FAT и NTFS

Возможности работы с файлами и папками в Windows Server 2003 зависят от типа файловой системы. Серверы и рабочие станции Windows Server 2003 поддерживают FAT и NTFS.

Тома FAT

На томах FAT состояние файлов и папок отслеживается *по* таблице размещения. Возможности FAT ограничены, хотя и обеспечивают основные функции работы с файлами и папками. В Windows Server 2003 поддерживает две версии FAT (табл. 13-1):

- **FAT16** широко используется в Microsoft Windows NT 4.0. FAT16 поддерживает 16-битную таблицу размещения файлов, обычно ее называют просто FAT. Эта система оптимальна для томов размером менее 2 Гбайт;
- **FAT32** появилась во втором выпуске Windows 95 (OSR 2) и Windows 98. FAT32 поддерживает 32-битную таблицу раз-

мещения файлов и кластеры меньшего размера, чем FAT. за счет чего эффективнее использует пространство диска. В Windows Server 2003 FAT32 поддерживает тома размером до 32 Гбайт.

Таблица 13-1. Сравнение характеристик FAT и FAT32

Характеристика	FAT	FAT32
Размер элемента таблицы размещения файлов	16 бит	32 бита
Максимальный размер раздела	4 Гбайт; наилучший до 2 Гбайт	2 Тбайт; в Windows Server 2003 ограничен до 32 Гбайт
Максимальный размер файла	2 Гбайт	4 Гбайт
Поддерживается операционными системами	MS-DOS, все аерсии Windows	Windows 95 OSR2. Windows 98, Windows Me, Windows XP. Windows 2000 и Windows Server 2003
Поддерживает малый размер кластеров	Нет	Да
Поддерживает возможности NTFS 4.0	Нет	Нет
Поддерживает возможности NTFS 5.0	Нет	Нет
Используется на дискетах	Да	Да
Используется на съемных носителях	Да	Да

Использование NTFS

NTFS предлагает мощные средства для работы с файлами и папками. Существуют две версии NTFS.

- **NTFS 4.0** используется в Windows NT 4.0. Полностью поддерживает управление локальным и удаленным доступом к файлам и папкам, а также технологии сжатия Windows. Не поддерживает большую часть возможностей файловой системы Windows 2000 и Windows Server 2003.
- NTFS 5.0 применяется в Windows 2000 и Windows Server 2003. Полностью поддерживает такие возможности, как служба каталогов Active Directory, дисковые квоты, сжатие, шифрование и др. Эта система поддерживается полностью в Windows 2000 и Windows Server 2003 и частично — в Windows NT 4.0 SP4 или более поздних выпусках.

Примечание Если вы создали разделы NTFS в Windows NT 4.0 и обновили систему до Windows 2000 или Windows Server 2003, разделы до NTFS 5.0 автоматически не обновляются. Вам придется явно выбрать обновление разделов при установке ОС или при установке Active Directory на сервер.

В табл. 13-2 кратко сравниваются характеристики NTFS 4.0 и NTFS 5.O. Системы Windows NT 4.0 SP4 или более поздние могут обращаться к файлам и папкам NTFS 5.0, но не используют все новые возможности NTFS.

Таблица 13-2. Сравнение характеристик NTFS 4.0 и NTFS 5.0

Характеристика	NTFS 4.0	NTFS 5.0
Максимальный размер раздела	32 Гбайт	2 Тбайт на дисках с главной загрузочной записью (MBR) и 18 экзабайт на дисках GPT (GUID Partition Tabie)
Максимальный размер файла	32 Гбайт	Ограничен только размером тома
Поддерживается операционными системами	Windows NT 4.0. Windows 2000, Windows Server 2003	Windows 2000, Windows Server 2003 и Windows NT 4.0 SP 4
Расширенные права доступа к файлам	Да	Да
Поддерживает сжатие Windows	Да	Да
Поддерживает шифрование Windows	Нет	Да
Поддерживает структуры Active Directory	Нет	Да
Поддерживает разреженные файлы	Нет	Да
Поддерживает внешнее хранилище	Нет	Да
Поддерживает дисковые квоты	Нет	Да
Используется на дискетах	Нет	Нет
Используется на съемных носителях	Да	Да

Имена файлов

Соглашения Windows Server 2003 об именах применяются и к файлам, к к панкам. Мы для простоты будем говорить только об именах файлов, подразумевая, что сказанное относится также и к папкам. Допускается, чтобы имена файлов в Windows Server 2003 содержали и прописные, и строчные буквы, но это влияет только на их отображение. С точки зрения системы имена от регистра не зависят. Это значит, что вы можете сохранить файл MyBook.doc и имя файла будет показано именно в таком виде. Однако вам не удастся сохранить в той же папке файл mybook.doc.

И NTFS, и FAT32 поддерживают длинные имена файлов — до 255 символов. Допустимо в названиях файлов применять почти все символы, включая пробелы, кроме:

? * / \ : - < > |

Совет Пробелы в именах файлов иногда вызывают проблемы с доступом к ним. При ссылке на такой файл может понадобиться взять его имя в кавычки. Если вы планируете опубликовать файл в Интернете, удалите из его имени все пробелы или замените их символами подчеркивания (_), чтобы браузеры гарантированно получили доступ к нему.

Допустимы следующие имена файлов:

- My Favorite Short Story.doc;
- My_Favorite_Short_Story.doc;
- My..Favorite..Short..Story.doc;
- My Favorite Short Story!!!.doc;
- Мой любимый_короткий..рассказ!.doc.

Доступ к длинным именам файлов из MS-DOS

В MS-DOS с 16-битной файловой системой FAT имена файлов и папок ограничены 8 символами и 3 символами расширения файла, например CHAPTER4.TXT. Это соглашение об именах часто называют правилом «8.3» или стандартным правилом именования файлов MS-DOS. При обращении к файлам и папкам с длинными именами из утилит командной строки возможны проблемы.

Для поддержки доступа к длинным именам для всех файлов и папок в системе создаются сокращенные имена, соот-

ветствующие стандартным правилам именования файлов MS-DOS. Чтобы увидеть сокращенные имена файлов, вводят команду:

```
dir /X
```

Обычно сокращенное имя файла выглядит примерно так:

```
PROGRA~1.DOC
```

Как Windows Server 2003 создает сокращенное имя файла

Windows Server 2003 создает сокращенное имя файла из длинного по следующим правилам:

- все пробелы в имени файла удаляются — имя файла My Favorite Short Story.doc превращается в MyFavoriteShort-Story.doc;
- удаляются все точки в имени файла, кроме точки, отделяющей имя файла от его расширения. Имя файла My..Favorite..Short..Story.doc превращается в My Fa voriteShort Story.doc;
- недопустимые по правилам именования файлов в MS-DOS символы заменяются символом подчеркивания (_) — имя файла My[Favorite]ShortStory.doc превращается в My_Favorite_ShortStory.doc;
- все оставшиеся символы переводятся в верхний регистр — имя файла My Favorite Short Story.doc превращается в MY-FAVORITESHORTSTORY.DOC.

Затем применяются правила сокращения для создания стандартного имени файла MS-DOS.

Правила сокращения

Для приведения к виду «8.3» имя файла и его расширение сокращаются, если это необходимо:

- расширение файла сокращается до первых трех символов: имя файла Mary.text становится MARY.TEX;
- имя файла сокращается до первых 6 символов (это корневое имя файла), и добавляется уникальный указатель вида *~n*, где *n* — номер файла с 6-символьным именем: имя файла My Favorite Short Story.doc превращается в MYFA-VO~1.DOC; второй файл в той же папке, у которого имя сократится до MYFAVO, станет MYFAVO~2.DOC.

Примечание Если у вас много файлов с похожими именами, вы можете увидеть результат применения другого правила создания короткого имени файла. Если более 4 файлов используют одинаковый 6-символьный корень, дополнительные имена файлов создаются комбинацией первых двух символов имени файла и 4-символьного кода с добавлением после него уникального указателя. Если в папке хранятся файлы MYFAVO~1.DOC, MYFAVO~2.DOC, MYFAVO~3.DOC и MYFAVO~4.DOC, дополнительные файлы с этим корнем могут быть названы MY3140~1.DOC, MY40C7~1.DOC, и MYEACC~1.DOC.

Советы по работе с файлами, папками и дисками

В Windows Server 2003 предусмотрено много способов работы с файлами и папками. Наиболее часто применяются такие операции, как копирование и перемещение. Они реализуются как в пределах одного окна, так и между окнами.

Просмотр свойств файла и папки

Проводник (Windows Explorer), папки Мой компьютер (My Computer) и Сетевое окружение (My Network Places) позволяют просматривать свойства файлов и папок одним из двух способов:

- щелкнув правой кнопкой значок файла или папки и выбрав команду Свойства (Properties);
- выделив файл или папку, а затем выбрав команду Свойства (Properties) из меню Файл (File).

На рис. 13-1 показано окно свойств папки на томе NTFS. Вкладка Общие (General) отображает краткую информацию о папке и позволяет назначить атрибуты, перечисленные далее:

- Только **чтение** (Read-Only) — показывает, предназначены ли файл или папка только для чтения. Такой файл или папку нельзя изменить или случайно удалить;
- **Скрытый (Hidden)** -- определяет, отображается ли файл в списках. Вы можете перекрыть действие этого атрибута, разрешив Проводнику отображать скрытые файлы;
- **Другие (Advanced)** - позволяет пометить файл как сжатый, шифрованный и архивированный.

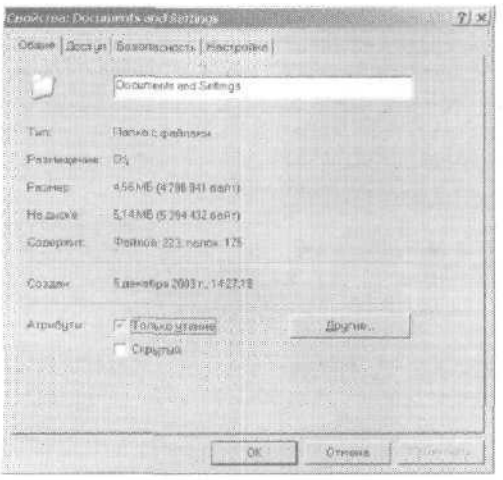


Рис. 13-1. Окна свойств для файла и папки похожи

Отображение скрытых и сжатых файлов в Проводнике

Администратору часто приходится просматривать системные файлы типа динамически подключаемых библиотек (dynamic-link library, DLL), а также сжатые или несжатые файлы. Но по умолчанию Проводник не показывает файлы с атрибутом «скрытый», как не показывает разницу между сжатыми и несжатыми файлами. Чтобы изменить начальные параметры, в меню Сервис (Tools) выберите команду Свойства папки (Folder Options) и перейдите на вкладку Вид (View), показанную на рис. 13-2:

- чтобы отобразить скрытые файлы, установите переключатель Показывать скрытые файлы и папки (Show hidden files and folders);
- чтобы всегда отображать расширения файлов, сбросьте флажок Скрывать расширения для зарегистрированных типов файлов (Hide file extensions for known file types);
- чтобы отобразить скрытые файлы ОС, сбросьте флажок Скрывать защищенные системные файлы (Hide protected operating system files);
- для подсвечивания сжатых файлов и папок установите флажок Отображать сжатые файлы и папки другим цветом (Display compressed files and folders with alternate color).

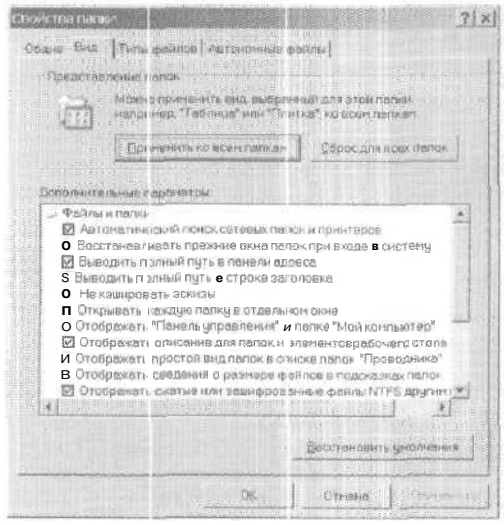


Рис. 13-2. Параметры Проводника настраиваются в диалоговом окне Свойства папки (Folder Options)

Выделение файлов и папок

Отдельный файл или несколько файлов в Проводнике можно выделить по-разному. Одиночный файл выделяется щелчком. Чтобы выделить несколько файлов:

- по очереди щелкните нужные файлы при нажатой клавише Ctrl;
- щелкните первый и последний файл при нажатой клавише Shift.

Копирование и перемещение файлов и папок перетаскиванием

Вы можете скопировать или переместить объекты в любое открытое окно или видимую область на рабочем столе.

1. Выберите объекты, которые хотите скопировать или переместить.
2. Перетащите эти объекты в новое место мышью.
3. Если вы перетаскиваете файл или папку на другой диск, они автоматически копируются. Чтобы переместить файл, при перетаскивании удерживайте нажатой клавишу Shift.

4. Если вы перетаскиваете файл или папку в новое место на том же диске, Windows Server 2003 перемещает этот объект. Для предотвращения этого при перетаскивании удерживайте нажатой клавишу Ctrl.

Примечание При копировании и перемещении перетаскиванием исходное местоположение файла и место назначения должны быть видны. Это значит, что вам может понадобиться открыть несколько копий Проводника или несколько окон и раскрыть папки внутри этих окон.

Копирование файлов и папок в места, которые не отображаются в данный момент

Проводник позволяет скопировать объекты в места, не отображаемые в данный момент.

1. Выделите **объекты** для **копирования и** перетащите их **в панель** папок.
2. Медленно подтащите объекты к самой верхней или к самой нижней папке, видимой на панели. Дерево папок начнет прокручиваться вверх или вниз.
3. Дойдя до папки назначения, отпустите кнопку мыши. Если эта папка находится на другом диске, объект скопируется; в противном случае он будет перемещен.

Копирование и вставка файлов

Я предпочитаю перемещать файлы с помощью операций копирования и вставки. При этом не нужно беспокоиться о том, был файл скопирован или перемещен. Вы просто копируете файлы в буфер обмена и вставляете их, куда нужно. Так можно даже скопировать файл в ту же самую папку — перетаскиванием вы бы этого никогда не добились.

1. Выделите объекты, которые хотите скопировать, щелкните их правой кнопкой и выберите Копировать (Copy). Команда Копировать (Copy) доступна также из меню Правка (Edit) или при нажатии клавиш Ctrl+C.
2. Щелкните правой кнопкой целевую папку и выберите команду Вставить (Paste). Вы также можете выбрать Вставить (Paste) из меню Правка (Edit) или нажать Ctrl+V.

Примечание Windows Server 2003 обычно не копирует файлы и папки в специальные окна. Например, как правило,

нельзя скопировать файлы и затем вставить их в окно Мой компьютер (My Computer).

Перемещение файлов вырезанием и вставкой

1. Выделите объекты, которые хотите переместить, щелкните их правой кнопкой и выберите Вырезать (Cut). Команда Вырезать (Cut) доступна также из меню Правка (Edit) или при нажатии клавиш Ctrl+X.
2. Щелкните правой кнопкой целевую панку и выберите команду Вставить (Paste). Вы также можете выбрать Вставить (Paste) из меню Правка (Edit) или нажать Ctrl+V.
3. Когда появится запрос на подтверждение перемещения выбранных объектов, щелкните OK.

Примечание Когда вы используете команды Вырезать (Cut) и Вставить (Paste), Windows Server 2003 не сразу удаляет объект из первоначального местоположения. Команда Вырезать (Cut) просто копирует объект в буфер обмена. Файл удаляется со старого места после команды Вставить (Paste).

Форматирование дискет и других съемных носителей

Проводник упрощает работу с дискетами и другими съемными носителями. Например, он позволяет форматировать диски.

1. Вставьте дискету или другой съемный диск, который хотите отформатировать.
2. Правой кнопкой щелкните соответствующий значок на панели папок Проводника.
3. В контекстном меню выберите Форматировать (Format), затем задайте параметры форматирования в диалоговом окне. Для дискет доступна только файловая система FAT. Для других типов съемных дисков, например Zip, можно использовать FAT, FAT32 или NTFS.

Примечание Если вы форматируете съемный диск как раздел NTFS, на нем создается раздел NTFS 5.O. Windows 2000 и Windows Server 2003, в отличие от Windows NT 4.0, позволяют извлечь раздел, отформатированный как NTFS, в любой момент. Щелкните кнопку выброса на дисководе или правой кнопкой щелкните значок диска в Проводнике Windows и выберите Извлечь (Eject).

4. Щелкните Начать (Start).

Копирование дискет

1. Правой кнопкой щелкните значок дискеты на панели папок Проводника и из контекстного меню выберите Копировать диск (Copy Disk).
2. Укажите исходный диск в поле Копировать из (Copy From) и диск назначения в поле Копировать в (Copy To). Если у вас на компьютере только один дисковод для гибких дисков, значения в этих полях совпадут (рис. 13-3).
3. Щелкните Start (Начать), а затем после соответствующих подсказок вставьте исходный диск и диск назначения. Индикатор в нижней части окна копирования диска показывает состояние процесса.

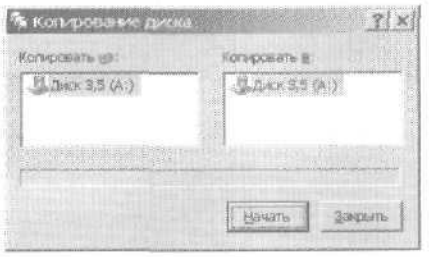


Рис. 13-3. Это диалоговое окно служит для копирования дискет

Глава 14

Общий доступ к данным, безопасность и аудит

Общий доступ к данным позволяет удаленным пользователям обращаться к сетевым ресурсам: файлам, папкам и дискам. Когда вы делаете общими папку или диск, все их файлы и вложенные папки становятся доступны другим пользователям сети. Управлять доступом к определенным файлам и вложенным папкам в общей папке можно только на разделах файловой системы NTFS, где для предоставления и запрета доступа к файлам и папкам служат списки управления доступом (access control lists, ACL).

Разрешения безопасности относятся ко всем ресурсам разделов NTFS — файлам, папкам и объектам службы каталогов Active Directory. Обычно только администраторы имеют право управлять объектами Active Directory, но вы можете делегировать эти полномочия другим пользователям, открыв им доступ к информации в Active Directory для просмотра и изменения. Разрешения для пользователей задаются в списках управления доступом. Отслеживая доступ к объектам, вы сможете детально контролировать сетевую активность и обеспечивать доступ к ресурсам только авторизованным пользователям.

Общий доступ к папкам на локальных и удаленных системах

Общие ресурсы открыты для доступа удаленных пользователей. Разрешения для общих папок не распространяются на пользователей, регистрирующихся локально на сервере или на рабочей станции, где расположены эти общие папки.

- Для предоставления удаленным пользователям доступа к файлам в своей сети служат стандартные разрешения доступа к папкам.

- Для предоставления удаленным пользователям доступа к файлам из Web применяется Web-доступ, реализуемый, только если на системе установлены службы Internet Information Services.

Просмотр имеющихся общих ресурсов

Вы можете просмотреть общие папки на локальном или удаленном компьютере.

1. В консоли Управление компьютером (Computer Management) подключитесь к нужному компьютеру.
2. В дереве консоли раскройте последовательно узлы Служебные программы (System Tools) и Общие папки (Shared Folders), затем выберите Общие ресурсы (Shares). Будут отображены текущие общие ресурсы системы (рис. 14-1).

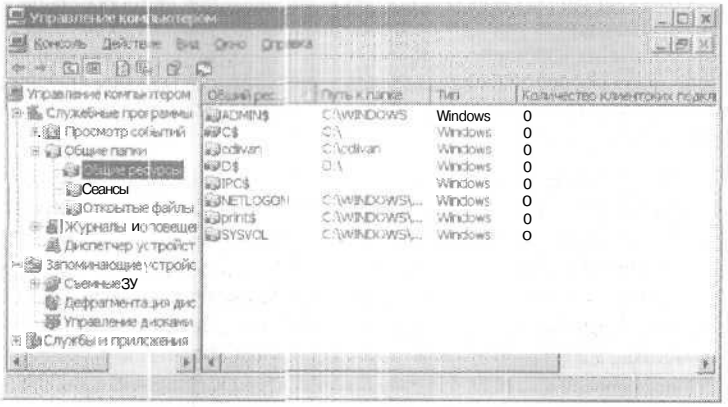


Рис. 14-1. Список **доступных** ресурсов в узле Общие папки (Shared Folders)

В панели сведений содержится следующая информация:

- **Общий ресурс (Share Name) — имя общей папки;**
- Путь к папке (Folder Path) — полный путь к папке на локальной системе;
- Тип (Type) — тип компьютера, который может использовать этот ресурс;
- Количество клиентских подключений (# Client Connections) — количество клиентов, имеющих доступ к ресурсу в данный момент;

- **Описание (Share Description) — описание ресурса.**

Примечание Запись «Windows» в столбце Тип (Type) означает, что к ресурсу могут обращаться все клиенты Microsoft Windows, а также другие разрешенные клиенты, например пользователи Macintosh. Запись «Macintosh» означает, что к этому ресурсу имеют право обращаться только клиенты Macintosh.

Создание общих папок

В Microsoft Windows Server 2003 предусмотрено два способа предоставления общего доступа: к локальным папкам через Проводник (Windows Explorer) или к локальным и удаленным панкам через консоль Управление компьютером (Computer Management).

Консоль Управление компьютером (Computer Management) позволяет управлять общими ресурсами с любого компьютера сети. Для создания общих папок на Windows Server 2003 вы должны быть членом группы Администраторы (Administrators) или Операторы сервера (Server Operators).

Общая папка с помощью консоли Управление компьютером (Computer Management) создается так.

1. Щелкните правой кнопкой элемент Управление компьютером (Computer Management) в дереве консоли и выберите Подключиться к другому компьютеру (Connect to Another Computer). Укажите нужный компьютер.
2. В дереве консоли раскройте последовательно узлы Служебные программы (System Tools) и Общие папки (Shared Folders), а затем выберите Общие ресурсы (Shares). Отобразятся текущие общие ресурсы системы.
3. Щелкнув правой кнопкой элемент Общие ресурсы (Shares), выберите команду Новый общий ресурс (New Share). Откроется Мастер создания общих ресурсов (Share a Folder Wizard). Щелкните Далее (Next).
4. В поле Путь к папке (Folder Path) наберите полный локальный путь к папке, к которой хотите открыть доступ (рис. 14-2), например C:\Data\CorpDocuments. Если вы не знаете пути к папке, найдите ее с помощью кнопки Обзор (Browse). Щелкните Далее (Next).

Примечание Если путь не найден, мастер может создать его. Щелкните Да (Yes), когда появится предложение создать нужную папку.

Рис. 14-2. Мастер создания общих ресурсов (Share a Folder Wizard) позволяет создать новый общий ресурс на выбранном компьютере

5. Введите имя ресурса в поле Общий ресурс (Share Name). Это имя папки, по которому к ней будут обращаться пользователи сети. Имена ресурсов должны быть уникальными для каждой системы.

Совет Ресурс будет скрыт от пользователей сети, если его общее имя заканчивается символом $, например PrivEngData$. Такой ресурс не отображается при просмотре сети средствами Проводника (Windows Explorer), NET VIEW и других подобных утилит. Пользователь может подключиться к такому ресурсу, только зная его имя и обладая необходимыми полномочиями.

6. При желании введите описание ресурса. Впоследствии, когда вы будете просматривать общие ресурсы на каком-то компьютере, описание отобразится в консоли Управление компьютером (Computer Management).
7. По умолчанию ресурс настроен так, что для автономного использования доступны только файлы и программы, указанные пользователем. Чтоб разрешить автономное использование всех файлов и программ ресурса или, напротив, полностью запретить его, щелкните кнопку Изменить (Change) и задайте нужные параметры в диалоговом окне Настройка автономного режима (Offline Settings).
8. Щелкните Далее (Next), а затем настройте базовые разрешения доступа к ресурсу, как показано на рис. 14-3 (подроб-

нее — R разделе «Управление разрешениями доступа к общему ресурсу»). Вам доступны следующие параметры:

- **У всех пользователей доступ только для чтения (All** users **have** read-only **access)** — пользователи могут только просматривать файлы. Создавать, изменять или удалять файлы и папки им не разрешается;
- **Администраторы имеют полный доступ, остальные — доступ** только для **чтения (Administrators have full** access; **other users** have **read-only access) —** администраторы могут создавать, изменять и удалять файлы и папки, а на томах NTFS также назначать *разрешения* и становиться владельцами файлов и панок. Другие *пользователи* могут только просматривать файлы. Создавать, изменять или удалять файлы и папки им не разрешается;
- **Администраторы имеют полный доступ, остальные — доступ для чтения и записи (Administrators** have full **access; other** users **have read and** write **access)** – администраторам доступны все возможные действия с файлами и папками. Другие пользователи имеют право создавать, изменять или удалять файлы и папки;
- **Использовать особые права** доступа **к** общей **папке (Use** custom share and folder **permissions)** — позволяет настраивать доступ для конкретных пользователей и групп. Обычно это — самый удобный вариант.

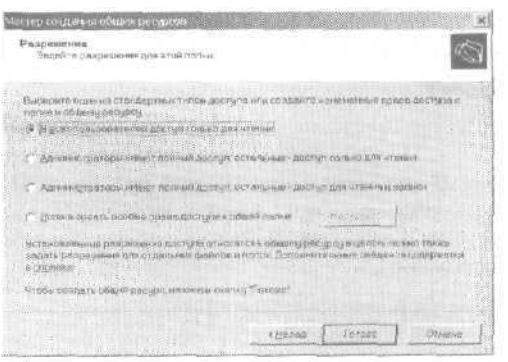


Рис. 14-3. Настройка разрешений доступа к общему ресурсу

9. Щелкните Готово (Finish) и Закрыть (Close).

Примечание В Проводнике на значке папки появится изображение руки, означающее, что папка стала общей.

Совет Создав общий ресурс, предназначенный для всех пользователей сети, опубликуйте его в Active Directory. Это облегчит пользователям поиск ресурса. Чтобы опубликовать ресурс в Active Directory, щелкните его правой кнопкой в консоли Управление компьютером (Computer Management) и выберите Свойства (Properties). Перейдите на вкладку Публикация (Publish) выберите Опубликовать этот общий ресурс в Active Directory (Publish this share in Active Directory), введите описание и информацию о владельце, а затем щелкните OK.

Создание дополнительных общих ресурсов на базе существующего

Отдельным папкам можно сопоставить несколько ресурсов общего доступа, причем каждый может иметь свое имя и набор разрешений доступа. Создавая дополнительные ресурсы на базе существующего, следуйте инструкциям по созданию ресурса предыдущего раздела с такими изменениями:

- присваивая имя ресурсу (пункт 5), убедитесь, что оно отличается от других, ранее присвоенных;
- в описании ресурса (пункт 6) объясните, для чего он используется (и чем отличается от других ресурсов для той же папки).

Управление разрешениями доступа к общему ресурсу

Разрешения доступа устанавливают максимально возможные действия в общей папке. По умолчанию при создании общего ресурса любой пользователь сети имеет доступ только на его чтение. Обратите на это внимание — в предыдущих версиях всем пользователям сети по умолчанию предоставлялся полный доступ к общему ресурсу.

На томах NTFS для дальнейшего ограничения возможных действий пользователей в дополнение к разрешениями общего ресурса вы вправе применять разрешения NTFS для файлов и папок. На томах FAT управление доступом осуществляется только с помощью разрешений общего ресурса.

Виды разрешений доступа к общим ресурсам

В этом разделе перечислены разрешения доступа к ресурсам по степени ограничения от более строгих к менее строгим.

- **Нет доступа (No Access) — доступ к ресурсу** запрещен.
- Чтение (Read) — с этим разрешением пользователь может:
  - видеть имена файлов и папок;
  - иметь доступ к подпапкам общего ресурса;
  - читать данные и атрибуты файлов;
  - запускать на выполнение программы.
- Изменение (Change) — пользователям разрешено читать данные из папки, а также:
  - создавать файлы и подпапки;
  - изменять файлы;
  - изменять атрибуты файлов и подпапок;
  - удалять файлы и подпапки.
- Полный доступ (Full Control) — пользователи имеют разрешения на чтение и изменение, а также в разделах NTFS дополнительно получают возможность:
  - изменять разрешения доступа к файлам и папкам;
  - становиться владельцами файлов и папок.

Вы можете назначить разрешения доступа к общим ресурсам пользователям и группам, в том числе неявным группам. О *неявных* группах рассказано в главе 8.

Просмотр разрешений доступа к общему ресурсу

1. В консоли Управление компьютером (Computer Management) подключитесь к компьютеру, на котором создан общий ресурс.
2. В дереве консоли раскройте последовательно узлы Служебные программы (System Tools) и Общие папки (Shared Folders), а затем выберите Общие ресурсы (Shares).
3. Правой кнопкой щелкните ресурс, который хотите посмотреть, и выберите Свойства (Properties).
4. В диалоговом окне со свойствами ресурса перейдите на вкладку Разрешения для общего ресурса (Share Permissions), показанную на рис. 14-4. Теперь вы видите, какие пользователи и группы имеют доступ к этому ресурсу, и тип этого доступа.

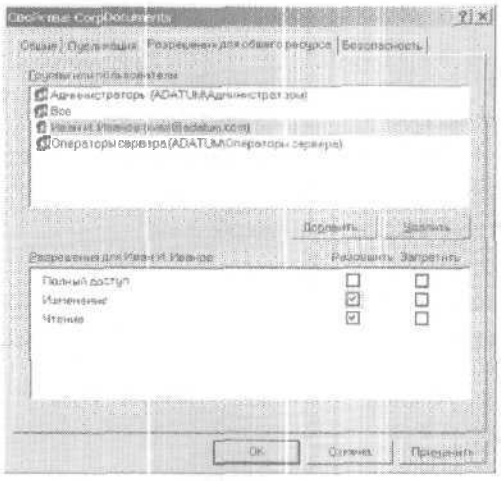


Рис. 14-4. На вкладке Разрешения для общего ресурса (Share Permissions) показаны пользователи и группы, имеющие доступ к ресурсу, и тип этого доступа

Настройка разрешений доступа к общему ресурсу

В коасоли Управление компьютером (Computer Management) можно добавить разрешения доступа пользователя, компьютера и группы к ресурсу.

1. Правой кнопкой щелкните ресурс, которым хотите управлять, и выберите Свойства (Properties).
2. В окне свойств перейдите на вкладку Разрешения для общего ресурса (Share Permissions).
3. Щелкните Добавить (Add). Откроется окно, показанное на рис. 14-5.
4. Введите имя пользователя. компьютера или группы из текущего домена и щелкните Проверить имена (Check Names).
   - Если найдено единственное совпадение, диалоговое окно будет автоматически обновлено, а введенное вами имя — подчеркнуто.
   - Если совпадений не найдено, вы ввели имя с ошибкой или используете неверное расположение. Исправьте имя и снова щелкните Проверить имена (Check Names) или с помощью кнопки Размещение (Locations) укажите новое расположение.

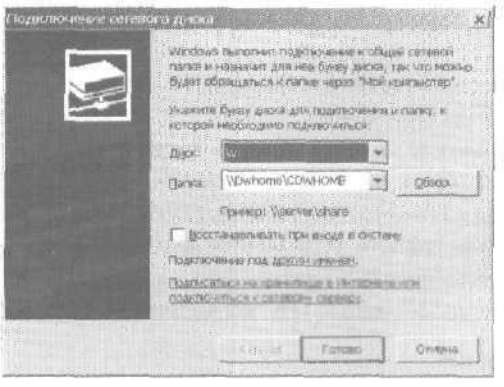


Рис. 14-5. Добавление пользователей и групп, которые должны иметь доступ к ресурсу

- Если найдено несколько совпадений, выделите нужное имя или имена и щелкните OK. Чтобы продолжить добавление пользователей, компьютеров или групп, введите точку с запятой (;) и повторите этот пункт.

Примечание Кнопка Размещение (Locations) открывает доступ к учетным записям из других доменов. Щелкните ее для просмотра списка текущего домена, доверенных доменов и других ресурсов, к которым вы имеете доступ. Поскольку в Windows Server 2003 используется транзитивное доверие, у вас обычно есть доступ ко всем доменам в дереве или лесу.

5. Щелкните OK. Пользователи и группы будут добавлены в список имен для общего ресурса.
6. Настройте разрешения доступа для каждого пользователя, компьютера и группы, выбирая учетную запись и предоставляя или отменяя нужные разрешения.
7. Щелкните OK. О назначении дополнительных разрешений безопасности на томе NTFS рассказано в разделе «Разрешения доступа к файлам и папкам».

Изменение существующих разрешений

Вы можете изменить разрешения доступа к общему ресурсу, которые назначили пользователю, компьютеру или группе. В консоли Управление компьютером (Computer Management) выполните следующие действия.

1. Правой кнопкой щелкните ресурс, которым хотите управлять, и выберите Свойства (Properties).
2. В окне свойств ресурса щелкните вкладку Разрешения для общего ресурса (Share Permissions).
3. Выделите пользователя, компьютер или группу, разрешения на доступ к которым вы хотите изменить.
4. Используйте поля в области Разрешения (Permissions) для предоставления или запрета разрешений доступа.
5. Повторите эти действия для других пользователей, компьютеров или групп. Щелкните OK, когда закончите.

Удаление разрешений

Удалить разрешения доступа к общему ресурсу, назначенные пользователям, компьютерам и группам, можно в окне Разрешения для общего ресурса (Share Permissions). В консоли Управление компьютером (Computer Management) выполните следующие действия.

1. Правой кнопкой щелкните ресурс, которым хотите управлять, и выберите Свойства (Properties).
2. В окне свойств ресурса щелкните вкладку Разрешения для общего ресурса (Share Permissions).
3. Выделите пользователя, компьютер или группу, разрешения доступа которых вы хотите удалить, и щелкните Удалить (Remove).
4. Повторите эти действия *для* других пользователей, компьютеров или групп, и щелкните OK.

Управление общими ресурсами

Администратору часто придется управлять общими папками.

Понятие о специальных ресурсах

Когда вы устанавливаете Windows Server 2003, ОС автоматически создает специальные ресурсы. Их также называют *административными* (administrative) и *скрытыми* (hidden). Эти ресурсы облегчают системное администрирование. Вы не можете настроить разрешения доступа к автоматически создаваемым специальным ресурсам — ОС назначает их сама. Однако вы вправе удалить специальные ресурсы, если какие-то из них вам не нужны.

Доступность специальных ресурсов определяют параметры системы. В табл. 14-1 перечислены правила использования специальных ресурсов.

Таблица 14-1. Специальные ресурсы, используемые в Windows Server 2003

Имя специального ресурса	Описание	Использование
ADMIN$	Используется во время удаленного администрирования системы. Предоставляет доступ *к* папке *%SystemRoot%*	На рабочих станциях и серверах доступ к этому ресурсу имеют члены групп Администраторы (Administrators) и Операторы архива (Backup Operators). На контроллерах домена к ним добавляются члены группы Операторы сервера (Server Operators)
FAX$	Поддерживает сетевые факсы	Используется факс-клиентами при отправке факсов
IPC$	Поддерживает именованные каналы во время удаленного IPC-доступа	Используется программами во время удаленного администрирования и при просмотре общих ресурсов
NETLOGON	Поддерживает службу Net Logon	Применяется службой Net Logon при обработке запросов на регистрацию в домене. Все пользователи имеют доступ на чтение
Microsoft UAM Volume	Поддерживает службы файлов и печати Macintosh	Используется файловым сервером и сервером печати для Macintosh
PRINT$	Поддерживает общие принтеры, обеспечивая доступ к драйверам принтеров	Используется общими принтерами. Все пользователи имеют доступ на чтение. Администраторы, операторы сервера и операторы печати имеют полный доступ
SYSVOL	Поддерживает Active Directory	Используется для хранения данных и объектов Active Directory
Буква_диска$	Позволяет администраторам подключаться к корневой папке диска. Эти ресурсы отображаются как C$, D$, E$ и т. д.	На рабочих станциях и серверах доступ к этому ресурсу имеют администраторы и операторы архива. На контроллерах домена к ним добавляются операторы сервера

Подключение к специальным ресурсам

Имела специальных ресурсов заканч и ваются символом «$». Хотя эти ресурсы и не отображаются R I Iроводнике (Windows Explorer), администраторы и некоторые операторы имеют право подключаться к ним. Для этого необходимо выполнить следующие действия.

1. В Проводнике в меню Сервис (Tools) выберите Подключить сетевой диск (Map Network Drive). Откроется диалоговое окно, показанное на рис. 14-6.

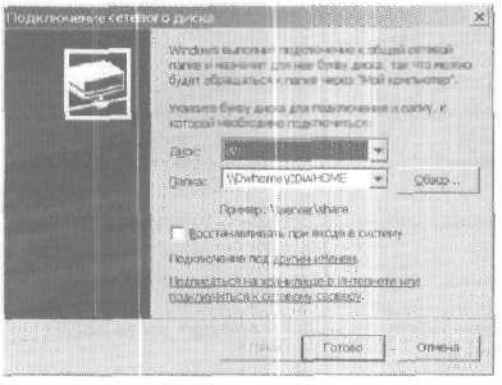


Рис. 14-6. Подключение к специальному ресурсу

2. В поле Диск (Drive) выберите свободную букву диска — для доступа к специальному ресурсу.
3. В ноле Папка (Folder) наберите UNC-путь к нужному ресурсу. Например, для доступа к ресурсу C$ на сервере Twiddle нужно ввести **\\TWIDDLE\C$**.
4. Щелкните OK.

После подключения к специальному ресурсу вы получаете доступ к нему, как к любому другому диску. Поскольку специальные ресурсы защищены, вам не нужно беспокоиться, что обычные пользователи получат доступ к этому ресурсу. Когда вы подключаетесь к ресурсу впервые, вам может быть предложено ввести имя пользователя и пароль.

Просмотр сеансов пользователей и компьютеров

Консоль Управление компьютером (Computer Management) помогает отследить все подключения к общим ресурсам в системе Windows Server 2003. Как только пользователь или ком-

пьютер подключаются к общему ресурсу, подключение отображается в узле Сеансы (Sessions).

Вот как просмотреть подключения к общим ресурсам.

1. В консоли Управление компьютером (Computer Management) подключитесь к компьютеру, на котором создан ресурс.
2. В дереве консоли раскройте последовательно узлы Служебные программы (System Tools) и Общие папки (Shared Folders), а затем выберите Сеансы (Sessions).
3. Просмотрите список подключенных к ресурсу пользователей или компьютеров (рис. 14-7).

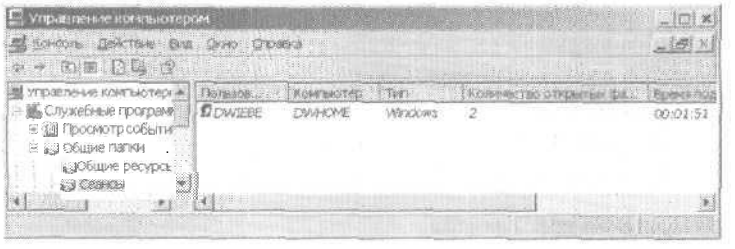


Рис. 14-7. Просмотр подключений пользователей и компьютеров

Узел Сеансы (Sessions) дает важную **информацию о подключениях** пользователей и компьютеров:

- Пользователь (User) — имена пользователей/компьютеров, подключенных к общим ресурсам; имена компьютеров показаны с суффиксом «$», чтобы отличить их от имен пользователей;
- **Компьютер (Computer)** — имя компьютера;
- Тип (Type) — тип используемого сетевого подключения;
- Количество открытых файлов (Open Files) — количество файлов, с которыми пользователь активно работает;
- **Время подсоединения (Connected Time) — время,** прошедшее с начала соединения;
- **Время простоя (Idle Time) — время,** прошедшее с момента, **когда** соединение **использовалось в** последний раз;
- Гость (Guest) — регистрировался ли пользователь как гость.

Управление сеансами и общими ресурсами

Прежде чем вы отключите сервер или приложение, работающее на нем, желательно отключить пользователей от общих

ресурсов. Кроме того, пользователей отключают, когда вы собираетесь изменить разрешения доступа, или совсем удалить общий ресурс, или снять блокировку файлов. Для этого необходимо завершить относящиеся к пользователю сеансы.

Завершение отдельных сеансов

Вот как отключить отдельных пользователей от общих ресурсов.

1. Б консоли Управление компьютером (Computer Management) подключитесь к компьютеру, на котором создан ресурс,
2. Б дереве консоли раскройте последовательно узлы Служебные программы (System Tools) и Общие папки (Shared Folders), а затем выберите Сеансы (Sessions).
3. Правой кнопкой щелкните пользовательский сеанс и выберите Закрыть сеанс (Close Session).
4. Щелкните OK для подтверждения действия.

Завершение всех сеансов

Чтобы отключить от общих ресурсов всех пользователей, выполните следующие действия.

1. В консоли Управление компьютером (Computer Management) подключитесь к компьютеру, на котором создан ресурс,
2. В дереве консоли раскройте последовательно узлы Служебные программы (System Tools) и Общие папки (Shared Folders), а затем щелкните правой кнопкой Сеансы (Sessions).
3. Выбрав Отключить все сеансы (Disconnect All Sessions), щелкните OK для подтверждения действия.

Примечание Помните: вы отключаете **пользователей** от **общих** ресурсов, а не от домена. Вы **можете заставить** пользователей завершить сеанс после **их входа** в домен, только ограничив разрешенное время работы или средствами групповой политики. Так что отключение **пользователей** от общего **ресурса не отключает их от сети.**

Управление открытыми ресурсами

Пока пользователь подключен к общему ресурсу, отдельные файлы и объекты ресурса, с которыми он активно работает, **отображаются** в узле Открытые файлы (Open Files), Этот узел

может показать файлы, которые пользователь открыл, но не редактирует в данный момент.

Вот как получить доступ к узлу Открытые файлы (Open Files).

1. В консоли Управление компьютером (Computer Management) подключитесь к компьютеру, на котором создан ресурс.
2. В дереве консоли раскройте последовательно узлы Служебные программы (System Tools) и Общие папки (Shared Folders), а затем выберите Открытые файлы (Open Files). Отобразится узел Открытые файлы (Open Files), предоставляющий следующую информацию об использовании ресурса (рис. 14-8):
   - Открытый файл (Open File) — путь к открытому файлу или папке на локальной системе; может также быть именованным каналом, например \PIPE\spools для буферизации печати;
   - Пользователь (Accessed By) — имя пользователя, открывшего файл;
   - **Тип (Type)** — тип используемого сетевого подключения;
   - Блокир. (# Locks) — количество блокировок ресурса;
   - Режим открытия (Open Mode) — использовавшийся при открытии ресурса режим доступа: чтения, записи или чтения-записи.

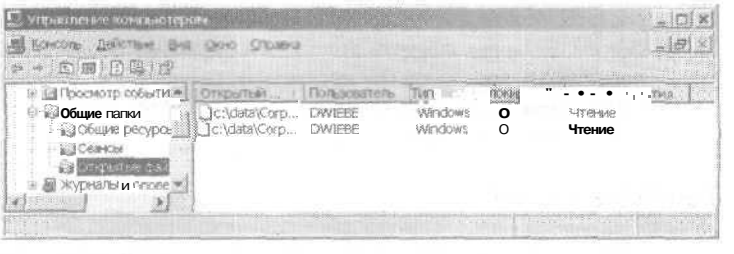


Рис. 14-8. Вы можете управлять открытыми ресурсами, используя узел Открытые файлы (Open Files)

Закрытие открытого файла

1. В консоли Управление компьютером (Computer Management) подключитесь к компьютеру, с которым хотите работать.

2. В дереве консоли раскройте последовательно узлы Служебные программы (System Tools) и Общие ланки (Shared Folders), а затем выберите Открытые файлы (Open Files).
3. Правой кнопкой щелкните открытый файл и выберите Закрыть открытый файл (Close Open File).
4. Щелкните OK для подтверждения действия.

Закрытие всех открытых файлов

\. В консоли Управление компьютером (Computer Management) подключитесь к компьютеру, с которым хотите работать.
2. В дереве консоли раскройте последовательно узлы Служебные программы (System Tools) и Общие папки (Shared Folders), а затем щелкните правой кнопкой Открытые файлы (Opel Files).
3. Выбрав Отключить все открытые файлы (Disconnect All Open Files), щелкните OK для подтверждения действия.

Прекращение общего доступа к файлам и папкам

1. В консоли Управление компьютером (Computer Management) подключитесь к компьютеру, на котором создан ресурс и раскройте узел Общие ресурсы (Shares).
2. Правой кнопкой щелкните ресурс, который хотите удалить, и выберите Прекратить общий доступ (Stop Sharing). Щелкните Да (Yes) для подтверждения действия.

Внимание! Никогда не удаляйте папку, содержащую общие ресурсы, предварительно не прекратив доступ к этим ресурсам. Если вы забудете это сделать, Windows Server 2003 попытается восстановить доступ при следующем запуске компьютера, в результате чего появится запись об ошибке в системном журнале.

Теневые копии

Если в вашей организации активно используются общие папки, рассмотрите возможность создания *теневых копий* (shadow copies) этих общих папок, т. е. периодически обновляемых архивных копий файлов из общих папок. Они сохранят вам и другим администраторам сети немало времени, особенно если вам часто приходится восстанавливать из архива потерянные, ошибочно перезаписанные или испорченные файлы,

Основные понятия

Создавать теневые копии разрешено только на томах NTFS. Компонент Теневая копия (Shadow Copy) позволяет автоматически создавать резервные копии файлов в общих папках на данном томе. Если на файловом сервере существует три тома NTFS с общими папками на каждом, следует настроить этот компонент для каждого тома в отдельности.

По умолчанию теневые копии создаются дважды в день с понедельника но пятницу в 7:00 и 0:00. Для создания первой теневой копии на томе вам понадобится не менее 100 Мбайт свободного пространства. Объем диска, который будет занят в дальнейшем, зависит от количества данных в общих папках тома. Максимальное дисковое пространство, используемое компонентом Теневая копия (Shadow Copy), можно ограничить,

Для настройки и просмотра текущих параметров теневого копирования предназначена вкладка Теневые копии (Shadow Copies) окна свойств диска. Щелкните правой кнопкой значок нужного диска в Проводнике (Windows Explorer) или консоли Управление компьютером (Computer Management), выберите Свойства (Properties) и перейдите на *эту* вкладку. На панели Выберите том (Select a volume) отображаются следующие сведения:

- Том (Volume) — метка тома NTFS на выбранном диске;
- Время следующего запуска (Next Run Time) — время очередного теневого копирования или информация о том, что оно отключено;
- **Общие ресурсы** (Shares) — количество общих папок на томе;
- **Использовано** (Used) — объем диска, занятый теневыми копиями.

Отдельные теневые копии на выбранном томе перечислены в панели Теневые копии выбранного тома (Shadow copies of selected volume) с указанием даты и времени создания.

Создание теневых копий

Чтобы создать теневую копию па томе NTFS с общими папками, выполните следующие действия.

1. Откройте консоль Управление компьютером (Computer Management) и щелкните правой кнопкой одноименный элемент в дереве консоли. Выберите в контекстном меню ко-

манду Подключиться к другому компьютеру (Connect to another computer). Выберите компьютер, с которым собираетесь работать.

2. Раскройте узел Запоминающие устройства (Storage) и выделите элемент Управление дисками (Disk Management). В области сведений отобразятся тома на выбранном компьютере.
3. В списке томов или в графической области щелкните правой кнопкой нужный том и выберите Свойства (Properties).
4. Перейдите на вкладку Теневые копии (Shadow Copies) и выделите в списке Выберите том (Select a volume) нужный том.
5. Щелкните кнопку Параметры (Settings), чтобы задать максимальный размер теневых копий на томе и изменить стандартное расписание. Закончив настройку, щелкните OK.
6. Щелкните кнопку Создать (Create Now). На томе будет создана первая теневая копия и задано расписание последующего копирования.

Удаление теневых копий

При необходимости, например для освобождения дискового пространства, отдельные теневые копии на томе можно удалить. Вот как это делается.

1. Откройте консоль Управление компьютером (Computer Management) и щелкните правой кнопкой одноименный элемент в дереве консоли. Выберите в контекстном меню команду Подключиться к другому компьютеру (Connect to another computer). Укажите компьютер, с которым собираетесь работать.
2. Раскройте узел Запоминающие устройства (Storage) и выделите элемент Управление дисками (Disk Management). В области сведений отобразятся тома на указанном компьютере.
3. В списке томов или в графической области щелкните правой кнопкой нужный том и выберите Свойства (Properties).
4. Перейдите на вкладку Теневые копии (Shadow Copies) и выделите в списке Выберите том (Select a volume) нужный том.
5. Выделите нужную (точнее, ненужную) теневую копию и щелкните кнопку Удалить (Delete Now).

Отказ от теневого копирования

Если теневое копирование общих папок на томе вам более не нужно, отключите компонент Теневая копия (Shadow Copy).

Новые теневые копии после этого создаваться не будут, а старые будут удалены. Вот как отключить теневое копирование,

1. Откройте консоль Управление компьютером (Computer Management) и щелкните правой кнопкой одноименный элемент в дереве консоли. Выберите в контекстном меню команду Подключиться к другому компьютеру (Connect to another computer). Укажите компьютер, с которым собираетесь работать.
2. Раскройте узел Запоминающие устройства (Storage) и выделите элемент Управление дисками (Disk Management). В области сведений отобразятся тома на указанном компьютере.
3. В списке томов или в графической области щелкните правой кнопкой нужный том и выберите Свойства (Properties).
4. Перейдите на вкладку Теневые копии (Shadow Copies), выделите в списке Выберите том (Select a volume) нужный том и щелкните Отключить (Disable).
5. Подтвердите отключение, щелкнув Да (Yes).

Подключение к сетевым дискам

Пользователи могут подключаться к общим ресурсам сети. Эти соединения выглядят как диски, к которым пользователи обращаются так же, как к локальным дискам в своих системах.

Примечание Когда пользователи подключаются к сетевым дискам, на них действует не только набор разрешений доступа к общим ресурсам, но и разрешения доступа к файлам или папкам Windows Server 2003. Различия в этих наборах разрешений обычно становятся причиной того, что пользователям не удается получить доступ к отдельным файлам и подпапкам на сетевом диске.

Подключение сетевого диска

Б Windows Server 2003 подключение к сетевому диску осуществляется путем назначения ему буквы. Вот что для этого нужно сделать,

1. **После** регистрации пользователя запустите **Проводник на его компьютере.**
2. В меню Сервис (Tools) выберите Подключить сетевой диск (Map Network Drive). Откроется диалоговое окно Подключение сетевого диска (Map Network Drive),

3. В списке Диск (Drive) укажите свободную букву диска для создания сетевого диска, к которому можно обращаться через Проводник и папку Мой компьютер (My Computer). Другой способ — создать сетевой диск, не назначая буквы. Этот диск открывается в собственном окне Проводника и недоступен через окно Мой компьютер (My Computer).
4. В поле Папка (Folder) наберите UNC-путь к нужному ресурсу. Например, для доступа к ресурсу DOCS на сервере ROMEO следует ввести **\\ROMEO\DOCS.** Если вы не знаете точного места размещения ресурса, щелкните Обзор (Browse) для его поиска.
5. Чтобы сетевой диск автоматически подключался в последующих сеансах, установите флажок Восстанавливать при входе в систему (Reconnect at logon).
6. Для подключения от имени пользователя, отличного от того, под которым вы регистрировались в системе, щелкните гиперссылку Подключение под другим именем (Different User Name) и введите имя пользователя и пароль.
7. Щелкните OK.

Отключение сетевого диска

Сетевой диск отключается так.

1. После регистрации пользователя запустите Проводник (Windows Explorer) на компьютере пользователя.
2. В меню Сервис (Tools) выберите Отключить сетевой диск (Disconnect Network Drive).
3. Укажите нужный диск и щелкните OK.

Управление объектами, правами владения и наследованием

В Windows Server 2003 реализован объектный подход к описанию ресурсов и управлению разрешениями доступа. Объекты, описывающие ресурсы, определяются в разделах NTFS и в Active Directory. На разделах NTFS можно настраивать разрешения доступа к файлам и панкам, а средствами Active Directory — разрешения доступа к другим объектам, таким, как пользователи, компьютеры и группы.

Объекты и диспетчеры объектов

Независимо от того, где определен объект: в разделе NTFS или в Active Directory, у каждого типа объектов свой диспетчер и базовые средства управления. Диспетчер объектов управляет параметрами объекта и разрешениями доступа к нему. Базовые средства управления — предпочтительные инструменты работы с объектами. Объекты, их диспетчеры и средства управления перечислены в табл. 14-2.

Таблица 14-2. Объекты Windows Server 2003

Тип объекта	Диспетчер объекта	Средство управления
Файлы и папки	NTFS	Проводник (Windows Explorer)
Общие ресурсы	Служба Server	Проводник, консоль Управление компьютером (Computer Management)
Записи реестра	Реестр Windows	Редактор реестра (regedit)
Службы	Контроллеры служб	Набор средств настройки безопасности (Security Configuration Tool Set)
Принтеры	Спулер печати	Папка Принтеры (Printers)

Владение объектами

В Windows Server 2003 владелец объекта не обязательно является его *создателем*, но именно владелец объекта полностью управляет им. Владелец объекта может разрешать доступ и назначать других пользователей владельцами объекта.

Администратор вправе завладеть любыми объектами в сети. За счет этого для авторизованных администраторов нельзя заблокировать файлы, папки, принтеры и другие ресурсы, Но, став владельцем файлов, вам (в большинстве случаев) не удастся вернуть их предыдущему владельцу. Поэтому администратор не сможет получить доступ к файлу, а затем скрыть этот факт.

Порядок назначения прав владения изначально определяется местом размещения создаваемого ресурса. Обычно группа Администраторы (Administrators) считается текущим владельцем объекта, а его действительный создатель имеет право стать владельцем.

Передать владение можно такими способами:

- если администраторы изначально назначаются владельцами, создатель объекта может стать владельцем при условии, что он сделает это прежде, чем кто-либо другой станет владельцем;

- текущий владелец может предоставить разрешение Смена владельца (Take Ownership) другим пользователям, разрешив им становиться владельцами объекта;
- администратор может стать владельцем объекта, взяв его под свое управление.

Вот как сменить владельца объекта.

1. Запустите средство управления этим объектом. Например, если хотите работать с файлами/папками, запустите Проводник (Windows Explorer).
2. Правой кнопкой щелкните объект, владельцем которого хотите стать.
3. Выберите Свойства (Properties). В окне свойств перейдите на вкладку Безопасность (Security).
4. Щелкнув кнопку Дополнительно (Advanced), откройте диалоговое окно Дополнительные параметры безопасности (Advanced Security Settings). Перейдите на вкладку Владелец (Owner), показанную на рис. 14-9,

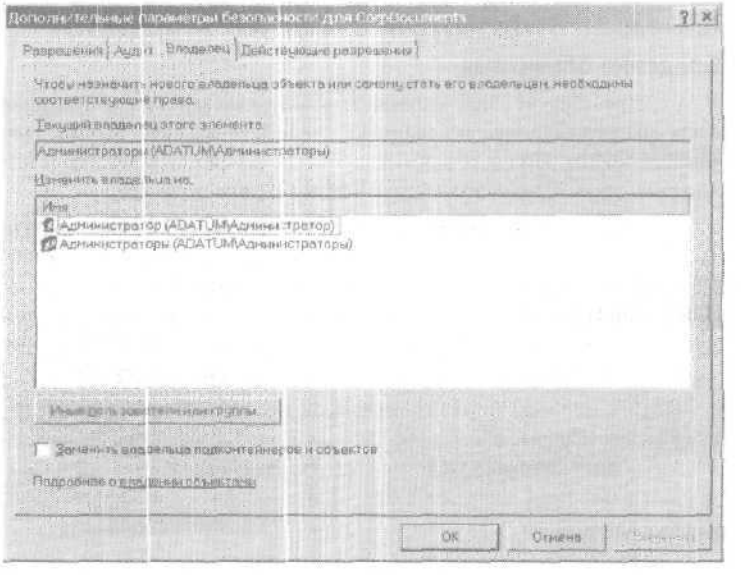


Рис. 14-9. На вкладке Владелец (Owner) **можно** сменить владельца файла

5. Выберите имя нового владельца в списке Изменить владельца на (Change owner to), а затем щелкните OK.

Совет Вступая во владение папкой, вы можете также стать владельцем всех файлов и подпапок в ней. Для этого нужно установить флажок Заменить владельца подконтейнеров и объектов (Replace owner on subcontainers and objects). Эта процедура работает и для других вложенных объектов.

Наследование объектов

Объекты определяются с использованием структуры «родитель — потомок». Родительский объект — объект верхнего уровня. Дочерний в иерархии расположен ниже родительского, Например, папка C:\ является родительской для папок C:\data и C:\backups. Любые подпапки, созданные в C:\data или C:\backups являются дочерними для этих папок и «внучатыми» для C:\.

Дочерние объекты могут наследовать разрешения от родительских объектов. Все объекты Windows Server 2003 по умолчанию создаются с разрешением наследования. Это значит, что дочерние объекты автоматически наследуют разрешения родительских, поэтому разрешения родительского объекта управляют доступом к дочернему. Чтобы изменить разрешения дочернего объекта:

- отредактируйте разрешения родительского объекта;
- остановите наследование разрешений от родительского объекта, а затем назначьте разрешения для дочернего;
- выберите противоположное значение разрешения для перекрытия унаследованного: например, если родитель предоставляет какое-то разрешение, запретите его для дочернего объекта.

Вот как разрешить или запретить наследование разрешений от родительского объекта.

1. Запустите средство управления для данного объекта. Например, если хотите работать с файлами и папками, запустите Проводник.
2. I Iравой кнопкой щелкните объект, с которым хотите работать.
3. Выберите Свойства (Properties). В окне свойств перейдите на вкладку Безопасность (Security).
4. Щелкнув кнопку Дополнительно (Advanced), откройте диалоговое окно Дополнительные параметры безопасности (Advanced Security Settings).

5. На вкладке Разрешения (Permission) установите или снимите флажок Разрешить наследование разрешений от родительского объекта к этому объекту... (Allow inheritable permissions from the parent to propagate to this object...). Щелкните OK.

Разрешения доступа к файлам и папкам

В разделах NTFS вы можете настраивать разрешения безопасности для файлов и папок. Эти разрешения позволяют и запрещают доступ к файлам и папкам. Разрешения безопасности можно просмотреть.

1. В Проводнике правой кнопкой щелкните файл или папку, с которыми хотите работать.
2. Выберите Свойства (Properties). В окне свойств перейдите на вкладку Безопасность (Security).
3. Выделите пользователя, компьютер и группу, разрешения которых хотите просмотреть. Если разрешения затенены, они наследуются от родительского объекта.

Понятие разрешений доступа к файлам и папкам

В этом разделе перечислены базовые разрешения, которые вы можете назначить файлу и папке (табл. 14-3).

Таблица 14-3. Разрешения файлов и папок в Windows Server 2003

Разрешение	Позволяет для папок	Позволяет для файлов
Чтение (Read)	Просмотр списка файлов и подпапок	Просмотр и копирование содержимого файла
Запись (Write)	Добавление файлов и подпапок	Запись в файл
Чтение и выполнение (Read & Execute)	Просмотр списка файлов и подпапок, а также исполнение файлов (наследуется файлами и папками)	Просмотр и копирование содержимого файла, а также исполнение файла
Список содержимого папки (List Folder Contents)	Просмотр списка файлов и подпапок, а также исполнение файлов (наследуется только папками)	—
Изменить (Modify)	Чтение и запись файлов и подпапок, удаление папки	Чтение, запись и удаление файла
Полный доступ (Full Control)	Чтение, запись, изменение и удаление файлов и подпапок	Чтение, запись, изменение и удаление файла

Когда вы работаете с разрешениями файлов и папок, учтите следующее:

- Чтение (Read) — единственное разрешение, необходимое для выполнения сценариев. Разрешение Выполнение (Execute) не требуется;
- разрешение Чтение (Read) требуется для доступа к ярлыкам и их целевым объектам;
- предоставляя пользователю разрешение записи в файл, вы тем самым позволяете ему удалить содержимое файла, хотя сам файл пользователю удалить не удастся;
- получив полный доступ к папке, пользователь сможет удалять файлы в ней независимо от разрешений на сами эти файлы.

Базовые разрешения создаются комбинацией специальных разрешений в логических группах. Далее указаны специальные разрешения, используемые при создании базовых разрешений для файлов (табл. 14-4). Применяя дополнительные параметры разрешения, вы можете назначать специальные разрешения индивидуально. При изучении специальных разрешений учтите следующее:

- доступ пользователю следует предоставлять явно, иначе доступ ему запрещен;
- действия, которые может выполнять пользователь, суммируются от всех разрешений, назначенных пользователю и всем группам, членом которых он является. Например, пользователь GeorgcJ имеет доступ на чтение, кроме того, он входит в группу Techies, которая имеет право вносить изменения. В итоге GeorgeJ тоже получает Это право. Если Techies будут включены в группу Администраторы (Administrators), которой предоставлен полный доступ, GeorgeJ также получит полный доступ к этому файлу.

Таблица 14-4. Специальные разрешения для файлов

Специальное разрешение	Основные разрешения				
	Полный доступ (Full Control)	Изменить (Modify)	Чтение и выполнение (Read & Execute)	Чтение (Read)	Запись (Write)
Обзор папок/Выполнение файлов (Traverse Folder/ Execute File)	Да	Да	Да		
Содержание папки/ Чтение данных (List Folder/Read Data)	Да	Да	Да	Да	
Чтение атрибутов (Read Attributes)	Да	Да	Да	Да	
Чтение дополнительных атрибутов (Read Extended Attributes)	Да	Да	Да	Да	
Создание файлов/Запись данных (Create Files/ Write Data)	Да	Да			Да
Создание папок/Дозапись данных (Create Folders/ Append Data)	Да	Да			Да
Запись атрибутов (Write Attributes)	Да	Да			Да
Запись дополнительных атрибутов (Write Extended Attributes)	Да	Да			Да
Удаление подпапок и файлов (Delete Subfolders and Files)	Да				
Удаление (Delete)	Да	Да			
Чтение разрешений (Read Permissions)	Да	Да	Да	Да	Да
Смена разрешений (Change Permissions)	Да				
Смена владельца (Take Ownership)	Да				

Далее перечислены специальные разрешения, используемые для создания **базовых** разрешений для папок (табл. 14-5). При изучении специальных разрешений учтите следующие рекомендации.

Таблица 14-5. Специальные разрешения для папок

Специальное разрешение	Основные разрешения					
	Полный доступ (Full Control)	Изменить (Modify)	Чтение и выполнение (Read & Execute)	Список содержимого папки (List Folder Contents)	Чтение (Read)	Запись (Write)
Обзор папок/Выполнение файлов (Traverse Folder/ Execute File)	Да	Да	Да	Да		
Содержание папки/ Чтение данных (List Folder/Read Data)	Да	Да	Да	Да	Да	
Чтение атрибутов (Read Attributes)	Да	Да	Да	Да	Да	
Чтение дополнительных атрибутов (Read Extended Attributes)	Да	Да	Да	Да	Да	
Создание файлов/ Дозапись данных (Create Folders/ Append Data)	Да	Да				Да
Создание папок/ Дозапись данных (Create Folders/Append Data)	Да	Да				Да
Запись атрибутов (Write Attributes)	Да	Да				Да
Запись дополнительных атрибутов (Write Extended Attributes)	Да	Да				Да
Удаление подпапок и файлов (Delete Subfolders and Files)	Да					
Удаление (Delete)	Да	Да				
Чтение разрешений (Read Permissions)	Да	Да	Да	Да	Да	Да
Смена разрешений (Change Permissions)	Да					
Смена владельца (Take Ownership)	Да					

- Устанавливаяразрешения для родительской папки, вы можете заставить все файлы и подпапки внутри этой папки унаследовать ее разрешения: выберите 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).
- Файлы,создаваемые в папках, наследуютнекоторые параметры разрешения. Эти параметры показаны как стандартные разрешения файла.

Настройка разрешений для файла и папки

1. В Проводнике правой кнопкой щелкните файл или папку, с которыми хотите работать.
2. В появившемся меню выберите Свойства (Properties), а затем в окне свойств прейдите на вкладку Безопасность (Security), показанную на рис. 14-10.

Рис. 14-10. Вкладка Безопасность (Security) позволяет настроить базовые разрешения для файла или папки

3. Пользователи и группы, которые уже имеют доступ к файлу или папке, перечислены в списке Группы или пользователи (Group or user names). Вы можете изменить разрешения для этих пользователей и групп.

- Выделите пользователя/группу, разрешения которых хотите изменить.
- В списке Разрешения (Permissions) предоставьте/запретите разрешения доступа.

Совет Наследуемые разрешения затенены. Если вы хотите перекрыть наследуемое разрешение, выберите противоположное значение.

4. Чтобы задать разрешения доступа для дополнительных пользователей, компьютеров или групп, щелкните Добавить (Add). Откроется диалоговое окно, показанное на рис. 14-11.

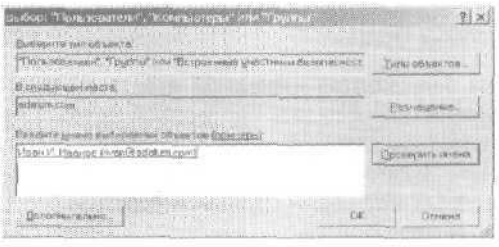


Рис. 14-11. Укажите пользователей, компьютеры/группы, которым нужно предоставить/запретить доступ

5. Введите имя пользователя, компьютера или группы из текущего домена и щелкните Проверить имена (Check Names).
   - Если найдено единственное совпадение, диалоговое окно будет автоматически обновлено, а введенное вами имя — подчеркнуто.
   - Если совпадений не найдено, вы ввели имя с ошибкой или указали неверное расположение. Исправьте имя и снова щелкните Проверить имена (Check Names) или с помощью кнопки Размещение (Locations) выберите новое расположение.
   - Если найдено несколько совладений, выделите нужное имя или имена и щелкните OK. Чтобы продолжить добавление пользователей, компьютеров или групп, введите точку с запятой (;) и повторите этот пункт.
6. В списке Группы или пользователи (Group or user names) выделите нужных пользователя, компьютер или группу, а затем посредством полей в области Разрешения (Permissions) предоставьте/запретите разрешения доступа. Повто-

рите эти действия для других пользователей, компьютеров или групп.

7. Щелкните OK, когда закончите.

Аудит системных ресурсов

Аудит – лучший способ проследить, что случилось с системой Windows Server 2003. Он полезен при сборе информации об использовании ресурсов — доступе к файлам, регистрации в системе и изменениях системных параметров. Как только произойдет событие, которое вы настроили для аудита, оно записывается в системный журнал безопасности, где вы сможете просмотреть его. Журнал безопасности доступен в консоли Просмотр событий (Event Viewer).

Примечание На большинство изменений аудита вы получаете право, зарегистрировавшись под учетной записью из группы Администраторы (Administrators) или получив разрешение Управление аудитом и журналом безопасности (Manage Auditing and Security Log) в групповой политике.

Настройка политик аудита

Политики аудита — важный фактор обеспечения безопасности и целостности системы. Почти каждая компьютерная система в сети должна быть настроена для протоколирования определенных параметров безопасности. Политики аудита настраиваются с применением групповой политики: вы можете задать политики аудита для всего сайта, домена или организационного подразделения (ОП). Или же настроить политики для отдельной рабочей станции/сервера.

Открыв контейнер групповой политики, настройте политику аудита.

1. Откройте узел Политика аудита (Audit Policy), последовательно спускаясь по дереву консоли (рис. 14-12).
2. Просмотрите текущие параметры аудита:
   - Аудит входа в систему (Audit Logon Events) отслеживает события, связанные с регистрацией пользователя, окончанием сеанса работы и удаленными соединениями с сетевыми системами;
   - **Аудит доступа к объектам (Audit Object Access)** отслеживает использование системных ресурсов: файлов, ка-

талогов, общих ресурсов, принтеров и объектов Active Directory;

- **Аудит доступа к службе каталогов (Audit Directory Service Access)** отслеживает доступ к Active Directory. События генерируются каждый раз, когда пользователи/компьютеры получают доступ к каталогу;
- **Аудит изменения политики (Audit Policy Change)** отслеживает изменения разрешений доступа пользователей, аудита и доверительных отношений;
- **Аудит использования привилегий (Audit Privilege Use)** отслеживает применение разрешений доступа и привилегий пользователя типа права резервного копирования файлов и каталогов;

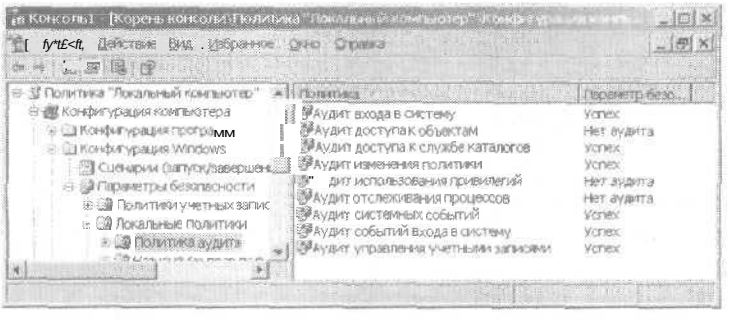


Рис. 14-12. Настройка политики аудита с использованием узла **Политика** аудита (Audit Policy) в групповой политике

Примечание Политика аудита привилегий не отслеживает события, относящиеся к системному доступу, например использование права интерактивного входа/разрешения доступа к компьютеру из сети. Эти события отслеживаются аудитом входа в систему.

- **Аудит отслеживания процессов (Audit Process Tracking)** отслеживает системные процессы и ресурсы, ими используемые;
- **Аудит системных событий (Audit System Events)** отслеживает запуск, выключение и перезагрузку системы, а также действия, влияющие на безопасность системы или на журнал безопасности;

- Аудит событий входа в систему (Audit Account Logon Events) отслеживает события, относящиеся к регистрации и окончанию работы пользователя в системе;
- Аудит управления учетными записями (Audit Account Management) отслеживает управление учетными записями посредством консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers). События генерируются каждый раз, когда учетные записи пользователя, компьютера или группы создаются, изменяются или удаляются.

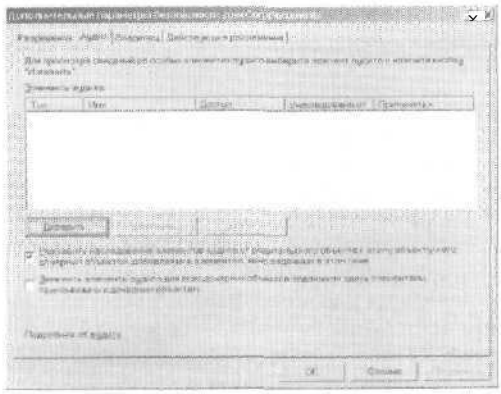
3. Для настройки политики аудита дважды щелкните ее элемент или щелкните его правой кнопкой и выберите Свойства (Properties). Откроется окно свойств этой политики.
4. Выберите Вести аудит следующих попыток доступа (Audit these attempts), а затем установите флажок Успех (Success), Отказ (Failure) или оба сразу. Включение первого флажка протоколирует успешные события, второго — события отказа, например неудачные попытки входа.
5. Щелкните OK.

Аудит файлов и папок

Включив политику Аудит доступа к объектам (Audit Object Access), вы можете задать уровень аудита для отдельных папок или файлов. Лудит этого типа доступен только на томах NTFS.

Аудит файла или папки настраивается так,

1. В Проводнике щелкните правой кнопкой файл или папку, для которых хотите включить аудит, и выберите Свойства (Properties).
2. На вкладке Безопасность (Security) щелкните кнопку Дополнительно (Advanced).
3. В открывшемся окне перейдите на вкладку Аудит (Auditing), показанную на рис. 14-13.
4. Чтобы наследовать параметры аудита от родительского объекта, установите флажок Разрешить наследование элементов аудита от родительского объекта к этому объекту... (Allow inheritable auditing entries from the parent to propagate to this object...).
5. Если вы хотите, чтобы дочерние объекты текущего объекта наследовали его параметры, выберите Заменить элементы аудита... (Replace Auditing Entries...).



Рис, 14-13. На вкладке Аудит (Auditing) настраивают политики аудита отдельных файлов и **папок**

6. В списке Элементы аудита (Auditing Entries) укажите пользователей, группы или компьютеры, чьи действия вы желаете отслеживать с помощью аудита. Чтобы удалить учетную запись, выберите ее в списке Элементы аудита (Auditing Entries) и щелкните Удалить (Remove).
7. Чтобы добавить конкретные учетные записи, щелкните Добавить (Add) и укажите имя учетной записи. Щелкнув OK, вы увидите диалоговое окно Элемент аудита для (Auditing Entry For), показанное на рис.14-14.

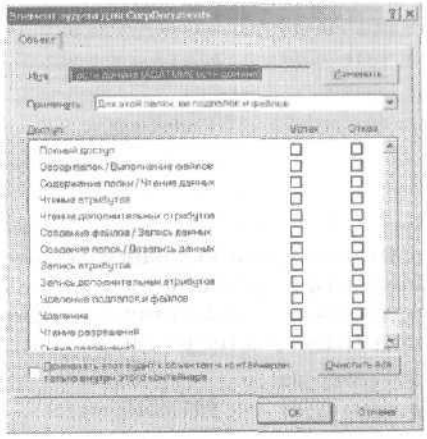


Рис. **14-14.** В окне Элемент аудита для (Auditing Entry For) задайте элементы аудита для пользователя, компьютера или группы

Примечание Для контроля с помощью аудита действий всех пользователей предназначена специальная группа Все (Everyone).

8. В списке Применять (Apply Onto) определите, где применять аудит объектов.
9. Установите флажки Успех (Successful), Отказ (Failed) или оба сразу для каждого из событий, к которым хотите применять аудит. Первый протоколирует успешные события, типа успешного чтения файла, второй — неудачные события, например неудавшееся удаление файла. События, для которых вы можете использовать аудит, — те же, что и специальные разрешения (табл. 14-5), за исключением того, что не разрешается отслеживать средствами аудита синхронизацию автономных файлов и папок.
10. Щелкните OK, когда закончите. Повторите описанный процесс для аудита других пользователей, групп или компьютеров.

Аудит объектов Active Directory

Если в групповой политике включен параметр Аудит доступа к службе каталогов (Audit Directory Service Access), вы можете задать уровень аудита для объектов Active Directory. Это позволяет точно управлять наблюдением за использованием объекта.

Аудит объекта настраивается так.

1. В консоли Active Directory — пользователи и компьютеры (Active Directory Users and Computers) найдите контейнер объекта.
2. Правой кнопкой щелкните объект, для которого будет применяться аудит, и выберите Свойства (Properties).
3. На вкладке Безопасность (Security) щелкните кнопку Дополнительно (Advanced).
4. Перейдите на вкладку Аудит (Auditing). Чтобы наследовать параметры аудита от родительского объекта, выберите Разрешить наследование элементов аудита от родительского объекта к этому объекту... (Allow inheritable auditing entries from the parent to propagate to this object...).
5. В списке Элементы аудита (Auditing Entries) укажите пользователей, группы или компьютеры, чьи действия вы желаете отслеживать с помощью аудита. Чтобы удалить учетную

запись, выберите ее в списке Элементы аудита (Auditing Entries) и щелкните Удалить (Remove).

6. Чтобы добавить определенные учетные записи, щелкните Добавить (Add) и укажите имя учетной записи. Щелкнув OK, вы увидите диалоговое окно Элемент аудита для (Auditing Entry For).
7. Используйте список Применять (Apply Onto), чтобы указать, где применять аудит объектов.
8. Выберите флажки Успех (Successful), Отказ (Failed) или оба сразу для каждого из событий, которые хотите отслеживать.
9. Щелкните OK, когда закончите. Повторите описанный процесс для аудита других пользователей, групп или компьютеров.

Квотирование диска

Дисковые квоты (disk quotas) позволяют управлять объемом диска, занимаемым пользователями. Квоты настраиваются отдельно для каждого тома. Применять их можно только на томах NTFS.

Основные понятия

Обычно квотирование задается на важных томах, например содержащих важные корпоративные общие ресурсы. У квот два основных параметра:

- Предел дисковой квоты (**Disk** quota limit) — максимальный объем диска, который может быть использован как для записи информации данного пользователя, так и для записи информации о данном пользователе;
- Порог предупреждения дисковой квоты (Disk quota warning level) — объем диска, занятый пользователем, по достижении которого пользователю передается предупреждение о скором исчерпании квоты.

Совет Если вы задаете квоты только для контроля за использованием диска конкретными пользователями, применяйте квотирование в «мягком» варианте. В этом случае вы узнаете о превышении квоты по записи события в журнал приложений, а пользователь сможет и дальше заполнять диск.

Дисковые квоты ограничивают объем диска только для пользователей. Администратор может использовать диск даже при превышении квоты.

Обычно предельный объем дискового пространства задается в мегабайтах или гигабайтах. Порог предупреждения указывается в процентах от объема квоты, например 90-95%.

Дисковые квоты разрешается задавать как на локальных, так и на удаленных томах.

- При назначении квот на локальном томе вы работаете с локальным диском. При этом учитываются не только файлы пользователя, но и файлы приложений, которые попали в системную папку в результате установки пользователем какого-либо приложения. В некоторых случаях это вызывает превышение квоты, причину которого пользователь не понимает. Поэтому повышайте предел квотирования для пользователей, которым разрешено устанавливать приложения.
- Чтобы управлять квотами на **удаленном томе,** нужно сделать общим ресурсом его корневую папку. Не забывайте, что квоты задаются отдельно для каждого тома. Если на удаленном файловом сервере предусмотрены различные тома для данных разного типа, квоты на них следует отслеживать отдельно.
- Настраивать квоты имеют право только администраторы домена и локальные администраторы. Первый шаг в настройке квот — включение соответствующей групповой политики. Это можно сделать как на локальном уровне (для одного компьютера), так и на уровне предприятия (для групп пользователей или компьютеров).

Контроль за квотами повышает нагрузку на компьютеры, которая зависит от количества настроенных квот, полного и использованного объема томов, а также от количества пользователей, для которых заданы квоты.

Хотя формально квоты назначаются пользователям, в реальности Windows Server 2003 управляет ими с помощью идентификаторов безопасности (security identifiers, SID). Поэтому при изменении имени пользователя параметры квот останутся теми же. Использование SID приводит к незначительному повышению нагрузки при просмотре дисковых квот, так как при этом Windows Server 2003 приходится сопоставлять идентификаторы SID с именам учетных записей. Это также означает, что при просмотре квот необходимо соединение с локальным диспетчером пользователей или с контроллером домена Active Directory.

Имена, сопоставленные с идентификаторами, сохраняются в локальном кэше. Его обновление происходит нечасто, поэтому не удивляйтесь возникшим несоответствиям, а просто вручную обновите информацию, нажав клавишу F5.

Настройка политик дисковых квот

Лучше всего настраивать дисковые квоты с помощью групповой политики. При этом вы задаете общие правила, которые автоматически применяются при включении квотирования на индивидуальных томах. Это позволяет избежать задания одних и тех же параметров па каждом томе, для которого вы хотите назначить квотирование.

Политики, управляющие дисковыми квотами, перечислены в табл. 14-6. Они назначаются на системном уровне. Доступ к ним открывается из узла Конфигурация компьютера\Административные шаблоны\Система\Дисковые квоты (Computer Configuration\Administrative Templates\System\Disk Quotas).

Таблица 14-6. Политики дисковых квот

Политика	Описание
Включить дисковые квоты (Enable disk quotas)	Включает или выключает дисковые квоты на всех томах NTFS компьютера и не дает пользователям изменить параметры квотирования
Задать предел дисковой кьоты (Enforce disk quota limit)	Определяет строгость предела квотирования. Если предел задан, то пользователю, превысившему квоту, будет отказано в предоставлении дискового пространства. Эта политика отменяет параметры, заданные на вкладке Квота (Quota) окна свойств тома NTFS
Предел квоты по умолчанию и уровень предупреждения (Default quota limit and warning level)	Задает предел квоты и уровень предупреждения. Действует только на новых пользователей
Вести журнал даже при превышении предела квоты (Log event when quota limit exceeded)	Задает запись события в журнал при достижении пользователями предела квотирования. Не дает пользователям изменять параметры ведения журнала
Заносить событие превышения уровня предупреждения квоты (Log event when quota warning level exceeded)	Задает запись события в журнал при достижении пользователями уровня предупреждения квоты

1. Откройте консоль Групповая политика (Group Policy) для системы, с которой хотите работать, например, для файлового сервера. Откройте узел Дисковые квоты (Disk Quotas).
2. Дважды щелкните политику Включить дисковые квоты (Enable disk quotas) и на вкладке Параметр (Setting) установите переключатель Включен (Enabled). Щелкните кнопку Следующий параметр (Next Setting). Откроется окно политики Задать предел дисковой квоты (Enforce disk quota limit).
3. Чтобы включить дисковое квотирование на всех томах NTFS этого компьютера, щелкните Включен (Enabled). В противном случае щелкните Отключен (Disabled), а затем задайте квоты для каждого тома в отдельности (подробнее — далее в этой главе).
4. Щелкните кнопку Следующий параметр (Next Setting). Откроется окно политики Предел киоты по умолчанию и уровень предупреждения (Default quota limit and warning level), показанное на рис, 14-15. Щелкните Включен (Enabled).

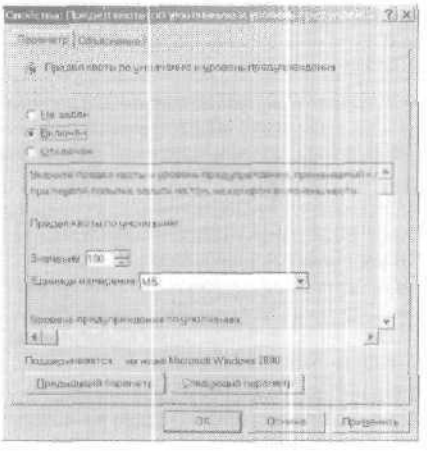


Рис. 14-15. Основные параметры дискового квотирования

5. В области Предел квоты по умолчанию (Default quota limit) укажите предел по умолчанию для пользователей, впервые осуществляющих запись на том с включенным квотированием. Это значение не применяется к текущим пользователям и не затрагивает уже заданные значения.
6. Немного прокрутив вниз вспомогательное окно на этой вкладке, укажите предел предупреждения.

7. Щелкните кнопку Следующий параметр (Next Setting). Откроется окно политики Вести журнал даже при превышении предела квоты (Log event when quota limit exceeded). Щелкните Включен (Enabled).
8. Щелкните кнопку Следующий параметр (Next Setting). Откроется окно политики Заносить событие превышения уровня предупреждения квоты (Log event when quota warning level exceeded). Щелкните Включен (Enabled).
9. Щелкните кнопку Следующий параметр (Next Setting). Откроется окно Применять политику к съемным носителям (Apply policy to removable media). Щелкните Отключен (Disabled).
10. Щелкните OK.

Совет Чтобы политики вступили в действие немедленно, откройте узел Конфигурация компьютера\Административные шаблоны\Система\Групповая политика (Computer Configuration\Administrative Templates\System\Group Policy) и дважды щелкните политику Обработка политики дисковой квоты (Disk quota policy processing). Щелкните Включен (Enabled) и установите флажок Обрабатывать, даже если объекты групповой политики не изменились (Process even if the group policy objects have not changed). Щелкните OK.

Включение квотирования на томе NTFS

Включив соответствующие политики, вы можете задать квоты на локальных и удаленных томах с помощью консоли Управление компьютером (Computer Management).

Чтобы включить квотирование на томе NTFS, выполните следующие действия.

1. Откройте консоль Управление компьютером (Computer Management) и щелкните правой кнопкой одноименный элемент в дереве консоли. Выберите Подключиться к другому компьютеру (Connect to Another Computer). Укажите компьютер, с которым хотите работать.
2. Раскройте узел Запоминающие устройства (Storage) и выделите элемент Управление дисками (Disk Management). В области сведений отобразятся тома на выбранном компьютере.
3. В списке томов или в графической области щелкните правой кнопкой нужный том и выберите Свойства (Properties).

4. Перейдите на вкладку Квота (Quota) и установите флажок Включить управление квотами (Enable Quota Management), как показано на рис. 14-16. Если вы управляете квотами с помощью групповой политики, параметры окажутся недоступными. Для их изменения воспользуйтесь консолью Групповая политика (Group Policy).

Совет Работая с вкладкой Квота (Quota), обращайте особое внимание на значок светофора и описание статуса квотирования рядом с ним. Если квоты не настроены, на светофоре горит красный свет. Желтый сигнал свидетельствует, что система занята или обновляет квоты. Если квоты настроены, на светофоре горит зеленый свет.

Рис. 14-16. Здесь настраиваются параметры квотирования

5. Установите переключатель Выделять на диске не более (Limit disk space to) и задайте предел квотирования. В поле Порог выдачи предупреждений (Set warning level to) задайте порог в процентах от указанного предела квоты.

rt> Совет Квотирование можно настроить отдельно для каждого пользователя. Для этого следует щелкнуть кнопку Записи квот (Quota Entries). Имейте в виду, что эти записи можно экспортировать, а затем импортировать на другом томе.

6. Чтобы пользователи не занимали место на диске сверх своей квоты, установите флажок Не выделять место на диске при превышении квоты (Deny disk space to users exceeding quota limit).

7. С помощью флажков в нижней части вкладки задайте запись в журнал сообщений о превышении квоты или о достижении порога предупреждения.
8. Щелкните OK. Windows Server 2003 просканирует том и обновит данные о его использовании.

Просмотр записей квот

Контроль за использованием диска ведется для каждого пользователя в отдельности. При включенном квотировании для каждого пользователя, хранящего свои данные на томе, заводится периодически обновляемая запись в файле квоты. В ней записаны следующие данные: текущий объем диска, занятый пользователем, пределы квотирования, порог предупреждения и др.

Чтобы просмотреть текущие параметры квотирования, выполните следующие действия.

1. Откройте консоль Управление компьютером (Computer Management) и щелкните правой кнопкой одноименный элемент в дереве консоли. Выберите Подключиться к другому компьютеру (Connect to Another Computer). Укажите компьютер, с которым хотите работать.
2. Раскройте узел Запоминающие устройства (Storage) и выделите элемент Управление дисками (Disk Management). Б области сведений отобразятся тома на выбранном компьютере.
3. В списке томов или в графической области щелкните правой кнопкой нужный том и выберите Свойства (Properties),
4. На вкладке Квота (Quota) щелкните кнопку Записи квот (Quota Entries). В открывшемся диалоговом окне будет показан статус квотирования для всех пользователей.

Создание записей квот

Вы можете создать записи квот для пользователей, которые еще не сохраняли свои данные на томе, и настраивать квотирование для отдельных пользователей. К этому, например, приходится прибегать, если среди пользователей есть сотрудник, который работает с большими объемами информации и которому стандартная квота мала. Индивидуально следует также настраивать квоты для администраторов.

Совет Не допускайте беспорядка в индивидуальной настройке квотирования и внимательно следите за отдельными записями квот. В идеале все параметры квотирования нужно за-

писывать в отдельный журнал, чтобы ваша политика распределения дискового пространства была понятна другим администраторам. Мой опыт подсказывает, что индивидуальная настройка квотирования нужна только некоторым группам пользователей. Иногда лучше выделить для каждой из таких групп отдельный том и применить на нем правила квотирования, соответствующие потребностям данной группы. В этом случае вы сможете избежать индивидуальной настройки квот.

Чтобы создать запись квоты на томе, выполните следующие действия.

1. Откройте диалоговое окно диалоговое окно с записями квот, как описано в предыдущем разделе. В нем перечислены существующие записи квот для всех пользователей. Чтобы обновить список, нажмите F5.
2. Чтобы создать новую запись, выберите в меню Квота (Quota) команду Создать запись квоты (New Quota Entry).
3. В открывшемся диалоговом окне введите нужное имя пользователя и щелкните кнопку Проверить имена (Check Names). Если найдены совпадения, выделите среди них нужное и щелкните OK. Если совпадений не найдено, исправьте имя и повторите поиск. Закончив работу, щелкните OK.
4. Откроется диалоговое окно Добавление новой квоты (Add New Quota Entry), показанное на рис. 14-17. Теперь вы можете отменить все ограничения для этого пользователя, установив переключатель Не ограничивать выделение места на диске (Do not limit disk usage). Чтобы задать пределы квотирования, установите переключатель Выделять на диске не более (Limit disk space to).
5. Щелкните OK.

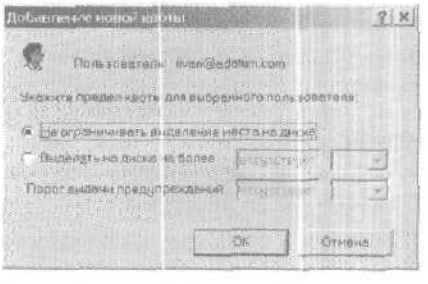


Рис. 14-17, В этом окне задаются индивидуальные параметры квотирования

Удаление записей квот

Удаление записи производится в том случае, если пользователю этот том больше не нужен. При удалении записи квот на экране отображается список всех файлов данного пользователя. Вы можете их удалить, стать их владельцем или переместить в заданную папку на другом томе.

Чтобы удалить запись квоты для одного из пользователей, выполните следующие действия.

1. Откройте диалоговое окно с записями квот, как описано в разделе «Просмотр записей квот». В нем перечислены существующие записи квот для всех пользователей. Чтобы обновить список, нажмите F5.
2. Выделите запись, которую хотите удалить, и нажмите Delete или выберите в меню Квота (Quota) команду Удалить запись квоты (Delete Quota Entry).
3. Подтвердите удаление, щелкнув Да (Yes). Откроется диалоговое окно со списком текущих файлов пользователя.
4. Раскрыв список Файлы, которыми владеет (List Files Owned By), отобразите файлы пользователя, запись квоты которого вы удаляете, и укажите, что с ними нужно сделать. Действие можно задавать как для отдельных файлов, так и для групп, выделенных клавишами Shift и Ctrl. Вы можете:
   - **удалить выделенные файлы,** нажав клавишу Delete (на экране появится запрос на подтверждение удаления);
   - **стать владельцем выделенных файлов,** щелкнув Смена владельца (Take Ownership);
   - **переместить выделенные файлы,** введя путь к папке на другом томе или отыскав ее с помощью кнопки Обзор (Browse).
5. Щелкните Закрыть (Close). Если вы все сделали правильно, запись квоты будет удалена.

Экспорт и импорт записей квот

Чтобы вам не приходилось создавать записи квот на каждом томе в отдельности, в Windows Server 2003 предусмотрена возможность их экспорта с одного тома и импорта на другой. Оба тома должны быть томами NTFS. Вот что нужно сделать, чтобы экспортировать, а затем импортировать записи квот.

1. Откройте консоль Управление компьютером (Computer Management) и щелкните правой кнопкой одноименный элемент в дереве консоли. Выберите Подключиться к другому компьютеру (Connect to Another Computer). Укажите компьютер, с которым хотите работать.
2. Раскройте узел Запоминающие устройства (Storage) и вы* делите элемент Управление дисками (Disk Management). В области сведений отобразятся тома на выбранном компьютере.
3. В списке томов или в графической области щелкните правой кнопкой нужный том и выберите Свойства (Properties).
4. Щелкните кнопку Записи квот (Quota Entries) на вкладке Квота (Quota).
5. Выберите команду Экспорт (Export) в меню Квота (Quota). На экране появится диалоговое окно Параметры экспорта квоты (Export Quota Settings). Перейдите в нужную папку и задайте имя файла для сохранения параметров квотирования. Щелкните Сохранить (Save).

Совет Сохраняйте файл сразу на целевом томе. Проблем с его передачей по сети не возникнет — файлы квот обычно очень малы.

6. Выберите в меню Квота (Quota) команду Закрыть (Close).
7. Откройте консоль Управление компьютером (Computer Management) и щелкните правой кнопкой одноименный элемент в дереве консоли. Выберите Подключиться к другому компьютеру (Connect to Another Computer). Укажите компьютер, на котором находится целевой том.
8. Откройте окно свойств для целевого тома и щелкните кнопку Записи квот (Quota Entries) на вкладке Квота (Quota).
9. Выберите в меню Квота (Quota) команду Импорт (Import). Найдите только что сохраненный файл и щелкните Открыть (Open).
10. Если на целевом томе уже созданы собственные записи квот, вам будет предложено сохранить их или заменить импортируемыми записями. При возникновении конфликта щелкните Да (Yes), чтобы заменить существующую запись, или Нет (No), чтобы оставить ее. Чтобы выбранное действие выполнялось для всех записей, прежде чем щелкнуть

Да (Yes) или Нет (No), установите флажок Применить ко всем записям квот (Do this for all quota entries).

Отказ от использования квот

Вы вправе отказаться от квотирования для отдельных или для всех пользователей тома. В первом случае ограничения на дисковое пространство будут сняты с конкретного пользователя, но останутся в силе для всех остальных. При выключении квот на всем томе контроль за использованием диска прекращается полностью. Отключение квотирования для отдельного пользователя описано в разделе *«Создание записей* квот». Чтобы выключить квотирование на всем диске, выполните следующие действия.

1. Откройте консоль Управление компьютером (Computer Management) и щелкните правой кнопкой одноименный элемент в дереве консоли. Выберите Подключиться к другому компьютеру (Connect to Another Computer). Укажите компьютер, с которым хотите работать.
2. Раскройте узел Запоминающие устройства (Storage) и выделите элемент Управление дисками (Disk Management). В области сведений отобразятся тома на выбранном компьютере.
3. В списке томов или в графической области щелкните правой кнопкой нужный том и выберите Свойства (Properties).
4. На вкладке Квота (Quota) сбросьте флажок Включить управление квотами (Enable Quota Management). Щелкните OK.

Глава 15

Архивация и восстановление данных

Данные — сердце компании. Вант задача — уберечь их от всех напастей. Для этого вы должны составить план архивации и восстановления корпоративной информации. Архивация файлов защитит их от случайной порчи, отказа БД, сбоев оборудования и даже стихийных явлений. В обязанности администратора входит архивировать данные и хранить архивы в безопасном месте.

Разработка плана архивации и восстановления

Важные файлы становятся жертвой неловкого пользователя, критическая информация портится из-за неполадок на жестком диске, стихийное бедствие превращает офис в руины, но ничто не страшно тому, кто вовремя разработал и воплотил в жизнь план архивации и восстановления данных.

Понятие плана архивации

Создание и реализация плана архивации и восстановления информации — непростая задача. Вам надо определить, какие данные требуют архивации, как часто проводить архивацию и т. п. При создании плана ответьте на следующие вопросы.

- Насколько важны данные? Этот критерий поможет решить, как, когда и какую информацию сохранять. Для критичной информации, например баз данных, следует создавать избыточные архивные наборы, охватывающие несколько периодов архивации. Для менее важной информации, например для текущих пользовательских файлов, сложный план архивации не нужен, достаточно регулярно сохранять их и уметь легко восстанавливать.

- **К какому типу относится архивируемая информация? Тип** информации поможет определить необходимость архивации данных: как и когда данные должны быть сохранены.
- **Как часто изменяются данные?** Частота изменения влияет на выбор частоты архивирования. Например, ежедневно меняющиеся данные необходимо сохранять каждый день.
- **Нужно ли дополнить архивацию созданием теневых копий?** Помните, что теневая копия — это дополнение к архивации, но ни в коем случае не ее замена. Подробнее о теневых копиях — в главе 14.
- **Как быстро нужно восстанавливать данные?** Время — важный факчор при создании плана архивации. В критичных к скорости системах нужно проводить восстановление очень быстро.
- **Какое оборудование оптимально для архивации и есть ли оно у вас?** Для своевременной архинации вам понадобится несколько архивирующих устройств и несколько наборов носителей. Аппаратные средства архивации включают ленточные накопители (это наименее дорогой, но и самый медленный тип носителя), оптические диски и съемные дисковые накопители.
- **Кто отвечает за выполнение плана архивации и восстановления данных?** В идеале и за разработку плана, и собственно за архивацию и восстановление должен отвечать один человек.
- **Какое время оптимально для архивации?** Архивация в период наименьшей загрузки системы пройдет быстрее, но не всегда возможно провести ее в удобные часы. Поэтому с особой тщательностью архивируйте ключевые данные.
- **Нужно ли сохранять архивы вне офиса?** Хранение архивов вне офиса — важный фактор на случай стихийного бедствия. Вместе с архивами сохраните и копии ПО для установки или переустановки ОС.

Типы архивации

Среди прочих атрибутов файлов и папок в Windows имеется атрибут Архивный (Archive). Он часто используется в качестве указания, нужно ли архивировать данный объект. Если атрибут включен, файл или папка, возможно, нуждаются в архивации. Основные типы архивации таковы.

- Обычная (полная) архивация. Все выделенные файлы архивируются независимо от значения архивного атрибута. После архивации файла атрибут сбрасывается. Если затем файл изменяется, архивный атрибут снова включается, указывая, что файл нуждается в архивации.
- **Копирующая** архивация. Все выделенные файлы архивируются независимо от значения архивного атрибута. В отличие от обычной архивации атрибут не изменяется. Это позволяет затем выполнять архивацию другого типа.
- Разностная архивация. Архивируются файлы, которые были изменены со времени последней обычной архивации, т. е. файлы с установленным архивным атрибутом, но сам атрибут при этом не сбрасывается. Это позволяет позже выполнить архивацию другого типа.
- Добавочная архивация. Архивируются файлы, которые были изменены со времени последней обычной или добавочной архивации, т. е. файлы с установленным архивным атрибутом. После архивации атрибут сбрасывается. Включается он при очередном изменении файла, показывая, что необходима архивация.
- Ежедневная архивация. Сохраняются файлы, измененные за прошедший день. Этот тип архивации не изменяет архивные атрибуты файлов.

Вы можете еженедельно выполнять полную архивацию и вдобавок к этому ежедневную, разностную и добавочную архивацию. Вы также можете создать расширенный архивный набор для ежемесячных и ежеквартальных архивов, включающих в себя нерегулярно архивируемые файлы.

Совет Бывает, проходят недели и месяцы прежде чем кто-нибудь обнаружит, что пропал нужный файл или источник данных. Поэтому, планируя ежемесячные или ежеквартальные архивы, не забудьте, что вам может потребоваться восстановить устаревшие данные.

В предыдущих версиях программы Архивация (Backup) из комплекта Windows при попытке архивирования открытых файлов в журнал производилась запись об ошибке. Программа Архивация (Backup) из Windows Server 2003 автоматически создает архивную версию открытого файла на основе его теневой копии.

Разностная и добавочная архивации

Различие между разностной и добавочной архивациями очень существенно (табл. 15-1). При *разностной архивации* (differential backup) вы сохраняете все файлы, которые были изменены с момента последней полной архивации (т. е. размер разностного архива со временем увеличивается). При *добавочной архивации* (incremental backup) вы сохраняете файлы, измененные с момента последней полкой или добавочной архивации (т. е. добавочный архив, как правило, гораздо меньше полного).

Таблица 15-1. Технологии добавочной и разностной архивации

День недели	Еженедельная полная архивация с ежедневной разностной архивацией	Еженедельная полная архивация с ежедневной добавочной архивацией
Воскресенье	Выполнена полная архивация	Выполнена полная архивация
Понедельник	Разностный архив содержит все изменения, произошедшие с воскресенья	Добавочный архив содержит все изменения, произошедшие с воскресенья
Вторник	Разностный архив содержит все изменения, произошедшие с воскресенья	Добавочный архив содержит все изменения, произошедшие с понедельника
Среда	Разностный архив содержит все изменения, произошедшие е воскресенья	Добавочный архив содержит все изменения, произошедшие со вторника
Четверг	Разностный архив содержит все изменения, произошедшие с воскресенья	Добавочный архив содержит все изменения, произошедшие со среды
Пятница	Разностный архив содержит все изменения, произошедшие с воскресенья	Добавочный архив содержит все изменения, произошедшие с четверга
Суббота	Разностный архив содержит все изменения, произошедшие с воскресенья	Добавочный архив содержит все изменения, произошедшие С пятницы

Выбор архивных устройств и носителей

Определив, какие данные и как часто архивировать, можно выбрать аппаратные средства архивации и необходимые носители. Инструментов для архивации данных множество. Одни - быстрые и дорогие, другие — медленные и надежные. Выбор подходящего оборудования для организации зависит от многих факторов.

- **Емкость** — количество регулярно архивируемых данных. Справится ли оборудование с нагрузкой в отведенное время?
- **Надежность** аппаратных средств и носителей. Можете ли вы пожертвовать надежностью ради экономии или скорости?
- **Расширяемость** решения. Удовлетворяет ли ваше решение потребностям роста организации?
- **Скорость** архивации и восстановления. Можете ли вы пожертвовать скоростью ради снижения стоимости?
- **Цена** архивации приемлема для вашего бюджета?

Типовые решения архивации

Итак, на план архивации влияют емкость, надежность, расширяемость, скорость и цена. Определив, какие из этих факторов наиболее важны для вашей организации, вы примете подходящее решение. Вот некоторые общие рекомендации.

- **Ленточные накопители** — самые распространенные устройства архивации. Данные хранятся на кассетах с магнитной лентой. Лента относительно недорога, но не особенно надежна: она может помяться или растянуться, с течением времени — размагнититься и перестать считываться. Средняя емкость кассет с лентой варьируется от 4 до 10 Гбайт. По сравнению с другими решениями ленточные накопители довольно медленны. Их достоинство — невысокая цена.
- **Накопители на цифровой** ленте (digital audio **tape, DAT)** — пришли на смену традиционным ленточным накопителям. Существует несколько форматов DAT. Наиболее часто используются ленты DLT (Digital Linear Tape) и Super DLT. Ленты DLT IV обладают емкостью 35–40 Гбайт без сжатия и 70-80 Гбайт со сжатием. В крупных организациях иногда разумнее применять ленты LTO (Linear Tape Open) или AIT (Advanced Intelligent Tape). Обычно объем лент LTO составляет 100 Гбайт без сжатия и 200 Гбайт со сжатием. Для лент AIT-3 соответствующие емкости составляют 100 и 260 Гбайт.
- **Ленточная библиотека с автозагрузкой —** устройство для создания расширенных архивных томов на нескольких лентах, которых хватает для нужд всего предприятия. Ленты набора в процессе архивации или восстановления данных

автоматически меняются. В большинстве таких библиотек применяются DAT-ленты. Их главный «минус» — высокая цена.

- Магнитооптические накопители с автозагрузкой подобны ленточным библиотекам, только вместо лент в них используются магнитооптические диски. Цена также очень высока.
- **Съемные диски,** например Iomega Jazz емкостью 1-2 Гбайт, все чаще используются в качестве устройств архивации. Они обладают хорошей скоростью и удобны в работе, но стоят дороже ленточных или DAT-накопителей.
- Дисковые накопители обеспечивают наивысшую скорость при архивации и восстановлении файлов. Если при архивации на ленту вам потребуются часы, то дисковый накопитель позволяет завершить процесс за несколько минут. К недостаткам дисковых накопителей следует отнести относительно высокую иену.

При установке любых устройств архивации, кроме ленточных и DAT-накопителей, необходимо указать ОС контроллеры и драйверы, используемые накопителями. Подробнее об установке устройств и драйверов — в главе 2.

Покупка и использование лент

Количество лент зависит от того, сколько данных и как часто вы будете архивировать и сколько дополнительных наборов данных собираетесь хранить. Общепринятый способ использования лент — чередующийся график, по которому по очереди используются два или более набора лент. Его смысл в том, что вы увеличиваете долговечность лент за счет снижения интенсивности их использоиания и в то же время сокращаете количество лент, необходимых для хранения данных.

Один из самых популярных графиков подразумевает использование 10 лент. При этом ленты делят на два набора, по одной ленте на каждый рабочий день недели. Первый набор используется в первую неделю, второй — в следующую. В пятницу по графику проводится полная архивация, с понедельника по четверг — добавочная. Если добавить третий набор лент, то вы сможете по очереди один из наборов хранить в безопасном месте вне офиса.

Совет График с использованием 10 лент разработан для 5-дневной рабочей недели. Если ваша организация работает 7 дней в неделю, необходимы ленты для архивации в выходные дни. В этом случае потребуется 14 лент: 2 набора по 7. По воскресеньям рекомендуется проводить полную архивацию, а с понедельника по субботу — добавочную.

Архивация данных

Для создания архивов данных на локальных или удаленных системах в Windows Server 2003 включена программа Архивация (Backup). Она годится для архивирования файлов и панок. для их восстановления из архивов, для доступа к архивным накопителям, для доступа к удаленным ресурсам из окна Сетевое окружение (My Network Places), создания образа состояния системы для последующей архивации и восстановления, планирования архивации с помощью Планировщика заданий (Task Scheduler) и создания аварийного диска.

Запуск утилиты Архивация (Backup)

Программу Архивация (Backup) можно запустить несколькими способами.

- В меню Пуск (Start) выберите Выполнить (Run). В диалоговом окне наберите ntbackup и щелкните OK.
- Щелкните кнопку Пуск (Start), раскройте меню Программы (Programs) или Все программы (All Programs), затем Стандартные (Accessories), Служебные (System Tools), а затем — Архивация данных (Backup).

В первый раз программа Архивация (Backup) запускается *в* режиме мастера. Администратору более удобен расширенный режим, позволяющий настраивать большее количество параметров. Сбросьте флажок Всегда запускать в режиме мастера (Always start in wizard mode), а затем щелкните гиперссылку Расширенный режим (Advanced Mode). На экране появится главный интерфейс программы Архивация (Backup), показанный на рис. 15-1. Как видите, здесь четыре вкладки:

- **Добро пожаловать! (Welcome)** — содержит кнопки для запуска Мастера архивации (Backup Wizard), Мастера восстановления (Restore Wizard) и Мастера аварийного восстановления системы (Automated System Recovery Wizard);

- **Архивация** (Backup) — интерфейс для выбора архивируемых данных на локальных или сетевых дисках;
- Восстановление и управление носителем (Restore and Manage Media) — интерфейс для восстановления заархивированных данных на прежнем или на новом месте;
- Запланированные задания (Schedule Jobs) — позволяет спланировать задания, а также просматривать список выполненных и запланированных заданий.

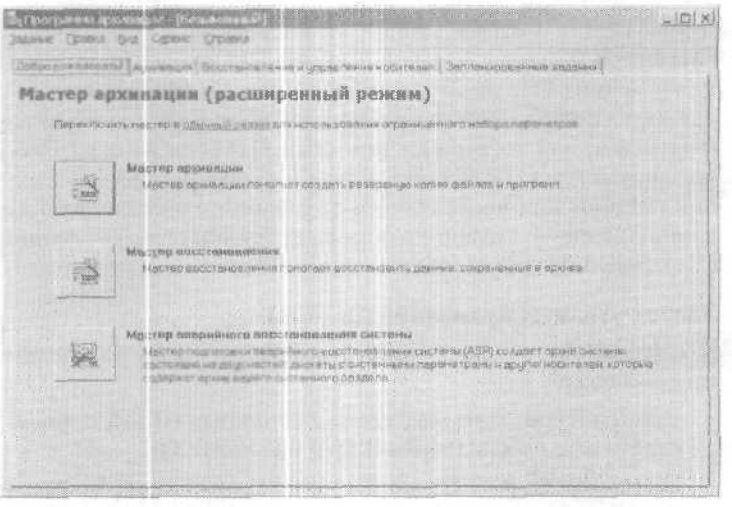


Рис. 15-1. Утилита Архивация (Backup) предоставляет интерфейс для архивации и восстановления данных

Для выполнения архивации и восстановления данных вам потребуются необходимые права и полномочия. Члены групп Администраторы (Administrators) и Операторы архива (Backup Operators) могут архинировать и восстанавливать файлы любого типа независимо от того, кто владеет файлом и какие файлу назначены разрешения. Кроме того, файл вправе архивировать его владельцы и тс, у кого есть разрешения Чтение (Read), Чтение и выполнение (Read and Execute), Изменить (Modify) или Полный доступ (Full Control) для этого файла.

Примечание Локальным учетным записям доступна только локальная система, а доменные имеют более высокие

полномочия. Поэтому члены локальной группы администраторов могут работать только с файлами на локальной системе, а члены группы администраторов домена — с файлами во всем домене.

Программа Архивация (Backup) предоставляет расширения для работы с особыми типами данных, перечисленными ниже;

- **Данные состояния системы** — важные системные файлы, необходимые для восстановления работоспособности локальнойсистемы;
- **Данные Exchange Server — файлы данных и** хранилища информации Exchange. Вам нужно сохранить **эти данные** для восстановления работы Exchange Server. Этот тип данных предоставляют только системы с Exchange Server;
- **Данные о съемных ЗУ** располагаются в папке *%System-Root%*\System32\Ntmsdata. Если вы их сохраните, то сможете воспользоваться расширенными возможностями программы Архивация (Backup) для восстановления конфигурации съемных ЗУ;
- **Данные удаленных хранилищ** хранятся в папке *%System-Root%*\ System32\Remotestorage. При восстановлении просто скопируйте данные удаленного хранилища обратно в эту папку.

Параметры архивации по умолчанию

Для создания архивов предназначены Мастер архивации (Backup Wizard) и вкладка Архивация (Backup). В обоих случаях используются параметры по умолчанию. Чтобы просмотреть или изменить эти параметры, выполните следующие действия.

1. Щелкните ссылку Расширенный режим (Advanced Mode) в первом окне Мастера архивации или восстановления (Backup or Restore Wizard).
2. Выберите в меню Сервис (Tools) команду Параметры (Options).

Открывшееся окно, показанное на рис. 15-2, содержит пять вкладок: Общие (General), Восстановление (Restore), Тип архива (Backup Type), Журнал архивации (Backup Log) и Исключение файлов (Exclude Files).

Рис. 15-2. Установка параметров по умолчанию утилиты Архивация (Backup)

Общие параметры архивации

Общие параметры архивации перечислены в табл. 15-2.

Таблица 15-2. Общие параметры архивации

Параметр	Описание
Оценивать информацию о выборе файлов перед выполнением операций архивации или восстановления (Compute selection information before backup and restore operations)	Подсчет числа файлов и байт, которые будут заархивированы или восстановлены в ходе текущего задания архивации или восстановления. Эти сведения подсчитываются и выводятся перед началом процесса архивации или восстановления
Использовать каталоги носителей для ускорения построения каталогов восстановления на диске < Use the catalogs on the media to speed up building restore catalogs on disk)	Выбор каталога носителя для создания на диске каталога, в котором восстанавливаются данные. Это самый быстрый способ построения каталога на диске. Сбросьте этот параметр, если каталога нет, он поврежден или недоступен по иным причинам
Проверять данные после завершения архивации (Verify **Data** After The Backup Completes)	Проверка соответствия архивных данных и исходных данных па жестком диске. Если эти данные не совпадают, значит, носитель или файл архива содержит ошибки. В этом случае повторите архивацию, используя другой носитель или файл

Таблица 15-2. Общие параметры архивации *(окончание)*

Параметр	Описание
Архивировать содержимое подключенных дисков (Back up the contents of mounted drives)	Архивация данных на подключенном диске. Если этот флажок установлен, при архивации подключенного диска выполняется архивация хранящихся па нем данных. Если флажок не установлен, при архивации подключенного диска выполняется архивация только сведений о его путях
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)	Отображение диалогового окна, если при запуске архивации не работает служба съемных носителей. При архивации данных в файл, который затем будет записан на дискету, жесткий или съемный диск, не устанавливайте этот флажок. Если предполагается архивация данных на ленту или другой носитель, управляемый службой съемных носителей, его следует установить
Выводить предупреждение, если при запуске программы архивации имеется доступны и распознаваемый носитель (Show alert message when T start the backup utility and there is recognizable mediaavailable)	Отображение диалогового окна, если при запуске архивации в пуле импортированных носителей доступен новый носитель
Выводить предупреждение при вставке нового носителя (Show alert message when new media is inserted)	Отображение диалогового окна при обнаружении нового носителя службой съемных носителей
Разрешить всегда использовать распознанный носитель без предупреждения (Always allow use of recognizable media without prompting)	Разрешает службе съемных носителей автоматически перемещать *новый* носитель в пул архивных носителей

Установка параметров восстановления и архивации

На поведение **процессов архивации и восстановления влияют** следующие параметры **(табл. 15-3).**

Таблица 15-3. Параметры восстановления, типа **архива** и журнала архивации

Вкладка	Параметр	Описание
Восстановление (Restore)	Не заменять файл на компьютере (рекомендуется) | Do not replace the file on my computer (recommended)]	Отказ от копирования из архива файлов, копии которых уже имеются на диске
	Заменять файл на компьютере, только если он старее (Replace the file on disk only if the file on disk is older)	Включение замены старых файлов па диске новыми копиями из архива
	Всегда заменять файл на компьютере (Always replace the file on my computer)	Замена всех файлов на диске файлами из архива независимо от времени последнего изменения тех и других
Тип архива (Backup Type)	Используемый по умолчанию тип архива (Default Backup Type)	Список типов архивации — Обычный (Normal), Копирующий (Copy). Разностный (Differential), Добавочный (Incremental), Ежедневный (Daily)
Журнал архивации (Backup Log)	Подробная (Detailed)	Сохранение подробной записи о выполняемых заданиях архивации и восстановления
	Краткая сводка (Summary)	Сохранение краткой сводки выполняемых заданий архивации и восстановления
	Никакой (None)	Отказ от создания файла журнала заданий архивации и восстановления

Просмотр и установка исключений файлов

Многие типы системных файлов по умолчанию исключены из архивации. Чтобы просмотреть исключения, перейдите на вкладку Исключение файлов (Exclude Files) диалогового окна параметров архивации. Исключение файлов основано на информации об их владельцах. Вы можете исключить из архива как файлы всех пользователей, так и пользователя, зарегистрировавшегося в данный момент в системе (рис. 15-3).

Рис. 15-3. Просмотр исключений файлов для пользователей

Чтобы исключить файлы, выполните следующие действия.

1. В диалоговом окне параметров архинации перейдите на вкладку Исключение файлов (Exclude Files).
2. Чтобы исключить файлы, принадлежащие всем пользователям, щелкните Добавить (Add New) под списком Файлы, исключенные для всех пользователей (Files excluded for all users). Чтобы исключить файлы, владельцем которых являетесь только вы, щелкните Добавить (Add New) под списком Файлы, исключенные для пользователя... (Files excluded for user...). Появится диалоговое окно Добавление исключаемых файлов (Add Excluded Files), показанное на рис. 15-4.
3. Чтобы исключить файлы зарегистрированного типа, щелкните тин файла в списке Зарегистрированный тип файла (Registered File Type). Можно также просто ввести расширение файла с точкой в поле Особая маска файла (Custom File Mask), например .**DOC** или .**BAK**.
4. Введите диск или путь файла в поле Применяется к пути (Applies to path). Если вы не сбросите флажок Применять ко всем подпапкам (Applies to all subfolders), также будут исключены все файлы из всех подпапок данного пути. Так, если вы ввели C:\ и установили Применять ко всем подпапкам (Applies to all subfolders), псе файлы с выбранным расширением будут исключены, где бы на диске C: они ни встретились. Щелкните OK.

Рис. 15-4, Установка исключений файлов для пользователей

Совет Введите в качестве пути обратную косую черту (\), чтобы исключить файлы заданного типа на всех файловых системах. Допустим, на компьютере есть жесткие диски C, D и E. Введя этот символ в поле Применяется к пути (Applies to path), вы исключите файлы с заданным расширением на всех трех дисках.

Чтобы изменить существующие исключения, сделайте так.

1. В диалоговом окне параметров архивации перейдите на вкладку Исключение файлов (Exclude Files).
2. Выберите существующее исключение и щелкните Изменить (Edit), чтобы отредактировать его, или Удалить (Remove), чтобы удалить его.
3. По завершении редактирования щелкните Применить (Apply).

Архивация данных с помощью мастера архивации

Мастер запускается так.

1. Запустите программу Архинация (Backup) и щелкните кнопку Мастер архивации (Backup Wizard). Затем щелкните Далее (Next).

Примечание Вы можете сначала выбрать файлы на вкладке Архивация (Backup), а затем запустить Мастер архива-

ции (Backup Wizard). Тогда вы заархивируете только выделенные файлы. Щелкнув Да (Yes) в открывшемся информационном окне, вы сразу перейдете в диалоговое окно Элементы для архивации (Items to Back Up), щелкнув Нет (No) — снимете выделение с выбранных файлов и запустите мастер в обычном режиме.

2. Выберите, что вы хотите архивировать:
   - **Архивировать все данные на этом компьютере (Back up everything on this computer)** — архивируются все данные на компьютере, включая данные состояния системы;
   - **Архивировать выбранные файлы,** диски или **сетевые данные (Back up** selected files, **drives, or network data)** — архивируются только выбранные данные;
   - **Архивировать только данные состояния системы (Only back up the system** state **data)** — создается архив данных состояния системы.

Примечание На серверах Windows Server 2003, не являющихся контроллерами доменов, к данным состояния системы относятся основные загрузочные и системные файлы, реестр Windows и БД COM+. На контроллерах домена данные состояния системы также включают данные службы каталогов Active Directory и файлы из системного тома (Sysvol).

3. Щелкните Далее (Next). Выберите данные для архивации (рис. 15-5).
   - Установите или сбросьте флажки рядом с дисками и папками. Если установить флажок диска (папки), выбираются все папки и файлы на нем (в ней). При сбросе флажка все папки и файлы на диске (в папке) исключаются из архивации.
   - Чтобы выделить определенный файл или папку, щелкните значок «+». Теперь вы можете установить или сбросить флажок отдельного файла или папки. При этом флажок родительского элемента затенен, т. е. не все файлы на нем выбраны для архивации.
4. Щелкните Далее (Next) и укажите тип носителя архива. Задайте имя файла, если хотите сохранить архив к файл. Выберите устройство хранения, если хотите сохранить архив файлов и папок на ленте или съемном диске.

Рис. 15-5. Выберите диски, папки и файлы для архивации

Совет При архивации в файл он, как правило, имеет расширение .BKF, но вы можете выбрать и другое расширение. Помните, что для управления лентами и съемными дисками используется служба съемных носителей. Если нет ни одного доступного носителя, вам будет предложено разместить носитель в пуле. См. раздел «Управление пулом носителей».

5. Задайте файл архива или носитель. Если вы архивируете в файл, введите путь и имя файла или щелкните Обзор (Browse) для его поиска. Если вы архивируете на ленту или съемный диск, выберите ленту или диск. Щелкните Далее (Next).
6. Щелкните Дополнительно (Advanced), чтобы изменить параметры по умолчанию или задать расписание для выполнения архивации. Вот некоторые из параметров, которые вы можете здесь задать:
   - Проверять данные после архивации (Verify data after backup) — если этот параметр включен, каждый файл архива сравнивается с оригинальным файлом. Проверка данных защищает архив от ошибок записи и сбоев;
   - **Использовать аппаратное сжатие, если возможно (Use hardware compression, if available)** — этот **параметр до-**

ступен, только когда устройство поддерживает аппаратное сжатие. Прочитать сжатую информацию способны только совместимые устройства. Это значит, что данные разрешено восстанавливать только с накопителя того же изготовителя;

- Отключить теневое копирование состояния тома (Disable Volume Shadow Copy) — отказ от теневого копирования томов. Теневые копии томов используются для архивирования файлов, в которые в данный момент производится запись. Если вы отключите этот параметр, программа Архивация (Backup) будет пропускать такие файлы.

7. Пройдите остальные окна мастера и щелкните Готово (Finish). Вы можете отменить выполняемую архивацию, щелкнув Отмена (Cancel) в диалоговых окнах Информация о наборе (Set Information) или Ход архивации (Backup Progress).

Примечание В окне Ход архивации (Backup Progress) отображается текущее состояние архивации. Обратите внимание на количество обработанных файлов и на их суммарный размер. Если вы работаете с ленточной библиотекой, в ходе операции вам, возможно, придется добавить дополнительные носители.

Примечание Программа Архивация (Backup) ведет себя поразному в зависимости от типа и состояния файла. Если файл открыт, она попытается архивировать последнюю записанную версию. Если файл заблокирован, он не будет архивирован. Не будут архивированы и файлы из списка исключений.

8. По завершении архивации щелкните Закрыть (Close) для окончания процесса или Отчет (Report) — для просмотра журнала архивации.

Архивация файлов без помощи мастера

Допустимо проводить архинацию файлов вручную.

1. Запустив программу Архивация (Backup), перейдите на одноименную вкладку (рис. 15-6).
2. Выберите в меню Задание (Job) команду Создать (New). Щелкните Да (Yes).
3. Выделите данные для архивации.
   - Отметьте или сбросьте флажки рядом с дисками или папками. Если отметить флажок диска, все папки и фай-

лы на кем будут выбраны, при сбросе флажка все папки и файлы диска исключаются из архивации.

- Чтобы выделить определенный файл или папку, щелкните значок «+». Теперь установите или сбросьте флажок отдельного файла или папки. При этом флажок диска затенен, т. е. не все файлы на нем выбраны для архивации.
- Чтобы сохранить данные состояния системы, установите флажок System State ветви Мой компьютер (My Computer). Для серверов, не являющихся контроллерами доменов, в данные состояния системы входят основные загрузочные и системные файлы, реестр Windows и база данных COM+. Для контроллеров домена в данные состояния системы также включаются данные службы каталогов Active Directory и файлы, хранящиеся на системном томе.
- Чтобы архивировать данные сервера Microsoft Exchange, установите флажок Microsoft Exchange в ветви Мой компьютер (My Computer). Введите UNC-имя сервера Microsoft Exchange, который нужно сохранить, например **\\CorpMail.**

Рис. 15-6. Настройте архивацию и щелкните Архивировать (Start Backup)

4. В списке Местоназначение архива (Backup Destination) укажите тип носителя архива. Если вы выбрали Файл (File), архивация проводится в файл, если внешнее хранилище — файлы и папки сохраняются на ленту или съемный диск.
5. В списке Носитель архива или имя файла (Backup media or file name) выберите файл архива или носитель. Если вы архивируете в файл, введите путь и имя файла или щелкните Обзор (Braw.se), если на ленту или съемный диск — укажите ленту или диск.
6. Щелкните кнопку Архивировать (Start Backup). Появится диалоговое окно Сведения о задании архивации (Backup Job Information) со следующими параметрами (рис. 15-7):

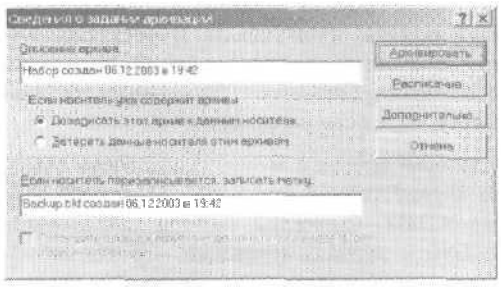


Рис. 15-7. В диалоговом окне Сведения о задании архивации (Backup Job Information) настройте параметры архивации

- Описание архива (Backup Description) задает метку архива, которая используется только при текущей архивации;
- **Дозаписать** этот архив к данным носителя (Append this backup to the media) — добавляет текущее задание архивации к имеющемуся файлу или на имеющуюся ленту;
- Затереть данные носителя этим архивом (Replace the data on the media with this backup) удаляет файл архива или все задания архивации, сохраненные на лепте, перед запуском нового задания архивации;
- Если носитель перезаписывается, **записать** метку (If the media is overwritten, use this label to identify the media) задает метку носителя, которая записывается только при использовании чистого носителя или записи поверх существующих данных;

- **Разрешать доступ к архивным данным только владельцам и администраторам (Allow only the owner and the Administrator access to the backup data)** — при перезаписи данных с помощью этого флажка вы можете указать, что доступ к данным архива имеют только владелец и администратор.

7. Щелкните кнопку Дополнительно (Advanced), чтобы настроить дополнительные параметры. Затем щелкните OK.
8. Если вы не хотите выполнить архивацию немедленно, щелкните кнопку Расписание (Schedule). Когда появится предложение записать текущие параметры архивации, щелкните Да (Yes). Затем введите имя сценария выбора и щелкните Сохранить (Save). Укажите пользователя, от имени которого должно запускаться задание, и его пароль. В окне Параметры запланированного задания (Scheduled Job Options) введите имя задания, щелкните Свойства (Properties) и составьте расписание. Пропустите остальные пункты.

Примечание Сценарии выбора и журналы архивации сохраняются в папке *%UserProfile%*\Local Settings\Microsoft\ WindowsNT\NTBackup\Data. Сценарии выбора сохраняются с расширением .BKS, а журналы архивации — с расширением .LOG. Вы можете просмотреть содержимое этих файлов в любом стандартном текстовом редакторе.

9. Чтобы начать архивацию немедленно, щелкните Архивировать (Start Backup). Для отмены выполняемой архивации щелкните Отмена (Cancel) в диалоговых окнах Информация о наборе (Set Information) или Ход архивации (Backup Progress).
10. По завершении архивации щелкните Закрыть (Close) или Отчет (Report).

Восстановление данных с помощью мастера

Для восстановления данных используют Мастер восстановления (Restore Wizard) или вкладку Восстанонленис (Restore). Чтобы восстановить данные с помощью мастера, выполните следующие действия.

1. Убедитесь, что необходимый для работы архивный набор загружен в библиотеку.
2. Запустите утилиту Архинация (Backup). Щелкните кнопку Мастер восстановления (Restore Wizard), а затем — Далее (Next).

Примечание Разрешается сначала выбрать файлы на вкладке Восстановление (Restore), а затем запустить мастер восстановления. Тогда вы восстановите только выделенные файлы. Щелкнув Да (Yes) в открывшемся информационном окне, вы сразу перейдете в диалоговое окно, показанное на рис. 15-8, щелкнув Нет (No) — снимете выделение с выбранных файлов и запустите мастер в обычном режиме,

3. Щелкните Далее (Next) и выберите данные для восстановления (рис. 15-8). В левой части окна отображаются файлы, организованные в тома, в правом — наборы носителей.
   - Отметьте флажки диска, папки или файла, которые хотите восстановить. Если набор носителей, с которым вы будете работать, не отображен, щелкните Файл импорта (Import File) и введите путь к папке, где хранится архив.
   - Чтобы восстановить данные о состоянии системы, установите флажок Состояние системы (System State). Если вы восстанавливаете файлы в исходное положение, текущие данные состояния системы будут заменены на восстанавливаемые. Если восстановление выполняется в альтернативное размещение, восстанавливаются только реестр, системные загрузочные файлы и файлы папки Sysvol.

Совет По умолчанию Active Directory и другие реплицируемые данные, например данные папки Sysvol, на контроллерах домена не восстанавливаются. Эта информация реплицируется на контроллер после его перезапуска, что защищает ее от случайной перезаписи (см. также раздел «Восстановление Active Directory»).

   - Чтобы восстановить Microsoft Exchange, выделите данные Microsoft Exchange. Перед запуском восстановления вы увидите диалоговое окно Восстановление Microsoft Exchange (Restoring Microsoft Exchange). Если вы собираетесь восстанавливать банк сообщений, введите UNC-имя сервера Microsoft Exchange, например **\\CorpMail**. При восстановлении другого сервера выберите Стереть все имеющиеся данные (Erase all existing data): все существующие данные уничтожатся, и будет создан новый банк.

Примечание Перед запуском процесса восстановления на сервере Exchange останавливаются службы Information Store и Directory. После восстановления перезапустите их.

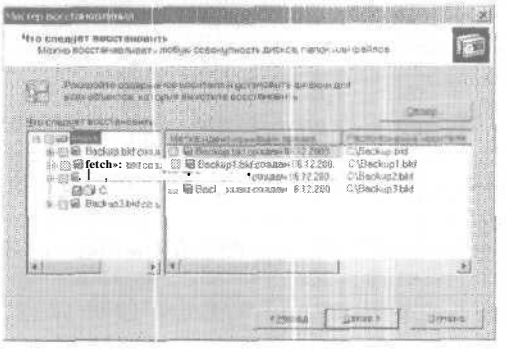


Рис. 15-8. Выделение файлов и папок для восстановления

4. Щелкните Далее (Next), затем Дополнительно (Advanced), чтобы изменить параметры по умолчанию, в частности место для восстановления.
   - **Исходное размещение (Original Location)** — файлы и папки восстанавливаются в то место, с которого были заархивированы.
   - **Альтернативное размещение (Alternate Location)** — данные восстанавливаются в указанное место с сохранением структуры папок. Выбрав этот параметр, введите путь или используйте для поиска нужной папки кнопку Обзор (Browse).
   - **Одну папку (Single Folder)** — все файлы восстанавливаются в одну папку без сохранения структуры папок. Выбран этот параметр, введите путь или используйте для поиска нужной папки кнопку Обзор (Browse).

Совет Если вы не уверены, что следует восстанавливать данные в исходное размещение, выберите Альтернативное размещение (Alternate Location) и задайте новое расположение, например **C:\temp.** Поскольку файлы находятся во временной папке, их можно сравнить с существующими файлами и решить, восстанавливать ли их. Помните: всегда следует восстанавливать данные, архивированные с дисков с файловой системой NTFS, на диски NTFS. Только

тогда можно быть уверенным, что разрешения восстановятся, а шифрование и сжатие NTFS сохранятся.

5. Пройдите через все окна мастера и щелкните Готово (Finish). При необходимости введите путь или имя архива. Чтобы прервать восстановление, щелкните Отмена (Cancel) в окнах Информация о наборе (Set Information) или Ход восстановления (Restore Progress).
6. Завершив восстановление, щелкните Закрыть (Close) или Отчет (Report) — для просмотра журнала, содержащего информацию о ходе процесса восстановления.

Восстановление данных без помощи мастера

Данные можно восстановить вручную.

1. При необходимости загрузите архивный набор из библиотеки.
2. Запустите утилиту Архивация (Backup) и перейдите на вкладку Восстановление и управление носителем (Restore and Manage Media), показанную на рис. 15-9.

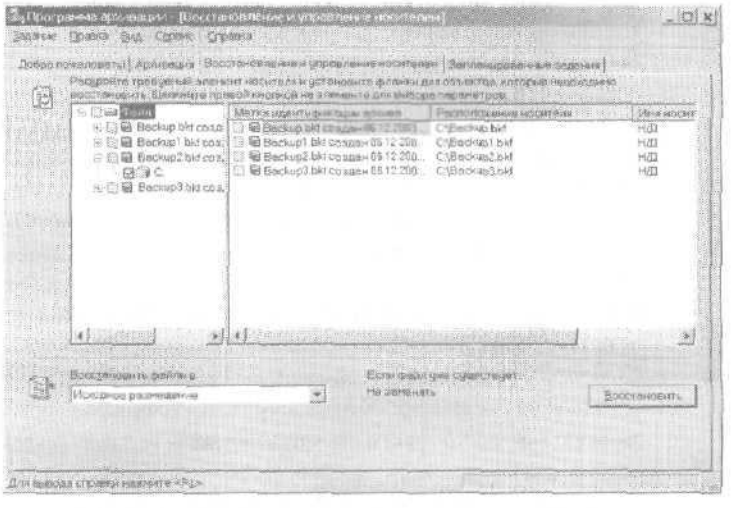


Рис. 15-9. Выбор файлов и папок для восстановления на вкладке Восстановление и управление носителем (Restore and Manage Media)

3. Укажите данные для косстановления. В левом окне отображаются файлы, организованные в тома. В нравом окне по-

казаны наборы носителей. Если набор носителей, с которым вы собирались работать, не отображен, щелкните правой кнопкой файл в левом окне, выберите Каталог (Catalog), затем введите имя или путь используемого каталога.

4. В списке Восстановить файлы в (Restore Files To) выберите место для восстановления (см. пункт 4 предыдущего раздела).
5. Задайте способ восстановления файлов, выбрав в меню Сервис (Tools) команду Параметры (Options):
   - Не заменять файл на компьютере (рекомендуется) [Do not replace the file on my computer (recommended)] — выберите этот параметр, если вы не хотите копировать поверх существующих файлов;
   - Заменять файл на компьютере, только если он старее (Replace the file on disk only if the file on disk is older) — выберите этот параметр, чтобы заменить старые файлы на диске более свежими версиями из архива;
   - **Всегда заменять файл на компьютере (Always replace** the file on my computer) — выберите этот параметр, чтобы заменить все файлы на диске файлами из архива.
6. Щелкните OK.
7. Щелкните Восстановить (Start Restore). Появится диалоговое окно Подтверждение восстановления (Confirm Restore). На этом этапе можно задать дополнительные параметры восстановления, щелкнув кнопку Дополнительно (Advanced).
8. Щелкните OK. При необходимости введите путь или имя архива. Вы можете прервать восстановление, щелкнув Отмена (Cancel) в окнах Информация о наборе сведений (Set Information) или Ход восстановления (Restore Progress).
9. Завершив восстановление, щелкните Закрыть (Close) или Отчет (Report) — для просмотра журнала, содержащего информацию о ходе процесса восстановления.

Восстановление Active Directory

Сначала надо определить, в каком режиме восстанавливать данные состояния контроллера: полномочном или неполномочном. По умолчанию задан последний. В этом режиме Active Directory и другие реплицируемые данные восстанавливаются с использованием информации с других контроллеров. По-

этому вы можете безопасно восстановить отказавший контроллер бел потери новой информации Active Directory. С другой стороны, если вы пытаетесь восстановить Active Directory но всей сети с использованием архивных данных, необходимо полномочное восстановление. В этом режиме данные восстанавливаются на одном контроллере домена, а затем реплицируются на другие.

Чтобы восстановить Active Directory на контроллере домена с дальнейшей репликацией восстановленных данных по всей сети, выполните следующие действия.

1. Выключите сервер контроллера домена.
2. Запустите сервер. В процессе загрузки на этапе выбора ОС нажмите F8.
3. Выберите Восстановление службы каталогов (Directory Services Restore Mode).
4. После запуска системы восстановите данные состояния системы и другие необходимые файлы с помощью утилиты Архивация (Backup).
5. После восстановления данных, но перед перезапуском системы с помощью инструмента Ntdsutil пометьте объекты как полномочные. Проверьте данные Active Directory.
6. Перезапустите сервер. После загрузки сервера данные Active Directory должны реплицироваться по домену.

Архивация и восстановление данных удаленной системы

Утилита Архивация (Backup) позволяет архивировать данные удаленных систем. Для этого перед началом архивации необходимо создать сетевые диски удаленных файловых систем. При архивации данных с сетевых дисков убедитесь, что выбран параметр Архивировать содержимое подключенных дисков (Back up the contents of mounted drives). Иначе сохранятся только ссылки на папки, но не сами данные.

Утилита Архивация (Backup) позволяет восстановить данные удаленных систем. При этом вы можете указать место восстановления в окне Сетевое окружение (My Network Places). Если вы восстанавливаете данные на сетевой диск взамен существующей системы, убедитесь, что отмечен флажок Восстановление точек соединения, а также ссылок для файлов и папок ниже соединения на исходное размещение (Restore

junction points, and restore file and folder data under junction points to the original location),

Просмотр журналов архивации

Журналы архивации — это текстовые файлы в кодировке Unicode, хранящиеся в папке *%UserProfile%*\Local Settings\Application Data\Microsoft\Windows NT\NTBackup\Data. Их имена имеют формат backup##.log, причем backup01.log — исходный файл журнала, созданный утилитой Архивация (Backup).

Хотя вы вправе самостоятельно открывать эти журналы в любом текстовом редакторе, в программе Архивация (Backup) предусмотрена команда для доступа к ним. Выполните следующие действия.

1. Работая в расширенном режиме, выберите в меню Сервис (Tools) команду Отчет (Report). Откроется диалоговое окно Отчеты архивации (Backup Reports).
2. Выделите журнал и щелкните кнопку Просмотр (View). Журнал откроется в текстовом редакторе по умолчанию.
3. Чтобы напечатать журнал, выделите его и щелкните Печать (Print). Журнал будет напечатан на принтере по умолчанию.

Архивирование шифрованных данных и сертификатов шифрования

Если в вашей организации используется шифрованная файловая система EFS (Encrypting File System), в план резервного копирования и восстановления данных следует включить дополнительные процедуры. Вам придется специально продумать ответы на вопросы, связанные с личными сертификатами шифрования, агентами восстановления EFS и политикой восстановления EFS (подробнее — в главе 11). В принципе, архивирование и восстановление шифрованных данных аналогично архивированию и восстановлению обычных данных, Нужно лишь использовать для этого архивные программы, поддерживающие EFS. Однако риск возникновения различных проблем в этом случае значительно больше.

Архивирование и восстановление шифрованных данных не подразумевает автоматического сохранения сертификата, который необходим для работы с ними. Сертификат содержит-

ся в профиле пользователя, поэтому с чтением восстановленных шифрованных данных не возникнет никаких проблем, если учетная запись пользователя осталась в системе, а его профиль либо невредим, либо также архивирован и впоследствии восстановлен. В противном случае не обойтись без агента восстановления. Поэтому архивирование и восстановление сертификата шифрования необходимо предусмотреть в плане.

Архивация сертификатов шифрования

Для архивации и восстановления личных сертификатов шифрования используется оснастка Сертификаты (Certificates). Личные сертификаты сохраняются в формате PFX (Personal Information Exchange). Для архивации личных сертификатов выполните следующие действия.

1. Зарегистрируйтесь на компьютере, на котором хранится нужный личный сертификат, с учетной записью пользователя — владельца сертификата. Щелкните кнопку Пуск (Start) и выберите команду Выполнить (Run).
2. Введите **mmc** в поле Открыть (Open) и щелкните OK. Откроется пустая консоль MMC.
3. Выберите в меню Файл (File) команду Добавить или удалить оснастку (Add/Remove Snap-In).
4. Щелкните кнопку Добавить (Add) на вкладке Изолированная оснастка (Standalone). Выделите элемент Сертификаты (Certificates) и щелкните Добавить (Add). Откроется диалоговое окно Оснастка диспетчера сертификатов (Certificates Snap-in).
5. Установите переключатель Моей учетной записи пользователя (My user account) и щелкните Готово (Finish).
6. Щелкните Закрыть (Close) и OK.
7. Последовательно разверните узлы Сертификаты — текущий пользователь (Certificates — Current User), Личные (Personal) и Сертификаты (Certificates). Щелкните правой кнопкой сертификат, который хотите сохранить, раскройте подменю Все задачи (All Tasks) и выберите Экспорт (Export). Запустится Мастер экспорта сертификатов (Certificate Export Wizard).
8. Щелкните Далее (Next). Выберите Да, экспортировать закрытый ключ (Yes, export the private key). Щелкните Далее (Next).

9. Щелкните Далее (Next), приняв значения параметров по умолчанию, а затем введите пароль для сертификата.
10. Укажите расположение файла сертификата. Файл сохраняется с расширением .pfx.
11. Щелкните Далее (Next) и Готово (Finish). Откроется окно с информацией о завершении экспорта. Щелкните OK.

Восстановление сертификатов шифрования

Заархивированный сертификат можно восстановить не только на исходном компьютере, но и на любом другом компьютере сети. Собственно, именно так осуществляется перенос сертификата с системы на систему. Для этого нужно выполнить следующие действия.

1. Скопируйте файл .pfx на дискету и зарегистрируйтесь на компьютере, где предполагается использоваться сертификат.

Примечание Для регистрации на целевом компьютере необходима учетная запись пользователя, чей сертификат вы переносите. Если вы воспользуетесь любой другой учетной записью, пользователь со своими зашифрованными данными работать не сможет.

2. Откройте оснастку Сертификаты (Certificates), как описано в предыдущем разделе.
3. Разверните узел Сертификаты — текущий пользователь (Certificates – Current User) и щелкните правой кнопкой элемент Личные (Personal). Раскройте подменю Все задачи (All Tasks) и выберите команду Импорт (Import). Будет запущен Мастер импорта сертификатов (Certificate Import Wizard).
4. Щелкните Далее (Next) и вставьте дискету в дисковод.
5. Щелкните Обзор (Browse) и найдите файл личного сертификата на дискете. Выделите его и щелкните Открыть (Орел).
6. Щелкните Далее (Next). Введите пароль личного сертификата и еще раз щелкните Далее (Next).
7. По умолчанию сертификат размещается в папке Личные (Personal). Если вас это устраивает, щелкните Далее (Next) и Готово (Finish). На экране появится окно с информацией о завершении импорта. Щелкните OK.

Аварийное восстановление системы

Архивация — это только часть общего плана аварийного восстановления. Для гарантированного восстановления системы в любой ситуации вам понадобятся диски аварийного восстановления и загрузочные диски. Возможно, понадобится установить Консоль восстановления (Recovery Console).

Чтобы восстановить систему, сделайте так.

1. Попытайтесь запустить систему в безопасном режиме (см. раздел «Запуск системы R безопасном режиме» этой главы).
2. Попытайтесь восстановить систему с помощью данных аварийного восстановления (см. раздел «Использование данных аварийного восстановления» этой главы).
3. Попытайтесь восстановить систему с помощью консоли восстановления (см. раздел «Работа с консолью восстановления» этой главы).
4. Восстановите систему из архива. Убедитесь, что были восстановлены данные состояния системы и необходимые файлы.

Создание данных аварийного восстановления

Автоматически создаваемые *данные аварийного восстановления системы* (System Recovery Data) помогут восстановить систему, если она не загружается. В эти данные включены основные системные файлы, загрузочный сектор и среда запуска системы. Вам следует создать такие данные для каждого компьютера сети, начиная с серверов Windows Server 2003. Кроме того, их нужно обновлять при установке служебных пакетов, работе с загрузочным диском или модификации окружения загрузки.

.0. **Совет** По завершении установки ОС основная информация для восстановления записана в папку *%SystemRoot%*\Repair системного раздела. В папке Repair хранится копия данных локального диспетчера учетных записей безопасности (Security Account Manager, SAM) и других системных файлов. Но папка не содержит резервной копии реестра Windows. При подготовке данных аварийного восстановления вам следует указать на необходимость ее создания.

Данные аварийного восстановления создаются так.

1. Запустите утилиту Архивация (Backup). При необходимости перейдите в расширенный режим, в первом окне утили-

ты щелкните кнопку Мастер аварийного восстановления системы (Automated System Recovery Wizard) и Далее (Next).

2. Дождавшись соответствующего запроса системы, вставьте чистую отформатированную дискету в дисковод.
3. Чтобы создать резервную копию реестра, установите флажок Архивировать реестр в папку восстановления (Also backup the registry to the repair directory). Копия реестра будет создана в папке *%SystemRoot%*\Repair. Для восстановления реестра необходимо использовать Консоль восстановления (Recovery Console).
4. Щелкните OK. По окончании процесса выньте дискету и пометьте ее как диск аварийного восстановления системы.

Запуск системы в безопасном режиме

Если система не загружается в обычном режиме, воспользуйтесь для восстановления работоспособности и поиска неисправностей *безопасным режимом* (safe mode). В этом режиме загружаются только основные файлы, службы и драйверы, включая драйверы мыши, клавиатуры, монитора, хранилищ данных и видеоадаптера. Сетевые драйверы и службы запускаются, только если вы выберете вариант загрузки Безопасный режим с загрузкой сетевых драйверов (Safe Mode With Networking). Обычно сначала стоит попробовать обойтись только безопасным режимом загрузки и лишь в случае неудачи прибегнуть к данным аварийного восстановления или консоли восстановления.

В безопасном режиме система запускается так.

1. Запустите (перезапустите) систему.
2. В процессе загрузки на этапе выбора ОС нажмите F8.
3. Выберите вариант Безопасный режим (Safe Mode) и нажмите Enter. Выбор конкретного вида безопасного режима зависит от ситуации. Вот основные варианты загрузки:
   - **Безопасный режим** (Safe **Mode)** — в процессе инициализации загружаются только основные файлы, службы и драйверы. Ни одна сетевая служба или драйвер не запускаются;
   - **Безопасный режим с поддержкой командной** строки **(Safe Mode with Command Prompt)** — загружаются основные файлы, службы и драйверы. Вместо графическо-

го интерфейса Windows Server 2003 запускается командная строка. Ни одна сетевая служба или драйвер не запускаются;

- **Безопасный режим с загрузкой сетевых драйверов** (Safe **Mode with Networking)** — загружаются основные файлы, службы и драйверы, а также службы и драйверы, необходимые для работы с сетью;
- **Включить протоколирование загрузки (Enable Boot Logging)** — в журнале загрузки создаются записи обо всех событиях запуска;
- **Включить режим VGA (Enable VGA Mode)** — система загружается в режиме VGA. Это полезно, когда настройки дисплея не поддерживаются монитором;
- **Загрузка последней удачной конфигурации (Last Known Good** Configuration) — запуск компьютера в безопасном режиме с использованием информации из реестра, сохраненной после последнего завершения работы;
- **Восстановление службы каталогов (Directory Services Recovery Mode)** — запуск системы в безопасном режиме и восстановление службы каталогов. Доступно только на контроллерах домена Windows Server 2003;
- **Режим** отладки **(Debugging Mode)** — запуск системы в режиме отладки ошибок ОС.

4. Если при запуске в безопасном режиме проблема не проявилась, можно исключить из списка ее возможных причин параметры но умолчанию и драйверы основных устройств. Если проблемы возникли при добавлении нового устройства или обновлении драйвера, используйте безопасный режим для удаления устройства и отмены обновления драйвера.

Использование данных аварийного восстановления

Если вы не можете восстановить работоспособность системы в безопасном режиме, ваш следующий шаг — применение данных аварийного восстановления. Его используют в двух ситуациях. Первая: повреждение загрузочного раздела и основных системных файлов. Вторая: проблема в настройке параметров загрузки. Однако вам не удастся восстановить реестр. Для этого понадобится консоль восстановления.

С помощью данных аварийного восстановления систему восстанавливают так.

1. Вставьте компакт-диск Windows Server 2003 или первый загрузочный диск и перезапустите компьютер. При загрузке с дискет по мере необходимости вставляйте дополнительные загрузочные дискеты.
2. Когда запуститься программа установки, следуйте указаниям, а затем выберите Восстановление (Repair), нажав клавишу R.
3. Вставьте компакт-диск Windows Server 2003 в дисковод, если еще этого не сделали.
4. Выберите аварийное восстановление, нажав R, а затем нажмите одну из двух клавиш:
   - M (Manual) — чтобы вручную восстановить системные файлы, загрузочный раздел или параметры загрузки (этот режим предназначен только опытным пользователям и администраторам);
   - F (Fast) — чтобы ОС сама попыталась решить проблемы с системными файлами, загрузочным разделом и параметрами загрузки.
5. Вставьте диск с данными аварийного восстановления. Поврежденные или отсутствующие файлы будут переписаны с компакт-диска Windows Server 2003 или из панки *%SystemRoot%*\Repairсистемного раздела. Возможно, после записи файлов придется переустановить пакеты обновлений и провести другие изменения.
6. Если восстановление прошло успешно, система перезагрузится в обычном режиме. В противном случае вам придется использовать консоль восстановления.

Работа с консолью восстановления

Консоль восстановления (Recovery Console) — один из последних шансов восстановить систему. Она работает в режиме командной строки и идеально подходит для решения проблем с файлами, дисками и службами. Консоль восстановления позволяет выявить и устранить ошибки загрузочного сектора и главной загрузочной записи, подключить и отключить драйверы устройств и службы, изменять атрибуты файлов томов FAT, FAT32 и NTFS; читать и записывать файлы томов FAT, FAT32 и NTFS, копировать файлы с компакт-дисков или дискет на жесткие диски; проверять и форматировать диски.

Вы можете запустить консоль восстановления с загрузочного диска или установить ее в качестве варианта загрузки.

Установка консоли восстановления в качестве варианта загрузки

Этот способ годится для систем с частыми и регулярными сбоями. Благодаря ему для доступа к консоли не понадобятся загрузочные диски. Такой вариант работает, только если система загружена. Если вам не удастся загрузить систему, обратитесь к разделу «Запуск консоли восстановления вручную».

В качестве варианта загрузки консоль восстановления устанавливается так.

1. Вставьте компакт-диск Windows 2000 в дисковод.
2. Щелкните кнопку Пуск (Start) и выберите команду Выполнить (Run).
3. **Введите h:\i386\winnt32.exe /cmdcons, где *h* — буква дисковода CD-ROM.**
4. **Щелкните** OK, **а затем Да** (Yes).

Примечание Обычно **устанавливать** и запускать консоль восстановления имеет право только администратор. Чтобы разрешить это рядовым пользователям, включите на локальном компьютере политику Консоль восстановления: разрешить автоматический вход администратора (Recovery console: Allow automatic administrative logon) из узла Конфигурация компьютера/Конфигурация Windows/Параметры безопасности/Локальные политики/Параметры безопасности **(Computer** Configuration/Windows Settings/Security Settings/ **Local** Policies/Security Options).

Запуск консоли восстановления вручную

Если система не загружается и вам не удается установить консоль восстановления в качестве варианта загрузки, компьютер и консоль можно запустить так.

1. Вставьте компакт-диск Windows Server 2003 или первый загрузочный диск и перезапустите компьютер.
2. Следуйте указаниям программы установки, а затем выберите Восстановление (Repair), нажав клавишу R.
3. **Вставьте компакт-диск Windows Server 2003 в** дисковод, если еще этого не сделали.

4. Нажмите клавишу C. Введите пароль администратора в ответ на соответствующее предложение.
5. После запуска системы вы увидите командную строку, в которой можно набирать команды консоли восстановления. Для выхода из консоли и перезагрузки компьютера введите **exit**.

Команды консоли восстановления

Консоль восстановления работает в режиме командной строки. Чтобы познакомится со всеми ее командами, введите **help.** Наиболее часто вы будете пользоваться командами ATTRIB, NET, FIXBOOT, FIXMBR **и** EXIT. Команда ATTRIB изменяет атрибуты файлов, NET позволяет подключиться к обшей папке па другом компьютере, FIXBOOT и FIXMBR — это тяжелая артиллерия, с их помощью разрешаются проблемы с загрузочным сектором и главной загрузочной записью на системных дисках. Сделав все необходимые изменения, с помощью команды EXIT выйдите из консоли и перезагрузите компьютер.

Удаление консоли восстановления

Если вам более не требуется загружать консоль восстановления, ее можно удалить.

1. Запустите Проводник (Windows Explorer) и выберите диск, на который установили консоль восстановления. Обычно это **загрузочный** диск.
2. В меню Сервис (Tools) выберите Свойства папки (Folder Options).
3. На вкладке Вид (View) установите переключатель Показывать скрытые файлы и папки (Show hidden files and folders) и сбросьте флажок Скрывать защищенные системные файлы (Hide protected operating system files). Щелкните OK.
4. Удалите из корневой пайки загрузочного диска папку Cmdcons и файл Cmldr.
5. Правой кнопкой щелкните файл Boot.ini и выберите Свойства (Properties).
6. В окне свойств сбросьте флажок Только чтение (Read-Only) и щелкните OK.
7. Откройте файл Boot.ini в Блокноте (Notepad). Удалите запись, запускающую консоль восстановления. Она выглядит так:

```
C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows Server 2003
Recovery Console" /cmdcons
```

8. Сохраните файл Boot.ini и восстановите его атрибут Только чтение (Read-Only).

Консоль восстановления более не будет появляться в списке вариантов загрузки. Конечно, позже вы можете переустановить ее или запускать в ручном режиме.

Управление пулом носителей

Наборы лент организованы в пулы носителей, работа с которыми описана далее.

Основные сведения о пулах носителей

Управление *пулом носителей* (media pool) реализуется в узле Съемные ЗУ (Removable Storage) консоли Управление компьютером (Computer Management), как показано на рис. 15-10. Внутри этого узла все носители отнесены к определенным типам. Концепция пула носителей очень динамична. В одну библиотеку можно включать несколько пулов, некоторые пулы носителей охватывают несколько библиотек. Разрешается выстраивать пулы в иерархию, в которой пулы верхнего уровня включают пулы нижнего уровня, а те в свою очередь содержат наборы лент или дисков.

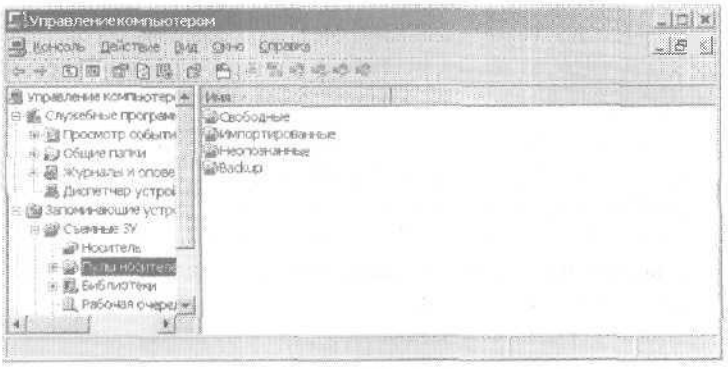


Рис. 15-10. Утилитой Архивация (Backup) используются носители, размещенные в пулах приложения Backup и Свободные (Free)

В узле **Съемные ЗУ** (Removable Storage) **пулы** разделены **на** следующие типы.

- Неопознанные (Unrecognized) — носители, не распознанные узлом Съемные ЗУ (Removable Storage), например новые носители, на которые еще не производилась запись. Чтобы сделать неопознанные носители доступными для использования, переместите их в пул свободных носителей. Если перед этим вы извлечете носитель, он автоматически удаляется из базы данных узла Съемные ЗУ (Removable Storage) и больше не отображается.
- Свободные (Free) — содержит носители, которые в настоящий момент не используются и не хранят данные. Эти носители доступны приложениям.
- Импортированные (Import) — содержит носители, которые распознаны узлом Съемные ЗУ (Removable Storage), но не использовались ранее. Например, если вы переместили носитель из одного места в другое, он может отображаться как импортированный. Для повторного применения носителя на новом месте переместите его в пул свободных носителей или в один из пулов приложений.
- Пул приложения — содержит носители, используемые и управляемые каким-то приложением, например Архивация (Backup). Пулом этого типа управляют члены групп Администраторы (Administrators) и Операторы архива (Backup Operators). Вы можете настроить автоматический перенос носителей из пула Свободные (Free) в пул приложения. Носители из пула приложения далее перемещать нельзя.

Пулы свободных, неопознанных и импортированных носителей относятся к так называемым *системным пулам носителей* (system media pools). Их, в отличие от пулов приложений, удалять нельзя.

Перемещение носителя в другой пул

Вы можете переместить носитель в другой пул, сделав его доступным для использования.

1. В консоли Управление компьютером (Computer Management) раскройте узел Съемные ЗУ (Removable Storage), а затем раскройте узлы Библиотеки (Libraries) и Пулы носителей (Media Pools).
2. Разверните пул, в котором содержится нужный вам носитель.

3. Перетащите носитель на значок нужного пула в дереве консоли.

Внимание! Перемещение носителя в пул свободных носителей уничтожит данные на носителе. Переносить в пул свободных носителей носители, предназначенные только для чтения, нельзя.

Создание пулов приложений

1. В узле Съемные ЗУ (Removable Storage) правой кнопкой щелкните элемент Пулы носителей (Media Pools) или существующий пул приложения и выберите Создать пул носителей (Create Media Pool).
2. В диалоговом окне Свойства: Создать новый пул носителей (Create a New Media Pool Properties) введите имя и описание пула носителей (рис. 15-11).

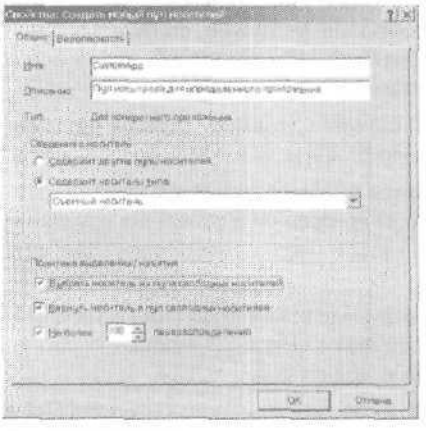


Рис. 15-11. Укажите тип носителя и задайте правила выделения носителя и его изъятия

3. Установите переключатель Содержит носители типа (Contains media of type) и выберите тип носителя из списка. Если пул содержит другие пулы носителей, установите переключатель Содержит другие пулы носителей (Contains other media pools).
4. Завершите процесс, щелкнув OK. Задайте размещение носителя и настройте для него параметры безопасности (подробнее — далее в этой главе).

Изменение типа носителей в пуле носителей

Каждый пул может содержать носители только одного типа. Обычно тип носителей задается при создании пула, но вы вправе изменять его.

1. В узле Съемные ЗУ (Removable Storage) дважды щелкните Пулы носителей (Media Pools).
2. Правой кнопкой щелкните нужный пул и выберите Свойства (Properties).
3. На вкладке Общие (General) щелкните Содержит носители типа (Contains media of type) и выберите тип носителя из списка.

Настройка политики выделения и изъятия

Вы можете настроить пулы приложений на автоматическое *выделение* (allocation) и *изъятие* (deallocation) свободных носителей. При этом, если приложению понадобится носитель, оно его получит. Если носитель больше не нужен, он будет возвращен в пул свободных носителей. Настраивают, размещают и освобождают носители таким образом.

1. В узле Съемные ЗУ (Removable Storage) дважды щелкните Пулы носителей (Media Pools).
2. Правой кнопкой щелкните нужный пул и выберите Свойства (Properties), Этот пул должен содержать носители определенного типа и не должен быть контейнером для других пулов носителей.
3. Флажки группы Политика выделения/изъятия (Allocation/ Deallocation Policy) на вкладке Общие (General) позволяют управлять выделением носителей.
   - **Выбрать носитель из** пула **свободных носителей (Draw media from Free media pool)** — автоматическое перемещение лент или дисков из пула свободных носителей в данный пул при необходимости. Если этот флажок не помечен, при нехватке носителей ленты или диски придется перемещать из пула свободных носителей вручную.
   - **Вернуть носитель в пул свободных носителей (Return media to Free media pool)** — автоматический возврат лент или дисков в пул свободных носителей, если они больше не требуются приложению. Если этот флажок не помечен, ненужные ленты и диски придется возвращать

в пул свободных носителей вручную, чтобы они оказались доступными другим приложениям.

- **Не более (Limit Reallocations)** — ограничение числа перераспределений лент и носителей из пула свободных носителей в другие пулы. Если этот флажок помечен, измените значение по умолчанию, введя другое значение.

4. Щелкните OK.

Управление доступом к съемным носителям

Подобно другим объектам Windows Server 2003, у съемных носителей имеется набор разрешений. Их можно задавать как для узла Съемные ЗУ (Removable Storage) в целом, так и для отдельных пулов, библиотек и носителей. Эти разрешения описаны в табл. 15-4.

Примечание Помните, что эти разрешения применяются к системе съемных ЗУ, но не к файлам, которые хранятся на носителях.

Таблица 15-4. Разрешения съемных носителей

Разрешение	Для всей системы съемных ЗУ	Для носителей, пулов и библиотек
Использование (Use)	Разрешает доступ на чтение к узлу Съемные ЗУ (Removable Storage), но не к носителям, пулам или библиотекам	Разрешает доступ на чтение к конкретному носителю, пулу или библиотеке. Разрешает пользователю вставлять и извлекать носитель и просматривать оглавление ленты
Изменить (Modify)	Разрешает чтение и запись. Пользователь может создавать пулы носителей и управлять очередями	Пользователь может изменять свойства носителя, пула или библиотеки
Элемент управления (Control)	Разрешает все, что допускается разрешениями Использование (Use) и Изменить (Modify). Кроме того, пользователь вправе удалять пулы и библиотеки	Разрешает пользователю вставлять и извлекать носитель и просматривать оглавление ленты, а также удалять пулы и библиотеки
Смена разрешений (Modify Permissions)	Разрешает пользователю изменять разрешения носителей, пулов и библиотек	Позволяет пользователю изменять разрешения носителей, пулов и библиотек

Таблица 15-4. Разрешения съемных носителей *(окончание)*

Разрешение	Для всей системы съемных ЗУ	Для носителей, **пулов** и библиотек
Просмотр разрешений (View Permissions)	Разрешает пользователю просматривать разрешения носителей, пулов и библиотек	Позволяет пользователю просматривать разрешения носителей, пулов и библиотек

Изначально узлом Съемные ЗУ (Removable Storage) могут управлять только сама ОС, администраторы и операторы архива. Доступ обычных пользователей к съемным носителям ограничен. Если вы применяете съемные носители не только для архивации данных, права пользователей можно расширить. Чтобы просмотреть заданные разрешения и изменить их, выполните следующие действия.

1. Щелкните правой кнопкой нужный элемент узла Съемные ЗУ (Removable Storage).
2. Выберите команду Свойства (Properties) и перейдите на вкладку Безопасность (Security), показанную на рис. 15-12.

Рис. 15-12. Здесь настраиваются разрешения съемных носителей

3. В списке Группы или пользователи (Group or user names) перечислены пользователи и группы, которым уже назначены разрешения для работы с элементов. Чтобы изменить эти разрешения, выделите пользователя или группу и за-

дайте разрешения в списке Разрешения для (Permissions for). Чтобы добавить пользователя, компьютер или группу, щелкните кнопку Добавить (Add).

4. Щелкните OK.

Удаление пулов приложений

Чтобы удалить пул приложения, щелкните его правой кнопкой и выберите Удалить (Delete). Удаляйте только ненужные пулы носителей.

Примечание Вы не сможете удалить пулы приложений, созданные Windows Server 2003.

Управление рабочими очередями, запросами и операторами

При работе со съемными носителями следует обращать особое внимание на рабочие очереди, запросы операторов и защиту данных.

Рабочая очередь

Рабочей очередью (work queue) называется область узла Съемные ЗУ (Removable Storage), в которой отображается информацииобоперациях,инициированныхадминистраторами,операторами архива и другими пользователями с соответствующими правами. Для каждой операции в рабочей очереди указан ее статус:

- Ожидание (Waiting) — операцияждет своей очереди на исполнение;
- В работе (In Progress) — операциявыполняется;
- Завершено (Completed) — операция успешно выполнена;
- Отменено (Cancelled) — выполнение операции прервано администратором или другим оператором;
- Завершить не удалось (Failed) — при выполнении операции возникли ошибки.

По умолчанию завершенные, отмененные и неудачные запросы остаются в очереди в течение 72 часов. Ожидающие и выполняемые операции остаются в очереди до изменения их статуса. При желании вы можете выполнить с этими операциями следующиедействия:

- **изменить порядок следования операций подключения,** чтобы более важные для вас операции выполнялись прежде менее важных (подробнее — далее в этой главе);
- отменить операцию с помощью команды из контекстного меню, чтобы освободить дисковод или носитель для выполнения другой операции;
- **удалить завершенную, отмененную или неудачную операцию** вручную **или** автоматически (подробнее — далее в этой **главе).**

Устранение неполадок с ожидающими операциями

Операция в состоянии ожидания может быть индикатором потенциальной проблемы, например некорректного состояния ресурса. Если операция пребывает в состоянии ожидания продолжительное время, может оказаться, что ресурс не подключен, не активирован или просто работает некорректно. Для исправления проблемы вам, вероятно, придется отменить операцию, устранить неполадку с ресурсом, а затем начать операцию заново.

Изменение порядка операций подключения

При наличии нескольких ожидающих операций разрешается изменить порядок их выполнения, выполнив следующие действия.

1. Щелкните правой кнопкой нужную операцию и выберите Переупорядочить установку (Re-Order Mounts). Откроется диалоговое окно Изменение порядка подключения (Change Mount Order).
2. Задайте новое положение операции в очереди.
3. Щелкните OK.

Управление удалением операций

По умолчанию завершенные, отмененные и неудавшиеся операции удаляются из рабочей очереди через 72 часа. Этот порядок можно изменить;

- удалив операции вручную — щелкните операцию правой кнопкой и выберите Удалить (Delete);
- удалив все операции — щелкните правой кнопкой элемент Рабочая очередь (Work Queue), выберите Свойства (Properties) и щелкните кнопку Удалить все сейчас (Delete All Now);

- **перенастроив время автоматического удаления.**

Чтобы изменить порядок автоматического удаления операций, сделайте так.

1. Щелкните правой кнопкой элемент Рабочая очередь (Work Queue) ? выберите Свойства (Properties). Откроется диалоговое окно, показанное на рис. 15-13.

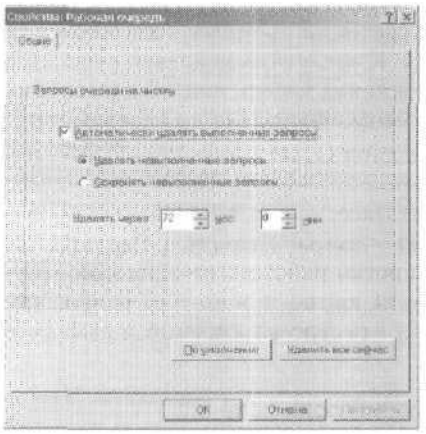


Рис. 15-13. Управление автоматическим удалением операций

2. Чтобы отказаться от автоматического удаления операций, сбросьте флажок Автоматически удалять выполненные запросы (Automatically delete completed requests) и щелкните OK.
3. Чтобы автоматически удалять выполненные операции, установите флажок Автоматически удалять выполненные запросы (Automatically delete completed requests).
4. Установите переключатель Удалять невыполненные запросы (Delete failed requests), чтобы задать автоматическое удаление неудавшихся запросов. Чтобы оставить их в очереди, установите переключатель Сохранять невыполненные запросы (Keep failed requests).
5. Задайте интервал автоматического удаления запросов с помощью счетчиков Удалять через (Delete After).
6. Щелкните OK.

Очередь запросов оператора

Очередью запросов оператора (operator requests) называется область узла Съемные ЗУ (Removable Storage), в которой отображается состояние запросов, нуждающихся во вмешательстве администратора или оператора архива.

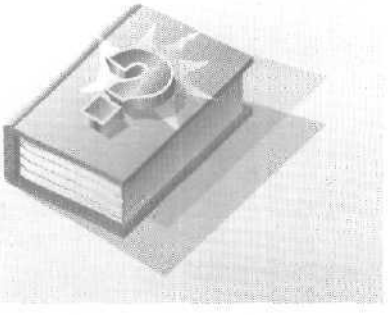
Элементы очереди запросов оператора представляют собой действия, которые должны выполнить вручную вы или другой оператор. Они создаются системой съемных носителей или совместимым приложением. К числу этих действий относятся вставка чистящей ленты, вставка кассет или обслуживание библиотеки. Каждому действию присваивается определенный статус. Вы можете либо выполнить действие, либо отказаться от него. По умолчанию выполненные или отмененные запросы остаются в очереди на 72 часа. Статусы запросов таковы:

- Завершено (Completed) — запрос выполнен. Выполнение запроса детектируется системой автоматически или отмечается оператором. Чтобы вручную пометить запрос как выполненный, щелкните его правой кнопкой и выберите Завершить (Complete);
- Отказано (Refused) — запрос не будет выполнен. Чтобы вручную отменить запрос, щелкните его правой кнопкой и выберите Отказать (Refuse);
- Поставлен в очередь (Submitted) — запрос инициирован системой съемных носителей или совместимым приложением, и система ожидает его выполнения.

Часть IV

Администрирование сети Microsoft Windows Server 2003

Эта часть посвящена проблемам администрирования сетей Microsoft Windows Server 2003. 8 главе 16 содержатся сведения по установке, настройке и тестированию сетей TCP/IP. В главе 17 обсуждается установка и настройка принтеров и серверов печати, а также устранение неполадок, связанных с их работой. В главе 18 рассказывается об управлении клиентами и серверами DHCP. В главе 19 рассматривается настройка клиентов и серверов WINS. Наконец, глава 20 посвящена настройке DNS в сетях Windows Server 2003,



Глава 16

Управление сетями TCP/IP

Для обмена данными между компьютерами используются базовые сетевые протоколы, встроенные в Microsoft Windows Server 2003. Мы рассмотрим протокол TCP/IP (Transmission Control Protocol/Internet Protocol), представляющий собой совокупность протоколов и служб, обеспечивающих передачу информации по сети. TCP/IP — основной протокол, используемый в межсетевых коммуникациях. В сравнении с другими сетевыми протоколами настроить TCP/IP довольно сложно, но эта сложность компенсируется его гибкостью. Эта глава посвящена настройке и управлению сетями TCP/IP.

Примечание Права на установку и управление сетью TCP/IP определяются групповыми политиками из узлов Конфигурация пользователя\Административные шаблоны\Сеть\Сетевые подключения (User Configuration\Administrative Templates\Network\Network Connections) и Конфигурация компьютера\Административные шаблоны\Система\Групповая политика (Computer Configuration\Administrative Templates\System\Group Policy). Подробнее — в главе 4.

Установка сети TCP/IP

Для организации сети TCP/IP нужно установить одну или несколько сетевых плат и настроить протокол TCP/IP.

Установка сетевой платы

Сетевая плата, или *сетевой адаптер,* — это устройство, предназначенное для обмена данными по сети. Чтобы установить ее, выключите компьютер, установите сетевую плату в разъем и снова включите компьютер. При загрузке Windows Server 2003 скорее всего обнаружит и настроит сетевую плату автоматически. При необходимости встаньте диск с драйверами. Если ОС плату не

обнаружила, установите се вручную, как описано в главе 2. После установки платы настройте сетевые службы,

Установка протокола TCP/IP

По умолчанию протокол TCP/IP устанавливается автоматически одновременно с ОС Windows Server 2003. Чтобы установить TCP/IP вручную, войдите в систему по учетной записи с привилегиями администратора и выполните следующие действия.

1. В окне Панели управления (Control Panel) щелкните дважды значок Сетевые подключения (Network Connections).
2. Выберите соединение, с которым вы намерены работать.

Примечание Соединения по локальной сети создаются автоматически для каждой из сетевых плат, установленных на компьютере. О создании подключений других типов читайте в разделе «Управление сетевыми подключениями» этой главы.

3. В диалоговом окне Состояние (Status) щелкните кнопку Свойства (Properties). Откроется диалоговое окно свойств подключения (рис. 16-1).

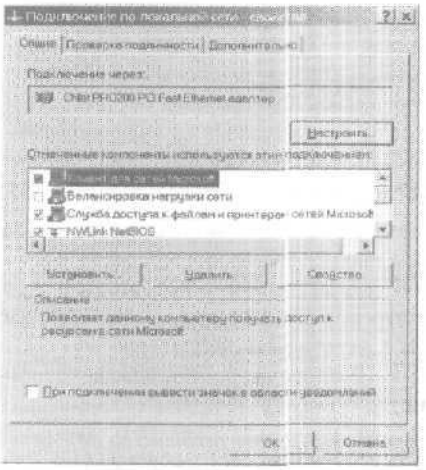


Рис. 16-1. Окно свойств подключения по локальной сети

4. Если протокола TCP/IP нет в списке установленных компонентов, его следует установить. Щелкните кнопку Установить (Install), выделите вариант Протокол (Protocol) и щелкните Добавить (Add). В диалоговом окне Выбор сетевого прото-

кола (Select Network Protocol) выделите протокол TCP/IP и щелкните OK.

5. Убедитесь, что в окне свойств подключения по локальной сети установлен флажок Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP)], и щелкните OK.

Настройка сети TCP/IP

Для передачи информации по сети TCP/IP используются IP-адреса, которые в Windows Server 2003 назначаются несколькими различными способами.

- **Вручную** — IP-адрес, назначенный вручную, называется *статическим* (static). Статические IP-адреса обычно назначаются серверам Windows Server 2003. Помимо статического IP-адреса компьютеру нужно назначить и другие параметры, без которых он не сможет работать в сети.
- Динамически — такое назначение адресов выполняется при наличии в сети сервера DHCP (Dynamic Host Configuration Protocol). Динамическое назначение IP-адресов по умолчанию настраивается на рабочих станциях Windows.
- Автоматически — если компьютер настроен на использование DHCP, а в сети DHCP-сервер отсутствует, Windows Server 2003 автоматически назначает компьютеру IP-адрес из диапазона от 169.254.0.1 до 169.254.255.254 с маской подсети 255.255.0.0.

Настройка статических IP-адресов

Одновременно со статическим IP-адресом вы должны задать на компьютере и другие сетевые параметры, например маску подсети и (при необходимости) шлюз по умолчанию, используемый для обмена данными с другими сетями. IP-адрес — это числовой идентификатор компьютера. Схема адресации зависит от способа организации сети. Обычно IP-адрес выделяется из некоторого блока, назначенного данному сегменту сети. Так, если компьютер находится в сегменте сети с адресом 192.168.10.0, то его IP-адрес лежит в диапазоне 192.168.10.1-192.168.10.254. Адрес 192.168.10.255 обычно резервируется для широковещательных сообщений.

Если локальная сеть подключена к Интернету напрямую, IP-адреса, назначаемые компьютерам, должны быть уникальны. Если сеть является закрытой, т. е. не имеет прямого вы-

хода в Интернет, следует использовать закрытые IP-адреса (табл. 16-1).

Таблица 16-1. Адреса закрытых сетей

Идентификатор частной сети	Маска подсети	Диапазон IP-адресов
10.0.0.0	255.0.0.0	10.0.0.1-10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1-172.31.255.254
192.168.0.0	255.255.0.0	192.168.255.254

Все остальные адреса являются открытыми и должны быть арендованы или куплены.

Проверка адреса с помощью утилиты Ping

Прежде чем назначить статический IP-адрес, следует убедиться в том, что он свободен (не используется и не зарезервирован службой DHCP). Для этого применяют утилиту Ping. Открыв окно командной строки, введите **ping** и нужный IP-адрес, например

```
ping 192.168.10.12
```

Если вы получили положительный ответ, то IP-адрес занят и вам следует выбрать другой I P-адрес. Если при всех попытках ответ в течение времени ожидания не получен, этот IP-адрес в данное время неактивен и, вероятно, не используется.

Назначение статического IP-адреса

Статические IP-адреса назначаются так.

1. В окне Панель управления (Control Panel) дважды щелкните значок Сетевые подключения (Network Connections).
2. Выберите или дважды щелкните нужное сетевое подключение.
3. Щелкните кнопку Свойства (Properties) и дважды щелкните элемент Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP)|. Откроется диалоговое окно свойств TCP/IP (рис. 16-2).
4. Щелкните переключатель Использовать следующий IP-адрес (Use the following IP address) и введите IP-адрес системы в поле IP-адрес (IP Address). Он должен быть уникальным в пределах вашей сети.

Рис. 16-2. Диалоговое окно свойств TCP/IP

5. В поле Маска подсети (Subnet Mask) значение подставляется автоматически. Исправьте его согласно настроенным в вашей организации подсетям или оставьте неизменным, если в вашей сети подсети не используются.
6. Чтобы компьютер получил доступ к другим подсетям, сетям и Интернету, задайте шлюз по умолчанию, т. е. введите в поле Основной шлюз (Default Gateway) IP-адрес маршрутизатора в вашей сети.
7. Введите адреса основного и дополнительного DNS-серверов, с помощью которых в сети осуществляется разрешение имен.
8. Щелкните OK. Повторите эти действия для других сетевых плат. Каждой сетевой плате требуется уникальный IP-адрес.
9. При необходимости настройте службу WINS.

Настройка динамической IP-адресации

Служба DHCP обеспечивает централизованное управление IP-адресами и стандартными параметрами TCP/IP. Если в сети установлен сервер DHCP, сетевой плате на любом компьютере можно назначить динамический IP-адрес. Кроме того, сервер DHCP автоматизирует настройку и других параметров TCP/IP. Динамическую адресацию не следует применять для серверов Windows

Server 2003, так как динамические IP-адреса могут изменяться. Динамическая адресация настраивается так.

1. В окне Панели управления (Control Panel) дважды щелкните значок Сетевые подключения (Network Connections). Затем выберите или дважды щелкните нужное сетевое подключение,
2. Щелкните кнопку Свойства (Properties) и дважды щелкните элемент Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP)]. Откроется диалоговое окно свойств TCP/IP.
3. Установите переключатель Получить IP-адрес автоматически (Obtain an IP address automatically). Если DHCP-сервер передаст клиентам адреса DNS-серверов, установите переключатель Получить адрес DNS-сервера автоматически (Obtain DNS server address automatically). Чтобы отказаться от автоматически назначаемого адреса DNS-сервера, установите переключатель Использовать следующие адреса DNS-серверов (Use the following DNS server addresses) и введите адреса основного и дополнительного серверов.
4. Щелкните OK. Затем при необходимости настройте дополнительные параметры IP-адреса, DNS и WINS.

Настройка автоматического частного IP-адреса

Если в процессе загрузки системы ей не удалось установить связь с DHCP-сервером или срок аренды текущего IP-адреса истек, компьютеру автоматически присваивается IP-адрес, по умолчанию лежащий в диапазоне от 169.254.0.1 до 169.254.255.254 с маской подсети 255.255.0.0. Компьютер с автоматическим IP-адресом фактически изолирован в своем сетевом сегменте, поскольку при автоматической настройке IP-адреса не задаются шлюз но умолчанию, DNS-сервер и WINS-сервер.

Чтобы компьютер использовал определенный IP-адрес при отсутствии DHCP-сервера, следует вручную задать альтернативную конфигурацию. Это удобно, в частности, для пользователей портативных компьютеров, которые одинаково часто работают как в сети, так и вне се. Вы можете настроить портативный компьютер на использование динамического IP-адреса на работе и альтернативного IP-адреса дома или в командировке.

Вот как настраивается автоматический IP-адрес.

1. В окне Панели управления (Control Panel) дважды щелкните значок Сетевые подключения (Network Connections). За-

тем выберите или дважды щелкните нужное сетевое подключение.

2. Щелкните кнопку Свойства (Properties) и дважды щелкните элемент Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP)]. Откроется диалоговое окно свойств TCP/IP.
3. Установите переключатель Получить IP-адрес автоматически (Obtain an IP address automatically), если еще не сделали этого, и перейдите на вкладку Альтернативная конфигурация (Alternate Configuration), показанную на рис. 16-3.

Рис. 16-3. Вкладка Альтернативная конфигурация (Alternate Configuration) позволяет настроить альтернативный IP-адрес компьютера

4. Установите переключатель Настраиваемый пользователем (User Configured option) и введите нужный IP-адрес в одноименное поле. Он должен удовлетворять условиям табл. 16-1 и не должен использоваться где-либо еще.
5. В поле Маска подсети (Subnet Mask) значение подставляется автоматически. Исправьте его согласно настроенным в вашей организации подсетям или не изменяйте, если в вашей сети подсети не используются.
6. Чтобы компьютер получил доступ к другим подсетям, сетям и Интернету, задайте шлюз по умолчанию, т. е. введите в по-

ле Основной шлюз (Default Gateway) IP-адрес маршрутизатора в вашей сети.

7. Введите адреса основного и дополнительного DNS-серверов, с помощью которых в сети осуществляется разрешение имен.
8. При необходимости введите адреса основного и дополнительного WINS-серверов.
9. Щелкните OK.

Настройка нескольких IP-адресов и шлюзов

Компьютер Windows Server 2003 может поддерживать несколько IP-адресов даже при наличии единственной сетевой платы. Такая необходимость возникает, когда:

- компьютердолжен выступать в ролинескольких компьютеров. Это актуально, например, для компьютера, па котором одновременно запущены службы Web. FTP и SMTPДля каждой из этих служб удобно использовать различные IP-адреса;
- сеть разбита на несколько логических сетей (подсетей) и компьютер должен иметь доступ к каждой из них. В этом случае одной сетевой плате также понадобятся несколько IP-адресов, например адрес 192.168.10.8 для доступа из подсети 192.168.10.0 и адрес 192.168.11.8 для доступа из подсети 192.168.11.0.

Если сетевая плата одна, IP-адреса должны принадлежать одному сетевому сегменту или сегментам одной логической сети. Если сеть разбита на несколько физических сетей, вам потребуется несколько сетевых плат, каждой из которых будет назначен IP-адрес, соответствующий отдельному физическому сегменту сети.

Совет Для соединения нескольких сетей воспользуйтесь функциями IP-маршрутизации или создайте сетевой мост. Сервер-маршрутизатор с двумя сетевыми платами, каждая из которых настроена для работы со своей сетью, позволяет обмениваться данными между сетями. При этом используются Служба маршрутизации и удаленного доступа (Routing And Remote Access services) и подходящий протокол маршрутизации, например RIP (Routing Information Protocol). IP-маршрутизация предназначена для средних и крупных предприятий и требует сложной настройки. Мосты удобны в небольших сетях и доступны только компьютерам с ОС Windows Server 2003.

Назначение адресов и шлюзов

Чтобы назначить одной сетевой плате несколько IP-адресов и шлюзов, выполните следующие действия.

1. В окне Панели управления (Control Panel) дважды щелкните значок Сетевые подключения (Network Connections). Затем выберите или дважды щелкните нужное сетевое подключение.
2. Щелкните кнопку Свойства (Properties) и дважды щелкните элемент Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP)]. Откроется диалоговое окно свойств TCP/IP.
3. Щелкните кнопку Дополнительно (Advanced). Откроется окно Дополнительные параметры TCP/IP (Advanced TCP/IP Settings), показанное на рис. 16-4.

Рис. 16-4. Это диалоговое окно позволяет настроить несколько IP-адресов и шлюзов

4. Перейдите на вкладку Параметры IP (IP Settings), щелкните кнопку Добавить (Add) в области IP-адреса (IP Addresses) и введите IP-адрес и маску подсети. Повторите эти действия для каждого IP-адреса, который нужно назначить сетевой плате.
5. Укажите дополнительные шлюзы, щелкнув кнопку Добавить (Add) в области Шлюз (Gateway).

6. Метрика характеризует относительную стоимость использования шлюза. Если в параметрах настройки компьютера указано несколько шлюзов по умолчанию, в первую очередь используется шлюз с наименьшей метрикой. Если связь с ним установить не удается, Windows Server 2003 пытается соединиться со следующим шлюзом. По умолчанию ОС присваивает шлюзу метрику автоматически. Чтобы переназначить ее вручную, сбросьте флажок Автоматическое назначение метрики (Automatic Metric) и введите метрику в соответствующее поле.
7. Щелкните Добавить (Add) и повторите пункты 5-6 для каждого шлюза, который хотите добавить.

Настройка DNS

Служба разрешения имен DNS предназначена для определения IP-адреса компьютера по его имени. Она позволяет использовать вместо трудно запоминаемых IP-адресов понятные имена, например, *http://www.msn.com* или *http://www.microsoft.com*. DNS является основной службой имен для Windows Server 2003 и Интернета.

Совет Для работы DNS в сети нужно установить DNS-сервер. Подробнее — в главе 20.

Основные параметры DNS

Основные параметры DNS настраиваются так.

1. Б окне Панели управления (Control Panel) дважды щелкните значок Сетевые подключения (Network Connections). Затем выберите или дважды щелкните нужное сегевое подключение.
2. Щелкните кнопку Свойства (Properties) и дважды щелкните элемент Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP)]. Откроется диалоговое окно свойств TCP/IP.
3. Если в сети имеется DHCP-сервер, передающий клиентам адреса DNS-серверов, установите переключатель Получить адрес DNS-сервера автоматически (Obtain DNS server address automatically). Чтобы отказаться от автоматически назначаемого адреса установите переключатель Использовать следующие адреса DNS-серверов (Use the following DNS server addresses) и введите адреса основного и дополнительного DNS-серверов.

Дополнительные параметры DNS

Для настройки дополнительных параметров службы DNS предназначена вкладка DNS диалогового окна Дополнительные параметры TCP/IP (Advanced TCP/IP Settings), показанная на рис. 16-5. Она содержит следующие поля.

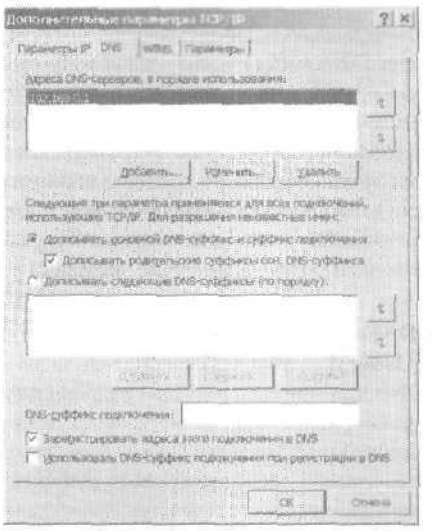


Рис. 16-5. Вкладка DNS диалогового окна Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)

- **Адреса DNS-серверов, в порядке использования (DNS server** addresses, in order of use) — IP-адреса серверов DNS, используемых для разрешения имен доменов. Кнопки Добавить (Add), Изменить (Edit) и Удалить (Remove) позволяют добавлять, редактировать и удалять DNS-серверы соответственно. Вы вправе использовать для разрешения имен несколько серверов, при этом их приоритет определяется положением в списке. Если первый сервер не отвечает на запрос разрешения имени, запрос посылается на второй и т. д. Помните, что запрос передается на следующий сервер, только если предыдущий не отвечает, но никак не из-за того, что тот не смог разрешить указанное имя. Кнопки со стрелками позволяют изменить положение сервера в списке.
- Дописывать **основной DNS-суффикс и суффикс** подключения **(Append primary and** connection **specific DNS suffixes)** — этот

переключатель служит для разрешения неполных имен компьютеров в основном домене. Например, если компьютер Rage расположен в родительском домене *microsoft.com,* его имя будет преобразовано в *rage.microsoft.com.* Родительский домен задастся на вкладке Имя компьютера (Network Identification) диалогового окна свойств системы.

- Дописывать **родительские** суффиксы **осн. DNS-суффикса (Append** parent: suffixes of the primary DNS suffix) — этот флажок применяется для разрешения неполных доменных имен в иерархии «родительский — дочерний». Если имя не удается разрешить в данном домене, к нему добавляется суффикс родительского домена. Так продолжается, пока не будет достигнута вершина иерархии. Например, если компьютер Rage расположен в домене *dev.microsoft.com* служба DNS сначала попытается разрешить имя *rage.dev.microsoft.com,* а в случае неудачи — *rage.microsoft.com.*
- Дописывать **следующие DNS-суффиксы (по порядку)** [Append These DNS Suffixes (In **Order)]** — этот переключатель позволяет задать суффиксы DNS для применения при разрешении имен вместо суффикса родительского домена. Кнопки Добавить (Add), Удалить (Remove) и Изменить (Edit) позволяют, соответственно, добавить, удалить и редактировать суффиксы. Для разрешения имен можно использовать несколько суффиксов, при этом их приоритет определяется порядком следования в списке. Если запрос разрешения имени не выполняется с применением первого суффикса, используется второй и т. д. Кнопки со стрелками позволяют изменить положение суффикса в списке.
- **DNS-суффикс подключения (DNS suffix for this connection)** - суффикс DNS, указанный в этом поле, перекрывает доменные имена, которые дописываются, если установлены параметры, описанные ранее. Обычно здесь используется доменное имя, заданное на вкладке Имя компьютера (Network Identification) диалогового окна свойств системы.
- **Зарегистрировать адреса этого подключения в DNS (Register this connection's addresses** in **DNS)** — этот флажок позволяет зарегистрировать в DNS все IP-адреса данного соединения под полным доменным именем компьютера.
- **Использовать DNS-суффикс подключения при регистрации в DNS (Use** this **connection's DNS suffix in DNS registration) — этот**

флажок позволяет зарегистрировать в DNS все IP-адреса данного соединения под именем родительского домена.

Настройка WINS

Служба WINS преобразует имена компьютеров NetBIOS в IP-адреса и помогает компьютерам определять адреса других компьютеров в сети. Для работы службы в сети нужно установить сервер WINS. Службу WINS поддерживают все предыдущие версии Windows, поэтому в Windows Server 2003 она оставлена по соображениям совместимости.

Для разрешения имен NetBIOS в ОС Windows Server 2003 также используется локальный файл LMHOSTS. Он применяется, когда обычные методы разрешения имен не срабатывают. В грамотно настроенной сети эти файлы практически не нужны. Так что основным методом разрешения имен NetBIOS является служба WINS.

Служба WINS настраивается так.

1. Откройте диалоговое окно Дополнительные параметры TCP/IP (Advanced TCP/IP Settings) и перейдите на вкладку WINS (рис. 16-6),

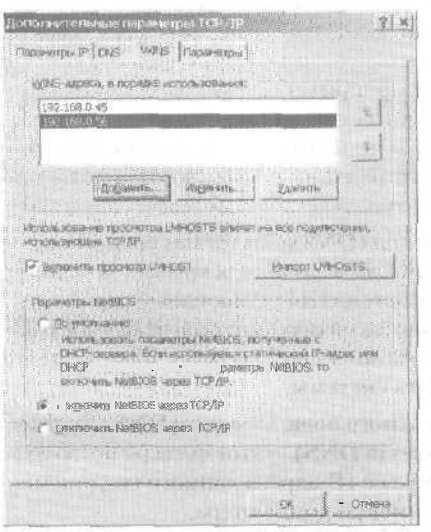


Рис. 16-6. Вкладка WINS диалогового окна Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)

2. В списке WINS-адреса, в порядке использования (WINS addresses, in order of use) перечислены IP-адреса серверов WINS, применяемых для разрешения имен NetBIOS. Кнопки Добавить (Add), Удалить (Remove) и Изменить (Edit) позволяют добавлять, удалять и редактировать эти адреса соответственно.
3. Вы вправе использовать для разрешения имен NetBIOS несколько серверов WINS, при этом их приоритет определяется положением в списке. Если первому серверу WINS не удается ответить на запрос разрешения имени NetBIOS, запрос посылается на второй и т. д. Помните, что TCP/IP отправляет запрос на следующий сервер, только если предыдущий не отвечает, но не из-за того, что тот не смог разрешить указанное имя. Чтобы изменить положение сервера в списке, воспользуйтесь кнопками со стрелками.
4. Чтобы включить поиск по файлу LMHOSTS, установите флажок Включить просмотр LMHOSTS (Enable LMHOSTS lookup). Чтобы компьютер использовал файл LMHOSTS, расположенный на определенном компьютере сети, укажите его с помощью кнопки Импорт LMHOSTS (Import LMHOSTS).

Совет Файлы LMHOSTS поддерживаются на каждом компьютере индивидуально и поэтому ненадежны. Не полагайтесь на них — лучше обеспечьте работоспособность и доступность серверов DNS и WINS.

5. Для разрешения имен WINS требуются службы NetBIOS через TCP/IP (NetBIOS Over TCP/IP). Чтобы настроить разрешение имен WINS с помощью NetBIOS, выберите один из следующих переключателей:
   - при использовании службы DHCP и динамической адресации удобно загружать параметры NetBIOS с DHCP-сервера. Для этого достаточно установить переключатель По умолчанию (Default);
   - при использовании статической IP-адресации или в случае, если DHCP-сервер не передает параметры NetBIOS, установите переключатель Включить NetBIOS через TCP/IP (Enable NetBIOS Over TCP/IP);
   - если WINS и NetBIOS в сети не используются, установите переключатель Отключить NetBIOS через TCP/IP

(Disable NetBIOS Over TCP/IP). В этом случае широковещательные рассылки NetBIOS отключаются.

6. Повторите эту процедуру для других сетевых плат.

Настройка дополнительных сетевых компонентов

В Windows Server 2003 предусмотрено множество дополнительных сетевых клиентов, служб и протоколов. Для их установки предназначены диалоговое окно свойств сетевого подключения и Мастер дополнительных сетевых компонентов Windows (Windows Optional Networking Components Wizard).

Установка и удаление сетевых компонентов

Для установки сетевых клиентов, служб и протоколов, перечисленных в табл. 16-2. предназначено диалоговое окно свойств сетевого подключения.

Таблица 16-2. Сетевые компоненты Windows Server 2003

Компонент	Описание
Microsoft TCP/IP версия 6 (Microsoft TCP/IP V6)	Предоставляет протоколы сетевого уровня, поддерживающие IP версии 6 (IPv6). Обеспечивает 128-разрядное адресное пространство. Прежде чем устанавливать и использовать IPv6, хорошо изучите этот протокол
NWLink IPX/SPX/ NetBIOS-совместимый транспортный протокол (NWLink IPX/SPX/ NetBIOS Compatible Transport Protocol)	Позволяет компьютеру устанавливать связь с серверами NetWare но протоколу IPX/SPX
Драйвер сетевого монитора (Network Monitor Driver)	Позволяет сетевому монитору анализировать пакеты. передаваемые по сети
Клиент для сетей Microsoft (Client for Microsoft Networks)	Позволяет компьютеру работать с ресурсами сетей Windows
Клиент для сетей NetWare (Client Services for NetWare)	Позволяет компьютеру работать с ресурсами сетей NetWare
Надежный многоадресный протокол (Reliable Multicast Protocol)	Позволяет настроить компьютер для групповых широковещательных рассылок

Таблица 16-2. Сетевые компоненты Windows Server 2003 *(окончание)*

Компонент	Описание
Планировщик пакетов QoS (QoS Packet Scheduler)	Обеспечивает работу служб управления сетевым трафиком
Протокол AppleTalk(AppleTalk Protocol)	Позволяет другим узлам взаимодействовать с данным компьютерам но протоколу AppleTalk. Сервер Windows Server 2003 благодаря этому протоколу может функционировать как маршрутизатор AppleTalk
Протокол объявлений служб (Service Advertising Protocol)	Позволяет «рекламировать» серверы и адреса в сети. Этот протокол используют для поиска серверов и служб серверы Netware, работающие с протоколом IPX/SPX
Служба доступа к файлам и принтерам сетей Microsoft (File and Printer Sharing for Microsoft Networks)	Позволяет другим узлам работать с ресурсами данного компьютера

Любой из перечисленных в таблице компонентов можно установить или удалить.

1. В окне Панели управления (Control Panel) щелкните дважды значок Сетевые подключения (Network Connections), а затем дважды щелкните нужное сетевое соединение.
2. Щелкните кнопку Свойства (Properties).
3. Откроется диалоговое окно свойств подключения со списком установленных компонентов.
   - Чтобы **отключить** компонент, сбросьте связанный с ним флажок.
   - Чтобы удалить компонент, выделите его и щелкните кнопку Удалить (Uninstall). Щелкните кнопку Да (Yes), чтобы подтвердить удаление.
   - Чтобы установить компонент, щелкните кнопку Установить (Install). Откроется диалоговое окно Выбор типа сетевого компонента (Select Network Component Type). Выберите тип компонента (клиент, протокол или служба) и щелкните кнопку Добавить (Add). Укажите нужный компонент.

Установка необязательных сетевых компонентов

Для установки необязательных сетевых компонентов предназначен Мастер дополнительных сетевых компонентов Windows (Windows Optional Networking Components Wizard). Для обеспечения работы этих компонентов иногда приходится устанавливать дополнительные утилиты.

Необязательные сетевые компоненты перечислены в табл. 16-3. В первом столбце указано имя, под которым пакет значится в окне Компоненты Windows (Windows Components). Чтобы просмотреть список отдельных компонентов, щелкните кнопку Состав (Details).

Таблица 16-3. Необязательные сетевые компоненты Windows Server 2003

Компонент	Название отдельного компонента	Описание
Средства управления и наблюдения (Management and Monitoring Tools)	Пакет администрирования диспетчера подключений (Manager Administration Kit)	Инструмент для создания пользовательских соединений удаленного доступа, которые рассылаются пользователям
	Службы точек подключений (Connection Point Services)	Служба Телефонная книга (Phone Book), позволяющая рассылать телефонные книги
	Средства сетевого монитора (Network Monitor Tools)	Инструменты сетевого монитора для анализа сетевого трафика
	Протокол SNMP [Simple Network Management Protocol (SNMP)]	Установка SNMP и агентов SNMP
	WMI поставщик SNMP (WMI SNMP Provider), Поставщик установщика Windows через WMI (WMI Windows Installer Provider)	Компоненты для доступа инструментарию управления Windows (Windows Management Instrumentation, WMI)
Сетевые службы (Networking Services)	DNS	Позволяет настроить компьютер в качестве DNS-сервера

Таблица 16-3. Необязательные сетевые компоненты Windows Server 2003 *(окончание)*

Компонент	Название отдельного компонента	Описание
	DHCP	Позволяет настроить компьютер в качестве DHCP-сервера
	Служба проверки подлинности в Интернете (Internet Authentication Service)	Обеспечивает аутентификацию, авторизацию и ведение учета пользователей удаленного доступа и виртуальных частных сетей
	RPC через HTTP-прокси (RPC Over HTTP Proxy)	Позволяет передавать распределенные COM-объекты с помощью протокола HTTP
	Простые службы TCP/IP (Simple TCP/IP Services)	Базовые службы TCP/IP
	WINS	Позволяет настроить компьютер в качестве WINS-сервера
Другие службы доступа к файлам и принтерам в сети (Other Network File and Print Services)	Файловые службы Macintosh (File Services for Macintosh)	Позволяют пользователям Macintosh работать с файлами, размещенными на сервере Windows Server 2003
	Службы печати для Macintosh (Print Services for Macintosh)	Позволяют пользователям Macintosh посылать задания на печать на принтер, размещенный на сервере Windows Server 2003
	Службы печати для Unix (Print Services for Unix)	Позволяют пользователям Unix посылать задания на печать на принтер, размещенный на сервере Windows Server 2003

Необязательные сетевые компоненты устанавливают так.

1. В Панели управления (Control Panel) выберите или дважды щелкните команду Установка и удаление программ (Add or Remove Programs).
2. Перейдите на вкладку Установка компонентов Windows (Add/Remove Windows Components). Запустится Мастер компонен-

тов Windows (Windows Components Wizard), окно которого показано на рис. 16-7. Щелкните Далее (Next).

3. В открывшемся диалоговом окне выделите нужный пакет и щелкните кнопку Состав (Details).
4. Установите флажки у нужных компонентов и щелкните OK.
5. Щелкните Далее (Next). Выбранные компоненты будут установлены.

Рис. 16-7. Выделите нужный пакет компонентов и щелкните кнопку Состав (Details)

Управление сетевыми подключениями

Этот раздел посвящен созданию сетевых подключений и управлению ими. Помните, что подключения по локальной сети создаются автоматически при загрузке компьютера, подключенного к сети, поэтому этот тип соединений вручную создавать не нужно.

Создание сетевого подключения

Windows Server 2003 позволяет настроить большое количество различных удаленных и сетевых соединений. Вот что для этого следует сделать.

1. В Панели управления (Control Panel) выберите команду Сетевые подключения (Network Connections), а затем щелкните Мастер новых подключений (New Connection Wizard).
2. Щелкните Далее (Next) и выберите нужный тип соединения (рис. 16-8):

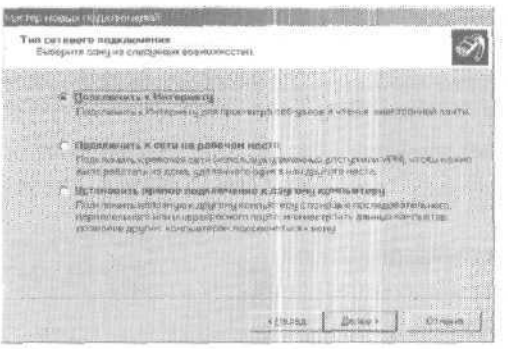


Рис. 16-8. Типы соединений

- **Подключить к Интернету (Connect to the Internet)** — позволяет организовать доступ в Интернет, например посредством телефонной линии. После подключения к поставщику услуг Интернета соединение можно сделать общим для других компьютеров;
- **Подключить к сети на рабочем месте (Connect to the network at my workplace)** — позволяет организовать соединение с корпоративной сетью через Интернет. Соединение может быть осуществлено посредством стандартного телефонного доступа или VPN-соединения;
- Установить прямое подключение к другому компьютеру (Set up an advanced connection) - позволяет организовать прямое соединение с другим компьютером через последовательный, параллельный или инфракрасный порт. Попутно настраивается доступ к компьютеру через входящие соединения посредством служб удаленного доступа. Если компьютер поддерживает VPN, прямые или коммутируемые соединения, необходимо также настроить поддержку входящих соединений.

3. Дальнейшие действия зависят от выбранного типа соединения. Выполните инструкции в окнах мастера и щелкните Готово (Finish).

Безопасность удаленных соединений

Иногда необходимо настроить сервер так. чтобы он получил доступ к сетям филиалов или других удаленных площадок. При этом необходимо обеспечить должную защиту аутентификаци-

онной информации, передаваемой в удаленную сеть, а значит, предусмотреть передачу пароля и других важных сведений в зашифрованном виде с использованием методики общего ключа или какой-либо другой. Есть три способа проверки регистрационной информации:

- незашифрованный пароль передается через подключение в виде простого текста;
- зашифрованный пароль передается через подключение с помощью какой-либо безопасной технологии, например Проверки подлинности Windows (Windows Authentication);
- вход в систему осуществляется посредством смарт-карты.

В случае коммутируемого и широкополосного соединения можно использовать любой из перечисленных вариантов. В случае VPN-соединения допустимы только защищенные методы. В двух последних случаях вы вправе задать обязательное шифрование данных. Если шифрование данных не выполняется, соединение автоматически разрывается. Этот вариант позволяет защитить данные, передаваемые через удаленное соединение.

Чтобы настроить защищенное удаленное соединение, выполните следующие действия.

1. В окне Панели управления (Control Panel) щелкните дважды значок Сетевые подключения (Network Connections). Щелкните правой кнопкой нужное подключение и выберите Свойства (Properties). Откроется диалоговое окно свойств подключения.
2. Перейдите на вкладку Безопасность (Security).
3. В области Параметры безопасности (Security Options) укажите стандартный вариант или настройте дополнительный вариант проверки подлинности. К первым относятся: Небезопасный пароль (Allow Unsecured Password), Безопасный пароль (Require Secure Password) и Смарт-карта (Use Smart Card).
4. При выборе безопасного пароля вы вправе задать автоматическое использование в данном подключении того же имени пользователя и пароля, что применяется для входа в Windows. Здесь же задается обязательное шифрование регистрационной информации. Помните, что обе этих возможности должны поддерживаться удаленным компьютером. Если это не так, проверка регистрационной информации окажется невозможной и соединение не будет установлено.

Проверка статуса, скорости и активности подключения

Чтобы проверить статус локального соединения, в окне Панели управления (Control Panel) щелкните дважды значок Сетевые подключения (Network Connections), затем щелкните правой кнопкой нужное подключение и выберите Состояние (Status). На вкладке Общие (General) открывшегося диалогового окна содержится следующая информация (рис. 16-9):

- **Состояние (Status)** — как правило, в этом поле всегда отображается Подключено (Connected), так как при изменении состояния ОС просто закрывает это диалоговое окно;
- **Длительность (Duration)** — продолжительность соединения;
- Скорость (Speed) — скорость обмена данными, например 10 Мбит/с или 100 Мбит/с для локальных сетей;
- **Пакетов (Packets)** — число пакетов TCP/IP, переданных через соединение.

Рис. 16-9. Сводная информация о подключении

Просмотр параметров сети

Windows Server 2003 предоставляет несколько способов доступа к текущим параметрам сетевых плат. Чтобы посмотреть их с помощью диалогового окна состояния, выполните следующие действия.

1. В окне Панели управления (Control Panel) щелкните дважды значок Сетевые подключения (Network Connections), затем щелкните правой кнопкой нужное подключение и выберите Состояние (Status).

2. Перейдите на вкладку Поддержка (Support), показанную на рис. 16-10. Здесь указаны тип адреса (настроенный вручную, динамический и пр.), IP-адрес сетевого интерфейса, маска подсети и адрес шлюза по умолчанию.

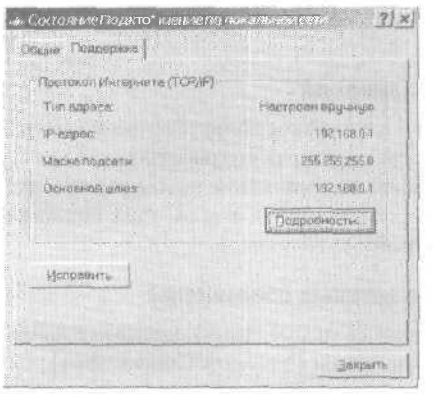


Рис. 16-10. Текущие параметры сетевого подключения

3. Чтобы получить более детальную информацию, щелкните кнопку Подробности (Details). Откроется диалоговое окно Детали сетевого подключения (Network Connection Details), в котором содержится следующая информация:
   - **Физический адрес (Physical Address)** — аппаратный адрес сетевой платы;
   - **DHCP-сервер (DHCP Server)** - IP-адрес DHCP-сервера, от которого получена текущая аренда;
   - **DNS-серверы (DNS Servers)** — IP-адреса DNS-серверов;
   - **Основной WINS-сервер (Primary WINS Server)** — IP-адрес главного WINS-сервера;
   - **Дополнительный WINS-сервер (Secondary WINS Server)** — IP-адрес дополнительного WINS-сервера;
   - **Аренда получена (Lease Obtained)** — дата и время получения аренды DHCP;
   - **Аренда истекает (Lease Expires)** — дата и время истечения аренды DHCP.

Для просмотра параметров сети вы вправе также воспользоваться утилитой Ipconfig, работающей в режиме командной строки.

1. В меню Пуск (Start) выберите команду Выполнить (Run), Введите **cmd** и щелкните OK. Откроется окно командной строки.
2. В окне командной строки введите **ipconfig /all,** чтобы просмотреть подробную информацию о настройке всех сетевых плат компьютера.

Копирование сетевых соединений

Если вам предстоит внести в параметры подключения критические изменения, которые могут нарушить его работоспособность, предварительно создайте копию подключения: щелкните его правой кнопкой и выберите Создать копию (Create Copy). Подключения по локальной сети копировать нельзя.

Включение и отключение сетевых соединений

1. В окне Панели управления (Control Panel) щелкните дважды значок Сетевые подключения (Network Connections).
2. Чтобы отключить соединение, щелкните его правой кнопкой и выберите Отключить (Disconnect) или Запретить (Disable).
3. Чтобы включить соединение, щелкните его правой кнопкой и выберите команду Подключить (Connect) или Разрешить (Enable).

Удаление сетевых соединений

1. В окне Панели управления (Control Panel) щелкните дважды значок Сетевые подключения (Network Connections).
2. Щелкните правой кнопкой соединение, которое хотите удалить, и выберите Удалить (Delete). Щелкните кнопку Да (Yes), чтобы подтвердить удаление.

Примечание Подключение по локальной сети удалить нельзя.

Переименование сетевых соединений

Windows Server 2003 присваивает подключениям имена при их создании. Чтобы переименовать соединение, щелкните его правой кнопкой, выберите Переименовать (Rename) и введите новое имя. Если на компьютере организовано несколько подключений, желательно давать им понятные имена, чтобы их проще было различать.

Восстановление сетевых соединений

Неполадки в работе подключения возникают при отсоединении сетевого кабеля или при неисправности сетевой платы. Обычно после подключения кабеля и устранения проблем с платой соединение восстанавливается автоматически. Если этого не произошло, щелкните *подключение правой кнопкой* и выберите *Исправить* (Repair). Если и это не помогло, вам придется выполнить диагностику и тестирование. Как это сделать, описано в следующем разделе.

Диагностика и тестирование параметров сети

В Windows Server 2003 предусмотрено много средств для поиска неполадок и проверки соединений TCP/IP. В этом разделе рассматривается несколько основных проверок, которые следует выполнять каждый раз, когда вы устанавливаете или изменяете параметры сетевой настройки компьютера. Затем анализируются методики проведения более детального поиска неполадок.

Простейшее тестирование сети

После изменения сетевых параметров работу подключения необходимо протестировать. Проще всего проверить работоспособность TCP/IP с помощью команды Ping. Синтаксис ее таков:

```
ping узел
```

где *узел* — имя узла.

Посредством утилиты Ping сеть можно проверить несколькими способами:

- **попытаться обратиться к компьютеру по его IP-адресу** — если компьютер настроен правильно и нужный узел доступен, на запрос утилиты Ping должен придти ответ;
- **в доменах, поддерживающих службу WINS, попытаться обратиться к компьютеру по его NetBIOS-имени** — если имена NetBIOS разрешаются правильно, служба WINS настроена должным образом;
- **в доменах, поддерживающих службу DNS, попытаться обратиться к компьютеру по его DNS-имени** — если имена узлов DNS разрешаются правильно, служба DNS настроена должным образом.

Проверьте также средства Windows для просмотра сети (для этого компьютер должен быть членом домена Windows Server 2003, в котором разрешен поиск компьютеров). Войдите в систему, откройте Проводник (Windows Explorer) или папку Сетевое окружение (My Network Places) и попробуйте найти другие компьютеры домена. После этого войдите в другой компьютер и попытайтесь найти тот, который только что настроили. Если эти тесты выполняются, разрешение имен DNS в локальной сети настроено правильно. В противном случае проверьте параметры DNS и протоколов.

Освобождение и обновление аренды DHCP

DHCP-серверы способны автоматически назначать многие сетевые параметры, в том числе IP-адреса, шлюзы по умолчанию, основные и дополнительные DNS-серверы, основные и дополнительные WINS-серверы и т. д. Все эти параметры сдаются компьютеру в аренду, которая действительна *в* течение ограниченного периода времени и *должна* периодически **обновляться.** Чтобы обновить аренду, компьютер обращается к DHCP-серверу, предоставившему аренду. Если этот сервер доступен, то аренда обновляется и отсчет срока аренды начинается заново. При необходимости вы вправе обновить аренду вручную.

При назначении аренды и и процессе обновления могут возникнуть проблемы, препятствующие сетевому обмену. Если сервер недоступен вплоть до окончания срока аренды, IP-адрес становится недействительным. В этом случае компьютеру присваивается альтернативный IP-адрес, параметры которого в большинстве случаев не позволяют нормально работать в сети. Чтобы устранить проблему, следует освободить и обновить аренду DHCP

Другая проблема возникает при переносе компьютера из одного офиса в другой или из одной подсети в другую. При использовании параметров, полученных от «чужого» DHCP-сервсра, компьютер иногда начинает работать медленно или некорректно. В этом случае аренду DHCP также необходимо освободить и обновить.

Вот как освободить и обновить аренду с помощью утилиты Ipconfig.

1. В меню Пуск (Start) выберите команду Выполнить (Run). В поле Открыть (Open) введите **cmd** и щелкните OK. Откроется окно командной строки.

2. Чтобы освободить аренду, введите **ipconfig** /release.
3. **Чтобы обновить аренду, введите ipconfig /renew.**
4. Чтобы проверить обновленные параметры, введите ipconfig /all.

Регистрация и очистка DNS

В кэше DNS хранится история запросов DNS, выполненных в ходе доступа пользователя к сетевым ресурсам по протоколу TCP/IP. Этот кэш содержит прямые просмотры (разрешение имени хоста в IP-адрес) и обратные просмотры (разрешение IP-адреса в имя хоста). Если запись о некотором хосте занесена в кэш, компьютеру больше не требуется обращаться к внешним серверам для получения DNS-информации об этом хосте. DNS-запросы разрешаются на месте.

Время хранения записи в кэше зависит от значения параметра TTL, присвоенного записи сервером-источником. Чтобы просмотреть текущие записи и присвоенные им значения TTL, введите в командной строке ipconfig **/displaydns**. Время жизни записи измеряется в секундах. Локальный компьютер постоянно ведет его обратный отсчет. Когда значение TTL становится равным пулю, запись автоматически удаляется из кэша.

Иногда требуется вручную очистить кэш, чтобы удалить старые записи и дать компьютеру возможность обновить DNS-записи раньше, чем истечет заданный срок. Обычно это необходимо после изменения IP-адресов в сети, когда текущие записи в кэше оказываются устаревшими.

Совет Уменьшайте величину TTL для записей DNS за несколько недель до запланированного изменения IP-адресов. Обычно время жизни записей нужно сокращать с нескольких дней до нескольких часов, чтобы обеспечить скорейшее распространение изменений на все компьютеры. После внесения изменений восстановите исходное значение TTL, чтобы сократить число запросов на обновление.

В большинстве случаев для решения проблем с кэшем DNS нужно либо очистить его, либо перерегистрировать DNS. При очистке из кэша удаляются все DNS-записи, и их создание начинается заново. Перерегистрация означает, что Windows Server 2003 обновляет все текущие аренды DHCP, а затем проверяет все DNS-записи в кэше. Как правило, предпочтитель-

нес полностью очистить кэш и дать возможность компьютеру постепенно выполнить необходимые просмотры. Перерегистрацию DNS следует проводить только в том случае, если вы подозреваете, что проблемы связаны с DHCP и кэшем DNS.

Чтобы очистить или перерегистрировать записи DNS с помощью Ipconfig, выполните следующие действия.

1. В меню Пуск (Start) выберите команду Выполнить (Run). В поле Открыть (Open) введите **cmd** и щелкните OK. Откроется окно командной строки.
2. Чтобы очистить кэш. введите **ipconfig /flushdns**.
3. Чтобы обновить аренду DHCP и повторно зарегистрировать записи, введите **ipconfig /registerdns**.
4. Чтобы проверить результат операции, введите в командной строке ipconfig **/displaydns**.

Детальная диагностика сетевых неполадок

Одна из наиболее сложных задач — поиск сетевых неполадок. Между службами, протоколами и параметрами существует множество взаимосвязей, поэтому локализация проблемы зачастую крайне нелегка. К счастью, Windows Server 2003 содержит мощный инструментарий для диагностики сетевых неполадок связанных с:

- общими проблемами сетевых соединений;
- параметрами службИнтернета дляэлектронной почты, групп новостей и прокси-серверов;
- параметрами модемов, сетевыхклиентов и сетевых плат;
- параметрами DNS, DHCP и WINS;
- шлюзами по умолчанию и IP-адресами.

Чтобы провести диагностику с параметрами по умолчанию, выполните следующие действия.

1. Щелкните Пуск (Start) и выберите Справка и поддержка (Help and Support). Откроется Центр справки и поддержки (Help and Support Center).
2. В разделе Задачи поддержки (Support Tasks) щелкните Служебные программы (Tools). Затем в левой панели разверните узел Средства центра справки и поддержки (Help and Support Center Tools) и щелкните Диагностика сети (Network Diagnostics).

3. Щелкните Собрать информацию (Scan Your System), чтобы начать проверку.

Во время проверки на экран выводится индикатор выполнения проверки. В состав тестов по умолчанию входят тесты ping для проверки доступа к сети, тесты соединения через настроенные модемы и сетевые платы, а также проверки служб электронной почты, трупп новостей и прокси. Кроме того, после проверок выдается информация о конфигурации компьютера и ОС.

По завершении проверки ее результаты отображаются на экране (рис. 16-11). При анализе результатов обратите внимание на пункты, отмеченные Не задан (Not Configured) или Тест не пройден (Failed). Щелкните знак «плюс» (+) слева от записи, чтобы вывести подробную диагностическую информацию.

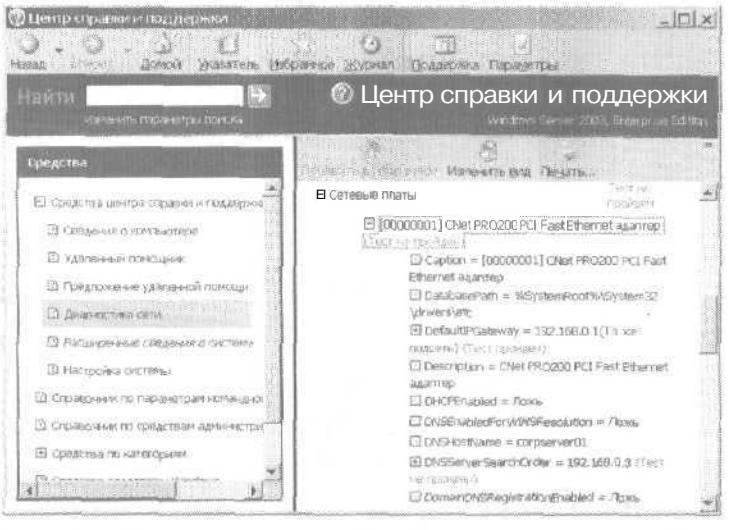


Рис. 16-11. Использование сетевой диагностики для локализации неполадок в параметрах сети

Продолжайте просмотр информации, пока не найдете проблемный участок. Например, в моей тестовой системе был неправильно настроен адрес DNS-сервера. Проверка показала, что проблема связана с главной сетевой платой. Раскрыв запись для сетевой платы, я обнаружил, что в качестве ошибочного отмечено поле DNSServerSearchOrder. Поняв, что ком-

пьютер не может отправлять пакеты DNS-серверу, я легко нашел причину затруднений. После обновления параметров настройки на DHCP-сервере и обновления аренды DHCP компьютер получил возможность правильно разрешать DNS.

Чтобы провести более детальное тестирование, щелкните Настроить параметры сбора информации (Set Scanning Options) и выберите дополнительные тесты. Затем вновь запустите диагностические тесты.

Глава 17

Управление сетевыми принтерами

Чтобы предоставить удаленным пользователям доступ к печатающему устройству, подключенному к компьютеру с Microsoft Windows Server 2003, администратор должен сделать компьютер сервером печати и настроить его для совместного использования печатающих устройств в сети.

Эта глава посвящена настройке, предоставлению доступа, администрированию и устранению неполадок, связанных с работой общих принтеров. В главе не рассматривается печать через Интернет.

Устранение неполадок в работе принтера

Знание принципов работы принтера сэкономит вам часы, которые потребуются для устранения неполадок в его работе. При печати документа взаимодействуют многочисленные процессы, драйверы и аппаратные устройства. Если принтер подключен к серверу печати, в процессе печати задействованы следующие компоненты.

- Драйвер принтера (printer driver). Когда документ посылается на печать, загружается драйвер принтера. Загрузка производится с локального или удаленного компьютера в зависимости от того, куда подключено печатающее устройство. Доступность драйвера принтера на удаленном компьютере зависит от ОС и архитектуры процессора. Если компьютеру не удается получить последнюю версию драйвера принтера, это, возможно, связано с тем, что администратор не включил драйвер для данной ОС. Подробнее — в разделе «Управление драйверами принтеров».
- **Локальный спулер печати (local print spool) и обработчик печати (print processor).** Приложение, отправляющее документ

па печать, использует драйвер принтера для преобразования документа в формат, понятный печатающему устройству. Затем компьютер отправляет документ в локальный спулер печати, который в свою очередь передает его обработчику, который уже непосредственно подготавливает данные для печати.

- Маршрутизатор (rooter) и спулер печати на сервере печати. Подготовленные данные передаются обратно в локальный спулер. Если печать выполняется на удаленном устройстве, данные направляются маршрутизатором в спулер на сервере печати. В Windows Server 2003 маршрутизатором печати является программа WINSPOOL.EXE, в задачи которой входит поиск удаленного принтера, управление заданиями печати и загрузка драйверов принтера. Обычно в невыполнении любой из этих задач виноват именно маршрутизатор. Об исправлении неполадок, связанных с его работой, написано в разделах «Решение проблем с очередью печати» и «Настройка разрешений доступа к принтерам». Если предложенные в них способы не помогут, попробуйте заменить или восстановить файл WINSPOOL.EXE.
- Принтер (очередь печати). Из спулера печати документ попадает в *стек* (stack), или *очередь* (queue), печатающего устройства. Документ, помещенный в очередь на печать, называют *заданием печати* (print job). Время пребывания документа в очереди на печать зависит от его приоритета и позиции. Подробнее — в разделе «Настройка времени и приоритета заданий печати».
- Монитор печати (print monitor). Когда подходит очередь печати документа, монитор печати отправляет его на печатающее устройство.

  Монитор принтера, используемый ОС Windows Server 2003, зависит от конфигурации и типа печатающего устройства. По умолчанию им является файл LOCALMON.DLL. Производители печатающих устройств часто разрабатывают собственные мониторы печати, например HPMON.DLL, применяемый устройствами компании Hewlett-Packard.
- **Печатающее** устройство **(print device).** Печатающим называют устройство, предназначенное для печати документа на бумаге.

Примечание Основной смысл загрузки драйверов с удаленного компьютера состоит в том, что при обновлении драйвера принтера вам не нужно устанавливать новую версию на всех компьютерах сети — достаточно заменить драйвер только на сервере печати. Подробнее — в разделе «Управление драйверами принтеров».

Право установки и управления принтерами определяется групповой политикой. Если у вас возникают проблемы при работе с принтером и вы полагаете, что они связаны с групповой политикой, проверьте ее настройку в следующих узлах:

- Конфигурация компьютера\Административные шаблоны\Принтеры (Computer Configuration\Administrative Templates\Printers);
- Конфигурация пользователя\Административные шаблоны\Панель управления\Принтеры (User Configuration\Administrative Templates\Control Panel\Printers);
- Конфигурация пользователя\Административные шаблоны\Панель задач и меню «Пуск» (User Configuration\Administrative Templates\Start Menu and Taskbar).

Установка принтеров

Windows Server 2003 позволяет устанавливать принтеры и управлять ими из любой точки сети. Для установки и обслуживания принтеров служит папка Принтеры и факсы (Printers and Faxes), Чтобы открыть ее на локальном компьютере, выберите команду Принтеры и факсы (Printers and Faxes) в меню Пуск (Start) или в Панели управления (Control Panel). На удален ном компьютере доступ к этой папке можно получить через папку Сетевое окружение (My Network Places): войдите в домен, выберите нужный компьютер и дважды щелкните значок Принтеры (Printers),

Локальные и сетевые принтеры

Все печатающие устройства, подключенные к сети, делятся на два типа:

- локальные (local) подключены непосредственно к компьютеру, к ним имеет доступ только тот пользователь, который па нем работает;

- **сетевые (network)** — эти печатающие устройства доступны с удаленного компьютера; сетевое печатающее устройство можно подключить к серверу печати или непосредственно к сети через собственную сетевую плату.

Примечание Ключевое различие между локальным и сетевым принтерами состоит в том, что локальный принтер не является общим ресурсом. О том, как сделать локальный принтер сетевым, написано в разделе «Открытие и закрытие доступа к принтеру».

Сетевой принтер устанавливается как компонент сервера печати или как самостоятельное устройство, подключенное к сети. *Сервер печати* (print server) — это сервер или рабочая станция, обеспечивающие совместное использование одного или нескольких принтеров, подключенных к компьютеру или сети.

Сервером печати может быть любая система с Windows Server 2003. Его основная задача — управление общими печатающими устройствами и очередью печати. Основное преимущество серверов печати заключается в централизованном управлении очередью печати и отсутствии необходимости устанавливать драйверы принтера на компьютерах клиентов.

Однако использовать сервер печати не обязательно. Пользователи могут работать с принтерами, подключенными к сети напрямую. При этом работа с сетевым принтером во многом напоминает работу с локальным. Единственное отличие в том, что доступ к принтеру могут получить несколько пользователей, у каждого из которых будет своя очередь печати. Каждая очередь печати обслуживается отдельно, в результате чего иногда возникают трудности при администрировании и устранении неполадок.

Чтобы установить или настроить новый принтер, нужно быть членом групп Администраторы (Administrators), Операторы печати (Print Operators), Операторы сервера (Server Operators). Чтобы подключиться и напечатать документ на принтере, необходимы соответствующие разрешения доступа. Подробнее — в разделе «Настройка разрешений доступа к принтерам».

Установка физически подключенного печатающего устройства

Физическое подключение означает, что устройство печати подсоединено к компьютеру через последовательный порт, парал-

лельный порт, шину USB или ИК-порт. Физически подключенные принтеры можно конфигурировать как локальные или сетевые печатные устройства. Ключевое различие в том, что локальное устройство доступно только пользователям, зарегистрировавшимся на компьютере, а сетевое устройство доступно всем пользователям сети. Помните, что рабочая станция или сервер, в который вы вошли, становится сервером печати для устройства, которое вы конфигурируете.

Чтобы установить физически подключенное печатное устройство, зарегистрируйтесь локально на сервере печати, который вы хотите настроить, или воспользуйтесь удаленным соединением через папку Сетевое окружение (My Network Places). Если вы настраиваете локальный принтер Plug and Play, зарегистрировавшись на сервере печати, установка займет пару секунд. Чтобы установить устройство печати, выполните следующие действия.

1. Подсоедините устройство к серверу с помощью последовательного, параллельного или USB-кабеля и включите его.
2. Если ОС обнаружит печатающее устройство, установка необходимого драйвера начнется автоматически. Если драйвер не будет найден, ОС предложит вставить установочный компакт-диск Windows Server 2003 или дискету. Если системе не удалось обнаружить печатающее устройство автоматически, вам придется установить его вручную, как описано далее.
3. Windows Server 2003 автоматически делает принтер общим сетевым ресурсом, используя в качестве имени первые 8 символов имени принтера, удаляя пробелы. Например, общим именем принтера HP DeskJet 890C будет HPDeskJe. Чтобы изменить сетевое имя принтера, щелкните правой кнопкой мыши его значок в папке Принтеры и факсы (Printers and Faxes) и выберите Общий доступ (Sharing). Затем в поле Сетевое имя (Share Name) введите новое имя принтера.

Для установки устройства, которое не было обнаружено Windows автоматически, или удаленного устройства печати выполните следующие действия.

1. Откройте папку Принтеры и факсы (Printers and Faxes) на компьютере, который хотите сделать сервером печати.
   - На локальной системе выберите **Принтеры** и факсы (Printers and Faxes) в меню Пуск (Start) или в Панели управления (Control Panel).

- С помощью папки Сетевое окружение (My Network Places) найдите компьютер, параметры принтера которого хотите настроить, и затем выберите Принтеры и факсы (Printers and Faxes).

2. Щелкните дважды значок Установка принтера (Add Printer), чтобы запустить Мастер установки принтеров (Add Printer Wizard). Щелкните Далее (Next).
3. При установке локального принтера вы увидите окно, изображенное на рис. 17-1. Выберите Локальный принтер (Local printer attached to this computer), сбросьте флажок Автоматическое определение и установка принтера «Plug and Play» (Automatically detect and install my Plug and Play printer) и щелкните Далее (Next).

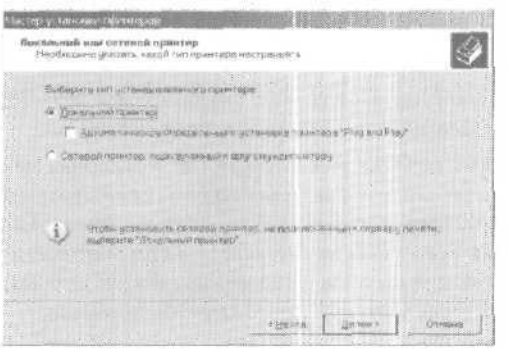


Рис. 17-1. Чтобы установить локальное печатающее устройство, установите переключатель Локальный принтер (Local printer attached to this computer)

4. При установке удаленного принтера Мастер установки принтеров (Add Printer Wizard) сразу переходит к окну Выберите порт принтера (Select a Printer Port). Установите переключатель Использовать порт (Use the following port) и выберите в списке соответствующий LPT-, COM- или ИК-порт или задайте печать в файл. В последнем случае Windows Server 2003 будет запрашивать имя файла при каждой попытке печати. Щелкните Далее (Next).
5. Выберите изготовителя и модель печатающего устройства (рис. 17-2). Если в списке нет нужного принтера, щелкните Установить с диска (Have Disk) и воспользуйтесь установочным диском из комплекта принтера.

Совет Если драйвер для вашей модели принтера найти не удалось, попробуйте воспользоваться универсальным драйвером или драйвером похожего печатающего устройства.

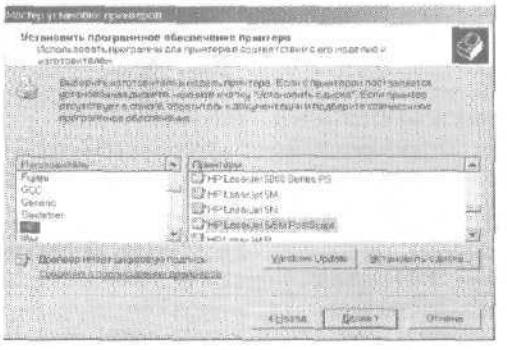


Рис. 17-2. Выберите изготовителя и модель печатающего устройства

6. Щелкните Далее (Next). Если драйвер принтера уже установлен, укажите, оставить его или заменить. Щелкните Далее (Next).
7. Назначьте принтеру имя, которое будет отображаться в папке Принтеры и факсы (Printers and Faxes). На локальной системе вы можете также установить принтер в качестве принтера по умолчанию. Щелкните Далее (Next).
8. Укажите, будет ли принтер доступен удаленным пользователям (рис. 17-3). Чтобы сделать принтер сетевым, установите переключатель Имя общего ресурса (Share Name) и введите имя.

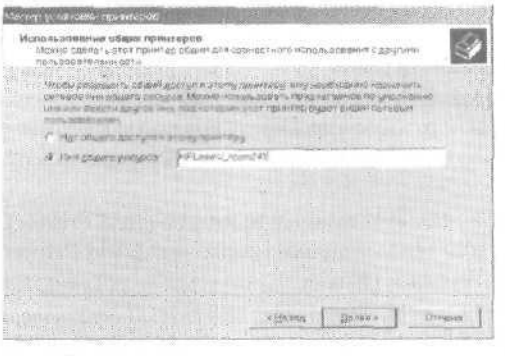


Рис. 17-3. Назначьте имя принтера для его использования через сеть

9. При желании введите описание принтера и его расположения. Эта информация поможет пользователю найти принтер и определить его возможности.
10. Щелкните Да (Yes), чтобы напечатать пробную страницу, или Нет (No). Щелкните Готово (Finish).

Когда Мастер установки принтеров (Add Printer Wizard) закончит установку нового принтера, в папке Принтеры я факсы (Printers and Faxes) появится дополнительный значок с заданным вами именем. Позже свойства принтера можно будет изменить. Подробнее — в разделе «Настройка свойств принтера».

Совет В папке Принтеры и факсы (Printers and Faxes) допускается создание нескольких принтеров для одного и того же печатающего устройства. Это позволяет задавать различные наборы свойств, удовлетворяющие различным потребностям. Например, на принтер с высоким приоритетом можно направлять срочные документы, а иа принтер с низким приоритетом — несрочные.

Установка сетевого печатающего устройства

Печатающее устройство можно подключить непосредственно к сети через собствен ную сетевую плату. Помните, что сервером печати для сетевого печатающего устройства считается тот сервер. на котором устройство сконфигурировано.

Чтобы установить подключенное к сети печатающее устройство, выполните следующие действия.

1. Откройте папку Принтеры и факсы (Printers and Faxes) на компьютере, который хотите сделать сервером печати.
   - На локальной системе выберите Принтеры и факсы (Printers and Faxes) в меню Пуск (Start) или в Панели управления (Control Panel).
   - С помощью папки Сетевое окружение (My Network Places) найдите компьютер, параметры принтера которого хотите настроить, и затем выберите Принтеры и факсы (Printers and Faxes).
2. Щелкните дважды значок Установка принтера (Add Printer), чтобы запустить Мастер установки принтеров (Add Printer Wizard). Щелкните Далее (Next).
3. Установите переключатель Локальный принтер (Local printer attached to this computer), сбросьте флажок Автоматическое определение и установка принтера «Plug and Play» (Auto-

matically detect and install my Plug and Play printer) и щелкните Далее (Next). Мастер установки принтеров (Add Printer Wizard) сразу переходит к окну Выберите порт принтера (Select a Printer Port),

4. Установите переключатель Создать новый порт (Create a new port), как показано на рис. 17-4, и укажите в списке вариант Standard TCP/IP Port. Щелкните Далее (Next). Запустится Мастер добавления стандартного TCP/IP порта принтера (Add Standard TCP/IP Printer Port Wizard).

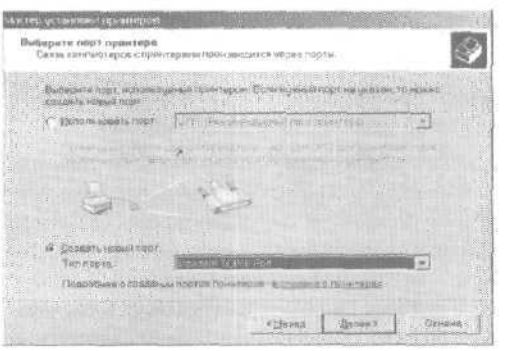


Рис. 17-4. Задайте порт TCP/IP для подключенного к сети принтера

5. Щелкните Далее (Next). В окне мастера (рис. 17-5) введите имя или IP-адрес печатающего устройства. Поле с именем порта заполнится автоматически. Например, если вы ввели IP-адрес 192.168.12.8, имя порта будет IP_192.168.12.8.

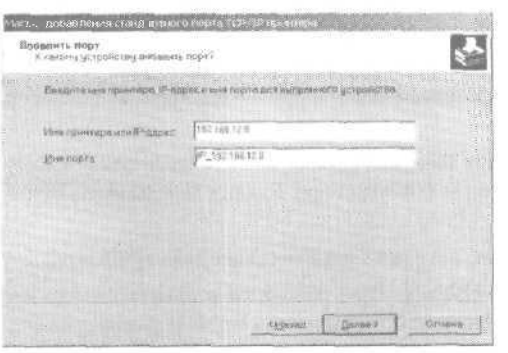


Рис. 17-5. Введите имя или IP-адрес сетевого принтера

Совет Имя порта может быть любым, лишь бы оно было уникально в системе. Если вы настраиваете сервер печати, который будет поддерживать несколько сетевых принтеров, обязательно запишите, какому принтеру какой порт соответствует.

6. Щелкните Далее (Next). Мастер попытается обнаружить печатающее устройство. В случае неудачи убедитесь, что:
   - устройство включено и подсоединено к сети;
   - принтер настроен правильно;
   - IP-адрес и имя принтера и предыдущем окне указаны верно.
7. Если IP-адрес или имя принтера указаны неверно, щелкните кнопку Назад (Back) и заново введите информацию.
8. Если информация задана верно, при необходимости укажите дополнительные параметры устройства. В области Тип устройства (Device Type) щелкните переключатель Обычное (Standard) и выберите принтер или сетевой адаптер, используемый принтером. Установив переключатель Особое (Custom) и щелкнув кнопку Параметры (Settings), вы сможете указать специфические параметры принтера, например протокол и SNMP-статус.
9. Щелкните Далее (Next) и Готово (Finish), чтобы завершить настройку корта. Мастер установки принтеров (Add Printer Wizard) начнет установку принтера.
10. В следующем окне мастера укажите изготовителя и модель принтера или щелкните кнопку Установить с диска (Have Disk), чтобы установить новый драйвер.
11. Щелкните Далее (Next). Если драйвер принтера уже установлен, ОС предложит заменить его или сохранить. Щелкните Далее (Next).
12. Назначьте принтеру имя, которое будет отображаться в папке Принтеры и факсы (Printers and Faxes). Щелкните Далее (Next).
13. При необходимости скорректируйте общее имя принтера.
14. Щелкните Далее (Next). При желании введите описание принтера и сведения о его расположении. Щелкните Далее (Next).

15. Щелкните Да (Yes), чтобы напечатать пробную страницу, или Нет (No). Щелкните Готово (Finish).

Подключение к сетевому принтеру

После создания сетевого принтера удаленные пользователи могут подключиться к нему и приступить к печати. Вам придется настроить соединение для каждого пользователем или предоставить это им самим. Соединение с принтером в Windows Server 2003 создают так.

1. Войдите в систему с правами пользователя. Откройте папку Принтеры и факсы (Printers and Faxes).
2. Дважды щелкните значок Установка принтера (Add Printer). Запустится Мастер установки принтеров (Add Printer Wizard). Установите переключатель Сетевой принтер (Network Printer) и щелкните Далее (Next).
3. В диалоговом окне Укажите принтер (Specify a Printer) выберите метод поиска сетевого принтера.
   - Найти принтер в Active Directory (Find a printer in the directory) — позволяет найти принтер в Active Directory. Туда автоматически попадают все общие принтеры в сети Windows Server 2003. При желании вы вправе их оттуда удалить.
   - **Подключиться к принтеру или выполнить обзор принтеров (кнопка «Далее») [Type the printer name, or click next to browse for a printer] — позволяет ввести сетевое имя принтера или найти его в структуре сети.**
   - **Подключиться к принтеру в Интернете, в домашней сети или в интрасети (Connect to a printer on the Internet or on your Intranet) — позволяет ввести URL принтера в Интернете.**
4. Щелкните Далее (Next).
5. Укажите, должен ли принтер использоваться по умолчанию в приложениях Windows, установив переключатель Да (Yes) или Нет (No), и щелкните Далее (Next).
6. Щелкните Готово (Finish).

После соединения пользователи могут отправлять документы на сетевой принтер, выбрав его имя в окне печати. Значок нового сетевого принтера появится в папке Принтеры и факсы (Printers and Faxes). Он позволяет настроить локальные параметры принтера.

Решение проблем с очередью печати

В Windows Server 2003 постановкой заданий печати в очередь управляет служба Диспетчер очереди печати (Print Spooler). Проблемы с очередью печати возникают, если эта служба не запущена. Для проверки ее состояния воспользуйтесь консолью Службы (Services).

1. В меню Администрирование (Administrative Tools) выберите команду Управление компьютером (Computer Management).
2. Щелкните правой кнопкой узел Управление компьютером (Computer Management) в дереве консоли и выберите Подключиться к другому компьютеру (Connect to Another Computer). Выберите нужный компьютер.
3. Раскройте узел Службы и приложения (Services and Applications) и выберите элемент Службы (Services).
4. Выделите службу Диспетчер очереди печати (Print Spooler). В столбце Состояние (Status) должно стоять Работает (Started). Если это не так, щелкните службу Диспетчер очереди печати (Print Spooler) правой кнопкой и выберите Пуск (Start).
5. Если это не поможет, проверьте работу служб, от которых зависит работа спулера печати:
   - Сервер печати TCP/IP (TCP/IP Print Server);
   - Сервер печати для Macintosh (Print Server for Macintosh);
   - Сервер печати для Unix (Print Server for Unix).

Совет Иногда в работе спулера печати наблюдаются нарушения. Симптомы: принтер «завис», задания не посылаются на печатающее устройство, печатается «мусор». Обычно проблему решает остановка и повторный запуск спулера печати.

Настройка свойств принтера

Свойства принтера назначаются в окне Свойства (Properties).

1. Откройте папку Принтеры и факсы (Printers and Faxes) нужного сервера печати.
2. Щелкните правой кнопкой значок нужного принтера и выберите команду Свойства (Properties). Откроется диалоговое окно свойств принтера (рис. 17-6).

Рис. 17-6. Задайте свойства принтера в диалоговом окне Свойства (Properties)

Описание и расположение принтера

На вкладке Общие (General) диалогового окна свойств принтера указываются сведения о принтере и о его расположении. Эти сведения весьма полезны в крупных организациях, когда пользователю нелегко разобраться во всех доступных печатающих устройствах. Укажите в описании тип устройства и фамилию тога, кто за него отвечает. В поле Размещение (Location) введите информацию о расположении принтера. Некоторые приложения, например Microsoft Word, отображают эту информацию непосредственно в окне печати.

Управление драйверами принтеров

В домене Windows Server 2003 драйверы принтера настраиваются и обновляются только на серверах печати. На клиентских Windows-компьютерах драйверы не обновляются, так как при необходимости они будут загружаться с сервера печати.

Обновление драйвера принтера

1. Откройте окно свойств принтера и перейдите на вкладку Дополнительно (Advanced).
2. Чтобы заменить драйвер на один из драйверов, также установленных и системе, выберите нужный вариант в списке Драйвер (Driver).

3. Если в списке нет нужного или вы хотите установить новый драйвер, щелкните кнопку Сменить (New Driver). Запустится Мастер установки драйверов принтера (Add Printer Driver Wizard). Щелкните Далее (Next). Щелкните кнопку Установить с диска (Have Disk), чтобы установить новый драйвер.
4. Щелкните Далее (Next) и Готово (Finish).

Настройка драйверов для сетевых клиентов

Установив принтер или обновив драйвер, выберите операционные системы, которые будут загружать драйвер с сервера печати, Это позволяет обновлять драйверы централизованно: вместо установки нового драйвера на каждом компьютере вы устанавливаете его на сервере печати и разрешаете клиентам загрузить обновление. Чтобы клиенты смогли загрузить новый драйвер, выполните следующие действия.

1. Щелкните правой кнопкой значок нужного принтера и выберите команду Свойства (Properties).
2. На вкладке Доступ (Sharing) щелкните кнопку Дополнительные драйверы (Additional Drivers). Откроется диалоговое окно Дополнительные драйверы (Additional Drivers), позволяющее выбрать ОС, которые будут загружать драйвер принтера.
3. При необходимости вставьте в дисковод компакт-диск Windows Server 2003 или установочный диск с драйверами для нужных ОС. Не забывайте, что на установочном компакт-диске Windows Server 2003 есть драйверы для большинства ОС семейства Windows и вариантов архитектуры процессора.

Настройка страницы-разделителя и режима печати

Страницы-разделители в Windows Server 2003 облегчают поиск нужного документа, а также облегчают переключение между режимами печати PostScript и PCL (Printer Control Language). Страница-разделитель для печатающего устройства настраивается так.

1. В диалоговом окне свойств нужного принтера перейдите на вкладку Дополнительно (Advanced) и щелкните кнопку Страница-разделитель (Separator Page).
2. В диалоговом окне Страница-разделитель (Separator Page) щелкните кнопку Обзор (Browse) и выберите одну из трех страниц-разделителей:

- **PCL.SEP** переключает печатающее устройство в режим PCL и печатает страницу-разделитель перед каждым документом;
- **PSCRIPT.SEP** переключает печатающее устройство в режим PostScript, но не печатает страницу-разделитель;
- **SYSPRINT.SEP** переключает печатающее устройство в режим PostScript и печатает страницу-разделитель перед каждым документом.

Чтобы отменить использование страницы-разделителя, откройте диалоговое окно Страница-разделитель (Separator Page) и удалите имя файла.

Изменение порта принтера

Порт принтера изменяется в диалоговом окне свойств принтера. Открыв диалоговое окно свойств принтера, перейдите на вкладку Порты (Ports). Чтобы включить или отключить порт, установите или сбросьте соответствующий флажок. Чтобы добавить порт, щелкните кнопку Добавить порт (Add Port), выберите тип порта и щелкните Новый порт (New Port). Чтобы полностью удалить порт, щелкните кнопку Удалить порт (Delete Port).

Настройка времени и приоритета заданий печати

Время и приоритет заданий печати по умолчанию настраиваются в диалоговом окне свойств принтера. Открыв его, перейдите на вкладку Дополнительно (Advanced), показанную на рис. 17-7.

Рис. 17-7. На вкладке Дополнительно (Advanced) задают время и приоритет заданий печати

Настройка времени доступа к принтеру

Вы вправе ограничить время доступа к принтеру. Переключатель Доступен всегда (Always Available) на вкладке Дополнительно (Advanced) открывает доступ к принтеру в любое время, а переключатель Доступен с (Available From) — только в определенные часы.

Настройка приоритета принтера

Приоритет заданий печати по умолчанию задается в поле Приоритет (Priority). Задания печати всегда выполняются в порядке приоритета, т. с. задания с высоким приоритетом печатаются первыми.

Настройка очереди печати

При работе с сетевым печатающим устройством файлы обычно не отправляются прямо на принтер, а выстраиваются в очередь. Для настройки очереди используются следующие параметры вкладки Дополнительно (Advanced):

- **Использовать очередь** печати **(ускорение работы приложений) [Spool print documents so program** finishes **printing faster]** — включает очередь заданий печати;
- **Начинать печать после**помещения **в очередь всего задания** (Start **printing** after last **page is spooled)** — задает начало печати только после того, как документ полностью помещен в очередь. Если печать будет прервана или отменена до этого момента, задание печати не будет выполнено;
- **Начинать печать немедленно (Start printing**immediately) — задает немедленную печать документа, если печатающее устройство не занято. Даже если печать будет прервана или отменена, часть документа все равно напечатается;
- **Печатать прямо на** принтер **(Print directly to the printer)** — выключает очередь.

Остальные флажки служат для настройки дополнительных параметров очереди:

- **Задерживать документы с неподходящими параметрами (Hold mismatched documents)** — спулер будет задерживать задания печати, которые не соответствуют параметрам печатающего устройства. Эта возможность удобна при частом изменении форматов печати или параметров лотка;

- Первыми печатать документы из очереди (Print spooled documents first) — задание, целиком помещенное в очередь, независимо от приоритета будет печататься прежде заданий, которые только ставятся в очередь;
- **Сохранять документы после печати (Keep printed documents)** — позволяет сохранить копию документа в принтере (обычно документы удаляются из очереди после печати). Как правило, этот параметр используется при печати трудно восстанавливаемых файлов — он позволяет напечатать документ, не прибегал к его восстановлению. Подробнее — в разделе «Приостановка, возобновление и повтор печати отдельных документов»;
- Включить дополнительные возможности печати (Enable advanced printing features) - разрешает задавать дополнительные параметры печати (если таковые имеются), например порядок страниц и количество страниц на каждом листе. Если при использовании дополнительных параметров у вас возникают проблемы, сбросьте этот флажок.

Открытие и закрытие доступа к принтеру

Для настройки доступа к принтеру щелкните правой кнопкой значок нужного принтера и выберите команду Общий доступ (Sharing). На открывшейся вкладке окна свойств принтера можно изменить общее имя принтера, а также открыть или закрыть доступ к принтеру.

- Чтобы открыть доступ к локальному принтеру (т. е. преобразовать его в сетевой принтер), установите переключатель Общий доступ к данному принтеру (Share this printer) и введите имя общего ресурса в поле Сетевое имя (Share Name). Щелкните OK.
- Чтобы изменить сетевое имя принтера, просто введите новое имя в поле Сетевое имя (Share Name) и щелкните OK.
- Чтобы закрыть доступ к общему принтеру, щелкните Нет общего доступа к данному принтеру (Do not share this printer), а затем OK.

Настройка разрешений доступа к принтерам

Поскольку сетевой принтер является общим ресурсом, доступ к нему можно ограничить посредством разрешений. Откройте окно свойств принтера и перейдите на вкладку Безопасность (Security).

ОС Windows Server 2003 поддерживает три разрешения доступа к принтерам: Печать (Print), Управление документами (Manage Documents) и Управление принтерами (Manage Printers), которые можно предоставлять и блокировать (табл. 17-1).

Таблица 17-1. Разрешения доступа к принтерам в Windows Server 2003

Действие	Печать (Print)	Управление документами (Manage Documents)	Управление принтерами (Manage Printers)
Печать документа	+	+	+
Приостановка, возобновление, повтор и отмена печати документа, отосланного непосредственно пользователем		+	+
Подключение к принтеру	+	+	+
Управление параметрами заданий печати		+	+
Приостановка, повтор и удаление заданий печати		+	+
Предоставление принтера в совместное использование			+
Изменение свойств принтера			+
Изменение разрешений принтера			+
Удаление принтера			+

При создании каждому принтеру назначаются стандартные разрешения доступа:

- группам Администраторы (Administrators), Операторы печати (Print Operators) и Операторы сервера (Server Operators) — полный контроль над принтерами, что подразумевает администрирование принтера и его заданий печати;
- создателю и владельцу — право управления своим документом, т. е. изменение параметров задания и его удаление;
- группе Все (Everyone) — право печати, что делает принтер доступным для всех пользователей сети.

Как и остальные наборы разрешений, базовые разрешения для принтеров представляют собой логические группы специальных разрешений. В табл. 17-2 перечислены специальные разрешения, используемые для создания базовых разрешений для принтеров.

Щелкнув кнопку Дополнительно (Advanced), вы сможете назначить эти специальные разрешения индивидуально.

Таблица 17-2. Специальные разрешения доступа к принтерам

Специальное разрешение	Печать (Print)	Управление документами (Manage Documents)	Управление принтерами (Manage Printers)
Печать	+		+
Управление документами		+	
Управление принтерами			+
Просмотр разрешений		+	+
Изменение разрешений		+	+
Получение прав владельца принтера		+	4

Аудит заданий печати

Windows Server 2003 поддерживает аудит большинства операций печати. Аудит операций с принтером настраивается так.

1. Откройте диалоговое окно свойств принтера, перейдите на вкладку Безопасность (Security) и щелкните кнопку Дополнительно (Advanced). Откроется диалоговое окно Дополнительные параметры безопасности (Advanced Security Settings).

Примечание По умолчанию аудит не выполняется. Чтобы разрешить аудит принтеров, настройте соответствующую групповую политику.

2. Перейдите на вкладку Аудит (Auditing) и с помощью кнопок Добавить (Add) и Удалить (Remove) сформируйте список пользователей и групп, действия которых должны подлежать аудиту.
3. С помощью флажков в столбцах Успех (Successful) и Отказ (Failed) задайте события, которые подлежат аудиту.
4. Щелкните OK.

Установка стандартных параметров документа

Стандартные параметры документа применяются при печати из программ, не являющихся приложениями Windows, например из командной строки MS-DOS. Стандартные параметры документа устанавливаются следующим образом.

1. Откройте папку Принтеры **и факсы (Printers and Faxes) и дважды** щелкните **значок нужного принтера.**
2. В меню Принтер (Printer) выберите команду Настройка печати (Printing Preferences).
3. Задайте стандартные **параметры** документа на **вкладках** Расположение (Layout) и Бумага **и качество** печати **(Paper/** Quality).

Настройка свойств сервера печати

Диалоговое окно Свойства сервера печати (Print Server Properties) позволяет управлять глобальными параметрами серверов печати. Оно открывается так.

1. Откройте панку Принтеры и факсы (Printers and Faxes) на сервере печати.
2. Выберите в меню Файл (File) команду Свойства сервера (Server Properties) или щелкните правой кнопкой мыши свободную область окна и выберите Свойства сервера (Server Properties).

В следующих разделах описаны некоторые свойства сервера печати, которые поддаются настройке.

Изменение положения папки Spool и настройка печати в NTFS

Папка очереди печати (Spool) содержит копии всех документов, которые находятся в очереди печати. По умолчанию она размещена в *%SystemRoot%*\system32\spool\PRINTERS. В файловой системе NTFS все пользователи, работающие с принтером, должны иметь разрешение па изменение этой папки, иначе они не смогут печатать. Разрешение для папки задается так.

1. Откройте папку Принтеры и факсы (Printers and Faxes) нужного сервера печати.
2. В меню Файл (File) выберите команду Свойства сервера (Server Properties).
3. Перейдите на вкладку Дополнительные параметры (Advanced). Расположение папки Spool указано в поле Папка очереди печати (Spool Folder). Запомните его.
4. Найдите папку в окне Проводника (Windows Explorer), щелкните ее правой кнопкой и выберите Свойства (Properties).

5. В окне свойств перейдите на вкладку Безопасность (Security) и проверьте правильность разрешений.

Повышение производительности печати

В больших корпорациях принтеры ежедневно печатают сотни и тысячи документов. Такая нагрузка требует от серверов печати высокой производительности. При ее недостатке в печати неизбежны задержки, разрушение документов и другие проблемы. В этом разделе описаны способы повышения производительности серверов печати.

- Подключайте принтеры к сети напрямую, а не через компьютерные порты. При таком способе подключения тратится меньше системных ресурсов (т. е. процессорного времени).
- Выделите для задач печати отдельный сервер. Если сервер печати занят решением других задач, он не способен быстро реагировать на запросы печати и управления принтерами.
- Переместите папку Spool на отдельный жесткий диск, предназначенный для печати (по умолчанию она хранится там же, где и ОС). Производительность операций ввода-вывода повысится при использовании диска с отдельным контроллером.

Регистрация событий, связанных с работой принтера

Для настройки регистрации событий, связанных с работой принтера, предназначено окно свойств сервера печати. Открыв его, перейдите на вкладку Дополнительные параметры (Advanced) и с помощью флажков задайте журналы, которые нужно вести.

Уведомление о завершении печати

Серверы печати способны уведомлять пользователей о завершении печати документа. По умолчанию эта возможность выключена, так как иногда она раздражает. Чтобы задать или отменить уведомление, откройте диалоговое окно свойств сервера печати, перейдите на вкладку Дополнительные параметры (Advanced) и включите или сбросьте флажок Уведомление о завершении удаленной печати документов (Notify when remote documents are printed). Кроме того, можно включить или сбросить флажок Передавать уведомление на компьютер, а не пользователю (Notify computer, not user, when remote documents are printed).

Управление заданиями печати локальных и удаленных принтеров

Для управления принтеров и заданиями печати служит окно управления печатью, которое открывается, когда вы дважды щелкаете значок принтера в папке Принтеры и факсы (Printers and Faxes) локального или удаленного компьютера.

Использование окна управления печатью

Окно управления печатью документов позволяет управлять принтерами и заданиями печати (рис. 17-8). В нем представлена информация о документах, которые находятся в очереди печати, а именно:

- Документ (Document Name) — имя файла документа, иногда с названием приложения, отправившего его на печать;
- Состояние (Status) — состояние задания печати (документа или принтера);
- **Владелец (Owner) —** владелец документа;
- Число страниц (Pages) — количество страниц в документе;
- Размер (Size) — размер документа;
- **Поставлено в очередь (Submitted) — дата и** время отправки документа **па печать;**
- Порт (Port) — порт, используемый при печати.

Рис. 17-8. Управление принтерами и заданиями печати из окна управления печатью

Приостановка принтера и возобновление печати

Чтобы приостановить работу принтера, откройте меню Принтер (Printer) и выберите команду Приостановить печать (Pause Printing). Возле нее появится галочка, которая свидетельствует, что работа принтера приостановлена. Принтер закончит выполнение текущего задания печати и приостановит печать оставшихся документов.

Чтобы возобновить работу принтера, снова дайте команду Приостановить печать (Pause Printing). Галочка рядом с ней должна исчезнуть.

Очистка очереди печати

Окно управления печатью документов позволяет очистить очередь печати. Для этого в меню Принтер (Printer) выберите команду Очистить очередь печати (Cancel All Documents).

Приостановка, возобновление и повтор печати отдельных документов

Состояние отдельных документов настраивается в окне управления печатью документов.

1. Выберите нужный документ в окне управления печатью документов.
2. В меню Документ (Document) выберите одну ил следующих команд;
   - Приостановить (Pause) — приостанавливает печать документа и уступает очередь печати другим документам;
   - **Продолжить (Resume)** — возобновляет печать документа с того места, где она была приостановлена;
   - **Перезапустить (Restart) — печатает документ с начала.**

Удаление документа и отмена задания печати

Чтобы удалить документ из очереди печати или отменить задание печати, выполните следующие действия.

1. Выделите нужный документ в окне управления печатью.
2. В меню Документ (Document) щелкните команду Отменить (Cancel) или нажмите клавишу Delete.

Примечание Большинство печатающих устройств кэшируют документы во внутреннем **буфере,** поэтому при отмене текущего задания печать документа может завершиться не **сразу.**

Просмотр свойств документа в очереди печати

Чтобы просмотреть свойства (источник, ориентация, размер) документа, находящегося в очереди печати, выполните одно из следующих действий:

- выделите нужный документ в окне управления печатью. В меню Документ (Document) выберите команду Свойства (Properties);
- дважды щелкните нужный документ в окне управления печатью.

Настройка приоритета отдельных документов

Приоритетом документа определяется очередность печати. Документы с высоким приоритетом печатаются первыми. Приоритет отдельных документов настраивается так.

1. Выделите нужный документ в окне управления печатью и в меню Документ (Document) выберите команду Свойства (Properties).
2. Перейдите на вкладку Общие (General) и задайте приоритет документа с помощью бегунка Приоритет (Priority): минимальный — 1, максимальный — 99.

Настройка времени печати отдельных документов

Если в организации ежедневно печатается множество документов, возможно, потребуется расписание печати. Например, в нем можно указать, чтобы большие задания печати с низким приоритетом выполнялись ночью. Время печати документа настраивается так.

1. Выделите нужный документ в окне управления печатью и в меню Документ (Document) выберите команду Свойства (Properties).
2. Перейдите на вкладку Общие (General), щелкните переключатель Только с (Only From) и задайте временной интервал, например, с полуночи до пяти часов утра. Теперь выбранный документ может быть напечатан только в указанный промежуток времени.

Глава 18

Клиенты и серверы DHCP

Протокол динамической конфигурации узла (Dynamic Host Configuration Protocol, DHCP) обеспечивает динамическую настройку параметров протокола TCP/IP на сетевых клиентах, чем существенно облегчает администрирование доменов службы каталогов Active Directory. При этом не только экономится время на настройку параметров системы, но и создается централизованный механизм изменения этих параметров. Для запуска службы DHCP в сети нужно настроить DHCP-сервер, предоставляющий клиентам сведения о сетевой конфигурации.

Знакомство с DHCP

DHCP — средство централизованного управления выделением IP-адресов, но этим его функции не ограничиваются. DHCP-сервер выдает клиентам основную информацию, необходимую для работы сети TCP/IP: IP-адрес, маску подсети, сведения о шлюзе по умолчанию, о первичных и вторичных DNS- и WINS-серверах, а также имя домена DNS.

Клиент DHCP и IP-адрес

Компьютер с динамическим IP-адресом называют *клиентом DHCP*. При загрузке компьютера DHCP-клиент запрашивает IP-адрес из пула адресов, выделенных данному DHCP-серверу, и использует адрес определенное время, называемое *сроком аренды* (lease). Спустя примерно половину этого срока клиент пытается возобновить аренду и повторяет эти попытки до успешного возобновления или до окончания срока аренды. Если возобновить аренду не удастся, клиент обращается к другому DHCP-серверу. Невозобновленный IP-адрес возвращается в пул адресов. Если клиент успешно связался с сервером, но его текущий IP-адрес не может быть возобновлен, DHCP-сервер присваивает клиенту новый IP-адрес.

DHCP-сервер обычно не влияет на процедуру загрузки или входа в сеть. Загрузка DHCP-клиента и регистрация пользователя в локальной системе возможна даже при неработающем DHCP-сервере.

Во время запуска DHCP-клиент пытается найти DHCP-сервер. Если это удалось, клиент получает от сервера нужную конфигурационную информацию. Если DHCP-сервер недоступен, а срок аренды клиента еще не истек, клиент опрашивает с помощью программы Ping стандартный шлюз, указанный при получении аренды. В случае успеха клиент считает, что, вероятно, находится в той же сети, в которой находился при получении аренды, и продолжает ею пользоваться. Неудачный опрос означает, что, возможно, клиент находится в другой сети. Тогда применяется автоконфигурация IP. Клиент также прибегает к ней, если DHCP-сервер недоступен, а срок аренды истек.

Автоконфигурация IP работает следующим образом.

1. Компьютер клиента выбирает IP-адрес из зарезервированной Microsoft подсети класса B — 169.254.0.0, маска подсети 255.255.0.0. Прежде чем задействовать IP-адрес, клиент проводит проверку по протоколу разрешения адресов (Address Resolution Protocol, ARP), чтобы убедиться, что выбранный IP-адрес не используется другим клиентом.
2. Если IP-адрес уже замят, клиент повторяет действие 1, пробуя до 10 IP-адресов, после чего сообщает об ошибке.

Примечание Если клиент отключен от сети, проверка ARP всегда будет успешной. В результате клиент использует первый же выбранный IP-адрес.

3. Если IP-адрес свободен, клиент настраивает сетевой интерфейс, используя этот адрес. Затем клиент пытается связаться с сервером DHCP, отправляя в сеть широковещательные запросы каждые 5 минут. Установив связь с сервером, клиент получает аренду и перенастраивает сетевой интерфейс.

Проверка назначения IP-адреса

Узнать выделенный компьютеру IP-адрес и другие сведения о конфигурации позволяет утилита Ipconfig. Чтобы получить информацию обо *всех* сетевых адаптерах компьютера, наберите в ко-

мандной строке ipconfig/all. Если TP-адрес был назначен автоматически, вы увидите строку IP-адрес автонастройки (Autoconfiguration IP Address). В приведенном ниже примере сетевому адаптеру автоматически назначен адрес 169.254.98.59:

```
Настройка протокола IP для Windows
   Имя компьютера. . . . . . . . . . . . . . . . . . . . . . . . corpserver01
   Основной DNS-суффикс . . . . . . . . . . . . . . . . . . . . microsoft.com
   Тип узла. . . . . . . . . . . . . . . . . . . . . . . . . . . гибридный
   IP-маршрутизация включена. . . . . . . . . . . . . . . . . . нет
   WINS-прокси включен. . . . . . . . . . . . . . . . . . . . . нет
   Порядок просмотра суффиксов DNS. . . . . . . . . . . . . . . microsoft.com
Подключение по локальной сети - Ethernet адаптер:
   DNS-суффикс этого подключения . . . . . . . . . . . . . . . :
   Описание. . . . . . . . . . . . . . . . . . . . . . . . . . . NDC ND5300
PnP Ethernet адаптер
   Физический адрес. . . . . . . . . . . . . . . . . . . . . . . 05-82-C6-F8-
FD-67
   DHCP включен. . . . . . . . . . . . . . . . . . . . . . . . . да
   Автонастройка включена . . . . . . . . . . . . . . . . . . . да
   IP-адрес автонастройки. . . . . . . . . . . . . . . . . . . . 169.254.98.59
   Маска подсети. . . . . . . . . . . . . . . . . . . . . . . . 255.255.0.0
   Основной шлюз. . . . . . . . . . . . . . . . . . . . . . . . :
   DNS-серверы . . . . . . . . . . . . . . . . . . . . . . . . . :
```

Области

Области (scopes) — это пулы IP-адресов, присваиваемых клиентам в процессе аренды и резервирования. Резервирование отличается от аренды тем, что назначенный компьютеру IP-адрес остается за этим компьютером, пока вы не отмените резервирование. Так можно присвоить постоянные адреса ограниченному кругу клиентов DHCP.

Посредством создания области вы ограничиваете диапазон IP-адресов, доступных клиентам DHCP. Например, для основной области предприятия можно выделить диапазон IP-адресов 192.168.12.2–192.168.12.250. В областях разрешается использовать открытые или частные IP-адреса:

- в сетях класса A: 1.0.0.0–126.255.255.255;
- **в сетях класса B:** 128.0.0.0-191.255.255.255;
- в сетях класса C: 192.0.0.0–223.255.255.255;
- **в сетях класса D:** 224.0.0.0-239.255.255.255.

Примечание IP-адресом 127.0.0.1 всегда обозначается сам локальный компьютер.

Один сервер DHCP способен управлять несколькими областями, относящимися к одному из следующих типов.

- Обычная область (normal scope) служит для присвоения пулов адресов сетям класса A, B и C.
- Многоадресная область (multicast scope) позволяет присвоить пул адресов сетям класса D. На компьютерах эти адреса используются как вторичные в дополнение к стандартным IP-адресам сетей класса A, B или C.
- **Суперобласть (superscope)** — контейнер, содержащий другие области и облегчающий управление ими.

Совет Вы вправе создавать области в разных сегментах сети, но обычно рекомендуется, чтобы эти сегменты находились в сети одного класса. Не забудьте настроить ретрансляцию DHCP для передачи широковещательных запросов между сегментами сети посредством службы маршрутизации и удаленного доступа и службы агента ретрансляции DHCP. Кроме того, в качестве агентов ретрансляции допускается использовать некоторые маршрутизаторы.

Установка сервера DHCP

Динамическое выделение IP-адресов возможно только при наличии в сети DHCP-сервера. Компоненты DHCP устанавливаются при помощи мастера установки компонентов Windows, а запуск и авторизация сервера осуществляются из консоли DHCP. Предоставлять клиентам динамические IP-адреса вправе только авторизованные серверы DHCP.

Установка компонентов DHCP

Чтобы сервер с Microsoft Windows Server 2003 мог работать в качестве DHCP-сервера, выполните следующие действия.

1. В меню Пуск (Start) выберите Программы (Programs) или Все программы (All Programs), затем щелкните Администрирование (Administrative Tools) и Мастер настройки сервера (Configure Your Server).
2. Дважды щелкните Далее (Next). Появятся текущие роли сервера. Выделите роль DHCP-сервер (DHCP Server) и дважды

щелкните Далее (Next). Мастер установит DHCP и запустит Мастер создания области (New Scope Wizard).

3. Если вы хотите сразу же создать начальную область для DHCP-сервера, щелкните Далее (Next) и выполните действия, описанные в разделе «Управление областями DHCP». В противном случае щелкните Отмена (Cancel) и создайте необходимые области позднее.
4. Щелкните Готово (Finish). Чтобы использовать сервер, вы должны авторизовать его в домене, как описано в разделе «Авторизация сервера DHCP в Active Directory». Далее вам необходимо создать и активизировать все необходимые области DHCP.

Запуск и использование консоли DHCP

После установки DHCP-сервера настройка и управление динамической IP-адресацией осуществляется из консоли DHCP (рис. 18-1). Команда для ее запуска располагается в меню Администрирование (Administrative Tools). В главном окне консоли DHCP две панели. Слева перечислены все DHCP-серверы домена, упорядоченные по IP-адресам, включая локальный компьютер, если окно открыто на DHCP-сервере. Справа приведены подробные *сведения* о выбранном объекте.

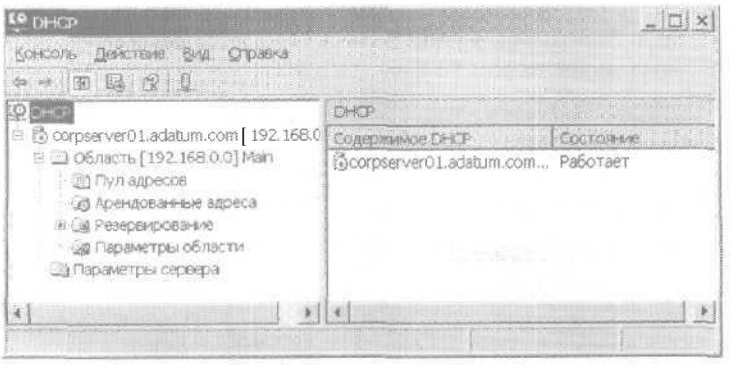


Рис. 18-1. Консоль **DHCP** служит для управления конфигурацией DHCP-сервера

Значки серверов и узлов областей отображают их текущее состояние. Для серверов значки могут быть такими:

- зеленая стрелка вверх — служба DHCP запущена, сервер активен;

- красная буква «X» --- у консоли нет доступа к серверу: служба DHCP остановлена или сервер недоступен;
- красная стрелка вниз — сервер DHCP не авторизован;
- синий значок — изменилось состояние сервера или система выдала предупреждение.

Значки областей имеют следующие значения:

- красная стрелка вниз — область неактивна;
- синий значок — изменилось состояние области или система выдала предупреждение.

Примечание Доступ к консоли DHCP можно получить из консоли Управление компьютером (Computer Management). Запустите ее, подключитесь к серверу, которым хотите управлять, затем раскройте Службы и приложения (Services and Applications) и выберите DHCP.

Соединение с удаленными серверами DHCP

Открыв консоль DHCP, вы подключитесь к локальному серверу. Чтобы подключиться к удаленному серверу, выполните следующие действия

1. Щелкните правой кнопкой корень консоли DHCP и выберите Добавить сервер (Add Server). Откроется диалоговое окно, показанное па рис. 18-2.

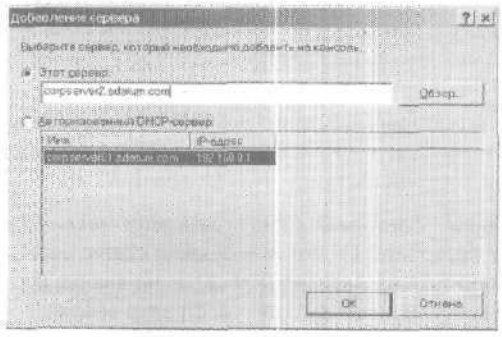


Рис. 18-2. Если вашего сервера DHCP нет в консоли, добавьте его

2. Установите переключатель Этот сервер (This server) и введите IP-адрес или имя DHCP-сервера, которым хотите управлять. Чтобы настроить один из авторизованных серверов DHCP,

установите переключатель Авторизованный DHCP-сервер (This authorized DHCP server) и щелкните нужный сервер. Помните, что вы вправе управлять только серверами в доверенных доменах.

3. Щелкните OK. Новый DHCP-сервер появится в дереве консоли.

Примечание После подключения к удаленному серверу некоторые параметры иногда оказываются недоступными. Для решения этой проблемы, как правило, достаточно щелкнуть правой кнопкой мыши узел сервера и выбрать Обновить (Refresh).

Запуск и остановка сервера DHCP

Серверами DHCP управляют е помощью одноименной службы. Как и любую другую, вы вправе ее запустить, отключить, приостановить и перезапустить посредством узла Службы (Services) консоли Управление компьютером (Computer Management) или из командной строки. Кроме того, службой DHCP можно управлять из консоли DHCP. Щелкните правой кнопкой сервер, которым хотите управлять, выберите Все задачи (All Tasks), а затем щелкните Запустить (Start), Остановить (Stop), Приостановить (Pause), Продолжить (Resume) или Перезапустить (Restart).

Авторизация сервера DHCP в Active Directory

Перед использованием DHCP-сервера в домене вы должны авторизовать его в Active Directory. Авторизация означает, что сервер уполномочен выдавать динамические IP-адреса в домене. Windows Server 2003 требует авторизации, чтобы предотвратить обслуживание клиентов домена чужими серверами.

Чтобы авторизовать сервер из консоли DHCP, щелкните его правой кнопкой и выберите Авторизовать (Authorize). Для отмены авторизации щелкните Запретить (Unauthorize).

Примечание Процесс авторизации иногда длится несколько минут, поэтому потерпите. По его завершении статус сервера должен измениться на Активно (Active), а на значке сервера в дереве консоли появится зеленая стрелка вверх.

Примечание Для авторизации сервера DHCP в Active Directory иногда приходится регистрироваться на контроллере домена или удаленно подключаться к нему.

Настройка DHCP-сервера

При установке нового сервера DHCP на нем автоматически задаются параметры, оптимальные для данного сетевого окружения. Обычно менять их не следует. Заниматься настройкой сервера приходится для решения проблем производительности или для установки дополнительных параметров. Для настройки сервера DHCP щелкните его правой кнопкой и выберите Свойства (Properties). Окно свойств DHCP-сервера показано на рис. 18-3.

Рис. 18-3. Управление статистикой, аудитом, интеграцией с DNS и другими свойствами DHCP-сервера

Привязка DHCP-сервера к конкретному IP-адресу

Сервер с несколькими сетевыми адаптерами имеет несколько сетевых подключений соответственно и может предоставлять службу DHCP по любому ил них. Но иногда нужно, чтобы сервер DHCP обслуживал не все доступные соединения. Например, если сервер подключен к сетям 10 и 100 Мбит/с, но в данный момент требуется, чтобы весь DHCP-трафик проходил через быстрое соединение.

Для привязки DHCP к конкретному сетевому соединению выполните следующие действия.

1. В консоли DHCP правой кнопкой щелкните нужный сервер и выберите Свойства (Properties).

2. Перейдите на вкладку Другие (Advanced) и щелкните кнопку Привязки (Bindings).
3. В списке сетевых подключений сервера DHCP установите флажки только у тех соединений, которые должны использоваться для передачи сведений DHCP-клиентам.
4. Щелкните OK.

Обновление статистики DHCP

В консоли DHCP отображается статистика доступности и использования IP-адресов. По умолчанию она обновляется только при запуске консоли DHCP или по щелчку кнопки Обновление (Refresh) на панели инструментов. Если вы регулярно обращаетесь к статистике DHCP, настройте ее автоматическое обновление.

1. В консоли DHCP правой кнопкой щелкните сервер и выберите Свойства (Properties).
2. На вкладке Общие (General) выберите Автоматически обновлять статистику каждые (Automatically update statistics every) и введите интервал времени в часах и минутах. Затем щелкните OK.

Аудит DHCP и устранение неполадок

Система Windows Server 2003 изначально настроена на аудит DHCP. По умолчанию журнал аудита находится в папке *%SystemRoot%*\system32\DHCP — там хранятся отдельные файлы для каждого дня педели. Файл журнала для понедельника называется DhcpSrvMon.log, для вторника — DhcpSrvTue.log и т. д.

При запуске сервера DHCP или наступлении нового дня в файл журнала записывается сообщение-заголовок. В нем резюмированы события DHCP и их значение. При запуске и остановке службы DHCP очистка журнала не выполняется. Данные журнала обнуляются, только если запись в него не производилась последние 24 часа. Вам не нужно следить за использованием дискового пространства сервером DHCP — по умолчанию он делает это сам.

Разрешение и запрет аудита DHCP

1. В консоли DHCP правой кнопкой щелкните сервер и выберите Свойства (Properties).
2. На вкладке Общие (General) выберите Вести журнал аудита DHCP (Enable DHCP audit logging). Щелкните OK.

Размещение журналов аудита DHCP

По умолчанию журналы DHCP хранятся в панке *%System-Root%*\system32\DHCP, но вы вправе изменить их расположение,

1. В консоли DHCP правой кнопкой щелкните нужный сервер и выберите Свойства (Properties).
2. На вкладке Другие (Advanced) введите путь к файлам в поле Журнал аудита (Audit Log File Path) или щелкните Обзор (Browse), чтобы выбрать новую папку
3. Щелкните OK. ОС потребует перезапустить службу сервера DHCP. Щелкните Да (Yes).

Изменение параметров журнала

В DHCP-сервер встроен мониторинг использования дискового пространства- По умолчанию максимальный размер всех файлов журнала сервера DHCP — 70 Мбайт, причем каждый отдельный файл может занимать не более одной седьмой этого объема. Если лимит в 70 Мбайт превышен или объем отдельного файла журнала превышает установленное для него значение, аудит DHCP прекращается, пока файлы журнала не будут очищены. Обычно это происходит, когда сервер очищает файл журнала *за* прошедшую неделю.

Параметры реестра, управляющие журналом и другими параметрами DHCP, расположены в разделе HKEY LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCP-Server\Parameters. Записью журнала управляют следующие параметры реестра:

- **DhcpLogFilesMaxSize** задает максимальный размер всех файлов журнала (по умолчанию 70 Мбайт);
- **DhcpLogDiskSpaceCheckInterval** определяет частоту проверок использования дискового пространства (по умолчанию каждые 50 минут);
- **DhcpLogMinSpaceOnDisk** устанавливает пороговое значение свободного места на диске; если свободного места на диске меньше, запись журнала временно прекращается (по умолчанию 20 Мбайт).

Автоматически создается только параметр DhcpLogFile-MaxSize. Остальные параметры при необходимости создаются вручную.

Интеграция DHCP и DNS

DNS используется для разрешения имен компьютеров в доменах Active Directory и в Интернете. Протокол динамического обновления DNS избавляет вас от необходимости вручную регистрировать DHCP-клиенты в DNS, позволяя клиенту и серверу DHCP при необходимости зарегистрировать записи прямого и обратного просмотра в DNS. В стандартной конфигурации DHCP клиенты под управлением Windows Server 2003 автоматически обновляют свои записи в DNS после аренды IP-адреса. Сервер DHGP обновляет записи о клиентах с более ранними версиями Windows после предоставления аренды.

Совет Серверы DNS на базе Windows NT 4.0 не поддерживают протокол динамического обновления, поэтому их записи автоматически не обновляются. Чтобы обойти это ограничение, разрешите поиск WINS для клиентов DHCP, использующих NetBIOS. Тогда клиенты смогут найти другие компьютеры средствами WINS. Но лучше обновить старые серверы DNS до Windows Server 2003.

Чтобы просмотреть и изменить параметры интеграции с DNS, выполните следующие действия.

1. В консоли DHCP щелкните сервер правой кнопкой и выберите Свойства (Properties).
2. Перейдите на вкладку Служба DNS (DNS), показанную на рис. 18-4.

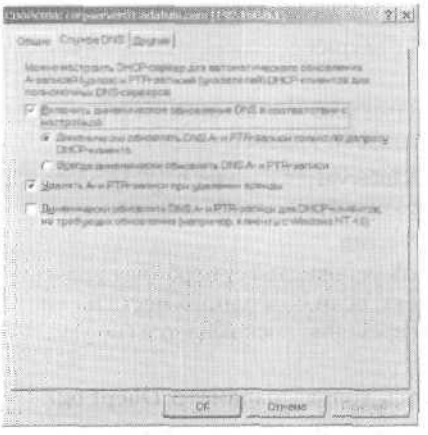


Рис. 18-4. Стандартные параметры интеграции DNS с DHCP

Предотвращение конфликтов IP-адресов

Конфликт IP-адресов — типичная причина неполадок DHCP. Два компьютера одной сети не могут иметь одинаковых IP-адресов. Если компьютеру присвоен IP-адрес, уже имеющийся в сети, один или оба компьютера будут от нес отключены. Для удобства выявления и предотвращения потенциальных конфликтов желательно включить диагностику конфликтов IP-адресов.

1. В консоли DHCP правой кнопкой щелкните сервер и выберите Свойства (Properties).
2. На вкладке Другие (Advanced) задайте ненулевое значение параметра Число попыток определения конфликтов (Conflict detection attempts). Этот параметр определяет число проверок IP-адреса сервером с помощью команды ping перед выдачей адреса в аренду.

Примечание Когда клиент запрашивает аренду, сервер проверяет пул доступных адресов и предоставляет в аренду один из них. При этом он не опрашивает сеть, чтобы убедиться, что предоставляемый адрес действительно свободен. Но в интенсивно работающей сети этот адрес мог быть присвоен одному из компьютеров другим администратором. Кроме того, иногда с точки зрения DHCP-сервера срок аренды адреса уже истек, а с точки зрения клиентского компьютера, который некоторое время был отключен от сети, а потом вновь включился в нее, все еще длится. Чтобы избежать подобных накладок, задайте ненулевое число попыток распознавания конфликтов.

Сохранение и восстановление конфигурации DHCP

После настройки всех необходимых параметров DHCP сохраните конфигурацию сервера, чтобы потом ее удалось легко восстановить. Для этого введите в командной строке команду

```
netsh dump dhcp > dhcpconfig.dmp
```

Здесь dhcpconfig.dmp — имя создаваемого сценария конфигурации. Для восстановления конфигурацию введите команду

```
netsh exec dhcpconfig.dmp
```

Совет Эта методика позволяет скопировать настройку на другой сервер DHCP: просто скопируйте сценарий в папку целевого компьютера и выполните указанную команду.

Управление областями DHCP

Установив сервер DHCP, настройте области, которые будут им использованы. Как уже говорилось, области бывают трех видов — суперобласти, обычные и многоадресные.

Суперобласти

Суперобласть — это контейнер областей, напоминающий организационное подразделение в Active Directory. Суперобласть упрощает управление обычными областями сети, позволяя одним действием активизировать или отключить сразу несколько областей. Также вы вправе просматривать статистику всех областей суперобласти, не проверяя каждую в отдельности.

Создание суперобласти

1. В консоли DHCP щелкните сервер правой кнопкой и выберите Создать суперобласть (New Superscope). Запустится Мастер создания суперобласти (New Superscope Wizard).
2. Щелкните Далее (Next) и введите имя суперобласти.
3. Выберите области, которые нужно добавить в суперобласть, выделив их в списке Доступные области (Available Scopes).
4. Щелкните Далее (Next), а затем — Готово (Finish).

Добавление областей к суперобласти

Добавить области в суперобласть можно как при ее создании, так и после этого.

1. Щелкните выбранную область правой кнопкой и выберите Добавить в суперобласть (Add to Superscope).
2. Выберите суперобласть в окне Добавление области (Add Scope).
3. Щелкните OK.

Удаление областей из суперобласти

1. Щелкните правой кнопкой нужную область и выберите Удалить из суперобласти (Remove from Superscope).
2. Подтвердите действие, щелкнув Да (Yes). Если это была последняя область суперобласти, суперобласть автоматически удаляется.

Активизация и отключение суперобласти

При активизации (отключении) суперобласти одновременно активизируются (отключаются) все входящие в нее области. Для

активизации (отключения) суперобласти щелкните ее правой кнопкой и выберите соответственно Активировать (Activate) или Деактивировать (Deactivate).

Удаление суперобласти

При удалении суперобласти удаляется только контейнер, но не области внутри него. Чтобы удалить и их, сделайте это после удаления суперобласти. Чтобы удалить суперобласть, щелкните ее правой кнопкой и выберите Удалить (Delete), а затем щелкните Да (Yes).

Создание областей

Область предоставляет собой пул 1 Р-адрссов, доступных клиентам DHCP. Обычные области включают в себя адреса сетей класса A, B или C, а многоадресные — адреса сети класса D. Обычные и многоадресные области создаются раздельно, но управляются одинаково. Главное различие состоит в том, что к многоадресным областям неприменимо резервирование. Для них также нельзя задать дополнительные параметры — WINS, DNS, маршрутизацию и т. п.

Создание обычной области

1. В консоли DHCP щелкните правой кнопкой нужный сервер или суперобласть.
2. Выберите Создать область (New Scope). Запустится мастер создания новой области. Щелкните Далее (Next).
3. Введите имя и описание новой области и щелкните Далее (Next).
4. В полях Начальный IP-адрес (Start IP Address) и Конечный IP-адрес (End IP Address) задайте диапазон IP-адресов, входящих в область.

Примечание Как правило, области не содержат адреса вида x.x.x.0 и x.x.x.255, которые резервируются соответственно для адресов сетей и широковещательных рассылок. Поэтому вместо диапазона 192.168.10.0-192.168.10.255 укажите 192.168.10.1-192.168.10.254.

5. Остальные ноля этого окна определяют параметры подсетей и заполняются автоматически (рис. 18-5). Если в сети нет подсетей, используите стандартные значения.

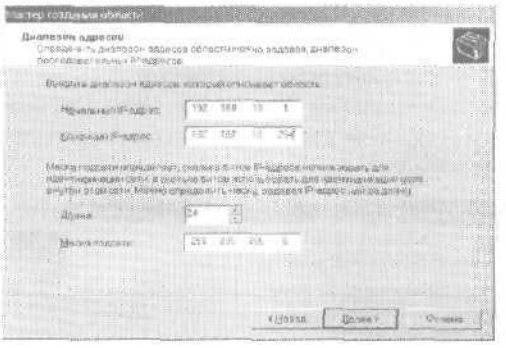


Рис. 18-5. В окне мастера создания области укажите диапазон IP-адресов новой области

6. Щелкните Далее (Next). Следующее окно появится, если введенный диапазон охватывает разные сети. Вам будет предложено создать суперобласть, содержащую отдельную область для каждой сети. Щелкните Да (Yes) и Далее (Next). Если вы ошиблись, щелкните Назад (Back) и исправьте диапазон введенных адресов.
7. Определите диапазоны IP-адресов, исключаемые из области, вводя их границы в полях Начальный IP-адрес (Start IP Address) и Конечный IP-адрес (End IP Address) и щелкая Добавить (Add). Чтобы удалить диапазон, выделите его и списке Исключаемый диапазон адресов (Excluded Addresses) и щелкните Удалить (Remove).
8. Задайте продолжительность аренды для области (по умолчанию — 8 дней).

Совет Из-за слишком большого срока аренды снижается эффективность DHCP и исчерпывается запас доступных IP-адресов, особенно если в сети работает много пользователей, не являющихся ее постоянными клиентами. Оптимальный срок аренды для большинства сетей — от 1 до 3 суток,

9. Щелкните Да (Yes), если хотите настроить параметры DNS, WINS, шлюзов и т. п. В противном случае щелкните Нет (No) и пропустите пункты 10–14.
10. Щелкните Далее (Next), введите IP-адрес первого основного шлюза и щелкните Добавить (Add). Повторите эту процедуру для остальных стандартных шлюзов. При необходимости

измените **порядок** обращения клиентов к шлюзам с помощью кнопок Вверх (Up) **и Вниз** (Down).

11. Щелкните Далее (Next) и настройте параметры DNS, которые будут передаваться клиентам DHCP (рис. 18-6). Введите имя родительского домена, чтобы DNS могла разрешить неполные имена компьютеров.

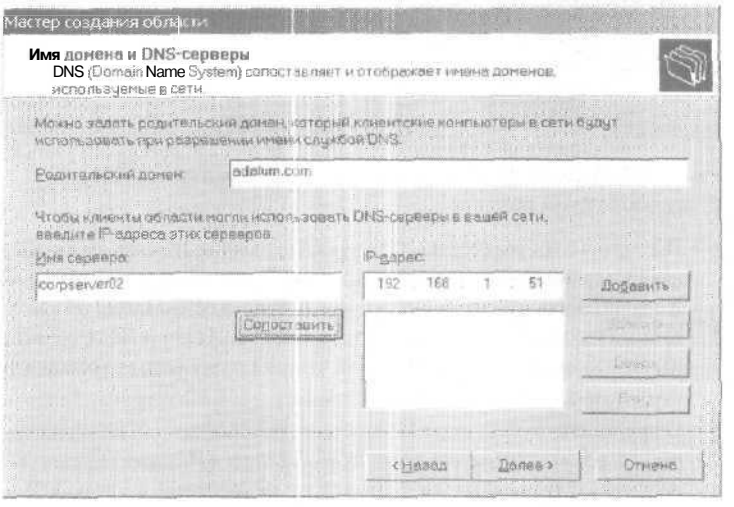


Рис. 18-6. Настройка стандартных параметров DNS для клиентов DHCP

12. В поле IP-адрес (IP Address) введите IP-адрес первичного DNS-сервера. Щелкните Добавить (Add). Повторите процедуру для дополнительных серверов DNS. Расположение IP-адресок в списке определяет очередность обращения к ним. При необходимости измените порядок адресов с помощью кнопок Вверх (Up) и Вниз (Down). Щелкните Далее (Next).

Совет Если вам известно имя сервера, но не его IP-адрес, введите имя в поле Имя сервера (Server Name) и щелкните Сопоставить (Resolve).

13. Аналогично настройте стандартные параметры WINS для клиентов DHCP. Щелкните Далее (Next).

14. Чтобы активизировать область, щелкните Да, я хочу активировать эту область сейчас (Yes, I will activate this scope now). *Или* щелкните Нет, я активирую эту область позже (No, I will activate this scope later). Щелкните Далее (Next).

15. Щелкните Готово (Finish).

Создание **многоадресной области**

1. В консоли DHCP щелкните правой кнопкой значок сервера.
2. В контекстном меню **выберите** Создать многоадресную область (New Multicast Scope) — запустится мастер создания многоадресной области. Щелкните Далее (Next).
3. Введите имя и описание новой области и щелкните Далее (Next).
4. В полях Начальный IP-адрес (Start IP Address) и Конечный IP-адрес (End IP Address) задайте диапазон IP-адресов, входящих в область. Многоадресные области должны определяться IP-адресами класса D. Это означает, что разрешен диапазон адресов от 224.0.0.0 до 239.255.255.255.
5. Рассылаемые компьютерами пакеты с широковещательными адресами характеризуются параметром TTL (time-to-live, время жизни), равным максимальному числу маршрутизаторов, через которые разрешается пройти пакету, Оставьте его стандартное значение (32), чего достаточно для большинства сетей, или увеличьте в соответствии с числом маршрутизаторов в вашей сети. Щелкните Далее (Next).
6. Задайте диапазоны **IP-адресов,** которые не будут **включены** в область. Щелкните Далее **(Next).**
7. Задайте продолжительность аренды области (по умолчанию — 30 дней). Щелкните Далее (Next).

Примечание Если вы недостаточно компетентны в вопросах широковещательной рассылки, не меняйте стандартных значений. Многоадресная аренда используется не так, как обычная. Широковещательный IP-адрес иногда применяется несколькими компьютерами, и все они могут иметь права аренды этого IP-адреса. Рекомендуемая длительность многоадресной аренды в большинстве сетей — от 30 до 60 дней.

8. Если хотите активизировать область, щелкните Да (Yes), в противном случае щелкните Далее (Next).
9. Щелкните Готово (Finish).

Настройка параметров для клиентов области

Параметры области позволяют тонко управлять ее работой и задавать стандартные иарамегры клиентов TCP/IP, использующих

данную область. Так, вы вправе разрешить клиентам автоматически находить в сети серверы DNS или определить параметры стандартных шлюзов, WINS и т. п. Параметры области применимы только к обычным областям, но не к многоадресным.

Вы вправе определить параметры областей:

- глобально для всех областей, настроив стандартные параметры сервера;
- для области, настроив параметры области;
- для клиента, настроив параметры резервирования;
- **для класса клиентов.**

Параметры области выстроены в иерархию, определяющую выбор действующего параметра. Порядок расположения соответствует очередности в приведенном только что списке. То есть:

- параметры области преобладают над глобальными параметрами;
- параметры клиента преобладают над параметрами области и глобальными;
- параметры класса преобладают над всеми остальными.

Просмотр и назначение параметров сервера

Параметры сервера относятся ко всем созданным на нем областям. Чтобы посмотреть или отредактировать их, выполните следующие действия.

1. В консоли DHCP двойным щелчком откройте нужный сервер.
2. Для просмотра параметров щелкните элемент Параметры сервера (Server Options). В правой панели отобразятся текущие параметры.
3. Для перенастройки параметров щелкните правой кнопкой элемент Параметры сервера (Server Options) и выберите Настроить параметры (Configure Options). В открывшемся диалоговом окне отметьте флажками нужные параметры и заполните необходимые поля в панели ввода данных.

Просмотр и настройка параметров областей

Эти параметры уникальны для каждой области и имеют приоритет над стандартными параметрами сервера.

I. Откройте нужную область в консоли DHCP.

2. Для просмотра параметров щелкните элемент Параметры области (Scope Options). В правой панели отобразятся текущие параметры.
3. Для изменения параметров щелкните правой кнопкой элемент Параметры области (Scope Options) и выберите Настроить параметры (Configure Options). Откроется окно настройки параметров области (рис. 18-7). В нем отметьте флажками нужные параметры и заполните необходимые поля в панели ввода данных.

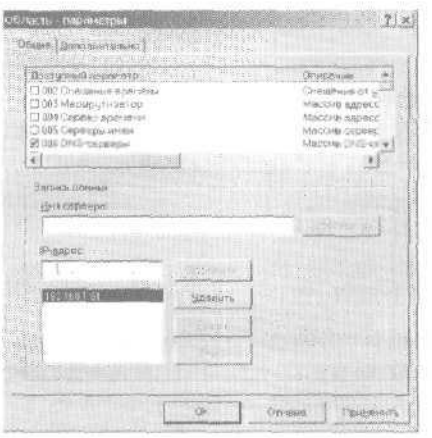


Рис. 18-7. Для каждого параметра области предусмотрены свои поля для ввода данных

Просмотр и настройка параметров резервирования

Эти параметры относятся к клиенту, за которым резервируется конкретный IP-адрес. Они уникальны для каждого клиента и имеют приоритет над параметрами сервера и области.

1. Откройте нужную область в консоли DHCP.
2. Дважды щелкните папку **Резервирование** (Reservations) нужной **области.**
3. Щелкните объект резервирования, чтобы вывести его текущие параметры в правой панели.
4. Чтобы их изменить, щелкните объект правой кнопкой и выберите Настроить параметры (Configure Options). В открывшемся диалоговом окне отметьте флажками нужные параметры и заполните необходимые поля в панели ввода данных.

Настройка области

Не путайте настройку параметров самой области с настройкой параметров, которые рассылаются ее клиентам.

Настройка параметров области

1. Откройте консоль DHCP и дважды щелкните сервер, области которого хотите настроить.
2. Щелкните правой кнопкой нужную область и выберите Свойства (Properties).
3. Измените нужные параметры, например срок действия аренды.
4. Щелкните OK.

Активизация и отключение областей

В консоли DHCP неактивные области помечены значком с красной стрелкой вниз, а активные — значком обычной папки.

- Чтобы активировать область, щелкните ее правой кнопкой и выберите Активировать (Active).
- Чтобы отключить область, щелкните ее правой кнопкой и выберите Деактивировать (Deactive).

Примечание Деактивация отключает область, но не прекращает текущую аренду клиентов. О прекращении аренды рассказано в разделе «Высвобождение адресов и аренды».

Применение протокола BOOTP

BOOTP — протокол динамической адресации, предшествующий DHCP. Обычные области его не поддерживают. Если вам по каким-то причинам нужно включить его поддержку, выполните следующие действия.

1. Щелкните правой кнопкой модифицируемую область и выберите Свойства (Properties).
2. На вкладке Дополнительно (Advanced) щелкните Обоих типов серверов (Both).
3. При необходимости задайте продолжительность аренды для клиентов BOOTP. Щелкните OK.

Удаление области

1. В консоли DHCP щелкните правой кнопкой удаляемую область и выберите Удалить (Delete).
2. Подтвердите удаление области, щелкнув Да (Yes).

Настройка нескольких областей

В одной сети разрешается настроить несколько областей, обслуживаемых одним или несколькими серверами DHCP. При этом чрезвычайно важно помнить, что диапазоны адресов, используемые разными областями, не должны перекрываться. Каждая область должна владеть уникальным диапазоном адресов, иначе один и тот же IP-адрес может быть выдан различным клиентам DHCP, что помешает работе сети.

Рассмотрим пример. На сервере А вы создаете область с диапазоном 192.168.10.1–192.168.10.99, на сервере В - с диапазоном 192.168.10.100–192.168.10.199, на сервере С - с диапазоном 192.168.10.100–192.168.10.199. Каждый из этих серверов имеет право отвечать на сообщения о запросе аренды DHCP и присваивать IP-адреса клиентам. При отказе одного из них обслуживать сеть будут остальные.

Управление пулом адресов, арендой и резервированием

В областях есть отдельные папки для пулов адресов, аренды и резервирования, позволяющие посмотреть текущую статистику и управлять этими элементами.

Просмотр статистики области

Статистика области — это общая информация об адресном пуле текущей области или суперобласти. Чтобы посмотреть статистику, щелкните правой кнопкой интересующую область или суперобласть и выберите Отобразить статистику (Display Statistics). Появится диалоговое окно со следующими полями:

- Всего областей (Total Scopes) — количество областей и суперобласти;
- Всего адресов (Total Addresses) — количество IP-адресов, присвоенных области;
- **Используется (In Use)** — количество адресов, используемых в настоящее время. Показана абсолютная величина и процентное отношение к общему числу доступных адресов. Если это отношение — 85% и более, увеличьте количество доступных адресов или освободите занятые;
- Доступно (Available) — количество доступных для использования адресов. Показана абсолютная величина и процент от общего числа доступных адресов.

Создание и удаление диапазона исключений

Можно исключить IP-адреса из области, определив диапазон исключений. Область может содержать несколько таких диапазонов. Вот как настроить новый диапазон исключений.

1. В консоли DHCP откройте нужную область, щелкните правой кнопкой папку Пул адресов (Address Pool) и выберите Диапазон исключения (New Exclusion Range).
2. Введите начальный и конечный адрес диапазона и щелкните Add (Добавить). Выбранный диапазон должен находиться в пределах диапазона адресов данной области и не должен использоваться в данный момент. Повторите эти действия для добавления других диапазонов.
3. Щелкните Закрыть (Close).

Чтобы удалить диапазон исключений, щелкните его правой кнопкой и выберите Удалить (Delete).

Резервирование адресов DHCP

Постоянные IP-адреса присваиваются DHCP-клиентам несколькими способами. Например, установив переключатель Без ограничений (Unlimited) в диалоговом окне свойств области, всем ее клиентам вы выдадите адреса в бессрочную аренду. Другой способ — зарезервировать адрес за DHCP-клиентом. Такой DHCP-клиент всегда получает от DHCP-сервера один и тот же IP-адрес, но при этом вы сохраняете возможность централизованного управления, которое делает технологию DHCP столь привлекательной.

Вот как зарезервировать IP-адрес за клиентом.

1. В консоли DHCP откройте нужную область, щелкните правой кнопкой папку Резервирование (Reservations) и выберите Создать резервирование (New Reservation). Откроется одноименное диалоговое окно (рис. 18-8).
2. В поле Имя клиента (Reservation Name) введите короткое описание клиента. Это поле служит только для идентификации.
3. В поле IP-адрес (IP Address) введите IP-адрес, который хотите закрепить за клиентом. Он должен находиться в диапазоне адресов выбранной области.
4. В поле MAC-адрес (MAC Address) введите аппаратный адрес сетевого адаптера на клиентском компьютере. Чтобы узнать MAC-адрес, введите в командной строке компьютера-клиента команду **ipconfig** /all.

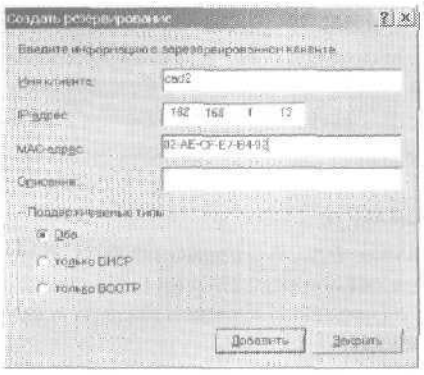


Рис. 18-8. Резервирование IP-адреса для клиента

5. При желании введите комментарий в поле Описание (Description).
6. По умолчанию поддерживаются как клиенты DHCP, так и клиенты BOOTP. Этот вариант идеален для большинства случаев. Измените его, если вам непременно нужно исключить конкретный тип клиентов.
7. Щелкните Добавить (Add).

Высвобождение адресов и аренды

Применение зарезервированных адресов имеет ряд ограничений:

- зарезервированные адреса не переназначаются автоматически. Если адрес, зарезервированный нами за определенным клиентом, уже используется на другом компьютере, сначала освободите его, прекратив аренду или введя в командной строке компьютера-клиента **ipconfig /release;**
- клиенты непереходят на зарезервированныйадрес автоматически. Если в данный момент клиент владеет другим IP-адресом, для получения зарезервированного адреса он должен освободить старый адрес и послать новый запрос на DHCP-сервер.

Изменение свойств резервирования

1. В консоли DHCP откройте нужную область и щелкните папку Резервирование (Reservations).
2. Щелкните папку правой кнопкой и выберите Свойства (Properties). Измените свойства резервирования и щелкните OK.

Удаление аренды и резервирования

1. В консоли DHCP откройте нужную область и щелкните папку Арендованные адреса (Address Leases) или Резервирование (Reservations).
2. Щелкнув правой кнопкой аренду или резервирование, выберите Удалить (Delete).
3. Подтвердите удаление, щелкнув Да (Yes).

Аренда или резервирование будут удалены из DHCP, но клиент при этом может и не освободить IP-адрес, Чтобы заставить его сделать это, па компьютере клиента введите в командной строке **ipconfig** /release.

Резервное копирование и восстановление базы данных DHCP

Серверы DHCP храпят данные об аренде и резервировании DHCP в лапке *%SystemRoot%*\System32\dhcp.Ключевые файлы базы данных DHCP таковы:

- **DHCP.MDB** — основной файл БД сервера DHCP;
- **J50.LOG** — файл журналаопераций, служит длявосстановления незаконченных операций при отказе сервера;
- **J50.CHK** - файлконтрольной точки, применяемый для усечения файла журнала сервера DHCP;
- **Res1.log** — резервный файл журнала для сервера DHCP;
- Res2.log — резервный файл журнала длясервера DHCP;
- **Tmp.edb** —временный рабочийфайл для сервера DHCP;

Резервное копирование базы данных DHCP

В папке *%SystemRoot%*\System32\dhcpхранятся БД DHCP и данные о настройке DHCP. По умолчанию БД автоматически сохраняется каждые 60 минут. Чтобы произвести резервное копирование базы данных вручную, выполните следующие действия.

1. В консоли DHCP правой кнопкой мыши щелкните сервер, данные которого хотите сохранить, и выберите Архивировать (Backup).
2. В диалоговом окне Обзор папок (Browse for Folder) укажите папку, в которой будет храниться резервная копия базы данных DHCP, и щелкните OK.

Параметры реестра, отвечающие за размещение резервной копии и периодичность сохранения данных DHCP, а также другие параметры DHCP хранятся в разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters.

Следующие ключи реестра управляют базой данных и настройкой архивирования:

- **BackupDatabasePath** —задает положение базы данных DHCP Этот параметр устанавливается в диалоговом окне свойств сервера на вкладке Другие (Advanced) в поле База данных DHCP (Database Path);
- **DatabaseName** — задает имя главного файла базы данных DHCP. Значение по умолчанию — DHCP.mdb;
- **BackupInterval** —интервал между копированием в минутах. По умолчанию — 60 минут;
- **DatabaseCleanInterval** — время очистки элементов базы данных. По умолчанию — через каждые 60 минут.

Восстановление БД DHCP из резервной копии

1. При необходимости восстановите работающую копию папки *%SystemRoot%*\System32\dhcp\backup с ленточного накопителя или другого архивного устройства. Затем запустите консоль DHCP, правой кнопкой мыши щелкните сервер, который хотите восстановить, и выберите Восстановить (Restore).
2. В диалоговом окне Обзор папок (Browse for Folder) выберите папку, в которой хранится резервная копия базы данных DHCP, и щелкните OK.

Примечание Во время восстановления базы данных служба DHCP прекращает работу. Поэтому клиентам временно не удается связаться с сервером DHCP, чтобы получить IP-адреса,

Перенос БД DHCP на другой сервер

Если вам нужно пронести какое-либо масштабное обслуживание сервера, на котором работает DHCP, вы, вероятно, захотите временно перенести эту службу на другой сервер. Для этого необходимо выполнить несколько действий на обоих серверах. На целевом сервере сделайте следующее.

1. Установите DHCP и перезапустите сервер.

2. Остановите службу DHCP посредством консоли Службы (Services).
3. Удалите содержимое папки *%SystemRoot%*\System32\dhcp.

На исходном сервере сделайте следующее.

1. Остановите службу DHCP посредством консоли Службы (Services).
2. После остановки службы DHCP выключите ее, чтобы она более не запускалась.
3. Скопируйте все содержимое папки *%SystemRoot%*\System32\dhcp в аналогичную папку на целевом сервере.
4. Запустите службу DHCP на целевом сервере.

Восстановление БД DHCP с помощью утилиты JETPACK.EXE

Иногда целостность базы данных DHCP нарушается, и в системном журнале появляются сообщения об ошибках с DHCP-сервером в качестве источника и ссылками па ошибки базы данных Jet. Для определения и решения проблем базы данных предназначена утилита JETPACK.EXE.

1. Остановите службу DHCP посредством консоли Службы (Services).
2. Откройте окно командной строки.
3. Перейдите в папку базы данных DHCP. По умолчанию это *%SystemRoot%*\System32\dhcp.
4. Введите команду

```
jetpack  dhcp.mbd  dhcptempt.mbd
```

где dhcp.mbd — имя базы данных DHCP, а dhcptempt.mbd — имя временного файла, используемого утилитой Jetpack.

Утилита Jetpack выполнит следующие действия:

- проверит базу данных на предмет несоответствий и пр.;
- исправит любые ошибки несоответствия, записав все изменения во временный файл базы данных;
- сожмет базу данных, записав все изменения во временный файл базы данных;
- заменит исходный файл базы данных временным файлом и завершит работу.

Если утилите Jetpack не удалось восстановить базу данных, восстановите ее самостоятельно из резервной копии или воссоздайте посредством службы DHCP.

Регенерация БД DHCP средствами DHCP-сервера

В редких случаях восстановить базу данных не удается ни с помощью программы Jetpack.exe, ни из резервной копии (см. раздел «Восстановление БД DHCP из резервной копии»). Если это случилось или вы просто собираетесь создать БД DHCP «с нуля», выполните следующие действия.

1. Остановите службу DHCP посредством консоли Службы (Services).
2. Удалите содержимое папки *%SystemRoot%*\System32\dhcp. Чтобы не дать серверу восстановиться из предыдущей резервной копии, удалите и ее содержимое.

Примечание Не удаляйте файлы БД, если повреждены ключи реестра, связанные с DHCP. Они должны быть доступны для восстановления БД DHCP.

3. Перезапустите **DHCP-сервер.**
4. Никакая информация об арендованных и зарезервированных адресах в консоли DHCP не *отображается.* Чтобы восстановить активные аренды в каждой области, следует согласовать области сервера. Подробнее — в следующем разделе.
5. Чтобы предотвратить конфликты, вызванные уже заключенными соглашениями об аренде, включите определение конфликтов адресов на следующие несколько дней, как описано в разделе «Предотвращение конфликтов IP-адресов».

Воссоздание арендованных и зарезервированных адресов

В процессе согласования БД выполняется сверка арендованных и зарезервированных адресов с информацией в БД DHCP на сервере. Если между сведениями в реестре Windows и базе данных сервера DHCP обнаружены несоответствия, вы можете выбрать и согласовать любые рассогласованные элементы. После этой операции DHCP возвращает IP-адрес его изначальному владельцу или создает для этого адреса временное резервирование. Когда истечет срок аренды, адрес возвращается в пул для последующего использования.

Вы вправе согласовывать области как по отдельности, так и все сразу. Чтобы согласовать одну область, выполните следующие действия.

1. В консоли DHCP правой кнопкой мыши щелкните область, с которой хотите работать, и выберите Согласование (Reconcile).
2. В диалоговом окне Согласовать (Reconcile) щелкните кнопку Проверить (Verify). В окне отобразятся обнаруженные несоответствия.
3. Выделите отображенные адреса и щелкните Согласовать (Reconcile), чтобы исправить несоответствия.
4. Если несоответствия не обнаружены, щелкните OK.

Чтобы согласовать все области на сервере, выполните следующие действия.

1. В консоли DHCP правой кнопкой мыши щелкните нужный сервер и выберите Согласование всех областей (Reconcile All Scopes).
2. В диалоговом окне Согласование всех областей (Reconcile All Scopes) щелкните кнопку Проверить (Verify). В окне отобразятся обнаруженные несоответствия.
3. Выделите отображенные адреса и щелкните Согласовать (Reconcile), чтобы исправить несоответствия.
4. Если несоответствия не обнаружены, щелкните **OK.**

Глава 19

Поддержка WINS

Служба имен Интернета для Windows (Windows Internet Naming Service, WINS) разрешает имена компьютеров в IP-адреса, т. с. по имени компьютера определяет его IP-адрес, по которому компьютеры в сети Microsoft находят друг друга и обмениваются информацией. WINS необходима для поддержки версий Windows, предшествующих Windows 2000, и старых программ, использующих NetBIOS поверх TCP/IP, например для поддержки утилиты командной строки NET. Если у вас в сети нет ранних версий Windows и требующих совместимости с ними приложений, WINS вам не понадобится.

Разрешение имен WINS и передачу информации между компьютерами обеспечивает интерфейс прикладного программирования (application programming interface, API) NetBIOS. Он содержит набор команд, с помощью которых приложения получают доступ к службам сеансового уровня. Обычно в сетях Windows используются расширенные варианты NetBIOS: NetBEUI (NetBIOS Enhanced User Interface) и NetBIOS поверх TCP/IP (NetBIOS over TCP/IP, NBT). Мы рассмотрим WINS и NBT.

В Windows Server 2003 WINS автоматически не устанавливается. Чтобы установить ее, вам придется выполнить следующие действия.

1. Откройте меню Администрирование (Administrative Tools) и выберите команду Мастер настройки сервера (Configure Your Server).
2. Дважды щелкните Далее (Next).
3. Выделите роль WINS-сервер (WINS Server) и дважды щелкните Далее (Next). WINS-сервер будет установлен на вашем компьютере. При необходимости вставьте в дисковод установочный компакт-диск Windows Server 2003.

4. Щелкните Готово (Finish) и закройте консоль Управление данным сервером (Manage Your Server).

Теперь служба WINS будет автоматически запускаться при каждой загрузке системы. Если этого не происходит, запустите ее вручную. Подробнее — в разделе «Запуск и остановка WINS-сервера».

Примечание Сервер WINS должен иметь статический IP-адрес,

Знакомство с WINS и NetBIOS поверх TCP/IP

Служба WJNS с максимальной эффективностью работает в сетях «клиент — сервер»: клиент WINS посылает WINS-серверу запрос на разрешение имени, а WINS-сервер обрабатывает запрос и отвечает на него. Для передачи запросов WINS и другой информации компьютеры используют NetBIOS. Поддержка NetBIOS поверх TCP/IP устанавливается автоматически при установке стека протоколов TCP/IP на клиенты или серверы сетей Microsoft. NetBIOS поверх TCP/IP — это служба сеансового уровня, позволяющая приложениям Net BIOS работать через стек TCP/IP.

Для разрешения имен компьютеров в IP-адреса в приложениях NetBIOS применяются WINS или локальный файл LMHOSTS. В более ранних по сравнению с Windows 2000 сетях служба WINS являлась основной службой разрешения имен. В сетях Windows Server 2003 эта роль отдана DNS, а WINS обеспечивает в устаревших системах просмотр списка ресурсов сети и занимается поиском ресурсов NetBIOS для систем на базе Windows 2000, Windows XP и Windows Server 2003.

Настройка клиентов и серверов WINS

Настройка клиента WINS заключается в указании IP-адресов WINS-серверов сети. По этим IP-адресам клиент связывается с ними. даже если серверы располагаются в других подсетях. Клиенты также способны связываться друг с другом, запрашивая IP-адреса компьютеров внутри сегмента локальной сети посредством широковещательных запросов. Использовать этот метод для разрешения имен компьютеров в IP-адреса могут также любые не WINS-клиенты, поддерживающие данный тип широковещательных сообщений.

Связываясь с WINS-сервером, клиент устанавливает сеанс. Этот процесс можно разделить на три ключевых этапа.

- Регистрация имени — клиент сообщает серверу имя своего компьютера и его IP-адрес и просит включить эту информацию в БД WINS. Если имя и IP-адрес не используются другим компьютером в сети, WINS-сервер принимает запрос и регистрирует клиента в БД WINS.
- Обновление имени — клиент использует имя лишь в течение определенного периода, называемого временем аренды. Каждому клиенту сообщается интервал обновления, в течение которого аренда должна быть обновлена. За это время клиент должен перерегистрироваться на WINS-сервере.
- Освобождение имени — если клиент не обновляет аренду, зарегистрированное имя освобождается, что позволяет другим системам в сети использовать то же имя компьютера или IP-адрес. Имя также освобождается при завершении работы WINS-клиента.

Примечание О настройке WINS-клиента рассказано в главе 16. О настройке WINS-сервера читайте в разделе «Настройка WINS-сервера» этой главы.

Методы разрешения имени

Соединившись с WINS-сервером, клиент вправе обращаться с запросами к службе разрешения имен. Метод разрешения имен компьютеров в IP-адреса зависит от настройки сети. Всего таких методов четыре.

- **B-узел** (broadcast node, широковещательный узел) разрешает имена в IP-адреса посредством широковещательных сообщений. Компьютер, которому нужно разрешить имя, рассылает по локальной сети широковещательное сообщение с запросом IP-адреса по имени компьютера.
- **P-узел** (point-to-point node, узел «точка — точка») разрешает имена в IP-адреса с помощью WINS-сервера. Когда клиенту нужно разрешить имя компьютера в IP-адрес, клиент отправляет серверу имя, а тот в ответ посылает адрес.
- **M-узел** (mixed node, смешанный узел) комбинирует запросы b- и p-узла. WINS-клиент смешанного типа сначала пытается применить широковещательный запрос, а в случае неудачи обращается к WINS-серверу. Поскольку разрешение имени начинается с широковещательного запроса, m-узел загружает сеть широковещательным трафиком в той же степени, что и b-узел.

- **H-узел (hybrid node, гибридный узел)** также комбинирует запросы b-узла и p-узла, но при этом сначала используется запрос к WINS-серверу и лишь в случае неудачи начинается рассылка широковещательного сообщения. Поэтому в большинстве сетей h-узлы работают быстрее. По умолчанию для разрешения имен WINS применяется именно этот метод.

Клиенты Windows используют для разрешения имен метод p-узла, если в сети есть WINS-серверы, и метод b-узла, если таких серверов нет. Кроме того, для разрешения имен применяются DNS и локальные файлы LMHOSTS и HOSTS. О работе с DNS рассказано в главе 20.

Совет Если в вашей сети применяется DHCP (глава 18), вы должны указать метод разрешения имен для клиентов DHCP. Для этого задайте параметр области или DHCP-сервера за номером 046 — Тип узла WINS/NBT (WINS/NBT Node Type). Наивысшую производительность и наименьшую нагрузку на сеть обеспечивает метод h-узла.

Консоль WINS

Для управления параметрами WINS-сервера предназначена консоль WINS.

Знакомство с консолью WINS

Главное окно консоли WINS разделено на две панели (рис. 19-1). В левой перечислены WINS-серверы в домене, упорядоченные по их IP-адресам, в том числе и локальный компьютер, если он является WINS-сервером.

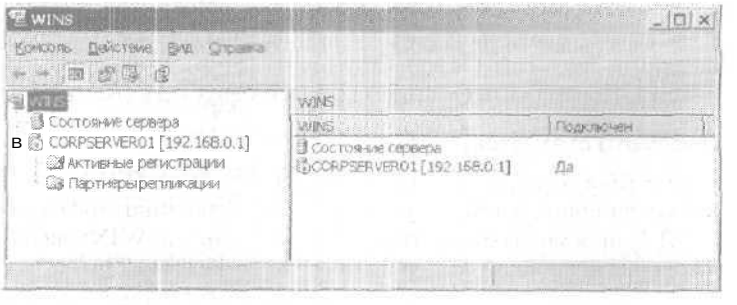


Рис. 19-1. Для настройки WINS-сервера служит консоль WINS

Дважды щелкнув запись в левой панели, вы раскроете список, содержащий папки Активные регистрации (Active Registrations) и Партнеры репликации (Replication Partners). В первой отображается информация о зарегистрированных именах компьютеров. Во второй содержится сводная информация о WINS-серверах, с которыми данный сервер обменивается регистрационной информацией.

Добавление WINS-сервера на консоль WINS

Если в консоли WINS нет WINS-сервера, который вы хотите настроить, выполните следующие действия.

1. Щелкните правой кнопкой элемент WINS в дереве консоли и выберите Добавить сервер (Add Server).
2. Введите IP-адрес или имя WINS-сервера, которым собираетесь управлять.
3. Щелкните OK.

Примечание Доступ к консоли WINS открывается из консоли Управление компьютером (Computer Management). Запустите ее, подключитесь к серверу, которым хотите управлять, затем раскройте узел Службы и приложения (Services and Applications) и выберите WINS.

Запуск и остановка WINS-сервера

Серверами WINS управляют с помощью одноименной службы. Как и любую другую, вы вправе ее запустить, отключить, приостановить и перезапустить посредством узла Службы (Services) консоли Управление компьютером (Computer Management) или из командной строки. Кроме того, службой WINS можно управлять из консоли WINS. Щелкните правой кнопкой сервер, которым хотите управлять, выберите Все задачи (All Tasks), а затем щелкните Запустить (Start), Остановить (Stop), Приостановить (Pause), Продолжить (Resume) или Перезапустить (Restart).

Просмотр статистики сервера

Статистика сервера — это сводная информация о WINS, которая может пригодиться для управления и диагностики этой службы. Для просмотра статистики сервера в консоли WINS щелкните правой кнопкой сервер и выберите Отобразить статистику сервера (Display Server Statistics). В открывающемся по этой команде окне содержится следующая информация:

- **Время запуска сервера (Server Start Time) — время запуска** службы WINS;
- **База данных проинициализирована (Database Initialized) — время инициализации БД WINS на** сервере;
- Последняя очистка статистики (Statistics Last Cleared) — время, когда в последний раз обнулялись статистические данные на сервере;
- Последняя репликация по расписанию (Last Periodic Replication) — время, когда БД WINS была в последний раз реплицирована по истечении временного интервала репликации;
- **Последняя репликация вручную (Last Manual Replication) —** время, когда БД WINS была в последний раз реплицирована **администратором;**
- **Последняя репликация изменения состояния сети (Last Net Update Replication)** — время, когда БД WINS была в последний раз реплицирована на основании полученного из сети запроса;
- **Последнее репликация изменения адреса (Last Address Change** Replication) — время, когда БД WINS была в последний раз реплицирована на основании сообщения об изменении адреса;
- Общее число запросов (Total Queries) — общее число запросов, принятых сервером с момента последнего запуска. В поле Запись найдена (Records Found) показано число успешно разрешенных запросов, и поле Запись не найдена (Records not Found) — число неудовлетворенных запросов;
- Всего освобождено (Total Releases) — общее число сообщений о том, что приложение NetBIOS освободило зарезервированное имя и отключилось. В поле Запись найдена (Records Found) показано число успешно выполненных освобождений, в поле Запись не найдена (Records not Found) — число неудачных освобождений;
- Уникальных регистрации (Unique Registrations) — общее количество полученных и удовлетворенных сообщений от клиентов WINS о регистрации имени. В поле Конфликты (Conflicts) показано число конфликтов имен для каждого уникального имени компьютера, в поле Обновления (Renewals) - число обновлений для каждого уникального имени компьютера;

- **Регистрации группы (Group Registrations)** — общее количество полученных и удовлетворенных сообщений от групп о регистрации имени. В поле Конфликты (Conflicts) показано число конфликтов для имен групп, в поле **Обновления** (Renewals) — число обновлений для **имен** групп;
- **Всего получено регистрации (Total Registrations)** — общее количество сообщений о регистрации имени, **принятых** от клиентов WINS;
- **Последняя автоматическая очистка (Last Periodic Scavenging)** — время последней очистки **по** причине истечения интервала обновления, заданного в конфигурации WINS-сервера;
- **Последняя очистка вручную (Last Manual Scavenging)** — время последней очистки по запросу администратора;
- **Время последнего окончания очистки (Last Extinction Scavenging)** — время последней очистки но причине истечения интервала устаревания, заданного в **конфигурации** WINS-сервера;
- **Время последней проверки очистки (Last Verification Scavenging)** — время последней очистки по причине истечения интервала проверки, заданного R конфигурации WINS-ссрвера;
- **Партнер WINS-сервера (WINS Partner) — число** удачных репликаций и неудачных попыток установления **связи** с партнерами WINS.

Настройка WINS-сервера

Когда вы устанавливаете WINS-сервер, он настраивается со стандартными параметрами. **Чтобы** изменить их, выполните следующие действия.

1. В консоли WINS щелкните правой кнопкой сервер, с которым хотите работать, и выберите Свойства (Properties). Откроется диалоговое окно, показанное на рис. 19-2.
2. **Измените** значения параметров на вкладках Общие (General), Интервалы **(Intervals),** Проверка базы данных (Database Verification) и Дополнительно **(Advanced).** Подробнее — в следующих **разделах.**
3. Щелкните **OK.**

Рис. 19-2. Окно свойств WINS-сервера

Обновление статистики WINS

По умолчанию статистика регистрации адресов и репликации в консоли WINS обновляется каждые 10 минут. Вот как изменить этот интервал или отказаться от автоматического обновления.

1. В консоли WINS щелкните правой кнопкой сервер, с которым хотите работать, и выберите Свойства (Properties).
2. Перейдите на вкладку Общие (General).
3. Установите флажок Автоматически обновлять статистику каждые (Automatically update statistics every) и введите значение интервала в часах, минутах и секундах.
4. Для остановки автоматического обновления сбросьте флажок Автоматически обновлять статистику каждые (Automatically update statistics every) и щелкните OK.

Управление регистрацией, обновлением и освобождением имен

Имена компьютеров регистрируются в БД WINS на период *аренды* (lease). Параметрами аренды управляют, задавая интервалы обновления, устаревания и проверки.

1. В консоли WINS щелкните прапой кнопкой сервер, с которым хотите работать, и выберите Свойства (Properties).
2. Перейдите на вкладку Интервалы (Intervals), показанную на рис. 19-3. На ней задаются такие параметры:

- **Интервал обновления (Renewal Interval)** — интервал, в течение которого клиент WINS должен обновить имя своего компьютера (период аренды). Обычно клиенты пытаются выполнить обновление, когда проходит 50% периода аренды. Минимальное значение — 40 минут. Значение по умолчанию — 6 дней, при этом клиенты пытаются возобновлять аренду каждые 3 дня;
- **Интервал удаления (Extinction Interval)** — интервал, по истечении которого имя компьютера считается устаревшим. Устаревшим имя компьютера считается после его освобождения. Это значение должно быть больше или равно меньшему из двух значений: интервал обновления или 4 дня;
- **Тайм-аут устаревания (Extinction Timeout)** — задает интервал, в течение которого устаревшее имя компьютера может быть физически удалено из БД WINS. Значение по умолчанию — 4 дня;
- **Интервал проверки (Verification Interval)** — интервал, по истечении которого WINS-сервер должен проверить старые имена, которыми он не владеет. Если имена неактивны, они удаляются. Минимальное значение — 24 дня. Обычно в эту категорию попадают имена компьютеров, зарегистрированные на другом WINS-сервере и потому имеющие другого владельца.

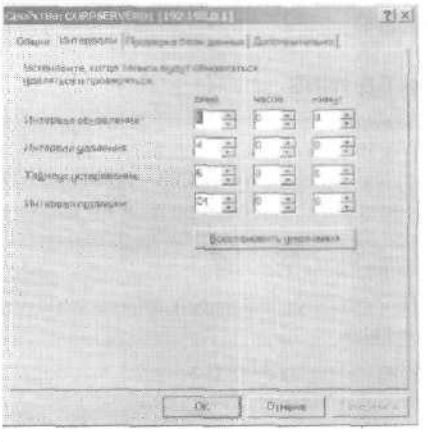


Рис. 19-3. Настройте интервалы согласно требованиям вашей сети

Совет Чтобы лучше понять смысл этих интервалов, представьте их как этапы жизни имени в БД WINS. Интервал обновления управляет обновлением аренды действующих имен. Если имя не обновлено, оно помечается как устаревшее, и в силу вступает интервал удаления. Тайм-аут устаревания определяет, когда устаревшие имена исключаются из БД. Если вы задали интервал обновления 24 часа, интервал удаления — 48 часов и тайм-аут устаревания — 24 часа, потребуется до 96 часов, чтобы запись была удалена из БД WINS.

Запись событий WINS в журналах Windows

События WINS автоматически записываются в системный журнал. Вы не вправе совсем выключить эту возможность. С другой стороны, допускается временно задать запись в журнал более подробных сведении. Вот как это делается.

1. В консоли WINS щелкните правой кнопкой сервер, с которым хотите работать, и выберите Свойства (Properties).
2. Перейдите на вкладку Дополнительно (Advanced) и установите переключатель Вести запись подробного протокола в журнале событий Windows (Log detailed events to the Windows event logs).

Примечание Подробное протоколирование в активной сети существенно повышает нагрузку на WINS-сервер. Поэтому включайте подробный протокол только на время тестирования или устранения неисправностей.

Настройка номера версии БД WINS

Номер версии для БД WINS обновляется автоматически при внесении изменений. Если БД WINS повреждена и вы хотите восстановить ее, получите доступ к основному WINS-серверу и задайте значение номера версии выше, чем номера версий на всех удаленных партнерах. Так вы добьетесь передачи партнерам самой последней информации из базы данных.

Чтобы просмотреть или изменить текущий номер версии, выполните следующие действия.

1. В консоли WINS разверните узел нужного сервера, щелкните правой кнопкой элемент Активные регистрации (Active Registrations) и выберите Отобразить записи (Display Records).

2. На вкладке Владельцы записи (Record Owners) в столбце Наибольший номер (Highest ID) отображается наивысший номер версии для каждого сервера.
3. Запомните значение наивысшего номера версии и щелкните Отмена (Cancel).
4. Щелкните правой кнопкой запись основного WINS-сервера в дереве консоли и выберите Свойства (Properties).
5. На вкладке Дополнительно (Advanced) введите новое шестнадцатеричное значение в поле Начальный номер версии (Starting Version ID). Оно должно быть больше, чем значение, которое вы запомнили ранее. Щелкните OK.

Настройка пакетной обработки регистрации имен

Иногда в крупных сетях на WINS-сервере одновременно пытаются зарегистрироваться несколько сотен клиентов WINS. В этом случае WINS-сервер может переключиться в режим пакетной обработки, в котором он дает положительный ответ на запросы клиентов еще до того, как обработает их и внесет изменения в БД WINS.

При необходимости вы вправе изменить порог включения режима пакетной обработки, чтобы привести его в соответствие с размером сети и мощностью сервера. По умолчанию этот режим включается, если в очереди на обработку находятся более 500 регистрации и запросов имен. Новое значение порога задается следующим образом.

1. В консоли WINS щелкните правой кнопкой сервер, с которым хотите работать, и выберите Свойства (Properties).
2. На вкладке Дополнительно (Advanced) установите флажок Включить обработку пакетов (Enable Burst Handling), а затем настройте обработку пакетов с помощью переключателей:
   - Слабую (Low) — задаст порог в 300 регистраций и запросов имен;
   - Среднюю (Medium) — задает порог в 500 регистрации и запросов имен (по умолчанию);
   - **Высокую (High)** — задаст порог в 1000 регистрации и запросов имен;
   - **Особую (Custom)** — позволяет задать порог между 50 и 5000 вручную.

3. Щелкните OK.

Примечание Максимальное число регистрации и запросов имен, которое WINS-сервер способен принять одновременно, — 25 000. Если этот предел превышен, сервер прекращает прием запросов.

Сохранение и восстановление параметров WINS

Задав параметры WINS, сохраните их, чтобы затем иметь возможность восстановить их на WINS-сервере. Для сохранения параметров введите в командной строке

```
netsh WINS dump >> winsconfig.dmp
```

Здесь winsconfig.dmp — имя сценария настройки, который вы хотите создать. После создания этого сценария вы можете восстановить параметры, набрав

```
netsh exec winsconfig.dmp
```

Совет Этот способ также годится для настройки еще одного WINS-сервера с теми же параметрами: скопируйте сценарий настройки в папку на целевом компьютере и выполните его.

Настройка репликации БД WINS

WINS-серверы способны реплицировать базы друг друга, чтобы они всегда соответствовали текущему состоянию сети и отражали изменения в ней. Репликацию можно выполнять как автоматически, так и вручную.

Репликацию осуществляют извещающие и опрашивающие партнеры. *Извещающий партнер* (push partner) — это WINS-сервер, который уведомляет другие WINS-серверы об изменениях в сети, а *опрашивающий партнер* (pull partner) — это WINS-сервер, который запрашивает реплики с извещающего партнера. Вы вправе настроить любой WINS-сервер на исполнение роли извещающего или опрашивающего партнера или обеих ролей сразу.

Для повышения надежности репликации настройте постоянное соединение между партнерами. Партнеры сохраняют такое соединение в открытом состоянии, даже когда оно простаивает. Это позволяет WINS-серверам быстро и эффективно реплицировать изменения по всей сети.

Настройка стандартных параметров репликации

Перед созданием партнеров по репликации нужно задать параметры по умолчанию. Они используются для настройки новых извещающих и опрашивающих партнеров.

Назначение общих параметров

Общие параметры управляют репликацией **и миграцией. Чтобы** задать **их, выполните** следующие **действия.**

1. Раскройте в консоли WINS узел сервера, с которым хотите работать.
2. Правой кнопкой щелкните элемент Партнеры репликации (Replication Partners) и выберите Свойства (Properties).
3. На вкладке General (Общие) установите или сбросьте флажок Репликация только с партнерами (Replicate only with partners). Если этот флажок сброшен, вы вправе вручную проводить репликацию с любым WINS-сервером в сети.
4. Для не WINS-клиентов сети в БД создается статическая привязка, которая позволяет все-таки зарегистрировать их имела в WINS. Если несколько компьютеров могут использовать одни и те же IP-адреса, вы вправе настроить сервер так, чтобы WINS перезаписывал существующие записи информацией о новой регистрации. Для этого установите флажок Перезапись уникальных статических сопоставлений на этом сервере (Overwrite unique static mappings at this server). Щелкните OK.

Назначение стандартных параметров извещающей репликации

По умолчанию партнеры по репликации настраиваются как для извещающей, так и для опрашивающей репликации. Для автоматических обновлений обычно используется не извещающая, а опрашивающая репликация. Но поскольку партнеры настроены для обоих видов репликации, вы можете запускать извещающую репликацию вручную.

Чтобы извещающая репликация запускалась автоматически, выполните следующие действия.

1. В консоли WINS раскройте узел сервера, с которым хотите работать.
2. Правой кнопкой щелкните элемент Партнеры репликации (Replication Partners) и выберите Свойства (Properties).

3. Перейдите на вкладку Извещающая репликация (Push Replication), показанную на рис. 19-4.
4. По умолчанию извещающая репликация не выполняется ни при запуске WINS, ни при изменениях адресов. Чтобы изменить этот параметр, установите флажки При запуске службы (At service startup), При изменении адреса (When address changes) или оба сразу.
5. Параметр Число изменений в номере версии до репликации (Number of changes in version ID before replication) определяет количество регистрации и изменений, которые должны произойти до репликации БД. Этот счетчик накапливает только локальные изменения и не учитывает изменения, присланные другими партнерами. Если данный параметр равен 0, извещающая репликация не выполняется.
6. По умолчанию извещающие партнеры используют постоянные соединения. Если вас это не устраивает, сбросьте флажок Для распространения репликации среди партнеров использовать постоянные подключения (Use persistent connections for push replication partners). Щелкните OK.

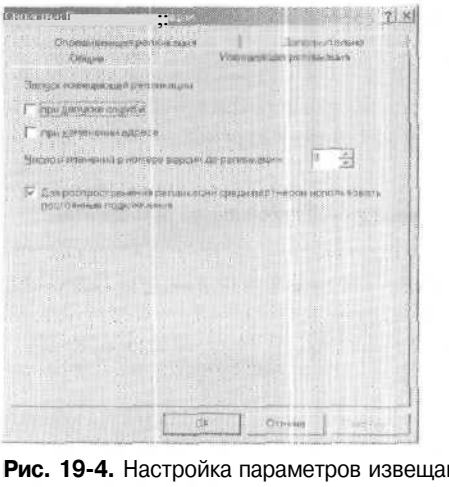


Рис. 19-4. Настройка параметров извещающей репликации

Назначение стандартных параметров **опрашивающей репликации**

Опрашивающая репликация — стандартный механизм репликации для партнеров, поэтому большая часть ее параметров назначается автоматичсски. Если вы предпочитаете использовать

извещающую репликацию, включите ее автоматический запуск на вкладке Извещающая репликация (Push Replication) и отключите стандартные параметры опрашивающей репликации на вкладке Опрашивающая репликация (Pull Replication).

Параметры опрашивающей репликации изменяются так.

1. В консоли WINS раскройте узел сервера, с которым хотите работать.
2. Правой кнопкой щелкните элемент Партнеры репликации (Replication Partners) и выберите Свойства (Properties).
3. Перейдите на вкладку Опрашивающая репликация (Pull Replication), показанную на рис. 19-5.

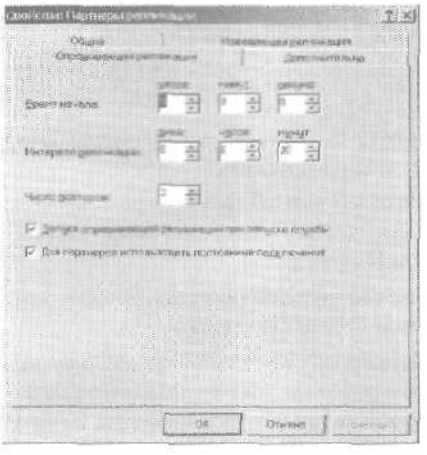


Рис. 19-5. Здесь задаются параметры опрашивающей репликации

4. В поле Время начала (Start time) задайте время, когда должна начинаться репликация.
5. В поле Интервал репликации (Replication interval) задайте период запуска репликации.
6. В поле Число повторов (Number of retries) задайте, сколько раз WINS-сервер должен пытаться соединиться с опрашивающим партнером, если первая попытка оказалась неудачной.
7. По умолчанию опрашивающая репликация запускается при запуске WINS-сервера. Для изменения такого поведения сбросьте флажок Запуск опрашивающей репликации при запуске службы (Start pull replication at service startup).

После этого опрашивающая репликация будет запускаться только во время, заданное в поле Время начала (Start time).

8. По умолчанию опрашивающие партнеры используют постоянные соединения. Если вас это не устраивает, сбросьте флажок Для партнеров использовать постоянные подключения (Use persistent connections for pull replication partners) и щелкните OK.

Создание извещающих и опрашивающих партнеров

В сети с несколькими WINS-серверами для репликации баз данных WINS необходимы извещающие и опрашивающие партнеры. Их начальная настройка осуществляется на основе стандартных параметров репликации, заданных на WINS-сервере. Настройте репликацию отдельно для каждого WINS-сервера в сети.

Чтобы сделать WINS-сервер извещающим или опрашивающим партнером, выполните следующие действия.

1. В консоли WINS раскройте узел сервера, для которого будете настраивать партнеры по репликации.
2. Правой кнопкой щелкните элемент Партнеры репликации (Replication Partners) и выберите Создать партнера по репликации (New Replication Partner).
3. Введите имя или IP-адрес партнера по репликации или найдите *ею с* помощью кнопки Обзор (Browse).
4. Щелкните OK. Если *с* сервером удается связаться, автоматически создается запись о репликации со стандартными параметрами. Сервер настраивается, как извещающий и опрашивающий партнер,

Изменение типа репликации и параметров партнеров

Стандартные параметры используются для начальной инициализации партнеров по репликации. Эти параметры для каждого партнера всегда можно изменить.

1. В консоли WINS раскройте узел сервера, для которого вы будете настраивать партнеры по репликации.
2. В дереве консоли щелкните элемент Партнеры репликации (Replication Partners). На правой панели будут показаны текущие партнеры по репликации для данного сервера.
3. Правой кнопкой щелкните запись нужного партнера по репликации и выберите Свойства (Properties).

4. Перейдите на вкладку Дополнительно (Advanced), показанную на рис. 19-6.

Рис. 19-6. Здесь изменяют **стандартные** параметры репликации для партнера

5. В списке Тип партнера репликации (Replication Partner Type) выберите тип репликации для этого партнера. По умолчанию большинство клиентов настроены как для извещающей, так и для опрашивающей репликации.
6. Задайте остальные параметры, руководствуясь сведениями из предыдущих разделов.
7. Щелкните OK.

Запуск репликации БД

Иногда требуется немедленно обновить БД WINS на партнерах по репликации. Сделать это можно несколькими способами:

- **Репликация со всеми партнерами** — щелкните правой кнопкой папку Партнеры репликации (Replication Partners) на сервере, БД которого хотите реплицировать, и выберите Запустить репликацию (Replicate Now);
- **Извещающая репликация со всеми партнерами** — щелкните правой кнопкой сервер, БД которого хотите реплицировать, и выберите Запустить извещающую репликацию (Start Push Replication);

- Опрашивающая репликация со всеми партнерами — щелкните правой кнопкой сервер, БД которого хотите реплицировать, и выберите Запустить опрашивающую репликацию (Start Pull Replication);
- Извещающая или опрашивающая репликация с отдельными партнерами — в консоли WINS щелкните панку Партнеры репликации (Replication Partners) на сервере, БД которого хотите реплицировать. Затем щелкните правой кнопкой партнер, с которым хотите реплицировать БД, и выберите Запустить извещающую репликацию (Start Push Replication) или Запустить опрашивающую репликацию (Start Pull Replication).

Управление БД WINS

Для поддержания работоспособности службы разрешения имен в сети вы должны активно управлять базой данных WINS.

Просмотр привязок в БД WINS

Выделите в дереве консоли WINS элемент Активные регистрации (Active Registrations). В правой панели отобразятся записи БД WINS, выбранные вами для просмотра. В начале каждой строки вы увидите один из двух значков: значок с одним компьютером свидетельствует, что данная привязка создана для уникального имени, значок с парой компьютеров — что данная привязка создана для группы, домена, Интернет-группы или многоадресной записи. В строках приведены следующие сведения:

- Имя записи (Record Name) — полное NetBIOS-имя компьютера, группы или службы, зарегистрированных в БД;
- Тип (Type) — тин записи, ассоциированный с привязкой, например 00h Workstation;
- IP-адрес (IP Address) — IP-адрес, ассоциированный с привязкой;
- Состояние (State) — статус записи, например активная или освобожденная;
- Статическая (Static) — значок «X» в этом столбце означает статическую привязку;
- Владелец (Owner) — IP-адрес WINS-сервера, владеющего записью;
- Версия (Version) — номер версии БД, в которой создана запись;

- **Истечение срока (Expiration)** — время и дата, когда истекает срок действия привязки (статическая привязка действует без ограничений по времени).

Очистка БД WINS

Вы должны периодически удалять из БД WINS старые имена компьютеров. Этот процесс называется *очисткой* (scavenging). Он запускается автоматически в соответствии с интервалом удаления и задержкой удаления, заданными в окне свойств сервера.

Чтобы запустить очистку вручную, выделите в консоли нужный WINS-сервер и выберите в меню Действие (Action) команду Очистить базу данных (Scavenge Database).

Проверка непротиворечивости БД WINS

В больших сетях с несколькими WINS-серверами БД разных серверов иногда не синхронизированы друг с другом. Для поддержания работоспособности WINS необходимо периодически проверять согласованность БД. Существуют два вида такой проверки: проверка согласованности БД и проверка согласованности номеров версий.

В первом случае WINS проверяет целостность записей БД на WINS-серверах. Для проверки согласованности выделите в консоли WINS нужный сервер и выберите в меню Действие (Action) команду Проверить согласованность базы данных (Verity Database Consistency).

Во втором случае WINS сверяет локальные записи с записями на других WINS-серверах. Для проверки согласованности номеров версий выделите в консоли нужный сервер и щелкните в меню Действие (Action) команду Проверить согласованность номеров версий (Verify Version ID Consistency).

Чтобы настроить автоматическую проверку согласованности БД, выполните следующие действия.

1. В консоли WINS щелкните правой кнопкой нужный сервер и выберите Свойства (Properties).
2. На вкладке Проверка базы данных (Database Verification) установите флажок Проверять непротиворечивость базы данных каждые (Verify database consistency every), как показано на рис. 19-7. Введите интервал времени для проверки.

Рис. 19-7. Настройте автоматическую проверку согласованности

3. В поле Начать проверку в (Begin verifying at) введите время, в которое должна начаться проверка.
4. При необходимости измените значение в поле Максимальное число записей, проверяемых за каждый период (Maximum number of records verified each period).
5. Вы вправе сверять записи с серверами-владельцами или со случайно выбранными партнерами. Случайный выбор лучше применять в большой сети, где немыслимо проверить все лап иси за один раз. Чтобы сверить записи только с серверами-владельцами, установите переключатель С сервером-владельцем (Owner Servers).
6. Щелкните OK.

Совет Учитывайте, что проверка требует много системных и сетевых ресурсов. Как правило, стоит задать интервал проверки, равный 24 часам, а затем ввести в поле Начать проверку в (Begin verifying at) какой-нибудь нерабочий час, например 2 часа, чтобы служба WINS проверяла БД ежедневно в 2 часа ночи.

Архивирование и восстановление БД WINS

Администраторы часто забывают о двух задачах, которые необходимо решать на WINS-сервере: резервном копировании и восстановлении БД WINS.

Настройка автоматического резервного копирования

Резервное копирование БД WINS по умолчанию не выполняется, поэтому в случае сбоя вы ее не восстановите. Для защиты БД от сбоев настройте автоматическое резервное копирование или периодически архивируйте ее вручную. Чтобы подготовить WINS к автоматическому резервному копированию, выполните следующие действия.

1. В консоли WINS щелкните правой кнопкой нужный сервер и выберите Свойства (Properties).
2. На вкладке Общие (General) в поле Путь резервной копии по умолчанию (Default backup path) введите путь к папке, которую хотите использовать для резервного копирования.
3. Установите флажок Архивировать базу данных WINS при завершении работы (Backup database during server shutdown).
4. Щелкните OK. Автоматическое архивирование будет выполняться каждые 3 часа. По умолчанию архив размещается в папке *%WinDir%*\System32\Wins.

Восстановление БД

1. В консоли WINS выберите сервер, с которым хотите работать.
2. В меню Действие (Action) выберите Все задачи (AH Tasks) и Остановить (Stop).
3. В меню Действие (Action) выберите Восстановить базу данных (Restore Database).
4. В окне Обзор папок (Browse for Folder) найдите подпапку wins_bak с самой свежей резервной копией и щелкните OK.
5. Если восстановление пройдет удачно, БД WINS вернется в состояние на момент создания копии. В меню Действие (Action) выберите Все задачи (All Tasks) и Запустить (Start).

Очистка WINS и запуск со свежей базой данных

Если восстановить WINS из резервной копии не удалось, очистите все записи и журналы WINS и начните составление БД заново.

1. В консоли WINS щелкните правой кнопкой нужный сервер и выберите Свойства (Properties).
2. На вкладке Дополнительно (Advanced) найдите путь к базе данных и запомните его, а затем щелкните OK. чтобы закрыть окно свойств.

3. В меню Действие (Action) выберите Все задачи (All Tasks) и Остановить (Stop), чтобы остановить сервер.
4. Удалите все файлы в папке БД WINS средствами Проводника (Windows Explorer).
5. В консоли WINS правой кнопкой щелкните восстанавливаемый сервер, раскройте подменю Все задачи (All Tasks) и выберите Запустить (Start).

Глава 20

Оптимизация DNS

В этой главе обсуждаются методики настройки и управления DNS в сети. DNS — служба разрешения имен, сопоставляющая имена компьютеров с IP-адресами. Посредством DNS полное имя узла, например *omega.microsoft.com,* разрешается в IP-адрес, по которому компьютеры находят друг друга. DNS работает через стек протоколов TCP/IP и способна интегрироваться с WINS, DHCP и службой каталогов Active Directory. Полная интеграция с этими сетевыми функциями позволяет оптимизировать DNS для доменов Windows Server 2003.

Знакомство с DNS

Посредством DNS группы компьютеров организуются в *домены,* которые в свою очередь выстроены в иерархическую структуру. Эта структура может охватывать как сеть предприятия, так и глобальную сеть — Интернет. Разные уровни иерархии соответствуют индивидуальным компьютерам, доменам организаций и доменам верхнего уровня. В полном имени узла *omega.microsoft.com, omega* представляет собой имя индивидуального компьютера, *microsoft* — домен организации, а *com* — домен верхнего уровня.

Домены верхнего уровня располагаются в *основании* иерархии DNS и поэтому называются ***корневыми*** (root domains). Их назначают по географическому расположению, по типу организации или по се назначению. Обычные домены типа *microsoft.com* также называют *родительскими* (parent). Родительские домены разделяются на *дочерние* (child) поддомены, соответствующие группам или отделам в пределах организации. Например, полное доменное имя компьютера в отделе кадров может выглядеть так — *jacob.hr.microsoft.com,* где *jacob* — имя узла, *hr* — дочерний домен, а *microsoft.com* — родительский.

Интеграция Active Directory и DNS

Как говорилось в главе 6, в доменах Active Directory структура именования и иерархия объектов реализованы посредством DNS. При установке первого контроллера домена в сети Active Directory вам будет предоставлена возможность автоматически установить DNS, если DNS-сервер не удастся найти в сети. На этом этапе вы также указываете, нужно ли полностью интегрировать DNS и Active Directory. При полной интеграции информация DNS хранится прямо в Active Directory, что делает доступными дополнительные возможности этой службы. Поэтому, как правило, пренебрегать полной интеграцией не следует. Важно отличать частичную и полную интеграцию.

- Частичная интеграция означает, что данные DNS хранятся в обычных текстовых файлах с расширением .DNS. По умолчанию они находятся в папке *%SystemRoot%*\System32\Dns. Обновления DNS обрабатываются через единственный полномочный DNS-сервер, назначенный основным DNS-сервером для конкретного домена или для области внутри домена, называемой *зоной* (zone). Клиенты, динамически обновляющие данные DNS средствами DHCP, должны быть настроены на работу с основным DNS-сервером в зоне, иначе их DNS-информация не будет обновляться. С другой стороны, динамическое обновление сетевых параметров посредством DHCP также не производится, если основной DNS-сервер недоступен.
- При полной интеграции DNS-информация хранится прямо в Active Directory и доступна через контейнер объекта dnsZones. Поскольку эти данные - часть Active Directory, доступ к ним имеет любой контроллер домена. Динамическое обновление средствами DHCP можно производить по модели с несколькими хозяевами. Это позволяет любому контроллеру домена, на котором запущена служба DNS, обрабатывать динамические обновления. Остальные клиенты, динамически обновляющие данные DNS через DHCP, вправе обращаться к любому DNS-серверу в своей зоне. Дополнительное преимущество интеграции каталогов — возможность задействовать систему безопасности каталогов при доступе к DNS-информации.

Преимущества полной интеграции с Active Directory проявляются также в способе репликации. При частичной интеграции DNS-информация хранится и реплицируется отдельно

от Active Directory. Имея две раздельные реплицируемые структуры, вы снижаете эффективность работы как DNS, так и Active Directory, и усложняете администрирование. Поскольку в DNS изменения реплицируются менее эффективно, чем к Active Directory, наличие двух структур также увеличивает сетевой трафик и время репликации изменений DNS.

Развертывание DNS в сети

Развертывание DNS заключается в настройке DNS-клиентов и DNS-серверов. Настраивая клиент, вы просто задаете в его конфигурации IP-адреса DNS-серверов в сети. Если в сети используется DHCP, задайте параметры области 006 DNS-серверы (006 DNS Servers) и 015 DNS-имя домена (015 DNS Domain Name). Подробнее — в главе 18. Кроме того, если компьютеры в сети должны быть доступны из других доменов Active Directory, для них следует создать записи в DNS. Записи DNS организованы в зоны — области внутри домена.

Примечание О настройке DNS-клиента рассказано в главе 16, о настройке DNS-сервера — в следующем разделе.

Установка DNS-серверов

Система Microsoft Windows Server 2003 способна исполнять функции DNS-сервера одного из четырех типов.

- **Основной интегрированный с Active Directory (Active Directory-integrated primary) — DNS-сервер, полностью интегрированный с Active Directory. Все данные DNS хранятся в каталоге.**
- Основной (primary) —главный DNS-сервер домена, частично интегрированный с Active Directory. Оригинал записей DNS и файлы конфигурации домена хранятся в текстовых файлах с расширением .DNS.
- Дополнительный (secondary) — резервный DNS-сервер, который хранит копию записей DNS, полученных от основного сервера, и выполняет обновления путем зонных передач. Дополнительный сервер получает данные DNS от основного сервера при запуске и использует их, пока они не устареют или не будут обновлены.
- Ограниченный сервер пересылки (forwarding-only) — кэширует DNS-информацию, полученную в результате поиска, и всегда передает запросы другим серверам. Данные DNS хранятся на нем, пока не устареют или не будут обновлены. В отличие от

дополнительного, ограниченный сервер пересылки не запрашивает полные копии файлов БД зоны, т. е. когда вы запускаете этот сервер, его база пуста.

Установка службы DNS

Функции DNS-серверов способны выполнять все контроллеры домена. В процессе установки контроллера домена вам, вероятно, предлагалось установить и настроить DNS. Если вы тогда ответили утвердительно, DNS уже установлена и настроена; вам не нужно ничего предпринимать.

Для установки DNS на рядовом сервере или на контроллере домена, где ее еще нет, выполните следующие действия.

1. Откройте меню Администрирование (Administrative Tools) и выберите Мастер настройки сервера (Configure Your Server Wizard). Щелкните Далее (Next).
2. Еще раз щелкните Далее (Next). В открывшемся окне перечислены все возможные роли сервера с пометками, какие из них уже сконфигурированы. Выделите вариант DNS-сервер (DNS Server).
3. Два раза щелкните Далее (Next). Мастер установит DNS и начнет настройку сервера. При необходимости вставьте компакт-диск Windows Server 2003,
4. Запустится Мастер настройки DNS-сервера (Configure a DNS server wizard). Щелкните Далее (Next).
5. Установите переключатель Настроить только корневые ссылки (Configure Root Hints Only), чтобы задать создание только основных структур DNS.
6. Щелкните Далее (Next). Мастер ищет имеющиеся структуры DNS и при необходимости изменяет их.
7. Два раза щелкните Готово (Finish). Закройте консоль Управление данным сервером (Manage Your Server).

Теперь служба DNS будет запускаться автоматически при каждой перезагрузке сервера. Если она не запускается, вам придется сделать это вручную (см. раздел «Запуск и остановка DNS-сервера»).

Настройка основного DNS-сервера

Каждому домену необходим основной DNS-сервер. обычный или интегрированный с Active Directory. На основном сервере зада-

ются зоны прямого и обратного просмотра. Первые служат для разрешения доменных имен в IP-адреса, вторые решают обратную задачу — искать доменное имя по IP-адресу (это необходимо для аутентификации DNS-запросов).

Установив службу DNS на сервере, настройте основной сервер.

1. Откройте меню Администрирование (Administrative Tools) и выберите DNS, Откроется консоль DNS (рис. 20-1).

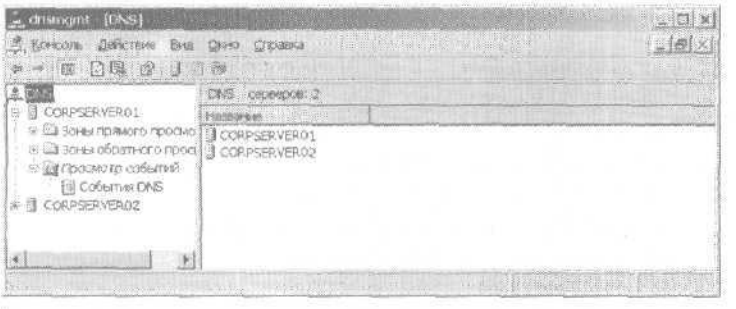


Рис. 20-1. С помощью консоли DNS вы управляете DNS-серверами сети

2. Если сервер, который вы хотите настроить, не указан в дереве консоли, подключитесь к нему. Правой кнопкой щелкните элемент DNS в дереве консоли и выберите Подключение к DNS-серверу (Connect to DNS Server). Если вы подключаетесь:
   - **к локальному серверу,** щелкните Этот компьютер (This Computer) и затем OK;
   - к удаленному серверу, щелкните Следующий компьютер (The Following Computer), введите имя или IP-адрес сервера и затем OK.
3. В дереве консоли появится запись для DNS-ссрвера. Щелкните ее правой кнопкой и выберите Создать новую зону (New Zone). Запустится мастер создания зоны. Щелкните Далее (Next).

Примечание Доступ к консоли DNS можно получить из консоли Управление компьютером (Computer Management). Запустите ее, подключитесь к серверу, которым хотите управлять, затем раскройте Службы и приложения (Services and Applications) и выберите DNS.

4. Выберите тип зоны (рис. 20-2). Поскольку вы настраиваете основной сервер, установите переключатель Основная зона (Primary Zone). Если вы хотите интегрировать сервер с Active Directory (на контроллере домена), установите переключатель Хранить зону в Active Directory (Store the zone in Active Directory). Если вы не хотите интегрировать DNS с Active Directory, сбросьте этот флажок. Щелкните Далее (Next).

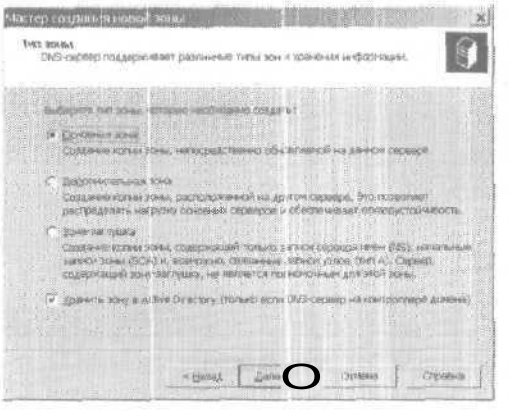


Рис. 20-2. Здесь задается тип зоны

5. Если вы интегрируете зону с Active Directory, выберите стратегию репликации, в противном случае переходите к пункту 6.
   - **На все DNS-серверы в лесу Active Directory (To all DNS servers in the Active Directory forest)** — самая широкая стратегия репликации. Помните, что в лес Active Directory включены все доменные деревья, использующие общий каталог с текущим доменом.
   - **На все DNS-серверы в** домене Active **Directory (To all DNS servers in the Active Directory domain)** — DNS-информация будет реплицироваться па DNS-серверы только в текущем домене и его дочерних доменах.
   - **На все контроллеры домена в домене Active Directory (To all domain controllers in the Active Directory domain)** — DNS-информация будет реплицироваться на все контроллеры к текущем домене и его дочерних доменах. Нужно учитывать, что не каждый контроллер домена является DNS-сервером.

6. Щелкните Далее (Next). Установите переключатель Зона прямого просмотра (Forward Lookup Zone) и щелкните Далее (Next).
7. Введите полное DNS-имя зоны. Оно определяет, где в иерархии домена DNS располагается сервер или зона. Например, если вы создаете основной сервер для домена *microsoft.com*, введите microsoft.com. Щелкните Далее (Next).
8. Если вы настраиваете основную зону, которая не интегрирована с Active Directory, задайте имя файла зоны или оставьте имя, предложенное ко умолчанию. Щелкните Далее (Next).
9. С помощью следующих переключателей выберите вид динамического обновления.
   - Разрешить только безопасные динамические обновления (Allow only secure dynamic updates) — если зона интегрирована с Active Directory, вы вправе ограничить список клиентов, которым разрешено выполнять динамические обновления, посредством списков управления доступом.
   - Разрешить любые динамические обновления (Allow both nonsecure and secure dynamic updates) — позволяет обновлять записи ресурса DNS всем клиентам.
   - Запретить динамические обновления (Do not allow dynamic updates) — отменяет динамические обновления DNS. Выбирайте этот вариант, только если зона не интегрирована с Active Directory.
10. Щелкните Далее (Next), а затем — Готово (Finish). Новая зона добавится к серверу с автоматически созданными основными записями DNS.
11. При необходимости повторите этот процесс, настроив зоны прямого просмотра для других доменов (один DNS-сервер способен обслуживать несколько доменов). Вам также нужно настроить зоны обратного просмотра (подробнее — в разделе «Настройка обратного просмотра»).
12. Создайте дополнительные записи для компьютеров, которые должны быть доступны из других доменов DNS (подробнее — в разделе «Управление записями DNS»).

Примечание Во многих организациях **сеть** разделяется на открытую и закрытую части. В открытой части располагаются Web-серверы, FTP-серверы и внешние почтовые серверы. В закрытой области размещены внутренние серверы и рабочие

станции. Параметры DNS для открытой области должны согласовываться с общим пространством имен Интернета. Здесь вы работаете с корневыми доменами .com, .org, .net и другими, а также с DNS-именами, зарегистрированными в Интернете, и IP-адресами, которые вы приобрели или взяли в аренду. В закрытой области вы вправе использовать любые DNS-имена, а закрытые IP-адреса должны соответствовать правилам, описанным в главе 16,

Настройка дополнительного DNS-сервера

Дополнительный DNS-сервер используется в качестве резервного. Если вы применяете полную интеграцию с Active Directory, дополнительные серверы настраивать не нужно. Лучше задайте обработку DNS на нескольких контроллерах домена. В случае частичной интеграции дополнительные серверы помогают снизить нагрузку на основной сервер. В небольшой сети в качестве дополнительных серверов можно указать имена серверов вашего провайдера Интернета. Обратитесь к провайдеру, чтобы тот настроил для вас дополнительные службы DNS.

Поскольку дополнительные серверы используют для большинства запросов зоны прямого просмотра, зоны обратного просмотра могут не понадобиться.

Чтобы настроить дополнительный DNS-сервер, выполните следующие действия.

1. Откройте консоль DNS и подключитесь к серверу, который хотите настроить.
2. Щелкните правой кнопкой запись сервера и выберите Создать новую зону (New Zone). Щелкните Далее (Next)
3. В окне Тип зоны (Zone Type) установите переключатель Дополнительная зона (Secondary Zone) и щелкните Далее (Next).
4. На дополнительном сервере могут использоваться файлы зон как прямого, так и обратного просмотра. Сначала создайте зону прямого просмотра, установив переключатель Зона прямого просмотра (Forward Lookup Zone) и щелкнув Далее (Next).
5. Введите полное DNS-имя зоны и щелкните Далее (Next).
6. Введите IP-адрес основного сервера зоны и щелкните Добавить (Add). Вы вправе указать здесь несколько адресов. Если первый сервер в списке недоступен, данные зоны будут копироваться со второго.

7. Щелкните Далее (Next) и Готово (Finish).
8. При необходимости настройте зоны обратного просмотра (см. следующий раздел).

Настройка обратного просмотра

Прямые просмотры нужны для разрешения имен доменов в IP-адреса, а обратные — для разрешения IP-адресов в имена доменов. Каждый сегмент вашей сети должен иметь зону обратного просмотра. Например, если у вас есть подсети 192.168.10.0, 192.168.11.0 и 192.168.12.0, вам необходимо три зоны обратного просмотра.

Стандартное правило именования зон обратного просмотра — запись идентификатора сети в обратном порядке и добавление суффикса in-addr.arpa. В предыдущем примере у вас должны получиться зоны 10.168.192.in-addr.arpa, 11.168.192.in-addr.arpa и 12.168.192.in-addr.arpa. Записи в зоне обратного просмотра должны быть синхронизированы с зоной прямого просмотра. При рассинхронизации зон проверка подлинности в домене может дать сбой.

Вот как создать зону обратного просмотра.

1. Запустите консоль DNS и подключитесь к серверу, который хотите настроить.
2. Щелкните правой кнопкой запись сервера и выберите Создать новую золу (New Zone). Запустится мастер создания зоны. Щелкните Далее (Next).
3. Если вы настраиваете основной сервер, интегрированный с Active Directory, установите переключатель Основная зона (Primary Zone) и убедитесь, что флажок Хранить зону в Active Directory (Store the zone in Active Directory) установлен. Если вы не хотите интегрировать DNS с Active Directory, установите переключатель Основная зона (Primary Zone) и сбросьте флажок Хранить зону в Active Directory (Store the zone in Active Directory). Щелкните Далее (Next).
4. Если вы конфигурируете зону обратного просмотра для дополнительного сервера, выберите Дополнительная зона (Secondary Zone) и щелкните Далее (Next).
5. Если вы интегрируете зону с Active Directory, выберите стратегию репликации, как описано в пункте 5 раздела «Настройка основного DNS-сервера».

6. Установите переключатель Зона обратного просмотра (Reverse Lookup Zone) и щелкните Далее (Next).
7. Введите идентификатор сети и маску подсети для зоны обратного просмотра. Вводимое значение задает стандартное имя для зоны обратного просмотра. Щелкните Далее (Next).

Совет Если ваша сеть разделена на несколько подсетей, скажем 192.168.10 и 192.168.11, введите здесь только сетевую часть имени зоны, т. е. 168.192. Зоны подсетей консоль DNS создаст сама.

8. Если вы настраиваете основной или дополнительный сервер, который не интегрирован с Active Directory, задайте имя файла зоны и щелкните Далее (Next).
9. С помощью соответствующих параметров задайте разрешение динамических обновлений, как описано в пункте 9 раздела «Настройка основного DNS-сервера».
10. Щелкните Далее (Next) и Готово (Finish).

Настроив зоны обратного просмотра, обратитесь в ИТ-отдел организации или к провайдеру, чтобы удостовериться, что зоны зарегистрированы в родительском домене.

Управление DNS-серверами

Консоль DNS — удобное средство управления локальными и удаленными DNS-серверами. Основное окно консоли DNS разделено на две панели (рис. 20-3). Левая открывает доступ к DNS-серверам и их зонам, правая показывает выбранный пункт в развернутом виде.

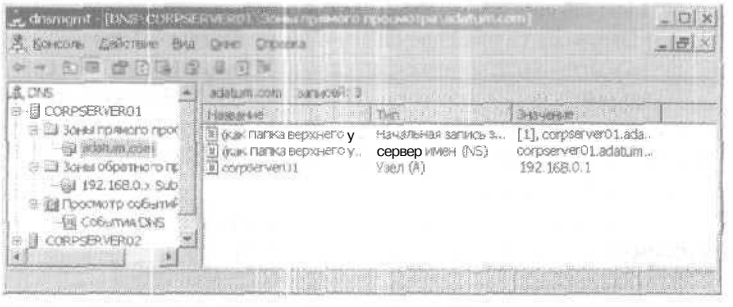


Рис. 20-3. Управляйте доменами и подсетями через папки зон прямого и обратного просмотра

Папки Зоны прямого просмотра (Forward Lookup Zones) и Зоны обратного просмотра (Reverse Lookup Zones) предоставляют доступ к доменам и подсетям, настроенным для использования на этом сервере. Выделив папку домена или подсети в левой панели, вы сможете управлять соответствующими записями DNS.

Добавление удаленных серверов в консоль DNS

1. Щелкните правой кнопкой элемент DNS в дереве консоли и выберите Подключение к DNS-ссрверу (Connect to DNS Server), чтобы открыть диалоговое окно, показанное на рис. 20-4.
2. Установите переключатель Этот компьютер (This Computer), если подключаетесь к локальному компьютеру, или Другой компьютер (The following computer). Введите IP-адрес или полное имя узла удаленного компьютера, к которому хотите подключиться.
3. Щелкните OK. Если подключение удалось, запись сервера появится в консоли.

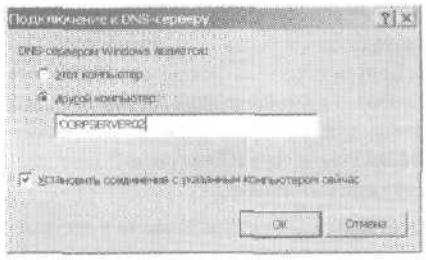


Рис. 20-4. Подключение к локальному или удаленному серверу

Примечание Если сервер недоступен из-за ограничений безопасности или проблем со службой удаленного вызова процедур (RPC), подключение не удастся. Однако вы вправе добавить сервер к консоли, щелкнув Да (Yes) в ответ на запрос,

Удаление сервера из консоли DNS

Чтобы удалить сервер из консоли DNS, выделите его и нажмите клавишу Delete. При этом сервер удаляется только из списка серверов; из сети он не удаляется.

Запуск и остановка DNS-сервера

Серверами DNS управляют с помощью одноименной службы. Как и любую другую, вы вправе ее запустить, отключить, приос-

тановить и перезапустить посредством узла Службы (Services) консоли Управление компьютером (Computer Management) или из командной строки. Кроме того, службой DNS можно управлять из консоли DNS. Щелкните правой кнопкой сервер, которым хотите управлять, выберите Все задачи (All Tasks), а затем щелкните Пуск (Start), Стоп (Stop), Пауза (Pause), Продолжить (Resume) или Перезапустить (Restart).

Создание дочерних доменов в зонах

Чтобы создать в зоне дочерний домен, выполните следующие действия.

1. В консоли DNS раскройте папку Зоны прямого просмотра (Forward Lookup Zones) для нужного вам сервера.
2. Щелкните правой кнопкой запись родительского домена и выберите Создать домен (New Domain).
3. Введите имя нового домена и щелкните OK.

Создание дочерних доменов в раздельных зонах

По мере роста организации приходится разделять пространство имен DNS на несколько зон. Если в штаб-квартире компании вы определили зону для родительского домена *microsoft.com,* то в филиалах вам понадобятся зоны для каждого офиса, например *memphis.micmsoft.com, newyork.microsoft.com* и *la.microsoft.com.* Дочерний домен создается следующим образом.

1. Установите DNS-сервер в каждом дочернем домене и создайте зоны прямого и обратного просмотра для дочернего домена (см. раздел «Установка DNS-серверов»).
2. На полномочном сервере DNS для родительского домена делегируйте полномочия каждому дочернему домену, чтобы дочерние домены могли разрешать и отвечать на DNS-запросы от компьютеров внутри и за пределами локальной подсети.

Полномочия дочернему домену делегируются следующим образом.

1. В консоли DNS раскройте папку Зоны прямого просмотра (Forward Lookup Zones) для сервера, с которым хотите работать.
2. Щелкните травой кнопкой запись родительского домена и выберите Создать делегирование (New Delegation). Запустится мастер делегирования.

3. Введите имя делегируемого домена (рис. 20-5), например ts, и щелкните Далее (Next). Вводимое вами имя автоматически будет подставлено в поле Полное доменное имя (Fully Qualified Domain Name). Щелкните Далее (Next).
4. Щелкните Добавить (Add) и введите полное имя DNS-сервера для дочернего домена, например **corpserver01.memphis.adatum.com**.

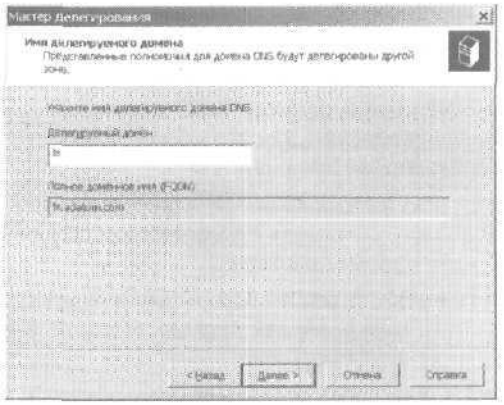


Рис. 20-5. Имя делегируемого домена автоматически подставляется в полное доменное имя

5. В поле IP-адрес (IP Address) введите основной IP-адрес сервера. Щелкните Добавить (Add). Повторите эти действия, чтобы задать дополнительные IP-адреса сервера. Порядок записей определяет приоритет использования IP-адресов; его можно изменить кнопками Вверх (Up) и Вниз (Down).

Совет Если к серверу настроен доступ по сети, введите имя сервера и щелкните кнопку Сопоставить (Resolve). IP-адрес автоматически отобразится в поле IP-адрес (IP Address) и будет добавлен в список.

6. Щелкните OK и повторите пункты 3-5, чтобы задать другие полномочные DNS-серверы для дочернего домена.
7. Щелкните Далее (Next) и Готово (Finish).

Удаление домена или подсети

1. В консоли DNS щелкните правой кнопкой запись домена или подсети.

2. Выберите Удалить (Delete) и подтвердите действие, щелкнув Да (Yes).

Примечание При удалении домена или подсети на основном или дополнительном сервере, который не интегрирован с Active Directory, удаляются все записи DNS из файла зоны, но не сам файл. Он остается в папке *%SystemRoot%*\System32\Dns. Его можно удалить вручную.

Управление записями DNS

Записи DNS необходимы компьютерам, доступным из Active Directory и доменов DNS. Типов записей DNS множество, но большинство обычно не используют, так что мы сосредоточимся на тех, что вам *действительно* понадобятся:

- A (address) — сопоставляет имя узла с IP-адресом. Количество этих записей должно совпадать с количеством сетевых адаптеров или IP-адресов у компьютера;
- **CNAME** (canonical name) — задает псевдоним для имени узла. Например, запись этого типа позволит узлу *zeta.microsoft.com* получить псевдоним *www.microsoft.com*;
- **MX** (mail exchange) - определяет сервер почтового обмена для домена;
- NS (name server) — указывает сервер имен для домена, обеспечивающий поиск DNS в разных зонах. Такой записью должны объявляться все основные и дополнительные серверы имен;
- **PTR** (pointer) — создает указатель, сопоставляющий IP-адрес с именем узла для выполнения обратного просмотра;
- **SOA (start of authority)** — описывает предпочтительный полномочный узел зоны, являющийся наиболее достоверным источником данных DNS.

Запись SOA создается автоматически при добавлении зоны и должна содержаться в каждом файле зоны.

Добавление записей A и PTR

A-запись сопоставляет имя узла с IP-адресом, а PTR-запись создает указатель на узел для обратного просмотра. Записи адреса и указателя допускается создавать одновременно или по отдельности.

1. В консоли DNS раскройте папку Зоны прямого просмотра (Forward Lookup Zones) для нужного нам сервера.
2. Щелкнув правой кнопкой домен, который хотите обновить, выберите Создать узел (New Host). Появится диалоговое окно, показанное на рис. 20-6.

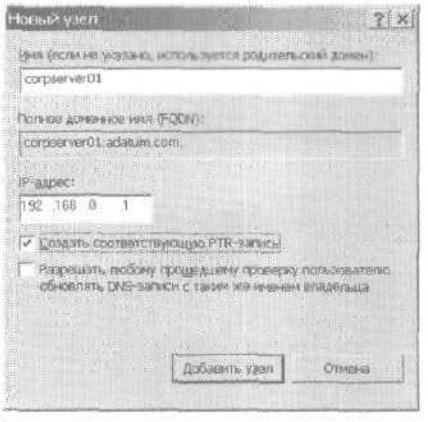


Рис. 20-6. Записи A и PTR создаются одновременно

3. Введите имя компьютера без пробелов, например **corpserver01**, и его IP-адрес.
4. Установите флажок Создать соответствующую PTR-запись [Create Associated Pointer (PTR) Record].

Примечание Создание PTR-записи допускается, только если доступна соответствующая зона обратного просмотра (см. раздел «Настройка обратного просмотра»). Флажок Разрешать любому прошедшему проверку пользователю... (Allow Any Authenticated Users...) доступен для DNS-сервера, сконфигурированного на контроллере домена.

5. Щелкните Добавить узел (Add Host). Повторите для добавления других узлов.
6. Щелкните Готово (Done).

Последующее добавление PTR-записи

1. Б консоли DNS раскройте папку Зоны обратного просмотра (Reverse Lookup Zones) для нужного вам сервера.

2. Щелкнув правой кнопкой подсеть, которую хотите обновить, и выберите Создать указатель (New Pointer). Откроется диалоговое окно, показанное на рис. 20-7.

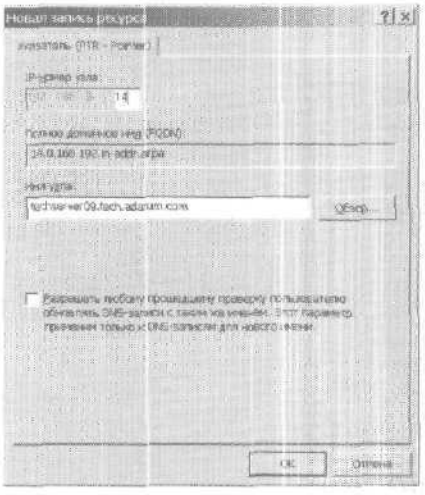


Рис. 20-7. PTR-запись можно добавлять отдельно от А-записи

3. Введите IP-номер узла и его имя. Щелкните OK.

Добавление записи CNAME

В CNAME-записях задаются псевдонимы узла, благодаря которым на компьютере могут работать различные серверы. Например, узел *gamma.microsoft.com* можно представить как *www.microsoft.com* и *ftp.microsoft.com*. CNAME-запись создается так.

1. В консоли DNS откройте панку Зоны прямого просмотра (Forward Lookup Zones) для нужного сервера.
2. Щелкнув правой кнопкой домен, который хотите обновить, выберите Создать псевдоним (New Alias). Откроется диалоговое окно, показанное на рис. 20-8.
3. Введите в поле Псевдоним (Alias Name) часть имени узла, например **www** или ftp.
4. В ноле Полное доменное имя конечного узла (Fully Qualified Name For Target Host) введите полное доменное имя компьютера, для которого создается псевдоним.
5. Щелкните OK.

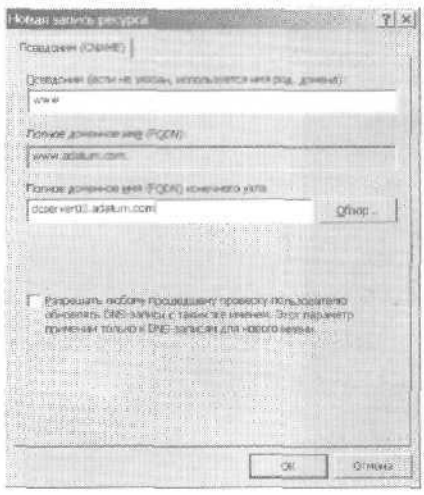


Рис. 20-8. Здесь создается CNAME-запись

Добавление сервера почтового обмена

Сервер почтового обмена, задаваемый MX-записью, отвечает за обработку или пересылку почты в домене. При создании MX-записи нужно определить приоритет почтового сервера в диапазоне от 0 до 65535. Почтовый сервер с наименьшим номером имеет самый высокий приоритет и первым получает почту. Если почту не удастся доставить, ее пытается получить почтовый сервер со следующим номером и т. д. MX-запись создается так.

1. В консоли DNS откройте папку Зоны прямого просмотра (Forward Lookup Zones) нужного вам сервера.
2. Щелкнув правой кнопкой домен, который хотите обновить, выберите Создать почтовый обменник (New Mail Exchanger). Откроется диалоговое окно, показанное на рис. 20-9.
3. Заполните следующие поля (в отдельных ситуациях некоторые из них недоступны):
   - Узел или дочерний домен (Host or child domain) — в большинстве случаев это поле заполнять не нужно. Отсутствие значения в нем означает, что имя почтового обменника совпадает с именем родительского домена;
   - Полное доменное имя (Fully qualified domain name) — полное имя домена, к которому относится MX-запись:

Рис. 20-9. Почтовые серверы с самым низким номером имеют самый высокий приоритет

- Полное доменное имя или почтовый сервер (Fully qualified domain name of mail server) — доменное имя почтовою сервера, отвечающего за прием и доставку почты. На этот сервер передаются сообщения, адресованные в домен, указанный в предыдущем поле;
- **Приоритет почтового сервера (Mail server priority) — значение от 0 до 65535.**

Совет Назначая приоритет, оставляйте место для дальнейшего роста. Скажем, введите 10 для почтового сервера с самым высоким приоритетом, 20 — для следующего и т. д.

4. Щелкните OK.

Добавление серверов имен

Записями NS идентифицируются серверы имен домена. Такая запись необходима на каждом основном и дополнительном сервере имен. Если дополнительный сервис предоставлен вашим провайдером, не забудьте добавить соответствующие записи NS. Запись NS создается следующим образом.

1. В консоли DNS откройте папку Зоны прямого просмотра (Forward Lookup Zones) нужного сервера.

2. Выделите папку домена в дереве, чтобы вывести в правой панели его записи DNS.
3. Щелкните правой кнопкой имеющуюся запись Сервер имен (Name Server) и выберите Свойства (Properties). Откроется диалоговое окно, показанное на рис. 20-10.

Рис. 20-10. Настройка серверов имен

4. Щелкните Добавить (Add).
5. Введите полное доменное имя добавляемого DNS-сервера.
6. В поле IP-адрес (IP Address) введите основной IP-адрес сервера. Щелкните Добавить (Add). Повторите эту операцию для дополнительных IP-адресов сервера. Порядок обращения к серверам позволяют кнопки Вверх (Up) и Вниз (Down).
7. Щелкните OK. Повторите пункты 4-7, чтобы указать другие DNS-серверы.

Просмотр и обновление записей DNS

1. Дважды щелкните нужную зону. Записи для зоны отобразятся в правой панели.
2. Дважды щелкните запись DNS, которую хотите просмотреть или обновить. В открывшемся окне сделайте нужные изменения и щелкните OK.

Обновление свойств зоны и записи SOA

Каждой зоне соответствует собственный набор настраиваемых свойств. В этом наборе посредством начальной записи зоны (SOA) задаются основные параметры зоны, уведомления об изменении и интеграция WINS. Чтобы настроить свойства зоны в консоли DNS:

- щелкните зону правой кнопкой и выберитеСвойства (Properties);
- выделите зону и выберите вменю Действие (Action) команду Свойства (Properties).

Окна свойств зон прямого и обратного просмотра почти идентичны — за единственным исключением. В окне свойств зоны прямого просмотра отображается вкладка WINS, позволяющая настроить прямой поиск NetBIOS-имен компьютеров, а в окне свойств зоны обратного просмотра — вкладка WINS-R, позволяющая настроить обратный просмотр для NetBIOS-имен компьютеров.

Редактирование записи SOA

Начальная запись зоны (start of authority, SOA) назначает полномочный сервер имен для данной зоны и задает ее основные свойства, например интервалы повтора и обновления, Чтобы изменить эту информацию, выполните следующие действия.

1. В консоли DNS щелкните правой кнопкой обновляемую зону и выберите Свойства (Properties).
2. Перейдите на вкладку Начальная запись зоны (SOA) [Start of Authority (SOA)] и введите нужные значения в поля, показанные на рис. 20-11.

На вкладке Начальная запись зоны (SOA) [Start Of Authority (SOA)] имеются следующие поля.

- **Серийный номер (Serial Number)** — номер, идентифицирующий версию файлов БД DNS. Обновляется автоматически при любом изменении файлов зоны или вручную. Дополнительные серверы используют его для установления факта изменения записей зон. Если серийный номер основного сервера больше серийного номера дополнительного, значит, записи изменились, и дополнительный сервер запрашивает обновленные записи для зоны. Вы также вправе настроить DNS

на уведомление дополнительных серверов об изменениях (это ускоряет процесс обновления).

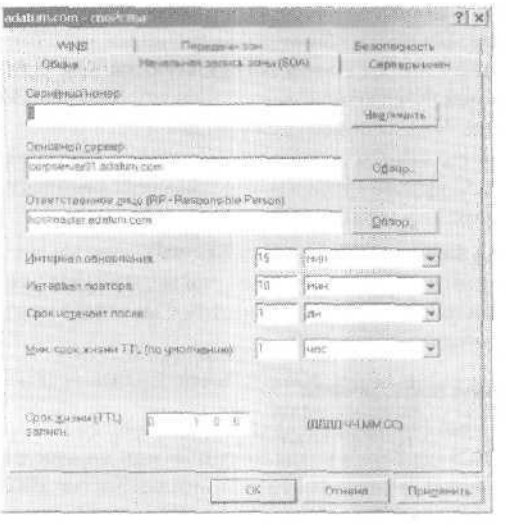


Рис. 20-11. Здесь задаются общие свойства зоны

- Основной сервер (Primary Server) — полное доменное имя сервера имен. Обратите внимание на точку в конце — она позволяет ограничить имя и гарантировать, что к имени не будет добавлена лишняя информация.
- Ответственное лицо (Responsible Person) — электронный адрес сотрудника, ответственного за домен. По умолчанию это *hostmaster* с точкой в конце, что соответствует адресу *hostmaster@ваш_домен.com*. Если вы будете вводить в это поле другой адрес, замените символ (@) на точку и еще одну точку поставьте в конце.
- Интервал обновления (Refresh Interval) - интервал, с которым дополнительный сервер проверяет обновления зон.
- Интервал повтора (Retry Interval) — время до повтора попытки загрузки БД зоны, если первая попытка оказалась неудачной,
- Срок истекает после (Expires After) — период, в течение которого действительна информация зоны на дополнительном сервере. Если за это время дополнительный сервер не загрузит данные с основного, он аннулирует данные в своем кэше и перестает отвечать на запросы DNS.

- Минимальный срок жизни TTL (по умолчанию) [Minimum (Default) TTL] — минимальное время жизни кэшированных записей на дополнительном сервере в формате «дни : часы : минуты : секунды». По достижении этого значения дополнительный сервер аннулирует соответствующую запись. Следующий запрос к ней будет отправлен основному серверу для разрешения имени. Чтобы сократить трафик в сети и повысить эффективность, задайте в этом поле большое значение, например 24 часа. С другой стороны, это замедлит распространение обновлений через Интернет.
- Срок жизни (TTL) записи (TTL For This Record) — время жизни самой SOA-записи в формате «дни : часы : минуты : секунды». Как правило, оно должно совпадать с минимальным временем жизни обычных записей.

Управление зонными передачами

В процессе *передачи зоны* (zone transfer) копия информации зоны передается другим DNS-серверам в том же самом или других доменах. По соображениям безопасности в Windows Server 2003 зонные передачи запрещены. Вы должны разрешить их для внутренних дополнительных серверов или для дополнительного сервера провайдера, а также указать тины серверов, на которые допускается передавать информацию зоны.

Ограничение доступа к информации зоны — важная мера предосторожности. Запрашивать обновления с основного сервера зоны должны только указанные вами серверы. Это позволит скрывать подробности строения внутренней сети от внешнего мира.

Чтобы разрешить зонные передачи и ограничить доступ к БД основной зоны, выполните следующие действия.

1. В консоли DNS щелкните правой кнопкой обновляемый домен или подсеть и выберите Свойства (Properties).
2. Перейдите на вкладку Передачи зон (Zone Transfers), показанную на рис. 20-12.
3. Установите флажок Разрешить передачи зон (Allow zone transfers).
4. Чтобы разрешить передачи только на серверы, перечисленные на вкладке Серверы имен (Name Servers), и щелкните Только на серверы, перечисленные на странице серверов имен (Only to servers listed on the Name Servers tab).

5. Чтобы явно указать серверы, на которые разрешены передачи, установите флажок Разрешить передачи зон (Allow Zone Transfers) и щелкните Только на серверы из этого списка (Only to the following servers). Введите IP-адреса серверов и щелкните OK.

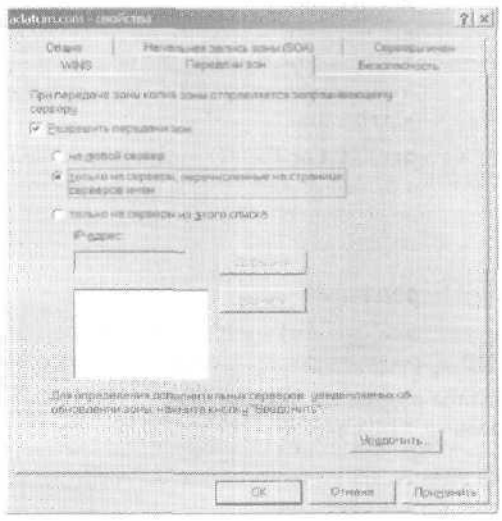


Рис. 20-12. Здесь настраиваются параметры зонных передач

Уведомление дополнительных серверов об изменениях

Чтобы основной сервер уведомлял дополнительные серверы имен об изменениях в БД зоны, выполните следующие действия.

1. В консоли DNS щелкните правой кнопкой нужный домен или подсеть и выберите Свойства (Properties).
2. На вкладке Передачи зон (Zone Transfers) щелкните кнопку Уведомить (Notify). Откроется диалоговое окно, показанное на рис. 20-13.
3. Установите флажок **Автоматически** уведомлять **(Automatically** notify), а затем установите переключатель:
   - **Уведомлять серверы со страницы серверов имен (Servers listed on the** Name **Servers tab),** чтобы уведомлять дополнительные серверы, *указанные* на вкладке Серверы имен (Name Servers);

- **Только указанные** серверы **(The** following **servers),** чтобы явно задать IP-адреса уведомляемых дополнительных серверов. Добавьте в список нужные IP-адреса.

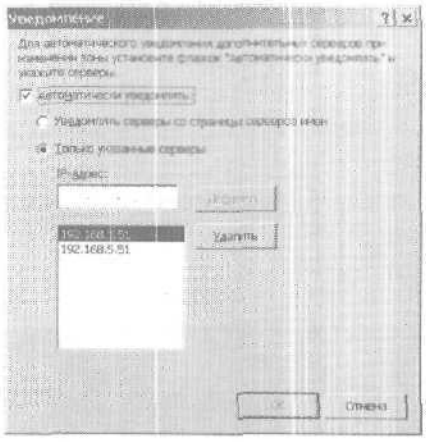


Рис. 20-13. Здесь задаются параметры уведомления дополнительных серверов

4. Щелкните OK два раза.

Настройка типа зоны

Чтобы изменить тип зоны и способ интеграции с Active Directory, выполните следующие действия.

1. В консоли DNS щелкните правой кнопкой обновляемый домен или подсеть и выберите Свойства (Properties).
2. На вкладке Общие (General) щелкните Изменить (Change). В окне Изменение типа зоны (Change Zone Type) задайте новый тип зоны.
3. Чтобы интегрировать зону с Active Directory, установите флажок Хранить зону в Active Directory (Store zone in Active Directory) или сбросьте его, чтобы отказаться от интегрирования.
4. Два раза щелкните OK.

Включение и выключение динамических обновлений

Динамические обновления позволяют клиентам DNS регистрировать и поддерживать собственные записи адреса и указателей. Это

полезно для компьютеров, настраиваемых средствами DHCP. Динамические обновления облегчают им поиск друг друга в сети, Интегрирование зоны с Active Directory позволяет проводить безопасные обновления с явным указанием пользователей и компьютеров, которым разрешено динамически обновлять DNS.

Динамические обновления включаются или выключаются так.

1. В консоли DNS щелкните правой кнопкой нужный домен или подсеть и выберите Свойства (Properties).
2. На вкладке Общие (General) выберите в списке Динамическое обновление (Dynamic Updates) один из перечисленных вариантов:
   - Никакие (None) — выключает динамические обновления;
   - Небезопасные и безопасные (Nonsecure and Secure) — включает любые динамические обновления;
   - Только безопасные (Secure Only) —включает динамические обновления через механизм безопасности Active Directory; доступно только при интеграции с Active Directory.
3. Щелкните OK.

Примечание Для DHCP должны также быть настроены параметры интеграции с DNS (подробнее — в главе 18).

Управление конфигурацией и безопасностью DNS-сервера

Для управления общей конфигурацией DNS-сервера воспользуйтесь окном его свойств. Здесь вы задаете или отменяете IP-адреса для сервера и управляете внешним доступом к нему. Тут же настраиваются мониторинг, регистрация и некоторые другие параметры.

Включение и выключение IP-адресов DNS-сервера

По умолчанию многоадресные DNS-серверы отвечают на запросы DNS через все доступные сетевые адаптеры и настроенные IP-адреса. В консоли DNS вы вправе указать, что сервер должен отвечать на запросы только по заданным IP-адресам.

1. В консоли DNS щелкните правой кнопкой настраиваемый сервер и выберите Свойства (Properties).

2. На вкладке Интерфейсы (Interfaces) установите переключатель Только по указанным IP-адресам (Only the following IP addresses), введите IP-адрес, который должен обслуживать DNS-запросы и щелкните Добавить (Add). При необходимости повторите эти действия, чтобы задать дополнительные адреса.
3. Щелкните OK.

Управление внешним доступом к DNS-серверам

Вы вправе указать, какие внутренние и внешние серверы имеют доступ к основному серверу, а также какие DNS-серверы в вашей организации имеют доступ к внешним серверам. Для этого нужно настроить пересылку внутри домена. С точки зрения пересылки DNS-серверы внутри домена разделяются таким образом:

- **непересылающий сервер (nonforwarder)** передает неразрешенные DNS-запросы заданным серверам пересылки, фактически играя роль их клиента;
- ограниченный сервер пересылки (forwarding-only server) способен только кэшировать ответы и передавать запросы на серверы пересылки. Его называют также *только кэширующим* (caching-only) DNS-сервером;
- **сервер пересылки (forwarder)** получаст запросы от непересылающих серверов и ограниченных серверов пересылки. Для разрешения запросов и передачи ответов другим DNS-серверам он использует обычные методы коммуникации DNS;
- **сервер условной пересылки (conditional forwarder)** пересылает запросы только в указанных DNS-доменах. Удобен в организациях с несколькими внутренними доменами.

Примечание Корневой сервер домена нельзя использовать для пересылки (за исключением условной пересылки в процессе разрешения внутренних имен), но все остальные серверы — можно.

Создание непересылающего DNS-сервера

1. В консоли DNS щелкните правой кнопкой настраиваемый сервер и выберите Свойства (Properties).
2. На вкладке Пересылка (Forwarders) в списке Домен DNS (DNS Domain) выберите вариант Все другие DNS-домены (All other DNS domains).

3. Введите IP-адреса серверов пересылки.
4. Щелкните Добавить (Add). Повторите процесс, чтобы задать дополнительные IP-адреса.
5. Задайте Время ожидания пересылки (Forward Time Out). В течение этого времени непересылающий сервер пытается получить отклик от текущего сервера пересылки. По истечении времени ожидания начинается опрос следующего сервера в списке. Значение по умолчанию — 5 секунд.
6. Щелкните OK.

Создание ограниченного сервера пересылки

1. В консоли DNS щелкните правой кнопкой настраиваемый сервер и выберите Свойства (Properties).
2. На вкладке Пересылка (Forwarders) в списке Домен DNS (DNS Domain) выберите вариант Все другие DNS-домены (All other DNS domains).
3. Установите флажок Не использовать рекурсию для этого домена (Do not use recursion for this domain).
4. Введите IP-адреса серверов пересылки.
5. Задайте Время ожидания пересылки (Forward Time Out),
6. Щелкните OK.

Создание сервера пересылки

Любой DNS-сервер, не определенный как непересылающий сервер или ограниченный сервер пересылки, считается сервером пересылки. Поэтому для его создания достаточно удостовериться, что вы *не установили* флажок Не использовать рекурсию для этого домена (Do not use recursion for this domain) и не задали пересылку сервером запросов на другие DNS-серверы данного домена,

Настройка условной пересылки

В сети с несколькими внутренними доменами DNS условная пересылка означает, что запросы о конкретном домене передаются для разрешения на конкретный DNS-сервер. Чтобы настроить условную пересылку, выполните следующие действия.

1. В консоли DNS щелкните правой кнопкой настраиваемый сервер и выберите Свойства (Properties).
2. На вкладке Пересылка (Forwarders) щелкните кнопку Создать (New). В диалоговом окне Новая пересылка (New For-

warder) введите имя домена, для которого задастся пересылка, и щелкните OK.

3. Выделите введенный домен в списке Домен DNS (DNS Domain), укажите IP-адрес полномочного DNS-сервера в этом домене и щелкните Добавить (Add). Вы вправе задать несколько IP-адресов.
4. Повторите пункты 2 и 3, чтобы настроить условную пересылку для других доменов.
5. Щелкните OK.

Ведение журнала событий DNS

По умолчанию служба DNS записывает в журнал все события DNS-сервера. Чтобы сузить список вносимых в журнал событий или вовсе отказаться от его ведения, выполните следующие действия.

1. В консоли DNS щелкните правой кнопкой настраиваемый сервер и выберите Свойства (Properties).
2. На вкладке Журнал событий (Event Logging) укажите события, которые хотите заносить *к* журнал. Если вы хотите отказаться от ведения журнала, установите переключатель Не заносить никакие события (No events).
3. Щелкните O K.

Ведение журнала отладки DNS

Выявить неполадки DNS позволяет временный журнал отладки, отслеживающий определенные типы событий DNS. Чтобы задать парамегры журнала отладки, выполните следующие действия.

1. В консоли DNS щелкните правой кнопкой настраиваемый сервер и выберите Свойства (Properties).
2. На вкладке Ведение журнала отладки (Debug Logging), показанной на рис. 20-14, установите флажок Записывать пакеты в журнал для отладки (Log packets for debugging) и укажите события, которые хотите отслеживать. -
3. *В* поле Имя и путь к файлу (File path and name) введите имя файла журнала,например Dns.log. По умолчанию журналы хранятся в папке *%SystemRoot%*\System32\Dns..
4. Щелкните OK. По окончании отладки сбросьте флажок Записывать пакеты в журналдля отладки (Log packets for debugging) на вкладке Ведение журнала отладки (Debug Logging).

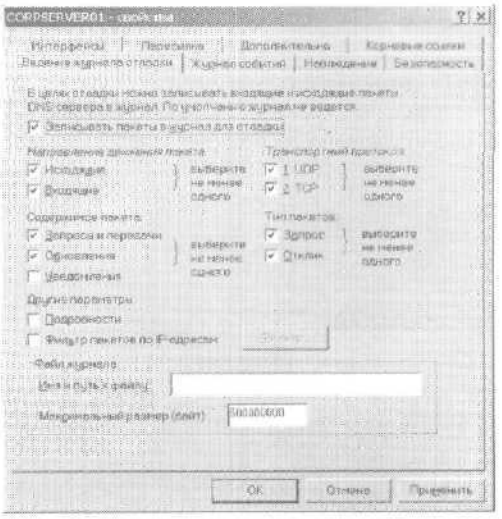


Рис. 20-14. Выберите события для записи в журнал отладки

Тестирование DNS-сервера

В Windows Server 2003 встроены специальные функции для тестирования DNS-серверов. Вы вправе проводить проверку вручную или автоматически.

1. В консоли DNS щелкните правой кнопкой настраиваемый сервер и выберите Свойства (Properties).
2. Перейдите на вкладку Наблюдение (Monitoring), показанную па рис. 20-15, и выберите способ тестирования:
   - **Простой запрос к этому DNS-серверу (A simple query against this DNS server),** чтобы проверить разрешение имен DNS на текущем сервере;
   - **Рекурсивный запрос к другим DNS-серверам (A recursive query to other DNS servers),** чтобы проверить разрешение имен DNS в домене.
3. Чтобы выполнить проверку вручную, щелкните Тест (Test Now). Чтобы назначить проверку по расписанию, установите флажок Автоматическое тестирование (Perform automatic testing at the following interval) и задайте интервал в секундах, минутах или часах.

Рис. 20-15. Настройте параметры проверки DNS-сервера

Совет Проверку следует проводить раз в несколько часов. Задавайте меньший интервал только для разрешения какой-либо проблемы.

1 Просмотрите результаты проверки, показанные в нижней части окна. Единичный отказ может быть результатом случайного сбоя, но несколько отказов подряд обычно свидетельствуют о проблеме с разрешением имен.

Совет Если все рекурсивные проверки заканчиваются неудачей, перейдите на вкладку Дополнительно (Advanced) и выясните, не установлен ли там флажок Отключить рекурсию (Disable Recursion).

Интеграция WINS и DNS

Интеграция с WINS позволяет DNS-серверу играть роль WINS-сервера или пересылать запросы WINS определенному WINS-серверу. Настроив WINS и DNS для совместной работы, вы вправе задать прямой и обратный просмотр по NetBIOS-именам компьютеров, настроить кэширование и время ожидания для разрешения имен WINS и полную интеграцию с областями NetBIOS.

Настройка просмотров WINS в DNS

Посредством WINS можно разрешить самую левую часть полного доменного имени. Вот как это делается. Сначала DNS-сервер ищет запись адреса для полного доменного имени. Если запись найдена, сервер разрешает имя, используя исключительно средства DNS. Если записи нет, сервер выделяет левую часть имени и с помощью WINS разрешает ее как NetBIOS-имя компьютера. Чтобы настроить просмотр WINS в DNS, выполните следующие действия.

1. В консоли DNS щелкните правой кнопкой настраиваемый домен и выберите Свойства (Properties).
2. Перейдите на вкладку WINS, установите флажок Использовать прямой просмотр WINS (Use WINS forward lookup) и введите IP-адреса WINS-серверов в сети. Вы должны указать как минимум один сервер WINS.
3. Чтобы запретить репликацию этой записи WINS на другие DNS-серверы в процессе зонной передачи, установите флажок Не выполнять репликацию этой записи (Do not replicate this record). Это удобно для выявления ошибок и сбоек передачи не Microsoft DNS-серверу. Щелкните OK.

Настройка обратного просмотра WINS в DNS

В процессе обратного просмотра WINS в DNS, IP-адрес узла разрешается в NetBIOS-имя компьютера. Сначала DNS-сервер ищет запись указателя для определенного IP-адреса. Если запись найдена, сервер использует ее для разрешения полного доменного имени. В противном случае сервер отправляет запрос WINS. WINS возвращает NetBIOS-имя компьютера для данного IP-адреса, после чего к имени компьютера добавляется имя домена.

Обратный просмотр WINS в DNS настраивается так.

1. В консоли DNS щелкните правой кнопкой настраиваемый сервер и выберите Свойства (Properties).
2. Перейдите на вкладку Обратный поиск WINS (WINS-R).
3. Установите флажок Использовать обратный поиск WINS (Use WINS-R lookup) и при необходимости Не выполнять репликацию этой записи (Do not replicate this record). Как и в случае прямого просмотра, обычно не рекомендуется реплицировать запись WINS-R на не Microsoft DNS-серверы.
4. В поле Домен, добавляемый к возвращенному имени (Domain to append to returned name) введите информацию об имени

домена, которое будет добавлено к имени компьютера, возвращенному WINS. Например, если вы введете здесь **seattle.domain.com** и WINS вернет NetBIOS-имя компьютера gamma, DNS-сервер соединит два значения и вернет gamma.seattle.domain.com.

5. Щелкните OK.

Кэширование параметров и время ожидания

Интегрируя WINS и DNS, вы должны настроить кэширование и время ожидания для WINS. Параметры кэша определяют, как долго действительны записи, возвращенные WINS. Время задержки определяет, как долго служба DNS ожидает ответа от WINS до возвращения ошибки. Эти значения задаются как для прямого, так и обратного просмотра WINS.

1. В консоли DNS щелкните правой кнопкой нужный домен или подсеть и выберите Свойства (Properties).
2. Перейдите па вкладку WINS или WINS-R и щелкните кнопку Дополнительно (Advanced). Откроется диалоговое окно, показанное па рис. 20-16.

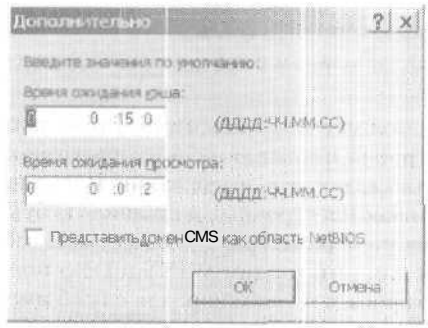


Рис. 20-16, Задайте параметры кэширования и времени ожидания для DNS

3. Задайте времена ожидания кэширования и просмотра в полях Время ожидания кэша (Cache time-out) и Время ожидания просмотра (Lookup time-out). По умолчанию DNS кэширует записи WINS па 15 минут, а время ожидания просмотра составляет 2 сек. Рекомендуется увеличить эти значения, например до 60 мин для кэширования и 3 сек для просмотра.
4. Щелкните OK.

Настройка полной интеграции с областями NetBIOS

При полной интеграции запросы разрешаются при помощи NetBIOS-имен компьютеров и областей NetBIOS. Прямой просмотр работает так. Сначала DNS-сервер ищет запись адреса для полного доменного имени и, найдя се, использует, чтобы разрешить имя средствами только DNS. Если запись не найдена, сервер разделяет имя на две части: крайняя левая часть считается NetBIOS-именем компьютера, а все остальное - именем NetBIOS-области. Эти значения передаются WINS для разрешения имени.

Полная интеграция WINS и DNS настраивается следующим образом.

1. В консоли DNS щелкните правой кнопкой настраиваемый домен или подсеть и выберите Свойства (Properties).
2. Перейдите на вкладку WINS или WINS-R и щелкните кнопку Дополнительно (Advanced),
3. Установите переключатель Представить домен DNS как область NETBIOS (Submit DNS domain as NetBIOS scope). Помните, что предварительно вы должны разрешить прямые и обратные просмотры WINS.
4. Щелкните OK. При необходимости повторите этот процесс для других доменов и подсетей.

Перед использованием этой методики убедитесь, что область NetBIOS правильно настроена и что для всех компьютеров в сети применяется согласованная схема именования. Поскольку в именах NetBIOS различаются строчные и прописные буквы, следите за использованием регистра. Учтите также, что в доменах с поддоменами для интеграции WINS и DNS поддоменам необходимо делегировать полномочия для служб именования.

Предметный указатель

Уильям Р. Станек

Microsoft Windows Server 2003. Справочник администратора

Перенод с английского под общей редакцией *Д. З. Вибе*

Переводчики *Д. З. Вибе, А. А. Вибе, И. М. Лебедев*

Редактор *Ю. П. Леонова*

Технический редактор *Н. Г. Тимченко*

Компьютерная верстка *В. Ю. Барыбин*

Дизайнер обложки *Е. В. Козлова*

Оригинал-макет выполнен с использованием издательской системы Adobe PageMaker 6.5

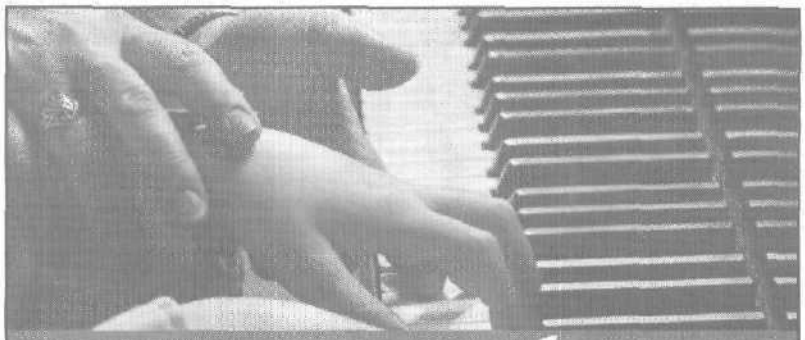
Главный редактор *А. И. Козлов*

Подготовлено к печати издательством «Русская Редакция»
121087, Москва, ул. Антонова-Овсеенко, д. 13
тел.: (095) 256-5120, тел./факс; (095) 256-4541
e-mail: info@rusedit.ru, http://www.rusediL.ru

РУССКАЯ РЕДАКЦИЯ

Подписано в печать 12.01.04 г. Тираж 3 000 экз.
Формат 84´108/32. Физ. п. л. 20

Отпечатано в ОАО «Типография «Новости»
105005, Москва, ул. Фр. Энгельса, 46



непрерывное обучение

как повысить отдачу от вложений в информационную инфраструктуру компании?

обучить специалистов в учебном центре softline

Даже грамотный специалист, занятый текущей работой, не в состоянии самостоятельно повышать свою квалификацию. Для этого у него нет ни времени, ни методических материалов. Только авторизованное обучение под руководством опытного инструктора позволяет эффективно на 100% использовать все возможности как IT-инфраструктуры, так и персонала компании.

Непрерывное обучение. Информационные технологии быстро меняются. Так же быстро *устаревают знания сотрудников. Мы предлагаем экономичный и эффективный способ* непрерывного обучения. Мы готовы разработать корпоративную программу обучения специально для сотрудников вашей компании.

Широкий набор курсов для профессионалов в области IT, которые хотят повысить свой уровень. Большое внимание уделяется вопросам построения правильной IT-инфраструктуры современной компании - вопросам безопасности, защиты данных, резервному копированию, администрированию сети и да.

Авторизованное обучение. SoftLine® является авторизованным учебным центром компаний Microsoft, Symantec, Citrix, VERITAS, и др.

Высокое качество обучения. Обучение ведут сертифицированные преподаватели по официальным методическим материалам. Высокое качество обучения подтверждается отзывами крупнейших компаний, входящих в ТОП 100 Российского рынка.

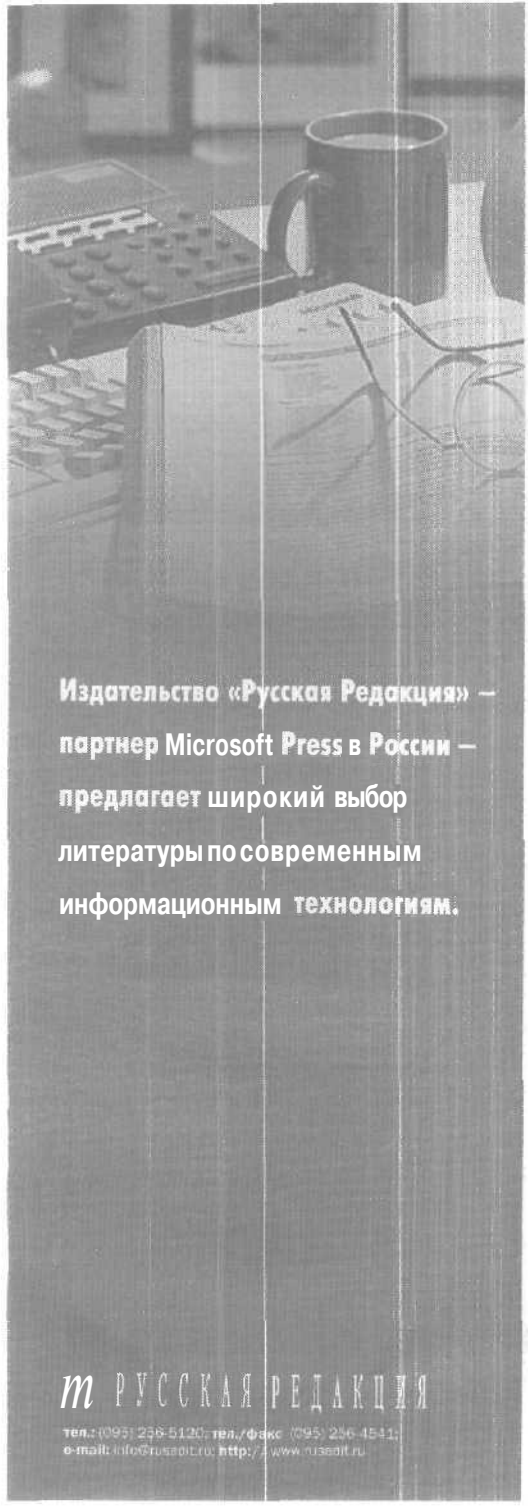
Корпоративные программы обучения. SoftLine® ориентируется на долгосрочные отношения с корпоративными клиентами. Мы предлагаем разработку непрерывной программы обучении сотрудников, которая позволит экономить ресурсы, выделяемые на обучение.

Обратитесь к консультантам учебного центра Анне Дмитраковой или Нине Доминго по тел.: +7(095)232-0023 и закажите бесплатный каталог учебных курсов.

softline®

программное обеспечение - лицензирование, обучение, консалтинг

+7(095)232-0023 www.softline.ru



Издательство «Русская Редакция» — партнер Microsoft Press в России — предлагает широкий выбор литературы по современным информационным технологиям.

РУССКАЯ РЕДАКЦИЯ

тел.: (095) 236-5120; тел./факс: (095) 236-4541;
e-mail: info@rusedit.ru; http://www.rusedit.ru

Наши книги Вы можете **приобрести**

- **в Москве:**

Специализированный магазин **«Компьютерная** и деловая **книга»**
Ленинский проспект, строение 38,
тел.: (095) 778-7269

«Библио-Глобус» ул. Мясницкая, 6,
тел.: (095) 928-3567

«Московский дом **книги»** ул. Новый Арбат, 8.
тел.: (095) 290-4507

«Дом технической книги» Ленинский пр-т, 40,
тел.: (095) 137-6019

«Молодая гвардия» ул Большая Полянка, 28,
тел : (095) 238-5001

«Дом книги на **Соколе»** Ленинградский пр-т, 73,
тел.: (095) 152-4511

«Дом книги на Войковской» Ленинградское ш .
13, стр. 1, тел.: (095) 150-6917

«Мир печати» ул 2-я Тверская-Ямская, 54.
тел.: (095) 978-5047

Торговый дом книги **«Москва»** ул Тверская, 8,
тел.: (095) 229-64B3

- **в Санкт-Петербурге:**

СПб Дом **книги,** Невский пр-т . 28
тел.: (812) 318-6402

СПб Двм военной книги, Невский пр-т., 20
Тел.:(812)312-0563. 314-7184

Магазин **«Подписные издания»**,
Литейный пр-т., 57. тел.: (812) 273-5053

Магазин **«Техническая** книга» ул. Пушкинская,
2, тел.: (812) 164-6565, 164-1413

Магазин **«Буквоед»**, Невский пр-т., 13.
тел.: (812) 312-6734

ЗАО «Торговый Двм «Диалект»,
тел.: (812) 247-1483

Оптово-розничный магазин «Наука и **техника»**,
тел.: (812) 567-7025

- **в Екатеринбурге:**

Магазин «Дом книги»,
ул. Валека, 12,
тел.: (3432) 59-4200

- **в Великом Новгороде:**

«Наука и техника».
ул. Большая Санкт-Петербургская, 44.
Дворец Молодежи, 2-й этаж

- **в Новосибирске:**

000 **«Топ-книга»**, тел.: (3832) 36-1026

- **в Алматы (Казахстан):**

ЧП Болат Амреев,
моб. тел.: 8-327-908-28-57. (3272) 76-1404

- **в Киеве (Украина):**

000 Издательство «Ирина-Пресс»,
тел.: (+1038044) 269-0423

«Техническая книга на **Петровке»**,
тел.: (+1038044) 268-5346

Microsoft®

Windows Server 2003

Справочник администратора

Компактный справочник по администрированию MicrosoftWindowsServer2003

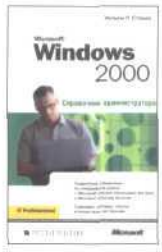
Это практическое пособие поможет быстро найти ответы на вопросы, возникающие при администрировании ОС семейства Microsoft Windows Server 2003 — будь в вашей сети хоть 50 пользователей, хоть 5000. Подробные таблицы, пошаговые инструкции и списки параметров позволяют мигом отыскать нужные сведения, благодаря чему время простоя сети сокращается до минимума.

Вы научитесь:

- управлять серверами Windows Server 2003;
- администрировать домены Active Directory, роли и организационные подразделения;
- автоматизировать решение административных задач посредством групповых политик;
- управлять доступом к системе посредством учетных записей пользователей и групп;
- устанавливать, настраивать и тестировать сети TCP/IP;
- использовать удаленный доступ;
- управлять файловыми системами, дисками, наборами томов и массивами RAID;
- оптимизировать производительность сервера и сети;
- настраивать DHCP, WINS и DNS;
- работать с сетевыми принтерами и серверами печати;
- настраивать шифрование, теневое копирование, синхронизацию времени и другие службы.

Издательство «Русская Редакция» представляет серию книг Microsoft Press

Справочник администратора (Administrator's Pocket Consultant)



Каждое издание серии объединяет в себе руководство по эксплуатации и подробный справочник по основным функциям и параметрам системы. Карманный справочник администратора — ваш идеальный помощник в повседневной работе!

ISBN 5-7502-0245-3

9 785750 202454

IT Professional

Web-узел издательства: **www.rusedit.ru**